Journal of applied logics (Print) ISSN 2631-9810
Journal of applied logics (Online) ISSN 2631-9829

Journal of Applied Logics

The IfCoLog Journal of Logics and their Applications

Volume 7 • Issue 4 • August 2020

Available online at
www.collegepublications.co.uk/journals/ifcolog/
Free open access

Journal of Applied Logics - IfCoLog
Journal of Logics and their Applications

Volume 7, Number 4

August 2020

Disclaimer

Statements of fact and opinion in the articles in Journal of Applied Logics - IfCoLog Journal of Logics and their Applications (JALs-FLAP) are those of the respective authors and contributors and not of the JALs-FLAP. Neither College Publications nor the JALs-FLAP make any representation, express or implied, in respect of the accuracy of the material in this journal and cannot accept any legal responsibility or liability for any errors or omissions that may be made. The reader should make his/her own evaluation as to the appropriateness or otherwise of any experimental technique described.

© Individual authors and College Publications 2020
All rights reserved.

ISBN 978-1-84890-343-2
ISSN (E) 2631-9829
ISSN (P) 2631-9810

College Publications
Scientific Director: Dov Gabbay
Managing Director: Jane Spurr

http://www.collegepublications.co.uk

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording or otherwise without prior permission, in writing, from the publisher.

Editorial Board

Editors-in-Chief
Dov M. Gabbay and Jörg Siekmann

Marcello D'Agostino
Natasha Alechina
Sandra Alves
Arnon Avron
Jan Broersen
Martin Caminada
Balder ten Cate
Agata Ciabttoni
Robin Cooper
Luis Farinas del Cerro
Esther David
Didier Dubois
PM Dung
David Fernandez Duque
Jan van Eijck
Marcelo Falappa
Amy Felty
Eduaro Fermé
Melvin Fitting
Michael Gabbay
Murdoch Gabbay
Thomas F. Gordon
Wesley H. Holliday
Sara Kalvala
Shalom Lappin
Beishui Liao
David Makinson
George Metcalfe
Claudia Nalon
Valeria de Paiva
Jeff Paris
David Pearce
Pavlos Peppas
Brigitte Pientka
Elaine Pimentel
Henri Prade
David Pym
Ruy de Queiroz
Ram Ramanujam
Chrtian Retoré
Ulrike Sattler
Jörg Siekmann
Jane Spurr
Kaile Su
Leon van der Torre
Yde Venema
Rineke Verbrugge
Heinrich Wansing
Jef Wijsen
John Woods
Michael Wooldridge
Anna Zamansky

Scope and Submissions

This journal considers submission in all areas of pure and applied logic, including:

pure logical systems
proof theory
constructive logic
categorical logic
modal and temporal logic
model theory
recursion theory
type theory
nominal theory
nonclassical logics
nonmonotonic logic
numerical and uncertainty reasoning
logic and AI
foundations of logic programming
belief change/revision
systems of knowledge and belief
logics and semantics of programming
specification and verification
agent theory
databases
dynamic logic
quantum logic
algebraic logic
logic and cognition
probabilistic logic
logic and networks
neuro-logical systems
complexity
argumentation theory
logic and computation
logic and language
logic engineering
knowledge-based systems
automated reasoning
knowledge representation
logic in hardware and VLSI
natural language
concurrent computation
planning

This journal will also consider papers on the application of logic in other subject areas: philosophy, cognitive science, physics etc. provided they have some formal content.

Submissions should be sent to Jane Spurr (jane@janespurr.net) as a pdf file, preferably compiled in LaTeX using the IFCoLog class file.

Contents

ARTICLES

Extending Ideas of Tait for Incorporating Higher-order Parameters in Schemes of Reflection **391**
Rupert McCallum

Measuring Inconsistency in Finitary First-order Logic **403**
John Grant

Some Applications of Boolean Valued Analysis **427**
A. G. Kusraev and S. S. Kutateladze

The Γ-ultraproduct and Averageable Classes **459**
Will Boney

Fragments of Quasi-Nelson: Two Negations **499**
Umberto Rivieccio

Optimal Polynomial-time Estimators: A Bayesian Notion of Approximation Algorithm **561**
Vanessa Kosoy and Alexander Appel

Extending Ideas of Tait for Incorporating Higher-order Parameters in Schemes of Reflection

Rupert McCallum
University of Tübingen
rupertmccallum@yahoo.com

Abstract

We formulate a new reflection principle which subsumes all of the reflection principles which were considered by Tait and Koellner and are also known to be consistent, and which is itself consistent relative to an ω-Erdős cardinal (because equivalent to the existence of a remarkable cardinal). The author was supported by the research grant DE 436/10-1 from Deutsche Forschungsgemeinschaft, while working at the University of Tübingen. Ralf Schindler provided very helpful assistance with identifying errors in earlier versions of the paper and providing a useful characterisation of remarkable cardinals which greatly simplified the argument that a cardinal is extremely reflective if and only if it is remarkable.

1 The reflection principles of Tait, and α-reflective cardinals

It is well known, and was first observed in [15], that a schema asserting reflection for first-order formulas with parameters – that is, that for each formula $\phi(x_1, x_2, \ldots x_n)$ we have the axiom that if $\phi(x_1, x_2, \ldots x_n)$ then $(\phi(x_1, x_2, \ldots x_n))^{V_\alpha}$ for some ordinal α such that $x_1, x_2, \ldots x_n \in V_\alpha$ – is implied by ZF. A slightly stronger version asserting for each formula $\phi(x_1, x_2, \ldots x_n)$ that there is a proper class of ordinals α such that, for all $x_1, x_2, \ldots x_n \in V_\alpha, \phi(x_1, x_2 \ldots x_n) \equiv (\phi(x_1, x_2, \ldots x_n))^{V_\alpha}$, is equivalent, given Extensionality, Separation, and Foundation, to ZF. The philosophical issues become more problematic when we consider whether we can meaningfully speak of higher-order properties of the universe and whether we should regard as justified reflection principles which reflect some higher-order property of the universe V down to a level V_α, or which posit the existence of a level V_κ such that all higher-order properties of

a certain kind are reflected down to some level V_β with $\beta < \kappa$, where β may perhaps depend on which property is being reflected. We shall gloss over the philosophical part of the discussion here and refer the reader to Tait's discussion in [5], contenting ourselves here with simply describing the various higher-order reflection principles that may be proposed.

If we consider reflection of higher-order formulas with second-order parameters, we arrive at various types of indescribable cardinals. For example, if κ is such that whenever any Π^n_m-formula ϕ with one free second-order variable X holds relative to V_κ (that is, type n variables are relativized to $V_{\kappa+n}$) for a particular value A of the free variable X, then there is always some $\beta < \kappa$ such that ϕ holds relative to V_β when $A \cap V_\beta$ is substituted for X, then such a cardinal κ is said to be Π^n_m-indescribable. There are various other natural generalizations of the notion of indescribability, all involving reflection with second-order parameters only. But when we move to third-order parameters and higher we encounter a difficulty: unrestricted reflection with such parameters leads to inconsistency, as was first observed by Reinhardt in [16]. A proof can be found on page 276 of [19].

If we are to countenance some forms of higher-order reflection involving parameters of third order or higher then what principled reasons can we offer for distinguishing it from those forms of reflection with such parameters which are known to be inconsistent? It is at this point in our discussion where we start to consider the large cardinals considered in [5] and [12].

Let us consider what Tait writes in [5] on the question of how to justify special cases of reflection with parameters of third and higher order.

"One plausible way to think about the difference between reflecting $\varphi(A)$ when A is second-order and when it is of higher-order is that, in the former case, reflection is asserting that, if $\varphi(A)$ holds in the structure $\langle R(\kappa), \in, A\rangle$, then it holds in the substructure $\langle R(\beta), \in, A^\beta\rangle$ for some $\beta < \kappa \ldots$ But, when A is higher-order, say of third-order this is no longer so. Now we are considering the structure $\langle R(\kappa), R(\kappa{+}1), \in, A\rangle$ and $\langle R(\beta), R(\beta{+}1), \in, A^\beta\rangle$. But, the latter is not a substructure of the former, that is the 'inclusion map' of the latter structure into the former is no longer single-valued: for subclasses X and Y of $R(\kappa), X \neq Y$ does not imply $X^\beta \neq Y^\beta$. Likewise for $X \in R(\kappa{+}1), X \notin A$ does not imply $X^\beta \notin A^\beta$. For this reason, the formulas that we can expect to be preserved in passing from the former structure to the latter must be suitably restricted and, in particular, should not contain the relation $\notin$ between second- and third-order objects or the relation $\neq$ between second-order objects."

He then uses these ideas to motivate the following family of reflection principles.

Definition 1.1. A formula in the nth-order language of set theory, for some $n < \omega$, is positive iff it is built up by means of the operations $\vee$, $\wedge$, $\forall$, $\exists$ from atoms of the form $x = y$, $x \neq y$, $x \in y$, $x \notin y$, $x \in Y^{(2)}$, $x \notin Y^{(2)}$ and $X^{(m)} = X'^{(m)}$ and $X^{(m)} \in Y^{(m+1)}$, where $m \geq 2$.

Definition 1.2. For a first-order or second-order variable A, and a finite ordinal n, we define $A_{n\times} = \{\langle n, x\rangle \mid x \in A\}, A_{/n} = \{x \mid \langle n, x\rangle \in A\}$, and for variables B of order greater than the second we define, by induction on the order of the variable, $B_{n\times} = \{X_{n\times} \mid X \in B\}, B_{/n} = \{X_{/n} \mid X \in B\}$, and for A and B of the same order $A + B = A_{0\times} \cup B_{1\times}$. Compositions of these operations are called contracting operations, and a formula is said to be positive in the extended sense if it is obtained from a positive formula by substitution for free variables of terms involving contracting operations.

Definition 1.3. For $0 < n < \omega$, $\Gamma^{(2)}_n$ is the class of formulas

$$\forall X_1^{(2)} \exists Y_1^{(k_1)} \dots \forall X_n^{(2)} \exists Y_n^{(k_n)} \varphi(X_1^{(2)}, Y_1^{(k_1)}, \dots, X_n^{(2)}, Y_n^{(k_n)}, A^{(l_1)}, \dots A^{(l_{n'})})$$

where φ is positive in the extended sense and does not have quantifiers or second or higher-order and $k_1, \dots k_n, l_1, \dots l_{n'}$ are natural numbers.

Definition 1.4. We say that V_κ satisfies $\Gamma^{(2)}_n$-reflection if, for all $\varphi \in \Gamma^{(2)}_n$, if $V_\kappa \models \varphi(A^{(m_1)}, A^{(m_2)}, \dots A^{(m_p)})$ then $V_\kappa \models \varphi^\delta(A^{(m_1),\delta}, A^{(m_2),\delta}, \dots A^{(m_p),\delta})$ for some $\delta < \kappa$.

Peter Koellner established in [8] that these reflection principles are consistent relative to an ω-Erdős cardinal. In [5] Tait proposes to define $\Gamma^{(m)}_n$ in the same way as the class of formulas $\Gamma^{(2)}_n$, except that universal quantifiers of order $\leq m$ are permitted. Koellner shows in [8] that this form of reflection is inconsistent when $m > 2$.

This raises the issue of whether we have principled grounds for refusing to accept those reflection principles of Tait which Peter Koellner proved to be inconsistent. In [12] I suggested a possible motivation for this. Given a formula in the higher-order language of set theory, it is possible to introduce Skolem functions and re-write it as a formula with universal quantifiers alone and the Skolem functions as parameters. Then just as Tait appealed to the idea that the inclusion map of a structure $(V_\beta, V_{\beta+1}, \in)$ into a structure $(V_\kappa, V_{\kappa+1}, \in)$ is not single-valued when $\beta < \kappa$

as a motivation for refusing to accept a "naive" form of third-order reflection which is easily proved to be inconsistent, so we can appeal to the idea that the Skolem functions witnessing the truth of a higher-order formula in V_κ may cease to be single-valued when we reflect down to V_β, to motivate refusing to accept those reflection principles of Tait which Koellner proved to be inconsistent. But on the other hand this still allows for plausible motivations to be given for the reflection principles discussed in [12] and the present paper.

In [12] I proposed the following large-cardinal axiom and attempted to provide motivation for it based on the ideas above.

Definition 1.5. We define $l(\gamma) = \gamma - 1$ if $0 < \gamma < \omega$ and $l(\gamma) = \gamma$ otherwise. We extend the definition $A^{(m+1),\beta} = \{B^{(m),\beta} \mid B^{(m)} \in A^{(m+1)}\}$ to $A^{(\alpha),\beta} = \{B^\beta \mid B \in A^{(\alpha)}\}$ for all ordinals $\alpha > 0$, it being understood that if V_κ is the domain of discourse then $A^{(\alpha)}$ ranges over $V_{\kappa+l(\alpha)}$.

Definition 1.6. Suppose that α, κ are ordinals such that $0 < \alpha < \kappa$ and that

(1) $S = \langle \{V_{\kappa+\gamma} \mid \gamma < \alpha\}, \in, f_1, f_2, \dots f_k, A_1, A_2, \dots A_n\rangle$ is a structure where each f_i is a function $V_{\kappa+l(\gamma_1)} \times V_{\kappa+l(\gamma_2)} \times \dots V_{\kappa+l(\gamma_i)} \to V_{\kappa+\zeta_i}$ for some ordinals $\gamma_1, \gamma_2, \dots \gamma_i, \zeta_i$ such that $l(\gamma_1), l(\gamma_2), \dots l(\gamma_i) < \alpha, 0 < \zeta_i < \alpha$, and each A_i is a subset of $V_{\kappa+\delta_i}$ for some $\delta_i < \alpha$
(2) φ is a formula true in the structure S, of the form
$\forall X_1^{(\gamma_1)} \forall X_2^{(\gamma_2)} \dots \forall X_k^{(\gamma_k)}$
$\psi(X_1^{(\gamma_1)}, f_1(X_1^{(\gamma_1)}), X_2^{(\gamma_2)}, f_2(X_1^{(\gamma_1)}, X_2^{(\gamma_2)}), \dots X_k^{(\gamma_k)}, f_k(X_1^{(\gamma_1)}, X_2^{(\gamma_2)}, \dots X_k^{(\gamma_k)}),$
$A_1, A_2, \dots A_j)$ with ψ a formula with first-order quantifiers only
(3) there exists a β such that $\alpha < \beta < \kappa$ and a mapping $j : V_{\beta+\alpha} \to V_{\kappa+\alpha}$, such that $j(X) \in V_{\kappa+\gamma}$ whenever $X \in V_{\beta+\gamma}$, $j(X) = X$ for all $X \in V_\beta$, and $j(X) \in j(Y)$ whenever $X \in Y$, and such that, in the structure
$S^\beta = \langle V_\beta, \{V_{\beta+\gamma} \mid 0 < \gamma < \alpha\}, \{V_{\kappa+\gamma} \mid 0 < \gamma < \alpha\}, \in, j, f_1, f_2, \dots f_k, A_1, A_2 \dots A_n\rangle$, with variables of order γ ranging over $V_{\beta+l(\gamma)}$, we have

$(*)\forall X_1^{(\gamma_1)} \forall X_2^{(\gamma_2)} \dots \forall X_k^{(\gamma_k)}$
$\psi(j(X_1^{(\gamma_1)}), f_1(j(X_1^{(\gamma_1)})), j(X_2^{(\gamma_2)}), f_2(j(X_1^{(\gamma_1)}), j(X_2^{(\gamma_2)})), \dots j(X_k^{(\gamma_k)}),$
$f_k(j(X_1^{(\gamma_1)}), j(X_2^{(\gamma_2)}), \dots j(X_k^{(\gamma_k)})), A_1, A_2, \dots A_n)$

Then we say that the formula φ with parameters $A_1, A_2, \dots A_n$ reflects down from S to β. If for all structures S of the above form and for all formulas φ of the above form

true in the structure S, this occurs for some $\beta < \kappa$, then κ is said to be α-reflective. [1]

Since in this definition I have introduced a mapping j to guide the reflection it may be questioned whether it still deserves to be called a reflection principle. I tried to motivate the acceptance of the existence of cardinals satisfying the above large-cardinal property as intrinsically justified by deriving it from yet another large-cardinal property. Specifically one may introduce the notion of an α-hyper-reflective cardinal for $\alpha > 0$. We do this by means of a definition identical to Definition 1.6, except that we have the higher-order variables of order γ in (*) of Definition 1.6 range over $V_{\kappa+l(\gamma)}$ rather than $V_{\beta+l(\gamma)}$, and remove reference to the mapping j. It is also necessary to require that the formula being reflected not contain subformulas of the form $X = Y$ for variables X, Y of order at least second order, in order for the resulting reflection principle to be consistent, this point was not noticed in [12]. One can then proceed to prove (assuming the axiom of choice) that an α-hyper-reflective cardinal is α-reflective. It is more plausible to think of an axiom positing the existence of an α-hyper-reflective cardinal as a reflection principle.

The choice of the term "hyper-reflective" is unfortunate; it is actually not hard to construct an argument that a cardinal κ is α-reflective if and only if it is α-hyper-reflective, for any ordinal α such that $0 < \alpha < \kappa$.

Lemma 1.7. For each ordinal $\alpha > 0$, a cardinal κ is α-hyper-reflective if and only if it is α-reflective.

Proof. The forward direction is easy. For the other direction, suppose that κ is α-reflective. Suppose that we have a formula of the form (*) in Definition 1.6, together with parameters corresponding to the free variables in the formula, including the variables for the Skolem functions, and satisfying the constraint that the formula has no subformula of the form $X = Y$ for formulas of at least second order, and that a mapping j witnesses that this formula reflects down to β for those parameters. Let us replace the Skolem functions with their restrictions to the range of the mapping j, we shall show that these restricted Skolem functions can be extended to Skolem functions on the entire domains of discourse for the higher-order variables such that the cardinal κ satisfies the definition of α-hyper-reflectiveness for the formula in

[1] At the time of writing [12] I was under the impression that the phrase "α-reflective cardinal" had not been used previously. This turned out not to be correct. Dmytro Taranovsky had introduced a completely different notion of "α-reflective cardinal" independently in a paper "Higher Order Set Theory with Reflective Cardinals" which at the time of writing is available on-line at http://web.mit.edu/dmytro/www/ReflectiveCardinals.htm. It should be emphasised that my notion of "α-reflective cardinal" is completely different to the notion introduced in Taranovsky's paper.

question with that choice of tuple of Skolem functions and other parameters, and if that can be shown for an arbitrary initial choice of formula and parameters, then that is sufficient to show that κ satisfies the definition of α-hyper-reflectiveness in general. Assume the mapping j and the ordinal β chosen so that the mapping j will witness that all other formulas of the form (*) – with the same number of initial higher-order quantifiers and the same free variables including Skolem function variables – are also reflected down to the same β for the original choice of parameters and Skolem functions. It can be seen that such a choice of j and β is possible, by considering the existence of a truth predicate for the class of formulas of the type being discussed, and applying the definition of being α-reflective to a formula involving that truth predicate. We shall show that on these assumptions it is always possible to extend the Skolem functions to the entire range of possible values for the appropriate higher-order variables, in such a way that the resulting choice of Skolem functions witnesses that the cardinal κ satisfies the definition of being α-hyper-reflective for that particular choice of formula and parameters and Skolem functions, and as observed before showing that this is true regardless of the initial choice of formula and Skolem functions and parameters is sufficient to prove the theorem.

Suppose that we are given an interpretation for each of the higher-order variables which appear in universally quantified form at the start of the original formula of the form (*), where not every value of such a higher-order variable is in the range of the mapping j. To extend the Skolem functions to every such tuple of values for the higher-order variables, use the values of the Skolem functions for tuples of elements of the range of j as a guide. Assume that we are trying to determine what the value of the Skolem function $f_n(X_1, X_2, \ldots X_k)$ should be, and assume as an induction hypothesis that we have already chosen values for $f_m(X_1, X_2, \ldots X_j)$ for $m < n$, and parameters $k(X_1), k(X_2), \ldots k(X_{k-1})$ in the range of the mapping j, such that any first-order formula with higher-order parameters is true of a tuple of parameters chosen from $\{X_1, f_1(X_1), X_2, f_2(X_1, X_2), \ldots X_{n-1}, f_{n-1}(X_1, X_2, \ldots X_{n-1})\}$ if and only if it is true of the corresponding tuple of parameters from $\{k(X_1)$, $f_1(k(X_1)), k(X_2), f_2(k(X_1), k(X_2)), \ldots k(X_{n-1}), f_{n-1}(k(X_1), k(X_2), \ldots$ $k(X_{n-1}))\}$. Then by our assumptions on the mapping j we can choose values for $k(X_n)$ and $f_k(X_1, X_2, \ldots X_n)$ so that the induction step goes through. If we use a well-ordering on the set of all possible tuples of parameters, so as to ensure that the the Skolem functions are always defined in this way for every possible tuple of parameters, then these Skolem functions will witness that κ satisfies the definition of being α-hyper-reflective for this particular formula and choice of parameters, and the initial choice of formula and Skolem functions and parameters was arbitrary. As

observed previously, this is sufficient to prove that every α-reflective cardinal is α-hyper-reflective, completing the proof of equivalence between the two properties. □

In [12] I gave a proof of the consistency of these large cardinals relative to an ω-Erdős cardinal. In the next section I want to extend this program further by formulating a stronger reflection principle and giving a consistency proof for it.

2 The new reflection principle

We begin by presenting one version of the new reflection principle, a natural generalization of the notion of an α-hyper-reflective cardinal.

Definition 2.1. A cardinal κ is said to be extremely reflective if, for each ordinal $\lambda > \kappa$, considering structures of the form $(V_\kappa, V_\lambda \setminus V_\kappa)$ and formulas ϕ in a two-sorted language holding in such a structure, of the same form as the formulas considered in the definition of α-hyper-reflective cardinal except that variables of at least second order are replaced with variables of the second sort, each such formula reflects down to some $\beta < \kappa$ in the same sense as in the definition of α-hyper-reflective cardinal. (Here we must recall that the constraint that the reflected formula has no subformula of the form $X = Y$ where X and Y are variables of the second sort is necessary.)

We now present an alternative definition of the same concept and then briefly indicate how one can prove that the two definitions are equivalent.

Definition 2.2. Suppose that κ is a cardinal with the following property. For any ordinal $\eta > \kappa$, and for any formula ϕ of the form described in the previous definition, there exists an ordinal $\lambda_\eta < \kappa$, and a family of sets $M_{\phi,a}$ (not necessarily transitive) for all $a \in V_\eta \setminus V_\kappa$, with $\mathrm{Card}(M_{\phi,a}) \leq \lambda_\eta$, and mappings $j_{\phi,a} : M_{\phi,a} \to V_\eta$, for each $a \in V_\eta \setminus V_\kappa$, such that $V_{\lambda_\eta} \cup \{\lambda_\eta\} \subseteq M_{\phi,a}$ for all $a \in V_\eta \setminus V_\kappa$, $\bigcup_{a \in V_\eta \setminus V_\kappa} M_{\phi,a} = V_{\rho_\eta}$ for some ρ_η, and for all $a \in V_\eta \setminus V_\kappa$ the mapping $j_{\phi,a}$ is elementary from $(V_{\lambda_\eta}, M_{\phi,a} \setminus V_{\lambda_\eta})$ into $(V_\kappa, V_\eta \setminus V_\kappa)$, for all formulas of the same form as ϕ (that is, the form described in the previous definition, with the constraint on subformulas of the form $X = Y$) such that the number of free variables (including free variables for Skolem functions) is no greater than that of ϕ, with critical point λ_η and such that $j_{\phi,a}(\lambda_\eta) = \kappa$, and $a \in \mathrm{range}(j_{\phi,a})$. We also require that given any n-tuple $(a_1, a_2, \ldots a_n)$ the mapping $j_{\phi,(a_1,a_2,\ldots a_n)}$ has domain containing the domains of $j_{\phi,a_1}, j_{\phi,a_2}, \ldots j_{\phi,a_n}$ and agrees with the map j_{ϕ,a_k} at a_k for each k such that $1 \leq k \leq n$. If κ has this property then κ is said to be an extremely reflective cardinal.

Using a similar argument to the one used to show that a cardinal is α-hyper-reflective if and only if it is α-reflective, together with the use of Skolem hulls, the first definition can be shown to be equivalent to the second one. To show that the first definition implies the second, use a sequence of formulas each of which is universal for a given level of complexity, and choose a sequence of families of Skolem functions for each such formula such that the families of Skolem functions in the sequence and consistent with one another, and use these families of Skolem functions to construct the maps $j_{\phi,a}$. It may not be immediately obvious that λ_η can be chosen independently of ϕ, but simply choose it to be as small as possible for each ϕ, then it can be easily seen that the resulting ordinal is independent of ϕ. To show that it is possible to choose the $M_{\phi,a}$ in such a way that $\bigcup_{a \in V_\eta \setminus V_\kappa} M_{\phi,a} = V_{\rho_\eta}$, consider that each $M_{\phi,a}$ could be embedded in an M constructed from a Skolem hull of larger cardinality but still of smaller cardinality than $\beth_\kappa$, so that $V_{\delta+1} \in M$ where $j(\delta) = \text{rank}(a)$, j being the mapping corresponding to the Skolem hull M. This indicates how it can be shown that the first definition implies the second, and it can be shown that the second implies the first using similar reason to that used to show that every α-reflective cardinal is α-hyper-reflective.

It can be shown that this reflection principle subsumes all the ones considered in [5], [8], and [12]. In fact it can be shown that an extremely reflective cardinal κ is α-reflective for all ordinals α such that $0 < \alpha < \kappa$ (and is a stationary limit of cardinals with this property). This point can easily be argued making use of the first definition given.

One easy upper bound for the consistency strength of an extremely reflective cardinal is that every supercompact cardinal is extremely reflective. This can be shown using Magidor's characterisation of supercompactness. It is also not hard to show that a measurable cardinal is a stationary limit of extremely reflective cardinals.

Before proceeding further, we note two errata in [12]. In the proof of Theorem 2.5 of [12] it is said that given any closed unbounded subset $C \subseteq \kappa(\omega)$, where $\kappa(\omega)$ is the first ω-Erdős cardinal, one may choose an ω-sequence of indiscernibles for any structure $\mathcal{S}$ with domain of discourse $V_{\kappa(\omega)}$ which lie in C. More needs to be said for the argument to work. It must be required that it be possible to choose the set of indiscernibles $I \subseteq C$ in such a way that each element of I is a critical point of an elementary embedding from the Skolem hull of I in $\mathcal{S}$ into itself. Fortunately this is possible as well. Further it was claimed that $\kappa(\omega)$ is a stationary limit of remarkable cardinals. What should have been said is that it is a stationary limit of cardinals κ with the property that $V_{\kappa(\omega)} \models$ "κ is remarkable". This result is Lemma

1.2 of [10]. Having noted these errata, we now proceed to the next result, showing that the property of being extremely reflective is in fact equivalent to the property of being remarkable.

Theorem 2.3. *A cardinal is extremely reflective if and only if it is remarkable.*

Proof. This is a corollary of the second definition given of "extremely reflective cardinal", and the following characterisation of remarkable cardinals which Ralf Schindler communicated to me in private email correspondence.

Let κ be an infinite cardinal. We consider two two-player games. The first one will be denoted by G^1_κ. Player I plays an ordinal $\alpha > \kappa$, player II plays two ordinals λ, β such that $\lambda < \beta < \kappa$, then from then on Player I plays elements $x_0, x_1, \ldots$ of V_β and Player II plays elements $y_0, y_1, \ldots$ of V_α, and player II wins if she is not the first one to break the following rules: $x_k \in V_\lambda \implies y_k = x_k$, and for every formula ϕ in the language of set theory and for all $k < \omega$, $V_\beta \models \phi(\lambda, x_0, \ldots x_{k-1}) \equiv V_\alpha \models \phi(\kappa, y_0, \ldots y_{k-1})$. The second game is denoted G^{crit}_κ, and this time after the first two moves, Player I plays X_0, Player II plays j_0, Player I plays X_1, Player II plays j_1, and so on, and the rules are $X_0 \subset X_1 \subset \ldots \subset V_\beta, j_0 \subset j_1 \subset \ldots$, and for all $k < \omega$, $\mathrm{Card}(X_k) \leq \lambda$, $j_k : X_k \to V_\alpha$, $j_k \restriction X_k \cap V_\lambda = \mathrm{id}$, and for every formula ϕ in the language of set theory, for all $n < \omega$, and for all $x_0, x_1, \ldots x_n \in X_k$, $V_\beta \models \phi(\lambda, x_0, x_1, \ldots x_n) \equiv V_\alpha \models \phi(\kappa, j_k(x_0), j_k(x_1), \ldots j_k(x_n))$. Again Player II wins if she is the first one not to break any rule. Ralf Schindler has shown that κ being remarkable is equivalent to Player II having a winning strategy in G^1_κ, which is in turn equivalent to Player II having a winning strategy in G^{crit}_κ. This charactrisation of remarkable cardinals was known to Schindler at the time that [18] appeared, and is in the spirit of Section 4 of that paper.

Using this characterisation of remarkable cardinals and our previous characterisation of extremely reflective cardinals, it can be shown that the two concepts are equivalent. If we assume that κ is remarkable in the sense just given then it is easy to see that κ is extremely reflective according to our second definition, and the converse is easy to show too, namely the winning strategy for player II in G^1_κ is the one whereby she plays $y_i := j_{\phi,(x_0,x_1,\ldots x_i)}(x_i)$ where ϕ has a sufficiently large number of free variables. Any violation of the rules would then witness a failure of the defining property for some $j_{\psi,b}$ with $x_0, x_1, \ldots x_i \in \mathrm{dom}\ j_{\psi,b}$ and ψ having enough free variables to cover both the complexity of the formula for which the rules are broken as well as all the free variables in that formula.

□

It now follows by Lemma 1.2 of [10] that extremely reflective cardinals are consistent relative to an ω-Erdős cardinal.

Reflection principles stronger than an ω-Erdős cardinal have been proposed by Welch and Roberts in [1] and [2] in response to Peter Koellner's challenge to formulate an intrinsically justified reflection principle with that level of consistency strength. In particular, Sam Roberts has formulated a reflection principle which implies a proper class of 1-extendible cardinals, and along lines which I will indicate in a different forthcoming paper on the topic, this line of thought can be taken at least up to the level of a supercompact cardinal. For attempted justifications from notions of reflection of still stronger large cardinals, in [17] Victoria Marshall motivates increasingly strong theories from notions of reflection which go all the way up to inconsistency with the axiom of choice. Whether principled reasons could be offered for stopping short of the point of inconsistency with choice would be an interesting topic to explore. This work has given an indication of how a certain kind of reflection principle can be extended up the point of remarkable cardinals. In other work we hope to take a more comprehensive look at the relations between reflection principles of the weak kind described here and the stronger reflection principles of the kind proposed by Welch and Roberts.

References

[1] Philip Welch. Obtaining Woodin's Cardinals. In *Logic in Harvard: Conference celebrating the birthday of Hugh Woodin,* eds. A. Caicedo, J. Cummings, P. Koellner & P. Larson, AMS Series, Contemporary Mathematics, vol. 690, 161-176, May 2017.

[2] Sam Roberts. A strong reflection principle. *The Review of Symbolic Logic,* vol. 10, Issue 4: 651 – 662, 2017.

[3] Neil Barton and Sy-David Friedman. Maximality and Ontology: How axiom content varies across philosophical frameworks, pre-print.

[4] William Tait. *The Provenance of Pure Reason: Essays In the Philosophy of Mathematics and Its History.* Oxford University Press, 2005.

[5] William Tait. Constructing Cardinals from Below. In [4], Oxford University Press, 2005, pp. 133–154.

[6] Thomas Forster. The Iterative Conception of Set, *The Review of Symbolic Logic* p. 97, vol. 1, no. 1, June 2008.

[7] Peter Koellner. The Search for New Axioms, Ph.D. thesis, 2003, Massachusetts Institute of Technology.

[8] Peter Koellner. On Reflection Principles, *Annals of Pure and Applied Logic,* vol. 157, Issues 2–3, pp. 206–219, 2009.

[9] Ralf Schindler. Proper Forcing and Remarkable Cardinals, *The Bulletin of Symbolic Logic* vol. 6, Issue 2, pp. 176–184. 2000.

[10] Ralf Schindler. Proper Forcing and Remarkable Cardinals II, *Journal of Symbolic Logic,* vol. 66, Issue 3, 1481-1492, 2001.

[11] Victoria Gitman and Ralf Schindler. Virtual Large Cardinals, pre-print.

[12] Rupert McCallum. A Consistency Proof for Some Restrictions of Tait's Reflection Principles, *Mathematical Logic Quarterly,* vol. 59, Issues 1–2, pp. 112–118, 2013.

[13] Kurt Gödel, *Collected Works, Volume II: Publications 1938-1974,* Oxford Univeristy Press, New York and Oxford, 1990, eds. Solomon Feferman, John W. Dawson, Jr., Stephen C. Kleene, Gregory H. Moore, Robert M. Solovay, and Jean van Heijenoort.

[14] Kurt Gödel. What is Cantor's continuum problem? In [13], pp. 254–270.

[15] Azriel Lévy. Axiom schemata of strong infinity in axiomatic set theory, *Pacific Journal of Mathematics* vol. 10, pp. 223–238, 1960.

[16] W. Reinhardt. Remarks on reflection principles, large cardinals, and elementary embeddings. In *Proceedings of symposia in pure mthematics,* vol. 10, pp. 189–205, 1974.

[17] M. Victoria Marshall R. Higher order reflection principles, *Journal of Symbolic Logic,* vol. 54, no. 2, pp. 474–489, 1989.

[18] Bagaria, J., Gitman, V., and Schindler, R. Generic Vopěnka's Principle, Remarkable cardinals, and the weak Proper Forcing Axiom. *Archive for Mathematical Logic,* vol. 56, Issue 1-2, pp. 1-20, 2017.

[19] Frank Drake. Set Theory: An Introduction to Large Cardinals. North-Holland Publishing Company, 1974.

 Received 7 December 2018

Measuring Inconsistency in Finitary First-Order Logic

John Grant
University of Maryland, College Park, USA
grant@cs.umd.edu

To: Jack Minker, my mentor and friend

Abstract

Since the early 2000s, researchers in logic and AI have developed a framework for measuring inconsistency in information. They proposed inconsistency measures as well as desirable properties for them and dealt with related issues. AI researchers are interested in this topic because some intelligent systems need to handle inconsistencies. However, the bulk of the research has been done for propositional knowledge bases, that is, finite sets of formulas in propositional logic. But much of the information that intelligent systems deal with, such as databases, use first-order logic formulas. The purpose of this paper is to extend inconsistency measuring to finite sets of first-order logic formulas. We propose five different measures and explain the rationale for each. Furthermore, we extend some of the properties proposed for propositional inconsistency measures to first-order logic and introduce several new properties appropriate for first-order logic. We show the satisfaction or violation of each property for each measure.

1 Introduction

Classical logic follows a rule stated in Latin as *ex contradictione quodlibet*, meaning that from a contradiction everything follows. This makes every set of inconsistent formulas trivial. Some logicians think that as a practical matter this rule is too strong. For this reason, many different paraconsistent logics [3], logics that do not follow *ex contradictione quodlibet*, have been proposed and studied. The issue has also been of interest to AI researchers, as some intelligent systems must deal with inconsistent information.

The first mention of the concept of measuring inconsistency was in [2]. That paper presented several ways of classifying the inconsistency of a set of formulas in

first-order logic. The first work that proposed a specific inconsistency measure was [7]. It defined an inconsistency measure that can be applied to any set of formulas in propositional logic. Since that time, numerous other measures have also been proposed. However, there is no general agreement about which, if any, is the best method. In this paper we use [12], which surveys most of this work. In fact, it gives the definitions for 22 inconsistency measures including the most popular ones. Due to the proliferation of proposed inconsistency measures, some researchers proposed properties, called rationality postulates, that a "good" inconsistency measure should satisfy. In fact, [12] defines 18 such properties but there is also no consensus about which of these should be required.

A significant limitation of such past work is that almost all of it deals only with formulas in propositional logic. But the information that AI systems deal with usually comes from various databases and other knowledge that can be represented in first-order logic, but not in propositional logic. The purpose of this paper is to define inconsistency measures that are appropriate for first-order logic formulas, thereby greatly expanding the applicability of previous work. It turns out that some of the propositional inconsistency measures can be extended to first-order logic in a straightforward manner. The problem is that such extensions do not handle quantification appropriately. For that, one needs an inconsistency measure defined specifically for first-order logic. However, we keep one important consideration from propositional logic: finiteness. While we do not use a specific finite bound, we will deal only with finite sets. In this respect, we follow the basic concepts of finite model theory, [8], a topic that has been investigated both in mathematical logic and computer science, particularly in database theory and computational complexity. The reason for the finiteness assumption in our case is that the existence of models of various infinite cardinalities impedes inconsistency measurement: such measures have finite values with a single infinity in special cases. Thus, in our setting everything is finite: the number of symbols in the language, the length of a formula (this is a feature of first-order logic but worth mentioning), the number of formulas (in the set under consideration), and the size of the models.

The plan of this paper is as follows. In Section 2 we review the basic definitions of inconsistency measuring in propositional logic, including some inconsistency measures and rationality postulates. Section 3 contains the syntax of and semantics of first-order logic in our setting. Then, Section 4 describes a finitary 3-valued semantics that will be used to define several inconsistency measures for first-order logic. In Section 5 we rephrase the propositional rationality postulates for our first-order setting and add new postulates appropriate for first-order logic inconsistency measures. Section 6 defines what we consider our main inconsistency measure for first-order logic formulas, fI, and then Section 7 shows which rationality postulates

in our list fI satisfies. The following four sections each define and study an additional inconsistency measure for first-order logic: Section 8 has a "weak" version of fI; Section 9 has a measure based on minimal inconsistent subsets; Section 10 counts only relations; and Section 11 is a relative measure that considers the ratio of the inconsistency with the total possible amount. The paper is summarized in Section 12.

2 Measuring Inconsistency in Propositional Logic

This section reviews work done on measuring inconsistency in propositional logic that is relevant to this paper. We refer to [12] for a thorough treatment of this topic. Essentially, an inconsistency measure is a function that can be applied to any finite set of propositional logic formulas, whose result is a nonnegative number or infinity. The idea is that the result is the inconsistency of the given set. In particular, this allows for the comparison of two such sets of formulas with respect to their inconsistency.

We start with a propositonal logic language that contains an unbounded finite set of atoms (propositions), and the propositional connectives $\neg$, $\wedge$, and $\vee$, as well as parentheses. Formulas are formed in the usual way. In this section we use α for a formula and A for a finite set of formulas. We write $\mathsf{Atoms}(\mathrm{A})$ for the set of atoms in A.

A classical interpretation i for A assigns each atom the truth value T or F; that is, $i : \mathsf{Atoms}(A) \to \{T, F\}$. Such an interpretation is extended to all propositional logic formulas in the usual way, using the truth tables for the connectives. We say that i *satisfies* α just in case the assignment of the truth values given by i makes α true. Then, i *satisfies* A iff i satisfies α for all $\alpha \in A$. A is *consistent* if there is an interpretation i that satisfies it; otherwise A is *inconsistent*. A *minimal inconsistent set (MIS)* is an inconsistent set all of whose proper subsets are consistent. We write $\mathsf{MI}(\mathrm{A})$ for the set of minimal inconsistent subsets of A. A formula is *problematic* if it is a member of some set $S \in \mathsf{MI}(A)$, *free* otherwise. We write $\mathsf{Problematic}(\mathrm{A})$ (resp. $\mathsf{Free(A)}$) for the set of problematic (resp. free) formulas of A.

Consider the following two sets: $A_1 = \{a, b, c, \neg a \vee \neg b \vee \neg c\}$ and $A_2 = \{a \wedge b, \neg a \wedge \neg b, c, \neg c\}$. Both A_1 and A_2 are inconsistent. But intuitively, A_2 appears to be more inconsistent than A_1. We would like an inconsistency measure to give a higher value to A_2 than to A_1, and in fact, that is what typically happens. There are several types of inconsistency measures. One type, usually called a syntactic measure, is based in some way on the minimal inconsistent sets of A. We will give below the simplest such measure, one that counts the number of minimal inconsistent subsets.

A semantic measure uses interpretations in its definition: we will give below the one that is typically used. Incidentally, not all inconsistency measures fall clearly into these two groups.

The purpose of this paper is to define the concept of an inconsistency measure for first-order logic. Our approach is to start with a propositional inconsistency measure and extend it in some way, so that it is applicable to first-order logic. After considering various extensions, we found that the most appropriate one to use is a well-known semantic measure. This measure uses a 3-valued propositional logic that we explain next.

Consider a 3-valued logic with the truth-values T, F, and B, where B indicates inconsistency. Thus, an interpretation i assigns to every atom one of the 3 truth-values. That is, in this case $i : \mathsf{Atoms}(A) \to \{T, F, B\}$. We need to define the truth-tables for the connectives. The measure we define uses Priest's Logic of Paradox [10], (but with the corresponding truth values t, f, and p). The truth tables use an ordering on the truth values, where $F < B < T$ and $\wedge$ computes the minimum value while $\vee$ computes the maximum value; also $\neg(B) = B$. So, for example, $B \wedge F = F$ and $B \vee F = B$. Then, an interpretation i satisfies a formula α iff the truth-value of α for i is T or B.

In the following definition, $\mathcal{A}$ stands for the set of all finite sets of propositional logic formulas.

Definition 1. *A function $I : \mathcal{A} \to \mathbb{R}_{\infty}^{\geq 0}$ is an* **inconsistency measure** *iff it satisfies the Consistency postulate:*

Consistency $I(A) = 0$ *iff A is consistent.*

This is a very general definition that fits all proposed inconsistency measures for propositional logic. Of the many propositional inconsistency measures proposed, we present only the two that will be important in our work for first-order logic.

Definition 2. *The following are two well-known propositional inconsistency measures.*
$I_{MI}(A) = |MI(A)|$.
$I_C(A) = min\{|i^{-1}(B)| \mid i \text{ satisfies } A\}$.

I_{MI} ([5]) counts the number of minimal inconsistent subsets, which in a sense counts the number of inconsistencies. I_C ([4]) counts the minimal number of distinct atoms that are involved in a minimal inconsistency. In particular, for the sets given above, $I_{MI}(A_1) = 1$, $I_{MI}(A_2) = 2$, $I_C(A_1) = 1$, and $I_C(A_2) = 3$. Both measures give a higher value to A_2 than to A_1, in accordance with our intuition that A_2 is more inconsistent than A_1. As we will show later, I_{MI}, as well as many other propositional

inconsistency measures, carry over to first-order logic; the problem with them is that they cannot differentiate between the existential and universal quantifiers. For this reason, we believe that an extension of I_C, which can distinguish between them, is more appropriate for first-order logic.

In order to differentiate among the large number of propositional inconsistency measures, some researchers proposed various properties, called *rationality postulates*, that intuitively a good inconsistency measure should satisfy. However, just as there is no general agreement about which inconsistency measure is best, there is also no agreement about which rationality postulates should be required, except for Consistency, that we put into the definition of inconsistency measure. Here we list 9 additional postulates.

Definition 3. *The following postulates will be considered:*

Monotony *If* $A \subseteq A'$, *then* $I(A) \leq I(A')$.

Independence *If* $\alpha \in \mathsf{Free}(A)$ *then* $I(A) = I(A \setminus \{\alpha\})$.

Dominance *If* α *is consistent and logically implies* β *then* $I(A \cup \{\alpha\}) \geq I(A \cup \{\beta\})$.

Super-Additivity *If* $A \cap A' = \emptyset$ *then* $I(A \cup A') \geq I(A) + I(A')$.

Penalty *If* $\alpha \in \mathsf{Problematic}(A)$ *then* $I(A) > I(A \setminus \{\alpha\})$.

MI-Separability *If* $\{\mathsf{MI}(A), \mathsf{MI}(A')\}$ *is a partition of* $\mathsf{MI}(A \cup A')$ *then* $I(A \cup A') = I(A) + I(A')$.

MI-Normalization *If* $M \in \mathsf{MI}(A)$ *then* $I(M) = 1$.

Equal Conflict *If* $M, M' \in \mathsf{MI}(A)$ *and* $|M| = |M'|$ *then* $I(M) = I(M')$.

Exchange *If* A_1 *is consistent and* A_1 *and* A_2 *are logically equivalent then for any set of formulas* A, $I(A \cup A_1) = I(A \cup A_2)$.

Monotony states that the addition of formulas cannot decrease the measure. Independence states that the removal of a free formula does not change the measure. Dominance states that if a first consistent formula logically implies a second formula, then the addition of the first to a set has a measure at least as great as the addition of the second. A confusing aspect of this postulate is that the first formula may already be in the set. These three postulates, as well as Consistency in the definition of an inconsistency measure, are from [6]. Super-Additivity considers two nonintersecting sets and requires the measure of the union to be at least the sum of the individual ones. Penalty is the counterpart of Independence: the removal of a problematic

formula decreases the measure. These two postulates are from [11]. MI-Separability, ([5]), like Super-Additivity, also involves two sets, but in this case, if the minimal inconsistent sets of the two sets form a partition of the minimal inconsistent sets of the union, then the measure of the union is the sum of the measures of the two sets. MI-Normalization ([6]) states that every minimal inconsistent subset has measure 1. Equal Conflict ([9] is a weaker condition than MI-Normalization: it requires minimal inconsistent sets of the same size to have the same measure. Finally, Exchange ([1]) states that the addition of two logically equivalent consistent sets to a set have the same inconsistency measure.

3 Syntax and Semantics for First-Order Logic

We will be using finitary first-order languages with equality, relation, and constant symbols. Recall that a function symbol can be represented as a relation symbol. We start by explaining the concepts in general and then how to specify a particular language. The results will be general, applying to any first-order language. We use $=$ for equality, R with subscripts for relation symbols, and c with subscripts for constant symbols. Variables are designated by x with subscripts. A *term* t with subscripts is either a constant symbol or a variable. Each relation symbol has an associated *arity*, which is a positive integer. The connectives $\neg$, $\wedge$, and $\vee$, as well as the quantifiers $\forall$ and $\exists$, and parentheses, as usual, are in the language.

A specific language is defined by its *signature*, which is a finite sequence starting with 0 or more positive integers followed by 0 or more zeros. For example, $sig = \langle 1, 2, 1, 0, 0\rangle$ is the signature for a language with 3 relation symbols: R_1 of arity 1, R_2 of arity 2, and R_3 of arity 1, and two constant symbols c_1 and c_2. An *atomic formula* has the form $t_i = t_j$ or $R_i(t_1, \ldots, t_n)$ where R_i has arity n. A *literal* is an atomic formula or its negation. We write $t_i \neq t_j$ for $\neg t_i = t_j$. Formulas are formed by applying the connectives $\wedge$ and $\vee$ to the literals and quantifiers in front of formulas. The difference between this definition and the standard one is that in this version negation is applied only to atomic formulas. This is not a real restriction, because for a formula where negation is applied elsewhere, there is a standard way to transform it to a logically equivalent formula where negation is applied only to atomic formulas. A formula with no free (unquantified) variable is called a *sentence*.

A *theory* is a finite set of sentences (in the specified language). We write A with subscripts for theories. As the language contains equality, a theory may give information about the possible number of elements in a model. The concept of model will be explained below: here we just point out this feature of a language with equality. For example, the sentence $E_2 = \forall x_1 \exists x_2 \forall x_3 (x_1 \neq x_2 \wedge (x_3 = x_1 \vee x_3 = x_2))$

states that the number of elements in a model must be 2. Similarly, sentences can be written with no relation or constant symbols (hence in every language) stating that the number of elements in a model must be k, less than k, less than or equal to k, bigger than k, and bigger than or equal to k for every positive integer k. This means that a theory in any first-order language may have an inconsistency involving equality: for example, if $A = \{E_2, E_3\}$. Another way that equality can cause an inconsistency is with a sentence like $\exists x_1(x_1 \neq x_1)$. While we need to deal with this issue, our interest is really in inconsistencies involving relation symbols. Therefore, these two types of inconsistencies will be treated differently when we define inconsistency measures. We call any sentence that restricts in some way the size of a model, like E_2, a *cardinality sentence*. Furthermore, we call any sentence or set of sentences an *equality inconsistency* iff it minimally (that is, no proper subset also) violates a property of equality. Both the sentence $\exists x_1(x_1 \neq x_1)$ and the set $\{E_2, E_3\}$ are equality inconsistencies.

The semantics of finitary first-order logic is standard by way of relational structures. We sketch the basic ideas here. Consider a language with signature $sig = \langle n_1, \ldots, n_k, 0, \ldots, 0\rangle$, where the n_i are positive integers and there are m zeros. Hence the language contains the k relation symbols $R_1, \ldots, R_k$, where each R_i has arity n_i, and the constant symbols $c_1, \ldots, c_m$. A *relational structure* for sig is a tuple $S = \langle D, f_1, \ldots, f_k, g\rangle$ where D is a finite set, say $D = \{d_1, \ldots, d_r\}$, each f_i is a function, $f_i : D^{n_i} \to \{T, F\}$, and $g : \{c_1, \ldots, c_m\} \to D$. The concept of when a relational structure is a model of a set of sentences is a well-known feature of first-order logic. Then, a set of sentences in first-order logic is *consistent* if it has a model; otherwise it is *inconsistent*. When we define an inconsistency measure for finitary first-order logic, we do so for the standard semantics involving relational structures.

4 A Finitary 3-Valued Semantics for First-Order Logic

Recall that the definition of I_C in Section 2 uses a 3-valued logic with the truth-values T, F, and B. Here we extend this semantics to first-order logic, in order to define an inconsistency measure for it.

The syntax is exactly the same as before, namely a language with signature $sig = \langle n_1, \ldots, n_k, 0, \ldots, 0\rangle$, where the n_i are positive integers and there are m zeros. The language contains the k relation symbols $R_1, \ldots, R_k$, where each R_i has arity n_i, and the constant symbols $c_1, \ldots, c_m$. For the 3-valued semantics, we define a 3-valued relational structure, that we simply call *structure*. A *structure* for sig is a tuple $S = \langle D, f_1, \ldots, f_k, g\rangle$ where D is a finite set, say $D = \{d_1, \ldots, d_r\}$, each f_i is a function, $f_i : D^{n_i} \to \{T, F, B\}$, and $g : \{c_1, \ldots, c_m\} \to D$. A structure S is

consistent iff $Range(f_i) = \{T, F\}$ for all f_i. Otherwise, S is inconsistent. We say that $|D|$ is the *size* of S.

Next we sketch the definition of when a sentence ϕ *holds* in a structure S, written $S \models \phi$. (Note that we use $\models$ for the 3-valued logic.) For this purpose, we enlarge the language by adding the r elements of D to the language as new constant symbols, $d_1, \ldots, d_r$. In the following we will not deal separately with formulas containing any constant symbol c_i, as we will assume that in the evaluation process it is changed to $g(c_i)$, which is an element of D. In order to simplify notation, we use $\vec{d_j}$ for a tuple of elements from D appropriate to the arity of the relation symbol under consideration. For equalities we write $S \models d_j = d_j$ for all $d_j \in D$ and $S \models d_j \neq d_\ell$ whenever $j \neq \ell$. For the literals involving a relation symbol we write $S \models R_i(\vec{d_j})$ iff $f_i(\vec{d_j}) \in \{T, B\}$ and $S \models \neg R_i(\vec{d_j})$ iff $f_i(\vec{d_j}) \in \{F, B\}$. This is where the 3-valued semantics differs from the classical 2-valued semantics. Conjunction and disjunction are defined in the standard way, that is, $S \models \phi \wedge \psi$ iff $S \models \phi$ and $S \models \psi$; $S \models \phi \vee \psi$ iff $S \models \phi$ or $S \models \psi$. Formally defining $\models$ for quantified formulas is a tedious process, just like in the classical case, and we use the standard method without giving the details here. Suppose that $\phi = Q_1 x_1 \ldots Q_\ell x_\ell(\psi)$, where each Q_i is a quantifier and ψ is a formula with the free variables $x_1, \ldots, x_\ell$ and no quantifiers. Determining if $S \models \phi$ involves going from left to right among the quantifiers and evaluating ψ by checking if the formula ψ (now with elements of D substituted for the free variables), where $\forall x_i$ is interpreted as "for all substitutions of $d \in D$ (for x_i)" and $\exists x_i$ is interpreted as "there exists a substitution $d \in D$ (for x_i)". Thus the testing becomes a matter of checking for finitely many cases the concept of a ground literal holding in S (along with the appropriate application of any conjunctions and disjunctions). When $S \models \phi$ we say that S is a *model* of ϕ. For a theory A, S is a model of A iff $S \models \phi$ for all $\phi \in A$.

Example 1. *Let* $sig = \langle 2, 2, 1, 0 \rangle$ *and* $S = \langle \{d_1, d_2, d_3\}, f_1, f_2, f_3, g \rangle$ *where*
$f_1(d_1, d_1) = T$, $f_1(d_1, d_2) = F$, $f_1(d_1, d_3) = B$,
$f_1(d_2, d_1) = F$, $f_1(d_2, d_2) = F$, $f_1(d_2, d_3) = B$,
$f_1(d_3, d_1) = T$, $f_1(d_3, d_2) = F$, $f_1(d_3, d_3) = F$,
$f_2(d_1, d_1) = F$, $f_2(d_1, d_2) = T$, $f_2(d_1, d_3) = T$,
$f_2(d_2, d_1) = B$, $f_2(d_2, d_2) = B$, $f_2(d_2, d_3) = T$,
$f_2(d_3, d_1) = T$, $f_2(d_3, d_2) = F$, $f_2(d_3, d_3) = B$,
$f_3(d_1) = T$, $f_3(d_2) = T$, $f_3(d_3) = F$, *and* $g(c_1) = d_2$.
Consider the sentence
$\phi = \forall x_1 \forall x_2 \exists x_3((\neg R_1(x_1, x_2) \vee R_2(x_2, x_3)) \wedge x_2 \neq x_3)$.
To show that $S \models \phi$ *we must take all* 9 *substitutions of pairs of elements of* D, $\langle x_1, x_2 \rangle$, *and for each case find a substitution of an element from* D *for* x_3 *such that with those substitutions for* x_1, x_2, x_3, *the formula* $(\neg R_1(x_1, x_2) \vee R_2(x_2, x_3)) \wedge x_2 \neq$

x_3) *holds in* S. *For example, for the substitution of* d_1 *for* x_1 *and* d_1 *for* x_2 *the choice of* d_2 *for* x_3 *works because* $S \models (\neg R_1(d_1, d_1) \vee R_2(d_1, d_2)) \wedge d_1 \neq d_2)$. *The other* 8 *cases can be done similarly.*

Recall from the previous section that using equalities it is possible to specify the possible number of objects in a model. We call a theory *equality inconsistent* if it contains sentences that cannot be satisfied by any structure on account of equality. Otherwise the theory is *equality consistent*. For example, the theory $A = \{E_2, E_3\}$ is equality inconsistent because no structure can have both size 2 and 3: the size is unique. On the other hand, expressing in first-order logic that "there are at least 10 elements" and "there are at most 20 elements" is possible and having just those 2 equality sentences gives an equality consistent theory.

Proposition 1. *Every equality consistent theory has a model.*

Proof. If A is equality consistent, then there must be at least one positive integer j such that a structure with j elements may be a model of A. Choose such a j and define in accordance with the signature, $S = \langle \{d_1, \ldots, d_j\}, f_1, \ldots, f_k, g \rangle$ such that $f_i(\vec{d}) = B$ for all f_i and $\vec{d}$ and g is such that it satisfies all equalities related to the constants c_i. Then all the ground literals must hold in S and hence all sentences obtained by applying the connectives and quantifiers must hold also. Therefore, $S \models A$. □

When we get to measuring the inconsistency of a theory, we will use the concept of the inconsistency of a structure. Let $S = \langle D, f_1, \ldots, f_k, g \rangle$. We define $Inc(S : f_i) = |\vec{d_j}|$ such that $f_i(\vec{d_j}) = B$ for each i, $1 \leq i \leq k$. That is, for each relation we count the number of times a tuple gets the truth value B for that relation, as each such value represents an inconsistency. Then we define *the inconsistency of a structure* S as $Inc(S) = \sum_{i=1}^{k} Inc(S; f_i)$, that is, we add the inconsistency for each relation. In particular, in Example 1, $Inc(S) = 5$.

Later we will need to use the concept of inconsistency reduction and enlargement.

Definition 4. *For a structure* $S = \langle D, f_1, \ldots, f_k, g \rangle$, *a structure of the same signature, domain, and assignment of constant symbols,* $S' = \langle D, f'_1, \ldots, f'_k, g \rangle$, *is an* inconsistency reduction *of* S *iff the following* 3 *conditions hold:*

1. *If* $f_i(\vec{d_j}) = T$ *then* $f'_i(\vec{d_j}) = T$.
2. *If* $f_i(\vec{d_j}) = F$ *then* $f'_i(\vec{d_j}) = F$.
3. *There is at least one* f_i *and* $\vec{d_j}$ *such that* $f_i(\vec{d_j}) = B$ *and either* $f'_i(\vec{d_j}) = T$ *or* $f'_i(\vec{d_j}) = F$.

In such a case we call S an inconsistency expansion *of S'.*

Proposition 2. *1. If S' is an inconsistency reduction of S then $Inc(S') < Inc(S)$.*

2. If $S \models A$ and S' is an inconsistency expansion of S then $S' \models A$.

Proof. 1. This follows from the definition of the inconsistency of a structure.

2. Every equality and inequality that holds in S must hold in S'. The same goes for every literal and then conjunction and disjunction of literals followed by the application of the quantifiers.

□

Note that S and S' having the same signature and $Inc(S') < Inc(S)$ does not imply that S is an inconsistency expansion of S'. For example, let $sig = \langle 1 \rangle$, $S = \langle \{d_1, d_2, d_3\}, f_1 \rangle$ and $S' = \langle \{d_1, d_2, d_3\}, f_1' \rangle$ where $f_1(d_1) = f_1(d_2) = B$, $f_1(d_3) = T$ and $f_1'(d_1) = f_1'(d_2) = T$, $f_1'(d_3) = B$. Then $Inc(S) = 2 > Inc(S') = 1$ but S is not an inconsistency expansion of S' on account of d_3.

5 Rationality Postulates in First-Order Logic

Section 2 gave definitions and postulates for propositional logic inconsistency measures. Recall that propositional inconsistency is measured in the context of classical 2-valued logic. The same will be the case when we extend the measures to first-order logic. But in order to do the extension, some modifications are needed. We say that a theory is *f-consistent* iff it has a consistent structure for a model. So, f-consistency means that there is a classical finite model. We call a theory *f-inconsistent* iff it has a model but no model is f-consistent. Thus there are three concepts concerning the consistency of a theory: f-consistent, f-inconsistent, and equality inconsistent, the latter as explained in Section 3

A theory may have models in infinitely many (finite) cardinalities. Consider the theory $A = \{\forall x_1 R(_1 x_1), \forall x_1 \neg R_1(x_1)\}$ in a language with $sig = \langle 1 \rangle$. How inconsistent is A? A has a model for every cardinality and if S is a model then it must have an inconsistency for each element of the domain. In determining the inconsistency of a theory we should consider the cardinalities of its models. Our method for accomplishing this is to allow the value of an inconsistency measure for a theory to be not just a specific number, as in the propositional case, but also a function of the size of a model represented by a parameter N. For the purpose of comparison, we will consider N to be larger than every specific finite integer.

Definition 5. *A* first-order inconsistency measure *is a function whose domain is the set of all theories such that for each theory A, either $I(A) = \infty$, or $I(A) =$ a nonnegative number, or $I(A) = f(N)$ where f is a function of the parameter N standing for the size of a model, such that I satisfies the following two postulates:*

f-Consistency *$I(A) = 0$ iff A is f-consistent.*

Equality Consistency *$I(A) = \infty$ iff A is equality inconsistent.*

Thus, for a first-order inconsistency measure there are two consistency requirements, as we consider every equality inconsistent theory to have the maximum possible inconsistency. Next, we consider the other postulates that we considered for propositional inconsistency measures in Section 2 to determine what changes, if any, are needed in the case of first-order logic. We write $f - \mathsf{MI}(A)$ for *the set of minimal f-inconsistent subsets of A*. Then, the *f-problematic* sentences are the ones in some minimal f-inconsistent subset; the other sentences are *f-free*. We say that ϕ *implies* ψ iff every model of ϕ is a model of ψ. Two theories are called *equivalent* iff they have the same models. For some of the postulates we deal with two theories, where one is a subset of another or we take the union or intersection. In those cases we assume that the theories have the same signature.

The following definition provides the first-order counterparts to the rationality postulates in Section 2. We also add several new postulates appropriate for first-order logic. For the one dealing with signatures we need a definition. Given $sig = \langle n_1, \ldots, n_k, 0, \ldots, 0\rangle$ with m zeros, we say that sig' is an *expansion* of sig iff sig' has the form
$sig' = \langle n_1, \ldots, n_k, n_{k+1}, \ldots, n_{k+\ell}, 0, \ldots, 0\rangle$ where either $\ell > 0$ or there are more than m zeros.

Here are the rationality postulates we will use for first-order logic.

Definition 6. *A is a theory; ϕ and ψ are sentences in first-order logic.*

f-Monotony *If $A \subseteq A'$ and $A' \setminus A$ contains no cardinality sentence, then $I(A) \leq I(A')$.*

f-Independence *If $\phi \in f - \mathsf{Free}(A)$ then $I(A) = I(A \setminus \{\phi\})$.*

f-Dominance *If ϕ implies ψ then $I(A \cup \{\phi\}) \geq I(A \cup \{\psi\})$.*

Super-Additivity *If $A \cap A' = \emptyset$ then $I(A \cup A') \geq I(A) + I(A')$.*

f-Penalty *If $\phi \in f - \mathsf{Problematic}(A)$ then $I(A) > I(A \setminus \{\phi\})$.*

f-MI-Separability *If* $\{f-\mathsf{MI}(A), f-\mathsf{MI}(A')\}$ *is a partition of* $f-\mathsf{MI}(A\cup A')$ *then* $I(A\cup A') = I(A) + I(A')$.

f-MI-Normalization *If* $M \in f-\mathsf{MI}(A)$ *then* $I(M) = 1$.

f-Equal Conflict *If* $M, M' \in f-\mathsf{MI}(A)$ *and* $|M| = |M'|$ *then* $I(M) = I(M')$.

f-Exchange *If* A_1 *is equivalent to* A_2 *then for any theory* A, $I(A\cup A_1) = I(A\cup A_2)$.

Signature Invariance *If* A *is a theory for signature* sig, sig' *is an expansion of* sig, A' *is the same theory as* A *but for* sig', *then* $I(A) = I(A')$.

Quantifier Change *If* $sig = \langle n\rangle$,
$A = \{Q_1x_1 \dots Q_nx_n(R_1(x_1,\dots,x_n) \wedge \neg(R_1(x_1,\dots,x_n))\}$, *where at least one of the quantifiers* Q_i *is* $\forall$, *and* A' *is obtained from* A *by changing at least one of the universal quantifiers to an existential quantifier, then* $I(A') < I(A)$.

The last two postulates are appropriate for first-order logic, but have no counterpart in propositional logic.. Let us now go back to Definition 2 and consider the counterpart of I_{MI}, but using minimal f-inconsistent subsets. Both A and A' in the Quantifier Change postulate have one minimal f-inconsistent subset; hence $I_{MI}(A) = I_{MI}(A') = 1$. Actually we don't need to deal with f-inconsistency at all; we get the same result for classical inconsistency. But intuitively A is more inconsistent than A'. This shows that a propositional inconsistency measure cannot differentiate between the two quantifiers.

6 The Inconsistency Measure fI

In this section we define what we consider to be the main inconsistency measure for finitary first-order logic.

Definition 7. *Let* A *be a theory.* fI *is defined using* 3 *cases:*

1. A *is equality inconsistent. Then* $fI(A) = \infty$.
2. *The size of a model of* A *has an upper bound,* s. *Then* $fI(A) = min\{Inc(S) \mid S \models A$ *and the size of* $S = s\}$.
3. A *has arbitrarily large models. We use the parameter* N *for the size of an arbitrarily large model of* A. *Then* $fI(A) = min\{Inc(S) \mid S \models A$ *and the size of* $S = N\}$.

It is clear from Definition 5 that fI is a first-order inconsistency measure. Next we give several examples to illustrate the computation of $fI(A)$.

Example 2. *Let* $A_1 = \{E_2, E_3\}$. *Then* $fI(A_1) = \infty$.

Example 3. *Let* $sig = \langle 2, 2\rangle$ *and*
$A_2 = \{\forall x_1 \forall x_2 R_1(x_1, x_2)$,
$\forall x_1 \forall x_2 \neg R_1(x_1, x_2)$,
$\forall x_1 \forall x_2 \forall x_3(\neg R_2(x_1, x_2) \vee \neg R_2(x_2, x_3) \vee x_1 \neq x_3)$,
$\exists x_1 \forall x_2(R_2(x_1, x_2) \wedge R_2(x_2, x_1))$,
$\exists x_1 \exists x_2(R_2(x_1, x_2) \wedge \neg R_2(x_1, x_2))\}$.
A_2 *has arbitrarily large models. Let* N *be the size of a model, say*
$S_2 = \langle \{d_1, \ldots, d_N\}, f_1, f_2\rangle$ *for some functions* f_1 *and* f_2. *The following assignment has the minimal number of inconsistencies:*
$f_1(d_i, d_j) = B$ *for all* d_i, d_j, $1 \leq i, j \leq N$,
$f_2(d_1, d_i) = B$ *for all* d_i, $1 \leq i \leq N$,
$f_2(d_i, d_1) = T$ *for all* d_i, $2 \leq i \leq N$,
$f_2(d_i, d_j) = F$ *for all* d_i, d_j, $2 \leq i, j \leq N$.
Hence $fI(A_2) = N^2 + N$.

Example 4. *Continuing with Example 3 let*
$A_3 = A_2 \cup \{\forall x_1 \ldots \forall x_6(x_1 = x_2 \vee x_1 = x_3 \vee x_1 = x_4 \vee x_1 = x_5 \vee x_1 = x_6)\}$.
So A_3 *is the same as* A_2 *except that the size of a model cannot exceed* 5.
Hence $fI(A_3) = 5^2 + 5 = 30$.

Example 5. *Let* $sig = \langle 2\rangle$ *and*
$A_4 = \{\forall x_1 \forall x_2 \forall x_3(\neg R_1(x_1, x_2) \vee \neg R_1(x_2, x_3) \vee R_1(x_1, x_3))$,
$\forall x_1 \forall x_2(\neg R_1(x_1, x_2) \vee \neg R_1(x_2, x_1) \vee x_1 = x_2)$,
$\forall x_1 R_1(x_1, x_1)$,
$\forall x_1 \forall x_2(R_1(x_1, x_2) \vee R_1(x_2, x_1))$,
$\forall x_1 \exists x_2(R_1(x_1, x_2) \wedge x_1 \neq x_2)\}$.
A_4 *is the theory of ordering (with* R_1 *for* $\leq$*) with no right endpoint.* A_4 *does not have a consistent finite model. Let* $S_4 = \langle \{d_1, \ldots, d_N\}, f_1\rangle$. *The following assignment has the minimum number of inconsistencies:*
$f_1(d_i, d_j) = T$, $1 \leq i \leq j \leq N$,
$f_1(d_j, d_i) = F$, $1 \leq i < j \leq N$ *except that* $f_1(d_N, d_1) = B$.
Hence $fI(A_4) = 1$.

7 Postulate Satisfaction for fI

This section considers the satisfaction of the rationality postulates given in Section 5.

Theorem 1. *fI satisfies f-Monotony, f-Dominance, f-Exchange, Signature Invariance, and Quantifier Change and violates f-Independence, Super-Additivity, f-Penalty, f-MI-Separability, f-MI-Normalization, and f-Equal Conflict.*

Proof. In several parts of the proof we use the same sentences. Let $\phi_1 = \forall x_1(R_1(x_1) \wedge \neg R_1(x_1))$ and $\phi_2 = \exists x_1(R_1(x_1) \wedge \neg R_1(x_1))$. For these formulas $sig = \langle 1 \rangle$.

f-Monotony Let $A \subseteq A'$ such that $A' \setminus A$ does not contain a cardinality sentence. If A has no models then neither does A' and hence $fI(A) = fI(A') = \infty$. If A has a model then every model of A' is a model of A. Hence by the minimality condition in the definition of fI, $fI(A) \leq fI(A')$.

f-Independence Let $sig = \langle 1, 1 \rangle$, $A = \{\forall x_1(R_1(x_1) \wedge \neg R_1(x_1) \wedge R_2(x_1)), \forall x_1 \neg R_2(x_1)\}$. Then, $f - \mathsf{MI}(A) = \{\{\forall x_1(R_1(x_1) \wedge \neg R_1(x_1) \wedge R_2(x_1))\}\}$. Hence $\forall x_1 \neg R_2(x_1) \in f - \mathsf{Free}(A)$. But $fI(A) = 2 \times N > fI(A \setminus \{\forall x_1 \neg R_2(x_1)\}) = N$.

f-Dominance If $A \cup \{\phi\}$ does not have a model then $fI(A \cup \{\phi\}) = \infty \geq fI(A \cup \{\psi\})$. Otherwise, every model of $A \cup \{\phi\}$ is a model of $A \cup \{\psi\}$ and hence $fI(A \cup \{\phi\}) \geq fI(A \cup \{\psi\})$.

Super-Additivity Let $A_1 = \{\phi_1\}$ and $A_2 = \{\phi_2\}$. Then $A_1 \cap A_2 = \emptyset$, $fI(A_1) = N$, $fI(A_2) = 1$, and $fI(A_1 \cup A_2) = N \not\geq fI(A_1) + fI(A_2) = N + 1$.

f-Penalty Let $A = \{\phi_1, \phi_2\}$. Then, $f - \mathsf{MI}(A) = \{\{\phi_1\}, \{\phi_2\}\}$.
Hence $\phi_2 \in f - \mathsf{Problematic}(A)$. But then $fI(A) = N \not> fI(A \setminus \{\phi_2\}) = N$.

f-MI-Separability For $A_1 = \{\phi_1\}$ and $A_2 = \{\phi_2\}$, the partition property is satisfied as shown in the proof of f-Penalty, but $fI(A_1 \cup A_2) = N \neq fI(A_1) + fI(A_2) = N + 1$.

f-MI-Normalization For $A = \{\phi_1, \phi_2\}$, $\{\phi_1\} \in f - \mathsf{MI}(A)$ but $fI(\{\phi_1\}) = N \neq 1$.

f-Equal Conflict $|\{\phi_1\}| = 1 = |\{\phi_2\}|$ but $fI(\{\phi_1\}) = N \neq fI(\{\phi_2\}) = 1$.

f-Exchange If $A \cup A_1$ does not have a model then neither does $A \cup A_2$ and so $fI(A \cup A_1) = fI(A \cup A_2) = \infty$. Otherwise $A \cup A_1$ and $A \cup A_2$ have the same models and hence $fI(A \cup A_1) = fI(A \cup A_2)$.

Signature Invariance The definition of fI does not take the signature into consideration.

Quantifier Change The effect of each universal quantifier is a multiplicative N, while the effect of each existential quantifier is a multiplicative 1. So, for

$A = \{Q_1x_1 \ldots Q_nx_n(R_1(x_1, \ldots, x_n) \wedge \neg(R_1(x_1, \ldots, x_n)\}$, $fI(A) = N^k$ where the number of universal quantifiers among the $\{Q_1, \ldots, Q_n\}$ is k. The change of each universal quantifier to its existential counterpart subtracts 1 from k. Therefore $fI(A') = N^h$ where $h < k$ and so $fI(A') < fI(A)$.

□

As we see from this theorem, many of the postulates proposed for propositional inconsistency measures and extended to first-order logic are violated by fI. These postulates are already controversial for propositional logic, and may just be inappropriate in this context. In each of the next four sections we propose an additional inconsistency measure for first-order logic. We provide the intuition for each and investigate their satisfaction of the postulates.

8 The Inconsistency Measure fI^w

As explained earlier, the measure fI can be thought of as the extension of the propositional inconsistency measure I_C to finitary first-order logic. In this section we present an inconsistency measure that does not have a counterpart in propositional logic. The reason is that this measure uses the meaning of quantifiers. Consider the following 3 theories in the signature $\langle 1 \rangle$: $A_1 = \{\exists x_1(R_1(x_1) \wedge \neg R_1(x_1))\}$, $A_2 = \{\exists x_1 R_1(x_1), \exists x_1 \neg R_1(x_1)\}$, and $A_3 = \{\forall x_1 R_1(x_1)\}$. A_1 is f-inconsistent while A_2 and A_3 are f-consistent. But there is a subtle difference between A_2 and A_3 regarding consistency. There is a structure M_2 of size 2 such that $f_1(d_1) = T$ and $f_1(d_2) = F$. M_2 is a consistent model of A_2. That is why A_2 is consistent. But there is an inconsistent model of A_2 of size 1, M_1, where $f_1(d_1) = B$. Actually, as shown in the proof of Proposition 1, it is always possible to obtain an inconsistent model for every equality consistent theory, such as A_2 and A_3. To avoid this issue, in this section we restrict our attention to just the minimal (to be defined in the next paragraph) inconsistent models. That will provide the difference between A_2 and A_3: every minimal model of A_3 is consistent but A_2 has an inconsistent minimal model.

Let M be an inconsistent model of A. We call M *minimal* iff no inconsistency reduction of M is a model of A. For the model M_1 of A_2 above, there are two inconsistency reductions: M_{11} where $f_1(d_1) = T$ and M_{12} where $f_1(d_1) = F$. Neither is a model of A_2. Hence, M_1 is a minimal inconsistent model of A_2. But for A_3, every inconsistent model has an inconsistency reduction to a consistent model by changing each B to T. Hence, no inconsistent model is a minimal model.

Now we define an inconsistency measure based on fI (a weak version of fI) that differentiates between A_2 and A_3.

Definition 8. *Let A be a theory. fI^w is defined using 3 cases:*

1. *A is equality inconsistent. Then $fI^w(A) = \infty$.*
2. *The size of a model of A has an upper bound, s. Then $fI^w(A) = max\{Inc(S) \mid S$ is a minimal model of A and the size of $S = s\}$.*
3. *A has arbitrarily large models. We use the parameter N for the size of an arbitrarily large model of A. Then $fI^w(A) = max\{Inc(S) \mid S$ is a minimal model of A and the size of $S = N\}$.*

For the case above, $fI^w(A_1) = fI(A_1) = 1$, $fI^w(A_3) = fI(A_3) = 0$, but $fI^w(A_2) = 1 \neq fI(A_2) = 0$. For the four examples in Section 6, fI^w gives the same results as fI. In general, $fI(A) \leq fI^w(A)$ for all theories A.

Next we consider postulate satisfaction for fI^w. The following result will be useful.

Proposition 3. *If every model of A' is a model of A then $fI^w(A) \leq fI^w(A')$.*

Proof. Let M' be a minimal model of A' such that $fI^w(A') = Inc(M')$. Then M' is a model of A so it is either a minimal model or it has an inconsistency reduction that is a minimal model. Then, by Proposition 2, the maximum value for every minimal model M of A, $Inc(M)$, cannot exceed $Inc(M')$. Hence $fI^w(A) \leq fI^w(A')$. □

As fI^w is very close to fI, it turns out that they satisfy the same postulates in our list.

Proposition 4. *fI^w satisfies f-Monotony, f-Dominance, f-Exchange, Signature Invariance, and Quantifier Change and violates f-Independence, Super-Additivity, f-Penalty, f-MI-Separability, f-MI-Normalization, and f-Equal Conflict.*

Proof. The same counterexamples work as for the proof of Theorem 1. For the proofs of f-Monotony and f-Dominance the proof uses the proposition just proved above. The other satisfaction proofs are the same as for Theorem 1. □

9 The Inconsistency Measure fMI

As explained in Section 2, using minimal inconsistent subsets does not differentiate between the quantifiers. Still, given that the I_{MI} inconsistency measure is highly regarded for propositional logic, it is worthwhile to consider its extension to first-order logic. That is what we do in this section, but in order to use a uniform formulation for this paper, we use the definitions from Section 5. That is, $f - \mathsf{MI}(A)$ is the set of minimal inconsistent subsets of A that are f-inconsistent.

Definition 9. *Let A be a theory. If A is equality inconsistent then $fMI(A) = \infty$. Otherwise $fMI(A) = |f - \mathsf{MI}(A)|$.*

The definition for fMI, unlike for fI and fI^w, does not have a parameter. So the value is either a nonnegative integer or infinity. Clearly, fMI satisfies the requirement for an inconsistency measure from Definition 5.

Next, we write the f-minimal inconsistent subsets of the examples from Section 6 and thereby compute fMI for them.

Example 6. *Continuing with Examples 2-5 we first list the set of f-minimal inconsistent subsets. Actually, we don't have to do this for A_1 because it is equality inconsistent. Hence $fMI(A_1) = \infty$.*
Next, $f - \mathsf{MI}(A_2) = \{\{\forall x_1 \forall x_2 R_1(x_1, x_2), \forall x_1 \forall x_2 \neg R_1(x_1, x_2)\},$
$\{\forall x_1 \forall x_2 \forall x_3 (\neg R_2(x_1, x_2) \vee \neg R_2(x_2, x_3) \vee x_1 \neq x_3), \exists x_1 \forall x_2 (R_2(x_1, x_2) \wedge R_2(x_2, x_1))\},$
$\{\exists x_1 \exists x_2 (R_2(x_1, x_2) \wedge \neg R_2(x_1, x_2))\}\}$
Hence, $fMI(A_2) = 3$.
For A_3, $f - \mathsf{MI}(A_3) = f - \mathsf{MI}(A_2)$; thus $fMI(A_3) = 3$.
Finally, for A_4 every proper subset has a consistent model. We show this here for two cases.
For the first four formulas, for a domain $D = \{d_1, \ldots, d_N\}$, let $f_1(d_i, d_j) = T$ for all $1 \leq i \leq j \leq N$, $f_1(d_i, d_j) = F$ for all $1 \leq j < i \leq N$.
For the last four formulas, for a domain $D = \{d_1, \ldots, d_N\}$, let $f_1(d_i, d_j) = T$ for all $1 \leq i \leq j \leq N$, $f_1(d_N, d_1) = T$, and $f_1(d_i, d_j) = F$ otherwise.
Hence $f - \mathsf{MI}(A_4) = \{\{A_4\}\}$ and so $fMI(A_4) = 1$.

Next we consider the satisfaction of the postulates for fMI.

Theorem 2. *fMI satisfies f-Monotony, f-Independence, Super-Additivity, f-Penalty, f-MI-Separability, f-MI-Normalization, f-Equal Conflict, and Signature Invariance, and violates f-Dominance, f-Exchange, and Quantifier Change.*

Proof. The properties are checked in order.

f-Monotony Let $A \subseteq A'$ such that $A' \setminus A$ does not contain a cardinality sentence.. If A has no models then $fMI(A) = fMI(A') = \infty$. Otherwise, every minimal f-inconsistent subset of A must also be a minimal f-inconsistent subset of A'. Hence, $fMI(A) \leq fMI(A')$.

f-Independence If $\phi \in f - \mathsf{Free}(A)$ then $\phi \notin A'$ for any $A' \in f - \mathsf{MI}(A)$. Hence, A and $A \setminus \{\phi\}$ have the same minimal f-inconsistent subsets. Therefore, $fMI(A \setminus \{\phi\}) = fMI(A)$.

f-Dominance Let $A = \{\forall x_1 R(x_1), \forall x_1 \neg R_1(x_1)\}$, $\phi = \forall x_1 R_1(x_1)$ and $\psi = \exists x_1 R_1(x_1)$. Here, ϕ implies ψ, $A \cup \{\phi\} = A$ and $A \cup \{\psi\} = \{\forall x_1 R_1(x_1), \forall x_1 \neg R_1(x_1), \exists x_1 R_1(x_1)\}$. Then, $fMI(A \cup \{\psi\}) = 1 \not\geq fMI(A \cup \{\psi\}) = 2$.

Super-Additivity If $A \cap A' = \emptyset$ then $f - \mathsf{MI}(A) \subseteq f - \mathsf{MI}(A \cup A')$ and $f - \mathsf{MI}(A') \subseteq f - \mathsf{MI}(A \cup A')$ while $f - \mathsf{MI}(A) \cap f - \mathsf{MI}(A') = \emptyset$. Hence, $fMI(A \cup A') \geq fMI(A) + fMI(A')$.

f-Penalty If $\phi \in f - \mathsf{Problematic}(A)$ then $f - \mathsf{MI}(A \setminus \{\phi\})$ is a proper subset of $f - \mathsf{MI}(A)$ because all minimal f-inconsistent subsets of A that contain ϕ are removed. Hence, $fMI(A) > fMI(A \setminus \{\phi\})$.

f-MI-Separability This follows from the partition and the definition of fMI.

f-MI-Normalization This follows from the definition of fMI.

f-Equal Conflict f-MI-Normalization implies f-Equal Conflict.

f-Exchange Let $A = \emptyset$, $A_1 = \{\forall x_1 R_1(x_1), \forall x_1 \neg R_1(x_1)\}$ and $A_2 = \{\forall x_1 R_1(x_1), \forall x_1 \neg R_1(x_1), \exists x_1 R_1(x_1)\}$. Then A_1 is equivalent to A_2 but $fMI(A \cup A_1) = 1 \neq fMI(A \cup A_2) = 2$.

Signature Invariance The definition of fMI does not take the signature into consideration.

Quantifier Change For $A = \{Q_1 x_1 \ldots Q_n x_n (R_1(x_1, \ldots, x_n) \wedge \neg(R_1(x_1, \ldots, x_n)\}$, $fMI(A) = 1$ no matter which quantifiers Q_i represent.

□

10 The Inconsistency Measure fRI

Consider the case where $sig = \langle 1, 1, 1, 1, 1\rangle$ and the two theories
$A_1 = \{\forall x_1 R_1(x_1), \forall x_1 R_2(x_1), \forall x_1 R_3(x_1), \forall x_1 R_4(x_1), \forall x_1 R_5(x_1), \forall x_1 \neg R_2(x_1)\}$ and
$A_2 = \{\exists x_1 (R_1(x_1) \wedge \neg R_1(x_1) \wedge R_2(x_1) \wedge \neg R_2(x_1) \wedge R_3(x_1) \wedge \neg R_3(x_1) \wedge R_4(x_1) \wedge \neg R_4(x_1) \wedge R_5(x_1) \wedge \neg R_5(x_1))\}$.
Comparing the inconsistency of A_1 and A_2, we get $fI(A_1) = fI^w(A_1) = N$, $fIM(A_1) = 1$. $fI(A_2) = fI^w(A_2) = 5$, $fIM(A_2) = 1$. Thus fI and fI^w consider A_1 more inconsistent than A_2, while fMI considers them equally inconsistent. But consider that A_2 involves 5 relations in inconsistencies, while A_1 has only 1 such relation. In this section, we define a measure that gives A_2 a higher inconsistency

value than A_1 for exactly that reason. This new measure is a sort of a global measure that does not involve local considerations for the relations.

Section 4 contained the definition of the inconsistency of a structure. Now we define the *relation inconsistency* of a structure $S = \langle D, f_1, \ldots, f_k, e_1, \ldots, e_m \rangle$, written $RInc(S)$ as the number of functions, f_i, for which there is some $\vec{d_j}$ such that $f_i(\vec{d_j}) = B$. Thus relation inconsistency counts the number of relations for which S has at least one inconsistency. Now we can define the inconsistency measure fRI.

Definition 10. *Let A be a theory. There are two cases for fRI.*

1. *If A is equality inconsistent then $fRI(A) = \infty$.*
2. *If A has models then $fRI(A) = min\{RInc(S) \mid S \models A\}$.*

Example 7. *For Examples 2 - 5 $fRI(A_1) = \infty$, $fRI(A_2) = fRI(A_3) = 2$, and $fRI(A_4) = 1$.*

Example 8. *Let $sig = \langle 1, 1 \rangle$ and*
$A_5 = \{\forall x_1(R_1(x_1) \wedge R_2(x_1)), \exists x_1(\neg R_1(x_1) \wedge \neg R_2(x_1)) \vee \forall x_1 \neg R_1(x_1)\}$.
From the point of view of calculating fI, choose the model S of size N such that $f_1(d_1) = f_2(d_1) = B$, $f_1(d_i) = f_2(d_i) = T$, $2 \leq i \leq N$, so that $fI(A_5) = 2$. But for calculating fRI, S is not the right model because $RInc(S) = 2$. Instead, choose S' such that $f'_1(d_i) = B, 1 \leq i \leq N$ and $f'_2(d_i) = T, 1 \leq i \leq N$, so that $RInc(S') = 1$, and therefore $fRI(A_5) = 1$. Note that S' has more inconsistencies than S, but its inconsistencies involve only one relation.

Next, we investigate the satisfaction of the postulates for fRI. It turns out that the result is almost the same as for fI and many of the proofs are the same or similar.

Proposition 5. *fRI satisfies f-Monotony, f-Dominance, f-Exchange, and Signature Invariance, and violates f-Independence, Super-Additivity, f-Penalty, f-MI-Separability, f-MI-Normalization, f-Equal Conflict, and Quantifier Change.*

Proof. The proof is based on the proof of Theorem 1, so we indicate only the differences between them, if any. In particular, we use the same sentences $\phi_1 = \forall x_1(R_1(x_1) \wedge \neg R_1(x_1))$ and $\phi_2 = \exists x_1(R_1(x_1) \wedge \neg R_1(x_1))$.

f-Monotony Same proof.

f-Independence Same example and $fRI(A) = 2 \neq fRI(A \setminus \{\forall x_1 \neg R_2(x_1)\}) = 1$.

f-Dominance Same proof.

Super-Additivity Same example and $fRI(A_1 \cup A_2) = 1 \not\geq fRI(A_1) + fRI(A_2) = 1 + 1$.

f-Penalty Same example and $fRI(A) = 1 \not> fRI(A \setminus \{\phi_2\}) = 1$.

f-MI-Separability Same example and $fRI(A_1 \cup A_2) = 1 \neq fRI(A_1) + fRI(A_2) = 1 + 1$.

f-MI-Normalization Let $\phi_3 = \exists x_1(R_1(x_1) \wedge \neg R_1(x_1) \wedge R_2(x_1) \wedge \neg R_2(x_1))$ and $A = \{\phi_3\}$. Then $\{\phi_3\} \in f - \mathsf{MI}(A)$ but $fRI(A) = 2$

f-Equal Conflict $|\{\phi_1\}| = 1 = |\{\phi_3\}|$ but $fRI(\{\phi_1\}) = 1 \neq fRI(\{\phi_3\}) = 2$.

f-Exchange Same proof.

Signature Invariance The definition of fRI does not take the signature into consideration.

Quantifier Change $fRI(A') = 1 \not> fRI(A) = 1$.

□

11 The Inconsistency Measure fI_r

In the research literature on propositional inconsistency measures, a distinction between two types is often not clearly stated. Absolute inconsistency measures measure the total amount of inconsistency in the set. The four inconsistency measures presented so far are all absolute measures: they use different criteria, but in some way they measure the totality of the inconsistency. Another way to measure inconsistency is as a proportion, that is, what proportion of the theory is inconsistent. Such a measure is called a *relative* inconsistency measure. In the propositional case, such a measure must have a value between 0 and 1, but in the first-order case, where some theories do not have even inconsistent models, we also allow the value to be ∞. In general, any absolute inconsistency measure can be relativized; we do it here for our main measure fI.

Consider an arbitrary signature $sig = \langle n_1, \ldots, n_k, 0, \ldots, 0\rangle$ and a structure $S = \langle D, f_1, \ldots, f_k, g\rangle$ for it. The most inconsistent such structure has $f_i(\vec{d_j}) = B$ for all i, j. Hence, for such a structure S, $fI(S) = |D|^{n_1} + \ldots + |D|^{n_k}$. When the theory allows finite models of arbitrarily large size, using the parameter N we obtain $N^{n_1} + \ldots + N^{n_k}$.

Definition 11. *Let A be a theory in the signature $sig = \langle n_1, \ldots, n_k \rangle$. There are* 3 *cases.*

1. *A is equality inconsistent. Then $fI_r(A) = \infty$.*
2. *The size of a model of A has an upper bound, s. Then $fI_r(A) = \frac{fI(A)}{(s^{n_1}+\ldots s^{n_k})}$.*
3. *A has arbitrarily large models. We use the parameter N for the size of an arbitrarily large model of A. Then $fI_r(A) = \frac{fI(A)}{(N^{n_1}+\ldots N^{n_k})}$.*

Example 9. *Continuing with Examples 2 - 5 as well as Example 8, we obtain:* $fI_r(A_1) = \infty$, $fI_r(A_2) = \frac{N^2+N}{2\times N^2} = \frac{N+1}{2\times N}$, $fI_r(A_3) = \frac{30}{50} = 0.6$, $fI_r(A_4) = \frac{1}{N^2}$, $fI_r(A_5) = \frac{2}{2\times N} = \frac{1}{N}$.

Next, we investigate the satisfaction of postulates for fI_r. It turns out that with the exception of Signature Invariance, fI_r satisfies the same postulates as fI.

Proposition 6. *fI_r satisfies f-Monotony, f-Dominance, f-Exchange, and Quantifier Change, and violates f-Independence, Super-Additivity, f-Penalty, f-MI-Separability, f-MI-Normalization, f-Equal Conflict, and Signature Invariance.*

Proof. The proof is based on the proof of Theorem 1, so we indicate only the differences between them, if any. In particular, we use the same sentences $\phi_1 = \forall x_1(R_1(x_1) \wedge \neg R_1(x_1))$ and $\phi_2 = \exists x_1(R_1(x_1) \wedge \neg R_1(x_1))$.

f-Monotony The case where A has no models is the same. If A has a model, we use our assumption that A and A' have the same signature. Thus the denominator is the same for both and the result follows from $fI(A) \leq fI(A')$.

f-Independence Same example and $fI_r(A) = \frac{2\times N}{2\times N} = 1 \neq fI_r(A \setminus \{\forall x_1 \neg R_2(x_1)\}) = \frac{N}{2\times N} = \frac{1}{2}$.

f-Dominance Same proof and the denominators are the same.

Super-Additivity Same example and $fI_r(A_1 \cup A_2) = \frac{N}{N} = 1 \not\geq fI_r(A_1) + fI_r(A_2) = 1 + \frac{1}{N}$.

f-Penalty Same example and $fI_r(A) = \frac{N}{N} = 1 \not> fI_r(A \setminus \{\phi_2\}) = \frac{N}{N} = 1$.

f-MI-Separability Same example and $fI_r(A_1 \cup A_2) = \frac{N}{N} = 1 \neq fI_r(A_1) + fI_r(A_2) = 1 + \frac{1}{N}$.

f-MI-Normalization Let $A = \{\phi_2\}$. Then $\{\phi_2\} \in f - \mathsf{MI}(A)$ but $fI_r(A) = \frac{1}{N} \neq 1$.

f-Equal Conflict $|\{\phi_1\}| = 1 = |\{\phi_2\}|$ but $fI_r(\{\phi_1\}) = \frac{N}{N} = 1 \neq fI_r(\{\phi_2\}) = \frac{1}{N}$.

f-Exchange Same proof and the denominators are the same.

Signature Invariance When the signature changes, the denominator changes.

Quantifier Change Same proof and the denominators are the same.

□

12 Summary

The purpose of this paper was to extend the concept of measuring inconsistency from propositional logic, where much work has been done, to finitary first-order logic. For this purpose we defined an alternative semantics for first-order logic. Using this semantics we defined five inconsistency measures appropriate for first-order logic. We also investigated various properties of these inconsistency measures, including properties extended from propositional logic and some new properties appropriate for first-order logic. This paper gives a general approach to inconsistency measuring for unrestricted first-order logic formulas.

In Table 1 we indicate postulate satisfaction for the five inconsistency measures we introduced. The measure fMI satisfies more of them than the others, but it does not satisfy the very important Quantifier Change postulate. The same objection arises to most other inconsistency measures obtained from propositional logic measures. Actually, if our interest is only in counting the number of different relations that are involved in an inconsistency, then fRI is a good choice, even though it also does not satisfy Quantifier Change. As far as the other three measures are concerned, fI^W measures a slightly different concept that has no counterpart in propositional logic. In general we think that fI (resp. fI_r) is the most suitable absolute (resp. relative) inconsistency measure for finitary first-order logic.

In this paper we dealt with the full power of first-order logic. But information in databases often consists of a restricted class of first-order logic formulas. Thus, for specific applications, it will be appropriate to define inconsistency measures designed for such classes.

Acknowledgement I wish to thank the referees for many very useful comments.

	FFOL Inconsistency Measures				
	fI	fI^W	fMI	fRI	fI_r
f-Monotony	✓	✓	✓	✓	✓
f-Independence	✗	✗	✓	✗	✗
f-Dominance	✓	✓	✗	✓	✓
Super-Additivity	✗	✗	✓	✗	✗
f-Penalty	✗	✗	✓	✗	✗
f-MI-Separability	✗	✗	✓	✗	✗
f-MI-Normalization	✗	✗	✓	✗	✗
f-Equal Conflict	✗	✗	✓	✗	✗
f-Exchange	✓	✓	✗	✓	✓
Signature Invariance	✓	✓	✓	✓	✗
Quantifier Change	✓	✓	✗	✗	✓

Table 1: Postulate satisfaction of FFOL inconsistency measures

References

[1] Besnard, Ph., Revisiting postulates for inconsistency measures. In: *JELIA'14*, 383–396.

[2] Grant, J. (1978). Classifications for inconsistent theories. *Notre Dame Journal of Formal Logic*, *XIX*(3), 435–444.

[3] Carnielli, W. A. and Coniglio, M. E., *Paraconsistent Logic: Consistency, Contradiction and Negation*, Dordrecht, Springer.

[4] Grant, J. and Hunter, A., Measuring consistency gain and information loss in stepwise inconsistency resolution. In: *ECSQARU 2011*, 362–373. Springer-Verlag.

[5] Hunter, A. and Konieczny, S. (2008). Measuring inconsistency through minimal inconsistent sets. In: *KR'06*, 358–366, AAAI Press.

[6] Hunter, A. and Konieczny, S. (2010). On the measure of conflicts: Shapley inconsistency values. *Artificial Intelligence*, *174*(14), 1007–1026.

[7] Knight, K. M. (2002). Measuring inconsistency. *Journal of Philosophical Logic*, *31*, 77–98.

[8] Libkin, L., *Elements of Finite Model Theory*, Dordrecht, Springer.

[9] Mu, K., Liu, W., and Jin, Z. (2011). A general framework for measuring inconsistency through minimal inconsistent sets. *Knowledge and Information Systems*, *27*(1), 85–114.

[10] Priest, G. (1979). The logic of paradox. *Journal of Philosophical Logic*, *8*, 219–241.

[11] Thimm, M. (2009). Measuring inconsistency in probabilistic knowledge bases. In *UAI'09*, 530-537, AUAI Press.

[12] Thimm, M. (2018). On the evaluation of inconsistency measures. In J. Grant & M. V. Martinez (Eds.), *Measuring Inconsistency in Information*, 169–194, College Publications.

 Received 9 December 2019

Some Applications of Boolean Valued Analysis

A. G. Kusraev
Southern Mathematical Institute, Vladikavkaz Scientific Center of the RAS
kusraev@smath.ru

S. S. Kutateladze
Sobolev Institute of Mathematics, Siberian Division of the RAS
sskutmath.nsc.ru

Abstract. This is an overview of the basic techniques and applications of Boolean valued analysis. Exposition focuses on the Boolean valued transfer principle for vector lattices and positive operators, Banach spaces and injective Banach lattices, AW^*-modules and AW^*-algebras, etc.

Keywords: Boolean valued universe, ascent, descent, transfer principle

1 Boolean Valued Requisites

In the beginning of the 1960s Cohen propounded his *method of forcing* and proved that the negation of the continuum hypothesis is consistent with the axioms of Zermelo–Fraenkel set theory (cp. [16]). The contemplation over the Cohen method gave rise to the *Boolean valued models of set theory*, which were first introduced by Scott and Solovay (see [115] and [129]). A systematic account of the theory of Boolean valued models and its applications to independence proofs can be found in [11], [40], [119], and [128].

Scott foresaw the role of Boolean valued models in mathematics and wrote as far back as in 1969 (see [116, p. 91]): *"We must ask whether there is any interest in these nonstandard models aside from the independence proof; that is do they have any mathematical interest? The answer must be yes, but we cannot yet give a really good arguments."* Some impressive arguments are available today (see, for example, [67], [68], [69], and [122]).

The term "Boolean valued analysis" appeared within the realm of mathematical logic. It was Takeuti, a renowned expert in proof theory, who introduced the term. Takeuti defined Boolean valued analysis in [122, p. 1] as "an application of Scott–Solovay's Boolean valued models of set theory to analysis." More precisely, Boolean valued analysis signifies the technique of studying the properties of an arbitrary mathematical object by comparison between its representations in two different set-theoretic models whose construction utilizes principally distinct Boolean algebras. As these models, the classical Cantorian paradise in the shape of the *von Neumann universe* $\mathbb{V}$ and a specially-trimmed *Boolean valued universe* $\mathbb{V}^{(\mathbb{B})}$ are usually taken. Comparison analysis is carried out by some interplay between the universes $\mathbb{V}$ and $\mathbb{V}^{(\mathbb{B})}$.

The needed information on the theory of Boolean valued analysis is briefly presented in [56, Chapter 9] and [69, Chapter 1]; details may be found in [67] and [68]. A short survey of the Boolean machinery is also in [78]. See more on the Boolean valued models and the independence proofs in [11], [40], and [128].

Throughout the sequel $\mathbb{B}$ is a complete Boolean algebra with unity $\mathbb{1}$ and zero $\mathbb{0}$. A *partition of unity* in $\mathbb{B}$ is a family $(b_\xi)_{\xi\in\Xi}\subset\mathbb{B}$ such that $\bigvee_{\xi\in\Xi} b_\xi=\mathbb{1}$ and $b_\xi\wedge b_\eta=\mathbb{0}$ whenever $\xi\neq\eta$. We let $:=$ denote the assignment by definition, while $\mathbb{R}$ and $\mathbb{C}$ symbolize the reals and the complexes. Recall also that ZFC is an abbreviation for *Zermelo–Fraenkel axiomatic set theory* with the *axiom of choice*.

1.1. Boolean valued universe and Boolean valued truth [69, § 1.2]. Given a complete Boolean algebra $\mathbb{B}$, we can define the *Boolean valued* universe $\mathbb{V}^{(\mathbb{B})}$, the class of $\mathbb{B}$-*valued sets*. For making statements about $\mathbb{V}^{(\mathbb{B})}$ take an arbitrary formula $\varphi=\varphi(u_1,\dots,u_n)$ of the language of set theory and replace the variables $u_1,\dots,u_n$ by elements $x_1,\dots,x_n\in\mathbb{V}^{(\mathbb{B})}$. Then we obtain some statement about the objects $x_1,\dots,x_n$. There is a natural way of assigning to each formula some element $[\![\varphi(x_1,\dots,x_n)]\!]\in\mathbb{B}$ that serves as the *"Boolean truth-value"* of $\varphi(u_1,\dots,u_n)$ in $\mathbb{V}^{(\mathbb{B})}$ and is defined by induction on the complexity of φ, using the naturally defined truth-values $[\![x\in y]\!]\in\mathbb{B}$ and $[\![x=y]\!]\in\mathbb{B}$, where $x,y\in\mathbb{V}^{(\mathbb{B})}$. We say that $\varphi(x_1,\dots,x_n)$ is *valid within* $\mathbb{V}^{(\mathbb{B})}$ provided that $[\![\varphi(x_1,\dots,x_n)]\!]=\mathbb{1}$. In this event, we will also write $\mathbb{V}^{(\mathbb{B})}\vDash\varphi(x_1,\dots,x_n)$.

1.2. Ascending–descending machinery [69, § 1.5, § 1.6, and § 2.2]. No comparison is feasible without some dialog between $\mathbb{V}$ and $\mathbb{V}^{(\mathbb{B})}$. The relevant *technique of ascending and descending* bases on the operations of the canonical embedding, descent, and ascent.

(1) The canonical embedding. There is a *canonical embedding* of the von Neumann universe $\mathbb{V}$ into the Boolean valued universe $\mathbb{V}^{(\mathbb{B})}$ which sends $x\in\mathbb{V}$ to its *standard name* $x^\wedge\in\mathbb{V}^{(\mathbb{B})}$. The standard name sends $\mathbb{V}$ onto $\mathbb{V}^{(2)}$, where

$2 := \{\mathbb{0}, \mathbb{1}\} \subset \mathbb{B}$.

(2) Descent. Given a member x of a Boolean valued universe $\mathbb{V}^{(\mathbb{B})}$, define the *descent* $x{\downarrow}$ of x by $x{\downarrow} := \{y \in \mathbb{V}^{(\mathbb{B})} : [\![y \in x]\!] = \mathbb{1}\}$. The class $x{\downarrow}$ is a set; i.e., $x{\downarrow} \in \mathbb{V}$ for every $x \in \mathbb{V}^{(\mathbb{B})}$.

(3) Ascent. Assume that $x \in \mathbb{V}$ and $x \subset \mathbb{V}^{(\mathbb{B})}$. Then there exists a unique $x{\uparrow} \in \mathbb{V}^{(\mathbb{B})}$ such that $[\![u \in x{\uparrow}]\!] = \bigvee\{[\![u = y]\!] : y \in x\}$ for all $u \in \mathbb{V}^{(\mathbb{B})}$. The member $x{\uparrow}$ is the *ascent* of x.

The operations of descent, ascent, and canonical embedding can be naturally extended to mappings and relations, so that they are applicable to algebraic structures. The various functors of Boolean valued analysis thus arise whose interplay is of import in applications; see [67, Chapter 3] and [68, Chapter 5].

1.3. Principles of Boolean valued set theory [69, § 1.4]. The main properties of a Boolean valued universe $\mathbb{V}^{(\mathbb{B})}$ are collected in the four propositions:

(1) Transfer Principle. If $\varphi(x_1, \dots, x_n)$ is a theorem of ZFC then so is the following formula: $(\forall x_1, \dots, x_n \in \mathbb{V}^{(\mathbb{B})})\, \mathbb{V}^{(\mathbb{B})} \models \varphi(x_1, \dots, x_n)$.

(2) Maximum Principle. To each formula φ of ZFC there is a member x_0 of $\mathbb{V}^{(\mathbb{B})}$ satisfying $[\![(\exists x)\, \varphi(x)]\!] = [\![\varphi(x_0)]\!]$. In particular, if $\mathbb{V}^{(\mathbb{B})} \models (\exists x)\, \varphi(x)$, then there exists $x_0 \in \mathbb{V}^{(\mathbb{B})}$ such that $\mathbb{V}^{(\mathbb{B})} \models \varphi(x_0)$.

(3) Mixing Principle. For every family $(x_\xi)_{\xi \in \Xi}$ in $\mathbb{V}^{(\mathbb{B})}$ and every partition of unity $(b_\xi)_{\xi \in \Xi}$ in $\mathbb{B}$ there exists a unique $x \in \mathbb{V}^{(\mathbb{B})}$ satisfying $b_\xi \le [\![x = x_\xi]\!]$ for all $\xi \in \Xi$. This unique x is the *mixing* of (x_ξ) by (b_ξ) and is denoted as follows: $x = \operatorname{mix}_{\xi \in \Xi}(b_\xi x_\xi) = \operatorname{mix}\{b_\xi x_\xi : \xi \in \Xi\}$.

A formula is *bounded* or *restricted* provided that each of its quantifiers occurs in the form $(\forall\, x \in y)$ or $(\exists\, x \in y)$ or if it can be proved to be equivalent in ZFC to such a formula.

(4) Restricted Transfer Principle. Given a restricted formula φ of ZFC and $x_1, \dots, x_n \in \mathbb{V}$, we have in ZFC that

$$\varphi(x_1, \dots, x_n) \iff \mathbb{V}^{(\mathbb{B})} \models \varphi(x_1^\wedge, \dots, x_n^\wedge).$$

The transfer principle tells us that all theorems of ZFC are true in $\mathbb{V}^{(\mathbb{B})}$; the maximum principle guarantees the existence of various "Boolean valued objects"; the mixing principle shows how these objects may be constructed. The transfer principle does not mean that if a theorem is true for an algebraic structure $\mathfrak{A}$ within $\mathbb{V}^{(\mathbb{B})}$, then the theorem is true also for its descent $\mathfrak{A}{\downarrow}$ in $\mathbb{V}$. The question of when this happens was first studied by Gordon [25] and Jech [38].

1.4. Boolean valued technology. To prove the relative consistency of some set-theoretic propositions we use a Boolean valued universe $\mathbb{V}^{(\mathbb{B})}$ as follows: Let

$\mathscr{T}$ and $\mathscr{S}$ be some enrichments of Zermelo–Fraenkel theory ZF (without choice). Assume that the consistency of ZF implies the consistency of $\mathscr{S}$. Assume further that we can define $\mathbb{B}$ so that $\mathscr{S} \models$ "B is a complete Boolean algebra" and $\mathscr{S} \models [\![\varphi]\!] = \mathbb{1}$ for every axiom φ of $\mathscr{T}$. Then the consistency of ZF implies the consistency of $\mathscr{T}$. That is how we use $\mathbb{V}^{(\mathbb{B})}$ in foundational studies.

Other possibilities for applying $\mathbb{V}^{(\mathbb{B})}$ base on the fact that irrespective of the choice of a Boolean algebra $\mathbb{B}$, the universe is an arena for testing an arbitrary mathematical event. By the principles of transfer and maximum, every $\mathbb{V}^{(\mathbb{B})}$ has the objects that play the roles of numbers, groups, Banach spaces, manifolds, and whatever constructs of mathematics that are already introduced into practice or still remain undiscovered. These objects may be viewed as some nonstandard realizations of the relevant originals.

All ZFC theorems acquire interpretations for the members of $\mathbb{V}^{(\mathbb{B})}$, attaining the top truth-value. We thus obtain a new technology of comparison between the interpretations of mathematical facts in the universes over various complete Boolean algebras. Developing the relevant tools is the crux of Boolean valued analysis.

A general scheme of the method is as follows (see [68] and [69]). Assume that $\mathbf{X} \subset \mathbb{V}$ and $\mathbb{X} \subset \mathbb{V}^{(\mathbb{B})}$ are two classes of mathematical objects and we are able to prove the possibility of

Boolean Valued Representation: Each $X \in \mathbf{X}$ embeds into a Boolean valued model, becoming an object $\mathscr{X} \in \mathbb{X}$ within $\mathbb{V}^{(\mathbb{B})}$.

The *Boolean Valued Transfer Principle* tells us that every theorem about $\mathscr{X}$ within Zermelo–Fraenkel set theory has its counterpart for the original object X interpreted as a Boolean valued object $\mathscr{X}$.

The *Boolean Valued Machinery* enables us to perform some translation of theorems from $\mathscr{X} \in \mathbb{V}^{(\mathbb{B})}$ to $X \in \mathbb{V}$ by using the appropriate general operations and the principles of Boolean valued analysis.

2 Vector Lattices

The reader can find the relevant information on the theory of vector lattices and order bounded operators in Aliprantis and Burkinshaw [4], Kusraev [56], Luxemburg and Zaanen [86], Meyer–Nieberg [89], Schaefer [114], Vulikh [130], and Zaanen [132].

Definition 1. A *vector lattice* or a *Riesz space* is a real vector space X equipped with a partial order $\leq$ for which the *join* $x \vee y$ and the *meet* $x \wedge y$ exist for all $x, y \in X$, and such that the *positive cone* $X_+ := \{x \in X : 0 \leq x\}$ is closed under addition and multiplication by positive reals and for any $x, y \in X$ the relations $x \leq y$ and $0 \leq y - x$ are equivalent. A *Banach lattice* is a vector lattice that is

also a Banach space whose order is connected with the norm by the condition that $|x| \le |y|$ implies $\|x\| \le \|y\|$ for all $x, y \in X$.

