On Effective Representations of Well Quasi-Orderings

Simon Halfon

universite PARIS-SACLAY

Thèse de doctorat ED STIC, NNT 2018SACLN021

école normale supérieure paris-saclay

On Effective Representations of Well Quasi-Orderings

Thèse de doctorat de l'Université Paris-Saclay
préparée à l'École Normale Supérieure de Cachan
au sein du Laboratoire Spécification & Vérification

Présentée et soutenue à Cachan, le 29 juin 2018, par

Simon Halfon

Composition du jury :

Dietrich Kuske Professeur, Technische Universität Ilmenau	Rapporteur
Peter Habermehl Maître de Conférences, Université Paris-Diderot	Rapporteur
Mirna Dzamonja Professeure, University of East Anglia	Examinatrice
Gilles Geeraerts Associate Professor, Université Libre de Bruxelles	Examinateur
Sylvain Conchon Professeur, Université Paris-Sud	Président du Jury
Philippe Schnoebelen Directeur de Recherche, CNRS	Directeur de thèse
Sylvain Schmitz Maître de Conférences, ENS Paris-Saclay	Co-encadrant de thèse

Acknowledgements

I would like to thank the reviewers of this thesis for their careful proofreading and precious comment. You brought to my attention several flaws, and solving them helped me improving many parts, and gave me a deeper understanding of my results. In particular, this made me found some connections I was not aware of, which gave me a great guideline for my defense.

I also thank members of the jury for doing me the honor of attending to my PhD defense. In particular, special thanks for my PhD advisors for taking me on this three years long journey throughout the world of research. They have always been available for my questions and valued my work. It has been a pleasure working with you two: thank you a million.

I would also like to thank the co-author (and main author) of my first paper: Christoph Haase. You taught me a lot as we were writing this article, and your advice became ground rules for writing this thesis and other papers. It has been a pleasure working with you. It has also been a pleasure working with Dmitry Chistikov who joined us on the journal version of this article, as he had solved our main open problem. I also thank all the people with whom I had the chance to share a publication: Piotr, thank you for inviting me to help you solve your problem. Stefan, and Piotr, thank you for all your precious comments on my talks. Georg: it was a pleasure working with you. I admire your efficiency at solving the problems we were working on, and your efficiency to write a very good paper in a rush (although for you, it was your “most relaxed LICS submission”).

Most generally, thank you to all members of LSV, you all contribute in making this lab a terrific place, and it has truly been a pleasure being around you for the past three years. I remember Alain telling us at a MPRI lecture that LSV has the policy of only hiring nice people: “we would not hire the next Einstein if he was not a friendly person”. Well I have to believe you now Alain. And of all LSV members, I especially thank those that take care of us everyday, and take care of our silly mistakes: Catherine, Virginie, Thida, Imane, Francis, Hugues. Whenever one of us (no name) booked a flight for NYC when the conference only was in the state of New York, tried to print without being connected to the network, deleted files accidentely, came back from conferences without the receipts, or went to summer schools without train tickets: thank you for helping us then.

More generally, I have met a lot of kind and fascinating people during my three-year journey in the world of research. There is a general feeling of being part of the same family, because we are inhabited of the same passion in mathematics and computer

science, and it is quite an enjoyable feeling. I particularly remember the joy I felt being part of event as the 20th anniversary of LSV, the Dagstuhl Seminar on WQOs (thanks to Jean and the organizers for their invitation on such a short notice), or the Bravas kickoff meeting. There were great experiences during which I have learned a lot, and have enjoyed discussion with talented people. This feeling of being part of a worldwide family will be one the aspect I will miss the most as I begin my career as a teacher.

Speaking of teaching, my PhD offered me wonderful opportunities to teach at the ENS Cachan, under the direction of Jean Goubault-Larrecq. Thank you Jean for sharing your teaching experience with me and helping me provide relevant exercises to illustrate your lectures. Thank you to Claudine Picarrony for allowing me to intervene in her lectures for preparation to Agregation, and most of all for her many pieces of advice on what to do after my PhD.

I would also like to thank all my fellow PhD students from LSV, from lunch to gouter, through coffe break and sometimes dinners, for their support throughout the difficult moments of a PhD. Jeremy: thank you for the introductionnary classes in category theory on the way home. Nathan thank you for the circuit complexity class walk through during lunches. Samy, thank you for bringing timed and robust systems to my attention. No I'm kiding, you know very well what I thank you for ;-) Many thanks to Antoine Dallon, whom I shared an office with, and that probably is the most quiet neighbour one could wish for. Now that I am done writing this manuscript, I can help you dig those moats you wanted ! Thanks to Anthony, my other neighbour, for your active participation to this manuscript: first the magnificient symbol $\cap$ (1 brownie point to whoever finds its occurence in the thesis), and later for brining to me a whole new view of the -WQOs. And I thank our older brothers: Marie, Guillaume, Rémi, Lucca: thank you for bringing to my attention that our diet is not healthy. I am writing this line at 9:30 pm at LSV (thank god this is not a ZRR !), just after a dinner out with other Cachannais, and we had a long discussion on where to get dinner, and had the drastic conclusion that there are no ways of eating healthy around that campus, hence the reputation of students from Cachan. I wish to all future students of the resplendent ENS Paris-Saclay that the landscape will be more diverse in Saclay. And finally I thank the youngsters: Adrien, for being my successor in the high concil, Charlie for being my heir to the Advenced Complexity course. Keep the traditions going.

To all the Nadines I did not thank yet, and to those I thanked already, Nadine ! I nadine you with all my nadine: Presidente, Davy, Romaing, Samy, Sarah, Joris, Skippy, Seya, Jeremy, Sushi, Nala, Wasa, ... Thank you for your support during the B-weeks, thank you for keeping me from starvation, thank you for all your help around the house.

Many thanks to my writing companions: Miette, after two bachelors and two masters, you will soon be twice doctor in science ! Any typo in this manuscript can be attributed to Aloha, mistaking my keyboard for a DDR Pad (#Skippy). Thanks to Alpha for sharing his deep understanding of -WQOs, and to Coquillette for biting my power plug. Thanks to Miss and Yang for their discrete presence once in a while.

And of course, I want to thank my family, for always being there for me. There is a running joke in my family that each of my life's "important" moment were shadowed by my older sisters greater achievment. My first day in middle school was my sister's first day in medical studies. I graduated highschool the same year she became "Interne des Hopitaux" (Christian's prounonciation). Some days before my oral exam for ENS, I was driving my three-days-old niece from the hospital where she were born back to her home. Allison, maybe your constant crying at night is the reason I wasn't accepted at Centrale Paris, hence in a sense, this thesis wouldn't have happened without you ! Thank you ! And most recently, my sister was 8-months pregnant for my wedding, and almost couldn't attend it. So sisters, what did you plan for June 2018 ? Or maybe this defense does not count as important: "So, as you know, me and Dad are in Paris on the 9th and 10th of June, could you maybe schedule your defense on the 8th so that your father can be there ?".

And of course, thank YOU, for being there and showing me how to write acknoledgements: thank you, for being you and making me whole.

Contents

Chapter 1

Introduction

Well Quasi-Ordering (WQO) is a notion from order theory that lies between well-orders (ordinals) and well-founded quasi-orderings: a well-order is WQO, and a WQO is well-founded. It enjoys several equivalent definitions (see Section 2.3), and has therefore been introduced several times independently, as people were interested in one of the characterization. Higman [1] studied orderings having the *finite basis property*: every subset has a non-empty but finite set of minimal elements (see (WQO4) in Section 2.3), as a generalization of well-orderings (every subset has exactly one minimal element). In the 1940's, Vazsonyi and Erdös were interested in conjectures of the form of (WQO1), and thus naturally introduced WQOs with this definition. The concept of WQOs has also been introduced as a strengthening of well-founded quasi-orderings: for instance, the powerset of a well-founded order (ordered with the domination ordering, see Section 7.3) may not be well-founded. But it is if the QO one started with is WQO (see (WQO7) in Section 2.3). More generally, WQOs enjoy many more closure properties than well-founded orderings, letting them be easier to work with. This is I think the reason of the success of this notion in many areas of mathematics and computer science: Combinatorics, Topology, Automata Theory and Formal Languages, Proof Theory, Term Rewriting, Graph Theory, Program Verification, and more. See [2] for an early history of the concept and [3] for a recent survey on the use of WQOs in many areas of mathematics and computer science, written as a report of a Dagstuhl seminar bringing together researchers from many different communities of mathematics and computer science around the central notion of WQOs. Note that even though WQOs enjoy closure properties under many natural operations, a *better* notion has been introduced by Nash-Williams in the late 1960's, which enjoys even more closure properties. This notion, *Better Quasi-Orderings* is defined in Section 9.2.

Although WQO have proved their strength in many areas of computer science, our motivations will mainly come from Program Verification. Nonetheless, the results of this thesis are general and may be of interest for any computer scientist working with WQOs.

WQOs in Program Verification The efficiency of well-founded orderings to prove program termination, already suggested by Turing [4], is widely known. It is thus not a surprise that WQOs may be used to show program termination. More generally, several alternative definitions of WQOs (see Section 2.3) contain a flavor of finiteness, which is what makes WQOs powerful objects in computer science.

In the 1990's, Finkel, Schnoebelen, Abdullah and Jonsson introduced a large class of infinite state systems, *Well Structured Transition Systems (WSTS)*, which can be verified using generic methods conceptually similar to the ones used to verify finite state systems (see [5, 6] for surveys). The key ingredient in the notion of WSTS is the presence of a WQO compatible with the structure of the transition system. The finite basis property (cf. above) ensures that some infinite sets of states enjoy finite representations, and under mild effectiveness assumptions, we may perform computations with those sets, ultimately proving verification properties of the system (coverability, termination, boundedness, ...). Last year, the main contributors to this generic framework which has flourished during the last 20 years, have received the CAV award.

Outline. In the first part of this thesis, we define a notion of effectiveness for WQOs, and proceed to prove that a large class of WQOs is effective in this sense. Our notion of effectiveness includes most of the requirements needed for generic algorithms. In the second part, we study some logical aspect of WQOs.

Chapter 2

Basics of Order Theory and Well Quasi-Orderings

This chapter is devoted to defining the terminology we use throughout this manuscript. We also recall well-known facts from order-theory, along with the main ideas for their proofs, which are voluntarily kept concise. For a deeper presentation of these notions, we invite the reader to refer to [7, 2] for instance.

2.1 Preliminaries

Natural Numbers. The set of all natural numbers is denoted $\mathbb{N}$. When used on natural numbers, $\leq$ denotes the usual ordering on $\mathbb{N}$. The finite set $\{1, \ldots, n\}$ will be denoted $[n]$. A *permutation* is a bijection from $[n]$ to $[n]$. The set of all permutations, denoted S_n, is a group, sometimes called the *symmetric group*. It has $n!$ elements, which is asymptotically exponential in n (by Stirling formula: $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$).

Sets. We use standard set-theoretic operations on sets: membership $x \in S$, inclusion $S \subseteq T$, union $S \cup T$, intersection $S \cap T$, set difference $S \setminus T$. Given a set X, the set of all subsets of X is denoted $\mathcal{P}(X)$. When $S \in \mathcal{P}(X)$ and X is clear from the context, the set difference $X \setminus S$, called the *complement* of S and will be denoted $\complement S$. If $\boldsymbol{A}$ is a set of sets, $\bigcup \boldsymbol{A}$ denotes the set $\bigcup_{S \in \boldsymbol{A}} S$ (a notation coming from set-theory).

Relations. A *relation* R on a set X is a subset of $X \times X$. As such, we use set-theoretic operations on relations, e.g. $R \subseteq S$ means $\forall x, y \in X.\ xRy \Rightarrow xSy$, where xRy denotes membership $(x, y) \in R$. Given a relation R on a set X and a function $f : X \to Y$, we also refer to the image of R by f to denote the relation $S \stackrel{\text{def}}{=} \{(f(x), f(y)) \mid x, y \in X \text{ and } xRy\}$.

We sometimes use the functional point of view, for instance the composition of two relations R_1 and R_2 is the relation $R = R_1 \circ R_2$ defined by $xRy \stackrel{\text{def}}{\Leftrightarrow} \exists z.\ xR_1z \wedge zR_2y$.

A relation is:

- *reflexive* if $\forall x \in X.\, xRx$,
- *transitive* if $\forall x, y, z \in X.\, xRy \wedge yRz \Rightarrow xRz$,
- *symmetric* if $\forall x, y \in X.\, xRy \Rightarrow yRx$,
- *antisymmetric* if $\forall x, y \in X.\, (xRy \wedge yRx) \Rightarrow x = y$.

An *equivalence relation* is a reflexive, transitive and symmetric relation. Let E be such a relation on X. Elements x and y in X such that xEy are called *equivalent*. For every $x \in X$, $[x]_E$, or $[x]$ when E is understood, denotes the *equivalence class* of X: $[x] = \{y \in X \mid xEy\}$. We say that x is a representant of $[x]$. Observe that $[x] = [y] \iff xEy$. As a consequence, two equivalence classes are either equal or disjoint. It follows that equivalence classes form a partition of X (conversely, any partition of X defines an equivalence relation).

The *quotient of X by E*, denoted X/E, is the set of equivalence classes of E.

A relation which is reflexive and transitive is called a *quasi-ordering*.

We will often use the abbreviations xRy, z and x, yRz to express $xRy \wedge xRz$ and $xRz \wedge yRz$, respectively.

Sequences. We assume some familiarity with ordinals. Given an ordinal α, we denote by $\boldsymbol{\alpha}$ the set of strictly smaller ordinals, i.e. $\boldsymbol{\alpha} \stackrel{\text{def}}{=} \{\beta \mid \beta < \alpha\}$. A *sequence* over X is a function $\boldsymbol{s} : \boldsymbol{\alpha} \to X$ for some ordinal α. The *length* of a sequence $\boldsymbol{s}$, denoted $|\boldsymbol{s}|$, is the ordinal α, if $\boldsymbol{\alpha}$ is its domain. The only sequence of length 0, denoted ϵ, is also called the *empty sequence*. The set (or class) of sequences of length α is denoted X^α, and $X^{<\alpha} = \bigcup_{\beta<\alpha} X^\beta$. The *concatenation* of two sequences $\boldsymbol{s}$ and $\boldsymbol{t}$ over the same set X of length α and β respectively is the sequence of length $(\alpha + \beta)$ denoted $\boldsymbol{s} \cdot \boldsymbol{t}$ and defined by $(\boldsymbol{s} \cdot \boldsymbol{t})(\gamma) = \boldsymbol{s}(\gamma)$ if $\gamma < \alpha$, and $(\boldsymbol{s} \cdot \boldsymbol{t})(\alpha + \gamma) = \boldsymbol{t}(\gamma)$ if $\gamma < \beta$. This operation is associative.

When $(X, \leq)$ is a quasi-ordered set (see below), sequences are quasi-ordered with the *embedding quasi-ordering*: if $\boldsymbol{s}$ and $\boldsymbol{t}$ are sequences of length α and β respectively, then

$$\boldsymbol{s} \leq \boldsymbol{t} \stackrel{\text{def}}{\Leftrightarrow} \exists f : \boldsymbol{\alpha} \to \boldsymbol{\beta} \text{ strictly increasing} .\, \forall \gamma < \alpha.\, \boldsymbol{s}(\gamma) \leq \boldsymbol{t}(f(\gamma))$$

When $\boldsymbol{s} \leq \boldsymbol{t}$, the function f is called a *witness* of the embedding of $\boldsymbol{s}$ in $\boldsymbol{t}$. A *subsequence* of a sequence $\boldsymbol{t}$ is a sequence $\boldsymbol{s}$ that embeds into $\boldsymbol{t}$ when the order considered on X is the equality.

A sequence is finite if its length is a natural number. The set of finite sequences over X is denoted X^* instead of $X^{<\omega}$, and the embedding quasi-ordering between finite sequences will be denoted $\leq_*$. Finite sequences are often described by the ordered list of their images: $\boldsymbol{u} = x_1 x_2 \cdots x_n \cdots$ where $x_i = \boldsymbol{u}(i-1)$. When X is a finite alphabet (i.e. a finite set ordered with equality), finite sequences over X are often called *finite words*. In Section 11.1, we freely use regular expressions like $(ab)^* + (ba)^*$ to denote regular languages. Given a letter $a \in X$, $|u|_a$ denotes the number of occurrences of a in u. A word $\boldsymbol{v}$ is a *factor* of $\boldsymbol{u}$ if there exist words $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ such that $\boldsymbol{u} = \boldsymbol{u}_1 \boldsymbol{v} \boldsymbol{u}_2$. If furthermore $\boldsymbol{u}_1 = \epsilon$ then $\boldsymbol{v}$ is a *prefix* of u, while if $\boldsymbol{u}_2 = \epsilon$ then $\boldsymbol{v}$ is a *suffix* of $\boldsymbol{u}$.

2.2 Order Theory

Orderings. Let X be a set. A *quasi-ordering* (abbreviated QO) on X is a reflexive and transitive relation, often denoted $\leq$, on X. If $x \leq y$, we say that x is smaller than y, or y is greater than x, which is also denoted $y \geq x$. If $\leq$ is also anti-symmetric, then it is called a *partial-ordering*, or often simply an *ordering*. Every quasi-order $(X, \leq)$ defines a partial-ordering on $X/\equiv$, where $\equiv$ is the equivalence relation defined by $\equiv = \leq \cap \geq$.

A quasi-ordering $(X, \leq)$ is said to be *total*, or *linear*, if every pair of elements is comparable: $\leq \cup \geq = X^2$. If $(X, \leq)$ is not linear, there are some incomparable elements. We define for this cases the relation $\perp$: $x \perp y \overset{\text{def}}{\Leftrightarrow} x \not\leq y \wedge y \not\leq x$. A *chain* Y of $(X, \leq)$ is a subset of X which is totally ordered, that is $(Y, \leq_Y)$ where $\leq_Y$ is the restriction of $\leq$ to Y, is a total (partial-) order. An *antichain* of X is a subset $S \subseteq X$ such that elements of S are pairwise incomparable: $\forall x, y \in S.\ x \neq y \Rightarrow x \perp y$. A QO $(X, \leq)$ is FAC (for *finite antichain condition*) if it has no infinite antichains.

Given a QO $(X, \leq)$, we define its associated *strict ordering*, denoted $<$, by $< = \leq \smallsetminus \equiv$. The QO is *well-founded* if there are no infinite strictly decreasing sequences $x_1 > x_2 > x_3 > \ldots$ in $(X, \leq)$. If it is also antisymmetric and linear, then we say it is a *well-order*. Note that ordinals are exactly equivalence classes of well-orderings for order-isomorphism equivalence relation (cf. next paragraph).

An *extension* of a quasi-ordering $\leq$ on X is a quasi-ordering $\leq'$ also on X such that $\leq \subseteq \leq'$.

An element $x \in X$ is said to be *minimal* in $S \subseteq X$ if for every $y \in S$, $y \leq x \Rightarrow x \leq y$. Equivalently, x is minimal if there are no $y \in S$ such that $y < x$. *Maximal* elements are defined dually.

Mappings between Quasi-Ordered Sets. A mapping $f : X \to Y$ between two quasi-ordered sets $(X, \leq_X)$, $(Y, \leq_Y)$ is:

- *monotone* if for every $x, y \in X$, $x \leq_X y \Rightarrow f(x) \leq_Y f(y)$.
- a *reflection* if for every $x, y \in X$, $f(x) \leq_Y f(y) \Rightarrow x \leq_X y$
- an *embedding* of X into Y if it is a monotone reflection, that is for every $x, y \in X$, $x \leq_X y \iff f(x) \leq_Y f(y)$.
- An *isomorphism* if it is a bijective embedding.

As long as we are only interested in the properties of the quasi-ordering, two isomorphic QOs can be considered identical.

Closed Subsets. Given a subset $S \subseteq X$ of a QO $(X, \leq)$, we define:

- its *downward-closure* $\downarrow S \overset{\text{def}}{=} \{x \in X \mid \exists y \in S.\ x \leq y\}$
- its *upward-closure* $\uparrow S \overset{\text{def}}{=} \{y \in X \mid \exists x \in S.\ x \leq y\}$
- its *strict-downward-closure* $\downarrow_< S \overset{\text{def}}{=} \{x \in X \mid \exists y \in S.\ x < y\}$

- its *strict-upward-closure* $\uparrow_{>} S \stackrel{\text{def}}{=} \{y \in X \mid \exists x \in S.\, x < y\}$

When $(X, \leq)$ is not clear from the context, we use the more explicit notation $\uparrow_X S$ (resp. $\downarrow_X S$), or $\uparrow_{\leq} S$. Sometimes, we only subscript by a symbol that clearly refers to some specific QO, e.g. if the QO is $\leq_{\text{st}}$, we write $\downarrow_{\text{st}}$ instead of $\downarrow_{\leq_{\text{st}}}$.

In the case S is a singleton, we write $\uparrow x$ for $\uparrow\{x\}$ and $\downarrow x$ for $\downarrow\{x\}$, when it causes no confusion (e.g. not when x is itself a set). With this abbreviation, $\uparrow S = \bigcup_{x \in S} \uparrow x$ and $\downarrow S = \bigcup_{x \in S} \downarrow x$. These relations are particularly interesting when S is a finite set.

A subset U of X is said to be *upward-closed* when $U = \uparrow U$. A subset D of X is said to be *downward-closed* when $U = \downarrow U$. We denote the set of all upward-closed sets of X by $\mathit{Up}(X) \subseteq \mathcal{P}(X)$ and the set of all downward-closed sets of X by $\mathit{Down}(X) \subseteq \mathcal{P}(X)$. The sets $\mathit{Up}(X)$ and $\mathit{Down}(X)$ are closed under union and intersection. Besides, upward- and downward-closed sets are dual in the following sense: the complement function from $\mathcal{P}(X)$ to itself is an isomorphism between $(\mathit{Up}(X), \supseteq)$ and $(\mathit{Down}(X), \subseteq)$, and it is an involution. As such, upward- and downward-closed sets will share many property, and we will often talk about *closed subsets* to denote upward- and (respectively) downward-closed sets.

Irreducible Subsets. A subset $S \subseteq X$ is said to be *(up)-directed* if for every $x, y \in S$, there exists $z \in S$ such that $x \leq z$ and $y \leq z$. Similarly, S is said to be *(down)-directed* if for every $x, y \in S$, there exists $z \in S$ such that $x \geq z$ and $y \geq z$. When the adjective *directed* is used alone, it will always mean (up)-directed. A *filter* of X is a non-empty upward-closed (down)-directed subset of X. The set of filters of X is denoted $\mathit{Fil}(X)$. An *ideal* of X is a non-empty downward-closed (up)-directed subset of X. The set of ideals of X is denoted $\mathit{Idl}(X)$. Filters *are not* complements of ideals, and vice versa. Observe that for every $x \in X$, $\uparrow x \in \mathit{Fil}(X)$ and $\downarrow x \in \mathit{Idl}(X)$. Such subsets are respectively called *principal filters* and *principal ideals*.

The main property of filters and ideals is their irreducibility in $\mathit{Up}(X)$ and $\mathit{Down}(X)$ respectively. Formally, an upward-closed set $U \in \mathit{Up}(X)$ is *irreducible* if it is non-empty, and for every $U_1, U_2 \in \mathit{Up}(X)$, $U \subseteq U_1 \cup U_2$ implies that $U \subseteq U_1$ or $U \subseteq U_2$. Similarly, a downward-closed set D is *irreducible* if it is non-empty, and for every $D_1, D_2 \in \mathit{Down}(X)$, $D \subseteq D_1 \cup D_2$ implies $D \subseteq D_1$ or $D \subseteq D_2$. Irreducible sets are those that cannot be written as a finite union of the others: $D \in \mathit{Down}(X)$ is irreducible if and only if for every $D_1, \ldots, D_n \in \mathit{Down}(X)$, $D = D_1 \cup \cdots \cup D_n$ implies $D = D_i$ for some i. The statement also holds for irreducible sets of $\mathit{Up}(X)$.

The following proposition relates irreducibility and directedness:

Proposition 2.2.1. *Filters are exactly the irreducible sets of $\mathit{Up}(X)$ and ideals are exactly the irreducible sets of $\mathit{Down}(X)$.*

Proof. We provide a proof that a downward-closed set of X is an ideal if and only if it is irreducible. The proof for upward-closed sets is dual.

($\Rightarrow$) Let I be an ideal of X and $D_1, D_2 \in \mathit{Down}(X)$ such that $I \subseteq D_1 \cup D_2$. We show that if $I \not\subseteq D_1$, then $I \subseteq D_2$. Let $x \in I \setminus D_1 \subseteq D_2 \setminus D_1$. For any $y \in I$, there exists $z \in I$ such that $z \geq x, y$. Since D_1 is downward-closed and $x \not{}n D_1$, $z \notin D_1$. Therefore $z \in D_2$, and thus $y \in D_2$, since D_2 is downward-closed.

($\Leftarrow$) By contraposition, let $D \in Down(X)$ which is not an ideal, that is there exist $x, y \in D$ such that $\uparrow x \cap \uparrow y \cap D = \emptyset$, or equivalently $D \subseteq \complement(\uparrow x \cap \uparrow y)$. Define $D_1 = \complement \uparrow x$ and $D_2 = \complement \uparrow y$. Then $D_1 \cup D_2 = \complement(\uparrow x \cap \uparrow y)$ and thus $D \subseteq D_1 \cup D_2$. Besides, x and y are incomparable, since otherwise $\max(x, y)$ would belong to $D \cap \uparrow x \cap \uparrow y$. Therefore, $x \in D \smallsetminus D_2$ and $y \in D \smallsetminus D_1$. $\square$

2.3 Well Quasi Orderings

A QO $(X, \leq)$ is a *well-quasi ordering* (WQO for short) if and only if one of the following equivalent statements holds:

(WQO1) Every infinite sequence $x_0, x_1, x_2, \ldots$ has an *increasing pair*, that is a pair $x_i \leq x_j$ for $i < j$. A sequence will be called *good* if it has an increasing pair, and *bad* otherwise. Thus in a WQO, all bad sequences are finite.

(WQO2) Every infinite sequence $x_0, x_1, x_2, \ldots$ has an infinite increasing subsequence: $\exists i_0 < i_1 < \ldots$ such that $x_{i_0} \leq x_{i_1} \leq \ldots$

(WQO3) $(X, \leq)$ is FAC and well-founded.

(WQO4) Every non-empty subset $S \subseteq X$ has a finite basis, that is a finite set B such that $\uparrow B = \uparrow S$. Intuitively, this can be thought of as "S has finitely many minimal elements", which is formally wrong because there might be infinitely many equivalent elements. We will denote by $\min(S)$ any finite basis of S which is minimal for inclusion. Given any two such finite basis B_1 and B_2, there exist a bijection that maps elements B_1 to equivalent elements (for $\leq$) of B_2.

(WQO5) Every upward-closed set $U \in Up(X)$ is a finite union of principal filters.

(WQO6) $(Up(X), \supseteq)$ is well-founded.

(WQO7) $(Down(X), \subseteq)$ is well-founded.

Proof. Of equivalence

(WQO2) $\Rightarrow$ (WQO1): trivial.

(WQO1) $\Rightarrow$ (WQO3): An antichain is a bad sequence, hence cannot be infinite. Similarly, a strictly decreasing sequence is a bad sequence, hence cannot be infinite.

(WQO3) $\Rightarrow$ (WQO2): This is the difficult implication. It relies on the Infinite Ramsey Theorem. Let $(x_n)_{n \in \mathbb{N}}$ be an infinite sequence of elements of X. We color the infinite complete graph $G = (\mathbb{N}, \{\{i, j\} \mid i, j \in \mathbb{N}, i \neq j\})$ with the three colors $\{\leq, >, \perp\}$. As expected, a two-element subset $\{i, j\}$ with $i < j \in \mathbb{N}$ is colored with $\leq$ if $x_i \leq x_j$, with $>$ if $x_i > x_j$, and with $\perp$ otherwise. Now, the Infinite Ramsey Theorem states that G has an infinite monochromatic clique. An infinite clique of G colored with $>$ induces a strictly decreasing infinite subsequence of $(x_n)_{n \in \mathbb{N}}$, which is impossible since $(X, \leq)$ is well-founded. An infinite clique of G colored with $\perp$ induces an infinite antichain in X, which is also impossible. Therefore, there is in G an infinite clique colored with $\leq$, i.e. an infinite increasing subsequence of $(x_n)_{n \in \mathbb{N}}$.

(WQO3) $\Rightarrow$ (WQO4): Let S be a subset of X. Since $(X, \leq)$ is well-founded, S has a non-empty subset M of minimal elements, and $\uparrow M = \uparrow S$. Besides, it is easy to see that if x is minimal in S and $y \equiv x$, then y is minimal as well. It follows that M is a union of equivalence class for $\equiv$. Consider B a set obtained from M by taking exactly one member of each these equivalence class. Of course, $\uparrow B = \uparrow M = \uparrow S$. Moreover, since elements of B are minimal in S but non equivalent, they form an antichain, hence B is finite.

Now, let B_1 and B_2 two finite basis of S that are minimal for inclusion. Let $x \in B_1$. Since $\uparrow B_1 = \uparrow B_2$, there exists $y \in B_2$ such that $y \leq x$, and conversely, there exists $z \in B_1$ such that $z \leq y$. It follows that $z \leq x$. If $z \neq x$, $B_1 \smallsetminus \{x\}$ is still a finite basis of S which is in contradiction with B_1 being minimal. Therefore $z = x$ which means that $x \equiv y$. If there exists $y' \in B_2$ such that $y' \leq x$, the same reasoning leads to $x \equiv y'$, hence $y \equiv y'$, which is impossible by minimality of B_2.

It follows that for every $x \in B_1$, there exists a unique equivalent $y \in B_2$. This provides an injective mapping of elements of B_1 to equivalent elements of B_2. By symmetry between B_1 and B_2, the mapping is actually bijective.

(WQO3) $\Leftarrow$ (WQO4): Since any subset of X has a non-empty subset of minimal elements, $(X, \leq)$ is well-founded. Besides, for any antichain A, $A = \min(A)$, and thus A is finite.

(WQO4) $\Rightarrow$ (WQO5): An upward-closed set U is in particular a subset of X. Therefore there exists a finite basis B such that $\uparrow B = \uparrow U = U$. Since B is finite, $\uparrow B = \bigcup_{x \in B} \uparrow x$ is a finite union.

(WQO4) $\Leftarrow$ (WQO5): Conversely, for an arbitrary subset $S \subseteq X$, any finite decomposition of the upward-closed set $\uparrow S = \bigcup_{i=1}^{n} \uparrow x_i$ provides a finite basis.

(WQO6) $\Leftrightarrow$ (WQO7): follows from the prior observation on $\complement$ being an isomorphism between $(Up(X), \supseteq)$ and $(Down(X), \subseteq)$ (cf. end of paragraph on Closed Subsets).

(WQO2) $\Rightarrow$ (WQO6): given a strictly increasing sequence $U_0 \subsetneq U_1 \subsetneq U_2 \subsetneq \cdots$ of upward-closed sets, define a sequence of elements of X as follows: $x_0 \in U_0$, and for all i, $x_i \in U_i \smallsetminus U_{i-1}$. Such a sequence exists since (U_n) is strictly increasing. Moreover, the sequence (x_n) is bad, hence finite. Indeed, let $i < j$, $x_j \in U_j \smallsetminus U_{j-1}$, and $U_i \subseteq U_{j-1}$, thus $u_j \notin U_i$. But U_i is upward-closed, so $x_i \leq x_j$ would imply $x_j \in U_i$.

(WQO7) $\Rightarrow$ (WQO1): given an infinite sequence $(x_n)_{n \in \mathbb{N}}$ of elements of X, we define a decreasing sequence of downward-closed sets $D_i = \bigcup_{j \geq i} \downarrow x_j$. The sequence $(D_n)_{n \in \mathbb{N}}$ is decreasing for $\subseteq$ by construction. Thus, there exists $i \in \mathbb{N}$ such that $D_i = D_{i+1}$. In particular, $x_i \in D_i = D_{i+1}$ and therefore $x_i \in \downarrow x_j$ for some $j > i$, which is equivalent to $x_i \leq x_j$. $\square$

The property that bad sequences are finite is of course very useful in computer science, for instance in the context of proving termination of programs. However, such a finiteness property already lies in the definition of well-foundedness. What makes WQO a more practical tool than well-founded orderings is that the notion is preserved under many operations on quasi-ordered sets. Cartesian products (with component-wise quasi-ordering [8]) and finite sequences (with the Higman or subword quasi-ordering [1]) are the most prominent examples. In Part I, many such constructions will be presented in details. In addition to these, we would like to mention that several quasi-orderings on trees labeled with elements of a WQO are WQOs themselves. And of course, the famous Robertson-Seymour Theorem states that the minor ordering on graphs (labeled by elements in a WQO) is a WQO [9].

Properties of Closed Subsets of a WQO. The following theorem is due to Bonnet and proved in [10]. Similar proofs can also be found in [11, 12]. To the best of the author's knowledge, the proof presented below is new.

Theorem 2.3.1 (Bonnet)**.** *A QO $(X, \leq)$ is FAC if and only if every downward-closed set of X is a finite union of ideals, if and only if every upward-closed set of X is a finite union of filters.*

Proof. A QO $(X, \leq)$ is FAC if and only if $(X, \geq)$ is FAC. Upward-closed sets of $(X, \leq)$ being downward-closed sets of $(X, \geq)$, and filters of $(X, \leq)$ being ideals of $(X, \leq)$, we only need to show the first equivalence.

($\Leftarrow$) Let $S \subseteq X$ be an infinite subset of X. If the downward-closure $\downarrow S$ has an ideal decomposition $\downarrow S = I_1 \cup \dots \cup I_n$, then there must be infinitely many $x \in S$ that belong to the same ideal I_{i_0}. Take x, y two elements of S that belong to I_{i_0}, by directedness there exists $z \in I_{i_0}$ such that $z \geq x, y$. But $I_{i_0} \subseteq \downarrow S$, therefore there exists $t \in S$ such that $t \geq z \geq x, y$, and S is not an antichain.