In the sequel, we assume that all vector lattices X are *Archimedean*; i.e., for every pair $x, y \in X$ it follows from $(\forall\, n \in \mathbb{N})\ nx \le y$ that $x \le 0$. Most of the vector spaces that appear naturally in analysis (L^p, l^p, $C(K)$, c, c_0, etc.) are Archimedean vector lattices with respect to the pointwise or coordinatewise order.

Definition 2. Two elements $x, y \in X$ are *disjoint* and write $x \perp y$ if $|x| \wedge |y| = 0$ where the *modulus* $|x|$ of x is defined as $|x| := x \vee (-x)$. A vector $0 < \mathbb{1} \in X$ said to be a *weak order unit* whenever $\mathbb{1}^\perp = \{0\}$. A *band* in a vector lattice X is a subset of the form $B := A^\perp := \{x \in X : (\forall\, a \in A)\, |x| \wedge |a| = 0\}$ for a nonempty $A \subset X$. The inclusion ordered set of all bands in X is a complete Boolean algebra denoted by $\mathbb{B}(X)$.

Definition 3. A band B in X such that $X = B \oplus B^\perp$ is referred to as a *projection band,* while the associated projection (onto B parallel to $B^\perp$) is a *band projection.* The set of all band projections $\mathbb{P}(X)$ in X also forms a Boolean algebra in which $\pi \le \rho$ means $\pi(X) \subset \rho(X)$. If each band in X admits a band projection then $\mathbb{B}(X) \simeq \mathbb{P}(X)$.

Definition 4. A subset $U \subset X$ is *order bounded* if U lies in an *order interval* $[a, b] := \{x \in X :\ a \le x \le b\}$ for some $a, b \in X$. A vector lattice X is *Dedekind complete* (respectively, *laterally complete*) if every nonempty order bounded set (respectively, each nonempty set of pairwise disjoint positive vectors) U in X has a least upper bound $\sup(U) \in X$. The vector lattice that is laterally complete and Dedekind complete simultaneously is referred to as *universally complete.*

Definition 5. Say that a net (x_α) in a vector lattice X *o-converges* to $x \in X$ and write $x = o\text{-}\lim x_\alpha$ if there exists a decreasing net $(e_\beta)_{\beta \in \mathrm{B}}$ in X such that $\inf\{e_\beta :\ \beta \in \mathrm{B}\} = 0$ and for each $\beta \in \mathrm{B}$ there is $\alpha(\beta) \in \mathrm{A}$ with $|x_\alpha - x| \le e_\beta$ for all $\alpha \ge \alpha(\beta)$.

Example 6. Assume that a measure space (Ω, Σ, μ) is semifinite; i.e., if $A \in \Sigma$ and $\mu(A) = \infty$ then there exists $B \in \Sigma$ with $B \subset A$ and $0 < \mu(A) < \infty$. The vector lattice $L^0(\mu) := L^0(\Omega, \Sigma, \mu)$ (of cosets) of μ-measurable functions on Ω is universally complete if and only if (Ω, Σ, μ) is *localizable.* In this event $L^p(\Omega, \Sigma, \mu)$ is Dedekind complete; see [21, 241G]. Observe that $\mathbb{P}(L^0(\Omega, \Sigma, \mu)) \simeq \Sigma/\mu^{-1}(0)$.

Example 7. Given a complete Boolean algebra $\mathbb{B}$ of orthogonal projections in a Hilbert space H, denote by $\langle \mathbb{B} \rangle$ the space of all selfadjoint operators on H whose spectral resolutions are in $\mathbb{B}$; i.e., $A \in \langle \mathbb{B} \rangle$ if and only if $A = \int_{\mathbb{R}} \lambda\, dE_\lambda$ and $E_\lambda \in \mathbb{B}$

for all $\lambda \in \mathbb{R}$. Define the partial order in $\langle \mathbb{B} \rangle$ by putting $A \geq B$ whenever $\langle Ax, x \rangle \geq \langle Bx, x \rangle$ holds for all $x \in \mathscr{D}(A) \cap \mathscr{D}(B)$, where $\mathscr{D}(A) \subset H$ stands for the domain of A. Then $\langle \mathbb{B} \rangle$ is a universally complete vector lattice and $\mathbb{P}(\langle \mathbb{B} \rangle) \simeq \mathbb{B}$.

Applying the transfer principle and the maximum principle to the theorem of ZFC stating the existence of the field of real numbers, we find $\mathscr{R} \in \mathbb{V}^{(\mathbb{B})}$, the *reals within* $\mathbb{V}^{(\mathbb{B})}$ for which $[\![\mathscr{R} \text{ is the reals}]\!] = \mathbb{1}$. The fundamental result of Boolean valued analysis is the Gordon Theorem describing an interplay between $\mathbb{R}$, $\mathbb{R}^\wedge$, $\mathscr{R}$, and $\mathbf{R} = \mathscr{R}\downarrow$; see [69, § 2.2–§ 2.4].

Theorem 8. (Gordon Theorem). *Let $\mathbb{B}$ be a complete Boolean algebra, and let $\mathscr{R}$ be the reals within $\mathbb{V}^{(\mathbb{B})}$. Endow $\mathbf{R}$ with the descended operations and order. Then*

(1) *The algebraic structure $\mathbf{R}$ is a universally complete vector lattice.*

(2) *The field $\mathscr{R} \in \mathbb{V}^{(\mathbb{B})}$ can be chosen so that $[\![\mathbb{R}^\wedge \text{ is a dense subfield of } \mathscr{R}]\!] = \mathbb{1}$.*

(3) *There is a Boolean isomorphism χ from $\mathbb{B}$ onto $\mathbb{P}(\mathbf{R})$ such that*

$$\chi(b)x = \chi(b)y \Longleftrightarrow b \leq [\![x = y]\!],$$
$$\chi(b)x \leq \chi(b)y \Longleftrightarrow b \leq [\![x \leq y]\!]$$
$$(x, y \in \mathbf{R};\ b \in \mathbb{B}).$$

As regards the further development of the theory of vector lattices on using Theorem 8; see Kusraev and Kutateladze [69, § 2.2–§ 2.11]. Note that the versions of the Gordon Theorem which involve the multiplicative structure and complexification are true as well.

Definition 9. An *f-algebra* is a vector lattice X equipped with a distributive multiplication such that if $x, y \in X_+$ then $xy \in X_+$, and if $x \wedge y = 0$ then $(ax) \wedge y = (xa) \wedge y = 0$ for all $a \in X_+$. An f-algebra is *semiprime* provided that $xy = 0$ implies $x \perp y$ for all x and y. A *complex vector lattice* $X_{\mathbb{C}}$ is the complexification $X_{\mathbb{C}} := X \oplus iX$ (with i standing for the imaginary unity) of a real vector lattice X.

In the complex version of Example 7, $\langle \mathbb{B} \rangle$ consists of all normal operators $A + iB$ with $A, B \in \langle \mathbb{B} \rangle$ and the product AB is defined as the unique selfadjoint extension of the operator $x \mapsto A(Bx) = B(Ax)$ $(x \in \mathscr{D}(A) \cap \mathscr{D}(B))$.

Theorem 10. (1) *The universally complete vector lattice $\mathscr{R}\downarrow$ with the descended multiplication is a semiprime f-algebra with the ring unity $\mathbb{1} := 1^\wedge$. Moreover, for every $b \in \mathbb{B}$ the band projection $\chi(b) \in \mathbb{P}(\mathbf{R})$ acts as multiplication by $\chi(b)\mathbb{1}$.*

(2) *Let $\mathscr{C}$ be the field of complex numbers within $\mathbb{V}^{(\mathbb{B})}$. Then the algebraic system $\mathscr{C}\downarrow$ is a universally complete complex f-algebra. Moreover, $\mathscr{C}\downarrow$ is the complexification of the universally complete real f-algebra $\mathscr{R}\downarrow$; i.e., $\mathscr{C}\downarrow = \mathscr{R}\downarrow \oplus i\mathscr{R}\downarrow$.*

Remark 11. If μ is a Maharam measure and $\mathbb{B}$ in the Gordon Theorem is the algebra of all μ-measurable sets modulo μ-negligible sets, then $\mathscr{R}\downarrow$ is lattice isomorphic to $L^0(\mu)$; see Example 6. If $\mathbb{B}$ is a complete Boolean algebra of projections in a Hilbert space H then $\mathscr{R}\downarrow$ is isomorphic to $\langle\mathbb{B}\rangle$; see Example 7. The two indicated particular cases of Gordon's Theorem were intensively and fruitfully exploited by Takeuti [122]–[125]. The object $\mathscr{R}\downarrow$ for general Boolean algebras was also studied by Jech [37], [38], and [39] who in fact rediscovered Gordon's Theorem. The difference is that in [37] a (complex) universally complete vector lattice with unit is defined by another system of axioms and is referred to as a complete *Stone algebra*. Selecting special $\mathbb{B}$'s, it is possible to obtain some properties of $\mathscr{R}$. For instance, Solovay proved the existence of $\mathbb{B}$ such that all subsets of the reals are Lebesgue measurable in $\mathbb{V}^{(\mathbb{B})}$; see [118].

Remark 12. Interpretation of an arbitrary field in a Boolean valued model leads to the class of rationally complete semiprime commutative rings (see Lambek [82] for the definitions). Gordon proved in [26] that if K is a rationally complete semiprime commutative ring and $\mathbb{B}$ stands for the Boolean algebra of all annihilator ideals of K, then there is an internal field $\mathscr{K} \in \mathbb{V}^{(\mathbb{B})}$, the *Boolean valued representation* of K, such that the ring K is isomorphic to $\mathscr{K}\downarrow$. It follows that the Horn theories of fields and rationally complete semiprime commutative rings coincide. Details may be found in [67, Theorems 4.5.6 and 4.5.7] and [68, Theorems 8.3.1 and 8.3.2]. Note also that Smith in [120] established an equivalence between the category of commutative regular rings and the category of Boolean valued fields. Boolean valued rings, integral domains, and fields were examine also by Nishimura [97] and [103]. Here we also point out the article by Nishimura [90] on the Boolean-valued analysis of continuous geometries and the article by Chupin [15] with a solution to Problem 18 in the book by Goodearl [22, p. 346].

Remark 13. In another article [27], Gordon found the following description of the class of modules arising as descents of vector spaces from Boolean valued models: Assume that K and $\mathscr{K}$ are the same as in Remark 12. For every strongly unital injective K-module M there exists $\mathscr{M} \in \mathbb{V}^{(\mathbb{B})}$, the *Boolean valued representation* of the module M, such that M is isomorphic to $\mathscr{M}\downarrow$; also see [67, 4.5.10 (5)]. Now, if $\mathscr{M}$ and $\mathscr{M}'$ are Boolean valued representations of M and M', respectively, then by the transfer principle, $\mathscr{M}$ and $\mathscr{M}'$ are isomorphic if and only if they have Hamel bases of the same cardinality. Using the descent functor and the description of Boolean valued cardinals enables us to obtain a classification of strongly unitary injective modules. The result was obtained recently by Chilin and Karimov [14] with the superfluous assumption $K = L^0(\mu)$ (but without any instance of Boolean valued analysis).

3 Positive Operators

The aim of this section is to establish some variants of the Boolean valued transfer principle from functionals to operators between vector lattices.

Let X and Y be vector lattices. By $L(X,Y)$ we denote the space of all linear operators from X to Y. Take $T\in L(X,Y)$. Call T *positive* and write $T\geq 0$ provided that $T(X_+)\subset Y_+$. Call T *order bounded* or *o-bounded* whenever T sends each order bounded subset of X to an order bounded subset of Y.

The set of all order bounded operators from X to Y is denoted by $L^{\sim}(X,Y)$. The order relation in $L^{\sim}(X,Y)$ is defined as follows: $S\geq T\mathrel{\Longleftrightarrow} S-T\geq 0$.

The celebrated Riesz–Kantorovich Theorem tells us that if X and Y are vector lattices with Y Dedekind complete, then $L^{\sim}(X,Y)$ is a Dedekind complete vector lattice. Moreover, in this event every order bounded operator T is *regular*; i.e., T can be presented as a difference of two positive operators.

The fact that X is a vector lattice over the ordered field $\mathbb{R}$ may be rewritten as a restricted formula, say, $\varphi(X,\mathbb{R})$. Hence, recalling the restricted transfer principle, we come to the identity $[\![\,\varphi(X^{\wedge},\mathbb{R}^{\wedge})\,]\!]=\mathbb{1}$ which amounts to saying that $X^{\wedge}$ is a vector lattice over the ordered field $\mathbb{R}^{\wedge}$ within $\mathbb{V}^{(\mathbb{B})}$. Similarly, the positive cone X_+ is defined by a restricted formula; hence $\mathbb{V}^{(\mathbb{B})}\models (X^{\wedge})_+=(X_+)^{\wedge}$. By the same reason $|x^{\wedge}|=|x|^{\wedge}$, $(x\vee y)^{\wedge}=x^{\wedge}\vee y^{\wedge}$, $(x\wedge y)^{\wedge}=x^{\wedge}\wedge y^{\wedge}$ for all $x,y\in X$, since the lattice operations $\vee$, $\wedge$, and $|\cdot|$ in X are defined by restricted formulas.

Let $X^{\wedge\sim}:=L^{\sim}_{\mathbb{R}^{\wedge}}(X^{\wedge},\mathscr{R})$ be the space of regular $\mathbb{R}^{\wedge}$-linear functionals from $X^{\wedge}$ to $\mathscr{R}$. More precisely, $\mathscr{R}$ is considered as a vector space over the field $\mathbb{R}^{\wedge}$ and by the maximum principle there exists $X^{\wedge\sim}\in\mathbb{V}^{(\mathbb{B})}$ such that $[\![X^{\wedge\sim}$, the set of $\mathbb{R}^{\wedge}$-linear order bounded functionals from $X^{\wedge}$ to $\mathscr{R}$, is a vector space over $\mathscr{R}$ ordered by the cone of positive functionals$]\!]=\mathbb{1}$. A functional $\tau\in X^{\wedge\sim}$ is positive whenever $[\![\tau\geq 0]\!]=\mathbb{1}$.

Definition 14. Let $X\in\mathbb{V}$ and $Y\in\mathbb{V}^{(\mathbb{B})}$ be such that $X\neq\varnothing$ and $[\![Y\neq\varnothing]\!]=\mathbb{1}$. Given an operator $T:X\to Y{\downarrow}$, there exists a unique $T{\uparrow}\in\mathbb{V}^{(\mathbb{B})}$ (called the *modified ascent* of T) such that $[\![T{\uparrow}:X^{\wedge}\to Y]\!]=\mathbb{1}$ and $[\![T{\uparrow}(x^{\wedge})=T(x)]\!]=\mathbb{1}$ for all $x\in X$. Given a member $\tau\in\mathbb{V}^{(\mathbb{B})}$ with $[\![\tau:X^{\wedge}\to Y]\!]=\mathbb{1}$, there exists a unique $\tau{\downarrow}:X\to Y{\downarrow}$ (called the *modified descent* of τ) with $[\![\tau(x^{\wedge})=\tau{\downarrow}(x)]\!]=\mathbb{1}$ for all $x\in X$.

Definition 15. A linear operator T from X to Y is a *lattice homomorphism* whenever $T(x_1\vee x_2)=Tx_1\vee Tx_2$ for all $x_1,x_2\in X$. Say that T is *disjointness preserving* if $|x|\wedge|y|=0$ implies $|T(x)|\wedge|T(y)|=0$ for all $x,y\in X$. Two vector lattices X and Y are said to be *lattice isomorphic* if there is a lattice isomorphism from X onto Y. Let $\mathrm{Hom}(X,Y)$ and $L^{\sim}_{dp}(X,Y)$ stand for the sets of all lattice homomorphisms and all disjointness preserving operators from X to Y, respectively.

Theorem 16. *Let X and Y be vector lattices with Y universally complete and represented as $Y = \mathscr{R}\downarrow$. Given $T \in L^{\sim}(X,Y)$, the modified ascent $T\uparrow$ is an order bounded $\mathbb{R}^{\wedge}$-linear functional on $X^{\wedge}$ within $\mathbb{V}^{(\mathbb{B})}$; i.e., $[\![T\uparrow \in X^{\wedge\sim}]\!] = \mathbb{1}$. The mapping $T \mapsto T\uparrow$ is a lattice isomorphism between the Dedekind complete vector lattices $L^{\sim}(X,Y)$ and $X^{\wedge\sim}\downarrow$.*

As an example of the application of Theorem 16, we will describe some property of an order bounded operator $T \in L^{\sim}(X,Y)$ in terms of the kernels $\ker(bT) = \{x \in X : b \circ Tx = 0\}$ of its *stratum* bT with $b \in \mathbb{P}(Y)$. To this end, assume $Y = \mathscr{R}\downarrow$, put $\tau := T\uparrow$, and observe that $T \in \mathrm{Hom}(X,Y)$ if and only if $[\![\tau \in \mathrm{Hom}(X^{\wedge}, \mathscr{R})]\!] = \mathbb{1}$ and $T \in L^{\sim}_{dp}(X,Y)$ if and only if $[\![\tau \in (X^{\wedge\sim})_{dp}]\!] = \mathbb{1}$. Moreover, X_0 is an order ideal (or sublattice, or Grothendieck subspace) in X if and only if $[\![$ so is $X_0^{\wedge}$ in $X^{\wedge}]\!] = \mathbb{1}$. Recall that a subspace $X_0 \subset X$ is a *Grothendieck subspace* provided that $x \vee y \vee 0 + x \wedge y \wedge 0 \in X_0$ for all $x, y \in X_0$. Combining the above, we can reduce the problem about the operator T to studying the functional τ. The following result is due to Kutateladze [76] and [77]; also see [69, § 3.4–§ 3.6].

Theorem 17. *Let X and Y be vector lattices with Y Dedekind complete, $\mathbb{B} := \mathbb{P}(Y)$, and let $T : X \to Y$ be an order bounded operator. The following assertions hold:*

(1) *T is disjointness preserving if and only if the kernel of each stratum bT of T with $b \in \mathbb{P}(Y)$ is an order ideal in X.*

(2) *An operator T is the difference of two lattice homomorphisms if and only if the kernel of each stratum bT of T with $b \in \mathbb{B}$ is a vector sublattice of X.*

(3) *The modulus $|T|$ of T is the sum of some pair of lattice homomorphisms if and only if the kernel of each stratum bT of T with $b \in \mathbb{B}$ is a Grothendieck subspace of X.*

The modified ascent mapping $T \mapsto T\uparrow$ has the disadvantage that it does not preserve order continuity. Now consider an embedding into $\mathbb{V}^{(\mathbb{B})}$ preserving o-continuity.

Definition 18. An operator $T : X \to Y$ between vector lattices is *order continuous* provided that $o\text{-}\lim Tx_\alpha = 0$ in Y for every net (x_α) with $o\text{-}\lim x_\alpha = 0$ in X. A positive operator $T : X \to Y$ enjoys the *Maharam property* (or is *order interval preserving*) whenever $T[0,x] = [0,Tx]$ for every $0 \le x \in X$; i.e., if for all $0 \le x \in X$ and $0 \le y \le Tx$ there is some $0 \le u \in X$ such that $Tu = y$ and $0 \le u \le x$. A *Maharam operator* is an order continuous linear operator whose modulus has the Maharam property.

Definition 19. A positive operator $T : X \to Y$ has the *Levi property* if $Y = T(X)^{\perp\perp}$ and $\sup x_\alpha$ exists in X for every increasing net $(x_\alpha) \subset X_+$, provided that the net (Tx_α) is order bounded in Y. Given an order bounded order continuous operator

T from X to Y, denote by $\mathscr{D}_m(T)$ the largest ideal of the universal completion X^{u} onto which we may extend T by order continuity. For a positive order continuous operator T we have $X = \mathscr{D}_m(T)$ if and only if T has the Levi property.

The following result states that each Maharam operator is representable as an order continuous linear functional in an appropriate Boolean valued model. This Boolean valued status of the concept of Maharam operator was found by Kusraev [50] and [51].

Theorem 20. *Let X be a Dedekind complete vector lattice, $Y := \mathscr{R}\!\downarrow$, and let $T : X \to Y$ be a positive Maharam operator with $Y = T(X)^{\perp\perp}$. Then there are $\mathscr{X}$ and $\tau \in \mathbb{V}^{(\mathbb{B})}$ such that*

(1) *$[\![\mathscr{X}$ is a Dedekind complete vector lattice and $\tau : \mathscr{X} \to \mathscr{R}$ is an order continuous strictly positive functional with the Levi property $]\!] = \mathbb{1}$.*

(2) *$\mathscr{X}\!\downarrow$ is a Dedekind complete vector lattice and a unital f-module over the f-algebra $\mathscr{R}\!\downarrow$.*

(3) *$\tau\!\downarrow : \mathscr{X}\!\downarrow \to \mathscr{R}\!\downarrow$ is a strictly positive Maharam operator with the Levi property and an $\mathscr{R}\!\downarrow$-module homomorphism.*

(4) *There exists an order continuous lattice homomorphism $\varphi : X \to \mathscr{X}\!\downarrow$ such that $\varphi(X)$ is order dense ideal of $\mathscr{X}\!\downarrow$ and $T = \tau\!\downarrow \circ \varphi$.*

Remark 21. The Maharam operators stem from the theory of Maharam's "full-valued" integrals which was developed in 1949–1953 (see the survey [87]). Luxemburg in the joint articles with de Pagter [84] and Schep [85] extended some portion of Maharam's theory to the case of positive operators in Dedekind complete vector lattices; in particular, some operator versions of the Hahn Decomposition Theorem and the Radon–Nikodým Theorem were obtained in [85]. The Maharam ideas were transferred to the convex operators by Kusraev [48] and [49]. More results, applications, and references on Maharam operators can be found in [56], [66], and [69].

Remark 22. Suppose that X is a vector lattice over a dense subfield $\mathbb{F} \subset \mathbb{R}$ and $\varphi : X \to \mathbb{R}$ is a strictly positive $\mathbb{F}$-linear functional. Then the completion X^{φ} of the normed lattice $(X, \|\cdot\|_{\varphi})$ with $\|x\|_{\varphi} := \varphi(|x|)$ is an AL-space that includes X. This simple constriction interpreted within a Boolean valued model yields an extension of an arbitrary positive operator to a Maharam operator, i.e. the *Maharam extension*. This was done by Akilov, Kolesnikov, and Kusraev in [5] and [6]. Later, Luxemburg and de Pagter [84] constructed the Maharam extension for a given ideal of operators in $L^{\sim}(X, Y)$ without using Boolean valued analysis.

Remark 23. In 1935 Kantorovich in his first definitive article on vector lattices (see [41]) wrote: *"In this note, I define the new type of space that I call a semiordered*

linear space. The introduction of such a space allows us to study linear operations of one abstract class (*those with values in such a space*) *as linear functionals.*" Here Kantorovich stated an important *heuristic transfer principle*; Theorems 16 and 20 present two instances of the mathematical implementation of this principle.

4 Boolean Valued Banach Spaces

In this section we discuss Banach spaces within a Boolean valued universe. We start with the concept of Banach–Kantorovich space (not to be confused with that of *Kantorovich–Banach space* or, shortly, *KB-space* which is by definition a Banach lattice with an order continuous Levi norm; see [2, p. 89] and [89, Definition 2.4.11].)

Definition 24. Consider a vector space X and a real vector lattice Λ. A Λ-*valued norm* is a mapping $\boldsymbol{|}\cdot\boldsymbol{|} : X \to \Lambda_+$ such that $\boldsymbol{|}x\boldsymbol{|} = 0$ implies $x = 0$, $\boldsymbol{|}\lambda x\boldsymbol{|} = |\lambda|\,\boldsymbol{|}x\boldsymbol{|}$, and $\boldsymbol{|}x + y\boldsymbol{|} \le \boldsymbol{|}x\boldsymbol{|} + \boldsymbol{|}y\boldsymbol{|}$ for all $x, y \in X$ and $\lambda \in \mathbb{R}$. A Λ-valued norm is *decomposable* if, for each decomposition $\boldsymbol{|}x\boldsymbol{|} = \lambda_1 + \lambda_2$ with $\lambda_1, \lambda_2 \in \Lambda_+$ and $x \in X$, there exist $x_1, x_2 \in X$ such that $x = x_1 + x_2$ and $\boldsymbol{|}x_k\boldsymbol{|} = \lambda_k$ $(k := 1, 2)$.

Definition 25. A *Banach–Kantorovich space* over a Dedekind complete vector lattice Λ is a vector space X with a decomposable norm $\boldsymbol{|}\cdot\boldsymbol{|} : X \to \Lambda$ which is norm complete in the sense that, given a net $(x_\alpha)_{\alpha\in\mathrm{A}}$ in X with $(\boldsymbol{|}x_\alpha - x_\beta\boldsymbol{|})_{(\alpha,\beta)\in\mathrm{A}\times\mathrm{A}}$ o-convergent to the zero of Λ, there exists $x \in X$ such that $(\boldsymbol{|}x_\alpha - x\boldsymbol{|})_{\alpha\in\mathrm{A}}$ is o-convergent to the zero of Λ.

Definition 26. A Banach–Kantorovich space over Λ is *universally complete* in case Λ is universally complete. By a *universal completion* of a Λ-normed space $(X, \boldsymbol{|}\cdot\boldsymbol{|})$ we mean a universally complete Banach–Kantorovich space Y over Λ^u together with a linear isometry $\imath : X \to Y$ (i.e., $\boldsymbol{|}\imath(x)\boldsymbol{|} = \boldsymbol{|}x\boldsymbol{|}$ for all $x \in X$) such that each universally complete subspace of Y containing $\imath(X)$ coincides with Y.

Definition 27. A linear operator $T : X \to Y$ between Banach–Kantorovich spaces over Λ is Λ-bounded if $\boldsymbol{|}Tx\boldsymbol{|} \le \lambda\,\boldsymbol{|}x\boldsymbol{|}$ $(x \in X)$ for some $\lambda \in \Lambda_+$; the least such λ is denoted by $\boldsymbol{|}T\boldsymbol{|}$. Define $\mathscr{L}_\Lambda(X, Y)$ as the space of Λ-bounded operators from X to Y.

The following two theorems stating that the category of Banach–Kantorovich spaces over $\Lambda = \mathscr{R}\downarrow$ and Λ-bounded linear operators is equivalent to the category of Banach spaces and bounded linear operators within $\mathbb{V}^{(\mathbb{B})}$ were established by Kusraev [51] (see [52], [56], and [67] for full details).

Theorem 28. *Let $(\mathscr{X}, \|\cdot\|)$ be a Banach space within the model $\mathbb{V}^{(\mathbb{B})}$. If $X := \mathscr{X}\downarrow$ and $\boldsymbol{|}\cdot\boldsymbol{|} := \|\cdot\|\downarrow$, then $(X, \boldsymbol{|}\cdot\boldsymbol{|})$ is a universally complete Banach–Kantorovich space*

over $\mathscr{R}\downarrow$; moreover, the relations $b \le [\![x = 0]\!]$ and $\chi(b)x = 0$ are equivalent for all $b \in \mathbb{B}$ and $x \in X$. Conversely, for every lattice-normed space $(X, |\cdot|)$ with $\mathbb{B} \simeq \mathbb{P}\,(|X|^{\perp\perp})$, there exists a unique (up to a linear isometry) Banach space $\mathscr{X}$ within $\mathbb{V}^{(\mathbb{B})}$, for which the descent $\mathscr{X}\downarrow$ is a universal completion of X.

Theorem 29. *Let $\mathscr{X}$ and $\mathscr{Y}$ be Boolean valued representations of Banach–Kantorovich spaces X and Y over some universally complete vector lattice Λ. Let $\mathscr{L}^{\mathbb{B}}(\mathscr{X}, \mathscr{Y})$ be the space of bounded linear operators from $\mathscr{X}$ into $\mathscr{Y}$ within $\mathbb{V}^{(\mathbb{B})}$, where $\mathbb{B} := \mathbb{P}(E)$. The descent and ascent operations implement linear isometries between the Banach–Kantorovich spaces $\mathscr{L}_\Lambda(X, Y)$ and $\mathscr{L}^{\mathbb{B}}(\mathscr{X}, \mathscr{Y})\downarrow$.*

Let $\Lambda := \mathscr{R}\Downarrow$ be the *bounded part* of the vector lattice $\mathscr{R}\downarrow$; i.e., Λ consists of all $x \in \mathscr{R}\downarrow$ with $|x| \le C\mathbb{1}$ for some $C \in \mathbb{R}$, where $\mathbb{1} := 1^\wedge \in \mathscr{R}\downarrow$. Take a Banach space $\mathscr{X}$ within $\mathbb{V}^{(\mathbb{B})}$ and put $\mathscr{X}\Downarrow := \{x \in \mathscr{X}\downarrow : |x| \in \Lambda\}$. Endow $\mathscr{X}\Downarrow$ with a mixed norm

$$|||x||| := \big\| |x| \big\|_\infty := \inf\{0 < C \in \mathbb{R} : |x| \le C\mathbb{1}\}.$$

We will write $\Lambda = \Lambda(\mathbb{B})$ if $\mathscr{R} \in \mathbb{V}^{(\mathbb{B})}$ and $\bar{\Lambda} := \mathscr{C}\Downarrow = \Lambda \oplus i\Lambda$; i.e., $\bar{\Lambda}$ is the complexification of Λ.

Definition 30. The normed space $(\mathscr{X}\Downarrow, |||\cdot|||)$ is the *bounded descent* of $\mathscr{X}$. If $\tau : \mathscr{X} \to \mathscr{Y}$ is a bounded linear operator then $\tau\Downarrow$ denotes the restriction of $\tau\downarrow$ to $\mathscr{X}\Downarrow$.

The bounded descent of an internal Banach space is a Banach space. Thus, the natural question arises: *Which Banach spaces are linearly isometric to the bounded descents of internal Banach spaces?* The answer is given in terms of $\mathbb{B}$-cyclic Banach spaces. Let $\mathscr{B}$ be a complete Boolean algebra of norm one projections in a Banach space X with the Boolean operations: $\pi \wedge \rho := \pi \circ \rho = \rho \circ \pi$, $\pi \vee \rho = \pi + \rho - \pi \circ \rho$, $\pi^* = I_X - \pi$ $(\pi, \rho \in \mathscr{B})$, and the zero and identity operators in X serve as the zero and unity of the Boolean algebra $\mathscr{B}$.

Definition 31. If $(b_\xi)_{\xi\in\Xi}$ is a partition of unity in $\mathscr{B}$ and $(x_\xi)_{\xi\in\Xi}$ is a family in X, then the element $x \in X$ with $b_\xi x_\xi = b_\xi x$ for all $\xi \in \Xi$ is a *mixing* of (x_ξ) with respect to (b_ξ). A Banach space X is $\mathbb{B}$-*cyclic* if $\mathbb{B}$ is a complete Boolean algebra isomorphic to $\mathscr{B}$ and the mixing of every family in the unit ball of X with respect to every partition of unity in $\mathbb{B}$ (with the same index set) exists in the unit ball and is unique; see [56, Definitions 7.3.1 and 7.3.3]. In the sequel we will identify $\mathscr{B}$ and $\mathbb{B}$.

Let X and Y be Banach spaces with $\mathbb{B} \subset \mathscr{L}(X)$ and $\mathbb{B} \subset \mathscr{L}(Y)$. An operator $T : X \to Y$ is $\mathbb{B}$-*linear*, whenever T is linear and commutes with all projections in

$\mathbb{B}$, i.e. in the case that $b \circ T = T \circ b$. The set of all bounded $\mathbb{B}$-linear operators from X into Y denote by $\mathscr{L}_{\mathbb{B}}(X,Y)$. The terms $\mathbb{B}$-*isomorphism* and $\mathbb{B}$-*isometry* are self-evident. The space $X^{\#} := \mathscr{L}_{\mathbb{B}}(X,\Lambda)$, where $\Lambda = \Lambda(\mathbb{B})$, is $\mathbb{B}$-*dual* to X.

The following result can be easily deduced from Theorem 28 and the fact that a Banach lattice $(X, \|\cdot\|)$ is $\mathbb{B}$-cyclic with respect to a complete Boolean algebra $\mathbb{B}$ of projections if and only if X is a Banach–Kantorovich space with a $\Lambda(\mathbb{B})$-valued norm $|\cdot|$ such that $\|x\| = \| |x| \|_\infty$ for all $x \in X$; see Kusraev [53].

Theorem 32. *The bounded descent of a Banach space from the model $\mathbb{V}^{(\mathbb{B})}$ is a $\mathbb{B}$-cyclic Banach space. Conversely, if X is a $\mathbb{B}$-cyclic Banach space, then in the model $\mathbb{V}^{(\mathbb{B})}$ there is a Banach space $\mathscr{X}$ unique up to an isometric isomorphism whose bounded descent $\mathscr{X}\Downarrow$ is $\mathbb{B}$-isometric to X.*

The element $\mathscr{X} \in \mathbb{V}^{(\mathbb{B})}$ from Theorem 32 is the *Boolean valued representation of* X. Let $\mathscr{X}$ and $\mathscr{Y}$ be the Boolean valued representations of $\mathbb{B}$-cyclic Banach spaces X and Y, respectively. Denote by $\mathscr{L}(\mathscr{X},\mathscr{Y})$ an element in $\mathbb{V}^{(\mathbb{B})}$ representing the space of bounded linear operators from $\mathscr{X}$ into $\mathscr{Y}$. As in Theorem 29, the bounded descent of the Banach space $\mathscr{L}(\mathscr{X},\mathscr{Y})$ and the $\mathbb{B}$-cyclic Banach space $\mathscr{L}_{\mathbb{B}}(X,Y)$ are isometrically $\mathbb{B}$-isomorphic. Moreover, the functor of bounded descent establishes an equivalence of the category of Banach spaces and bounded linear operators within $\mathbb{V}^{(\mathbb{B})}$ with the category of $\mathbb{B}$-cyclic Banach spaces and norm bounded $\mathbb{B}$-linear operators.

Definition 33. Let $\bar{\Lambda} = \bar{\Lambda}(\mathbb{B})$ with unity $\mathbb{1}$ and consider a unital $\bar{\Lambda}$-module X. The mapping $\langle\cdot\,|\,\cdot\rangle : X \times X \to \bar{\Lambda}$ is a $\bar{\Lambda}$-*valued inner product* if, for all $x, y, z \in X$ and $\lambda \in \bar{\Lambda}$, the following are satisfied:

(1) $\langle x\,|\,x\rangle \geq 0$; $\langle x\,|\,x\rangle = 0 \Longleftrightarrow x = 0$;
(2) $\langle x\,|\,y\rangle = \langle y\,|\,x\rangle^*$;
(3) $\langle \lambda x\,|\,y\rangle = \lambda\langle x\,|\,y\rangle$;
(4) $\langle x+y\,|\,z\rangle = \langle x\,|\,z\rangle + \langle y\,|\,z\rangle$.

Using a $\bar{\Lambda}$-valued inner product, we introduce the norm by $|||x||| := \sqrt{\|\langle x|x\rangle\|}$ $(x \in X)$ and the decomposable Λ-valued norm by $|x| := \sqrt{\langle x|x\rangle}$ $(x \in X)$. Obviously, $|||x||| = \big\||x|\big\|_\infty$ for all $x \in X$, and so X is a space with mixed norm.

Definition 34. Let X be a $\bar{\Lambda}$-module with an inner product $\langle\cdot\,|\,\cdot\rangle : X \times X \to \bar{\Lambda}$. If X is complete with respect to the mixed norm $|||\cdot|||$ then X is a C^*-*module* over $\bar{\Lambda}$. A unitary C^*-module X over $\bar{\Lambda}(\mathbb{B})$ is a *Kaplansky–Hilbert module* or AW^*-*module* if X enjoys one (hence, both) of the equivalent conditions: (1) $(X, |||\cdot|||)$ is a $\mathbb{B}$-cyclic Banach space and (2) $(X, |\cdot|)$ is a Banach–Kantorovich space over $\bar{\Lambda}(\mathbb{B})$.

The equivalence (1) $\Longleftrightarrow$ (2) in Definition 34 follows from Theorem 32 and it is clear that some counterparts of Theorems 28 and 29 are true for Kaplansky–Hilbert modules. This result was obtained by Ozawa in [104] and [106].

Theorem 35. *The bounded descent functor establishes an equivalence of the category of Hilbert spaces and bounded linear operators within* $\mathbb{V}^{(\mathbb{B})}$ *with the category of Kaplansky–Hilbert modules over* $\bar{\Lambda}(\mathbb{B})$ *and bounded* $\mathbb{B}$*-linear operators.*

Remark 36. The concept of vector space normed by the elements of a vector lattice was introduced by Kantorovich in 1936 [42]. The first applications of vector norms and metrics were related to the method of successive approximations in numerical analysis. The modern theory of lattice-normed spaces and dominated operators on them is presented in Kusraev [56].

Remark 37. The bounded descent of 30 appeared in the research by Takeuti into von Neumann algebras and C^*-algebras within Boolean valued models; see [126] and [127]. Then the technique was developed in the research by Ozawa into the Boolean valued interpretation of the theory of Hilbert spaces; see [104] and [106]. Theorem 32 is due to Kusraev in [51], [53]; also see [52] and [56]. Similar results were obtained by Ozawa [111, Theorem 5.2]; the difference is in the fact that Ozawa [111] deals with Banach spaces possessing an extra module structure over $\Lambda(\mathbb{B})$ which may be recovered in each $\mathbb{B}$-cyclic Banach space. Nishimura [100] established the Boolean valued transfer principle from L^*-algebras to AL^*-algebras in the spirit of the Takeuti–Ozawa theory of AW^*-modules; also see [95]. (An L^*-algebra is a complex Lie algebra whose vector space is a Hilbert space endowed with an involution and some axiom connecting the Lie bracket, inner product, and involution.)

Remark 38. In [106] Ozawa found a complete system of isomorphism invariants for Kaplansky–Hilbert modules: There is one-to-one correspondence between the isomorphism classes of Kaplansky–Hilbert modules over $\bar{\Lambda}(\mathbb{B})$ and the cardinals in $\mathbb{V}^{(\mathbb{B})}$. At the same time each Kaplansky–Hilbert module admits a direct sum decomposition into homogeneous components. Using these results, Kusraev obtained the following functional representation: To each Kaplansky–Hilbert module X there exist a set of cardinals Γ and a family of nonempty extremally disconnected compact spaces $(Q_\gamma)_{\gamma\in\Gamma}$ such that there is a unitary equivalence $X \simeq \sum^{\oplus}_{\gamma\in\Gamma} C_{\#}(Q_\gamma, l_2(\gamma))$. (Here $C_{\#}(Q,X)$ is the space of cosets of X-valued bounded continuous functions defined on comeager subsets of Q; see [67, 6.4.1] and [69, 5.13.3].) The representation is not unique and, as discovered Ozawa in [106], the reason for this is the *cardinal shift* phenomena in $\mathbb{V}^{(\mathbb{B})}$: Given two infinite cardinals $\varkappa < \lambda$, there is a complete Boolean algebra $\mathbb{B}$ such that $\mathbb{V}^{(\mathbb{B})} \models |\varkappa^\wedge| = |\lambda^\wedge|$, and so the injective Banach lattices $C_{\#}\big(K, l_2(\varkappa)\big)$ and $C_{\#}\big(K, l_2(\lambda)\big)$ are lattice $\mathbb{B}$-isometric with K the Stone representation space for $\mathbb{B}$; see [67] and [68].

5 Injective Banach Lattices

In this section we present the instance of the Boolean valued transfer principle from AL-spaces to injective Banach lattices which states that each injective Banach lattice is embedded into an appropriate Boolean valued model, becoming an AL-space; see Kusraev [59], [60], [61], and [62]. First we consider Boolean valued Banach lattices.

Definition 39. A Banach lattice X is an *AL-space* (resp., *AM-space*) if $\|x+y\| = \|x\|+\|y\|$ (resp., $\|x\vee y\| = \max\{\|x\|, \|y\|\}$) whenever $x\wedge y = 0$. An AM-space has a (strong order) *unit* $u \geq 0$ if the order interval $[-u, u]$ is the unit ball of X.

Definition 40. A band projection π in a Banach lattice X is an *M-projection* if $\|x\| = \max\{\|\pi x\|, \|\pi^{\perp} x\|\}$ for all $x \in X$, where $\pi^{\perp} := I_X - \pi$. The collection of all M-projections forms a subalgebra $\mathbb{M}(X)$ of $\mathbb{P}(X)$ in X. A Banach lattice X is *$\mathbb{B}$-cyclic* whenever X is a $\mathbb{B}$-cyclic Banach space for a complete subalgebra $\mathbb{B} \subset \mathbb{M}(X)$. A $\mathbb{B}$-isometric lattice homomorphism is referred to as *lattice $\mathbb{B}$-isometry*.

Theorem 41. *The bounded descent of a Banach lattice from the model $\mathbb{V}^{(\mathbb{B})}$ is a $\mathbb{B}$-cyclic Banach lattice. Conversely, if X is a $\mathbb{B}$-cyclic Banach lattice, then in the model $\mathbb{V}^{(\mathbb{B})}$ there is a Banach lattice $\mathscr{X}$ unique up to an isometric isomorphism whose bounded descent is lattice $\mathbb{B}$-isometric to X. Moreover, $\pi \mapsto \pi\Downarrow$ is an isomorphism of Boolean algebras $\mathbb{M}(\mathscr{X})\downarrow$ and $\mathbb{M}(X)$; in symbols, $\mathbb{M}(\mathscr{X})\downarrow \simeq \mathbb{M}(\mathscr{X}\Downarrow)$.*

Definition 42. A real Banach lattice X is *injective* whenever, for every Banach lattice Y, every closed vector sublattice $Y_0 \subset Y$, and every positive linear operator $T_0 : Y_0 \to X$ there exists a positive linear extension $T : Y \to X$ with $\|T_0\| = \|T\|$.

Thus, the injective Banach lattices are the injective objects in the category of Banach lattices with the positive contractions as morphisms. Arendt [7, Theorem 2.2] proved that the injective objects are the same if the regular operators with contractive modulus are taken as morphisms.

The first example of an injective Banach lattice was indicated by Abramovich in [1] without introducing the term: *A Dedekind complete AM-space with unit is an injective Banach lattice*. Later this fact was rediscovered by Lotz in [83], where the concept of injective Banach lattice was introduced. Lotz also proved that *each AL-space is an injective Banach lattice*; see [83, Proposition 3.2]. This shows that there is an essential difference between the injective Banach lattices and injective Banach spaces, since $C(K)$ with an extremally disconnected compact set K is the only injective object (up to isomorphism) in the category of Banach spaces and linear contractions (see the Nachbin–Goodner–Kelley–Hasumi Theorem [81, Theorem 6]) An important contribution to the study of injective Banach lattices was made by

Cartwright [13] who found the *order intersection property* and proved that a Banach lattice X is injective if and only if X has the order intersection property and there exists a positive contractive projection in X'' onto X (the property (P)); see [69, Definition 5.10.9 (3), Theorems 5.10.10, and 5.10.11]. Another significant advance is due to Haydon [30]. He discovered that an injective Banach space has a mixed *AM-AL*-structure and proved three representation theorems [30, Theorems 5C, 6H, and 7B].

Theorem 43. *The bounded descent $\mathscr{X}{\Downarrow}$ of an AL-space $\mathscr{X}$ from $\mathbb{V}^{(\mathbb{B})}$ is an injective Banach lattice with $\mathbb{B} \simeq \mathbb{M}(\mathscr{X}{\Downarrow})$. Conversely, if X is an injective Banach lattice and $\mathbb{B} \simeq \mathbb{M}(X)$, then there exists an AL-space $\mathscr{X}$ within $\mathbb{V}^{(\mathbb{B})}$ whose bounded descent is lattice $\mathbb{B}$-isometric to X; in symbols, $X \simeq_{\mathbb{B}} \mathscr{X}{\Downarrow}$.*

According to Theorem 43, each theorem about *AL*-spaces within Zermelo–Fraenkel set theory has its counterpart for injective Banach lattices. Translation of theorems from *AL*-spaces to injective Banach lattices is carried out by the functors of Boolean valued analysis. Combining Theorems 20 and 43 yields the following result.

Theorem 44. *If Φ is some strictly positive Maharam operator with the Levi property that takes values in a Dedekind complete AM-space Λ with unit and $|||x||| = \|\Phi(|x|)\|_\infty$ $(x \in L^1(\Phi))$, then $(L^1(\Phi), |||\cdot|||)$ is an injective Banach lattice and there is a Boolean isomorphism φ from $\mathbb{B} := \mathbb{P}(\Lambda)$ onto $\mathbb{M}(L^1(\Phi))$ such that $\pi \circ \Phi = \Phi \circ \varphi(\pi)$ for all $\pi \in \mathbb{B}$. Conversely, every injective Banach lattice X is lattice $\mathbb{B}$-isometric to $(L^1(\Phi), |||\cdot|||)$ for some strictly positive Maharam operator Φ with the Levi property that takes values in a Dedekind complete AM-space Λ with unit, where $\mathbb{B} = \mathbb{P}(\Lambda) \simeq \mathbb{M}(X)$.*

Consider the question of the functional representation of injective Banach lattices. For every cardinal γ, there exists a canonical measure on the unit cube $[0,1]^\gamma$, i.e. the γth power of Lebesgue's measure on $[0,1]$. The associated Banach lattice of integrable functions will be denoted by $L_1([0,1]^\gamma)$. The celebrated Kakutani–Maharam representation result tells us that for each *AL*-space $\mathscr{X}$ there exists a unique family of cardinals $(\delta_\gamma)_{\gamma\in\Gamma\cup\{0\}}$ with Γ a set of infinite cardinals such that δ_γ is either equal to 1 or is uncountable for all $\gamma \in \Gamma$ and

$$\mathscr{X} \simeq l_1(\gamma_0) \oplus \sum\nolimits_{\gamma\in\Gamma}^{\oplus} \delta_\gamma L_1\big([0,1]^\gamma\big), \tag{1}$$

where $\simeq$ stands for lattice isometry, while $\oplus$ and $\sum^{\oplus}$ denote l_1-joins, and δY denotes the l_1-join of δ copies of Y; see [81] and [117]. Thus, the Banach lattices $l^1(\gamma_0)$ and

$L_1([0,1]^\gamma)$ are the "building blocks" for AL-spaces. By transfer the result is true for a Boolean valued representation $\mathscr{X}$ of an injective Banach lattice X. Having worked with the descent and ascent functors, we can find that the building blocks for X are injective Banach lattices $C_\#(K, l^1(\alpha))$ and $C_\#(K, L_1([0,1]^\gamma))$. Every injective Banach lattice is lattice $\mathbb{B}$-isometric to a *injective direct sum* of these building blocks. For an injective Banach lattice X there exist families $(K_{\beta\gamma})_{\beta\in \mathrm{B}(\gamma)}$ $(\gamma \in \Gamma)$ and $(K_\alpha)_{\alpha\in \mathrm{A}}$, where Γ is a set of infinite cardinals, A and $\mathrm{B}(\gamma)$ are the sets of cardinals, and each element of $\mathrm{B}(\gamma)$ is either equal to 1 or is uncountable for all $\gamma \in \Gamma$, such that $K_{\beta\gamma}$ and $K_{\beta\gamma}$ make up the partition of unity in the Boolean algebra of clopen subsets of the Stone representation space of $\mathbb{M}(X)$ and the representation holds:

$$X \simeq_{\mathbb{B}} \Big(\sum_{\alpha\in \mathrm{A}} C_\#(K_\alpha, l^1(\alpha)) \Big)_\infty \boxplus \sum_{\gamma\in\Gamma}^{\boxplus} \Big(\sum_{\beta\in \mathrm{B}(\gamma)} \beta \diamond C_\#(K_{\beta\gamma}, L^1([0,1]^\gamma)) \Big)_\infty , \qquad (2)$$

where $\beta \diamond Y$ stands for the injective direct sum of δ copies of Y and $\sum$ denotes the l_∞-join. The formula (2) is the descent of the internal representation (1), while the injective direct sum $\sum^{\boxplus}$ of injective Banach lattices can be defined as the descent of the internal l^1-join within $\mathbb{V}^{(\mathbb{B})}$. For more details see [60], [61]. The representation (2) of an injective Banach lattice is not unique in general for the same reason as in Remark 38: If $\varkappa < \lambda$ and $\mathbb{V}^{(\mathbb{B})} \models |\varkappa^\wedge| = |\lambda^\wedge|$, then $C_\#(K, L^1([0,1]^\varkappa))$ and $C_\#(K, L^1([0,1]^\gamma))$ are lattice $\mathbb{B}$-isometric. The above enables us to give a complete isometric classification of injective Banach lattices; see [60] and [61].

Remark 45. We indicate a few more results obtained by using the Boolean valued transfer principle for injective Banach lattices. The Daugavet equation in injective Banach latices, injective Banach lattices of operators, the Boolean valued interpretation of the theory of cone absolutely summing operators, and the operators factoring through injective Banach lattices are examined in Kusraev [63]; Kusraev and Wickstead [72] (also see [69]). The following Boolean value version of Ando's Theorem was obtained by Kusraev and Kutateladze [70, Theorem 6.4]: Each closed $\mathbb{B}$-complete sublattice in a $\mathbb{B}$-cyclic Banach lattice X admits a positive contractive projection commuting with projections from $\mathbb{B} = \mathbb{M}(X)$ if and only if there exists a partition of unity $(\pi_\gamma)_{\Gamma\cup\{0\}}$ in $\mathbb{B}$ with Γ being a nonempty set of cardinals such that $\pi_0 X \simeq_{\pi_0\mathbb{B}} L^p(\Phi)$ for some $\mathbb{1} \le p \in \Lambda^u$ and injective Banach lattice $L := L^1(\Phi)$, for which $\mathbb{M}(L) \simeq \pi_0\mathbb{B}$, and $\pi_\gamma X \simeq_{\pi_\gamma\mathbb{B}} C_\#(Q_\gamma, c_0(\gamma))$ for all $\gamma \in \Gamma$, where Q_γ is a clopen subset of the Stone representation space Q of $\mathbb{B}$ corresponding to the projection π_γ.

6 C^*-Algebras and AW^*-Algebras

This section deals with a transfer principle for C^*-algebras and AW^*-algebras and a classification of type I AW^*-algebras. We start with C^*-algebras. See Berberian [12], Sakai [113], and Takesaki [121] for the needed information on the topic.

Definition 46. A $\mathbb{B}$-cyclic *C^*-algebra* or *$\mathbb{B}$-C^*-algebra* A is a C^*-algebra that is a $\mathbb{B}$-cyclic Banach space and for each projection $\pi \in \mathbb{B}$ we have $\pi(xy) = \pi(x)y = x\pi(y)$ and $\pi(x^*) = \pi(x)^*$ for all $x, y \in A$. An element $z \in A$ is *central* provided that z commutes with every member of A. The *center* of a T^*-algebra A is the set $\mathscr{Z}(A)$ of all central elements. Clearly, $\mathscr{Z}(A)$ is a commutative C^*-subalgebra of A and $\mathbb{C}\mathbb{1} \subset \mathscr{Z}(A)$.

The Boolean valued transfer principle for C^*-algebras, discovered by Takeuti [127], is stated below in terms of the complete Boolean algebra of projections. As regards other formulations that use a module structure, see Ozawa [109, Theorem 2], [111, Theorem 6.3] and Takeuti [127, Theorem 1.1]).

Theorem 47. *If $\mathscr{A}$ is a C^*-algebra within $\mathbb{V}^{(\mathbb{B})}$ then $A := \mathscr{A}\Downarrow$ is a $\mathbb{B}$-C^*-algebra. Conversely, for each $\mathbb{B}$-C^*-algebra A there exists C^*-algebra $\mathscr{A}$ within $\mathbb{V}^{(\mathbb{B})}$ such that A is $*$-$\mathbb{B}$-isomorphic to $\mathscr{A}\Downarrow$.*

Definition 48. An *AW^*-algebra* is a C^*-algebra presenting a Baer $*$-algebra. More explicitly, an AW^*-algebra is a C^*-algebra A whose every *right annihilator* $M^\perp := \{y \in A : (\forall x \in M)\ xy = 0\}$ has the form pA, with p a projection. A *projection* p is a hermitian ($p^* = p$) idempotent ($p^2 = p$) element. If $\mathscr{Z}(A) = \{\lambda\mathbb{1} : \lambda \in \mathbb{C}\}$ then the AW^*-algebra A is an *AW^*-factor*.

The symbol $\mathbb{P}(A)$ stands for the set of all projections of an involutive algebra A. Denote the set of all central projections by $\mathbb{P}_c(A)$. Observe that $\bar{\Lambda} := \mathscr{C}\Downarrow$ is a commutative AW^*-algebra and $\mathbb{P}(\bar{\Lambda}) = \mathbb{P}_c(\Lambda)$. If $\bar{\Lambda} = \mathscr{Z}(A)$ then $\bar{\Lambda} = \bar{\Lambda}(\mathbb{B})$ with $\mathbb{B} = \mathbb{P}_c(A)$. An AW^*-algebra A is a $\mathbb{B}$-cyclic C^*-algebra for every order closed subalgebra $\mathbb{B}$ of the complete Boolean algebra $\mathbb{P}_c(A)$. This fact together with Theorem 32 yields the following result due to Ozawa [109].

Theorem 49. *If $\mathscr{A}$ is an AW^*-algebra within $\mathbb{V}^{(\mathbb{B})}$ then $A := \mathscr{A}\Downarrow$ is also an AW^*-algebra and $\mathbb{P}_c(A)$ has an order closed subalgebra isomorphic to $\mathbb{B}$. Conversely, if A is an AW^*-algebra and $\mathbb{B}$ is an order closed subalgebra of the Boolean algebra $\mathbb{P}_c(A)$ then there is an AW^*-algebra $\mathscr{A}$ within $\mathbb{V}^{(\mathbb{B})}$ such that $\mathscr{A}\Downarrow$ is $*$-$\mathbb{B}$-isomorphic with A. Moreover, $\mathscr{A}$ is an AW^*-factor if and only if $\mathbb{B} := \mathbb{P}_c(A)$.*

The classification of an AW^*-algebra into types is determined from the structure of its lattice of projections; see [56] and [113]. It is important to emphasize the *absoluteness* of types; i.e., the Boolean valued representation preserves this classification; see Takeuti [126] and Ozawa [109]. Similar absoluteness theorems in a completely lattice-theoretical framework were established by Nishimura [93]. We recall only the definition of type I AW^*-algebra.

Definition 50. A projection $\pi \in A$ is *abelian* provided that the algebra $\pi A \pi$ is commutative. An algebra A has *type* I, if each nonzero projection in A contains a nonzero abelian projection. Say that a C^*-algebra A is $\mathbb{B}$-*embeddable* whenever there are a type I AW^*-algebra N with $\mathbb{B} = \mathbb{P}_c(N)$ and a $*$-monomorphism $\pi : A \to N$ such that $\pi(A)$ coincides with the bicommutant $\pi(S)''$ of $\pi(A)$ in N. Furthermore, if $\mathbb{B} = \mathbb{P}_c(A)$ then A is *centrally embeddable*.

Definition 51. A $\mathbb{B}$-cyclic Banach space Y is $\mathbb{B}$-*dual* or $\mathbb{B}$-*bidual* provided that, respectively, $Y \simeq_{\mathbb{B}} X^{\#}$ or $Y \simeq_{\mathbb{B}} X^{\#\#}$ for some $\mathbb{B}$-cyclic Banach space X, where $\simeq_{\mathbb{B}}$ stands for isometric $\mathbb{B}$-isomorphy. (Recall that $X^{\#} := \mathscr{L}_{\mathbb{B}}(X, \mathbb{B}(\Lambda))$ and $\Lambda = \Lambda(\mathbb{B})$.) Say that Y is a $\mathbb{B}$-*predual* of X if $Y^{\#} \simeq_{\mathbb{B}} X$ and Y is $\mathbb{B}$-*selfdual* if $Y \simeq_{\mathbb{B}} Y^{\#}$.

Ozawa [111, Theorems A, B, and C] characterized those C^*-algebras that are $\mathbb{B}$-*dual*, $\mathbb{B}$-*bidual*, and $\mathbb{B}$-*selfdual* (in terms of the $\bar{\Lambda}(\mathbb{B})$-module instead of the Boolean algebra of projections $\mathbb{B}$). He also proved that a $\mathbb{B}$-embeddable C^*-algebra has a predual unique up to $\mathbb{B}$-isometry which is a Kaplansky–Hilbert module over $\bar{\Lambda}(\mathbb{B})$; see [111, Theorem D]).

Let X be a Kaplansky–Hilbert module over $\bar{\Lambda}$ and denote by $B_{\Lambda}(X)$ the space of all continuous $\bar{\Lambda}$-linear operators in X. Since a $\bar{\Lambda}$-linear operator is continuous if and only if it has an adjoint, $B_{\Lambda}(X)$ is an AW^*-algebra of type I with center isomorphic to $\bar{\Lambda}$. As it was shown by Kaplansky [45], a type I AW^*-algebra A is isomorphic to $B_{\bar{\Lambda}}(X)$ for some Kaplansky–Hilbert module X over $\bar{\Lambda}(\mathbb{B})$ with $\mathbb{B} = \mathbb{P}_c(A)$. Taking into account Theorem 35, we arrive at the following transfer principle from von Neumann algebras to embeddable AW^*-algebras (see Ozawa [107, Theorem 2.3] and [109, Theorem 6]):

Theorem 52. *Let $\mathscr{A}$ be a C^*-algebra within $\mathbb{V}^{(\mathbb{B})}$ and let A be the bounded descent of $\mathscr{A}$. Then A is a $\mathbb{B}$-embeddable AW^*-algebra if and only if $\mathscr{A}$ is a von Neumann algebra within $\mathbb{V}^{(\mathbb{B})}$. The algebra A is centrally embeddable if and only if $\mathscr{A}$ is a von Neumann factor within $\mathbb{V}^{(\mathbb{B})}$.*

We now present a complete system of $*$-isomorphism invariants for type I AW^*-algebras due to Ozawa [106]. Every automorphism π of a complete Boolean algebra $\mathbb{B}$ can be extended to a Boolean truth-value preserving automorphism π^* of $\mathbb{V}^{(\mathbb{B})}$; see [69, § 1.3].

Definition 53. Two internal cardinals $\alpha, \beta \in \mathbb{V}^{(\mathbb{B})}$ are said to be *congruent* if there is an automorphism π of $\mathbb{B}$ with $\beta = \pi^*(\alpha)$. The *congruence class* of α is defined as $[\alpha] := \{\pi^*(\alpha) : \pi \text{ is an automorphism of } \mathbb{B}\}$. Given a type I AW^*-algebra A with center isomorphic to $\bar{\Lambda}(\mathbb{B})$, define the *degree* $\mathrm{Deg}(A)$ of A as $[\mathrm{Dim}(X)]$, where X is a Kaplansky–Hilbert module over $\bar{\Lambda}(\mathbb{B})$ such that A is $*$-isomorphic to $B_\Lambda(X)$ and $\mathrm{Dim}(X) \in \mathbb{V}^{(\mathbb{B})}$ is the dimension of the Boolean valued representation $\mathscr{X} \in \mathbb{V}^{(\mathbb{B})}$ of X.

Theorem 54. *Two type I AW^*-algebras are $*$-isomorphic if and only if their centers are $*$-isomorphic and they have the same degree. For every nonzero cardinal α within $\mathbb{V}^{(\mathbb{B})}$ there is a type I AW^*-algebra A with $\mathscr{Z}(A)$ isomorphic to $\bar{\Lambda}(\mathbb{B})$ and* $\mathrm{Deg}(A) = [\alpha]$.

Remark 55. The modern structural theory of AW^*-algebras originates with the articles [43]–[45] by Kaplansky. These objects appear naturally by way of algebraization of the theory of von Neumann operator algebras. The study of C^*-algebras and von Neumann algebras by Boolean valued models was started by Takeuti with [125] and [126]. See Korol′ and Chilin [46], Nishimura [91], [94], [98], [101], and Ozawa [104]–[111] for further related developments.

Remark 56. Combining the results about the Boolean valued representations of AW^*-algebras with the analytical representations for dominated operators, we come to some functional representations of AW^*-algebras (see Kusraev [56]): *To each type I AW^*-algebra A there exist a set of cardinals Γ and a family of nonempty extremally disconnected compact spaces $(Q_\gamma)_{\gamma\in\Gamma}$ such that there is a $*$-$\mathbb{B}$-isomorphism:*

$$A \simeq \sum_{\gamma\in\Gamma}^{\oplus} SC_{\#}(Q_\gamma, B(l_2(\gamma))).$$

Remark 57. Boolean valued analysis of AW^*-algebras yields a negative solution to the Kaplansky problem of unique decomposition of a type I AW^*-algebra into the direct sum of homogeneous components. Ozawa gave this solution in [106] and [108]. The lack of uniqueness is tied with the effect of the *cardinal shift*. The cardinal shift is impossible in the case when the Boolean algebra of central idempotents $\mathbb{B}$ under study satisfies the countable chain condition, and so the decomposition in question is unique. Kaplansky established the uniqueness of the decomposition on assuming that $\mathbb{B}$ satisfies the countable chain condition and conjectured that uniqueness fails in general; see [45].

Remark 58. The concept of Kaplansky–Hilbert module was introduced by Kaplansky in [45] under the name AW^*-module. In the introduction he wrote: "... *the new*

idea is to generalize Hilbert space by allowing the inner product to take values in a more general ring then the complex numbers. After the appropriate preliminary theory of these AW-modules has been developed, one can operate with a general AW*-algebra of type I in almost the same manner as with the factor*." In other words, the central elements of an AW^*-algebra can be taken as complex numbers and one can work with factors rather than general AW^*-algebras. Needles to say, this is a version of Kantorovich's heuristic principle; see Remark 23.

7 Miscellany

7.1 The Wickstead problem

An operator in a vector lattice is *band preserving* if each band is its invariant subspace. The following question was raised by Wickstead in [131]: Which vector lattices have the property (sometimes called the *Wickstead property*) that every linear band preserving operator in them is automatically order bounded? One of the principal technical tools is the concept of *d-basis* which is presented in the memoir [3, Section 4]. Boolean valued analysis reduces the Wickstead problem to that of order boundedness of the endomorphisms of the field $\mathscr{R}$ or $\mathscr{C}$ viewed as a vector lattice and algebra over the field $\mathbb{R}^\wedge$ or $\mathbb{C}^\wedge$, respectively; see [69, § 4.2]. In particular, each d-basis is just a Boolean valued Hamel basis [69, § 4.5]. Gutman [33] proved that a vector lattice X has the Wickstead property if and only if the Boolean algebra $\mathbb{P}(X)$ is σ-distributive if and only if $\mathscr{R}$ and $\mathbb{R}^\wedge$ coincide within $\mathbb{V}^{(\mathbb{B})}$. Kusraev [57] established that in a universally complete complex vector lattice X with a fixed f-algebra multiplication the Wickstead property is equivalent to each of the following assertions: (1) there is no nonzero derivation in X; (2) every band preserving endomorphism in X is a band projection; (3) there is no nontrivial band preserving automorphism in X. The history and state of the art of the Wickstead problem are presented in [34] and [69, Chapter 4]. It worth mentioning here that the question of automatic continuity of homomorphisms from a Banach algebra of continuous functions into an arbitrary Banach algebra is independent of ZFC; see Dales and Woodin [18] as well as Dales and Oliveri [17].

7.2 A transfer principle in harmonic analysis

In [124] Takeuti introduced the Fourier transform for the mappings defined on a locally compact abelian group and having as values pairwise commutable normal operators in a Hilbert space. By applying the transfer principle, he developed a general technique for translating classical results to operator-valued functions. In particu-

lar he established a version of the Bochner Theorem describing the set of all inverse Fourier transforms of positive operator-valued Radon measures. Similar results were obtained by Gordon and Lyubetskii within their theory of the Boolean extension of a uniform space; see [28] and [29]. Nishimura [92] extended Takeuti's Boolean valued approach to abstract harmonic analysis on locally compact abelian groups to locally compact groups (not abelian in general). Kusraev and Malyugin in [71] improved Takeuti's results in the following directions: more general arrival spaces (including Banach spaces and Dedekind complete vector lattices) were considered, the class of dominated mappings was identified with the set of all inverse Fourier transforms of order bounded quasi-Radon vector measures, and the construction of a Boolean valued universe was eliminated from the definitions and statements of the results.

7.3 Boolean compactness

Combining the notions of Boolean mixing and compactness yields the concept of mix-*compactness* (or *cyclic compactness*) and the corresponding class of linear operators. Consider a Λ-metric space (X,ρ) with $\Lambda=\mathscr{R}\downarrow$. A subset $K\subset X$ is mix-*compact* if K is mix-complete and for every sequence $(x_n)_{n\in\mathbb{N}}\subset K$ there is $x\in K$ such that $\inf_{n\geqslant k}\rho(x_n,x)=0$ for all $k\in\mathbb{N}$. Clearly, in case $\Lambda=\mathbb{R}$ mix-compactness is equivalent to compactness in the metric topology. The concept of cyclic compactness was first studied by Kusraev [47] and [52]. Section 8.5 in [56] deals with the cyclically compact linear operators on $\mathbb{B}$-cyclic Banach spaces. Gönüllü [31] and [32] found the Lidskii trace formula and the Rayleigh–Ritz minimax formula for cyclically compact operators in Kaplansky–Hilbert modules. The equivalent concept of mix-compact subset of a lattice-normed space was introduced in Gutman and Lisovskaya [35]. Basing on Boolean valued analysis, they proved some counterparts of the three classical theorems for arbitrary lattice-normed spaces over universally complete vector lattices, namely, the boundedness principle, the Banach–Steinhaus Theorem, and the uniform boundedness principle for a compact convex set; see [35, Theorems 2.4, 2.6, and 3.3]. In [63] and [72] Kusraev and Wickstead examine the question of when the space of compact operators is a vector lattice or an injective vector lattice. Moreover, a Dodds–Fremlin–Wickstead type domination result for cyclically compact operators was obtained in [72, Theorem 8.13].

7.4 *JB*-algebras

The JB-algebras are nonassociative real analogs of C^*-algebras and von Neumann operator algebras. The theory of these algebras exists as a branch of functional analysis since the mid 1960s; see [10] and [36]. The Boolean valued approach to

JB-algebras is outlined by Kusraev [54] and [55]. In [54] a $\mathbb{B}$-JB-algebra is defined as a JB-algebra that is a $\mathbb{B}$-cyclic Banach space with respect to a complete Boolean algebra of central idempotents $\mathbb{B}$ and, naturally, it turns out that $\mathbb{B}$-JL-algebras are the bounded descents of JB-algebras from $\mathbb{V}^{(\mathbb{B})}$ [54, Theorem 3.1]. Then it is proved that a $\mathbb{B}$-JB-algebra A is a $\mathbb{B}$-dual space if and only if A is monotone complete and admits a separating set of $\Lambda(\mathbb{B})$-valued normal states [54, Theorem 4.2]. An algebra A satisfying one of these equivalent conditions is a $\mathbb{B}$-JBW-*algebra*. Each $\mathbb{B}$-JBW-factor A admits a unique decomposition $A = eA \oplus e^*A$ with a central projection $e \in \mathbb{B}$, $e^* := 1 - e$, such that the algebra eA has a faithful representation in the algebra of selfadjoint operators on a Kaplansky–Hilbert module and e^*A is isomorphic to $C(Q, M_3^8)$, where Q is the Stone representation space of the Boolean algebra $e^*B := [0, e^*]$ and $M_3^8 := M_3(\mathbb{O})$ is the algebra of hermitian (3×3)-matrices over the Cayley numbers $\mathbb{O}$; see [54, Theorem 4.6]. A full classification of type I_2 AJW-algebras was obtained in [55]. More details and references are collected in [54], [58], and [68].

7.5 Convex analysis

One of the most important concepts in convex analysis is that of *support set* or *subdifferential at zero*, i.e. the convex set of linear operators majorized by a sublinear operator; see [66]. The intrinsic characterization of subdifferentials was first formulated as a conjecture by Kutateladze in [73] and then it was proved by Kusraev and Kutateladze (see [64] and [65]): *A weakly order bounded set of operators is a subdifferential if and only if it is operator convex and closed with respect to pointwise order convergence.* The result is well known for functionals and the Boolean valued transfer principle enables one to translate the result to the operators taking values in the universally complete vector lattice that is the descent of the reals. Similarly, we can recover a subdifferential from its extreme points on using the classical Krein–Milman Theorem and its Milman's inversion. Kutateladze in [74] and [75] weakened the boundedness assumption in the spirit of the classical theory of caps which was developed by Choquet and his followers; see [8] and [112]. The peculiarity of his approach consists in working with the new notion of operator cap. An operator cap is not a cap in the classical sense in general but becomes a usual cap in the scalar case. More precisely, when studying convex sets of operators it is appropriate to use operator caps rather than conventional caps, i.e. the descents of scalar caps from a suitable Boolean valued model; see [66] for details. Recently Kutateladze applied Boolean valued analysis to deriving the operator versions of the classical Farkas Lemma in the theory of simultaneous linear inequalities and proved the Lagrange principle for dominated polyhedral sublinear operators; see [79] and [80].

7.6 Mathematical finance

In order to provide an analytical basis to some problems of *mathematical finance* in a multiperiod setup with a dynamic flow of information, the two approaches were proposed: randomized convex analysis (Filipovic, Kupper, and Vogelpoth [20]) and conditional set theory (Drapeau, Jamnesahn, Karliczek, and Kupper [19]). It is proved in Avilés and Zapata [9, Theorems 2.2 and 3.1] that: (1) the category of mix-complete L^0-convex modules and continuous L^0-linear operators is equivalent to the category of locally convex spaces and continuous linear operators within $\mathbb{V}^{(\mathbb{B})}$; (2) the category of conditional sets and conditional mappings is equivalent to the category of sets and mappings within $\mathbb{V}^{(\mathbb{B})}$; also see [133]. Thus, *Boolean valued analysis* provides a natural framework for the study of *locally L^0-convex analysis* and *conditional set theory* and to explore new applications to conditional risk measures, equilibrium theory, optimal stochastic control, financial preferences, etc. More details and references are collected in [9], [133], and [134].

References

[1] Yuri Abramovich, *Injective envelopes of normed lattices,* Soviet Math. Dokl., **12**(4) 1971, pp. 511–514.

[2] Yuri Abramovich and Charlambos Aliprantis, *Positive Operators*, in William Johnson and Joram Lindenstrauss (eds.) Handbook of the Geometry of Banach Spaces. Vol. 1, Elsevier, Amsterdam etc. 2001, pp. 85–122.

[3] Yuri Abramovich and Arkady Kitover, *Inverses of Disjointness Preserving Operators*, Mem. Amer. Math. Soc. **143**(679), Providence, R. I., 2000.

[4] Charlambos Aliprantis and Owen Burkinshaw, Positive Operators, Acad. Press Inc., London etc. (1985).

[5] Gleb Akilov, Evgenii Kolesnikov, and Anatoly Kusraev, *Lebesgue extension of a positive operator*, Soviet Math. Dokl., **37**(1) 1988, pp. 88–91.

[6] Gleb Akilov, Evgenii Kolesnikov, and Anatoly Kusraev, *On the order continuous extension of a positive operator*, Siberian Math. J., **29** (5) 1988, pp. 24–35.

[7] Wolfgang Arendt, *Factorization by lattice homomorphisms*, Math. Z., **185** (4) 1984, pp. 567–571.

[8] Leonard Asimow, *Extremal structure of well-capped convex set*, Trans. Amer. Math. Soc., **138** (1969), pp. 363–375.

[9] Antonio Avilés and José Miguel Zapata, *Boolean valued models as a foundation for locally L^0-convex analysis and conditional set theory*, J. Appl. Log., **5** (1) 2018, pp. 389–420.

[10] Shavkat Ayupov, *Jordan operator algebras*, J. Soviet Math., **37** (6) 1987, pp. 1422–1448.

[11] John Bell, Boolean-Valued Models and Independence Proofs in Set Theory, Clarendon Press, New York etc. 1985.

[12] Sterling Berberian, Baer $*$-Rings, Springer-Verlag, Berlin 1972.

[13] Donald Cartwright, *Extension of positive operators between Banach lattices*, Mem. Amer. Math. Soc., **164** 1975.

[14] Vladimir Chilin and Jasurbek Karimov, *Laterally complete $C_\infty(Q)$-modules*, Vladikavkaz Math. J., **16** (2) 2014, pp. 69–78.

[15] Nikolai Chupin, *On problem 18 in Goodearl's book "Von Neumann regular rings"*, Siberian Math. J., **32** (1) 1991, pp. 132–137.

[16] Paul Cohen, Set Theory and the Continuum Hypothesis, Benjamin, New York etc. 1966.

[17] Garth Dales and Gianluigi Oliveri, Truth in Mathematics, Clarendon Press, Oxford 1998.

[18] Garth Dales and Hugh Woodin, An Introduction to Independence for Analysts, Cambridge, Cambridge University Press 1987.

[19] Samuel Drapeau, Ascar Jamneshan, Martin Karliczek, and Michael Kupper, *The algebra of conditional sets, and the concepts of conditional topology and compactness*, J. Math. Anal. Appl., **437** (1) 2016, pp. 561–589.

[20] Damir Filipović, Michael Kupper, and Nicolas Vogelpoth, *Separation and duality in locally L^0-convex modules*, J. Funct. Anal., **256** 2009, pp. 3996–4029.

[21] David Fremlin, Measure Theory. Vol. 2, Torres Fremlin, Colchester, 2003 (corrected 2nd printing).

[22] Kenneth Goodearl, Von Neumann Regular Rings, Krieger Publ. Comp., Malabar Fl 1991.

[23] Evgenii Gordon, *Real numbers in Boolean valued models of set theory, and K-spaces*, Soviet Math. Dokl., **18** (4) 1978, pp. 1481–1484.

[24] Evgenii Gordon, *K-spaces in Boolean valued models of set theory*, Soviet Math. Dokl., **23** (4) 1981, pp. 579–582.

[25] Evgenii Gordon, *Theorems of preservation of relations in K-spaces*, Siberian Math. J., **23** (3) 1982, pp. 336–344.

[26] Evgenii Gordon, *Rationally Complete Semiprime Commutative Rings in Boolean Valued Models of Set Theory*, Gorkii 1983 (VINITI, **3286-83**) [in Russian].

[27] Evgenii Gordon, *Strongly Unital Injective Modules as Linear Spaces in Boolean Valued Models of Set Theory*, Gorkii 1984 (VINITI, **770–85**) [in Russian].

[28] Evgenii Gordon and Vassily Lyubetskii, *Some applications of nonstandard analysis in the theory of Boolean valued measures*, Soviet Math. Dokl., **23** (5) 1981, pp. 142–146.

[29] Evgenii Gordon and Vassily Lyubetskii, *Boolean extensions of uniform structures*, in Studies on Non-Classical Logics and Formal Systems, Nauka, Moscow (1983), pp. 82–153.

[30] Richard Haydon, *Injective Banach lattices*, Math. Z., **156** 1977, pp. 19–47.

[31] Uğur Gönüllü, *Trace class and Lidslii trace formula on Kaplansky–Hilbert modules*, Vladikavkaz Math. J., **16** (2) 2014, pp. 29–37.

[32] Uğur Gönüllü, *The Rayleigh–Ritz minimax formula in Kaplansky–Hilbert modules*,

Positivity, **19** (2) 2015, pp. 347–354.

[33] Alexandr Gutman, *Locally one-dimensional K-spaces and σ-distributive Boolean algebras,* Siberian Adv. Math., **5** (2) 1995, pp. 99–121.

[34] Aleksandr Gutman, Anatoly Kusraev, and Semen Kutateladze, *The Wickstead Problem,* Sib. Elektron. Mat. Izv., **5** 2008, pp. 293–333.

[35] Alexandr Gutman and Svetlana Lisovskaya, *The boundedness principle for lattice-normed spaces,* Siberian Math. J., **50** (5) 2009, pp. 830–837.

[36] Harald Hanshe-Olsen and Erling St⊘rmer, Jordan Operator Algebras, Pitman Publ. Inc., Boston etc. 1984.

[37] Thomas Jech, *Abstract theory of abelian operator algebras: an application of forcing,* Trans. Amer. Math. Soc., **289** (1) 1985, pp. 133–162.

[38] Thomas Jech, *First order theory of complete Stonean algebras (Boolean-valued real and complex numbers),* Canad. Math. Bull., **30** (4) 1987, pp. 385–392.

[39] Thomas Jech, *Boolean-linear spaces*, Adv. Math., **81** (2) 1990, pp. 117–197.

[40] Thomas Jech, Set Theory, Springer-Verlag, Berlin 1997.

[41] Leonid Kantorovich, *On semiordered linear spaces and their applications to the theory of linear operations,* Dokl. Akad. Nauk SSSR, **4** (1–2) 1935, pp. 11–14; Engl. transl.: in L. V. Kantorovich, Selected Works. Part I, Gordon and Breach Publishers, 1996, pp. 213–216.

[42] Leonid Kantorovich, *On a class of functional equations,* Dokl. Akad. Nauk SSSR, **4** (5) 1936, pp. 211–216.

[43] Irving Kaplansky, *Projections in Banach algebras,* Ann. of Math., **53** (2) 1951, pp. 235–249.

[44] Irving Kaplansky, *Algebras of type I,* Ann. of Math., **56** (2) 1952, pp. 460–472.

[45] Irving Kaplansky, *Modules over operator algebras,* Amer. J. Math., **75** (4) 1953, pp. 839–858.

[46] Aleksandr Korol′ and Vladimir Chilin, *Measurable operators in a Boolean-valued model of set theory,* Dokl. Akad. Nauk UzSSR, **3** 1989, pp. 7–9.

[47] Anatoly Kusraev, *Boolean valued analysis of duality of extended modules,* Soviet Math. Dokl., **26** (5) 1982, pp. 732–735.

[48] Anatoly Kusraev, *General disintegration formulas,* Soviet Math. Dokl., **26** (6) 1982, pp. 255–259.

[49] Anatoly Kusraev, *Abstract disintegration in Kantorovich spaces,* Siberian Math. J., **25** (5) 1984, pp. 749–757.

[50] Anatoly Kusraev, *Order continuous functionals in Boolean valued models of set theory,* Siberian Math. J., **25** (1) 1984, pp. 57–65.

[51] Anatoly Kusraev, *Banach–Kantorovich spaces,* Siberian Math. J., **26** (2) (1985), pp. 254–259.

[52] Anatoly Kusraev, Vector Duality and Its Applications, Nauka, Novosibirsk 1985 [in Russian].

[53] Anatoly Kusraev, *Linear operators in lattice-normed spaces*, in Studies on Geometry in the Large and Mathematical Analysis. Trudy Inst. Mat., **9** 1987, pp. 84–123 [in Russian].

[54] Anatoly Kusraev, *Boolean valued analysis and JB-algebras*, Siberian Math. J., **35** (1) 1994, pp. 114–122.

[55] Anatoly Kusraev, *On the structure of type I_2 AJW-algebras*, Siberian Math. J., **40** (4) 1999, pp. 764–774.

[56] Anatoly Kusraev, Dominated Operators, Kluwer Academic Publishers, Dordrecht 2000.

[57] Anatoly Kusraev, *Automorphisms and derivations in extended complex f-algebras*, Siberian Math. J., **47** (1) 2006, pp. 97–107.

[58] Anatoly Kusraev, *Boolean valued analysis of normed Jordan algebras*, in Anatoly Kusraev and Vladimir M. Tikhomirov (eds.) Studies on Functional Analysis and Its Applications, Nauka, Moscow (2006), pp. 50–124.

[59] Anatoly Kusraev, *Boolean valued analysis and injective Banach lattices*, Dokl. Math., **85** (3) 2012, pp. 341–343.

[60] Anatoly Kusraev, *The classification of injective Banach lattices*, Dokl. Math., **88** (3) 2013, pp. 1–4.

[61] Anatoly Kusraev, *Injective Banach lattices: A survey*, Eurasian Math. J., **5** (3) 2014, pp. 58–79.

[62] Anatoly Kusraev, *Boolean valued transfer principle for injective Banach lattices*, Siberian Math. J., **25** (1) 2015, pp. 57–65.

[63] Anatoly Kusraev, *Operators on injective Banach lattices*, Vladikavkaz Math. J., **18** (1) 2016, pp. 42–50.

[64] Anatoly Kusraev and Semen Kutateladze, *Analysis of subdifferentials with the aid of Boolean-valued models*, Soviet Math. Dokl., **26** (5) 1982, pp. 202–204.

[65] Anatoly Kusraev and Semen Kutateladze, *Subdifferentials in Boolean-valued models of set theory*, Siberian Math. J., **24** (5) 1983, pp. 735–746.

[66] Anatoly Kusraev and Semen Kutateladze, Subdifferentials: Theory and Applications, Kluwer Academic Publishers, Dordrecht 1995.

[67] Anatoly Kusraev, Semen Kutateladze, Boolean Valued Analysis, Kluwer Academic Publishers, Dordrecht 1999.

[68] Anatoly Kusraev and Semen Kutateladze, Introduction to Boolean Valued Analysis, Nauka, Moscow 2005 [in Russian].

[69] Anatoly Kusraev and Semen Kutateladze, Boolean Valued Analysis: Selected Topics, Southern Math. Inst. 2014 (Trends in Science: The South of Russia. A Math. Monogr. Vol. 6).

[70] Anatoly Kusraev and Semen Kutateladze, *Two applications of Boolean valued analysis*, Siberian Math. J., **29** (5) 2019, pp. 902–910.

[71] Anatoly Kusraev and Sergei Malyugin, *On the Fourier transform of dominated mappings*, Siberian Math. J., **35** (6) 1994, pp. 1141–1156.

[72] Anatoly Kusraev and Antony Wickstead, Some Problems Concerning Operators on

Banach Lattices, Queen's University Belfast, Pure Math. Research Center, Preprint **5** 2016.

[73] Semen Kutateladze, *Support sets of sublinear operators,* Soviet Math. Dokl., **17** (5) 1977, pp. 1428–1431.

[74] Semen Kutateladze, *Caps and faces of sets of operators,* Soviet Math. Dokl., **31** (1) 1985, pp. 66–68.

[75] Semen Kutateladze, *Criteria for subdifferentials that represent caps and faces,* Siberian Math. J., **27** (3) 1986, pp. 417–423.

[76] Semen Kutateladze, *On differences of lattice homomorphisms,* Siberian Math. J., **46** (2) 2005, pp. 393–396.

[77] Semen Kutateladze, *On Grothendieck* subspaces, Siberian Math. J., **46** (3) 2005, pp. 620–624.

[78] Semen Kutateladze, *What is Boolean valued analysis?* Siberian Adv. Math., **17** (2) 2007, pp. 91–111.

[79] Semen Kutateladze, *Farkas lemma revisited,* Siberian Math. J., **51** (1) 2010, pp. 78–87.

[80] Semen Kutateladze, *Polyhedral Lagrange principle,* Siberian Math. J. **52** (3) 2011, pp. 484–486.

[81] Elton Lacey, The Isometric Theory of Classical Banach Spaces, Springer-Verlag, Berlin etc. 1974.

[82] Joachim Lambek, Lectures on Rings and Modules, Blaisdell, Toronto 1966.

[83] Heinrich Lotz, *Extensions and liftings of positive linear mappings on Banach lattices,* Trans. Amer. Math. Soc., **211** (1975), pp. 85–100.

[84] Wilhelmus Luxemburg and Ben de Pagter, *Maharam extension of positive operators and f-algebras,* Positivity, **6** (2) 2002, pp. 147–190.

[85] Wilhelmus Luxemburg and Anton Schep, *A Radon–Nikodým type theorem for positive operators and a dual,* Indag. Math., **40** 1978, pp. 357–375.

[86] Wilhelmus Luxemburg and Adriaan Zaanen, Riesz Spaces. Vol.1, North Holland, Amsterdam and London 1971.

[87] Dorothy Maharam, *On positive operators,* Contemp. Math., **26** 1984, pp. 263–277.

[88] Patrick Mangheni, *The classification of injective Banach lattices,* Israel J. Math., **48** 1984, pp. 341–347.

[89] Peter Meyer-Nieberg, Banach Lattices, Springer-Verlag, Berlin etc., 1991.

[90] Hirokazu Nishimura, *An approach to the dimension theory of continuous geometry from the standpoint of Boolean valued analysis,* Publ. Res. Inst. Math. Sci., **20** (5) 1984, pp. 1091–1101.

[91] Hirokazu Nishimura, *Boolean valued decomposition theory of states*, Publ. Res. Inst. Math. Sci., **21** (5) 1985, pp. 1051–1058.

[92] Hirokazu Nishimura, *Some applications of Boolean valued set theory to abstract harmonic analysis on locally compact groups*, Publ. Res. Inst. Math. Sci., **21** (1) 1985, pp. 181–190.

[93] Hirokazu Nishimura, *On the absoluteness of types in Boolean valued lattices,* Z. Math. Logik Grundlag. Math., **36** (3) 1990, pp. 241–246.

[94] Hirokazu Nishimura, *Some connections between Boolean valued analysis and topological reduction theory for C^*-algebras,* Z. Math. Logik Grundlag. Math., **36** (5) 1990, pp. 471–479.

[95] Hirokazu Nishimura, *Boolean valued Lie algebras,* J. Symbolic Logic, **56** (2) 1991, pp. 731–741.

[96] Hirokazu Nishimura, *Foundations of Boolean valued algebraic geometry,* Z. Math. Logik Grundlag. Math., **37** (5) 1991, pp. 421–438.

[97] Hirokazu Nishimura, *Some Boolean valued commutative algebra,* Z. Math. Logik Grundlag. Math., **37** (4) 1991, pp. 367–384.

[98] Hirokazu Nishimura, *On a duality between Boolean valued analysis and topological reduction theory,* Math. Logic Quart., **39** (1) 1993, pp. 23–32.

[99] Hirokazu Nishimura, *On the duality between Boolean valued analysis and reduction theory under the assumption of separability,* Internat. J. Theoret. Phys., **32** (3) 1993, pp. 443–488.

[100] Hirokazu Nishimura, *Boolean transfer principle from L^*-algebras to AL^*-algebras,* Math. Logic Quart., **39** (1) 1993, pp. 241–250.

[101] Hirokazu Nishimura, *A Boolean valued approach to Gleason's theorem,* Rep. Math. Phys., **34** (2) 1994, pp. 125–132.

[102] Hirokazu Nishimura, *Boolean valued and Stone algebra valued measure theories,* Math. Logic Quart., **40** (1) 1994, pp. 69–75.

[103] Hirokazu Nishimura, *Boolean valued Dedekind domains,* Math. Logic Quart., **37** (1) 1991, pp. 65–76.

[104] Masanao Ozawa, *Boolean valued interpretation of Hilbert space theory,* J. Math. Soc. Japan, **35** (4) 1983, pp. 609–627.

[105] Masanao Ozawa, *Boolean valued analysis and type I AW^*-algebras,* Proc. Japan Acad. Ser. A Math. Sci., **59A** (8) 1983, pp. 368–371.

[106] Masanao Ozawa, *A classification of type I AW^*-algebras and Boolean valued analysis,* Proc. Japan Acad. Ser. A Math. Sci., **36** (4) 1984, pp. 589–608.

[107] Masanao Ozawa, *A transfer principle from von Neumann algebras to AW^*-algebras,* J. London Math. Soc., **32** (1) 1985, pp. 141–148.

[108] Masanao Ozawa, *Nonuniqueness of the cardinality attached to homogeneous AW^*-algebras,* Proc. Amer. Math. Soc., **93** 1985, pp. 681–684.

[109] Masanao Ozawa, *Boolean valued analysis approach to the trace problem of AW^*-algebras,* J. London Math. Soc., **33** (2) 1986, pp. 347–354.

[110] Masanao Ozawa, *Embeddable AW^*-algebras and regular completions,* J. London Math. Soc., **34** (3) 1986, pp. 511–523.

[111] Masanao Ozawa, *Boolean valued interpretation of Banach space theory and module structures of von Neumann algebras,* Nagoya Math. J., **117** 1990, pp. 1–36.

[112] Robert Phelps, Lectures on Choquet's Theorem, Springer-Verlag, Berlin etc. 2001.

[113] Shoichiro Sakai, C^*-Algebras and W^*-Algebras, Springer-Verlag, Berlin etc. 1971.

[114] Helmut Schaefer, Banach Lattices and Positive Operators, Springer-Verlag, Berlin etc. 1974.

[115] Dana Scott, Boolean-Valued Models for Set Theory, Mimeographed Notes for the 1967 Amer. Math. Soc. Symposium on Axiomatic Set Theory, 1967.

[116] Dana Scott, *Boolean Models and Nonstandard Analysis,* in W. A. J. Luxemburg (ed.) Applications of Model Theory to Algebra, Analysis, and Probability, Holt, Rinehart, and Winston, New York etc. 1969, pp. 87–92.

[117] Zbigniew Semadeni, Banach Spaces of Continuous Functions, Warszawa, Polish Scientific Publishers 1971.

[118] Robert Solovay, *A model of set theory in which every set of reals is Lebesgue measurable,* Ann. of Math., **92** (2) 1970, pp. 1–56.

[119] Robert Solovay and Stanley Tennenbaum, *Iterated Cohen extensions and Souslin's problem,* Ann. Math., **94** (2) 1972, pp. 201–245.

[120] Kay Smith, *Commutative regular rings and Boolean valued fields,* J. Symbolic Logic, **49** (1) 1984, pp. 281–297.

[121] Masamichi Takesaki, Theory of Operator Algebras. Vol. 1, Springer-Verlag, New York 1979.

[122] Gaisi Takeuti, Two Applications of Logic to Mathematics, Iwanami and Princeton Univ. Press, Tokyo and Princeton 1978.

[123] Gaisi Takeuti, *Boolean valued analysis,* in Applications of Sheaves (Proc. Res. Sympos. Appl. Sheaf Theory to Logic, Algebra and Anal., Univ. Durham, Durham, 1977), Springer-Verlag, Berlin etc. (1979), pp. 714–731

[124] Gaisi Takeuti, *A transfer principle in harmonic analysis,* J. Symbolic Logic, **44** (3) 1979, pp. 417–440.

[125] Gaisi Takeuti, *Boolean completion and m-convergence,* in Categorical Aspects of Topology and Analysis (Ottawa, Ont., 1980) (Lecture Notes in Math., **915**, Springer-Verlag, Berlin etc. 1982, pp. 333–350.

[126] Gaisi Takeuti, *Von Neumann algebras and Boolean valued analysis,* J. Math. Soc. Japan, **35** (1) 1983, pp. 1–21.

[127] Gaisi Takeuti, *C^*-algebras and Boolean valued analysis,* Japan. J. Math. **9** (2) 1983, pp. 207–246.

[128] Gaisi Takeuti and Wilson Zaring, Axiomatic Set Theory, Springer-Verlag, New York 1973.

[129] Petr Vopěnka, *General theory of ∇-models,* Comment. Math. Univ. Carolinae, **8** (1) 1967, pp. 147–170.

[130] Boris Vulikh, Introduction to the Theory of Partially Ordered Spaces, Wolters-Noordhoff Scientific Publications LTD, Groningen 1967.

[131] Antony Wickstead, *Representation and duality of multiplication operators on*

Archimedean Riesz spaces, Comp. Math., **35** (3) 1977, pp. 225–238.

[132] Adriaan Zaanen, Riesz Spaces. Vol. 2, North Holland, Amsterdam etc. 1983.

[133] José Miguel Zapata, A Boolean Valued Models Approach to L^0-Convex Analysis, Conditional Risk and Stochastic Control, PhD Thesis, Universidad de Murcia 2018.

[134] José Miguel Zapata, *A Boolean valued model approach to conditional risk,* Vladikavkaz Math. Journal **21** (4), 2019, pp. 71–89.

Received 27 March 2019

The Γ-ultraproduct and Averageable Classes

Will Boney
Texas State University
wb1011@txstate.edu

Abstract. This paper introduces the Γ-ultraproduct, which is designed to take a collection of structures omitting some fixed set of unary types Γ and average them into a structure that also omits those types. The motivation comes from the Banach space ultraproduct, and generalizes other existing constructions such as the torsion submodule. Motivated by examples and counterexamples, we explore conditions on classes that make the Γ-ultraproduct well-behaved and apply results from the existing literature on classification for nonelementary classes. We use torsion modules over PIDs as an extended example.

1 Introduction

Ultraproducts are an invaluable tool in first-order model theory. The ability to create a new structure that is the "average" of some collection of structures has far-reaching implications, most importantly the compactness theorem. When trying to adapt first-order results (such as various results of classification theory) to nonelementary contexts, the lack of compactness is a major stumbling block. One strategy is to use set-theoretic hypotheses to allow very complete ultrafilters (as was done in [5,16,17]). Another approach is to assume that the class satisfies some fragment of compactness; an example of this is the property tameness, which was introduced by Grossberg and VanDieren [12] and has seen a large amount of activity in recent years.

We examine a different approach. Rather than appealing to the uniform construction of the ultraproduct, we fix a collection Γ of types to be omitted in advance and then build the Γ-ultraproduct with the express purpose of creating an average that omits those types. More precisely, fix the following:

- a language τ;

- a collection of unary τ-types Γ; and
- a collection of τ-structures $\{M_i : i \in I\}$ that each omit every type in Γ.

We sometimes refer to this collection as *the data*, see Hypothesis 2.1.

The main definition of this paper is the Γ-ultraproduct of this data by some ultrafilter U, which is denoted $\prod^{\Gamma} M_i/U$.

Definition 1.1. *Fix an ultrafilter U on I.*

$$\prod_{i\in I}^{\Gamma} M_i := \{f \in \prod M_i \quad : \quad \text{there is some } X_f \in U \text{ such that, for each } p \in \Gamma, \text{ there is a } \phi_f^p(x) \in p \text{ such that } M_i \models \neg\phi_f^p(f(i)) \text{ for each } i \in X_f\}$$

- *Form $\prod^{\Gamma} M_i/U$ by giving it universe $\prod^{\Gamma} M_i/U := \{[f]_U : f \in \prod^{\Gamma} M_i\}$ and inheriting the functions and relations from the full ultraproduct $\prod M_i/U$.*
- *If $\Gamma = \{p\}$, then we write $\prod^p M_i/U$.*

Given $[f]_U \in \prod^{\Gamma} M_i/U$, we call a choice function $p \in \Gamma \mapsto \phi_f^p$ as in the definition a *witness* for $[f]_U$'s inclusion in the Γ-ultraproduct. We typically denote witnesses and choice functions by $\mathcal{C}$. Note that there are often many witnesses for a single element.

Unlike the normal ultraproduct, there is no reason to suspect that the Γ-ultraproduct is always well-behaved or is even a τ-structure; these issues and examples of where things go wrong are explored in Section 2. Note that the assumption that the types of Γ are unary is crucial for this definition. This allows the inclusion criteria for $\prod_{i\in I}^{\Gamma} M_i$ to be local, i.e., only depend on the function on consideration. If the types were *not* unary (such as those expressing a group is locally finite), then determining wether a choice function f were to be included would require a witness that involves the other included choice functions in some way. There seems to be no uniform way to generalize the above definition in this case. Indeed, simply coding tuples as single elements with projection functions does not avoid this necessity: the resulting Γ-ultraproduct might omit the coded types, but fail to satisfy the sentences stating that finite tuples are coded as elements.

Section 3 introduces *averageable classes* (roughly nonelementary classes where the appropriate Γ is well-behaved) and applies some results from the classification theory of Abstract Elementary Classes; Theorem 3.12 here gives a dividing line in the number of models for averageable classes. Section 4 gives several examples

of averageable classes, including dense linearly ordered groups with a cofinal $\mathbb{Z}$-chain. Section 5 develops the example of torsion modules over a PID, including the appropriate Łoś' Theorem and some stability theory.

This construction can be seen as a generalization of two well-known constructions: ultraproducts of multi-sorted structures and Banach space ultraproducts. Subsection 4.4 shows how to view the ultraproduct of multi-sorted structures as the appropriate Γ-ultraproduct. Moreover, if Γ is finite (as it is in most of our examples, with Banach spaces and Archimedean fields being the only non-examples in this paper), there is a single type p_Γ such that omitting p_Γ is equivalent to omitting all of Γ. Then, we could attempt to impose a sorted structure on a model omitting Γ by which formula of p_Γ it omits, and attempt to translate the language and syntax to a sorted one. This would be an alternate presentation of these results: being able to sort the language corresponds to Γ-closed (Definition 2.3) and being able to sort the formulas corresponds to Γ-nice (Definition 2.10). We chose the current presentation in part because some choice of equally valid presentations must be made, but also to accommodate cases of omitting infinitely many types and to avoid the unnaturality discussed below. We discuss a third possible presentation in Section 2.5.

In the standard Banach space ultraproduct, the elements of $\prod \mathcal{B}_i/U$ are sequences of bounded norm that are modded out by the equivalence relation

$$(x_i) \sim_U (y_i) \iff \lim_U \|x_i - y_i\|^{\mathcal{B}_i} = 0$$

In the standard model-theoretic ultraproduct, the elements of $\prod M_i/U$ are sequences that are modded out by the equivalence relation

$$(x_i) \sim_U (y_i) \iff \{i : x_i = y_i\} \in U$$

Both constructions contain a step that ignores U-small differences; this is the equivalence relations. However, the Banach space ultraproduct contains an extra step that excludes unbounded sequences. In model theoretic language, this amounts to excluding sequences that would realize the type $\{\|x\| > n : n < \omega\}$. The model theoretic ultraproduct has no similar step. We add such a step to arrive at $\prod^\Gamma M_i/U$. Example 4.1 goes into greater detail about the application of the Γ-ultraproduct to Banach spaces. Indeed, this example was the original motivation for the Γ-ultraproduct as an attempt to generalize the extra step of throwing away unbounded elements to more general situations. Note that, in continuous first-order logic (see [4]), attention is restricted to uniformly bounded metric spaces and, thus, avoid the extra step. Ben Yaacov [3] has explored continuous logic in unbounded metric spaces. The key there is to restrict the logic to only allow quantifiers that specify where that type is

omitted, that is, quantifiers that turn $\phi(x, \mathbf{y})$ into $\exists x \, (\|x\| < n \wedge \phi(x, \mathbf{y}))$ for some particular $n < \omega$; see Observation 2.9 for a discussion of that technique here.

Many of the proofs of this paper (particularly the basic exploration of the Γ-ultraproduct in Section 2) are straightforward (especially in light of the above comparisons). However, there seems to be no place in the literature that discusses these constructions in this generality or applies them to achieve compactness-like results in nonelementary classes. In particular, the results of Section 5 on the compactness and classification theory of torsion modules over PIDs is new. While these results could have been obtained by "sorting" the structures and applying the ultraproduct of sorted structures[1], this class is always considered as a nonelementary (single-sorted) class. Moreover, the translation to a sorted class would be very unnatural: the single addition function $+$ would replaced by a collection of addition functions $\{+_{r,r'} \mid r, r' \in R\}$ (and similarly for other functions). Moreover, formulas like "$\exists z(x + z = y)$" would not survive the sorting translation and one would be forced to specify an annihilator of x, y, and z to use such a formula. Thus, we prefer to work with torsion modules as a "sortable" class, rather than one that is actually sorted.

2 Properties of $\prod^{\Gamma} M_i/U$

Our main goal will be analyzing compactness in classes of the form $(EC(T, \Gamma), \prec)$ or $(EC(T, \Gamma), \subset)$ via the Γ-ultraproduct (recall the definition of the Γ-ultraproduct from Definition 1.1 and that $EC(T, \Gamma)$ is the class of all models of T that omit each type in Γ). However, in this section we analyze this construction in more generality; we specialize back to these classes in Section 3. For the rest of this section and the next, fix the data that goes into the Γ-ultraproduct.

Hypothesis 2.1. *Fix the following:*

- *a language τ;*
- *a collection of unary τ-types Γ; and*
- *a collection of τ-structures $\{M_i : i \in I\}$ that each omit every type in Γ.*

This definition and the discussion below work in a great deal of generality, in particular allowing many unary types of different sizes. In concrete cases, Γ often

[1] Or, in the case $R = \mathbb{Z}$, imposing a metric on torsion abelian groups by setting $d(g, h) = \log o(g - h)$.

consists of a single countable type and the reader can simplify to this case with little loss.

The analysis of $\prod^\Gamma M_i/U$ breaks along two main questions:

- Is $\prod^\Gamma M_i/U$ a structure, specifically a substructure of $\prod M_i/U$?
- Is $\prod^\Gamma M_i/U$ an elementary substructure of $\prod M_i/U$?

We analyze each of this separately, although we first provide examples that the answer to each question can be no.

Example 2.2.

1. *Set $M = (\omega, +, |, 2)$, $I = \omega$, $p(x) = \left\{(2^k \mid x) \wedge (x \neq 0) : k < \omega\right\}$, where the ' $|$' is the symbol for 'divides.' Then $[n \mapsto 1]_U, [n \mapsto 2^n - 1]_U \in \prod^p M/U$, but*

$$[n \mapsto 1]_U + [n \mapsto 2^n - 1]_U = [n \mapsto 2^n]_U \notin \prod^p M/U$$

   Thus $\prod^p M/U$ is not closed under addition.

2. *Let τ be the two-sorted language $\langle N_1, N_2; +_1, \times_1, 1_1; +_2, \times_2, 1_2; \times_{1,2}\rangle$ where $\times_{1,2} : N_1 \times N_2 \to N_1$. Take $M = \langle \mathbb{N}, \mathbb{N}'; +, \times, 1; +', \times', 1'; \times^*\rangle$ where $\mathbb{N}$ and $\mathbb{N}'$ are disjoint copies of the naturals and $\times^*$ is also normal multiplication. Then this structure omits the type of a nonstandard element of the second sort $p(x) = \{N_2(x) \wedge (1 + \cdots + 1 \neq x) : n < \omega\}$. Then $\prod^p M/U$ is a structure. In particular, N_2 remains standard but N_1 is just $\prod \mathbb{N}/U$. To see the failures of Łoś' Theorem described above,*

   - *the formula $\psi(x) \equiv$ "$\exists y \in N_2(1_1 \times_{1,2} y = x)$" is true of all $n \in N_1^M$, but is not true of $[n \mapsto n]_U \in N_1^{\prod^p M/U}$.*
   - *the sentence $\phi \equiv$ "$\forall x \in N_1 \exists y \in N_2(1_1 \times_{1,2} y = x)$" is true in M, but not in $\prod^p M/U$ for the above reason.*

Note that the first example shows that the class of classically valued fields does not fit into the framework described here; compactness results in that class will be explored in Boney [8].

These examples and Example 2.16 below give an indication of when things don't fit nicely into this framework. Section 4 collects several positive examples.

2.1 Structure

For $\prod^\Gamma M_i/U$ to be a structure, all that is necessary is that $\prod^\Gamma M_i/U$ is closed under functions. This means that, if $[f_0,]_U \ldots, [f_{n-1}]_U \in \prod^\Gamma M_i/U$ have witnesses to their inclusion and F is a function of the structure $\prod M_i/U$, then $F([f_0]_U, \ldots, [f_{n-1}]_U)$ has a witness as well. However, in many cases, there is a degree of uniformity where tuples with the same sequence of witnesses are always mapped to an element with a fixed witness.

Definition 2.3. *The collection $\{M_i : i \in I\}$ is Γ-closed iff for all n-ary functions F of τ, there is a function g_F that takes in n choice functions on Γ and outputs a choice function on Γ such that*

for all $[f_1]_U, \ldots, [f_n]_U \in \prod^\Gamma M_i/U$ with witnesses $\mathcal{C}_1, \ldots, \mathcal{C}_n$, we have that, for each $i \in I$ and $p \in \Gamma$,

$$M_i \vDash \neg\phi\left(F\left(f_1(i), \ldots, f_n(i)\right)\right)$$

where $\phi = g_F\left(\mathcal{C}_1, \ldots, \mathcal{C}_n\right)(p)$

Abelian torsion groups are an example of this: the order of $h+k$ can be computed from the orders of h and k; see Section 4.2. There, g_+ takes in natural numbers (representing choice functions on the singleton set of the torsion type) and outputs a natural number such that $g_+(o(h), o(k))$ is an order of $h + k$.

It is clear that if $\{M_i : i \in I\}$ is Γ-closed, then $\prod^\Gamma M_i/U$ is a structure for all ultrafilters U; the witness to $F([f_0]_U, \ldots, [f_{n-1}]_U)$ is $g_F(\mathcal{C}_1, \ldots, \mathcal{C}_n)$.

The main advantage of Γ-closedness is in the study of classes of models omitting Γ when Γ is finite because this property is captured by the first order theory of M. We say that a class $EC(T, \Gamma)$ is Γ-closed iff every collection of models from it is Γ-closed.

Proposition 2.4. *Suppose Γ is finite and T is $\forall(\Gamma \cup \neg\Gamma)$-complete. Then $EC(T, \Gamma)$ is Γ-closed iff some collection $\{M_i \in EC(T, \Gamma) : i \in I\}$ is.*

The notation "$\forall(\Gamma \cup \neg\Gamma)$-complete" means that T decides all first order sentences whose quantifiers are a universal followed by a quantifier string that appears in Γ or a universal followed by the negation of such a string. In practical terms, this means the large formula a few lines below is decided by the theory. Similar expressions have the obvious meaning.

Proof: Being Γ-closed can be expressed by the following scheme: for each $F \in \tau$, sequence of choice functions $\mathcal{C}_0, \ldots, \mathcal{C}_{n-1}$, and type $p \in \Gamma$, include the sentence

$$\forall x_0, \ldots, x_{n-1} \left(\left(\bigwedge_{q \in \Gamma, i<n} \neg \mathcal{C}_i(q)(x_i) \right) \rightarrow \neg g_F(\mathcal{C}_0, \ldots, \mathcal{C}_{n-1})(p)(F(x_0, \ldots, x_{n-1})) \right)$$

where g_F is the witness for F from the definition of Γ-closed. Since Γ is finite, this is first order of the desired complexity. †

If $\prod^{\Gamma} M_i/U$ is a structure, then it is a substructure of $\prod M_i/U$. This immediately gives us a universal version of Łoś' Theorem.

Theorem 2.5 (Universal Łoś' Theorem)**.** *Suppose $\prod^{\Gamma} M_i/U$ is a structure. If $\phi(x_0, \ldots, x_n)$ is a universal formula and $[f_0]_U, \ldots, [f_{n-1}]_U \in \prod^{\Gamma} M_i/U$, then*

$$\{i \in I : M_i \models \phi(f_0(i), \ldots, f_{n-1}(i))\} \in U \implies \prod^{\Gamma} M_i/U \models \phi([f_0]_U, \ldots, [f_{n-1}]_U)$$

Proof: The key point is that, since $\prod^{\Gamma} M_i/U$ is a structure, it is a substructure of the full ultraproduct $\prod M_i/U$. Thus, universal formulas transfer from $\prod M_i/U$ to $\prod^{\Gamma} M_i/U$. †

Remark 2.6. *A proof by induction on formula complexity (mirroring the proof of the standard version of Łoś' Theorem) is also possible. This proof is longer, but provides extra information: if ϕ and ψ are formulas that transfer from a U-large set of M_i to $\prod^{\Gamma} M_i/U$, then conjunction, disjunction, and universal quantification preserves this transfer, while negation reverses it. This finer analysis is used in Section 5.2.*

This has important implications for Γ consisting of existential types.

Proposition 2.7. *Suppose $\prod^{\Gamma} M_i/U$ is a structure and the types of Γ contain only existential formulas.*

1. *$\prod^{\Gamma} M_i/U$ omits Γ.*
2. *If Γ is finite and each M_i satisfies a common (and complete) $\exists\forall$-theory $T_{\exists\forall}$, then $\prod^{\Gamma} M_i/U \models T_{\exists\forall}$.*

Proof:

1. Let $[f]_U \in \prod^\Gamma M_i/U$ and $p \in \Gamma$. By definition, there is $\phi_p \in p$ such that $\{i \in I : M_i \vDash \neg\phi_p(f(i))\} \in U$. Since $\neg\phi_p$ is universal, $\prod^\Gamma M_i/U \vDash \neg\phi_p(m)$ by Universal Łoś' Theorem 2.5.