($\Rightarrow$) By contraposition, let $D \in Down(X)$ that does not admit a finite ideal decomposition. We apply Zorn's Lemma to the quasi-ordered set $(\mathcal{P}(\mathcal{P}(D) \cap Idl(X)), \leq_c)$, where $\leq_c$ denotes the *covering quasi-ordering* defined by: $\boldsymbol{A} \leq_c \boldsymbol{B}$ iff $\bigcup \boldsymbol{A} \subseteq \bigcup \boldsymbol{B}$ iff $\forall I \in \boldsymbol{A}.\ I \subseteq \bigcup \boldsymbol{B}$. Note that $\mathcal{P}(D) \cap Idl(X) = Idl(D, \leq)$, where $(D, \leq)$ is the QO obtained by restricting $(X, \leq)$ to D (this relies on the fact that D is downward-closed, the structure of the ideals of a restriction is more complex in general, see Section 4.3). Therefore, given $\boldsymbol{A}$ a set of ideals of D, $\bigcup \boldsymbol{A}$ is a downward-closed subset of D, and $\leq_c$ corresponds to inclusion for downward-closed sets.

In order to apply Zorn's Lemma, we show that every chain of $\mathcal{P}(Idl(D))$ has an upper bound. Given such a chain $\boldsymbol{C}$, define $\boldsymbol{A} = \bigcup \boldsymbol{C} \subseteq Idl(D)$. For $\boldsymbol{B} \in \boldsymbol{C}$, $\boldsymbol{B} \leq_c \boldsymbol{A}$ since $\boldsymbol{B} \subseteq \boldsymbol{A}$. Therefore, by Zorn's Lemma, $(\mathcal{P}(\mathcal{P}(D) \cap Idl(X)), \leq_c)$ has a maximal element $\boldsymbol{M} \subseteq Idl(D)$, that is for every $\boldsymbol{A} \subseteq Idl(D)$, $\boldsymbol{M} \not<_c \boldsymbol{A}$. In particular, for any $I \in \boldsymbol{M}$, $\boldsymbol{M} \not<_c (\boldsymbol{M} \smallsetminus \{I\})$, i.e. $\exists K \in \boldsymbol{M}.\ K \not\subseteq \bigcup_{J \in \boldsymbol{M} \smallsetminus \{I\}} J$. Trivially, $K \subseteq \bigcup_{J \in \boldsymbol{M} \smallsetminus \{I\}} J$ for $K \in \boldsymbol{M} \smallsetminus \{I\}$. Therefore, for the above condition to be true, the following must hold: $I \not\subseteq \bigcup_{J \in \boldsymbol{M} \smallsetminus \{I\}} J$. In other words, $\forall I \in \boldsymbol{M}.\ \exists x_I \in I.\ \forall J \in \boldsymbol{M}.\ (J \neq I \Rightarrow x_I \notin J)$. Using the axiom of choice, we can chose such an element x_I for every $I \in \boldsymbol{M}$. The resulting set $\{x_I \mid I \in \boldsymbol{M}\}$ is obviously an antichain of $(X, \leq)$. It remains to show that $\boldsymbol{M}$ is infinite. For this, we show that $\bigcup \boldsymbol{M} = D$, and since we assumed that D cannot be decomposed as a finite union of ideals, it follows that $\boldsymbol{M}$ is infinite. For the sake of contradiction, assume $\bigcup \boldsymbol{M}$ is a strict subset of D. Then let $x \in D \smallsetminus \bigcup \boldsymbol{M}$, we have $\boldsymbol{M} <_c \boldsymbol{M} \cup \{\downarrow x\}$, contradicting the maximality of $\boldsymbol{M}$. $\square$

Since a WQO is in particular a FAC QO, it follows that downward-closed and upward-closed sets of a WQO are finite unions of ideals and filters, respectively. Actually, there is a more direct and much easier proof of this fact in the case of a WQO. For upward-closed sets, the decomposition already follows from (WQO5) above. Note that this even proves that upward-closed sets are finite unions of principal filters, and indeed, all filters are principal in a WQO.

For downward-closed sets, the decomposition can be proved by induction on $(Down(X), \subseteq)$, which is well-founded when $(X, \leq)$ is a WQO (cf. (WQO7)). Actually, the general case is often proved using this special case (cf. [10, 11, 12]).

Note that the situation is not symmetric between upward-closed and downward-closed sets of a WQO: unlike for filters, not all ideals are principal. Indeed, (WQO5) shows that all filters of $(X, \leq)$ are principal when $(X, \leq)$ is a WQO. Therefore, all ideals are principal if and only if $(X, \geq)$ is a WQO. But $\leq$ and $\geq$ are simultaneously WQOs if and only if X is finite.

Even though not all ideals are principal, principal ideals convey the good intuition: an ideal is always the downward-closure $\downarrow x$ of some element x, however sometimes this element x is not in X: it is a limit point. When X is countable, this intuition can be made formal: ideals are exactly the downward-closure of chains. That is, ideals are limits of increasing sequences. More generally, a partially-ordered set $(X, \leq)$ can always be seen as a topological set $(X_a, \mathcal{O})$ equipped with the Alexandroff topology. In this setting, a topological operation called *sobrification* that essentially consists in adding the "missing limits" applied to $(X_a, \mathcal{O})$ corresponds exactly to the set of ideals. When $(X, \leq)$ is WQO, $(X_a, \mathcal{O})$ is Noetherian (for the Alexandroff topology). But topological spaces can be Noetherian for other topologies, in which case they may not correspond to some WQO. Noetherian spaces therefore constitute a generalization of WQOs, closed under more operations (e.g. infinite powerset). For more details, see [13] and references therein.

Cardinalities Let $(X, \leq)$ be a WQO. From the fact that all filters are principal, it follows that $(Fil(X), \subseteq)$ is order-isomorphic to $(X/\equiv, \leq)$, where $\equiv$ is the equivalence relation induced by $\leq$. Besides, the irreducibility of filters (Proposition 2.2.1) entails that $(Up(X), \subseteq)$ embeds in $(\mathcal{P}_f(Fil(X)), \sqsubseteq_{\mathcal{H}})$, where $\mathcal{P}_f$ denotes the finitary powerset and $\sqsubseteq_{\mathcal{H}}$ denotes the *Hoare* quasi-ordering defined by: For $\boldsymbol{A}, \boldsymbol{B} \subseteq \mathcal{P}_f(Fil(X))$, $\boldsymbol{A} \sqsubseteq_{\mathcal{H}} \boldsymbol{B} \overset{\text{def}}{\Leftrightarrow} \forall F \in \boldsymbol{A}.\ \exists F' \in \boldsymbol{B}.\ F \subseteq F'$. Furthermore, $(Up(X), \subseteq)$ is isomorphic to the quotient $\mathcal{P}_f(Fil(X))/\equiv_{\mathcal{H}}$, where $\equiv_{\sqsubseteq_{\mathcal{H}}} = \mathcal{H} \cap \sqsupseteq_{\mathcal{H}}$. More details on the Hoare quasi-ordering are given in Section 7.3.

From this isomorphism, it follows that if $X/\equiv$ is infinite, $Up(X)$ has the same cardinality as X. Since $Down(X)$ is isomorphic to $Up(X)$, it also has the same cardinality. Finally, $(Down(X), \subseteq)$ is isomorphic to $(\mathcal{P}_f(Idl(X))/\equiv_{\mathcal{H}}, \sqsubseteq_{\mathcal{H}})$ (cf. Proposition 2.2.1 as well), and thus $Idl(X)$ also have the same cardinality. If X is finite, all ideals are principal and thus $Idl(X)$ is isomorphic to $X/\equiv$.

Theorem 2.3.1 was originally proved to obtain these results on cardinalities [10]. In this manuscript, we are interested in computability properties of WQOs, therefore all WQOs will be countable (see Section below).

2.4 Notes on Computability

Subsequently, we assume some familiarity with classical computability theory. In this thesis, our aim is to compute operations within quasi-orders. Notably, given a QO $(X, \leq)$, we want to compute mathematical operations in the QOs $(Up(X), \subseteq)$ and

$(Down(X), \subseteq)$.

For the following discussion, let us fix a model of computations, e.g. Turing machines working over a finite alphabet A. In this framework, the notions of decidability and computability are only defined for subsets of A^* and functions from A^* to A^*. Then, what does it mean that $\leq$ is decidable on X, for some QO $(X, \leq)$? To give a meaning to this expression, we encode X into A^*. Formally, this is done by considering a recursive subset $\hat{X}$ of A^* (this is the *syntax* of X) and a function $[\![\cdot]\!]$ from $\hat{X}$ to X (this is the *semantic* of the syntax). Elements of $\hat{X}$ encode elements of X: an element $x \in X$ is encoded (represented) by any $\hat{x} \in \hat{X}$ such that $[\![\hat{x}]\!] = x$. To say that $\hat{X}$ encodes X, we want to make sure that every element of X is actually encoded in $\hat{X}$, that is $[\![\cdot]\!]$ is surjective. However, we don't require the semantic function to be injective, that is an element of X might have several encodings. Note that the semantic is a surjective function from a countable set to X, hence X is countable.

Now, observe that the quasi-ordering $\leq$ on X defines a quasi-ordering $\hat{\leq}$ on $\hat{X}$ by:

$$\mathtt{x} \hat{\leq} \mathtt{y} \overset{\text{def}}{\Leftrightarrow} [\![\mathtt{x}]\!] \leq [\![\mathtt{y}]\!]$$

We can now make formal the statement "$\leq$ is decidable": it is if $\hat{\leq}$ is decidable. Since $\hat{\leq} \subseteq A^* \times A^*$, the statement "$\hat{\leq}$ is decidable" is defined in classical theory of computations. However, the statement "$\leq$ is decidable" is formally defined only once a syntax for elements of X and a semantic function have been fixed.

Definition 2.4.1.

- *Given a set X, we say that $(\hat{X}, [\![\cdot]\!])$ is a* representation *(or an* encoding*) of X if $\hat{X}$ is a recursive subset of A^* and $[\![\cdot]\!]$ is a surjective function from $\hat{X}$ to X.*
- *Given a representation $(\hat{X}, [\![\cdot]\!])$ of a set X, a subset Y of X is said to be decidable if $\{\hat{x} \in \hat{X} \mid [\![\hat{x}]\!] \in Y\}$ is a decidable set of $\hat{X}$.*
- *Given two sets X and Y, and representations $(\hat{X}, [\![\cdot]\!]_X)$ and $(\hat{Y}, [\![\cdot]\!]_Y)$ of these two sets, we say that a function $f : X \to Y$ is computable if there exists a computable (in the sense of the model of computations) function $\hat{f} : \hat{X} \to \hat{Y}$ such that for every $\hat{x} \in \hat{X}$, $[\![\hat{f}(\hat{x})]\!]_Y = f([\![\hat{x}]\!]_X)$.*

According to the equivalence of the main models of computations (Turing machine, Gödel's recursive functions, Church's lambda calculus, . . .), the definition above would be equivalent if we replaced encodings into A^* with encodings into $\mathbb{N}$ for instance.

We will say that relation is decidable if it is decidable as a subset of $X \times X$: classical theory of computations provides ways to encode $X \times X$, or X^*, etc. given an encoding of X. These will be used silently in the remainder of this manuscript. More generally, we will take a step back from the precise model, and only use high-level structures (pairs, lists, trees, ...) to describe the encodings we will use for the sets we will encounter. This approach avoids the burden of dealing with technical encodings into finite words over a finite alphabet (Turing machines) or natural numbers (Gödel's recursive functions) for instance; especially since the encodings we will use will always be very simple.

Remark 2.4.2. *Observe that even if $\leq$ is a partial-ordering on X, $\hat{\leq}$ might not be antisymmetric on $\hat{X}$, because $[\![\cdot]\!]$ is not injective. More precisely, $[\![\cdot]\!]$ is an embedding from $(\hat{X}, \hat{\leq})$ to $(X, \leq)$, but not an isomorphism. The reason why we do not require $[\![\cdot]\!]$ to be injective might become clearer later.*

Given a QO $(X, \leq)$ and an encoding of X, it is natural to ask that $\leq$ is decidable for this encoding. However, we will not require equality to be. This leads to the somewhat strange behavior that given two encodings $\hat{x}, \hat{y} \in \hat{X}$, we cannot tell whether they represent the same element ($[\![\hat{x}]\!] = [\![\hat{y}]\!]$) or only equivalent ones ($[\![\hat{x}]\!] \equiv [\![\hat{y}]\!]$). In particular, an encoding of X that makes the quasi-ordering $\leq$ decidable is also an encoding of $X/\equiv$ that makes the partial-ordering $\leq$ over $X/\equiv$ decidable. More generally, if $(X, \leq_X)$ and $(Y, \leq_Y)$ are two QOs such that there exists a surjective embedding f of X into Y, any encoding of X that makes $\leq_X$ decidable is also a valid encoding of Y that makes $\leq_Y$ decidable: the semantic function for Y is obtained by composing the semantic function for X with f.

Part I

The Ideal Approach to Computing with Closed Sets

Joint work with J.Goubault-Larrecq, P. Karandikar, N. Narayan Kumar and Ph. Schnoebelen

The general idea behind many generic algorithms from WSTS theory is a fix-point computation of an infinite closed subset, e.g. the set of *coverable* configurations. Classically, these algorithms are described in terms of upward-closed sets, that are representable by a finite basis (WQO5). More recently, many results suggested that it was more beneficial to work with downward-closed sets: the *coverability set* of a WSTS is downward-closed, and it is a central object in the theory [14, 15]; and it has been shown that computing with downward-closed sets provides better running-time in practice, notably using acceleration techniques [16, 17, 18, 19, 20, 21, 22, 23].

The issue is that downward-closed sets do not enjoy the same property as upward-closed sets of having a finite basis: for instance in $\mathbb{N}^2$ ordered with the product ordering $\langle n, m\rangle \leq_\times \langle n', m'\rangle \overset{\text{def}}{\Leftrightarrow} n \leq n' \wedge m \leq m'$, the subset $[0, 3] \times \mathbb{N}$ is downward-closed, but cannot be described as the downward-closure of some finite subset. In the particular case of $\mathbb{N}^k$, it has first been observed in [16] that downward-closed sets could be represented as the downward-closure of some finite subset of $(\mathbb{N} \cup \{\omega\})^k$. Later in [19], a similar property has been observed for the set of finite sequences over a finite alphabet, ordered with the embedding relation: downward-closed sets can be represented using *simple regular expressions*. These two positive examples lead to a general solution: the notion of *Adequate Domain of Limits* (see [24]). An adequate domain of limits essentially is a generalization of the two cases above: it is a set of limit elements missing from X to be able to express every downward-closed sets. Assuming the existence of such an adequate domain of limits, generic algorithms computing with downward-closed sets can be designed.

Ideals, a frequently rediscovered concept. Although it has long been known that downward-closed sets of a WQO can be decomposed as finite union of ideals (Theorem 2.3.1), the notion of ideals has only been brought to the domain of Verification quite recently, in [13]. In this article, it is proven that the set of ideals is an adequate domain of limits, and the smallest one, that is any adequate domain of limits embeds the set of ideals. Moreover, the extra elements introduced to handle downward-closed sets of $\mathbb{N}^k$ and A^* are exactly the ideals of these WQOs. This is not the first time the notion of ideals is rediscovered: in [25], one can find a proof that downward-closed sets are union of ideals which uses a completely different terminology.

Since their appearance in the domain of verification, ideals have several times proved themselves to be the right notion. Their structure carries more information than filters, which can be useful to analyze the complexity of algorithms relying on the well-foundedness of $Down(X)$ [26, 27]. Some important results with difficult and adhoc proofs have successfully been rethought in terms of ideals [28, 26], which leaves more options for generalizations. Besides, since ideals are intuitively limit elements of X, the structure of $Idl(X)$ is often close to that of X, this is essential in Section 9.4 for instance. This also offers the possibility to define the *completion* of a WSTS [29], whose states are ideals of the original states. Ideals were also applied to *separability of languages* [30, 31].

Contributions In WSTS theory, the notion of *effective WQO* has almost as many definitions as occurrences. At the very least, elements of an effective WQO can be computationally represented and compared (i.e. $\leq$ is decidable for the chosen representation of elements of X). However, no unified framework has been defined: authors usually simply gather every assumptions they need for the design of their particular algorithm, and later proceed to show that these assumptions are trivially satisfied in their application. Our purpose here is to free people from this burden: we define a notion of effective WQO that should contain most of the ones present in the literature, and prove that a large class of WQOs, notably including most of the natural WQOs encountered in computer science, is effective. Our definition entails the computability of several operations on WQOs and their closed subsets which should be enough for the design of most of the algorithms that use WQOs.

More precisely, our definition assumes that we can represent elements of X, but also ideals of X, and that we can compare them. From there, we can represent upward-closed and downward-closed sets decomposing them in union of filters/ideals. We further assume the computability of all set-theoretic operations: union, intersection and complement.

As stated before, our motivation comes from verification, but the results are applicable anywhere.

Related Work This approach has been developed in [13], and our work is strongly inspired by it. On the one hand, our work is less general: we deal with WQOs and constructions preserving those, while they work with the more general notion of Noetherian spaces, which is preserved under constructions that do not preserve WQOs. On the other hand, we believe our presentation is more suited for computer scientists: it deals more specifically with WQOs, hence requires less knowledge of advanced notions from topology, which also allows us to describe more precisely how to compute set-theoretic operations, and their complexity. That is, we hope our presentation is closer to an actual implementation, and provide relevant insight to this end.

At the end of some sections, we provide references for earlier related results. When no such references are given, it means that our results are novel, as far as we know.

Chapter 3

Ideally Effective Well Quasi-Orders

As mentioned in the previous chapter, our goal is to represent and compute with closed subsets of WQOs. In this chapter, we introduce ideally effective WQOs. The idea is that our definition should meet every ad-hoc assumptions one needs when describing generic algorithms for the class of WSTS for instance. More precisely, we want to be able to compare closed-subset, test membership of an element in a closed subset, and compute unions, intersections and complements of closed subsets.

3.1 Formal Definition

The first step to talk about the computability of some operations over some QO is to fix the representation (see Section 2.4). Here, we are interested in operations over three QOs: $(X, \leq)$, $(Up(X), \subseteq)$ and $(Down(X), \subseteq)$. Usually, upward-closed sets are simply represented through their finite basis, and recently, ideals have proved themselves to be *the right notion* to represent downward-closed sets. We formalize this idea.

Assume we are given a representation for X. Then, since all filters are principal, the same representation can be used for $Fil(X)$, i.e. $\uparrow x$ and x share the same encodings. Now we have seen that upward-closed sets can be decomposed as finite unions of filters, hence we will represent upward-closed sets as collections of filters, e.g. lists (or arrays, or trees, ...) of encodings of elements of X.

Observe that whenever $\leq$ is decidable on X, we can also decide inclusion for filters:

$$\uparrow x \subseteq \uparrow y \iff x \geq y$$

And since filters are irreducible, inclusion of upward-closed sets reduces to a quadratic number of inclusion tests on filters:

$$\bigcup_i \uparrow x_i \subseteq \bigcup_j \uparrow y_j \iff \bigwedge_i \bigvee_j \uparrow x_i \subseteq \uparrow y_j$$

Therefore, from an encoding of X, we can represent in a generic way $Fil(X)$ and $Up(X)$. Moreover, the decidability of $\leq$ entails the decidability of inclusion on both those sets.

Now for downward-closed sets, we wish to do the same: downward-closed sets can be decomposed as finite unions of ideals (Theorem 2.3.1). Unfortunately, there is no generic way to represent ideals from the elements of X. We will therefore need to assume an encoding of ideals.

This is formalized in the following definition.

Definition 3.1.1 (Ideally Effective WQOs)**.** *A WQO* $(X, \leq)$ *further equipped with representations for* X *and* $Idl(X)$ *is* ideally effective *if all the requirements below are satisfied:*

(OD) *The quasi-ordering is decidable.*

(ID) *Ideal inclusion is decidable.*

and the following functions are computable:

(PI) *Principal ideals:* $\left\{ \begin{array}{ccc} X & \to & Idl(X) \\ x & \mapsto & \downarrow x \end{array} \right.$

(CF) *Complementing filters:* $\left\{ \begin{array}{ccc} X & \to & Down(X) \\ x & \mapsto & X \smallsetminus \uparrow x \end{array} \right.$

(CI) *Complementing Ideals:* $\left\{ \begin{array}{ccc} Idl(X) & \to & Up(X) \\ I & \mapsto & X \smallsetminus I \end{array} \right.$

(IF) *Intersecting Filters:* $\left\{ \begin{array}{ccc} X \times X & \to & Up(X) \\ (x, y) & \mapsto & \uparrow x \cap \uparrow y \end{array} \right.$

(II) *Intersecting Ideals:* $\left\{ \begin{array}{ccc} Idl(X) \times Idl(X) & \to & Down(X) \\ (I, J) & \mapsto & I \cap J \end{array} \right.$

An ideally effective WQO $(X, \leq)$ *is moreover said to be* polynomial-time *if there exist polynomial-time procedures for all the operations listed above.*

Some immediate remarks are in order:

- The encodings of $Fil(X)$, $Up(X)$ and $Down(X)$ are the ones obtained generically from encodings of X and $Idl(X)$, as described before the definition

- This formal definition indeed captures what we wanted, all the simple set-theoretic operations on $Up(X)$ and $Down(X)$ that are not explicitly listed follow trivially from the one listed:

  - The counter-part to requirement (PI) for upward-closed set is trivial since filters share a common representation with the elements of X.
  - Membership of an element $x \in X$ in closed subsets reduces to membership in filters and ideals, which itself can be tested by first computing $\uparrow x$ or $\downarrow x$ and using inclusion.

- Union of closed subsets is trivial with our encoding of $Up(X)$ and $Down(X)$.
- Intersections and complements of closed subsets reduce to intersections and complements of filters and ideals.

- Note that if $\leq$ is not antisymmetric, filters of X may have several representations, since $\uparrow x = \uparrow y$ if $x \equiv y$. In other words, the semantic function for filters might not be injective, even when the semantic function for X is.

  Similarly, the encoding of a closed subset is not unique. For instance if $U = \bigcup_i F_i$ is an upward-closed set, encoded as a union of filters, then U can also be encoded by $(\bigcup_i F_i) \cup F$ for any filter F which is a strict subset of one of the F_i.

  However, in the case of closed subset, we can define (almost) canonical representations that are computable from any other representation. Formally, we say that a decomposition $\bigcup_{i \in I} F_i$ of an upward-closed set U is *canonical* if for any $i, j \in I$, $i \neq j$ implies $F_i \not\subseteq F_j$. Testing whether a given representation is canonical is decidable since we can decide inclusion of filters, and if $F_i \subseteq F_j$ for some $i, j \in I$, then F_i can be dropped from the decomposition of U and we obtain a "simpler" encoding of U. By iterating, we eventually compute a canonical representation of U.

  It is not difficult to show that there is exactly one canonical decomposition of U as a union of filters. However, this does not mean that we have found a canonical encoding of U since there might be several encodings for this same decomposition: for instance if encoding unions as list, the order is irrelevant and every permutation of the list gives another encoding of the same decomposition. Moreover, we have seen above that filters may have several encodings, leading to even more possible encodings of the canonical decomposition of U.

  The situation is exactly the same for ideals: there exist a unique canonical decomposition of any downward-closed set D, that is we can write D as a finite union of pairwise incomparable (for inclusion) ideals. However, there might be several encodings of this canonical decomposition.

- The asymmetry in the definition between upward-closed and downward-closed sets is not surprising expected since WQOs are well-founded but the reverse orderings need not be.

Alternative Representations of Closed Subsets As noted before, assuming solely that elements of a WQO $(X, \leq)$ can be represented and the decidability of $\leq$, we can already represent and compare upward-closed sets, using their finite basis. It is then always possible to represent downward-closed sets by their complement. We call it the *excluded minor representation*: a downward-closed set D is represented by the minimal set of elements it does not contain. This may seem simpler than extra assumptions on the representability of ideals, but this representation has some drawbacks. First it breaks the symmetry between upward-closed and downward-closed sets. Moreover, union of downward-closed subsets then corresponds to intersection of upward-closed sets, which may be costly, while we would like union to be the most basic operation on closed subsets. Besides we can show it might not be decidable to distinguish ideals among downward-closed sets with this representation. Sometimes, ideals carry valuable information that may not be directly read on their complement [26, 27].

Another issue is the size of the representations of closed subsets. For instance in Section 6.1, we prove that set-theoretic operations require exponential-time to be computed, by showing that the output of those operations might be exponential. This comes from our representation as union of filters/ideals that can become quite large. Many practical tools suffer from this explosion of the size of the representation of closed subsets, solutions to this problem are investigated in [32].

3.2 Basic Ideally Effective WQOs

We quickly show that the simplest WQOs are ideally effective. They will be used later as building blocks for more complex WQOs.

3.2.1 Finite Quasi-Orderings

The simplest WQOs one can think of probably are *finite alphabets*. They consist of a finite set A ordered with equality. Most of the time it is used as a starting point to build more complex WQOs, as in the case of finite sequences with the Higman ordering (Section 6.1), extensively studied in language theory. It is also used in verification to order states of well-structured transition systems.

The ideals of $(A, =)$ are all principal: indeed since ideals are finite in this case, they have maximal elements, and by directedness the maximal element is unique ($=$ is antisymmetric). More generally, one can show that the ideals of a finite WQO $(X, \leq)$ are all principal, which is no surprise: if X is finite then $(X, \geq)$ is a WQO as well, of which the filters are the ideals of $(X, \leq)$, hence all principal. Moreover, ideal inclusion in this case is the same as the ordering: $\downarrow x \subseteq \downarrow y \iff x \leq y$.

This suggests using the same representations for ideals as for elements, and elements of $(A, =)$ can for instance be represented using natural numbers up to $|A| - 1$. Similarly, for any finite X, we can represent its element using numbers up to $|X| - 1$. We claim that for these representations, $(A, =)$, and more generally any finite WQO $(X, \leq)$, are ideally effective.

(OD) In the case of $(A, =)$, deciding equality is trivial. In the general case, $\leq$ is a finite predicate, hence computable.

(ID) As argued before, inclusion on ideals is the same as the ordering on the elements.

(PI) With our representations, $x \mapsto \downarrow x$ simply is the identity function.

In the case of a finite alphabet, filters are ideals and vice versa: $\uparrow a = \downarrow a = \{a\}$ for any $a \in A$. Therefore, the following equations suffice to conclude:

$$\begin{aligned} \complement\{a\} &= A \smallsetminus \{a\}, \\ \{a\} \cap \{b\} &= \emptyset \quad \text{when } a \neq b, \\ \{a\} \cap \{a\} &= \{a\} \end{aligned}$$

In the case of a finite WQO, the four operations can be performed by brute force enumeration. For instance, to compute $\downarrow x \cap \downarrow y$ it suffices to test whether $z \leq x \wedge z \leq y$ for every $z \in X$.

3.2.2 Natural Numbers

The linear order $(\mathbb{N}, \leq)$ is among the most frequently occurring WQOs in computer science. Observe that since $\leq$ is linear, any downward-closed set is actually an ideal, except the empty set $\emptyset$. There are two kinds of downward-closed sets in $\mathbb{N}$: those that are bounded, i.e. of the form $\downarrow n$, and the whole set $\mathbb{N}$ itself. The first kind constitutes all the principal ideals. The second kind is often denoted $\downarrow \omega$, for instance in [16].

This suggests to represent ideals of $\mathbb{N}$ as natural numbers plus a special symbol ω. Using this representation (and the obvious one for $\mathbb{N}$), $(\mathbb{N}, \leq)$ is ideally effective.

The natural ordering on $\mathbb{N}$ is of course decidable, and ideal inclusion can be decided as follows: principal ideals are compared as the elements, and $\downarrow \omega$ is greater than all the others. Hence, ideals of $(\mathbb{N}, \leq)$ are linearly ordered (and observe that filters are as well), which makes intersections trivial: it consists of the maximum for filters and of the minimum for ideals. Finally, complements are computed as follows:

$$\complement \uparrow(n+1) = \downarrow n \qquad \complement \downarrow n = \uparrow(n+1)$$
$$\complement \uparrow 0 = \emptyset \qquad \complement \downarrow \omega = \emptyset$$

3.2.3 Ordinals

The prior analysis can be extended to an important class of linear WQOs: ordinals. For the rest of this section, we assume basic knowledge of ordinals. Given an ordinal α, we write $\boldsymbol{\alpha}$ for the set of ordinals $\{\beta \mid \beta \leq \alpha\}$, in accordance with the classical set-theoretic construction of ordinals.

Let $(X, \leq) = (\boldsymbol{\alpha}, \leq)$. Once again, X being linearly ordered, its ideals are its downward-closed sets (except $\emptyset$). Therefore, there are three types of ideals:

1. $I = X$,
2. I has a maximal element $\beta \in X$, in which case $I = \downarrow \beta$,
3. Or I has a supremum $\beta \in X \smallsetminus I$, in which case $I = \downarrow_{<} \beta = \boldsymbol{\beta}$.

Note that in the second case, $I = \downarrow \beta = \downarrow_{<} (\beta + 1) = \boldsymbol{\beta + 1}$. Thus every ideal of $(X, \leq)$ is a $\boldsymbol{\beta}$ for some $\beta \in \boldsymbol{\alpha + 1} \smallsetminus 0$, and ideal inclusion coincides with the natural ordering on $\boldsymbol{\alpha + 1}$.

Now, assuming that we can represent elements of X in a way that makes $\leq$ decidable, $(X, \leq)$ is ideally effective. Indeed, a representation for $\boldsymbol{\alpha}$ and a decision procedure for $\leq$ are easily extended to $(\boldsymbol{\alpha + 1}, \leq)$ (the smallest ordinal which is not recursive is a limit ordinal). Therefore, ideal inclusion is decidable for X. Intersections are computable as the maximum for filters, minimum for ideals. Finally, complements are computed as follows:

$$\mathsf{C}\!\uparrow\!\beta = \boldsymbol{\beta} \qquad\qquad \mathsf{C}\boldsymbol{\beta} = \uparrow\!\beta \qquad\qquad \text{for } \beta \in \boldsymbol{\alpha}$$
$$\mathsf{C}\!\uparrow\!0 = \emptyset \qquad\qquad \mathsf{C}\boldsymbol{\alpha} = \emptyset$$

Note that this representation of ideals in the case $\alpha = \omega$ is not the same as the representation for $(\mathbb{N}, \leq)$ given before: in one case we use $\downarrow_< n$ for principal ideals while in the other we use $\downarrow n$.

Remark 3.2.1. *The computability conditions that the ordinal $\boldsymbol{\alpha}$ must satisfy is voluntarily vague. Notation systems for high ordinals can be complicated, and it does not fit our purpose to give a technical and lengthy analysis of this case. We will mostly use the fact that ω^2 is ideally effective in Chapter 8, for which a canonical notation system is well-known and understood: the* Cantor Normal Form *with base ω.*

3.3 Ideally Effective Constructions

One strength of the notion of WQO is that it is preserved under many constructions: Cartesian product (Dickson's Lemma, cf. Section 5.3), finite sequences (Higman's Lemma, cf. Section 6.1), finite trees (Kruskal's Theorem), finite sets (cf. Section 7.3), etc. Many of the WQOs encountered in practice (in verification, graph theory, semantics, logic, …) are actually built by incremental application of such constructions, starting from simple WQOs (essentially the ones seen in the previous section). Therefore, proving that these constructions not only preserve the property of being WQO, but also ideal effectiveness is a powerful way to prove that most of the WQOs used in practice are ideally effective. To this end, we introduce the following notions.

Definition 3.3.1. *A* presentation *of an ideally effective WQO $(X, \leq)$, is a list of:*

- *encodings for X and $Idl(X)$,*
- *algorithms for the seven computable functions required by Definition 3.1.1,*

(XI) — *the ideal decomposition $X = \bigcup_{i<n} I_i$ of X as a downward-closed set,*

(XF) — *as well as its filter decomposition $X = \bigcup_{i<n'} F_i$.*

A presentation is said to be polynomial-time *(resp.* exponential-time*) if all seven algorithms listed above are polynomial-time computable (resp. exponential-time computable).*

Obviously, a WQO is ideally effective if and only if it has a presentation as defined in Definition 3.3.1, and it is a polynomial-time ideally effective WQO if and only if it has a polynomial-time presentation.

The notion of presentations as actual objects is needed because they are the actual inputs of our WQO constructions. This explains why we added (XI) and (XF) in the requirements. For a given $(X, \leq)$, the ideal and filter decompositions of X always exist and requiring them in Definition 3.1.1 would make no sense (constants are always computable). However, these decompositions are needed by algorithms who work uniformly on WQOs given via their presentations, notably to complement the empty upward- or downward-closed subset.

Let us informally call *order-theoretic construction* (construction for short) any operation C that produces a quasi-ordering $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ from given quasi-orderings $(X_1, \leq_1), \ldots, (X_n, \leq_n)$. In subsequent sections, C will be instantiated with very well-known constructions, such as Cartesian product with component-wise ordering, finite sequences with Higman's ordering, finite sets with the Hoare quasi-ordering, and so on. In practice, we will always have $n = 1$ or 2. We also say that an order-theoretic construction preserves WQO if $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ is a WQO whenever $(X_1, \leq_1), \ldots, (X_n, \leq_n)$ are. The constructions we just mentioned are well-known to be WQO-preserving. We extend this concept to ideally effective WQOs:

Definition 3.3.2. *An order-theoretic WQO-preserving construction C is said to be* ideally effective *if, for every ideally effective WQOs $(X_1, \leq_1), \ldots, (X_n, \leq_n)$,*

- *$C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ is ideally effective.*
- *A presentation of $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ is computable from presentations of the ideally effective WQOs $(X_i, \leq_i)$ ($i = 1, \ldots, n$).*

Construction C is moreover said to be polynomial-time *if a polynomial-time presentation of $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ is computable from polynomial-time presentations of the ideally effective WQOs $(X_i, \leq_i)$ ($i = 1, \ldots, n$).*

Note that a construction C being polynomial-time says nothing about the complexity of producing the polynomial-time presentation of $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ from polynomial-time presentations of the $(X_i, \leq_i)$.

In the following chapters, we prove many of the common WQO-preserving constructions to be ideally effective. This proves that most of the WQOs we use in practice are ideally effective. But it also proves that procedures to compute set-theoretic operations in these WQOs can themselves be automatically computed. Furthermore, for constructions that are not polynomial, we provide exponential lower bounds.