2. Let $\exists \mathbf{x}\psi(\mathbf{x})$ be in $T_{\exists\forall}$ with ψ universal and fix some $i_0 \in I$. Then there are $m_1, \ldots, m_n \in M_{i_0}$ such that $M_{i_0} \vDash \psi(m_1, \ldots, m_n)$. Because M_{i_0} omits Γ (recall Hypothesis 2.1), for each $p \in \Gamma$ and $\ell = 1, \ldots, n$, there is $\phi_p^\ell \in p$ such that $M_{i_0} \vDash \neg\phi_p^\ell(m_\ell)$. Then,

$$M_{i_0} \vDash \exists \mathbf{x} \left(\psi(x_1, \ldots, x_n) \wedge \bigwedge_{p\in\Gamma;\ell\leq n} \neg\phi_p^\ell(x_\ell) \right)$$

This is an $\exists\forall$-sentence, and is thus part of $T_{\exists\forall}$. For each $i \in I$, there is $m_1^i, \ldots, m_n^i \in M_i$ such that

$$M_i \vDash \psi(m_1^i, \ldots, m_n^i) \wedge \bigwedge_{p\in\Gamma;\ell\leq n} \neg\phi_p^\ell(m_\ell^i)$$

Define functions $g_1, \ldots, g_n$ by $g_\ell(i) = m_\ell^i$. Then the function $p \mapsto \phi_p^\ell$ witnesses that $[g_\ell]_U \in \prod^\Gamma M_i/U$. By Universal Łoś' Theorem 2.5, we have that

$$\prod^\Gamma M_i/U \vDash \psi\left([g_1]_U, \ldots, [g_n]_U\right)$$

So $\prod^\Gamma M_i/U \vDash \exists \mathbf{x}\psi(\mathbf{x})$, as desired.

†

Indeed, if Γ is finite (but not necessarily existential), a similar proof shows that if each M_i satisfy a common $\exists(\neg\Gamma \cup \forall)$-theory, then $\prod^\Gamma M_i/U$ models the $\exists\forall$ part of the common theory. Note that the $\exists\forall$ level is sharp as Example 2.2.(2) gives an example of a Γ-ultrapower that doesn't have the same $\forall\exists$ theory as the original model.

2.2 Elementary Substructure

For this subsection, we assume that the Γ-ultraproduct forms a structure.

Hypothesis 2.8. *Using the notation of Hypothesis 2.1, $\prod^\Gamma M_i/U$ is a structure.*

The second line of analysis of the Γ-ultraproduct is finding the class of formulas $\phi(\mathbf{x})$ such that for all $[f_0]_U, \ldots, [f_{n-1}]_U \in \prod^\Gamma M_i/U$,

$$\{i \in I : M_i \vDash \phi(f_0(i), \ldots, f_{n-1}(i))\} \in U \iff \prod^\Gamma M_i/U \vDash \phi([f_0]_U, \ldots, [f_{n-1}]_U)$$

We know that this class contains the universal formulas and, indeed, is closed under universal quantification. However, Example 2.2.(2) shows that existential quantification causes problems. The problem is that the witnesses to an existential formula involving parameters that omit Γ uniformly might not omit Γ uniformly.

When Γ is finite, some level of existential quantification is allowed by essentially forcing a witness to exist as part of the condition on the existential.

Observation 2.9. *Suppose* Γ *is finite. If Łoś' Theorem holds for* $\phi(x, \mathbf{y})$ *then it also holds for*

$$\exists x \left(\phi(x, \mathbf{y}) \wedge \bigwedge_{p \in \Gamma} \neg \mathcal{C}(p)(x) \right)$$

for any choice function $\mathcal{C}$ *on* Γ*. Recalling Ben Yaacov's work on metric ultraproducts in unbounded metric structures, this condition is similar to his requirement that the formula is bounded [3, Definition 2.7].*

In general, there are two main ways of guaranteeing the transfer of all existential statements: Γ-niceness and quantifier elimination.

Γ-niceness is the appropriate generalization of Γ-closed to the situation of existentials.

Definition 2.10. $\{M_i : i \in \Gamma\}$ *is* Γ*-nice iff for all existential formulas* $\psi :\equiv \exists x \phi(x, \mathbf{y})$ *from* τ*, there is a function* g_ψ *that takes in* $\ell(\mathbf{y})$ *choice functions on* Γ *and outputs a choice function on* Γ *such that*

for all $[f_1]_U, \ldots, [f_n]_U \in \prod^\Gamma M_i/U$ *with witnesses* $\mathcal{C}_1, \ldots, \mathcal{C}_n$ *and* $i \in I$*, if* $M_i \vDash \exists x \phi(x, f_1(i), \ldots, f_n(i))$*, then there is* $m \in M_i$ *such that, for all* $p \in \Gamma$*,*

$$M_i \vDash \phi(m, f_1(i), \ldots, f_n(i)) \wedge \neg \chi(m)$$

$$\text{where } \chi = g_\psi(\mathcal{C}_1, \ldots, \mathcal{C}_n)(p).$$

The following basic facts about Γ-niceness are obvious.

Proposition 2.11. *1. If the data is* Γ*-nice, then it is* Γ*-closed.*

2. The data is Γ*-nice iff there is a skolemization of the data that is* Γ*-closed.*

3. If Γ *is finite, then being* Γ*-nice is first-order expressible.*

Proof: For (1), set $g_F := g_{\exists x(F(\mathbf{y})=x)}$. For (2), take $g_{F_{\exists x\phi(x;\mathbf{y})}} = g_{\exists x\phi(x;\mathbf{y})}$ where $F_{\exists x\phi(x;\mathbf{y})}$ is the skolem function for $\exists x\phi(x;\mathbf{y})$. For (3), the proof follows as in Proposition 2.7.(2). †

The main use of Γ-niceness is as a sufficient condition for Łoś' Theorem to hold.

Theorem 2.12 (Łoś' Theorem)**.** *Suppose the data is* Γ*-nice and* U *is an ultrafilter on* I*. If* $\phi(x_1, \ldots, x_n)$ *is a formula and* $[f_1]_U, \ldots, [f_n]_U \in \prod^\Gamma M_i/U$*, then*

$$\{i \in I : M_i \models \phi(f_1(i), \ldots, f_n(i))\} \in U \iff \prod^\Gamma M_i/U \models \phi([f_1]_U, \ldots, [f_n]_U)$$

Proof: By Proposition 2.11 and Theorem 2.5 (and Remark 2.6), all that needs to be shown is that adding an existential quantifier maintains transfer from "true in U-many M_i's" to "true in $\prod^\Gamma M_i/U$." That is, suppose $\phi(\mathbf{y}) = \exists x\psi(x, \mathbf{y})$ such that, for all $[f_0]_U, \ldots, [f_n]_U \in \prod^\Gamma M_i/U$,

$$\{i \in I : M_i \models \psi(f_0(i), \ldots, f_n(i))\} \in U \iff \prod^\Gamma M_i/U \models \psi([f_0]_U, \ldots, [f_n]_U)$$

We want to show that, for all $[f_1]_U, \ldots, [f_n]_U \in \prod^\Gamma M_i/U$,

$$\begin{aligned} X := \{i \in I : M_i \models \exists x\psi(x, f_1(i), \ldots, f_{n-1}(i))\} \in U \implies \\ \prod^\Gamma M_i/U \models \exists x\psi(x, [f_1]_U, \ldots, [f_{n-1}]_U) \end{aligned}$$

Suppose we have such a tuple with witnesses $\mathcal{C}_1, \ldots, \mathcal{C}_n$. By Γ-niceness, for each $i \in X$, there is $m_i \in M_i$ as in the definition. Then $[i \mapsto m_i]_U$ is in $\prod^\Gamma M_i/U$, as witnessed by $g_\psi(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ and $\{i \in I : M_i \models \psi(m_i, f_1(i), \ldots, f_n(i))\} \in U$. By the induction assumption,

$$\prod^\Gamma M_i/U \vDash \psi([i \mapsto m_i]_U, [f_1]_U, \ldots, [f_n]_U)$$

as desired. †

Once we have the full strength of Łoś' Theorem, we are guaranteed the resulting structure omits the desired types.

Proposition 2.13 (Type Omission)**.** *Suppose the data is* Γ*-nice (or just Łos' Theorem holds). Then* $\prod^{\Gamma} M_i/U$ *omits each type in* Γ*.*

Proof: Let $[f]_U \in \prod^{\Gamma} M_i/U$. This is witnessed by some $\mathcal{C}$. For each $p \in \Gamma$,

$$\{i \in I : M_i \vDash \neg \mathcal{C}(p)\,(f(i))\} \in U$$

By Theorem 2.12,

$$\prod^{\Gamma} M_i/U \vDash \neg \mathcal{C}(p)\,([f]_U)$$

So every element of $\prod^{\Gamma} M_i/U$ does not realize any type from Γ. †

Summarizing our results so far, we have the following.

Corollary 2.14. *If the data is* Γ*-nice, then* $\prod^{\Gamma} M_i/U$ *is a* τ*-structure that satisfies Łoś' Theorem and omits every type in* Γ*. In particular, if* $M_i \in EC(T, \Gamma)$ *for all* $i \in I$*, then* $\prod^{\Gamma} M_i/U \in EC(T, \Gamma)$*.*

Proof: By Theorems 2.12 and 2.13. †

We now turn to another method for proving Łoś' Theorem that seems more ad-hoc, but has proven more useful in practice (at least in Sections 4 and 5): quantifier elimination. This method involves directly proving that the Γ-ultraproduct is a structure that models the theory T and, if T has only partial quantifier elimination, proving that Łoś' Theorem holds for the necessary class of formulas. Examples of this are $DLOG\mathbb{Z}$ (Section 4.3) and torsion modules over PIDs (Section 5). This final example makes use of the full generality of the following proposition since modules only have quantifier elimination to p. p. formulas.

Proposition 2.15. *Fix a collection of formulas* Δ*. Suppose each* $M_i \vDash T$*,* $\prod^{\Gamma} M_i/U \vDash T$*, T has quantifier elimination to* Δ*-formulas, and Łoś' Theorem for* Δ*-formulas holds. Then the full Łoś' Theorem holds.*

Proof: Immediate. †

2.3 Ultrapowers

We now turn our attention to ultrapowers, where $M_i = M$ for all $i \in I$. In this case, set $æ : M \to \prod^{\Gamma} M_i/U$ to be the ultrapower map $æ(m) = [i \mapsto m]_U$. This function is well-defined even if $\prod^{\Gamma} M_i/U$ is not a structure, and the statement of

Łos' Theorem is equivalent to æ being an elementary embedding. We would also like to know when this construction gives rise to a proper extension. Unfortunately, this is not always the case.

Example 2.16. *Let U be an ultrafilter on I. Take the ultraproduct of $\mathbb{N} = \langle \omega, +, \cdot, < \rangle$ omitting $p(x) = \{x > n : n < \omega\}$; then $j : \mathbb{N} \cong \prod^p \mathbb{N}/U$.*

Proof: The data is obviously Γ-closed: $g_+(x, y) = x + y$ and $g_\cdot(x, y) = x \cdot y$. This is enough to make the conclusion well-formed, i.e. $\prod^p \mathbb{N}/U$ is a structure. If $f \in \prod^p \mathbb{N}$, then there is some $k_f < \omega$ such that $f(i) < k_f$ for all $i \in I$. Since U is ω-complete (as are all ultrafilters) and k_f is finite, there is some $n_f < k_f$ such that $\{i \in I : f(i) = n_f\} \in U$. Thus, $[f]_U = [i \mapsto n_f]_U$ and the mapping $h : \prod^p \mathbb{N}/U \to \mathbb{N}$ by $h([f]_U) = n_f$ is an isomorphism. †

This did not give rise to a new model because the choice function witnessing $f \in \prod^p \mathbb{N}$, here characterized by a single natural number, determined which element of $\mathbb{N}$ the function represented. In order to ensure that j is not surjective, we need to ensure that there are many choices that give rise to the same $\mathcal{C}$. Indeed, this characterization is reversible.

Theorem 2.17. *Suppose M omits Γ. Then the following are equivalent:*

1. *There is infinite $X \subset M$ and choice function $\mathcal{C}$ such that, for all $m \in X$ and $p \in \Gamma$,*
$$M \vDash \neg \mathcal{C}(p)(m)$$
2. *There is a nonprincipal ultrafilter U such that $j : M \to \prod^\Gamma M/U$ is not surjective.*

Proof: For (1) implies (2), let U be any nonprincipal ultrafilter on ω. Then let $f : \omega \to X$ enumerate distinct members of X. By definition of X, $f \in \prod^\Gamma M$. Since U is nonprincipal, f is not U-equal to any constant function. Thus, $[f]_U$ is an extra element in $\prod^\Gamma M/U$.
For (2) implies (1), let $[f]_U$ be a new element of $\prod^\Gamma M/U$. Then, for each $m \in M$,

$$X_f \cap \{i \in I : f(i) = m\} \notin U$$

Then $f\text{“}X_f \subset M$ is infinite and, taking $\mathcal{C}$ to be the choice function witnessing $f \in \prod^\Gamma M$, we have that, for each $m \in f\text{“}X_f$ and $p \in \Gamma$,

$$M \vDash \neg \mathcal{C}(p)(m)$$

†

Corollary 2.18. *If $\|M\| > \prod_{p\in\Gamma} |p|$, then there is an ultrafilter U such that $j : M \to \prod^\Gamma M/U$ is not surjective.*

Proof: For each $x \in M$, pick a choice function $\mathcal{C}^x$ such that, for all $p \in \Gamma$, $M \vDash \neg\mathcal{C}^x(p)(x)$. There are $\prod |p|$ many possible values for $\mathcal{C}^x$. Since $\|M\|$ is greater than this, there must be some infinite $X \subset |M|$ such that the choice is constant. Then apply Theorem 2.17. †

Corollary 2.19. *Suppose p is countable and M is uncountable. If U is nonprincipal, then $\prod^p M/U \ncong M$.*

2.4 Changing the language

One strength of the ultraproduct is its robustness under changing the language. Unfortunately, the Γ-ultraproduct does not share this robustness. However, some results remain, which gives rise to a form of Γ-compactness in Theorem 3.3, and there are sometimes natural conditions, such as in Section 4.1, that determine when the expansions are well-behaved.

As with quantifier elimination, adding constants does not impact the properties discussed above (Γ-closed, etc.). As an example, we show that Γ-niceness is preserved.

Proposition 2.20. *Suppose $\{M_i : i \in I\}$ is Γ-nice and M_i^* is an expansion of M_i by constants $\{c_j : j < \kappa\}$ such that, for all $j < \kappa$, $c_j^{M_i}$ omits each type at the same place for all $i \in I$; that is, for each $p \in \Gamma$, there is $\phi_j(x) \in p$ such that $M_i \vDash \neg\phi_j(c_j)$ for all $i \in I$. Then $\{M_i^* : i \in I\}$ is Γ-nice.*

Proof: Let $\psi^*(\mathbf{y}) = \exists x\phi^*(x, \mathbf{y})$ be an existential formula in the expanded language. Then, there are new constants $\mathbf{c}$ such that $\exists x\phi(x, \mathbf{y}, \mathbf{c}) = \psi(\mathbf{y}, \mathbf{c})$ and ϕ is a formula in the original language. Set $g_{\psi^*}(\mathbf{z}) := g_\psi(\mathbf{z}, \bar{\mathcal{C}})$, where $\bar{\mathcal{C}}$ are the choice functions for the $\mathbf{c}$; these exist by hypothesis. Then g_{ψ^*} witness the Γ-niceness. †

In general, expanding the language by functions or relations does not preserve these properties. For instance, an added function might pick out elements that omit the types "wildly" on a domain that omits the types at the same place. This is of course unfortunate because these are the expansions that are most often useful. However, this means that the study of when expanding the language preserves these properties is of great interest. One example is given in Subsection 4.1. Another example, given below, shows that this investigation allows us to get compactness results outside of omitting types classes.

We will use Q for the quantifier "there exists uncountably many." Then $\mathbb{L}(Q)$ refers to the extension of the logic $\mathbb{L}$ obtained by allowing this quantifier. Set T to be the $\mathbb{L}(Q)$-theory that says E is an equivalence relations and each class is countable; this is a first order axiom and $\forall x \neg Q y E(x, y)$. This is the most basic example of a quasiminimal class and of a non-finitary AEC (the strong substructure is substructure plus equivalence classes don't grow; see Kirby [15] for an explicit description of this class and overview of quasiminimal classes). Thus, this is not a type-omitting class, but there is a well-known method that allows the expression of $\mathbb{L}_{\omega_1,\omega}(Q)$ in terms of $\mathbb{L}_{\omega_1,\omega}$ in an expanded language (see, for instance, the proof of [1, Theorem 5.1.8]). This expansion is not canonical and typically gives rise to non-unary types. However, in this example, the combination of the facts that the $\mathbb{L}(Q)$-subformula has only one free variable and the fact that the quasiminimal closure is trivial allows us to get a compactness result.

Expand τ by adding countably many unary predicates $\{R_n(x) : n < \omega\}$ and expand a model of T by making R_n true of exactly one member of each equivalence class. Set T^* to be the first order part of T plus $\forall x \exists! y \, (R_n(y) \wedge E(x, y))$ for each $n < \omega$ and set $p(x) = \{\neg R_n(x) : n < \omega\}$. The following is straightforward.

Claim 2.21. *Let $\{M_i : i \in I\}$ be models of T and U an ultrafilter on I. If M_i^* is an expansion of M_i to a model of T^* omitting p, then*

$$\left(\prod^p M_i^* / U \right) \restriction \tau \vDash T$$

and Łoś' Theorem holds. Moreover, $(\prod^p M_i^*/U) \restriction \tau$ does not depend on the choice of the expansion.

This is a very basic example and the consequences are more easily obtained by analyzing it as a quasiminimal class. However, it gives hope that more intractable $\mathbb{L}(Q)$ classes can be analyzed via the Γ-ultraproduct.

2.5 A different approach

We have given a construction of $\prod^\Gamma M_i/U$ that is intimately tied to the ultraproduct. However, if Γ is a finite set of types, then there is an equivalent way of constructing the Γ-ultraproduct.

Given a model M and a set Γ of unary types, set the Γ-*hull of* M to be

$$\Gamma(M) := \{m \in M : \forall p \in \Gamma, m \text{ does not realize } p\}$$

If Γ is finite, then $\Gamma\left(\prod M_i/U\right) = \prod^\Gamma M_i/U$. In the study of Γ-hulls, many of the

same issues arise in the analysis of the Γ-hull as in the analysis of the Γ-ultraproduct, but with the relationship between $\Gamma(M)$ and M taking center stage. For instance, Section 2.2 would be replaced by an exploration of how elementary $\Gamma(M)$ is in M.

This paper focused on the Γ-ultraproduct over the Γ-hull for two related reasons. First, the main goal of viewing nonelementary classes as averageable is that some form of compactness holds there. Thus, working with ultraproducts is very natural. Second, some classes have a stronger Łoś' Theorem between $\{M_i : i \in I\}$ and $\prod^{\Gamma} M_i/U$ than there is (in general) elementarity between $\Gamma(M)$ and M. This again makes $\prod^{\Gamma} M_i/U$ the natural choice. An example of the second is abelian torsion groups. For instance, $tor(\mathbb{Z} \oplus \mathbb{Z}_2) = \mathbb{Z}_2$ and $\mathbb{Z} \oplus \mathbb{Z}_2$ are very different, but the full Łoś' Theorem holds for the class of torsion abelian groups by Theorem 5.10.

In general, we have, as sets,

$$\prod^{\Gamma} M_i/U \subset \Gamma\left(\prod M_i/U\right) \subset \prod M_i/U$$

It would be interseting to find a nonelementary class and Γ (necessarily infinite) where the Γ-hull of the ultraproduct was the proper structure to analyze, e.g., it is different from the Γ-ultraproduct and the Γ-hull is in the class, but the Γ-ultraproduct is not.

3 Averageable Classes

We now consider classes that are well behaved under the Γ-ultraproduct. We use the language of Abstract Elementary Classes (AECs) here; Baldwin [1], Grossberg [11], and Shelah [21] are the standard references. The main object of study are classes $\mathbb{K}$ of models that omit all types from Γ such that *all* sets of models from $\mathbb{K}$ are Γ-closed or Γ-nice and such that the strong substructure relation under consideration is preserved under Γ-ultraproducts. The examples we consider all fall into one of two cases:

1. $(EC(T, \Gamma), \subset)$ when T is $\exists\forall$, the types of Γ are existential, and $EC(T, \Gamma)$ is Γ-closed.
2. $(EC(T, \Gamma), \prec)$ when $EC(T, \Gamma)$ is Γ-nice.

The reader can easily focus on these, but we introduce a joint generalization of these cases to keep from stating our results twice and for potential future applications.

Definition 3.1. *A class* $(\mathbb{K}, \prec_{\mathbb{K}})$ *is* averageable *iff there is a collection of first-order formulas* $\mathcal{F}_{\mathbb{K}} = \mathcal{F}$ *that contains all atomic formulas and a collection of unary types* Γ *such that*

- *for all* $\phi(x) \in p \in \Gamma$, $\neg\phi(x) \in \mathcal{F}$;
- *the strong substructure* $\prec_{\mathbb{K}}$ *is* $\mathcal{F}$*-elementary substructure;*
- *given any* $\{M_i \in \mathbb{K} : i \in I\}$ *and any ultrafilter* U *on* I, $\prod^{\Gamma} M_i/U \in \mathbb{K}$ *and this* Γ*-ultraproduct satisfies Łoś' Theorem for the formulas in* $\mathcal{F}$*; and*
- *each* $M \in \mathbb{K}$ *omits each* $p \in \Gamma$.

Being an averageable class gives a very strong compactness result within the incompact framework of AECs; this was seen using large cardinals in Boney [5] and exploited in Boney and Grossberg [9] axiomatically.

The first property of averageable classes is a (much) better Hanf number.

Proposition 3.2. *Suppose that* $\mathbb{K}$ *is averageable and set* $\kappa = \prod |p|$. *Then* $\mathbb{K}_{>\kappa}$ *has no maximal models.*

This follows directly from Corollary 2.18. The normal Hanf number is $\beth_{(2^{|T|})^+}$, while $\prod |p| \leq 2^{|T|}$.

A stronger result builds on Proposition 2.20. Because they omit types, averageable classes are not compact. However, they satisfy a strong approximation to compactness that we call local compactness.

Theorem 3.3 (Local Compactness)**.** *Suppose that* $(EC(T, \Gamma), \prec)$ *is an averageable class with* $\mathcal{F}$*;* T^* *is an extension of* T *in* $\tau^* := \tau(T) \cup \{c_i : i < \kappa\}$ *such that each new sentence of* T^* *comes from substituting new constants into a formula from* $\mathcal{F}$*; and choice functions* $\{\mathcal{C}_i : i < \kappa\}$ *on* Γ *with* $T_0 = \{\neg\mathcal{C}_i(p)(c_i) : i < \kappa, p \in \Gamma\}$.

If, for every finite $T^- \subset T^*$, *there is* $M^* \models T^- \cup T_0$ *that omits all of* Γ, *then* T^* *has a model omitting all of* Γ.

Looking at the space $gS^n(\emptyset)$ of syntactic n-types that are realized in some model of $EC(T, \Gamma)$ when Γ is finite leads to the name local compactness. Equip this space with the logic topology, where the basic open sets are

$$[\![\phi]\!] := \{q \in gS^n(\emptyset) : \phi \in q\}$$

Then this space is not compact unless Γ is trivial. But it is locally compact: if $p \in gS^n(\emptyset)$ and $\mathcal{C}_1, \ldots, \mathcal{C}_n$ are the corresponding choice functions, then

$$\left[\!\!\left[\bigwedge_{p \in \Gamma, i < n} \neg\mathcal{C}_i(p)((x_i) \right]\!\!\right]$$

is a compact clopen neighborhood of p, with the compactness of the neighborhood following by the theorem. When n or Γ is infinite, this set is no longer clopen (so the space is no longer locally compact), but the set above is still compact and typically contains more than just p.

Proof: For each finite $T^- \subset T^*$, let $M^*_{T^-}$ be the model advertised in the hypothesis and let M_{T^-} be its restriction to $\tau(T)$. Let U be a fine ultrafilter on $P_\omega T^*$; recall that fineness means that $[\phi^*] := \{s \in P_\omega T^* : \phi^* \in s\}$ is in U for each $\phi^* \in T^*$. Set

$$M := \prod_{T^- \in P_\omega T^*}^{\Gamma} M_{T^-}/U$$

By averageability, $M \in EC(T, \Gamma)$ and Łoś' Theorem holds for $\mathcal{F}$. Now expand M to a τ^* structure M^* by setting $c_i^{M^*} := [T^- \mapsto c_i^{M^*_{T^-}}]_U$. Note that $\mathcal{C}_i$ is the witness to $c_i^{M^*} \in M$, so this is a valid definition.

Now we claim that M^* is the model satisfying T^* and omitting Γ. Since $M \in EC(T, \Gamma)$, it satisfies T and omits Γ and naming additional constants does not change this. Let $\phi \in T^*$ be a new sentence. Then it is of the form $\psi(c_{i_1}, \ldots, c_{i_n})$ for some $\psi \in \mathcal{F}$. By the fineness of the ultrafilter,

$$[\phi] = \{T^- \in P_\omega T^* : M_{T^-} \vDash \psi(c_{i_1}^{M^*_{T^-}}, \ldots, c_{i_n}^{M^*_{T^-}})\} \in U$$

Since Łoś' Theorem holds for ψ, this means that

$$M^* \vDash \psi\left(c_{i_1}^{M^*}, \ldots, c_{i_n}^{M^*}\right)$$

Since this holds for every $\phi \in T^*$, we have $M^* \vDash T^*$, as desired. †

Although complex to parse, local compactness has a very nice corollary.

Corollary 3.4. *Suppose $EC(T, \Gamma)$ is Γ-nice and p is a type such that every finite subset is a realizable in a model of $EC(T, \Gamma)$ with some fixed witness. Then p is realized in a model of $EC(T, \Gamma)$.*

Many other uses of compactness follow similarly, such as a criteria for amalgamation similar to first-order (see [14, Theorem 6.5.1]).

Corollary 3.5. *Suppose $EC(T, \Gamma)$ is Γ-nice. Then it has amalgamation.*

Indeed, much of the rest of this section is more easily proven with the local compactness result above. However, we have lost some generality by restricting

ourselves to averageable classes of the form $EC(T, \Gamma)$. For instance, this excludes the $\mathbb{L}(Q)$-axiomatizable class discussed in Section 2.4. Although this is the form of our examples, we prove the following results in greater generality and, therefore, without local compactness.

Following [5], we get the following result about tameness and type shortness. Tameness and type shortness are locality results for Galois types. We only prove type shortness (and not the tameness which follows), so we define that here. For full definitions, see, e.g., [5, Section 3].

Definition 3.6. *Let $(\mathbb{K}, \prec_{\mathbb{K}})$ be an AEC and I a linear order.*

- *Given $M \prec_{\mathbb{K}} N_1, N_2$ from $\mathbb{K}$ and $\langle x_i^\ell \mid i \in I\rangle$, we say that*

$$\left(\langle x_i^1 \mid i \in I\rangle, M, N_1\right) E_{AT} \left(\langle x_i^2 \mid i \in I\rangle, M, N_2\right)$$

  iff there is $N^* \in \mathbb{K}$ and $g_\ell : N_\ell \to_M N^*$ such that $g_1(x_i^1) = g_2(x_i^2)$ for all $i \in I$.

- *Given $M \prec_{\mathbb{K}} N_1, N_2$ from $\mathbb{K}$ and $\langle x_i^\ell \mid i \in I\rangle$, we say that $(\langle x_i^1 \mid i \in I\rangle, M, N_1)$ and $(\langle x_i^2 \mid i \in I\rangle, M, N_2)$ have the same Galois type, written*

$$gtp(\langle x_i^1 \mid i \in I\rangle / M; N_1) = gtp(\langle x_i^2 \mid i \in I\rangle / M; N_2)$$

  iff they are related by the transitive closure of E_{AT}. The length of the Galois type $gtp(\langle x_i^1 \mid i \in I\rangle / M; N_1)$ is the index I

- *$\mathbb{K}$ is* fully $< \kappa$-type short *iff for all I and for all Galois types $gtp(\langle x_i^1 \mid i \in I\rangle / M; N_1)$ and $gtp(\langle x_i^2 \mid i \in I\rangle / M; N_2)$, we have*

$$gtp(\langle x_i^1 \mid i \in I\rangle / M; N_1) = gtp(\langle x_i^2 \mid i \in I\rangle / M; N_2)$$

  iff for all $I_0 \subset I$ of size $< \kappa$

$$gtp(\langle x_i^1 \mid i \in I_0\rangle / M; N_1) = gtp(\langle x_i^2 \mid i \in I_0\rangle / M; N_2)$$

Note that, if $\mathbb{K}$ satisfies amalgamation, then E_{AT} is already transitive. Full $< \omega$-type shortness follows from the assertion that Galois types are syntactic (in some sublogic of $\mathbb{L}_{\infty,\omega}$). For examples of AECs that are *not* type short, see Baldwin-Shelah [2].

Theorem 3.7. *Suppose $\mathbb{K}$ is averageable. Then $\mathbb{K}$ is fully $< \omega$-tame and -type short.*

This relies on the following lemma, which says that the ultraproduct of $\mathbb{K}$-embeddings is also a $\mathbb{K}$-embedding. Recall that averageability means there is a fragment $\mathcal{F}_{\mathbb{K}}$ so the $\mathbb{K}$-embeddings are precisely the $\mathcal{F}_{\mathbb{K}}$-elementary ones.

Lemma 3.8. *Suppose that $\langle M_i : i \in I\rangle$ and $\langle N_i : i \in I\rangle$ and $f_i : M_i \to N_i$ is a $\mathbb{K}$-embedding. Then $f : \prod^{\Gamma} M_i/U \to \prod^{\Gamma} N_i/U$ by $f([i \mapsto m_i]_U) = [i \mapsto f_i(m_i)]_U$ is a $\mathbb{K}$-embedding.*

Proof: First, we need to know that $[i \mapsto f_i(m_i)]_U$ is in $\prod^{\Gamma} N_i/U$. This is true because, by the $\mathcal{F}_{\mathbb{K}}$-elementarity of each f_i,

$$M_i \vDash \neg\phi^j_k(m_i) \implies N_i \vDash \neg\phi^j_k(f_i(m_i))$$

So $k([i \mapsto m_i]_U)$ is a witness for $[i \mapsto f_i(m_i)]_U$. Thus f is a $\mathbb{K}$-embedding. †

Proof of Theorem 3.7: We prove the type shortness and note that it implies the tameness by [5, Theorem 3.5]. Since we are not assuming amalgamation, we will show type shortness holds for atomic Galois equivalence. Suppose that $X = \langle x_i \in M_1 : i \in I\rangle$ and $Y = \langle y_i \in M_2 : i \in I\rangle$ are given such that, for all $I_0 \in P_\omega I$,

$$(\langle x_i : i \in I_0\rangle/\emptyset; M_1)E_{AT}(\langle y_i : i \in I_0\rangle/\emptyset; M_2)$$

That is, there is $N_{I_0} \in \mathbb{K}$ and $f^\ell_{I_0} : M_\ell \to N_{I_0}$ such that $f^1_{I_0}(x_i) = f^2_{I_0}(y_i)$ for all $i \in I_0$. Let U be a fine ultrafilter on $P_\omega I$. Then, following [5], set

- $N = \prod^{\Gamma}_{I_0 \in P_\omega I} N_{I_0}/U$;
- $f^\ell : M_\ell \to N$ is given by $f^\ell(m) = [I_0 \mapsto f^\ell_{I_0}(m)]_U$

N is well-defined by hypothesis and f^ℓ is a $\mathbb{K}$-embedding by Lemma 3.8. For each $i \in I$, $\{I_0 \in P_\omega I : f^1_{I_0}(x_i) = f^2_{I_0}(y_i)\}$ contains $[i] := \{I_0 \in P_\omega I : i \in I_0\} \in U$ by the fineness. So $f^1(x_i) = f^2(y_i)$ for all $i \in I$. Then

$$(X/\emptyset; M_1)E_{AT}(Y/\emptyset; M_2)$$

†

We now look at some stability theory. Following [9], we can define two notions of coheir. There are two because the syntactic notion of type from the formulas $\mathcal{F}$ and the Galois notion of type from considering $\mathbb{K}$ as an AEC do not necessarily coincide, although having the same Galois type implies having the same $\mathcal{F}$-type

The first is Galois coheir $\overset{Gal}{\downarrow}$ (this could also be called s-coheir). In this case, we consider Galois types over finite domains. When Galois types are syntactic, these are complete syntactic types over a finite set. The second is t-coheir $\overset{t}{\downarrow}$, which is more like the first order version.

Definition 3.9. *Let $\mathbb{K}$ be an averageable class.*

1. *Given $A, B, C \subset M$ with $M \in \mathbb{K}$, we say $A \overset{Gal}{\underset{C}{\downarrow}}^{M} B$ iff*

$$\text{for all finite } a \in A, b \in B, c \in C, \ gtp(a/bc) \text{ is realized in } C.$$

2. *$\mathbb{K}$ has the* weak Galois order property *iff there are finite tuples $\langle a_i, b_i \in M : i < \omega \rangle$ and c and types $p \neq q \in gS(c)$ such that, for all $i, j < \omega$,*

$$j < i \implies a_i b_j \vDash q$$

$$j \geq i \implies a_i b_j \vDash p$$

3. *Given $A, B, C \subset M$, we say $A \overset{t}{\underset{C}{\downarrow}}^{M} B$ iff*

$$\text{for all finite } a \in A, b \in B, c \in C \text{ and } \phi(x, y, z) \in \mathcal{F}_{\mathbb{K}}, \text{ if } M \vDash \phi(a, b, c), \text{ then there is } c' \in C \text{ such that } M \vDash \phi(c', b, c).$$

4. *$\mathbb{K}$ has the* weak order property *iff there are finite tuples $\langle a_i, b_i \in M : i < \omega \rangle$ and a formula $\phi(x, y, c) \in \mathcal{F}_{\mathbb{K}}$ with $c \in M$ such that, for all $i, j < \omega$,*

$$j < i \iff M \vDash \phi(a_i, b_j, c)$$

Note that we have begun talking about Galois types over sets even though we only have amalgamation over models. This adds some additional dificulties, but we are careful to avoid them here. The adjective 'weak' in describing the order property means that we only require ω length orders, rather than all ordinal lengths as in Shelah [23].

This ultraproduct allows us to weaken the requirements on getting this to be an independence relation the same way as in [9, Section 8].

Theorem 3.10. *If $\mathbb{K}$ is an averageable class with amalgamation that doesn't have the weak Galois order property and every model is $\aleph_0$-Galois saturated, then $\overset{Gal}{\downarrow}$ is an independence relation in the sense of [9].*

Theorem 3.11. *If $\mathbb{K}$ is an averageable class with amalgamation that doesn't have the weak order property and $\mathcal{F}$ is first-order logic, then $\overset{t}{\downarrow}$ is an independence relation in the sense of [9].*

Note that neither of these coheir's are precisely the definition given in [9]: [9] only considered Galois types over models (so $\overset{Gal}{\downarrow}$ was not used) and there was no logic to choose (so $\overset{t}{\downarrow}$ was not possible). Nonetheless, the proofs of the above theorems go through the same arguments as in [9, Theorem 5.1]. The changes are minor, so we omit the details. The interested reader can find the details on the author's website [6]; the above results are Theorems 6 and 10, respectively, from there. Note that an advantage of using $\overset{t}{\downarrow}$ is that Existence holds for free when $\mathcal{F}$ is closed under existentials, although the disadvantadge is that $\overset{t}{\downarrow}$ doesn't always have the semantic consequences often desired when dealing with types, that is, if working in a class where syntactic types are not Galois types. Additionally, with a little more stability, [10] shows that the two notions are the same if all models are $\aleph_0$-Galois saturated.

We have so far seen that averageable classes are very much like elementary classes. The following result is a further restriction on the behavior of averageable classes. It is easy to construct an averageable class with only a single model; take the standard model of arithmetic. For general Abstract Elementary Classes, there are many more possibilities for the spectrum function of a class without arbitrarily large models. However, the following result shows that, in the case of averageable classes, there are not.

Theorem 3.12. *Let Γ be a finite set of countable existential types and let M be a structure omitting Γ that is Γ-closed. Then, either*

(*a*) *every τ structure omitting Γ and satisfying the same $\exists\forall$-theory as M is isomorphic to M; or*

(*b*) *there are $\subset$-extensions of M of all sizes, each satisfying the same $\exists\forall$-theory.*

If Γ consists of just quantifier free types, then the requirement in (a) can be relaxed to just the same $\exists$- and $\forall$-theory.

We have stated the theorem in the simplest case. However, variations are possible that strengthen the amount of Łoś' Theorem that holds and strengthen the similarity between the models; this means that it can be applied to situations such as $DLOG\mathbb{Z}$ or torsion modules over PIDs. However, the countability of Γ remains crucial for the proof.

Theorem 3.13. *Let Γ be a finite set of countable types and let M be a structure omitting Γ that is Γ-nice. Then, either*

(*a*) *every τ structure omitting Γ and elementarily equivalent to M is isomorphic to M; or*

(*b*) *there are $\prec$-extensions of M of all sizes.*

Proof of Theorem 3.12: Enumerate each $p \in \Gamma$ as $\{\phi_n^p(x) : n < \omega\}$. Set

$$\psi_\ell(x) := \wedge_{p\in\Gamma} \vee_{n<\ell} \neg\phi_n^p(x)$$

We use these formulas to measure the type omission of all types of Γ jointly. Recall from Theorem 2.17, that the Γ-ultraproduct produces a proper extension if there is an infinite subset of M that all satisfy the same ψ_ℓ. This property separates our cases:

$$\text{There is } \ell_0 < \omega \text{ such that } \psi_{\ell_0}(\omega) \text{ is infinite.} \qquad (*)$$

First, suppose property (*) fails; we will show that (*a*) holds. For each $\ell < \omega$, $\psi_\ell(M)$ is finite. Thus, M is countable and we can enumerate it as $\{m_i : i < \omega\}$. For each $i < \omega$, pick some ℓ_i such that $M \vDash \psi_{\ell_i}(m_i)$. Then, define

$$\begin{aligned} k_\ell &= |\{n < \omega : \ell_i = \ell\}| \\ K_\ell &= |\psi_\ell(M)| \end{aligned}$$

Note $k_\ell \leq K_\ell < \omega$.

Let N be a model omitting Γ and having the same $\exists\forall$-theory as M. Note that

$$\exists x_0, \ldots, x_{K_\ell - 1} \left(\bigwedge_{i<K_\ell} \psi_\ell(x_i) \right)$$

$$\forall x_0, \ldots, x_{K_\ell} \left(\bigwedge_{i\leq K_\ell} \psi_\ell(x_i) \rightarrow \bigvee_{i\neq j\leq K_\ell} x_i = x_j \right)$$

are both $\exists\forall$-sentences, so $|\psi_\ell(N)| = |\psi_\ell(M)|$. In particular, N is also countable. We want to define bijections between these sets that fit together to be an isomorphism between the entire models; this is done through a finite injury-style argument.

We construct sequences $\{k_i^L : i < L\}$ for $L < \omega$ such that

1. for each $L < \omega$, we have $tp_{qf}(m_i : i < L) = tp_{qf}(k_i^L : i < L)$ and, for all $\ell < \omega$,

$$M \vDash \psi_\ell(m_i) \iff N \vDash \psi_\ell(k_i^L)$$

2. for each $i < \omega$, the sequence $\langle k_i^L : i < L < \omega \rangle$ eventually stabilizes.

This is enough: For $i < \omega$, set k_i to be the eventual value of $\langle k_i^L : i < L < \omega \rangle$. Our isomorphism f will take m_i to k_i. This is an isomorphism onto its range by the first part of (1). Furthermore, by the second part of (1),

$$|\psi_\ell(M)| = |\psi_\ell(N) \cap f(M)| = |\psi_\ell(N)|$$

Since the $\psi_\ell(N)$ are finite and exhaust N, we have $f(M) = N$. Thus, $M \cong N$, as desired.

Construction: The following claim is key.

Claim: For all $\mathbf{m} \in M$, there is $\mathbf{n} \in N$ such that $tp_{qf}(\mathbf{m}) = tp_{qf}(\mathbf{n})$ and $N \vDash \psi_{\ell_i^*}(k_i)$, where ℓ_i^* is the picked witness for m_i, the ith member of $\mathbf{m}$.

Suppose not. Let

$$N^* = \{\mathbf{n}' \in {}^{\ell(\mathbf{m})}N : \forall i. N \vDash \psi_{\ell_i^*}(n_i')\}$$

Note that N^* is finite. Then, for each $\mathbf{n}' \in N^*$, there is a quantifier-free $\phi_{\mathbf{n}'}(\mathbf{x})$ that holds of $\mathbf{m}$, but not of $\mathbf{n}'$. Set

$$\psi := \exists \mathbf{x} \left(\bigwedge_i \psi_{\ell_i^*}(x_i) \wedge \bigwedge_{\mathbf{n}' \in N^*} \phi_{\mathbf{n}'}(\mathbf{x}) \right)$$

This is an $\exists(\neg\Gamma)$-sentence satisfied by M and not by N, a contradiction. Thus, the claim is proved.

Now we are ready to build $\{k_i^L : i < l\}$ by induction on $L < \omega$.

Set k_0^1 to satisfy the same qf-type as m_0 and satisfy the appropriate ψ_ℓ.

For $L > 1$, the above Claim says that there is at least one sequence satisfying (1) for $m_0, \ldots, m_{L-1}$. Pick $\{k_i^L : i < L\}$ to be the sequence satisfying (1) that agrees with the largest possible initial segment of $\{k_i^{L-1} : i < L - 1\}$.

It is clear that this construction satisfies (1). To see it satisfies (2), note that there are only finitely many choices for the ith element. Thus, if an initial segment changed infinitely often, it would necessarily repeat; however, repetition is forbidden by the construction.

Second, suppose property (*) holds; we will show that (b) holds. We know that the Γ-ultraproduct is a proper extension. We will iterate this.

For each ordinal, we will construct $M_\alpha \equiv_{\exists(\neg\Gamma)} M$ that omits Γ and a coherent set of nonsurjective embeddings $f_{\beta,\alpha} : M_\beta \to M_\alpha$ for $\beta < \alpha$.

For $\alpha = 0$, set $M_0 = M$.

For $\alpha = \beta + 1$, set $M_\alpha := \prod^\Gamma M_\beta/U$, for U a nonprincipal ultrafilter on ω. Note that this is a structure since the data is Γ-closed by Proposition 2.4 and Proposition 2.7.(2). Then the ultrapower map j is a nonsurjective embedding. Set $f_{\gamma,\alpha} = j \circ f_{\gamma,\beta}$ for each $\gamma \leq \beta$.

For α limit. Let U be a nonprinicipal uniform ultrafilter on α and set $M_\alpha := \prod^\Gamma_\beta M_\beta/U$; note that this is a Γ-ultraproduct rather than a Γ-ultrapower. Again, this is a structure. This shares the same $\exists(\neg\Gamma)$ theory of the M_β's.

Define $f_{\beta,\alpha} : M_\beta \to M_\alpha$ by $f_{\beta,\alpha}(m) = [g^m_{\beta,\alpha}]_U$ where

$$g^m_{\beta,\alpha}(\gamma) = \begin{cases} f_{\beta,\gamma}(m) & \beta \leq \gamma < \alpha \\ 0 & \gamma < \beta \end{cases}$$

Then this is a nonsurjective $\mathbb{K}$-embedding such that $f_{\beta,\alpha} = f_{\gamma,\alpha} \circ f_{\beta,\gamma}$.

Since this chain is increasing, $M_\alpha \geq |M| + |\alpha|$, giving us the desired result. †

4 Examples

We now give several examples of type-omitting classes $EC(T, \Gamma)$ for which our construction gives some compactness results. The meaning of "some compactness results" is left vague, but the general behavior is that these are averageable classes for the appropriate fragment $\mathcal{F}$. Another class of examples from torsion modules over PIDs is discussed in the next section.

As a final cautionary example, we discuss the case of Archimedean fields. Typically, Archimedean fields are presented as ordered fields omitting the type of an infinite element $p_\infty(x) = \{x > n \cdot 1 : n < \omega\}$. However, if we take the theory of fields (of characteristic 0) and this type, then the data is not even p-closed: the p_∞-ultraproduct has no positive infinite element, but does have infinitesimals and a negative infinite element; thus it's not closed under the field operations. Thus, to fit into this framework, Γ must contain continuum many types, one each to explicitly omit the positive and negative infinite elements and the infinitesimal elements above and below each standard element. After these types are added, the class is Γ-closed with $\mathbb{R}$ as a maximal model of size $2^{\aleph_0} = |\mathbb{R}|$ (this maximality agrees nicely with Theorem 2.17).

Another example along these lines is to consider differentially closed fields where every element is differentially algebraic over the constants (so it omits the type of a differential transcendental).

4.1 Banach Spaces

Banach spaces are the motivating example from this work: viewing continuous first-order logic as a certain fragment of $\mathbb{L}_{\omega_1,\omega}$ (see Boney [7]) lead to viewing the Banach space ultraproduct as one that, in part, omits unbounded elements by simply excluding them. We outline how this can be put into this framework.

Let $\tau_b = \langle B, R; +_B, 0_B; +_R, \cdot_R, 0_R, 1_R, <_R, c_r; \|\cdot\|, \cdot_{scalar}\rangle_{r\in\mathbb{R}}$ be the two sorted language of normed linear spaces. Then T_b says that

- $\{c_r : r \in \mathbb{R}\}$ is a copy of $\mathbb{R}$; and
- B is a vector space over R, with norm $\|\cdot\| : B \to R$.

We want to ensure that, in the ultraproduct, R and B each have no nonstandard elements, i.e., omit the type of an element of R that is not some c_r. Similar to the case of Archimedean fields, it is not enough to omit a single type; instead every nonnegative real must have a types specifying there is no nonstandard real around it and a type specifying there are not Banach space elements that would be mapped to such an element.

- $p_\infty(x) = \{R(x) \wedge (x < -n \vee n < x) : n < \omega\}$;
- $p_r(x) = \{R(x) \wedge (x \neq c_r) \wedge (c_{r-\frac{1}{n}} < x < c_{r+\frac{1}{n}}) : n < \omega\}$ for $r \in \mathbb{R}$;
- $q_\infty(x) = \{B(x) \wedge (\|x\| < -n \vee n < \|x\|) : n < \omega\}$; and
- $q_r(x) = \{B(x) \wedge (\|x\| \neq c_r) \wedge (c_{r-\frac{1}{n}} < x < c_{r+\frac{1}{n}}) : n < \omega\}$.

Set $\Gamma = \{p_r(x) : r \in \mathbb{R} \cup \{\infty\}\} \cup \{q_r(x) : r \in \mathbb{R}^{\geq 0} \cup \{\infty\}\}$. We omit the details, but $EC(T_b, \Gamma)$ is Γ-closed: the key details is that the standard real number that two sequences correspond to can be used to calculate the standard real number their sum or product corresponds to. This means that the Universal Łoś' Theorem holds. Additionally, by Observation 2.9, the class of formulas which Łoś' Theorem holds is closed under "bounded quantification," that is, of the form

$$\exists x \, (\phi(x, \mathbf{y}) \wedge \|x\| < c)$$

for some $c > 0$.

Comparing this with first-order continuous logic, there is not a requirement that the space be of bounded diameter. Moreover, the condition above recovers some of the results from Ben Yaacov [3] about unbounded metric spaces.

Other results for continuous logic can be recovered through these methods. For instance, when trying to extend the language τ_b and preserve the Γ-closedness of the class, the relevant condition turns out to be uniform continuity of the function or relation, which agrees with the results from continuous first-order logic. Additionally, a continuous version of the Γ-ultraproduct can be developed along the same lines.

4.2 Abelian Torsion Groups

Let $\tau_g = \{+, 0, -\cdot\}$ and T_{ag} be the theory of abelian groups, where $-\cdot$ is the additive inverse. Abelian torsion groups are models of T_{ag} that omit $tor(x) = \{n \cdot x \neq 0 : n < \omega\}$. We claim that abelian torsion groups are *tor*-closed.

Proposition 4.1. *If G is an abelian group, then it is tor-closed.*

Proof: Given $g \in G$, we have that $G \vDash \neg(n \cdot g \neq 0)$ exactly when $o(g) \mid n$. Since $o(g) = o(-g)$ and $o(g_1 + g_2) = \text{lcm}(o(g_1), o(g_2)) \mid o(g_1)o(g_2)$, setting $g_-(n) = n$ and $g_+(n, m) = nm$ shows that G is *tor*-closed. †

A more in depth analysis shows the full Łoś' Theorem holds in the wider class of torsion modules over a PID.

4.3 DLOG$\mathbb{Z}$

We consider the theory of densely ordered abelian groups[2] with the infinitary property of having a cofinal $\mathbb{Z}$-chain. The first order part of this theory was first shown to have quantifier elimination by Skolem [26][3]. We will show that the first order portion of the theory is preserved by the appropriate p-ultraproduct, and then use quantifier elimination to bootstrap the full version of Łoś' Theorem.

Set $T := Th(\mathbb{Q}, <, +, -, 0, 1, n)_{n\in\mathbb{Z}}$ and $Z(x) := \{x \leq c_n \text{ or } c_m \leq x : n < m \in \mathbb{Z}\}$, where c_n is the constant representing n. By a model of DLOG$\mathbb{Z}$, we mean a model of T that omits Z, i.e. one where $\{c_n : n \in \mathbb{Z}\}$ is a discrete, countable sequence that is cofinal in both directions. This theory has quantifier elimination and is axiomatized by the axioms for an ordered, uniquely divisible, torsion-free abelian group that is dense as an ordering and the elementary diagram of $(\mathbb{Z}, +, <)$.

Proposition 4.2. *$(EC(T, Z), \prec)$ is closed under Z-ultraproducts and they satisfy Łoś' Theorem. Morever, this is a class with amalgamation where Galois types are syntactic.*

[2]Note that the group structure is not crucial here, and the same analysis could be done with the theory of dense linear orders with a cofinal $\mathbb{Z}$-chain.

[3]For a little more history, see the introduction of Hieronymi [13]. Also, Miller [18] contains a proof and is more easily accessible than Skolem's original

Proof: Let M_i be a model of DLOG$\mathbb{Z}$ for each $i \in I$ and let U be an ultrafilter on I.

Claim 4.3. *$\prod^Z M_i/U$ is a structure that models T.*

Proof: We have to show that it contains the constants and is closed under functions. Each c_n is represented by $[i \mapsto c_n^{M_i}]_U$, which fails to satisfy "$x \leq c_{n-1}$ or $c_{n+1} \leq x$" everywhere. Next we look at addition; subtraction is similar. Let $[f]_U, [g]_U \in \prod^Z M_i/U$ that are witnessed by

$$\begin{aligned} c_{n_f} < \quad & [f]_U \quad < c_{m_f} \\ c_{n_g} < \quad & [g]_U \quad < c_{m_g} \end{aligned}$$

Then $[f]_U + [g]_U = [f+g]_U \in \prod^Z M_i/U$ as witnessed by

$$c_{n_{f+g}} = c_{n_f} + c_{n_g} < [f]_U + [g]_U < c_{m_f} + c_{m_g} = c_{m_{f+g}}$$

Since $\prod^Z M_i/U$ is a structure, we now wish to show it models T. We know $\exists\forall$-sentences transfer, so we only need to show that the existentials in the divisibility of the group and denseness of the order hold.
For the divisibility, suppose $[f]_U \in \prod^Z M_i/U$ and $k < \omega$ such that there is $X \in U$ and $n_f < m_f \in \mathbb{Z}$ such that, for all $i \in X$, $M_i \vDash c_{n_f} < f(i) < c_{n_g}$. Then, for each $i \in I$, there is $\frac{f}{k}(i) \in M_i$ such that

$$M_i \vDash k \cdot \frac{f}{k}(i) = f(i) \wedge (c_{-|n_f|-|m_f|} < \frac{f}{k}(i) < c_{|n_f|+|m_f|}$$

For the denseness, suppose $[f]_U, [g]_U \in \prod^Z M_i/U$ such that $\prod^Z M_i/U \vDash [f]_u < [g]_U$. Thus, there is $X \in U$ and $n_f < m_f, n_g < m_g \in \mathbb{Z}$ such that, for all $i \in X$, we have

1. $M_i \vDash f(i) < g(i)$;
2. $M_i \vDash c_{n_f} < f(i) < c_{m_f}$; and
3. $M_i \vDash c_{n_g} < g(i) < c_{m_g}$.

We can find $h \in \prod M_i$ such that $M_i \vDash f(i) < h(i) < g(i)$. For $i \in X$, we have $M_i \vDash c_{n_f} < h(i) < c_{n_g}$. Thus, $[h]_U \in \prod^Z M_i/U$ and $\prod^Z M_i/U \vDash [f]_U < [h]_U < [g]_U$.

Claim 4.4. *The Z-ultraproduct satisfies Łoś' Theorem.*

This follows by Proposition 2.15 and quantifier elimination.

Second, we show that the class has amalgamation and that Galois types are syntactic. Note that, by definition of the class, having the same Galois type implies having the same syntactic type. Let $M_0 \prec M_1, M_2 \in EC(T, Z)$, possibly with $a_\ell \in M_\ell$ such that $tp(a_1/M_0; M_1) = tp(a_2/M_0; M_2)$. Then, since the elementary class of models of T has amalgamation and has that syntactic types are Galois types, there is $N^* \vDash T$ and $f_\ell : M_\ell \to_{M_0} N^*$ such that, if we are dealing with types, $f_1(a_1) = f_2(a_2)$. N^* might realize p, but set N to be the substructure of N^* with universe $\{x \in N \mid \exists n, m \in \mathbb{Z}. N^* \vDash c_n < x < c_m\}$. This is a substructure of N^* that models T, contains $f_1(M_1)$ and $f_2(M_2)$, and omits p. By quantifier elimination, these inclusions are actually elementary substructure. Thus N is the desired amalgam. Additionally, if we are dealing with the type statement, $f_1(a_1) = f_2(a_2)$, so $gtp(a_1/M_0; M_1) = gtp(a_2/M_0; M_2)$ as desired. †

This example can be generalized by looking at ordered R-vector spaces over an ordered division ring R rather than just ordered divisible abelian group. By [27, Corollary 1.(7.8)], this wider class also has quantifier elimination and the argument works in the same way.

4.4 Multi-sorted first order logic

Take a multi-sorted language τ with sorts $\{S_\alpha : \alpha < \kappa\}$ and a theory T. There is a natural correspondence between multi-sorted models of T and models of a (non-sorted) first-order theory T^* in the language $\tau^* := \tau \cup \{S_\alpha : \alpha < \kappa\}$ that omit the type $sort(x) := \{\neg S_\alpha(x) : \alpha < \kappa\}$. Then, the class $EC(T^*, sort)$ is not $sort$-nice, but is still well-behaved with respect to the $sort$-ultraproduct in the following sense.

Proposition 4.5. *$EC(T^*, sort)$ satisfies Łoś' Theorem with respect to τ^* formulas that come from sorted τ formulas.*

Proof: First, we observe that the class is $sort$-closed: if F be a function of τ, then T^* determines the sort of F applied to any valid input. This means that a the universal Łoś' Theorem holds. Moreover, suppose that $\exists x \phi(x, \mathbf{y})$ is a τ^* formula that comes from a sorted τ formula. Then, this formula determines which sort a witness x would be in. This is precisely the information required to define the function $g_{\exists x \phi(x, \mathbf{y})}$; note that it is a constant function. Thus, the set of formulas that $EC(T^*, sort)$ satisfies Łoś' Theorem with contain all quantifier-free τ^* formulas that come from sorted τ formulas and is closed under exstentials. By applying Remark 2.6, this extends to the class of all formulas coming from sorted τ formulas, as desired. †

This allows one to read off the normal compactness results of sorted first-order logic from the results of this paper; moreover, Theorem 3.12 means that a sorted

model has proper elementary extensions iff one of the sorts has infinite size. Indeed, this correspondence seems to go both ways and one could likely perform the same analysis in this paper by looking at which EC classes are "sortable."

4.5 Highly Complete Ultrafilters

Our final example shows that, if there are very complete ultraproducts, then this new ultraproduct coincides with the classic one.

Theorem 4.6. *If U is χ-complete, $\chi > |\Gamma|$, and $\chi > |p|$ for all $p \in \Gamma$, then $\prod^\Gamma M_i/U = \prod M_i/U$.*

Proof: We always have $\prod^\Gamma M_i \subset \prod M_i$. Let $f \in \prod M_i$. We want to show $f \in \prod^\Gamma M_i$ by finding a witness. For each $\phi \in p \in \Gamma$, set $X_\phi^{f,p} := \{i \in I : M_i \vDash \neg\phi(f(i))\}$. For each $p \in \Gamma$, I is the union of $\{X_\phi^{f,p} : \phi \in p\}$. Since $|p| < \chi$, there is some ϕ_p such that $X_{\phi_p}^{f,p} \in U$. Then

$$X^f = \cap_{p\in\Gamma} X_{\phi_p}^{f,p} \in U$$

shows that the map $p \mapsto \phi_p$ is a witness. Thus $\prod^\Gamma M_i = \prod M_i$. †

Note that, if κ is some large cardinal giving rise to κ-complete ultrafilters and τ is averageable with respect to κ-complete ultrafilters, then τ will satisfy the relevant parts of the last section with κ in place of ω; see [5] and [9, Section 8] for what is relevant.

5 Torsion Modules

In this section, we explore the previous results applied to torsion modules over PIDs and apply some results for nonelementary stability theory. The stability theoretic results are not deep (and probably follow from results about modules and other properties of torsion modules), but we intend this to show what can be done.

5.1 The Torsion Ultraproduct

For this subsection, assume that R is a commutative ring with unity.[4]

We review some basics of the model theory of modules, using Prest [19] as the reference. The language is $\tau_R = \langle +, r\cdot, -, 0\rangle_{r\in R}$. Then the theory of R-modules T_R

[4]The following weakening of commutativity is also sufficient: $\forall x\forall y\exists z(xy = zx)$. Then we can take the ultraproduct of left torsion modules.

is the statement of all of the module axioms; note that this is a universal theory. Given a module M and $m \in M$, set

$$\mathcal{O}^M(m) := \{r \in R : r \cdot m = 0 \text{ and } r \text{ is regular}\}$$

Recall that regular elements are those that are not zero divisors. We drop the M if it is clear. If this set is non-empty and $m \neq 0$, then m is a torsion element and every element of $\mathcal{O}(m)$ is called an order of m. If every element of M is a torsion element, then M is a torsion module.

Note that Shelah [24] has recently explored the more general behavior of $\mathbb{L}_{\lambda,\mu}$-theories of modules, but does not deal with compactness or nonforking[5].

Set $tor(x) = \{r \cdot x \neq 0 : r \in R \text{ and } r \text{ is regular}\}$ to be the type of a torsion-free element. Let $\{M_i : i \in I\}$ be a collection of torsion modules (i.e. modules that omit tor) and let U be an ultrafilter on I. Then the tor-ultraproduct is

$$\prod^{tor} M_i/U := \{[f]_U \quad : \quad f \in \prod M_i \text{ and there is } X_f \in U \text{ and } r_f \in R \text{ such that } r_f \in \mathcal{O}^{M_i}(m_i) \text{ for all } i \in X_f\}$$

Proposition 5.1. *$EC(T_R, tor)$ is tor-closed and the universal Łoś' Theorem holds.*

Proof: Note that the first part implies the second by Theorem 2.5.

We need to construct functions that tell us the order of a sum, etc. based on the order of the inputs. For later use, we do more: for each τ_R-term $\tau(\mathbf{x})$, we inductively construct $f_\tau : R^{\ell(\mathbf{x})} \to R$ such that $f''_\tau \prod \mathcal{O}(m_i) \subset \mathcal{O}(\tau(m_0, \ldots, m_{n-1}))$

- if $\tau(\mathbf{x}) = x_i$, then $f_\tau(\mathbf{r}) = r_i$;
- if $\tau = s \cdot \sigma$, then $f_\tau = f_\sigma$;
- if $\tau = \sigma + \chi$, then $f_\tau = f_\sigma f_\chi$; and
- if $\tau = -\sigma$, then $f_\tau = f_\sigma$.

Thus, $EC(T_R, tor)$ is tor-closed..

In fact, in this case, we have $\prod^{tor} M_i/U$ is precisely the torsion subgroup of the full ultraproduct $\prod M_i/U$. Thus, the construction of the tor-ultraproduct is not new, but we can use the results from earlier sections and the model theory of modules to get some new results.

Further study of the ultraproduct requires specialization to PIDs, but we already have the following dividing line for modules. Roughly, this says that, given a torsion

[5] [24] says he intends to deal with nonforking in [25], but this has yet to appear.

module over a countable commutative ring, either it is the only torsion module like it *or* there are torsion modules like it of all sizes.

Corollary 5.2. *Let M be a torsion module over a countable, commutative ring. Then either*

1. *every torsion module that is $\exists$- and $\forall$-equivalent to M is in fact isomorphic to M; or*
2. *there are torsion $\subset_\forall$-extensions of M of all sizes (in fact, the all model the same $\exists\forall$ theory).*

Note that there is no explicitly stated restriction on the size of the module in (1), but M will necessarily be countable as will any torsion module $\forall$-equivalent to it.

Proof: This is Theorem 3.12 in this context. †

5.2 Torsion Compactness over PIDs

For the remained of this subsection, assume that R is a principal ideal domain. Note that PIDs are integral domains, so all nonzero elements are regular.

The goal of this subsection is to prove Łoś' Theorem for elementarily equivalent modules. The proof of this uses Proposition 2.15 and has two steps:

1. recall that T_R has p. p. elimination of quantifiers; and
2. show that Łoś' Theorem holds for p. p. formulas (and a little more).

We need to recall the key facts about p. p. elimination of quantifiers.

Definition 5.3. *$\phi(\mathbf{x})$ is a p. p. (primitive positive) formula iff it is a conjunction of formulas of the form $p^n \mid \tau(\mathbf{x})$ and $\tau(\mathbf{x}) = 0$ for a term τ, a prime $p \in R$, and $n < \omega$.*

Note that p. p. formulas have a more general definition (see [19, Section 2] for the more general definition and a deeper discussion of their role in the model thoery of modules), but this is an equivalent formulation in PIDs ([19, Theorem 2.$\mathbb{Z}$1]). Indeed this formulation is the key reason we have specified to PIDs as it allows us to prove Łoś' Theorem for p. p. formulas. Note that Shelah [24, Theorem 2.4] has a much more general version of this result for $\mathbb{L}_{\lambda,\theta}$-theories of modules (note he calls these formulas p. e. or "positive existential"), but the first-order version suffices.

Given a complete theory of a module, all formulas are equivalent to a boolean combination of p. p. formulas. However, a more precise result involving invariants conditions is true.

Definition 5.4. *Given a module and p. p. formulas $\phi(\mathbf{x})$ and $\psi(\mathbf{x})$, set $Inv(M, \phi, \psi) = |\phi(M)/\phi(M) \cap \psi(M)|$. An* invariants condition *is the assertion that $Inv(M, \phi, \psi)$ is either greater than or less than some $k < \omega$.*

Fact 5.5 ([19].2.13)**.** *If $\phi(\mathbf{x})$ is a formula, then there is a boolean combination of invariants conditions σ and a boolean combination of p. p. formulas $\psi(\mathbf{x})$ such that*

$$T_R \vdash \forall \mathbf{x}(\phi(\mathbf{x}) \iff (\sigma \wedge \psi(\mathbf{x})))$$

Lemma 5.6. *Suppose all M_i are elementarily equivalent. Given $[f_0]_U, \ldots, [f_{n-1}]_U \in \prod^{tor} M_i/U$ and p. p. $\phi(\mathbf{x})$,*

$$\{i \in I : M_i \vDash \phi(f_0(i), f_{n-1}(i))\} \in U \iff \prod^{tor} M_i/U \vDash \phi([f_0]_U, \ldots, [f_{n-1}]_U)$$

Proof: Note that $\neg\phi(\mathbf{x})$ is universal, so right to left follows from Theorem 5.1 above. For the other direction, suppose $\phi(\mathbf{x})$ is of the following form:

$$\bigwedge_{j<m} (\exists y_j . p_j^{n_j} \cdot y_j = \tau_j(\mathbf{x})) \wedge \bigwedge_{j<m'} (\sigma_j(\mathbf{x}) = 0)$$

and that $Y := \{i \in I : M_i \vDash \phi(f_0(i), \ldots, f_{n-1}(i))\} \in U$. The difficulty is establishing that the existential witnesses lie in the *tor*-ultraproduct. By the definition of the *tor*-ultraproduct, each parameter $[f_k]_U$ has some fixed order on a U-large set, say $r_k \in \mathcal{O}^{M_i}(f_k(i))$ for all $i \in X_k \in U$. Then $r := f_{\tau_i}(r_0, \ldots, r_{n-1})$ will be an order for them on $X := \cap_{k<n} X_k$; recall that f_τ was constructed in the proof of Proposition 5.1.

For each $i \in Y$ and $j < m$, find m_j^i such that

$$M_i \vDash p_j^{n_j} \cdot m_j^i = \tau_j(f_0(i), \ldots, f_{n-1}(i))$$

Then r is also an order for each m_j^i when $i \in X$. We define $g_j \in \prod M_i$ by

$$g_j(i) = \begin{cases} m_j^i & \text{if } i \in X \cap Y \\ 0 & \text{otherwise} \end{cases}$$

Then r and $X \cap Y \in U$ witness that $[g_j]_U \in \prod^{tor} M_i/U$ for each $j < m$ and

$$\prod^{tor} M_i/U \vDash p_j^{n_j} \cdot [g_j]_U = \tau_j([f_0]_U, \ldots, [f_{n-1}]_U)$$

Thus, $\prod^{tor} M_i/U \vDash \phi([f_0]_U, \ldots, [f_{n-1}]_U)$, as desired.

We can easily extend this result to boolean combinations of p. p. formulas.

Corollary 5.7. *Suppose M_i are elementarily equivalent. Given $[f_0]_U, \ldots, [f_{n-1}]_U \in \prod^{tor} M_i/U$ and a boolean combination of p. p. $\phi(\mathbf{x})$,*

$$\{i \in I : M_i \vDash \phi(f_0(i), \ldots, f_{n-1}(i))\} \in U \iff \prod^{tor} M_i/U \vDash \phi([f_0]_U, \ldots, [f_{n-1}]_U)$$

Remark 5.8. *Lemma 5.6 is the key result that requires the specialization to modules over PIDs, and it's not currently known if this holds in general for commutative rings. As an alternate hypothesis, this result also holds if all annihilator ideals are prime.*

We can use the fact that Łoś' Theorem holds for p. p. formulas to show that it also holds for boolean combinations of invariants conditions (these are sometimes called invariants sentences).

Lemma 5.9. *Suppose that all M_i are elementarily equivalent. Let ϕ be a boolean combination of invariants conditions. Then ϕ is part of the common theory of the M_i's iff $\prod^{tor} M_i/U \vDash \phi$.*

Proof: Since a negation of a boolean combination is itself a boolean combination, it suffices to show one direction. Thus, assume that $M_i \vDash \phi$ for all $i \in I$. Since conjunctions and disjunctions transfer (see Remark 2.6 or easy to work out the details), we only have to show this for $Inv(M, \phi, \psi) \geq k$ and $Inv(M, \phi, \psi) < k$. WLOG, assume ψ implies ϕ. Note that

$$\begin{aligned} Inv(M, \phi, \psi) \geq k &\equiv \text{“}\exists \mathbf{v}_0, \ldots, \mathbf{v}_{k-1}(\bigwedge_{i<k} \phi(\mathbf{v}_i) \wedge \bigwedge_{j<i<k} \neg\psi(\mathbf{v}_j - \mathbf{v}_i))\text{”} \\ Inv(M, \phi, \psi) < k &\equiv \text{“}\forall \mathbf{v}_0, \ldots, \mathbf{v}_{k-1}(\bigvee_{i<k} \neg\phi(\mathbf{v}_i) \vee \bigvee_{j<i<k} \psi(\mathbf{v}_j - \mathbf{v}_i))\text{”} \end{aligned}$$

$Inv(M, \phi, \psi) \geq k$ is $\exists\forall$, so the result holds by Proposition 2.7. The formula “$\bigvee_{i<k} \neg\phi(\mathbf{v}_i) \vee \bigvee_{j<i<k} \psi(\mathbf{v}_j - \mathbf{v}_i)$” is a boolean combination of p. p. formulas, so it transfers by Corollary 5.7. Then $Inv(M, \phi, \psi) < k$ is universal over a formula that transfers, so it transfers as well; again, see Remark 2.6 or work out the

details. †

We now have all of the tools that we need to prove the full version of Łoś' Theorem.

Theorem 5.10. *Let T_R^* be a complete theory τ_R-theory extending T_R (recall R is a PID). Then $EC(T_R^*, tor)$ satisfies Łoś' Theorem with the tor-ultraproduct.*

Proof: Suppose that $\{M_i \mid i \in I\}$ are torsion models of T_R^* and U is an ultrafilter on I. Then $\prod^{tor} M_i/U$ is a torsion module by Proposition 5.1. Let $[f_0]_U, \ldots, [f_{n-1}]_U \in \prod^{tor} M_i/U$ and $\phi(\mathbf{x})$ be a formula. By Fact 5.5, $\phi(\mathbf{x})$ is equivalent modulo T_R to a boolean combination σ of invariants conditions and a boolean combination $\psi(\mathbf{x})$ of p. p. formulas. Then

$$\begin{aligned}
\{i \in I : M_i \vDash \phi(f_0(i), \ldots, f_{n-1}(i))\} \in U &\iff \{i \in I : M_i \vDash \sigma \wedge \psi(f_0(i), \ldots, f_{n-1}(i))\} \in U \\
&\iff \prod^{tor} M_i/U \vDash \sigma \wedge \psi([f_0]_U, \ldots, [f_{n-1}]_U) \\
&\iff \prod^{tor} M_i/U \vDash \phi([f_0]_U, \ldots, [f_{n-1}]_U)
\end{aligned}$$

The first and third equivalence is by Fact 5.5 and the second equivalence is by Corollary 5.7 and Lemma 5.9. †

5.3 Examples

For this subsection, we specialize to $R = \mathbb{Z}$. That is, we examine abelian torsion groups.

We look at some examples of torsion abelian groups and examine how the groups differ from their *tor*-ultraproducts and how the AEC $(\mathrm{Mod}(T \cup \{\forall x \bigvee_{n<\omega} n \cdot x = 0\}), \prec)$ differs from the elementary class $(\mathrm{Mod}(T), \prec)$.

We list some torsion abelian groups G such that $G \precneqq \prod^{tor} G/U \precneqq \prod G/U$[6]. The main point here is the inequalities, as the elementary substructure results follow from Theorem 5.10. If G does not have finite exponent, then $\prod G/U$ necessarily contains elements with no order, so $\prod^{tor} G/U \subsetneq \prod G/U$. Theorem 2.17 gives a condition for $G \subsetneq \prod^{tor} G/U$. In this context, the result becomes:

If there is some $n < \omega$ such that there are infinitely many $g \in G$ such that $o(g) \mid n$, then $G \subsetneq \prod^{tor} G/U$.

[6]Formally, G is not a subset of $\prod^{tor} G/U$, but is canonically embedded in it; we blur this distinction by identifying $g \in G$ and $[i \mapsto g]_U \in \prod^{tor} G/U$

Thus, the following groups are all proper elementary subgroups of their *tor*-ultraproducts (for any nonprincipal ultrafilter).

1. $\oplus_{n<\omega}\mathbb{Z}_n$
2. More generally, $\oplus_{n<\omega}\mathbb{Z}_{s_n}$ for any sequence $\langle s_n : n < \omega\rangle$ such that there is a prime p that divides infinitely many of the s_n's
3. $\oplus_{n<\omega}\mathbb{Z}(p^\infty)$ for any prime p or $\oplus_{n<\omega}\mathbb{Q}/\mathbb{Z}$

Note that $\mathbb{Z}(p^\infty)$ and $\mathbb{Q}/\mathbb{Z}$ (or the sum of finitely many of them) do not satisfy this criterion. Thus, by Theorem 5.2, any torsion group elementarily equivalent to them is in fact isomorphic to them.

Consider $G = \oplus_{n<\omega}\mathbb{Z}_{2^n}$ and $I = \omega$. Note that, for any nonzero $g \in G$, there is a maximum $k < \omega$ such that $2^k \mid g$. However, this is not the case in $\prod^{tor} G/U$: set $f : I \to \omega$ sucht that $f(i)$ is 2^{i-1} in $\mathbb{Z}_{2^i}$, i.e. $f(i) \in \prod \mathbb{Z}_{2^n}$ such that

$$f(i)(n) = \begin{cases} 2^{i-1} & \text{if } i = n \\ 0 & \text{otherwise} \end{cases}$$

Then each $f(i)$ has order 2, so $[f]_U \in \prod^{tor} G/U$. However, for every $k < \omega$,

$$\{i \in I : G \vDash \exists y.2^k \cdot y = f(i)\} = \omega - (k+1) \in U$$

So $\prod^{tor} G/U \vDash 2^k \mid [f]_U$ for all $k < \omega$. Thus there are countable submodels of $\prod^{tor} G/U$ not isomorphic to G. Thus, $Th(G)$ is not countably categorical amongst abelian torsion groups.

In contrast, we now examine $Th(\oplus\mathbb{Z}(p^\infty))$. We will show that this theory is not categorical as an elementary class, but it is categorical in all cardinals (and more) in the class of abelian torsion groups[7].

This gives a concrete example of a torsion group where more stability theoretic machinery is available when viewing it as a member of a nonelementary class.

For the first part, we note the following general fact.

Proposition 5.11. *If R is a PID and M is a torsion module such that*

1. *$annM = \{0\}$; and*
2. *there is $r \in R$ such that $\{m \in M : r \in \mathcal{O}(m)\}$,*

[7]More formally, this means that the class $Mod(Th(\oplus\mathbb{Z}(p^\infty)))$ is not categorical, but $Mod(Th(\oplus\mathbb{Z}(p^\infty)) \cup \{\forall x \bigvee_{n<\omega} n \cdot x = 0\})$ is categorical in all cardinals.

then $Th(M)$ is not categorical in any $\lambda \geq |R|$.

If $R = \mathbb{Z}$, then the first condition says that M is not of finite exponent.

Proof: WLOG, $|M| = |R|$. The given conditions ensure that, for any torsion $M' \equiv M$,

$$M' \precneqq \prod^{tor} M'/U \precneqq \prod M/U$$

and that $\prod M/U$ is not torsion. Thus, we have a torsion and non-torsion module elementarily equivalent to M in all cardinalities of size at least $|R|$. Since torsion and non-torsion modules are obviously non-isomorphic, we have the result. †

For the second part, we show that, if we have torsion $G \equiv \oplus_{n<\omega}\mathbb{Z}(p^\infty)$, then $G \cong \oplus_{i<|G|}\mathbb{Z}(p^\infty)$. We rely on the following well-known fact about divisible abelian groups.

Fact 5.12. *Every divisible group is isomorphic to a direct sum of copies of $\mathbb{Q}$ and $\mathbb{Z}(q^\infty)$.*

Since we know G is a divisible p-group, it cannot contain any copies of $\mathbb{Q}$ or $\mathbb{Z}(q^\infty)$ for $q \neq p$. Also, every element of G has infinitely many pth roots, so it cannot be a direct sum of finitely many copies of $\mathbb{Z}(p^\infty)$. Thus, $G \cong \oplus_{i<|G|}\mathbb{Z}(p^\infty)$.

5.4 Some Stability Theory

Now that a compactness result is established, we wish to explore some stability theory for torsion modules over a PID (considered as an AEC). It is already known that all modules are stable (see [19, Theorem 3.A]), but we have seen that examining nonelementary classes can give stronger results.

Definition 5.13. *Let M be an infinite torsion module over a PID. Then $\mathbb{K}_M$ is the AEC whose models are all torsion modules elementarily equivalent to M (in the sense of first-order logic) and where $\prec$ is elementary substructure.*

It is easy to see that this is an AEC. This class is averageable by Theorem 5.10. Furthermore, this AEC is nicely behaved in the sense that amalgamation holds; Galois types are (first-order) syntactic types; and $\mathbb{K}_M$ has no maximal models holds unless all models are isomorphic to M.

Proposition 5.14. *$\mathbb{K}_M$ has amalgamation, joint embedding, and Galois types are syntactic.*

Proof: We show amalgamation and Galois types are syntactic together. Note that, since strong substructure is elementary substructure, having the same Galois type implies having the same syntactic type. Let $M_0 \prec M_1, M_2$ from $\mathbb{K}_M$, possibly with $a_\ell \in M_\ell$ such that $tp(a_1/M_0; M_1) = tp(a_2/M_0, M_2)$. Then, by amalgamation for first order theories, we can find a module N^* and $f_\ell : M_\ell \to N^*$, for $\ell = 1, 2$, that agree on M_0 and (if they exist) $f_1(a_1) = f_2(a_2)$. Set N to be the torsion subgroup of N^*. The torsion radical preserves pure embeddings and picks out a pure subgroup, so we have

$$f_\ell(M_\ell) \subset_{pure} N \subset_{pure} N^*$$

Since they are elementarily equivalent, $Inv(f_\ell(M_\ell), \phi, \psi) = Inv(N^*, \phi, \psi)$ for all p. p. formulas ϕ and ψ and pureness implies that N has the same invariants conditions. Thus, N is elementarily equivalent and the embeddings are elementary. Furthermore, the f_ℓ witness that a_1 and a_2 have the same Galois type.

The proof of joint embedding is similar. †

Note that although two tuples having the same Galois type and having the same syntactic type are the same, the "Galois types are syntactic" result above should *not* be taken to mean that any consistent, complete set of formulas is realized as a Galois type; obviously, this is not true a non-torsion element. However, we do have a local compactness result: any partial type is realizable iff there is a fixed order such that all of its finite subsets are realizable with that fixed order.

Proposition 5.15. *Let $A \subset N \in \mathbb{K}_M$ and $p(\mathbf{x})$ be a consistent set of formulas with parameters in A. Then there is an extension of N that realizes p iff there are $r_0, \ldots, r_{n-1} \in R$ such that, for every finite $q \subset p$, there is an extension of N that realizes $q \cup \{r_i \cdot x_i = 0 : i < n\}$.*

Proof: This is Theorem 3.3 in this context. †

Proposition 5.16. $\mathbb{K}_M$ *has no maximal models or consists of a single model up to isomorphism.*

Proof: Follows directly from Theorem 3.13. †

Since this class is stable, we have a unique independence relation.

Theorem 5.17. *1. $\mathbb{K}_M$ is Galois stable at least in all λ^ω.*

2. Coheir is a stability-like independence relation.

3. *Any independence relation satisfying Existence, Extension, and Uniqueness is coheir.*

Proof:

1. $\mathbb{K}_M$ has less types than $Mod(Th(M))$ (this uses that Galois types are syntactic), which is stable (see [19, Chapter 3, Example 1]).
2. This follows from Theorem 3.11.
3. This is [10, Corollary 5.18]

As a consequence of the last statement, this means that the good frame defined by nonsplitting from Vasey [28] is the same as coheir in $\mathbb{K}_{\oplus_{n<\omega}\mathbb{Z}(p^\infty)}$.

Acknowledgment

This work was begun while the author was working towards his PhD under Rami Grossberg and he is grateful for his guidance and support. Part of this material is based upon work done while the author was supported by the National Science Foundation under Grant No. DMS-1402191.

References

[1] John Baldwin, **Categoricity**, University Lecture Series, American Mathematical Society, 2009.

[2] John Baldwin and Saharon Shelah, *Examples of non-locality*, Journal of Symbolic Logic **73** (2008), 765–782.

[3] Itai Ben Yaacov, *Continuous first order logic for unbounded metric structures*, Journal of Mathematical Logic **8** (2008)

[4] Itai Ben Yaacov, Alexander Berenstein, C. Ward Henson, Alexander Usvyatsov, *Model theory for metric structures*, **Model theory with applications to algebra and analysis, vol. 2** (Chatzidakis, Macpherson, Pillay, Wilke eds.). London Math Society Lecture Note Series, Cambridge University Press, 2008.

[5] Will Boney, *Tameness from large cardinals axioms*, Journal of Symbolic Logic **79** (2014), 1092–1119.

[6] Will Boney, *Coheir in Averageable Classes*, `https://wboney.wp.txstate.edu/boneyavcoheir/`

[7] Will Boney, A Presentation Theorem for Continuous Logic and Metric Abstract Elementary Classes, *Mathematical Logic Quarterly*, vol 63, no 5, 2017, 397–414.

[8] Will Boney, *Some Model Theory of Classsically Valued Fields*, In preparation.

[9] Will Boney and Rami Grossberg, Forking in Short and Tame Abstract Elementary Classes, *Annals of Pure and Applied Logic*, vol 168, no 8, 2017, 1517-1551.

[10] Will Boney, Rami Grossberg, Alexei Kolesnikov, and Sebastien Vasey. *Canonical Forking in AECs*, Annals of Pure and Applied Logic **167** (2016), 590–613

[11] Rami Grossberg, *Classification theory for abstract elementary classes*, **Logic and Algebra**, ed. Yi Zhang, Contemporary Mathematics, Vol 302, AMS, (2002), pp. 165–204.

[12] Rami Grossberg and Monica VanDieren, *Galois-stability for tame abstract elementary classes*, Journal of Mathematical Logic **6** (2006), no. 1, 25–49.

[13] Philipp Hieronymi, *Expansions of the ordered additive group of real numbers by two discrete subgroups*, Journal of Symbolic Logic **81** (2016), 1091–1115.

[14] Wilfrid Hodges, **Model Theory**. Cambridge University Press, 1993.

[15] Jonathan Kirby, *On quasiminimal excellent classes*, Journal of Symbolic Logic **75** (2010), 551-564

[16] Oren Kolman and Saharon Shelah, *Categoricity of theories in $L_{\kappa\omega}$, when κ is a measureable cardinal, part 1*, Fundamenta Mathematica **151** (1996), 209-240

[17] Michael Makkai and Saharon Shelah, *Categoricity of theories in $L_{\kappa\omega}$, with κ a compact cardinal*, Annals of Pure and Applied Logic **47** (1990), 41–97.

[18] Chris Miller, *Expansions of dense linear orders with the Intermediate Value Property*, Journal of Symbolic Logic **66** (2001), 1783-1790

[19] Mike Prest, **Model Theory and Modules**. London Mathematical Society Lecture Notes Series **130** (1988). Cambridge University Press, Cambridge.

[20] Saharon Shelah, **Classification theory and the number of nonisomorphic models**, 2nd ed., vol. 92, North-Holland Publishing Co., Amsterdam, xxxiv+705 pp, 1990.

[21] Saharon Shelah, **Classification Theory for Abstract Elementary Classes**, vol. 1 & 2, Mathematical Logic and Foundations, no. 18 & 20, College Publications, 2009.

[22] Saharon Shelah, *Classification of nonelementary classes, II. Abstract Elementary Classes*, Classification theory (John Baldwin, ed.), 1987, pp. 419–497.

[23] Saharon Shelah, *Categoricity for abstract classes with amalgamation*, Annals of Pure and Applied Logic **98** (1990), 261–294.

[24] Saharon Shelah, *Modules and Infinitary Logics*, (Groups and Model theory) Contemporary Mathematics **576** (2012), 305-316

[25] Saharon Shelah, *On superstable aec of modules*, In preparation

[26] Thoralf Skolem, *Uber einige Satzfunktionen in der Arithmetik*, Skrifter Vitenskapsakadetiet i Oslo **7** (1931), 1-28

[27] Lou van den Dries, **Tame Topology and O-minimal Structures**, Cambridge University Press, 1998.

[28] Sebastien Vasey, *Forking and superstability in tame AECs*, Journal of Symbolic Logic **81** (2016), 357–383.

 Received 31 August 2019

Fragments of Quasi-Nelson: Two Negations

Umberto Rivieccio*
Departamento de Informática e Matemática Aplicada,
Universidade Federal do Rio Grande do Norte,
Natal, Brasil
urivieccio@dimap.ufrn.br

Abstract

The variety of quasi-Nelson algebras has been recently singled out and characterised in several equivalent ways: among others, as (1) the class of bounded commutative integral (but not necessarily involutive) residuated lattices satisfying the Nelson identity, as well as (2) the class of $(0, 1)$-congruence orderable commutative integral residuated lattices. Logically, quasi-Nelson algebras are the algebraic counterpart of quasi-Nelson logic, which is the (algebraisable) extension of the substructural logic $\mathcal{FL}_{ew}$ (Full Lambek calculus with Exchange and Weakening) by the Nelson axiom. Quasi-Nelson logic may also be viewed as a common generalisation of both Nelson's constructive logic with strong negation and intuitionistic logic. The present paper focusses on the subreducts of quasi-Nelson algebras obtained by eliding the implication while keeping the two term-definable negations. It is shown that, similarly to the involutive case (treated by A. Sendlewski in 1991), this class of algebras is a variety that can be characterised by means of twist-structures over pseudo-complemented distributive lattices. In this way we extend to a non-involutive setting the well-known connection between Nelson and Heyting algebras, as well as Sendlewski's result relating Kleene algebras with a weak pseudo-complementation and pseudo-complemented distributive lattices.

1 Introduction

Nelson's constructive logic with strong negation $\mathcal{N}$ (introduced in [16]; see also [17, 25, 29]) is a well-known and by now fairly well-understood non-classical logic that

*The author acknowledges partial funding by the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq, Brazil), under the grant 313643/2017-2 (Bolsas de Produtividade em Pesquisa - PQ).

combines the constructive approach of positive intuitionistic logic with a classical (i.e. De Morgan) negation. The algebraic models of $\mathcal{N}$, forming a variety called *Nelson algebras* or *Nelson residuated lattices*, have been studied since at least the late 1950's (firstly by H. Rasiowa; see [17] and references therein) and are also by now fairly well understood. One of the main algebraic insights on this variety came, towards the end of the 1970's, with the realisation (independently due to M. M. Fidel and D. Vakarelov) that every Nelson algebra can be represented as a special binary product (here called a *twist-structure*) of a Heyting algebra. This correspondence was formulated as a categorical equivalence (by A. Sendlewski in the early 1990's) between Nelson algebras and a category of enriched Heyting algebras, which made it possible to transfer a number of fundamental results from the more widely studied theory of intuitionistic logic to the realm of Nelson algebras.

The most important advance in the theory of Nelson algebras since Sendlewski's work in the 1990's was probably the discovery that Nelson logic can be viewed as one of the so-called substructural logics. This result (first proved in 2008 by M. Spinks and R. Veroff [27, 28]) entails that (modulo algebraic signature formalities) Nelson algebras can be presented as a subvariety of (bounded, commutative, integral) residuated lattices [5]; hence the alternative name of *Nelson residuated lattices*. Given the flourish of studies on substructural logics and residuated structures (leading to and following the book [5]), this alternative perspective on Nelson algebras has proven quite fruitful. Indeed, it has made in the first place possible to recover or recast a number of results on Nelson algebras by specialising more general ones about residuated structures. Furthermore, and perhaps more interestingly, it allowed scholars to formulate new questions that can be best appreciated within the wider theory of residuated lattices. Among these is the problem that led to the introduction of *quasi-Nelson algebras*, which can be phrased as follows.

We know, by the results of M. Spinks and R. Veroff, that Nelson algebras can be viewed as the class of (bounded, commutative, integral) residuated lattices that additionally satisfy the involutive law ($x \approx (x \Rightarrow 0) \Rightarrow 0$) and the identity (Nelson) displayed in Section 2. Hence, all results that are specific to Nelson algebras (as opposed to general residuated lattices), including the connection with Heyting algebras discovered by Vakarelov and Fidel, essentially depend on involutivity and (Nelson). Do they indeed rely, one may ask, equally on both properties or perhaps just on one of them?

It is interesting to note that, while the class of involutive residuated lattices has attracted a fair amount of attention in the algebraic logic community (see e.g. [6, 8]), the class of residuated lattices satisfying the identity (Nelson) alone was never considered before [22]. It is not difficult to convince oneself that the involutive identity alone is not sufficient to obtain a result such as the Fidel-Vakarelov-Sendlewski rep-

resentation (at least in the forms that we know) of Nelson algebras as products of Heyting algebras. On the other hand, the identity (Nelson), which could be speculated to be sufficient, has proved to be difficult to work with. It is also possible that other 'hidden' identities may be involved, such as the so-called *3-potency* (corresponding to the logical axiom sometimes called $3,2$-*contraction*) – which indeed corresponds to quite a powerful structural property – or the lattice-theoretic distributive laws. In an involutive setting, both properties are consequences of (Nelson): but does this hold true once we drop involutivity?

In the papers [22, 23] my coauthors and I addressed the above-mentioned problem in broad terms: namely, we tried to determine how much of the structure theory of Nelson algebras can be reconstructed (within the context of residuated lattices) in the presence of the identity (Nelson) but independently of the involutive law. To our surprise, it turned out that some of the most characteristic results on Nelson algebras do not require involutivity.

In [22, 23] we have shown, in particular, that (a suitable generalisation of) the Fidel-Vakarelov-Sendlewski construction can be performed in a not-necessarily involutive context: thus making it possible to recover the connection between Heyting algebras and 'non-involutive Nelson algebras', a variety of algebras that we proposed to call *quasi-Nelson algebras* (alias *quasi-Nelson residuated lattices*) in analogy with Sankappanavar's quasi-De Morgan algebras. This variety we have also characterised by a purely congruence-theoretical property introduced in [15] under the name of $(0,1)$-*congruence orderability*; the main result being that among (bounded, commutative, integral) residuated lattices, quasi-Nelson algebras are precisely the $(0,1)$-congruence orderable ones. We generalised in this way the characterisation of Nelson algebras obtained in [15], namely that, if we restrict ourselves to the class of involutive residuated lattices, then the $(0,1)$-congruence orderable ones are precisely the Nelson residuated lattices.

A further advantage of viewing Nelson's logic $\mathcal{N}$ as a substructural logic (which, as such, extends the logic of all residuated lattices, known as *Full Lambek Calculus* or $\mathcal{FL}$) is the possibility to work with logics that are algebraisable in the sense of [4]. In such a context, every algebraic identity corresponds one-to-one to a logical axiom and vice-versa; algebraic identities characterise subvarieties of the class of all residuated lattices, while logical axioms characterise axiomatic extensions of $\mathcal{FL}$. The logic $\mathcal{QN}$ of quasi-Nelson algebras is also determined by this correspondence: $\mathcal{QN}$ is precisely the logic obtained by extending $\mathcal{FL}$ with axioms corresponding to commutativity, integrality, boundedness and the identity (Nelson). On the other hand, in analogy with Nelson's logic $\mathcal{N}$, it should also be possible to view the logic $\mathcal{QN}$ in the old-fashioned way (in keeping with D. Nelson's original presentation, later adopted by H. Rasiowa), namely as an expansion of positive intuitionistic logic

by a new negation connective[1]. This approach is pursued in [14], and the resulting logic is axiomatised and shown to be algebraisable, as expected, with respect to quasi-Nelson algebras (there presented as algebras having a Heyting-like implication enriched with a new negation operator, rather than as a subclass of residuated lattices).

From a logical point of view, it is worthwhile observing that, once we get rid of the involutive law (corresponding to the logical axiom $((p \Rightarrow \bot) \Rightarrow \bot) \Rightarrow p$), the addition of Nelson's axiom (Nelson-Ax) to $\mathcal{FL}$ does not make the resulting logic (i.e. $\mathcal{QN}$) incomparable with intuitionistic logic, because Nelson's axiom is (trivially) sound w.r.t. the intuitionistic semantics. This entails that, while Nelson's logic $\mathcal{N}$ is incomparable with intuitionistic logic (the only common extension being classical logic), quasi-Nelson logic $\mathcal{QN}$ can be viewed as a common generalisation of both Nelson's and intuitionistic logic[2]. This, indeed, is a remarkable difference between Nelson's and quasi-Nelson logic, as well as between Nelson and quasi-Nelson algebras[3].

The aim of the present paper is to carry on the investigation of quasi-Nelson algebras initiated in [22, 23] by focussing on the implication-free fragment of the algebraic language. More precisely, we get rid of the implication while keeping the *two* negation operators that are term-definable in the full language of quasi-Nelson algebras. Notice that, in the absence of the implication, the above-mentioned correspondence between logics and algebras that is a corollary of algebraisability is lost (cf. Proposition 5.7). This notwithstanding, we will show that a twist-structure construction can be used to characterise the class of algebras corresponding to the implication-free fragment (i.e. the subreducts) of quasi-Nelson algebras. This is the main result of the paper, from which we derive a few applications to subvarieties of the class of 'implicationless quasi-Nelson algebras'. As a by-product, we will also obtain further insight on the class of quasi-Nelson algebras in the form of an alternative twist-structure representation (see Section 8).

The present study can be viewed as a non-involutive counterpart of Sendlewski's investigations into the two-negation fragment of Nelson algebras [26]. This variety

[1]By an *extension* or *strengthening* (of a given logic) we mean a stronger logic over the same language; by an *expansion* we mean a logic obtained by adding new connectives.

[2]Already at this point, the reader might be wondering whether $\mathcal{QN}$ is precisely the meet (or intersection), in the lattice of all logics extending $\mathcal{FL}$, of Nelson's logic and intuitionistic logic. This is not the case: $\mathcal{QN}$ is strictly weaker than this intersection (see [20, Subsection 3.1]).

[3]The above considerations entail, in particular, that Heyting algebras can be represented as twist-structures *over Heyting algebras* [23]. This is of course a degenerate case in the representation, yet one that is not entirely devoid of information. Indeed, the result shows how the (order-reversing) Heyting negation operator can be decomposed into two order-preserving maps (the n and p introduced in Definition 2.5 below) from (subsets of) the Heyting algebra to itself.

of algebras, called *wp-Kleene algebras*, is shown in [26] to correspond, via a twist-structure construction, to pseudo-complemented distributive lattices (i.e. the subreducts of Heyting algebras with negation but without implication). In Sendlewski's terms, this entails that the functor that relates Nelson and Heyting algebras can be extended to a functor with similar properties relating the implication-free subreducts of both classes.

As we will show, the majority of results contained in [26] can be retrieved from the ones established in the present study by restricting our attention to involutive algebras. A close comparison of the two papers will also reveal that, while most techniques from [26] allow for a straightforward generalisation to the non-involutive context, the correspondence between subvarieties of *wp*-Kleene algebras and of pseudo-complemented distributive lattices does not; thus suggesting that the lattice of subvarieties of 'non-involutive *wp*-Kleene algebras' may indeed be intrinsically more complex than its involutive counterpart.

Besides [26], the only antecedents to the present paper (that I know of) are the studies by A. Monteiro's school on the implication-free subreducts of Nelson algebras, as well as the recent [19], in which the class of implication-free subreducts of quasi-Nelson algebras (with just one negation, the primitive one, in the language) is characterised, also by means of twist-structures. In the present paper we shall, indeed, rely on a few results from [19] that will allow us to shorten our proofs. The reader should however be aware that such a dependency is inessential. In fact, as will be demonstrated, the added expressivity given by the presence of the second negation would allow us to establish all our results without any reference to [19].

The paper is organised as follows. Section 2 contains preliminary observations and definitions on the main classes of algebras involved in our study. In Section 3 we introduce the 'concrete' twist-structure construction meant to provide a representation for the implication-free subreducts of quasi-Nelson algebras. An abstract (equational) presentation for the corresponding algebras, that in keeping with Sendlewski's terminology we call *weakly pseudo-complemented quasi-Kleene algebras* (WPQK-algebras), is contained in Section 4. The twist-structure representation result is also proved in this section (Theorem 4.10). The subsequent Section 5 focusses on the relation between quasi-Nelson and WPQK-algebras, establishing in particular that the latter is precisely the class of implication-free subreducts of the former. Section 6 introduces a more fine-grained twist-structure representation, so as to provide a basis on which one can build a co-variant categorical equivalence between WPQK-algebras and enriched (pairs of) pseudo-complemented distributive lattices; Sendlewski's equivalence between *wp*-Kleene algebras and enriched pseudo-complemented distributive lattices is recovered by specialising our result to the involutive case. Section 7 relates the congruence lattice of a WPQK-algebra to the

congruence lattices of the corresponding factors given by the twist representation; the result that (in the involutive case) Sendlewski's functor preserves the structure of the congruence lattice can also be obtained as a consequence of our Theorem 7.8. The very brief Section 8 translates a few observations from the preceding ones into an alternative, modally-oriented twist representation for WPQK-algebras. The main import of the latter is the indication of a potentially novel perspective on the study of WPQK and quasi-Nelson algebras via twist-structures: from this alternative point of view, the counterpart of a WPQK (or quasi-Nelson) algebra should be taken to be one (enriched) algebra with a (so-called) *nucleus* operator rather than two algebras related by maps. Section 9 collects some information on a few subvarieties of WPQK-algebras that admit a simple characterisation in terms of the twist representation. Section 10 closes the paper with a few final considerations and perspectives on future research.

2 Quasi-Nelson Logic, Algebras and Residuated Lattices

Let us begin by introducing quasi-Nelson algebras, the algebras in the full language (regarding which we refer the reader to [22, 23] for further details and proofs; see also [5] for all unexplained algebraic and logical terminology). The most convenient way to do so is to take the substructural route, starting from the notion of residuated lattice.

Definition 2.1. A *commutative integral bounded residuated lattice* (CIBRL) is an algebra $\mathbf{A} = \langle A; \wedge, \vee, *, \Rightarrow, 0, 1\rangle$ of type $\langle 2, 2, 2, 2, 0, 0\rangle$ such that:

(i) $\langle A; *, 1\rangle$ is a commutative monoid, (Mon)

(ii) $\langle A; \wedge, \vee, 0, 1\rangle$ is a bounded lattice (with order $\leq$), (Lat)

(iii) $a * b \leq c$ iff $a \leq b \Rightarrow c$ for all $a, b, c \in A$. (Res)

Despite item (iii) above, the class of CIBRLs is equationally definable (a variety). A slightly more general class (that we will not need much in the present context) is that of (not-necessarily lower-bounded) commutative integral residuated lattices (CIRLs), which differ from CIBRLs because the constant 0 is not included in the algebraic signature. As hinted at in the introduction, CIRLs are the algebraic counterpart of the logic called $\mathcal{FL}_{ew}$, which is the extension of the Full Lambek Calculus $\mathcal{FL}$ obtained by adding the rules of *exchange* (e) and *weakening* (w). This entails that CIBRLs are the algebraic counterpart of the expansion of $\mathcal{FL}_{ew}$ by a

propositional constant (usually denoted $\bot$ or 0) meant to be interpreted as the least element on the algebras.

If the logical/algebraic signature does include a constant symbol 0 (as will always be assumed in the present paper), then one can define a *negation* connective in the logic by $\sim p := p \Rightarrow 0$, to which corresponds a similarly defined negation operator on every algebraic model. This allows us to write the *Nelson axiom*

$$((p \Rightarrow (p \Rightarrow q)) \wedge (\sim q \Rightarrow (\sim q \Rightarrow \sim p))) \Rightarrow (p \Rightarrow q) \qquad \text{(Nelson-Ax)}$$

whose *alter ego*, on algebraic models, is the *Nelson identity*:

$$(x \Rightarrow (x \Rightarrow y)) \wedge (\sim y \Rightarrow (\sim y \Rightarrow \sim x)) \approx x \Rightarrow y. \qquad \text{(Nelson)}$$

As mentioned earlier, the papers [22, 23, 14] concern the logic obtained by extending $\mathcal{FL}_{ew}$ (with a 0 constant) with the addition of the Nelson axiom. We called this logic *quasi-Nelson logic*, and the corresponding algebras *quasi-Nelson algebras* or *quasi-Nelson residuated lattices*. Further adding the double negation axiom ($\sim\sim p \Rightarrow p$) to quasi-Nelson logic, one obtains Nelson's constructive logic with strong negation $\mathcal{N}$, whose algebraic counterpart is the variety of Nelson algebras.

Definition 2.2. A *quasi-Nelson residuated lattice* (or *quasi-Nelson algebra*) is a CIBRL that satisfies the identity (Nelson). A *Nelson residuated lattice* (or *Nelson algebra*) is a quasi-Nelson residuated lattice that satisfies the involutive identity $\sim\sim x \approx x$.

As hinted at earlier, every Heyting algebra satisfies the identity (Nelson), and is therefore an example of a quasi-Nelson algebra (by contrast, the only examples of Heyting algebras which are also Nelson algebras are the Boolean algebras). The class of quasi-Nelson algebras can thus be viewed as a common generalisation of Heyting algebras and Nelson algebras.

An observation that will be central to the present study is that, within Nelson and quasi-Nelson logic, a second implication connective $\to$ can be defined by $p \to q := p \Rightarrow (p \Rightarrow q)$. There is no doubt that $\to$ is an implication in its own right, and this is indeed the implication connective originally taken as primitive by D. Nelson (followed H. Rasiowa and so on) in defining his logic. Traditionally, $\to$ is called the *weak implication*, while $\Rightarrow$ is the *strong* one. Taking the former as primitive, the strong implication can be recovered by defining $p \Rightarrow q := (p \to q) \wedge (\sim q \to \sim p)$; the monoid connective $*$ is also definable as $p * q := \sim(p \Rightarrow \sim q)$. Indeed, one of the main results in the theory of Nelson logic/algebras (which, as shown in [22, 23], extends to quasi-Nelson without dramatic changes) is that the presentation over the language $\{\wedge, \vee, *, \Rightarrow, \sim, 0, 1\}$ of Definition 2.2 ('Nelson residuated lattices') is equivalent, on

the level of both logic and algebras, to the one over the language $\{\wedge, \vee, \to, \sim, 0, 1\}$, corresponding to the original denomination of 'Nelson algebras'.

The presence of the weak implication (either as a primitive or as a defined connective) in the (quasi-)Nelson setting makes it possible to introduce a second negation $\neg$ (alternative to $\sim$) given by $\neg p := p \to 0$. In the literature on Nelson logic this new connective has been sometimes called the 'intuitionistic negation' (the primitive $\sim$ being the 'strong' or De Morgan negation). This terminology makes little sense outside the involutive setting, because the primitive negation $\sim$ is also 'intuitionistic' (as mentioned above, Heyting algebras are quasi-Nelson algebras); in fact, it may well be argued that $\sim$ is closer to intuitionistic negation than $\neg$ (see e.g. the observations immediately preceding Proposition 4.3). Following Sendlewski, we shall call $\neg$ a *weak pseudo-complement(ation)*.

The paper [26] introduces and studies the class of algebras obtained by eliding the implication(s) from the language of Nelson algebras while taking both negations as primitive. This is a variety of algebras dubbed *Kleene algebras with a weak pseudo-complementation* (or *wp-Kleene algebras* for short; see Definition 4.14). In [26], a number of results are established about *wp*-Kleene algebras, including the fundamental one that they can be represented through (what we here call) twist-structures over pseudo-complemented distributive lattices. This observation is then used to obtain information on the subdirectly irreducible members of the variety of *wp*-Kleene algebras and on the lattice of its subvarieties.

In the present paper we undertake a study similar to Sendlewski's but extended to 'non-involutive *wp*-Kleene algebras', which we are going to define by applying Sendlewski's procedure to quasi-Nelson algebras in lieu of Nelson algebras. Virtually all results obtained here will thus be generalisations of Sendlewski's, which will allow us to recover those of [26] by specialising to involutive algebras. This holds true even of those results that appear much less satisfactory than their involutive counterparts (e.g. Theorem 7.8). More than a fault on our part, this is (as we will demonstrate) an indication that 'non-involutive *wp*-Kleene algebras' are an essentially more complex class than their involutive counterparts.

We now proceed to introduce formally the classes of algebras involved in the present study. As observed in [22, Proposition 2.7], the $\{\wedge, \vee, \sim, 0, 1\}$-reduct of every quasi-Nelson algebra is a 'lower quasi-De Morgan' algebra according to the terminology introduced by H.P. Sankappanavar [24]. It will be useful to have the definition at hand. Here and henceforth, we use the symbol $\approx$ to represent formal equality between algebraic terms, and we write $s \ll t$ as a shorthand for the identity (or equation) $s \wedge t \approx s$.

Definition 2.3 ([24])**.** A *semi-De Morgan algebra* is an algebra $\mathbf{A} = \langle A; \wedge, \vee, \sim, 0, 1\rangle$

of type $\langle 2, 2, 1, 0, 0\rangle$ satisfying the following properties:

(SD1) $\langle A; \wedge, \vee, 0, 1\rangle$ is a bounded distributive lattice,

(SD2) $\sim 0 \approx 1$ and $\sim 1 \approx 0$,

(SD3) $\sim(x \vee y) \approx \sim x \wedge \sim y$,

(SD4) $\sim\sim(x \wedge y) \approx \sim\sim x \wedge \sim\sim y$,

(SD5) $\sim x \approx \sim\sim\sim x$.

A *lower quasi-De Morgan algebra* is a semi-De Morgan algebra that satisfies:

(QD) $x \ll \sim\sim x$.

A *De Morgan algebra* can be defined as a semi-De Morgan algebra that satisfies the involutive identity $\sim\sim x \approx x$.

In the sequel of the paper (especially in proofs) we shall refer to properties (SD2) to (SD5), collectively, as to the *semi-De Morgan identities* (or *laws*). The axiomatisation of lower quasi-De Morgan algebras introduced above does not completely characterise the class of implication-free subreducts of quasi-Nelson algebras. These form a more specific class, called *quasi-Kleene algebras*, that we introduced and studied in [19, Definition 2.2].

Definition 2.4. A *quasi-Kleene algebra* $\mathbf{A}$ is a semi-De Morgan algebra that additionally satisfies the following identities:

(QK1) $x \wedge \sim x \ll y \vee \sim y$, (the Kleene identity)

(QK2) $x \ll \sim\sim x$, (thus $\mathbf{A}$ is a lower quasi-De Morgan algebra)

(QK3) $\sim\sim x \wedge \sim(x \wedge y) \ll \sim x \vee \sim y$,

(QK4) $\sim\sim x \wedge \sim x \ll x$.

A *Kleene algebra* can be defined as a quasi-Kleene algebra that satisfies the involutive identity: $\sim\sim x \approx x$.

While semi-De Morgan algebras are due to Sankappanavar, De Morgan algebras (alongside Kleene algebras) have been studied since the late 1950's, beginning with the works of J.A. Kalman, A. Monteiro and his school. Every Nelson algebra has a Kleene algebra reduct; indeed, Kalman's results easily entail that Kleene algebras are precisely the $\{\wedge, \vee, \sim\}$-subreducts of Nelson algebras. Similarly, we have shown

in [19, Corollary 6.6] that quasi-Kleene algebras are the $\{\wedge, \vee, \sim\}$-subreducts of quasi-Nelson algebras. In keeping with this observation, we shall introduce the abstract algebras meant to characterise the $\{\wedge, \vee, \sim, \neg\}$-subreducts of quasi-Nelson algebras as a class of quasi-Kleene algebras expanded with a new negation $\neg$ (see Definition 4.2).

Before proceeding with the definitions, we need to recall another key result from the theory of quasi-Nelson algebras. This is the twist-structure representation mentioned in the Introduction.

Definition 2.5. Given Heyting algebras $\mathbf{H}_+ = \langle H_+, \wedge_+, \vee_+, \to_+, 0_+, 1_+\rangle$ and $\mathbf{H}_- = \langle H_-, \wedge_-, \vee_-, \to_-, 0_-, 1_-\rangle$, let $n\colon H_+ \to H_-$ and $p\colon H_- \to H_+$ be maps satisfying the following properties:

(i) n preserves finite meets, finite joins and the bounds,

(ii) p preserves finite meets and the bounds,

(iii) $n \circ p = Id_{H_-}$ and $Id_{H_+} \leq_+ p \circ n$.

The algebra $\mathbf{H}_+ \bowtie \mathbf{H}_- = \langle H_+ \times H_-, \wedge, \vee, \to, \sim, 0, 1\rangle$ is defined as follows. For all $\langle a_+, a_-\rangle, \langle b_+, b_-\rangle \in H_+ \times H_-$,

$$\begin{aligned}
1 &= \langle 1_+, 0_-\rangle \\
0 &= \langle 0_+, 1_-\rangle \\
\sim\langle a_+, a_-\rangle &= \langle p(a_-), n(a_+)\rangle \\
\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle &= \langle a_+ \wedge_+ b_+, a_- \vee_- b_-\rangle \\
\langle a_+, a_-\rangle \vee \langle b_+, b_-\rangle &= \langle a_+ \vee_+ b_+, a_- \wedge_- b_-\rangle \\
\langle a_+, a_-\rangle \to \langle b_+, b_-\rangle &= \langle a_+ \to_+ b_+, n(a_+) \wedge_- b_-)\rangle.
\end{aligned}$$

A *quasi-Nelson twist-structure* $\mathbf{A}$ over $\mathbf{H}_+ \bowtie \mathbf{H}_-$ is a $\{\wedge, \vee, \to, \sim, 0, 1\}$-subalgebra of $\mathbf{H}_+ \bowtie \mathbf{H}_-$ with carrier set A satisfying $\pi_1(A) = H_+$ and $a_+ \wedge_+ p(a_-) = 0_+$ for all $\langle a_+, a_-\rangle \in A$.

The reader familiar with the representation of Nelson algebras will recognise the above definition (introduced in [22], refined in [23]) as a generalisation of the Fidel-Vakarelov-Sendlewski construction for Nelson algebras. Indeed, the latter can be viewed as a special case of Definition 2.5 in which the maps n and p are mutually inverse Heyting algebra isomorphisms.

Upon defining $x \Rightarrow y := (x \to y) \wedge (\sim y \to \sim x)$ and $x * y := x \wedge y \wedge \sim(x \Rightarrow \sim y)$, every quasi-Nelson twist-structure gives rise to a quasi-Nelson residuated lattice (the

operations $\Rightarrow$ and $*$ could obviously be introduced as primitive in Definition 2.5; we have not done so for the sake of consistency with the notation introduced in [22], which is the traditional one for Nelson algebras). More importantly, *every quasi-Nelson residuated lattice/algebra arises in this way* [22, Proposition 6]. The twist-structure construction thus provides a more concrete way to obtain all members of the abstractly-defined class of quasi-Nelson algebras/residuated lattices. As we shall see throughout the whole paper, one of the advantages of such a representation is that it is highly helpful in simplifying the algebraic calculations (verifying or refuting identities, etc.).

We shall not give here further details on the twist representation for quasi-Nelson algebras; these can be found in [22, 23], and will also be demonstrated in the course of our treatment of twist-structures in the next sections. In view of our study of subreducts, what is important to observe at this point is that Definition 2.5 can be straightforwardly restricted to the language $\{\wedge, \vee, \sim, \neg, 0, 1\}$ in which the $\neg$ operation is given component-wise, for all $\langle a_+, a_-\rangle \in A$, by $\langle a_+, a_-\rangle \to \langle 0_+, 1_-\rangle$. This is precisely what we shall do with Definition 3.1 in the next section; our final aim being to show that every subreduct of a quasi-Nelson algebra can be obtained in this way.

3 Concretely: Weakly Pseudo-Complemented Quasi-Kleene Twist-Structures

We begin by describing a twist-structure construction for "implication-free quasi-Nelson algebras with two negations", i.e. algebras $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ with no implication but having both the quasi-Nelson negation $\sim$ and the weak pseudo-complement $\neg$, which is defined, on quasi-Nelson algebras, via the weak implication by $\neg x := x \to 0$. The definitions are a pretty straightforward restriction of those for the algebras in the full language (Definition 2.5); the interesting result is that they are indeed sufficient to characterise the algebras in the reduced language, i.e. the subreducts of quasi-Nelson algebras[4].

Recall that *pseudo-complemented distributive lattices* (also called *distributive p-algebras* or simply *p-lattices*) are algebras $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ of type $\langle 2, 2, 1, 0, 0\rangle$ that are precisely the $\{\wedge, \vee, \neg, 0, 1\}$-subreducts of Heyting algebras [2, Chapter VIII].This class can be axiomatized by requiring $\langle A; \wedge, \vee, 0, 1\rangle$ to be a bounded distributive lattice (with order $\leq$, bottom 0 and top 1) satisfying the property that, for all

[4]We include the constants 0 and 1 in the language from the start because they are term-definable. That is, the $\{\wedge, \vee, \sim, \neg\}$- and the $\{\wedge, \vee, \sim, \neg, 0, 1\}$-fragment of the quasi-Nelson algebraic language determine the same class of algebras (this is a consequence, e.g., of item (ii) of Proposition 4.12).

$a, b \in A$,

(P) $\quad a \leq \neg b \quad$ if and only if $\quad a \wedge b = 0.$ (pseudo-complement)

We shall refer to (P) as to the property of the pseudo-complement. It is useful to keep in mind that, on every distributive lattice A, the pseudo-complement $\neg b$ of each $b \in A$ (if it exists) is uniquely determined by the lattice structure in the following way:

$$\neg b = \bigvee \{a \in A : a \wedge b = 0\}.$$

Definition 3.1. Given a p-lattice $\mathbf{A}_+ = \langle A_+; \wedge_+, \vee_+, \neg_+, 0_+, 1_+ \rangle$, a bounded distributive lattice $\mathbf{A}_- = \langle A_-; \wedge_-, \vee_-, 0_-, 1_- \rangle$ and maps $n\colon A_+ \to A_-$ and $p\colon A_- \to A_+$ satisfying the following properties:

(i) n is a bounded lattice homomorphism,

(ii) p preserves finite meets and both lattice bounds,

(iii) $n \circ p = Id_{A_-}$ and $Id_{A_+} \leq_+ p \circ n$,

the algebra $\mathbf{A}_+ \bowtie \mathbf{A}_- = \langle A_+ \times A_-; \wedge, \vee, \sim, \neg, 0, 1 \rangle$ is defined as follows. For all $\langle a_+, a_- \rangle, \langle b_+, b_- \rangle \in A_+ \times A_-$,

$$\begin{aligned}
1 &= \langle 1_+, 0_- \rangle \\
0 &= \langle 0_+, 1_- \rangle \\
\sim\langle a_+, a_- \rangle &= \langle p(a_-), n(a_+) \rangle \\
\neg\langle a_+, a_- \rangle &= \langle \neg_+ a_+, n(a_+) \rangle \\
\langle a_+, a_- \rangle \wedge \langle b_+, b_- \rangle &= \langle a_+ \wedge_+ b_+, a_- \vee_- b_- \rangle \\
\langle a_+, a_- \rangle \vee \langle b_+, b_- \rangle &= \langle a_+ \vee_+ b_+, a_- \wedge_- b_- \rangle
\end{aligned}$$

A *weakly pseudo-complemented quasi-Kleene twist-structure* (for short, a WPQK twist-structure) $\mathbf{A}$ over $\mathbf{A}_+ \bowtie \mathbf{A}_-$ is a $\{\wedge, \vee, \sim, \neg, 0, 1\}$-subalgebra of $\mathbf{A}_+ \bowtie \mathbf{A}_-$ with carrier set A satisfying $\pi_1(A) = A_+$ and $a_+ \wedge_+ p(a_-) = 0_+$ for all $\langle a_+, a_- \rangle \in A$.

The definition immediately implies that both maps n and p are order-preserving (we will often use this observation, with or without warning, in subsequent proofs). Going forward, we shall write $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$ to indicate that $\mathbf{A}$ is a WPQK twist-structure over $\mathbf{A}_+ \bowtie \mathbf{A}_-$, leaving implicit the maps n and p when no confusion is likely to arise.

Remark 3.2. Observe that the requirement $a_+ \wedge_+ p(a_-) = 0_+$ in Definition 3.1 entails $a_- \wedge_- n(a_+) = 0_-$. Indeed, using the properties of n and of the composite map $n \circ p$, from $a_+ \wedge_+ p(a_-) = 0_+$ we have $n(a_+ \wedge_+ p(a_-)) = n(a_+) \wedge_- np(a_-) = n(a_+) \wedge_- a_- = n(0_+) = 0_-$. Also, it is easy to check that $\pi_1(A) = A_+$ entails $\pi_2(A) = A_-$.

Remark 3.3. To make sure that Definition 3.1 is sound, we need to check that the set

$$A := \{\langle a_+, a_-\rangle \in A_+ \times A_- : a_+ \wedge_+ p(a_-) = 0_+\}$$

is closed under the twist-structure operations, and is therefore the universe of the largest WPQK twist-structure over $\mathbf{A}_+ \bowtie \mathbf{A}_-$. Let us consider first the two negations. For $\sim$, we need to show that $p(a_-) \wedge_+ pn(a_+) = 0_+$ whenever $a_+ \wedge_+ p(a_-) = 0_+$. Recalling that p preserves meets and the bounds (and Remark 3.2), we have $p(a_-) \wedge_+ pn(a_+) = p(a_- \wedge_- n(a_+)) = p(0_-) = 0_+$. For the $\neg$ negation, we need to check that $\neg_+ a_+ \wedge_+ pn(a_+) = 0_+$. Recall that, on every pseudo-complemented lattice, from $\neg_+ a_+ \leq_+ \neg_+ a_+$ one obtains $\neg_+ a_+ \wedge_+ a_+ = 0_+$. Thus, using $Id_{A_+} \leq_+ p \circ n$, we have $\neg_+ a_+ \wedge_+ pn(a_+) \leq_+ pn(\neg_+ a_+) \wedge_+ pn(a_+) = pn(\neg_+ a_+ \wedge_+ a_+) = pn(0_+) = 0_+$. Moving to the binary operations, we assume $a_+ \wedge_+ p(a_-) = b_+ \wedge_+ p(b_-) = 0_+$. Recall that p preserves meets and that $\mathbf{A}_+$ is a distributive. Then, for $\wedge$, using Remark 3.2 and the inequality $Id_{A_+} \leq_+ p \circ n$, we have $a_+ \wedge_+ b_+ \wedge_+ p(a_- \vee_- b_-) \leq_+ pn(a_+) \wedge_+ pn(b_+) \wedge_+ p(a_- \vee_- b_-) = p(n(a_+) \wedge_- n(b_+) \wedge_- (a_- \vee_- b_-)) = p((n(a_+) \wedge_- n(b_+) \wedge_- a_-) \vee_- (n(a_+) \wedge_- n(b_+) \wedge_- b_-)) = p((0_- \wedge_- n(b_+)) \vee_- (n(a_+) \wedge_- 0_-)) = p(0_-) = 0_+$. For $\vee$, we need to check that $(a_+ \vee_+ b_+) \wedge_+ p(a_- \wedge_- b_-) = 0_+$. Recalling that p preserves meets (and that $\mathbf{A}_+$ is a distributive), We have $(a_+ \vee_+ b_+) \wedge_+ p(a_- \wedge_- b_-) = (a_+ \vee_+ b_+) \wedge_+ p(a_-) \wedge_+ p(b_-) = (a_+ \wedge_+ p(a_-) \wedge_+ p(b_-)) \vee_+ (b_+ \wedge_+ p(a_-) \wedge_+ p(b_-)) = (0_+ \wedge_+ p(b_-)) \vee_+ (0_+ \wedge_+ p(a_-)) = 0_+$, as required.

The following proposition shows that one of the apparent asymmetries between $\mathbf{A}_+$ and $\mathbf{A}_-$ in Definition 3.1 is merely superficial (others, as we shall see, are not).

Proposition 3.4. *For all $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$, the lattice $\mathbf{A}_-$ is pseudo-complemented, with the pseudo-complement given by $\neg_- a_- = n(\neg_+ p(a_-))$ for all $a_- \in A_-$. Furthermore, both maps n and p preserve the pseudo-complement operation (hence, n is a p-lattice homomorphism).*

Proof. Let us check that, for all $a_-, b_- \in A_-$,

$$b_- \leq_- n(\neg_+ p(a_-)) \quad \text{if and only if} \quad a_- \wedge_- b_- = 0_-.$$

Notice that $a_- \wedge_- n(\neg_+ p(a_-)) = np(a_-) \wedge_- n(\neg_+ p(a_-)) = n(p(a_-) \wedge_+ \neg_+ p(a_-)) = n(0_+) = 0_-$. Thus, assuming $b_- \leq_- n(\neg_+ p(a_-))$, we have $a_- \wedge_- b_- \leq_- a_- \wedge_-$

$n(\neg_+ p(a_-)) = 0_-$. Conversely, if $a_- \wedge_- b_- = 0_-$, then $p(a_- \wedge_- b_-) = p(a_-) \wedge_+ p(b_-) = 0_+ = p(0_-)$. By (P), this implies $p(b_-) \leq_+ \neg_+ p(a_-)$, from which we obtain $np(b_-) = b_- \leq_- n(\neg_+ p(a_-))$, as required.

Let us check that p preserves the pseudo-complement, that is, $p(\neg_- a_-) = pn(\neg_+ p(a_-)) = \neg_+ p(a_-)$ for all $a_- \in A_-$. The inequality $\neg_+ p(a_-) \leq_+ pn(\neg_+ p(a_-))$ holds because $Id_{A_+} \leq_+ p \circ n$. It remains to show $pn(\neg_+ p(a_-)) \leq_+ \neg_+ p(a_-)$. Using the property of the pseudo-complement, from $\neg_- a_- = n(\neg_+ p(a_-))$ we have $a_- \wedge_- n(\neg_+ p(a_-)) = 0_-$. Then $p(a_- \wedge_- n(\neg_+ p(a_-))) = p(a_-) \wedge_+ pn((\neg_+ p(a_-)) = p(0_-) = 0_+$. Hence, again by the property of the pseudo-complement, $p(a_-) \wedge_+ pn((\neg_+ p(a_-)) = 0_+$ gives us $pn((\neg_+ p(a_-)) \leq_+ \neg_+ p(a_-)$, as required.

To see that n preserves the pseudo-complement operation, observe that, for all $a_+ \in A_+$, one has $\neg_+ a_+ = \neg_+ pn(a_+)$. In fact, on the one hand (since $Id_{A_+} \leq_+ p \circ n$) we have $a_+ \leq_+ pn(a_+)$. Since the pseudo-complement is order-reversing, it follows that $\neg_+ pn(a_+) \leq_+ \neg_+ a_+$. By the property of the pseudo-complement, the other inequality $\neg_+ a_+ \leq_+ \neg_+ pn(a_+)$ holds iff $\neg_+ a_+ \wedge_+ pn(a_+) = 0_+$. Observe that $Id_{A_+} \leq_+ p \circ n$ (together with the requirement that both p and n preserve finite meets and the bounds) gives us $\neg_+ a_+ \wedge_+ pn(a_+) \leq_+ pn(\neg_+ a_+) \wedge_+ pn(a_+) = pn(\neg_+ a_+ \wedge_+ a_+) = pn(0_+) = 0_+$. Thus $\neg_+ a_+ = \neg_+ pn(a_+)$. Then $n(\neg_+ a_+)) = n(\neg_+ pn(a_+)) = \neg_- n(a_+)$, as claimed. □

Let $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$ and $\langle a_+, a_- \rangle, \langle b_+, b_- \rangle \in A$. Observe that the lattice order $\leq$ of $\mathbf{A}$ is given component-wise by:

$$\langle a_+, a_- \rangle \leq \langle b_+, b_- \rangle \quad \text{iff} \quad (a_+ \leq_+ b_+ \text{ and } b_- \leq_- a_-).$$

We shall write:

$$\langle a_+, a_- \rangle \preccurlyeq \langle b_+, b_- \rangle \quad \text{as a shorthand for} \quad \langle a_+, a_- \rangle \leq {\sim}\langle a_+, a_- \rangle \vee \langle b_+, b_- \rangle$$

$$\langle a_+, a_- \rangle \equiv \langle b_+, b_- \rangle \quad \text{for} \quad (\langle a_+, a_- \rangle \preccurlyeq \langle b_+, b_- \rangle \text{ and } \langle b_+, b_- \rangle \preccurlyeq \langle a_+, a_- \rangle).$$

Lemma 3.5. *Let $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$ be a WPQK twist-structure. For all elements $\langle a_+, a_- \rangle, \langle b_+, b_- \rangle \in A$, we have:*

(i) $\langle a_+, a_- \rangle \preccurlyeq \langle b_+, b_- \rangle$ *iff* $a_+ \leq_+ b_+$ *iff* $\langle a_+, a_- \rangle \wedge {\sim}\neg\langle a_+, a_- \rangle \leq \langle b_+, b_- \rangle \wedge {\sim}\neg\langle b_+, b_- \rangle$.

(ii) ${\sim}\langle b_+, b_- \rangle \preccurlyeq {\sim}\langle a_+, a_- \rangle$ *iff* $b_- \leq_- a_-$.

(iii) $\langle a_+, a_- \rangle \equiv \langle b_+, b_- \rangle$ *iff* $a_+ = b_+$.

(iv) $\langle a_+, a_- \rangle \leq \langle b_+, b_- \rangle$ *iff* $(\langle a_+, a_- \rangle \preccurlyeq \langle b_+, b_- \rangle$ *and* ${\sim}\langle b_+, b_- \rangle \preccurlyeq {\sim}\langle a_+, a_- \rangle)$.

(v) $\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$ *iff* $\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle \leq {\sim}\langle b_+, b_-\rangle$.

(vi) $\neg(\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle) = \langle 1_+, 0_-\rangle$ *iff* $\neg\neg\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$ *iff* $a_+ \wedge_+ b_+ = 0_+$.

(vii) $\langle a_+, a_-\rangle \wedge {\sim}\langle a_+, a_-\rangle = {\sim}{\sim}\langle a_+, a_-\rangle \wedge {\sim}\langle a_+, a_-\rangle$.

(viii) $\langle a_+, a_-\rangle \wedge {\sim}\langle a_+, a_-\rangle = \langle a_+, a_-\rangle \wedge \neg\langle a_+, a_-\rangle$.

(ix) ${\sim}\langle a_+, a_-\rangle \leq \neg\langle a_+, a_-\rangle$.

(x) $\langle a_+, a_-\rangle \wedge \neg\langle a_+, a_-\rangle \leq \langle b_+, b_-\rangle \vee \neg\langle b_+, b_-\rangle$.

(xi) $\neg(\langle a_+, a_-\rangle \vee \langle b_+, b_-\rangle) = \neg\langle a_+, a_-\rangle \wedge \neg\langle b_+, b_-\rangle$.

(xii) $\neg\neg\neg\langle a_+, a_-\rangle \leq \neg\langle a_+, a_-\rangle$.

(xiii) ${\sim}{\sim}\neg\langle a_+, a_-\rangle = \neg\langle a_+, a_-\rangle$.

(xiv) ${\sim}\neg\langle a_+, a_-\rangle \equiv {\sim}{\sim}\langle a_+, a_-\rangle$.

Proof. (i). Applying the component-wise definitions, we have $\langle a_+, a_-\rangle \preccurlyeq \langle b_+, b_-\rangle$ if and only if $a_+ \leq_+ p(a_-) \vee_+ b_+$ and $n(a_+) \wedge_- b_- \leq_- a_-$. Thus $a_+ = a_+ \wedge_+ (p(a_-) \vee_+ b_+)$. Observe that, using distributivity and the requirement $a_+ \wedge_+ p(a_-) = 0_+$, we have $a_+ = a_+ \wedge_+ (p(a_-) \vee_+ b_+) = (a_+ \wedge_+ p(a_-)) \vee_+ (a_+ \wedge_+ b_+) = 0_+ \vee_+ (a_+ \wedge_+ b_+) = a_+ \wedge_+ b_+$. Hence, $\langle a_+, a_-\rangle \preccurlyeq \langle b_+, b_-\rangle$ entails $a_+ \leq_+ b_+$. But also, conversely, $a_+ \leq_+ b_+$ entails $\langle a_+, a_-\rangle \preccurlyeq \langle b_+, b_-\rangle$. To see this, observe that, by monotonicity of n, from $a_+ \leq_+ b_+$ we get $n(a_+) \leq_+ n(b_+)$. Then $n(a_+) \wedge_- b_- \leq_- n(b_+) \wedge_- b_- = 0_-$ (Remark 3.2). This implies $n(a_+) \wedge_- b_- \leq_- a_-$, and so $\langle a_+, a_-\rangle \preccurlyeq \langle b_+, b_-\rangle$.
This settles the first equivalence. As to the second, let us compute: $\langle a_+, a_-\rangle \wedge {\sim}\neg\langle a_+, a_-\rangle = \langle a_+ \wedge_+ pn(a_+), a_- \vee_- n(\neg_+ a_+)\rangle = \langle a_+, n(\neg_+ a_+)\rangle$. The last passage is justified by the following reasoning. On the one hand, the equality $a_+ \wedge_+ pn(a_+) = a_+$ holds by the requirement $Id_{A_+} \leq_+ p \circ n$. On the other, using $n \circ p = Id_{A_-}$ and the requirement that n preserves finite joins, we have $a_- \vee_- n(\neg_+ a_+) = np(a_-) \vee_- n(\neg_+ a_+) = n(p(a_-) \vee_+ \neg_+ a_+)$. Observe that the requirement $a_+ \wedge_+ p(a_-) = 0_+$ implies, by the property of the pseudo-complement, $p(a_-) \leq_+ \neg_+ a_+$. Hence, $n(p(a_-) \vee_+ \neg_+ a_+) = n(\neg_+ a_+)$. Then $\langle a_+, a_-\rangle \wedge {\sim}\neg\langle a_+, a_-\rangle = \langle a_+, n(\neg_+ a_+)\rangle \leq \langle b_+, n(\neg_+ b_+)\rangle = \langle b_+, b_-\rangle \wedge {\sim}\neg\langle b_+, b_-\rangle$ obviously implies $a_+ \leq_+ b_+$. Also, conversely, $a_+ \leq_+ b_+$ implies $\neg_+ b_+ \leq_+ \neg_+ a_+$ (the pseudo-complement operation is order-reversing), which gives us $n(\neg_+ b_+) \leq_- n(\neg_+ a_+)$ because n is order-preserving. Hence we obtain $\langle a_+, n(\neg_+ a_+)\rangle \leq \langle b_+, n(\neg_+ b_+)\rangle$, as required.

(ii). By item (i) above, we have ${\sim}\langle b_+, b_-\rangle \preccurlyeq {\sim}\langle a_+, a_-\rangle$ iff $p(b_-) \leq_+ p(a_-)$. Then, applying n to both sides and recalling that $n \circ p = Id_{A_-}$, we have $bp(b_-) = b_- \leq_- a_- = np(a_-)$, as claimed.

(iii). Follows immediately from item (i) above.

(iv). Follows from items (i) and (ii) above.

(v). Observe that $\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$ component-wise means $a_+ \leq_+ \neg_+ b_+$ (i.e., by pseudo-complementation, $a_+ \wedge_+ b_+ = 0_+$) and $n(b_+) \leq_- a_-$, while $\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle \leq \sim\langle b_+, b_-\rangle$ means $a_+ \wedge_+ b_+ \leq_+ p(b_-)$ and $n(b_+) \leq_- a_- \vee_- b_-$. It is thus obvious that $\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$ entails $\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle \leq \sim\langle a_+, a_-\rangle$. Let us show that the converse implication holds as well. From $a_+ \wedge_+ b_+ \leq_+ p(b_-)$ we have $a_+ \wedge_+ b_+ \leq_+ b_+ \wedge_+ p(b_-) = 0_+$. From $n(b_+) \leq_- a_- \vee_- b_-$, using distributivity and Remark 3.2, we have $n(b_+) = n(b_+) \wedge_- (a_- \vee_- b_-) = (n(b_+) \wedge_- a_-) \vee_- (n(b_+) \wedge_- b_-) = (n(b_+) \wedge_- a_-) \vee_- 0_- = n(b_+) \wedge_- a_-$. Thus $n(b_+) \leq_- a_- \vee_- b_-$ is equivalent to $n(b_+) \leq_- a_-$, as required.

(vi). Consider the first and last conditions in the statement. Firstly, observe that $a_+ \wedge_+ b_+ = 0_+$ entails $n(a_+ \wedge_+ b_+) = n(0_+) = 0_-$ and $\neg_+(a_+ \wedge_+ b_+) = \neg_+(0_+) = 1_+$. Secondly, observe that $\neg(\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle) = \langle 1_+, 0_-\rangle$ iff $\langle \neg_+(a_+ \wedge_+ b_+), n(a_+ \wedge_+ b_+)\rangle = \langle 1_+, 0_-\rangle$ iff $\neg_+(a_+ \wedge_+ b_+) = 1_+$ and $n(a_+ \wedge_+ b_+) = 0_-$. Since $Id_{A_+} \leq_+ p \circ n$, from $n(a_+ \wedge_+ b_+) = 0_-$ we have $pn(a_+ \wedge_+ b_+) = p(0_-) = 0_+$ and so $a_+ \wedge_+ b_+ \leq 0_+ = pn(a_+ \wedge_+ b_+)$. Hence, $\neg(\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle) = \langle 1_+, 0_-\rangle$ iff $a_+ \wedge_+ b_+ = 0_+$. As to the second condition, we have $\neg\neg\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$ iff $\langle \neg_+\neg_+ a_+, n(\neg_+ a_+)\rangle \leq \langle \neg_+ b_+, n(b_+)\rangle$ iff $\neg_+\neg_+ a_+ \leq_+ \neg_+ b_+$ and $n(b_+) \leq_- n(\neg_+ a_+)$. Using the property of the pseudo-complement, from $\neg_+\neg_+ a_+ \leq_+ \neg_+ b_+$ we obtain $\neg_+\neg_+ a_+ \wedge_+ b_+ \leq_+ 0_+$. Since $a_+ \leq_+ \neg_+\neg_+ a_+$, we have $a_+ \wedge_+ b_+ \leq_+ 0_+ = \neg_+\neg_+ a_+ \wedge_+ b_+$. Thus $\neg\neg\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$ entails $a_+ \wedge_+ b_+ = 0_+$. Conversely, from $a_+ \wedge_+ b_+ = 0_+$ (again by the property of the pseudo-complement) we have $b_+ \leq_+ \neg_+ a_+$ and also, since $\neg_+$ is order-reversing, $\neg_+\neg_+ a_+ \leq_+ b_+$. Also, from $b_+ \leq_+ \neg_+ a_+$, using that n is monotone, we have $n(b_+) \leq_- n(\neg_+ a_+)$. Thus $a_+ \wedge_+ b_+ = 0_+$ entails $\neg\neg\langle a_+, a_-\rangle \leq \neg\langle b_+, b_-\rangle$, which concludes our proof.

(vii). Since $\sim\sim\langle a_+, a_-\rangle = \langle pn(a_+), a_-\rangle$, the identity trivially holds for the second components. The first components are $a_+ \wedge_+ p(a_-)$ on the one hand and $pn(a_+) \wedge_+ p(a_-)$ on the other. Recalling Remark 3.2, we have $pn(a_+) \wedge_+ p(a_-) = p(n(a_+) \wedge_+ a_-) = p(0_-) = 0_+ = a_+ \wedge_+ p(a_-)$, as required.

(viii). Since $\sim\langle a_+, a_-\rangle = \langle p(a_-), n(a_+)\rangle$ and $\neg\langle a_+, a_-\rangle = \langle \neg_+ a_+, n(a_+)\rangle$, the identity trivially holds for the second components. The first give us, respectively, $a_+ \wedge_+ p(a_-) = 0_+$ and (using the property of the pseudo-complement) $a_+ \wedge_+ \neg_+ a_+ = 0_+$.

(ix). In this case too only the first components matter. These are $p(a_-)$ and $\neg_+ a_+$. By the property of the pseudo-complement, $p(a_-) \leq_+ \neg_+ a_+$ if and only if $p(a_-) \wedge_+ a_+ \leq_+ 0_+$, which holds by Definition 3.1.

(x). Let us calculate $\langle a_+, a_-\rangle \wedge \neg\langle a_+, a_-\rangle = \langle a_+ \wedge_+ \neg_+ a_+, a_- \vee_- n(a_+)\rangle$ and $\langle b_+, b_-\rangle \vee \neg\langle b_+, b_-\rangle = \langle b_+ \vee_+ \neg_+ b_+, b_- \wedge_- n(b_+)\rangle$. The result then follows from the

observation that $a_+ \wedge_+ \neg_+ a_+ = 0_+$ by (P) and $b_- \wedge_- n(b_+) = 0_-$ by Remark 3.2.

(xi). Let us calculate $\neg(\langle a_+, a_-\rangle \vee \langle b_+, b_-\rangle) = \langle \neg_+(a_+ \vee_+ b_+), n(a_+ \vee_+ b_+)\rangle$. and $\neg\langle a_+, a_-\rangle \wedge \neg\langle b_+, b_-\rangle = \langle \neg_+ a_+ \wedge_+ \neg_+ b_+, n(a_+) \vee_- n(b_+)\rangle$. Observe that the identity $\neg_+(a_+ \vee_+ b_+) = \neg_+ a_+ \wedge_+ \neg_+ b_+$ holds on any p-lattice [24], and $n(a_+ \vee_+ b_+) = n(a_+) \vee_- n(b_+)$ holds by item (i) of Definition 3.1. Thus the desired result follows.

(xii). Let us compute

$$\neg\neg\neg\langle a_+, a_-\rangle = \langle \neg_+\neg_+\neg_+ a_+, n(\neg_+\neg_+ a_+)\rangle = \langle \neg_+ a_+, n(\neg_+\neg_+ a_+)\rangle$$

and $\neg\langle a_+, a_-\rangle = \langle \neg_+ a_+, n(a_+)\rangle$. Thus, only the second components matter. Observe that $a_+ \leq_+ \neg_+\neg_+ a_+$ always holds on a p-lattice, hence so does $n(a_+) \leq_- n(\neg_+\neg_+ a_+)$. Thus, $\neg\neg\neg\langle a_+, a_-\rangle \leq \neg\langle a_+, a_-\rangle$.

(xiii). Let us compute:

$$\sim\sim\neg\langle a_+, a_-\rangle = \langle pn(\neg_+ a_+), np(n(a_+))\rangle = \langle pn(\neg_+ a_+), n(a_+)\rangle.$$

Since $\neg\langle a_+, a_-\rangle = \langle \neg_+ a_+, n(a_+)\rangle$, it suffices to show $pn(\neg_+ a_+) = \neg_+ a_+$. Since $Id_{A_+} \leq_+ p \circ n$, it suffices to show $pn(\neg_+ a_+) \leq_+ \neg_+ a_+$. By the property of the pseudo-complement, we have $pn(\neg_+ a_+) \leq_+ \neg_+ a_+$ iff $a_+ \wedge_+ pn(\neg_+ a_+) \leq_+ 0_+$. Observe that, using $Id_{A_+} \leq_+ p \circ n$ and that p and n preserve finite meets and the bottom element, we have $a_+ \wedge_+ pn(\neg_+ a_+) \leq_+ pn(a_+) \wedge_+ pn(\neg_+ a_+) = pn(a_+ \wedge_+ \neg_+ a_+) = pn(0_+) = 0_+$. Thus the result follows.

(xiv). Let us compute $\sim\neg\langle a_+, a_-\rangle = \sim\langle \neg_+ a_+, n(a_+)\rangle = \langle pn(a_+), n(\neg_+ a_+)\rangle$ and $\sim\sim\langle a_+, a_-\rangle = \langle pn(a_+), np(a_-)\rangle = \langle pn(a_+), a_-\rangle$. Then the result follows from item (iii) above.

□

Remark 3.6. In the context of Kleene algebras, the two properties stated in items (v) and (vi) of Lemma 3.5 define, in the terminology of A. Sendlewski [26, p. 22], the class of *Kleene algebras with a weak pseudo-complementation* (alias *wp*-Kleene algebras; see Definition 4.14). This is the reason behind our choice of the term 'weakly pseudo-complemented' for the above-defined twist-structures (and for the corresponding class of abstract algebras, that are going to be introduced in Definition 4.2).

4 Abstractly: Weakly Pseudo-Complemented Quasi-Kleene Algebras

Let **A** be a quasi-Kleene algebra (Definition 2.4). In keeping with the notation of the previous section, we write:

$$a \preccurlyeq b \quad \text{as a shorthand for} \quad a \leq \sim a \vee b$$

$$a \equiv b \quad \text{as a shorthand for} \quad (a \preccurlyeq b \text{ and } b \preccurlyeq a).$$

Remark 4.1. Observe that (the binary relation naturally associated to) $\preccurlyeq$ is reflexive (as well transitive: see below) on every quasi-Kleene algebra $\mathbf{A}$. It is also obvious that $a \leq b$ implies $a \preccurlyeq b$, for all $a, b \in A$. Thus, in particular, for all $a \in A$, we have $0 \preccurlyeq a \preccurlyeq 1$.

Definition 4.2. A *weakly pseudo-complemented quasi-Kleene algebra* (a WPQK-algebra, for short) is an algebra $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ of type $\langle 2, 2, 1, 1, 0, 0\rangle$ such that:

(i) $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ is a quasi-Kleene algebra (Definition 2.4).

(ii) for all $a, b, c, d \in A$,

(1) $a \preccurlyeq \neg b$ iff $a \wedge b \preccurlyeq 0$ (WP)

(2) $\sim \neg a \equiv \sim \sim a$.

By definition, WPQK-algebras form a quasi-variety. We will see that condition ii.1, the only proper quasi-equational one, can equivalently be replaced by three equations (Proposition 4.12, Corollary 4.13). Hence, WPQK-algebras are in fact a variety.

Our prime examples of WPQK-algebras are obviously the reducts of Nelson and quasi-Nelson algebras (cf. Proposition 4.4). It is also easy to check (cf. [24, Corollary 2.8]) that every p-lattice $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ forms a WPQK-algebra if we let $\sim x := \neg x$ (see Proposition 9.3). We will later introduce a simple construction that allows one to produce other non-trivial WPQK-algebras (Example 6.4). As we are going to show (Proposition 4.15), Sendlewski's wp-Kleene algebras (Definition 4.14) are precisely the subvariety of WPQK-algebras that satisfies the involutive identity $\sim \sim x \approx x$.

One may wonder whether the reduct $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ of a WPQK-algebra is also a quasi-Kleene algebra. This is not the case, because for instance the analogue of (QK2) for $\neg$ need not be satisfied (cf. Proposition 9.3). In fact, (SD4) and (SD5) may also fail, suggesting that $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ may not even be a semi-De Morgan algebra (cf. Proposition 9.7).

Proposition 4.3. *Every WPQK twist-structure* $\mathbf{A}$ *(Definition 3.1) is a WPQK-algebra (Definition 4.2).*

Proof. For the quasi-Kleene algebra conditions, see [19, Proposition 4.7]. Let us check item (ii) of Definition 4.2. Let $\langle a_+, a_-\rangle, \langle b_+, b_-\rangle \in A$. For ii.1, observe

that, by Lemma 3.5.i, we have $\langle a_+, a_-\rangle \preccurlyeq \neg\langle b_+, b_-\rangle$ iff $a_+ \leq_+ \neg_+ b_+$. By pseudo-complementation, $a_+ \leq_+ \neg_+ b_+$ iff $a_+ \wedge_+ b_+ = 0_+$. By Lemma 3.5.i again, we have $a_+ \wedge_+ b_+ = 0_+$ iff $\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle \preccurlyeq \langle 0_+, 1_-\rangle$. For ii.2, we calculate $\sim\neg\langle a_+, a_-\rangle = \sim\langle \neg_+ a_+, n(a_+)\rangle = \langle pn(a_+), n(\neg_+ a_+)\rangle$ and $\sim\sim a = \langle pn(a_+), np(a_-)\rangle$. Thus the result follows from Lemma 3.5.iii. □

The following proposition, like the preceding one, is a matter of routine checking (using the twist-structure representation of quasi-Nelson algebras [22, 23]).

Proposition 4.4. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \to, \sim, 0, 1\rangle$ *be a quasi-Nelson algebra. Upon defining* $\neg x := x \to 0$*, the structure* $\langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *is a WPQK-algebra.*

The following proposition is a direct consequence of [19, Lemma 3.3].

Proposition 4.5. *Let* $\mathbf{A}$ *be a WPQK-algebra and* $a, b, c, d \in A$*.*

(i) If $a \preccurlyeq b$ *and* $b \preccurlyeq c$*, then* $a \preccurlyeq c$*.*

(ii) If $a \preccurlyeq b$ *and* $c \preccurlyeq d$*, then* $a \vee c \preccurlyeq b \vee d$*.*

(iii) If $a \preccurlyeq b$ *and* $c \preccurlyeq d$*, then* $a \wedge c \preccurlyeq b \wedge d$*.*

Proposition 4.6. *Let* $\mathbf{A}$ *be a WPQK-algebra and* $a, b \in A$*.*

(i) If $a \equiv b$*, then* $\neg a \equiv \neg b$*.*

(ii) $a \preccurlyeq b$ *iff* $a \equiv a \wedge b$*.*

(iii) $a \leq b$ *iff* ($a \preccurlyeq b$ *and* $\sim b \preccurlyeq \sim a$)*.*

Proof. (i). Assume $a \equiv b$. Then, by Proposition 4.5.iii, $\neg a \wedge a \equiv \neg a \wedge b$. By [19, Prop. 3.15.ix] we have $\neg a \wedge a \preccurlyeq 0$. Thus (by Proposition 4.5.i) we obtain $\neg a \wedge b \preccurlyeq 0$. Applying Definition 4.2.ii.1, we then obtain $\neg a \preccurlyeq \neg b$. A similar reasoning allows us to obtain $\neg b \preccurlyeq \neg a$, as required.

(ii). Assume $a \preccurlyeq b$, and observe that (since $a \wedge b \leq a$ holds generally), by Remark 4.1 one always has $a \wedge b \preccurlyeq a$. By Proposition 4.6.iii, from $a \preccurlyeq b$ we can obtain $a \wedge a = a \preccurlyeq a \wedge b$. Hence, $a \equiv a \wedge b$, as required.
Conversely, assume $a \equiv a \wedge b$. Thus, in particular $a \preccurlyeq a \wedge b$. Then, using $a \wedge b \preccurlyeq b$ and Proposition 4.6.i, we have $a \preccurlyeq b$, as required.

(iii). Since $\mathbf{A}$ has a quasi-Kleene algebra reduct, the result follows from [19, Prop. 3.15.ii and Prop. 3.15.v]. □

Propositions 4.5 and 4.6 together establish the following important fact:

Corollary 4.7. *The relation $\equiv$ is a congruence of the $\{\sim\}$-free reduct of every WPQK-algebra.*

Proposition 4.8. *For every WPQK-algebra $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$, the quotient algebra $\mathbf{A}_+ = \langle A/\equiv; \wedge, \vee, \neg, 0, 1\rangle$ is a p-lattice.*

Proof. It is clear that the $\{\neg\}$-free reduct of $\mathbf{A}_+$ is a bounded distributive lattice. It remains to prove that the pseudo-complement law holds. Denoting by $\leq_+$ the lattice order of $\mathbf{A}_+$, assume $[a] \leq_+ \neg[b]$. This means that $[a] \wedge_+ \neg[b] = [a \wedge \neg b] = [a]$. From $a \wedge \neg b \equiv a$, using Proposition 4.5.iii, we have $a \wedge \neg b \wedge b \equiv a \wedge b$. Observe that, by Definition 4.2.ii.1, from $\neg b \preccurlyeq \neg b$ we have $\neg b \wedge b \preccurlyeq 0$. From this, using Proposition 4.5.iii, we get $a \wedge \neg b \wedge b \preccurlyeq a \wedge 0 = 0$. Thus, using the assumption $a \wedge b \preccurlyeq a \wedge \neg b \wedge b$ (and Proposition 4.5.i), we obtain $a \wedge b \preccurlyeq 0$. Since $0 \preccurlyeq a \wedge b$ holds generally, we conclude $a \wedge b \equiv 0$. Thus $0_+ = [a \wedge b] = [a] \wedge_+ [b]$, as required.
Conversely, assuming $[a] \wedge_+ [b] = 0_+$, we have $a \wedge b \equiv 0$, and in particular $a \wedge b \preccurlyeq 0$. Using by Definition 4.2.ii.1, we then have $a \preccurlyeq \neg b$. By Proposition 4.6.ii, this means $a \equiv a \wedge \neg b$ and so $[a] = [a \wedge \neg b] = [a] \wedge_+ \neg[b]$. Hence, $[a] \leq_+ \neg[b]$, as required. □

Let $\mathbf{A}$ be a WPQK-algebra. Consider the set $A_- := \{[\sim a] : a \in A\} \subseteq A_+$. We endow A_- with operations as follows. For all $a, b \in A$, let

$$[\sim a] \wedge_- [\sim b] := [\sim(a \vee b)] = [\sim a \wedge \sim b] = [\sim a] \wedge_+ [\sim b]$$

$$[\sim a] \vee_- [\sim b] := [\sim(a \wedge b)]$$

$$0_- := [\sim 1] = [0] = 0_+$$

$$1_- := [\sim 0] = [1] = 1_+.$$

The above equality $[\sim(a \vee b)] = [\sim a \wedge \sim b]$ holds because of the semi-De Morgan law (SD3); also note that A_- is obviously closed under the above-defined operations. Recalling Proposition 3.4, we can also define a pseudo-complement operation on A_- by

$$\neg_-[\sim a] := [\sim \sim \neg \sim a] = [\neg \sim a] = \neg_+[\sim a] \qquad \text{(cf. Proposition 4.11.xi).}$$

Proposition 4.9. *For every WPQK-algebra $\mathbf{A}$, we have that the algebra $\mathbf{A}_- = \langle A_-, \wedge_-, \vee_-, \neg_-, 0_-, 1_-\rangle$ is a p-lattice.*

Proof. It is clear that the $\vee_-$-free reduct of $\mathbf{A}_-$ is a bounded sub-meet-semilattice of $\mathbf{A}_+$. Let us see that $\vee_-$ is a join operation for $\wedge_-$. Observe that $\vee_-$ inherits idempotency, associativity and commutativity from $\wedge$. It remains to verify the

absorption law, which we can do as follows: $[\sim a] \vee_- ([\sim a] \wedge_- [\sim b]) = [\sim a] \vee_- [\sim(a \vee b)] = [\sim(a \wedge (a \vee b))] = [\sim a]$ and $[\sim a] \wedge_- ([\sim a] \vee_- [\sim b]) = [\sim a] \wedge_- [\sim(a \wedge b)] = [\sim(a \vee (a \wedge b))] = [\sim a]$. Let us check distributivity. Let $a, b, c \in A$. We have:

$$\begin{aligned}
[\sim a] \wedge_- ([\sim b] \vee_- [\sim c]) &= [\sim a] \wedge_- [\sim(b \wedge c)] \\
&= [\sim a \wedge \sim(b \wedge c)] \\
&= [\sim(a \vee (b \wedge c)] && \text{(SD3)} \\
&= [\sim((a \vee b) \wedge (a \vee c))] && \text{(distributivity)} \\
&= [\sim(a \vee b)] \vee_- [\sim(a \vee c)] \\
&= [\sim a \wedge \sim b] \vee_- [\sim a \wedge \sim c] && \text{(SD3)} \\
&= ([\sim a] \wedge_- [\sim b]) \vee_- ([\sim a] \wedge_- [\sim c]).
\end{aligned}$$

Finally, that $\neg_-$ is the pseudo-complement in A_- follows from Proposition 4.8 together with our earlier observation that $\neg_-[\sim a] = \neg_+[\sim a]$ for all $a \in A$. □

We proceed to define maps $p\colon A_- \to A_+$ and $n\colon A_+ \to A_-$ between $\mathbf{A}_+$ and $\mathbf{A}_-$ as follows. Let p be the identity map on A_-, and let $n[a] := [\sim\sim a]$ for all $a \in A$. Obviously p preserves the bounds and meets, as required by Definition 3.1.

Let us check that the map n is a bounded lattice homomorphism. It is easy to see that the bounds are preserved. Also, using the semi-De Morgan identity $\sim\sim(x \wedge y) = \sim\sim x \wedge \sim\sim y$, we have $n([a] \wedge_+ [b_+]) = n[a \wedge b] = [\sim\sim(a \wedge b)] = [\sim\sim a \wedge \sim\sim b] = [\sim\sim a] \wedge_- [\sim\sim b] = n[a] \wedge_- n[b]$. Using $\sim(x \vee y) = \sim x \wedge \sim y$, we have $n([a] \vee_+ [b_+]) = n[a \vee b] = [\sim\sim(a \vee b)] = [\sim(\sim a \wedge \sim b)] = [\sim\sim a] \vee_- [\sim\sim b] = n[a] \vee_- n[b]$. Let us verify that $n \circ p = Id_{A_-}$ and $Id_{A_+} \leq_+ p \circ n$. Using $\sim x \approx \sim\sim\sim x$, we have $np[\sim a] = n[\sim a] = [\sim\sim\sim a] = [\sim a]$. Thus $n \circ p = Id_{A_-}$. Observe that the identity of quasi-Kleene algebras $x \leq \sim\sim x$ entais $[a] = [a \wedge \sim\sim a] = [a] \wedge_+ [\sim\sim a]$ and so $[a] \leq_+ [\sim\sim a]$. Hence we have $[a] \leq_+ [\sim\sim a] = p[\sim\sim a] = pn[a]$, which shows that $Id_{A_+} \leq_+ p \circ n$.

Theorem 4.10. *Every WPQK-algebra* $\mathbf{A}$ *is isomorphic to a WPQK twist-structure over* $\mathbf{A}_+ \bowtie \mathbf{A}_-$ *through the map* $\iota\colon A \to A_+ \times A_-$ *given by* $\iota(a) := \langle [a], [\sim a] \rangle$ *for all* $a \in A$.

Proof. Injectivity of ι follows from item (iii) of Proposition 4.6. It is easy to check that ι preserves the $\sim$ negation. Let us see the case of the other operations. For

$a, b \in A$, we have:

$$\begin{aligned}\iota(a \wedge b) &= \langle [a \wedge b], [\sim(a \wedge b)] \rangle \\ &= \langle [a] \wedge_+ [b], [\sim a] \vee_- [\sim b] \rangle \\ &= \langle [a], [\sim a] \rangle \wedge \langle [b], [\sim b] \rangle \\ &= \iota(a) \wedge \iota(b).\end{aligned}$$

$$\begin{aligned}\iota(a \vee b) &= \langle [a \vee b], [\sim(a \vee b)] \rangle \\ &= \langle [a] \vee_+ [b], [\sim(a \vee b)] \rangle \\ &= \langle [a] \vee_+ [b], [\sim a \wedge \sim b] \rangle && \text{(SD3)} \\ &= \langle [a] \vee_+ [b], [\sim a] \wedge_- [\sim b] \rangle \\ &= \langle [a], [\sim a] \rangle \vee \langle [b], [\sim b] \rangle \\ &= \iota(a) \vee \iota(b).\end{aligned}$$

$$\begin{aligned}\iota(\neg a) &= \langle [\neg a], [\sim \neg a] \rangle \\ &= \langle [\neg a], [\sim \sim a] \rangle && \text{(Def. 4.2.ii.2)} \\ &= \langle \neg_+ [a], n[a] \rangle \\ &= \neg \iota(a).\end{aligned}$$

□

Thanks to Theorem 4.10, we can identify each WPQK-algebra $\mathbf{A}$ with a WPQK twist-structure $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$. We will often use this observation, whenever convenient, in subsequent proofs. To begin with, we have that all identities proved for WPQK twist-structures hold on every WPQK-algebra. This allows us to rephrase Lemma 3.5 as follows.

Proposition 4.11. *Let* $\mathbf{A}$ *be a WPQK-algebra and* $a, b \in A$.

(i) $a \preccurlyeq b$ *iff* $a \wedge \sim \neg a \leq b \wedge \sim \neg b$.

(ii) $a \leq b$ *iff* $(a \preccurlyeq b$ *and* $\sim b \preccurlyeq \sim a)$.

(iii) $a \leq \neg b$ *iff* $a \wedge b \leq \sim b$.

(iv) $\neg(a \wedge b) = 1$ *iff* $\neg\neg a \leq \neg b$.

(v) $a \wedge \sim a = \sim \sim a \wedge \sim a$.

(vi) $a \wedge {\sim} a = a \wedge \neg a$.

(vii) ${\sim} a \leq \neg a$.

(viii) $a \wedge \neg a \leq b \vee \neg b$.

(ix) $\neg(a \vee b) = \neg a \wedge \neg b$.

(x) $\neg\neg\neg a \leq \neg a$.

(xi) ${\sim}{\sim}\neg a = \neg a$.

(xii) ${\sim}\neg a \equiv {\sim}{\sim} a$.

The following result is an analogue of [2, Theorem 1, p. 155].

Proposition 4.12. *Item ii.1 in Definition 4.2 can equivalently be replaced by the following conditions: for all $a, b \in A$,*

(i) $\neg 1 = 0$,

(ii) $\neg(a \wedge {\sim} a) = 1$,

(iii) $a \wedge \neg(a \wedge b) \equiv a \wedge \neg b$.

Proof. We check that (i), (ii) and (iii) are satisfied by every WPQK twist-structure $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$. Since $\neg 1 \approx 0$ holds on any p-lattice. we easily have $\neg\langle 1_+, 0_+\rangle = \langle \neg_+ 1_+, n(1_+)\rangle = \langle 0_+, 1_+\rangle$. Regarding (ii), we have $\neg(\langle a_+, a_-\rangle \wedge {\sim}\langle a_+, a_-\rangle) = \langle \neg_+(a_+ \wedge_+ p(a_-)), n(a_+ \wedge_+ p(a_-))\rangle = \langle \neg_+ 0_+, n(0_+)\rangle = \langle 1_+, 0_-\rangle$. As to (iii), only the first components matter, and they are, respectively, $a_+ \wedge_+ \neg_+(a_+ \wedge b_+)$ and $a_+ \wedge \neg_+ b_+$. We know from [2, Theorem 1, p. 155], the identity $x \wedge \neg(x \wedge y) \approx x \wedge \neg y$ holds on every pseudo-complemented distributive lattice, hence the required result follows.

Conversely, assume (i), (ii) and (iii) hold. Observe that, since 0 is the bottom element, (ii) gives us, in particular, $\neg 0 = \neg(0 \wedge {\sim} 0) = 1$. Using this we can prove that $a \wedge \neg a \equiv 0$ for all $a \in A$. Indeed, using $\neg 0 = 1$ and that 1 is the top element, we have $a = a \wedge 1 = a \wedge \neg 0$, so $a \wedge \neg a = a \wedge \neg(a \wedge \neg 0)$, which entails $a \wedge \neg a \equiv a \wedge \neg(a \wedge \neg 0)$. By (iii) we have $a \wedge \neg(a \wedge \neg 0) \equiv a \wedge \neg\neg 0$ and, using also (i), we have $a \wedge \neg\neg 0 = a \wedge \neg 1 = a \wedge 0 = 0$. Thus $a \wedge \neg\neg 0 \equiv 0$ and, using the transitivity of $\equiv$ (Corollary 4.7), we obtain $a \wedge \neg a \equiv 0$, as claimed. Now, assume $a \preccurlyeq \neg b$. Using Proposition 4.5.iii, we have $a \wedge b \preccurlyeq \neg b \wedge b \equiv 0$. Thus, by transitivity of $\preccurlyeq$ (item (i) of Proposition 4.5), we have $a \wedge b \preccurlyeq 0$. Conversely, assume $a \wedge b \preccurlyeq 0$. By definition, this means $a \wedge b \leq {\sim}(a \wedge b) \vee 0 = {\sim}(a \wedge b)$. Then we can use (ii) to

obtain $\neg((a \wedge b) \wedge \sim(a \wedge b)) = \neg(a \wedge b) = 1$. Thus $a \wedge \neg(a \wedge b) = a \wedge 1 = a$, which entails $a \wedge \neg(a \wedge b) \equiv a$. Applying (iii) and the transitivity of $\equiv$, we have $a \equiv a \wedge \neg b$. Thus, by Proposition 4.6.ii, we conclude $a \preccurlyeq \neg b$, as required. □

Corollary 4.13. *The class of WPQK-algebras is a variety.*

Another application of Theorem 4.10 is the possibility to verify rather easily that Sendlewski's wp-Kleene algebras (cf. Remark 3.6) are precisely the subvariety of WPQK-algebras obtained by adding the involutive identity.

Definition 4.14 ([26], p. 20)**.** A *quasi weakly pseudo-complemented Kleene algebra (qwp-Kleene algebra)* is an algebra $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ of type $\langle 2, 2, 1, 1, 0, 0\rangle$ such that $\mathbf{A} = \langle A; \wedge, \vee, \sim, 0, 1\rangle$ is Kleene algebra (Definition 2.4) with order $\leq$ and the following condition is satisfied: for all $a, b \in A$,

$$a \leq \neg b \quad \text{iff} \quad a \wedge b \leq \sim b.$$

A *qwp*-Kleene algebra is a *Kleene algebra with a weak pseudo-complementation (wp-Kleene algebra)* if the following additional condition is satisfied: for all $a, b \in A$,

$$\neg(a \wedge b) = 1 \quad \text{iff} \quad \neg\neg a \leq \neg b \quad (\text{iff} \quad \neg\neg b \leq \neg a).$$

Proposition 4.15. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be an algebra of type* $\langle 2, 2, 1, 1, 0, 0\rangle$*. The following conditions are equivalent:*

(i) $\mathbf{A}$ *is an involutive WPQK-algebra.*

(ii) $\mathbf{A}$ *is a wp-Kleene algebra.*

Proof. Let $\mathbf{A}$ be an involutive WPQK-algebra. Then the reduct $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ is a Kleene algebra. Moreover, by items (v) and (vi) of Lemma 3.5 (v) and (vi), $\mathbf{A}$ satisfies the two conditions in Definition 4.14. Hence, $\mathbf{A}$ is a wp-Kleene algebra.

Conversely, assume $\mathbf{A}$ is a wp-Kleene algebra. Then the reduct $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ is a Kleene algebra, and every Kleene algebra is a quasi-Kleene algebra [19]. We proceed to verify item (ii) of Definition 4.2.

ii.1. Let $a, b \in A$. Assume $a \preccurlyeq \neg b$, i.e. $a \leq \sim a \vee \neg b$. From this, using the properties of the De Morgan negation, we have $\sim(\sim a \vee \neg b) = \sim\sim a \wedge \sim\neg b = a \wedge \sim\neg b \leq \sim a$. Since $\sim\neg b \leq b$ [26, Lemma 2.1.iii], we also have $a \wedge \sim\neg b \leq a \wedge b \leq \sim a$. Since $a \wedge b \leq a$ entails $\sim a \leq \sim(a \wedge b)$, we obtain $a \wedge b \leq \sim a \leq \sim(a \wedge b) = \sim(a \wedge b) \vee 0$, i.e. $a \wedge b \preccurlyeq 0$, as required.

Now assume $a \wedge b \preccurlyeq 0$, that is, $a \wedge b \leq \sim(a \wedge b)$. Then, by [26, Lemma 2.1.v], we have $\neg(a \wedge b) = 1$. By the properties of the weak pseudo-complement (Definition 4.14),

we have $\neg(a \wedge b) = 1$ iff $\neg\neg b \leq \neg a$ iff $\neg\neg b \wedge a \leq \sim a$. Using the properties of the De Morgan negation, we have $\sim\sim a = a \leq \sim(\neg\neg b \wedge a) = \sim\neg\neg b \vee \sim a$. Since $\sim\neg\neg b \leq \neg b$ [26, Lemma 2.1.iii], we also have $\sim\neg\neg b \vee \sim a \leq \neg b \vee \sim a$. Thus $a \leq \neg b \vee \sim a$, i.e. $a \preccurlyeq \neg b$, as required.

ii.2. By [26, Lemma 2.1.iii], we have $\sim\neg a \leq a$ for all $a \in A$, which (by the lattice properties) implies $\sim\neg a \leq \sim\sim\neg a \vee a$, that is, $\sim\neg a \preccurlyeq a$. Since $a = \sim\sim a$ (by the involutive identity for De Morgan negation), we obtain $\sim\neg a \preccurlyeq \sim\sim a$. To show $\sim\sim a \preccurlyeq \sim\neg a$ (i.e. $\sim\sim a \leq \sim\sim\sim a \vee \sim\neg a$), we reason as follows. By [26, Lemma 2.1.i] we have $a \wedge \neg a = \sim\sim a \wedge \neg a \leq \sim a$. Then, using De Morgan's laws, we obtain $\sim\sim a \leq \sim(\sim\sim a \wedge \neg a) = \sim\sim\sim a \vee \sim\neg a$, as required. □

Proposition 4.15, together with our earlier observation that p-lattices are also examples of WPQK-algebras, suggests the following considerations.

Let us denote by p-Lat the class of all p-lattices, by WPQK the class of WPQK-algebras and by wp-K the class of wp-Kleene algebras. As we will show, the intersection p-$\mathsf{Lat} \cap wp$-K is the class of Boolean algebras (Proposition 9.13). Regarding the union, we obviously have p-$\mathsf{Lat} \cup wp$-$\mathsf{K} \subseteq \mathsf{WPQK}$. Since (by Corollary 4.13) the class WPQK is closed (*inter alia*) under direct products, taking for instance $\mathbf{A}_1 \in p$-Lat and $\mathbf{A}_2 \in wp$-K (such that neither $\mathbf{A}_1$ nor $\mathbf{A}_2$ is a Boolean algebra), we can obtain a WPQK-algebra $\mathbf{A}_2 \times \mathbf{A}_2$ that is interesting in the sense that (as can be easily checked) $\mathbf{A}_1 \times \mathbf{A}_2$ is neither a p-lattice nor a wp-Kleene algebra. We will describe another simple method for producing non-trivial examples of WPQK-algebras in Example 6.4.

Denoting by $\mathbb{V}(\mathsf{C})$ the variety generated by the class C, by Corollary 4.13 we also have $\mathbb{V}(p\text{-}\mathsf{Lat} \cup wp\text{-}\mathsf{K}) \subseteq \mathsf{WPQK}$. This inclusion is strict, as the following reasoning shows (cf. our Footnote 2 on the corresponding problem regarding Heyting, Nelson and quasi-Nelson algebras/logic). Since we are in a congruence-distributive setting, we can invoke a classic result of Jónsson [11, Lemma 4.1] to conclude that the subdirectly irreducible algebras in $\mathbb{V}(p\text{-}\mathsf{Lat} \cup wp\text{-}\mathsf{K})$ belong to p-$\mathsf{Lat} \cup wp$-K. However, the WPQK-algebra $\mathbf{A}$ shown in Figure 1 is a counterexample to this: $\mathbf{A}$ is subdirectly irreducible (see Figure 2) and it can be easily checked that $\mathbf{A} \notin p\text{-}\mathsf{Lat} \cup wp\text{-}\mathsf{K}$.

5 WPQK vs. Quasi-Nelson Algebras

As observed earlier (Proposition 4.4), every quasi-Nelson algebra has a WPQK-algebra reduct. We now proceed to check that, indeed, WPQK-algebras are precisely the $\{\wedge, \vee, \sim, \neg, 0, 1\}$-subreducts of quasi-Nelson algebras. Let us begin by observing that there are WPQK-algebras which are not the reduct of any quasi-Nelson algebra.

Example 5.1. Let $\mathbf{L} = \langle L; \wedge, \vee, \neg, \bot, \top \rangle$ be the algebra defined as follows. $L = (\mathbb{N} \times \mathbb{N}) \cup \{\bot, \top\}$, where $\mathbb{N}$ denotes the set of natural numbers. The order $\leq$ on $\mathbb{N} \times \mathbb{N}$ is the direct product of the usual order on $\mathbb{N}$, and we set $\bot < \langle m, n \rangle < \top$ for all $\langle m, n \rangle \in \mathbb{N} \times \mathbb{N}$. Upon defining $\neg\bot = \top$ and $\neg\langle m, n \rangle = \neg\top = \bot$ for all $\langle m, n \rangle \in \mathbb{N} \times \mathbb{N}$, we have that $\mathbf{L}$ is a p-lattice. However, $\mathbf{A}$ cannot be endowed with a Heyting implication. Indeed, a Heyting implication $\rightarrow$ would have to satisfy, for example,

$$\langle 1, 0 \rangle \rightarrow \langle 0, 1 \rangle = \max\{\langle m, n \rangle \in L : \langle m, n \rangle \wedge \langle 1, 0 \rangle \leq \langle 0, 1 \rangle\}.$$

But

$$\{\langle m, n \rangle \in A : \langle m, n \rangle \wedge \langle 1, 0 \rangle \leq \langle 0, 1 \rangle\} = \{\langle 0, n \rangle : n \in \mathbb{N}\},$$

and this set does not have a maximum. Now, consider the (involutive) WPQK twist-structure $\mathbf{A} \leq \mathbf{L} \bowtie \mathbf{L}$ obtained by letting $n = p = Id_L$ and

$$A := \{\langle a, b \rangle \in L \times L : a \wedge b = \bot\}.$$

If $\mathbf{A}$ were the reduct of a quasi-Nelson algebra (in which case, indeed, $\mathbf{A}$ would be the reduct of a Nelson algebra), then $\mathbf{A}_+ = \langle A_+; \wedge_+, \vee_+, \rightarrow_+, 0_+, 1_+ \rangle$ would be a Heyting algebra such that $\langle A_+; \wedge_+, \vee_+, 0_+, 1_+ \rangle \cong \langle L; \wedge, \vee, \bot, \top \rangle$. This is impossible, because we have seen that on the lattice $\langle L; \wedge, \vee, \bot, \top \rangle$ one cannot define a Heyting implication.

The preceding example shows that there are WPQK-algebras that cannot be endowed with a quasi-Nelson implication. However, we are going to see that every WPQK-algebra can be embedded into a quasi-Nelson algebra. To do so, viewing a WPQK-algebra as a twist-structure $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$, we will begin by finding embeddings of $\mathbf{A}_+$ and $\mathbf{A}_-$ into corresponding Heyting algebras $\mathbf{H}_+, \mathbf{H}_-$, and will then show that the maps $n\colon A_+ \rightarrow A_-$ and $p\colon A_- \rightarrow A_+$ can be lifted to $\mathbf{H}_+$ and $\mathbf{H}_-$.

For constructing $\mathbf{H}_+, \mathbf{H}_-$ we will borrow a few results from the theory of canonical extensions. Recall that the *canonical extension* of a bounded distributive lattice $\mathbf{L}$ is a complete and completely distributive lattice into which $\mathbf{L}$ embeds. Every (bounded distributive) lattice $\mathbf{L}$ has a uniquely determined canonical extension, denoted $\mathbf{L}^\sigma$ (see e.g. [9] for further details and proofs). To simplify the notation, one usually assumes $L \subseteq L^\sigma$. Being a complete and completely distributive lattice, every canonical extension $\mathbf{L}^\sigma$ has a definable relative pseudo-complementation (i.e. a Heyting implication) given, for all $a, b \in L^\sigma$, by

$$a \rightarrow b := \bigvee\{c \in L^\sigma : a \wedge c \leq b\}. \tag{RP}$$

Let us also keep in mind that every Heyting algebra has a p-lattice reduct, in which the pseudo-complement operation $\neg$ is given by $\neg a = a \to 0$.

Since both $\mathbf{A}_+$ and $\mathbf{A}_-$ have a bounded distributive lattice reduct, we can construct the canonical extensions of these reducts, which we denote by $\mathbf{A}_+^\sigma$ and $\mathbf{A}_-^\sigma$. These algebras can be endowed with Heyting implications $\to_+, \to_-$ defined according to (RP), obtaining Heyting algebras $\mathbf{H}_+ := \langle \mathbf{A}_+^\sigma, \to_+ \rangle$ and $\mathbf{H}_- := \langle \mathbf{A}_-^\sigma, \to_- \rangle$. Regarding the extra operation (pseudo-complement) on $\mathbf{A}_+^\sigma$, we observe that the equations defining the pseudo-complement in a lattice are preserved by canonical extensions [1, Corollary 3.14]. That is, the canonical extension of a p-lattice is a p-lattice. Thus $\mathbf{A}_+^\sigma$ is, structurally, both a Heyting algebra (with $\to_+$ as implication, or relative pseudo-complement) and a p-lattice in which the pseudo-complement (call it $\neg_+$) is the extension (as defined in [1, p. 183]) of the pseudo-complement operation of $\mathbf{A}_+$. Moreover, for all $a \in \mathbf{A}_+^\sigma$, we have

$$\neg_+ a = a \to_+ 0_+$$

where 0_+ is the bottom element of $\mathbf{A}_+^\sigma$. This holds because both the Heyting implication and the pseudo-complement operation are completely determined by the lattice structure, therefore the pseudo-complement of $a \in \mathbf{A}_+^\sigma$ is given by

$$\bigvee \{c \in A_+^\sigma : a \wedge c = 0_+\}.$$

The previous considerations entail that (i) $\mathbf{A}_+$ embeds (as a bounded pseudo-complemented lattice) into the Heyting algebra $\mathbf{A}_+^\sigma$ and (ii) $\mathbf{A}_-$ embeds (as a bounded lattice) into the Heyting algebra $\mathbf{A}_-^\sigma$. We proceed to show that the maps $n\colon A_+ \to A_-$ and $p\colon A_- \to A_+$ can be extended to H_+ and H_- so as to preserve the desired properties.

The problem of extending maps is well studied within the theory of canonical extensions. Every map between (bounded distributive) lattices (such as our $n\colon L_+ \to L_-$) can be extended in two ways, obtaining two maps (usually denoted n^σ and n^π) from L_+^σ to L_-^σ which agree with n on L_+. However, if the map is meet-preserving (as is our case), then $n^\sigma = n^\pi$ [9, Lemma 4.4, Corollary 4.7], so we need not choose between the two. At this point, proving that the extended maps n^σ, p^σ satisfy the desired properties is straightforward, modulo the following lemma [19, Lemma 6.4].

Lemma 5.2. *Let* $\mathbf{M}_+ = \langle M_+, \wedge_+, \to_+ \rangle$ *and* $\mathbf{M}_- = \langle M_-, \wedge_-, \to_- \rangle$ *be implicative meet-semilattices*[5] *and* $n\colon M_+ \to M_-$ *and* $p\colon M_- \to M_+$ *be maps satisfying the following properties:*

[5]Implicative meet-semilattices are the $\langle \wedge, \to \rangle$-subreducts of Heyting algebras, corresponding to the conjunction-implication fragment of intuitionistic logic. Thus, in particular, the $\langle \wedge, \to \rangle$-reduct of every Heyting algebra is an implicative meet-semilattice.

(i) n *preserves finite meets,*

(ii) p *preserves finite meets,*

(iii) $n \circ p = Id_{M_-}$ *and* $Id_{M_+} \leq_+ p \circ n$.

Then p *also preserves the implication.*

Proposition 5.3. *Let* $\langle \mathbf{A}_+, \mathbf{A}_-, n, p\rangle$ *be a tuple satisfying the conditions of Definition 3.1. Then the tuple* $\langle \mathbf{H}_+, \mathbf{H}_-, n^\sigma, p^\sigma\rangle$, *where* $\mathbf{H}_+ := \langle \mathbf{A}_+^\sigma, \to_+\rangle$ *and* $\mathbf{H}_- := \langle \mathbf{A}_-^\sigma, \to_-\rangle$ *are defined as before, satisfies the conditions of Definition 2.5.*

Proof. In the light of the preceding discussion, we only need to check that the maps n and p satisfy items (i) to (iii) of Definition 2.5. For items (i) and (ii) we can invoke [9, Corollary 4.7], whereas (iii) easily follows from [9, Lemma 4.5]. □

Theorem 5.4. *Every WPQK-algebra is embeddable into a quasi-Nelson algebra.*

Proof. As discussed earlier, we use Theorem 4.10 to view a WPQK-algebra $\mathbf{A}$ as a WPQK twist-structure $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$, where $A_+ \subseteq H_+ = A_+^\sigma$ and $A_- \subseteq H_- = A_-^\sigma$. Constructing the algebra $\mathbf{H}_+ \bowtie \mathbf{H}_-$ as indicated in Proposition 5.3, we have $A \subseteq H_+ \times H_-$. Let $A^\sigma := \{\langle a_+, a_-\rangle \in H_+ \times H_- : a_+ \wedge_+ p^\sigma(a_-) = 0_+\}$. As observed in [22], the set A^σ is the universe of (the largest) quasi-Nelson twist-structure over $\mathbf{H}_+ \bowtie \mathbf{H}_-$, which we denote by $\mathbf{A}^\sigma$. Moreover, $A \subseteq A^\sigma$ because of the last condition in Definition 3.1. So $\mathbf{A}$ is a $\{\wedge, \vee, \sim, \neg, 0, 1\}$-subalgebra of $\mathbf{A}^\sigma$, as claimed. □

Theorem 5.4 easily entails that the equational presentation of WPQK-algebras of Definition 4.2 constitutes a complete axiomatization of the $\{\to\}$-free equational consequence of quasi-Nelson algebras; this result, in turn, implies that the "logic of WPQK-algebras" will correspond to the $\{\to\}$-free fragment of quasi-Nelson logic.

Corollary 5.5. *The class of* $\{\wedge, \vee, \sim, \neg, 0, 1\}$*-subreducts of quasi-Nelson algebras is the variety of WPQK-algebras. The class of* $\{\wedge, \vee, \sim, \neg, 0, 1\}$*-subreducts of Nelson algebras is the variety of wp-Kleene algebras.*

Although a logical calculus corresponding to WPQK-algebras (or even to *wp*-Kleene algebras) has not been defined, the preceding results are sufficient for us to make a few considerations about the logics of WPQK and *wp*-Kleene algebras from an algebraic logic point of view.

Denote by $\models_{\mathcal{QN}^*}$ the logical consequence corresponding to the $\{\wedge, \vee, \sim, \neg, 0, 1\}$-fragment of quasi-Nelson logic $\models_{\mathcal{QN}}$ (as defined e.g. in [14]). Thus, $\Gamma \models_{\mathcal{QN}^*} \varphi$ if and only if $\Gamma \models_{\mathcal{QN}} \varphi$, for all formulas Γ, φ that belong to the $\{\wedge, \vee, \sim, \neg, 0, 1\}$-fragment of the language of quasi-Nelson logic. Similarly, let $\models_{\mathcal{N}^*}$ denote the

$\{\wedge, \vee, \sim, \neg, 0, 1\}$-fragment of Nelson logic $\models_{\mathcal{N}}$. On the other hand, let $\models_{\mathcal{WPQK}}$ and $\models_{wp\mathcal{K}}$ denote, respectively, the consequences determined by the class of matrices $\{\langle \mathbf{A}, \{1\}\rangle : \mathbf{A}$ is a WPQK algebra$\}$ and $\{\langle \mathbf{A}, \{1\}\rangle : \mathbf{A}$ is a *wp*-Kleene algebra$\}$. The following proposition is an immediate consequence of Corollary 5.5.

Proposition 5.6. *$\models_{\mathcal{QN}^*}$ and $\models_{\mathcal{N}^*}$ coincide, respectively, with $\models_{\mathcal{WPQK}}$ and $\models_{wp\mathcal{K}}$.*

Proposition 5.7. *$\models_{\mathcal{WPQK}}$ and $\models_{wp\mathcal{K}}$ are not algebraisable in the sense of [4].*

Proof. If we show that $\models_{wpK}$ is not algebraisable, the non-algebraisability of $\models_{\mathcal{WPQK}}$ will follow, because algebraisability is preserved by extensions and $\models_{wpK}$ extends $\models_{WPQK}$. Let $\mathbf{L} = \langle \{0, a, b, 1\}; \wedge, \vee, \neg, 0, 1\rangle$ be the four-element totally ordered *p*-lattice, with $0 < a < b < 1$. The order determines the behaviour of the pseudo-complement operation, which is given by $\neg 1 = \neg a = \neg b = 0$ and $\neg 0 = 1$. For $\nabla = \{a, b, 1\}$, consider the *wp*-Kleene algebra $\mathbf{A} = Tw(\mathbf{L}, \nabla)$, which is also a totally ordered (six-element) lattice with elements $\langle 0, 1\rangle < \langle 0, b\rangle < \langle 0, a\rangle < \langle a, 0\rangle < \langle b, 0\rangle < \langle 1, 0\rangle$. The lattice of congruences of $\mathbf{A}$ has five elements, the non-trivial ones being: θ_1, having as non-trivial blocks $\{\langle a, 0\rangle, \langle b, 0\rangle\}, \{\langle 0, a\rangle, \langle 0, b\rangle\}$, θ_2 having as non-trivial blocks $\{\langle 1, 0\rangle, \langle b, 0\rangle\}, \{\langle 0, 1\rangle, \langle 0, b\rangle\}$, and $\theta_3 = \theta_1 \cup \theta_2$. If $\models_{wpK}$ were algebraisable, there would be an isomorphism between the lattice of logical $\models_{wpK}$-filters on $\mathbf{A}$ and the congruences of $\mathbf{A}$ given by the Leibniz operator Ω [4, Theorem 5.1]. There would thus be four non-trivial $\models_{wpK}$-filters F_0, F_1, F_2, F_3 on $\mathbf{A}$ such that $\Omega(F_0) = Id$, $\Omega(F_1) = \theta_1$, $\Omega(F_2) = \theta_2$ and $\Omega(F_3) = \theta_3$. Since $p \models_{wpK} p \vee q$ obviously holds, all the $\models_{wpK}$-filters on $\mathbf{A}$ must be increasing sets (i.e., on a chain, lattice filters). Observe that $F_0 \subseteq F_1 \subseteq F_3$ and $F_0 \subseteq F_2 \subseteq F_3$. Since $F_0 \neq \emptyset$ (an algebraisable logic must have theorems), both F_1 and F_2 must have at least two elements, and F_3 must have at least three elements. The only lattice filter with at least three elements having θ_3 as its Leibniz congruence is the principal up-set $\uparrow\langle a, 0\rangle$. Hence, $F_3 = \uparrow\langle a, 0\rangle$. This means that $F_2 = \uparrow\langle b, 0\rangle$ and $F_0 = \{\langle 1, 0\rangle\}$. But then $\Omega(F_0) = \theta_1$, which contradicts $\Omega(F_0) = Id$. Hence, there can be no isomorphism between $\models_{wpK}$-filters on $\mathbf{A}$ and the congruences of $\mathbf{A}$. □

An altogether different question from the one considered in Proposition 5.7 is whether the class of WPQK-algebras (resp. *wp*-Kleene algebras) might be the equivalent algebraic semantics of some algebraisable logic (different from $\models_{\mathcal{QN}^*}$, resp. $\models_{\mathcal{N}^*}$); that is, as some authors might put it, whether WPQK-algebras (respectively, *wp*-Kleene algebras) form a class of "algebras of logic" in such a strong sense. As far as WPQK-algebras are concerned, it is easy to show that the answer is negative. This holds because *p*-lattices can be viewed as a subclass of WPQK-algebras (Proposition 9.3), and *p*-lattices are not the equivalent algebraic semantics of any

algebraisable logic [18, Theorem 3.1]. This argument does not apply to *wp*-Kleene algebras (cf. Proposition 9.13), and indeed the corresponding question concerning this class is open.

6 Refining the Twist Representation

In this section we sharpen the twist representation of WPQK-algebras in the spirit of the Sendlewski-Odintsov filter-ideal representation of Nelson algebras and $N4$-lattices. Let us consider again the algebra $\mathbf{A}_+ \bowtie \mathbf{A}_-$ introduced in Definition 3.1. We showed in Remark 3.3 that the set

$$\{\langle a_+, a_-\rangle \in A_+ \times A_- : a_+ \wedge_+ p(a_-) = 0_+\}$$

is closed under all the algebraic operations of $\mathbf{A}_+ \bowtie \mathbf{A}_-$, and is therefore the universe of the largest twist-structure over $\mathbf{A}_+ \bowtie \mathbf{A}_-$. We can obtain arbitrary twist-structures by considering subsets of $A_+ \times A_-$ defined as follows.

Let $\nabla \subseteq A_+$ be a lattice filter of $\mathbf{A}_+$. We shall say that ∇ is *dense* if it contains the set $D(\mathbf{A}_+)$ of dense elements of $\mathbf{A}_+$, defined as follows:

$$D(\mathbf{A}_+) := \{a_+ \vee_+ \neg_+ a_+ : a_+ \in A_+\} = \{a_+ \in A_+ : \neg_+ a_+ = 0_+\}.$$

Given a dense filter $\nabla \supseteq D(\mathbf{A}_+)$ of $\mathbf{A}_+$, define the set:

$$Tw\langle A_+, A_-, \nabla\rangle := \{\langle a_+, a_-\rangle \in A_+ \times A_- : a_+ \vee_+ p(a_-) \in \nabla,\ a_+ \wedge_+ p(a_-) = 0_+\}.$$

In what follows, instead of $Tw\langle A_+, A_-, \nabla\rangle$, we shall sometimes use the more complete notation $Tw\langle A_+, A_-, n, p, \nabla\rangle$ if the role of the maps n and p needs to be emphasised.

Proposition 6.1. *Let $\mathbf{A}_+, \mathbf{A}_-, n, p$ be given as per Definition 3.1 and let ∇ be a dense filter of $\mathbf{A}_+$. The set $Tw(A_+, A_-, \nabla)$ is the universe of a twist-structure over $\mathbf{A}_+ \bowtie \mathbf{A}_-$.*

Proof. Notice that 'one half' of the proof (the one corresponding to the condition $a_+ \wedge_+ p(a_-) = 0_+$) has already been established in Remark 3.3. We thus need to deal with the condition $a_+ \vee_+ p(a_-) \in \nabla$. Let $\langle a_+, a_-\rangle \in Tw(A_+, A_-, \nabla)$, so that $a_+ \vee_+ p(a_-) \in \nabla$ and $a_+ \wedge_+ p(a_-) = 0_+$. From $Id_{A_+} \leq_+ p \circ n$ we have $a_+ \vee_+ p(a_-) \leq_+ p(a_-) \vee_+ pn(a_+)$, and thus $p(a_-) \vee_+ pn(a_+) \in \nabla$. This shows that $Tw(A_+, A_-, \nabla)$ is closed under the $\sim$ negation. For the negation $\neg$ we need to check that $\neg_+ a_+ \vee_+ pn(a_+) \in \nabla$. This follows from the density condition: from $a_+ \vee_+ \neg_+ a_+ \in \nabla$ and $a_+ \vee_+ \neg_+ a_+ \leq_+ \neg_+ a_+ \vee_+ pn(a_+)$, we obtain the desired result. For closure

under $\wedge$ we need to check that, given $\langle a_+, a_-\rangle, \langle b_+, b_-\rangle \in Tw(A_+, A_-, \nabla)$, we have $(a_+ \wedge_+ b_+) \vee_+ p(a_- \vee_- b_-) \in \nabla$. By distributivity, we have $(a_+ \wedge_+ b_+) \vee_+ p(a_- \vee_- b_-) = (a_+ \vee_+ p(a_- \vee_- b_-)) \wedge_+ (b_+ \vee_+ p(a_- \vee_- b_-))$. Since $a_+ \vee_+ p(a_-) \leq_+ a_+ \vee_+ p(a_- \vee_- b_-)$, from the assumption $a_+ \vee_+ p(a_-) \in \nabla$ we obtain $a_+ \vee_+ p(a_- \vee_- b_-) \in \nabla$. A similar reasoning, using the assumption $b_+ \vee_+ p(b_-) \in \nabla$, gives us $b_+ \vee_+ p(a_- \vee_- b_-) \in \nabla$. Thus, the result follows from the closure of ∇ under $\wedge_+$. Regarding $\vee$, we need to ensure that $a_+ \vee b_+ \vee_+ p(a_- \wedge_- b_-) \in \nabla$. Since p preserves meets, we have $a_+ \vee_+ b_+ \vee_+ p(a_- \wedge_- b_-) = a_+ \vee_+ b_+ \vee_+ (p(a_-) \wedge_+ p(b_-)) = (a_+ \vee_+ b_+ \vee_+ p(a_-)) \wedge_+ (a_+ \vee_+ b_+ \vee_+ p(b_-))$. Since $a_+ \vee_+ p(a_-) \leq_+ a_+ \vee_+ b_+ \vee_+ p(a_-)$ and $a_+ \vee_+ p(a_-) \in \nabla$, we have $a_+ \vee_+ b_+ \vee_+ p(a_-) \in \nabla$. A similar reasoning shows that the assumption $b_+ \vee_+ p(b_-) \in \nabla$ entails $a_+ \vee_+ b_+ \vee_+ p(b_-) \in \nabla$. Hence the result follows from the closure of ∇ under $\wedge_+$. □

To see that the twist-structures with universe $Tw\langle A_+, A_-, \nabla\rangle$ are all the possible twist-structures over $\mathbf{A}_+ \bowtie \mathbf{A}_-$, consider an arbitrary WPQK twist-structure $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$. Define the set

$$I(\mathbf{A}) := \{\langle a_+, a_-\rangle \in A : {\sim}\langle a_+, a_-\rangle \leq \langle a_+, a_-\rangle\}.$$

A simpler description of $I(\mathbf{A})$ is this one:

$$I(\mathbf{A}) = \{\langle a_+, 0_-\rangle : \langle a_+, 0_-\rangle \in A\}.$$

Indeed, it is clear that every element of the form $\langle a_+, 0_-\rangle$ satisfies ${\sim}\langle a_+, 0_-\rangle = \langle 0_+, n(a_+)\rangle \leq \langle a_+, 0_-\rangle$. But conversely, the condition ${\sim}\langle a_+, a_-\rangle \leq \langle a_+, a_-\rangle$ entails $p(a_-) \leq_+ a_+$. In such a case, recalling the requirement $a_+ \wedge_+ p(a_-) = 0_+$, one has $a_+ \wedge_+ p(a_-) = p(a_-) = 0_+$. Then $np(a_-) = a_- = n(0_+) = 0_-$.

Theorem 6.2. *Let $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$ be a WPQK twist-structure.*

(i) *$I(\mathbf{A})$ is a lattice filter of $\mathbf{A}$.*

(ii) *$\nabla_{\mathbf{A}} := \pi_1[I(\mathbf{A})]$ is a lattice filter of $\mathbf{A}_+$.*

(iii) *$D(\mathbf{A}_+) \subseteq \nabla_{\mathbf{A}}$.*

(iv) *$A = Tw\langle A_+, A_-, \nabla_{\mathbf{A}}\rangle$.*

Proof. (i). Recalling that $I(\mathbf{A}) = \{\langle a_+, 0_-\rangle : \langle a_+, 0_-\rangle \in A\}$, this is straightforward. Obviously the top element $\langle 1_+, 0_-\rangle$ of $\mathbf{A}$ belongs to $I(\mathbf{A})$. Assuming $\langle a_+, 0_-\rangle \in I(\mathbf{A})$ and $\langle a_+, 0_-\rangle \leq \langle b_+, b_-\rangle$, we have $b_- \leq_- 0_-$, so that $\langle b_+, b_-\rangle = \langle b_+, 0_-\rangle \in (\mathbf{A})$. Finally, if $\langle a_+, 0_-\rangle, \langle b_+, 0_-\rangle \in I(\mathbf{A})$, then $\langle a_+, 0_-\rangle \wedge \langle b_+, 0_-\rangle = \langle a_+ \wedge_+ b_+, 0_- \vee_- 0_-\rangle = \langle a_+ \wedge_+ b_+, 0_-\rangle \in I(\mathbf{A})$.

(ii). It follows from the preceding item that $1_+ \in \nabla_{\mathbf{A}}$. Further, assume $a_+ \in \nabla_{\mathbf{A}}$ and $a_+ \leq_+ b_+$. The former assumption implies that $\langle a_+, 0_- \rangle \in I(\mathbf{A})$. From the latter, letting $\langle b_+, b_- \rangle \in A$ (such an element must exist in $\mathbf{A}$, by the requirement that $\pi_1(A) = A_+$ in Definition 3.1), we have $\langle a_+, 0_+ \rangle \vee \langle b_+, b_- \rangle = \langle a_+ \vee_+ b_+, 0_- \wedge_- b_- \rangle = \langle b_+, 0_- \rangle$. Then $\langle b_+, 0_- \rangle \in I(\mathbf{A})$ and so $b_+ \in \nabla_{\mathbf{A}}$, as required. Lastly, assuming $a_+, b_+ \in \nabla_{\mathbf{A}}$, we have $\langle a_+, 0_- \rangle, \langle b_+, 0_- \rangle \in I(\mathbf{A})$. Hence, by item (i) above, we have $\langle a_+ \wedge_+ b_+, 0_- \rangle \in I(\mathbf{A})$ and so $a_+ \wedge_+ b_+ \in \nabla_{\mathbf{A}}$.

(iii). Let $a_+ \vee_+ \neg_+ a_+ \in D(\mathbf{A}_+)$. Then $a_+ \in A_+$ and, since $\pi_1(A) = A_+$, there is $a_- \in A_-$ with $\langle a_+, a_- \rangle \in A$. Then $\langle a_+, a_- \rangle \vee \neg \langle a_+, a_- \rangle = \langle a_+, a_- \rangle \vee \langle \neg_+ a_+, n(a_+) \rangle = \langle a_+ \vee_+ \neg_+ a_+, a_- \wedge_- n(a_+) \rangle = \langle a_+ \vee_+ \neg_+ a_+, 0_- \rangle \in A$ (the last equality holding by Remark 3.2). Then $a_+ \vee_+ \neg_+ a_+ \in \nabla_{\mathbf{A}}$, as required.

(iv). The inclusion $A \subseteq Tw\langle A_+, A_-, \nabla_{\mathbf{A}} \rangle$ is straightforward. Indeed, for all $\langle a_+, a_- \rangle \in A$, using Remark 3.2) we have $\langle a_+, a_- \rangle \vee \sim \langle a_+, a_- \rangle = \langle a_+ \vee_+ p(a_-), a_- \wedge_- n(a_+) \rangle = \langle a_+ \vee_+ p(a_-), 0_- \rangle \in I(\mathbf{A})$. Thus $a_+ \vee_+ p(a_-) \in \nabla_{\mathbf{A}}$ and so $\langle a_+, a_- \rangle \in Tw\langle A_+, A_-, \nabla_{\mathbf{A}} \rangle$. Conversely, assume $\langle a_+, a_- \rangle \in Tw\langle A_+, A_-, \nabla_{\mathbf{A}} \rangle$, i.e. $a_+ \vee_+ p(a_-) \in \nabla_{\mathbf{A}}$ and $a_+ \wedge_+ p(a_-) = 0_+$. From the first condition we have $\langle a_+ \vee_+ p(a_-), 0_- \rangle \in I(\mathbf{A}) \subseteq A$. Also, from $p(a_-) \in A_+$ and $\pi_1(A) = A_+$, we have that there is $b_- \in A_-$ such that $\langle p(a_-), b_- \rangle \in A$. Recalling $n \circ p = Id_{A_-}$, we have $\neg \langle p(a_-), b_- \rangle = \langle \neg_+ p(a_-), np(a_-) \rangle = \langle \neg_+ p(a_-), a_- \rangle \in A$.

We further compute:

$$
\begin{aligned}
&\langle a_+ \vee_+ p(a_-), 0_- \rangle \wedge \langle \neg_+ p(a_-), a_- \rangle = \\
&= \langle (a_+ \vee_+ p(a_-)) \wedge_+ \neg_+ p(a_-), 0_- \vee_- a_- \rangle \\
&= \langle (a_+ \vee_+ p(a_-)) \wedge_+ \neg_+ p(a_-), a_- \rangle \\
&= [\text{by distributivity}] \\
&= \langle (a_+ \wedge_+ \neg_+ p(a_-)) \vee_+ (p(a_-) \wedge_+ \neg_+ p(a_-)), a_- \rangle \\
&= [\text{using } x \wedge_+ \neg_+ x = 0_+] \\
&= \langle (a_+ \wedge_+ \neg_+ p(a_-)) \vee_+ 0_+, a_- \rangle \\
&= \langle a_+ \wedge_+ \neg_+ p(a_-), a_- \rangle \\
&= [\text{using } a_+ \wedge_+ p(a_-) = 0_+] \\
&= \langle a_+, a_- \rangle.
\end{aligned}
$$

Hence, $\langle a_+, a_- \rangle \in A$ and so $Tw\langle A_+, A_-, \nabla_{\mathbf{A}} \rangle \subseteq A$. □

Remark 6.3. Theorem 6.2 can be used to establish a (co-variant) equivalence of categories between (1) a category having WPQK-algebras as objects and algebraic homomorphisms between them as morphisms, and (2) a category having tuples of type $\langle \mathbf{A}_+, \mathbf{A}_-, n, p, \nabla \rangle$ as objects and as morphisms pairs of maps $\langle h_+, h_- \rangle$ which

preserve the tuple structure. We shall not pursue this here; the interested reader is referred to [21] for the relevant details.

As an application of Theorem 6.2, we describe in the next example a simple method for constructing interesting WPQK-algebras (*qua* twist-structures).

Example 6.4. Let $\mathbf{A}_+ = \langle A_+, \wedge_+, \vee_+, \neg_+, 0_+, 1_+\rangle$ be a p-lattice having a splitting element, that is, an element $c_+ \in A_+$ such that, for all $a_+ \in A_+$, either $a_+ <_+ c_+$ or $c_+ \leq_+ a_+$. It is well known that such a splitting element exists, for instance, in every subdirectly irreducible p-lattice [13, Theorem 2], in which case c_+ is the unique co-atom. Thus $A_+ = [0_+, c_+] \cup [c_+, 1_+]$, where $[0_+, c_+] := \{a_+ \in A_+ : a_+ \leq_+ c_+\}$ and $[c_+, 1_+] := \{a_+ \in A_+ : c_+ \leq_+ a_+\}$. Let us observe that $[c_+, 1_+] \subseteq D(\mathbf{A}_+)$, where $D(\mathbf{A}_+)$ denotes the set of dense elements of $\mathbf{A}_+$ given by

$$D(\mathbf{A}_+) = \{a_+ \vee_+ \neg_+ a_+ : a_+ \in A_+\} = \{a_+ \in A_+ : \neg_+ a_+ = 0_+\}.$$

Using the latter characterization, it is easy to show that $[c_+, 1_+] \subseteq D(\mathbf{A}_+)$. Observe that (disregarding the nullary constant 1_+) the interval $[0_+, c_+]$ is a subalgebra of $\mathbf{A}_+$. Thus $[0_+, c_+]$ can itself be viewed as a p-lattice, with bottom element 0_+ and top element c_+. Denote this algebra by $\mathbf{A}([0_+, c_+])$.
Let $\mathbf{A}_- = \langle A_-, \wedge_-, \vee_-, 0_-, 1_-\rangle$ be an isomorphic copy of the bounded lattice reduct of $\mathbf{A}([0_+, c_+])$. We denote by $a_- \in A_-$ the element corresponding, via the isomorphism, to each $a_+ \in [0_+, c_+]$. Thus $1_- = c_-$.

Define maps $n\colon A_+ \to A_-$ and $p\colon A_- \to A_+$ as follows. Let $n(a_+) = a_-$ for $a_+ < c_+$ and $n(a_+) = 1_-$ for $c_+ \leq_+ a_+$. Let $p(1_-) = 1_+$ and $p(a_-) = a_+$ for $a_- \in A_-$ with $a_- <_- 1_-$. It is easy to verify that the maps thus defined satisfy all the conditions of Definition 3.1. Thus we can obtain a WPQK twist-structure $\mathbf{A}$ over $\mathbf{A}_+ \bowtie \mathbf{A}_-$ by choosing a filter ∇ such that $[c_+, 1_+] \subseteq D(\mathbf{A}_+) \subseteq \nabla$. Note that $\langle c_+, 0_+\rangle$ will itself be a splitting element in $\mathbf{A}$. More importantly, observe that:

(i) if $c_+ \neq 1_+$, then n is not injective, which implies that $\mathbf{A}$ is not a wp-Kleene lattice (see Proposition 9.12);

(ii) if $[c_+, 1_+] \subsetneq \nabla$, then $n(\nabla) \neq \{1_-\}$, so $\mathbf{A}$ is not a p-lattice (see Proposition 9.2).

Thus, the method described above allows us to construct examples of WPQK-algebras which do not belong to either of these already known subvarieties.

Figure 1 shows the Hasse diagram of a WPQK-algebra $\mathbf{A}$ obtained by the method in Example 6.4, together with the corresponding p-lattices $\mathbf{A}_+$ and $\mathbf{A}_-$. We do not indicate the pseudo-complement operations on $\mathbf{A}_+$ and $\mathbf{A}_-$ on the diagram, as these are determined by the lattice structure. The maps n and p are given by $p(x_-) = x_+$

for all $x_- \in A_-$, $n(x_+) = 1_-$ for $x_+ \in \{e_+, 1_+\}$ and $n(x_+) = x_-$ otherwise. This determines the behaviour of all operations on $\mathbf{A}$. It can be checked that $\mathbf{A}$ is not a *wp*-Kleene algebra, because the negation $\sim$ is not involutive: $\sim\sim\langle e_+, 0_-\rangle = \langle 1_+, 0_+\rangle$. Also, $\mathbf{A}$ is not a *p*-lattice because $\neg\langle 0_+, c_-\rangle = \langle 1_+, 0_-\rangle$, and $\langle 1_+, 0_-\rangle$ is not the pseudo-complement of $\langle 0_+, c_-\rangle$.

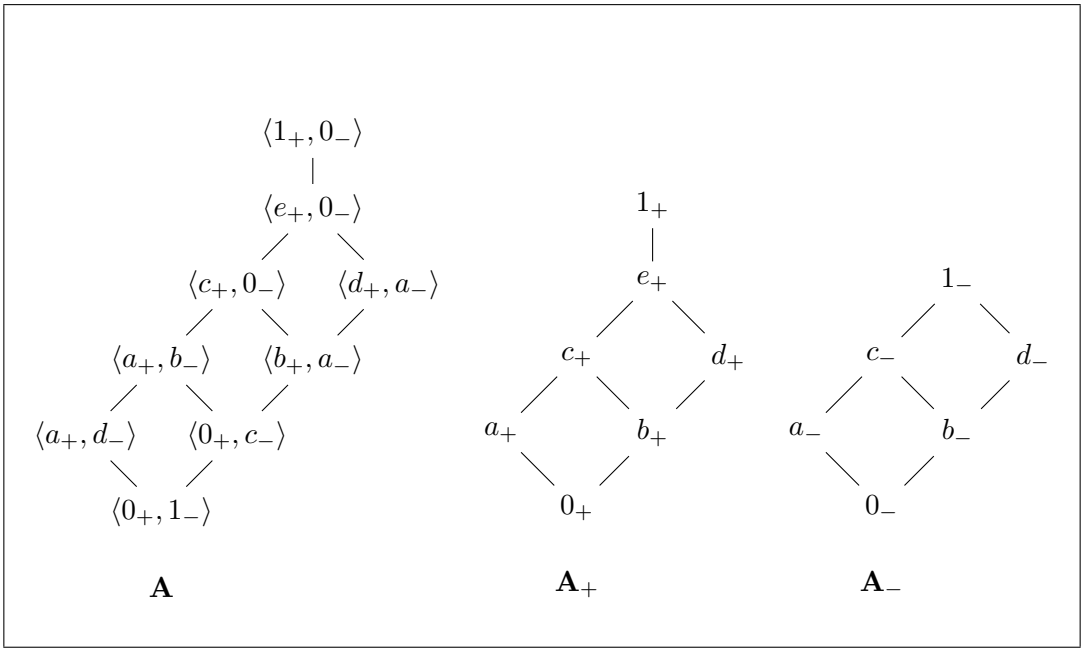

Figure 1: A WPQK-algebra constructed according to Example 6.4.

Figure 2 shows the congruence lattices of $\mathbf{A}, \mathbf{A}_+$ and $\mathbf{A}_-$; note that $\mathbf{A}_-$ is here viewed as a *p*-lattice rather than just a lattice. We shall see with Theorem 7.5 (cf. also Proposition 7.3) that the lattice $\mathrm{Con}(\mathbf{A})$ is in general embeddable into $\mathrm{Con}(\mathbf{A}_+)$ via a map denoted $(.)^*$. The names of the elements of $\mathrm{Con}(\mathbf{A}_+)$ on the diagram have been chosen to reflect this observation. Notice that the congruence η, which is the one having as only non-singleton blocks $\{b_+, d_+\}$ and $\{c_+, e_+\}$, is (the only one) not in the image of $(.)^*$ because $\eta \notin \mathrm{Con}^{\Box}(\mathbf{A}_+)$; see Theorem 7.8. Indeed, since $\langle c_+, e_+\rangle \in \eta$, if we had $\eta \in \mathrm{Con}^{\Box}(\mathbf{A}_+)$, then we should also have $\langle pn(c_+), pn(e_+)\rangle = \langle c_+, 1_+\rangle \in \eta$, which is not the case. We shall also see that $\mathrm{Con}(\mathbf{A}_-)$ is embeddable into $\mathrm{Con}(\mathbf{A}_+)$ by a map denoted $(.)^{\Box}$ (Proposition 7.13). On the diagram, the embedding is given by $(A_- \times A_-)^{\Box} = A_+ \times A_+$, $(Id_{A_-})^{\Box} = \theta_0^*$ and $(\rho_i)^{\Box} = \theta_i^*$ for $1 \leq i \leq 4$.

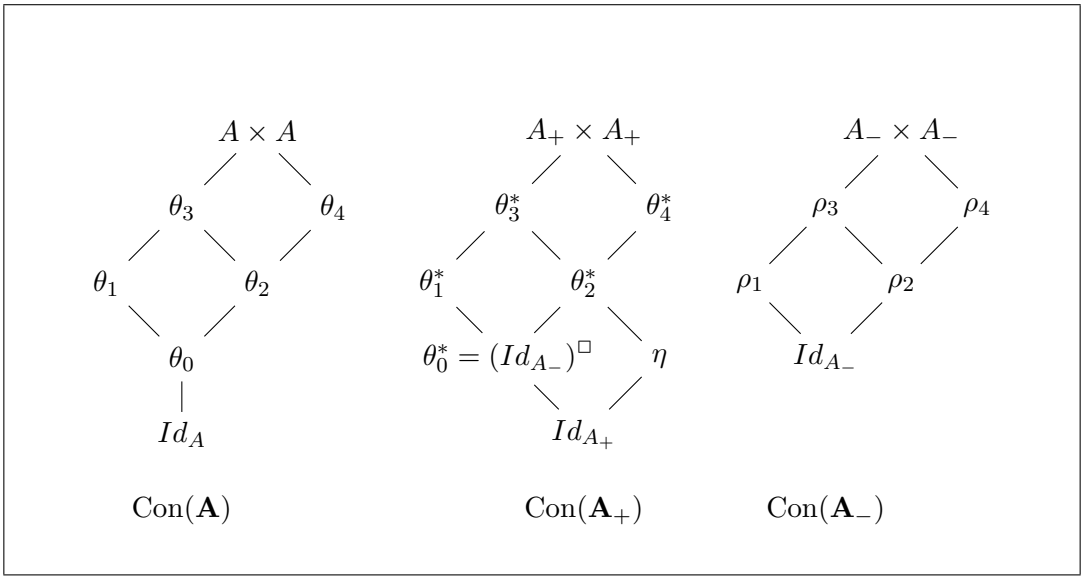

Figure 2: The corresponding congruence lattices.

7 Congruences and the p-Skeleton

In this section we shall obtain more information on the lattice of congruences of a WPQK-algebra, and in particular on how it relates to the congruences of the underlying factor algebra given in the twist-structure representation. To do so, we will employ a non-involutive generalisation of Sendlewski's *p-skeleton* construction for *wp*-Kleene algebras.

Let **A** be a WPQK-algebra and $a \in A$. Define the operation:

$$a^* := a \wedge {\sim}\neg a.$$

It may be useful to observe the behaviour of the $*$ operation on a twist-structure. Recalling the proof of Lemma 3.5.i, we have that, for every twist-structure **A** and every pair $\langle a_+, a_- \rangle \in A$,

$$\langle a_+, a_- \rangle^* = \langle a_+, a_- \rangle \wedge {\sim}\neg \langle a_+, a_- \rangle = \langle a_+, n(\neg_+ a_+) \rangle.$$

For our purposes, the key feature of this operation is that it leaves the first component of each pair unchanged while deleting the second one. Using this observation, we can easily obtain a number of useful properties listed below.

Lemma 7.1. *Let* **A** *be a WPQK-algebra and* $a, b \in A$.

(i) $a \equiv b$ *iff* $a^* = b^*$.

(ii) $a = b$ *iff* ($a^* = b^*$ *and* $(\sim a)^* = (\sim b)^*$).

(iii) $(a \vee b)^* = (a^* \vee b^*)^* = a^* \vee b^*$.

(iv) $(a \wedge b)^* = (a^* \wedge b^*)^*$.

(v) $\neg(a^*) = \neg a$

(vi) $0^* = 0$ *and* $1^* = 1$.

(vii) $(\sim\sim a)^* = (\sim\neg a)^*$.

(viii) $\sim(a^*) = \sim\sim\neg a$.

(ix) $a^{**} = a^*$.

Proof. (i). Follows from item (i) of Proposition 4.11.

(ii). Follows from (ii) of Proposition 4.11.

It is convenient to check the remaining items on a twist-structure $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$. Let $a = \langle a_+, a_- \rangle, b = \langle b_+, b_- \rangle \in A$, and recall from Lemma 3.5.i that $\langle a_+, a_- \rangle^* = \langle a_+, a_- \rangle \wedge \sim\neg\langle a_+, a_- \rangle = \langle a_+, n(\neg_+ a_+) \rangle$.

(iii). Let us compute $\langle a_+, a_- \rangle^* \vee \langle b_+, b_- \rangle^* = \langle a_+ \vee_+ b_+, n(\neg_+ a_+) \wedge_- n(\neg_+ b_+) \rangle$. Observe that, using the requirement that n preserves finite meets and the semi-De Morgan identities (for the pseudo-complement), we have $n(\neg_+ a_+) \wedge_- n(\neg_+ b_+) = n(\neg_+ a_+ \wedge_+ \neg_+ b_+) = n(\neg_+(a_+ \vee_+ b_+))$ Thus we have

$$\langle a_+, a_- \rangle^* \vee \langle b_+, b_- \rangle^* = \langle a_+ \vee_+ b_+, n(\neg_+(a_+ \vee_+ b_+)) \rangle = (\langle a_+, a_- \rangle \vee \langle b_+, b_- \rangle)^*,$$

as required. Having established $a^* \vee b^* = (a \vee b)^*$, to show that $(a^* \vee b^*)^* = a^* \vee b^*$ it suffices to observe that $(a^*)^* = a^*$ for all $a \in A$, which is very easily checked on twist-structures.

(iv). It suffices to compute $(\langle a_+, a_- \rangle \wedge \langle b_+, b_- \rangle)^* = \langle a_+ \wedge_+ b_+, n(\neg_+(a_+ \wedge_+ b_+)) \rangle$ and $(\langle a_+, a_- \rangle^* \wedge \langle b_+, b_- \rangle^*)^* = \langle a_+ \wedge_+ b_+, n(\neg_+ a_+) \vee_- n(\neg_+ b_+) \rangle^* = \langle a_+ \wedge_+ b_+, n(\neg_+(a_+ \wedge_+ b_+)) \rangle$.

(v). On the one hand, we have

$$\neg(\langle a_+, a_- \rangle^*) = \neg(\langle a_+, n(\neg_+ a_+) \rangle) = \langle \neg_+ a_+, n(a_+) \rangle$$

and, on the other, $\neg\langle a_+, a_- \rangle = \langle \neg_+ a_+, n(a_+) \rangle$.

(vi). Also straightforward to check on a twist-structure.

(vii). Follows from item (i) above, together with Proposition 4.11.xii.

(viii). On a twist-structure, let us compute $\sim(\langle a_+, a_-\rangle^*) = \sim\langle a_+, n(\neg_+ a_+)\rangle = \langle pn(\neg_+ a_+), n(a_+)\rangle$. and $\sim\sim\neg\langle a_+, a_-\rangle = \sim\sim\langle \neg_+ a_+, n(a_+)\rangle = \langle pn(\neg_+ a_+), n(a_+)\rangle$.

(ix). Straightforward to check on a twist-structure. □

The preceding proposition should have made it clear that the $*$ operation is a way of "internalising" the relation $\equiv$ on $\mathbf{A}$, thus allowing us to find an isomorphic copy of the quotient $\mathbf{A}_+$ inside $\mathbf{A}$ itself. The p-skeleton defined below makes this intuition more precise.

Definition 7.2. The *p-skeleton* $\mathbf{A}^*$ of a WPQK algebra $\mathbf{A}$ is the algebra $\mathbf{A}^* = \langle A^*; \wedge^*, \vee^*, \neg^*, 0^*, 1^*\rangle$ where $A^* := \{a^* : a \in A\}$ and, for all $a, b \in A^*$,

$$a \wedge^* b := (a \wedge b)^*$$

$$a \vee^* b := (a \vee b)^* = a \vee b \qquad \text{(cf. Lemma 7.1.iii)}$$

$$\neg^* a := (\neg a)^*$$

$$0^* := 0$$

$$1^* := 1.$$

As mentioned earlier, Definition 7.2 and the results that it will allow us to prove are obviously a generalisation of Sendlewski's p-skeleton functor [26, Section 4]. Notice that, if the WPQK-algebra $\mathbf{A}$ happens to be a wp-Kleene algebra (Definition 4.14), then $a^* = \sim\neg a$ for all $a \in A$ [26, Lemma 2.1.iii], so we recover precisely Sendlewski's original definition.

Proposition 7.3. *For every WPQK-algebra* $\mathbf{A}$*, the map* $\alpha\colon A_+ \to A^*$ *given by* $\alpha([a]) = a^*$ *for all* $a \in A$ *is a p-lattice isomorphism between* $\mathbf{A}_+$ *and* $\mathbf{A}^*$ *(hence,* $\mathbf{A}^*$ *is a p-lattice).*

Proof. Lemma 7.1.i guarantees at the same time that α is a well-defined and injective map. Surjectivity is obvious. Let us check that the p-lattice operations are preserved. To improve readability, we write $\alpha[a]$ instead of $\alpha([a])$. The case of the constants is straightforward. Using Lemma 7.1.iii, we have $\alpha([a] \vee_+ [b]) = \alpha[a \vee b] = (a \vee b)^* = (a^* \vee b^*)^* = a^* \vee^* b^* = \alpha[a] \vee^* \alpha[b]$. Using Lemma 7.1.iv, we have $\alpha([a] \wedge_+ [b]) = \alpha[a \wedge b] = (a \wedge b)^* = (a^* \wedge b^*)^* = a^* \wedge^* b^* = \alpha[a] \wedge^* \alpha[b]$. Using Lemma 7.1.v, we have $\alpha(\neg_+[a]) = \alpha[\neg a] = (\neg a)^* = (\neg(a^*))^* = \neg^*(a^*) = \neg^*\alpha[a]$. □

Proposition 7.3 suggests that an alternative way of obtaining a twist-structure representation for WPQK-algebras is to use the p-skeleton $\mathbf{A}^*$ (instead of $\mathbf{A}_+$) as first factor and the map given by $a \mapsto a^*$ instead of the relation $\equiv$ (see Proposition 7.10 for the corresponding result concerning $\mathbf{A}_-$). We will state this formally later on (Theorem 7.11). For the time being, we are going to employ $\mathbf{A}^*$ to explore the relationship between the congruences of a WPQK-algebra and those of the corresponding p-lattice factor(s).