Chapter 4

Generic Constructions on WQOs

Before we proceed to show that natural order-constructions are ideally effective (in the sense of Definition 3.3.2), we study three more abstract transformations that will be useful in several subsequent chapters: in the first section we identify conditions for the extension of an ideally effective WQO to be ideally effective as well, we then study the particular case of a quotient under an equivalence relation. Finally, we identify conditions for the subset of an ideally effective WQO to be ideally effective as well.

4.1 Extension of a WQO

Let $(X, \leq)$ be a WQO and let $\leq'$ be an extension of $\leq$, as defined in Section 2.2. Then $(X, \leq')$ is also a WQO: an increasing pair for $\leq$ is in particular an increasing pair for $\leq'$. In this section, we investigate the ideals of $(X, \leq')$ and present sufficient conditions for $(X, \leq')$ to be ideally effective, assuming $(X, \leq)$ is.

Note that $D \in \mathit{Down}(X, \leq)$ might not be downward-closed for $\leq'$. However, directedness is preserved. In the other direction, $\mathit{Down}(X, \leq') \subseteq \mathit{Down}(X, \leq)$, but a directed set for $\leq'$ might not be directed for $\leq$. This observation leads to the following proposition:

Proposition 4.1.1. *Given a WQO $(X, \leq)$ and an extension $\leq'$ of $\leq$, the ideals of $(X, \leq')$ are exactly the downward closures under $\leq'$ of the ideals of $(X, \leq)$. That is,*

$$\mathit{Idl}(X, \leq') = \{\downarrow_{\leq'} I \mid I \in \mathit{Idl}(X, \leq)\} .$$

Proof. $(\supseteq)$: Let I be an ideal under $\leq$. Even though I may not be downward-closed in $(X, \leq')$, it is still directed. From there, it is easy to establish that $\downarrow_{\leq'} I$ is directed as well, non empty, and obviously downward-closed for $\leq'$. Thus it is an ideal of $(X, \leq')$.

$(\subseteq)$: Let J be an ideal of $(X, \leq')$. Although J may not be directed in $(X, \leq)$, it is still downward-closed under $\leq$, hence it can be decomposed as a finite union of ideals of $(X, \leq)$: $J = I_1 \cup \cdots \cup I_n$. Then $J = \downarrow_{\leq'} J = \downarrow_{\leq'} I_1 \cup \cdots \cup \downarrow_{\leq'} I_n$. Now by irreducibility of ideals, we have $J = \downarrow_{\leq'} I_i$ for some $i \in [n]$. □

Assuming we have a representation for X and $Idl(X, \leq)$, the proposition above suggests to represent ideals of $(X, \leq')$ using the same representation as for ideals of $(X, \leq)$, but changing the semantic function: an encoding of $I \in Idl(X, \leq)$ can also represent the ideal $\downarrow_{\leq'} I \in Idl(X, \leq')$. The proposition ensures we can encode every ideals of $Idl(X, \leq')$ this way. Note that there might be several ideals I of $(X, \leq)$ representing the same ideal $\downarrow_{\leq'} I$ of $(X, \leq')$: the representation of an ideal may not be unique.

Of course, given two ideals $I, J \in Idl(X, \leq)$, $I \subseteq J \Rightarrow \downarrow_{\leq'} I \subseteq \downarrow_{\leq'} J$. Unfortunately, the converse is not true. Actually, we can show that with the chosen representation of ideals of $(X, \leq')$, ideal effectiveness of $(X, \leq)$ does not imply ideal effectiveness of $(X, \leq')$: already ideal inclusion can become undecidable. This is proved in Section 8.2. Lexicographic product will provide a more natural example of extension that fails to be ideally effective (see Section 5.4).

Therefore, to obtain effectiveness results on $(X, \leq')$ we need to make some computability assumptions on $\leq'$.

Theorem 4.1.2. *Let $(X, \leq)$ be an ideally effective WQO and $\leq'$ an extension of $\leq$. Then, $(X, \leq')$ is ideally effective for the aforementioned encodings of X and $Idl(X, \leq')$, whenever the following functions are computable:*

$$\begin{array}{rrl} \mathcal{C}l_{\mathrm{I}} & : Idl(X, \leq) & \to Down(X, \leq) \\ & I & \mapsto \downarrow_{\leq'} I \end{array} \qquad \begin{array}{rrl} \mathcal{C}l_{\mathrm{F}} & : (X, \leq) & \to Up(X, \leq) \\ & x & \mapsto \uparrow_{\leq'} x \end{array}$$

Moreover, under these assumptions, a presentation of $(X, \leq')$ can be computed from a presentation of $(X, \leq)$ and algorithms realizing $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$. Furthermore, given polynomial-time algorithms for $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$, and if the presentation of $(X, \leq)$ is polynomial-time, then the compute presentation of $(X, \leq')$ is polynomial-time.

Note that if $I \in Idl(X, \leq)$, then $\downarrow_{\leq'} I$ is also downward-closed for $\leq$ and thus can be represented as a downward-closed set of $(X, \leq)$. It is precisely this representation that the function $\mathcal{C}l_{\mathrm{I}}$ outputs. Same goes for $\mathcal{C}l_{\mathrm{F}}$: $\uparrow_{\leq'} x \in Up(X, \leq)$. Observe that to obtain a more symmetrical situation, we could have defined $\mathcal{C}l_{\mathrm{F}}$ on filters of $(X, \leq)$ by: $\mathcal{C}l_{\mathrm{F}}(F) = \uparrow_{\leq'} F$. But since filters are principal, $F = \uparrow x$ for some $x \in X$, and the expression $\uparrow_{\leq'}(\uparrow x)$ is more simply written as $\uparrow_{\leq'} x$.

Note that using functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$, it is possible to compute the downward and upward closure under $\leq'$ of arbitrary downward- and upward-closed sets for $\leq$ using the canonical decompositions: $\downarrow_{\leq'}(I_1 \cup \cdots \cup I_n) = (\downarrow_{\leq'} I_1) \cup \cdots \cup (\downarrow_{\leq'} I_n)$ and $\uparrow_{\leq'}(\uparrow x_1 \cup \cdots \cup \uparrow x_n) = \uparrow_{\leq'} x \cup \cdots \cup \uparrow_{\leq'} x_n$.

Proof. We proceed to show that $(X, \leq')$ is ideally effective.

(OD): One can tests $x \leq' y$, since this is equivalent to $y \in \mathcal{C}l_{\mathrm{F}}(x)$. Alternatively, $x \leq' y$ can also be tested using the function $\mathcal{C}l_{\mathrm{I}}$ instead of $\mathcal{C}l_{\mathrm{F}}$: $x \leq' y \iff x \in \mathcal{C}l_{\mathrm{I}}(\downarrow_{\leq} y)$.

(ID): Ideal inclusion can be decided using $\mathcal{C}l_{\mathrm{I}}$ and the inclusion test for downward-closed sets of $(X, \leq)$: $\downarrow_{\leq'} I_1 \subseteq \downarrow_{\leq'} I_2 \Leftrightarrow I_1 \subseteq \mathcal{C}l_{\mathrm{I}} I_2$.

(PI): The principal ideal $\downarrow_{\leq'} x$ of $(X, \leq')$ is represented by $\downarrow_{\leq} x$, since $\downarrow_{\leq'}(\downarrow_{\leq} x) = \downarrow_{\leq'} x$.

(CF): For $x \in X$, the filter complement $X \smallsetminus \uparrow_{\leq'} x$ is $X \smallsetminus \mathcal{C}l_{\mathrm{F}}(x)$ which can be computed, using (CF) and (II) for $(X, \leq)$, as a downward-closed set in $(X, \leq)$. This is represented by an ideal decomposition $D = \bigcup_{i<n} I_i$ which is canonical in $(X, \leq)$ but not necessarily in $(X, \leq')$ since one may have $\downarrow_{\leq'} I_i \subseteq \downarrow_{\leq'} I_j$ for $i \neq j$. However, extracting the canonical ideal decomposition wrt. $\leq'$ can be done using (ID) for $(X, \leq')$.

(II): Intersection of ideals is computed with $\downarrow_{\leq'} I_1 \cap \downarrow_{\leq'} I_2 = \mathcal{C}l_{\mathrm{I}}(I_1) \cap \mathcal{C}l_{\mathrm{I}}(I_2)$. Here again, this result in an ideal decomposition that is canonical for $\leq$ but not for $\leq'$ until we process it as done for (CF).

(CI), (IF) : dual operations are obtained similarly.

With algorithms for the closure functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$, the presentation above is computable from a presentation of $(X, \leq)$. Moreover, this presentation is obviously polynomial-time when algorithms for $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ and the presentation of $(X, \leq)$ are polynomial-time.

Regarding (XF) and (XI), we note that filter and ideal decompositions of X for $\leq$ are also valid decompositions for $\leq'$. However, these decompositions might not be canonical for $\leq'$ even if they are for $\leq$, in which case the canonical decompositions can be obtained using (OD) and (ID), as usual.

□

Observe that in the presentation of $(X, \leq')$ described in the proof above, we often have to compose functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ with operations in $(X, \leq)$. When everything is polynomial-time, the composition remains polynomial-time. However, when both operations in $(X, \leq)$ and functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ are exponential, it might lead to doubly exponential procedures. The following Lemma gives sufficient conditions for $(X, \leq')$ to be an exponential-time ideally effective WQO. It will be used several times in subsequent sections.

Lemma 4.1.3. *Let $(X, \leq)$ be an ideally effective WQO and $\leq'$ an extension of $\leq$. We denote by $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ the functions from Theorem 4.1.2. Assume the following conditions:*

1. *The WQO $(X, \leq)$ is an exponential-time ideally effective WQO,*

2. *Function $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ can be computed in exponential-time,*

3. *For every $x \in X$, every filter from the decomposition of $\mathcal{C}l_{\mathrm{F}}(x)$ is of polynomial size in $|x|$.*

4. *For every $I \in Idl(X, \leq)$, every ideal from the decomposition of $\mathcal{C}l_{\mathrm{I}}(I)$ is of polynomial size in $|I|$.*

Then, $(X, \leq')$ *is an exponential-time ideally effective WQO.*

The notion of size we use comes from the encoding: the size of an object is the size of its representation (formally the lemma should be stated with encodings and semantic functions ...).

Proof. We simply show that the presentation of $(X, \leq')$ described in the proof of Theorem 4.1.2 is exponential-time (instead of the *a priori* doubly-exponential upper bound).

We only present the proof for (IF), the idea being the same for the six other procedures.

Given $u, v \in X$, we have:

$$\begin{aligned}
\uparrow_{\leq'} u \cap \uparrow_{\leq'} v &= \mathcal{C}l_{\mathrm{F}}(u) \cap \mathcal{C}l_{\mathrm{F}}(v) \\
&= (\uparrow u_1 \cup \dots \cup \uparrow u_n) \cap (\uparrow v_1 \cup \dots \cup \uparrow v_m) \\
&= \bigcup_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \uparrow u_i \cap \uparrow v_j
\end{aligned}$$

where $(\uparrow u_1 \cup \dots \cup \uparrow u_n)$ is the filter decomposition in $(X, \leq)$ of $\mathcal{C}l_{\mathrm{F}}(u)$ (and respectively for v), and where n and m are at most exponential in $|u|$ and $|v|$, respectively. Now, since $|u_i|$ and $|v_j|$ are polynomial in $|u|$ and $|v|$, $\uparrow u_i \cap \uparrow v_j$ can be computed in time exponential in $|u|$ and $|v|$, and finally, computing $\uparrow_{\leq'} u \cap \uparrow_{\leq'} v$ reduces to a quadratic number of exponential operations. $\square$

4.2 Quotienting under a Compatible Equivalence

We now apply the results of Section 4.1 to the most commonly encountered case of extensions: quotient under an equivalence relation. Given $(X, \leq)$ a WQO and E an equivalence relation on X such that $\leq \circ E = E \circ \leq$, define $\leq_E = \leq \circ E = E \circ \leq$. It is a relation on X, which we may see as a relation on the quotient X/E if convenient (hence the name of the section). Here, $\circ$ denotes the composition of relations, defined as follows: for all $x, y \in X$, $xR \circ Sy$ if and only if there exists z such that xRz and zSy.

The relation $\leq_E$ is clearly reflexive, and is transitive since

$$\leq_E \circ \leq_E = (\leq \circ E) \circ (\leq \circ E) = \leq \circ \, (E \circ \leq) \circ E = \leq \circ \, (\leq \circ \, E) \circ E = \leq \circ \, E = \leq_E$$

Observe that $\leq_E$ is an extension of $\leq$, and thus results on quotients can be seen as an application of Section 4.1. However, since quotients are of such importance in computer science (and used more often than mere extensions), we reformulate Theorem 4.1.2 in this specific context: functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ take an interesting form. As in the case of extensions, elements and ideals of $(X, \leq_E)$ will be represented using the data structures coming from a presentation of $(X, \leq)$.

Theorem 4.2.1. *Let* $(X, \leq)$ *be an ideally effective WQO and* E *be an equivalence relation on* X *compatible with* $\leq$*. Then,* $(X, \leq_E)$ *is ideally effective for the aforementioned data structures of* X *and* $Idl(X, \leq_E)$*, whenever the following functions are* *computable:*

$$\mathcal{C}l_{\mathrm{I}} \;:\; \mathit{Idl}(X,\le) \;\to\; \mathit{Down}(X,\le) \qquad\qquad \mathcal{C}l_{\mathrm{F}} \;:\; (X,\le) \;\to\; \mathit{Up}(X,\le)$$
$$I \;\mapsto\; \overline{I} \qquad\qquad\qquad\qquad x \;\mapsto\; \uparrow\overline{x}$$

where, given $S \subseteq X$, $\overline{S}$ denotes the closure under E of S, i.e., $\overline{S} \stackrel{def}{=} \{y \mid \exists x \in S : x\ E\ y\}$. In particular, $\overline{x}$ simply is the equivalence class of x.

Moreover, under these assumptions, we can compute a presentation of $(X, \le_E)$ from a presentation of $(X, \le)$.

Proof. In the light of Theorem 4.1.2, it suffices to show $\downarrow_{\le_E} F = \overline{F}$ and $\downarrow_{\le_E} I = \overline{I}$ for any filter F and any ideal I of $(X, \le)$. The first equality follows from $\le_E = \le \circ\, E$ while the second comes from $\le_E = E \circ \le$. This is why we introduced the compatibility condition $\le \circ\, E = E \circ \le$. ☐

In particular, we see that the ideals of $(X, \le_E)$ are exactly the closures under E of the ideals of $(X, \le)$. That is, $\mathit{Idl}(X, \le_E) = \{\overline{I} : I \in \mathit{Idl}(X, \le)\}$.

4.3 Induced WQOs

Let $(X, \le)$ be a WQO. A subset Y of X (not necessarily finite) induces a quasi-ordering $(Y, \le \cap\, Y \times Y)$ which is also WQO. In this section, we investigate the ideal effectiveness of this WQO.

Any subset $S \subseteq X$ induces a subset $Y \cap S$ in Y. Obviously, if S is upward-closed (or downward-closed) in X, then it induces an upward-closed (resp. downward-closed) subset in Y. However an ideal I or a filter F in X does not always induce an ideal or a filter in Y. In the other direction though, if $J \in \mathit{Idl}(Y)$, the downward closure $\downarrow_X J$ is an ideal of X. Therefore, to describe the ideals of Y, we need to identify those ideals of X that are of the form $\downarrow_X J$ for some ideal J of Y. This is captured by the following notion:

Definition 4.3.1. *Given a WQO $(X, \le)$ and a subset Y of X, we say that an ideal $I \in \mathit{Idl}(X)$ is* in the adherence *of Y if $I = \downarrow_X (I \cap Y)$.*

In particular this implies that $I \subseteq \downarrow_X Y$ (we say that I is "below Y") and $I \cap Y \neq \emptyset$ (we say that I is "crossing Y"). The converse implication does not hold, as witnessed by $X = \mathbb{N}$, $Y = [1,3] \cup [5,7]$ and $I = \downarrow 4$.

We now show that the ideals of Y are exactly the subsets induced by ideals of X that are in the adherence of Y.

Theorem 4.3.2. *Let $(X, \le)$ be a WQO and Y be a subset of X. A subset J of Y is an ideal of Y if and only if $J = I \cap Y$ for some $I \in \mathit{Idl}(X)$ in the adherence of Y. In this case, $I = \downarrow_X J$, and is thus uniquely determined from J.*

Proof. $(\Rightarrow)$: If $J \in \mathit{Idl}(Y)$ then $I \stackrel{\text{def}}{=} \downarrow_X J$ is directed hence is an ideal of X. Clearly, $J = I \cap Y$, so I is in the adherence of Y.
$(\Leftarrow)$: If $I \in \mathit{Idl}(X)$ is in the adherence of Y then $J \stackrel{\text{def}}{=} I \cap Y$ is non-empty (since I is

crossing Y) and it is directed since for any $x, y \in J$ there is $z \in I$ above x and y, and $z \leq z'$ for some $z' \in J$ since I is below Y.

Uniqueness is clear since the compatibility assumption "$I = \downarrow_X(I \cap Y)$" completely determines I from the ideal $J = I \cap Y$ it induces. $\square$

An alternative definition of *adherence* often found in the literature (e.g. in [28, 30]) is the following one: an ideal $I \in \mathit{Idl}(X)$ is in the adherence of Y if and only if there exists a directed subset $\Delta \subseteq Y$ such that $I = \downarrow_X \Delta$. The two definitions are equivalent [30, Lemma 14], so that, notably, Theorem 4.3.2 extends Lemma 4.6 from [28].

that the two notions of adherence coincide.
$(\Rightarrow)$: Assume $I = \downarrow_X(I \cap Y)$. We show that $\Delta = I \cap Y$ is directed: let $x, y \in \Delta \subseteq I$, since I is directed, there exists $z \in I$ such that $z \geq x, y$. But since $I = \downarrow_X \Delta$, there exists $z' \in \Delta$ such that $z' \geq z \geq x, y$, which proves that Δ is directed.
$(\Leftarrow)$: Assume that there exists a directed subset $\Delta \subseteq Y$ such that $I = \downarrow_X \Delta$. Then $\downarrow_X(I \cap Y) = \downarrow_X(\downarrow_X \Delta \cap Y) = \downarrow_X(\Delta \cap Y) = \downarrow_X \Delta = I$. $\square$

Similarly, we can define a notion of adherence for filters. However, in this case, the condition $F = \uparrow_X(F \cap Y)$ for some filter $F = \uparrow x$ is actually equivalent to $x \in Y$ (actually to $x' \in Y$ for some $x' \equiv_X x$ when $\leq$ is not antisymmetric). In other words, filters in the adherence of Y are exactly filters of the form $\uparrow y$ for some $y \in Y$. This is no surprise: $(Y, \leq)$ is a WQO and therefore, its filters are principal.

Assuming that $(X, \leq)$ is an ideally effective WQO, and given $Y \subseteq X$, we can simply represent elements of Y by restricting the data structure for X to Y. This requires that Y is a recursive set. Alternatively, Theorem 4.3.2 suggests that we represent ideals of Y as ideals of X that are in the adherence of Y. This requires that we can decide membership in the adherence of Y. As in the case of extensions, the ideal effectiveness of $(Y, \leq)$ does not always follow from the ideal effectiveness of $(X, \leq)$ (see Section 8.4). We therefore have to introduce extra assumptions.

Theorem 4.3.3. *Let $(X, \leq)$ be a WQO and $Y \subseteq X$. Then $(Y, \leq)$ is ideally effective (for the aforementioned representations) provided:*

- *membership in Y is decidable over (the representation for) X,*
- *the following functions are computable:*

$$\begin{array}{llll} \mathcal{S}_\mathrm{I} & : \mathit{Idl}(X, \leq) & \to \mathit{Down}(X, \leq) \qquad \mathcal{S}_\mathrm{F} & : \mathit{Fil}(X, \leq) \to \mathit{Up}(X, \leq) \\ & \quad I & \mapsto \downarrow_X(I \cap Y) \qquad\qquad & \quad F \mapsto \uparrow_X(F \cap Y) \end{array}$$

Moreover, in this case, a presentation of $(Y, \leq)$ can be computed from a presentation of $(X, \leq)$. Furthermore, if functions $\mathcal{S}_\mathrm{I}$ and $\mathcal{S}_\mathrm{F}$ are computable in polynomial-time, and $(X, \leq)$ is a polynomial-time ideally effective WQO, then so is $(Y, \leq)$.

The rest of this subsection is dedicated to the proof of this theorem.

First, let us mention that our first assumption implies that we have a data structure for elements of Y and that thanks to function $\mathcal{S}_\mathrm{I}$, we can decide whether an ideal I of X is in the adherence of Y: it suffices to check that $\mathcal{S}_\mathrm{I}(I) = I$.

Let us prove that $(Y, \leq)$ is ideally effective.

(OD): since $\leq$ is decidable on X, its restriction to Y is still decidable.

(ID): Given two ideals I_1, I_2 that are in the adherence of Y, $I_1 \cap Y \subseteq I_2 \cap Y \iff I_1 \subseteq I_2$. The left-to-right implication uses that $I_i = \downarrow_X (I_i \cap Y)$. Therefore, inclusion for ideals of Y can be implemented by relying on (ID) for X.

(PI): if $y \in Y$, then $\downarrow_X y$ is adherent to Y and $\downarrow_X y \cap Y = \downarrow_Y y$.

For the four remaining operations, we need to be able to compute a representation of $D \cap Y$ and $U \cap Y$ for $D \in \mathit{Down}(X)$ and $U \in \mathit{Up}(X)$.

Lemma 4.3.4. *Let $D \in \mathit{Down}(X)$. The canonical decomposition of $\downarrow_X (D \cap Y)$ (as a downward-closed set of X) is a canonical representation of $D \cap Y$ (as a downward-closed set of Y).*

Proof. Let $\bigcup_i I_i$ be the *canonical* decomposition of $\downarrow_X (D \cap Y)$. Remember that an ideal J of Y is represented by the unique ideal I of X which is in the adherence of Y such that $J = I \cap Y$. Thus, stating that $\bigcup_i I_i$ is a canonical representation of $D \cap Y$ means that:

1. $D \cap Y = \bigcup_i (I_i \cap Y)$;
2. for every i, $I_i \cap Y$ is an ideal of Y;
3. $I_i \cap Y$ and $I_j \cap Y$ are incomparable for inclusion, for $i \neq j$.

For the first point, $\bigcup_i (I_i \cap Y) = (\bigcup_i I_i) \cap Y = (\downarrow_X (D \cap Y)) \cap Y = D \cap Y$.

We now argue that each $I_i \cap Y$ is a correct representation of an ideal of Y, i.e., all I_i's are in the adherence of Y. One inclusion being trivial, we need to show that $I_i \subseteq \downarrow_X (I_i \cap Y)$, for every i. Let $x_i \in I_i$. Since the ideals I_j are incomparable for inclusion, there exists $x'_i \in I_i$ such that $x_i \leq x'_i$ and for any $j \neq i$, $x'_i \notin I_j$ (I_i is directed). Besides, $x'_i \in I_i \subseteq \downarrow_X (D \cap Y)$ and thus there is an element x''_i such that $x'_i \leq x''_i \in D \cap Y$. As the sets I_j are downward-closed, x''_i cannot belong to any I_j with $j \neq 0$, hence x''_i is in $I_i \cap Y$. Therefore, $x_i \in \downarrow_X (I_i \cap Y)$.

Finally, the ideal decomposition $D \cap Y = \bigcup_j (I_j \cap Y)$ is canonical since the I_j's are incomparable in X (recall the above criterion for inclusion of ideals of Y). ☐

Observe that if $D = \bigcup_i I_i$ then $\downarrow_X (D \cap Y) = \bigcup_i \downarrow_X (I_i \cap Y) = \bigcup_i \mathcal{S}_{\mathrm{I}}(I)$. Thus the canonical representation of $D \cap Y$ is indeed computable from $D \in \mathit{Down}(X)$.

We now present the dual of the previous lemma:

Lemma 4.3.5. *Given $U \in \mathit{Up}(X)$, a canonical representation of $U \cap Y$ (as an upward-closed set of Y) can be computed from a canonical representation of $\uparrow_X (U \cap Y)$ (as an upward-closed set of X).*

Proof. Let $\bigcup_i \uparrow x_i$ be a canonical filter decomposition (in X) of the upward-closed set $\uparrow_X (U \cap Y)$. We first prove that for every i, x_i is equivalent to some element of Y. Indeed, since $\uparrow_X x_i \subseteq \uparrow_X (U \cap Y)$, there exists $y \in U \cap Y$ with $y \leq x_i$. But then, y must be in some $\uparrow_X x_j$. Since the decomposition is canonical, the x_j's are incomparable, hence we cannot have $x_j \leq y \leq x_i$ for $j \neq i$. Thus, $x_i \equiv y \in Y$.

Moreover, we can compute a canonical filter decomposition of $\uparrow_X(U \cap Y)$ using only elements in Y: for each x_i, it is decidable whether $x_i \in Y$ (our first assumption on Y). If not, we can enumerate elements of Y until we find some $y_i \equiv x_i$. Such an element exists, and thus the enumeration terminates.

We thus obtain a canonical filter decomposition $\bigcup_i \uparrow y_i$ of $\downarrow_X(U \cap Y)$ with $y_i \in Y$. The rest of the proof is similar to the proof of Lemma 4.3.4. $\square$

Here also, a canonical representation of $\uparrow_X(U \cap Y)$ is computable from U, using the function $\mathcal{S}_{\mathrm{F}}$.

We can now describe procedures for the four remaining operations:

(CF)**:** Given $y \in Y$, the complement of $\uparrow_Y y$ is computed by using the equality $Y \smallsetminus \uparrow_Y y = (X \smallsetminus \uparrow_X y) \cap Y$. The downward-closed set $(X \smallsetminus \uparrow_X y)$ is computable using (CF) for X, and its intersection with Y is computable using Lemma 4.3.4.

(II)**:** Given two ideals I and I' in the adherence of Y, the intersection of the ideals they induce is $(I \cap Y) \cap (I' \cap Y) = (I \cap I') \cap Y$, which is computable using (II) for X and Lemma 4.3.4.

(IF)**:** Computing the intersection of filters is similar to computing the intersection of ideals: given $y_1, y_2 \in Y$, $(\uparrow_Y y_1) \cap (\uparrow_Y y_2) = (\uparrow_X y_1 \cap \uparrow_X y_2) \cap Y$, which is computable using (IF) for X and Lemma 4.3.5.

(CI)**:** Given an ideal I in the adherence of Y, $Y \smallsetminus (I \cap Y) = (X \smallsetminus I) \cap Y$, which is computable using (CI) for X and Lemma 4.3.5.

Finally, and as always, the above presentation can be computed from a presentation of $(X, \leq)$, thanks to the functions $\mathcal{S}_{\mathrm{I}}$ and $\mathcal{S}_{\mathrm{F}}$. Notably, the ideal decomposition of Y can be computed as the subset induced by the downward-closed set X of X, using Lemma 4.3.4, and the filter decomposition of Y can be computed as the subset induced by the upward-closed set X of X, using Lemma 4.3.5.

Remark 4.3.6. *If Y is a downward-closed subset of X, then an ideal I is adherent to Y if and only if $I \subseteq Y$, and therefore $Idl(Y) = Idl(X) \cap \mathcal{P}(Y)$. Moreover, $\mathcal{S}_{\mathrm{I}}$ is computable thanks to* (II)*, and $\mathcal{S}_{\mathrm{F}}(\uparrow x) = \uparrow x$ if $x \in Y$, $\mathcal{S}_{\mathrm{F}}(\uparrow x) = \emptyset$ otherwise. Indeed, if $x \notin Y$, then $\uparrow x \cap Y = \emptyset$.*

Similarly, if Y is upward-closed, $\mathcal{S}_{\mathrm{F}}$ can be computed with (II)*, and $\mathcal{S}_{\mathrm{I}}(I) = I$ if $Y \cap I \neq \emptyset$, $\mathcal{S}_{\mathrm{I}}(I) = \emptyset$ otherwise. Again, $Y \cap I \neq \emptyset$ if and only if $\exists x \in \min(Y) : x \in I$. Given such an x, then $\forall y \in I : \exists z \in I : z \geq x, y$ by directedness. Therefore, $I \subseteq \downarrow(I \cap \uparrow x) \subseteq \downarrow(I \cap Y)$.*

4.4 References and Related Work

The notion of adherence has first been introduced in [28]. In this paper, the authors use the notion of ideals to "demystify" the data-structures used in the well-known but obscure proof of decidability of the reachability problem for Petri Nets first shown by Kosaraju, Lambert and Mayr. Intuitively, they define, using natural constructions on WQOs, an over-approximation of the set of all runs of a given Petri Net. In the light of this section, the ideals of the actual set of runs are the ideals of the over-approximation that are adherent to the actual set of runs, which motivated the introduction of adherence in the first place. Note that in this setting, $\mathcal{S}_{\mathrm{I}}$ is not computable.

The notion of adherence has also been successfully applied to *separability by piecewise testable languages* in language theory [30] and [31].

Chapter 5

Sums and Products of WQOs

The results of this chapter are easily obtained and widely known. They are nonetheless included here for completeness, since sums and products constitute basic constructions that naturally appear when working with WQOs (see Section 9.2 for instance). They also provide warm-up examples to practice our definition.

5.1 Disjoint Sums

The *disjoint sum* $X_\sqcup = X_1 \sqcup X_2$ of two WQOs $(X_1, \leq_1)$ and $(X_2, \leq_2)$ is the set $\{1\} \times X_1 \cup \{2\} \times X_2$, well quasi-ordered by:

$$\langle i, x\rangle \leq_\sqcup \langle j, y\rangle \text{ iff } i = j \text{ and } x \leq_i y \ .$$

This structure is obviously well quasi-ordered when $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are.

We let the reader check the following characterization.

Proposition 5.1.1 (Ideals of $\boldsymbol{X_1 \sqcup X_2}$). *Given $(X_1, \leq_1)$ and $(X_2, \leq_2)$ two WQOs, the ideals of $(X_1 \sqcup X_2, \leq_\sqcup)$ are exactly the sets of the form $I = \{i\} \times J$ with $i \in \{1, 2\}$ and J an ideal of X_i.*

Thus $(Idl(X_1 \sqcup X_2), \subseteq)$ is isomorphic to $(Idl(X_1), \subseteq) \sqcup (Idl(X_2), \subseteq)$.

Given data structures for X_1 and X_2, we use the natural data structure for $X_1 \sqcup X_2$. Moreover, Proposition 5.1.1 shows that ideals of the WQO $(X_1 \sqcup X_2, \leq_\sqcup)$ can similarly be represented using data structure for $Idl(X_1)$ and $Idl(X_2)$.

Theorem 5.1.2. *With the above representations of elements and ideals, disjoint union is a polynomial-time ideally effective construction.*

Sketch. Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be two ideally effective WQOs.

In the following, we write $\bar{\imath}$ for $3 - i$ when $i \in \{1, 2\}$, so that $\{i, \bar{\imath}\} = \{1, 2\}$. We also abuse notation and, for a downward-closed subset $D = \bigcup_a I_a$ of X_i, we write $\langle i, D\rangle$ to denote $\bigcup_a \langle i, I_a\rangle$, a downward-closed subset of $X_\sqcup$ represented via ideals. Similarly, for an upward-closed subset $U = \bigcup_a \uparrow_{X_i} x_a$ of X_i, we let $\langle i, U\rangle$ denote $\bigcup_a \uparrow_\sqcup \langle i, x_a\rangle$.

(OD): the definition of $\leq_\sqcup$ is already an implementation.

(ID): we use $\langle i, J\rangle \subseteq \langle i', J'\rangle \iff i = i' \wedge J \subseteq J'$.

(PI): we use $\downarrow_\sqcup\langle i, x\rangle = \langle i, \downarrow_i x\rangle$ for $i \in \{1, 2\}$.

(CF): we use $X_\sqcup \smallsetminus \uparrow_\sqcup\langle i, x\rangle = \langle i, X_i \smallsetminus \uparrow_i x\rangle \cup \langle \bar{\imath}, X_{\bar{\imath}}\rangle$. Note that this relies on (CF) for X_i (to express $X_i \smallsetminus \uparrow_i x$ as a union of ideals) and on (XI) for $X_{\bar{\imath}}$.

(II): we rely on (II) for X_1 and X_2, using

$$\langle i, I\rangle \cap \langle j, J\rangle = \begin{cases} \langle i, I \cap J\rangle & \text{if } i = j, \\ \emptyset & \text{otherwise.} \end{cases}$$

Operations (CI) to complement ideals and (IF) to intersect filters are analogous.

Observe that the presentation of $(X_1 \sqcup X_2, \leq_\sqcup)$ described above is clearly computable from presentations for $(X_i, \leq_i)$ $(i = 1, 2)$, and is polynomial-time when the presentations for $(X_i, \leq_i)$ $(i = 1, 2)$ are. Notably, a filter (resp. ideal) decomposition of $X_1 \sqcup X_2$ is easily obtained by taking the union of filter (resp. ideal) decompositions of X_1 and X_2, thus establishing (XF) (resp. (XI)).

□

5.2 Lexicographic Sums

The *lexicographic sum* $X_1 + X_2$ of two WQOs $(X_1, \leq_1)$, $(X_2, \leq_2)$ has the same support set as for their disjoint sum (i.e., $X_+ \stackrel{\text{def}}{=} X_\sqcup$); only the quasi-ordering is different:

$$\langle i, x\rangle \leq_+ \langle j, y\rangle \text{ iff } i < j \text{ or } (i = j \text{ and } x \leq_i y)\ .$$

Note that $\leq_+$ extends $\leq_\sqcup$ (i.e. $\leq_\sqcup \subseteq \leq_+$), thus it is a WQO. Although we could apply the results obtained in Section 4.1, we rather deal with this case by hand.

Again, the following characterization is easy to obtain.

Proposition 5.2.1 (Ideals of $\boldsymbol{X_1 \oplus X_2}$)**.** *Given two WQOs $(X_1, \leq_1)$ and $(X_2, \leq_2)$, the ideals of $X_1 \oplus X_2$ are exactly the sets of the form $\{1\} \times J_1$ with $J_1 \in Idl(X_1)$, or of the form $\{1\} \times X_1 \cup \{2\} \times J_2$ with $J_2 \in Idl(X_2)$.*

Thus $(Idl(X_1 \oplus X_2), \subseteq)$ is isomorphic to $(Idl(X_1), \subseteq) \oplus (Idl(X_2), \subseteq)$, which leads to a simple data structure for the set of ideals[1] when X_1 and X_2 are effective.

Theorem 5.2.2. *With the above representations, lexicographic union is a polynomial-time ideally effective construction.*

Sketch. Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be two ideally effective WQOs. We reuse the abbreviations $\langle i, U\rangle$, $\langle i, D\rangle$, $\bar{\imath}, \ldots$, introduced for disjoint sums. Also, we only consider the case where both X_1 and X_2 are non-empty (the claim is trivial otherwise).

[1] Note that with this representation, a pair $\langle i, J\rangle$ where $J \in Idl(X_i)$ denotes $\{1\} \times J$ when $i = 1$, and $\{1\} \times X_1 \cup \{2\} \times J$ —and not $\{2\} \times J$— when $i = 2$.

(OD)**:** follows from the definition.

(ID)**:** ideal inclusion can be tested as the lexicographic sum of $Idl(X_1)$ and $Idl(X_2)$.

(PI)**:** $\downarrow_{\oplus}\langle i, x\rangle$ is (represented by) $\langle i, \downarrow_i x\rangle$.

(CF)**:** the complement $X_{\oplus} \smallsetminus \uparrow_{\oplus}\langle i, x\rangle$ is (represented by) $\langle i, X_i \smallsetminus \uparrow_i x\rangle$ except when $i = 2$ and $\uparrow_i x = X_2$, in which case $X_{\oplus} \smallsetminus \uparrow_{\oplus}\langle 2, x\rangle$ is $\langle 1, X_1\rangle$.

(II)**:** intersection of two ideals considers two cases. First $\langle 1, I\rangle \cap \langle 2, J\rangle$ is (represented by) $\langle 1, I\rangle$ for ideals issued from different components in $X_{\oplus}$. For $\langle i, I\rangle \cap \langle i, J\rangle$, i.e., ideals issued from the same component, we use $\langle i, I \cap J\rangle$ except when $i = 2$ and $I \cap J = \emptyset$, in which case $\langle 2, I\rangle \cap \langle 2, J\rangle$ is $\langle 1, X_1\rangle$.

Procedures for the dual operations (CI) and (IF) are similar. Moreover, the presentation above is obviously computable from presentations for $(X_1, \leq_1)$ and $(X_2, \leq_2)$. Regarding (XI) and (XF), the ideal decomposition of $X_1 \oplus X_2$ is the ideal decomposition of X_2 and the filter decomposition of $X_1 \oplus X_2$ is the filter decomposition of X_1. Finally, the fact that disjoint sum is a polynomial-time construction is again trivial. □

5.3 Cartesian Products and Dickson's Lemma

Given two QOs $(X_1, \leq_1)$ and $(X_2, \leq_2)$, we define the *component-wise quasi-ordering* $\leq_\times$ on the Cartesian product $X_1 \times X_2$ by $\langle x_1, x_2\rangle \leq_\times \langle y_1, y_2\rangle \overset{\text{def}}{\Leftrightarrow} x_1 \leq_1 y_1 \wedge x_2 \leq_2 y_2$. Dickson's Lemma states that $(X_1 \times X_2, \leq_\times)$ is a WQO when $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are.

The ideals of $(X_1 \times X_2, \leq_\times)$ are well known.

Proposition 5.3.1 (Ideals of $\boldsymbol{X_1 \times X_2}$)**.** *Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be two WQOs. A subset I is an ideal of $X_1 \times X_2$ if, and only if, $I = I_1 \times I_2$ for some ideals I_1, I_2 of X_1 and X_2 respectively.*

Proof. ($\Leftarrow$): One checks that $I = I_1 \times I_2$ is non-empty, downward-closed, and directed, when I_1 and I_2 are. For directedness, we consider two elements $\langle x_1, x_2\rangle$ and $\langle y_1, y_2\rangle$ in I. Since I_1 is directed and contains x_1, y_1, it contains some z_1 with $x_1 \leq_1 z_1$ and $y_1 \leq_1 z_1$. Similarly I_2 contains some z_2 above x_2 and y_2 (wrt. $\leq_2$). Finally, $\langle z_1, z_2\rangle$ is in I, and above both $\langle x_1, y_1\rangle$ and $\langle x_2, y_2\rangle$.
($\Rightarrow$): Consider $I \in Idl(X_1 \times X_2)$ and write I_1 and I_2 for its projections on X_1 and X_2. These projections are downward-closed (since I is), non-empty (since I is) and directed (since I is), hence they are ideals (in X_1 and X_2). We now show that $I_1 \times I_2 \subseteq I$. Consider an arbitrary $x_1 \in I_1$: since I_1 is the projection of I, there is some $y_2 \in X_2$ such that $\langle x_1, y_2\rangle \in I$. Similarly, for any $x_2 \in I_2$, there is some $y_1 \in X_1$ such that $\langle y_1, x_2\rangle \in I$. Since I is directed, there is some $\langle z_1, z_2\rangle \in I$ with $\langle x_1, y_2\rangle \leq_\times \langle z_1, z_2\rangle$ and $\langle y_1, x_2\rangle \leq_\times \langle z_1, z_2\rangle$. But then $x_1 \leq_1 z_1$ and $x_2 \leq_2 z_2$. Thus $\langle x_1, x_2\rangle \in I$ since I contains $\langle z_1, z_2\rangle$ and is downward-closed. Hence $I = I_1 \times I_2$ and I is a product of ideals. □

Thus $Idl(X_1 \times X_2, \subseteq)$ is isomorphic to $(Idl(X_1), \subseteq) \times (Idl(X_2), \subseteq)$. If $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are ideally effective, we naturally represent elements of $X_1 \times X_2$ as pairs of elements of X_1 and X_2, and similarly ideals of $(X_1 \times X_2, \leq_\times)$ as pairs of ideals of X_1 and X_2.

Theorem 5.3.2. *With the above representations, Cartesian product is a polynomial-time ideally effective construction.*

Proof. Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be two ideally effective WQOs.

Let D_1 and D_2 be downward-closed sets of $(X_1, \leq_1)$ and $(X_2, \leq_2)$ respectively, given by some ideal decompositions $D_1 = \bigcup_i I_{1,i}$ and $D_2 = \bigcup_j I_{2,j}$. Then $D_1 \times D_2$ is downward-closed in $X_1 \times X_2$, and it decomposes as $\bigcup_i \bigcup_j I_{1,i} \times I_{2,j}$ since products distribute over unions. The same reasoning holds for upward-closed sets and their filter decompositions and we rely on these properties in the following explanations.

(OD): the ordering $\leq_\times$ is obviously decidable.

(ID): $I_1 \times I_2 \subseteq J_1 \times J_2$ iff $I_1 \subseteq J_1$ and $I_2 \subseteq J_2$ (exercise; the non-emptiness of ideals is required here).

(PI): $\downarrow\langle x_1, x_2\rangle = \downarrow x_1 \times \downarrow x_2$.

(II): to compute intersections, use $(I_1 \times I_2) \cap (I'_1 \times I'_2) = (I_1 \cap I'_1) \times (I_2 \cap I'_2)$, and build the product of downward-closed sets as explained above.

(CF): to complement filters, use $(X_1 \times X_2) \smallsetminus \uparrow_\times\langle x_1, x_2\rangle = \big[(X_1 \smallsetminus \uparrow x_1) \times X_2\big] \cup \big[X_1 \times (X_2 \smallsetminus \uparrow x_2)\big]$ and build products of downward-closed sets.

Procedures for the remaining operations are obtained similarly. Note that here too, the presentation above is computable from presentations for $(X_1, \leq_1)$ and $(X_2, \leq_2)$. Notably, a filter and ideal decomposition of $X_1 \times X_2$ is easily obtained from decompositions of X_1 and X_2, by distributing products over unions. Finally, the procedures described above are obviously polynomial-time when the presentations of $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are. $\square$

References and Related Work The most prominent use of the product quasi-ordering in verification is with the WQO $(\mathbb{N}^k, \leq_\times)$ of vectors of natural numbers. Without explicitly mentioning the notion of ideals, they have long been used under the form of *omega-vectors* (e.g. [16] and successor work), that is vectors of elements of $\mathbb{N}_\omega = \mathbb{N} \cup \{\omega\}$. In terms of ideals, we now know that $\mathbb{N}_\omega$ simply is a convenient representation for $Idl(\mathbb{N})$, and thus $\mathbb{N}_\omega^k$ is a convenient representation for $Idl(\mathbb{N}^k)$. Set-theoretic operations are not difficult to perform in $(\mathbb{N}^k, \leq_\times)$, computational description of these operations are given in [21] for instance.

It is not difficult to generalize these results to an arbitrary product of WQOs $X_1 \times X_2$. It is therefore difficult to find any reference on that matter. We can simply mention that the structure of ideals of $(X^k, \leq_\times)$ is given as a lemma to characterize the ideals of $(X^*, \leq_*)$ (see next chapter) in [12].

The results of these sections can be generalized to Noetherian spaces [13]. There, the fact that ideals of the product are products of ideals is expressed as "Sobrification commutes with finite products", and includes a reference to this more general result.

5.4 Lexicographic Product

Given $(X_1, \leq_1)$ and $(X_2, \leq_2)$ QOs, the lexicographic quasi-ordering $\leq_{\mathrm{lex}}$ is the QO defined on the cartesian product $X_1 \times X_2$ by $\langle x_1, x_2\rangle \leq_{\mathrm{lex}} \langle y_1, y_2\rangle \overset{\mathrm{def}}{\Leftrightarrow} x_1 <_1 y_1 \vee (x_1 \equiv_1 y_1 \wedge x_2 \leq_2 y_2)$, where $\equiv_1 \overset{\mathrm{def}}{=} \leq_1 \cap \geq_1$ and $<_1 \;=\; \leq_1 \smallsetminus \equiv_1$. Moreover, if $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are WQOs, then $(X_1 \times X_2, \leq_{\mathrm{lex}})$ is a WQO as well, since $\leq_\times \subseteq \leq_{\mathrm{lex}}$. The other important property of the lexicographic quasi-ordering is that it is linear when its arguments are. More precisely, the lexicographic product of two ordinals is by definition their product.

Since $\leq_\times \subseteq \leq_{\mathrm{lex}}$, we are in the setting of Section 4.1: the ideal effectiveness of $(X_1 \times X_2, \leq_{\mathrm{lex}})$ comes for free provided the two following functions are computable:

$$\begin{array}{llll}
\mathcal{C}l_{\mathrm{I}} & : \mathit{Idl}(X_1 \times X_2, \leq_\times) & \to \mathit{Down}(X_1 \times X_2, \leq_\times) \\
 & I \times J & \mapsto {\downarrow_{\mathrm{lex}}}(I \times J) \\
\mathcal{C}l_{\mathrm{F}} & : (X_1 \times X_2, \leq_\times) & \to \mathit{Up}(X_1 \times X_2, \leq_\times) \\
 & \langle x, y\rangle & \mapsto {\uparrow_{\leq_{\mathrm{lex}}}}\langle x, y\rangle
\end{array}$$

The expressions of these two functions in this particular case are given in the next proposition.

Proposition 5.4.1. *Given $I \in \mathit{Idl}(X_1)$, $J \in \mathit{Idl}(X_2)$, $x \in A$ and $y \in B$:*

$$\mathcal{C}l_{\mathrm{I}}(I \times J) = \begin{cases} ({\downarrow} x_I \times J) \cup ({\downarrow_{<_1}} x_I \times X_2) & \text{when } I = {\downarrow} x_I \text{ for some } x_I \in X_1 \\ I \times X_2 & \text{otherwise} \end{cases}$$

$$\mathcal{C}l_{\mathrm{F}}(\langle x, y\rangle) = {\uparrow_\times}\langle x, y\rangle \cup ({\uparrow_{>_1}} x \times X_2)$$

Proof. Both left-to-right inclusions are trivial. Assume $I = {\downarrow} x_I$ is a principal ideal of X_1, and let $\langle y, z\rangle \in {\downarrow_{<_1}} x_I \times X_2$. Since $y <_1 x$, $\langle y, z\rangle \leq_{\mathrm{lex}} \langle x, t\rangle$ for any $t \in X_2$. Since J is non-empty, $\langle y, z\rangle \in {\downarrow_{\mathrm{lex}}} I \times J$.

On the other hand, if I is not principal, then I has no maximal element. That is, for any $y \in I$, there exists a strictly greater $x \in I$. Therefore, for any $z \in X_2$, $\langle y, z\rangle \leq_{\mathrm{lex}} \langle x, t\rangle$ for any $t \in X_2$, and in particular for some $t \in J$. Thus $\langle y, z\rangle \in {\downarrow_{\mathrm{lex}}} I \times J$.

The correctness of the expression for $\mathcal{C}l_{\mathrm{F}}$ is analogous. ☐

Observe that ${\downarrow_<} x = {\downarrow} x \cap (X_1 \smallsetminus {\uparrow} x)$ and ${\uparrow_>} x = {\uparrow} x \cap (X_1 \smallsetminus {\downarrow} x)$ for any $x \in X_1$. Therefore, these expressions are computable when $(X, \leq_1)$ is ideally effective. Moreover, from the filter and ideal decomposition of X_2, it is simple to obtain the actual filter decomposition of ${\uparrow_{>_1}} x \times X_2$ and the actual ideal decomposition of ${\downarrow_{<_1}} x \times X_2$. However, a last obstacle remains to the computability of $\mathcal{C}l_{\mathrm{I}}$: we need to be able to decide whether a given ideal is principal. This is not an assumption listed in Definition 3.1.1, and does not follow from our definition in general. We provide in Section 8.3 an ideally effective WQO for which it is undecidable to say whether a given ideal is principal. Taking a lexicographic over this WQO, we also show that function $\mathcal{C}l_{\mathrm{I}}$ is not computable in general.

For a time, I thought that only the shortcut provided by Section 4.1 was made impracticable by this result, and that we could prove directly (axiom after axiom) that $(X_1 \times X_2, \leq_{\mathrm{lex}})$ was ideally effective. Unfortunately, this is not the case: Dietrich

Kuske found a mistake in one of my proofs, and I soon realized it couldn't be corrected. In the end, the WQO provided in Section 8.3 for which function $\mathcal{C}l_{\mathrm{I}}$ is not computable is also a counter example to the ideal effectiveness of the lexicographic product. In conclusion, the lexicographic product, despite being a natural construction, is not ideally effective according to our definition.

Nonetheless, in commonly used WQOs, testing whether an ideal is principal is trivially decidable. We therefore obtain the following weaker result:

Theorem 5.4.2. *Given $(X_1, \leq_1)$ and $(X_2, \leq_2)$ ideally effective WQOs such that it is decidable whether a given ideal of $Idl(X_1)$ is principal, then $(X_1 \times X_2, \leq_{\mathrm{lex}})$ is an ideally effective WQO.*

Moreover, from (polynomial-time) presentations of $(X_1, \leq_1)$ and $(X_2, \leq_2)$ and a (polynomial-time) algorithm to test principality of ideals of $(X_1, \leq_1)$, we can compute a (polynomial-time) presentation of $(X_1 \times X_2, \leq_{\mathrm{lex}})$.

Proof. Follows from Theorem 4.1.2 and the analysis of functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ above. $\square$

Chapter 6

Finite Sequences over WQOs

6.1 Higman's Quasi-Ordering

A QO $(X, \leq)$ is a WQO if and only if $(X^*, \leq_*)$ is a WQO as well (Higman's Lemma), where as defined in Chapter 2, X^* is the set of all finite sequences over X, and $\leq_*$ denotes the embedding quasi-ordering between sequences. We sometimes refer to $(X^*, \leq_*)$ as the Higman extension of $(X, \leq)$ and $\leq_*$ is called Higman's quasi-ordering.

Elements of X^* will be denoted in bold font, such as $\boldsymbol{u}, \boldsymbol{v}, ...$, while elements of X are denoted $x, y, ...$ In particular, if $x \in X$, then $\boldsymbol{x} \in X^*$ denotes the sequence of length one containing only the symbol x. The product (for concatenation) of two sets of sequences $\boldsymbol{U}, \boldsymbol{V} \subseteq X^*$ is denoted $\boldsymbol{U} \cdot \boldsymbol{V} \stackrel{\text{def}}{=} \{\boldsymbol{u} \cdot \boldsymbol{v} \mid \boldsymbol{u} \in \boldsymbol{U}, \boldsymbol{v} \in \boldsymbol{V}\}$.

The structure of ideals of $(X^*, \leq_*)$ is given in [12] where the following theorem is proved. An alternative proof is presented at the end of Section 6.1.2.

Theorem 6.1.1. *The ideals of $(X, \leq_*)$ are exactly the finite products of* atoms $\boldsymbol{P} = \boldsymbol{A}_1 \cdots \boldsymbol{A}_n$*, where* atoms *are:*

- *any set of the form $D^* \subseteq X^*$ for $D \in Down(X)$,*
- *or any set of the form $\downarrow_* I = \{\boldsymbol{x} \in X^* \mid x \in I\} \cup \{\epsilon\}$ for $I \in Idl(X)$. Subsequently, $\downarrow_* I$ will be denoted $I + \epsilon$ (this notation comes from regular expressions in language theory).*

This theorem states that any ideal of $(X^*, \leq_*)$ can be decomposed as a finite product of atoms. However, for instance for X the finite alphabet $\{a, b\}$, we have $(a+\epsilon)(a+b)^* = (a+b)^*$. That is to say, ideals of $(X^*, \leq_*)$ admit several decompositions as products of atoms. In Section 6.1.3, we define a canonical atom decomposition for ideals of $(X^*, \leq_*)$ which is easily obtained from any other decomposition (as in the case of upward- and downward-closed sets, it suffices to remove redundancies). But, we do not need this canonical decomposition to prove ideal effectiveness, and therefore we proceed to the main theorem of this section: the ideal effectiveness of the Higman extension, which is stated and proved in the next subsection. We then give a proof of

Theorem 6.1.1 in Section 6.1.2, define the canonical decomposition in Section 6.1.3 and provide some references and pointers to related work in Section 6.1.4.

6.1.1 The Higman Extension is Ideally Effective

First, let us a fix a representation for X^* and $Idl(X^*, \leq_*)$: as expected, we will simply represent finite sequences of elements of X as lists of encodings of X (assuming a representation for X). Similarly, the theorem above suggests representing ideals as finite sequences (e.g. lists) of atoms. For that, we need a representation for atoms. Assuming a representation for X and $Idl(X)$, we represent downward-closed sets of X as always, which gives us representations for each of the two kinds of atoms. Now the full set of atoms can be seen as $Idl(X) \sqcup Down(X)$ which we can represent as we did in Section 5.1. Observe that the empty sequence of atoms, denoted $\boldsymbol{\epsilon}$ to avoid confusion with the empty sequence $\epsilon \in X^*$, denotes the singleton ideal $\{\epsilon\}$.

Theorem 6.1.2. *With the above representations, the Higman extension is an ideally effective construction. It is not polynomial-time in general. Given a polynomial-time presentation of an ideally effective WQO* $(X, \leq)$*, we can compute an exponential-time presentation of* $(X^*, \leq_*)$*.*

The proof of this theorem being quite long, it is structured in several sub-parts, one for each of the main operations: (ID), (CF), (II), (IF), (CI). Each of these subsections will include a description of the operation at hand as well as complexity lower and upper bounds. The easier requirements from Definition 3.1.1 are shown valid below.

Proof. Let $(X, \leq)$ be an ideally effective WQO.

(OD)**:** deciding $\leq_*$ over X^* reduces to comparing elements of X, e.g. by looking for a *leftmost embedding*.

(PI)**:** given a finite sequence $\boldsymbol{u} = x_1 \cdots x_n$, the principal ideal $\downarrow \boldsymbol{u}$ is represented by the product $(\downarrow x_1 + \epsilon) \cdots (\downarrow x_n + \epsilon)$.

The fact that a (exponential-time) presentation of $(X^*, \leq_*)$ can be computed from a (polynomial-time) presentation of $(X, \leq)$ will be clear from the procedures described in the next subsections and their complexity analysis. Notably, for (XF), the filter decomposition of $X^* = \uparrow \boldsymbol{\epsilon}$ is given by the empty sequence (and does not depend on X), while for (XI) we note that X^* is already an ideal made of a single atom.

The fact that the Higman extension is not a polynomial-time construction follows from the complexity lower bounds presented in the next subsections. □

Before we move on to the technical part of the proof of the theorem above, let us introduce some convenient notations.

Given $D = \bigcup_i I_i \in Down(X)$, we write $D + \epsilon$ to denote $\bigcup_i (I_i + \epsilon) \in Down(X^*)$. We will call such subsets *generalized atoms*. Products of atoms and generalized atoms are downward-closed sets of X^*. From such a product $\boldsymbol{P}$ describing a downward-closed sets $\mathcal{D}$ of X^*, it is possible to recover the actual ideal decomposition of $\mathcal{D}$ by distributing the products over the unions in $\boldsymbol{P}$. However, the ideal decomposition of $\mathcal{D}$ might be of size exponential in the size of $\boldsymbol{P}$.

We will also use shortcuts to denote upward-closed sets. Given two upward-closed sets of sequences $\boldsymbol{U} = \bigcup_i \uparrow \boldsymbol{u}_i$ and $\boldsymbol{V} = \bigcup_j \uparrow \boldsymbol{v}_j$, the product $\boldsymbol{U} \cdot \boldsymbol{V}$ is upward-closed and its filter decomposition can be computed by $\boldsymbol{U} \cdot \boldsymbol{V} = \bigcup_{i,j} \uparrow(\boldsymbol{u}_i \cdot \boldsymbol{v}_j)$. Moreover, if $U = \bigcup_i \uparrow_X x_i \in Up(X)$ is an upward-closed set of $(X, \leq)$, then we can see U as a set of sequences of length 1, and $\uparrow_* U = \bigcup_i \uparrow_* \boldsymbol{x}_i$. Therefore, an upward-closed set of X can always be understood as an upward-closed set of X^*. This will be used silently.

Ideal Inclusion (ID)

Proposition 6.1.3. *Inclusion between ideals of $(X^*, \leq_*)$ can be tested using a linear number of inclusion tests between downward-closed sets of X, using a sort of* left-most embedding *search. When $(X, \leq)$ is an ideally effective WQO, the following equations implicitly describe an inductive algorithm deciding inclusion between ideals of $(X^*, \leq_*)$:*

1. *Atoms are compared as follows:*

$$
\begin{aligned}
(I_1 + \epsilon) \subseteq (I_2 + \epsilon) &\iff I_1 \subseteq I_2, \\
(I + \epsilon) \subseteq D^* &\iff I \subseteq D, \\
D_1^* \subseteq D_2^* &\iff D_1 \subseteq D_2, \\
D^* \subseteq (I + \epsilon) &\iff D = \emptyset.
\end{aligned}
$$

2. *for any ideal $\boldsymbol{P}$: $\boldsymbol{\epsilon} \subseteq \boldsymbol{P}$,*

3. *for any ideal $\boldsymbol{P}$ and atom $\boldsymbol{A}$: $\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{\epsilon} \iff \boldsymbol{A} = \emptyset^* \wedge \boldsymbol{P} \subseteq \boldsymbol{\epsilon}$*

4. *Finally, for any atoms $\boldsymbol{A}$ and $\boldsymbol{B}$, and any ideals $\boldsymbol{P}$ and $\boldsymbol{Q}$:*

   (a) *if $\boldsymbol{A} \not\subseteq \boldsymbol{B}$ then:*

   $$\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q} \iff \boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{Q}$$

   (b) *if $\boldsymbol{A} \subseteq \boldsymbol{B}$ as in the first equivalence of case 1, i.e. $\boldsymbol{A} = (I_1 + \epsilon)$, $\boldsymbol{B} = (I_2 + \epsilon)$ for some $I_1, I_2 \in Idl(X)$, then:*

   $$\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q} \iff \boldsymbol{P} \subseteq \boldsymbol{Q}$$

   (c) *if $\boldsymbol{A} \subseteq \boldsymbol{B}$ as in any of the three other equivalences of case 1, then:*

   $$\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q} \iff \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q}$$

Proof. The three first cases being trivial, we concentrate on the forth one.

4a It is always true that $\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{Q} \to \boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B}\dot{\boldsymbol{Q}}$. Conversely, let $\boldsymbol{u} \cdot \boldsymbol{v} \in \boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q}$. Assuming $\boldsymbol{A} \not\subseteq \boldsymbol{B}$, there exists $\boldsymbol{w}' \in \boldsymbol{A} \smallsetminus \boldsymbol{B}$ and by directedness, there exists $\boldsymbol{w} \in \boldsymbol{A} \smallsetminus \boldsymbol{B}$ such that $\boldsymbol{w} \geq \boldsymbol{u}$. Now, if $\boldsymbol{A} = I + \epsilon$ for some $I \in Idl(X)$, then $\boldsymbol{w}$ is of length one, is not in $\boldsymbol{B}$ and thus $\boldsymbol{w} \cdot \boldsymbol{v}$, which is in $\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q}$ has to actually be in $\boldsymbol{Q}$. Since $\boldsymbol{Q}$ is downward-closed, $\boldsymbol{u} \cdot \boldsymbol{v} \in \boldsymbol{Q}$.

   Otherwise, $\boldsymbol{A} = D^*$ for some $D \in Down(X)$. In this case, $\boldsymbol{w} \cdot \boldsymbol{w} \in \boldsymbol{A}$ and thus $\boldsymbol{wwv} \in \boldsymbol{B} \cdot \boldsymbol{Q}$. Because $\boldsymbol{w} \notin \boldsymbol{B}$, this implies $\boldsymbol{wv} \in \boldsymbol{Q}$, which again implies $\boldsymbol{uv} \in \boldsymbol{Q}$.

4b Here also, right-to-left implication is trivial. Conversely, assume $\boldsymbol{A} \cdot \boldsymbol{P} \subseteq \boldsymbol{B} \cdot \boldsymbol{Q}$ and $\boldsymbol{A} = (I_1 + \epsilon)$ and $\boldsymbol{B} = (I_2 + \epsilon)$ for some $I_1 \subseteq I_2 \in \mathit{Idl}(X)$. Let $\boldsymbol{u} \in \boldsymbol{P}$. Pick $x \in I_1$: $x\boldsymbol{u} \in \boldsymbol{A} \cdot \boldsymbol{P}$, thus $x\boldsymbol{u} \in \boldsymbol{B} \cdot \boldsymbol{Q}$. Therefore, $\boldsymbol{u} \in \boldsymbol{Q}$ since sequences of $\boldsymbol{B}$ have length at most one.

4c Left-to-right implication is trivial. For the other implication, decompose $\boldsymbol{P}$ in $\boldsymbol{P}_1 \cdot \boldsymbol{P}_2$ with $\boldsymbol{P}_1 \subseteq \boldsymbol{B}$ and $\boldsymbol{P}_2 \subseteq \boldsymbol{Q}$. Now observe that whenever $\boldsymbol{A} \subseteq \boldsymbol{B}$ but they are not both atoms of the form $I+\epsilon$ for some $I \in \mathit{Idl}(X)$, then $\boldsymbol{A} \cdot \boldsymbol{P}_1 \subseteq \boldsymbol{B}$. Therefore, $\boldsymbol{A} \cdot \boldsymbol{P} \boldsymbol{B} \cdot \boldsymbol{Q}$.

□

Observe that when $(X, \leq)$ is a polynomial-time ideally effective WQO, the algorithm described above runs in polynomial-time.

Complementing Filters (CF)

Proposition 6.1.4. *Complements of filters can be inductively computed using the following equations: Given $\boldsymbol{w} \in X^*$ and $x \in X$,*

(6.1) $$X^* \smallsetminus \uparrow \epsilon = \emptyset \text{ (empty union)}$$

(6.2) $$X^* \smallsetminus \uparrow \boldsymbol{x} = (X \smallsetminus \uparrow x)^*$$

(6.3) $$X^* \smallsetminus \uparrow x\boldsymbol{w} = (X \smallsetminus \uparrow x)^* \cdot (X + \epsilon) \cdot (X^* \smallsetminus \uparrow \boldsymbol{w})$$

Note that X might not be an ideal, and thus $X + \epsilon$ might be a generalized atom (not an actual atom). In this case, to compute the actual ideal decomposition of $X^* \smallsetminus \uparrow \boldsymbol{w}$, we need to distribute the products over the unions that comes from the ideal decomposition of X. This step might result in an exponential blow up. For instance, take X to be the finite ordering that consists of three elements $0, 1$ and $1'$ with $0 < 1$, $0 < 1'$ and $1 \perp 1'$. Then $X^* \smallsetminus \uparrow 0^{n+1}$ consists of all sequences of length at most n. Thus its canonical ideal decomposition has size 2^n: $X^* \smallsetminus \uparrow 0^{n+1} = \bigcup_{\boldsymbol{u} \in \{1,1'\}^n} \downarrow \boldsymbol{u}$.

Note however that in the commonly encountered case where X is a finite alphabet, the operation of complementing filters can be performed in polynomial-time. Indeed, if $X = \{a_1, \ldots, a_n\}$ is a finite alphabet (i.e. ordered with equality), then $X = \bigcup_{i=1}^n \downarrow a_i$, which is not an ideal for $n > 1$. But since $X \smallsetminus \uparrow a_i = \bigcup_{j \neq i} \downarrow a_j$, $(X \smallsetminus \uparrow a_i)^* \cdot (X + \epsilon) = (X \smallsetminus \uparrow a_i)^* \cdot (a_i + \epsilon)$ which is an ideal. In [12], the authors prove this finer expression to complement filters. for an arbitrary WQO $(X, \leq)$:

$$X^* \smallsetminus \uparrow xy\boldsymbol{w} = (X \smallsetminus \uparrow x)^* \cdot [\downarrow(\uparrow x \cap \uparrow y) + \epsilon] \cdot (X^* \smallsetminus \uparrow y\boldsymbol{w})$$

In general, our setting does not guarantee that the expression $\downarrow U$ is computable for $U \in \mathit{Up}(X)$, but when X is a finite alphabet, the expression $(\uparrow x \cap \uparrow y)$ either denotes the empty set or $(x + \epsilon)$ when $x = y$. Therefore, using this expression, one directly obtains the canonical form of the complement of a filter of X^* in the case of a finite alphabet.

Proof. (of Proposition 6.1.4)
Equations 6.1 and 6.2 are obvious. For the third equation:

($\supseteq$) If $\boldsymbol{w}' = \boldsymbol{u}y\boldsymbol{v}$ with $\boldsymbol{u} \in (X \smallsetminus \uparrow x)^*$, $y \in X + \epsilon$ and $\boldsymbol{v} \in (X^* \smallsetminus \uparrow \boldsymbol{w})$, then assume $x\boldsymbol{w} \leq \boldsymbol{w}'$, then either $x = y$ and $\boldsymbol{w} \leq \boldsymbol{v}$ which is a contradiction, or $x\boldsymbol{w} \leq \boldsymbol{v}$, which is also a contradiction.

($\subseteq$) Let $\boldsymbol{w}' \notin \uparrow x\boldsymbol{w}$. Then either $\boldsymbol{w}' \in (X \smallsetminus \uparrow x)^*$, or we can write $\boldsymbol{w}' = \boldsymbol{u}y\boldsymbol{v}$ with $\boldsymbol{u} \in (X \smallsetminus \uparrow x)^*$ and $y \geq x$. Moreover, $\boldsymbol{v} \notin \uparrow \boldsymbol{w}$, since otherwise $x\boldsymbol{w} \leq y\boldsymbol{v} \leq \boldsymbol{u}y\boldsymbol{v} = \boldsymbol{w}'$. Therefore, $\boldsymbol{w}' \in (X \smallsetminus \uparrow x)^* \cdot (X + \epsilon) \cdot (X^* \smallsetminus \uparrow \boldsymbol{w})$. $\square$

Intersecting Ideals (II)

Proposition 6.1.5. *The intersection of two ideals of* $(X^*, \leq_*)$ *can be computed inductively using the following equations:*

$$
\begin{aligned}
\boldsymbol{P} \cap \boldsymbol{\epsilon} &= \boldsymbol{\epsilon} \\
D_1^* \cdot \boldsymbol{P} \cap D_2^* \cdot \boldsymbol{Q} &= (D_1 \cap D_2)^* \cdot \big[((D_1^* \cdot \boldsymbol{P}) \cap \boldsymbol{Q}) \cup (\boldsymbol{P} \cap (D_2^* \cdot \boldsymbol{Q}))\big] \\
(I_1 + \epsilon) \cdot \boldsymbol{P} \cap (I_2 + \epsilon) \cdot \boldsymbol{Q} &= \big[((I_1 + \epsilon) \cdot \boldsymbol{P}) \cap \boldsymbol{Q}\big] \cup \big[\boldsymbol{P} \cap ((I_2 + \epsilon) \cdot \boldsymbol{Q})\big] \cup \\
&\qquad\qquad \cup \big[\big((I_1 \cap I_2) + \epsilon\big) \cdot (\boldsymbol{P} \cap \boldsymbol{Q})\big] \\
D^* \cdot \boldsymbol{P} \cap (I + \epsilon) \cdot \boldsymbol{Q} &= \big[\boldsymbol{P} \cap ((I + \epsilon) \cdot \boldsymbol{Q})\big] \cup \big[\big((D \cap I) + \epsilon\big) \cdot (D^* \cdot \boldsymbol{P} \cap \boldsymbol{Q})\big]
\end{aligned}
$$

Note that, in addition to using generalized atoms ($I_1 \cap I_2$ and $D \cap I$ may not be ideals), we use expressions that mix unions and products. The actual ideal decomposition is obtained when distributing the products over the unions. This is computable, but may again result in an exponential blow-up of the ideal decomposition. This is witnessed by the following example: take $X = \{a, b\}$ a two-symbol alphabet and $D = \downarrow(aba)^n \cap \downarrow(bab)^n$. Every word $\boldsymbol{u}$ in $\{ab, ba\}^n$ is a maximal element of D: membership is obvious, and maximality can be proved using the number of symbols a and b in $\boldsymbol{u}$, $\boldsymbol{u}$ has as many a's as $(bab)^n$ and as many b's as $(aba)^n$. Therefore, D is the union of exponentially many incomparable ideals (words of the same size are either equal or incomparable).