Lemma 7.4 (cf. [26], Lemma 5.1)**.** *Let* $\mathbf{A}$ *be a WPQK-algebra, let* $\theta \in \mathrm{Con}(\mathbf{A})$ *and* $a, b \in A$*. The following conditions are equivalent:*

(i) $\langle a, b\rangle \in \theta$.

(ii) $\langle a^*, b^*\rangle, \langle (\sim a)^*, (\sim b)^*\rangle \in \theta$.

Proof. It is plain that (i) implies (ii). Conversely, assume (ii). Thus, in the quotient $\mathbf{A}/\theta$ we have $[a^*]_\theta = [b^*]_\theta$ and $[(\sim a)^*]_\theta = [(\sim b)^*]_\theta$. Observe that $[a^*]_\theta = ([a]_\theta)^*$ and, likewise, $[(\sim a)^*]_\theta = (\sim [a]_\theta)^*$. Observe also, by Corollary 4.13, that the class of WPQK-algebras is closed under homomorphic images. Hence $\mathbf{A}/\theta$ is a WPQK-algebra. Then, by item (i) of Lemma 7.1, we have $[a]_\theta \equiv [b]_\theta$ and $\sim[a]_\theta \equiv \sim[b]_\theta$. By item (iii) of Proposition 4.6, this gives us $[a]_\theta = [b]_\theta$, that is $\langle a, b\rangle \in \theta$, as required. □

Theorem 7.5. *For every WPQK-algebra* $\mathbf{A}$*, the lattice* $Con(\mathbf{A})$ *is embeddable into the lattice* $Con(\mathbf{A}^*)$ *via the map* $(.)^*$ *given, for all* $\theta \in Con(\mathbf{A})$*, by* $\theta^* := \theta \cap (A^* \times A^*)$*. The embedding obviously preserves the least and greatest elements.*

Proof. It is plain that $\theta^* \in \mathrm{Con}(\mathbf{A}^*)$ for all $\theta \in \mathrm{Con}(\mathbf{A})$. Obviously the map $(.)^*$ preserves arbitrary intersections, so it is order-preserving. Notice also that $(.)^*$ preserves both the least and the greatest element (compare this with Proposition 7.13). Let us show that $(.)^*$ is also order-reflecting (which implies injectivity). Assume $\theta_1^* = \theta_1 \cap (A^* \times A^*) \subseteq \theta_2 \cap (A^* \times A^*) = \theta_2^*$ for some $\theta_1, \theta_2 \in \mathrm{Con}(\mathbf{A})$. Let $\langle a, b\rangle \in \theta_1$. Then, by Lemma 7.4, we have $\langle a^*, b^*\rangle, \langle (\sim a)^*, (\sim b)^*\rangle \in \theta_1$. Since $a^*, b^*, (\sim a)^*, (\sim b)^* \in A^*$, we have $\langle a^*, b^*\rangle, \langle (\sim a)^*, (\sim b)^*\rangle \in \theta_1^* \subseteq \theta_2^*$. Thus $\langle a^*, b^*\rangle, \langle (\sim a)^*, (\sim b)^*\rangle \in \theta_2$ which, again by Lemma 7.4, gives us $\langle a, b\rangle \in \theta_2$. Hence, $\theta_1 \subseteq \theta_2$, as required. □

For involutive WPQK-algebras (i.e. Sendlewski's *wp*-Kleene algebras), one can improve on Theorem 7.5 by showing $\mathrm{Con}(\mathbf{A}) \cong \mathrm{Con}(\mathbf{A}^*)$ [26, Theorem 5.2]; one can also obtain this result as a corollary to our Theorem 7.8 below. Such an isomorphism does not exist, in general, for WPQK-algebras. In fact, we have constructed

earlier (Figures 1 and 2) a subdirectly irreducible WPQK-algebra $\mathbf{A}$ such that neither the p-lattice $\mathbf{A}^*$ nor $\mathbf{A}_-$ (viewed as either a p-lattice or a lattice) is subdirectly irreducible[6]. We may observe, in particular, that every congruence of $\mathbf{A}^*$ having the form θ^* for some $\theta \in \mathrm{Con}(\mathbf{A})$ satisfies a characteristic property. Indeed, one has $\langle (\sim\sim a)^*, (\sim\sim b)^* \rangle \in \theta^*$ whenever $\langle a, b\rangle \in \theta^*$ (notice that this trivially holds on all *wp*-Kleene algebras). Indeed, this is *the only* non-trivial property that congruences having the form θ^* possess. We proceed to translate this intuition into a mathematical result.

For every WPQK-algebra $\mathbf{A}$ and $a \in A$, define $\Box a := (\sim\neg a)^*$. It may be useful to keep in mind that, if $\mathbf{A}$ is viewed as a twist-structure, then we have, for all $\langle a_+, a_-\rangle \in A$,

$$\Box\langle a_+, a_-\rangle = \langle pn(a_+), n(\neg_+ pn(a_+))\rangle = \langle pn(a_+), n(\neg_+ a_+)\rangle.$$

The equality $n(\neg_+ pn(a_+)) = n(\neg_+ a_+)$ holds because, on the one hand, from $a_+ \leq_+ pn(a_+)$ we obtain $\neg_+ pn(a_+) \leq_+ \neg_+ a_+$ and from this $n(\neg_+ pn(a_+)) \leq_+ n(\neg_+ a_+)$. On the other hand, we can obtain the other inequality $n(\neg_+ a_+) \leq_+ n(\neg_+ pn(a_+))$ as follows. We have $pn(a_+) \wedge_+ \neg_+ a_+ \leq_+ pn(a_+) \wedge_+ pn(\neg_+ a_+) = pn(a_+ \wedge_+ \neg_+ a_+) = pn(0_+) = 0_+$. From $pn(a_+) \wedge_+ \neg_+ a_+ = 0_+$, using the property of the pseudocomplement, we have $\neg_+ a_+ \leq_+ \neg_+ pn(a_+)$, so $n(\neg_+ a_+) \leq_+ n(\neg_+ pn(a_+))$, as required.

The p-skeleton A^* is obviously closed under the $\Box$ operation; thus we may consider the enriched algebra $\langle \mathbf{A}^*, \Box\rangle$. We also define

$$\mathrm{Con}^{\Box}(\mathbf{A}^*) := \{\eta \in \mathrm{Con}(\mathbf{A}^*) : \langle \Box a, \Box b\rangle \in \eta \text{ whenever } \langle a, b\rangle \in \eta\}.$$

It is easy to verify that $\mathrm{Con}^{\Box}(\mathbf{A}^*)$ is closed under arbitrary intersections. Thus $\langle \mathrm{Con}^{\Box}(\mathbf{A}^*), \subseteq\rangle$ is a complete lattice whose meet coincides with that of $\langle \mathrm{Con}(\mathbf{A}^*), \subseteq\rangle$. Indeed, $\langle \mathrm{Con}^{\Box}(\mathbf{A}^*), \subseteq\rangle$ is just the lattice of all congruences of the algebra $\langle \mathbf{A}^*, \Box\rangle$. Our next aim is to show that this lattice is isomorphic to $\mathrm{Con}(\mathbf{A})$.

In the following lemma we state a few properties of the $\Box$ operator that will be useful in subsequent proof.

Lemma 7.6. *Let* $\mathbf{A}$ *be a WPQK-algebra and* $a, b \in A$.

(i) $\Box a = (\sim\sim a)^* = (\sim\sim(a^*))^* = (\sim\neg(a^*))^*$.

(ii) $\Box(\neg^*(a^*)) = (\sim(a^*))^* = \Box\neg\Box a$.

[6]This not only destroys all hope of having $\mathrm{Con}(\mathbf{A}) \cong \mathrm{Con}(\mathbf{A}^+)$ or $\mathrm{Con}(\mathbf{A}) \cong \mathrm{Con}(\mathbf{A}^-)$, but also disproves the conjecture that the embedding of Theorem 7.5 might at least preserve the monolith congruence (cf. [26, Corollary 5.4]).

(iii) $\Box 1 = 1$ *and* $\Box 0 = 0$.

(iv) $\Box(a \wedge b) = \Box(a \wedge^* b) = \Box a \wedge^* \Box b$.

(v) $\Box a = \Box\Box a$.

(vi) $a^* \leq \Box a = \Box(a^*)$.

(vii) $\Box(\sim a) = (\sim a)^*$.

(viii) $\Box(((\sim a)^*) \vee ((\sim b)^*)) = \Box(\sim(a \wedge b))$.

(ix) $\Box(\Box a \vee \Box b) = \Box(a \vee b)$.

Proof. (i). By Proposition 4.11.xii and Lemma 7.1.i, we have $\Box a = (\sim\sim a)^*$. The remaining equalities follow from the observation that $\sim\sim a \equiv \sim\sim(a^*)$ and $\sim\neg a \equiv \sim\neg(a^*)$ which are easily checked on twist-structures. We also check the following items on twist-structures.

(ii). Recalling that $\Box\langle a_+, a_-\rangle = \langle pn(a_+), n(\neg_+ pn(a_+))\rangle$, we have

$$\begin{aligned}\Box(\neg^*(\langle a_+, a_-\rangle^*)) &= \Box(\neg^*(\langle a_+, n(\neg_+ a_+\rangle)) \\ &= \Box(\langle \neg_+ a_+, n(a_+)\rangle^*) \\ &= \Box\langle \neg_+ a_+, n(\neg_+\neg_+ a_+)\rangle \\ &= \langle pn(\neg_+ a_+), n(\neg_+ pn(\neg_+ a_+))\rangle.\end{aligned}$$

Let us compute: $(\sim(\langle a_+, a_-\rangle^*))^* = (\sim\langle a_+, n(\neg_+ a_+)\rangle)^* = \langle pn(\neg_+ a_+), n(a_+)\rangle^* = \langle pn(\neg_+ a_+), n(\neg_+ pn(\neg_+ a_+))\rangle$. The first equality then follows. As to the second, let us compute:

$$\Box\neg\Box\langle a_+, a_-\rangle = \langle pn(\neg_+ pn(a_+)), n(\neg_+ pn(\neg_+ pn(a_+)))\rangle.$$

Recall from the proof of Proposition 3.4 that $\neg_+ a_+ = \neg_+ pn(a_+)$ for all $a_+ \in A_+$. Then $pn(\neg_+ a_+) = pn(\neg_+ pn(a_+))$, which entails

$$n(\neg_+ pn(\neg_+ a_+)) = n(\neg_+ pn(\neg_+ pn(a_+))),$$

as required.

(iii). Very easy.

(iv). Recall that, on a twist-structure, $\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle = \langle a_+ \wedge_+ b_+, a_- \vee_- b_-\rangle$ and $\langle a_+, a_-\rangle \wedge^* \langle b_+, b_-\rangle = \langle a_+ \wedge_+ b_+, n(\neg_+(a_+ \wedge_+ b_+))\rangle$. The first equality then simply follows from the observation that the $\Box$ operation only uses the first component of each pair. As to the second, we have $\Box(\langle a_+, a_-\rangle \wedge^* \langle b_+, b_-\rangle) = \Box(\langle a_+ \wedge_+$

$b_+, a_- \vee_- b_-\rangle^*) = \Box\langle a_+ \wedge_+ b_+, n(\neg_+(a_+ \wedge_+ b_+))\rangle = \Box\langle a_+ \wedge_+ b_+, n(\neg_+(a_+ \wedge_+ b_+))\rangle = \langle pn(a_+ \wedge_+ b_+), n(\neg_+(a_+ \wedge_+ b_+))\rangle$ Since p and n preserve finite meets, we also have $\Box a \wedge^* \Box b = (\langle pn(a_+), n(\neg_+ a_+)\rangle \wedge \langle pn(b_+), n(\neg_+ b_+)\rangle)^* = \langle pn(a_+) \wedge_+ pn(b_+), n(\neg_+ a_+) \vee_- n(\neg_+ b_+)\rangle^* = \langle pn(a_+) \wedge_+ pn(b_+), n(\neg_+ a_+) \vee_- n(\neg_+ b_+)\rangle^* = \langle pn(a_+ \wedge_+ b_+), n(\neg_+ a_+) \vee_- n(\neg_+ b_+)\rangle^* = \langle pn(a_+ \wedge_+ b_+), n(\neg_+ pn(a_+ \wedge_+ b_+))\rangle$. The first equality then follows from our earlier observation that $n(\neg_+ pn(c_+)) = n(\neg_+ c_+)$ for all $c_+ \in A_+$.

(v). We shall prove this directly: but note that it also follows (using the lattice properties) by item (ix) below. Let us compute:

$$\Box\Box\langle a_+, a_-\rangle = \Box\langle pn(a_+), n(\neg_+ a_+)\rangle = \langle pnpn(a_+), n(\neg_+ pn(a_+))\rangle.$$

Now $n \circ p = Id_{A_-}$ gives us $pnpn(a_+) = pn(a_+)$, and we have already observed that $n(\neg_+ pn(a_+)) = n(\neg_+ a_+)$. Thus the result follows.

(vi). The equality $\Box a = \Box(a^*)$ is very easily checked on a twist-structure: observe that the $\Box$ operator disregards the first component of each pair $\langle a_+, a_-\rangle$, and recall that $\langle a_+, a_-\rangle^* \langle a_+, n(\neg_+(a_+))\rangle$. As to the inequality $a^* \leq \Box a$, recall that $\langle a_+, a_-\rangle^* = \langle a_+, n(\neg_+ a_+)\rangle$. We thus need to check that $\langle a_+, n(\neg_+ a_+)\rangle \leq \langle pn(a_+), n(\neg_+ a_+)\rangle$, which follows from $Id_{A_+} \leq_+ p \circ n$.

(vii). By item (i) above and the semi-De Morgan identities, we have $\Box(\sim a) = (\sim\sim\sim a)^* = (\sim a)^*$.

(viii). Let us compute:

$$\begin{aligned}\Box(((\sim\langle a_+, a_-\rangle)^*) \vee ((\sim\langle b_+, b_-\rangle)^*)) &= \Box(\langle p(a_-), n(\neg_+ p(a_-)\rangle \vee \langle p(b_-), n(\neg_+ p(b_-)\rangle) \\ &= \langle pn(p(a_-) \vee_+ p(b_-)), n(\neg_+(p(a_-) \vee_+ p(b_-)))\rangle \\ &= \langle p(a_- \vee_- b_-)), n(\neg_+(p(a_-) \vee_+ p(b_-)))\rangle.\end{aligned}$$

The last equality holds because, using $n \circ p = Id_{A_-}$ and the fact that n preserves finite joins, $pn(p(a_-) \vee_+ p(b_-)) = p(np(a_-) \vee_- np(b_-)) = p(a_- \vee_- b_-)$. On the other hand, also using $n \circ p = Id_{A_-}$, we have $\Box(\sim(\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle)) = \Box\langle p(a_- \vee_- b_-), n(a_+ \wedge_+ b_+)\rangle = \langle pnp(a_- \vee_- b_-), n(\neg_+ p(a_- \vee_- b_-))\rangle = \langle p(a_- \vee_- b_-), n(\neg_+ p(a_- \vee_- b_-))\rangle$. Thus the first components are equal. As to the second ones, from $p(a_-) \vee_+ p(b_-) \leq_+ p(a_- \vee_- b_-)$ we get $\neg_+(p(a_- \vee_- b_-)) \leq_+ \neg_+(p(a_-) \vee_+ p(b_-))$ and $n(\neg_+(p(a_- \vee_- b_-))) \leq_- n(\neg_+(p(a_-) \vee_+ p(b_-)))$. To show $n(\neg_+(p(a_-) \vee_+ p(b_-))) \leq_- n(\neg_+(p(a_- \vee_- b_-)))$ it is sufficient (by monotonicity of n) to check that $\neg_+(p(a_-) \vee_+ p(b_-)) \leq_+ \neg_+(p(a_- \vee_- b_-))$. By the property of the pseudo-complement, this holds iff $p(a_- \vee_- b_-) \wedge_+ \neg_+(p(a_-) \vee_+ p(b_-)) = 0_+$. Observe that, using the semi-De Morgan identities (for $\neg_+$), we have $p(a_- \vee_- b_-) \wedge_+ \neg_+(p(a_-) \vee_+ p(b_-)) = p(a_- \vee_- b_-) \wedge_+ \neg_+ p(a_-) \wedge_+ \neg_+ p(b_-)$. Using $Id_{A_+} \leq_+ p \circ n$, the observation that p and n preserve finite meets and distributivity, we have $p(a_- \vee_- b_-) \wedge_+ \neg_+ p(a_-) \wedge_+ \neg_+ p(b_-) \leq_+ p(a_- \vee_- b_-) \wedge_+$

$pn(\neg_+ p(a_-) \wedge_+ \neg_+ p(b_-)) = p((a_- \vee_- b_-) \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-))) = p((a_- \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-))) \vee_- (b_- \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-))))$. Observe that, using $n \circ p = Id_{A_-}$ and the fact that n preserves finite meets (and the bottom element), we have $a_- \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-))) = np(a_-) \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-))) = n(p(a_-) \wedge_+ \neg_+ p(a_-) \wedge_+ \neg_+ p(b_-)) = n(0_+ \wedge_+ \neg_+ p(b_-)) = n(0_+) = 0_-$. In a similar way we obtain $b_- \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-)) = 0_-$. Thus $p((a_- \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-))) \vee_- (b_- \wedge_- n(\neg_+ p(a_-)) \wedge_- n(\neg_+ p(b_-)))) = p(0_- \vee_- 0_-) = 0_+$, which gives us the desired result.

(ix). Let us compute:

$$\begin{aligned}\Box(\Box\langle a_+, a_-\rangle \vee \Box\langle b_+, b_-\rangle) &= \Box\langle pn(a_+) \vee_+ pn(b_+), n(\neg_+ a_+) \wedge_- n(\neg_+ b_+)\rangle \\ &= \langle pn(pn(a_+) \vee_+ pn(b_+)), n(\neg_+(pn(a_+) \vee_+ pn(b_+)))\rangle\end{aligned}$$

and $\Box(\langle a_+, a_-\rangle \vee \langle b_+, b_-\rangle) = \langle pn(a_+ \vee_+ b_+), n(\neg_+(a_+ \vee_+ b_+))\rangle$. Recalling that n preserves finite joins and that $n \circ p = Id_{A_-}$, we have $pn(pn(a_+) \vee_+ pn(b_+)) = p(npn(a_+) \vee_- npn(b_+)) = p(n(a_+) \vee_- n(b_+)) = pn(a_+ \vee_+ b_+)$. Thus, the first components are equal. As to the second components, we can use the semi-De Morgan identities (for $\neg_+$) and the fact that n preserves finite meets to obtain $n(\neg_+(a_+ \vee_+ b_+)) = n(\neg_+ a_+ \wedge_+ \neg_+ b_+) = n(\neg_+ a_+) \wedge_- n(\neg_+ b_+)$ and, similarly, $n(\neg_+(pn(a_+) \vee_+ pn(b_+))) = n(\neg_+ pn(a_+)) \wedge_- n(\neg_+ pn(b_+))$. Then the result follows from our earlier observation (just after the definition of $\Box$) that $n(\neg_+ pn(c_+)) = n(\neg_+ c_+)$ for any $c_+ \in A_+$. □

Lemma 7.7. *Let* $\mathbf{A}$ *be a WPQK-algebra and* $\eta \in Con^{\Box}(\mathbf{A}^*)$. *Then the relation*

$$\eta_* := \{\langle a, b\rangle \in A \times A : \langle a^*, b^*\rangle, \langle(\sim a)^*, (\sim b)^*\rangle \in \eta\}$$

is a congruence of $\mathbf{A}$.

Proof. It is clear that η_* is an equivalence relation. We proceed to check the compatibility with the operations of $\mathbf{A}$.

($\sim$). Assume $\langle a, b\rangle \in \eta_*$, which means $\langle a^*, b^*\rangle$, $\langle(\sim a)^*, (\sim b)^*\rangle \in \eta$. Using Lemma 7.6.i, from the first assumption we can obtain

$$\langle \Box(a^*), \Box(b^*)\rangle = \langle(\sim\sim(a^*))^*, (\sim\sim(a^*))^*\rangle = \langle(\sim\sim a)^*, (\sim\sim a)^*\rangle \in \eta.$$

Thus $\langle \sim a, \sim b\rangle \in \eta_*$.

($\neg$). From the assumption $\langle a^*, b^*\rangle \in \eta$ we also have

$$\langle \neg^*(a^*), \neg^*(b^*)\rangle = \langle(\neg(a^*))^*, (\neg(b^*))^*\rangle = \langle(\neg a)^*, (\neg b)^*\rangle \in \eta,$$

the last equality holding by Lemma 7.1.v. That $\langle(\sim\sim a)^*, (\sim\sim a)^*\rangle \in \eta$ has been already established. By Proposition 4.11.xii, we have

$$\langle(\sim\sim a)^*, (\sim\sim a)^*\rangle = \langle(\sim\neg a)^*, (\sim\neg b)^*\rangle.$$

Thus $\langle(\sim\neg a)^*, (\sim\neg b)^*\rangle \in \eta$, which shows that $\langle\neg a, \neg b\rangle \in \eta_*$.

($\wedge$). Assuming $\langle a, b\rangle$, $\langle c, d\rangle \in \eta_*$, we have $\langle a^*, b^*\rangle$, $\langle(\sim a)^*, (\sim b)^*\rangle$, $\langle c^*, d^*\rangle$, $\langle(\sim c)^*, (\sim d)^*\rangle \in \eta$. Using Lemma 7.1.iv, from $\langle a^*, b^*\rangle, \langle c^*, d^*\rangle \in \eta$ we obtain $\langle(a^*) \wedge^* (c^*), (b^*) \wedge^* (d^*)\rangle = \langle((a^*) \wedge (c^*))^*, ((b^*) \wedge (d^*))^*\rangle = \langle(a \wedge c)^*, (b \wedge d)^*\rangle \in \eta$. Using Lemma 7.1.iii, from $\langle(\sim a)^*, (\sim b)^*\rangle, \langle(\sim c)^*, (\sim d)^*\rangle \in \eta$ we obtain $\langle((\sim a)^*) \vee^* ((\sim c)^*), ((\sim b)^*) \vee^* ((\sim d)^*)\rangle = \langle(((\sim a)^*) \vee ((\sim c)^*))^*, (((\sim b)^*) \vee ((\sim d)^*)^*\rangle = \langle(\sim a \vee \sim c)^*, (\sim b \vee \sim d)^*\rangle \in \eta$. From this we have $\langle\Box((\sim a \vee \sim c)^*), \Box((\sim b \vee \sim d)^*)\rangle = \langle(\sim\neg((\sim a \vee \sim c)^*))^*, (\sim\neg((\sim b \vee \sim d)^*))^*\rangle \in \eta$. By Lemma 7.1.vii, we have that $\langle(\sim\neg((\sim a \vee \sim c)^*))^*, (\sim\neg((\sim b \vee \sim d)^*))^*\rangle = \langle(\sim\sim((\sim a \vee \sim c)^*))^*, (\sim\sim((\sim b \vee \sim d)^*))^*\rangle$. By Lemma 7.6.i, we have $\langle(\sim\sim((\sim a \vee \sim c)^*))^*, (\sim\sim((\sim b \vee \sim d)^*))^*\rangle = \langle(\sim\sim(\sim a \vee \sim c))^*, (\sim\sim(\sim b \vee \sim d))^*\rangle$. Observe that, by the semi-De Morgan identities, we have $\sim\sim(\sim a \vee \sim c) = \sim(\sim\sim a \wedge \sim\sim c) = \sim\sim\sim(a \wedge c) = \sim(a \wedge c)$ and similarly $\sim\sim(\sim b \vee \sim d) = \sim(b \wedge d)$. Then $\langle(\sim(a \wedge c))^*, (\sim(b \wedge d))^*\rangle \in \eta$, which together with $\langle(a \wedge c)^*, (b \wedge d)^*\rangle \in \eta$ give us $\langle a \wedge c, b \wedge d\rangle \in \eta_*$, as required.

($\vee$). Using Lemma 7.1.iii, from the assumptions $\langle a^*, b^*\rangle$, and $\langle c^*, d^*\rangle \in \eta$ we get $\langle(a^*) \vee^* (c^*), (b^*) \vee^* (d^*)\rangle = \langle((a^*) \vee (c^*))^*, ((b^*) \vee (d^*))^*\rangle = \langle(a \vee c)^*, (b \vee d)^*\rangle \in \eta$. Using Lemma 7.1.iv, from the assumptions $\langle(\sim a)^*, (\sim b)^*\rangle$, $\langle(\sim c)^*, (\sim d)^*\rangle \in \eta$ we have $\langle((\sim a)^*) \wedge^* ((\sim c)^*), ((\sim b)^*) \wedge^* ((\sim d)^*)\rangle = \langle(((\sim a)^*) \wedge ((\sim c)^*))^*, (((\sim b)^*) \wedge^* ((\sim d)^*))^*\rangle = \langle(\sim a \wedge \sim c)^*, (\sim b \wedge \sim d)^*\rangle \in \eta$. By the semi-De Morgan identities, $\sim a \wedge \sim c = \sim(a \vee c)$ and $\sim b \wedge \sim d = \sim(b \vee d)$. Hence, $\langle(\sim(a \vee c))^*, (\sim(b \vee d))^*\rangle \in \eta$, which gives us $\langle a \vee c, b \vee d\rangle \in \eta_*$, as required. □

Theorem 7.8. *For every WPQK-algebra* $\mathbf{A}$*, the lattice* $Con(\mathbf{A})$ *is isomorphic to the lattice* $Con^{\Box}(\mathbf{A}^*)$ *via the mutually inverse maps* $(.)^*$ *and* $(.)_*$ *defined as follows:*

for $\theta \in Con(\mathbf{A})$*, let* $\theta^* := \theta \cap (A^* \times A^*)$*;*

for $\eta \in Con^{\Box}(\mathbf{A}^*)$ *and* $a, b \in A$*,* $\langle a, b\rangle \in \eta_*$ *iff* $\langle a^*, b^*\rangle, \langle(\sim a)^*, (\sim b)^*\rangle \in \eta$*.*

Proof. We have seen in Theorem 7.5 that the map $(.)^*$ is order-preserving, order-reflecting and injective. We have also observed earlier that $\theta^* \in \mathrm{Con}^{\Box}(\mathbf{A}^*)$ for all $\theta \in \mathrm{Con}(\mathbf{A})$. It remains to show that, if the codomain is $\mathrm{Con}^{\Box}(\mathbf{A}^*)$, then $(.)^*$ is onto. We will use the inverse map $(.)_*$ defined above.

By Lemma 7.7 we have $\eta_* \in \mathrm{Con}(\mathbf{A})$ for all $\eta \in \mathrm{Con}^{\Box}(\mathbf{A}^*)$. Let us check that $\eta = (\eta_*)^*$. Let $a, b \in A^*$. Observe that, by Lemma 7.1.ix, we have $a^* = a$ and $b^* = b$. Now, $\langle a, b\rangle \in (\eta_*)^*$ holds iff $\langle a, b\rangle \in \eta_*$ iff $\langle a^*, b^*\rangle = \langle a, b\rangle, \langle(\sim a)^*, (\sim b)^*\rangle \in \eta$. It is thus clear that $(\eta_*)^* \subseteq \eta$. Conversely, assume $\langle a, b\rangle = \langle a^*, b^*\rangle \in \eta$. Then

$\langle \neg^*(a^*), \neg^*(b^*)\rangle \in \eta$, from which we can also obtain $\langle \Box(\neg^*(a^*)), \Box(\neg^*(b^*))\rangle \in \eta$. By Lemma 7.6.ii, we have $\langle \Box(\neg^*(a^*)), \Box(\neg^*(b^*))\rangle = \langle (\sim(a^*))^*, (\sim(b^*))^*\rangle$. Thus $\langle (\sim(a^*))^*, (\sim(b^*))^*\rangle = \langle (\sim a)^*, (\sim b)^*\rangle \in \eta$, which entails $\eta \subseteq (\eta_*)^*$. □

We have seen (Figures 1 and 2) that a WPQK-algebra $\mathbf{A} \leq \mathbf{A}_+ \bowtie \mathbf{A}_-$ may be subdirectly irreducible even if neither $\mathbf{A}_+ (\cong \mathbf{A}^*)$ nor $\mathbf{A}_-$ (viewed as either p-lattices or lattices) are subdirectly irreducible. Theorem 7.8 can however be used to obtain a sufficient condition for a WPQK-algebra $\mathbf{A}$ to be subdirectly irreducible.

Corollary 7.9. *Let $\mathbf{A}$ be a WPQK-algebra, with $\mathbf{A}^*$ a subdirectly irreducible p-lattice. Then $\mathbf{A}$ is subdirectly irreducible.*

Proof. By [13, Theorem 2], every subdirectly irreducible p-lattice $\mathbf{A}^*$ is obtained by adding a new top element 1 to a Boolean lattice. Then, in particular, $\mathbf{A}^*$ has a unique co-atom c and the monolith congruence $\theta \in \mathrm{Con}(\mathbf{A}^*)$ is given by $\theta = \{\langle a, b\rangle \in \mathbf{A}^* \times \mathbf{A}^* : a = b \text{ or } a, b \in \{c, 1\}\}$. Using this description, it is not difficult to check that $\theta \in \mathrm{Con}^{\Box}(\mathbf{A}^*)$. Indeed, if $\langle a, b\rangle \in \theta$, then either $a = b$ (in which case $\Box a = \Box b$ and so $\langle \Box a, \Box b\rangle \in \theta$), or $a = c$ and $b = 1$. By items (iii) and (vi) of Lemma 7.6, we have $c \leq \Box c \leq \Box 1 = 1$. Hence, $\Box c \in \{c, 1\}$ and $\langle \Box c, \Box 1\rangle = \langle \Box c, 1\rangle \in \theta$, as required. By Theorem 7.8, this entails that θ_* is the monolith congruence of $\mathbf{A}$. Thus $\mathbf{A}$ is subdirectly irreducible. □

Theorem 7.8 (also bearing in mind Proposition 7.3) seems to suggest that, as far as congruences are concerned, a more faithful counterpart of a WPQK-algebra $\mathbf{A}$ would be the enriched algebra $\langle \mathbf{A}^*, \Box\rangle$ rather than the p-lattice $\mathbf{A}^*$ (alias $\mathbf{A}_+$). We will make this intuition precise in the next section. For the time being, we demonstrate that the map $\Box$ gives us the opportunity to state a result concerning the other factor ($\mathbf{A}_-$) that is an analogue to Proposition 7.3.

Given a WPQK-algebra $\mathbf{A}$, define:

$$A^{\Box} := \{\Box a : a \in A\}.$$

Observe that, since $\Box a = (\sim \neg a)^*$, we have $A^{\Box} \subseteq A^*$. We define operations on $A^{\Box}$ as follows: for all $a, b \in A^{\Box}$,

$$a \wedge^{\Box} b := \Box(a \wedge^* b) = \Box a \wedge^* \Box b = a \wedge^* b \qquad \text{(Lemma 7.6.iv and .v)}$$

$$a \vee^{\Box} b := \Box(a \vee b)$$

$$0^{\Box} := \Box 0 = 0 \qquad \text{(Lemma 7.6.iii)}$$

$$1^{\Box} := \Box 1 = 1 \qquad \text{(Lemma 7.6.iii).}$$

$$\neg^{\Box} a := \Box \neg a \qquad \text{(Lemma 7.6.iii).}$$

Proposition 7.10. *For every WPQK-algebra* $\mathbf{A}$*, the map* $\beta\colon A_- \to A^{\Box}$ *given by* $\beta([\sim a]) = \Box \sim a$ *for all* $a \in A$ *is a p-lattice isomorphism between* $\mathbf{A}_-$ *and* $\mathbf{A}^{\Box}$ *(hence,* $\mathbf{A}^{\Box}$ *is a p-lattice).*

Proof. To improve readability, we write $\beta[a]$ instead of $\beta([a])$. Let us preliminarily observe that, by Lemma 7.6.vii, we have $\beta[\sim a] = \Box \sim a = (\sim a)^*$ for all $a \in A$. By Lemma 7.1.i, we also have $\sim a \equiv \sim b$ iff $(\sim a)^* \equiv (\sim b)^*$ for all $a, b \in A$. This means that $\beta[\sim a] = \beta[\sim b]$ iff $[\sim a] = [\sim b]$. Thus β is a well-defined and injective map. Surjectivity is also easily verified. Indeed, if $a \in A^{\Box}$, then $a = \Box b = (\sim \neg b)^* = \beta[\sim \neg b]$ for $[\sim \neg b] \in A_-$. Let us check that the lattice operations are preserved. The case of the constants is straightforward. Using Lemma 7.1.iv and the semi-De Morgan identities, we have $\beta([\sim a] \wedge_- [\sim b]) = \beta([\sim a \wedge \sim b]) = \beta[\sim(a \vee b)] = (\sim(a \vee b))^* = (\sim a \wedge \sim b)^* = ((\sim a)^* \wedge (\sim b)^*)^* = (\sim a)^* \wedge^* (\sim b)^* = \beta[\sim a] \wedge^{\Box} \beta[\sim b]$. Using Lemma 7.6.viii, we have $\beta([\sim a] \vee_- [\sim b]) = \beta[\sim(a \wedge b)] = \Box(\sim(a \wedge b)) = \Box(((\sim a)^*) \vee ((\sim b)^*)) = ((\sim a)^*) \vee^{\Box} ((\sim b)^*) = \beta[\sim a] \vee^{\Box} \beta[\sim b]$. Regarding the pseudo-complement operation, observe that, by Lemma 7.1.v, we have $\neg \sim a = \neg((\sim a)^*)$ for all $a \in A$. This entails $\Box \neg \sim a = \Box \neg((\sim a)^*)$, which gives us $\beta(\neg_-[\sim a]) = \beta[\neg \sim a] = \Box \neg \sim a = \Box \neg((\sim a)^*) = \neg^{\Box}((\sim a)^*) = \neg^{\Box} \beta[\sim a]$, as required. □

Joining Proposition 7.10 with Proposition 7.3 and Theorem 4.10, we can restate the twist representation result for WPQK-algebras replacing $\mathbf{A}_+$ and $\mathbf{A}_-$ by their internalised alter egos $\mathbf{A}^*$ and $\mathbf{A}^{\Box}$ (Theorem 7.11 below). Indeed, it suffices to find suitable counterparts of the maps $n\colon A_+ \to A_-$ and $p\colon A_- \to A_+$. It is easy to check that these are, respectively, the map $\Box\colon A^* \to A^{\Box}$ and the identity map on $A^{\Box}$.

Theorem 7.11. *Every WPQK-algebra* $\mathbf{A}$ *is isomorphic to a WPQK twist-structure over* $\mathbf{A}^* \bowtie \mathbf{A}^{\Box}$ *through the map* $\phi\colon A \to A^* \times A^{\Box}$ *given by* $\phi(a) := \langle a^*, (\sim a)^* \rangle$ *for all* $a \in A$*.*

Observe that on a *wp*-Kleene algebra $\mathbf{A}$ (by Lemma 7.1.ix) we have $\Box a = a^{**} = a^*$ for all $a \in A$. Thus $\mathbf{A}^* = \mathbf{A}^{\Box}$ and Theorem 7.11 gives us precisely Sendlewski's representation result.

Remark 7.12. Since every quasi-Nelson algebra $\mathbf{A}$ has a WPQK-algebra reduct (Proposition 4.4), we can consider the corresponding *p*-skeleton $\mathbf{A}^*$ defined as before.

In this case, upon defining $a \to^* b := (a \to b)^*$ for all $a, b \in A^*$, we have that $\langle \mathbf{A}, \to^* \rangle$ is a Heyting algebra isomorphic to the factor $\mathbf{A}_+$ given by the twist-representation (cf. Definition 2.5). Similarly, the algebra $\mathbf{A}^\Box$ can be endowed with an implication given by $a \to^\Box b := \Box(a \to b)$ for all $a, b \in A^\Box$ so that $\langle \mathbf{A}^\Box, \to^\Box \rangle$ is a Heyting algebra isomorphic to $\mathbf{A}_-$. Then, defining the maps $n\colon A^* \to A^\Box$ and $p\colon A^\Box \to A^*$ as for WPQK-algebras, we can obtain an alternative representation for quasi-Nelson algebras analogue to Theorem 7.11.

At this point we could (if we wished to) use Theorem 7.11 to rewrite Theorem 6.2 replacing $\mathbf{A}_+$ and $\mathbf{A}_-$ by $\mathbf{A}^*$ and $\mathbf{A}^\Box$. A more interesting observation is that, for the purpose of the representation, we can altogether dispense with the second factor (whether we call it $\mathbf{A}_-$ or $\mathbf{A}^\Box$). We will illustrate this in the next section; but before we move on to this, one might wonder, is there anything interesting we can say about the congruences of $\mathbf{A}^\Box$?

Proposition 7.13. *For every WPQK-algebra* $\mathbf{A}$*, the lattice* $Con(\mathbf{A}^\Box)$*, where is* $\mathbf{A}^\Box$ *is viewed as a p-lattice, is embeddable into* $\mathrm{Con}^\Box(\mathbf{A}^*)$*, and thus also into* $Con(\mathbf{A}^*)$*, via the map* $(.)^\Box$ *given, for all* $\theta \in Con(\mathbf{A}^\Box)$*, by*

$$\theta^\Box := \{\langle a, b\rangle \in A^* \times A^* : \langle \Box a, \Box b\rangle \in \theta\}.$$

The embedding $(.)^\Box$ *preserves the greatest but not necessarily the least element.*

Proof. It is clear that the map $(.)^\Box$ preserves the top element; that the least element is not necessarily preserved follows from the example shown earlier on Figure 2. The map $(.)^\Box$ is clearly order-preserving, and it is easy to see that it is also order-reflecting (hence, injective). To check this, assume $\theta^\Box \subseteq \eta^\Box$ for some $\theta, \eta \in \mathrm{Con}(\mathbf{A}^\Box)$ and let $\langle a, b\rangle \in \theta$ for some $a, b \in A^\Box$. Then $a = \Box a'$ and $b = \Box b'$ for some $a', b' \in A$ and, by Proposition 7.6.v, $\Box\Box a' = \Box a'$ and $\Box\Box b' = \Box b'$. Hence, $\Box a = a$ and $\Box b = b$. Thus $\langle a, b\rangle \in \theta$ is equivalent to $\langle \Box a, \Box b\rangle \in \theta$, which implies $\langle a, b\rangle \in \theta^\Box$. Then $\langle a, b\rangle \in \eta^\Box$, that is, $\langle \Box a, \Box b\rangle = \langle a, b\rangle \in \eta$. Thus $\theta \subseteq \eta$, as claimed. It remains to check that $\theta^\Box \in \mathrm{Con}^\Box(\mathbf{A}^*)$ for all $\theta \in \mathrm{Con}(\mathbf{A}^\Box)$. It is clear that $\theta^\Box \in \mathrm{Con}(\mathbf{A}^*)$ is an equivalence relation. Also observe that, if we check that $\theta^\Box \in \mathrm{Con}(\mathbf{A}^*)$, then $\theta^\Box \in \mathrm{Con}^\Box(\mathbf{A}^*)$ will immediately follow. Indeed, by the definition of $\theta^\Box$, we have $\langle a, b\rangle \in \theta^\Box$ iff (by Lemma 7.6.v) $\langle \Box a, \Box b\rangle = \langle \Box\Box a, \Box\Box b\rangle \in \theta$, and so $\langle \Box a, \Box b\rangle \in \theta^\Box$. Let us check that $\theta^\Box$ is compatible with the pseudo-complement operation. Let $a, b \in A^*$ be such that $\langle a, b\rangle \in \theta^\Box$, i.e. $\langle \Box a, \Box b\rangle \in \theta$. Then, by the compatibility of θ with $\neg^\Box$, we have $\langle \neg^\Box\Box a, \neg^\Box\Box b\rangle = \langle \Box\neg\Box a, \Box\neg\Box b\rangle \in \theta$. By Lemma 7.6.ii we have $\Box\neg\Box a = \Box(\neg^*(a^*))$ and likewise $\Box\neg\Box b = \Box(\neg^*(b^*))$. Then $\langle \Box(\neg^*(a^*)), \Box(\neg^*(b^*))\rangle \in \theta$. Since $a, b \in A^*$, we also have $a^* = a$ and $b^* = b$ (Lemma 7.1.ix). Hence, $\langle \Box(\neg^*(a^*)), \Box(\neg^*(b^*))\rangle = \langle \Box(\neg^* a), \Box(\neg^* b)\rangle \in \theta$, that is,

$\langle \neg^* a, \neg^* b\rangle \in \theta^\Box$. We next check that $\theta^\Box$ is compatible with the lattice operations. Assume $\langle a, b\rangle, \langle c, d\rangle \in \theta^\Box$ for $a, b, c, d \in A^*$, i.e. $\langle \Box a, \Box b\rangle, \langle \Box c, \Box d\rangle \in \theta$. Then we have $\langle \Box a \wedge^\Box \Box c, \Box b \wedge^\Box \Box d\rangle = \langle \Box(a \wedge c), \Box(b \wedge d)\rangle \in \theta$. By Lemma 7.6.iv,

$$\langle \Box(a \wedge c), \Box(b \wedge d)\rangle = \langle \Box(a \wedge^* c), \Box(b \wedge^* d)\rangle \in \theta,$$

that is, $\langle a \wedge^* c, b \wedge^* d\rangle \in \theta^\Box$. This settles the case of the meet; as to the join, the assumptions give us $\langle \Box a \vee^\Box \Box c, \Box b \vee^\Box \Box d\rangle = \langle \Box(a \vee c), \Box(b \vee d)\rangle \in \theta$. By Lemma 7.1.iii we have $a \vee c = a \vee^* c$ and $b \vee d = b \vee^* d$. Then the result follows. □

Recalling Theorem 7.8, we see that Proposition 7.13 immediately entails the following result.

Corollary 7.14. *For every WPQK-algebra* $\mathbf{A}$*, the lattice* $Con(\mathbf{A}^\Box)$*, where is* $\mathbf{A}^\Box$ *is viewed as a p-lattice, is embeddable into* $\mathrm{Con}(\mathbf{A})$*. The embedding preserves the greatest but not necessarily the least element.*

8 An Alternative Representation: Nuclear p-Lattices

Definition 8.1. We shall call *nuclear p-lattice* (*np*-lattice for short) an algebra $\mathbf{A} = \langle A; \wedge, \vee, \neg, \Box, 0, 1\rangle$ of type $\langle 2, 2, 1, 1, 0, 0\rangle$ such that:

(i) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ is a p-lattice (with order $\leq$).

(ii) The operator $\Box$ is a *nucleus* on A, that is, for all $a, b, c, d \in A$,

(1) $\Box 0 = 0$

(2) $\Box(a \wedge b) = \Box a \wedge \Box b$

(3) $a \leq \Box a = \Box\Box a$.

An example of an *np*-lattice (indeed, *the* intended example for us) is the algebra $\langle \mathbf{A}^*, \Box\rangle$ considered in the preceding subsection. Equivalently, one may think of the p-lattice $\mathbf{A}_+ = \langle A_+; \wedge_+, \vee_+, \neg_+, 0_+, 1_+\rangle$ introduced in Definition 3.1 enriched with an operation $\Box$ given by $\Box a_+ := pn(a_+)$ for all $a_+ \in A_+$. More generally, any p-lattice $\mathbf{A}$ may be viewed as an *np*-lattice if one lets $\Box a := \neg\neg a$ for all $a \in A$.

The properties introduced in Definition 8.1 are precisely saying that the $\Box$ operator is a (dense) *nucleus* in the sense of e.g. [3]. Nuclei are well studied in the context of Heyting algebras and residuated lattices (concerning the latter, several results can be found in [5]). The paper [7] is also relevant, for the authors introduce a representation of Sugihara monoids (the algebraic counterpart of relevance logic $\mathcal{RM}^t$) as twist-structures over nuclear (semi-linear) Heyting algebras.

Remark 8.2. Every *np*-lattice $\mathbf{A}$ satisfies $\Box 1 = 1$ (since item ii.3 implies $1 \leq \Box 1$) and $\Box(\Box a \vee \Box b) = \Box(a \vee b)$ for all $a, b \in A$ (cf. Lemma 7.6.ix). Indeed, since $\Box$ is order-preserving (by item ii.2), from $a, b \leq a \vee b$ we have $\Box a, \Box b \leq \Box(a \vee b)$ and $\Box a \vee \Box b \leq \Box(a \vee b)$. Using also item ii.3, we have $\Box(\Box a \vee \Box b) \leq \Box\Box(a \vee b) = \Box(a \vee b)$. On the other hand, from $a \leq \Box a$ and $b \leq \Box b$ we have $a \vee b \leq \Box a \vee \Box b$, so $\Box(a \vee b) \leq \Box(\Box a \vee \Box b)$.

Proposition 8.3. *For every WPQK-algebra* $\mathbf{A}$*, the algebra* $\langle \mathbf{A}^*, \Box \rangle$ *is an np-lattice.*

Proof. We have seen in Proposition 7.3 that $\mathbf{A}^*$ is a *p*-lattice. The remaining properties of Definition 8.1 are proven in Lemma 7.6 (precisely, in items (iii) to (vi) of the Lemma). □

Given an *np*-lattice $\mathbf{A} = \langle A; \wedge, \vee, \neg, \Box, 0, 1 \rangle$, we proceed to define an algebra $\mathbf{A}^{\Box} = \langle A^{\Box}; \wedge^{\Box}, \vee^{\Box}, 0^{\Box}, 1^{\Box} \rangle$, following the intuitions gathered in the preceding subsection. We let

$$A^{\Box} := \{\Box a : a \in A\}$$

and define operations on $A^{\Box}$ as follows: for all $a, b \in A^{\Box}$,

$$a \wedge^{\Box} b := \Box(a \wedge b) = \Box a \wedge \Box b = a \wedge b \qquad \text{(by Def. 8.1.ii.3)}$$

$$a \vee^{\Box} b := \Box(a \vee b)$$

$$0^{\Box} := \Box 0 = 0$$

$$1^{\Box} := \Box 1 = 1.$$

Proposition 8.4. *Let* $\mathbf{A}$ *be an np-lattice.*

(i) The map $\Box : A \to A^{\Box}$ *is a (surjective) bounded lattice homomorphism between* $\mathbf{A}$ *and* $\mathbf{A}^{\Box}$ *(thus* $\mathbf{A}^{\Box}$ *is a bounded distributive lattice). Furthermore, defining* $\neg^{\Box} a := \Box\neg a$*, we have that* $\mathbf{A}^{\Box}$ *is a p-lattice and* $\Box$ *a p-lattice homomorphism.*

(ii) The identity map $Id_{A^{\Box}} : A^{\Box} \to A$ *preserves finite meets and the lattice bounds.*

(iii) $\Box \circ Id_{A^{\Box}} = Id_{A^{\Box}}$ *and* $Id_A \leq Id_{A^{\Box}} \circ \Box$*.*

Proof. (i). It is clear that the map $\Box$ is surjective. Also, by Definition 8.1.ii.1, the lattice bounds are preserved. The meet is preserved by Definition 8.1.ii.2. As to the join, by Remark 8.2, we have $\Box(a \vee b) = \Box(\Box a \vee \Box b) = \Box a \vee^{\Box} \Box b$. Let us check that $\Box\neg a$ is the pseudo-complement in $\mathbf{A}^{\Box}$ of each $a \in A^{\Box}$. Observe that

$a \wedge \Box\neg a = \Box a \wedge \Box\neg a = \Box(a \wedge \neg a) = \Box 0 = 0$. Further, suppose $a \wedge b = 0$ for some $b \in A^{\Box}$. Then $b \leq \neg a$, so $b \wedge \Box\neg a = \Box b \wedge \Box\neg a = \Box(b \wedge \neg a) = \Box b = b$. So $b \leq \Box\neg a$, as required.

(ii). It is clear that $Id_{A^{\Box}}$ preserves the bounds. Regarding the meet, let $a, b \in A^{\Box}$. Then $a = \Box a'$ and $b = \Box b'$ for some $a', b' \in A$. Then, using Definition 8.1.ii.2 and ii.3, we have $Id_{A^{\Box}}(a \wedge^{\Box} b) = Id_{A^{\Box}}(\Box a' \wedge^{\Box} \Box b') = \Box(\Box a' \wedge \Box b') = \Box\Box a' \wedge \Box\Box b' = \Box a' \wedge \Box b' = a \wedge b = Id_{A^{\Box}}(a) \wedge Id_{A^{\Box}}(b)$. Observe that joins are not necessarily preserved, for in general one may have $Id_{A^{\Box}}(a \vee^{\Box} b) = Id_{A^{\Box}}(\Box a' \vee^{\Box} \Box b') = \Box(\Box a' \vee \Box b') = \Box(a' \vee b') \neq \Box a' \vee \Box b' = a \vee b = Id_{A^{\Box}}(a) \vee Id_{A^{\Box}}(b)$.

(iii). Let $a \in A^{\Box}$, so that $a = \Box a'$ for some $a' \in A$. Using Definition 8.1.ii.3, we have $(\Box \circ Id_{A^{\Box}})(a) = (\Box \circ Id_{A^{\Box}})(\Box a') = \Box\Box a' = \Box a' = a$. For $a \in A$, using Definition 8.1.ii.3 we have $a \leq \Box a = (Id_{A^{\Box}} \circ \Box)(a)$. □

By Proposition 8.4, every *np*-lattice $\mathbf{A}$ determines the *p*-lattice $\mathbf{A}^{\Box}$ as well as maps $\Box : A \to A^{\Box}$ and $Id_{A^{\Box}} : A^{\Box} \to A$ which satisfy the properties of Definition 3.1. Thus, we have a twist-structure $\mathbf{A} \bowtie \mathbf{A}^{\Box}$, that we may just denote by $Tw(\mathbf{A})$, since it is completely determined by $\mathbf{A}$. Moreover, by Theorem 7.11, every WPQK-algebra is representable as a twist-structure of this type. We state this formally in the next theorem.

Theorem 8.5. *Every WPQK-algebra* $\mathbf{A}$ *is isomorphic to a WPQK twist-structure over the np-lattice* $\langle \mathbf{A}^*, \Box \rangle$ *through the map* $\phi\colon A \to A^* \times A^{\Box}$ *given by* $\phi(a) := \langle a^*, (\sim a)^* \rangle$ *for all* $a \in A$.

Recalling Theorem 7.8, we immediately obtain the following result.

Corollary 8.6. *For every WPQK-algebra* $\mathbf{A}$*, the lattice* $Con(\mathbf{A})$ *is isomorphic to the congruence lattice of the corresponding np-lattice* $\langle \mathbf{A}^*, \Box \rangle$.

Corollary 8.6 indicates that, in order to obtain a better characterisation of congruence lattices of WPQK-algebras, we need to study the congruences of *np*-lattices; we leave this as a suggestion for future research.

Theorem 8.5 can obviously be refined by considering the filter $\nabla_{\mathbf{A}} \subseteq A^*$, obtaining an analogue of Theorem 6.2: every WPQK-algebra is representable as a twist-structure $Tw(\mathbf{A}^*, \nabla_{\mathbf{A}})$, where $\mathbf{A}^*$ is an *np*-lattice and $\nabla_{\mathbf{A}}$ is a filter containing the dense elements of $\mathbf{A}^*$. It is also easy to observe that a WPQK-algebra $\mathbf{A}$ is a *wp*-Kleene algebra (Definition 4.14) if and only if the $\Box$ operator on the corresponding *np*-lattice $\langle \mathbf{A}^*, \Box \rangle$ is 'trivial', that is, if $\Box a = a$ for all $a \in A^*$. In such a case we have $\mathrm{Con}(\mathbf{A}^*) = \mathrm{Con}(\langle \mathbf{A}^*, \Box \rangle) \cong \mathrm{Con}(\mathbf{A})$, thus recovering Sendlewski's result [26, Theorem 5.2].

Given the preceding considerations and the close relationship between WPQK- and quasi-Nelson algebras (Section 5), one may wonder whether the 'modal' (or 'nuclear') approach might provide further insight on quasi-Nelson algebras[7]. This may well be the case; but observe that, as far as congruences are concerned, on a quasi-Nelson algebra one can prove that $\mathrm{Con}(\mathbf{A}_+) \cong \mathrm{Con}(\mathbf{A})$ [23, Proposition 8]. This entails that the $\Box$ operator on $\mathbf{A}_+$ (if one were to define it) will have no impact on the congruences of (the $\Box$-free reduct of) $\mathbf{A}_+$.

9 Subvarieties of WPQK-Algebras

In the same way as quasi-Nelson algebras can be viewed as a common generalisation of Heyting and Nelson algebras, WPQK-algebras can be viewed as a common generalisation of *p*-lattices and *wp*-Kleene algebras. Because of this generality, the task of describing the lattice of sub-(quasi-)varieties of WPQK-algebras cannot be expected to be an easy one, and we will not address it in this paper. However, we are going to demonstrate how Theorem 6.2 can be employed to characterise certain subvarieties.

Recall from [24] that a semi-De Morgan algebra $\langle A; \wedge, \vee, \sim\rangle$ is a called a *demi-p-lattice* if it satisfies the identity $\sim x \wedge \sim\sim x \approx 0$. An *almost p-lattice* is a demi-*p*-lattice (or, equivalently, a semi-De Morgan algebra) that further satisfies $x \wedge \sim x \approx 0$. A *p*-lattice is a demi-*p*-lattice that is also a lower quasi-De Morgan algebra, i.e. one that satisfies $x \ll \sim\sim x$. Alternatively, one can define a *p*-lattice as a semi-De Morgan algebra that satisfies $x \wedge \sim(x \wedge y) \approx x \wedge \sim y$ (see [24] for proofs of these results). Last but not least, a *Stone lattice* is a *p*-lattice satisfying $\sim x \vee \sim\sim x \approx 1$.

Given a WPQK-algebra $\mathbf{A}$, in general it makes sense to ask (1) when the $\sim$-free reduct of $\mathbf{A}$ is in the above classes, as well as (2) when the same happens with the $\neg$-free reduct. In the following propositions we provide a number of equivalent conditions/characterisations.

Proposition 9.1. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \sim(x \wedge y) \approx \sim x \vee \sim y$, *(i.e.* $\langle A; \wedge, \vee, \sim, 0, 1\rangle$, *is an Ockham algebra)*

(ii) $\mathbf{A} \models \sim(x \wedge y) \ll \sim x \vee \sim y$,

[7] Indeed, the algebra $\langle \mathbf{A}_+, \Box\rangle$ corresponding to a quasi-Nelson algebra $\mathbf{A}$ via the twist representation will be precisely a Heyting algebra with a nucleus of the type considered in [3], which suggests a connection with the work of Bezhanishivli and Ghilardi that may be worthwhile exploring in future research (see [21]). The isomorphism $\mathrm{Con}(\mathbf{A}_+) \cong \mathrm{Con}(\mathbf{A})$ can also be obtained as a corollary of the general theory of nuclei on residuated lattices [7, Theorem 7.1].

(iii) p *preserves finite joins.*

Proof. The equivalence between (i) and (ii) holds on every semi-De Morgan algebra. That (i) is equivalent to $p(a_- \vee_- b_-) = p(a_-) \vee_+ p(b_-)$ is a matter of routine checking on a twist-structure. □

Proposition 9.2. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \sim\sim x \wedge \sim x \approx 0$, *(*$\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *is a demi-p-lattice)*

(ii) $\mathbf{A} \models x \wedge \neg x \approx 0$, *(*$\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is an almost-p-lattice)*

(iii) $\mathbf{A} \models x \wedge \sim x \approx 0$, *(*$\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *is an almost-p-lattice)*

(iv) $\mathbf{A} \models x \wedge \sim(x \wedge y) \approx x \wedge \sim y$, *(*$\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *is a p-lattice)*

(v) $\mathbf{A} \models \neg x \ll \sim x$,

(vi) $\mathbf{A} \models \neg x \approx \sim x$, *(*$\langle A; \wedge, \vee, \neg, 0, 1\rangle = \langle A; \wedge, \vee, \sim, 0, 1\rangle$*)*

(vii) $\mathbf{A} \models x \ll \neg\neg x$,

(viii) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is a quasi-Kleene algebra (Definition 2.4),*

(ix) $\neg_+ a_+ \leq_+ p(a_-)$ *for all* $\langle a_+, a_-\rangle \in A$,

(x) $\neg_+ a_+ = p(a_-)$ *for all* $\langle a_+, a_-\rangle \in A$,

(xi) $n(\nabla) = 1_-$,

(xii) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is p-lattice and* $A = A^*$.

Proof. We have seen in Proposition 4.11 that the following identities hold on every WPQK-algebra:

$$\sim\sim x \wedge \sim x \approx x \wedge \neg x \approx x \wedge \sim x.$$

This immediately implies that items (i)–(iii) are all equivalent. By Sankappanavar's results [24], a lower quasi-De Morgan algebra satisfying (iii) must also satisfy (iv). Similarly, a semi-De Morgan algebra satisfying (iv) is a p-lattice and must therefore satisfy (iii). This shows the equivalence of (i)–(iv).

Now assume (iv). Then $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ is a p-lattice where $\sim$ is the pseudo-complement operation and, since we have shown that (iv) is equivalent to (ii), we also have $\neg a \wedge a = 0$ for all $a \in A$. Then, by the property of the pseudo-complement, we have $\neg a \leq \sim a$. Thus (v) follows. Observe that, by item (vii) of Proposition 4.11,

the identity $\sim x \ll \neg x$ holds on all WPQK-algebras. Thus (v) implies (vi). By a similar argument, since $x \ll \sim\sim x$ holds on all WPQK-algebras, we have that (vi) implies (vii).

Regarding (vii), observe that, for $\langle a_+, a_-\rangle \in A$, we have $\langle a_+, a_-\rangle \leq \neg\neg\langle a_+, a_-\rangle$ iff $a_+ \leq_+ \neg_+\neg_+ a_+$ and $n(\neg_+ a_+) \leq_- a_-$. The former inequality always holds on a p-lattice, but from the latter we have $pn(\neg_+ a_+) \leq_- p(a_-)$. Since $\neg_+ a_+ \leq_+ pn(\neg_+ a_+)$, we obtain $\neg_+ a_+ \leq_+ p(a_-)$. Observe that the inequality $p(a_-) \leq_+ \neg_+ a_+$ holds in general. In fact, by the property of the pseudo-complement, we have $p(a_-) \leq_+ \neg_+ a_+$ iff $a_+ \wedge_+ p(a_-) = 0_+$, which we know to hold on every twist-structure. This shows that (ix) and (x) are equivalent, and are both implied by (vii). Notice, further, that the equality $p(a_-) = \neg_+ a_+$ implies $a_- = np(a_-) = n(\neg_+ a_+)$. This means that every element of the twist-structure has the form $\langle a_+, n(\neg_+ a_+)\rangle$ for some $a_+ \in A_+$, and is thus determined by its first component. Recall that $\langle a_+, a_-\rangle \wedge \sim\langle a_+, a_-\rangle = \langle 0_+, a_- \vee_- n(a_+)\rangle$. Assuming (vii), we then have $a_- \vee_- n(a_+) = n(\neg_+ a_+) \vee_- n(a_+) = n(\neg_+ 0_+) = n(1_+) = 1_-$. Hence, $\langle a_+, a_-\rangle \wedge \sim\langle a_+, a_-\rangle = \langle 0_+, 1_-\rangle$, which means that (iii) holds. Thus (vii) implies (and is therefore equivalent to) any of the items (i)–(iv). Regarding (viii), observe that it is implied by (ii). Also, conversely, (viii) clearly implies (vii), which we have just shown to be equivalent with (ii). Thus the items (i), (ii), (iii), (iv), (vii) and (viii) are all equivalent. From this we have that (viii) implies (vii) which, as we have seen, implies (ix) and (x). Recalling that n preserves finite joins, we also obtain that (vii) implies (xi): for all $\langle a_+, a_-\rangle \in A$, one has $n(a_+ \vee_+ a_-) = n(a_+ \vee_+ \neg_+ a_+) = n(a_+) \vee_- n(\neg_+ a_+) = 1_-$. Thus (viii) implies (xi) as well. Now, assuming (xi), we have

$$n(a_+ \vee_+ p(a_-)) = n(a_+) \vee_- np(a_-) = n(a_+) \vee_- a_- = 1_-,$$

which entails (i). This means that all items from (i) to (xi) are equivalent. To conclude the proof, observe that (xii) implies (ii), and so implies all other items. Conversely, if (using (vii), for example) every element is of the form $\langle a_+, n(\neg_+ a_+)\rangle$, then clearly the map $(.)^*$ is the identity on A. Thus $\mathbf{A}^* = \langle A; \wedge, \vee, \neg, 0, 1\rangle$, which entails (by Proposition 7.3) that $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ is a p-lattice, as required. □

We list below a selection of items from the preceding proposition that give different characterisations for the $\sim$-free reduct of a WPQK-algebra being itself a p-lattice.

Proposition 9.3. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra. The following are equivalent:*

(i) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is a p-lattice,*

(ii) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is an almost-p-lattice,*

(iii) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is a quasi-Kleene algebra,*

(iv) $\langle A; \wedge, \vee, \neg, 0, 1\rangle = \mathbf{A}^* \cong \mathbf{A}_+$,

(v) $\langle A; \wedge, \vee, \neg, 0, 1\rangle \cong \langle A; \wedge, \vee, \sim, 0, 1\rangle$,

(vi) $\mathbf{A} \models x \ll \neg\neg x$,

(vii) $\mathbf{A} \models x \wedge \neg x \approx 0$.

Proposition 9.4. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \sim\sim x \vee \sim x \approx 1$, *(i.e.* $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *is a Stone lattice),*

(ii) $p(n(a_+)) \vee_+ p(a_-) = 1_+$ *for all* $\langle a_+, a_-\rangle \in A$.

Proof. Observe that (i) easily entails (using the semi-De Morgan identities) the identity $\sim\sim x \wedge \sim x \approx 0$. Thus, by Proposition 9.2, (i) implies that $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ is a p-lattice. Indeed, in general a Stone lattice is defined precisely as a p-lattice satisfying (i). That this condition corresponds, on twist-structures, to (ii) is a matter of routine checking. □

Proposition 9.5. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \neg x \ll \neg\neg\neg x$,

(ii) $\mathbf{A} \models \neg x \approx \neg\neg\neg x$,

(iii) $n(\neg_+\neg_+ a_+) \leq_- n(a_+)$ *for all* $a_+ \in A_+$,

(iv) $n(\neg_+\neg_+ a_+) = n(a_+)$ *for all* $a_+ \in A_+$.

Proof. Recall (Lemma 3.5.xii) that $\neg\neg\neg x \ll \neg x$ holds on every WPQK-algebra, and that $n(a_+) \leq_- n(\neg_+\neg_+ a_+)$ also holds generally. The proof of Lemma 3.5.xii shows that the converse inequality $\neg x \ll \neg\neg\neg x$ holds precisely when $n(\neg_+\neg_+ a_+) \leq_- n(a_+)$ for all $a_+ \in A_+$. □

Proposition 9.6. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \neg\neg x \wedge \neg\neg y \ll \neg\neg(x \wedge y)$,

(ii) $\mathbf{A} \models \neg\neg x \wedge \neg\neg y \approx \neg\neg(x \wedge y)$,

(iii) $n(\neg_+(a_+ \wedge_+ b_+)) \leq_- n(\neg_+ a_+ \vee_+ \neg_+ b_+)$ *for all* $a_+, b_+ \in A_+$,

(iv) $n(\neg_+(a_+ \wedge_+ b_+)) = n(\neg_+ a_+ \vee_+ \neg_+ b_+)$ *for all* $a_+, b_+ \in A_+$.

Proof. On the one hand, we have

$$\begin{aligned}\neg\neg(\langle a_+, a_-\rangle \wedge \langle b_+, b_-\rangle) &= \langle \neg_+\neg_+(a_+ \wedge_+ b_+), n(\neg_+(a_+ \wedge_+ b_+))\rangle \\ &= \langle \neg_+\neg_+ a_+ \wedge_+ \neg_+\neg_+ b_+, n(\neg_+(a_+ \wedge_+ b_+))\rangle.\end{aligned}$$

On the other,

$$\begin{aligned}\neg\neg\langle a_+, a_-\rangle \wedge \neg\neg\langle b_+, b_-\rangle &= \langle \neg_+\neg_+ a_+, n(\neg_+ a_+)\rangle \wedge \langle \neg_+\neg_+ b_+, n(\neg_+ b_+)\rangle \\ &= \langle \neg_+\neg_+ a_+ \wedge_+ \neg_+\neg_+ b_+, n(\neg_+ a_+) \vee_- n(\neg_+ b_+)\rangle \\ &= \langle \neg_+\neg_+ a_+ \wedge_+ \neg_+\neg_+ b_+, n(\neg_+ a_+ \vee_+ \neg_+ b_+)\rangle.\end{aligned}$$

So only the second components matter. Since $\neg_+$ is order-reversing, the inequality $\neg_+ a_+ \vee_+ \neg_+ b_+ \leq_+ \neg_+(a_+ \wedge_+ b_+)$ always holds on a p-lattice, and entails the inequality $n(\neg_+ a_+ \vee_+ \neg_+ b_+) \leq_- n(\neg_+(a_+ \wedge_+ b_+))$. Thus, it is clear that all items correspond to the requirement that $n(\neg_+(a_+ \wedge_+ b_+)) \leq_- n(\neg_+ a_+ \vee_+ \neg_+ b_+)$ for all $a_+, b_+ \in A_+$. □

By joining the two preceding results, we obtain the following characterization.

Proposition 9.7. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is a semi-De Morgan algebra,*

(ii) $n(\neg_+\neg_+ a_+) = n(a_+)$ *and* $n(\neg_+(a_+ \wedge_+ b_+)) = n(\neg_+ a_+ \vee_+ \neg_+ b_+)$, *for all* $a_+, b_+ \in A_+$.

Proposition 9.8. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \neg\neg x \vee \neg x \approx 1$,

(ii) $\mathbf{A}_+$ *is a Stone lattice.*

Proof. Let us calculate $\neg\neg\langle a_+, a_-\rangle \vee \neg\langle a_+, a_-\rangle = \langle \neg_+ a_+ \vee_+ \neg_+\neg_+ a_+, n(a_+) \wedge_- n(\neg_+ a_+)\rangle = \langle \neg_+ a_+ \vee_+ \neg_+\neg_+ a_+, n(a_+ \wedge_+ \neg_+ a_+)\rangle = \langle \neg_+ a_+ \vee_+ \neg_+\neg_+ a_+, n(0_+)\rangle = \langle \neg_+ a_+ \vee_+ \neg_+\neg_+ a_+, 0_-\rangle$. It is thus clear that requiring $\neg\neg\langle a_+, a_-\rangle \vee \neg\langle a_+, a_-\rangle = \langle 1_+, 0_-\rangle$ implies that $\mathbf{A}_+$ is a Stone lattice. Thus (i) entails (ii). The converse is also straightforward (recall that, for all $a_+ \in A_+$, there is $a_- \in A_-$ such that $\langle a_+, a_-\rangle \in A$). □

Proposition 9.9. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \neg\neg x \ll x$,

(ii) $\mathbf{A} \models x \vee \neg x \approx 1$, *(i.e.* $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is a Boolean algebra),*

(iii) $\mathbf{A}_+$ *is a Boolean algebra.*

Proof. Consider (i). On a twist-structure, this means:

$$\neg\neg\langle a_+, a_-\rangle = \langle \neg_+\neg_+ a_+, n(\neg_+ a_+)\rangle \leq \langle a_+, a_-\rangle.$$

That is, $\neg_+\neg_+ a_+ \leq_+ a_+$ and $a_- \leq_- n(\neg_+ a_+)$. The latter condition is always satisfied by a twist-structure. Indeed, by the requirement that $a_+ \wedge_+ p(a_-) = 0_+$, using the property of the pseudo-complement, we can obtain $p(a_-) \leq_+ \neg_+ a_+$, and from this (by the monotonicity of n and $n \circ p = Id_{A_-}$) we get $np(a_-) = a_- \leq_- n(\neg_+ a_+)$. On the other hand, since $a_+ \leq_+ \neg_+\neg_+ a_+$ holds on every p-lattice, using the former condition ($\neg_+\neg_+ a_+ \leq_+ a_+$) we have $\neg_+\neg_+ a_+ = a_+$. This entails that $\mathbf{A}_+$ is a Boolean algebra. Using this, it is easy to check that (ii) holds, for $\langle a_+, a_-\rangle \vee \neg\langle a_+, a_-\rangle = \langle a_+ \vee_+ \neg_+ a_+, a_- \wedge_- n(a_+)\rangle = \langle a_+ \vee_+ \neg_+ a_+, 0_-\rangle$. It is also clear that requiring $\langle a_+, a_-\rangle \vee \neg\langle a_+, a_-\rangle = \langle 1_+, 0_-\rangle$ implies that $\mathbf{A}_+$ is a Boolean algebra, which in turn entails (i). □

Proposition 9.10. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra. with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models x \wedge \sim\neg\sim x \approx 0$,

(ii) $\mathbf{A}_-$ *is a Boolean algebra with complement given by* $\neg_- a_- = n(\neg_+ p(a_-))$.

Proof. Let us compute:

$$\begin{aligned}\langle a_+, a_-\rangle \wedge \sim\neg\sim\langle a_+, a_-\rangle &= \langle a_+ \wedge_+ p(a_-), a_- \vee_- n(\neg_+ p(a_-))\rangle \\ &= \langle 0_+, a_- \vee_- n(\neg_+ p(a_-))\rangle.\end{aligned}$$

Thus, (i) is equivalent to $a_- \vee_- n(\neg_+ p(a_-)) = 1_-$. In such a case, $n(\neg_+ p(a_-))$ is the Boolean complement of a_- in $\mathbf{A}_-$. To see this, it is sufficient to observe that $a_- \wedge_- n(\neg_+ p(a_-)) = np(a_-) \wedge_- n(\neg_+ p(a_-)) = n(p(a_-) \wedge_+ \neg_+ p(a_-)) = n(0_+) = 0_-$. Thus (i) implies (ii). The converse is clear. □

Proposition 9.11. *Let* $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ *be a WPQK-algebra with* $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. *The following are equivalent:*

(i) $\mathbf{A} \models \neg\neg x \wedge \neg x \approx 0$, *($\langle A; \wedge, \vee, \neg, 0, 1\rangle$ is a demi-p-lattice),*

(ii) $n(D(\mathbf{A}_+)) = 1_-$.

Proof. For $\langle a_+, a_-\rangle \in A$, let us calculate $\neg\neg\langle a_+, a_-\rangle \wedge \neg\langle a_+, a_-\rangle = \langle \neg_+\neg_+ a_+ \wedge_+ \neg_+ a_+, n(\neg_+ a_+) \vee_- n(a_+)\rangle = \langle 0_+, n(\neg_+ a_+ \vee_+ a_+)\rangle$. We thus see that (i) means requiring that $n(\neg_+ a_+ \vee_+ a_+) = 1_+$. Thus, it suffices to observe that the set $D(\mathbf{A}_+)$ of dense elements of $\mathbf{A}_+$ is precisely made of all elements of the form $\neg_+ a_+ \vee_+ a_+$ for some $a_+ \in A_+$. □

In the next propositions we focus on involutive WPQK-algebras, i.e. Sendlewski's wp-Kleene algebras (Definition 4.14).

Proposition 9.12. *Let $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ be a WPQK-algebra with $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$. The following are equivalent:*

(i) $\mathbf{A} \models \sim\sim x \ll x$,

(ii) $\mathbf{A} \models \sim\sim x \approx x$,

(iii) $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *is a Kleene algebra,*

(iv) $\mathbf{A}$ *is a wp-Kleene algebra,*

(v) The maps n and p are mutually inverse bounded (p-)lattice isomorphisms.

Proof. The equivalence of (i)–(iii) has been observed before. That these items are equivalent to (iv) has been proven in Proposition 4.15. Regarding (v), observe that the involutive identity holds iff $p \circ n = Id_{A_+}$. Since $n \circ p = Id_{A_-}$ holds generally, we have that p and n are mutually inverse bijections. Moreover, they are monotone maps, which entails that they are lattice isomorphisms. Lastly, notice that the pseudo-complement operation (cf. Proposition 3.4) is completely determined by the lattice structure, which implies that it is also preserved by n and p. □

Observe that, if $\mathbf{A}$ is a wp-Kleene algebra such that $A = Tw\langle A_+, A_-, n, p, \nabla\rangle$, then $\mathbf{A}$ is completely determined by the pair $\langle A_+, \nabla\rangle$. Thus, we can can simply write $A = Tw\langle A_+, \nabla\rangle$.

Proposition 9.13. *Let $\mathbf{A} = \langle A; \wedge, \vee, \sim, \neg, 0, 1\rangle$ be a wp-Kleene algebra with $A = Tw\langle A_+, \nabla\rangle$. The following are equivalent:*

(i) $\mathbf{A} \models x \approx \neg\neg x$,

(ii) $\mathbf{A} \models x \ll \neg\neg x$,

(iii) $\mathbf{A} \models \neg x \ll \sim x$,

(iv) $\mathbf{A} \models \neg x \approx \sim x$, *i.e.* $\langle A; \wedge, \vee, \neg, 0, 1\rangle = \langle A; \wedge, \vee, \sim, 0, 1\rangle$,

(v) $\mathbf{A} \models \neg x \approx \neg\neg\neg x$,

(vi) $\mathbf{A} \models \neg x \ll \neg\neg\neg x$,

(vii) $\mathbf{A} \models x \vee \sim x \approx 1$,

(viii) $\mathbf{A}_+$ *is a Boolean algebra isomorphic to* $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *(and* $\langle A; \wedge, \vee, \neg, 0, 1\rangle$*) through the map given by* $a_+ \mapsto \langle a_+, \neg_+ a_+\rangle$ *for all* $a_+ \in A_+$,

(ix) $\langle A; \wedge, \vee, \sim, 0, 1\rangle$ *is a Boolean algebra,*

(x) $\langle A; \wedge, \vee, \neg, 0, 1\rangle$ *is a semi-De Morgan algebra,*

(xi) $\nabla = \{1_+\}$.

Proof. Clearly (i) implies (ii). The equivalence among (ii), (iii) and (iv) has been proven earlier (Proposition 9.2). Assuming (iv), we have $\neg\langle a_+, a_-\rangle = \langle \neg_+ a_+, a_+\rangle = \langle a_-, a_+\rangle = \sim\langle a_+, a_-\rangle$ for all $\langle a_+, a_-\rangle \in A$ (notice we are assuming $A_+ = A_-$ because we are in a wp-Kleene algebra). Thus every element of A is of the form $\langle a_+, \neg_+ a_+\rangle$. Using $\neg x \approx \sim x$, we have $\neg\neg\langle a_+, \neg_+ a_+\rangle = \langle \neg_+\neg_+ a_+, \neg_+ a_+\rangle = \sim\sim\langle a_+, \neg_+ a_+\rangle = \langle a_+, \neg_+ a_+\rangle$. Hence, $\neg_+\neg_+ a_+ = a_+$. Since (using the semi-De Morgan identities for $\neg_+$) we have $\neg\neg\neg\langle a_+, a_-\rangle = \langle \neg_+\neg_+\neg_+ a_+, \neg_+\neg_+ a_+\rangle = \langle \neg_+ a_+, \neg_+\neg_+ a_+\rangle$, it is clear that $\neg_+\neg_+ a_+ = a_+$ implies that (v) holds. Clearly (v) implies (vi). Now, (vi) implies $\neg_+\neg_+ a_+ \leq_+ a_+$ and so $\neg_+\neg_+ a_+ = a_+$. Thus, as observed before, $\mathbf{A}_+$ is an involutive p-lattice, i.e. a Boolean algebra. Then $\langle a_+, \neg_+ a_+\rangle \vee \neg\langle a_+, \neg_+ a_+\rangle = \langle a_+ \vee_+ \neg_+ a_+, \neg_+ a_+ \wedge_+ a_+\rangle = \langle 1_+, 0_+\rangle$, which means that (vii) is satisfied. In turn, (vii) entails $a_+ \vee_+ a_- = 1_+$ for all $\langle a_+, a_-\rangle \in A$, and so for all $a_+ \in A_+$. Since $a_+ \wedge_+ a_- = 0_+$ holds in general, this means that a_- is the Boolean complement of a_+ in $\mathbf{A}_+$. Then a_- is also the pseudo-complement of a_+, which gives us $a_- = \neg_+ a_+$ for all $a_+ \in A_+$. Hence, $\langle A_+; \wedge_+, \vee_+, \neg_+, 0_+, 1_+\rangle$ is a Boolean algebra. Checking that the map defined in item (viii) is a Boolean algebra isomorphism is straightforward. Hence, (vii) entails (viii). It is clear that (viii) entails (ix). It is also clear that (ix) implies (x). Now, assuming (x), we have $\mathbf{A} \models \neg x \ll \neg\neg\neg x$ (for this equation is part of the definition of semi-De Morgan algebras), which is (vi), and ee have seen that (vi) implies (viii). Thus A_+ is a Boolean algebra, and every element of $\mathbf{A}$ has the form $\langle a_+, \neg_+ a_+\rangle$ for some $a_+ \in A_+$. Then $n(a_+ \vee_+ \neg_+ a_+) = n(1_+) = 1_-$, which shows that (xi) holds. Lastly, assume (xi). Then $a_+ \vee_+ a_- = 1_+$ for all $\langle a_+, a_-\rangle \in A$, and so for all $a_+ \in A_+$. Then we can reason as before to conclude

that a_- is the Boolean complement and the pseudo-complement of $a_+ \in A_+$, which entails $\neg\langle a_+, a_-\rangle = \langle \neg_+ a_+, a_+\rangle = \langle a_-, a_+\rangle = \sim\langle a_+, a_-\rangle$. Thus we obtain (iv), which as mentioned earlier is equivalent to (i), closing the circle. □

10 Conclusions and Future Work

The present paper, together with [19], may be considered a first essay in characterising a fragment of quasi-Nelson algebras/logic. As we have seen, twist-structures turn out to be a particularly useful tool in this endeavour, and we speculate that similar techniques could be successfully applied to other (if not all) fragments. Observe that, in a non-involutive setting, the language $\{\wedge, \vee, *, \to, \Rightarrow, \sim, 0, 1\}$ in which Nelson algebras/logic are traditionally presented offers a number of independent combinations. Indeed, certain inter-definabilities among operations/connectives that are well known in the Nelson literature also hold in the quasi-Nelson setting; one can for example define (*salva veritate*):

$$x * y := x \wedge y \wedge \sim(x \Rightarrow \sim y)$$

$$x \Rightarrow y := (x \to y) \wedge (\sim y \to \sim x)$$

$$x \to y := x \Rightarrow (x \Rightarrow y)$$

$$\sim x := x \Rightarrow 0$$

$$0 := \sim(x \to x) \quad \text{or} \quad 0 := \sim(x \Rightarrow x) \quad \text{or} \quad 0 := x * \sim x$$

$$1 := x \to x \quad \text{or} \quad 1 := x \Rightarrow x \quad \text{or} \quad 1 := \sim(x * \sim x).$$

Others equivalences are however lost, for in general on quasi-Nelson algebras one has:

$$x \wedge y \neq \sim(\sim x \vee \sim y)$$

$$x \vee y \neq \sim(\sim x \wedge \sim y)$$

$$x * y \neq \sim(x \Rightarrow \sim y)$$

$$x \Rightarrow y \neq \sim(x * \sim y).$$

For example, while in the Nelson setting both fragments $\{\wedge, *, \sim\}$ and $\{\vee, \Rightarrow, 0\}$ are as expressive as the full language, once we drop the involutive law they may (in principle) determine distinct classes of algebras and different logics. Characterising fragments such as these, or even a systematic study of *all* fragments of quasi-Nelson

algebras/logic, will be the subject of future investigation. Notice that, besides its intrinsic interest, this project will have an impact on (involutive) Nelson logic as well, given that several fragments of Nelson algebras/logic (indeed, *all* of them, except those corresponding to Kleene algebras and *wp*-Kleene algebras) have not been studied yet.

Concerning WPQK-algebras in particular, the most intriguing issue currently left open is probably obtaining a better characterisation of their congruence lattices. Such a result would hopefully lead to a useful description of the subdirectly irreducible WPQK-algebras, thus providing a basis for a systematic study of the subvariety lattice of WPQK-algebras. As mentioned in Section 8, a means to achieving such a characterisation may perhaps be a study of WPQK-algebras in the guise of twist-structures over nuclear p-lattices; in turn, the congruences of nuclear p-lattices (and of the subdirectly irreducible algebras in particular) might be more easily understood through a frame-theoretic perspective (in the sense e.g. of the so-called Jónsson-Tarski duality for Boolean algebras with operators).

To conclude the conclusions, let us briefly return to the topic of logics associated to WPQK and *wp*-Kleene algebras. We have seen with Proposition 5.7 that the consequence $\models_{wpK}$, corresponding to the $\{\wedge, \vee, \sim, \neg, 0, 1\}$-fragment of Nelson logic (hence, *a fortiori*, the consequence $\models_{WPQK}$ of the corresponding fragment of quasi-Nelson logic), is not algebraisable. We believe that, analogously to the logic of p-lattices (as shown in [18]), neither of these systems is even protoalgebraic. This would entail that a (Hilbert-style) axiomatisation for $\models_{WPQK}$ (resp. $\models_{wpK}$) will not be obtained 'algorithmically' by translating the identities that constitute an equational presentation for WPQK (resp. *wp*-Kleene) algebras as varieties. The previous considerations also suggest that (once more in parallel to the logic of p-lattices [18]) Gentzen-style calculi might provide a more suitable framework for a logical understanding of these consequence relations. On the other hand, having established the twist representation result for WPQK and *wp*-Kleene algebras, we speculate that a multi-type approach (similar to the one applied in [10] to bilattice logic, also based on a twist representation) may also provide valuable insight into the proof theory of WPQK and *wp*-Kleene logics.

References

[1] A. Almeida. Canonical Extensions and Relational Representations of Lattices with Negation. *Studia Logica*, 91:171–199, 2009.

[2] R. Balbes and P. Dwinger. *Distributive lattices.* University of Missouri Press, Columbia, Mo., 1974.

[3] G. Bezhanishvili and S. Ghilardi. An algebraic approach to subframe logics. Intuitionistic case. *Annals of Pure and Applied Logic*, 147(1-2):84–100, 2007.

[4] W. J. Blok and D. Pigozzi. *Algebraizable logics*, volume 396 of *Mem. Amer. Math. Soc.* A.M.S., Providence, January 1989.

[5] N. Galatos, P. Jipsen, T. Kowalski, and H. Ono. *Residuated Lattices: an algebraic glimpse at substructural logics*, volume 151 of *Studies in Logic and the Foundations of Mathematics*. Elsevier, Amsterdam, 2007.

[6] N. Galatos and J. G. Raftery. Adding involution to residuated structures. *Studia Logica*, 77:181–207, 2004.

[7] N. Galatos and J. G. Raftery. Idempotent residuated structures: some category equivalences and their applications. *Transactions of the American Mathematical Society*, 367(5):3189–3223, 2015.

[8] A-N. Hsieh and J. G. Raftery. Conserving involution in residuated structures. *Mathematical Logic Quarterly*. 53:583–609, 2007.

[9] M. Gehrke and J. Harding. Bounded lattice expansions. *Journal of Algebra*, 238(1):345–371, 2001.

[10] G. Greco, F. Liang, A. Palmigiano, and U. Rivieccio. Bilattice logic properly displayed. *Fuzzy Sets and Systems*, 363:138–155, 2019.

[11] B. Jónsson. Algebras whose congruence lattices are distributive. *Mathematica Scandinavica*, 21:110–121, 1967.

[12] A. Jung and U. Rivieccio. A duality for two-sorted lattices. Submitted.

[13] H. Lakser. The structure of pseudocomplemented distributive lattices. I. Subdirect decomposition. *Transactions of the Americal Mathematical Society*, 156:335–342, 1971.

[14] F. Liang and T. Nascimento. Algebraic semantics for quasi-Nelson logic. In R. Iemhoff, M. Moortgat, and R. de Queiroz, editors, *Logic, Language, Information, and Computation. Proc. WoLLIC 2019*, volume 11541 of *Lecture Notes in Computer Science*, pages 450–466, Springer, Berlin, Heidelberg, 2019.

[15] M. Spinks, U. Rivieccio, and T. Nascimento. Compatibly involutive residuated lattices and the Nelson identity. *Soft Computing*, 23:2297–2320, 2019.

[16] D. Nelson. Constructible falsity. *Journal of Symbolic Logic*, 14:16–26, 1949.

[17] H. Rasiowa. *An algebraic approach to non-classical logics*, volume 78 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1974.

[18] J. Rebagliato and V. Verdú. On the algebraization of some Gentzen systems. *Fundamenta Informaticae, Special Issue on Algebraic Logic and its Applications*, 18:319–338, 1993.

[19] U. Rivieccio. Representation of De Morgan and (semi-)Kleene lattices. *Soft Computing*, 24 (12):8685–8716, 2020.

[20] U. Rivieccio and R. Jansana. Quasi-Nelson algebras and fragments. Submitted.

[21] U. Rivieccio, R. Jansana, and T. Nascimento. Two dualities for weakly pseudocomplemented quasi-Kleene algebras. In: Lesot M.J. et al. (eds), *Information Processing and Management of Uncertainty in Knowledge-Based Systems. IPMU 2020. Communi-*

cations in Computer and Information Science, vol. 1239, Springer, pp. 634-653, 2020.

[22] U. Rivieccio and M. Spinks. Quasi-Nelson algebras. *Electronic Notes in Theoretical Computer Science*, 344:169–188, 2019.

[23] U. Rivieccio and M. Spinks. Quasi-Nelson; or, non-involutive Nelson algebras. To appear in *Trends in Logic* (special issue dedicated to the *AsubL 2018* conference).

[24] H. P. Sankappanavar. Semi-De Morgan algebras. *Journal of Symbolic Logic*, 52:712–724, 1987.

[25] A. Sendlewski. Some investigations of varieties of $\mathcal{N}$-lattices. *Studia Logica*, 43:257–280, 1984.

[26] A. Sendlewski. Topologicality of Kleene algebras with a weak pseudocomplementation over distributive p-algebras. *Reports on Mathematical Logic*, 25:13–56, 1991.

[27] Spinks, M., Veroff, R.: Constructive logic with strong negation is a substructural logic. I. *Studia Logica*, 88, 325–348 (2008)

[28] Spinks, M., Veroff, R.: Constructive logic with strong negation is a substructural logic. II. *Studia Logica*, 89, 401–425 (2008)

[29] D. Vakarelov. Notes on $\mathcal{N}$-lattices and constructive logic with strong negation. *Studia Logica*, 36:109–125, 1977.

Received 8 December 2019

Optimal Polynomial-Time Estimators: A Bayesian Notion of Approximation Algorithm

Vanessa Kosoy
(Independent)
vanessa.kosoy@intelligence.org

Alexander Appel
(Independent)
alexappel8@gmail.com

Abstract

We introduce a new concept of approximation applicable to decision problems and functions, inspired by Bayesian probability. From the perspective of a Bayesian reasoner with limited computational resources, the answer to a problem that cannot be solved exactly is uncertain and therefore should be described by a random variable. It thus should make sense to talk about the expected value of this random variable, an idea we formalize in the language of average-case complexity theory by introducing the concept of "optimal polynomial-time estimators." We prove some existence theorems and completeness results, and show that optimal polynomial-time estimators exhibit many parallels with "classical" probability theory.

0 Introduction

0.1 Motivation

Imagine you are strolling in the city with a friend when a car passes by with the license plate number "7614829". Your friend proposes a wager, claiming that the number is composite and offering 10 : 1 odds in your favor. Knowing that your friend has no exceptional ability in mental arithmetic and that it's highly unlikely they saw this car before, you realize they are just guessing. Your mental arithmetic is also insufficient to test the number for primality, but is sufficient to check that

$7614829 \equiv 1 \pmod 3$ and $\frac{1}{\ln 7614829} \approx 0.06$. Arguing from the prime number theorem and observing that 7614829 is odd and is divisible neither by 3 nor by 5, you conclude that the probability 7614829 is prime is $\frac{1}{\ln 7614829} \times 2 \times \frac{3}{2} \times \frac{5}{4} \approx 22\%$. Convinced that the odds are in your favor, you accept the bet[1].

From the perspective of frequentist probability, the question "what is the probability 7614829 is prime?" seems meaningless. It is either prime or not, so there is no frequency to observe (unless the frequency is 0 or 1). From a Bayesian perspective, probability represents a degree of confidence; however, in classical Bayesian probability theory it is assumed that the only source of uncertainty is lack of information. The number 7614829 already contains all information needed to determine whether it is prime, so the probability again has to be 0 or 1. However, real life uncertainty is not only information-theoretic but also complexity-theoretic. Even when we have all of the information needed to obtain the answer, our computational resources are limited, and so we remain uncertain. The rigorous formalization of this idea is the main goal of the present work.

The idea of assigning probabilities to purely mathematical questions was studied by several authors [6,8,10,11,14], mainly in the setting of formal logic. That is, their approach was looking for functions from the set of sentences in some formal logical language to $[0, 1]$. However, although there is a strong intuitive case for assigning probabilities to sentences like

$$\varphi_1 := \text{“7614829 is prime”}$$

it is much less clear there is a meaningful assignment of probabilities to sentences like

$$\varphi_2 := \text{“there are no odd perfect numbers”}$$

or (even worse)

$$\varphi_3 := \text{“there is no cardinality } \kappa \text{ s.t. } \aleph_0 < \kappa < 2^{\aleph_0}\text{”}$$

A wager on φ_1 can be resolved in a predetermined finite amount of time (the amount of time it takes to test it directly). On the other hand, it is unknown how long the resolution of φ_2 will take. It is possible that there is an odd perfect number but finding it (or otherwise becoming certain of its existence) will take a very long time. It is also possible there is no odd perfect number, a fact that cannot be directly verified because of its infinite nature. It is possible that there is a proof of φ_2 within some formal theory, but accepting such a proof as resolution requires us

[1] Alas, $7614829 = 271 \times 28099$.

to be completely certain of the consistency of the theory (whereas it is arguable that the consistency of formal mathematical theories, especially more abstract theories like ZFC, is itself only known empirically and in particular with less than absolute certainty). Moreover, there is no knowing a priori whether a proof exists or how long it will take to find it. For φ_3 there is no way to "directly" verify either the sentence or its negation, and it is actually known to be independent of ZFC.

In the present work we avoid choosing a specific category of mathematical questions[2]. Instead, we consider the abstract setting of arbitrary distributional decision problems. This leads to the perspective that an assignment of probabilities is a form of *approximate* solution to a problem. This is not the same sense of approximation as used in optimization problems, where the approximation error is the difference between the ideal solution and the actual solution. Instead, the approximation error is the prediction accuracy of our probability assignment. This is also different from average-case complexity theory, where the solution is required to be exact on most input instances. However, the language of average-case complexity theory (in particular, the concept of a distributional decision problem) turns out to be well-suited to our purpose. The concept of "optimal polynomial-time estimator" that arises from the approach turns out to behave much like probabilities, or more generally expected values, in "classical" probability theory. They display an appropriate form of calibration. The "expected values" are linear in general and multiplicative for functions that are independent in an appropriate sense. There is a natural parallel of conditional probabilities. For simple examples constructed from one-way functions we get the probability values we expect. They are also well behaved in the complexity-theoretic sense that a natural class of reductions transforms optimal polynomial-time estimators into optimal polynomial-time estimators, and complete problems for these reductions exist for important complexity classes.

Optimal polynomial-time estimators turn out to be unique up to a certain equivalence relation. The existence of optimal polynomial-time estimators depends on the specific variety you consider. We show that in the non-uniform case (allowing advice) there is a variety of optimal polynomial-time estimators that exist for completely arbitrary problems. Uniform optimal polynomial-time estimators of this kind exist for a certain class of problems we call "samplable" which can be very roughly regarded as an average-case analogue of $\mathrm{NP} \cap \mathrm{coNP}$. More generally mapping the class of problems which admit optimal polynomial-time estimators allows for much further research.

[2]We do require that these questions can be represented as finite strings of bits.

0.2 Overview

Consider a language $L \subseteq \{0,1\}^*$ and a family $\{\mathcal{D}^k\}_{k\in\mathbb{N}}$ where each $\mathcal{D}^k$ is a probability distribution on $\{0,1\}^*$. We associate with L its characteristic function $\chi_L : \{0,1\}^* \to \{0,1\}$. A pair $(\mathcal{D}, L)$ is called a *distributional decision problem* [4]. Our goal is defining and studying the probabilities of "events" of the form $x \in L$[3] associated with the uncertainty resulting from limited computational resources. (Specifically, we will consider the resources of time, randomness and advice.)

The distributional complexity class $\text{HEUR}_{\text{neg}}\text{P}$ is defined as the set of distributional decision problems which admit a polynomial-time heuristic algorithm with negligible error probability [4]. That is, $(\mathcal{D}, L) \in \text{HEUR}_{\text{neg}}\text{P}$ iff there is $A : \mathbb{N} \times \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}$ (an algorithm which takes input in $\mathbb{N} \times \{0,1\}^*$ and produces output in $\{0,1\}$) s.t. $A(k,x)$ runs in time polynomial in k and $\Pr_{x\sim\mathcal{D}^k}[A(k,x) \neq \chi_L(x)]$ is a negligible function of k. We have the following equivalent condition. $(\mathcal{D}, L) \in \text{HEUR}_{\text{neg}}\text{P}$ iff there is $P : \mathbb{N} \times \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ s.t. $P(k,x)$ runs in time polynomial in k and $\mathrm{E}_{x\sim\mathcal{D}^k}[(P(k,x) - \chi_L(x))^2]$ is a negligible function of k. In the language of the present work, such a P is a called an "$\mathcal{F}_{\text{neg}}(\Gamma_0^1, \Gamma_0^1)$-perfect polynomial-time estimator for $(\mathcal{D}, \chi_L)$" (see Definition 5.1, Example 2.6 and Example 2.1).

Our main objects of study are algorithms satisfying a related but weaker condition. Namely, we consider P s.t. its error w.r.t. χ_L is not negligible but is *minimal up to a negligible function*. That is, we require that for any $Q : \mathbb{N} \times \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ s.t. $Q(k,x)$ also runs in time polynomial in k, there is a negligible function $\varepsilon(k)$ s.t.

$$\mathrm{E}_{x\sim\mathcal{D}^k}[(P(k,x) - \chi_L(x))^2] \leq \mathrm{E}_{x\sim\mathcal{D}^k}[(Q(k,x) - \chi_L(x))^2] + \varepsilon(k)$$

Such a P is called an "$\mathcal{F}_{neg}(\Gamma_0^1, \Gamma_0^1)$-optimal polynomial-time estimator for $(\mathcal{D}, \chi_L)$." More generally, we replace negligible functions by functions that lie in some space $\mathcal{F}$ which can represent different asymptotic conditions (see Definition 2.8), and we consider estimators that use certain asymptotic amounts of randomness and advice represented by a pair Γ of function spaces (see Definition 2.3). This brings us to the concept of an "$\mathcal{F}(\Gamma)$-optimal polynomial-time estimator" (see Definition 2.11).

Denote $\text{OP}[\mathcal{F}(\Gamma)]$ the set of distributional decision problems that admit $\mathcal{F}(\Gamma)$-optimal polynomial-time estimators. Obviously $\text{OP}[\mathcal{F}_{neg}(\Gamma_0^1, \Gamma_0^1)] \supseteq \text{HEUR}_{\text{neg}}\text{P}$. Moreover, if one-way functions exist the inclusion is proper since it is possible to use any function with a hard-core predicate to construct an example where the constant

[3] We will actually consider the more general case of a function $f : \{0,1\}^* \to \mathbb{R}$ and the "expected value" of $f(x)$, but for most purposes there is no difference of principle.

$\frac{1}{2}$ is an $\mathcal{F}_{neg}(\Gamma_0^1, \Gamma_0^1)$-optimal polynomial-time estimator (see Theorem 2.3). Thus, it seems that we constructed novel natural distributional complexity classes.

The distributional complexity class HeurP is defined as the set of distributional decision problems which admit a polynomial-time heuristic scheme [4]. That is, $(\mathcal{D}, L) \in \text{HeurP}$ iff there is $S : \mathbb{N}^2 \times \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}$ s.t. $S(K_0, K_1, x)$ runs in time polynomial in K_0, K_1 and[4] $\Pr_{x\sim\mathcal{D}^{K_0}}[S(K_0, K_1, x) \neq \chi_L(x)] \leq (K_1+1)^{-1}$. Analogously to before, we have the following equivalent condition. $(\mathcal{D}, L) \in \text{HeurP}$ iff there is $P : \mathbb{N}^2 \times \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ s.t. $P(K_0, K_1, x)$ runs in time polynomial in K_0, K_1 and for some $M > 0$, $\mathrm{E}_{x\sim\mathcal{D}^{K_0}}[(P(K_0, K_1, x) - \chi_L(x))^2] \leq M(K_1+1)^{-1}$. In the language of the present work, such a P is a called an "$\mathcal{F}_{(K_1+1)^{-1}}(\Gamma_0^2, \Gamma_0^2)$-optimal polynomial-time estimator for $(\mathcal{D}^\eta, \chi_L)$" (see Example 2.7), where $\mathcal{D}^\eta$ is a two-parameter ($K_0, K_1 \in \mathbb{N}$) family of distributions which is constant along the parameter K_1.

Again we can consider the corresponding weaker condition, that for all $Q : \mathbb{N}^2 \times \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ s.t. $Q(K_0, K_1, x)$ runs in time polynomial in K_0, K_1

$$\mathrm{E}_{x\sim\mathcal{D}^{K_0}}[(P(K_0, K_1, x) - \chi_L(x))^2] \leq \mathrm{E}_{x\sim\mathcal{D}^{K_0}}[(Q(K_0, K_1, x) - \chi_L(x))^2] + M(K_1+1)^{-1}$$

Such a P is called an "$\mathcal{F}_{(K_1+1)^{-1}}(\Gamma_0^2, \Gamma_0^2)$-optimal polynomial-time estimator for $(\mathcal{D}^\eta, \chi_L)$."

It is also useful to introduce the closely related concept of an "$\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator" (see Definition 2.13). For example, an $\mathcal{F}^\sharp_{(K_1+1)^{-1}}(\Gamma_0^2, \Gamma_0^2)$-optimal polynomial-time estimator P has to satisfy that for each $S : \mathbb{N}^2 \times \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ that is also polynomial-time there is $M > 0$ s.t.

$$|\mathrm{E}_{x\sim\mathcal{D}^{K_0}}[(P(K_0, K_1, x) - \chi_L(x))S(K_0, K_1, x)]| \leq M(K_1+1)^{-1}$$

We show that e.g. every $\mathcal{F}^\sharp_{(K_1+1)^{-1}}(\Gamma_0^2, \Gamma_{\log}^2)$-optimal polynomial-time estimator is in particular an $\mathcal{F}_{(K_1+1)^{-1}}(\Gamma_0^2, \Gamma_{\log}^2)$-optimal polynomial-time estimator (see Theorem 2.2), whereas every $\mathcal{F}_{(K_1+1)^{-1}}(\Gamma_0^2, \Gamma_{\log}^2)$-optimal polynomial-time estimator is in particular an $\mathcal{F}^\sharp_{(K_1+1)^{-\frac{1}{2}}}(\Gamma_0^2, \Gamma_{\log}^2)$-optimal polynomial-time estimator (see Theorem 2.1). Here, $\Gamma_{\log}^2$ indicates that we consider algorithms with advice of logarithmic length (see Example 2.4).

[4] We slightly reformulated the definition given in [4]: replaced the rational input parameter δ by the integer input parameter K_1. The equivalence of the two formulations may be observed via the substitution $\delta = (K_1+1)^{-1}$.

We claim that the concept of an optimal polynomial-time estimator is a formalisation of the intuition outlined in 0.1. A priori, this is plausible because the mean squared error is a proper scoring rule (the Brier score). Moreover, it is the only scoring rule which is "proper" for arbitrary expected value assignment rather than only probability assignment. To support this claim, we prove a number of results that form a parallel between probability theory and the theory of optimal polynomial-time estimators:

- According to Borel's law of large numbers, every event of probability p occurs with asymptotic frequency p. Therefore, if some algorithm P represents a notion of probability for $x \in L$, we expect that given $a, b \in \mathbb{Q}$ and considering $x \sim \mathcal{D}^k$ s.t. $a \leq P(x) \leq b$, the frequency with which $x \in L$ is asymptotically (in k) between a and b. In Bayesian statistics, probability assignments satisfying such a property are said to be "well calibrated" (see e.g. [7]). With some assumptions about allowed advice and the portion of the distribution falling in the $[a, b]$ interval, $\mathcal{F}(\Gamma)$-optimal polynomial-time estimators are well calibrated (see Corollary 3.1). In particular, if the aforementioned portion is bounded from below, this frequency lies in $[a, b]$ up to a function of the form $\sqrt{\varepsilon}$ for $\varepsilon \in \mathcal{F}$.

- Given $L_1, L_2 \subseteq \{0,1\}^*$ s.t. $L_1 \cap L_2 = \varnothing$ we expect a reasonable notion of probability to satisfy $\Pr[x \in L_1 \cup L_2] = \Pr[x \in L_1] + \Pr[x \in L_2]$. To satisfy this expectation, we show that given $\mathcal{D}$ any family of distributions, P_1 an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator for $(\mathcal{D}, L_1)$ and P_2 an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator for $(\mathcal{D}, L_2)$, $P_1 + P_2$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator for $(\mathcal{D}, L_1 \cup L_2)$. This observation in itself is trivial (see Proposition 3.1) but applying it to examples may require passing from an $\mathcal{F}(\Gamma)$-optimal polynomial-time estimator to an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator using the non-trivial Theorem 2.1.

- Consider $L, M \subseteq \{0,1\}^*$ and suppose we are trying to formalize the conditional probability $\Pr[x \in L \mid x \in M]$. There are two natural approaches. One is reducing it to unconditional probability using the identity

$$\Pr[x \in L \mid x \in M] = \frac{\Pr[x \in L \cap M]}{\Pr[x \in M]}$$

  We can then substitute optimal polynomial-time estimators for the numerator and denominator. The other is considering an optimal polynomial time-estimator for a family of conditional distributions. Luckily, these two approach

yield the same result. That is, we show that given $\mathcal{D}$ a family of distributions, P_{LM} an optimal polynomial time estimator for $(\mathcal{D}, L \cap M)$, P_M an optimal polynomial-time estimator for $(\mathcal{D}, M)$ and assuming $\mathcal{D}^K(M)$ is not too small (e.g. bounded from below), $P_M^{-1} P_{LM}$ is an optimal polynomial-time estimator for $(\mathcal{D} \mid M, L)$ (see Theorem 3.3). Conversely, given $P_{L|M}$ an optimal polynomial-time estimator for $(\mathcal{D} \mid M, L)$, $P_M P_{L|M}$ is an optimal polynomial-time estimator for $(\mathcal{D}, L \cap M)$ (see Theorem 3.2).

- For some pairs $L_1, L_2 \subseteq \{0,1\}^*$, the "events" $x \in L_1$ and $x \in L_2$ can be intuitively regarded as independent since learning whether $x \in L_2$ doesn't provide any information about whether $x \in L_1$ that a polynomial-time algorithm can use. We formalize one situation when this happens and show that in this situation the product of an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator (in certain form) for $(\mathcal{D}, L_1)$ by an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator for $(\mathcal{D}, L_2)$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator for $(\mathcal{D}, L_1 \cap L_2)$ (see Theorem 3.4). This is precisely analogous to the property of probabilities where the probability of the conjunction of independent events is the product of the separate probabilities. This is one of the central results of the present work.

Different complexity classes often have corresponding types of reductions that preserve them. In particular, reductions in average-case complexity theory have to satisfy an extra-condition that intuitively means that typical problem instances should not be mapped to rare problem instances. We define a class of reductions s.t. pull-backs of optimal polynomial-time estimators are optimal polynomial-time estimators. This requires stronger conditions than what is needed for preserving average-case complexity. Namely, a reduction π of $(\mathcal{D}, L)$ to $(\mathcal{E}, M)$ has to be "pseudo-invertible" i.e. there should be a way to sample $\mathcal{D} \mid \pi^{-1}(y)$ in polynomial time for y sampled from $\pi_* \mathcal{D}$, up to an error which is asymptotically small on average.

We give separate proofs for the invariance of $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimators (see Corollary 4.4) and the invariance of $\mathcal{F}(\Gamma)$-optimal polynomial-time estimators (see Corollary 4.5) without relying on Theorem 2.1 and Theorem 2.2 in order to produce a slightly stronger bound. We also show that this reduction class is rich enough to support complete problems for many problem classes e.g. SampNP (see Theorem 4.4).

Explicit construction of optimal polynomial-time estimators is likely to often be difficult because it requires proving a hardness result (that no polynomial-time estimator can outperform the given polynomial-time estimator). However, for a specific choice of $\mathcal{F}$ which we denote $\mathcal{F}_{\text{uni}}^{(n)}$ (see Example 2.8), we prove two broad

existence theorems.

The first (Theorem 5.1) shows that for suitable Γ (in particular it has to allow sufficiently long advice strings, e.g. logarithmic advice is sufficient), *any* distributional decision problem $(\mathcal{D}, L)$ admits an $\mathcal{F}_{\text{uni}}^{(n)}(\Gamma)$-optimal polynomial-time estimator for $(\mathcal{D}^\eta, L)$. The construction of this estimator is rather trivial: the advice string for (K_0, K_1) is the optimal (i.e. least $\mathrm{E}_{x\sim D^{K_0}}[(P(x) - f(x))^2]$) program that runs in time K_1 and is of length at most $l(K_0, K_1)$ where $l : \mathbb{N}^2 \to \mathbb{N}$ is some function which determines the allowed asymptotic advice length (Γ depends on l and an analogous function $r : \mathbb{N}^2 \to \mathbb{N}$ which determines the allowed asymptotic number of random bits used by the estimators). The non-trivial part here is the definition of $\mathcal{F}_{\text{uni}}^{(n)}$ which is s.t. allowing any estimator an amount of resources greater by a polynomial always translates to a reduction in error which lies in $\mathcal{F}_{\text{uni}}^{(n)}$.

The second (Theorem 5.2), which is another central result, shows that for suitable Γ (logarithmic advice and enough random e.g. logarithmic amount of random bits is sufficient), any distributional decision[5] problem $(\mathcal{D}, L)$ which is *samplable* (i.e. it is possible to efficiently sample pairs (x, t) where $x \in \{0,1\}^*$ is distributed approximately according to $\mathcal{D}$ and $t \in \mathbb{Q}$ is an estimate of $\chi_L(x)$ which is approximately unbiased on average) admits an $\mathcal{F}_{\text{uni}}^{(n)}(\Gamma)$-optimal polynomial-time estimator with the same advice strings as the sampler. In particular, if the sampler is uniform the estimator is also uniform.

The samplability property allows recasting the estimation problem as a learning problem. That is, we use the sampler to generate a number (we use $\mathcal{O}\left((\log K_1)^2\right)$) of problem instances for which an unbiased estimate of the correct answer is known, and we should now generalize from these instances to an instance for which the correct answer is unknown. The optimal polynomial-time estimator we construct accomplishes this using the empirical risk minimization principle from statical learning theory, applied to a hypothesis space which consists of programs. Specifically, the estimator iterates over all programs of length $O(\log K_1)$, runs each of them on the samples $\{(x_i, t_i)\}_{i\in[\mathcal{O}((\log K_1)^2)]}$ for time K_1 getting estimates $\{p_i\}_{i\in[\mathcal{O}((\log K_1)^2)]}$ and computes the empirical risk $\sum_{i\in[\mathcal{O}((\log K_1)^2)]}(p_i - t_i)^2$. It then selects the program with the minimal risk and runs it on the input for time K_1 to get the desired estimate. This is similar to Levin's universal search which dovetails all programs to get optimality. The optimality of this estimator is also closely related to the fundamental theorem of statistical learning theory for agnostic PAC learning [18]:

[5] All of the theorems are described for decision problems in the overview for the sake of simplicity but we actually prove them for "estimation" problems i.e. $f : \{0,1\}^* \to \mathbb{R}$ instead of $L \subseteq \{0,1\}^*$. Here this generalisation is more important since any efficient algorithm producing (x, t) pairs is the sampler of some distributional estimation problem.

like in agnostic PAC learning we get an estimate which is not necessarily accurate, but which is optimal within the hypothesis space (which in our case is the space of efficient estimators).

On the other hand, we rule out the existence of optimal polynomial-time estimators in the uniform case for certain problems. These negative results rely on the simple observation that if the veracity of $x \in L$ for $x \sim \mathcal{D}^k$ depends only on k, then advice strings of size $O(1)$ enable storing the exact answer to all such questions. Additionally, it is easy to see that an optimal polynomial-time estimator in the uniform case is still optimal when we allow $O(1)$ advice. This means that any optimal polynomial-time estimator for such a problem has to be a polynomial-time estimator. So, any problem of this form that doesn't have uniform polynomial-time estimators also doesn't have uniform optimal polynomial-time estimators. Consequently, any problem that is reducible to the former sort of problem also doesn't have optimal polynomial-time estimators.

Finally, we examine the uniqueness of optimal polynomial-time estimators for a fixed problem. We prove that if such an estimator exists, it is unique up to a difference which is asymptotically small on average (see Theorem 5.3). For example, given $(\mathcal{D}, L)$ a distributional decision problem s.t. the length of any $x \sim \mathcal{D}^k$ is bounded by some polynomial in k and P_1, P_2 two $\mathcal{F}^\sharp(\Gamma_0^1, \Gamma_0^1)$-optimal polynomial time estimators, $\mathrm{E}_{x \sim \mathcal{D}^k}[(P_1(k,x) - P_2(k,x))^2]$ is a function of k that lies in $\mathcal{F}$.

We are able to prove a stronger uniqueness result for optimal polynomial-time estimators for problems of the form $(\mathcal{D} \mid M, L)$ (see Theorem 5.4). Namely, if there is an optimal polynomial-time estimator P_M for $(\mathcal{D}, M)$ which takes values with a sufficiently strong lower bound then any P_{L1}, P_{L2} optimal polynomial-time estimators for $(\mathcal{D} \mid M, L)$ have an asymptotically small difference on average with respect to $\mathcal{D}$ (rather than $\mathcal{D} \mid M$). Informally, this means that whenever determining that $x \notin M$ is sufficiently hard, there are well-defined (up to an asymptotically small perturbation) probabilities for events of the form $x \in L$ conditioned by $x \in M$, even for instances which actually lie outside of M. That is, optimal polynomial-time estimators allow us asking counterfactual "what if" questions that are meaningless from a "classical" mathematical perspective due to the principle of explosion.

Many of our results make use of algorithms with advice strings, where the allowed asymptotic length of the advice strings is determined by the space of functions $\Gamma_{\mathfrak{A}}$. Such algorithms are not entirely realistic, but one way to interpret them is as real-time efficient (since we assume polynomial time) algorithms that require inefficient precomputation (at least this interpretation is valid when the advice strings are computable). The strength of the concept of an "$\mathcal{F}(\Gamma)$-optimal polynomial-time estimator" depends ambiguously on the size of $\Gamma_{\mathfrak{A}}$, since on the one hand larger $\Gamma_{\mathfrak{A}}$ allows for a greater choice of candidate optimal polynomial-time estimators, on the

other hand the estimator is required to be optimal in a larger class[6]. Sometimes it is possible to get the best of both worlds by having an estimator which uses few or no advice but is optimal in a class of estimators which use much advice (see e.g. Theorem 5.2).

Note that most of the theorems we get about $\mathcal{F}(\Gamma)$-optimal polynomial-time estimators require a lower bound on $\Gamma_{\mathfrak{A}}$ through the assumption that $\mathcal{F}$ is $\Gamma_{\mathfrak{A}}$-ample (see Definition 2.12). Theorem 2.1 which shows when an $\mathcal{F}(\Gamma)$-optimal polynomial-time estimator is also an $\mathcal{F}^{\frac{1}{2}\sharp}(\Gamma)$-optimal polynomial-time estimator (see Definition 2.9) also assumes a lower bound on $\Gamma_{\mathfrak{A}}$, but a weaker one. On the other hand, the converse Theorem 2.2 makes no such assumption and so do all other theorems about $\mathcal{F}^{\sharp}(\Gamma)$-optimal polynomial-time estimators (except indirectly since Theorem 2.1 is often required to construct an $\mathcal{F}^{\sharp}(\Gamma)$-optimal polynomial-time estimator in the first place).

0.3 Related work

Several authors starting from Gaifman studied the idea of assigning probabilities to sentences in formal logic [6, 8, 10, 11, 14]. Systems of formal logic such as Peano Arithmetic are very expressive, so such an assignment would have much broader applicability than most of the examples we are concerned about in the present work. On the other hand, the constructions achieved by those authors are either much further from realistic algorithms (e.g. require halting oracles or at least very expensive computations[7]) or have much weaker properties to attest to their interpretation as "probabilities".

Lutz [17] uses the theory of computable martingales to define when a set of sequences "appears for a polynomial-time observer" to have certain ν-measure with respect to a fixed probability measure ν on the set of infinite strings $\{0,1\}^\omega$. In particular, if a singleton $\{x\}$ has Lutz measure 1 (where $x \in \{0,1\}^\omega$), this means that x "looks like" a random sequence sampled from ν, as far as a polynomial-time observer can tell. This seems closely related to our idea of assigning "subjective probabilities for polynomial-time observers" to events that are otherwise deterministic. Formally relating and comparing the two setups remains a task for future work.

The notion that computational hardness often behaves like information-

[6]The same observation is true about the space $\Gamma_{\mathfrak{R}}$ which controls the allowed quantity of random bits.

[7]In fact, Theorem 5.1 shows optimal polynomial-time estimators exist for completely arbitrary distributional estimation problems, but the price is the need for advice strings which might be expensive or even uncomputable, depending on the problem. Nevertheless, these estimators are still "real-time efficient" which makes them semi-realistic in some sense.

theoretical uncertainty is well-known in complexity theory, although it hasn't been systematically formalized. For example see discussion of Theorem 7.5 in [12] or section 6.1 in [4]. Results such as Yao's XOR lemma can be interpreted as the transformation of "computational probabilities" under certain operations, which is resonant with our results e.g. Theorem 3.4. It seems likely that it is possible to fruitfully investigate these relations further.

Barak, Shaltiel and Wigderson [2] discuss notions of "entropy" for probability distributions that take computational hardness into account. Zheng [20] (Chapter 7) considers prediction markets where traders perform transactions via Boolean circuits of polynomial size. This is similar to our optimal polynomial-time estimators, in the sense that a loss function which is a proper scoring rule is minimized under computational resource constraints. However, Zheng doesn't study this concept beyond deriving a relation to the "pseudoentropy" mentioned above.

Much of the conceptual framework and results in average-case complexity theory, as detailed in Bogdanov and Trevisan's review [4], have analogues in this setting, and the distributional decision problems studied in average-case complexity theory are a special case of the distributional estimation problems studied in this paper. For example, the notion of a randomized Karp-reduction of distributional problems is analogous to the notion of a pseudo-invertible reduction used in this setting. The assertion that a predicate is (poly,$O(\rho)$)-inapproximable in the sense of Definition 7.9 in [12] is equivalent to the assertion that there is no perfect poly-time estimator for the predicate with "fall space" $O(\rho)$. Notably, the construction by Levin of a SampNP-complete problem [4] is closely related to our Theorem 4.4.

Different brands of "optimal algorithms" were previously defined and investigated in various contexts. Levin's universal search is an algorithm that solves the candid search form of any problem in NP in time which is minimal up to a polynomial (see Theorem 2.33 in [12]). Barak [1] uses instance checkers to construct algorithms optimal in this sense for decision problems (in particular for any problem that is EXP-complete). This concept also has a non-deterministic counterpart called "optimal proof system": see survey by Hirsch [13], which additionally discusses "optimal acceptors" (optimal algorithms that halt only on the "yes" instances of the problem). Notably, the latter survey also discusses the average-case rather than only the worst-case.

Khot's Unique Games Conjecture implies that many optimization problems have an algorithm which produces the best approximation factor possible in polynomial-time (see e.g. [16]). Barak and Steurer [3] speculate that even if the Unique Games Conjecture is false, the existence of an algorithm that is optimal in this sense for a large class of problems is plausible, and propose the Sum-of-Squares algorithm as a candidate.

Optimal polynomial-time estimators are optimal in a sense different from the examples above: they simultaneously run in polynomial-time, are applicable to decision problems and are of average-case nature. The metric they optimize is the average squared difference (Brier score) with the true function. Nevertheless, it might be interesting to explore connections and similarities with other types of optimal algorithms.

The structure of the paper is as follows. Section 1 fixes notation. Section 2 introduces the main definitions and gives a simple example using one-way functions. Section 3 shows the parallel between properties of optimal polynomial-time estimators and classical probability theory. Section 4 discusses behavior of optimal polynomial-time estimators under reductions and shows certain natural classes have complete problems under reductions that are appropriate. Section 5 discusses existence and uniqueness of optimal polynomial-time estimators. Section 6 discusses possible avenues for further research. The Appendix briefly reviews relevant material about hard-core predicates and one-way functions.

1 Notation

1.1 Sets, numbers and functions

$\mathbb{N}$ is the set of natural numbers. We will use the convention in which natural numbers start from 0, so $\mathbb{N} = \{0, 1, 2 \dots\}$.

$\mathbb{Z}$ is the ring of integers, $\mathbb{Q}$ is the field of rational numbers, $\mathbb{R}$ is the field of real numbers.

For $F \in \{\mathbb{Q}, \mathbb{R}\}$, $F^{>0} := \{x \in F \mid x > 0\}$, $F^{\geq 0} := \{x \in F \mid x \geq 0\}$.

Given $n \in \mathbb{N}$, $\mathbb{N}[K_0, K_1 \dots K_{n-1}]$ will stand for the set of polynomials with natural coefficients in the n variables $K_0, K_1 \dots K_{n-1}$.

For any $t \in \mathbb{R}$, $\lfloor t \rfloor := \max\{n \in \mathbb{Z} \mid n \leq t\}$, $\lceil t \rceil := \min\{n \in \mathbb{Z} \mid n \geq t\}$.

$\log : \mathbb{R}^{\geq 0} \to \mathbb{R} \sqcup \{-\infty\}$ will denote the logarithm in base 2.

Given $n \in \mathbb{N}$, $[n] := \{i \in \mathbb{N} \mid i < n\}$. Given sets $X_0, X_1 \dots X_{n-1}$, $x \in \prod_{i \in [n]} X_i$ and $m \in [n]$, $x_m \in X_m$ is the m-th component of the n-tuple x i.e. $x = (x_0, x_1 \dots x_{n-1})$.

Given a set X and $x, y \in X$, δ_{xy} (or $\delta_{x,y}$) will denote the the Kronecker delta

$$\delta_{xy} := \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases}$$

Given a set X and a subset Y, $\chi_Y : X \to \{0,1\}$ will denote the indicator function of Y (when X is assumed to be known from the context)

$$\chi_Y(x) := \begin{cases} 1 & \text{if } x \in Y \\ 0 & \text{if } x \notin Y \end{cases}$$

$\theta : \mathbb{R} \to \{0,1\}$ will denote the Heaviside step function $\theta := \chi_{[0,\infty)}$. $\operatorname{sgn} : \mathbb{R} \to \{-1,+1\}$ will denote the function $2\theta - 1$.

1.2 Probability distributions

For X a set, $\mathcal{P}(X)$ will denote the set of probability distributions on X. A probability distribution on X can be represented by a function $\mathcal{D} : X \to [0,1]$ s.t. $\sum_{x \in X} \mathcal{D}(x) = 1$. Abusing notation, we will use the same symbol to denote the function and the probability distribution. Given A a subset of X, we will use the notation

$$\mathcal{D}(A) := \Pr_{x \sim \mathcal{D}}[x \in A] = \sum_{x \in A} \mathcal{D}(x)$$

For X a set, $\mathcal{D} \in \mathcal{P}(X)$, V a finite dimensional vector space over $\mathbb{R}$ and $f : X \to V$, $\mathrm{E}_{x \sim \mathcal{D}}[f(x)]$ will denote the expected value of f with respect to $\mathcal{D}$, i.e.

$$\mathrm{E}_{x \sim \mathcal{D}}[f(x)] := \sum_{x \in X} \mathcal{D}(x) f(x)$$

We will the abbreviated notations $\mathrm{E}_{\mathcal{D}}[f(x)]$, $\mathrm{E}[f(x)]$, $\mathrm{E}_{\mathcal{D}}[f]$, $\mathrm{E}[f]$ when no confusion is likely to occur.

Given a set X and $\mathcal{D} \in \mathcal{P}(X)$, $\operatorname{supp} \mathcal{D}$ will denote the support of $\mathcal{D}$ i.e.

$$\operatorname{supp} \mathcal{D} = \{x \in X \mid \mathcal{D}(x) > 0\}$$

Given X, Y sets, $\mathcal{D} \in \mathcal{P}(X)$ and $f : X \to Y$ a mapping, $f_* \mathcal{D} \in \mathcal{P}(Y)$ will denote the corresponding pushforward distribution i.e.

$$(f_* \mathcal{D})(y) := \sum_{x \in f^{-1}(y)} \mathcal{D}(x)$$

Given X, Y sets, the notation $f : X \xrightarrow{\text{mk}} Y$ signifies f is a Markov kernel with source X and target Y. Given $x \in X$, f_x is the corresponding probability distribution on Y and $f(x)$ is a random variable sampled from f_x. Given $\mathcal{D} \in \mathcal{P}(X)$,

$\mathcal{D} \ltimes f \in \mathcal{P}(X \times Y)$ (resp. $f \rtimes \mathcal{D} \in \mathcal{P}(Y \times X)$) is the semidirect product distribution. $f_* \mathcal{D} \in \mathcal{P}(Y)$ is the pushforward distribution, i.e. $f_* \mathcal{D} := \pi_*(\mathcal{D} \ltimes f)$ where $\pi : X \times Y \to Y$ is the projection.

For X a set, $\mathcal{D} \in \mathcal{P}(X)$ and A a subset of X s.t. $\mathcal{D}(A) > 0$, $\mathcal{D} \mid A$ will denote the corresponding conditional probability distribution, i.e. $(\mathcal{D} \mid A)(B) := \frac{\mathcal{D}(B \cap A)}{\mathcal{D}(A)}$. Given Y another set, $f : X \xrightarrow{\text{mk}} Y$ and A a subset of Y s.t. $(\mathcal{D} \ltimes f)(X \times A) > 0$, $\mathcal{D} \mid f^{-1}(A) \in \mathcal{P}(X)$ is defined by

$$(\mathcal{D} \mid f^{-1}(A))(B) := (\mathcal{D} \ltimes f \mid X \times A)(B \times Y)$$

Note that when f is deterministic (i.e. f_x is a Dirac measure for every x), this corresponds to conditioning by the inverse image of A with respect to f. When $A = \{a\}$ we will use the shorthand notation $\mathcal{D} \mid f^{-1}(a)$.

Given X a set and $\mathcal{D}, \mathcal{E} \in \mathcal{P}(X)$, $\mathrm{d_{tv}}(\mathcal{D}, \mathcal{E})$ will denote the total variation distance between $\mathcal{D}$ and $\mathcal{E}$ i.e.

$$\mathrm{d_{tv}}(\mathcal{D}, \mathcal{E}) := \frac{1}{2} \sum_{x \in X} |\mathcal{D}(x) - \mathcal{E}(x)|$$

For X a set and $x \in X$, δ_x will denote the Dirac measure associated with x, i.e. $\delta_x(y) := \delta_{xy}$.

1.3 Algorithms

$\{0,1\}^*$ is the set of all finite binary strings (words), i.e. $\{0,1\}^* := \bigsqcup_{n \in \mathbb{N}} \{0,1\}^n$. For any $x \in \{0,1\}^*$, $|x|$ is the length of x i.e. $x \in \{0,1\}^{|x|}$. $\boldsymbol{\lambda} \in \{0,1\}^*$ is the empty string. For any $n \in \mathbb{N}$

$$\{0,1\}^{\leq n} := \{x \in \{0,1\}^* \mid |x| \leq n\}$$
$$\{0,1\}^{> n} := \{x \in \{0,1\}^* \mid |x| > n\}$$

For any $x \in \{0,1\}^*$ and $n \in \mathbb{N}$, $x_{<n}$ stands for the prefix of x of length n if $|x| \geq n$ and x otherwise. Given $x, y \in \{0,1\}^*$, xy stands for the concatenation of x and y (in particular $|xy| = |x| + |y|$). Given $n \in \mathbb{N}$ and $x_0, x_1 \ldots x_{n-1} \in \{0,1\}^*$, $\prod_{i \in [n]} x_i$ is also concatenation. Given $n \in \mathbb{N}$ and $x, y \in \{0,1\}^n$, $x \cdot y$ stands for $\bigoplus_{i \in [n]} x_i y_i$. For any $n \in \mathbb{N}$, $\mathrm{U}^n \in \mathcal{P}(\{0,1\}^n)$ is the uniform probability distribution.

Given $n \in \mathbb{N}$ and $x_0, x_1 \ldots x_{n-1} \in \{0,1\}^*$, $\langle x_0, x_1 \ldots x_{n-1} \rangle \in \{0,1\}^*$ denotes the encoding of $(x_0, x_1 \ldots x_{n-1})$ obtained by repeating each bit of $x_0, x_1 \ldots x_{n-1}$ twice and inserting the separators 01.

Definition 1.1. An *encoded set* is a set X together with an injection $\mathrm{c}_X : X \to \{0,1\}^*$ (the encoding) s.t. $\operatorname{Im} \mathrm{c}_X$ is decidable in polynomial time.

There are standard encodings we implicitly use throughout. $\mathbf{1}$ denotes an encoded set with 1 element $\bullet$ whose encoding is the empty string. $\{0,1\}^*$ is an encoded set with the trivial encoding $\mathrm{c}_{\{0,1\}^*}(x) := x$. $\mathbb{N}$ is an encoded set where $\mathrm{c}_{\mathbb{N}}(n)$ is the binary representation of n. $\mathbb{Q}$ is an encoded set where $\mathrm{c}_{\mathbb{Q}}(\frac{n}{m}) := \langle n, m \rangle$ for an irreducible fraction $\frac{n}{m}$. For any encoded set X and $L \in \mathrm{P}$, $\{x \in X \mid \mathrm{c}_X(x) \in L\}$ is an encoded set whose encoding is the restriction of c_X. For $X_0, X_1 \ldots X_{n-1}$ encoded sets, $\prod_{i \in [n]} X_i$ is an encoded set with encoding

$$\mathrm{c}_{\prod_{i \in [n]} X_i}(x_0, x_1 \ldots x_{n-1}) := \langle \mathrm{c}_{X_0}(x_0), \mathrm{c}_{X_1}(x_1) \ldots \mathrm{c}_{X_{n-1}}(x_{n-1}) \rangle$$

For any $n \in \mathbb{N}$ we use the shorthand notation $\mathrm{c}^n := \mathrm{c}_{(\{0,1\}^*)^n}$.

Given $n \in \mathbb{N}$, encoded sets $X_0, X_1 \ldots X_{n-1}$ and encoded set Y we use the notation $A : \prod_{i \in [n]} X_i \xrightarrow{\text{alg}} Y$ to mean a Turing machine with n input tapes that halts on every input for which the i-th tape is initialized to a value in $\operatorname{Im} \mathrm{c}_X$ and produces an output in $\operatorname{Im} \mathrm{c}_Y$. Given $\{x_i \in X_i\}_{i \in [n]}$ the notation $A(x_0, x_1 \ldots x_{n-1})$ stands for the unique $y \in Y$ s.t. applying A to the input composed of $\mathrm{c}_{X_i}(x_i)$ results in output $\mathrm{c}_Y(y)$. We use different input tapes for different components of the input instead of encoding the n-tuple as a single word in order to allow A to process some components of the input in time smaller than the length of other components. This involves abuse of notation since a Cartesian product of encoded sets is naturally an encoded set, but hopefully this won't cause much confusion.

Given $A : X \xrightarrow{\text{alg}} Y$ and $x \in X$, $\mathrm{T}_A(x)$ stands for the number of time steps in the computation of $A(x)$.

For any $n \in \mathbb{N}$, we fix $\mathcal{U}_n$, a prefix free universal Turing machine with $n+1$ input tapes: 1 program tape and n tapes that serve as input to the program. Given $n, k \in \mathbb{N}$, $a \in \{0,1\}^*$ and $\{x_i \in \{0,1\}^*\}_{i \in [n]}$, $\mathrm{ev}^k(a; x_0, x_1 \ldots x_{n-1})$ stands for the output of $\mathcal{U}_n$ when executed for k time steps on program a (continued by an infinite sequence of 0s) and inputs $\{x_i \in \{0,1\}^*\}_{i \in [n]}$.

2 Fundamentals

2.1 Basic concepts

2.1.1 Distributional estimation problems

We start with a simple model to help build intuition and motivate the following definitions.

Consider finite sets X and Y, $\mathcal{D} \in \mathcal{P}(X)$, a mapping $m : X \to Y$ and a function $f : X \to \mathbb{R}$. Suppose x was sampled from $\mathcal{D}$ and we were told $y := m(x)$ (but not told x itself). Our expected value of $f(x)$ in these conditions is $\mathrm{E}_{x \sim \mathcal{D}}[f(x) \mid m(x) = y]$.

Let $P : X \to \mathbb{R}$ be the function $P(x) := \mathrm{E}_{x' \sim \mathcal{D}}[f(x') \mid m(x') = m(x)]$. How can we characterize P without referring to the concept of a conditional expected value? For any $Q : X \to \mathbb{R}$ we can consider the "error" $\mathrm{E}_{\mathcal{D}}[(Q - f)^2]$. Q is called "efficient" when it factors as $Q = q \circ m$ for some $q : Y \to \mathbb{R}$. It is easy to see that P has the least error among all efficient functions.

Note that the characterization of P depends not only on f but also on $\mathcal{D}$. That is, the accuracy of an estimator depends on the prior probabilities to encounter different questions. In general, we assume that the possible questions are represented by elements of $\{0,1\}^*$. Thus we need to consider a probability distribution on $\{0,1\}^*$. However, in the spirit of average-case complexity theory we will only require our estimators to be *asymptotically* optimal. Therefore instead of considering a single probability distribution we consider a family of probability distribution indexed by integer parameters[8], where the role of the parameters is defining the relevant limit. We thereby arrive at the following:

Definition 2.1. Fix $n \in \mathbb{N}$. A *word ensemble of rank n* is a family $\{\mathcal{D}^K \in \mathcal{P}(\{0,1\}^*)\}_{K \in \mathbb{N}^n}$.

We will use the notation $\operatorname{supp} \mathcal{D} := \bigcup_{K \in \mathbb{N}^n} \operatorname{supp} \mathcal{D}^K$.

We now introduce our abstraction for a "class of mathematical questions" (with quantitative real-valued answers). This abstraction is a trivial generalization of the concept of a distributional decision problem from average-case complexity theory (see e.g. [4]).

Definition 2.2. Fix $n \in \mathbb{N}$. A *distributional estimation problem of rank n* is a pair $(\mathcal{D}, f)$ where $\mathcal{D}$ is a word ensemble of rank n and $f : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ is bounded.

2.1.2 Growth spaces and polynomial-time Γ-schemes

In the motivational model, the estimator was restricted to lie in a class of functions that factor through a fixed mapping. Of course we are interested in more realistic notions of efficiency. In the present work we consider restrictions on time complexity, access to random bits and size of advice strings. Spatial complexity is also of interest but treating it is out of our current scope. It is possible to consider weaker or stronger

[8] It is convenient to allow more than 1 parameter for reasons that will become clear in section 5. Roughly, some parameters represent the complexity of the input whereas other parameters represent the amount of computing resources available for probability estimation.

restrictions which we represent using the following abstraction which is closely tied to big-$\mathcal{O}$ notation:

Definition 2.3. Fix n. A *growth space* Γ of rank n is a set of functions $\gamma : \mathbb{N}^n \to \mathbb{N}$ s.t.

(i) $0 \in \Gamma$

(ii) If $\gamma_1, \gamma_2 \in \Gamma$ then $\gamma_1 + \gamma_2 \in \Gamma$.

(iii) If $\gamma_1 \in \Gamma$, $\gamma_2 : \mathbb{N}^n \to \mathbb{N}$ and $\forall K \in \mathbb{N}^n : \gamma_2(K) \leq \gamma_1(K)$ then $\gamma_2 \in \Gamma$.

(iv) For any $\gamma \in \Gamma$ there is a $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $\gamma \leq p$.

Example 2.1. For any $n \in \mathbb{N}$, we define Γ_0^n, a growth space of rank n. $\gamma \in \Gamma_0^n$ iff $\gamma \equiv 0$.

Example 2.2. For any $n \in \mathbb{N}$, we define Γ_1^n, a growth space of rank n. $\gamma \in \Gamma_1^n$ iff there is $c \in \mathbb{N}$ s.t. $\gamma \leq c$.

Example 2.3. For any $n \in \mathbb{N}$, we define Γ_{poly}^n, a growth space of rank n.

$$\Gamma_{\text{poly}}^n := \{\gamma : \mathbb{N}^n \to \mathbb{N} \mid \exists p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}] : \gamma \leq p\}$$

Example 2.4. For any $n \in \mathbb{N}$, we define $\Gamma_{\log}^n$, a growth space of rank n. $\gamma \in \Gamma_{\log}^n$ iff there is $c \in \mathbb{N}$ s.t. $\gamma(K_0, K_1 \dots K_{n-1}) \leq c \sum_{i \in [n]} \log(K_i + 1)$.

Definition 2.4. Fix $n \in \mathbb{N}^{>0}$. $\gamma : \mathbb{N}^n \to \mathbb{N}$ is said to be *steadily growing* when

(i) $\gamma \in \Gamma_{\text{poly}}^n$

(ii) $\forall J \in \mathbb{N}^{n-1}, k, l \in \mathbb{N} : k < l \implies \gamma(J, k) \leq \gamma(J, l)$

(iii) There is $s \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t.
$\forall J \in \mathbb{N}^{n-1}, k \in \mathbb{N} : \gamma(J, k) \leq \frac{1}{2}\gamma(J, s(J, k))$.

This could be thought of as a polynomial that is monotonically increasing in the last argument quickly enough that a polynomial increase in the last argument can double the available resources.

Example 2.5. For any $n \in \mathbb{N}^{>0}$ and γ^* steadily growing, we define Γ_{γ^*}, a growth space of rank n. $\gamma \in \Gamma_{\gamma^*}$ iff there is $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $\gamma(J, k) \leq \gamma^*(J, p(J, k))$. This is the space of functions that are bounded above by the reference function γ^* with the last argument growing at a polynomial rate.

To verify condition ii, consider γ_1, γ_2 s.t. $\gamma(J,k) \leq \gamma^*(J, p_1(J,k))$ and $\gamma_2(J,k) \leq \gamma^*(J, p_2(J,k))$. Choose $p, s \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $p \geq \max(p_1, p_2)$ and s is as in condition iii of Definition 2.4.

$$\gamma_1(J,k) + \gamma_2(J,k) \leq \gamma^*(J, p_1(J,k)) + \gamma^*(J, p_2(J,k))$$

$$\gamma_1(J,k) + \gamma_2(J,k) \leq 2\gamma^*(J, p(J,k))$$

$$\gamma_1(J,k) + \gamma_2(J,k) \leq \gamma^*(J, s(J, p(J,k)))$$

In particular taking $\gamma^*_{\mathrm{poly}}(J,k) := k$ and $\gamma^*_{\log}(J,k) := \lfloor \log(k+1) \rfloor$ we have $\Gamma^n_{\mathrm{poly}} = \Gamma_{\gamma^*_{\mathrm{poly}}}$, $\Gamma^n_{\log} = \Gamma_{\gamma^*_{\log}}$.

We now introduce our notion of an "efficient" algorithm.

Definition 2.5. Fix $n \in \mathbb{N}$ and $\Gamma = (\Gamma_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$ a pair of growth spaces of rank n that correspond to the length of the random and advice strings. Given encoded sets X and Y, a *polynomial-time Γ-scheme of signature $X \to Y$* is a triple $(S, \mathrm{r}_S, \mathrm{a}_S)$ where $S : \mathbb{N}^n \times X \times \{0,1\}^* \times \{0,1\}^* \xrightarrow{\mathrm{alg}} Y$, $\mathrm{r}_S : \mathbb{N}^n \times \{0,1\}^* \xrightarrow{\mathrm{alg}} \mathbb{N}$ and $\mathrm{a}_S : \mathbb{N}^n \to \{0,1\}^*$ are s.t.

(i) $\max_{x \in X} \max_{y,z \in \{0,1\}^*} \mathrm{T}_S(K,x,y,z) \in \Gamma^n_{\mathrm{poly}}$

(ii) $\max_{z \in \{0,1\}^*} \mathrm{T}_{\mathrm{r}_S}(K,z) \in \Gamma^n_{\mathrm{poly}}$. Note that r_S, the polynomial-time function that outputs the number of random bits to read, takes the advice string z as input.

(iii) The function $r : \mathbb{N}^n \to \mathbb{N}$ defined by $r(K) := \mathrm{r}_S(K, \mathrm{a}_S(K))$ lies in $\Gamma_{\mathfrak{R}}$.

(iv) $|\mathrm{a}_S| \in \Gamma_{\mathfrak{A}}$

Abusing notation, we denote the polynomial-time Γ-scheme $(S, \mathrm{r}_S, \mathrm{a}_S)$ by S. $S^K(x,y,z)$ will denote $S(K,x,y,z)$, $S^K(x,y)$ will denote $S(K,x,y,\mathrm{a}_S(K))$ and $S^K(x)$ will denote the Y-valued random variable which equals $S(K,x,y,a(K))$ for y sampled from $\mathrm{U}^{\mathrm{r}_S(K)}$. U^K_S will denote $\mathrm{U}^{\mathrm{r}_S(K)}$. We think of S as a randomized algorithm with advice where y are the internal coin tosses and a_S is the advice[9]. Similarly, $\mathrm{r}_S(K)$ will denote $\mathrm{r}_S(K, \mathrm{a}_S(K))$.

[9]Note that the number of random bits $\mathrm{r}_S(K)$ has to be efficiently computable modulo the advice $\mathrm{a}_S(K)$ rather than being an arbitrary function. This requirement is needed to prevent using the function r_S as advice in itself. In particular, when $\Gamma_{\mathfrak{A}} = \Gamma^2_0$, S represents a uniform randomized algorithm.

We will use the notation $S : X \xrightarrow{\Gamma} Y$ to signify S is a polynomial-time Γ-scheme of signature $X \to Y$.

There is a natural notion of composition for polynomial-time Γ-schemes.

Definition 2.6. Fix $n \in \mathbb{N}$ and $\Gamma = (\Gamma_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$ a pair of growth spaces of rank n. Consider encoded sets X, Y, Z and $S : X \xrightarrow{\Gamma} Y$, $T : Y \xrightarrow{\Gamma} Z$. Choose $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $|\mathrm{a}_S(K)| \leq p(K)$ and $|\mathrm{a}_T(K)| \leq p(K)$. We can then construct $U : X \xrightarrow{\Gamma} Z$ s.t. for any $K \in \mathbb{N}^n$, $a, b \in \{0,1\}^{\leq p(K)}$, $v \in \{0,1\}^{\mathrm{r}_T(K,a)}$, $w \in \{0,1\}^{\mathrm{r}_S(K,b)}$ and $x \in X$

$$\mathrm{a}_U(K) = \langle \mathrm{a}_T(K), \mathrm{a}_S(K) \rangle \tag{2.1}$$

$$\mathrm{r}_U(K, \langle a, b \rangle) = \mathrm{r}_T(K, a) + \mathrm{r}_S(K, b) \tag{2.2}$$

$$U^K(x, vw, \langle a, b \rangle) = T^K(S^K(x, w, b), v, a) \tag{2.3}$$

Such a U is called the *composition* of T and S and denoted $U = T \circ S$. There is a slight abuse of notation due to the freedoms in the construction of U but these freedoms have no real significance since all versions of $T \circ S$ induce the same Markov kernel from X to Z.

It will also be useful to consider families of polynomial-time Γ-schemes satisfying uniform resource bounds.

Definition 2.7. Fix $n \in \mathbb{N}$, $\Gamma = (\Gamma_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$ a pair of growth spaces of rank n and encoded sets X, Y. A set F of polynomial-time Γ-schemes of signature $X \to Y$ is called a *uniform family* when

(i) $\max_{S \in F} \max_{x \in X} \max_{y,z \in \{0,1\}^*} \mathrm{T}_S(K, x, y, z) \in \Gamma^n_{\mathrm{poly}}$

(ii) $\max_{S \in F} \max_{z \in \{0,1\}^*} \mathrm{T}_{\mathrm{r}_S}(K, z) \in \Gamma^n_{\mathrm{poly}}$

(iii) $\max_{S \in F} \mathrm{r}_S \in \Gamma_{\mathfrak{R}}$

(iv) $\max_{S \in F} |\mathrm{a}_S(K)| \in \Gamma_{\mathfrak{A}}$

(v) There are only finitely many different machines S and r_S for $S \in F$.

The details of this definition are motivated by the following proposition.

Proposition 2.1. *Fix $n \in \mathbb{N}$ and $\Gamma = (\Gamma_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$ a pair of growth spaces of rank n s.t. $1 \in \Gamma_{\mathfrak{A}}$. Consider X, Y encoded sets, F a uniform family of polynomial-time Γ-schemes of signature $X \to Y$ and a collection $\{\mathcal{S}_K \in F\}_{K \in \mathbb{N}^n}$. Then, there is $\Delta_{\mathcal{S}} : X \xrightarrow{\Gamma} Y$ s.t. for any $K \in \mathbb{N}^n$, $x \in X$ and $y \in Y$, $\Pr[\Delta^K_{\mathcal{S}}(x) = y] = \Pr[\mathcal{S}^K_K(x) = y]$.*

Proof. Choose $p, q \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ (time bounds to emulate an arbitrary randomness function and algorithm from the uniform family) and $\{a_K, b_K \in \{0,1\}^*\}_{K \in \mathbb{N}^n}$ (encodings of the randomness functions and algorithms, which by the definition of a uniform family, can be a finite set) s.t. there is only a finite number of different words a_K and b_K, and for any $K, L \in \mathbb{N}^n$, $x \in X$ and $y, z \in \{0,1\}^*$

$$\mathrm{ev}^{q(L)}(b_K; \mathrm{c}_{\mathbb{N}^n}(L), z) = \mathrm{r}_{S_K}(L, z)$$
$$\mathrm{ev}^{p(L)}(a_K; \mathrm{c}_{\mathbb{N}^n}(L), x, y, z) = S_K^L(x, y, z)$$

Now, use the nonzero advice string to encode which algorithm is to be used on which input. Construct $\Delta_{\mathcal{S}}$ s.t. for any $K \in \mathbb{N}^n$, $x \in X$, $y, w \in \{0,1\}^*$, $u \in \{0,1\}^{\leq \max_{K \in \mathbb{N}^n} |a_K|}$ and $v \in \{0,1\}^{\leq \max_{K \in \mathbb{N}^n} |b_K|}$

$$\mathrm{a}_{\Delta_{\mathcal{S}}}(K) = \langle a_K, b_K, \mathrm{a}_{\mathcal{S}_K}(K) \rangle$$
$$\mathrm{r}_{\Delta_{\mathcal{S}}}(K, \langle u, v, w \rangle) = \mathrm{ev}^{q(K)}(v; \mathrm{c}_{\mathbb{N}^n}(K), w)$$
$$\Delta_{\mathcal{S}}^K(x, y, \langle u, v, w \rangle) = \mathrm{ev}^{p(K)}(u; \mathrm{c}_{\mathbb{N}^n}(K), x, y, w)$$

□

2.1.3 Fall spaces

Fix $n \in \mathbb{N}$ and Γ a pair of growth spaces of rank n. Given a distributional estimation problem $(\mathcal{D}, f)$ and $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$, we can consider the estimation error $\mathrm{E}_{(x,y) \sim \mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K(x,y) - f(x))^2]$. It makes little sense to require this error to be minimal for every $K \in \mathbb{N}^n$, since we can always hard-code a finite number of answers into Q without violating the resource restrictions. Instead we require minimization up to an asymptotically small error. Since it makes sense to consider different kind of asymptotic requirements, we introduce an abstraction that corresponds to this choice.

Definition 2.8. Given $n \in \mathbb{N}$, a *fall space of rank* n is a set $\mathcal{F}$ of bounded functions $\varepsilon : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$ s.t.

(i) If $\varepsilon_1, \varepsilon_2 \in \mathcal{F}$ then $\varepsilon_1 + \varepsilon_2 \in \mathcal{F}$.

(ii) If $\varepsilon_1 \in \mathcal{F}$, $\varepsilon_2 : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$ and $\forall K \in \mathbb{N}^n : \varepsilon_2(K) \leq \varepsilon_1(K)$ then $\varepsilon_2 \in \mathcal{F}$.

(iii) There is $h \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $2^{-h} \in \mathcal{F}$.

Example 2.6. We define $\mathcal{F}_{\text{neg}}$, a fall space of rank 1. For any $\varepsilon : \mathbb{N} \to \mathbb{R}^{\geq 0}$ bounded, $\varepsilon \in \mathcal{F}_{\text{neg}}$ iff for any $d \in \mathbb{N}$, $\lim_{k\to\infty} k^d \varepsilon(k) = 0$.

Example 2.7. For any $n \in \mathbb{N}$ and $\zeta : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$, we define $\mathcal{F}_\zeta$ to be the set of $\varepsilon : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$ bounded s.t. there is $M \in \mathbb{R}$ for which $\varepsilon \leq M\zeta$. If there is $h \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $\zeta \geq 2^{-h}$ then $\mathcal{F}_\zeta$ is a fall space of rank n.

Example 2.8. For any $n \in \mathbb{N}^{>0}$ and $\varphi : \mathbb{N}^{n-1} \to \mathbb{N} \sqcup \{\infty\}$, we define $\mathcal{F}_{\text{uni}}^{(\varphi)}$, a fall space of rank n. For any $\varepsilon : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$ bounded, $\varepsilon \in \mathcal{F}_{\text{uni}}^{(\varphi)}$ iff there are $M \in \mathbb{R}^{>0}$ and $p \in \mathbb{N}[J_0, J_1 \dots J_{n-2}]$ s.t.

$$\forall J \in \mathbb{N}^{n-1} : \sum_{k=2}^{\varphi(J)-1} \frac{\varepsilon(J,k)}{k \log k} \leq M \log\log p(J) \tag{2.4}$$

To verify condition iii note that $2^{-K_{n-1}} \in \mathcal{F}_{\text{uni}}^{(t)}$.

For $\varphi \equiv \infty$ we use the notation $\mathcal{F}_{\text{uni}}^{(n)} := \mathcal{F}_{\text{uni}}^{(\varphi)}$.

For example, if $\varepsilon_1(J,k) := \frac{\log\log p(J)}{\log(k+2)}$ and $\varepsilon_2(J,k) := \frac{\log\log p(J)}{\log\log(k+2)}$, then $\varepsilon_1(J,k) \in \mathcal{F}_{\text{uni}}^{(n)}$, but $\varepsilon_2(J,k) \notin \mathcal{F}_{\text{uni}}^{(n)}$ because it falls too slowly to force the sum to converge.

Example 2.9. For any $n \in \mathbb{N}^{>0}$, we define $\mathcal{F}_{\text{mon}}^{(n)}$, a fall space of rank n. For any $\varepsilon : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$ bounded, $\varepsilon \in \mathcal{F}_{\text{mon}}^{(n)}$ iff the function $\bar{\varepsilon} : \mathbb{N}^n \to \mathbb{R}^{\geq 0}$ defined by $\bar{\varepsilon}(J,k) := \sup_{l \geq k} \varepsilon(J,l)$ satisfies $\bar{\varepsilon} \in \mathcal{F}_{\text{uni}}^{(n)}$.

The main motivation for examples 2.8 and 2.9 are the existence theorems proven in Section 5.

We note a few simple properties of fall spaces which will be useful in the following.

Proposition 2.2. *For any fall space $\mathcal{F}$, $0 \in \mathcal{F}$.*

Proof. Follows from conditions ii and iii, since $0 \leq 2^{-h}$. □

Proposition 2.3. *For any fall space $\mathcal{F}$, $\varepsilon \in \mathcal{F}$ and $c \in \mathbb{R}^{\geq 0}$, $c\varepsilon \in \mathcal{F}$.*

Proof. By induction, condition i implies that for any $m \in \mathbb{N}$, $m\varepsilon \in \mathcal{F}$. It follows that $c\varepsilon \in \mathcal{F}$ since $c\varepsilon \leq \lceil c \rceil \varepsilon$. □

Proposition 2.4. *For any fall space $\mathcal{F}$ and $\varepsilon_1, \varepsilon_2 \in \mathcal{F}$, $\max(\varepsilon_1, \varepsilon_2) \in \mathcal{F}$*

Proof.

$$\max(\varepsilon_1, \varepsilon_2) \leq \varepsilon_1 + \varepsilon_2$$

Proposition 2.5. *For any fall space $\mathcal{F}$, $\varepsilon \in \mathcal{F}$ and $\alpha \in \mathbb{R}$, if $\alpha \geq 1$ then $\varepsilon^\alpha \in \mathcal{F}$.*

Proof.

$$\varepsilon^\alpha = (\sup \varepsilon)^\alpha \left(\frac{\varepsilon}{\sup \varepsilon}\right)^\alpha \leq (\sup \varepsilon)^\alpha \frac{\varepsilon}{\sup \varepsilon} \in \mathcal{F}$$

□

Definition 2.9. For any fall space $\mathcal{F}$ and $\alpha \in \mathbb{R}^{>0}$, we define $\mathcal{F}^\alpha := \{\varepsilon^\alpha \mid \varepsilon \in \mathcal{F}\}$.

Proposition 2.6. *Consider $\mathcal{F}$ a fall space and $\alpha \in \mathbb{R}^{>0}$. Then, $\mathcal{F}^\alpha$ is a fall space.*

Proof. To check condition i, consider $\varepsilon_1, \varepsilon_2 \in \mathcal{F}$.

If $\alpha > 1$, $(\varepsilon_1^\alpha + \varepsilon_2^\alpha)^{\frac{1}{\alpha}} \leq \varepsilon_1 + \varepsilon_2 \in \mathcal{F}$ hence $(\varepsilon_1^\alpha + \varepsilon_2^\alpha)^{\frac{1}{\alpha}} \in \mathcal{F}$ and $\varepsilon_1^\alpha + \varepsilon_2^\alpha \in \mathcal{F}^\alpha$.

If $\alpha \leq 1$, $(\varepsilon_1^\alpha + \varepsilon_2^\alpha)^{\frac{1}{\alpha}} = 2^{\frac{1}{\alpha}} (\frac{\varepsilon_1^\alpha + \varepsilon_2^\alpha}{2})^{\frac{1}{\alpha}} \leq 2^{\frac{1}{\alpha}} \frac{\varepsilon_1 + \varepsilon_2}{2} \in \mathcal{F}$ hence $(\varepsilon_1^\alpha + \varepsilon_2^\alpha)^{\frac{1}{\alpha}} \in \mathcal{F}$ and $\varepsilon_1^\alpha + \varepsilon_2^\alpha \in \mathcal{F}^\alpha$.

Conditions ii and iii are obvious. □

Proposition 2.7. *Consider $\mathcal{F}$ a fall space and $\alpha_1, \alpha_2 \in \mathbb{R}^{>0}$ with $\alpha_1 \leq \alpha_2$. Then, $\mathcal{F}^{\alpha_2} \subseteq \mathcal{F}^{\alpha_1}$.*

Proof. Follows from Proposition 2.5. □

Definition 2.10. For any $n \in \mathbb{N}$, fall space $\mathcal{F}$ of rank n and $\gamma : \mathbb{N}^n \to \mathbb{R}$ s.t. $\inf \gamma > 0$, we define $\gamma\mathcal{F} := \{\gamma\varepsilon \text{ bounded} \mid \varepsilon \in \mathcal{F}\}$.

Proposition 2.8. *For any $n \in \mathbb{N}$, fall space $\mathcal{F}$ of rank n and $\gamma : \mathbb{N}^n \to \mathbb{R}$ s.t. $\inf \gamma > 0$, $\gamma\mathcal{F}$ is a fall space.*

Proof. Conditions i and ii are obvious. To verify condition iii note that for any $\varepsilon \in \mathcal{F}$ we have $\frac{\varepsilon}{\gamma} \leq \frac{\varepsilon}{\inf \gamma} \in \mathcal{F}$ and therefore $\varepsilon = \gamma\frac{\varepsilon}{\gamma} \in \gamma\mathcal{F}$. In particular if $h \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ is s.t. $2^{-h} \in \mathcal{F}$ then $2^{-h} \in \gamma\mathcal{F}$. □

We will use several shorthand notations for relations between functions that hold "up to a function in $\mathcal{F}$." Given $f, g : \mathbb{N}^n \to \mathbb{R}$, the notation $f(K) \leq g(K) \pmod{\mathcal{F}}$ means

$$\exists \varepsilon \in \mathcal{F} \forall K \in \mathbb{N}^n : f(K) \leq g(K) + \varepsilon(K)$$

Similarly, $f(K) \geq g(K) \pmod{\mathcal{F}}$ means

$$\exists \varepsilon \in \mathcal{F} \forall K \in \mathbb{N}^n : f(K) \geq g(K) - \varepsilon(K)$$

$f(K) \equiv g(K) \pmod{\mathcal{F}}$ means $|f - g| \in \mathcal{F}$.

For families $\{f_\alpha, g_\alpha : \mathbb{N}^n \to \mathbb{R}\}_{\alpha \in I}$ (where I is some set), $f_\alpha(K) \overset{\alpha}{\leq} g_\alpha(K) \pmod{\mathcal{F}}$ means that

$$\exists \varepsilon \in \mathcal{F} \forall \alpha \in I, K \in \mathbb{N}^n : f_\alpha(K) \leq g_\alpha(K) + \varepsilon(K)$$

$f_\alpha(K) \overset{\alpha}{\geq} g_\alpha(K) \pmod{\mathcal{F}}$ and $f_\alpha(K) \overset{\alpha}{\equiv} g_\alpha(K) \pmod{\mathcal{F}}$ are defined analogously.

2.1.4 Optimal polynomial-time estimators

We are now ready to give our central definition, which corresponds to a notion of "expected value" for distributional estimation problems.

Definition 2.11. Fix $n \in \mathbb{N}$, Γ a pair of growth spaces of rank n and $\mathcal{F}$ a fall space of rank n. Consider $(\mathcal{D}, f)$ a distributional estimation problem and $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ with bounded range. P is called an $\mathcal{F}(\Gamma)$-*optimal polynomial-time estimator for* $(\mathcal{D}, f)$ when for any $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] \pmod{\mathcal{F}} \tag{2.5}$$

For the sake of brevity, we will say "$\mathcal{F}(\Gamma)$-optimal estimator" rather than "$\mathcal{F}(\Gamma)$-optimal polynomial-time estimator."

Distributional *decision* problems are the special case when the range of f is $\{0,1\}$. In this special case, the outputs of an optimal polynomial-time estimator can be thought of as probabilities[10].

2.2 Basic properties

From now on we fix $n \in \mathbb{N}^{>0}$, $\Gamma := (\Gamma_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$ a pair of growth spaces of rank n and $\mathcal{F}$ a fall space of rank n. All word ensembles and distributional estimation problems will be of rank n unless specified otherwise.

In this subsection we discuss some basic properties of optimal polynomial-time estimators which will be used in the following.

[10] With some caveats. First, P can take values outside $[0,1]$ but it's easy to see that clipping all values to $[0,1]$ preserves optimality. Second, $P^K(x,y) = 1$ doesn't imply $f(x) = 1$ and $P^K(x,y) = 0$ doesn't imply $f(x) = 0$. We can try to fix this using a logarithmic error function instead of the squared norm, however this creates other difficulties and is outside the scope of the present work.

2.2.1 Optimality relative to uniform families

Note that ε in 2.5 depends on Q. However in some sense the optimality condition is automatically uniform w.r.t. the resources required by Q. The following Proposition 2.9 can be used to reduce domination of a uniform family to domination of a single polynomial-time Γ-scheme constructed via Proposition 2.1.

Proposition 2.9. *Consider $(\mathcal{D}, f)$ a distributional estimation problem, P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$ and F a uniform family of polynomial-time Γ-schemes of signature $\{0,1\}^* \to \mathbb{Q}$. Then there is $\varepsilon \in \mathcal{F}$ s.t. for any $Q \in F$*

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] + \varepsilon(K) \tag{2.6}$$

Proof. For any $K \in \mathbb{N}^n$, $\{\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] \mid Q \in F\}$ is a finite set because F is a uniform family so the runtime of Q^K is bounded by a polynomial in K that doesn't depend on Q. Therefore we can choose

$$Q_K \in \arg\min_{Q \in F} \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2]$$

By Proposition 2.1, there is $\bar{Q} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\bar{Q}^K(x)$ is distributed the same as $Q_K^K(x)$.

Since P is an $\mathcal{F}(\Gamma)$-optimal estimator, there is $\varepsilon \in \mathcal{F}$ s.t.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{\bar{Q}}^K}[(\bar{Q}^K - f)^2] + \varepsilon(K) \tag{2.7}$$

For any $Q \in F$, we have

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{\bar{Q}}^K}[(\bar{Q}^K - f)^2] = \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{Q_K}^K}[(Q_K^K - f)^2]$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{\bar{Q}}^K}[(\bar{Q}^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] \tag{2.8}$$

Combining 2.7 and 2.8 we get the desired result. □

2.2.2 Random versus advice

As usual, random is no more powerful than advice (see e.g. Theorem 6.3 in [12]). This is demonstrated by the following two propositions.

Proposition 2.10. *Observe that $\bar{\Gamma}_{\mathfrak{R}} := \Gamma_{\mathfrak{R}} + \Gamma_{\mathfrak{A}}$ is a growth space and denote $\bar{\Gamma} := (\bar{\Gamma}_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$. Consider $(\mathcal{D}, f)$ a distributional estimation problem and P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. Then, P is also an $\mathcal{F}(\bar{\Gamma})$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. The proof will proceed by taking a Q with access to extra randomness, and then considering another algorithm $\overline{Q}$ with access to the old amount of randomness, which uses the advice to encode an optimal prefix to the random string. Then we just need to show that $\overline{Q}$ dominates Q and is dominated by P. This proof strategy also applies to the next proposition.

Consider any $Q : \{0,1\}^* \xrightarrow{\bar{\Gamma}} \mathbb{Q}$. Suppose $\mathrm{r}_Q = r_{\mathfrak{R}} + r_{\mathfrak{A}}$ where $r_{\mathfrak{R}} \in \Gamma_{\mathfrak{R}}$ and $r_{\mathfrak{A}} \in \Gamma_{\mathfrak{A}}$. For any $K \in \mathbb{N}^n$, choose

$$\bar{\mathrm{a}}_Q(K) \in \operatorname*{arg\,min}_{y \in \{0,1\}^{r_{\mathfrak{A}}(K)}} \mathrm{E}_{(x,z)\sim \mathcal{D}^K \times U^{r_{\mathfrak{R}}(K)}}[(Q^K(x, yz) - f(x))^2]$$

As is easy to see, there is $\bar{Q} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for all $K \in \mathbb{N}^n$, $x \in \operatorname{supp} \mathcal{D}^K$ and $z \in \{0,1\}^{r_{\mathfrak{R}}(K)}$

$$\begin{aligned} \mathrm{a}_{\bar{Q}}(K) &= \langle \mathrm{a}_Q(K), \bar{\mathrm{a}}_Q(K) \rangle \\ \mathrm{r}_{\bar{Q}}(K) &= r_{\mathfrak{R}}(K) \\ \bar{Q}^K(x, z) &= Q^K(x, \bar{\mathrm{a}}_Q(K) z) \end{aligned}$$

It follows that there is $\varepsilon \in \mathcal{F}$ s.t.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times U^{r_{\mathfrak{R}}(K)}}[(\bar{Q}^K - f)^2] + \varepsilon(K)$$

Obviously $\mathrm{E}_{\mathcal{D}^K \times U^{r_{\mathfrak{R}}(K)}}[(\bar{Q}^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2]$ therefore

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] + \varepsilon(K)$$

□

Proposition 2.11. *Denote $\bar{\Gamma}_{\mathfrak{R}} := \Gamma_{\mathfrak{R}} + \Gamma_{\mathfrak{A}}$ and $\bar{\Gamma} := (\bar{\Gamma}_{\mathfrak{R}}, \Gamma_{\mathfrak{A}})$. Consider $(\mathcal{D}, f)$ a distributional estimation problem and $\bar{P}$ an $\mathcal{F}(\bar{\Gamma})$-optimal estimator for $(\mathcal{D}, f)$. Then, there exists an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. Suppose $\mathrm{r}_{\bar{P}} = r_{\mathfrak{R}} + r_{\mathfrak{A}}$ where $r_{\mathfrak{R}} \in \Gamma_{\mathfrak{R}}$ and $r_{\mathfrak{A}} \in \Gamma_{\mathfrak{A}}$. For any $K \in \mathbb{N}^n$, choose

$$\bar{\mathrm{a}}_P(K) \in \operatorname*{arg\,min}_{y \in \{0,1\}^{r_{\mathfrak{A}}(K)}} \mathrm{E}_{(x,z)\sim \mathcal{D}^K \times \mathrm{U}^{r_{\mathfrak{R}}(K)}}[(\bar{P}^K(x, yz) - f(x))^2]$$

We can construct $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ so that for all $K \in \mathbb{N}^n$, $x \in \operatorname{supp} \mathcal{D}^K$ and $z \in \{0,1\}^{r_{\mathfrak{R}}(K)}$

$$\begin{aligned} \mathrm{a}_P(K) &:= \langle \mathrm{a}_{\bar{P}}(K), \bar{\mathrm{a}}_P(K) \rangle \\ \mathrm{r}_P(K) &= r_{\mathfrak{R}}(K) \\ P^K(x,z) &= \bar{P}^K(x, \bar{\mathrm{a}}_P(K)z) \end{aligned}$$

Clearly $\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^{r_{\mathfrak{R}}(K)}}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{\bar{P}}}[(\bar{P}^K - f)^2]$ and therefore P is an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. □

2.2.3 Optimality of weighted error

Although the word ensemble plays a central role in the definition of an optimal polynomial-time estimator, the dependence on the word ensemble is lax in some sense. To see this, consider the following proposition.

Definition 2.12. Given a growth space Γ_* of rank n, $\mathcal{F}$ is called Γ_*-*ample* when there is $\zeta : \mathbb{N}^n \to (0, \frac{1}{2}]$ s.t. $\zeta \in \mathcal{F}$ and $\lfloor \log \frac{1}{\zeta} \rfloor \in \Gamma_*$.

The intuitive interpretation of this is that, when Γ_* represents the amount of advice, the advice bits are sufficient to write down an approximation to some parameter with error at most ζ.

Example 2.10. Any fall space of rank n is Γ^n_{poly}-ample, due to condition iii of Definition 2.8.

Example 2.11. $\mathcal{F}^{(n)}_{\mathrm{uni}}$ is $\Gamma^n_{\log}$-ample since we can take $\zeta(K) := (K_{n-1} + 2)^{-1}$.

Proposition 2.12. *Assume $\mathcal{F}$ is $\Gamma_{\mathfrak{A}}$-ample. Consider $(\mathcal{D}, f)$ a distributional estimation problem, P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$, $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ and $W : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}^{\geq 0}$ bounded s.t. $\mathrm{r}_W \geq \max(\mathrm{r}_P, \mathrm{r}_Q)$. Denote $\mathcal{D}^K_W := \mathcal{D}^K \times \mathrm{U}^K_W$. Then*

$$\begin{aligned} &\mathrm{E}_{\mathcal{D}^K_W}[W^K(x,y)(P^K(x, y_{<\mathrm{r}_P(K)}) - f(x))^2] \\ &\qquad \leq \mathrm{E}_{\mathcal{D}^K_W}[W^K(x,y)(Q^K(x, y_{<\mathrm{r}_Q(K)}) - f(x))^2] \pmod{\mathcal{F}} \end{aligned}$$

This essentially says that if there is enough advice available, then an optimal estimator continues to be optimal when a poly-time adversary assigns weights to how important the various problem instances are. The proof will come after the following corollary.

The relationship to the role of the word ensemble is as follows.

Corollary 2.1. *Assume $\mathcal{F}$ is $\Gamma_{\mathfrak{A}}$-ample. Consider $(\mathcal{D}, f)$ a distributional estimation problem and P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. Consider $W : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}^{\geq 0}$ bounded s.t. for any $K \in \mathbb{N}^n$ there is $x \in \operatorname{supp} \mathcal{D}^K$ and $y \in \{0,1\}^{\mathrm{r}_W(K)}$ s.t. $W^K(x,y) > 0$. Define $\gamma : \mathbb{N}^n \to \mathbb{R}$ by $\gamma(K) := \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K]^{-1}$ and denote $\mathcal{F}_W := \gamma\mathcal{F}$. Define the word ensemble $\mathcal{E}$ by*

$$\mathcal{E}^K(x) := \frac{\mathrm{E}_{y \sim \mathrm{U}_W^K}[W^K(x,y)]\mathcal{D}^K(x)}{\mathrm{E}_{(x',y) \sim \mathcal{D}^K \times \mathrm{U}_W^K}[W^K(x',y)]}$$

Then, P is an $\mathcal{F}_W(\Gamma)$-optimal estimator for $(\mathcal{E}, f)$.

That is, if the distribution on problem instances is reweighted by a poly-time adversary, an optimal estimator will continue being optimal, although with an increased error if the expected weight assigned by the adversary keeps falling as K grows. Therefore, the property of being an optimal estimator is robust against some types of "distributional shift", when sufficient advice is available.

Proof of Corollary 2.1. Consider any $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$. Proposition 2.12 implies there is $\varepsilon \in \mathcal{F}$ s.t.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_W^K}[W^K(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K \times \mathrm{U}_W^K}[W^K(Q^K - f)^2] + \varepsilon(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[\mathrm{E}_{\mathrm{U}_W^K}[W^K](P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[\mathrm{E}_{\mathrm{U}_W^K}[W^K](Q^K - f)^2] + \varepsilon(K)$$

Dividing both sides of the inequality by $\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K(x)]$ we get

$$\mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] + \frac{\varepsilon(K)}{\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K(x)]}$$

Let M be the supremum of the left hand side.

$$\mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] + \min\left(\frac{\varepsilon(K)}{\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K(x)]}, M\right)$$

The second term on the right hand side is clearly in $\mathcal{F}_W$. □

We now give the proof of Proposition 2.12.

Proof of Proposition 2.12. The proof will construct a uniform family of algorithms that use their advice to encode an approximation of some number t, and use P if W assigns a weight less than the approximation, and Q otherwise. P dominates all the algorithms in this family, and after some reshuffling, and integrating over t, W can be recovered, and this leads to the desired result.

Consider $\zeta : \mathbb{N}^n \to (0, \frac{1}{2}]$ s.t. $\zeta \in \mathcal{F}$ and $\lfloor \log \frac{1}{\zeta} \rfloor \in \Gamma_{\mathfrak{A}}$. For any $K \in \mathbb{N}^n$ and $t \in \mathbb{R}$, let $\rho_\zeta^K(t) \in \operatorname*{arg\,min}_{s \in \mathbb{Q} \cap [t-\zeta(K), t+\zeta(K)]} |\mathrm{c}_{\mathbb{Q}}(s)|$. Denote $M := \sup W$. It is easy to see that there is $\gamma \in \Gamma_{\mathfrak{A}}$ s.t. for any $t \in [0, M]$, $|\mathrm{c}_{\mathbb{Q}}(\rho_\zeta^K(t))| \leq \gamma(K)$.

For any $t \in \mathbb{R}$ there is $Q_t : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_Q = \mathrm{r}_W$ and for any $x \in \operatorname{supp} \mathcal{D}^K$ and $y \in \{0,1\}^{\mathrm{r}_W(K)}$

$$Q_t^K(x,y) = \begin{cases} Q^K(x, y_{<\mathrm{r}_Q(K)}) \text{ if } W^K(x,y) \geq \rho_\zeta^K(t) \\ P^K(x, y_{<\mathrm{r}_P(K)}) \text{ if } W^K(x,y) < \rho_\zeta^K(t) \end{cases}$$

Moreover we can construct the Q_t for all $t \in [0, M]$ s.t. they form a uniform family. By Proposition 2.9 there is $\varepsilon \in \mathcal{F}$ s.t. for all $t \in [0, M]$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[(Q_t^K - f)^2] + \varepsilon(K)$$

$$\mathrm{E}_{(x,y) \sim \mathcal{D}^K \times \mathrm{U}_W^K}[(P^K(x, y_{<\mathrm{r}_P(K)}) - f(x))^2 - (Q_t^K(x,y) - f(x))^2] \leq \varepsilon(K)$$

The expression inside the expected values vanishes when $W^K(x,y) < \rho_\zeta^K(t)$. In other cases,

$$Q_t^K(x,y) = Q^K(x, y_{<\mathrm{r}_Q(K)})$$

We get

$$\mathrm{E}_{(x,y) \sim \mathcal{D}^K \times \mathrm{U}_W^K}[\theta(W^K(x,y) - \rho_\zeta^K(t)) \cdot \\ ((P^K(x, y_{<\mathrm{r}_P(K)}) - f(x))^2 - (Q^K(x, y_{<\mathrm{r}_Q(K)}) - f(x))^2)] \leq \varepsilon(K)$$

We integrate both sides of the inequality over t from 0 to M.

$$\mathrm{E}\left[\int_0^M \theta(W^K - \rho_\zeta^K(t))\, \mathrm{d}t \cdot ((P^K - f)^2 - (Q^K - f)^2)\right] \leq M\varepsilon(K) \tag{2.9}$$

For any $s \in \mathbb{R}$

$$\int_0^M \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t = \int_0^{s-\zeta(K)} \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t + \int_{s-\zeta(K)}^{s+\zeta(K)} \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t + \int_{s+\zeta(K)}^{M} \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t$$

$|\rho_\zeta^K(t)-t| \leq \zeta(K)$ therefore the integrand in the first term is 1 and in the last term 0:

$$\int_0^M \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t = \int_0^{s-\zeta(K)} \mathrm{d}t + \int_{s-\zeta(K)}^{s+\zeta(K)} \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t$$

$$\int_0^M \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t = s-\zeta(K) + \int_{s-\zeta(K)}^{s+\zeta(K)} \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t$$

$$\int_0^M \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t - s = -\zeta(K) + \int_{s-\zeta(K)}^{s+\zeta(K)} \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t$$

$$\int_0^M \theta(s-\rho_\zeta^K(t))\,\mathrm{d}t - s \in [-\zeta(K), \zeta(K)] \tag{2.10}$$

Combining 2.9 and 2.10 we conclude that for some $M' \in \mathbb{R}$

$$\mathrm{E}[W^K \cdot ((P^K-f)^2 - (Q^K-f)^2)] \leq M\varepsilon(K) + M'\zeta(K)$$

□

2.2.4 Amplification from zero to $O(1)$ advice

The following will be handy to prove negative existence results (see section 5).

Proposition 2.13. *Assume $\Gamma_{\mathfrak{A}} = \Gamma_0^n$. Consider $(\mathcal{D}, f)$ a distributional estimation problem and P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. Denote $\Gamma_1 := (\Gamma_{\mathfrak{R}}, \Gamma_1^n)$. Then, P is also an $\mathcal{F}(\Gamma_1)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. This proof proceeds by using the standard "domination of a uniform family" result to dominate all the algorithms with a bounded-size advice string that never changes. An algorithm with constant advice can be interpreted as switching around within this family, and thus is dominated. Consider any $Q : \{0,1\}^* \xrightarrow{\Gamma_1} \mathbb{Q}$. Choose $l \in \mathbb{N}$ s.t. $\forall K \in \mathbb{N}^n : |\mathrm{a}_Q(K)| \leq l$. For each $a \in \{0,1\}^{\leq l}$, construct $Q_a : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $K \in \mathbb{N}^n$, $x, y \in \{0,1\}^*$

$$\mathrm{r}_{Q_a}(K) = \mathrm{r}_Q(K, a)$$
$$Q_a^K(x, y) = Q^K(x, y, a)$$

For some $\varepsilon_a \in \mathcal{F}$ we have

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{Q_a}^K}[(Q_a^K - f)^2] + \varepsilon_a(K)$$

Since the above holds for every $a \in \{0,1\}^{\leq l}$, we get

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] + \varepsilon_{\mathrm{a}_Q(K)}(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] + \sum_{a \in \{0,1\}^{\leq l}} \varepsilon_a(K)$$

□

2.3 Orthogonality theorems

There is a variant of Definition 2.11 which is nearly equivalent in many cases and often useful.

We can think of functions $f : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ as vectors in a real inner product space with inner product $\langle f, g \rangle := \mathrm{E}_{\mathcal{D}}[fg]$. Informally, we can think of polynomial-time Γ-schemes as a subspace (although a polynomial-time Γ-scheme is not even a function) and an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$ as the nearest point to f in this subspace. Now, given an inner product space V, a vector $f \in V$, an actual subspace $W \subseteq V$ and $p = \arg\min_{q \in W} \|q - f\|^2$, we have $\forall v \in W : \langle p - f, v \rangle = 0$. This motivates the following:

Definition 2.13. Consider $(\mathcal{D}, f)$ a distributional estimation problem and $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ with bounded range. P is called an $\mathcal{F}^\sharp(\Gamma)$-*optimal polynomial-time estimator for* $(\mathcal{D}, f)$ when for any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ with bounded range[11]

$$\mathrm{E}_{(x,y,z) \sim \mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K(x, y) - f(x)) S^K(x, P^K(x, y), z)] \equiv 0 \pmod{\mathcal{F}} \quad (2.11)$$

[11] The $\mathbb{Q}$-valued argument of S is only important for non-trivial $\Gamma_{\mathfrak{R}}$, otherwise we can absorb it into the definition of S using P as a subroutine.

For the sake of brevity, we will say "$\mathcal{F}^\sharp(\Gamma)$-optimal estimator" rather than "$\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator." This definition is interesting because it can be interpreted as a game against an adversary that is allowed to look at what the estimator outputs, which then predicts whether the estimator will overestimate or underestimate the true value. $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimators are inexploitable against this class of adversaries. As we will show shortly, inexploitability is a slightly stronger condition than optimality, in the sense than any $\mathcal{F}^\sharp(\Gamma)$-optimal polynomial-time estimator is $\mathcal{F}$-optimal, but going in the other direction requires at most logarithmic advice and is associated with an increase in the error. The inexploitability property will be used in many additional proofs.

The following theorem is the analogue in our language of the previous fact about inner product spaces. The notation $\mathcal{F}^{\frac{1}{2}}$ refers to Definition 2.9, i.e. it is just the set of square roots of all the functions in $\mathcal{F}$.

Theorem 2.1. *Assume there is $\zeta : \mathbb{N}^n \to (0, \frac{1}{4}]$ s.t. $\zeta \in \mathcal{F}^{\frac{1}{2}}$ and $\lfloor \log\log \frac{1}{\zeta} \rfloor \in \Gamma_{\mathfrak{A}}$[12]. Consider $(\mathcal{D}, f)$ a distributional estimation problem and P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. Then, P is also an $\mathcal{F}^{\frac{1}{2}\sharp}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. Assume without loss of generality that there is $h \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $\zeta \geq 2^{-h}$ (otherwise we can take any $h \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $2^{-h} \in \mathcal{F}$ and consider $\zeta' := \zeta + 2^{-h}$). Fix $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Consider any $\sigma : \mathbb{N}^n \to \{\pm 1\}$ and $m : \mathbb{N}^n \to \mathbb{N}$ s.t. $m \leq \log \frac{1}{\zeta}$ (in particular $m \leq h$). Define $t(K) := \sigma(K) 2^{-m(K)}$. It is easy to see there is $Q_t : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_{Q_t} = \mathrm{r}_P + \mathrm{r}_S$ and given $K \in \mathbb{N}^n$, $x \in \operatorname{supp} \mathcal{D}^K$, $y \in \{0,1\}^{\mathrm{r}_P(K)}$ and $z \in \{0,1\}^{\mathrm{r}_S(K)}$

$$Q_t^K(x, yz) = P^K(x, y) - t(K) S^K(x, P^K(x, y), z)$$

Moreover, we can construct Q_t for all admissible choices of t (but fixed S) to get a uniform family.

Applying Proposition 2.9, we conclude that there is $\varepsilon \in \mathcal{F}$ which doesn't depend on t s.t.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(Q_t^K - f)^2] + \varepsilon(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - t(K) S^K - f)^2] + \varepsilon(K)$$

[12] If $\Gamma_{\log}^n \subseteq \Gamma_{\mathfrak{A}}$ then this condition holds for any $\mathcal{F}$ since we can take $\zeta = 2^{-h}$ for $h \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)^2 - (P^K - t(K)S^K - f)^2] \leq \varepsilon(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(-t(K)(S^K)^2 + 2(P^K - f))S^K]t(K) \leq \varepsilon(K)$$

$$-\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(S^K)^2]t(K)^2 + 2\,\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K]t(K) \leq \varepsilon(K)$$

$$2\,\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K]t(K) \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(S^K)^2]t(K)^2 + \varepsilon(K)$$

$$2\,\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K]t(K) \leq (\sup|S^K|)^2 t(K)^2 + \varepsilon(K)$$

$$2\,\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K]\sigma(K)2^{-m(K)} \leq (\sup|S^K|)^2 4^{-m(K)} + \varepsilon(K)$$

Multiplying both sides by $2^{m(K)-1}$ we get

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K]\sigma(K) \leq \frac{1}{2}\left((\sup|S^K|)^2 2^{-m(K)} + \varepsilon(K)2^{m(K)}\right)$$

Let $\sigma(K) := \operatorname{sgn} \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_S^K}[(P^K - f)S^K]$.

$$|\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K]| \leq \frac{1}{2}((\sup|S^K|)^2 2^{-m(K)} + \varepsilon(K)2^{m(K)})$$

Let $m(K) := \min\left(\lfloor \frac{1}{2}\log\max(\frac{1}{\varepsilon(K)}, 1)\rfloor, \lfloor \log \frac{1}{\zeta(K)}\rfloor\right)$.

$$|\mathrm{E}[(P^K - f)S^K]| \leq (\sup|S^K|)^2 \max\left(\min\left(\varepsilon(K)^{\frac{1}{2}}, 1\right), \zeta(K)\right) + \frac{1}{2}\varepsilon(K)\min\left(\max\left(\varepsilon(K)^{-\frac{1}{2}}, 1\right), \zeta(K)^{-1}\right)$$

$$|\mathrm{E}[(P^K - f)S^K]| \leq (\sup|S^K|)^2 \max\left(\varepsilon(K)^{\frac{1}{2}}, \zeta(K)\right) + \frac{1}{2}\max\left(\varepsilon(K)^{\frac{1}{2}}, \varepsilon(K)\right)$$

The right hand side is obviously in $\mathcal{F}^{\frac{1}{2}}$. □

Note that it would still be possible to prove Theorem 2.1 if in Definition 2.13 we allowed S to depend on y directly instead of only through P. However, the definition as given appears more natural since it seems necessary to prove Theorem 3.4 in full generality.

Conversely to Theorem 2.1, we have the following:

Theorem 2.2. *Consider $(\mathcal{D}, f)$ a distributional estimation problem and P an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. Then, P is also an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. Consider any $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$. We have

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] = \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K \times \mathrm{U}_P^K}[(Q^K - P^K + P^K - f)^2]$$

$$\mathrm{E}[(Q^K - f)^2] = \mathrm{E}[(Q^K - P^K)^2] + 2\,\mathrm{E}[(Q^K - P^K)(P^K - f)] + \mathrm{E}[(P^K - f)^2]$$

$$\mathrm{E}[(P^K - f)^2] + \mathrm{E}[(Q^K - P^K)^2] = \mathrm{E}[(Q^K - f)^2] + 2\,\mathrm{E}[(P^K - Q^K)(P^K - f)]$$

$$\mathrm{E}[(P^K - f)^2] \leq \mathrm{E}[(Q^K - f)^2] + 2\,\mathrm{E}[(P^K - Q^K)(P^K - f)]$$

We can assume Q is bounded without loss of generality since given any Q it easy to construct bounded $\tilde{Q}$ s.t. $\mathrm{E}[(\tilde{Q}^K - f)^2] \leq \mathrm{E}[(Q^K - f)^2]$. Applying 2.11, we get 2.5.

□

2.4 Simple example

The concept of an optimal polynomial-time estimator is in some sense complementary to the concept of pseudorandomness: a pseudorandom process deterministically produces output that appears random to bounded algorithms whereas optimal polynomial-time estimators compute the moments of the perceived random distributions of the outputs of deterministic processes. To demonstrate this complementarity and give an elementary example of an optimal polynomial-time estimator, we use the concept of a hard-core predicate (which may be regarded as an elementary example of pseudorandomness). The notation $\mathcal{F}_{\mathrm{neg}}$ below refers to the fall space defined in Example 2.6 (functions that fall faster than any polynomial). $\frac{1}{2}$ is an optimal polynomial-time estimator for a hard-core predicate.

Theorem 2.3. *Consider $\mathcal{D}$ a word ensemble of rank 1 s.t. for any different $k, l \in \mathbb{N}$, $\operatorname{supp} \mathcal{D}^k \cap \operatorname{supp} \mathcal{D}^l = \varnothing$, $f : \operatorname{supp} \mathcal{D} \to \{0,1\}^*$ one-to-one and B a hard-core predicate of $(\mathcal{D}, f)$ (see Definition A.1). Define $m : \operatorname{supp} \mathcal{D} \to \mathbb{N}$ by*

$$\forall x \in \operatorname{supp} \mathcal{D}^k : m(x) := k$$

For every $k \in \mathbb{N}$, define $\mathcal{D}_f^k := f_*^k \mathcal{D}^k$. Finally, define $\chi_B : \operatorname{supp} \mathcal{D}_f \to \{0,1\}$ by

$$\chi_B(f(x)) := B^{m(x)}(x)$$

Let $\Gamma := (\Gamma^1_{\text{poly}}, \Gamma^1_0)$. Let $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ satisfy $P \equiv \frac{1}{2}$. Then, P is an $\mathcal{F}_{\text{neg}}(\Gamma)$-optimal estimator for $(\mathcal{D}_f, \chi_B)$.

Proof. Assume to the contrary that P is not optimal. Then there is $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$, $d \in \mathbb{N}$, an infinite set $I \subseteq \mathbb{N}$ and $\epsilon \in \mathbb{R}^{>0}$ s.t.

$$\forall k \in I : \mathrm{E}_{\mathcal{D}_f^k}[(\frac{1}{2} - \chi_B)^2] \geq \mathrm{E}_{\mathcal{D}_f^k \times \mathrm{U}_Q^k}[(Q^k - \chi_B)^2] + \frac{\epsilon}{k^d}$$

$$\forall k \in I : \mathrm{E}_{\mathcal{D}_f^k \times \mathrm{U}_Q^k}[(Q^k - \chi_B)^2] \leq \frac{1}{4} - \frac{\epsilon}{k^d}$$

$$\forall k \in I : \mathrm{E}_{\mathcal{D}_f^k}[(\mathrm{E}_{\mathrm{U}_Q^k}[Q^k] - \chi_B)^2] \leq \frac{1}{4} - \frac{\epsilon}{k^d}$$

There is $G : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}$ s.t. for all $x \in \{0,1\}^*$,

$$|\mathrm{E}[Q^k(x)] - \Pr[G^k(x) = 1]| \leq 2^{-k}$$

G^k works by evaluating $\alpha \leftarrow Q^k$ and then returning 1 with probability $\alpha \pm 2^{-k}$ and 0 with probability $1 - \alpha \pm 2^{-k}$, where the 2^{-k} error comes from rounding a rational number to a binary fraction. Denoting

$$\delta(x) := \mathrm{E}[Q^k(x)] - \Pr[G^k(x) = 1]$$

we get

$$\forall k \in I : \mathrm{E}_{\mathcal{D}_f^k}[(\Pr_{\mathrm{U}_G^k}[G^k = 1] + \delta - \chi_B)^2] \leq \frac{1}{4} - \frac{\epsilon}{k^d}$$

$$\forall k \in I : \mathrm{E}_{\mathcal{D}_f^k}[(\Pr_{\mathrm{U}_G^k}[G^k = 1] - \chi_f)^2] + 2\,\mathrm{E}_{\mathcal{D}_f^k}[(\Pr_{\mathrm{U}_G^k}[G^k = 1] - \chi_B)\delta] + \mathrm{E}_{\mathcal{D}_f^k}[\delta^2] \leq \frac{1}{4} - \frac{\epsilon}{k^d}$$

$$\forall k \in I : \mathrm{E}_{\mathcal{D}_f^k}[(\Pr_{\mathrm{U}_G^k}[G^k = 1] - \chi_B)^2] - 2 \cdot 2^{-k} - 4^{-k} \leq \frac{1}{4} - \frac{\epsilon}{k^d}$$

Since 2^{-k} falls faster than k^{-d}, there is $I_1 \subseteq \mathbb{N}$ infinite and $\epsilon_1 \in \mathbb{R}^{>0}$ s.t.

$$\forall k \in I_1 : \mathrm{E}_{\mathcal{D}_f^k}[(\Pr_{\mathrm{U}_G^k}[G^k = 1] - \chi_B)^2] \leq \frac{1}{4} - \frac{\epsilon_1}{k^d}$$

$$\forall k \in I_1 : \mathrm{E}_{\mathcal{D}_f^k}[|\Pr_{\mathrm{U}_G^k}[G^k = 1] - \chi_B|] \leq \sqrt{\frac{1}{4} - \frac{\epsilon_1}{k^d}}$$

$$\forall k \in I_1 : \mathrm{E}_{\mathcal{D}_f^k}[\Pr_{\mathrm{U}_G^k}[G^k \neq \chi_B]] \leq \sqrt{\frac{1}{4} - \frac{\epsilon_1}{k^d}}$$

$$\forall k \in I_1 : \mathrm{E}_{x \sim \mathcal{D}^k}[\Pr_{\mathrm{U}_G^k}[G^k(f(x)) \neq B^k(x)]] \leq \sqrt{\frac{1}{4} - \frac{\epsilon_1}{k^d}}$$

$$\forall k \in I_1 : \Pr_{\mathcal{D}^k \times \mathrm{U}_G^k}[G^k(f(x)) \neq B^k(x)] \leq \sqrt{\frac{1}{4} - \frac{\epsilon_1}{k^d}}$$

Since $\sqrt{t}$ is a concave function and the derivative of $\sqrt{t}$ is $\frac{1}{2\sqrt{t}}$, we have $\sqrt{t} \leq \sqrt{t_0} + \frac{t - t_0}{2\sqrt{t_0}}$. Taking $t_0 = \frac{1}{4}$ we get

$$\forall k \in I_1 : \Pr_{\mathcal{D}^k \times \mathrm{U}_G^k}[G^k(f(x)) \neq B^k(x)] \leq \frac{1}{2} - \frac{\epsilon_1}{k^d}$$

$$\forall k \in I_1 : \Pr_{\mathcal{D}^k \times \mathrm{U}_G^k}[G^k(f(x)) = B^k(x)] \geq \frac{1}{2} + \frac{\epsilon_1}{k^d}$$

This contradicts the definition of a hard-core predicate. □

Corollary 2.2. *Consider $f : \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}^*$ a one-to-one one-way function. For every $k \in \mathbb{N}$, define $f^{(k)} : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^*$ by $f^{(k)}(x,y) := \langle f(x), y \rangle$. Define the distributional estimation problem $(\mathcal{D}_{(f)}, \chi_f)$ by*

$$\mathcal{D}_{(f)}^k := f_*^{(k)}(\mathrm{U}^k \times \mathrm{U}^k)$$
$$\chi_f(\langle f(x), y \rangle) := x \cdot y$$

Let $\Gamma := (\Gamma_{\text{poly}}^1, \Gamma_0^1)$. Let $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ satisfy $P \equiv \frac{1}{2}$. Then, P is an $\mathcal{F}_{\text{neg}}(\Gamma)$-optimal estimator for $(\mathcal{D}_{(f)}, \chi_f)$.

Proof. Follows immediately from Theorem 2.3 and Theorem A.1. □

The following is the non-uniform version of Theorem 2.3 which we state without proof since the proof is a straightforward adaptation of the above.

Theorem 2.4. *Consider $\mathcal{D}$ a word ensemble s.t. for any different $k, l \in \mathbb{N}$, $\operatorname{supp}\mathcal{D}^k \cap \operatorname{supp}\mathcal{D}^l = \varnothing$, $f : \operatorname{supp}\mathcal{D} \to \{0,1\}^*$ one-to-one and B a non-uniformly hard-core predicate of $(\mathcal{D}, f)$ (see Definition A.2).*

Let $\Gamma := (\Gamma^1_{\text{poly}}, \Gamma^1_{\text{poly}})$. Let $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ satisfy $P \equiv \frac{1}{2}$. Then, P is an $\mathcal{F}_{\text{neg}}(\Gamma)$-optimal estimator for $(\mathcal{D}_f, \chi_B)$.

Corollary 2.3. *Consider $f : \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}^*$ a one-to-one non-uniformly hard to invert one-way function.*

Let $\Gamma := (\Gamma^1_{\text{poly}}, \Gamma^1_{\text{poly}})$. Let $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ satisfy $P \equiv \frac{1}{2}$. Then, P is an $\mathcal{F}_{\text{neg}}(\Gamma)$-optimal estimator for $(\mathcal{D}_f, \chi_f)$.

Proof. Follows immediately from Theorem 2.4 and Theorem A.2. □

3 Optimal estimators and probability theory

3.1 Calibration

From a Bayesian perspective, a good probability assignment should be well calibrated (see e.g. [7]). For example, suppose there are 100 people in a room and you assign each person a probability they are married. If there are 60 people you assigned probabilities in the range 70%-80%, the number of married people among these 60 should be close to the interval $60 \times [0.7, 0.8] = [42, 48]$. The same requirement can be made for expected value assignments. For example, if you now need to assign an expected value to the age of each person and you assigned an expected age in the range 30-40 to some sufficiently large group of people, the mean age in the group should be close to the interval $[30, 40]$.

We will now show that optimal polynomial-time estimators satisfy an analogous property.

Theorem 3.1. *Assume $\mathcal{F}$ is $\Gamma_{\mathfrak{A}}$-ample. Consider $(\mathcal{D}, f)$ a distributional estimation problem, P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$ and $W : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}^{\geq 0}$ bounded s.t. $\mathrm{r}_W \geq \mathrm{r}_P$ and for every $K \in \mathbb{N}^n$ there is $x \in \operatorname{supp}\mathcal{D}^K$ and $y \in \mathrm{U}^K_W$ with $W^K(x, y) > 0$. Denote*

$$\alpha(K) := \mathrm{E}_{(x,y)\sim\mathcal{D}^K \times \mathrm{U}^K_W}[W^K(x, y)]$$
$$\delta(K) := \mathrm{E}_{(x,y)\sim\mathcal{D}^K \times \mathrm{U}^K_W}[W^K(x, y)(P^K(x, y_{<\mathrm{r}_P(K)}) - f(x))]$$

Then, $\alpha^{-1}\delta^2 \in \mathcal{F}$.

Looking at the definition of an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator, we see that, when Q is $\{0,1\}$-valued to pick out a small subset of inputs, P may be biased on that small subset, because the bias isn't normalized by dividing by the fraction of probability mass where Q outputs 1. In the language of the above theorem, δ lies in $\mathcal{F}$, but $\frac{\delta}{\alpha}$ may not.

Proposition 2.12 says that, given ample advice, optimal estimators continue to be optimal (although with increased error) on small subsets of their input, which is a slightly stronger condition. Therefore, the above theorem essentially says that if enough advice is available for Proposition 2.12 to apply, the property of resistance to reweighting implies that, for the subset that W picks out, the unnormalized bias times the normalized bias is a small term that lies in $\mathcal{F}$.

To see the relationship between Theorem 3.1 and calibration, consider the following corollary.

Corollary 3.1. *Assume* $\mathcal{F}$ *is* $\Gamma_{\mathfrak{A}}$*-ample. Consider* $(\mathcal{D}, f)$ *a distributional estimation problem,* P *an* $\mathcal{F}(\Gamma)$*-optimal estimator for* $(\mathcal{D}, f)$ *and* $A, B : \mathbf{1} \xrightarrow{\Gamma} \mathbb{Q}$ *s.t.* $\mathrm{r}_A \equiv 0$ *and* $\mathrm{r}_B \equiv 0$. *Denote*

$$\alpha(K) := \Pr_{(x,y)\sim\mathcal{D}^K\times \mathrm{U}_P^K}[A^K \leq P^K(x,y) \leq B^K]$$

Then, there is $\varepsilon \in \mathcal{F}$ *s.t.*

$$A^K - \sqrt{\frac{\varepsilon(K)}{\alpha(K)}} \leq \mathrm{E}_{(x,y)\sim\mathcal{D}^K\times \mathrm{U}_P^K}[f(x) \mid A^K \leq P^K(x,y) \leq B^K] \leq B^K + \sqrt{\frac{\varepsilon(K)}{\alpha(K)}} \quad (3.1)$$

The appearance of α in the denominator in 3.1 is not surprising since we only expect calibration to hold for large sample size.

We now proceed with the proofs.

Proof of Corollary 3.1. Construct $W : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}$ s.t.

$$\mathrm{r}_W(K) = \mathrm{r}_P(K)$$
$$W^K(x,y) = \theta(P^K(x,y) - A^K)\theta(B^K - P^K(x,y))$$

Denote $\delta(K) := \mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_P^K}[W^K(P^K - f)]$ and $\varepsilon := \frac{\delta^2}{\alpha}$. According to Theorem 3.1, $\varepsilon \in \mathcal{F}$. We get

$$\frac{\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[W^K(P^K - f)]^2}{\alpha(K)} = \varepsilon(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[\theta(P^K(x,y) - A^K)\theta(B^K - P^K(x,y))(P^K - f)]^2 = \varepsilon(K)\alpha(K)$$

$$(\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[\theta(P^K(x,y) - A^K)\theta(B^K - P^K(x,y))] \cdot \mathrm{E}[P^K - f \mid A^K \leq P^K \leq B^K])^2 = \varepsilon(K)\alpha(K)$$

$$(\alpha(K)\,\mathrm{E}[P^K - f \mid A^K \leq P^K \leq B^K])^2 = \varepsilon(K)\alpha(K)$$

$$\alpha(K)\,\mathrm{E}[P^K - f \mid A^K \leq P^K \leq B^K]^2 = \varepsilon(K)$$

$$|\mathrm{E}[P^K - f \mid A^K \leq P^K \leq B^K]| = \sqrt{\frac{\varepsilon(K)}{\alpha(K)}} \tag{3.2}$$

On the other hand

$$\mathrm{E}[f \mid A^K \leq P^K \leq B^K] = \mathrm{E}[P^K - P^K + f \mid A^K \leq P^K \leq B^K]$$

$$\mathrm{E}[f \mid A^K \leq P^K \leq B^K] = \mathrm{E}[P^K \mid A^K \leq P^K \leq B^K] - \mathrm{E}[P^K - f \mid A^K \leq P^K \leq B^K]$$

Applying 3.2

$$\mathrm{E}[f \mid A^K \leq P^K \leq B^K] \leq \mathrm{E}[P^K \mid A^K \leq P^K \leq B^K] + \sqrt{\frac{\varepsilon(K)}{\alpha(K)}}$$

$$\mathrm{E}[f \mid A^K \leq P^K \leq B^K] \leq B^K + \sqrt{\frac{\varepsilon(K)}{\alpha(K)}}$$

In the same manner, we can show that

$$\mathrm{E}[f \mid A^K \leq P^K \leq B^K] \geq A^K - \sqrt{\frac{\varepsilon(K)}{\alpha(K)}}$$

□

Proof of Theorem 3.1. Consider $\zeta : \mathbb{N}^n \to (0, \frac{1}{2}]$ s.t. $\zeta \in \mathcal{F}$ and $\lfloor \log \frac{1}{\zeta} \rfloor \in \Gamma_{\mathfrak{A}}$. Define

$$I := \{K \in \mathbb{N}^n \mid \frac{|\delta(K)|}{\alpha(K)} \geq \zeta(K)\}$$
$$E^K := \mathbb{Q} \cap \left[\frac{|\delta(K)|}{2\alpha(K)}, \frac{|\delta(K)|}{\alpha(K)}\right]$$
$$\epsilon(K) \in (\operatorname{sgn} \delta(K)) \cdot \arg\min_{t \in E^K} |\mathrm{c}_{\mathbb{Q}}(t)|$$

It is easy to see that $|\mathrm{c}_{\mathbb{Q}}(\epsilon)| = O(\log \frac{\alpha}{|\delta|})$, hence we can construct $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $K \in I$ and $x, y \in \{0,1\}^*$

$$\mathrm{a}_Q(K) = \mathrm{c}_{\mathbb{Q}}(\epsilon(K))$$
$$\mathrm{r}_Q(K) = \mathrm{r}_P(K)$$
$$Q^K(x,y) = P^K(x,y) - \epsilon(K)$$

This algorithm uses the advice string to check whether the normalized bias is too high, and if it is, it perturbs the estimated values accordingly.

Applying Proposition 2.12 to P, Q and W, we conclude there is $\varepsilon \in \mathcal{F}$ s.t.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K (P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K (Q^K - f)^2] + \varepsilon(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K (P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K (P^K - f - \epsilon(K))^2] + \varepsilon(K)$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K ((P^K - f)^2 - (P^K - f - \epsilon(K))^2] \leq \varepsilon(K)$$

$$\epsilon(K) \,\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K (2(P^K - f) - \epsilon(K))] \leq \varepsilon(K)$$

$$\epsilon(K)(2 \,\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K (P^K - f)] - \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_W^K}[W^K]\epsilon(K)) \leq \varepsilon(K)$$

$$\epsilon(K)(2\delta(K) - \alpha(K)\epsilon(K)) \leq \varepsilon(K)$$

Dividing both sides by $\alpha(K)$ we get

$$\epsilon(K)\left(\frac{2\delta(K)}{\alpha(K)} - \epsilon(K)\right) \leq \frac{\varepsilon(K)}{\alpha(K)}$$

$$\frac{\delta(K)^2}{\alpha(K)^2} - \left(\epsilon(K) - \frac{\delta(K)}{\alpha(K)}\right)^2 \leq \frac{\varepsilon(K)}{\alpha(K)}$$

ϵ is between $\frac{\delta}{2\alpha}$ and $\frac{\delta}{\alpha}$ therefore $(\epsilon - \frac{\delta}{\alpha})^2 \leq (\frac{\delta}{2\alpha} - \frac{\delta}{\alpha})^2$ which yields

$$\frac{\delta(K)^2}{\alpha(K)^2} - \left(\frac{\delta(K)}{2\alpha(K)} - \frac{\delta(K)}{\alpha(K)}\right)^2 \leq \frac{\varepsilon(K)}{\alpha(K)}$$

$$\frac{3}{4} \cdot \frac{\delta(K)^2}{\alpha(K)^2} \leq \frac{\varepsilon(K)}{\alpha(K)}$$

$$\frac{\delta(K)^2}{\alpha(K)} \leq \frac{4}{3}\varepsilon(K)$$

□

3.2 Algebraic properties

In this subsection and subsection 3.4, we show that several algebraic identities satisfied by expected values have analogues for optimal polynomial-time estimators.

3.2.1 Linearity

Given F_1, F_2 random variables and $t_1, t_2 \in \mathbb{R}$, we have

$$\mathrm{E}[t_1 F_1 + t_2 F_2] = t_1 \mathrm{E}[F_1] + t_2 \mathrm{E}[F_2] \tag{3.3}$$

Optimal polynomial-time estimators have an analogous property:

Proposition 3.1. *Consider $\mathcal{D}$ a word ensemble, $f_1, f_2 : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ bounded and $t_1, t_2 \in \mathbb{Q}$. Denote $f := t_1 f_1 + t_2 f_2$. Suppose P_1 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f_1)$ and P_2 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f_2)$. Construct $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $x \in \operatorname{supp} \mathcal{D}^K$, $y_1 \in \{0,1\}^{\mathrm{r}_{P_1}(K)}$ and $y_2 \in \{0,1\}^{\mathrm{r}_{P_1}(K)}$*

$$\mathrm{a}_P(K) = \langle \mathrm{a}_{P_1}(K), \mathrm{a}_{P_2}(K) \rangle \tag{3.4}$$

$$\mathrm{r}_P(K) = \mathrm{r}_{P_1}(K) + \mathrm{r}_{P_2}(K) \tag{3.5}$$

$$P^K(x, y_1 y_2) = t_1 P_1^K(x, y_1) + t_2 P_2^K(x, y_2) \tag{3.6}$$

Then, P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.

Proof. Consider any bounded $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$. We have

$$\mathrm{E}[(P^K - f)S^K] = \mathrm{E}[(t_1 P_1^K + t_2 P_2^K - (t_1 f_1 + t_2 f_2))S^K]$$

$$\mathrm{E}[(P^K - f)S^K] = t_1 \mathrm{E}[(P_1^K - f_1)S^K] + t_2 \mathrm{E}[(P_2^K - f_2)S^K]$$

$$|\mathrm{E}[(P^K - f)S^K]| \leq |t_1| \cdot |\mathrm{E}[(P_1^K - f_1)S^K]| + |t_2| \cdot |\mathrm{E}[(P_2^K - f_2)S^K]|$$

Using 2.11 for P_1 and P_2 we see that the right hand side is in $\mathcal{F}$. □

3.2.2 Conditional expectation

Consider a random variable F and an event A. Denote χ_A the $\{0,1\}$-valued random variable corresponding to the indicator function of A. We have

$$\mathrm{E}[F \mid A] = \frac{\mathrm{E}[\chi_A F]}{\Pr[A]} \tag{3.7}$$

This identity is tautologous if interpreted as a definition of $\mathrm{E}[F \mid A]$. However, from the perspective of Bayesian probability it is more natural to think of $\mathrm{E}[F \mid A]$ as an atomic entity (the subjective expectation of F after observing A).

The language of optimal polynomial-time estimators provides a natural way to define an analogue of conditional expectation. Namely, consider a distributional estimation problem $(\mathcal{D}, f)$ and a decision problem $L \subseteq \{0,1\}^*$. Then, $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ represents the conditional expectation of f given L when it is an optimal polynomial-time estimator for $(\mathcal{D} \mid L, f)$. That is, the conditional expectation is the best estimate of $f(x)$ when the problem instance x is sampled with the *promise* $x \in L$.

The above perspective allows us stating and proving non-tautological theorems analogous to 3.7. We give two such theorems, corresponding to two different ways to group the variables in 3.7. Let χ_L be the indicator function for L. The first states that an optimal estimator for $\chi_L f$ can be made by multiplying together an optimal estimator for χ_L and a less accurate optimal estimator for $f|L$, and the second theorem states that a less accurate optimal estimator for $f|L$ can be made by dividing the output of an optimal estimator for $\chi_L f$ by the output of an optimal estimator for L. The amplification of error appears because L might be a low-probability event, and conditional probabilities for low-probability events are less accurate than conditional probabilities for high-probability events.

Theorem 3.2. *Consider $(\mathcal{D}, f)$ a distributional estimation problem and $L \subseteq \{0,1\}^*$ s.t. for all $K \in \mathbb{N}^n$, $\mathcal{D}^K(L) > 0$. Define $\gamma_L : \mathbb{N}^n \to \mathbb{R}$ by $\gamma_L(K) := \mathcal{D}^K(L)^{-1}$ and $\mathcal{F}_L := \gamma_L \mathcal{F}$. Let P_L be an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$ and $P_{f|L}$ be an $\mathcal{F}_L^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D} \mid L, f)$. Construct $P_{\chi f} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_{P_{\chi f}} = \mathrm{r}_{P_L} + \mathrm{r}_{P_{f|L}}$ and for any $x \in \{0,1\}^*$, $y \in \{0,1\}^{\mathrm{r}_{P_L}(K)}$ and $z \in \{0,1\}^{\mathrm{r}_{P_{f|L}}(K)}$*

$$P_{\chi f}^K(x, yz) = P_L^K(x, y) P_{f|L}^K(x, z) \tag{3.8}$$

Then, $P_{\chi f}$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L f)$.

Proof. Consider any $K \in \mathbb{N}^n$, $x \in \operatorname{supp} \mathcal{D}^K$, $y \in \{0,1\}^{\mathrm{r}_{P_L}(K)}$ and $z \in \{0,1\}^{\mathrm{r}_{P_{f|L}}(K)}$.

$$P_{\chi f}^K(x, yz) - \chi_L(x) f(x) = P_L^K(x, y) P_{f|L}^K(x, z) - \chi_L(x) f(x)$$

$$\begin{aligned} &P_{\chi f}^K(x, yz) - \chi_L(x) f(x) \\ &\quad = P_L^K(x, y) P_{f|L}^K(x, z) - \chi_L(x) P_{f|L}^K(x, z) + \chi_L(x) P_{f|L}^K(x, z) - \chi_L(x) f(x) \end{aligned}$$

$$P_{\chi f}^K(x, yz) - \chi_L(x) f(x) = (P_L^K(x, y) - \chi_L(x)) P_{f|L}^K(x, z) + \chi_L(x) (P_{f|L}^K(x, z) - f(x))$$

Consider any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded. We get

$$\begin{aligned} &\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P_{\chi f}^K - \chi_L f) S^K] \\ &\quad = \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P_L^K - \chi_L) P_{f|L}^K S^K)] + \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[\chi_L (P_{f|L}^K - f) S^K] \end{aligned}$$

Using the fact that P_L^K is $\mathcal{F}^\sharp(\Gamma)$-optimal for $(\mathcal{D}, \chi_L)$,

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P_{\chi f}^K - \chi_L f) S^K] \equiv \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[\chi_L (P_{f|L}^K - f) S^K] \pmod{\mathcal{F}}$$

$$\begin{aligned} &\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P_{\chi f}^K - \chi_L f) S^K] \\ &\qquad \equiv \mathcal{D}^K(L)\, \mathrm{E}_{(\mathcal{D}^K \mid L) \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P_{f|L}^K - f) S^K] \pmod{\mathcal{F}} \end{aligned}$$

Using the fact that $P^K_{f|L}$ is $\mathcal{F}^\sharp_L(\Gamma)$-optimal for $(\mathcal{D} \mid L, f)$, we conclude

$$|\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P^K_{\chi f} - \chi_L f) S^K]| \equiv 0 \pmod{\mathcal{F}}$$

□

Theorem 3.3. *Consider $(\mathcal{D}, f)$ a distributional estimation problem and $L \subseteq \{0,1\}^*$ s.t. for all $K \in \mathbb{N}^n$, $\mathcal{D}^K(L) > 0$. Define $\gamma_L : \mathbb{N}^n \to \mathbb{R}$ by $\gamma(K) := \mathcal{D}^K(L)^{-1}$ and $\mathcal{F}_L := \gamma_L \mathcal{F}$. Let P_L be an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$ and $P_{\chi f}$ be an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L f)$. Choose any $M \in \mathbb{Q}$ s.t. $M \geq \sup|f|$ and construct $P_{f|L} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_{P_{f|L}} = \mathrm{r}_{P_L} + \mathrm{r}_{P_{\chi f}}$ and for any $x \in \{0,1\}^*$, $y \in \{0,1\}^{\mathrm{r}_{P_L}(K)}$ and $z \in \{0,1\}^{\mathrm{r}_{P_{\chi f}}(K)}$*

$$P^K_{f|L}(x, yz) = \begin{cases} P^K_L(x,y)^{-1} P^K_{\chi f}(x,z) \text{ if this number is in } [-M, M] \\ M \text{ if } P^K_L(x,y) = 0 \text{ or } P^K_L(x,y)^{-1} P^K_{\chi f}(x,z) > M \\ -M \text{ if } P^K_L(x,y)^{-1} P^K_{\chi f}(x,z) < -M \end{cases} \tag{3.9}$$

Then, $P_{f|L}$ is an $\mathcal{F}^\sharp_L(\Gamma)$-optimal estimator for $(\mathcal{D} \mid L, f)$.

In order to prove Theorem 3.3, we will need the following.

Consider $s, t \in \mathbb{Q}$, an $[s,t]$-valued random variable F and an event A. Denote χ_A the $\{0,1\}$-valued random variable corresponding to the indicator function of A. We have

$$\Pr[A] s \leq \mathrm{E}[\chi_A F] \leq \Pr[A] t \tag{3.10}$$

For optimal polynomial-time estimators the analogous inequalities don't have to hold strictly (they only hold within an asymptotically small error), but the following proposition shows they can always be enforced.

Proposition 3.2. *Consider $(\mathcal{D}, f)$ a distributional estimation problem, $L \subseteq \{0,1\}^*$ and $s, t \in \mathbb{Q}$ s.t. $s \leq \inf f$, $t \geq \sup f$. Let P_L be an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$ and $P_{\chi f}$ be an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L f)$. Construct $\tilde{P}_{\chi f} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_{\tilde{P}_{\chi f}} = \mathrm{r}_{P_L} + \mathrm{r}_{P_{\chi f}}$ and for any $y \in \{0,1\}^{\mathrm{r}_{P_L}(K)}$ and $z \in \{0,1\}^{\mathrm{r}_{P_{\chi f}}(K)}$, $\tilde{P}^K_{\chi f}(x, yz) = \min(\max(P^K_{\chi f}(x,z), P^K_L(x,y)s), P^K_L(x,y)t)$. Denote*

$$\mathcal{D}^K_P := \mathcal{D}^K \times \mathrm{U}^K_{P_L} \times \mathrm{U}^K_{P_{\chi f}}$$

Then, for any $S : \{0,1\}^* \times \mathbb{Q}^2 \xrightarrow{\Gamma} \mathbb{Q}$ bounded

$$\mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K(x) - \chi_L(x) f(x)) S^K(x, P_L^K(x), P_{\chi f}^K(x))] \equiv 0 \pmod{\mathcal{F}} \tag{3.11}$$

In particular, $\tilde{P}$ is also an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L f)$.

Proof. P_L is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$, therefore

$$\mathrm{E}_{\mathcal{D}_P^K}[(P_L^K - \chi_L)\theta(P_{\chi f}^K - P_L^K t)] \equiv 0 \pmod{\mathcal{F}} \tag{3.12}$$

$P_{\chi f}$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L f)$, therefore

$$\mathrm{E}_{\mathcal{D}_P^K}[(P_{\chi f}^K - \chi_L f)\theta(P_{\chi f}^K - P_L^K t)] \equiv 0 \pmod{\mathcal{F}} \tag{3.13}$$

Multiplying 3.12 by t and subtracting 3.13 we get

$$\mathrm{E}_{\mathcal{D}_P^K}[(P_L^K t - P_{\chi f}^K - \chi_L \cdot (t - f))\theta(P_{\chi f}^K - P_L^K t)] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}_P^K}[(P_L^K t - P_{\chi f}^K)\theta(P_{\chi f}^K - P_L^K t)] \equiv \mathrm{E}_{\mathcal{D}_P^K}[\chi_L \cdot (t - f)\theta(P_{\chi f}^K - P_L^K t)] \pmod{\mathcal{F}}$$

The left-hand side is non-positive and the right-hand side is non-negative, therefore

$$\mathrm{E}_{\mathcal{D}_P^K}[(P_L^K t - P_{\chi f}^K)\theta(P_{\chi f}^K - P_L^K t)] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}_P^K}[(\tilde{P}_{\chi f}^K - P_{\chi f}^K)\theta(P_{\chi f}^K - \tilde{P}_{\chi f}^K)] \equiv 0 \pmod{\mathcal{F}} \tag{3.14}$$

In the same way we can show that

$$\mathrm{E}_{\mathcal{D}_P^K}[(P_L^K s - P_{\chi f}^K)\theta(P_L^K s - P_{\chi f}^K)] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}_P^K}[(\tilde{P}_{\chi f}^K - P_{\chi f}^K)\theta(\tilde{P}_{\chi f}^K - P_{\chi f}^K)] \equiv 0 \pmod{\mathcal{F}} \tag{3.15}$$

Subtracting 3.14 from 3.15, we get

$$\mathrm{E}_{\mathcal{D}_P^K}[(\tilde{P}_{\chi f}^K - P_{\chi f}^K)(\theta(\tilde{P}_{\chi f}^K - P_{\chi f}^K) - \theta(P_{\chi f}^K - \tilde{P}_{\chi f}^K))] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}_P^K}[|\tilde{P}_{\chi f}^K - P_{\chi f}^K|] \equiv 0 \pmod{\mathcal{F}} \tag{3.16}$$

Consider any $S : \{0,1\}^* \times \mathbb{Q}^2 \xrightarrow{\Gamma} \mathbb{Q}$ bounded.

$$\mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - \chi_L f) S^K(x, P_L^K, P_{\chi f}^K)] \\ = \mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - P_{\chi f}^K + P_{\chi f}^K - \chi_L f) S^K(x, P_L^K, P_{\chi f}^K)]$$

$$\mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - \chi_L f) S^K] = \mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - P_{\chi f}^K) S^K] + \mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(P_{\chi f}^K - \chi_L f) S^K]$$

Using the fact that $P_{\chi f}$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L f)$, we get

$$\mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - \chi_L f) S^K] \equiv \mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - P_{\chi f}^K) S^K] \pmod{\mathcal{F}}$$

$$|\mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - \chi_L f) S^K]| \leq \mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[|\tilde{P}_{\chi f}^K - P_{\chi f}^K|] \sup S \pmod{\mathcal{F}}$$

Applying 3.16 we conclude that

$$\mathrm{E}_{\mathcal{D}_P^K \times \mathrm{U}_S^K}[(\tilde{P}_{\chi f}^K - \chi_L f) S^K] \equiv 0 \pmod{\mathcal{F}}$$

□

Proof of Theorem 3.3. Construct $\tilde{P}_{\chi f} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_{\tilde{P}_{\chi f}} = \mathrm{r}_{P_L} + \mathrm{r}_{P_{\chi f}}$ and for any $x \in \{0,1\}^*$, $y \in \{0,1\}^{\mathrm{r}_{P_L}(K)}$ and $z \in \{0,1\}^{\mathrm{r}_{P_{\chi f}}(K)}$

$$\tilde{P}_{\chi f}^K(x, yz) = \min(\max(P_{\chi f}^K(x, z), -P_L^K(x, y)M), P_L^K(x, y)M)$$

For any $x \in \{0,1\}^*$, $y \in \{0,1\}^{\mathrm{r}_{P_L}(K)}$ and $z \in \{0,1\}^{\mathrm{r}_{P_{\chi f}}(K)}$, we have

$$\tilde{P}_{\chi f}^K(x, yz) = P_L^K(x, y) P_{f|L}^K(x, yz)$$

$$\tilde{P}_{\chi f}^K(x, yz) - \chi_L(x) f(x) = P_L^K(x, y) P_{f|L}^K(x, yz) - \chi_L(x) f(x)$$

$$\tilde{P}_{\chi f}^K(x, yz) - \chi_L(x) f(x) \\ = P_L^K(x, y) P_{f|L}^K(x, z) - \chi_L(x) P_{f|L}^K(x, yz) + \chi_L(x) P_{f|L}^K(x, yz) - \chi_L(x) f(x)$$

$$\tilde{P}^K_{\chi f}(x, yz) - \chi_L(x) f(x) = (P^K_L(x, y) - \chi_L(x)) P^K_{f|L}(x, yz) + \chi_L(x)(P^K_{f|L}(x, yz) - f(x))$$

$$\chi_L(x)(P^K_{f|L}(x, yz) - f(x)) = \tilde{P}^K_{\chi f}(x, yz) - \chi_L(x) f(x) - (P^K_L(x, y) - \chi_L(x)) P^K_{f|L}(x, yz)$$

Consider any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Denote

$$\mathcal{D}^K_{PS} := \mathcal{D}^K \times \mathrm{U}^K_{P_L} \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S$$

We have

$$\begin{aligned}&\mathrm{E}_{\mathcal{D}^K_{PS}}[\chi_L(P^K_{f|L} - f) S^K(x, P^K_{f|L})] \\ &\quad = E_{\mathcal{D}^K_{PS}}[(\tilde{P}^K_{\chi f} - \chi_L f) S^K(x, P^K_{f|L})] - E_{\mathcal{D}^K_{PS}}[(P^K_L - \chi_L) P^K_{f|L} S^K(x, P^K_{f|L})]\end{aligned}$$

Applying Proposition 3.2 to the first term on the right-hand side and the fact P^K_L is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$ to the second term on the right-hand side,

$$\mathrm{E}_{\mathcal{D}^K_{PS}}[\chi_L(P^K_{f|L} - f) S^K(x, P^K_{f|L})] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathcal{D}^K(L)\, \mathrm{E}_{(\mathcal{D}^K|L) \times \mathrm{U}^K_{P_L} \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P^K_{f|L} - f) S^K(x, P^K_{f|L})] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{(\mathcal{D}^K|L) \times \mathrm{U}^K_{P_L} \times \mathrm{U}^K_{P_{\chi f}} \times \mathrm{U}^K_S}[(P^K_{f|L} - f) S^K(x, P^K_{f|L})] \equiv 0 \pmod{\mathcal{F}_L}$$

□

3.3 Polynomial-time MΓ-schemes and samplers

The next subsection and subsequent sections will require several new concepts. Here, we introduce these concepts and discuss some of their properties.