Proof. (of Proposition 6.1.5)
The first two equations are obviously correct. The other right-to-left inclusions are easily checked using Proposition 6.1.3. For the left-to-right directions:

- Let $\boldsymbol{u} \in (D_1^* \cdot \boldsymbol{P} \cap D_2^* \cdot \boldsymbol{Q})$. Let $\boldsymbol{v}$ be the longest prefix of $\boldsymbol{u}$ which is in D_1^*. Without loss of generality, we assume that the longest prefix of $\boldsymbol{u}$ which is in D_2^* is longer than $|\boldsymbol{v}|$, and thus can be written $\boldsymbol{v}\boldsymbol{w}$ for some $\boldsymbol{w} \in X^*$. Moreover, there exists $\boldsymbol{t} \in X^*$ so that $\boldsymbol{u} = \boldsymbol{v}\boldsymbol{w}\boldsymbol{t}$. We have, $\boldsymbol{v} \in (D_1 \cap D_2)^*$, $\boldsymbol{w}\boldsymbol{t} \in \boldsymbol{P}$ and $\boldsymbol{t} \in \boldsymbol{Q}$. Therefore, $\boldsymbol{w}\boldsymbol{t} \in \boldsymbol{P} \cap D_2^*\boldsymbol{Q}$.

- Let $x \cdot \boldsymbol{u} \in (I_1 + \epsilon) \cdot \boldsymbol{P} \cap (I_2 + \epsilon) \cdot \boldsymbol{Q}$. Depending on whether $x \in I_1 \smallsetminus I_2$, $x \in I_2 \smallsetminus I_1$ or $x \in I_1 \cap I_2$, $\boldsymbol{u}$ is easily proved to be in one of the three sets it should belong to. In the case x is neither in I_1 nor I_2, then $\boldsymbol{u}$ belongs to all three sets.

- The last case is proved similarly. $\square$

Intersecting Filters (IF)

Proposition 6.1.6. *The intersection of two filters can be computed inductively using the following equations, for $\boldsymbol{w}, \boldsymbol{v} \in X^*$ and $x, y \in X$:*

$$\begin{aligned}
\uparrow \boldsymbol{v} \cap \uparrow \epsilon &= \uparrow \boldsymbol{v} \\
\uparrow \epsilon \cap \uparrow \boldsymbol{w} &= \uparrow \boldsymbol{w} \\
\uparrow \boldsymbol{xv} \cap \uparrow \boldsymbol{yw} &= \big[(\uparrow \boldsymbol{x}) \cdot (\uparrow \boldsymbol{v} \cap \uparrow \boldsymbol{yw})\big] \cup \big[(\uparrow \boldsymbol{y}) \cdot (\uparrow \boldsymbol{xv} \cap \uparrow \boldsymbol{w})\big] \cup \\
&\qquad \cup \big[(\uparrow_X x \cap \uparrow_X y) \cdot (\uparrow \boldsymbol{v} \cap \uparrow \boldsymbol{w})\big]
\end{aligned}$$

The actual filter decomposition of this last upward-closed set can be computed following the remark at the beginning of this section.

Proof. The first two equations are trivial. For the third, right-to-left inclusion is obvious. Left-to-right inclusion: consider $\boldsymbol{u} \in \uparrow a\boldsymbol{v} \cap \uparrow b\boldsymbol{w}$. Let $\boldsymbol{u}'$ be the shortest suffix of $\boldsymbol{u}$ which belongs to $\uparrow a\boldsymbol{v} \cap \uparrow b\boldsymbol{w}$. Consider cases depending on whether the first letter of $\boldsymbol{u}'$ is above x and y in X. $\square$

The naive implementation of this procedure runs in exponential-time, and it is asymptotically optimal: the canonical decomposition of the upward-closed set $\uparrow a^n \cap \uparrow b^n$ has at least $\binom{2n}{n}$ minimal elements (this corresponds to all the words in the shuffle product $a^n \sqcup\!\sqcup\, b^n$).

Complementing Ideals (CI)

In this subsection we present a procedure to complement ideals. We first show how to complement atoms, and then how to complement products of atoms.

- If $D \subseteq X$ is downward-closed, then $X^* \smallsetminus D^*$ consists of all words which have at least one letter not in D. That is, compute $X \smallsetminus D = \uparrow x_1 \cup \ldots \cup \uparrow x_n$, using (CI) for X. Then $X^* \smallsetminus D^* = \uparrow \boldsymbol{x}_1 + \ldots + \uparrow \boldsymbol{x}_n$.
- If $I \subseteq X$ is an ideal, then $X^* \smallsetminus (I + \epsilon)$ consists of all words which have at least one letter not in I, and all words with at least two letters. The former is obtained as in the previous case. The latter is $\uparrow_* X \cdot X$, easily computed in a similar way using (XF) for X.

We now consider products $\boldsymbol{A}_1 \cdots \boldsymbol{A}_n$ of atoms. We know how to compute $\boldsymbol{U}_i = \complement \boldsymbol{A}_i$. We thus use the relation $\complement(\boldsymbol{A}_1 \cdots \boldsymbol{A}_n) = \complement(\complement \boldsymbol{U}_1 \cdots \complement \boldsymbol{U}_n)$, which motivates the following definition:

Definition 6.1.7. *Define the operator $\odot : Up(X^*) \times Up(X^*) \to Up(X^*)$ as $\boldsymbol{U} \odot \boldsymbol{V} := \complement(\complement \boldsymbol{U} \cdot \complement \boldsymbol{V})$.*

Note that $\boldsymbol{U} \odot \boldsymbol{V}$ is obviously upward-closed when $\boldsymbol{U}$ and $\boldsymbol{V}$ are. The operation $\odot$ is easily shown associative using the associativity of the product, thus $\boldsymbol{U}_1 \odot \ldots \odot \boldsymbol{U}_n = \complement(\complement \boldsymbol{U}_1 \cdot \ldots \cdot \complement \boldsymbol{U}_n)$. The previous relation becomes $\complement(\boldsymbol{A}_1 \cdots \boldsymbol{A}_n) = \boldsymbol{U}_1 \odot \cdots \odot \boldsymbol{U}_n$, and it only remains to show that $\odot$ is computable on upward-closed sets. In what follows, we will often use the following obvious characterization: $\boldsymbol{w} \in \boldsymbol{S} \odot \boldsymbol{T}$ if and only if for all factorizations $\boldsymbol{w} = \boldsymbol{w}_1\boldsymbol{w}_2$, $\boldsymbol{w}_1 \in \boldsymbol{S}$ or $\boldsymbol{w}_2 \in \boldsymbol{T}$.

We first show that $\odot$ is computable on filters, and later show that $\odot$ distributes over unions.

Lemma 6.1.8. *On principal filters, $\odot$ can be computed using the following equations:*

$$\begin{aligned} \uparrow \boldsymbol{v} \odot \uparrow \epsilon &= X^* \\ \uparrow \epsilon \odot \uparrow \boldsymbol{w} &= X^* \\ \uparrow \boldsymbol{v}a \odot \uparrow b\boldsymbol{w} &= \uparrow(\boldsymbol{v}ab\boldsymbol{w}) \cup (\uparrow \boldsymbol{v}) \cdot (\uparrow_X a \cap \uparrow_X b) \cdot (\uparrow \boldsymbol{w}) \end{aligned}$$

where $\boldsymbol{v}, \boldsymbol{w} \in X^*$ and $a, b \in X$.

Proof. The first two equations are obvious. For the third:

($\supseteq$) If $\boldsymbol{u} \geq_* \boldsymbol{v}ab\boldsymbol{w}$, then for every factorization of $\boldsymbol{u} = \boldsymbol{u}_1\boldsymbol{u}_2$, the left factor $\boldsymbol{u}_1$ is above $\boldsymbol{v}a$, or the right factor $\boldsymbol{u}_2$ is above $b\boldsymbol{w}$, and thus $\boldsymbol{u} \in \uparrow \boldsymbol{v}a \odot \uparrow b\boldsymbol{w}$. If $\boldsymbol{u} \geq_* \boldsymbol{v}c\boldsymbol{w}$, where $c \in X$ is such that $c \geq a$ and $c \geq b$, then in every factorization of $\boldsymbol{u} = \boldsymbol{u}_1\boldsymbol{u}_2$, c appears either in the left factor $\boldsymbol{u}_1$ or in the right factor $\boldsymbol{u}_2$, and this suffices to show that either $\boldsymbol{u} \geq_* \boldsymbol{v}a$ or $\boldsymbol{u} \geq_* b\boldsymbol{w}$.

($\subseteq$) Let $\boldsymbol{u} \in (\uparrow \boldsymbol{v}) \odot (\uparrow \boldsymbol{w})$. From the factorizations $\boldsymbol{u} = \boldsymbol{u} \cdot \epsilon$ and $\boldsymbol{u} = \epsilon \cdot z$ we get $\boldsymbol{v}a \leq_* \boldsymbol{u}$ and $b\boldsymbol{w} \leq_* \boldsymbol{u}$. Consider the shortest prefix of $\boldsymbol{u}$ into which $\boldsymbol{v}a$ embeds and the shortest suffix into which $b\boldsymbol{w}$ embeds. If these factors don't overlap, we get $\boldsymbol{u} \geq_* \boldsymbol{v}ab\boldsymbol{w}$. If they overlap, the overlap must have length exactly one (otherwise $\boldsymbol{u}$ can be split anywhere in the middle of the overlap to obtain a contradiction). Write $\boldsymbol{u} = \boldsymbol{u}_1c\boldsymbol{u}_2$ where $c \in X$ is the overlap. Then $\boldsymbol{u}_1 \geq_* \boldsymbol{v}$, $c \geq a$, $c \geq b$, and $\boldsymbol{u}_2 \geq_* \boldsymbol{w}$, which proves the statement. □

It now remains to show that $\odot$ distributes over unions.

Lemma 6.1.9. *Given $\boldsymbol{U}, \boldsymbol{U}_1, \boldsymbol{U}_2$ three upward-closed sets of X^*, we have:*

$$\begin{aligned} (\boldsymbol{U}_1 \cup \boldsymbol{U}_2) \odot \boldsymbol{U} = (\boldsymbol{U}_1 \odot \boldsymbol{U}) \cup (\boldsymbol{U}_2 \odot \boldsymbol{U}) \\ \boldsymbol{U} \odot (\boldsymbol{U}_1 \cup \boldsymbol{U}_2) = (\boldsymbol{U} \odot \boldsymbol{U}_1) \cup (\boldsymbol{U} \odot \boldsymbol{U}_2) \end{aligned}$$

Proof. We actually show the equivalent statement that product distributes over intersection for downward-closed sets. Let $\boldsymbol{D} = \complement\boldsymbol{U}$, $\boldsymbol{D}_1 = \complement\boldsymbol{U}_1$ and $\boldsymbol{D}_2 = \complement\boldsymbol{U}_2$, we show that $(\boldsymbol{D}_1 \cap \boldsymbol{D}_2) \cdot \boldsymbol{D} = (\boldsymbol{D}_1 \cdot \boldsymbol{D}) \cap (\boldsymbol{D}_2 \cdot \boldsymbol{D})$, and $\boldsymbol{D} \cdot (\boldsymbol{D}_1 \cap \boldsymbol{D}_2) = (\boldsymbol{D} \cdot \boldsymbol{D}_1) \cap (\boldsymbol{D} \cdot \boldsymbol{D}_2)$.

We only show the first equation, the second one being symmetrical. The left-to-right inclusion is obvious. For the right-to-left inclusion, let $\boldsymbol{w} \in \boldsymbol{D}_1 \cdot \boldsymbol{D} \cap \boldsymbol{D}_2 \cdot \boldsymbol{D}$. Then $\boldsymbol{w} = \boldsymbol{u}_1\boldsymbol{v}_1$ for some $\boldsymbol{u}_1 \in \boldsymbol{D}_1$ and $\boldsymbol{v}_1 \in \boldsymbol{D}$. Also, $\boldsymbol{w} = \boldsymbol{u}_2\boldsymbol{v}_2$ for some $\boldsymbol{u}_2 \in \boldsymbol{D}_2$ and $\boldsymbol{v}_2 \in \boldsymbol{D}$. One of $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ is a prefix of the other. Assume $\boldsymbol{u}_1$ is a prefix of $\boldsymbol{u}_2$ (the other case is analogous). Since $\boldsymbol{D}_2$ is downward-closed and $\boldsymbol{u}_1 \leq_* \boldsymbol{u}_2$, $\boldsymbol{u}_1 \in \boldsymbol{D}_2$. Thus, $\boldsymbol{u}_1 \in \boldsymbol{D}_1 \cap \boldsymbol{D}_2$ and $\boldsymbol{v}_1 \in \boldsymbol{D}$, $\boldsymbol{w} = \boldsymbol{u}_1\boldsymbol{v}_1 \in (\boldsymbol{D}_1 \cap \boldsymbol{D}_2) \cdot \boldsymbol{D}$. □

It follows that computing $\complement\boldsymbol{A}_1 \odot \cdots \odot \complement\boldsymbol{A}_n = (U_1 \odot \cdots \odot U_n)$ reduces to computing $\odot$ on filters, which is computable by Lemma 6.1.8. However, distributing over the unions can once again lead to an exponential blow-up. This is unavoidable, as shown below.

Proposition 6.1.10. *The upward-closed set $\complement{\downarrow}(ab)^n$ where $X = \{a, b\}$ is a two-symbol alphabet has an exponential number (in n) of minimal elements.*

Thus, ideals of X^* cannot be complemented in polynomial-time, even in the simple case where X is a two-symbol alphabet.

Proof. Since $\odot$ is associative, $\complement{\downarrow}(ab)^n = (\complement{\downarrow}(ab)^{n-1}) \odot (\complement{\downarrow}ab) = (\complement{\downarrow}(ab)^{n-1}) \odot (\uparrow ba \cup \uparrow bb \cup \uparrow aa)$. This identity suggests to proceed by induction.

Let $\bigcup_{i=1}^{m} \uparrow \boldsymbol{u}_i$ be the canonical decomposition of $\complement{\downarrow}(ab)^n$. Define the subsets of indexes $S_{\boldsymbol{v}} = \{i \in [m] \mid \boldsymbol{v} \text{ is a suffix of } \boldsymbol{u}_i\}$.

$$
\begin{aligned}
\complement{\downarrow}(ab)^{n+1} =& (\complement{\downarrow}(ab)^n) \odot (\uparrow ba \cup \uparrow bb \cup \uparrow aa) \\
=& (\bigcup_{i=1}^{m} \uparrow \boldsymbol{u}_i) \odot (\uparrow ba \cup \uparrow bb \cup \uparrow aa) \\
=& (\bigcup_{i \in S_{aa}} \uparrow \boldsymbol{u}_i) \odot (\uparrow ba \cup \uparrow bb \cup \uparrow aa) \cup \\
& \quad (\bigcup_{i \in S_{ba}} \uparrow \boldsymbol{u}_i) \odot (\uparrow ba \cup \uparrow bb \cup \uparrow aa) \cup \\
& \quad\quad (\bigcup_{i \in S_{b}} \uparrow b\boldsymbol{u}_i) \odot (\uparrow ba \cup \uparrow bb \cup \uparrow aa) \\
=& (\bigcup_{i \in S_{aa}} \uparrow \boldsymbol{u}_i ba \cup \uparrow \boldsymbol{u}_i bb \cup \uparrow \boldsymbol{u}_i a) \cup \\
& \quad (\bigcup_{i \in S_{ba}} \uparrow \boldsymbol{u}_i ba \cup \uparrow \boldsymbol{u}_i bb \cup \uparrow \boldsymbol{u}_i a) \cup \\
& \quad\quad (\bigcup_{i \in S_{b}} \uparrow \boldsymbol{u}_i a \cup \uparrow \boldsymbol{u}_i b \cup \uparrow \boldsymbol{u}_i aa)
\end{aligned}
$$

This last step follow from the particular form that Lemma 6.1.8 takes when $X = A$ a finite alphabet: indeed, for $a, b \in A$, either $a \neq b$ and $\uparrow_A a \cap \uparrow_A b = \emptyset$ which means $\uparrow \boldsymbol{v}a \odot \uparrow b\boldsymbol{w} = \uparrow \boldsymbol{v}ab\boldsymbol{w}$; or $a = b$ in which case $\uparrow \boldsymbol{v}a \odot \uparrow a\boldsymbol{w} = \uparrow \boldsymbol{v}aa\boldsymbol{w} \cup \uparrow \boldsymbol{v}a\boldsymbol{w} = \uparrow \boldsymbol{v}a\boldsymbol{w}$ since $\boldsymbol{v}a\boldsymbol{w} \leq \boldsymbol{v}aa\boldsymbol{w}$.

Now, observe that for $i \in S_{aa} \cup S_{ba}$, $\boldsymbol{u}_i a \leq \boldsymbol{u}_i ba$; and for $i \in S_b$, $\boldsymbol{u}_i a \leq \boldsymbol{u}_i aa$, thus we obtain:

$$
\complement{\downarrow}(ab)^{n+1} = (\bigcup_{i \in S_{aa}} \uparrow \boldsymbol{u}_i bb \cup \uparrow \boldsymbol{u}_i a) \cup (\bigcup_{i \in S_{ba}} \uparrow \boldsymbol{u}_i bb \cup \uparrow \boldsymbol{u}_i a) \cup (\bigcup_{i \in S_{b}} \uparrow \boldsymbol{u}_i a \cup \uparrow \boldsymbol{u}_i b) \tag{6.4}
$$

There is one last less obvious redundancy: for $n \geq 2$ and $i \in S_{ba}$, there exists $\boldsymbol{u}'_i$ in the canonical decomposition of $\complement(\downarrow(ab)^{n-1})$ such that $\boldsymbol{u}_i = \boldsymbol{u}'_i a$. Indeed, we see in Equation 6.4 that a's can only be added one by one. Thus, $\boldsymbol{u}'_i$ having b as a suffix, there exists $j \in [m]$ such that $\boldsymbol{u}_j = \boldsymbol{u}'_i b$. This entails $j \in S_b$, and thus $\boldsymbol{u}_j b = \boldsymbol{u}'_i bb$ appears in the decomposition of $\complement\downarrow(ab)^{n+1}$. Since $\boldsymbol{u}'_i bb \leq \boldsymbol{u}'_i abb = \boldsymbol{u}_i bb$, the element $\boldsymbol{u}_i bb$ is not minimal in the decomposition and can be removed. We finally obtain:

$$\complement\downarrow(ab)^{n+1} = (\bigcup_{i\in S_{aa}} \uparrow\boldsymbol{u}_i bb \cup \uparrow\boldsymbol{u}_i a) \cup (\bigcup_{i\in S_{ba}} \uparrow\boldsymbol{u}_i a) \cup (\bigcup_{i\in S_b} \uparrow\boldsymbol{u}_i a \cup \uparrow\boldsymbol{u}_i b) \tag{6.5}$$

(6.6)

We now prove that the decomposition above is indeed minimal. First, $\boldsymbol{u}_i bb \leq \boldsymbol{u}_j a$ or $\boldsymbol{u}_i bb \leq \boldsymbol{u}_j b$ imply $\boldsymbol{u}_i b \leq \boldsymbol{u}_j$ which is impossible since the decomposition $\bigcup_{i=1}^m u_i$ is canonical, i.e. the u_i's are incomparable. Moreover, $\boldsymbol{u}_i bb \leq \boldsymbol{u}_j bb$ implies $\boldsymbol{u}_i \leq \boldsymbol{u}_j$ which implies $i = j$ since $\bigcup_{i=1}^m \uparrow\boldsymbol{u}_i$ is the canonical decomposition of $\complement\downarrow(ab)^n$. Similarly, $\boldsymbol{u}_i a \leq \boldsymbol{u}_j b$ and $\boldsymbol{u}_i a \leq \boldsymbol{u}_j bb$ are impossible, and $\boldsymbol{u}_i a \leq \boldsymbol{u}_j a$ implies $i = j$. The only non trivial case is when $\boldsymbol{u}_i b \leq \boldsymbol{u}_j bb$. This implies that $i \in S_b$ and $j \in S_{aa}$, and of course that $\boldsymbol{u}_i \leq \boldsymbol{u}_j b$. Again, assume $n \geq 2$, and denote by $\boldsymbol{u}'_i$ and $\boldsymbol{u}'_j$ the minimal elements of $\complement\downarrow(ab)^{n-1}$ from which $\boldsymbol{u}_i$ and $\boldsymbol{u}_j$ are respectively built. Then, $\boldsymbol{u}_j = \boldsymbol{u}'_j a$ and a is a suffix of $\boldsymbol{u}'_j$. As for $\boldsymbol{u}_i$, it is either equal to $\boldsymbol{u}'_i b$, and b is a suffix of $\boldsymbol{u}'_i$; or to $\boldsymbol{u}'_i bb$, in which case aa is a suffix of $\boldsymbol{u}'_i$. In the first case, we have $\boldsymbol{u}'_i b \leq \boldsymbol{u}'_j ab$ which implies $\boldsymbol{u}'_i \leq \boldsymbol{u}'_j$, thus $\boldsymbol{u}'_i = \boldsymbol{u}'_j$ by canonicity of the decomposition at rank $n-1$, but this is impossible since one ends with a and the other with b. In the second case, $\boldsymbol{u}'_i bb \leq \boldsymbol{u}'_j ab$, which implies $\boldsymbol{u}'_i b \leq \boldsymbol{u}'_j$, which leads to the same kind of impossibility.

In conclusion, the decomposition given in Equation 6.5 is canonical, and its number of element is given by $u_n + v_n + w_n \stackrel{\text{def}}{=} |S_{aa}| + |S_{ba}| + |S_b|$, where the sequences are inductively defined by:

$$\begin{aligned} u_{n+1} &= u_n + v_n \\ v_{n+1} &= w_n \\ w_{n+1} &= w_n + u_n \end{aligned}$$

Thus, $U_n = \begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix} = A^n U_0$ where $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$. This matrix has only one real eigenvalue $\lambda \simeq 1.75488 > 1$ and two conjugate complex eigenvalues $0.122561 \pm 0.744862i$ of absolute value strictly smaller than λ. As a consequence, λ^n will asymptotically dominate the expression, and the sequences u_n, v_n and w_n are exponential in n. □

6.1.2 A proof of Theorem 6.1.1

It is not difficult to see that atoms indeed are ideals (downward-closed and directed), and that $Idl(X^*, \leq_*)$ is closed under products. Therefore, products of atoms all are ideals, and our objective is to prove the other inclusion: all ideals of $(X^*, \leq_*)$ can be written as a finite product of atoms.

Propositions 6.1.4 and 6.1.5 do not actually rely on the structure of ideals. They can be understood as:

- The complement of a filter is a finite product of atoms.

- The finite products of atoms are closed under intersections.

Let $\boldsymbol{I} \in Idl(X^*, \leq_*)$. Its complement $\complement\boldsymbol{I}$ is upward-closed, and can therefore be decomposed $\complement\boldsymbol{I} = \bigcup_i F_i$ as a finite union of filters. It follows that $\boldsymbol{I} = \complement(\complement\boldsymbol{I}) = \bigcap_i \complement F_i$. The downward-closed sets $\complement F_i$ are finite unions of finite products of atoms (Proposition 6.1.4), and their intersection is also a finite union of finite product of atoms (Proposition 6.1.5). Finite products of atoms being ideals, $\boldsymbol{I}$ can be written as a finite union of ideals of $(X^*, \leq_*)$. But since ideals are irreducible (Proposition 2.2.1), $\boldsymbol{I}$ is a finite product of atoms.

6.1.3 Canonical Ideal Decomposition

Note that when X is the finite alphabet $\{a, b\}$, then $(a+\epsilon)(a+b)^* = (a+b)^*$, thus the representations we use for ideals are not unique. Intuitively, the expression $(a+\epsilon)$ is subsumed by $(a+b)^*$. In general, if $\boldsymbol{A}$ is an atom and D is downward-closed in X such that $\boldsymbol{A} \subseteq D^*$, then $\boldsymbol{A}D^* = D^*\boldsymbol{A} = D^*$. Subsequently, we show that these are the only cause of non-uniqueness: avoiding such redundancies, every ideal has a unique representation (assuming unique representations for ideals of X).

Below, we use letters such as $\mathtt{A}, \mathtt{P}$, etc to denote sequences of atoms (syntax), and corresponding letters such as $\boldsymbol{A}$, $\boldsymbol{P}$, etc to denote the ideals obtained by taking the product (semantic). For example if $\mathtt{P} = (\mathtt{A}_1, \mathtt{A}_2, \ldots, \mathtt{A}_n)$, then $\boldsymbol{P} = \boldsymbol{A}_1\boldsymbol{A}_2\ldots\boldsymbol{A}_n$. Thus it is possible to have $\mathtt{P}, \mathtt{Q}$ such that $\mathtt{P} \neq \mathtt{Q}$ but $\boldsymbol{P} = \boldsymbol{Q}$.

Definition 6.1.11. *A sequence of atoms $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_n$ is said to be* reduced *if for all i, the following hold:*

- $\boldsymbol{A}_i \neq \{\epsilon\} = \emptyset^*$.
- *If $i+1 \leq n$ and $\boldsymbol{A}_{i+1}$ is some D^*, then $\boldsymbol{A}_i \not\subseteq \boldsymbol{A}_{i+1}$.*
- *If $i-1 \geq 1$ and $\boldsymbol{A}_{i-1}$ is some D^*, then $\boldsymbol{A}_i \not\subseteq \boldsymbol{A}_{i-1}$.*

Every ideal has a reduced decomposition into atoms, since any decomposition can be converted to a reduced one by dropping atoms which are redundant as per Definition 6.1.11. It remains to show uniqueness of the reduced representation:

Theorem 6.1.12. *If $\mathtt{P}$ and $\mathtt{Q}$ are reduced sequences of atoms such that $\boldsymbol{P} = \boldsymbol{Q}$, then $\mathtt{P} = \mathtt{Q}$.*

Proof. By induction on $|\mathtt{P}| + |\mathtt{Q}|$. The result is trivial if $|\mathtt{P}| \leq 1$ or $|\mathtt{Q}| \leq 1$.

Otherwise, let us write $\mathtt{P}$ as $\mathtt{A}_1\mathtt{A}_2\mathtt{P}'$ and $\mathtt{Q}$ as $\mathtt{B}_1\mathtt{B}_2\mathtt{Q}'$.

We first show that $\boldsymbol{A}_1 = \boldsymbol{B}_1$. If $\boldsymbol{A}_1 \not\subseteq \boldsymbol{B}_1$, since $\boldsymbol{P} \subseteq \boldsymbol{Q}$, the inclusion test described in Proposition 6.1.3 gives us $\boldsymbol{P} \subseteq \boldsymbol{B}_2\boldsymbol{Q}' \subseteq \boldsymbol{B}_1\boldsymbol{B}_2\boldsymbol{Q}' \subseteq \boldsymbol{P}$, so $\boldsymbol{P} = \boldsymbol{B}_2\boldsymbol{Q}'$, and the induction hypothesis then yields $\mathtt{P} = \mathtt{B}_2\mathtt{Q}'$. Similarly, if $\boldsymbol{B}_1 \not\subseteq \boldsymbol{A}_1$, then $\mathtt{Q} = \mathtt{A}_2\mathtt{P}'$. In particular, $\boldsymbol{A}_1$ and $\boldsymbol{B}_1$ cannot be incomparable, otherwise $\mathtt{Q} = \mathtt{B}_1\mathtt{B}_2\mathtt{Q}' = \mathtt{B}_1\mathtt{P} = \mathtt{B}_1\mathtt{A}_1\mathtt{A}_2\mathtt{P}' = \mathtt{B}_1\mathtt{A}_1\mathtt{Q}$, which is impossible since $\mathtt{Q}$ and $\mathtt{B}_1\mathtt{A}_1\mathtt{Q}$ do not even have the same length. Hence, $\boldsymbol{B}_1$ must contain or be contained in $\boldsymbol{A}_1$. Without loss of generality, we assume $\boldsymbol{B}_1 \subseteq \boldsymbol{A}_1$. For the sake of contradiction, let us assume that $\boldsymbol{A}_1 \not\subseteq \boldsymbol{B}_1$. In that case, we have seen that $\mathtt{P} = \mathtt{B}_2\mathtt{Q}'$, which in particular implies

$\mathtt{A}_1 = \mathtt{B}_2$. Since $\boldsymbol{B}_1 \subseteq \boldsymbol{A}_1 = \boldsymbol{B}_2$, and $\mathtt{Q}$ is reduced, $\mathtt{B}_2$ cannot be of the form D^*, hence is equal to $I_2 + \epsilon$ for some ideal I_2 of X. Since $\boldsymbol{B}_1 \subseteq \boldsymbol{B}_2$, $\mathtt{B}_1$ cannot be of the form D^* either, and must therefore be equal to $I_1 + \epsilon$ for some ideal I_1 of X. Moreover, $I_1 \subseteq I_2$. We apply Proposition 6.1.3 to the inclusion of $\boldsymbol{Q} = \boldsymbol{B}_1\boldsymbol{B}_2\boldsymbol{Q}'$ in $\boldsymbol{P} = \boldsymbol{A}_1\boldsymbol{A}_2\boldsymbol{P}' = \boldsymbol{B}_2\boldsymbol{A}_2\boldsymbol{P}'$ and we obtain that $\boldsymbol{B}_2\boldsymbol{Q}' \subseteq \boldsymbol{A}_2\boldsymbol{P}'$. From the inclusions $\boldsymbol{B}_2\boldsymbol{Q}' \subseteq \boldsymbol{A}_2\boldsymbol{P}' \subseteq \boldsymbol{P} = \boldsymbol{B}_2\boldsymbol{Q}'$, we deduce that $\boldsymbol{A}_2\boldsymbol{P}' = \boldsymbol{B}_2\boldsymbol{Q}'$, hence by induction hypothesis $\mathtt{A}_2\mathtt{P}' = \mathtt{B}_2\mathtt{Q}'$. This is impossible since $\mathtt{P} = \mathtt{B}_2\mathtt{Q}'$, which implies that $\mathtt{P} = \mathtt{A}_2\mathtt{P}'$, which contradicts $\mathtt{P} = \mathtt{A}_1\mathtt{A}_2\mathtt{P}'$.

We now want to show that $\boldsymbol{A}_2\boldsymbol{P}' = \boldsymbol{B}_2\boldsymbol{Q}'$. Since the situation is symmetric, we only prove one inclusion. We distinguish two cases.

1. If $\boldsymbol{A}_1$ is of the form $I + \epsilon$, then so is $\boldsymbol{B}_1$ and Proposition 6.1.3 directly implies $\boldsymbol{A}_2\boldsymbol{P}' \subseteq \boldsymbol{B}_2\boldsymbol{Q}'$.

2. Otherwise, $\boldsymbol{A}_1$ is of the form D^*, in which case $\boldsymbol{A}_2 \not\subseteq \boldsymbol{A}_1 = \boldsymbol{B}_1$, because $\mathtt{P}$ is reduced. Therefore, by Proposition 6.1.3, $\boldsymbol{A}_2\boldsymbol{P}' \subseteq \boldsymbol{B}_2\boldsymbol{Q}'$.

By symmetry, we obtain $\boldsymbol{A}_2\boldsymbol{P}' = \boldsymbol{B}_2\boldsymbol{Q}'$ and conclude the proof with the induction hypothesis. □

6.1.4 Concluding Remarks

Complexity In conclusion, we have shown that all of the four main set-theoretic operations (intersection of filters and ideals, complements of filters and ideals) require exponential-time, and already for rather simple WQOs: in the most common case of sequences over a finite alphabet, already three among these four operations are exponential. Only, the quasi-ordering and ideal inclusion can be decided in polynomial time.

References and Related Work The quasi-ordering $\leq_*$ was studied by Higman in [1] where he proved that $(X^*, \leq_*)$ is a WQO if and only if $(X, \leq)$ is.

The structure of the ideals of $(X^*, \leq_*)$ was first studied by Jullien in [33], in the case where X is a finite alphabet. His proof is essentially the one we sketched at the end of Section 6.1.2. His results were later generalized to any WQO X by Kabil and Pouzet in [12]. They present a different proof, and further generalizations of this result to quasi-orderings that are out of scope of this thesis.

Abdulla, Bouajjani and Jonsson independently implicitly rediscovered the structure of the ideals of $(A^*, \leq_*)$, where A is a finite alphabet, in [17]. They use the fact, due to Higman, that downward-closed languages are regular, and prove by induction over regular expressions that for every regular expression recognizing a downward-closed language, there exists a *simple regular expression (SRE)* recognizing the same language, where simple regular expressions are exactly finite unions of finite products of atoms.

They also provide a linear-time algorithm to decide inclusion between downward-closed sets represented as SREs, and they define the same normal form as ours for SREs, which is computable in quadratic-time from any other representation. In [19], Abdulla et al. prove that downward-closed sets can be represented as SREs using the same proof as the one Jullien presented in [33], i.e. which we generalized for any WQO X at the end of Section 6.1.2. In particular, this proof requires to express $\complement \uparrow \boldsymbol{w}$ as an SRE and to show that SREs are closed under intersection. In other terms, they essentially prove (CF) and (II).

In [18], Abdulla et al. use the WQO $((A^{\circledast})^*, \leq_*)$, where A is a finite alphabet, and finite multisets over A (see Section 7.1) are quasi-ordered with $\leq_{\mathrm{emb}}$. They provide a structure to represent downward-closed sets of $(A^{\circledast}, \leq_{\mathrm{emb}})$ and $((A^{\circledast})^*, \leq_*)$ which is essentially the one obtained when composing results from this chapter with Section 7.1.

Here also, these results have been generalized to Noetherian spaces in [13]. The structure of the ideals then is still the same in this context.

Finally, we would like to point out that some alternative representations of downward-closed sets are investigated, in particular in the case of finite sequences over a finite alphabet, since it is the most common case (with motivations coming from language theory). For instance in [34], the authors represent closed sets with automata, and study the state complexity of closure operations on regular languages (represented as deterministic, non deterministic or alternating automata).

6.2 Finite Sequences under Stuttering

Let $(X, \leq)$ be a WQO. Its sequence extension under the stuttering quasi-order (or simply stuttering extension) is $(X^*, \leq_{\mathrm{st}})$, where X^*, as before, is the set of all finite sequences from X. The quasi-ordering $\leq_{\mathrm{st}}$ over X^* is defined by

$$x_1 \dots x_n \leq_{\mathrm{st}} y_1 \dots y_m \overset{\mathrm{def}}{\Leftrightarrow} \exists f : [n] \to [m] \text{ increasing} .\ \forall i \in [n].\ x_i \leq y_{f(i)}$$

The only difference with $\leq_*$ is that we do not require the witness f to be strictly increasing, but only increasing. For instance, if $X = \{a, b\}$ is a finite alphabet, then $aabbaa \leq_{\mathrm{st}} aba \leq_{\mathrm{st}} aabbaa$ but $aabbaa \not\leq_{\mathrm{st}} ab$. Or with $X = \mathbb{N}$, $1 \cdot 1 \cdot 1 \leq_{\mathrm{st}} 2$. Note that even if $(X, \leq)$ is a partial-order, $(X^*, \leq_{\mathrm{st}})$ need not be (e.g. $2 \cdot 2 \leq_{\mathrm{st}} 2 \leq_{\mathrm{st}} 2 \cdot 2$).