3.3.1 Congruent measure families

The notation $f(K) \equiv g(K) \pmod{\mathcal{F}}$ can be conveniently generalized from real-valued functions to families of probability distributions.

Definition 3.1. Consider a set X and two families $\{\mathcal{D}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$ and $\{\mathcal{E}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$. We say that $\mathcal{D}$ *is congruent to* $\mathcal{E}$ *modulo* $\mathcal{F}$ when $\mathrm{d_{tv}}(\mathcal{D}^K, \mathcal{E}^K) \in \mathcal{F}$. In this case we write $\mathcal{D}^K \equiv \mathcal{E}^K \pmod{\mathcal{F}}$ or $\mathcal{D} \equiv \mathcal{E} \pmod{\mathcal{F}}$.

Congruence of probability distributions modulo $\mathcal{F}$ has several convenient properties which follow from elementary properties of total variation distance.

Proposition 3.3. *Congruence of probability distributions modulo $\mathcal{F}$ is an equivalence relation.*

Proof. Obvious since $\mathrm{d_{tv}}$ is a metric. □

Proposition 3.4. *Consider X a set, $\{\mathcal{D}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$, $\{\mathcal{E}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$ and $\{f^K : X \to \mathbb{R}\}_{K \in \mathbb{N}^n}$ a uniformly bounded family of functions. Assume $\mathcal{D} \equiv \mathcal{E} \pmod{\mathcal{F}}$. Then*

$$\mathrm{E}_{x \sim \mathcal{D}^K}[f^K(x)] \equiv \mathrm{E}_{x \sim \mathcal{E}^K}[f^K(x)] \pmod{\mathcal{F}} \tag{3.17}$$

Proof. $|\mathrm{E}_{x \sim \mathcal{D}^K}[f^K(x)] - \mathrm{E}_{x \sim \mathcal{E}^K}[f^K(x)]| \leq (\sup f - \inf f)\, \mathrm{d_{tv}}(\mathcal{D}^K, \mathcal{E}^K)$ □

Proposition 3.5. *Consider X, Y sets, $\{\mathcal{D}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$, $\{\mathcal{E}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$ and $\{f^K : X \xrightarrow{\mathrm{mk}} Y\}_{K \in \mathbb{N}^n}$ a family of Markov kernels. Then, $\mathcal{D} \equiv \mathcal{E} \pmod{\mathcal{F}}$ implies*

$$\mathcal{D}^K \ltimes f^K \equiv \mathcal{E}^K \ltimes f^K \pmod{\mathcal{F}} \tag{3.18}$$

Proof. Total variation distance is contracted by semi-direct product with a Markov kernel therefore $\mathrm{d_{tv}}(\mathcal{D}^K \ltimes f^K, \mathcal{E}^K \ltimes f^K) \leq \mathrm{d_{tv}}(\mathcal{D}^K, \mathcal{E}^K)$. □

Proposition 3.6. *Consider X, Y sets, $\{\mathcal{D}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$, $\{\mathcal{E}^K \in \mathcal{P}(X)\}_{K \in \mathbb{N}^n}$ and $\{f^K : X \xrightarrow{\mathrm{mk}} Y\}_{K \in \mathbb{N}^n}$ a family of Markov kernels. Then, $\mathcal{D} \equiv \mathcal{E} \pmod{\mathcal{F}}$ implies*

$$f^K_* \mathcal{D}^K \equiv f^K_* \mathcal{E}^K \pmod{\mathcal{F}} \tag{3.19}$$

Proof. Total variation distance is contracted by pushforward therefore

$$\mathrm{d_{tv}}(f_*^K \mathcal{D}^K, f_*^K \mathcal{E}^K) \leq \mathrm{d_{tv}}(\mathcal{D}^K, \mathcal{E}^K)$$

□

Proposition 3.7. *Consider X_1, X_2 sets, $\{\mathcal{D}_1^K \in \mathcal{P}(X_1)\}_{K \in \mathbb{N}^n}$, $\{\mathcal{E}_1^K \in \mathcal{P}(X_1)\}_{K \in \mathbb{N}^n}$, $\{\mathcal{D}_2^K \in \mathcal{P}(X_2)\}_{K \in \mathbb{N}^n}$ and $\{\mathcal{E}_2^K \in \mathcal{P}(X_2)\}_{K \in \mathbb{N}^n}$. Then, $\mathcal{D}_1 \equiv \mathcal{E}_1 \pmod{\mathcal{F}}$ and $\mathcal{D}_2 \equiv \mathcal{E}_2 \pmod{\mathcal{F}}$ imply*

$$\mathcal{D}_1^K \times \mathcal{D}_2^K \equiv \mathcal{E}_1^K \times \mathcal{E}_2^K \pmod{\mathcal{F}} \tag{3.20}$$

Proof. Total variation distance is subadditive w.r.t. direct products therefore

$$\mathrm{d_{tv}}(\mathcal{D}_1^K \times \mathcal{D}_2^K, \mathcal{E}_1^K \times \mathcal{E}_2^K) \leq \mathrm{d_{tv}}(\mathcal{D}_1^K, \mathcal{E}_1^K) + \mathrm{d_{tv}}(\mathcal{D}_2^K, \mathcal{E}_2^K)$$

□

3.3.2 Polynomial-time MΓ-schemes

The concept of a polynomial-time Γ-scheme can be generalized in a way which allows the advice to become random in itself.

Definition 3.2. Given encoded sets X and Y, a *polynomial-time* MΓ*-scheme of signature* $X \to Y$ is a triple $(S, \mathrm{r}_S, \mathrm{M}_S)$ where $S : \mathbb{N}^n \times X \times \{0,1\}^* \times \{0,1\}^* \xrightarrow{\text{alg}} Y$, $\mathrm{r}_S : \mathbb{N}^n \times \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{N}$ and $\{\mathrm{M}_S^K \in \mathcal{P}(\{0,1\}^*)\}_{K \in \mathbb{N}^n}$ are s.t.

(i) $\max_{x \in X} \max_{y,z \in \{0,1\}^*} \mathrm{T}_S(K, x, y, z) \in \Gamma^n_{\mathrm{poly}}$

(ii) $\max_{z \in \{0,1\}^*} \mathrm{T}_{\mathrm{r}_S}(K, z) \in \Gamma^n_{\mathrm{poly}}$

(iii) There is $r \in \Gamma_{\mathfrak{R}}$ s.t. for any $K \in \mathbb{N}^n$ and $z \in \operatorname{supp} \mathrm{M}_S^K$, $\mathrm{r}_S(K, z) \leq r(K)$.

(iv) There is $l \in \Gamma_{\mathfrak{A}}$ s.t. for any $K \in \mathbb{N}^n$, $\operatorname{supp} \mathrm{M}_S^K \subseteq \{0,1\}^{l(K)}$.

Abusing notation, we denote the polynomial-time MΓ-scheme $(S, \mathrm{r}_S, \mathrm{M}_S)$ by S.

$\mathrm{r}_S^K(z)$ will denote $\mathrm{r}_S(K, z)$. $\mathrm{UM}_S^K \in \mathcal{P}(\{0,1\}^* \times \{0,1\}^*)$ is the joint probability distribution over advice bitstrings and randomness bitstrings, given by

$$\mathrm{UM}_S^K(y,z) := \mathrm{M}_S^K(z)\delta_{|y|,\mathrm{r}_S^K(z)}2^{-\mathrm{r}_S^K(z)}$$

$S^K(x,y,z)$ will denote $S(K,x,y,z)$. Given $w = (y,z)$, $S^K(x,w)$ will denote $S(K,x,y,z)$. $S^K(x)$ will denote the Y-valued random variable which equals $S(K,x,y,z)$ for (y,z) sampled from UM_S^K. S_x^K will denote the probability distribution of this random variable i.e. S_x^K is the push-forward of UM_S^K by the mapping $(y,z) \mapsto S(K,x,y,z)$.

We think of S as a randomized algorithm with advice which is random in itself. In particular any polynomial-time Γ-scheme S can be regarded as a polynomial-time MΓ-scheme with

$$\mathrm{M}_S^K(z) := \delta_{z\,\mathrm{a}_S^K}$$

We will use the notation $S : X \xrightarrow{\mathrm{M}\Gamma} Y$ to signify S is a polynomial-time MΓ-scheme of signature $X \to Y$.

We introduce composition of MΓ-schemes as well.

Definition 3.3. Consider encoded sets X, Y, Z and $S : X \xrightarrow{\mathrm{M}\Gamma} Y$, $T : Y \xrightarrow{\mathrm{M}\Gamma} Z$. Choose $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t.

$$\operatorname{supp} \mathrm{M}_S^K \subseteq \{0,1\}^{\leq p(K)}$$
$$\operatorname{supp} \mathrm{M}_T^K \subseteq \{0,1\}^{\leq p(K)}$$

We can then construct $U : X \xrightarrow{\Gamma} Z$ s.t. for any $K \in \mathbb{N}^n$, $a, b \in \{0,1\}^{\leq p(K)}$, $v \in \{0,1\}^{\mathrm{r}_S(K,a)}$, $w \in \{0,1\}^{\mathrm{r}_T(K,b)}$ and $x \in X$

$$\mathrm{M}_U^K = \mathrm{c}_*^2(\mathrm{M}_S^K \times \mathrm{M}_T^K) \tag{3.21}$$
$$\mathrm{r}_U(K, \langle a, b \rangle) = \mathrm{r}_T(K,a) + \mathrm{r}_S(K,b) \tag{3.22}$$
$$U^K(x, vw, \langle a, b \rangle) = T^K(S^K(x,w,b), v, a) \tag{3.23}$$

Such a U is called the *composition* of T and S and denoted $U = T \circ S$.

3.3.3 Samplers and samplability

The concept of a *samplable* word ensemble is commonly used in average-case complexity theory. Here we introduce a relaxation of this concept which allows approximate sampling with an error compatible with the given fall space. We then proceed to introduce samplable distributional estimation problems.

Samplable word ensembles can be thought of as those ensembles which can be produced by a computationally bounded process. Samplable distributional estimation problems can be thought of as those questions that can be efficiently produced together with their answers, like an exam where the examinee cannot easily find the answer but the examinator knows it (even though the examinator is also computationally bounded).

Definition 3.4. A word ensemble $\mathcal{D}$ is called *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable* (resp. *polynomial-time $\mathcal{F}(\Gamma)$-samplable*) when there is a polynomial-time MΓ-scheme (resp. polynomial-time Γ-scheme) σ of signature $\mathbf{1} \to \{0,1\}^*$ s.t. $\mathcal{D}^K \equiv \sigma_\bullet^K$ (mod $\mathcal{F}$).

In this case, σ is called a *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler (resp. polynomial-time $\mathcal{F}(\Gamma)$-sampler) of $\mathcal{D}$*.

Definition 3.5. A distributional estimation problem $(\mathcal{D}, f)$ is called *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable (resp. polynomial-time $\mathcal{F}(\Gamma)$-samplable)* when there is a polynomial-time MΓ-scheme (resp. polynomial-time Γ-scheme) σ of signature $\mathbf{1} \to \{0,1\}^* \times \mathbb{Q}$ s.t.

(i) σ_0 is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler (resp. polynomial-time $\mathcal{F}(\Gamma)$-sampler) of $\mathcal{D}$.

(ii) For any $K \in \mathbb{N}^n$, denote $X_\sigma^K := \operatorname{supp} \sigma_{0\bullet}^K$. For any $x \in \{0,1\}^*$, denote

$$f_\sigma^K(x) := \begin{cases} \mathrm{E}_{z \sim \mathrm{UM}_\sigma^K}[\sigma^K(z)_1 \mid \sigma^K(z)_0 = x] \text{ if } x \in X_\sigma^K \\ 0 \text{ if } x \notin X_\sigma^K \end{cases}$$

We require that the function $\varepsilon(K) := \mathrm{E}_{x \sim \mathcal{D}^K}[|f_\sigma^K(x) - f(x)|]$ is in $\mathcal{F}$.

This represents the requirement of being able to efficiently generate question-answer pairs, such that the distribution of questions converges to the distribution $\mathcal{D}$, and the answers converge to the true output of the function f.

When $\sup|\sigma_1| < \infty$ (since f is bounded, this can always be assumed without loss of generality), σ is called a *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler (resp. polynomial-time $\mathcal{F}(\Gamma)$-sampler) of $(\mathcal{D}, f)$*.

For sufficiently large $\Gamma_{\mathfrak{A}}$ the requirements of $\mathcal{F}(\mathrm{M}\Gamma)$-samplability become very weak, as seen in the following propositions, which essentially say that if the bitstrings on which $\mathcal{D}$ is supported are short enough relative to the length of the advice string, then the randomized advice can just duplicate the distribution. And if there is ample advice available, then the randomized advice can also output an approximation to the true value of $f(x)$ along with x.

Proposition 3.8. *Consider a word ensemble $\mathcal{D}$ s.t. for some $l \in \Gamma_{\mathfrak{A}}$*

$$\mathcal{D}^K(\{0,1\}^{\leq l(K)}) \equiv 1 \pmod{\mathcal{F}} \tag{3.24}$$

Denote $I := \{K \in \mathbb{N}^n \mid \mathcal{D}^K(\{0,1\}^{\leq l(K)}) > 0\}$. Consider $\sigma : \mathbf{1} \xrightarrow{\mathrm{M}\Gamma} \{0,1\}^*$ s.t. for any $K \in I$

$$\mathrm{M}_\sigma^K := \mathcal{D}^K \mid \{0,1\}^{\leq l(K)}$$
$$\sigma^K(y,z) = z$$

Then, σ is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$. In particular, since such an σ can always be constructed, $\mathcal{D}$ is polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable.

Proof. $\chi_I \geq \mathcal{D}^K(\{0,1\}^{\leq l(K)})$, $1-\chi_I \leq 1-\mathcal{D}^K(\{0,1\}^{\leq l(K)})$ and therefore $1-\chi_I \in \mathcal{F}$.

Given $K \in I$, $\sigma_\bullet^K = \mathcal{D}^K \mid \{0,1\}^{\leq l(K)}$ and we get

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \mathrm{d_{tv}}(\mathcal{D}^K, \mathcal{D}^K \mid \{0,1\}^{\leq l(K)})$$

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \frac{1}{2} \sum_{x \in \{0,1\}^*} |\mathcal{D}^K(x) - (\mathcal{D}^K \mid \{0,1\}^{\leq l(K)})(x)|$$

Denote $\chi^K := \chi_{\{0,1\}^{\leq l(K)}}$.

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \frac{1}{2} \sum_{x \in \{0,1\}^*} |\mathcal{D}^K(x) - \frac{\chi^K(x)\mathcal{D}^K(x)}{\mathcal{D}^K(\{0,1\}^{\leq l(K)})}|$$

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \frac{1}{2} \sum_{x \in \{0,1\}^*} \mathcal{D}^K(x)|1 - \frac{\chi^K(x)}{\mathcal{D}^K(\{0,1\}^{\leq l(K)})}|$$

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \frac{1}{2}\left(\sum_{x\in\{0,1\}^{\leq l(K)}} \mathcal{D}^K(x)|1 - \frac{\chi^K(x)}{\mathcal{D}^K(\{0,1\}^{\leq l(K)})}| + \sum_{x\in\{0,1\}^{>l(K)}} \mathcal{D}^K(x)|1 - \frac{\chi^K(x)}{\mathcal{D}^K(\{0,1\}^{\leq l(K)})}|\right)$$

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \frac{1}{2}\left(\sum_{x\in\{0,1\}^{\leq l(K)}} \mathcal{D}^K(x)\left(\frac{1}{\mathcal{D}^K(\{0,1\}^{\leq l(K)})} - 1\right) + \sum_{x\in\{0,1\}^{>l(K)}} \mathcal{D}^K(x)\right)$$

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = \frac{1}{2}\left(\mathcal{D}^K(\{0,1\}^{\leq l(K)})\left(\frac{1}{\mathcal{D}^K(\{0,1\}^{\leq l(K)})} - 1\right) + 1 - \mathcal{D}^K(\{0,1\}^{\leq l(K)})\right)$$

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) = 1 - \mathcal{D}^K(\{0,1\}^{\leq l(K)})$$

Given arbitrary $K \in \mathbb{N}^n$,

$$\mathrm{d_{tv}}(\mathcal{D}^K, \sigma_\bullet^K) \leq \max(1 - \mathcal{D}^K(\{0,1\}^{\leq l(K)}), 1 - \chi_I)$$

□

Proposition 3.9. *Assume $\mathcal{F}$ is $\Gamma_{\mathfrak{A}}$-ample. Consider a distributional estimation problem $(\mathcal{D}, f)$ s.t. for some $l \in \Gamma_{\mathfrak{A}}$, 3.24 holds. Then, $(\mathcal{D}, f)$ is polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable.*

Proof. Consider $\zeta : \mathbb{N}^n \to (0, \frac{1}{2}]$ s.t. $\zeta \in \mathcal{F}$ and $\lfloor \log \frac{1}{\zeta} \rfloor \in \Gamma_{\mathfrak{A}}$. For any $K \in \mathbb{N}^n$ and $t \in \mathbb{R}$, let $\rho^K(t) \in \operatorname*{arg\,min}_{s\in\mathbb{Q}\cap[t-\zeta(K),t+\zeta(K)]} |\mathrm{c}_{\mathbb{Q}}(s)|$. For any $K \in \mathbb{N}^n$, define $\alpha^K : \{0,1\}^* \to \{0,1\}^*$ by

$$\alpha^K(x) := \langle x, c_{\mathbb{Q}}(\rho^K(f(x)))\rangle$$

Denote

$$I := \{K \in \mathbb{N}^n \mid \mathcal{D}^K(\{0,1\}^{\leq l(K)}) > 0\}$$

Construct $\sigma : \mathbf{1} \xrightarrow{\mathrm{M\Gamma}} \{0,1\}^* \times \mathbb{Q}$ s.t. for any $K \in I$

$$\mathrm{M}_\sigma^K := \alpha_*^K(\mathcal{D}^K \mid \{0,1\}^{\leq l(K)})$$
$$\sigma^K(y, \langle z, \mathrm{c}_{\mathbb{Q}}(t)\rangle) = (z, t)$$

By Proposition 3.8, σ_0 is a polynomial-time $\mathcal{F}(\mathrm{M\Gamma})$-sampler of $\mathcal{D}$.

Let f_σ^K be defined as in Definition 3.5. Consider any $K \in \mathbb{N}^n$. It is easy to see that for any $x \in \operatorname{supp}\mathcal{D}^K \cap \{0,1\}^{\leq l(K)}$, $f_\sigma^K(x) = \rho^K(f(x))$ (for $K \notin I$ this is vacuously true). Also, for any $x \in \{0,1\}^{>l(K)}$, $f_\sigma^K(x) = 0$. Denote

$$p^K := \mathcal{D}^K(\{0,1\}^{\leq l(K)})$$

We get

$$\mathrm{E}_{\mathcal{D}^K}[|f_\sigma^K(x) - f(x)|] = p^K \,\mathrm{E}_{\mathcal{D}^K}[|f_\sigma^K(x) - f(x)| \mid |x| \leq l(K)] + (1 - p^K)\,\mathrm{E}_{\mathcal{D}^K}[|f_\sigma^K(x) - f(x)| \mid |x| > l(K)]$$

$$\mathrm{E}_{\mathcal{D}^K}[|f_\sigma^K(x) - f(x)|] = p^K \,\mathrm{E}_{\mathcal{D}^K}[|\rho^K(f(x)) - f(x)| \mid |x| \leq l(K)] + (1 - p^K)\,\mathrm{E}_{\mathcal{D}^K}[|f(x)| \mid |x| > l(K)]$$

$$\mathrm{E}_{\mathcal{D}^K}[|f_\sigma^K(x) - f(x)|] \leq p^K\zeta(K) + (1 - p^K)\sup|f|$$

The right hand side is obviously in $\mathcal{F}$. □

We now introduce the notions of samplability over a given "base space" Y.

Definition 3.6. Consider a word ensemble $\mathcal{D}$, an encoded set Y and a family of Markov kernels $\{\pi^K : \operatorname{supp}\mathcal{D}^K \xrightarrow{\mathrm{mk}} Y\}_{K\in\mathbb{N}^n}$. $\mathcal{D}$ is called *polynomial-time $\mathcal{F}(\mathrm{M\Gamma})$-samplable (resp. polynomial-time $\mathcal{F}(\Gamma)$-samplable) relative to* π when there is a

polynomial-time MΓ-scheme (resp. polynomial-time Γ-scheme) σ of signature $Y \to \{0,1\}^*$ s.t. $\mathrm{E}_{y\sim\pi_*^K\mathcal{D}^K}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(y), \sigma_y^K)] \in \mathcal{F}$.

In this case, σ is called a *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler (resp. polynomial-time $\mathcal{F}(\Gamma)$-sampler) of $\mathcal{D}$ relative to π*. That is, even though the underlying distribution may not be samplable, if some evidence (y) is given, that permits sampling from the distribution conditional on y.

Definition 3.7. Consider a distributional estimation problem $(\mathcal{D}, f)$, an encoded set Y and a family of Markov kernels $\{\pi^K : \operatorname{supp}\mathcal{D}^K \xrightarrow{\mathrm{mk}} Y\}_{K\in\mathbb{N}^n}$. $(\mathcal{D}, f)$ is called *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable (resp. polynomial-time $\mathcal{F}(\Gamma)$-samplable) relative to π* when there is a polynomial-time MΓ-scheme (resp. polynomial-time Γ-scheme) σ of signature $Y \to \{0,1\}^* \times \mathbb{Q}$ s.t.

(i) σ_0 is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler (resp. polynomial-time $\mathcal{F}(\Gamma)$-sampler) of $\mathcal{D}$ relative to π.

(ii) For any $K \in \mathbb{N}^n$, $y \in Y$, Denote $X_{\sigma,y}^K := \operatorname{supp}\sigma_{0y}^K$. For any $x \in \{0,1\}^*$, denote

$$f_\sigma^K(x,y) := \begin{cases} \mathrm{E}_{z\sim\mathrm{UM}_\sigma^K}[\sigma^K(y,z)_1 \mid \sigma^K(y,z)_0 = x] \text{ if } x \in X_{\sigma,y}^K \\ 0 \text{ if } x \notin X_{\sigma,y}^K \end{cases}$$

We require that the function $\varepsilon(K) := \mathrm{E}_{(x,y)\sim\mathcal{D}^K\ltimes\pi^K}[|f_\sigma^K(x,y) - f(x)|]$ is in $\mathcal{F}$.

When $\sup|\sigma_1| < \infty$, σ is called a *polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler (resp. polynomial-time $\mathcal{F}(\Gamma)$-sampler) of $(\mathcal{D}, f)$ relative to π*.

Note that relative samplability reduces to absolute (ordinary) samplability when $Y = \mathbf{1}$.

The following propositions are basic properties of samplable ensembles and problems which often come in handy. Proposition 3.10 states that the expectation of a function $h(x)$ remains approximately unchanged when x is replaced with a sampler of $\mathcal{D}$, and Proposition 3.11 states that the expectation of the product of $h(x)$ and $f(x)$ remains approximately unchanged when x and $f(x)$ are replaced by question/answer pairs produced by a sampler for $(\mathcal{D}, f)$.

Proposition 3.10. *Consider a word ensemble $\mathcal{D}$, an encoded set Y, a family $\{\pi^K : \operatorname{supp}\mathcal{D}^K \xrightarrow{\mathrm{mk}} Y\}_{K\in\mathbb{N}^n}$, a set I and a uniformly bounded family $\{h_\alpha^K : (\operatorname{supp}\mathcal{D})\times Y \to \mathbb{R}\}_{\alpha\in I, K\in\mathbb{N}^n}$. Suppose σ is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$ relative to π. Then*

$$\mathrm{E}_{(x,y)\sim\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] \overset{\alpha}{\equiv} \mathrm{E}_{(y,z)\sim\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)] \pmod{\mathcal{F}} \quad (3.25)$$

Proof. If we sample (x, y) from $\mathcal{D}^K \ltimes \pi^K$ and then sample x' from $\mathcal{D}^K \mid (\pi^K)^{-1}(y)$, (x', y) will obey the distribution $\mathcal{D}^K \ltimes \pi^K$. Denote $\mathcal{D}_y^K := \mathcal{D}^K \mid (\pi^K)^{-1}(y)$. We get

$$\mathrm{E}_{(x,y)\sim\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] = \mathrm{E}_{(x,y)\sim\mathcal{D}^K\ltimes\pi^K}[\mathrm{E}_{x'\sim\mathcal{D}_y^K}[h_\alpha^K(x',y)]]$$

$$\begin{aligned}\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] - \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]\\ = \mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[\mathrm{E}_{\mathcal{D}_y^K}[h_\alpha^K(x',y)]] - \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]\end{aligned}$$

$$\begin{aligned}\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] - \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]\\ = \mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[\mathrm{E}_{\mathcal{D}_y^K}[h_\alpha^K(x',y)] - \mathrm{E}_{\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]]\end{aligned}$$

$$\begin{aligned}\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] - \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]\\ = \mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[\mathrm{E}_{\mathcal{D}_y^K}[h_\alpha^K(x',y)] - \mathrm{E}_{\sigma_y^K}[h_\alpha^K(x',y)]]\end{aligned}$$

$$\begin{aligned}|\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] - \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]|\\ \le \mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[|\mathrm{E}_{\mathcal{D}_y^K}[h_\alpha^K(x',y)] - \mathrm{E}_{\sigma_y^K}[h_\alpha^K(x',y)]|]\end{aligned}$$

$$\begin{aligned}|\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[h_\alpha^K(x,y)] - \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z),y)]|\\ \le (\sup h - \inf h)\,\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[\mathrm{d_{tv}}(\mathcal{D}_y^K, \sigma_y^K)]\end{aligned}$$

Using the defining property of σ, we get the desired result. □

Proposition 3.11. *Consider a distributional estimation problem $(\mathcal{D}, f)$, an encoded set Y, a family $\{\pi^K : \operatorname{supp}\mathcal{D}^K \xrightarrow{\mathrm{mk}} Y\}_{K\in\mathbb{N}^n}$, a set I and a uniformly bounded family*

$$\{h_\alpha^K : (\operatorname{supp}\mathcal{D}) \times Y \to \mathbb{R}\}_{\alpha\in I, K\in\mathbb{N}^n}$$

Denote $\mathcal{D}_\pi^K := \mathcal{D}^K \ltimes \pi^K$. Suppose σ is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $(\mathcal{D}, f)$ relative to π. Then

$$\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] \overset{\alpha}{\equiv} \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z)_0,y)\sigma^K(y,z)_1] \pmod{\mathcal{F}} \quad (3.26)$$

Proof. Let f_σ^K be defined as in Definition 3.7.

$$\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] - \mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f_\sigma^K(x,y)] = \mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)(f(x) - f_\sigma^K(x,y))]$$

$$|\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] - \mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f_\sigma^K(x,y)]| \leq \mathrm{E}_{\mathcal{D}_\pi^K}[|h_\alpha^K(x,y)| \cdot |f(x) - f_\sigma^K(x,y)|]$$

$$|\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] - \mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f_\sigma^K(x,y)]| \leq (\sup|h|)\,\mathrm{E}_{\mathcal{D}_\pi^K}[|f(x) - f_\sigma^K(x,y)|]$$

By property (ii) of Definition 3.7

$$\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] \overset{\alpha}{\equiv} \mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f_\sigma^K(x,y)] \pmod{\mathcal{F}}$$

Using property (i) of Definition 3.7 we can apply Proposition 3.10 to the right hand side and get

$$\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] \overset{\alpha}{\equiv} \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z)_0,y)f_\sigma^K(\sigma^K(y,z)_0,y)] \pmod{\mathcal{F}}$$

$$\begin{aligned}\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] \overset{\alpha}{\equiv} \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[&h_\alpha^K(\sigma^K(y,z)_0,y)\cdot\\ &\mathrm{E}_{z'\sim\mathrm{UM}_\sigma^K}[\sigma^K(y,z')_1 \mid \sigma^K(y,z')_0 = \sigma^K(y,z)_0]] \pmod{\mathcal{F}}\end{aligned}$$

$$\mathrm{E}_{\mathcal{D}_\pi^K}[h_\alpha^K(x,y)f(x)] \overset{\alpha}{\equiv} \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{UM}_\sigma^K}[h_\alpha^K(\sigma^K(y,z)_0,y)\sigma^K(y,z)_1] \pmod{\mathcal{F}}$$

□

3.4 Independent variables

Independent random variables F_1, F_2 satisfy

$$\mathrm{E}[F_1F_2] = \mathrm{E}[F_1]\,\mathrm{E}[F_2] \tag{3.27}$$

To formulate an analogous property for optimal polynomial-time estimators, we need a notion of independence for distributional decision problems which doesn't make the identity tautologous. Consider distributional decision problems $(\mathcal{D}, f_1)$,

$(\mathcal{D}, f_2)$. Informally, f_1 is "independent" of f_2 when learning the value of $f_2(x)$ provides no efficiently accessible information about $f_1(x)$. In the present work, we won't try to formalise this in full generality. Instead, we will construct a specific scenario in which the independence assumption is justifiable.

We start with an informal description. Suppose that $f_1(x)$ depends only on part $\pi(x)$ of the information in x i.e. $f_1(x) = g(\pi(x))$. Suppose further that given $y = \pi(x)$ it is possible to efficiently produce samples x' of $\mathcal{D} \mid \pi^{-1}(y)$ for which $f_2(x')$ is known. Then, the knowledge of $f_2(x)$ doesn't provide new information about $g(\pi(x))$ since equivalent information can be efficiently produced without this knowledge, by observing y. Moreover, if we can only efficiently produce samples x' of $\mathcal{D} \mid \pi^{-1}(y)$ together with $\tilde{f}_2(x')$ an *unbiased estimate* of $f_2(x')$, we still expect the analogue of 3.27 to hold since the expected value of $\tilde{f}_2(x') - f_2(x')$ vanishes for any given x' so it is uncorrelated with $f_1(x)$.

The following theorem formalises this setting.

Theorem 3.4. *Consider $\mathcal{D}$ a word ensemble, $f_1, f_2 : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ bounded, $(\mathcal{E}, g)$ a distributional estimation problem and $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$. Assume the following conditions:*

(i) $\pi_*^K(\mathcal{D}^K) \equiv \mathcal{E}^K \pmod{\mathcal{F}}$

(ii) Denote $\bar{g} : \{0,1\}^* \to \mathbb{R}$ the extension of g by 0. We require

$$\mathrm{E}_{(x,z)\sim\mathcal{D}^K \times \mathrm{U}_\pi^K}[|f_1(x) - \bar{g}(\pi^K(x,z))|] \in \mathcal{F}$$

(iii) $(\mathcal{D}, f_2)$ is polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable relative to π.

Suppose P_1 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(g, \mathcal{E})$ and P_2 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f_2)$. Denote $P_\pi := P_1 \circ \pi$. Construct $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_P = \mathrm{r}_{P_\pi} + \mathrm{r}_{P_2}$ and for any $x \in \{0,1\}^*$, $z_1 \in \{0,1\}^{\mathrm{r}_{P_\pi}(K)}$ and $z_2 \in \{0,1\}^{\mathrm{r}_{P_2}(K)}$

$$P^K(x, z_1 z_2) = P_\pi^K(x, z_1) P_2^K(x, z_2) \tag{3.28}$$

Then, P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f_1 f_2)$.

In order to prove Theorem 3.4 we will need the following proposition, which takes the defining inexploitability property of an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator, and extends it to the adversary S having access to randomized advice, which can be done because deterministic advice can copy the "luckiest possible advice string" drawn from the distribution over advice strings.

Proposition 3.12. *Consider $(\mathcal{D}, f)$ a distributional estimation problem, P an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$ and $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\mathrm{M}\Gamma} \mathbb{Q}$ bounded. Then*

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{UM}_S^K}[(P^K(x,y) - f(x))S^K(x, P^K(x,y), z, w)] \equiv 0 \pmod{\mathcal{F}} \tag{3.29}$$

Proof. For any $K \in \mathbb{N}^n$, choose

$$w^K \in \operatorname*{arg\,max}_{w \in \operatorname{supp} \mathrm{M}_S^K} |\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}^{\mathrm{r}_S^K(w)}}[(P^K(x,y) - f(x))S^K(x, P^K(x,y), z, w)]|$$

Construct $\bar{S} : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ s.t.

$$\mathrm{r}_{\bar{S}}(K) = \mathrm{r}_S^K(w^K)$$
$$\bar{S}^K(x,t,z) = S^K(x,t,z,w^K)$$

P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$, therefore

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_{\bar{S}}^K}[(P^K(x,y) - f(x))\bar{S}^K(x, P^K(x,y), z)] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}^{\mathrm{r}_S^K(w)}}[(P^K(x,y) - f(x))S^K(x, P^K(x,y), z, w^K)] \equiv 0 \pmod{\mathcal{F}}$$

By construction of w^K, the absolute value of the left hand side is no less than the absolute value of the left hand side of 3.29. □

Proof of Theorem 3.4. Consider $K \in \mathbb{N}^n$, $x \in \operatorname{supp} \mathcal{D}^K$, $z_1 \in \{0,1\}^{\mathrm{r}_{P_1}(K)}$, $z_2 \in \{0,1\}^{\mathrm{r}_{P_2}(K)}$ and $z_3 \in \{0,1\}^{\mathrm{r}_\pi(K)}$.

$$P^K(x, z_1 z_3 z_2) - f_1(x)f_2(x) = P_\pi^K(x, z_1 z_3)P_2^K(x, z_2) - f_1(x)f_2(x)$$

Adding and subtracting $P_\pi^K(x, z_1 z_3)f_2(x)$ from the right hand side and grouping variables, we get

$$P^K(x, z_1 z_3 z_2) - f_1(x)f_2(x)$$
$$= P_\pi^K(x, z_1 z_3)(P_2^K(x, z_2) - f_2(x)) + (P_\pi^K(x, z_1 z_3) - f_1(x))f_2(x)$$

For any bounded $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ we get

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}[(P_2^K - f_2)P_\pi^K S^K]| + |\mathrm{E}[(P_\pi^K - f_1)f_2 S^K]|$$

P_2 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f_2)$ therefore the first term on the right hand side is in $\mathcal{F}$.

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}[(P_\pi^K - f_1)f_2 S^K]| \pmod{\mathcal{F}}$$

$$\begin{aligned}|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}[(P_\pi^K - f_1)f_2 S^K] - \mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K] \\ + \mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K]| \pmod{\mathcal{F}}\end{aligned}$$

$$\begin{aligned}|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}[(P_\pi^K - f_1)f_2 S^K] - \mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K]| \\ + |\mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K]| \pmod{\mathcal{F}}\end{aligned}$$

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}[(\bar{g}\circ\pi^K - f_1)f_2 S^K]| + |\mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K]| \pmod{\mathcal{F}}$$

$$\begin{aligned}|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq (\sup|f_2|)(\sup|S|)\,\mathrm{E}[|\bar{g}\circ\pi^K - f_1|] \\ + |\mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K]| \pmod{\mathcal{F}}\end{aligned}$$

Condition ii implies the first term on the right hand side is in $\mathcal{F}$.

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}[(P_\pi^K - \bar{g}\circ\pi^K)f_2 S^K]| \pmod{\mathcal{F}}$$

Denote $\mathrm{U}_{\mathrm{tot}}^K := \mathrm{U}_{P_1}^K \times \mathrm{U}_{P_2}^K \times \mathrm{U}_S^K$. We change variables inside the expected value on the right hand side by $y := \pi^K(x, z_3)$. Observing that (x, y) obeys the distribution $\mathcal{D}^K \ltimes \pi^K$ we get

$$\begin{aligned}|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}_{\mathcal{D}^K \ltimes \pi^K \times \mathrm{U}_{\mathrm{tot}}^K}[(P_1^K(y, z_1) - \bar{g}(y))\cdot \\ f_2(x)S^K(x, P_1^K(y, z_1)P_2^K(x, z_2), z_4)]| \pmod{\mathcal{F}}\end{aligned}$$

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}_{\mathcal{D}^K \ltimes \pi^K}[\mathrm{E}_{\mathrm{U}^K_{\mathrm{tot}}}[(P_1^K(y, z_1) - \bar{g}(y)) \cdot S^K(x, P_1^K(y, z_1) P_2^K(x, z_2), z_4)] f_2(x)]| \pmod{\mathcal{F}}$$

Let σ be a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $(\mathcal{D}, f_2)$ relative to π. Applying Proposition 3.11 to the right hand side we get

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}_{\pi^K_* \mathcal{D}^K \times \mathrm{UM}^K_\sigma}[\mathrm{E}[(P_1^K(y) - \bar{g}(y)) \cdot S^K(\sigma^K(y)_0, P_1^K(y) P_2^K(\sigma^K(y)_0))] \sigma^K(y)_1]| \pmod{\mathcal{F}}$$

Using condition i we conclude that

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}_{\mathcal{E}^k \times \mathrm{UM}^K_\sigma}[\mathrm{E}[(P_1^K(y) - g(y)) \cdot S^K(\sigma^K(y)_0, P_1^K(y) P_2^K(\sigma^K(y)_0))] \sigma^K(y)_1]| \pmod{\mathcal{F}}$$

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \leq |\mathrm{E}_{\mathcal{E}^k \times \mathrm{U}^K_{\mathrm{tot}} \times \mathrm{UM}^K_\sigma}[(P_1^K(y) - g(y)) \cdot S^K(\sigma^K(y)_0, P_1^K(y) P_2^K(\sigma^K(y)_0)) \sigma^K(y)_1]| \pmod{\mathcal{F}}$$

By Proposition 3.12, this implies

$$|\mathrm{E}[(P^K - f_1 f_2)S^K]| \equiv 0 \pmod{\mathcal{F}}$$

□

The following corollary demonstrates one natural scenario in which the conditions of Theorem 3.4 hold. The scenario is one where the distribution is $\mathcal{D}_1 \times \mathcal{D}_2$, and the task is to estimate $f_1(x_1) f_2(x_2)$. By Theorem 3.4, this can be done if there is a sampler for $(\mathcal{D}_2, f_2)$, and a sampler for $\mathcal{D}_1$.

Corollary 3.2. *Consider $(\mathcal{D}_1, f_1)$, $(\mathcal{D}_2, f_2)$ distributional estimation problems. Suppose P_1 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}_1, f_1)$, P_2 is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}_2, f_2)$, σ_1 is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler for $\mathcal{D}_1$ and σ_2 is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler for $(\mathcal{D}_2, f_2)$. Define $\mathcal{D}^K := \mathrm{c}^2_*(\mathcal{D}_1^k \times \mathcal{D}_2^k)$. Define $f : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ by $f(\langle x_1, x_2 \rangle) := f_1(x_1) f_2(x_2)$. Then, there is P, an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$, s.t. $\mathrm{r}_P = \mathrm{r}_{P_1} + \mathrm{r}_{P_2}$ and for any $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma^K_{1\bullet}$, $x_2 \in \{0,1\}^*$, $z_1 \in \{0,1\}^{\mathrm{r}_{P_1}(K)}$ and $z_2 \in \{0,1\}^{\mathrm{r}_{P_2}(K)}$*

$$P^K(\langle x_1, x_2\rangle, z_1 z_2) = P_1^K(x_1, z_1) P_2^K(x_2, z_2) \tag{3.30}$$

In order to prove Corollary 3.2, we'll need to prove several minor propositions first.

Proposition 3.13. *Consider $\mathcal{D}_1$, $\mathcal{D}_2$ word ensembles and σ_1, σ_2 which are polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplers for $\mathcal{D}_1$ and $\mathcal{D}_2$ respectively. Define $\mathcal{D}^k := \mathrm{c}_*^2(\mathcal{D}_1^k \times \mathcal{D}_2^k)$. Suppose $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$ is s.t. for any $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma_{1\bullet}^K$, $x_2 \in \operatorname{supp} \sigma_{2\bullet}^K$ and $z \in \{0,1\}^{\mathrm{r}_\pi(K)}$, $\pi^K(\langle x_1, x_2\rangle, z) = x_1$. Then $\pi_*^K \mathcal{D}^K \equiv \mathcal{D}_1^K \pmod{\mathcal{F}}$*

Proof. $\sigma_{1\bullet}^K \equiv \mathcal{D}_1^K \pmod{\mathcal{F}}$ and $\sigma_{2\bullet}^K \equiv \mathcal{D}_2^K \pmod{\mathcal{F}}$. By Proposition 3.7,

$$\sigma_{1\bullet}^K \times \sigma_{2\bullet}^K \equiv \mathcal{D}_1^K \times \mathcal{D}_2^K \pmod{\mathcal{F}}$$

Denote $\mathcal{D}_\sigma^K := \mathrm{c}_*^2(\sigma_{1\bullet}^K \times \sigma_{2\bullet}^K)$. We get $\mathcal{D}_\sigma^K \equiv \mathcal{D}^K \pmod{\mathcal{F}}$ and therefore $\pi_*^K \mathcal{D}_\sigma^K \equiv \pi_*^K \mathcal{D}^K \pmod{\mathcal{F}}$ (by Proposition 3.6). Obviously $\pi_*^K \mathcal{D}_\sigma^K = \sigma_{1\bullet}^K$. We conclude that $\pi_*^K \mathcal{D}^K \equiv \sigma_{1\bullet}^K \pmod{\mathcal{F}}$ and therefore $\pi_*^K \mathcal{D}^K \equiv \mathcal{D}_1 \pmod{\mathcal{F}}$ (by Proposition 3.3). □

Proposition 3.14. *Consider $\mathcal{D}_1$, $\mathcal{D}_2$ word ensembles and σ_1, σ_2 which are polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplers for $\mathcal{D}_1$ and $\mathcal{D}_2$ respectively. Suppose $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$ is s.t. for any $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma_{1\bullet}^K$, $x_2 \in \operatorname{supp} \sigma_{2\bullet}^K$ and $z \in \{0,1\}^{\mathrm{r}_\pi(K)}$, $\pi^K(\langle x_1, x_2\rangle, z) = x_1$. Then, for any $g : \operatorname{supp} \mathcal{D}_1 \to \mathbb{R}$ bounded and $\bar{g} : \{0,1\}^* \to \mathbb{R}$ its extension by 0, we have*

$$\mathrm{E}_{(x_1,x_2,z)\sim \mathcal{D}_1^K \times \mathcal{D}_2^K \times \mathrm{U}_\pi^K}[|g(x_1) - \bar{g}(\pi^K(\langle x_1, x_2\rangle, z))|] \in \mathcal{F}$$

Proof. Denote $M := \sup g - \inf g$.

$$\mathrm{E}[|g(x_1) - \bar{g}(\pi^K(\langle x_1, x_2\rangle))|] \leq M \Pr_{\mathcal{D}_1^K \times \mathcal{D}_2^K}[(x_1, x_2) \notin \operatorname{supp} \sigma_{1\bullet}^K \times \operatorname{supp} \sigma_{2\bullet}^K]$$

$$\mathrm{E}[|g(x_1) - \bar{g}(\pi^K(\langle x_1, x_2\rangle))|] \leq M \Pr_{\sigma_{1\bullet}^K \times \sigma_{2\bullet}^K}[(x_1, x_2) \notin \operatorname{supp} \sigma_{1\bullet}^K \times \operatorname{supp} \sigma_{2\bullet}^K] \pmod{\mathcal{F}}$$

$$\mathrm{E}[|g(x_1) - \bar{g}(\pi^K(\langle x_1, x_2\rangle))|] \equiv 0 \pmod{\mathcal{F}}$$

□

Proposition 3.15. *Consider word ensembles $\mathcal{D}_1$ and $\mathcal{D}_2$ with polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplers σ_1 and σ_2 respectively. Define $\mathcal{D}^k := \mathrm{c}_*^2(\mathcal{D}_1^k \times \mathcal{D}_2^k)$. Suppose $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$ is s.t. for any $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma_{1\bullet}^K$, $x_2 \in \{0,1\}^*$ and $z \in \{0,1\}^{\mathrm{r}_\pi(K)}$, $\pi^K(\langle x_1, x_2\rangle, z) = x_1$ and, conversely, if $x \in \{0,1\}^*$ is s.t. $\pi^K(x,z) = x_1$ then x is of the form $\langle x_1, x_2'\rangle$ for some $x_2' \in \{0,1\}^*$. Consider $\sigma : \{0,1\}^* \xrightarrow{\mathrm{M}\Gamma} \{0,1\}^*$ s.t. $\mathrm{UM}_\sigma^K = \mathrm{UM}_{\sigma_2}^K$ and for any $x \in \operatorname{supp} \sigma_{1\bullet}^K$, $\sigma^K(x,z,w) = \langle x, \sigma_2^K(z,w)\rangle$. Then, σ is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$ relative to π. In particular, since such an σ can always be constructed, $\mathcal{D}$ is polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable relative to π.*

Proof.

$$\mathcal{D}^K \equiv \mathrm{c}_*^2(\sigma_{1\bullet}^K \times \sigma_{2\bullet}^K) \pmod{\mathcal{F}}$$

$$\pi_*^K \mathcal{D}^K \equiv \pi_*^K \, \mathrm{c}_*^2(\sigma_{1\bullet}^K \times \sigma_{2\bullet}^K) \pmod{\mathcal{F}}$$

$$\pi_*^K \mathcal{D}^K \equiv \sigma_{1\bullet}^K \pmod{\mathcal{F}}$$

Denote $\mathcal{D}_x^K := \mathcal{D} \mid (\pi^K)^{-1}(x)$.

$$\mathrm{E}_{x \sim \pi_*^K \mathcal{D}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_x^K, \sigma_x^K)] \equiv \mathrm{E}_{x \sim \sigma_{1\bullet}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_x^K, \sigma_x^K)] \pmod{\mathcal{F}}$$

For any $x \in \operatorname{supp} \sigma_{1\bullet}^K$, $\mathcal{D}_x^K = \mathrm{c}_*^2(\delta_x \times \mathcal{D}_2^K)$ and $\sigma_x^K = \mathrm{c}_*^2(\delta_x \times \sigma_{2\bullet}^K)$.

$$\mathrm{E}_{x \sim \pi_*^K \mathcal{D}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_x^K, \sigma_x^K)] \equiv \mathrm{E}_{x \sim \sigma_{1\bullet}^K}[\mathrm{d}_{\mathrm{tv}}(\mathrm{c}_*^2(\delta_x \times \mathcal{D}_2^K), \mathrm{c}_*^2(\delta_x \times \sigma_{2\bullet}^K))] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{x \sim \pi_*^K \mathcal{D}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_x^K, \sigma_x^K)] \equiv \mathrm{E}_{x \sim \sigma_{1\bullet}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_2^K, \sigma_{2\bullet}^K)] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{x \sim \pi_*^K \mathcal{D}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_x^K, \sigma_x^K)] \equiv \mathrm{d}_{\mathrm{tv}}(\mathcal{D}_2^K, \sigma_{2\bullet}^K) \pmod{\mathcal{F}}$$

$$\mathrm{E}_{x \sim \pi_*^K \mathcal{D}^K}[\mathrm{d}_{\mathrm{tv}}(\mathcal{D}_x^K, \sigma_x^K)] \equiv 0 \pmod{\mathcal{F}}$$

□

Proposition 3.16. *Consider $\mathcal{D}_1$ a word ensemble with polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler σ and $(\mathcal{D}_2, f)$ a distributional estimation problem with polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler τ. Define the distributional estimation problem $(\mathcal{D}, \bar{f})$ by*

$$\mathcal{D}^k := \mathrm{c}_*^2(\mathcal{D}_1^k \times \mathcal{D}_2^k)$$
$$\bar{f}(\langle x_1, x_2 \rangle) = f(x_2)$$

Suppose $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$ *is s.t. for any* $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma_\bullet^K$, $x_2 \in \{0,1\}^*$ *and* $z \in \{0,1\}^{\mathrm{r}_\pi(K)}$, $\pi^K(\langle x_1, x_2 \rangle, z) = x_1$ *and, conversely, if* $x \in \{0,1\}^*$ *is s.t.* $\pi^K(x,z) = x_1$ *then* x *is of the form* $\langle x_1, x_2' \rangle$ *for some* $x_2' \in \{0,1\}^*$. *Then,* $(\mathcal{D}, \bar{f})$ *is polynomial-time* $\mathcal{F}(\mathrm{M}\Gamma)$*-samplable relative to* π.

Proof. Construct $\bar{\tau} : \{0,1\}^* \xrightarrow{\mathrm{M}\Gamma} \{0,1\}^* \times \mathbb{Q}$ s.t. $\mathrm{UM}_{\bar{\tau}}^K = \mathrm{UM}_\tau^K$ and for any $x \in \operatorname{supp} \sigma_\bullet^K$

$$\bar{\tau}^K(x,y,z) = (\langle x, \tau^K(y,z,w)_0 \rangle, \tau^K(y,z,w)_1)$$

By Proposition 3.15, $\bar{\tau}_0$ is a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$ relative to π.

$$\mathcal{D}^K \equiv \mathrm{c}_*^2(\sigma_\bullet^K \times \tau_{0\bullet}^K) \pmod{\mathcal{F}}$$

$$\mathcal{D}^K \ltimes \pi^K \equiv \mathrm{c}_*^2(\sigma_\bullet^K \times \tau_{0\bullet}^K) \ltimes \pi^K \pmod{\mathcal{F}}$$

Let f_τ^K and $f_{\bar{\tau}}^K$ be defined as in Definition 3.7.

$$\mathrm{E}_{(x,y)\sim\mathcal{D}^K\ltimes\pi^K}[|f_{\bar{\tau}}^K(x,y) - \bar{f}(x)|] \equiv \mathrm{E}_{(x,y)\sim\mathrm{c}_*^2(\sigma_\bullet^K\times\tau_{0\bullet}^K)\ltimes\pi^K}[|f_{\bar{\tau}}^K(x,y) - \bar{f}(x)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv \mathrm{E}_{(x_1,x_2)\sim\sigma_\bullet^K\times\tau_{0\bullet}^K}[|f_{\bar{\tau}}^K(\langle x_1,x_2\rangle, x_1) - \bar{f}(\langle x_1,x_2\rangle)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv \mathrm{E}_{(x_1,x_2)\sim\sigma_\bullet^K\times\tau_{0\bullet}^K}[|\mathrm{E}_{\mathrm{UM}_{\bar{\tau}}^K}[\bar{\tau}_1^K(x_1) \mid \bar{\tau}^K(x_1)_0 = \langle x_1,x_2\rangle] - f(x_2)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\ltimes\pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv \mathrm{E}_{(x_1,x_2)\sim\sigma_\bullet^K\times\tau_{0\bullet}^K}[|\mathrm{E}_{\mathrm{UM}_{\bar{\tau}}^K}[\tau_1^K \mid \langle x_1,\tau_0^K\rangle = \langle x_1,x_2\rangle] - f(x_2)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \ltimes \pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv \mathrm{E}_{(x_1,x_2)\sim\sigma_\bullet^K \times \tau_{0\bullet}^K}[|\mathrm{E}_{\mathrm{UM}_\tau^K}[\tau_1^K \mid \tau_0^K = x_2] - f(x_2)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \ltimes \pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv \mathrm{E}_{x_2\sim\tau_{0\bullet}^K}[|f_\tau^K(x_2) - f(x_2)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \ltimes \pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv \mathrm{E}_{x_2\sim\mathcal{D}_2^K}[|f_\tau^K(x_2) - f(x_2)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \ltimes \pi^K}[|f_{\bar{\tau}}^K - \bar{f}|] \equiv 0 \pmod{\mathcal{F}}$$

□

Proposition 3.17. *Consider word ensemble $\mathcal{D}_1$ with polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler σ and $(\mathcal{D}_2, f)$ a distributional estimation problem. Define the distributional estimation problem $(\mathcal{D}, \bar{f})$ by*

$$\mathcal{D}^k := \mathrm{c}_*^2(\mathcal{D}_1^k \times \mathcal{D}_2^k)$$
$$\bar{f}(\langle x_1, x_2\rangle) = f(x_2)$$

Suppose P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}_2, f)$. Let $\bar{P} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ be s.t. $\mathrm{r}_{\bar{P}} = \mathrm{r}_P$ and for any $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma_\bullet^K$, $x_2 \in \operatorname{supp} \mathcal{D}_2^K$ and $z \in \{0,1\}^{\mathrm{r}_P(K)}$, $\bar{P}^K(\langle x_1, x_2\rangle, z) = P^K(x_2, z)$. Then, $\bar{P}$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \bar{f})$.

Proof. Consider any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Denote $\mathrm{U}_{PS}^K := \mathrm{U}_P^K \times \mathrm{U}_S^K$, $\mathcal{D}_{PS}^K := \mathcal{D}^K \times \mathrm{U}_{PS}^K$.

$$\mathrm{E}_{\mathcal{D}_{PS}^K}[(\bar{P}^K(x) - \bar{f}(x))S^K(x, \bar{P}^K(x))]$$
$$= \mathrm{E}_{\mathcal{D}_1^K \times \mathcal{D}_2^K \times \mathrm{U}_{PS}^K}[(\bar{P}^K(\langle x_1, x_2\rangle) - \bar{f}(\langle x_1, x_2\rangle))S^K(\langle x_1, x_2\rangle, \bar{P}^K(\langle x_1, x_2\rangle))]$$

$$\mathrm{E}_{\mathcal{D}_{PS}^K}[(\bar{P}^K(x) - \bar{f}(x))S^K(x, \bar{P}^K(x))]$$
$$= \mathrm{E}_{\mathcal{D}_1^K \times \mathcal{D}_2^K \times \mathrm{U}_{PS}^K}[(\bar{P}^K(\langle x_1, x_2\rangle) - f(x_2))S^K(\langle x_1, x_2\rangle, \bar{P}^K(\langle x_1, x_2\rangle))]$$

$$\mathrm{E}_{\mathcal{D}_{PS}^K}[(\bar{P}^K(x) - \bar{f}(x))S^K(x, \bar{P}^K(x))]$$
$$= \mathrm{E}_{\mathcal{D}_1^K}[\mathrm{E}_{\mathcal{D}_2^K \times \mathrm{U}_{PS}^K}[(\bar{P}^K(\langle x_1, x_2\rangle) - f(x_2))S^K(\langle x_1, x_2\rangle, \bar{P}^K(\langle x_1, x_2\rangle))]]$$

Applying Proposition 3.10 (with $Y = \mathbf{1}$) to the right hand side, we get

$$\mathrm{E}_{\mathcal{D}_{PS}^K}[(\bar{P}^K - \bar{f})S^K] \equiv \mathrm{E}_{\mathrm{UM}_\sigma^K}[\mathrm{E}_{\mathcal{D}_2^K \times \mathrm{U}_{PS}^K}[(\bar{P}^K(\langle \sigma^K, x_2\rangle) - f(x_2))\cdot S^K(\langle \sigma^K, x_2\rangle, \bar{P}^K(\langle \sigma^K, x_2\rangle))]] \pmod{\mathcal{F}}$$

$$E_{\mathcal{D}_{PS}^K}[(\bar{P}^K - \bar{f})S^K] \equiv \mathrm{E}_{\mathrm{UM}_\sigma^K}[\mathrm{E}_{\mathcal{D}_2^K \times \mathrm{U}_{PS}^K}[(P^K(x_2) - f(x_2))\cdot S^K(\langle \sigma^K, x_2\rangle, P^K(x_2))]] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}_{PS}^K}[(\bar{P}^K - \bar{f})S^K] \equiv \mathrm{E}_{\mathcal{D}_2^K \times \mathrm{U}_{PS}^K \times \mathrm{UM}_\sigma^K}[(P^K(x_2) - f(x_2))\cdot S^K(\langle \sigma^K, x_2\rangle, P^K(x_2))] \pmod{\mathcal{F}}$$

Using the fact that P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}_2, f)$, we conclude

$$\mathrm{E}_{\mathcal{D}_{PS}^K}[(\bar{P}^K - \bar{f})S^K] \equiv 0 \pmod{\mathcal{F}}$$

□

Proof of Corollary 3.2. Define $\bar{f}_1, \bar{f}_2 : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ by $\bar{f}_1(\langle x_1, x_2\rangle) = f_1(x_1)$, $\bar{f}_2(\langle x_1, x_2\rangle) = f_2(x_2)$.

Construct $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$ s.t. $\mathrm{r}_\pi \equiv 0$, for any $K \in \mathbb{N}^n$, $x_1 \in \operatorname{supp} \sigma_{1\bullet}^K$ and $x_2 \in \{0,1\}^*$, $\pi^K(\langle x_1, x_2\rangle) = x_1$ and, conversely, if $x \in \{0,1\}^*$ is s.t. $\pi^K(x) = x_1$ then x is of the form $\langle x_1, x_2'\rangle$ for some $x_2' \in \{0,1\}^*$. This is possible because the runtime of σ_1^K is bounded by a polynomial in K so the length of σ_1^K's output is also bounded by a polynomial in K, implying π^K only has to read a polynomial size prefix of its input in order to output x_1. On the other hand, if the input is not of the form $\langle x_1, x_2\rangle$ for x_1 sufficiently short to be in $\operatorname{supp} \sigma_{1\bullet}^K$, π may output a string too long to be in $\operatorname{supp} \sigma_{1\bullet}^K$.

Construct $\bar{P} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. $\mathrm{r}_{\bar{P}} = \mathrm{r}_{P_2}$ and for any $x_1 \in \operatorname{supp} \sigma_{1\bullet}^K$, $x_2 \in \{0,1\}^*$ and $z \in \{0,1\}^{\mathrm{r}_{P_2}(K)}$, $\bar{P}^K(\langle x_1, x_2\rangle, z) = P_2^K(x_2, z)$. This is possible for the same

reason as above: $\bar{P}$ skips the polynomial size prefix corresponding to x_1 and then executes a simulation of running P_2 on x_2, even if x_2 is too long to read in full. By Proposition 3.17, $\bar{P}$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \bar{f}_2)$.

We apply Theorem 3.4 where $\bar{f}_1$, $\bar{f}_2$ play the roles of f_1, f_2 and $(\mathcal{D}_1, f_1)$ plays the role of $(\mathcal{E}, g)$: condition i holds due to Proposition 3.13, condition ii holds due to Proposition 3.14 and condition iii holds due to Proposition 3.16. This gives us P, an optimal polynomial-time estimator for $(\mathcal{D}, f)$ s.t. $\mathrm{r}_P = \mathrm{r}_{P_1} + \mathrm{r}_{P_2}$ and for any $z_1 \in \{0,1\}^{\mathrm{r}_{P_1}(K)}$ and $z_2 \in \{0,1\}^{\mathrm{r}_{P_1}(K)}$

$$P^K(x, z_1 z_2) = P_1^K(\pi^K(x), z_1)\bar{P}^K(x, z_2)$$

In particular, for any $x_1 \in \operatorname{supp} \sigma_1^K$ and $x_2 \in \{0,1\}^*$

$$P^K(\langle x_1, x_2\rangle, z_1 z_2) = P_1^K(x_1, z_2)P_2^K(x_2, z_2)$$

□

4 Reductions and completeness

In this section we study notions of Karp reduction between distributional estimation problems such that the pull-back of an optimal polynomial-time estimator is an optimal polynomial-time estimator. It is also interesting to study Cook reductions but we avoid it in the present work.

First, we demonstrate that the notion of Karp reduction used in average-case complexity theory is insufficiently strong for our purpose.

Consider the setting of Corollary 2.2. Denote $\mathcal{D}^k := \mathrm{U}^{2k}$ and define $\chi : \operatorname{supp} \mathcal{D} \to \{0,1\}$ s.t. for any $x, y \in \{0,1\}^k$, $\chi(xy) = x \cdot y$. Construct $\pi_f : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$ s.t. for any $x, y \in \{0,1\}^k$, $\pi_f^k(xy) = \langle f(x), y\rangle$. π_f can be regarded as a Karp reduction of $(\mathcal{D}, \chi)$ to $(\mathcal{D}_{(f)}, \chi_f)$ since for any $z \in \operatorname{supp} \mathcal{D}^k$ we have $\chi_f(\pi_f^k(z)) = \chi(z)$ and $(\pi_f)_* \mathcal{D} = \mathcal{D}_{(f)}$[13]. However, the pullback of P is *not* an $\mathcal{F}_{\mathrm{neg}}(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi)$ since its error is $\mathrm{E}_{z \sim \mathcal{D}^k}[(\frac{1}{2} - \chi(z))^2] = \frac{1}{4}$ whereas we can construct $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $z \in \operatorname{supp} \mathcal{D}^k$, $Q^k(z) = \chi(z)$ and therefore $\mathrm{E}_{z \sim \mathcal{D}^k}[(Q^k(z) - \chi(z))^2] = 0$.

We will describe several types of reductions that preserve optimal polynomial-time estimators. After that, we will characterize reductions that can be constructed by composing those types and prove a completeness theorem.

[13] This is a much stronger condition than what is needed for a reduction to preserve average-case complexity. See [4] for details.

4.1 Strict pseudo-invertible reductions

Definition 4.1. Consider $(\mathcal{D}, f)$, $(\mathcal{E}, g)$ distributional estimation problems and $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$. π is called a *precise strict pseudo-invertible $\mathcal{F}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$* when

(i) $\pi_*^K \mathcal{D}^K \equiv \mathcal{E}^K \pmod{\mathcal{F}}$

(ii) Denote $\bar{g} : \{0,1\}^* \to \mathbb{R}$ the extension of g by 0. We require

$$\mathrm{E}_{(x,z)\sim\mathcal{D}^K \times \mathrm{U}_\pi^K}[|f(x) - \bar{g}(\pi^K(x,z))|] \equiv 0 \pmod{\mathcal{F}}$$

(iii) $\mathcal{D}$ is polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable relative to π.

Note that condition iii is violated in the one-way function example above, and in particular it ensures that the problem doesn't become significantly more difficult after applying π.

Also, notice the similarity of condition ii to a randomized Karp reduction (page 189 in [12]). Reexpressing that definition in our terminology, it is $\forall x : \mathrm{E}_{z\sim\mathrm{U}_\pi^K}[|f(x) - g(\pi^K(x,z))|] \leq \mu(K)$, where μ is a negligible function.

Precise strict pseudo-invertible $\mathcal{F}(\Gamma)$-reductions preserve $\mathcal{F}^\sharp(\Gamma)$-optimal estimators as a simple corollary of Theorem 3.4:

Corollary 4.1. *Consider $(\mathcal{D}, f)$, $(\mathcal{E}, g)$ distributional estimation problems and π a precise strict pseudo-invertible $\mathcal{F}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$. Suppose P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$. Then, $P \circ \pi$ is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. Follows directly from Theorem 3.4 for $f_1 = f$, $f_2 \equiv 1$, $P_2 \equiv 1$. This relies on the trivial observation that $(\mathcal{D}, 1)$ is samplable relative to π iff $\mathcal{D}$ is samplable relative to π. □

$\mathcal{F}(\Gamma)$-optimal estimators are also preserved.

Theorem 4.1. *Consider $(\mathcal{D}, f)$, $(\mathcal{E}, g)$ distributional estimation problems and π a precise strict pseudo-invertible $\mathcal{F}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$. Suppose P is an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$. Then, $P \circ \pi$ is an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.*

Proposition 4.1. *Consider $(\mathcal{D}, f)$ a distributional estimation problem and P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$. Then, for any $Q : \{0,1\}^* \xrightarrow{\mathrm{M}\Gamma} \mathbb{Q}$ bounded*

$$\mathrm{E}_{(x,y)\sim\mathcal{D}^K\times\mathrm{U}_P^K}[(P^K(x,y)-f(x))^2] \leq \mathrm{E}_{(x,y)\sim\mathcal{D}^K\times\mathrm{UM}_Q^K}[(Q^K(x,y)-f(x))^2] \pmod{\mathcal{F}} \tag{4.1}$$

Proof. For any $K \in \mathbb{N}^n$, choose

$$w^K \in \operatorname*{arg\,max}_{w\in\operatorname{supp}\mathrm{M}_Q^K} \mathrm{E}_{(x,z)\sim\mathcal{D}^K\times\mathrm{U}^{\mathrm{r}_Q^K(w)}}[(Q^K(x,z,w)-f(x))^2]$$

Construct $\bar{Q} : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t.

$$\mathrm{r}_{\bar{Q}}(K) = \mathrm{r}_Q^K(w^K)$$
$$\bar{Q}^K(x,z) = \bar{Q}^K(x,z,w)$$

Equation 2.5 for $\bar{Q}$ implies 4.1. □

Proposition 4.2. *Consider $\{F^K\}_{K\in\mathbb{N}^n}$, $\{G_1^K\}_{K\in\mathbb{N}^n}$, $\{G_2^K\}_{K\in\mathbb{N}^n}$ uniformly bounded families of random variables and suppose $\mathrm{E}[|G_1^K - G_2^K|] \in \mathcal{F}$. Then*

$$\mathrm{E}[(F^K+G_1^K)^2] \equiv \mathrm{E}[(F^K+G_2^K)^2] \pmod{\mathcal{F}} \tag{4.2}$$

Proof.

$$\mathrm{E}[(F^K+G_1^K)^2] - \mathrm{E}[(F^K+G_2^K)^2] = \mathrm{E}[(2F^K+G_1^K+G_2^K)(G_1^K-G_2^K)]$$

$$|\mathrm{E}[(F^K+G_1^K)^2] - \mathrm{E}[(F^K+G_2^K)^2]| \leq (2\sup F + \sup G_1 + \sup G_2)\,\mathrm{E}[|G_1^K - G_2^K|]$$

□

Proof of Theorem 4.1. Let σ be an $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$ relative to π. Consider any $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Applying Proposition 4.1 for P and $Q\circ\sigma$, we get

$$\mathrm{E}_{\mathcal{E}^K\times\mathrm{U}_P^K}[(P^K-g)^2] \leq \mathrm{E}_{\mathcal{E}^K\times\mathrm{U}_Q^K\times\mathrm{UM}_\sigma^K}[((Q\circ\sigma)^K-g)^2] \pmod{\mathcal{F}}$$

Using condition i of Definition 4.1

$$\mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{U}_P^K}[(P^K-\bar{g})^2] \leq \mathrm{E}_{\pi_*^K\mathcal{D}^K\times\mathrm{U}_Q^K\times\mathrm{UM}_\sigma^K}[((Q\circ\sigma)^K-\bar{g})^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\pi_*^K \mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - \bar{g})^2] \leq \mathrm{E}_{\pi_*^K \mathcal{D}^K \times \mathrm{UM}_\sigma^K}[\mathrm{E}_{\mathrm{U}_Q^K}[((Q \circ \sigma)^K - \bar{g})^2]] \pmod{\mathcal{F}}$$

The right hand side has the form of the right hand side in 3.25 enabling us to apply Proposition 3.10 and get

$$\mathrm{E}_{\pi_*^K \mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - \bar{g})^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_\pi^K}[\mathrm{E}_{\mathrm{U}_Q^K}[(Q^K - \bar{g} \circ \pi^K)^2]] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_\pi^K \times \mathrm{U}_P^K}[((P \circ \pi)^K - \bar{g} \circ \pi^K)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_\pi^K \times \mathrm{U}_Q^K}[(Q^K - \bar{g} \circ \pi^K)^2] \pmod{\mathcal{F}}$$

By Proposition 4.2 and condition ii of Definition 4.1

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_\pi^K \times \mathrm{U}_P^K}[((P \circ \pi)^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] \pmod{\mathcal{F}}$$

□

We now consider a more general type of reduction which only preserves the function on average (the only difference is in condition ii):

Definition 4.2. Consider $(\mathcal{D}, f)$, $(\mathcal{E}, g)$ distributional estimation problems and $\pi : \{0,1\}^* \xrightarrow{\Gamma} \{0,1\}^*$. π is called a *strict pseudo-invertible $\mathcal{F}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$* when

(i) $\pi_*^K \mathcal{D}^K \equiv \mathcal{E}^K \pmod{\mathcal{F}}$

(ii) Denote $\bar{g} : \{0,1\}^* \to \mathbb{R}$ the extension of g by 0. We require

$$\mathrm{E}_{(x,z) \sim \mathcal{D}^K}[|f(x) - \mathrm{E}_{\mathrm{U}_\pi^K}[g(\pi^K(x,z))]|] \equiv 0 \pmod{\mathcal{F}}$$

(iii) $\mathcal{D}$ is polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-samplable relative to π.

Theorem 4.2. *Suppose $\gamma \in \Gamma^n_{\mathrm{poly}}$ is s.t. $\gamma^{-\frac{1}{2}} \in \mathcal{F}$. Consider $(\mathcal{D}, f)$, $(\mathcal{E}, g)$ distributional estimation problems, π a strict pseudo-invertible $\mathcal{F}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ and P_g an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$. Assume $\gamma(\mathrm{r}_P + \mathrm{r}_\pi) \in \Gamma_{\mathfrak{R}}$. Construct P_f s.t. for any $\{z_i \in \{0,1\}^{\mathrm{r}_\pi(K)}\}_{i \in [\gamma(K)]}$ and $\{w_i \in \{0,1\}^{\mathrm{r}_{P_g}(K)}\}_{i \in [\gamma(K)]}$*

$$\mathrm{r}_{P_f}(K) = \gamma(K)(\mathrm{r}_{P_g}(K) + \mathrm{r}_\pi(K)) \tag{4.3}$$

$$P_f^K\left(x, \prod_{i\in[\gamma(K)]} w_i z_i\right) = \frac{1}{\gamma(K)} \sum_{i\in[\gamma(K)]} P_g^K(\pi^K(x, z_i), w_i) \tag{4.4}$$

Then, P_f is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.

Proposition 4.3. *Consider $\gamma \in \Gamma^n_{\mathrm{poly}}$, $\mathcal{D}$ a word ensemble and $\bar{g} : \{0,1\}^* \to \mathbb{R}$ bounded. Then,*

$$\mathrm{E}_{(x,z)\sim\mathcal{D}^K\times\prod_{i\in[\gamma(K)]}\mathrm{U}_\pi^K}[|\mathrm{E}_{z\sim\mathrm{U}_\pi^K}[\bar{g}(\pi^K(x,z))] - \frac{1}{\gamma(K)}\sum_{i\in[\gamma(K)]}\bar{g}(\pi^K(x,z_i))|] \leq \frac{\sup|\bar{g}|}{\gamma(K)^{\frac{1}{2}}} \tag{4.5}$$

Proof. Denote $\mathrm{U}_\gamma^K := \prod_{i\in[\gamma(K)]}\mathrm{U}_\pi^K$. Using $|X| = \sqrt{X^2}$, applying Jensen's inequality to move the square root outside the second expectation, and partially pulling the $\frac{1}{\gamma(K)}$ out,

$$\mathrm{E}[|\mathrm{E}[\bar{g}(\pi^K(x,z))] - \frac{1}{\gamma(K)}\sum_{i\in[\gamma(K)]}\bar{g}(\pi^K(x,z_i))|]$$

$$\leq \frac{1}{\sqrt{\gamma(K)}}\,\mathrm{E}_{\mathcal{D}^K}\left[\sqrt{\frac{1}{\gamma(K)}\,\mathrm{E}_{\mathrm{U}_\gamma^K}\left[\left(\sum_{i\in[\gamma(K)]}\mathrm{E}_{\mathrm{U}_\pi^K}[\bar{g}(\pi^K(x,z))] - \bar{g}(\pi^K(x,z_i))\right)^2\right]}\right]$$

Because the z_i are i.i.d, the sum of the variances is the variance of the sum, so

$$\mathrm{E}_{\mathrm{U}_\gamma^K}\left[\left(\sum_{i\in[\gamma(K)]}\mathrm{E}_{\mathrm{U}_\pi^K}[\bar{g}(\pi^K(x,z))] - \bar{g}(\pi^K(x,z_i))\right)^2\right] = \gamma(K)\,\mathrm{Var}_{\mathrm{U}_\pi^K}[\bar{g}(\pi^K(x,z))]$$

Substituting this into the previous equation, canceling $\gamma(K)$, and using the fact that $\sqrt{\mathrm{Var}(X)} \leq \sup|X|$, we get

$$\mathrm{E}[|\mathrm{E}[\bar{g}(\pi^K(x,z))] - \frac{1}{\gamma(K)}\sum_{i\in[\gamma(K)]}\bar{g}(\pi^K(x,z_i))|] \leq \frac{\sup|\bar{g}|}{\gamma(K)^{\frac{1}{2}}}$$

□

Proof of Theorem 4.2. Consider any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Denote $\mathrm{U}^K_{PS} := \mathrm{U}^K_{P_f} \times \mathrm{U}^K_S$. Using condition ii of Definition 4.2

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{PS}}[(P_f^K(x) - f(x))S(x, P_f^K(x))] \\ \equiv \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{PS}}[(P_f^K(x) - \mathrm{E}_{\mathrm{U}^K_\pi}[g(\pi^K(x))])S(x, P_f^K(x))] \pmod{\mathcal{F}}$$

Using the construction of P_f, the assumption on γ and Proposition 4.3, we get

$$\mathrm{E}[(P_f^K - f)S] \equiv \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{PS}}\left[\left(\frac{1}{\gamma(K)} \sum_{i \in [\gamma(K)]} P_g^K(\pi^K(x, z_i), w_i) \right.\right. \\ \left.\left. - \frac{1}{\gamma(K)} \sum_{i \in [\gamma(K)]} \bar{g}(\pi^K(x, z_i))\right) S(x, P_f^K(x))\right] \pmod{\mathcal{F}}$$

$$\mathrm{E}[(P_f^K - f)S] \equiv \\ \frac{1}{\gamma(K)} \sum_{i \in [\gamma(K)]} \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{PS}}[(P_g^K(\pi^K(x, z_i), w_i) - \bar{g}(\pi^K(x, z_i)))S(x, P_f^K(x))] \pmod{\mathcal{F}}$$

All the terms in the sum are equal, therefore

$$\mathrm{E}[(P_f^K - f)S] \equiv \\ \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_{PS}}[(P_g^K(\pi^K(x, z_0), w_0) - \bar{g}(\pi^K(x, z_0)))S(x, P_f^K(x))] \pmod{\mathcal{F}}$$

Let σ be a polynomial-time $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$ relative to π. Denote

$$\mathcal{D}_\pi^K := \pi_*^K \mathcal{D}^K$$
$$\mathrm{U}_0^K := \left(\prod_{i \in [\gamma(K)]} \mathrm{U}^K_{P_g}\right) \times \left(\prod_{i \in [\gamma(K)] \setminus 0} \mathrm{U}^K_\pi\right) \times \mathrm{U}^K_S \times \mathrm{UM}^K_\sigma$$

Applying Proposition 3.10 we get

$$\mathrm{E}[(P_f^K - f)S] \equiv \mathrm{E}_{\mathcal{D}_\pi^K \times \mathrm{U}_0^K}\left[(P_g^K - \bar{g})\cdot S\left(\sigma^K, \frac{1}{\gamma(K)}(P_g^K + \sum_{i\in[\gamma(K)]\setminus 0} P_g^K(\pi^K(\sigma^K, z_i)))\right)\right] \pmod{\mathcal{F}}$$

Using condition i of Definition 4.2, we get

$$\mathrm{E}[(P_f^K - f)S] \equiv \mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_0^K}\left[(P_g^K - g)\cdot S\left(\sigma^K, \frac{1}{\gamma(K)}(P_g^K + \sum_{i\in[\gamma(K)]\setminus 0} P_g^K(\pi^K(\sigma^K, z_j)))\right)\right] \pmod{\mathcal{F}}$$

P_g is a $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$, therefore

$$\mathrm{E}[(P_f^K - f)S] \equiv 0 \pmod{\mathcal{F}}$$

□

Above we showed that strict pseudo-invertible reductions preserve $\mathcal{F}^\sharp(\Gamma)$-optimal estimators. We will now see that they preserve $\mathcal{F}(\Gamma)$-optimal estimators as well, as Theorem 4.3 states.

Theorem 4.3. *Suppose $\gamma \in \Gamma^n_{\mathrm{poly}}$ is s.t. $\gamma^{-\frac{1}{2}} \in \mathcal{F}$. Consider $(\mathcal{D}, f)$, $(\mathcal{E}, g)$ distributional estimation problems, π a strict pseudo-invertible $\mathcal{F}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ and P_g an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$. Assume $\mathrm{r}_P + \gamma\,\mathrm{r}_\pi \in \Gamma_{\mathfrak{R}}$. Construct P_f s.t. for any $\{z_i \in \{0,1\}^{\mathrm{r}_\pi(K)}\}_{i\in[\gamma(K)]}$ and $w \in \{0,1\}^{\mathrm{r}_{P_g}(K)}$*

$$\mathrm{r}_{P_f}(K) = \mathrm{r}_{P_g}(K) + \gamma(K)\,\mathrm{r}_\pi(K) \tag{4.6}$$

$$P_f^K\left(x, w \prod_{i\in[\gamma(K)]} z_i\right) = \frac{1}{\gamma(K)} \sum_{i\in[\gamma(K)]} P_g^K(\pi^K(x, z_i), w) \tag{4.7}$$

Then, P_f is an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, g)$.

Proposition 4.4. *Consider F a bounded random variable and $s, t \in \mathbb{R}$. Then*

$$\mathrm{E}[(F-s)^2 - (F-t)^2] = (\mathrm{E}[F] - s)^2 - (\mathrm{E}[F] - t)^2 \tag{4.8}$$

Proof.

$$\mathrm{E}[(F-s)^2-(F-t)^2]=\mathrm{E}[(2F-s-t)(t-s)]$$

$$\mathrm{E}[(F-s)^2-(F-t)^2]=(2\,\mathrm{E}[F]-s-t)(t-s)$$

$$\mathrm{E}[(F-s)^2-(F-t)^2]=(\mathrm{E}[F]-s)^2-(\mathrm{E}[F]-t)^2$$

□

Proof of Theorem 4.3. Let σ be an $\mathcal{F}(\mathrm{M}\Gamma)$-sampler of $\mathcal{D}$ relative to π. Consider any $Q_f : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Construct $Q_g : \{0,1\}^* \xrightarrow{\mathrm{M}\Gamma} \mathbb{Q}$ s.t. for any $z_\sigma \in \mathrm{UM}^K_\sigma$, $z_Q \in \{0,1\}^{\mathrm{r}_{Q_f}(K)}$, $z_\pi \in \{0,1\}^{\gamma(K)\,\mathrm{r}_\pi(K)}$ and $z_g \in \{0,1\}^{\mathrm{r}_{P_g}(K)}$

$$\mathrm{M}^K_{Q_g} = c^4_*(\mathrm{M}^K_\sigma \times \mathrm{M}^K_{Q_f} \times \mathrm{M}^K_\pi \times \mathrm{M}^K_{P_g})$$

$$\mathrm{r}^K_{Q_g}(\langle z_{\sigma 1}, \mathrm{a}_{Q_f}(K), \mathrm{a}_\pi(K), \mathrm{a}_{P_g}(K)\rangle) = \mathrm{r}^K_\sigma(z_{\sigma 1}) + \mathrm{r}_{Q_f}(K) + \gamma(K)\,\mathrm{r}_\pi(K) + \mathrm{r}_{P_g}(K)$$

$$\begin{aligned} &Q^K_g(x, z_{\sigma 0} z_Q z_\pi z_g, \langle z_{\sigma 1}, \mathrm{a}_{Q_f}(K), \mathrm{a}_\pi(K), \mathrm{a}_{P_g}(K)\rangle) \\ &\qquad = Q^K_f(\sigma^K(x, z_\sigma), z_Q) - P^K_f(\sigma^K(x, z_\sigma), z_g z_\pi) + P^K_g(x, z_g) \end{aligned}$$

Applying Proposition 4.1 for P_g and Q_g, we get

$$\mathrm{E}_{\mathcal{E}^K \times \mathrm{U}^K_{P_g}}[(P^K_g - g)^2] \le \mathrm{E}_{\mathcal{E}^K \times \mathrm{UM}^K_{Q_g}}[(Q^K_g - g)^2] \pmod{\mathcal{F}}$$

Using condition i of Definition 4.2

$$\mathrm{E}_{\pi^K_* \mathcal{D}^K \times \mathrm{U}^K_{P_g}}[(P^K_g - \bar{g})^2] \le \mathrm{E}_{\pi^K_* \mathcal{D}^K \times \mathrm{UM}^K_{Q_g}}[(Q^K_g - \bar{g})^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\pi^K_* \mathcal{D}^K \times \mathrm{U}^K_{P_g}}[(P^K_g - \bar{g})^2] \le \mathrm{E}_{\pi^K_* \mathcal{D}^K \times \mathrm{UM}^K_{Q_g}}[((Q_f \circ \sigma)^K - (P_f \circ \sigma)^K + P^K_g - \bar{g})^2] \pmod{\mathcal{F}}$$

The right hand side has the form of the right hand side in 3.25 enabling us to apply Proposition 3.10 and get

$$\begin{aligned} &\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_\pi \times \mathrm{U}^K_{P_g}}[((P_g \circ \pi)^K - \bar{g} \circ \pi^K)^2] \\ &\qquad \le \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_\pi \times \mathrm{U}^K_{Q_f} \times \mathrm{U}^K_{P_f}}[(Q^K_f - P^K_f + (P_g \circ \pi)^K - \bar{g} \circ \pi^K)^2] \pmod{\mathcal{F}} \end{aligned}$$

We can consider the expressions within the expected values on both sides as random variables w.r.t. U_π^K while fixing the other components of the distribution. This allows us applying Proposition 4.4 to the difference between the right hand side and the left hand side (with the terms that don't depend on U_π^K playing the role of the constants), which results in moving the expected value over U_π^K inside the squares. Let $\mathrm{U}_{PQ}^K := \mathrm{U}_{Q_f}^K \times \mathrm{U}_{P_f}^K$.

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{P_g}^K}[\mathrm{E}_{\mathrm{U}_\pi^K}[(P_g \circ \pi)^K - \bar{g} \circ \pi^K]^2]$$
$$\leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{PQ}^K}[(Q_f^K - P_f^K + \mathrm{E}_{\mathrm{U}_\pi^K}[(P_g \circ \pi)^K - \bar{g} \circ \pi^K])^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{P_g}^K}[(\mathrm{E}_{\mathrm{U}_\pi^K}[(P_g \circ \pi)^K] - \mathrm{E}_{\mathrm{U}_\pi^K}[\bar{g} \circ \pi^K])^2]$$
$$\leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{PQ}^K}[(Q_f^K - P_f^K + \mathrm{E}_{\mathrm{U}_\pi^K}[(P_g \circ \pi)^K] - \mathrm{E}_{\mathrm{U}_\pi^K}[\bar{g} \circ \pi^K])^2] \pmod{\mathcal{F}}$$

We now apply Proposition 4.2 via condition ii of Definition 4.2

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{P_g}^K}[(\mathrm{E}_{\mathrm{U}_\pi^K}[(P_g \circ \pi)^K] - f)^2]$$
$$\leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{PQ}^K}[(Q_f^K - P_f^K + \mathrm{E}_{\mathrm{U}_\pi^K}[(P_g \circ \pi)^K] - f)^2] \pmod{\mathcal{F}}$$

Denote $y_i := \pi^K(x, z_i)$ where the z_i are sampled independently from U_π^K. Applying Proposition 4.2 via Proposition 4.3 and the assumption on γ, we get

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{P_f}^K}\left[\left(\frac{1}{\gamma(K)} \sum_{i \in [\gamma(K)]} P_g^K(y_i) - f\right)^2\right]$$
$$\leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{PQ}^K}\left[\left(Q_f^K - P_f^K + \frac{1}{\gamma(K)} \sum_{i \in [\gamma(K)]} P_g^K(y_i) - f\right)^2\right] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{P_f}^K}[(P_f^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{PQ}^K}[(Q_f^K - P_f^K + P_f^K - f)^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{P_f}^K}[(P_f^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_{Q_f}^K}[(Q_f^K - f)^2] \pmod{\mathcal{F}}$$

□

4.2 Dominance

Next, we consider a scenario in which the identity mapping can be regarded as a valid reduction between distributional estimation problems that have the same function but different word ensembles.

Definition 4.3. Consider $\mathcal{D}$, $\mathcal{E}$ word ensembles. $\mathcal{D}$ is said to be $\mathcal{F}(\Gamma)$-*dominated by* $\mathcal{E}$ when there is $W : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}^{\geq 0}$ bounded s.t.

$$\sum_{x \in \{0,1\}^*} |\mathcal{E}^K(x) \operatorname{E}_{\mathrm{U}_W^K}[W^K(x)] - \mathcal{D}^K(x)| \in \mathcal{F} \tag{4.9}$$

In this case, W is called a *Radon-Nikodym* $\mathcal{F}(\Gamma)$-*derivative of* $\mathcal{D}$ *w.r.t.* $\mathcal{E}$.

Proposition 4.5. *Consider* $\mathcal{D}$, $\mathcal{E}$ *word ensembles,* $f : \operatorname{supp}\mathcal{D} \cup \operatorname{supp}\mathcal{E} \to \mathbb{R}$ *bounded and* P *an* $\mathcal{F}^\sharp(\Gamma)$-*optimal estimator for* $(\mathcal{E}, f)$*. Suppose* $\mathcal{D}$ *is* $\mathcal{F}(\Gamma)$-*dominated by* $\mathcal{E}$*. Then,* P *is an* $\mathcal{F}^\sharp(\Gamma)$-*optimal estimator for* $(\mathcal{D}, f)$*.*

Proof. Let W be a Radon-Nikodym $\mathcal{F}(\Gamma)$-derivative of $\mathcal{D}$ w.r.t. $\mathcal{E}$. Consider any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded.

$$\operatorname{E}_{\mathcal{E}^K \times \mathrm{U}_P^K \times \mathrm{U}_W^K \times \mathrm{U}_S^K}[(P^K(x) - f(x))W^K(x)S^K(x, P^K(x))] \equiv 0 \pmod{\mathcal{F}}$$

$$\sum_{x \in \{0,1\}^*} \mathcal{E}^K(x) \operatorname{E}_{\mathrm{U}_W^K}[W^K(x)] \operatorname{E}_{\mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K(x) - f(x))S^K(x, P^K(x))] \equiv 0 \pmod{\mathcal{F}}$$

$$\sum_{x \in \{0,1\}^*} (\mathcal{E}^K(x) \operatorname{E}_{\mathrm{U}_W^K}[W^K(x)] - \mathcal{D}^K(x) + \mathcal{D}^K(x)) \cdot \operatorname{E}_{\mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K(x) - f(x))S^K(x, P^K(x))] \equiv 0 \pmod{\mathcal{F}}$$

$$\sum_{x \in \{0,1\}^*} (\mathcal{E}^K(x) \operatorname{E}_{\mathrm{U}_W^K}[W^K(x)] - \mathcal{D}^K(x)) \operatorname{E}_{\mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K] + \sum_{x \in \{0,1\}^*} \mathcal{D}^K(x) \operatorname{E}_{\mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S] \equiv$$
$$- \sum_{x \in \{0,1\}^*} (\mathcal{E}^K(x)\, \mathrm{E}_{\mathrm{U}_W^K}[W^K(x)] - \mathcal{D}^K(x))\, \mathrm{E}_{\mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S^K] \pmod{\mathcal{F}}$$

$$|\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S]| \leq$$
$$(\sup|P| + \sup|f|) \sup|S| \sum_{x \in \{0,1\}^*} |\mathcal{E}^K(x)\, \mathrm{E}_{\mathrm{U}_W^K}[W^K(x)] - \mathcal{D}^K(x)| \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K - f)S] \equiv 0 \pmod{\mathcal{F}}$$

□

The corresponding statement for $\mathcal{F}(\Gamma)$-optimal estimators may be regarded as a generalization of Corollary 2.1.

Proposition 4.6. *Assume $\mathcal{F}$ is $\Gamma_{\mathfrak{A}}$-ample. Consider $\mathcal{D}$, $\mathcal{E}$ word ensembles, $f : \operatorname{supp}\mathcal{D} \cup \operatorname{supp}\mathcal{E} \to \mathbb{R}$ bounded and P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{E}, f)$. Suppose $\mathcal{D}$ is $\mathcal{F}(\Gamma)$-dominated by $\mathcal{E}$. Then, P is an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. Let W be a Radon-Nikodym $\mathcal{F}(\Gamma)$-derivative of $\mathcal{D}$ w.r.t. $\mathcal{E}$. Consider any $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. According to Proposition 2.12

$$\mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_W^K \times \mathrm{U}_P^K}[W^K(x)(P^K(x) - f(x))^2]$$
$$\leq \mathrm{E}_{\mathcal{E}^K \times \mathrm{U}_W^K \times \mathrm{U}_Q^K}[W^K(x)(Q^K(x) - f(x))^2] \pmod{\mathcal{F}}$$

$$\sum_{x \in \{0,1\}^*} \mathcal{E}^K(x)\, \mathrm{E}_{\mathrm{U}_W^K}[W^K(x)]\, \mathrm{E}_{\mathrm{U}_P^K}[(P^K(x) - f(x))^2]$$
$$\leq \sum_{x \in \{0,1\}^*} \mathcal{E}^K(x)\, \mathrm{E}_{\mathrm{U}_W^K}[W^K(x)]\, \mathrm{E}_{\mathrm{U}_Q^K}[(Q^K(x) - f(x))^2] \pmod{\mathcal{F}}$$

Using the assumption on W

$$\sum_{x\in\{0,1\}^*} \mathcal{D}^K(x)\,\mathrm{E}_{\mathrm{U}_P^K}[(P^K(x)-f(x))^2] \leq \sum_{x\in\{0,1\}^*} \mathcal{D}^K(x)\,\mathrm{E}_{\mathrm{U}_Q^K}[(Q^K(x)-f(x))^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\times\mathrm{U}_P^K}[(P^K(x)-f(x))^2] \leq \mathrm{E}_{\mathcal{D}^K\times\mathrm{U}_Q^K}[(Q^K(x)-f(x))^2] \pmod{\mathcal{F}}$$

□

4.3 Ensemble pullbacks

Finally, we consider another scenario in which the identity mapping is a valid reduction. This scenario is a simple re-indexing of the word ensemble (redefinition of the security parameters). For the remainder of section 4, we fix some $m \in \mathbb{N}$. Note that is important that the growth spaces for the resources and fall space for the error, after reindexing, lie in the growth spaces and fall space of the new problem.

Definition 4.4. We denote $\Gamma^{mn}_{\mathrm{poly}} := \{\gamma : \mathbb{N}^m \to \mathbb{N}^n \mid \forall i \in [n] : \gamma_i \in \Gamma^m_{\mathrm{poly}}\}$.

Definition 4.5. Consider Γ_* a growth space of rank n and $\alpha \in \Gamma^{mn}_{\mathrm{poly}}$. We introduce the notation

$$\Gamma_*\alpha := \{\gamma_\alpha : \mathbb{N}^m \to \mathbb{R}^{\geq 0} \mid \exists \gamma \in \Gamma_* : \gamma_\alpha \leq \gamma \circ \alpha\} \tag{4.10}$$

Obviously $\Gamma_*\alpha$ is a growth space of rank m.
We also denote $\Gamma\alpha := (\Gamma_{\mathfrak{R}}\alpha, \Gamma_{\mathfrak{A}}\alpha)$.

Definition 4.6. Consider $\alpha \in \Gamma^{mn}_{\mathrm{poly}}$. We introduce the notation

$$\mathcal{F}\alpha := \{\varepsilon_\alpha : \mathbb{N}^m \to \mathbb{R}^{\geq 0} \text{ bounded} \mid \exists \varepsilon \in \mathcal{F} : \varepsilon_\alpha \leq \varepsilon \circ \alpha\} \tag{4.11}$$

Proposition 4.7. *For any $\alpha \in \Gamma^{mn}_{\mathrm{poly}}$, $\mathcal{F}\alpha$ is a fall space.*

Proof. Conditions i and ii are obvious. To verify condition iii, consider $h \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $2^{-h} \in \mathcal{F}$. Note that since the coefficients of h are non-negative it is non-decreasing in all arguments. Consider $p : \mathbb{N}^m \to \mathbb{N}^n$ a polynomial map s.t. for any $i \in [n]$, $\alpha_i \leq p_i$. We have $2^{-h\circ p} \leq 2^{-h\circ\alpha}$ and therefore $2^{-h\circ p} \in \mathcal{F}\alpha$. □

Definition 4.7. Consider $\mathcal{D}$ a word ensemble of rank n and $\alpha : \mathbb{N}^m \to \mathbb{N}^n$. The *pull-back of $\mathcal{D}$ by α*, denoted $\mathcal{D}^\alpha$, is the word ensemble of rank m given by $(\mathcal{D}^\alpha)^k := \mathcal{D}^{\alpha(k)}$.

Definition 4.8. Consider X, Y encoded sets, $S : X \xrightarrow{\Gamma} Y$ and $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ s.t. $\alpha \in \Gamma^{mn}_{\text{poly}}$ as a function and $\mathrm{T}_\alpha \in \Gamma^m_{\text{poly}}$. We define $S^\alpha : X \xrightarrow{\Gamma\alpha} Y$ by requiring that for any $L \in \mathbb{N}^m$, $\mathrm{r}_{S^\alpha}(L) = \mathrm{r}_S(\alpha(L))$ and $(S^\alpha)^L(x, y) = S^{\alpha(L)}(x, y)$.

Proposition 4.8. *Consider X, Y encoded sets, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ and $\beta \in \Gamma^{nm}_{\text{poly}}$. Assume that $\mathrm{T}_\alpha \in \Gamma^m_{\text{poly}}$ and $\forall L \in \mathbb{N}^m : \beta(\alpha(L)) = L$. Then, for any $S : X \xrightarrow{\Gamma\alpha} Y$ there is $\tilde{S} : X \xrightarrow{\Gamma} Y$ s.t. for all $K \in \mathbb{N}^n$ that satisfy $\alpha(\beta(K)) = K$, $x \in X$ and $y, z \in \{0,1\}^*$*

$$\mathrm{a}_{\tilde{S}}(K) = \mathrm{a}_S(\beta(K)) \tag{4.12}$$

$$\mathrm{r}^K_{\tilde{S}}(z) = \mathrm{r}^{\beta(K)}_S(z) \tag{4.13}$$

$$\tilde{S}^K(x, y, z) = S^{\beta(K)}(x, y, z) \tag{4.14}$$

Proof. To see there is no obstruction of time complexity, note that β can be computed by some $\beta^* : \mathbb{N}^n \xrightarrow{\text{alg}} \mathbb{N}^m$ s.t. $\mathrm{T}_{\beta^*} \in \Gamma^n_{\text{poly}}$. Given input K, β^* works by iterating over all L within some polynomial size range (thanks to the assumption $\beta \in \Gamma^{nm}_{\text{poly}}$) and checking the condition $\alpha(L) = K$.

To see there are no obstructions of random or advice complexity, note there is $\gamma_{\mathfrak{R}} \in \Gamma_{\mathfrak{R}}$ s.t. $\mathrm{r}_S(L) \leq \gamma_{\mathfrak{R}}(\alpha(L))$ and $\gamma_{\mathfrak{A}} \in \Gamma_{\mathfrak{A}}$ s.t. $|\mathrm{a}_S(L)| \leq \gamma_{\mathfrak{A}}(\alpha(L))$. In particular, if $K \in \mathbb{N}^n$ is s.t. $\alpha(\beta(K)) = K$ then $\mathrm{r}_S(\beta(K)) \leq \gamma_{\mathfrak{R}}(K)$ and $|\mathrm{a}_S(\beta(K))| \leq \gamma_{\mathfrak{A}}(K)$. □

Definition 4.9. $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ is called an *efficient injection* when $\alpha \in \Gamma^{mn}_{\text{poly}}$ as a function, $\mathrm{T}_\alpha \in \Gamma^m_{\text{poly}}$ and there is $\beta \in \Gamma^{nm}_{\text{poly}}$ s.t. $\forall L \in \mathbb{N}^m : \beta(\alpha(L)) = L$.

Proposition 4.9. *Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank n, P an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$ and $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection. Then, P^α is an $\mathcal{F}\alpha^\sharp(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}^\alpha, f)$.*

Proof. Consider any $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma\alpha} \mathbb{Q}$ bounded. Construct $\tilde{S} : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ by applying Proposition 4.8 to S. There is $\varepsilon \in \mathcal{F}$ s.t. for any $K \in \mathbb{N}^n$

$$|\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}^K_P \times \mathrm{U}^K_{\tilde{S}}}[(P^K(x, y) - f(x))\tilde{S}^K(x, P^K(x, y), z)]| = \varepsilon(K)$$

Substituting $\alpha(L)$ for K, we get

$$|\mathrm{E}_{\mathcal{D}^{\alpha(L)}\times \mathrm{U}_P^{\alpha(L)}\times \mathrm{U}_{\tilde{S}}^{\alpha(L)}}[(P^{\alpha(L)}(x,y)-f(x))\tilde{S}^{\alpha(L)}(x,P^{\alpha(L)}(x,y),z)]|=\varepsilon(\alpha(L))$$

$$|\mathrm{E}_{(\mathcal{D}^{\alpha})^L\times \mathrm{U}_{P^\alpha}^{L}\times \mathrm{U}_{\tilde{S}}^{\alpha(L)}}[((P^{\alpha})^L(x,y)-f(x))\tilde{S}^{\alpha(L)}(x,(P^{\alpha})^L(x,y),z)]|=\varepsilon(\alpha(L))$$

We have $\alpha(\beta(\alpha(L))=\alpha(L)$, therefore

$$|\mathrm{E}_{(\mathcal{D}^{\alpha})^L\times \mathrm{U}_{P^\alpha}^{L}\times \mathrm{U}_{S}^{\beta(\alpha(L))}}[((P^{\alpha})^L(x,y)-f(x))S^{\beta(\alpha(L))}(x,(P^{\alpha})^L(x,y),z)]|=\varepsilon(\alpha(L))$$

$$|\mathrm{E}_{(\mathcal{D}^{\alpha})^L\times \mathrm{U}_{P^\alpha}^{L}\times \mathrm{U}_{S}^{L}}[((P^{\alpha})^L(x,y)-f(x))S^{L}(x,(P^{\alpha})^L(x,y),z)]|=\varepsilon(\alpha(L))$$

□

Proposition 4.10. *Consider $(\mathcal{D},f)$ a distributional estimation problem of rank n, P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D},f)$ and $\alpha:\mathbb{N}^m\xrightarrow{\text{alg}}\mathbb{N}^n$ an efficient injection. Then, P^α is an $\mathcal{F}\alpha(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}^\alpha,f)$.*

Proof. Consider any $Q:\{0,1\}^*\xrightarrow{\Gamma\alpha}\mathbb{Q}$ bounded. Construct $\tilde{Q}:\{0,1\}^*\xrightarrow{\Gamma}\mathbb{Q}$ by applying Proposition 4.8 to Q. There is $\varepsilon\in\mathcal{F}$ s.t.

$$\mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_P^K}[(P^K(x,y)-f(x))^2]\leq \mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_{\tilde{Q}}^K}[(\tilde{Q}^K(x,y)-f(x))^2]+\varepsilon(K)$$

Substituting $\alpha(L)$ for K, we get

$$\mathrm{E}_{\mathcal{D}^{\alpha(L)}\times \mathrm{U}_P^{\alpha(L)}}[(P^{\alpha(L)}(x,y)-f(x))^2]\leq \mathrm{E}_{\mathcal{D}^{\alpha(L)}\times \mathrm{U}_{\tilde{Q}}^{\alpha(L)}}[(\tilde{Q}^{\alpha(L)}(x,y)-f(x))^2]+\varepsilon(\alpha(L))$$

$$\mathrm{E}_{(\mathcal{D}^{\alpha})^L\times \mathrm{U}_{P^\alpha}^{L}}[((P^{\alpha})^L(x,y)-f(x))^2]\leq \mathrm{E}_{(\mathcal{D}^{\alpha})^L\times \mathrm{U}_{\tilde{Q}}^{\alpha(L)}}[(\tilde{Q}^{\alpha(L)}(x,y)-f(x))^2]+\varepsilon(\alpha(L))$$

We have $\alpha(\beta(\alpha(L))=\alpha(L)$, therefore

$$\mathrm{E}_{(\mathcal{D}^\alpha)^L \times \mathrm{U}_{P^\alpha}^L}[((P^\alpha)^L(x,y) - f(x))^2] \leq \mathrm{E}_{(\mathcal{D}^\alpha)^L \times \mathrm{U}_Q^{\beta(\alpha(L))}}[(Q^{\beta(\alpha(L))}(x,y) - f(x))^2] + \varepsilon(\alpha(L))$$

$$\mathrm{E}_{(\mathcal{D}^\alpha)^L \times \mathrm{U}_{P^\alpha}^L}[((P^\alpha)^L(x,y) - f(x))^2] \leq \mathrm{E}_{(\mathcal{D}^\alpha)^L \times \mathrm{U}_Q^L}[(Q^L(x,y) - f(x))^2] + \varepsilon(\alpha(L))$$

□

4.4 Lax pseudo-invertible reductions

We now consider compositions of reductions of different types. For the remainder of the section, we fix $\mathcal{G}$, a fall space of rank m.

Definition 4.10. Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank m, $(\mathcal{E}, g)$ a distributional estimation problem of rank n, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection and $\pi : \{0,1\}^* \xrightarrow{\Gamma\alpha} \{0,1\}^*$. π is called a *precise pseudo-invertible $\mathcal{G}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ over α* when

(i) $\pi_*\mathcal{D}$ is $\mathcal{G}(\Gamma\alpha)$-dominated by $\mathcal{E}^\alpha$.

(ii) Denote $\bar{g} : \{0,1\}^* \to \mathbb{R}$ the extension of g by 0. We require

$$\mathrm{E}_{(x,z)\sim\mathcal{D}^K \times \mathrm{U}_\pi^K}[|f(x) - \bar{g}(\pi^K(x,z))|] \equiv 0 \pmod{\mathcal{G}}$$

(iii) $\mathcal{D}$ is $\mathcal{G}(\mathrm{M}\Gamma\alpha)$-samplable relative to π.

Corollary 4.2. *Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank m, $(\mathcal{E}, g)$ distributional estimation problem of rank n, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection and π a precise pseudo-invertible $\mathcal{G}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ over α. Assume $\mathcal{F}\alpha \subseteq \mathcal{G}$. Suppose P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$. Then, $P^\alpha \circ \pi$ is a $\mathcal{G}^\sharp(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. By Proposition 4.9, P^α is an $\mathcal{F}\alpha^\sharp(\Gamma\alpha)$-optimal estimator (and in particular a $\mathcal{G}^\sharp(\Gamma\alpha)$-optimal estimator) for $(\mathcal{E}^\alpha, g)$. By Proposition 4.5 and condition i of Definition 4.10, P^α is also a $\mathcal{G}^\sharp(\Gamma\alpha)$-optimal estimator for $(\pi_*\mathcal{D}, g)$. By Corollary 4.1 and conditions ii and iii of Definition 4.10, $P^\alpha \circ \pi$ is a $\mathcal{G}^\sharp(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}, f)$. □

Corollary 4.3. *Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank m, $(\mathcal{E}, g)$ distributional estimation problem of rank n, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection and π a precise pseudo-invertible $\mathcal{G}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ over α. Assume $\mathcal{F}\alpha \subseteq \mathcal{G}$ and $\mathcal{G}$ is $\Gamma_{\mathfrak{A}}\alpha$-ample. Suppose P is an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$. Then, $P^\alpha \circ \pi$ is a $\mathcal{G}(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}, f)$.*

Proof. Completely analogous to proof of Corollary 4.2. □

Definition 4.11. Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank m, $(\mathcal{E}, g)$ a distributional estimation problem of rank n, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection and $\pi : \{0,1\}^* \xrightarrow{\Gamma\alpha} \{0,1\}^*$. π is called a *pseudo-invertible $\mathcal{G}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ over α* when

(i) $\pi_*\mathcal{D}$ is $\mathcal{G}(\Gamma\alpha)$-dominated by $\mathcal{E}^\alpha$.

(ii) Denote $\bar{g} : \{0,1\}^* \to \mathbb{R}$ the extension of g by 0. We require

$$\mathrm{E}_{(x,z)\sim\mathcal{D}^K}[|f(x) - \mathrm{E}_{\mathrm{U}_\pi^K}[g(\pi^K(x,z))]|] \equiv 0 \pmod{\mathcal{G}}$$

(iii) $\mathcal{D}$ is $\mathcal{G}(\mathrm{M}\Gamma\alpha)$-samplable relative to π.

The following corollaries are completely analogous to Corollary 4.2 and therefore given without proof. We also drop the explicit constructions of the optimal polynomial-time estimators which are obviously modeled on Theorem 4.2 and Theorem 4.3.

Corollary 4.4. *Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank m, $(\mathcal{E}, g)$ distributional estimation problem of rank n, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection and π a pseudo-invertible $\mathcal{G}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ over α. Assume $\mathcal{F}\alpha \subseteq \mathcal{G}$. Suppose there exist P an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$ and $\gamma \in \Gamma^m_{\text{poly}}$ s.t. $\gamma^{-\frac{1}{2}} \in \mathcal{G}$ and $\gamma(\mathrm{r}_P \circ \alpha + \mathrm{r}_\pi) \in \Gamma_{\mathfrak{R}}\alpha$. Then, there exists a $\mathcal{G}^\sharp(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}, f)$.*

Corollary 4.5. *Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank m, $(\mathcal{E}, g)$ distributional estimation problem of rank n, $\alpha : \mathbb{N}^m \xrightarrow{\text{alg}} \mathbb{N}^n$ an efficient injection and π a pseudo-invertible $\mathcal{G}(\Gamma)$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{E}, g)$ over α. Assume $\mathcal{F}\alpha \subseteq \mathcal{G}$ and $\mathcal{G}$ is $\Gamma_{\mathfrak{A}}\alpha$-ample. Suppose there exist P an $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{E}, g)$ and $\gamma \in \Gamma^m_{\text{poly}}$ s.t. $\gamma^{-\frac{1}{2}} \in \mathcal{G}$ and $\mathrm{r}_P \circ \alpha + \gamma\,\mathrm{r}_\pi \in \Gamma_{\mathfrak{R}}\alpha$. Then, there exists a $\mathcal{G}(\Gamma\alpha)$-optimal estimator for $(\mathcal{D}, f)$.*

Note that the last results involved passing from fall space $\mathcal{F}$ and growth spaces

Γ to fall space $\mathcal{G}$ and growth spaces $\Gamma\alpha$, however in many natural examples $m = n$, $\mathcal{G} = \mathcal{F}$ and $\Gamma\alpha = \Gamma$. In particular, the following propositions are often applicable.