Another way to define this quasi-ordering is the following: define the stuttering equivalence relation $\sim_{\mathrm{st}}$ on X^* as the smallest equivalence relation such that for all $\boldsymbol{u}, \boldsymbol{v} \in X^*$ and $a \in X$, $\boldsymbol{u}a\boldsymbol{v} \sim_{\mathrm{st}} \boldsymbol{u}aa\boldsymbol{v}$. Informally, this equivalence does not distinguish between words which differ only in the number of times consecutive characters are repeated. Then, $\leq_{\mathrm{st}} = \leq_* \circ \sim_{\mathrm{st}}$, where $\circ$ denotes the composition of relations, as defined in Section 4.2. However, the results from Section 4.2 cannot be applied to this quasi-ordering since $\leq_{\mathrm{st}} \neq \sim_{\mathrm{st}} \circ \leq_*$. If X is a finite alphabet, this equation holds and $(X^*, \leq_{\mathrm{st}})$ can be treated as a quotient. Also observe that $\sim_{\mathrm{st}}$ is *not* the same as the equivalence relation $\equiv_{\mathrm{st}} = \leq_{\mathrm{st}} \cap \geq_{\mathrm{st}}$ induced by the quasi-ordering, even if $(X, \leq)$ is a partial-order $\leq$. For instance, if $a \leq b$ in X, then $ab \equiv_{\mathrm{st}} b$ in X^*, but $ab \sim_{\mathrm{st}} b$ does not hold. However the inclusion $\sim_{\mathrm{st}} \subseteq \equiv_{\mathrm{st}}$ is always valid.

6.2.1 The Stuttering Extension is Ideally Effective

Obviously, $\leq_{\mathrm{st}}$ is an extension of $\leq_*$, thus $\leq_{\mathrm{st}}$ is a WQO and Section 4.1 applies. That is, the ideals of $(X^*, \leq_{\mathrm{st}})$ are of the form $\downarrow_{\leq_{\mathrm{st}}} I$ for I an ideal of $(X^*, \leq_*)$. Moreover,

- if D is a downward-closed subset of X, then $\downarrow_{\leq_{\mathrm{st}}} D^* = D^*$,
- if I is an ideal of $(X, \leq)$, then $\downarrow_{\leq_{\mathrm{st}}} (I + \epsilon) = I^*$,
- if $\boldsymbol{P}_1$ and $\boldsymbol{P}_2$ are ideals of $(X^*, \leq_*)$ (cf. Section 6.1), then $\downarrow_{\leq_{\mathrm{st}}} (\boldsymbol{P}_1 \cdot \boldsymbol{P}_2) = (\downarrow_{\leq_{\mathrm{st}}} \boldsymbol{P}_1) \cdot (\downarrow_{\leq_{\mathrm{st}}} \boldsymbol{P}_2)$.

Therefore, the downward closure for $\leq_{\mathrm{st}}$ of an ideal of $(X^*, \leq_*)$ can be written as a product of atoms of the form D^*, the atoms of the form $(I + \epsilon)$ being transformed into I^*.

Lemma 6.2.1. *Ideals of* $(X^*, \leq_{\mathrm{st}})$ *are products* $D_1^* \cdots D_n^*$*, for* $D_i \in \mathit{Down}(X)$.

Assuming we have a representation for X and $\mathit{Idl}(X)$, we can use the same representation of X^* as before, and the lemma above suggests a simple representation for ideals of $(X^*, \leq_{\mathrm{st}})$: as lists of downward-closed sets of $(X, \leq)$.

Theorem 6.2.2. *With the above representations, the stuttering extension is an ideally effective construction. It is not polynomial-time in general. Given a polynomial-time presentation of an ideally effective WQO* $(X, \leq)$*, we can compute an exponential-time presentation of* $(X^*, \leq_{\mathrm{st}})$.

Proof. Let $(X, \leq)$ be an ideally effective WQO. Then $(X^*, \leq_*)$ is ideally effective as well. Therefore, in the light of Theorem 4.1.2, to prove that the stuttering extension is an ideally effective construction, it suffices to show that the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ introduced in Section 4.1 are computable in this particular context. The fact that the stuttering extension is not a polynomial-time construction follows from the complexity lower bounds presented in Section 6.2.3. To prove the last part of the theorem, i.e. that we can compute an exponential-time presentation of $(X^*, \leq_{\mathrm{st}})$ when $(X, \leq)$ is a polynomial-time ideally effective WQO, we rely on Lemma 4.1.3.

The function $\mathcal{C}l_{\mathrm{I}}$ is easily shown computable using the equations above: given a product of atoms $\boldsymbol{P} = \boldsymbol{A}_1 \cdots \boldsymbol{A}_n \in \mathit{Idl}(X^*, \leq_*)$,

$$\mathcal{C}l_{\mathrm{I}}(\boldsymbol{P}) = \downarrow_{\leq_{\mathrm{st}}} \boldsymbol{P} = (\downarrow_{\leq_{\mathrm{st}}} \boldsymbol{A}_1) \cdots (\downarrow_{\leq_{\mathrm{st}}} \boldsymbol{A}_n)$$

and the image of an atom by $\mathcal{C}l_{\mathrm{I}}$ is obtained by $\mathcal{C}l_{\mathrm{I}}(D^*) = \downarrow_{\leq_{\mathrm{st}}} D^* = D^*$ for $D \in \mathit{Down}(X)$ and $\mathcal{C}l_{\mathrm{I}}(I + \epsilon) = I^*$ for $I \in \mathit{Idl}(X)$. Thus $\mathcal{C}l_{\mathrm{I}}$ is computable in linear-time.

The function $\mathcal{C}l_{\mathrm{F}}$ is computable as well, although less straight-forward: given $\boldsymbol{u} = x_1 \cdots x_n \in X^*$,

$$\mathcal{C}l_{\mathrm{F}}(\boldsymbol{u}) \;=\; \uparrow_{\mathrm{st}} \boldsymbol{u} \;=\; \uparrow_* \left\{ y_1 \cdots y_k \;\middle|\; \begin{array}{c} 0 \leq k \leq n \\ 0 = i_0 < i_1 < \cdots < i_k = n \\ \forall j \in [k].\; y_j \in \min(\bigcap_{i_{j-1} < \ell \leq i_j} \uparrow_X x_\ell) \end{array} \right\}$$

Intuitively, the set ranges over all ways to cut $\boldsymbol{u}$ in k pieces (factor), and embeds the i-th piece entirely into the same element y_i.

Note that the expression above is the fully generic formula to describe the function $\mathcal{C}l_{\mathrm{F}}$ for any X. Since there are exponentially many families of indexes i_j to range over, this expression is computable in exponential-time. In Section 6.2.3, we show that this blow-up is unavoidable, already for a WQO as simple as $\mathbb{N}^2$. However, in simple cases, $\mathcal{C}l_{\mathrm{F}}(\boldsymbol{w})$ takes a much simpler form and is computable in linear-time. For instance, for $X = \mathbb{N}$ ordered naturally, $\mathcal{C}l_{\mathrm{F}}(x_1 \cdots x_n) = \uparrow_*(\max_{1\leq i\leq n} x_i)$, and for $X = A$ a finite alphabet, $\mathcal{C}l_{\mathrm{F}}(\boldsymbol{w}) = \uparrow_* \boldsymbol{v}$ where $\boldsymbol{v}$ is the shortest (in length) element of the class of $\boldsymbol{w}$ for $\sim_{st}$ (that is, $\boldsymbol{v}$ is the word $\boldsymbol{w}$ where we remove all stuttering). Indeed, when X is a finite alphabet, we have seen that $\leq_{\mathrm{st}}$ can be obtained as a quotient of $\leq_*$ with the equivalence relation $\sim_{\mathrm{st}}$. And we have seen in Section 4.2 that in the case of a quotient, $\mathcal{C}l_{\mathrm{F}}$ simply outputs the closure of a given filter under the equivalence relation. Here, any class of $\sim_{\mathrm{st}}$ has indeed a unique minimal element for $\leq_*$, which is obtained from any member of the class from removing stuttering.

We now prove the correction of the above expression for the function $\mathcal{C}l_{\mathrm{F}}$. The right-to-left inclusion being obvious, we focus on the other inclusion. Given $\boldsymbol{w} \geq_{\mathrm{st}} x_1 \cdots x_n$, there exist an increasing mapping p from $[n]$ to $[|\boldsymbol{w}|]$ such that each x_i is associated to a greater element in $\boldsymbol{w}$. Denoting the image of p by $\{y_1, \ldots, y_k\}$, this entails a decomposition of $\boldsymbol{w} = \boldsymbol{w}_0 y_1 \boldsymbol{w}_1 y_2 \cdots y_k \boldsymbol{w}_k$ where the y_i's are in X and the $\boldsymbol{w}_i$'s in X^*. Further define i_j to be the greatest i such that $p(i) = j$ (i.e. the index of the right-most symbol of $x_1 \cdots x_n$ to be mapped to y_j). It follows that $0 = i_0 < i_1 < \cdots < i_k = n$, and for all $\ell \in [n]$ and $j \in [k]$, $i_{j-1} < \ell \leq i_j \Rightarrow x_\ell \leq y_j$. Then $\boldsymbol{w} \geq_* y_1 \cdots y_k$ which is indeed an element of the set described in the proposition.

In conclusion, the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ introduced in Section 4.1 are computable, therefore, by Theorems 4.1.2 and 6.1.2, stuttering extension is an ideally effective construction. As mentioned at the beginning of the proof, the fact that it is not a polynomial-time construction will follow from Section 6.2.3 where we provide exponential lower bounds for several operations in $(A^*, \leq_{\mathrm{st}})$, the stuttering extension of a finite alphabet $(A, =)$. The latter being a polynomial-time ideally effective WQO, it proves that stuttering extension does not preserve the polynomial-time complexity of WQOs. Note that per our definition of polynomial-time construction, an exponential lower bound for only one operation of $(A^*, \leq_{\mathrm{st}})$ would have been enough to conclude. But we provide a complete complexity analysis of a presentation of $(X^*, \leq_{\mathrm{st}})$. Notably, in Section 6.2.2, we provide polynomial-time upper bounds when possible.

But for now, let us simply prove the last part of the theorem: let $(X, \leq)$ be an ideally effective WQO given by a polynomial-time presentation. Let us prove that the presentation of $(X^*, \leq_{\mathrm{st}})$ implicitly described above (through Theorem 4.1.2 is indeed exponential-time. It suffices to observe that we are in the setting of Lemma 4.1.3. Indeed, if we have a polynomial-time presentation of $(X, \leq)$, then we can compute an exponential-time presentation of $(X^*, \leq_*)$ using Theorem 6.1.2. Secondly, the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ described above can obviously be computed in exponential-time. Thirdly, observe that for any $\boldsymbol{u} \in X^*$, every filter in the filter decomposition of $\mathcal{C}l_{\mathrm{F}}(\boldsymbol{u})$ as an upward-closed set of $(X^*, \leq_*)$ is of linear size in $|\boldsymbol{u}|$: to describe $\mathcal{C}l_{\mathrm{F}}(\boldsymbol{u})$ we used sequences $y_1 \cdots y_k$ for $k \leq n$ whose elements y_i are obtained using a polynomial number of filter intersection in the polynomial-time WQO $(X, \leq)$. Therefore, elements y_i have encodings whose size are bounded by a polynomial in the size of elements of $\boldsymbol{u}$. Finally, the function $\mathcal{C}l_{\mathrm{I}}$ being computable in linear time, its output is of course of linear size at most.

The four assumptions from Lemma 4.1.3 being fulfilled, we have proved that

$(X^*, \leq_{\mathrm{st}})$ has an exponential-time presentation. However, not all procedures in this presentation are actually exponential-time. We refine this statement in the next two subsections, by providing for each operation in $(X^*, \leq_{\mathrm{st}})$ either an exponential-time lower bound (matching the upper bound we have just shown) or a polynomial-time upper bound. $\square$

6.2.2 Better Complexity Upper Bounds

Let $(X, \leq)$ be a polynomial-time ideally effective WQO. In this subsection, we provide better upper bounds for the procedures of the ideally effective WQO $(X^*, \leq_{\mathrm{st}})$.

The presentation of $(X^*, \leq_{\mathrm{st}})$ we have given in the proof above is obtained from a presentation of $(X, \leq)$ as a somewhat abstract composition of the proof of Theorems 6.1.2 and 4.1.2. But of course, the structure of $(X^*, \leq_{\mathrm{st}})$ is quite simple and can be understood directly.

Notably, the quasi-ordering $\leq_{\mathrm{st}}$ can be decided using a linear number of comparison in X, searching for the *left-most embedding*, as we did to decide $\leq_*$. Similarly, ideals of $(X^*, \leq_{\mathrm{st}})$ are in particular ideals of $(X^*, \leq_*)$ (they are products of atoms of the form D^* for $D \in \mathit{Down}(X)$), and thus ideal inclusion can be decided using the polynomial-time procedures given in Proposition 6.1.3. Finally, the function that maps $\boldsymbol{u} \in X^*$ to $\downarrow_{\mathrm{st}} \boldsymbol{u}$ is quite simple as well: if $\boldsymbol{u} = x_1 \cdots x_n$, then $\downarrow_{\mathrm{st}} \boldsymbol{u} = (\downarrow_X x_1)^* \cdots (\downarrow_X x_n)^*$.

Note that there is a more abstract way to understand these three results. Looking closely at the proof of Theorem 4.1.2, one may notice that these three operations ((OD), (ID), (PI)) can be performed using only the function $\mathcal{C}l_{\mathrm{I}}$, which can be computed in linear-time here. Moreover, these three operations could also be performed in polynomial-time in $(X^*, \leq_*)$ (remember we assumed $(X, \leq)$ is a polynomial-time ideally effective WQO). Therefore it is no surprise that the composition of the two can still be performed in polynomial-time.

Next, we give a polynomial-time procedure to complement filters:

Proposition 6.2.3. (CF)*:* $X^* \setminus \uparrow_{\mathrm{st}}(x_1 \cdots x_n) = (X \setminus \uparrow x_1)^* \cdots (X \setminus \uparrow x_n)^*$

Proof. $(\subseteq)$ Let $y_1 \cdots y_m$ that is not greater than $x_1 \cdots x_n$ for $\leq_{\mathrm{st}}$. Consider $f : [k] \to [m]$ (for some $k < n$) the longest left-most embedding of $x_1 \cdots x_n$ into $y_1 \cdots y_m$, that is $x_1 \cdots x_k \leq_{\mathrm{st}} y_1 \cdots y_m$ but $x_1 \cdots x_k \cdot x_{k+1} \not\leq_{\mathrm{st}} y_1 \cdots y_m$. Since this is the left-most embedding, the elements y_i for $i < f(1)$ are not in $\uparrow_X x_1$, and thus $y_1 \cdots y_{f(1)-1} \in (\complement \uparrow_X x_1)^*$. Similarly, $y_{f(1)} \cdots y_{f(2)-1} \in (\complement \uparrow_X x_2)^*$ (consider this sequence to be empty if $f(1) = f(2)$). And so on, up to $y_{f(k)} \cdots y_m \in (\complement \uparrow_X x_{k+1})^*$, since otherwise we would have $x_1 \cdots x_k \cdot x_{k+1} \leq_{\mathrm{st}} y_1 \cdots y_m$. In the end we have shown that $y_1 \cdots y_m \in (\complement \uparrow_X x_1)^* \cdots (\complement \uparrow_X x_{k+1})^* \subseteq (\complement \uparrow_X x_1)^* \cdots (\complement \uparrow_X x_n)^*$.

$(\supseteq)$ Let $\boldsymbol{v} = \boldsymbol{v}_1 \cdots \boldsymbol{v}_n \in (\complement \uparrow_X x_1)^* \cdots (\complement \uparrow_X x_n)^*$, where $\boldsymbol{v}_i \in (\complement \uparrow_X x_i)^*$ for $i \in [n]$. Assume $x_1 \cdots x_n \leq_{\mathrm{st}} \boldsymbol{v}$, consider an embedding $f : [n] \to [|v|]$ that witnesses this inequality and consider the function g that maps $i \in [n]$ to $j \in [n]$ if the $f(i)$-th element of the sequence $\boldsymbol{v}$ is in $\boldsymbol{v}_j$. Then, because $\boldsymbol{v}_1 \in (\complement \uparrow_X x_1)^*$, $g(1) > 1$. Moreover, $g(2) \geq g(1) > 1$ but $v_2 \in (\complement \uparrow_X x_2)^*$ thus $g(2) > 2$. And so on by induction we show that $g(i) > i$, which is impossible for $g(n)$, reaching a contradiction and proving that $x_1 \cdots x_n \not\leq_{\mathrm{st}} \boldsymbol{v}$. $\square$

6.2.3 Complexity Lower Bounds

Previously, we have exhibited a linear-time procedure for (CF). This proves that there might exist more efficient procedures than the one obtained by composing Theorems 4.1.2 and 6.1.2. Subsequently, we show that for the three remaining operations, namely (II), (CI) and (IF), no generic polynomial-time procedure exist. That is, asymptotically, the procedures we have obtained in Theorem 6.2.2 are optimal.

Our first observation is that, unlike in the case of $(X^*, \leq_*)$, we won't be able to provide an exponential-lower bound in the simple case of a two-symbol alphabet. Indeed, when quotiented by $\sim_{\mathrm{st}}$, the structure of $\{a, b\}^*$ is very simple: there are only two words of any given size $n > 0$: $(ab)^(n/2)$ and $(ba)^(n/2)$ if n is even, $(ab)^m a$ and $(ba)^m b$ if $n = 2{*}m{+}1$. As a result, $(\{a, b\}^*, \leq_{\mathrm{st}})$ is isomorphic to $\mathbf{0} \oplus (\mathbb{N} \times \{a, b\}, \leq_{\mathrm{lex}}$). All operations are computable in polynomial-time in this WQO. We thus consider $A = \{a, b, c\}$ a three-symbol alphabet, and prove that (II), (CI) and (IF) for $(A^*, \leq_{\mathrm{st}})$ require exponential-time computations.

(II): The canonical ideal decomposition of the downward-closed set $(a^*b^*c^*)^n \cap (b^*a^*c^*)^n$ has exponential size.

Indeed, all ideals of the form $x_1^* c^* x_2^* \cdots x_n^* c^*$ for $x_i \in \{a, b\}$ are maximal for inclusion in $(a^*b^*c^*)^n \cap (b^*a^*c^*)^n$.

(CI): The upward-closed set $\complement(a^*(b{+}c)^*)^n$ has exponentially many minimal elements.

Indeed, we prove that every word $x_1 a x_2 \cdots x_n a$ for $x_i \in \{b, c\}$ is a minimal element of this upward-closed set.

Let $\boldsymbol{u} = x_1 a x_2 \cdots x_n a$ be such a word. Observe that $\boldsymbol{u} \in (a^*(b + c)^*)^n$ if and only if $I \stackrel{\text{def}}{=} x_1^* a^* \cdots x_n^* a^* \subseteq (a^*(b + c)^*)^n$. This cannot be the case: there are n occurrences of a^* on both sides, hence the a^* must be mapped to each other. That leaves no option for x_1^*. Therefore, $\boldsymbol{u} \in \complement(a^*b^*c^*)^n$.

It remains to show that $\boldsymbol{u}$ is minimal. If $\boldsymbol{v}$ is strictly smaller (for stuttering) than $\boldsymbol{u}$, then it belongs to $I_i = x_1^* a^* \cdots a^* x_i^* x_{i+1}^* a^* \cdots x_n^* a^*$ for some $i \in [n]$, or to $J_i = x_1^* a^* \cdots x_{i-1}^* a^* a^* x_{i+1}^* \cdots x_n^* a^*$ for some $i \in [n]$. The ideal I_i is I where we removed an atom a^* while J_i is I where we removed the atom x_i^*. Now, because $a^*a^* = a^*$ and $x_i^* x_{i+1}^* \subseteq (b + c)^*$, all ideals I_i and J_i are subsets of $(a^*(b + c)^*)^n$, which proves the minimality of $\boldsymbol{u}$.

(IF): The upward-closed set $\uparrow_{\mathrm{st}}(ac)^n \cap \uparrow_{\mathrm{st}}(bc)^n$ has exponentially many minimal elements. Indeed, applying Section 4.1:

$$\begin{aligned}
\uparrow_{\mathrm{st}}(ac)^n \cap \uparrow_{\mathrm{st}}(bc)^n &= \mathcal{C}l_{\mathrm{F}}((ac)^n) \cap \mathcal{C}l_{\mathrm{F}}((bc)^n) \\
&= \uparrow_*(ac)^n \cap \uparrow_*(bc)^n
\end{aligned}$$

This last set has exponentially many minimal elements (for $\leq_*$): at least one per element in $a^n \sqcup b^n$. Moreover, since there is no repetition of a letter in either $(ac)^n$ or $(bc)^n$, none of these minimal elements have repetitions either (i.e. none can be written $\boldsymbol{u} = \boldsymbol{u}_1 aa \boldsymbol{u}_2$ or $\boldsymbol{u} = \boldsymbol{u}_1 bb \boldsymbol{u}_2$). Thus, on these words, $\leq_*$ and $\leq_{\mathrm{st}}$ coincide, and these exponentially many minimal elements are also minimal for $\leq_{\mathrm{st}}$.

Finally, we provide an exponential lower bound for the function $\mathcal{C}l_{\mathrm{F}}$. In simple cases, namely when $(X, \leq)$ is either $(\mathbb{N}, \leq)$ or a finite alphabet, the function $\mathcal{C}l_{\mathrm{F}}$ is computable in polynomial-time as sketched in the proof of Theorem 6.2.2. We therefore look at the stuttering extension of $(\mathbb{N}^2, \leq_\times)$, which is the next simplest WQO we could think of.

Proposition 6.2.4. *Let $\boldsymbol{w}_n = \langle 0, n\rangle\langle 1, n-1\rangle \cdots \langle n, 0\rangle \in (\mathbb{N}^2)^*$ (it consists of all elements of $\mathbb{N}^2$ whose sum is equal to n). The set $\uparrow_{\mathrm{st}} \boldsymbol{w}_n$, where $\mathbb{N}^2$ is equipped with the product ordering, has exponentially many pairwise incomparable minimal elements for $\leq_*$. In particular, function $\mathcal{C}l_{\mathrm{F}}$ requires exponential-time to compute.*

Proof. Applying the expression of $\mathcal{C}l_{\mathrm{F}}$ given in the proof of Theorem 6.2.2:

$$
\begin{array}{lll}
\uparrow_{\mathrm{st}} w_n = & \uparrow_*\langle n, n\rangle & \cup \\
\bigcup_{i=0}^{n-1} & \uparrow_*\langle i, n\rangle\langle n, n-i-1\rangle & \cup \\
\bigcup_{0\leq i<j<n} & \uparrow_*\langle i, n-1\rangle\langle j, n-i-1\rangle\langle n, n-j-1\rangle & \cup \\
 & \cdots & \\
\bigcup_{\substack{0\leq i_1<\ldots\\<i_{k-1}<n}} & \uparrow_*\langle i_1, n-1\rangle\langle i_2, n-i_1-1\rangle\cdots(n, n-i_{k-1}-1\rangle & \cup \\
 & \cdots & \\
 & \uparrow_* \boldsymbol{w}_n &
\end{array}
$$

Each line in the above description corresponds to a value of $k \in [n]$: the first line corresponds to $k = 1$, $\boldsymbol{w}_n$ is decomposed in one piece, the second line to $k = 2$, $\boldsymbol{w}_n$ is decomposed in two pieces, etc., and the last line is obtained for $k = n$. We now argue that this decomposition of the upward closed set $\uparrow_{\mathrm{st}} \boldsymbol{w}_n$ is canonical. Because $\leq_*$ is antisymmetric here, and since all of those sequences are pairwise distinct, it suffices to show that each sequence is minimal (for $\leq_*$) in $\uparrow_{\mathrm{st}} \boldsymbol{w}_n$. Let $0 < k \leq n$ and $i_0 = 0 < i_1 < \cdots < i_{k-1} < i_k = n$, and $\boldsymbol{u} = \Pi_{j=1}^{k}\langle i_j, n-i_{j-1}-1\rangle = \langle i_1, n-1\rangle\langle i_2, n-i_1-1\rangle \cdots \langle n, n-i_{k-1}-1\rangle$. We show that if $\boldsymbol{v} <_* \boldsymbol{u}$ then $\boldsymbol{w}_n \not\leq_{\mathrm{st}} \boldsymbol{v}$. For any such $\boldsymbol{v} <_* \boldsymbol{u}$, there exists an index $1 \leq \ell \leq k$ such that $\boldsymbol{v}$ is smaller than some word obtained from $\boldsymbol{u}$ by replacing the ℓ-th symbol by a strictly smaller element. That is, $\boldsymbol{v}$ is smaller than some $\langle i_1, n-1\rangle\langle i_2, n-i_1-1\rangle \cdots \langle i_{\ell-1}, n-i_{\ell-2}-1\rangle \cdot x \cdot \langle i_{\ell+1}, n-i_\ell-1\rangle \cdots \langle n, n-i_{k-1}-1\rangle$ for some $1 \leq \ell < k$ and $x <_\times \langle i_\ell, n-i_{\ell-1}\rangle$. But then, $\boldsymbol{w}_n \not\leq_{\mathrm{st}} \boldsymbol{v}$ since letter $\langle i_\ell, n-i_\ell\rangle$ isn't smaller than any letter in $\boldsymbol{v}$. ☐

6.3 Finite Sequences on a Circle

Consider a WQO $(X, \leq)$, and define an equivalence relation $\sim_{\mathrm{cj}}$ on X^* as follows: $\boldsymbol{u} \sim_{\mathrm{cj}} \boldsymbol{v}$ iff there exist $\boldsymbol{w}, \boldsymbol{t}$ such that $\boldsymbol{u} = \boldsymbol{wt}$ and $\boldsymbol{v} = \boldsymbol{tw}$. One can imagine an equivalence class of $\sim_{\mathrm{cj}}$ as a word written on an (oriented) circle instead of a line. We can now define a notion of *subwords under conjugacy* via $\leq_{\mathrm{cj}} \stackrel{\text{def}}{=} \sim_{\mathrm{cj}} \circ \leq_*$, which is exactly the relation denoted $\preceq_c$ in [19, p.49]. We call the QO $(X^*, \leq_{\mathrm{cj}})$ the conjugacy extension of the QO $(X, \leq)$. The conjugacy extension is a WQO-preserving construction.

6.3.1 The Conjugacy Extension is Ideally Effective

Since $\leq_* \circ \sim_{\mathrm{cj}} = \sim_{\mathrm{cj}} \circ \leq_*$, the results from Section 4.2 apply to $(X^*, \leq_{\mathrm{cj}})$. Notably, assuming we can represent some set X of a WQO $(X, \leq)$ and the set $Idl(X)$ of its ideals, we know how to represent the elements of X^* (as usual) and the set of the ideals of $(X^*, \leq_{\mathrm{cj}})$.

Theorem 6.3.1. *With the above representations, the conjugacy extension is an ideally effective construction. It is not polynomial-time in general. Given a polynomial-time presentation of an ideally effective WQO* $(X, \leq)$*, we can compute an exponential-time presentation of* $(X^*, \leq_{\mathrm{cj}})$.

Proof. Let $(X, \leq)$ be an ideally effective WQO. Then $(X^*, \leq_*)$ is ideally effective as well. Therefore, in the light of Theorem 4.2.1, to prove that the conjugacy extension is an ideally effective construction, it suffices to show that the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ defined in Section 4.2 are computable in this particular context. The fact that the conjugacy extension is not a polynomial-time construction follows from the complexity lower bounds presented in Section 6.3.2. The last part of the theorem will be trivial here.

Recall from Section 4.2 that in this context, $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ simply correspond to closure under $\sim_{\mathrm{cj}}$. Notably, $\mathcal{C}l_{\mathrm{F}}(\uparrow_* \boldsymbol{w}) = \uparrow_{\mathrm{cj}} \boldsymbol{w} = \uparrow_* \overline{\boldsymbol{w}}$, where $\overline{\boldsymbol{w}}$ denotes the equivalence class of $\boldsymbol{w} \in X^*$ under $\sim_{\mathrm{cj}}$. Here, the equivalence class of some $\boldsymbol{w} \in X^*$ is given by $\{c^{(i)}(\boldsymbol{w}) \mid 1 \leq i \leq |\boldsymbol{w}|\}$, where $c^{(i)}$ designates the i-th iterate of the cycle operator $c(w_1 \cdots w_n) = w_2 \cdots w_n w_1$, which corresponds to rotating the sequence i times. Thus, the function $\mathcal{C}l_{\mathrm{F}}$ is computable in polynomial-time (linear-time if the data structure used to encode finite sequences allows to compute the cycle operator c in constant time. However, for linked lists for instance, c has a quadratic cost).

The function $\mathcal{C}l_{\mathrm{I}}$ is similar: remember ideals of $(X^*, \leq_*)$ are finite sequences of atoms, where atoms are either D^* for some downward-closed set D of X, or $I + \epsilon$, for I some ideal of X. Then, given $\boldsymbol{P} = \boldsymbol{A}_1 \cdots \boldsymbol{A}_k$ an ideal of $(X^*, \leq_*)$:

$$\mathcal{C}l_{\mathrm{I}}(\boldsymbol{P}) = \overline{\boldsymbol{P}} = \bigcup_{i=1}^{k} c^{(i)}(\boldsymbol{P}) \cdot e(\boldsymbol{A}_i)$$

where $e(D^*) = D^*$ and $e(I + \epsilon) = \epsilon$, and c is here used as the cycle operator on the set of sequences over atoms. The presence of the extra $e(\boldsymbol{A}_i)$ in the above expression might become clearer when considering a simple example as $\boldsymbol{P} = a^* b^*$. Indeed, $aabb \in \boldsymbol{P}$, thus $abba \in \mathcal{C}l_{\mathrm{I}}(\boldsymbol{P})$.

Since the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ are computable, by Theorem 4.2.1 and Theorem 6.1.2, the conjugacy extension is ideally effective. More precisely, from a polynomial-time presentation of $(X, \leq)$, we can compute an exponential-time presentation of

$(X^*, \leq_*)$ from which we can compute a presentation of $(X^*, \leq_{\mathrm{cj}})$ using Theorem 4.2.1. Moreover, since the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ are computable in polynomial-time, the latter presentation is exponential-time as well.

As in the case of the stuttering extension, we can be a little bit more precise, and mention that we actually obtain polynomial-time procedures to decide the quasi-ordering $\leq_{\mathrm{cj}}$ (OD), inclusion on $Idl(X^*, \leq_{\mathrm{cj}})$ (ID), and the principal ideal function (PI). However, for the four remaining operations, i.e. (CF), (II), (CI) and (IF), we provide in Section 6.3.2 matching exponential-time lower bounds. In particular, the conjugacy extension is not a polynomial-time construction. $\square$

6.3.2 Complexity Lower Bounds

Exponential lower bounds for $(X^*, \leq_{\mathrm{cj}})$ are obtained for the same families that were used for $(X^*, \leq_*)$.

(CF): Filters (for $\leq_*$) of sequences over a finite alphabet can be complemented in polynomial time, hence, so can filters for $\leq_{\mathrm{cj}}$ ($\mathcal{C}l_{\mathrm{F}}$ is computable in polynomial-time). Consider, as in the case of the Higman quasi-ordering, the finite ordering $(X, \leq)$ consisting of three element $0, 1$ and $1'$ such that $0 \leq 1, 1'$. Since $\uparrow_{\mathrm{cj}} 0^{n+1} = \uparrow_* 0^{n+1}$, $X^* \smallsetminus \uparrow_{\mathrm{cj}} 0^{n+1} = \bigcup_{\boldsymbol{u} \in (1+1')^n} \uparrow_{\mathrm{cj}} \boldsymbol{u}$. Moreover, given two sequences $\boldsymbol{u}, \boldsymbol{v} \in X^*$ of the same length, $\boldsymbol{u} \leq_{\mathrm{cj}} \boldsymbol{v}$ iff $\boldsymbol{u} \sim_{\mathrm{cj}} \boldsymbol{v}$. Thus, the canonical ideal decomposition of $X^* \smallsetminus 0^{n+1}$ is obtained by removing equivalent elements in the expression above. However, there are at most n sequences in the equivalence class of some sequence $\boldsymbol{u}$ of length n. Thus, the canonical ideal decomposition of the downward-closed set above has at least $2^n/n$ maximal elements.

(IF): In a similar manner, since $\uparrow_{\mathrm{cj}} a^n = \uparrow_* a^n$ and $\uparrow_{\mathrm{cj}} b^n = \uparrow_* b^n$, the canonical filter decomposition of $\uparrow_{\mathrm{cj}} a^n \cap \uparrow_{\mathrm{cj}} b^n$ has exponentially many minimal elements.

(CI): Here, we again consider the same example as in Section 6.1: complementing the family of ideals $\downarrow_{\mathrm{cj}}(ab)^n$.

Let $m \in \mathbb{N}$ and $n = 5m - 1$. Subsequently, we exhibit a family $\mathcal{F}$ elements of $\downarrow_{\mathrm{cj}}(ab)^n$ such that at least exponentially many (in m, and thus in n) members of $\mathcal{F}$ are minimal in $\downarrow_{\mathrm{cj}}(ab)^n$.

Define the family $\mathcal{F}$ as the family of sequences $\boldsymbol{u} = a^{k_1} b^{k'_1} a^{k_2} \cdots a^{k_m} b^{k'_m}$ such that for all i, $k_i \geq 2$, $k'_i \geq 2$ and $\sum_{i=1}^{m} k_i + k'_i = |u| = n + m + 1$.