Proposition 4.11. *Assume Γ_* is a growth space of rank n s.t. for any $\gamma \in \Gamma_*$ and $\alpha \in \Gamma^{nn}_{\mathrm{poly}}$, $\gamma \circ \alpha \in \Gamma_*$. Let $\alpha^*, \beta^* \in \Gamma^{nn}_{\mathrm{poly}}$ be s.t. $\beta^*(\alpha^*(K)) = K$. Then, $\Gamma_*\alpha^* = \Gamma_*$.*

Proof. For any $\gamma_\alpha \in \Gamma_*\alpha^*$ there is $\gamma \in \Gamma_*$ s.t. $\gamma_\alpha \leq \gamma \circ \alpha \in \Gamma_*$. Conversely, for any $\gamma \in \Gamma_*$ we have $\gamma = \gamma \circ \beta \circ \alpha \in \Gamma_*\alpha^*$. □

Proposition 4.12. *Consider $r : \mathbb{N}^n \to \mathbb{N}$ steadily growing and $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ increasing in the last argument. Define $\alpha_p : \mathbb{N}^n \to \mathbb{N}$ by $\forall J \in \mathbb{N}^{n-1}, k \in \mathbb{N} : \alpha_p(J, k) = (J, p(J, k))$. Then, $\Gamma_r\alpha_p = \Gamma_r$.*

Proof. Consider $\gamma_\alpha \in \Gamma_r\alpha_p$. There is $\gamma \in \Gamma_r$ s.t. $\gamma_\alpha \leq \gamma \circ \alpha_p$. There is $q \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $\gamma(J, k) \leq r(J, q(J, k))$. We get $\gamma_\alpha(J, k) \leq \gamma(J, p(J, k)) \leq r(J, q(J, p(J, k)))$ and therefore $\gamma_\alpha \in \Gamma_r$. Conversely, consider $\gamma' \in \Gamma_r$. There is $q' \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s..t $\gamma'(J, k) \leq r(J, q'(J, k))$. $p(J, k) \geq k$ and r is non-decreasing in the last argument, implying that $r \leq r \circ \alpha_p$. We conclude that $\gamma'(J, k) \leq r(J, p(J, q'(J, k)))$ and therefore $\gamma' \in \Gamma_r\alpha_p$. □

4.5 Completeness

Fix $r, s : \mathbb{N}^n \xrightarrow{\text{alg}} \mathbb{N}$ s.t.

(i) $\mathrm{T}_r, \mathrm{T}_s \in \Gamma^n_{\mathrm{poly}}$

(ii) r and s are steadily growing.

(iii) $\forall K \in \mathbb{N}^n : 1 \leq r(K) \leq s(K)$

Denote $\Gamma_{\mathrm{det}} := (\Gamma^n_0, \Gamma^n_0)$, $\Gamma_{\mathrm{red}} := (\Gamma_r, \Gamma^n_0)$, $\Gamma_{\mathrm{smp}} := (\Gamma_s, \Gamma^n_0)$.

We will show that certain classes of functions paired with $\mathcal{F}(\Gamma_{\mathrm{smp}})$-samplable word ensembles have a distributional estimation problem which is complete w.r.t. precise pseudo-invertible $\mathcal{F}(\Gamma_{\mathrm{red}})$-reductions. This construction is an adaption of the standard construction of a complete problem for SampNP, as provided in Theorem 10.25 of [12].

Due to the large number of variables and functions in the following theorem, some intuitive exposition of the result seems helpful. A universal function $\mathfrak{F}$ will be considered, which takes three inputs. There is an element ϕ of some encoded set E that tells $\mathfrak{F}$ which (possibly hard-to-compute) function f to emulate, a time parameter k which controls the computational resources used in emulating f, and a

bit string x which is just the input to f. When k is sufficiently large, and b is chosen appropriately, $\mathfrak{F}(b,k,x) = f(x)$. The distribution $\mathcal{D}_{\mathfrak{F}}$ is over 4-element tuples of a bit string (which dictates what f is), the last coordinate of K (k), which serves as a time parameter, a bit string a (which can be interpreted as a sampler), and a bit string x (which is the output of the sampler when run for k steps.

For samplable distributions $\mathcal{D}$, and functions f which have a corresponding b that makes $\mathfrak{F}$ emulate them, there is a reduction to this universal problem. Observe that if $\mathcal{D}$ is samplable, there is some bit string a which encodes a turing machine that samples from $\mathcal{D}$. The reduction maps x to the tuple $(b, p(K), a, x)$, and then reindexes. (In particular, to ensure that the time parameter is large enough to fully run the sampler.)

Theorem 4.4. *Consider an encoded set E which is prefix-free, i.e. for all $\phi, \psi \in E$ and $z \in \{0,1\}^{>0}$, $\mathrm{c}_E(\phi) \neq \mathrm{c}_E(\psi)z$. Consider $\mathfrak{F} : E \times \mathbb{N} \times \{0,1\}^* \to \mathbb{R}$ bounded. For any $K \in \mathbb{N}^n$, define $\zeta^K : \{0,1\}^{*^2} \to \{0,1\}^{*^2}$ by*

$$\zeta^K(a,w) = (a, \mathrm{ev}^{K_{n-1}}(a; \mathrm{c}_{\mathbb{N}^n}(K), w)) \tag{4.15}$$

Define the distributional estimation problem $(\mathcal{D}_{\mathfrak{F}}, f_{\mathfrak{F}})$ by

$$\mathcal{D}_{\mathfrak{F}}^K := \mathrm{c}_*^4(\mathrm{U}^{r(K)} \times \mathrm{c}_{\mathbb{N}*}\, \delta_{K_{n-1}} \times \zeta_*^k(\mathrm{U}^{r(K)} \times \mathrm{U}^{s(K)})) \tag{4.16}$$

$$f_{\mathfrak{F}}(\langle b, \mathrm{c}_{\mathbb{N}}(k), a, x\rangle) := \begin{cases} \mathfrak{F}(\phi, k, x) \text{ if } \exists z \in \{0,1\}^* : b = \mathrm{c}_E(\phi)z \\ 0 \text{ if } \forall \phi \in E, z \in \{0,1\}^* : b \neq \mathrm{c}_E(\phi)z \end{cases} \tag{4.17}$$

For any $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$, define $\alpha_p : \mathbb{N}^n \to \mathbb{N}^n$ by

$$\forall J \in \mathbb{N}^{n-1}, k \in \mathbb{N} : \alpha_p(J,k) = (J, p(J,k)) \tag{4.18}$$

Consider a distributional estimation problem $(\mathcal{D}, f)$ s.t. $\mathcal{D}$ is $\mathcal{F}(\Gamma_{\mathrm{smp}})$-samplable and there are $\phi \in E$ and $q \in \mathbb{N}[k]$ s.t. for any $x \in \operatorname{supp} \mathcal{D}$ and $k \geq q(|x|)$, $f(x) = \mathfrak{F}(\phi, k, x)$. Then, there is a precise pseudo-invertible $\mathcal{F}(\Gamma_{\mathrm{red}})$-reduction from $(\mathcal{D}, f)$ to $(\mathcal{D}_{\mathfrak{F}}, f_{\mathfrak{F}})$ over α_p for some $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ increasing in the last argument (it is easy to see that any such α_p is an efficient injection).

Proof. Let σ be an $\mathcal{F}(\Gamma_{\mathrm{smp}})$-sampler of $\mathcal{D}$. Denote $b = \mathrm{c}_E(\phi)$. Choose $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ increasing in the last argument and $a \in \{0,1\}^*$ s.t. for any $K \in \mathbb{N}^n$, $z \in \{0,1\}^*$, $w_1 \in \{0,1\}^{\mathrm{r}_\sigma(K)}$ and $w_2 \in \{0,1\}^*$: $p(K) \geq q(\max_{x \in \operatorname{supp} \sigma_\bullet^K} |x|)$, $r(\alpha_p(K)) \geq |b|$, $r(\alpha_p(K)) \geq |a|$, $s(\alpha_p(K)) \geq \mathrm{r}_\sigma(K)$ and

$$\mathrm{ev}^{p(K)}(az; \mathrm{c}_{\mathbb{N}^n}(\alpha_p(K)), w_1 w_2) = \sigma^K(w_1)$$

The latter is possible because α_p can be efficiently inverted using binary search over K_{n-1}.

Denote $r_p := r \circ \alpha_p$. Note that $\Gamma_{\mathrm{red}} \alpha_p = \Gamma_{\mathrm{red}}$ by Proposition 4.12. We construct $\pi : \{0,1\}^* \xrightarrow{\Gamma_{\mathrm{red}}} \{0,1\}^*$ s.t. for any $K \in \mathbb{N}^n$, $x \in \operatorname{supp} \sigma_\bullet^K$, $z_b \in \{0,1\}^{r_p(K)-|b|}$ and $z_a \in \{0,1\}^{r_p(K)-|a|}$

$$\mathrm{r}_\pi(K) = 2r_p(K) - |a| - |b| \tag{4.19}$$

$$\pi^K(x, z_b z_a) = \langle b z_b, \mathrm{c}_{\mathbb{N}}(p(K)), a z_a, x \rangle \tag{4.20}$$

We also ensure that for any $K \in \mathbb{N}^n$, $x \in \{0,1\}^*$ and z_b, z_a as above, either 4.20 holds or

$$\pi^K(x, z_b z_a) = \boldsymbol{\lambda}$$

To verify condition i of Definition 4.10 (with α_p playing the role of the efficient injection), fix $h \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $h \geq r_p$ and $\operatorname{supp} \sigma_\bullet^K \subseteq \{0,1\}^{h(K)}$. Construct $W : \{0,1\}^* \xrightarrow{\Gamma_{\mathrm{det}}} \mathbb{Q}^{\geq 0}$ s.t.

$$W^K(y) = \begin{cases} 2^{|a|+|b|} \text{ if } \exists z_b, z_a, x \in \{0,1\}^{\leq h(K)} : y = \langle b z_b, \mathrm{c}_{\mathbb{N}}(p(K)), a z_a, x \rangle \\ 0 \text{ otherwise} \end{cases}$$

$\mathcal{D}^K \equiv \sigma_\bullet^K \pmod{\mathcal{F}}$ since σ is an $\mathcal{F}(\Gamma_{\mathrm{smp}})$-sampler of $\mathcal{D}$. By Proposition 3.6

$$\pi_*^K \mathcal{D}^K \equiv \pi_*^K \sigma_\bullet^K \pmod{\mathcal{F}}$$

It follows that

$$\sum_{y \in \{0,1\}^*} |\mathcal{D}_{\mathfrak{F}}^{\alpha_p(K)}(y) W^K(y) - (\pi_*^K \mathcal{D}^K)(y)| \equiv \sum_{y \in \{0,1\}^*} |\mathcal{D}_{\mathfrak{F}}^{\alpha_p(K)}(y) W^K(y) - (\pi_*^K \sigma_\bullet^K)(y)| \pmod{\mathcal{F}}$$

For any $y \in \{0,1\}^*$, if $W^K(y) = 0$ then $(\pi_*^K \sigma_\bullet^K)(y) = 0$, so the corresponding terms contribute nothing to the sum on the right hand side. Denote $\bar{\pi}^K(x, z_b, z_a) := \langle b z_b, \mathrm{c}_{\mathbb{N}}(p(K)), a z_a, x \rangle$.

$$\sum_{\{0,1\}^*} |\mathcal{D}_{\mathfrak{F}}^{\alpha_p(K)} W^K - \pi_*^K \mathcal{D}^K| \equiv$$

$$\sum_{\substack{z_b\in\{0,1\}^{\le h(K)}\\ z_a\in\{0,1\}^{\le h(K)}\\ x\in\{0,1\}^{\le h(K)}}} |\mathcal{D}_{\mathfrak{F}}^{\alpha_p(K)}(\bar\pi^K(x,z_b,z_a))2^{|a|+|b|} - (\pi_*^K\sigma_\bullet^K)(\bar\pi^K(x,z_b,z_a))| \equiv$$

$$\sum_{\substack{z_b\in\{0,1\}^{r_p(K)-|b|}\\ z_a\in\{0,1\}^{r_p(K)-|a|}\\ x\in\{0,1\}^{\le h(K)}}} |2^{-r_p(K)}2^{-r_p(K)}\sigma_\bullet^K(x)2^{|a|+|b|} - (\pi_*^K\sigma_\bullet^K)(\bar\pi^K(x,z_b,z_a))| \equiv$$

$$\sum_{\substack{z_1\in\{0,1\}^{r_p(K)-|a|}\\ z_2\in\{0,1\}^{r_p(K)-|b|}\\ x\in\{0,1\}^{\le h(K)}}} |2^{-2r_p(K)+|a|+|b|}\sigma_\bullet^K(x) - (\pi_*^K\sigma_\bullet^K)(\bar\pi^K(x,z_b,z_a))| \equiv$$

$$\sum_{\substack{z_1\in\{0,1\}^{r_p(K)-|a|}\\ z_2\in\{0,1\}^{r_p(K)-|b|}\\ x\in\{0,1\}^{\le h(K)}}} |2^{-2r_p(K)+|a|+|b|}\sigma_\bullet^K(x) - 2^{-(r_p(K)-|a|)}2^{-(r_p(K)-|b|)}\sigma_\bullet^K(x)| \equiv$$

$$0 \pmod{\mathcal{F}}$$

To verify condition ii of Definition 4.10, use Proposition 3.4 to get

$$\mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_\pi^K}[|f(x) - f_{\mathfrak{F}}(\pi^K(x,z))|] \equiv \mathrm{E}_{\sigma_\bullet^K\times \mathrm{U}_\pi^K}[|f(x) - f_{\mathfrak{F}}(\pi^K(x,z))|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_\pi^K}[|f(x) - f_{\mathfrak{F}}(\pi^K(x,z))|] \equiv \mathrm{E}_{\sigma_\bullet^K\times \mathrm{U}_\pi^K}[|f(x) - f_{\mathfrak{F}}(\langle bz_b, \mathrm{c}_{\mathbb{N}}(p(K)), az_a, x\rangle)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_\pi^K}[|f(x) - f_{\mathfrak{F}}(\pi^K(x,z))|] \equiv \mathrm{E}_{\sigma_\bullet^K\times \mathrm{U}_\pi^K}[|\mathfrak{F}(\phi,p(K),x) - \mathfrak{F}(\phi,p(K),x)|] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K\times \mathrm{U}_\pi^K}[|f(x) - f_{\mathfrak{F}}(\pi^K(x,z))|] \equiv 0 \pmod{\mathcal{F}}$$

To verify condition iii of Definition 4.10, construct $\tau : \{0,1\}^* \xrightarrow{\Gamma_{\det}} \{0,1\}^*$ s.t. for any $z_1, z_2 \in \{0,1\}^{r_p(K)}$ and $x \in \operatorname{supp}\sigma_\bullet^K$, $\tau^K(\langle z_1, \mathrm{c}_{\mathbb{N}}(p(K)), z_2, x\rangle) = x$. By Proposition 3.6 and Proposition 3.4

$$\mathrm{E}_{y\sim\pi_*^K\mathcal{D}^K}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(y), \tau_y^K)]$$
$$\equiv \mathrm{E}_{y\sim\pi_*^K\sigma_\bullet^K}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(y), \tau_y^K)] \pmod{\mathcal{F}}$$

Denoting $\mathrm{U}_{ba}^K := \mathrm{U}^{r_p(K)-|b|} \times \mathrm{U}^{r_p(K)-|a|}$

$$\mathrm{E}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(y), \tau_y^K)]$$
$$\equiv \mathrm{E}_{(z_b,z_a,x)\sim\mathrm{U}_{ba}^K\times\sigma_\bullet^K}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(\bar{\pi}^K(x,z_b,z_a)), \tau^K_{\bar{\pi}^K(x,z_b,z_a)})] \pmod{\mathcal{F}}$$

$$\mathrm{E}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(y), \tau_y^K)] \equiv \mathrm{E}_{(z_b,z_a,x)\sim\mathrm{U}_{ba}^K\times\sigma_\bullet^K}[\mathrm{d_{tv}}(\delta_x, \delta_x)] \pmod{\mathcal{F}}$$

$$\mathrm{E}[\mathrm{d_{tv}}(\mathcal{D}^K \mid (\pi^K)^{-1}(y), \tau_y^K)] \equiv 0 \pmod{\mathcal{F}}$$

□

Denote $\mathrm{X}_{\mathfrak{F}}$ the set of bounded functions $f : D \to \mathbb{R}$ (where $D \subseteq \{0,1\}^*$) satisfying the conditions of Theorem 4.4, and $\mathrm{SAMPX}_{\mathfrak{F}}[\mathcal{F}(\Gamma_{\mathrm{smp}})]$ the set of distributional estimation problems of the form $(\mathcal{D}, f)$ for $\mathcal{F}(\Gamma_{\mathrm{smp}})$-samplable $\mathcal{D}$ and $f \in \mathrm{X}_{\mathfrak{F}}$. Obviously $\mathcal{D}_{\mathfrak{F}}$ is $\mathcal{F}(\Gamma_{\mathrm{smp}})$-samplable. Therefore, if $f_{\mathfrak{F}} \in \mathrm{X}_{\mathfrak{F}}$ then $(\mathcal{D}_{\mathfrak{F}}, f_{\mathfrak{F}})$ is complete for $\mathrm{SAMPX}_{\mathfrak{F}}[\mathcal{F}(\Gamma_{\mathrm{smp}})]$ w.r.t. precise pseudo-invertible $\mathcal{F}(\Gamma_{\mathrm{red}})$-reductions over efficient injections of the form α_p.

Example 4.1. $n = 1$. $E_{\mathrm{NP}} \subseteq \{0,1\}^*$ is the set of valid programs for the universal machine $\mathcal{U}_2$. $\mathfrak{F}_{\mathrm{NP}}$ is given by

$$\mathfrak{F}_{\mathrm{NP}}(\phi, k, x) := \begin{cases} 1 \text{ if } \exists y \in \{0,1\}^k : \mathrm{ev}^k(\phi; x, y) = 1 \\ 0 \text{ otherwise} \end{cases} \tag{4.21}$$

Example 4.2. $n = 1$. $E_{\mathrm{EXP}} \subseteq \{0,1\}^*$ is the set of valid programs for the universal machine $\mathcal{U}_1$. $\mathfrak{F}_{\mathrm{EXP}}$ is given by

$$\mathfrak{F}_{\mathrm{EXP}}(\phi, k, x) := \begin{cases} 1 \text{ if } \mathrm{ev}^{2^k}(\phi; x) = 1 \\ 0 \text{ otherwise} \end{cases} \tag{4.22}$$

This completeness property implies that, under certain assumptions, optimal polynomial-time estimators exist for all problems in $\mathrm{SAMPX}_{\mathfrak{F}}[\mathcal{F}(\Gamma_{\mathrm{smp}})]$ if an optimal

polynomial-time estimator exists for $(\mathcal{D}_{\mathfrak{F}}, f_{\mathfrak{F}})$. More precisely and slightly more generally, we have the following corollaries. For the remainder of the section, fix $m \in \mathbb{N}$ s.t. $m \geq n$. For any $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$, define $\beta_p : \mathbb{N}^m \to \mathbb{N}^m$ by

$$\forall J \in \mathbb{N}^{n-1}, k \in \mathbb{N}, L \in \mathbb{N}^{m-n} : \beta_p(J, k, L) = (J, p(J, k), L) \tag{4.23}$$

Define $\eta : \mathbb{N}^m \to \mathbb{N}^n$ by

$$\forall K \in \mathbb{N}^n, L \in \mathbb{N}^{m-n} : \eta(K, L) = K \tag{4.24}$$

Corollary 4.6. *Fix $\mathcal{F}^{(m)}$ a fall space of rank m and $\Gamma^m = (\Gamma^m_{\mathfrak{R}}, \Gamma^m_{\mathfrak{A}})$ growth spaces of rank m. Assume that $\mathcal{F}\eta \subseteq \mathcal{F}^{(m)}$, $\Gamma_r\eta \subseteq \Gamma^m_{\mathfrak{R}}$ and for any $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ increasing in the last argument, $\mathcal{F}^{(m)}\beta_p \subseteq \mathcal{F}^{(m)}$, $\Gamma^m_{\mathfrak{R}}\beta_p = \Gamma^m_{\mathfrak{R}}$ and $\Gamma^m_{\mathfrak{A}}\beta_p = \Gamma^m_{\mathfrak{A}}$. In the setting of Theorem 4.4, assume there is an $\mathcal{F}^{(m)\sharp}(\Gamma^m)$-optimal estimator for $(\mathcal{D}^{\eta}_{\mathfrak{F}}, f_{\mathfrak{F}})$. Then, for any $(\mathcal{D}, f) \in \textsc{SampX}_{\mathfrak{F}}[\mathcal{F}(\Gamma_{smp})]$ there is an $\mathcal{F}^{(m)\sharp}(\Gamma^m)$-optimal estimator for $(\mathcal{D}^{\eta}, f)$.*

Proof. According to Theorem 4.4, there is π a precise pseudo-invertible $\mathcal{F}(\Gamma_{\mathrm{red}})$-reduction of $(\mathcal{D}, f)$ to $(\mathcal{D}_{\mathfrak{F}}, f_{\mathfrak{F}})$ over α_p for some $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ increasing in the last argument. This implies π^{η} is a precise pseudo-invertible $\mathcal{F}^{(m)}(\Gamma^m)$-reduction of $(\mathcal{D}^{\eta}, f)$ to $(\mathcal{D}^{\eta}_{\mathfrak{F}}, f_{\mathfrak{F}})$ over β_p. Applying Corollary 4.2, we get the desired result. □

Corollary 4.7. *Fix $\mathcal{F}^{(m)}$ a fall space of rank m and $\Gamma^m = (\Gamma^m_{\mathfrak{R}}, \Gamma^m_{\mathfrak{A}})$ growth spaces of rank m s.t. $\mathcal{F}^{(m)}$ is $\Gamma^m_{\mathfrak{A}}$-ample. Assume that $\mathcal{F}\eta \subseteq \mathcal{F}^{(m)}$, $\Gamma_r\eta \subseteq \Gamma^m_{\mathfrak{R}}$ and for any $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ increasing in the last argument, $\mathcal{F}^{(m)}\beta_p \subseteq \mathcal{F}^{(m)}$, $\Gamma^m_{\mathfrak{R}}\beta_p = \Gamma^m_{\mathfrak{R}}$ and $\Gamma^m_{\mathfrak{A}}\beta_p = \Gamma^m_{\mathfrak{A}}$. In the setting of Theorem 4.4, assume there is an $\mathcal{F}^{(m)}(\Gamma^m)$-optimal estimator for $(\mathcal{D}^{\eta}_{\mathfrak{F}}, f_{\mathfrak{F}})$. Then, for any $(\mathcal{D}, f) \in \textsc{SampX}_{\mathfrak{F}}[\mathcal{F}(\Gamma_{smp})]$ there is an $\mathcal{F}^{(m)}(\Gamma^m)$-optimal estimator for $(\mathcal{D}^{\eta}, f_{\phi})$.*

Proof. Completely analogous to proof of Corollary 4.6. □

In particular, the conditions of Corollary 4.6 and Corollary 4.7 can hold for $\mathcal{F} = \mathcal{F}_{\zeta}$ (the fall space of functions which are $O(\zeta)$; see Example 2.7) and $\mathcal{F}^{(m)} = \mathcal{F}^{(\varphi)}_{\mathrm{uni}}$ (see Example 2.8):

Proposition 4.13. *Consider $\varphi : \mathbb{N}^n \to \mathbb{N}$ non-decreasing in the last argument s.t. $\varphi \geq 3$. Define $\zeta : \mathbb{N}^n \to \mathbb{R}$ by*

$$\zeta(K) := \frac{\log\log(3 + \sum_{i\in[n]} K_i)}{\log\log\varphi(K)} \tag{4.25}$$

Assume ζ is bounded and there is $h \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $\zeta \geq 2^{-h}$. Let $m = n+1$. Then, $\mathcal{F}_\zeta \eta \subseteq \mathcal{F}^{(\varphi)}_{\text{uni}}$ and for any $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ increasing in the last argument, $\mathcal{F}^{(\varphi)}_{\text{uni}} \beta_p \subseteq \mathcal{F}^{(\varphi)}_{\text{uni}}$.

Proof. Consider any $\varepsilon_0 \in \mathcal{F}_\zeta$.

$$\sum_{l=2}^{\varphi(K)-1} \frac{\varepsilon_0(K)}{l\log l} \leq \frac{3}{2}(\log 3)\varepsilon_0(K) \int_2^{\varphi(K)} \frac{\mathrm{d}t}{t\log t}$$

$$\sum_{l=2}^{\varphi(K)-1} \frac{\varepsilon_0(K)}{l\log l} \leq \frac{3}{2}(\log 3)(\ln 2)^2 \varepsilon_0(K)\log\log\varphi(K)$$

For some $M_0 \in \mathbb{R}^{>0}$, $\varepsilon_0 \leq M_0\zeta$, therefore

$$\sum_{l=2}^{\varphi(K)-1} \frac{\varepsilon_0(K)}{l\log l} \leq \frac{3}{2}(\log 3)(\ln 2)^2 M_0\zeta(K)\log\log\varphi(K)$$

$$\sum_{l=2}^{\varphi(K)-1} \frac{\varepsilon_0(K)}{l\log l} \leq \frac{3}{2}(\log 3)(\ln 2)^2 M_0 \log\log(3 + \sum_{i\in[n]} K_i)$$

We got $\varepsilon_0 \circ \eta \in \mathcal{F}^{(\varphi)}_{\text{uni}}$. Now, consider any $\varepsilon_1 \in \mathcal{F}^{(\varphi)}_{\text{uni}}$ and $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ increasing in the last argument. Clearly, $p(K) \geq K_{n-1}$.

$$\sum_{l=2}^{\varphi(J,k)-1} \frac{\varepsilon_1(J, p(J,k), l)}{l\log l} \leq \sum_{l=2}^{\varphi(J,p(J,k))-1} \frac{\varepsilon_1(J, p(J,k), l)}{l\log l}$$

For some $M_1 \in \mathbb{R}^{>0}$ and $q \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$

$$\sum_{l=2}^{\varphi(J,k)-1} \frac{\varepsilon_1(J, p(J,k), l)}{l\log l} \leq M_1 \log\log q(J, p(J,k))$$

We got $\varepsilon_1 \circ \beta_p \in \mathcal{F}^{(\varphi)}_{\text{uni}}$. □

5 Existence and uniqueness

5.1 Existence

5.1.1 Positive results

We give two existence theorems for $\mathcal{F}_{\text{uni}}^{(n)}(\Gamma)$-optimal estimators (the fall space $\mathcal{F}_{\text{uni}}^{(n)}$ was defined in Example 2.8). Theorem 5.1 shows that, for appropriate steadily growing functions r and l, *all* distributional estimation problems of rank $n-1$ admit $\mathcal{F}_{\text{uni}}^{(n)}(\Gamma_r, \Gamma_l)$-optimal estimators when trivially extended to rank n. The extra parameter serves to control the resources available to the estimator. To illustrate its significance using the informal[14] example from the introduction, observe that the question "what is the probability 7614829 is prime?" should depend on the amount of available time. For example, we can use additional time to test for divisibility by additional smaller primes (or in some more clever way) until eventually we are able to test primality and assign a probability in $\{0, 1\}$.

However, in general the estimators constructed in Theorem 5.1 are non-uniform because they rely on the advice string to emulate the Q with the lowest Brier score. Theorem 5.2 shows that, under certain stronger assumptions on r and l, for *samplable* distributional estimation problems there is an estimator which requires only as much advice as the sampler. In particular, the existence of a uniform sampler implies the existence of a uniform $\mathcal{F}_{\text{uni}}^{(n)}(\Gamma_r, \Gamma_l)$-optimal estimator.

We will use the notation $\eta : \mathbb{N}^n \to \mathbb{N}^{n-1}$ defined by

$$\forall J \in \mathbb{N}^{n-1}, k \in \mathbb{N} : \eta(J, k) = J$$

Theorem 5.1. *Fix $l : \mathbb{N}^n \to \mathbb{N}^{>0}$ steadily growing. Denote $\Gamma_{\text{adv}}^n := (\Gamma_0^n, \Gamma_l)$. Fix $r : \mathbf{1} \xrightarrow{\Gamma_{\text{adv}}} \mathbb{N}$ steadily growing. Assume $\Gamma_{\mathfrak{R}} = \Gamma_r$, $\Gamma_{\mathfrak{A}} = \Gamma_l$. Consider $(\mathcal{D}, f)$ a distributional estimation problem of rank $n-1$. Then, there exists an $\mathcal{F}_{\text{uni}}^{(n)}(\Gamma)$-optimal estimator for $(\mathcal{D}^\eta, f)$.*

The following two propositions approximately state that, given an arbitrary function $\zeta(J, k)$ for which polynomial increases in k lead to a decrease in ζ, the difference between $\zeta(J, k)$ and some average of values after $\zeta(J, q(J, k))$ lies in $\mathcal{F}_{\text{uni}}^{(n)}$. Roughly, this occurs because either ζ falls quickly enough that, in the asymptotic tail, the values approximately vanish, or ζ falls slowly enough that, going polynomially further out doesn't change ζ very much.

[14] Strictly speaking, this example cannot be formalized in the framework as presented here since the set of prime numbers is in P. We can tackle it by e.g. taking NC instead of P as the permissible time complexity for our estimators, but we don't explore this variant in the present work.

Proposition 5.1. *For any $q \in \mathbb{N}[J_0, J_1 \dots J_{n-2}]$ s.t. $q \geq 2$ there are $\{\omega_q^K \in \mathcal{P}(\mathbb{N})\}_{K \in \mathbb{N}^n}$ s.t. for any $\zeta : \mathbb{N}^n \to \mathbb{R}$ bounded, if there is a function $\varepsilon \in \mathcal{F}_{\text{uni}}^{(n)}$ s.t.*

$$\forall J \in \mathbb{N}^{n-1}, k, k' \in \mathbb{N} : k' \geq (k+2)^{\lfloor \log q(J) \rfloor} - 2 \implies \zeta(J, k') \leq \zeta(J, k) + \varepsilon(J, k) \quad (5.1)$$

then

$$\zeta(J, k) \equiv \mathrm{E}_{i \sim \omega_p^{Jk}}[\zeta(J, (k+2)^{\lfloor \log q(J) \rfloor} - 2 + i)] \pmod{\mathcal{F}_{\text{uni}}^{(n)}} \quad (5.2)$$

Proof. Take any $a \in \mathbb{N}$ s.t. $a \geq 5$.

$$\int_{t=a}^{a^{\lfloor \log q(J) \rfloor}} \mathrm{d}(\log \log t) = \log \log a^{\lfloor \log q(J) \rfloor} - \log \log a$$

$$\int_{t=a}^{a^{\lfloor \log q(J) \rfloor}} \mathrm{d}(\log \log t) = \log(\lfloor \log q(J) \rfloor \log a) - \log \log a$$

$$\int_{t=a}^{a^{\lfloor \log q(J) \rfloor}} \mathrm{d}(\log \log t) = \log \lfloor \log q(J) \rfloor + \log \log a - \log \log a$$

$$\int_{t=a}^{a^{\lfloor \log q(J) \rfloor}} \mathrm{d}(\log \log t) = \log \lfloor \log q(J) \rfloor$$

Consider any $\zeta : \mathbb{N}^n \to \mathbb{R}$ bounded.

$$|\int_{t=a}^{a^{\lfloor \log q(J) \rfloor}} \zeta(J, \lfloor t \rfloor - 2) \, \mathrm{d}(\log \log t)| \leq (\sup|\zeta|) \log \lfloor \log q(J) \rfloor$$

In particular

$$|\int_{t=2}^{2^{\lfloor \log q(J) \rfloor}} \zeta(J, \lfloor t \rfloor - 2) \, \mathrm{d}(\log \log t)| \leq (\sup|\zeta|) \log \lfloor \log q(J) \rfloor$$

Adding the last two inequalities

$$|\int_{t=2}^{2^{\lfloor \log q(J) \rfloor}} \zeta(J, \lfloor t \rfloor - 2) \, \mathrm{d}(\log \log t)| + |\int_{t=a}^{a^{\lfloor \log q(J) \rfloor}} \zeta(J, \lfloor t \rfloor - 2) \, \mathrm{d}(\log \log t)| \leq 2(\sup|\zeta|) \log \lfloor \log q(J) \rfloor$$

$$\int_{t=2}^{2^{\lfloor \log q(J)\rfloor}} \zeta(J,\lfloor t\rfloor -2)\,\mathrm{d}(\log\log t) - \int_{t=a}^{a^{\lfloor \log q(J)\rfloor}} \zeta(J,\lfloor t\rfloor -2)\,\mathrm{d}(\log\log t) \le 2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

$$\int_{t=2}^{a} \zeta(J,\lfloor t\rfloor -2)\,\mathrm{d}(\log\log t) - \int_{t=2^{\lfloor \log q(J)\rfloor}}^{a^{\lfloor \log q(J)\rfloor}} \zeta(J,\lfloor t\rfloor -2)\,\mathrm{d}(\log\log t) \le 2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

We have $\mathrm{d}(\log\log t^{\lfloor \log q(J)\rfloor}) = \mathrm{d}(\log\log t)$ therefore we can substitute in the second term on the left hand side and get

$$\int_{t=2}^{a} \zeta(J,\lfloor t\rfloor -2)\,\mathrm{d}(\log\log t) - \int_{t=2}^{a} \zeta(J,\lfloor t^{\lfloor \log q(J)\rfloor}\rfloor -2)\,\mathrm{d}(\log\log t) \le 2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

$$\int_{t=2}^{a} (\zeta(J,\lfloor t\rfloor -2) - \zeta(J,\lfloor t^{\lfloor \log q(J)\rfloor}\rfloor -2))\,\mathrm{d}(\log\log t) \le 2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

$$\int_{2}^{a} (\zeta(J,\lfloor t\rfloor -2) - \zeta(J,\lfloor t^{\lfloor \log q(J)\rfloor}\rfloor -2))\frac{\mathrm{d}t}{(\ln 2)^2 t\log t} \le 2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

$$\sum_{k=0}^{a-3}\int_{k+2}^{k+3} \frac{\zeta(J,\lfloor t\rfloor -2) - \zeta(J,\lfloor t^{\lfloor \log q(J)\rfloor}\rfloor -2)}{t\log t}\,\mathrm{d}t \le 2(\ln 2)^2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

$$\sum_{k=0}^{a-3}\int_{0}^{1} \frac{\zeta(J,k) - \zeta(J,\lfloor (k+t+2)^{\lfloor \log q(J)\rfloor}\rfloor -2)}{(k+t+2)\log(k+t+2)}\,\mathrm{d}t \le 2(\ln 2)^2(\sup|\zeta|)\log\lfloor \log q(J)\rfloor$$

For $k \ge 2$ we have $(k+3)\log(k+3) \le \frac{5}{2}k\log\frac{5}{2}k \le \frac{5}{2}k\log k^{\log 5} = \frac{5}{2}(\log 5)k\log k$.

$$\sum_{k=2}^{a-3} \frac{\zeta(J,k) - \int_0^1 \zeta(J, \lfloor (k+t+2)^{\lfloor \log q(J) \rfloor} \rfloor - 2)\,\mathrm{d}t}{\frac{5}{2}(\log 5) k \log k} \leq 2(\ln 2)^2 (\sup|\zeta|) \log\lfloor \log q(J) \rfloor$$

Define

$$I_q^{Jk}(i) := \{t \in [0,1] \mid (k+t+2)^{\lfloor \log q(J) \rfloor} - (k+2)^{\lfloor \log q(J) \rfloor} \in [i, i+1)\}$$

$$\omega_q^K(i) := \begin{cases} \sup I_q^K - \inf I_q^K \text{ if } I_q^K \neq \varnothing \\ 0 \text{ otherwise} \end{cases}$$

We get

$$\sum_{k=2}^{a-3} \frac{\zeta(J,k) - \sum_{i=0}^{\infty} \zeta(J, (k+2)^{\lfloor \log q(J) \rfloor} - 2 + i)\omega_q^{Jk}(i)}{k \log k} \leq \frac{4}{5}(\ln 2)(\ln 5)(\sup|\zeta|) \log\lfloor \log q(J) \rfloor$$

Denote $M := \frac{4}{5}(\ln 2)(\ln 5)(\sup|\zeta|)$ and $\bar{\zeta}(J,k) := \sum_{i=0}^{\infty} \zeta(J, (k+2)^{\lfloor \log q(J) \rfloor} - 2 + i)\omega_q^{Jk}(i)$. Using 5.1

$$\zeta(J,k) - \bar{\zeta}(J,k) \geq -\epsilon(J,k)$$

$$|\zeta(J,k) - \bar{\zeta}(J,k)| \leq \zeta(J,k) - \bar{\zeta}(J,k) + 2\epsilon(J,k)$$

$$\sum_{k=2}^{a-3} \frac{|\zeta(J,k) - \bar{\zeta}(J,k)|}{k \log k} \leq M \log\lfloor \log q(J) \rfloor + 2 \sum_{k=2}^{a-3} \frac{\epsilon(J,k)}{k \log k}$$

Taking a to infinity and using the fact that $\epsilon \in \mathcal{F}_{\text{uni}}^{(n)}$, we get the desired result. □

Proposition 5.2. *For any $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ there are $\{\omega_p^K \in \mathcal{P}(\mathbb{N})\}_{K \in \mathbb{N}^n}$ s.t. for any $\zeta : \mathbb{N}^n \to \mathbb{R}$ bounded, if there is a function $\varepsilon \in \mathcal{F}_{\text{uni}}^{(n)}$ s.t.*

$$\forall J \in \mathbb{N}^{n-1}, k, k' \in \mathbb{N} : k' \geq p(J,k) \implies \zeta(J,k') \leq \zeta(J,k) + \varepsilon(J,k) \tag{5.3}$$

then

$$\zeta(J,k) \equiv \mathrm{E}_{i \sim \omega_p^{Jk}}[\zeta(J, p(J,k) + i)] \pmod{\mathcal{F}_{\text{uni}}^{(n)}} \tag{5.4}$$

Proof. Fix $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$. Choose $q \in \mathbb{N}[J_0, J_1 \dots J_{n-2}]$ s.t. $p(J,k) \leq (k+2)^{\lfloor \log q(J) \rfloor} - 2$. Let $\{\omega_q^K \in \mathcal{P}(\mathbb{N})\}_{K \in \mathbb{N}^n}$ be as in Proposition 5.1. Define $\{\omega_p^K \in \mathcal{P}(\mathbb{N})\}_{K \in \mathbb{N}^n}$ by

$$\Pr_{i \sim \omega_p^{Jk}}[i \geq k] = \Pr_{i \sim \omega_q^{Jk}}[i + (k+2)^{\lfloor \log q(J) \rfloor} - 2 - p(J,k) \geq k]$$

Suppose $\zeta : \mathbb{N}^n \to \mathbb{R}$ is bounded and s.t. 5.3 holds. In particular, 5.1 also holds. Therefore, we have 5.2. We rewrite it as follows

$$\zeta(J,k) \equiv \mathrm{E}_{i \sim \omega_q^{Jk}}[\zeta(J, p(J,k) + i + (k+2)^{\lfloor \log q(J) \rfloor} - 2 - p(J,k))] \pmod{\mathcal{F}_{\text{uni}}^{(n)}}$$

By definition of ω_p, 5.4 follows. □

In the following, we use the notation $\alpha_p(J,k) := (J, p(J,k))$.

Proposition 5.3. *Consider $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$, $(\mathcal{D}, f)$ a distributional estimation problem and $P, Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Suppose that*

$$\sup_{i \in \mathbb{N}} \mathrm{E}_{\mathcal{D}^{\alpha_{p+i}(K)} \times \mathrm{U}_P^{\alpha_{p+i}(K)}}[(P^{\alpha_{p+i}(K)} - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \pmod{\mathcal{F}_{\text{uni}}^{(n)}} \tag{5.5}$$

$$\sup_{i \in \mathbb{N}} \mathrm{E}_{\mathcal{D}^{\alpha_{p+i}(K)} \times \mathrm{U}_P^{\alpha_{p+i}(K)}}[(P^{\alpha_{p+i}(K)} - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] \pmod{\mathcal{F}_{\text{uni}}^{(n)}} \tag{5.6}$$

Then

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K - f)^2] \leq \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_Q^K}[(Q^K - f)^2] \pmod{\mathcal{F}_{\text{uni}}^{(n)}} \tag{5.7}$$

Proof. Define $\zeta(K) := \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K(x,y) - f(x))^2]$ and observe that 5.5 implies 5.3, allowing us to apply Proposition 5.2 and get

$$\begin{aligned}&\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K}[(P^K(x,y) - f(x))^2] \\ &\qquad \equiv \mathrm{E}_{\omega_p^K}[\mathrm{E}_{\mathcal{D}^{\alpha_{p+i}(K)} \times \mathrm{U}_P^{\alpha_{p+i}(K)}}[(P^{\alpha_{p+i}(K)}(x,y) - f(x))^2]] \pmod{\mathcal{F}_{\text{uni}}^{(n)}}\end{aligned}$$

Applying 5.6 to the right hand side, we get 5.7. □

Proof of Theorem 5.1. Fix $M \geq \sup|f|$ and construct $D : \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ s.t.

$$D(x) = \begin{cases} D(x) = \max(\min(t, +M), -M) \text{ if } x = \mathrm{c}_{\mathbb{Q}}(t) \\ D(x) = 0 \text{ if } x \notin \operatorname{Im} \mathrm{c}_{\mathbb{Q}} \end{cases}$$

Choose $a^* : \mathbb{N}^n \to \{0,1\}^*$ s.t.

$$a^*(K) \in \operatorname*{arg\,min}_{a \in \{0,1\}^{\leq l(K)}} \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^{r(K)}}[(D(\mathrm{ev}^{K_{n-1}}(a; x, y)) - f(x))^2] \tag{5.8}$$

Construct $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $K \in \mathbb{N}^n$, $x, y, b_0 \in \{0,1\}^*$ and $a_0 \in \{0,1\}^{\leq l(K)}$

$$\mathrm{a}_P(K) = \langle a^*(K), \mathrm{a}_r(K) \rangle \tag{5.9}$$

$$\mathrm{r}_P(K, \langle a_0, b_0 \rangle) = r(K, b_0) \tag{5.10}$$

$$P^K(x, y, \langle a_0, b_0 \rangle) = D(\mathrm{ev}^{K_{n-1}}(a_0; x, y)) \tag{5.11}$$

Consider $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Without loss of generality we can assume $\sup|Q| \leq M$ (otherwise we can replace Q by $\tilde{Q} := \max(\min(Q, +M), -M)$ and have $\mathrm{E}[(\tilde{Q} - f)^2] \leq \mathrm{E}[(Q - f)^2]$). Choose $q \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. for any $K \in \mathbb{N}^n$ there exists $a_Q^K \in \{0,1\}^{l(\alpha_q(K))}$ for which

$$\mathrm{r}_Q(K) \leq r(\alpha_q(K)) \tag{5.12}$$

$$\forall i \in \mathbb{N}, x, z \in \{0,1\}^*, y \in \{0,1\}^{\mathrm{r}_Q(K)} : D(\mathrm{ev}^{q(K)+i}(a_Q^K; x, yz)) = Q^K(x, y) \tag{5.13}$$

Take any $i \in \mathbb{N}$.

$$\mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}_P^{\alpha_{q+i}(K)}}[(P^{\alpha_{q+i}(K)}(x, y) - f(x))^2]$$
$$= \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^{r(\alpha_{q+i}(K))}}[(D(\mathrm{ev}^{q(K)+i}(a^*(\alpha_{q+i}(K)); x, y)) - f(x))^2]$$

Using 5.8

$$\mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}_P^{\alpha_{q+i}(K)}}[(P^{\alpha_{q+i}(K)}(x, y) - f(x))^2]$$
$$\leq \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^{r(\alpha_{q+i}(K))}}[(D(\mathrm{ev}^{q(K)+i}(a_Q^K; x, y)) - f(x))^2]$$

$$\mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}_P^{\alpha_{q+i}(K)}}[(P^{\alpha_{q+i}(K)}(x,y)-f(x))^2] \leq \mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}_Q^{K}}[(Q^{K}(x,y)-f(x))^2]$$

By the same reasoning we can choose $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $p \geq q$ and

$$\mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}_P^{\alpha_{p+i}(K)}}[(P^{\alpha_{p+i}(K)}(x,y)-f(x))^2] \leq \mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}_P^{K}}[(P^{K}(x,y)-f(x))^2]$$

Applying Proposition 5.3, we conclude that P is an $\mathcal{F}_{\mathrm{uni}}^{(n)}(\Gamma)$-optimal estimator for $(\mathcal{D}^\eta, f)$. □

We now proceed to study the special case of samplable problems. These problems admit an optimal polynomial-time estimator which is essentially a brute-force implementation of the empirical risk minimization principle in statistical learning. In particular, the optimality of this algorithm can be regarded as a manifestation of the fundamental theorem of agnostic PAC learning (see e.g. Theorem 6.7 in [18]). In our case the hypothesis space of the space of programs, so this algorithm can also be regarded as a variation of Levin's universal search. The advantage of this optimal polynomial-time estimator on the fully general construction of Theorem 5.1 is that the required advice is only the advice of the sampler. The notation $\mathcal{F}_{\mathrm{mon}}^{(n)}$ below refers to the fall space defined in Example 2.9.

Theorem 5.2. *Fix $r : \mathbb{N}^n \xrightarrow{\mathrm{alg}} \mathbb{N}$ s.t.*

(i) $\mathrm{T}_r \in \Gamma_{\mathrm{poly}}^n$

(ii) As a function, $r \in \Gamma_{\mathrm{poly}}^n$.

(iii) r is non-decreasing in the last argument.

(iv) There is $s \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. $\forall K \in \mathbb{N}^n : \log(K_{n-1}+4) r(K) \leq r(\alpha_s(K))$.

In particular, r is steadily growing. Assume $\Gamma_{\mathfrak{R}} = \Gamma_r$ and $\Gamma_{\mathfrak{A}} = \Gamma_{\log}^n$. Consider $(\mathcal{D}, f)$ an distributional estimation problem of rank $n-1$ and σ an $\mathcal{F}_{\mathrm{mon}}^{(n)}(\Gamma)$-sampler of $(\mathcal{D}^\eta, f)$. Then, there exists P an $\mathcal{F}_{\mathrm{uni}}^{(n)}(\Gamma)$-optimal estimator for $(\mathcal{D}^\eta, f)$ s.t. $\mathrm{a}_P = \mathrm{a}_\sigma$. In particular, if σ is uniform (i.e. $\mathrm{a}_\sigma \equiv \boldsymbol{\lambda}$) then so is P.

Proposition 5.4. *Fix $r \in \Gamma^n_{\text{poly}}$ s.t.*

(i) r is non-decreasing in the last argument.

(ii) There is $s \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $\forall K \in \mathbb{N}^n : \log(K_{n-1} + 4) r(K) \leq r(\alpha_s(K))$.

In particular, r is steadily growing. Consider any $\gamma \in \Gamma_r$ and define $\gamma' : \mathbb{N} \to \mathbb{N}$ by

$$\gamma'(K) := \lfloor \log(K_{n-1} + 2) \rfloor \gamma(K)$$

Then, $\gamma' \in \Gamma_r$

Proof. Choose $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $p(K) \geq K_{n-1}$ and $r(\alpha_p(K)) \geq \gamma(K)$. We get

$$\gamma'(K) \leq \lfloor \log(K_{n-1} + 2) \rfloor r(\alpha_p(K))$$

$$\gamma'(K) \leq \lfloor \log(p(K) + 4) \rfloor r(\alpha_p(K))$$

$$\gamma'(K) \leq r(\alpha_s(\alpha_p(K)))$$

□

Proposition 5.5. *Consider $(\mathcal{D}, f)$ a distributional estimation problem, σ an $\mathcal{F}(\Gamma)$-sampler of $(\mathcal{D}, f)$, I a set and $\{h^K_\alpha : \{0,1\}^* \xrightarrow{\text{mk}} \mathbb{R}\}_{\alpha \in I, K \in \mathbb{N}^n}$ uniformly bounded. Then*

$$\mathrm{E}_{\mathrm{U}^K_\sigma}[\mathrm{E}[(h^K_\alpha \circ \sigma^K_0 - \sigma^K_1)^2]] \overset{\alpha}{\equiv} \mathrm{E}_{\mathcal{D}^K}[\mathrm{E}[(h^K_\alpha - f)^2]] + \mathrm{E}_{\mathrm{U}^K_\sigma}[(f \circ \sigma^K_0 - \sigma^K_1)^2] \pmod{\mathcal{F}} \tag{5.14}$$

Proof. Denote $h^K_{\sigma\alpha} := h^K_\alpha \circ \sigma^K_0$, $f^K_\sigma := f \circ \sigma^K_0$. Proposition 3.10 implies

$$\mathrm{E}_{\mathrm{U}^K_\sigma}[(\mathrm{E}[h^K_{\sigma\alpha}] - f^K_\sigma) f^K_\sigma] \overset{\alpha}{\equiv} \mathrm{E}_{\mathcal{D}^K}[(\mathrm{E}[h^K_\alpha] - f) f] \pmod{\mathcal{F}}$$

Applying Proposition 3.11 to the right hand side

$$\mathrm{E}_{\mathrm{U}^K_\sigma}[(\mathrm{E}[h^K_{\sigma\alpha}] - f^K_\sigma) f^K_\sigma]] \overset{\alpha}{\equiv} \mathrm{E}_{\mathrm{U}^K_\sigma}[(\mathrm{E}[h^K_{\sigma\alpha}] - f^K_\sigma)\sigma^K_1] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathrm{U}_\sigma^K}[(\mathrm{E}[h_{\sigma\alpha}^K] - f_\sigma^K)(f_\sigma^K - \sigma_1^K)]] \overset{\alpha}{\equiv} 0 \pmod{\mathcal{F}} \tag{5.15}$$

On the other hand

$$\mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(h_{\sigma\alpha}^K - \sigma_1^K)^2]] = \mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(h_{\sigma\alpha}^K - f_\sigma^K + f_\sigma^K - \sigma_1^K)^2]]$$

$$\mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(h_{\sigma\alpha}^K - \sigma_1^K)^2]] = \mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(h_{\sigma\alpha}^K - f_\sigma^K)^2]] + 2\,\mathrm{E}_{\mathrm{U}_\sigma^K}[(\mathrm{E}[h_{\sigma\alpha}^K] - f_\sigma^K)(f_\sigma^K - \sigma_1^K)]] + \mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(f_\sigma^K - \sigma_1^K)^2]]$$

Applying Proposition 3.10 to the first term on the right hand side and 5.15 to the second term on the right hand side, we get 5.14. □

Proof of Theorem 5.2. Fix $M \geq \sup|f|$ and construct $D : \{0,1\}^* \xrightarrow{\text{alg}} \mathbb{Q}$ s.t.

$$D(x) = \begin{cases} D(x) = \max(\min(t, M), -M) \text{ if } x = \mathrm{c}_{\mathbb{Q}}(t) \\ D(x) = 0 \text{ if } x \notin \operatorname{Im} \mathrm{c}_{\mathbb{Q}} \end{cases}$$

Denote $l(K) := \lfloor \log(K_{n-1} + 2) \rfloor$. Denote $s(K) := 2\lceil M^2 \rceil l(K)^2$. Construct $R : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $K \in \mathbb{N}^n$, $w \in \{0,1\}^*$, $a \in \{0,1\}^{l(K)}$, $\{y_i \in \{0,1\}^{r_\sigma(K,w)}\}_{i \in [s(K)]}$ and $\{z_i \in \{0,1\}^{r(K)}\}_{i \in [s(K)]}$

$$\mathrm{a}_R(K) = \mathrm{a}_\sigma(K) \tag{5.16}$$

$$\mathrm{r}_R(K, w) = s(K)(\mathrm{r}_\sigma(K, w) + r(K)) \tag{5.17}$$

$$R^K\left(a, \prod_{i \in [s(K)]} y_i z_i, w\right) = \frac{1}{s(K)} \sum_{i \in [s(K)]} (D(\mathrm{ev}^{K_{n-1}}(a; \sigma^K(y_i, w)_0, z_i)) - \sigma^K(y_i, w)_1)^2 \tag{5.18}$$

That is, R generates $2\lceil M^2 \rceil l(K)^2$ estimates of f using σ and computes the "empirical risk" of the program a w.r.t. these estimates. Here, 5.17 is legitimate due to Proposition 5.4.

Construct $A : \mathbf{1} \xrightarrow{\Gamma} \{0,1\}^*$ s.t. for any $K \in \mathbb{N}^n$, $w \in \{0,1\}^*$, $\{y_i \in \{0,1\}^{r_\sigma(K,w)}\}_{i \in [s(K)]}$ and $\{z_i \in \{0,1\}^{r(K)}\}_{i \in [s(K)]}$

$$\mathrm{a}_A(K) = \mathrm{a}_\sigma(K) \tag{5.19}$$

$$\mathrm{r}_A(K, w) = \mathrm{r}_R(K, w) \tag{5.20}$$

$$A^K\left(\prod_{i\in[s(K)]} y_i z_i, w\right) \in \operatorname*{arg\,min}_{a\in\{0,1\}^{\leq l(K)}} R^K\left(a, \prod_{i\in[s(K)]} y_i z_i, w\right) \tag{5.21}$$

Finally, construct $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $K \in \mathbb{N}^n$, $w \in \{0,1\}^*$, $\{y_i \in \{0,1\}^{r_\sigma(K,w)}\}_{i\in[s(K)]}$, $\{z_i \in \{0,1\}^{r(K)}\}_{i\in[s(K)]}$ and $z_* \in \{0,1\}^{r(K)}$

$$\mathrm{a}_P(K) = \mathrm{a}_\sigma(K) \tag{5.22}$$

$$\mathrm{r}_P(K, w) = \mathrm{r}_R(K, w) + r(K) \tag{5.23}$$

$$P^K(x, \left(\prod_{i\in[s(K)]} y_i z_i\right) z_*, w) = D(\mathrm{ev}^{K_{n-1}}(A^K\left(\prod_{i\in[s(K)]} y_i z_i, w\right); x, z_*)) \tag{5.24}$$

Define $\varrho_0^K \in \mathbb{R}$ by

$$\varrho_0^K := \mathrm{E}_{\mathrm{U}_\sigma^K}[(f(\sigma^K(y)_0) - \sigma^K(y)_1)^2]$$

For any $b \in \{0,1\}^*$, define $\varrho^K(b)$ by

$$\varrho^K(b) := \mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}^{r(K)}}[(D(\mathrm{ev}^{K_{n-1}}(b; x, z)) - f(x))^2]$$

Consider any $\alpha : \mathbb{N}^n \to \{0,1\}^*$ s.t. $|\alpha(K)| \leq l(K)$. Define $h_\alpha^K : \{0,1\}^* \xrightarrow{\mathrm{mk}} \mathbb{R}$ by

$$\forall s, t \in \mathbb{R} : \Pr[h_\alpha^K(x) \in (s,t)] := \Pr_{z\sim \mathrm{U}^{r(K)}}[D(\mathrm{ev}^{K_{n-1}}(\alpha(K); x, z)) \in (s,t)]$$

By Proposition 5.5

$$\mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(h_\alpha^K(\sigma^K(y)_0) - \sigma^K(y)_1)^2]] \overset{\alpha}{\equiv}$$
$$\mathrm{E}_{\mathcal{D}^{\eta(K)}}[\mathrm{E}[(h_\alpha^K(x) - f(x))^2]] + \mathrm{E}_{\mathrm{U}_\sigma^K}[(f(\sigma^K(y)_0) - \sigma^K(y)_1)^2] \pmod{\mathcal{F}_{\mathrm{mon}}^{(n)}}$$

$$\mathrm{E}_{\mathrm{U}_\sigma^K}[\mathrm{E}[(h_\alpha^K(\sigma^K(y)_0) - \sigma^K(y)_1)^2]] \overset{\alpha}{\equiv} \varrho^K(\alpha(K)) + \varrho_0^K \pmod{\mathcal{F}_{\mathrm{mon}}^{(n)}} \tag{5.25}$$

$R^K(\alpha(K), y)$ is the average of $2\lceil M^2 \rceil l(K)^2$ independent and and identically distributed bounded random variables. By 5.25, there is $\varepsilon \in \mathcal{F}^{(n)}_{\text{mon}}$ that doesn't depend on α s.t. the expected value of these random variables is in $[\varrho^K(\alpha(K)) + \varrho^K_0 - \varepsilon(K), \varrho^K(\alpha(K)) + \varrho^K_0 + \varepsilon(K)]$. Applying Hoeffding's inequality we conclude that

$$\forall b \in \{0,1\}^{\leq l(K)} : \Pr_{\mathrm{U}^K_R}[R^K(b, y) > \varrho^K(b) + \varrho^K_0 + \varepsilon(K) + l(K)^{-1/2}] \leq 2^{-\log(e) l(K)}$$

In particular, since for any $b \in \{0,1\}^{l(K)}$, $R^K(A^K(y), y) \leq R^K(b, y)$

$$\forall b \in \{0,1\}^{\leq l(K)} : \Pr_{\mathrm{U}^K_R}[R^K(A^K(y), y) > \varrho^K(b) + \varrho^K_0 + \varepsilon(K) + l(K)^{-1/2}] \leq 2^{-\log(e) l(K)} \tag{5.26}$$

Similarly, we have

$$\forall b \in \{0,1\}^{\leq l(K)} : \Pr_{\mathrm{U}^K_R}[R^K(b, y) < \varrho^K(b) + \varrho^K_0 - \varepsilon(K) - l(K)^{-1/2}] \leq 2^{-\log(e) l(K)}$$

$$\Pr_{\mathrm{U}^K_R}[\exists b \in \{0,1\}^{\leq l(K)} : R^K(b, y) < \varrho^K(b) + \varrho^K_0 - \varepsilon(K) - l(K)^{-1/2}] \leq 2^{-(\log(e)-1) l(K)+1}$$

$$\Pr_{\mathrm{U}^K_R}[R^K(A^K(y), y) < \varrho^K(A^K(y)) + \varrho^K_0 - \varepsilon(K) - l(K)^{-1/2}] \leq 2^{-(\log(e)-1) l(K)+1} \tag{5.27}$$

Combining 5.26 and 5.27, we conclude that for any $b \in \{0,1\}^{\leq l(K)}$

$$\Pr_{\mathrm{U}^K_R}[\varrho^K(A^K(y)) + \varrho^K_0 - \varepsilon(K) - l(K)^{-1/2} > \varrho^K(b) + \varrho^K_0 + \varepsilon(K) + l(K)^{-1/2}] \leq 2^{-\log(e) l(K)} + 2^{-(\log(e)-1) l(K)+1}$$

$$\Pr_{\mathrm{U}^K_R}[\varrho^K(A^K(y)) > \varrho^K(b) + 2(\varepsilon(K) + l(K)^{-1/2})] \leq 2^{-(\log(e)-1) l(K)+2}$$

It follows that for some $M_0 \in \mathbb{R}^{>0}$

$$\mathrm{E}_{\mathrm{U}^K_R}[\varrho^K(A^K(y)] \leq \varrho^K(b) + 2(\varepsilon(K) + l(K)^{-1/2}) + 2^{-(\log(e)-1) l(K)+2} M_0$$

Denote $\varepsilon_1(K) := 2(\varepsilon(K) + l(K)^{-1/2}) + 2^{-(\log(e)-1)l(K)+2}M_0$. Note that $\varepsilon_1 \in \mathcal{F}^{(n)}_{\text{mon}}$ because ε is by assumption, the last two terms are monotonically decreasing, and both $\sum_{k=2}^{\infty} \frac{1}{k \log k \sqrt{\lfloor \log(k+2) \rfloor}}$ and $\sum_{k=2}^{\infty} \frac{2^{-(\log(e)-1)\lfloor \log(k+2) \rfloor}}{k \log k}$ converge.

$$\mathrm{E}_{\mathrm{U}^K_R}[\mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^{r(K)}}[(D(\mathrm{ev}^{K_{n-1}}(A^K(y); x, z)) - f(x))^2]] \leq \varrho^K(b) + \varepsilon_1(K)$$

$$\forall b \in \{0,1\}^{\leq l(K)} : \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^K_P}[(P^K(x, y) - f(x))^2] \leq \varrho^K(b) + \varepsilon_1(K)$$

Consider $Q : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. Without loss of generality we can assume $\sup|Q| \leq M$. Choose $q \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $q(K) \geq K_{n-1}$ and for all $K \in \mathbb{N}^n$, 5.12 and 5.13 hold.

$$\mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}_P^{\alpha_{q+i}(K)}}[(P^{\alpha_{q+i}(K)}(x, y) - f(x))^2] \leq \varrho^{\alpha_{q+i}(K)}(a^K_Q) + \varepsilon_1(\alpha_{q+i}(K))$$

$$\begin{aligned}\mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}_P^{\alpha_{q+i}(K)}}&[(P^{\alpha_{q+i}(K)}(x, y) - f(x))^2] \\ &\leq \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^{r(\alpha_{q+i}(K))}}[(D(\mathrm{ev}^{q(K)+i}(a^K_Q; x, z)) - f(x))^2] + \varepsilon_1(\alpha_{q+i}(K))\end{aligned}$$

$$\begin{aligned}\mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}_P^{\alpha_{q+i}(K)}}&[(P^{\alpha_{q+i}(K)}(x, y) - f(x))^2] \\ &\leq \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^K_Q}[(Q^K(x, z) - f(x))^2] + \varepsilon_1(\alpha_{q+i}(K))\end{aligned}$$

Define $\bar{\varepsilon}_1(K) := \sup_{k \geq K_{n-1}} \varepsilon_1(\eta(K), k)$. We have $\bar{\varepsilon}_1 \in \mathcal{F}^{(n)}_{\text{uni}}$ and $\varepsilon_1(\alpha_{q+i}(K)) \leq \bar{\varepsilon}_1(K)$ therefore

$$\begin{aligned}\sup_{i \in \mathbb{N}} \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}_P^{\alpha_{q+i}(K)}}&[(P^{\alpha_{q+i}(K)}(x, y) - f(x))^2] \\ &\leq \mathrm{E}_{\mathcal{D}^{\eta(K)} \times \mathrm{U}^K_Q}[(Q^K(x, z) - f(x))^2] \pmod{\mathcal{F}^{(n)}_{\text{uni}}}\end{aligned}$$

By the same reasoning we can choose $p \in \mathbb{N}[K_0, K_1 \dots K_{n-1}]$ s.t. $p \geq q$ and

$$\sup_{i\in\mathbb{N}} \mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}_P^{\alpha_{p+i}(K)}}[(P^{\alpha_{p+i}(K)}(x,y) - f(x))^2]$$
$$\leq \mathrm{E}_{\mathcal{D}^{\eta(K)}\times \mathrm{U}_P^{K}}[(P^{K}(x,y) - f(x))^2] \pmod{\mathcal{F}_{\mathrm{uni}}^{(n)}}$$

Applying Proposition 5.3, we conclude that P is an $\mathcal{F}_{\mathrm{uni}}^{(n)}(\Gamma)$-optimal estimator for $(\mathcal{D}^\eta, f)$. □

The above existence theorems employ the fall space $\mathcal{F}_{\mathrm{uni}}^{(n)}$ whose meaning might seem somewhat obscure. To shed some light on this, consider the following observation. Informally, optimal polynomial-time estimators represent "expected values" corresponding to the uncertainty resulting from bounding computing resources. When a function can be computed in polynomial time, this "expected value" has to approximate the function within $\mathcal{F}$ which corresponds to a state of "complete certainty." However, we will now demonstrate that when a function can only be computed in *quasi-polynomial* time, it still corresponds to complete certainty in the context of $\mathcal{F}_{\mathrm{uni}}^{(n)}(\Gamma)$-optimal estimators.

Definition 5.1. Consider $(\mathcal{D}, f)$ a distributional estimation problem and $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded. P is called an $\mathcal{F}(\Gamma)$-*perfect polynomial-time estimator for* $(\mathcal{D}, f)$ when

$$\mathrm{E}_{(x,y)\sim\mathcal{D}^K\times \mathrm{U}_P^K}[(P^K(x,y) - f(x))^2] \equiv 0 \pmod{\mathcal{F}} \tag{5.28}$$

For the sake of brevity, we will say "$\mathcal{F}(\Gamma)$-perfect estimator" rather than "$\mathcal{F}(\Gamma)$-perfect polynomial-time estimator."

Perfect polynomial-time estimators are essentially objects of "classical" average-case complexity theory. In particular, perfect polynomial-time estimators for distributional decision problems of rank 1 are closely related to heuristic algorithms in the sense of [4] (their existence is equivalent under mild assumptions), whereas perfect polynomial-time estimators for rank 2 problems of the form $(\mathcal{D}^\eta, \chi_L)$ with $\mathcal{D}$ of rank 1 are related to heuristic schemes.

Comparing the definition of a perfect estimator to the definition of an inapproximable predicate, (Definition 7.9 in [12]), if f is (poly, ρ)-inapproximable, and $\mathcal{D}^k = \mathrm{U}^k$, then for any $\zeta \in o(\rho)$, there is no $\mathcal{F}_\zeta(\Gamma_0^1, \Gamma_{\mathrm{poly}}^1)$-perfect estimator for $(\mathcal{D}, f)$.

Proposition 5.6. *Consider $(\mathcal{D}, f)$ a distributional estimation problem, $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ bounded, $m \in \mathbb{N}^{>0}$ and $p \in \mathbb{N}[J_0, J_1 \ldots J_{n-2}]$ s.t. $p \geq 2$. Define $q : \mathbb{N}^n \to \mathbb{N}$ by $q(J,k) := 2^{\lfloor \log p(J) \log \max(k,1) \rfloor^m}$. Suppose that*

$$\sup_{i \in \mathbb{N}} \mathrm{E}_{(x,y) \sim \mathcal{D}^K \times \mathrm{U}_P^{\alpha_{q+i}(K)}} [(P^{\alpha_{q+i}(K)}(x,y) - f(x))^2] \equiv 0 \pmod{\mathcal{F}_{\mathrm{uni}}^{(n)}} \tag{5.29}$$

Then, P is an $\mathcal{F}_{\mathrm{uni}}^{(n)}(\Gamma)$-perfect estimator for $(\mathcal{D}, f)$.

Proof. Define $\varepsilon : \mathbb{N}^n \to \mathbb{R}$ by

$$\varepsilon(K) := \mathrm{E}_{(x,y) \sim \mathcal{D}^K \times \mathrm{U}_P^K} [(P^K(x,y) - f(x))^2]$$

We have

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} = \int_2^{\infty} \frac{\varepsilon(J, \lfloor t \rfloor)}{\lfloor t \rfloor \log \lfloor t \rfloor} \, \mathrm{d}t$$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq \frac{3}{2} \log 3 \int_2^{\infty} \frac{\varepsilon(J, \lfloor t \rfloor)}{t \log t} \, \mathrm{d}t$$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq \frac{3}{2} (\log 3)(\ln 2)^2 \int_2^{\infty} \varepsilon(J, \lfloor t \rfloor) \, \mathrm{d}(\log \log t)$$

Substitute $t = 2^{(\log p(J) \log s)^m}$. Denoting $s_0 = 2^{(\log p(J))^{-1}}$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq \frac{3}{2} (\log 3)(\ln 2)^2 m \int_{s=s_0}^{\infty} \varepsilon(J, \lfloor 2^{(\log p(J) \log s)^m} \rfloor) \, \mathrm{d}(\log \log s)$$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq \frac{3}{2} (\log 3) m \int_{s_0}^{\infty} \frac{\varepsilon(J, \lfloor 2^{(\log p(J) \log s)^m} \rfloor)}{s \log s} \, \mathrm{d}s$$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq \frac{3}{2} (\log 3) m \int_{s_0}^{\infty} \frac{\sup_{i \in \mathbb{N}} \varepsilon(J, 2^{\lfloor \log p(J) \log \lfloor s \rfloor \rfloor^m} + i)}{s \log s} \, \mathrm{d}s$$

For some $M \in \mathbb{R}$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq M + \frac{3}{2} (\log 3) m \int_2^{\infty} \frac{\sup_{i \in \mathbb{N}} \varepsilon(J, 2^{\lfloor \log p(J) \log \lfloor s \rfloor \rfloor^m} + i)}{\lfloor s \rfloor \log \lfloor s \rfloor} \, \mathrm{d}s$$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq M + \frac{3}{2}(\log 3)m \sum_{k=2}^{\infty} \frac{\sup_{i \in \mathbb{N}} \varepsilon(J, 2^{\lfloor \log p(J) \log k \rfloor^m} + i)}{k \log k}$$

Using 5.29 we get that for some $M_1 \in \mathbb{R}^{>0}$ and $p_1 \in \mathbb{N}[J_0, J_1 \ldots J_{n-2}]$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq M + M_1 \log \log p_1(J)$$

Denoting $M_2 := 2^{M_1^{-1} M}$

$$\sum_{k=2}^{\infty} \frac{\varepsilon(J,k)}{k \log k} \leq M_1 \log \log p_1(J)^{M_2}$$

□

5.1.2 Negative results

The following propositions lead to disproving the existence of optimal polynomial-time estimators with no advice for certain distributional estimation problems.

Proposition 5.7. *Consider $h : \mathbb{N}^n \to \mathbb{R}$ bounded and $\mathcal{D}$ a word ensemble s.t. given $K_1, K_2 \in \mathbb{N}^n$, if $K_1 \neq K_2$ then $\operatorname{supp} \mathcal{D}^{K_1} \cap \operatorname{supp} \mathcal{D}^{K_2} = \varnothing$. Assume that either $1 \in \Gamma_{\mathfrak{A}}$ and the image of h is a finite subset of $\mathbb{Q}$ or $\mathcal{F}^{\frac{1}{2}}$ is $\Gamma_{\mathfrak{A}}$-ample. Define $f : \operatorname{supp} \mathcal{D} \to \mathbb{R}$ by requiring that for any $K \in \mathbb{N}^n$ and $x \in \operatorname{supp} \mathcal{D}^K$, $f(x) = h(K)$. Then, there exists an $\mathcal{F}(\Gamma)$-perfect estimator for $(\mathcal{D}, f)$.*

Proof. The idea is that, because the estimation problem only depends on the index K, the advice allows the estimator to either memorize f directly or closely approximate it.

In the case $\mathcal{F}^{\frac{1}{2}}$ is $\Gamma_{\mathfrak{A}}$-ample, let $\zeta : \mathbb{N}^n \to (0, \frac{1}{2}]$ be s.t. $\zeta \in \mathcal{F}^{\frac{1}{2}}$ and $\lfloor \log \frac{1}{\zeta} \rfloor \in \Gamma_{\mathfrak{A}}$. In the other case, let $\zeta \equiv 0$. For any $K \in \mathbb{N}^n$, let $\rho(K) \in \operatorname*{arg\,min}_{s \in \mathbb{Q} \cap [h(K) - \zeta(K), h(K) + \zeta(K)]} |\mathrm{c}_{\mathbb{Q}}(s)|$. It is easy to see that there is $\gamma \in \Gamma_{\mathfrak{A}}$ s.t. for any $K \in \mathbb{N}^n$, $|\mathrm{c}_{\mathbb{Q}}(\rho(K))| \leq \gamma(K)$. Construct $P : \{0,1\}^* \xrightarrow{\Gamma} \mathbb{Q}$ s.t. for any $K \in \mathbb{N}^n$, $x \in \{0,1\}^*$ and $t \in \mathbb{Q}$ s.t. $|\mathrm{c}_{\mathbb{Q}}(t)| \leq \gamma(K)$

$$\begin{aligned} \mathrm{a}_P(K) &= \mathrm{c}_{\mathbb{Q}}(\rho(K)) \\ \mathrm{r}_P(K) &= 0 \\ P^K(x, \boldsymbol{\lambda}, \mathrm{c}_{\mathbb{Q}}(t)) &= t \end{aligned}$$

We have

$$\mathrm{E}_{x\sim\mathcal{D}^K}[(P^K(x)-f(x))^2]=(\rho(K)-h(K))^2$$

$$\mathrm{E}_{x\sim\mathcal{D}^K}[(P^K(x)-f(x))^2]\leq\zeta(K)^2$$

□

In the setting of Proposition 5.7, any $\mathcal{F}(\Gamma)$-optimal estimator for $(\mathcal{D},f)$ has to be an $\mathcal{F}(\Gamma)$-perfect estimator. In particular, if no *uniform* $\mathcal{F}(\Gamma)$-perfect estimator exists then no uniform $\mathcal{F}(\Gamma)$-optimal estimator exists (and likewise for any other condition on the estimator).

Denote $\Gamma_0:=(\Gamma_{\mathfrak{R}},\Gamma_0^n)$, $\Gamma_1:=(\Gamma_{\mathfrak{R}},\Gamma_1^n)$. Taking $\Gamma=\Gamma_1$ in Proposition 5.7 and using Proposition 2.13, we conclude that if the image of h is a finite subset of $\mathbb{Q}$ and there is no $\mathcal{F}(\Gamma_0)$-perfect estimator for $(\mathcal{D},f)$ then there is no $\mathcal{F}(\Gamma_0)$-optimal estimator for $(\mathcal{D},f)$.

For distributional decision problems and $\mathcal{F}(\Gamma)$-samplable word ensembles we have the following stronger proposition: given an optimal estimator, we get not just a perfect estimator, but a "heuristic" algorithm that depends only on K and doesn't need a problem instance.

Proposition 5.8. *Let $\Delta=(\Delta_{\mathfrak{R}},\Delta_{\mathfrak{A}})$ be a pair of growth spaces of rank n s.t. $\Delta_{\mathfrak{R}}\subseteq\Gamma_{\mathfrak{R}}$, $\Delta_{\mathfrak{A}}\subseteq\Gamma_{\mathfrak{A}}$ and $1\in\Delta_{\mathfrak{A}}$. Consider $L\subseteq\mathbb{N}^n$ and $\mathcal{D}$ a word ensemble s.t. given $K_1,K_2\in\mathbb{N}^n$, if $K_1\neq K_2$ then $\operatorname{supp}\mathcal{D}^{K_1}\cap\operatorname{supp}\mathcal{D}^{K_2}=\varnothing$. Define $\chi:\operatorname{supp}\mathcal{D}\to\{0,1\}$ by requiring that for any $K\in\mathbb{N}^n$ and $x\in\operatorname{supp}\mathcal{D}^K$, $\chi(x)=\chi_L(K)$. Assume σ is an $\mathcal{F}(\Gamma)$-sampler of $\mathcal{D}$ and P is an $\mathcal{F}(\Delta)$-optimal estimator for $(\mathcal{D},\chi)$. Then there is $A:\mathbf{1}\xrightarrow{\Gamma}\{0,1\}$ s.t. $\mathrm{a}_A(K)=\langle\mathrm{a}_\sigma(K),\mathrm{a}_P(K)\rangle$ and*

$$\Pr_{y\sim\mathrm{U}_A^K}[A^K(y)=\chi_L(K)]\equiv 1\pmod{\mathcal{F}}\tag{5.30}$$

Proof. Construct A s.t. for any $K\in\mathbb{N}^n$, $y_1\in\{0,1\}^{\mathrm{r}_L(K)}$, $y_1\in\{0,1\}^{\mathrm{r}_P(K)}$

$$\mathrm{r}_A(K)=\mathrm{r}_\sigma(K)+\mathrm{r}_P(K)$$
$$A^K(y_1y_2)=\begin{cases}0\text{ if }P^K(\sigma^K(y_1),y_2)\leq\frac{1}{2}\\1\text{ if }P^K(\sigma^K(y_1),y_2)>\frac{1}{2}\end{cases}$$

We get

$$\Pr_{y\sim \mathrm{U}_A^K}[A^K(y) \neq \chi_L(K)] \leq \Pr_{y_1\sim \mathrm{U}_\sigma^K, y_2\sim \mathrm{U}_P^K}\left[|P^K(\sigma^K(y_1), y_2) - \chi_L(K)| \geq \frac{1}{2}\right]$$

$$\Pr_{y\sim \mathrm{U}_A^K}[A^K(y) \neq \chi_L(K)] \leq \Pr_{y_1\sim \mathrm{U}_\sigma^K, y_2\sim \mathrm{U}_P^K}\left[(P^K(\sigma^K(y_1), y_2) - \chi_L(K))^2 \geq \frac{1}{4}\right]$$

$$\Pr_{y\sim \mathrm{U}_A^K}[A^K(y) \neq \chi_L(K)] \leq 4\,\mathrm{E}_{y_1\sim \mathrm{U}_\sigma^K, y_2\sim \mathrm{U}_P^K}[(P^K(\sigma^K(y_1), y_2) - \chi_L(K))^2]$$

By Proposition 3.10

$$\Pr_{y\sim \mathrm{U}_A^K}[A^K(y) \neq \chi_L(K)] \leq 4\,\mathrm{E}_{x\sim \mathcal{D}^K, y_2\sim \mathrm{U}_P^K}[(P^K(x, y_2) - \chi_L(K))^2] \pmod{\mathcal{F}}$$

$$\Pr_{y\sim \mathrm{U}_A^K}[A^K(y) \neq \chi_L(K)] \leq 4\,\mathrm{E}_{x\sim \mathcal{D}^K, y_2\sim \mathrm{U}_P^K}[(P^K(x, y_2) - \chi(x))^2] \pmod{\mathcal{F}}$$

By Proposition 5.7, P is an $\mathcal{F}(\Delta)$-perfect estimator for $(\mathcal{D}, \chi)$, therefore

$$\Pr_{y\sim \mathrm{U}_A^K}[A^K(y) \neq \chi_L(K)] \equiv 0 \pmod{\mathcal{F}}$$

□

Again, the statement can be reversed to disprove the existence of $\mathcal{F}(\Delta)$-optimal estimators for $\Delta_{\mathfrak{A}} = \Gamma_0^n$.

Now we consider the special case $\mathcal{F} = \mathcal{F}_{\mathrm{uni}}^{(\varphi)}$, $\Gamma_{\mathfrak{R}} = \Gamma_{\mathrm{poly}}^n$. Consider the standard decomposition of the index into two parameters J (which is going to be the only relevant variable in the estimation problem) and k which controls the computation time available. The following proposition states that if there is an $\mathcal{F}_{\mathrm{uni}}^{(\varphi)}(\Delta)$-optimal estimator for $(\mathcal{D}, \chi)$, and an $\mathcal{F}_{\mathrm{uni}}^{(\varphi)}(\Gamma)$ sampler for $\mathcal{D}$, then quasi-polynomial computing resources suffice to get a bounded-error randomized algorithm for computing χ.

Proposition 5.9. *Consider* $\varphi : \mathbb{N}^{n-1} \to \mathbb{N}$ *superquasi-polynomial i.e. for any* $m \in \mathbb{N}$ *and* $p \in \mathbb{N}[J_0, J_1 \dots J_{n-2}]$ *there is at most a finite number of* $J \in \mathbb{N}^{n-1}$ *s.t.* $\varphi(J) \leq 2^{\lceil \log p(J) \rceil^m}$. *Suppose* $\Gamma_{\mathfrak{R}} = \Gamma^n_{\text{poly}}$. *Let* $\Delta = (\Delta_{\mathfrak{R}}, \Delta_{\mathfrak{A}})$ *be a pair of growth spaces of rank* n *s.t.* $\Delta_{\mathfrak{A}} \subseteq \Gamma_{\mathfrak{A}}$ *and* $1 \in \Delta_{\mathfrak{A}}$. *Consider* $L \subseteq \mathbb{N}^{n-1}$ *and* $\mathcal{D}$ *a word ensemble s.t. given* $K_1, K_2 \in \mathbb{N}^n$, *if* $K_1 \neq K_2$ *then* $\operatorname{supp} \mathcal{D}^{K_1} \cap \operatorname{supp} \mathcal{D}^{K_2} = \varnothing$. *Define* $\chi : \operatorname{supp} \mathcal{D} \to \{0,1\}$ *by requiring that for any* $J \in \mathbb{N}^{n-1}$, $k \in \mathbb{N}$ *and* $x \in \operatorname{supp} \mathcal{D}^{Jk}$, $\chi(x) = \chi_L(J)$. *Assume* σ *is an* $\mathcal{F}^{(\varphi)}_{\text{uni}}(\Gamma)$*-sampler of* $\mathcal{D}$ *and* P *is an* $\mathcal{F}^{(\varphi)}_{\text{uni}}(\Delta)$*-optimal estimator for* $(\mathcal{D}, \chi)$ *s.t.* $\mathrm{a}_\sigma(J,k)$ *and* $\mathrm{a}_P(J,k)$ *don't depend on* k. *Then, there are* $m \in \mathbb{N}$, $p \in \mathbb{N}[J_0, J_1 \dots J_{n-2}]$ *and* $B : \mathbf{1} \xrightarrow{\Gamma} \{0,1\}$ *s.t.* $p \geq 1$, $\mathrm{a}_B(K) = \langle \mathrm{a}_\sigma(K), \mathrm{a}_P(K) \rangle$ *and, defining* $q : \mathbb{N}^{n-1} \to \mathbb{N}$ *by* $q(J) := 2^{\lceil \log p(J) \rceil^m}$

$$\forall J \in \mathbb{N}^{n-1} : \Pr_{y \sim \mathrm{U}_B^{J,q(J)}}[B^{J,q(J)}(y) = \chi_L(J)] \geq \frac{2}{3} \tag{5.31}$$

Proof. Obviously it is enough to construct m, p and B s.t. 5.31 holds for all but a finite number of $J \in \mathbb{N}^{n-1}$. Use Proposition 5.8 to construct $A : \mathbf{1} \xrightarrow{\Gamma} \{0,1\}$. Given any $k \in \mathbb{N}$, define $\omega^k \in \mathcal{P}(\mathbb{N})$ s.t. for some $N \in \mathbb{R}^{>0}$

$$\omega^k(i) := \begin{cases} \frac{N}{i \log i} \text{ if } 2 \leq i < k \\ 0 \text{ if } i < 2 \text{ or } i \geq k \end{cases}$$

Denote $\Gamma^1 := (\Gamma^1_{\text{poly}}, \Gamma^1_0)$. Adapting the standard argument that any computable distribution is samplable, we can construct $\tau : \mathbf{1} \xrightarrow{\Gamma^1} \mathbb{N}$ s.t. $\operatorname{supp} \tau^k_\bullet \subseteq [k]$ and $\mathrm{d}_{\text{tv}}(\tau^k_\bullet, \omega^k) \leq \frac{1}{6}$. Construct $B : \mathbf{1} \xrightarrow{\Gamma} \{0,1\}$ s.t. for any $J \in \mathbb{N}^{n-1}$, $k \in \mathbb{N}$, $y \in \{0,1\}^{\mathrm{r}_\tau(J,k)}$ and $z \in \{0,1\}^*$

$$\mathrm{r}_B(J,k) \geq \mathrm{r}_\tau(k) + \max_{i \in [k]} \mathrm{r}_A(J,i)$$

$$B^{Jk}(y,z) = A^{J,\tau^k(y)}(z_{<\mathrm{r}_A(J,\tau^k(y))})$$

That is, B functions by generating a distribution over numbers up to k that is approximately $\frac{1}{i \log i}$, and then sampling from it to determine how much computing resources to allocate to A, which is a perfect estimator.

We know that for some $M \in \mathbb{R}^{\geq 0}$ and $p \in \mathbb{N}[J_0, J_1 \dots J_{n-2}]$ s.t. $p \geq 1$

$$\sum_{k=2}^{\varphi(J)-1} \frac{\Pr_{z \sim \mathrm{U}_A^{Jk}}[A^{Jk}(z) \neq \chi_L(J)]}{k \log k} \leq M \log \log p(J)$$

Take $m = \lceil \frac{6M}{(\ln 2)^2} \rceil$. We get

$$\mathrm{E}_{k\sim\omega^{q(J)}}[\Pr_{z\sim \mathrm{U}_A^{Jk}}[A^{Jk}(z)\neq\chi_L(J)]] = \frac{\sum_{k=2}^{q(J)-1}\frac{\Pr_{z\sim \mathrm{U}_A^{Jk}}[A^{Jk}(z)\neq\chi_L(J)]}{k\log k}}{\sum_{k=2}^{q(J)-1}\frac{1}{k\log k}}$$

Denote $I := \{J \in \mathbb{N}^{n-1} \mid \varphi(J) < q(J)\}$. We get

$$\forall J \in \mathbb{N}^{n-1}\setminus I : \mathrm{E}_{k\sim\omega^{q(J)}}[\Pr_{z\sim \mathrm{U}_A^{Jk}}[A^{Jk}(z)\neq\chi_L(J)]] \leq \frac{M\log\log p(J)}{\int_2^{q(J)}\frac{\mathrm{d}t}{t\log t}}$$

$$\forall J \in \mathbb{N}^{n-1}\setminus I : \mathrm{E}_{k\sim\omega^{q(J)}}[\Pr_{z\sim \mathrm{U}_A^{Jk}}[A^{Jk}(z)\neq\chi_L(J)]] \leq \frac{M\log\log p(J)}{(\ln 2)^2\log\log q(J)}$$

$$\forall J \in \mathbb{N}^{n-1}\setminus I : \mathrm{E}_{k\sim\omega^{q(J)}}[\Pr_{z\sim \mathrm{U}_A^{Jk}}[A^{Jk}(z)\neq\chi_L(J)]] \leq \frac{M\log\log p(J)}{(\ln 2)^2 m\log\lceil\log p(J)\rceil}$$

$$\forall J \in \mathbb{N}^{n-1}\setminus I : \mathrm{E}_{k\sim\omega^{q(J)}}[\Pr_{z\sim \mathrm{U}_A^{Jk}}[A^{Jk}(z)\neq\chi_L(J)]] \leq \frac{1}{6}$$

$$\forall J \in \mathbb{N}^{n-1}\setminus I : \mathrm{E}_{y\sim \mathrm{U}_\tau^{q(J)}}[\Pr_{z\sim \mathrm{U}_A^{J,\tau^{q(J)}(y)}}[A^{J,\tau^{q(J)}(y)}(z)\neq\chi_L(J)]] \leq \frac{1}{6}+\mathrm{d_{tv}}(\tau_\bullet^{q(J)},\omega^{q(J)})$$

$$\forall J \in \mathbb{N}^{n-1}\setminus I : \Pr_{y\sim \mathrm{U}_B^{J,q(J)}}[B^{J,q(J)}(y)\neq\chi_L(J)] \leq \frac{1}{3}$$

By the assumption on φ, I is a finite set therefore we got the desired result. □

For $n = 2$, we can think of L as a language using *unary* encoding of natural numbers. Proposition 5.9 and Proposition 2.13 imply that if $\Delta_{\mathfrak{A}} = \Gamma_0^n$, σ is uniform, and this language cannot be decided in quasi-polynomial time by a bounded-error randomized algorithm, then there is no $\mathcal{F}_{\mathrm{uni}}^{(\varphi)}(\Delta)$-optimal estimator for $(\mathcal{D},\chi)$.

Thanks to the results of section 4 and Theorem 2.2, these negative results imply non-existence results for $\mathcal{F}^\sharp(\Delta)$-optimal estimators[15] for any distributional estimation problem s.t. a problem admitting a negative result has an appropriate reduction to it.

[15]The need to use $\mathcal{F}^\sharp(\Delta)$-optimal estimators rather than $\mathcal{F}(\Delta)$-optimal estimators arises because the theorems about reductions as we formulated them don't apply to $\mathcal{F}(\Delta)$-optimal estimators with $\Delta = \Gamma_0^n$ or $\Delta = \Gamma_1^n$. This can be overcome by using somewhat more special reductions which still admit a similar completeness theorem, but we omit details in the present work.

5.2 Uniqueness

Since we view optimal polynomial-time estimators as computing "expected values", it is natural to expect that their values only depend on the distributional estimation problem rather than the particular optimal polynomial-time estimator. However, since they are defined via an asymptotic property exact uniqueness is impossible. Instead, different $\mathcal{F}^\sharp(\Gamma)$-optimal estimators have the expectation of the squared difference between their estimates fall fast enough to be in $\mathcal{F}$ (which is an equivalence relation on the set of arbitrary estimators).

Theorem 5.3. *Consider $(\mathcal{D}, f)$ a distributional estimation problem. Assume there is $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t.*

$$\mathcal{D}^K(\{0,1\}^{\leq p(K)}) \equiv 1 \pmod{\mathcal{F}} \tag{5.32}$$

Suppose P and Q are $\mathcal{F}^\sharp(\Gamma)$-optimal estimators for $(\mathcal{D}, f)$. Then

$$\mathrm{E}_{(x,y,z)\sim\mathcal{D}^K\times \mathrm{U}_P^K \times \mathrm{U}_Q^K}[(P^K(x,y) - Q^K(x,z))^2] \equiv 0 \pmod{\mathcal{F}} \tag{5.33}$$

Proof. Construct $S : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded s.t. for any $K \in \mathbb{N}^n$, $x \in \{0,1\}^{\leq p(K)}$, $t \in \operatorname{Im} P^K$ and $z \in \{0,1\}^{\mathrm{r}_Q(K)}$

$$\mathrm{r}_S(K) = \mathrm{r}_Q(K)$$
$$S^K(x,t,z) = t - Q^K(x,z)$$

Construct $T : \{0,1\}^* \times \mathbb{Q} \xrightarrow{\Gamma} \mathbb{Q}$ bounded s.t. for any $K \in \mathbb{N}^n$, $x \in \{0,1\}^{\leq p(K)}$, $s \in \operatorname{Im} Q^K$ and $y \in \{0,1\}^{\mathrm{r}_P(K)}$

$$\mathrm{r}_T(K) = \mathrm{r}_P(K)$$
$$T^K(x,s,y) = P^K(x,y) - s$$

P is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$, therefore

$$\mathrm{E}_{(x,y,z)\sim\mathcal{D}^K\times \mathrm{U}_P^K \times \mathrm{U}_S^K}[(P^K(x,y) - f(x))S^K(x, P^K(x,y), z)] \equiv 0 \pmod{\mathcal{F}}$$

The construction of S and 5.32 give

$$\mathrm{E}_{(x,y,z)\sim\mathcal{D}^K\times \mathrm{U}_P^K \times \mathrm{U}_Q^K}[(P^K(x,y) - f(x))(P^K(x,y) - Q^K(x,z))] \equiv 0 \pmod{\mathcal{F}} \tag{5.34}$$

Q is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, f)$, therefore

$$\mathrm{E}_{(x,z,y)\sim\mathcal{D}^K\times \mathrm{U}_Q^K\times \mathrm{U}_T^K}[(Q^K(x,z)-f(x))T^K(x,Q^K(x,z),y)]\equiv 0 \pmod{\mathcal{F}}$$

The construction of T and 5.32 give

$$\mathrm{E}_{(x,z,y)\sim\mathcal{D}^K\times \mathrm{U}_Q^K\times \mathrm{U}_P^K}[(Q^K(x,z)-f(x))(P^K(x,y)-Q^K(x,z))]\equiv 0 \pmod{\mathcal{F}} \quad (5.35)$$

Subtracting 5.35 from 5.34, we get 5.33. □

The notion of "conditional expected value" introduced in subsection 3.2 allows conditions which are occasionally *false*. In some sense this provides us with well-defined (probabilistic) answers to "what if" questions that are meaningless in formal logic due to the principle of explosion, a concept which was hypothesized to be useful for solving paradoxes in decision theory [19]. However, Theorem 5.3 suggests that the values of an optimal polynomial-time estimator are only meaningful inside $\operatorname{supp}\mathcal{D}^K$ whereas "conditional expected values" require using the word ensemble $\mathcal{D} \mid L$ (see Theorem 3.3) so violation of the condition (i.e. $x \notin L$) means falling outside the support of the word ensemble. On the other hand, we will now show that when the condition is unpredictable with the given amount of computational resources, a stronger uniqueness theorem holds that ensures "counterfactual" values are also stable, although the fall space measuring the difference of the optimal estimators is scaled up by a factor decreasing with the "degree of unpredictability".

Theorem 5.4. *Consider $(\mathcal{D}, f)$ a distributional estimation problem and $L \subseteq \{0,1\}^*$ s.t. for all $K \in \mathbb{N}^n$, $\mathcal{D}^K(L) > 0$. Define $\gamma_L : \mathbb{N}^n \to \mathbb{R}$ by $\gamma_L(K) := \mathcal{D}^K(L)^{-1}$ and $\mathcal{F}_L := \gamma_L\mathcal{F}$. Assume there is $p \in \mathbb{N}[K_0, K_1 \ldots K_{n-1}]$ s.t. 5.32 holds. Let R be an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$. Assume $\epsilon : \mathbb{N}^n \to \mathbb{R}^{>0}$ is s.t. for all $x, y \in \{0,1\}^*$, $R^K(x,y) \geq \epsilon(K)\mathcal{D}^K(L)$. Suppose P and Q are $\mathcal{F}_L^\sharp(\Gamma)$-optimal estimators for $(\mathcal{D} \mid L, f)$. Then*

$$\mathrm{E}_{(x,y,z)\sim\mathcal{D}^K\times \mathrm{U}_P^K\times \mathrm{U}_Q^K}[(P^K(x,y)-Q^K(x,z))^2]\equiv 0 \pmod{\epsilon^{-1}\mathcal{F}_L} \quad (5.36)$$

Proof. R is an $\mathcal{F}^\sharp(\Gamma)$-optimal estimator for $(\mathcal{D}, \chi_L)$, therefore

$$\mathrm{E}_{(x,y,z,w)\sim\mathcal{D}^K\times \mathrm{U}_P^K\times \mathrm{U}_Q^K\times \mathrm{U}_R^K}[(R^K(x,w)-\chi_L(x))(P^K(x,y)-Q^K(x,z))^2] \equiv 0 \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[R^K \cdot (P^K - Q^K)^2] \\ = \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[\chi_L \cdot (P^K - Q^K)^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[R^K \cdot (P^K - Q^K)^2] \\ = \mathcal{D}^K(L)\, \mathrm{E}_{\mathcal{D}^K|L \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[(P^K - Q^K)^2] \pmod{\mathcal{F}}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[\epsilon(K)\mathcal{D}^K(L)(P^K - Q^K)^2] \\ \leq \mathcal{D}^K(L)\, \mathrm{E}_{\mathcal{D}^K|L \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[(P^K - Q^K)^2] \pmod{\mathcal{F}}$$

$$\epsilon(K)\, \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[(P^K - Q^K)^2] \\ \leq \mathrm{E}_{\mathcal{D}^K|L \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[(P^K - Q^K)^2] \pmod{\mathcal{F}_L}$$

Applying Theorem 5.3 to the right hand side, we conclude

$$\epsilon(K)\, \mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[(P^K - Q^K)^2] \equiv 0 \pmod{\mathcal{F}_L}$$

$$\mathrm{E}_{\mathcal{D}^K \times \mathrm{U}_P^K \times \mathrm{U}_Q^K \times \mathrm{U}_R^K}[(P^K - Q^K)^2] \equiv 0 \pmod{\epsilon^{-1}\mathcal{F}_L}$$

□

Theorem 5.4 implies that in simple scenarios, "counterfactual" optimal estimates behave as intuitively expected, assuming L is "sufficiently unpredictable". For example, if there is an efficient algorithm that evaluates f correctly given the promise $x \in L$ then a conditional optimal polynomial-time estimator constructed using Theorem 3.3 will produce approximately the same values as this algorithm whether x is in L or not.

6 Discussion

The motivation for optimal polynomial-time estimators comes from the desire to quantify the uncertainty originating in computational resource bounds. We used this motivation to arrive at an intuitive definition, and proceeded to show the resulting object has many properties of "normal" probability theory, justifying its interpretation as a brand of expected value. Moreover, there are associated concepts of reductions and complete problems analogous to standard constructions in average-case complexity theory.

Thus, the class of distributional estimation problems admitting $\mathcal{F}(\Gamma)$-optimal estimators (or $\mathcal{F}^\sharp(\Gamma)$-optimal estimators) is a natural distributional complexity class. In light of the positive and negative existence results we have demonstrated, these new classes are unlikely to trivially coincide with any of the previously known classes. Mapping the boundary of these classes and understanding their relationships with other classes in average-case complexity theory seems to be ground for much further work. Moreover, it is possible to consider generalizations by including more types of computational resources e.g. space, parallelism and/or non-determinism.

As an example of a natural open problem, consider $(\mathcal{D}_{\mathrm{NP}}, f_{\mathrm{NP}})$, the complete problem for SampNP resulting from Theorem 4.4 with $n = 1$, $r(k) = s(k) = k$, $E = E_{\mathrm{NP}}$ and $\mathfrak{F} = \mathfrak{F}_{\mathrm{NP}}$. Theorem 5.1 implies that e.g. there is an $\mathcal{F}^{(2)}_{\mathrm{uni}}(\Gamma^2_{\mathrm{poly}}, \Gamma^2_{\mathrm{log}})$-optimal estimator for $(\mathcal{D}^\eta_{\mathrm{NP}}, f_{\mathrm{NP}})$. On the other hand, Proposition 5.9 implies that it is unlikely that there is an $\mathcal{F}^{(2)}_{\mathrm{uni}}(\Gamma^2_{\mathrm{poly}}, \Gamma^2_0)$-optimal estimator[16]. This, however, doesn't tell us anything about the existence of an $\mathcal{F}^{(2)}_{\mathrm{uni}}(\Gamma^2_{\mathrm{poly}}, \Gamma^2_1)$-optimal estimator. This question fits naturally into the theme of Impagliazzo's "worlds" [15]: if there is an $\mathcal{F}^{(2)}_{\mathrm{uni}}(\Gamma^2_{\mathrm{poly}}, \Gamma^2_0)$-*perfect* estimator for $(\mathcal{D}^\eta_{\mathrm{NP}}, f_{\mathrm{NP}})$ (a version of Impagliazzo's "Heuristica" which is considered unlikely), then the answer is tautologically positive. However, if there is no such perfect polynomial-time estimator then the optimal polynomial-time estimator may or may not exist, a possible new partition of "worlds"[17].

One area where applying these concepts seems natural is Artificial General Intelligence. Indeed, the von Neumann-Morgenstern theorem shows that perfect rational agents are expected utility maximizers but in general the exact evaluation of expected utility is intractable. It is thus natural to substitute an optimal polynomial-time estimator for utility, as the analogue of expected value in the computationally

[16] More precisely, it cannot exist assuming there is a unary language in NP that cannot be decided by a randomized algorithm in quasi-polynomial time with bounded probability of error.

[17] The relation to the worlds is somewhat disturbed by the role of $O(1)$ advice. We think there is a natural variant of this question that doesn't involve advice but it is out of the present scope.

bounded case. Further illuminating the connection, Theorem 5.2 shows how optimal polynomial-time estimators result from agnostic PAC learning.

Some results we left out of the present work show the existence of systems of optimal polynomial-time estimators that are "reflective" i.e. estimate systems of functions which depend on the estimators themselves. We constructed such systems using the Kakutani-Glicksberg-Fan theorem which requires the use of random advice strings, as in the definition of $\mathcal{F}(\text{M}\Gamma)$-samplers. Such systems can be used to model game theoretic behavior of computationally bounded rational agents, similarly to the use of reflective oracles [9] for unbounded agents.

Finally, we wish to express the hope that the present work will lead to incorporating more concepts from complexity theory into the theory of AGI, serving to create a stronger theoretical foundation for AI in general. The importance of building such a theoretical foundation is enormous since it is necessary to predict and control the outcome of the eventual creation of artificial agents with superhuman intelligence, an event which might otherwise trigger a catastrophe [5].

A Appendix

We review the definitions of hard-core predicate and one-way function and state the Goldreich-Levin theorem.

We will use the notation $\Gamma_{\text{det}} := (\Gamma^1_0, \Gamma^1_0)$, $\Gamma_{\text{rand}} := (\Gamma^1_{\text{poly}}, \Gamma^1_0)$, $\Gamma_{\text{circ}} := (\Gamma^1_0, \Gamma^1_{\text{poly}})$.

Definition A.1. Given $\mathcal{D}$ a word ensemble[18], $f : \operatorname{supp}\mathcal{D} \to \{0,1\}^*$ and $B : \{0,1\}^* \xrightarrow{\Gamma_{\text{det}}} \{0,1\}$, B is a called a *hard-core predicate* of $(\mathcal{D}, f)$ when for any $S : \{0,1\}^* \xrightarrow{\Gamma_{\text{rand}}} \{0,1\}$

$$\Pr_{(x,y)\sim\mathcal{D}^k\times \text{U}^k_S}[S^k(f(x),y) = B^k(x)] \leq \frac{1}{2} \pmod{\mathcal{F}_{\text{neg}}} \tag{A.1}$$

Definition A.2. Given $\mathcal{D}$ a word ensemble, $f : \operatorname{supp}\mathcal{D} \to \{0,1\}^*$ and $B : \{0,1\}^* \xrightarrow{\Gamma_{\text{det}}} \{0,1\}$, B is a called a *non-uniformly hard-core predicate* of $(\mathcal{D}, f)$ when for any $S : \{0,1\}^* \xrightarrow{\Gamma_{\text{circ}}} \{0,1\}$

[18]The standard definition of a hard-core predicate corresponds to the case $\mathcal{D}^k = \text{U}^k$. Here we allow for slightly greater generality.

$$\Pr_{x\sim\mathcal{D}^k}[S^k(f(x)) = B^k(x)] \leq \frac{1}{2} \pmod{\mathcal{F}_{\text{neg}}} \tag{A.2}$$

Definition A.3. $f : \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}^*$ is called an *one-way function* when

(i) There is $p : \mathbb{N} \to \mathbb{N}$ polynomial s.t. $\forall x \in \{0,1\}^* : \mathrm{T}_f(x) \leq p(|x|)$.

(ii) For any $S : \{0,1\}^* \xrightarrow{\Gamma_{\text{rand}}} \{0,1\}^*$

$$\Pr_{(x,y)\sim \mathrm{U}^k \times \mathrm{U}^k_S}[f(S^k(f(x), y)) = x] \equiv 0 \pmod{\mathcal{F}_{\text{neg}}} \tag{A.3}$$

Definition A.4. $f : \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}^*$ is called a *non-uniformly hard to invert* one-way function when

(i) There is $p : \mathbb{N} \to \mathbb{N}$ polynomial s.t. $\forall x \in \{0,1\}^* : \mathrm{T}_f(x) \leq p(|x|)$.

(ii) For any $S : \{0,1\}^* \xrightarrow{\Gamma_{\text{circ}}} \{0,1\}^*$

$$\Pr_{x\sim \mathrm{U}^k}[f(S^k(f(x))) = x] \equiv 0 \pmod{\mathcal{F}_{\text{neg}}} \tag{A.4}$$

It is easy to see that any non-uniformly hard-core predicate is in particular a hard-core predicate and any non-uniformly hard to invert one-way function is in particular a one-way function.

The following appears in [12] as Theorem 7.7. Here we state it in the notation of the present work.

Theorem A.1 (Goldreich-Levin)**.** *Consider a one-way function* $f : \{0,1\}^* \xrightarrow{\text{alg}} \{0,1\}^*$. *Let* $\mathcal{D}^k := \mathrm{U}^{2k}$, $f_{\text{GL}} : \operatorname{supp}\mathcal{D} \to \{0,1\}^*$ *and* $B : \{0,1\}^* \xrightarrow{\Gamma_{\text{det}}} \{0,1\}$ *be s.t. for any* $x, y \in \{0,1\}^k$, $f_{\text{GL}}(xy) = \langle f(x), y\rangle$ *and* $B^k(xy) = x \cdot y$. *Then, B is a hard-core predicate of* $(\mathcal{D}, f_{\text{GL}})$.

There is also a non-uniform version of the theorem which is not stated in [12], but its proof is a straightforward adaptation.

Theorem A.2. *In the setting of Theorem A.1, assume f is non-uniformly hard to invert. Then B is a non-uniformly hard-core predicate of* $(\mathcal{D}, f_{\text{GL}})$.

Funding

This work was partially supported by the Machine Intelligence Research Institute in Berkeley, California.

Acknowledgments

We thank Patrick LaVictoire for many useful discussions and also suggesting some corrections in the paper. We thank Scott Aaronson for reading a draft version of the paper and providing important advice on the form of presentation. We thank an anonymous reviewer, writing by the request of the Open Philanthropy Project, who read a draft version of the paper and provided useful suggestions. We thank Rob Bensinger for helping to polish some of the English. We thank Brian Njenga for locating typos. We thank Scott Garrabrant for useful discussions.

References

[1] Boaz Barak. *A Probabilistic-Time Hierarchy Theorem for "Slightly Non-uniform" Algorithms*, pages 194–208. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[2] Boaz Barak, Ronen Shaltiel, and Avi Wigderson. *Computational Analogues of Entropy*, pages 200–215. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[3] Boaz Barak and David Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. *CoRR*, abs/1404.5236, 2014.

[4] Andrej Bogdanov and Luca Trevisan. Average-Case Complexity. *FNT in Theoretical Computer Science*, 2(1):1–106, 2006.

[5] Nick Bostrom. *Superintelligence: Paths, dangers, strategies*. OUP Oxford, 2014.

[6] Paul Christiano. Non-Omniscience, Probabilistic Inference, and Metamathematics, jun 2014.

[7] A. P. Dawid. The well-calibrated bayesian. *Journal of the American Statistical Association*, 77(379):605–610, 1982.

[8] Abram Demski. Logical Prior Probability. In *Artificial General Intelligence*, pages 50–59. Springer Science + Business Media, 2012.

[9] Benja Fallenstein, Jessica Taylor, and Paul F. Christiano. Reflective Oracles: A Foundation for Game Theory in Artificial Intelligence. In *Logic Rationality, and Interaction*, pages 411–415. Springer Science + Business Media, 2015.

[10] Haim Gaifman. Reasoning with Limited Resources and Assigning Probabilities to Arithmetical Statements. *Synthese*, 140(1/2):97–119, may 2004.

[11] Scott Garrabrant, Siddharth Bhaskar, Abram Demski, Joanna Garrabrant, George Koleszarik, and Evan Lloyd. Asymptotic Logical Uncertainty and The Benford Test. *CoRR*, abs/1510.03370, 2015.

[12] Oded Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, New York, NY, USA, 1 edition, 2008.

[13] Edward A. Hirsch. *Optimal Acceptors and Optimal Proof Systems*, pages 28–39. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[14] Marcus Hutter, John W. Lloyd, Kee Siong Ng, and William T.B. Uther. Probabilities on Sentences in an Expressive Logic. *Journal of Applied Logic*, 11(4):386–420, dec 2013.

[15] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of the 10th Annual Structure in Complexity Theory Conference (SCT'95)*, SCT '95, pages 134–, Washington, DC, USA, 1995. IEEE Computer Society.

[16] Subhash Khot. On the unique games conjecture. In *Proceedings - 25th Annual IEEE Conference on Computational Complexity*, pages 99–121, 2010.

[17] Jack H Lutz. Resource-bounded measure. In *Computational Complexity, 1998. Proceedings. Thirteenth Annual IEEE Conference on*, pages 236–248. IEEE, 1998.

[18] Shai Shalev-Shwartz and Shai Ben-David. *Understanding Machine Learning: From Theory to Algorithms*. Cambridge University Press, New York, NY, USA, 2014.

[19] Nate Soares and Benja Fallenstein. Toward idealized decision theory. *CoRR*, abs/1507.01986, 2015.

[20] Jia Zheng. *A Uniform Min-max Theorem and Characterizations of Computational Randomness*. PhD thesis, Cambridge, MA, USA, 2014. AAI3611601.

 Received 21 November 2017