Elements of $\mathcal{F}$ are in $X^* \smallsetminus \downarrow_{\mathrm{cj}}(ab)^n$. Indeed, for $p, q \in \mathbb{N}$, $a^p b^q \leq_{\mathrm{cj}} (ab)^{p+q-1}$ but $a^p b^q \not\leq_{\mathrm{cj}} (ab)^{p+q-2}$. Thus, for $\boldsymbol{u} \in \mathcal{F}$, $\boldsymbol{u} \leq_{\mathrm{cj}} (ab)^{\sum_{i=1}^{m} k_i + k'_i - m} = (ab)^{n+1}$ but $\boldsymbol{u} \not\leq_{\mathrm{cj}} (ab)^n$. It follows that all elements from $\mathcal{F}$ are minimal for $\leq_{\mathrm{cj}}$ in $X^* \smallsetminus \downarrow_{\mathrm{cj}}(ab)^n$ (removing a symbol in $\boldsymbol{u} \in \mathcal{F}$ would entail $\boldsymbol{u} \leq_{\mathrm{cj}} (ab)^n$).

Moreover, members of $\mathcal{F}$ have the same length, hence they are either equivalent under $\sim_{\mathrm{cj}}$ or incomparable with respect to $\leq_{\mathrm{cj}}$. Since equivalence classes are of linear size in the length of the sequence, and the length of the sequences described above are linear in n, it suffices to show that $\mathcal{F}$ has exponentially many elements to conclude.

Observe that we can assign either $(2, 3)$ or $(3, 2)$ to the first $m - 1$ pairs (k_i, k'_i), and use the last pair to make the sum equal to $n+1+m$. Indeed, $\sum_{i=1}^{m} k_i + k'_i = 5(m - 1) + k_m + k'_m = n - 4 + k_m + k'_m$. Therefore, it suffices to chose $k_m + k'_m = 4 + m + 1$, which is always possible. This proves that $\mathcal{F}$ has at least 2^{m-1} elements, among which at least $\frac{2^{m-1}}{n+m+1}$ are minimal in $\downarrow_{\mathrm{cj}}(ab)^n$.

(II): Again, the example from Section 6.1 still witnesses an exponential blow-up. We have:

$$\begin{aligned} D &= \downarrow_{\mathrm{cj}}(aba)^n \cap \downarrow_{\mathrm{cj}}(bab)^n \\ &= \downarrow_*((aba)^n \cup (baa)^n \cup (aab)^n) \cap \downarrow_*((bab)^n \cup (abb)^n \cup (bba)^n) \end{aligned}$$

We know the decomposition of $(aba)^n \cap (bab)^n$ already contains exponentially many maximal sequences (see Section 6.1). These sequences are still maximal in D, since all sequences in D have length bounded by $2n$. Moreover, since all these maximal sequences have same length $2n$, the family remains exponential when quotiented by $\sim_{\mathrm{cj}}$.

Chapter 7

Finite Multisets over WQOs

Given a WQO $(X, \leq)$, we consider the set $X^{\circledast}$ of finite multisets over X. Intuitively, multisets are sets where an element might occur multiple times. Formally, a multiset $M \in X^{\circledast}$ is a function from X to $\mathbb{N}$: $M(x)$ denotes the number of occurrences of x in M. The support of a multiset M denoted $Supp(M)$ is the set $\{x \in X \mid M(x) \neq 0\}$. A multiset is said to be finite if its support is.

A natural algorithmic representation for these objects are lists of elements of X, but keeping in mind that a permutation of a list represents the same multiset. Formally, this means that $X^{\circledast}$ is the quotient of X^* by the equivalence relation $\sim$ defined for all $\boldsymbol{u}, \boldsymbol{v} \in X^*$ by $\boldsymbol{u} \sim \boldsymbol{v}$ iff the sequence $\boldsymbol{u}$ can be obtained by permuting the symbols in $\boldsymbol{v}$, i.e. formally if $\boldsymbol{u} = u_1 \cdots u_n$ and $\boldsymbol{v} = v_1 \cdots v_m$,

$$\boldsymbol{u} \sim \boldsymbol{v} \overset{\text{def}}{\Leftrightarrow} n = m \wedge \exists \sigma \in S_n. \forall i \in [n]. u_i = v_{\sigma(i)}$$

where S_n denotes the permutation group over $[n]$. In the rest of this section, we will use $\overline{\boldsymbol{u}}$ to denote the closure under $\sim$ of some $\boldsymbol{U} \subseteq X^*$. For single words such as $\boldsymbol{u} \in X^*$, we will denote the equivalence class of $\boldsymbol{u}$ as $\{\!|\boldsymbol{u}|\!\}$. Finite multisets are equivalence classes of sequences under $\sim$, and will be represented by any member of the class. For instance, if $X = \{a, b, c\}$ is a finite alphabet, $M = \{\!|aac|\!\}$ is the multiset such that $M(a) = 2$, $M(c) = 1$ and $M(b) = 0$. Its other representations are $M = \{\!|aca|\!\} = \{\!|caa|\!\}$. Sometimes, it will be more convenient to use the functional point of view, and we will define some multiset M by providing values $M(x)$ for every $x \in X$. It is necessary to check that multisets defined in this fashion are finite.

Below we introduce notations for several natural operations, in particular generalizations of set-theoretic operations:

- Multiset union: $(M_1+M_2)(x) = M_1(x)+M_2(x)$. It is clear from that definition why we denote this operation with the symbol $+$, but keep in mind that this operation simply is the quotiented version of sequence concatenation, that is $\{\!|\boldsymbol{uv}|\!\} = \{\!|\boldsymbol{u} \cdot \boldsymbol{v}|\!\} = \{\!|\boldsymbol{u}|\!\} + \{\!|\boldsymbol{v}|\!\}$. As in the case of sequences, we lift this operation to set of multisets. Recall that if $\boldsymbol{U}, \boldsymbol{V}$ are sets of sequences, $\boldsymbol{U} \cdot \boldsymbol{V} = \{\boldsymbol{u} \cdot \boldsymbol{v} \mid \boldsymbol{u} \in \boldsymbol{U}, \boldsymbol{v} \in \boldsymbol{V}\}$. Similarly, given $\boldsymbol{S}, \boldsymbol{T}$ sets of multisets, we note $\boldsymbol{S} \oplus \boldsymbol{T} = \{M + N \mid M \in \boldsymbol{S}, N \in \boldsymbol{T}\}$. In other words, $\overline{\boldsymbol{U} \cdot \boldsymbol{V}} = \overline{\boldsymbol{U}} \oplus \overline{\boldsymbol{V}}$.

We chose the notation $\oplus$ instead of overloading the symbol $+$ in order to avoid possible confusion with set union.

- Multiset difference: $(M_1 - M_2)(x) = \max(0, M_1(x) - M_2(x))$.
- Membership: $x \in M \Leftrightarrow x \in Supp(M) \Leftrightarrow M(x) > 0$.
- Inclusion: $M_1 \subseteq M_2 \Leftrightarrow \forall x \in X.\ M_1(x) \leq M_2(x)$.
- Set intersection, or infemum: $(M_1 \cap M_2)(x) = \min(M_1(x), M_2(x))$.
- Set union, or supremum: $(M_1 \cup M_2)(x) = \max(M_1(x), M_2(x))$.
- Cardinality: $|M| = \sum_{x \in X} M(x)$, or if $w \in X^*$ is a member of the equivalence class M, $|M| = |\{\!|w|\!\}| = |w|$. We will thus often refer to $|M|$ as the *length* of M, or its *size*.
- Restriction: given $Y \subseteq X$, the restriction of M seen as a function to the domain Y is defined by:

$$M_{|Y}(x) = \begin{cases} M(x) & \text{if } x \in Y \\ 0 & \text{otherwise} \end{cases}$$

- Set Difference: we will write $M \smallsetminus Y$ for $M_{|X \smallsetminus Y}$

We will denote the empty multiset, i.e. the only multiset of empty support, by $\emptyset$.

7.1 Multisets under the Embedding Quasi-Ordering

Since $X^{\circledast}$ is the quotient of X^* under $\sim$, it is natural to quasi-order it with $\leq_* \circ \sim$. We denote by $\leq_{\mathrm{emb}}$ this quasi-ordering on $X^{\circledast}$ and immediately observe that the assumption of Section 4.2 is satisfied: $\leq_* \circ \sim = \sim \circ \leq_*$.

In this particular case, we can also defined $\leq_{\mathrm{emb}}$ directly by:

$$\{\!|x_1 \cdots x_n|\!\} \leq_{emb} \{\!|y_1 \cdots y_m|\!\} \overset{\text{def}}{\Leftrightarrow} \exists f : [n] \to [m] \text{ injective s.t. } \forall i \in [n], x_i \leq y_{f(i)}$$

As in the case of words, a function f that satisfies the right-hand side of the above equivalence is said to be a *witness* of $\{\!|x_1 \cdots x_n|\!\} \leq_{emb} \{\!|y_1 \cdots y_m|\!\}$.

We now study the ideal effectiveness of the construction that maps a QO $(X, \leq)$ to the QO $(X^{\circledast}, \leq_{\mathrm{emb}})$, relying on Section 4.2.

7.1.1 The Finite Multiset Extension with Embedding is Ideally Effective

Theorem 7.1.1. *With the generic representations introduced in Section 4.2, the finite multiset extension with embedding is an ideally effective construction. It is not polynomial-time in general. Given a polynomial-time presentation of an ideally effective WQO $(X, \leq)$, we can compute an exponential-time presentation of $(X^{\circledast}, \leq_{\mathrm{emb}})$.*

Proof. Let $(X, \leq)$ be an ideally effective WQO. Then $(X^*, \leq_*)$ is ideally effective as well. Therefore, in the light of Theorem 4.2.1, to prove that the finite multiset extension with embedding is an ideally effective construction, it suffices to show that the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ introduced in Section 4.2 are computable in this particular context. The fact that this extension is not a polynomial-time construction follows from the complexity lower bounds presented in Section 7.1.3. To prove the last part of the theorem, i.e. that we can compute an exponential-time presentation of $(X^{\circledast}, \leq_{\mathrm{emb}})$ when $(X, \leq)$ is a polynomial-time ideally effective WQO, we rely on Lemma 4.1.3.

Here, the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ are defined as:

$$\begin{aligned} \mathcal{C}l_{\mathrm{I}} \quad &: \mathit{Idl}(X^*, \leq_*) &&\to \mathit{Down}(X^*, \leq_*) \\ & \qquad\qquad \boldsymbol{P} &&\mapsto \overline{\boldsymbol{P}} \\ \mathcal{C}l_{\mathrm{F}} \quad &: (X^*, \leq_*) &&\to \mathit{Up}(X^*, \leq_*) \\ & \qquad\qquad \boldsymbol{u} &&\mapsto \uparrow_* \overline{\boldsymbol{u}} \end{aligned}$$

where, as before, $\overline{\boldsymbol{U}}$ is the closure under $\sim$ of $\boldsymbol{U} \subseteq X^*$. When $\boldsymbol{u}$ is a single sequence, $\overline{\boldsymbol{u}}$ is the equivalence class of $\boldsymbol{u}$ under $\sim$. Although we have introduced the notation $\{\!|\boldsymbol{u}|\!\}$ for this equivalence class, we rather make the distinction between $\{\!|\boldsymbol{u}|\!\} \in X^{\circledast}$ as an element of $X^{\circledast}$ and $\overline{\boldsymbol{u}} \subseteq X^*$ as a subset of X^*.

According to the definition of $\sim$, the equivalence class of a finite sequence $\boldsymbol{u} \in X^*$ consists of all the possible permutations of $\boldsymbol{u}$, that is:

$$\overline{x_1 \cdots x_n} = \bigcup_{\sigma \in S_n} x_{\sigma(1)} \cdots x_{\sigma(n)}$$

Therefore, $\mathcal{C}l_{\mathrm{F}}(x_1 \cdots x_n) = \bigcup_{\sigma \in S_n} \uparrow_* x_{\sigma(1)} \cdots x_{\sigma(n)}$ is computable.

For the function $\mathcal{C}l_{\mathrm{I}}$, remember ideals of $(X^*, \leq_*)$ are finite sequences of atoms, where atoms are either D^* for some downward-closed set D of X, or $I + \epsilon$, for I some ideal of X. Observe that the atoms are already closed under $\sim$: for any $D \in \mathit{Down}(X)$ and $I \in \mathit{Idl}(X)$, $\overline{D^*} = D^*$ and $\overline{I + \epsilon} = I + \epsilon$. Moreover, given $\boldsymbol{U}, \boldsymbol{V} \subseteq X^*$ set of sequences, $\overline{\boldsymbol{U} \cdot \boldsymbol{V}} = \overline{\boldsymbol{V} \cdot \boldsymbol{U}}$ (in other words, the operator $\oplus$ introduced at the beginning of this chapter is commutative). It follows that given n atoms $A_1, \ldots, A_n$, and any permutation $\sigma \in S_n$, we have $\overline{A_1 \cdots A_n} = \overline{A_{\sigma(1)} \cdots A_{\sigma(n)}}$. Finally, we know that given $D \in \mathit{Down}(X)$, $D^* = D^* \cdot D^*$. Combining the two previous equations, we get that for any sequence of atoms $A_1, \ldots, A_n$ and any downward-closed set D, $D^* \cdot A_1 \cdot A_2 \cdots A_n = D^* \cdot A_1 \cdot D^* \cdot A_2 \cdots D^* \cdot A_n$.

Let $\boldsymbol{P} = A_1 \cdots A_n$ an ideal of $(X^*, \leq_*)$, we define the downward-closed set of X

$$D \stackrel{\text{def}}{=} \bigcup \big\{ E \in \mathit{Down}(X) \;\big|\; \exists i \in \{1, \cdots, n\} : E^* = \boldsymbol{A}_i \big\}.$$

Moreover, define $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ the maximal subsequence of $1, \ldots, n$ such that for all j, A_{i_j} is an atom of the form $I + \epsilon$ for some $I \in \mathit{Idl}(X)$. In particular, for every $i \in [n]$ such that for all $j \in [k]$, $i \neq i_j$, the atom A_i is of the form E^* for some $E \in \mathit{Down}(X)$. Using the equations established before, we conclude that for every $\sigma \in S_k$,

$$\overline{\boldsymbol{P}} = \overline{D^* A_{\sigma(1)} D^* \cdots D^* A_{\sigma(k)} D^*}$$

and thus,

$$\begin{aligned}\overline{\boldsymbol{P}} &= \bigcup_{\sigma\in S_k} \overline{D^*A_{\sigma(1)}D^*\cdots D^*A_{\sigma(k)}D^*}\\ &= \overline{\bigcup_{\sigma\in S_k} D^*A_{\sigma(1)}D^*\cdots D^*A_{\sigma(k)}D^*}\end{aligned}$$

Moreover, it is not difficult to see that $\bigcup_{\sigma\in S_k} D^*A_{\sigma(1)}D^*\cdots D^*A_{\sigma(k)}D^*$ is closed under $\sim$, which finally proves that:

$$\mathcal{C}l_{\mathrm{I}}(\boldsymbol{P}) = \bigcup_{\sigma\in S_k} D^*A_{\sigma(1)}D^*\cdots D^*A_{\sigma(k)}D^*$$

In conclusion, the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ are computable, hence $(X^{\circledast}, \leq_{\mathrm{emb}})$ is an ideally effective WQO and the finite multiset extension with embedding is ideally effective.

However, the algorithms implicitly described above to compute the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ run in exponential-time, since they enumerate all permutations over a set of linear size. Assuming $(X, \leq)$ is a polynomial-time Since the procedures of the presentation of $(X^{\circledast}, \leq_{\mathrm{emb}})$ provided by Theorem 4.2.1 compose these functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ with the procedures from the exponential-time ideally effective WQO $(X^*, \leq_*)$, the naive upper bound for these procedures on multisets is doubly-exponential. To prove that $(X^{\circledast}, \leq_{\mathrm{emb}})$ is an exponential-time WQO, we apply Lemma 4.1.3. The verification of the hypothesis of the lemma are immediate.

As in the case of the stuttering extension, we now provide a complete complexity analysis. Over the two next subsections, we provide for each of the seven operations of an ideally effective WQO either a polynomial-time algorithm or an exponential-time lower bound. The fact that the finite multiset extension with embedding is not a polynomial-time construction follows from any of those lower bounds.

Moreover, since finite multisets are an important structure in computer science, we also provide in the next subsections a better representation of ideals of $(X^{\circledast}, \leq_{\mathrm{emb}})$ and explicit procedures for the seven operations, that is procedures that do not rely on the composition of two abstract constructions. $\square$

7.1.2 Better Complexity Upper Bounds

Deciding The Quasi-Ordering $\leq_{\mathrm{emb}}$

A convenient characterization of the quasi-ordering $\leq_{\mathrm{emb}}$ is obtained using Hall's Marriage Theorem. Below, we restate Hall's Theorem. It can be found in any textbook about graph theory.

Theorem 7.1.2 (Hall)**.** *Let $G = (V_1 \sqcup V_2, E)$ be a finite bipartite graph. E contains the graph of an injection from V_1 to V_2 if and only if for every $W \subseteq V_1$, $|W| \leq |N_G(W)|$. Here we write $N_G(W)$ for the* neighborhood *of W: $N_G(W) = \{y \mid \exists x \in W.\ (x, y) \in E\}$.*

Here is how this theorem applies to $\leq_{\mathrm{emb}}$:

Proposition 7.1.3. *Let $(X, \leq)$ be a WQO. Let M, N be two finite multisets over X.*

$$N \leq_{\text{emb}} M \textit{ iff } \forall S \subseteq N.\ |S| \leq |M_{|\uparrow Supp(S)}|$$

Proof. Write $N = \{\!|x_1 \cdots x_n|\!\}$ and $M = \{\!|y_1, \ldots, y_m|\!\}$. Define the bipartite graph $G = ([n] \sqcup [m], E)$ where $(i, j) \in E$ iff $x_i \leq y_j$. This is the bipartite graph with elements of N in one bag, elements of M in the other bag, and elements in N are linked to elements in M that are greater. Then

$$\begin{aligned} N \leq_{\text{emb}} M &\text{ iff there is an injection } f : [n] \to [m] \text{ such that } \forall i \in [n].\ x_i \leq y_{f(i)} \\ &\text{ iff there is an injection } f : [n] \to [m] \text{ such that } \forall i \in [n].\ (i, f(i)) \in E \\ &\text{ iff } E \text{ contains the graph of an injection} \\ &\text{ iff } \forall W \subseteq [n].\ |W| \leq |N_G(W)| \end{aligned}$$

the last equivalence being by Theorem 7.1.2. Finally, a subset W of $[n]$ defines a multiset $S \subseteq N$ and $N_G(W)$ represents exactly the sub-multiset of elements of M that are greater than some elements of S, i.e. $M_{|\uparrow Supp(S)}$. ☐

From this characterization, we deduce a polynomial-time procedure to decide $\leq_{\text{emb}}$, assuming $(X, \leq)$ is ideally effective.

Corollary 7.1.4. (OD)*: Let $(X, \leq)$ be a QO such that X has a representation that makes $\leq$ decidable. Then, the quasi-ordering $\leq_{\text{emb}}$ over $X^{\circledast}$ is decidable. If $\leq$ can furthermore be decided in polynomial-time, then $\leq_{\text{emb}}$ can be decided in polynomial-time.*

Proof. In a graph $G = (V, E)$, a *matching* is a subset S of E such that all the edges of S have distinct ending points, that is no vertex is an ending point of two distinct edges in S. The injectivity condition in our statement of Hall's Theorem guarantees that the set of edges $S = \{(x, f(x)) \mid x \in V_1\}$ is a matching. The usual formulation of Hall's Theorem gives a necessary and sufficient condition for the existence of a matching that covers V_1.

Given multisets N and M represented as elements of X^* (cf. beginning of this chapter), consider the bipartite graph G defined in the proof of Proposition 7.1.3. When $\leq$ is decidable (on X), this graph is clearly computable using a quadratic number of call to a decision procedure for $\leq$. Therefore, if the decision procedure runs in polynomial-time, G is computable in polynomial-time. Besides, there are polynomial-time algorithms to compute the maximum size of a matching in a bipartite graph (see Ford-Fulkerson algorithm, or Hopcroft-Karp algorithm). Thus, the relation $\leq_{\text{emb}}$ can be decided: it suffices to compute the maximal size of a matching in G and test whether it is equal to $|N|$. This last part runs in polynomial-time when G is of polynomial size in $|M| + |N|$, notably when $\leq$ can be decided in polynomial-time. ☐

The Ideals of $(X^{\circledast}, \leq_{\text{emb}})$

Let $(X, \leq)$ be a WQO.

Following the representation chosen in Section 4.2, we have represented the ideals of $(X^{\circledast}, \leq_{\text{emb}})$ as the closure under $\sim$ of the ideals of $(X^*, \leq_*)$. As we have shown in the proof of Theorem 7.1.1, there are potentially exponentially many ideals of $(X^*, \leq_*)$ that share a same closure under $\sim$. Indeed, recall that for any sequence of atoms $A_1, \ldots, A_n$ and any $\sigma \in S_n$, $\overline{A_1 \cdots A_n} = \overline{A_{\sigma(1)} \cdots A_{\sigma(n)}}$.

We are going to define a canonical representation for ideals of $(X^{\circledast}, \leq_{\mathrm{emb}})$ which is furthermore computable from any other representation when $(X, \leq)$ is ideally effective. This canonical representation will notably allow us to design an efficient inclusion test for ideals. Recall that the inclusion test provided by the proof of Theorem 7.1.1 works as follows: given two ideals $\boldsymbol{P}, \boldsymbol{Q} \in Idl(X^*, \leq_*)$, we check whether $\overline{\boldsymbol{P}} \subseteq \overline{\boldsymbol{Q}}$ by checking whether $\boldsymbol{P} \subseteq \mathcal{C}l_{\mathrm{I}}(\boldsymbol{Q})$, and we have seen that in general, the function $\mathcal{C}l_{\mathrm{I}}$ is costly. Our canonical representation will allow to test for inclusion without using $\mathcal{C}l_{\mathrm{I}}$.

Let $\overline{\boldsymbol{P}}$ be an ideal of $(X^{\circledast}, \leq_{\mathrm{emb}})$, where $\boldsymbol{P} = A_1 \cdots A_n$ is some ideal of $(X^*, \leq_*)$.

$$\begin{aligned}
\overline{\boldsymbol{P}} &= \overline{A_1 \cdots A_n} \\
&= \bigoplus_{i=1}^{n} \overline{A_i} \quad \text{by definition of } \oplus \\
&= \bigoplus_{\substack{1 \leq i \leq n \\ A_i = E^*}} \overline{E^*} \oplus \bigoplus_{\substack{1 \leq i \leq n \\ A_i = I + \epsilon}} \bar{(}I + \epsilon)
\end{aligned}$$

This last step consists in grouping atoms per kind, as we did in the proof of Theorem 7.1.1. Recall that the atoms of the form E^* for $E \in Down(X)$ are closed under $\sim$, and thus $\overline{E^*} = E^*$. However, as the notation $\oplus$ suggests, we want to stress that we are in the world of multisets ($X^{\circledast} = X^*/\sim$) and not of finite sequences. Therefore, we rather write $\overline{E^*} = E^{\circledast}$.

As before, we introduce D to be the union of subsets $E \in Down(X)$ such that E^* is an atom of $\boldsymbol{P}$, so that $\bigoplus_{\substack{1 \leq i \leq n \\ A_i = E^*}} E^{\circledast} = D^{\circledast}$.

Now, given a finite multiset $M \in X^{\circledast}$ such that $M \in \overline{\boldsymbol{P}}$, by definition of $\oplus$, there exist $M_1, M_2 \in X^{\circledast}$ such that $M = M_1 + M_2$, $M_1 \in D^{\circledast}$ and

$$M_2 \in \bigoplus_{\substack{1 \leq i \leq n \\ A_i = I + \epsilon}} \bar{(}I + \epsilon). \tag{7.1}$$

As before, let $A_{i_1}, \ldots, A_{i_k}$ the atoms of $\boldsymbol{P}$ of the form $I + \epsilon$ for $I \in Idl(X)$, and more precisely, write $A_{i_k} = I_{i_k} + \epsilon$. Moreover, write $M_2 = \{\!|x_1 \ldots x_p|\!\}$ for some $p \in \mathbb{N}$. Equation 7.1 reformulates as $\{\!|x_1 \ldots x_p|\!\} \in \bigoplus_{j=1}^{k} I_{i_j} + epsilon$. Then, a little combinatorics shows:

$$\{\!|x_1 \cdots x_p|\!\} \in \bigoplus_{j=1}^{k} (I_{i_j} + \epsilon) \text{ iff}$$
$$\exists f : [p] \to [m] \text{ injective s.t.} \forall i \in [p].\ x_i \in I_{f(i)}$$

Note that this last expression is very similar to the definition $\leq_{\mathrm{emb}}$, but with $\in$ used instead of $\leq$. This motivates the following notation:

$$\{\!|x_1 \cdots x_p|\!\} \in_{\mathrm{emb}} \{\!|I_1 \cdots I_m|\!\} \overset{\text{def}}{\Leftrightarrow} \exists f : [p] \to [m] \text{ injective s.t.} \forall i \in [p].\ x_i \in I_{f(i)}$$

Note that the right-hand side is a finite multiset of ideals of X. Denoting $\boldsymbol{B} = \{I_{i_1} \cdots I_{i_k}\} \in \mathit{Idl}(X)^{\circledast}$ the multisets of all ideals I_{i_j} that appear in $\boldsymbol{P}$ (with multiplicity), we have proved that $\overline{P} = \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$, where as expected, $\downarrow_{\in} \boldsymbol{B} = \{M \in X^{\circledast} \mid M \in_{\mathrm{emb}} \boldsymbol{B}\}$.

Theorem 7.1.5. *Let $(X, \leq)$ be a WQO. Then:*

$$\mathit{Idl}(X^{\circledast}, \leq_{\mathrm{emb}}) = \{\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} \mid \boldsymbol{B} \in \mathit{Idl}(X)^{\circledast}, D \in \mathit{Down}(X)\}$$

where $\downarrow_{\in} \boldsymbol{B} = \{M \in X^{\circledast} \mid M \in_{\mathrm{emb}} \boldsymbol{B}\}$ and $\in_{\mathrm{emb}}$ is defined as $\leq_{\mathrm{emb}}$, but using $\in$ instead of $\leq$.

Before proving this theorem, we would like to present a convenient characterization of $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ that will be constantly used throughout this section. Given $\boldsymbol{B} \in \mathit{Idl}(X)^{\circledast}$ a multiset of ideals of X and $D \in \mathit{Down}(X)$ a downward-closed set of X:

$$\begin{aligned}\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} &= \{M_1 + M_2 \mid M_1 \in_{\mathrm{emb}} \boldsymbol{B} \ \wedge\ M_2 \in D^{\circledast}\} \\ &= \{M \mid M \setminus D \in_{\mathrm{emb}} \boldsymbol{B}\}\end{aligned}$$

Indeed, if M is such that $M \setminus D \in_{\mathrm{emb}} \boldsymbol{B}$, then define $M_1 = M \setminus D$ and $M_2 = M_{|D}$ to satisfy $M = M_1 + M_2 \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. For the other direction, for any decomposition $M = M_1 + M_2$ satisfying $M_1 \in_{\mathrm{emb}} \boldsymbol{B}$ and $M_2 \in D^{\circledast}$, M_2 must be a sub-multiset of $M_{|D}$, and thus $M \setminus D \subseteq M_1$. It is thus obvious that $M \setminus D \in_{\mathrm{emb}} \boldsymbol{B}$.

We are now ready to prove Theorem 7.1.5.

Proof. We know from Section 4.2 that ideals of $(X^{\circledast}, \leq_{\mathrm{emb}})$ are exactly the subsets $\overline{\boldsymbol{P}}$ for $\boldsymbol{P} \in \mathit{Idl}(X^*, \leq_*)$. We have shown above how for any ideal $\boldsymbol{P} \in \mathit{Idl}(X^*, \leq_*)$, $\boldsymbol{P}$ is of the desired form. Conversely, observe that given $D \in \mathit{Down}(X)$ and $\{\!|I_1 \cdots I_k|\!\} \in \mathit{Idl}(X)^{\circledast}$, we have $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} = \overline{(I_1 + \epsilon) \cdots (I_k + \epsilon) \cdot D^*}$.

Alternatively, we can also check "by hand" that $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ is an ideal of $(X^{\circledast}, \leq_{\mathrm{emb}})$:

- Downward-closed: let $M \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$, and $N \leq_{\mathrm{emb}} M$. Since D is downward-closed, $N \setminus D \leq_{\mathrm{emb}} M \setminus D$ (a witness can be obtained by restricting a witness for $N \leq_{\mathrm{emb}} M$). Moreover, composing the embeddings witnessing $N \setminus D \leq_{\mathrm{emb}} M \setminus D$ and $M \setminus D \in_{\mathrm{emb}} \boldsymbol{B}$, we obtain $N \setminus D \in_{\mathrm{emb}} \boldsymbol{B}$ (elements of $\boldsymbol{B}$ are downward-closed); hence $N \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$.

- Directed: let $M, N \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. Write $\boldsymbol{B} = \{\!|I_1 \cdots I_k|\!\}$. Define $P = M_{|D} + N_{|D} + \{\!|z_1 \cdots z_k|\!\}$ where for all $i \in [k]$, z_i is greater than every element of M and N that belong to I_i. Such an element z_i exists since I_i is directed, and M and N are finite. Obviously, $P \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ and $M, N \leq_{\mathrm{emb}} P$. ☐

Observe that this representation of ideals is not unique: for instance with $X = \mathbb{N}$, $\downarrow_{\in}\{\!|\downarrow 3 \cdot \downarrow 1|\!\} \oplus (\downarrow 2)^{\circledast} = \downarrow_{\in}\{\!|\downarrow 3|\!\} \oplus (\downarrow 2)^{\circledast}$. This form of ideals of $(X^{\circledast}, \leq_{\mathrm{emb}})$ is not yet canonical. But already for ideals of this form, we get an efficient inclusion test (cf. Corollary 7.1.7).

Proposition 7.1.6. *Let $(X, \leq)$ be a WQO. Let $\boldsymbol{B}_1, \boldsymbol{B}_2 \in \mathit{Idl}(X)^{\circledast}$ and $D_1, D_2 \in \mathit{Down}(X)$.*

$$\downarrow_{\in} \boldsymbol{B}_1 \oplus D_1^{\circledast} \subseteq \downarrow_{\in} \boldsymbol{B}_2 \oplus D_2^{\circledast} \textit{ iff } D_1 \subseteq D_2 \textit{ and } \boldsymbol{B}_1 \smallsetminus \mathit{Down}(D_2) \subseteq_{\mathrm{emb}} \boldsymbol{B}_2$$

Proof. Write $\boldsymbol{B} = \boldsymbol{B}_1 \smallsetminus \mathit{Down}(D_2) = \{\!|I_1 \cdots I_n \cdot \downarrow y_1 \cdots \downarrow y_m|\!\}$, where $I_1, \ldots, I_n$ are limit ideals (i.e. those that are not principal), and $y_1, \ldots, y_m \in X$.

($\Rightarrow$) For any $x \in D_1$, the multiset with $|\boldsymbol{B}_2| + 1$ copies of x is in $\downarrow_{\in} \boldsymbol{B}_1 \oplus D_1^{\circledast}$, hence it must be in $\downarrow_{\in} \boldsymbol{B}_2 \oplus D_2^{\circledast}$. However $M \in_{\mathrm{emb}} \boldsymbol{B}_2$ implies $|M| \leq |\boldsymbol{B}_2|$, thus x must be in D_2, proving $D_1 \subseteq D_2$.

If $n = 0$, then $\{\!|y_1 \cdots y_m|\!\} \in \downarrow_{\in} \boldsymbol{B}_1 \oplus D_1^{\circledast} \subseteq \downarrow_{\in} \boldsymbol{B}_2 \oplus D_2^{\circledast}$ with $y_i \notin D_2$ by definition, entailing $\{\!|y_1 \cdots y_m|\!\} \in_{\mathrm{emb}} \boldsymbol{B}_2$. This proves $\boldsymbol{B} \subseteq_{\mathrm{emb}} \boldsymbol{B}_2$.

Otherwise, $n \neq 0$ and the set $\boldsymbol{A} = \{\{\!|x_1 \cdots x_n \cdot y_1 \cdots y_m|\!\} \mid \forall i.\ x_i \in I_i \smallsetminus D_2\}$ is infinite, included in $\downarrow_{\in} \boldsymbol{B}_1 \oplus D_1^{\circledast} \subseteq \downarrow_{\in} \boldsymbol{B}_2 \oplus D_2^{\circledast}$ and the only way to have $\boldsymbol{A} \subseteq \downarrow_{\in} \boldsymbol{B}_2 \oplus D_2^{\circledast}$ is if $\forall M \in \boldsymbol{A}$, $M \in_{\mathrm{emb}} \boldsymbol{B}_2$. Now consider the set of embeddings from $[n+m]$ to $[|\boldsymbol{B}_2|]$, it is finite, hence infinitely many memberships are witnessed by a same embedding f. It is easy to see that f witnesses $\boldsymbol{B} \leq_{\mathrm{emb}} \boldsymbol{B}_2$.

($\Leftarrow$) Let $M \in \downarrow_{\in} \boldsymbol{B}_1 \oplus D_1^{\circledast}$. Since $D_1 \subseteq D_2$, $M \smallsetminus D_2 \leq_{\mathrm{emb}} M \smallsetminus D_1$. Moreover, $M \smallsetminus D_1 \in_{\mathrm{emb}} \boldsymbol{B}_1$, and therefore $M \smallsetminus D_2 \in_{\mathrm{emb}} \boldsymbol{B}$, by definition of $\boldsymbol{B}$. We conclude $M \smallsetminus D_2 \in_{\mathrm{emb}} \boldsymbol{B}_2$. ☐

Corollary 7.1.7. *If $(X, \leq)$ is a polynomial-time ideally effective WQO, then inclusion of ideals of $(X^{\circledast}, \leq_{\mathrm{emb}})$ is decidable in polynomial-time.*

Proof. If $(X, \leq)$ is a polynomial-time WQO, then we can compare downward-closed sets of $(X, \leq)$ in polynomial-time. Moreover, Corollary 7.1.4 applied to the QO $(\mathit{Idl}(X), \subseteq)$ entails that $\subseteq_{\mathrm{emb}}$ can be tested in polynomial-time.

Besides, given $\boldsymbol{P}$ an ideal of $(X^*, \leq_*)$, we can compute in polynomial-time D and $\boldsymbol{B}$ such that $\overline{\boldsymbol{P}} = \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$, following the implicit procedure described before Theorem 7.1.5. Then, the right-hand side of Proposition 7.1.6 can be tested in polynomial-time. ☐

Although we have just seen that rewriting ideals of $(X^{\circledast}, \leq_{\mathrm{emb}})$ under the form $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ is enough to get an efficient inclusion test, it is not difficult from there to get an actual canonical form.

Definition 7.1.8. *Let $(X, \leq)$ be a WQO. Given $\boldsymbol{B} \in \mathit{Idl}(X)^{\circledast}$ and $D \in \mathit{Down}(X)$, we say that the pair $(\boldsymbol{B}, D)$ is* reduced *if for every $I \in \boldsymbol{B}$, $I \not\subseteq D$.*

Proposition 7.1.9. *Let $(X, \leq)$ be a WQO and $\boldsymbol{I}$ be an ideal of $(X^{\circledast}, \leq_{\mathrm{emb}})$. Then there exist a unique $\boldsymbol{B} \in \mathit{Idl}(X)^{\circledast}$ and a unique $D \in \mathit{Down}(X)$ such that $(\boldsymbol{B}, D)$ is reduced and $\boldsymbol{I} = \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. We say that $(\boldsymbol{B}, D)$ is the* canonical representation *of $\boldsymbol{I}$. When $(X, \leq)$ is an (polynomial-time) ideally effective WQO, this unique reduced pair is computable (in polynomial-time) from any other pair $(\boldsymbol{B}', D')$ such that $\downarrow_{\in} \boldsymbol{B}' \oplus D'^{\circledast} = \boldsymbol{I}$.*

Proof. Uniqueness: if $\downarrow_{\in} \boldsymbol{B}_1 \oplus D_1^{\circledast} = \downarrow_{\in} \boldsymbol{B}_2 \oplus D_2^{\circledast}$ and that both representations are canonical, then by Proposition 7.1.6, $D_1 = D_2$, and thus $\forall I \in \boldsymbol{B}_i, I \not\subseteq D_i$. Therefore, the second condition directly gives $\boldsymbol{B}_1 \subseteq_{\mathrm{emb}} \boldsymbol{B}_2 \subseteq_{\mathrm{emb}} \boldsymbol{B}_1$, which implies $\boldsymbol{B}_1 = \boldsymbol{B}_2$.

Computability: If $(X, \leq)$ is effective, inclusion is decidable, thus one can compute the canonical representation of an ideal from any other representation by testing for every $I \in Supp(\boldsymbol{B})$ whether $I \subseteq D$. If it is the case, removing all copies of I from $\boldsymbol{B}$ does not change $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. $\square$

Of course, ideals and downward-closed sets of X might not have unique encodings, thus canonical representations might also have several encodings at the lowest level.

7.1.3 Explicit Expressions and Complexity Lower Bounds

In this section, we explicitly describe procedures to complement filters and ideals, and intersect filters and ideals, without relying on Section 4.2. For each of these four operations, we also provide exponential-time lower bounds. Observe that for a finite alphabet A, $(A^{\circledast}, \leq_{\mathrm{emb}})$ is isomorphic to $(\mathbb{N}^{|A|}, \leq_{\times})$. Thus, we have to turn to more complex WQOs to provide exponential lower bounds.

To increase readability of the proposition of this section, we will use the symbol $\times$ to denote iteration of multiset addition, i.e. $n \times M = \underbrace{M + \cdots + M}_{n \text{ times}}$. We also extend the definitions of $\in_{\mathrm{emb}}$ and $\downarrow_{\in}$ to multisets $\boldsymbol{B} \in Down(X)^{\circledast}$ of downward-closed sets of X (instead of ideals). In this case, $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ is not an ideal of $(X^{\circledast}, \leq_{\mathrm{emb}})$, but it is downward-closed. Besides, if $\boldsymbol{B} = \{\!|D_1, \ldots, D_m|\!\}$ and for all i, $D_i = \bigcup_{j=1}^{n_i} I_{i,j}$, then

$$\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} = \bigcup_{\substack{j_1 \in [n_1] \\ \cdots \\ j_m \in [n_m]}} \downarrow_{\in} \{\!|I_{1,j_1} \cdots I_{m,j_m}|\!\} \oplus D^{\circledast}$$

Thus, when a downward-closed set $\boldsymbol{D}$ of $(X^{\circledast}, \leq_{\mathrm{emb}})$ is given as a union of such sets $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$, it is possible to compute the actual ideal decomposition of $\boldsymbol{D}$. Note however that the ideal decomposition of $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ in this setting is polynomial in $|D_i|$ but exponential in m.

Complementing Filters (CF)

Proposition 7.1.10. *Let M be a multiset over X,*

$$X^{\circledast} \smallsetminus \uparrow M = \bigcup_{\substack{S \subseteq Supp(M) \\ S \neq \emptyset}} \downarrow_{\in} \{\!| \underbrace{X \cdots X}_{|M_{|S}|-1 \text{ times}} |\!\} \oplus [X \smallsetminus \uparrow S]^{\circledast}$$

The above expression is computable, using (XI) and (CF) for X. However, it requires exponential-time to enumerate all the subsets of M. This enumeration is shown to be unavoidable in the next proposition.

Note that X may not be an ideal, in which case the actual ideal decomposition is obtained by distributing the ideal decomposition of X as described at the beginning of this subsection.

Proof. For $T \subseteq M$, define the downward-closed set

$$\boldsymbol{D}(T) = \downarrow_{\in} \{\!\!| \underbrace{X \cdots X}_{|T|-1 \text{ times}} |\!\!\} \oplus [X \smallsetminus \uparrow Supp(T)]^{\circledast}$$

$$\begin{aligned} N \in X^{\circledast} \smallsetminus \uparrow M \text{ iff } & M \not\leq_{\text{emb}} N \\ \text{iff } & \exists T \subseteq M.\ |T| > |N_{|\uparrow Supp(T)}| \text{ (negating Proposition 7.1.3)} \\ \text{iff } & \bigvee_{\substack{T \subseteq M \\ T \neq \emptyset}} |N_{|\uparrow Supp(T)}| \leq |T| - 1 \\ \text{iff } & N \in \bigcup_{\substack{T \subseteq M \\ T \neq \emptyset}} \boldsymbol{D}(T) \end{aligned}$$

Now for $T \subseteq M$, let $S = Supp(T)$, it is obvious that $T \subseteq M_{|S}$ and $\boldsymbol{D}(T) \subseteq \boldsymbol{D}(M_{|S})$. We can thus restrict the union above to the union described in the proposition. $\square$

Proposition 7.1.11. *There exists an ideally effective WQO $(X, \leq)$ such that the expression provided in Proposition 7.1.10 is canonical. In particular, complementing filters of $(X^{\circledast}, \leq_{\text{emb}})$ requires exponential-time.*

Proof. Our goal is to provide a WQO X and an infinite family $(M_n)_{n \in \mathbb{N}}$ such that for any $n \in \mathbb{N}$ and any $S, T \subseteq M_n$, $\boldsymbol{D}(S)$ and $\boldsymbol{D}(T)$ are incomparable (for inclusion), provided $S \neq T$.

One can check that this is not the case for $X = \mathbb{N}$. Indeed, as soon as M has at least two ordered elements $n_1 \leq n_2$, $\boldsymbol{D}(\{\!\!| n_1 |\!\!\}) \subseteq \boldsymbol{D}(\{\!\!| n_1, n_2 |\!\!\})$. Since elements of $\mathbb{N}$ are linearly-ordered, we can prove:

$$\mathbb{N}^{\circledast} \smallsetminus \uparrow M = \downarrow_{\in} \{\!\!| \underbrace{X \cdots X}_{|M|-1 \text{ times}} |\!\!\}] \oplus [\downarrow \min(M) - 1]^{\circledast}$$

We thus take $X = \mathbb{N}^2$ (which is an ideal), and define $M_n = \{\!\!| \langle 0, n \rangle \langle 1, n - 1 \rangle \cdots \langle n, 0 \rangle |\!\!\}$. Now let S and T be two distinct subsets of M_n, we show that $\boldsymbol{D}(S) \not\subseteq \boldsymbol{D}(T)$.

- If $|S| \leq |T|$, but $S \neq T$, there exists $x \in Supp(T) \smallsetminus Supp(S)$, and since elements of M_n are pairwise incomparable, $x \notin \uparrow Supp(S)$. This proves that $\complement \uparrow Supp(S) \not\subseteq \complement \uparrow Supp(T)$, and by Proposition 7.1.6, $\boldsymbol{D}(S) \not\leq_{\text{emb}} \boldsymbol{D}(T)$.
- If $|S| > |T|$ then $\boldsymbol{D}(S) \not\leq_{\text{emb}} \boldsymbol{D}(T)$ since there are too many copies of X in $\boldsymbol{D}(S)$.

Notice that we have actually proved that our expression for $X^{\circledast} \smallsetminus \uparrow M$ is canonical if and only if M is an antichain. $\square$

Complementing Ideals (CI)

The procedure to complement ideals is very similar to the procedure to complement filters:

Proposition 7.1.12. *Given $\boldsymbol{B} \in (Idl(X, \leq))^{\circledast}$ and $D \in Down(X, \leq)$,*

$$X^{\circledast} \smallsetminus (\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}) = \bigcup_{\boldsymbol{S} \subseteq Supp(\boldsymbol{B})} \uparrow\{M \mid Supp(M) \subseteq U_{\boldsymbol{S},\boldsymbol{B},D} \wedge |M| = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1\}$$

where $U_{\boldsymbol{S},\boldsymbol{B},D} = \min(X \smallsetminus (D \cup \bigcup(Supp(\boldsymbol{B}) \smallsetminus \boldsymbol{S})))$.

Concretely, minimal multisets M of $X^{\circledast} \smallsetminus \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ are multisets of size exactly $|\boldsymbol{B}_{|\boldsymbol{S}}|+1$ whose elements are among the minimal elements of $X \smallsetminus (D \cup \bigcup(Supp(\boldsymbol{B}) \smallsetminus \boldsymbol{S}))$, for some $\boldsymbol{S} \subseteq Supp(\boldsymbol{B})$.

Proof. ($\subseteq$) Let $M \notin \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. That is to say, $M \smallsetminus D \notin_{\mathrm{emb}} \boldsymbol{B}$. Adapting Proposition 7.1.3, the latter is equivalent to the existence of $T \subseteq M \smallsetminus D$ such that $|\boldsymbol{B}_{|\boldsymbol{I}(T)}| < |T|$, where $\boldsymbol{I}(T) = \{I \in Idl(X) \mid I \cap Supp(T) \neq \emptyset\}$ (understand $\boldsymbol{I}(T)$ as the set of ideals that contain some element of T). Let $\boldsymbol{S} = Supp(\boldsymbol{B}) \cap \boldsymbol{I}(T)$, we show that $T \in \uparrow\{M \mid Supp(M) \subseteq U_{\boldsymbol{S},\boldsymbol{B},D} \wedge |M| = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1\}$. Indeed, $|T| \geq |\boldsymbol{B}_{|\boldsymbol{I}(T)}| + 1 = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1$. Moreover, given $x \in T$, $x \notin D$ since $T \subseteq M \smallsetminus D$, and x is not in any ideal $I \in \bigcup Supp(\boldsymbol{B}) \smallsetminus \boldsymbol{S}$ since by definition, if $x \in I$ then $I \in \boldsymbol{I}(T)$. We just showed that $Supp(T) \subseteq X \smallsetminus (D \cup \bigcup Supp(\boldsymbol{B}) \smallsetminus \boldsymbol{S})$. It is then not difficult to build a multiset $N \leq_{\mathrm{emb}} T$ that satisfies the desired conditions.

($\supseteq$) Let M such that $Supp(M) \subseteq U_{\boldsymbol{S},\boldsymbol{B},D}$ and $|M| = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1\}$ for some $\boldsymbol{S} \subseteq Supp(\boldsymbol{B})$. First of all $M = M \smallsetminus D$. Besides, an injective mapping f from M to $\boldsymbol{B}$ would define a submultiset of $\boldsymbol{B}$ of size $|M| = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1$. For cardinality reason, there must be an element $x \in M$ whose image $f(x) = I$ is not in $\boldsymbol{S}$. But it is then impossible to have $x \in f(x)$, and f cannot be a witness of an embedding $M \in_{\mathrm{emb}} \boldsymbol{B}$. Therefore, $M \notin \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. ☐

The above procedure can obviously be implemented in exponential-time. Observe that this is already unavoidable in the case of $(X, \leq) = (\mathbb{N}^2, \leq_{\times})$: consider $\boldsymbol{B}_n = n \times \{\!|\downarrow\langle 1, 1\rangle|\!\}$ and $D_n = \downarrow\langle 0, 0\rangle$. Indeed, it is immediate to check that any multiset of size $n + 1$ whose elements are among $\langle 0, 1\rangle$ and $\langle 1, 0\rangle$ is a minimal element of $X^{\circledast} \smallsetminus \downarrow_{\in} \boldsymbol{B}_n \oplus D_n^{\circledast}$. There are 2^n such multisets.

Below we present an optimization of the above procedure from which it is simple to derive a polynomial-time complexity implementation in the case of $(X, \leq) = (\mathbb{N}, \leq)$.

Proposition 7.1.13. *Given $\boldsymbol{B} \in (Idl(X, \leq))^{\circledast}$ and $D \in Down(X, \leq)$,*

$$X^{\circledast} \smallsetminus \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} = \bigcup_{\substack{\boldsymbol{S} \subseteq Supp(\boldsymbol{B}) \\ G(\boldsymbol{S}) \text{ is connected}}} \uparrow\{M \mid Supp(M) \subseteq U_{\boldsymbol{S},\boldsymbol{B},D} \wedge |M| = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1\}$$

where $G(\boldsymbol{S}) = (\boldsymbol{S}, E)$ and $E = \{(I, J) \mid I \cap J \smallsetminus (D \cup \bigcup \boldsymbol{B} \smallsetminus \boldsymbol{S}) \neq \emptyset\}$

This proposition claims that it suffices to take the union over subsets $\boldsymbol{S}$ of $Supp(\boldsymbol{B})$ that induce a connected graph $G(\boldsymbol{S})$. Now in the case of $\mathbb{N}$, ideals of $\boldsymbol{B}$ can be sorted, and it suffices to consider subsets $\boldsymbol{S} \subseteq Supp(\boldsymbol{B})$ that are convex in the following sense: if $I, J \in \boldsymbol{S}$ and $K \in \boldsymbol{B}$ such that $I \subseteq K \subseteq J$, then $K \in \boldsymbol{S}$ as well. It is obvious that subsets $\boldsymbol{S}$ that are not convex induce a non connected graph $G(\boldsymbol{S})$. Thus it suffices to take the union over convex subsets. Moreover, there are only a quadratic (in $|\boldsymbol{B}|$) number of convex subsets of $Supp(\boldsymbol{B})$. Besides, since filters of $\mathbb{N}$ have at most one minimal elements, the expression builds at most one multiset per subset $\boldsymbol{S} \subseteq Supp(\boldsymbol{B})$. Therefore, $\mathbb{N}^{\circledast} \smallsetminus \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ is computable in quadratic-time.

Proof. Let $\boldsymbol{S} \subseteq Supp(\boldsymbol{B})$ and M such that $Supp(M) \subseteq U_{\boldsymbol{S},\boldsymbol{B},D}$ and $|M| = |\boldsymbol{B}_{|\boldsymbol{S}}| + 1$. We show that if $G(\boldsymbol{S})$ is not connected then M is not minimal in $X^{\circledast} \smallsetminus \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$.

First of all, $Supp(M) \subseteq X \smallsetminus (D \cup \bigcup \boldsymbol{B} \smallsetminus \boldsymbol{S})$. Besides, if there exists some $x \in M$ such that $x \in X \smallsetminus (D \cup \bigcup \boldsymbol{B})$, then $\{\!|x|\!\} \leq_{\text{emb}} M$ and $\{\!|x|\!\} \notin \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. This implies that M is not minimal, except if $|M| = 1$, which would imply $\boldsymbol{S} = \boldsymbol{\emptyset}$, which would imply $G(\boldsymbol{S})$ is connected, which is a contradiction. We can now assume that $Supp(M) \subseteq \bigcup \boldsymbol{S}$.

Take $\boldsymbol{S}_1 \sqcup \boldsymbol{S}_2$ a non-trivial partition of $\boldsymbol{S}$ such that $\boldsymbol{S}_1 \times \boldsymbol{S}_2 \cap E = \emptyset$, i.e. for all $(I, J) \in \boldsymbol{S}_1 \times \boldsymbol{S}_2$, $I \cap J \smallsetminus (D \cup \bigcup \boldsymbol{B} \smallsetminus \boldsymbol{S}) = \emptyset$. Hence, for every $x \in M$, either $x \in \bigcup \boldsymbol{S}_1$ or $x \in \bigcup \boldsymbol{S}_2$, the two options being mutually exclusive.

Define $M_i = M_{|\bigcup \boldsymbol{S}_i}$ for $i = 1, 2$. In particular, $M = M_1 + M_2$. Moreover, $M_i \in_{\text{emb}} \boldsymbol{B}$ implies $M_i \in_{\text{emb}} \boldsymbol{B}_{|\boldsymbol{S}_i}$. It is thus impossible that both M_1 and M_2 belong to $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$: it would imply $M = M_1 + M_2 \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. Without loss of generality, assume $M_1 \notin \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. The elements of M_1 overall belong to only $m = |\boldsymbol{B}_{|\boldsymbol{S}_1}|$ ideals of $\boldsymbol{B}$. Thus, any submultiset N of M_1 with $m + 1$ elements is already not a member of $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$, and since $|\boldsymbol{S}_1| < |\boldsymbol{S}|$, such multisets N are *strictly* smaller than M. $\square$

Intersecting Filters (IF) **and Ideals** (II)

We now present procedures to intersect filters and ideals of $(X^{\circledast}, \leq_{\text{emb}})$. To emphasize the similarities between these two operations, we gather their description in a same proposition. Remember S_n stands for the group of permutations over $[n]$. The occurrence of S_n in the next formulas is no surprise, since S_n is at the heart of the equivalence relation $\sim$ from which multisets are built, and thus at the heart of functions $\mathcal{C}l_{\text{F}}$ and $\mathcal{C}l_{\text{I}}$. Yet, the two following formulas are less redundant than the expression one would directly get applying Section 4.2.

Proposition 7.1.14. *Given $M, N \in X^{\circledast}$, $\boldsymbol{B} \in Idl(X)^{\circledast}$ and $D \in Down(X)$:*

(IF)**:** *Intersection of filters:*

$$\uparrow M \cap \uparrow N = \uparrow \left\{ P + M_2 + N_2 \;\middle|\; \begin{array}{ll} M = M_1 + M_2, & |N_1| = |M_1| \\ N = N_1 + N_2, & P \in M_1 \tilde{\cap} N_1 \end{array} \right\}$$

where

$$\{\!|x_1 \cdots x_k|\!\} \mathbin{\tilde{\cap}} \{\!|y_1 \cdots y_k|\!\} = \\ \{\{\!|z_1 \cdots z_k|\!\} \mid \exists \sigma \in S_k.\, \forall i \in [k].\, z_i \in \min(\uparrow x_i \cap \uparrow y_{\sigma(i)})\}$$

(II)**:** *Intersection of ideals:*

$$\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} \cap \downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast} = \\ \bigcup_{\substack{\boldsymbol{B}=\boldsymbol{B}_1+\boldsymbol{B}_2 \\ \boldsymbol{C}=\boldsymbol{C}_1+\boldsymbol{C}_2 \\ |\boldsymbol{B}_1|=|\boldsymbol{B}_2|}} \downarrow_{\in} [\boldsymbol{B}_1 \mathbin{\tilde{\cap}} \boldsymbol{C}_1 + \boldsymbol{B}_2 \sqcap E + \boldsymbol{C}_2 \sqcap D] \oplus (D \cap E)^{\circledast}$$

where $\{\!|I_1 \cdots I_k|\!\} \mathbin{\tilde{\cap}} \{\!|J_1 \cdots J_k|\!\} = \bigcup_{\sigma \in S_k} \{\!|(I_1 \cap J_{\sigma(1)}) \cdots (I_k \cap J_{\sigma(k)})|\!\}$ *and* $\{\!|I_1 \cdots I_k|\!\} \sqcap D = \{\!|(I_1 \cap D) \cdots (I_k \cap D)|\!\}$

These expressions are computable in exponential-time (enumeration of $n!$ and $m!$ permutations). Here again, it is unavoidable in general, which is proved thereafter in Proposition 7.1.15.

Proof.

(IF): ($\supseteq$) It is immediate that every multiset $P + M_2 + N_2$ obtained as described in the proposition embeds both M and N.

($\subseteq$) Let $Q \in \uparrow M \cap \uparrow N$. There exist decompositions $Q = Q_1 + Q_2 + Q_3 + Q_4$, $M = M_1 + M_2$ and $N = N_1 + N_2$ such that:

- $|M_1| = |N_1| = |Q_1|$ and $M_1 \leq_{\text{emb}} Q_1$ and $N_1 \leq_{\text{emb}} Q_1$
- $|M_2| = |Q_2|$ and $M_2 \leq_{\text{emb}} Q_2$
- $|N_2| = |Q_3|$ and $N_2 \leq_{\text{emb}} Q_3$

Indeed, fix two embeddings f and g witnessing $M \leq_{\text{emb}} Q$ and $N \leq_{\text{emb}} Q$. Then take Q_1 to be the intersection of the images of f and g, while Q_2 is what remains of the image of f and Q_3 what remains of the image of g. Finally, Q_4 is what is outside both those images.

Now, by the first condition, Q_1 must be greater than some $P \in M_1 \mathbin{\tilde{\cap}} N_1$, and thus $P + M_2 + N_2 \leq_{\text{emb}} Q_1 + Q_2 + Q_3 \leq_{\text{emb}} Q$.

(II): ($\supseteq$) Given decompositions $\boldsymbol{B} = \boldsymbol{B}_1 + \boldsymbol{B}_2$, $\boldsymbol{C} = \boldsymbol{C}_1 + \boldsymbol{C}_2$ with $|\boldsymbol{B}_1| = |\boldsymbol{C}_1|$, we show $\downarrow_{\in} [\boldsymbol{B}_1 \mathbin{\tilde{\cap}} \boldsymbol{C}_1 + \boldsymbol{B}_2 \sqcap E + \boldsymbol{C}_2 \sqcap D] \oplus (D \cap E)^{\circledast} \subseteq \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ using Proposition 7.1.6. The inclusion in $\downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast}$ is analogous.

We have $\boldsymbol{B}_1 \mathbin{\tilde{\cap}} \boldsymbol{C}_1 \subseteq_{\text{emb}} \boldsymbol{B}_1$ and $\boldsymbol{B}_2 \sqcap E \subseteq_{\text{emb}} \boldsymbol{B}_2$, thus

$$\begin{aligned}(\boldsymbol{B}_1 \mathbin{\tilde{\cap}} \boldsymbol{C}_1 + \boldsymbol{B}_2 \sqcap E + \boldsymbol{C}_2 \sqcap D) \smallsetminus \mathit{Down}(D) &\subseteq_{\text{emb}} \boldsymbol{B}_1 \mathbin{\tilde{\cap}} \boldsymbol{C}_1 + \boldsymbol{B}_2 \sqcap E \\ &\subseteq_{\text{emb}} \boldsymbol{B}_1 + \boldsymbol{B}_2 = \boldsymbol{B}\end{aligned}$$

Moreover, $D \cap E \subseteq D$.

($\subseteq$): Let $M \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} \cap \downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast}$. Define $M_1 = M \smallsetminus (D \cup E)$, $M_2 = M \smallsetminus (D \cup \complement E)$, $M_3 = M \smallsetminus (\complement D \cup E)$. Thus, $M \smallsetminus (D \cap E) = M_1 + M_2 + M_3$. Moreover, $M_1 + M_2 = M \smallsetminus D \in_{\mathrm{emb}} \boldsymbol{B}$, hence we can decompose $\boldsymbol{B}$ in $\boldsymbol{B}_1 + \boldsymbol{B}_2$ such that $M_1 \in_{\mathrm{emb}} \boldsymbol{B}_1$, $M_2 \in_{\mathrm{emb}} \boldsymbol{B}_2$ and $|M_1| = |\boldsymbol{B}_1|$. Respectively, $M_1 + M_3 = M \smallsetminus E \in_{\mathrm{emb}} \boldsymbol{C}$ and we define $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ similarly. Therefore, $|\boldsymbol{B}_1| = |M_1| = |\boldsymbol{C}_1|$ and $M_1 \in_{\mathrm{emb}} \boldsymbol{B}_1 \tilde{\cap} \boldsymbol{C}_1$. Moreover, $Supp(M_2) \subseteq E$ and $M_2 \in_{\mathrm{emb}} \boldsymbol{B}_2$, thus $M_2 \in_{\mathrm{emb}} (\boldsymbol{B}_2 \sqcap E)$. Similarly $M_3 \in_{\mathrm{emb}} (\boldsymbol{C}_2 \sqcap D)$, which concludes the proof. $\square$

We now prove a lower bound matching the exponential upper bound given above. We show that intersections of filters and ideals are already exponential in $(\mathbb{N}^{2\circledast}, \leq_{\mathrm{emb}})$. As stated above, it is obviously polynomial in $(A^{\circledast}, \leq_{\mathrm{emb}})$, if A is a finite alphabet. It is also polynomial in $(\mathbb{N}^{\circledast}, \leq_{\mathrm{emb}})$, which will be proved in Proposition 7.1.16.

Proposition 7.1.15. *Let $(X, \leq) = (\mathbb{N}^2, \leq_{\times})$ and $n = 2m + 1$ be an odd integer. Define $M_n = \{\!|\langle n-1, 0\rangle \cdot \langle n-2, 1\rangle \cdots \langle m, m\rangle|\!\} = \sum_{i=0}^{m} \{\!|\langle n-i-1, i\rangle|\!\}$ and $N_n = \{\!|\langle 0, n-1\rangle \cdot \langle 1, n-2\rangle \cdots \langle m, m\rangle|\!\} = \sum_{i=0}^{m} \{\!|\langle i, n-i-1\rangle|\!\}$. Then:*

(IF)*: The upward-closed set $\uparrow M_n \cap \uparrow N_n$ has exponentially many (in n) minimal elements.*

(II)*: The downward-closed set $\downarrow M_n \cap \downarrow N_n$ has exponentially many (in n) maximal elements.*

It follows that both these operations require exponential-time computations.

Proof. Recall from Section 5.3 that $\uparrow\langle a, b\rangle \cap \uparrow\langle c, d\rangle = \uparrow\langle \max(a, c), \max(c, d)\rangle$ and $\downarrow\langle a, b\rangle \cap \downarrow\langle c, d\rangle = \downarrow\langle \min(a, c), \min(c, d)\rangle$. Given σ a permutation of $[0, m]$, define:

$$M_\sigma^{\uparrow} = \sum_{i=0}^{m} \{\!|\langle \max(n-i-1, \sigma(i)), \max(i, n-\sigma(i)-1)\rangle|\!\}$$

$$M_\sigma^{\downarrow} = \sum_{i=0}^{m} \{\!|\langle \min(n-i-1, \sigma(i)), \min(i, n-\sigma(i)-1)\rangle|\!\}$$

We now argue that multisets $M_\sigma^{\uparrow}$ are minimal elements of $\uparrow M_n \cap \uparrow N_n$ and $M_\sigma^{\downarrow}$ are maximal elements of $\downarrow M_n \cap \downarrow N_n$. This concludes the proof since these two families are exponential in n.

The multisets $M_\sigma^{\uparrow}$ are obviously members of $\uparrow M_n \cap \uparrow N_n$. Assume they are not minimal, then there exists a multiset P strictly smaller than some $M_\sigma^{\uparrow}$ which is in $\uparrow M_n \cap \uparrow N_n$. There are two possibilities for P to be *strictly* smaller: either it is shorter, i.e. $|P| < |M_\sigma^{\uparrow}| = m + 1$ but then $M_n \leq_{\mathrm{emb}} P$ is impossible since $|M_n| = m + 1$. Or $P \leq_{\mathrm{emb}} M_\sigma^{\uparrow} - \{\!|x|\!\} + \{\!|x - e_j|\!\}$ for some $x \in M_\sigma^{\uparrow}$ and some $j = 1, 2$ where $e_1 = \langle 1, 0\rangle$ and $e_2 = \langle 0, 1\rangle$. Without loss of generality, assume $j = 0$. Besides, $x = \langle \max(n-i-1, \sigma(i)), \max(i, n-\sigma(i)-1)\rangle$ for some $i \in [0, m]$. Depending on whether $i \geq n - \sigma(i) - 1$ this will either violates $M_n \leq_{\mathrm{emb}} P$ or $N_n \leq_{\mathrm{emb}} P$ considering the number of elements greater than $\max(i, n-\sigma(i)-1)$ in M_n or N_n. $\square$

Proposition 7.1.16. *There are polynomial-time procedures to intersect filters and ideals of* $(\mathbb{N}^\circledast, \leq_{\mathrm{emb}})$.

Proof.

(IF): Observe that since $(\mathbb{N}, \leq)$ is linear, multisets of $\mathbb{N}^\circledast$ can be sorted. In particular, if $M = \{\!|x_1 \cdots x_n|\!\}$ and $N = \{\!|y_1 \cdots y_m|\!\}$ with $x_1 > x_2 > \cdots > x_n$ and $y_1 > y_2 > \cdots > y_m$ and $n < m$ then $M \leq_{\mathrm{emb}} N$ if and only if $\forall i \in [n].\ x_i \leq y_i$.

Moreover, notice that if $|M| \leq |N|$, then $\uparrow M \cap \uparrow N = \uparrow(M + (|N| - |M|) \times \{\!|0|\!\}) \cap \uparrow N$, i.e. we can pad the shortest multiset with zeros. We can thus restrict our attention to multisets of the same length.

Given $M = \{\!|x_1 \cdots x_n|\!\}$ and $N = \{\!|y_1 \cdots y_n|\!\}$ with $x_1 > x_2 > \cdots > x_n$ and $y_1 > y_2 > \cdots > y_n$,

$$\uparrow M \cap \uparrow N = \uparrow\{\!|\max(x_1, y_1) \cdots \max(x_n, y_n)|\!\}$$

Indeed, if $\{\!|z_1 \cdots z_p|\!\} \in \uparrow M \cap \uparrow N$ with $z_1 > z_2 > \cdots > z_p$, then using the observation above, $z_i \geq \max(x_i, z_i)$ for $i \in [n]$.

(II): Here also, ideals of $\mathbb{N}$ are linearly ordered on the one hand, and ideals can be padded on the other hand. That is, we can restrict our attention to intersections $\downarrow_\in \boldsymbol{B} \oplus D^\circledast \cap \downarrow_\in \boldsymbol{C} \oplus E^\circledast$ of ideals of the following shape:

- $\boldsymbol{B} = \{\!|I_1 \cdots I_n|\!\}$ with $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$,
- $\boldsymbol{C} = \{\!|J_1 \cdots J_m|\!\}$ with $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_m$,
- We can assume $m = n$: assume otherwise suppose without loss of generality that $|\boldsymbol{B}| < |\boldsymbol{C}|$. We distinguish two cases:
  - Either $D \neq \emptyset$, in which case D is an ideal (all downward-closed sets of $\mathbb{N}$ are ideals, except $\emptyset$), in which case $\boldsymbol{B}$ can be padded with copies of D (cf. proof of Definition 7.1.8):

    $$\downarrow_\in \boldsymbol{B} \oplus D^\circledast = \downarrow_\in [\boldsymbol{B} + (|\boldsymbol{C}| - |\boldsymbol{B}|) \times \{\!|D|\!\}] \oplus D^\circledast$$

    .
  - Or $D = \emptyset$, in which case all multisets $M \in \downarrow_\in \boldsymbol{B} \oplus D^\circledast$ have length bounded by $n = |B|$. Thus

    $$\begin{aligned}\downarrow_\in \boldsymbol{B} \oplus D^\circledast \cap \downarrow_\in \boldsymbol{C} \oplus E^\circledast &= \downarrow_\in \boldsymbol{B} \oplus D^\circledast \cap (\mathbb{N}^{\leq n} \cap \downarrow_\in \boldsymbol{C} \oplus E^\circledast) \\ &= \downarrow_\in \boldsymbol{B} \oplus D^\circledast \cap \downarrow_\in \{\!|J_1 \cdots J_n|\!\} \oplus E^\circledast\end{aligned}$$

    where $\mathbb{N}^{\leq n}$ designates the set of multisets of length at most n of $\mathbb{N}$. Indeed, for a multiset of length bounded by n to be in $\downarrow_\in \boldsymbol{C} \oplus E^\circledast$, only the n greatest ideals of $\boldsymbol{C}$ are relevant.
- For all $I \in \boldsymbol{B}$, $D \subseteq I$: this is a weak form of the canonical form described in Definition 7.1.8. Indeed, assuming canonical form for the ideal $\downarrow_\in \boldsymbol{B} \oplus D^\circledast$ would entail that for all $I \in \boldsymbol{B}$, $I \not\subseteq D$, i.e. $D \subsetneq I$. But because of the previous step of padding, it might be the case that $D \in \boldsymbol{B}$.

- Similarly, for all $J \in \boldsymbol{C}$, $E \subseteq J$.

It is clear that from any two ideals $\boldsymbol{I}, \boldsymbol{J}$ of $(\mathbb{N}^{\circledast}, \leq_{\mathrm{emb}})$ we can produce in polynomial-time two ideals $(\boldsymbol{I}', \boldsymbol{J}')$ that have the specific form described above, and such that $\boldsymbol{I} \cap \boldsymbol{J} = \boldsymbol{I}' \cap \boldsymbol{J}'$. Now, for ideals $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ and $\downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast}$ satisfying the above conditions, we have:

$$\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} \cap \downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast} = \downarrow_{\in} \{\!|(I_1 \cap J_1) \cdots (I_n \cap J_n)|\!\} \oplus (D \cap E)^{\circledast}$$

We prove this equation by induction on n. The base case is trivial since $D^{\circledast} \cap E^{\circledast} = (D \cap E)^{\circledast}$. For the inductive case, let $x \in \mathbb{N}$ and $M \in \mathbb{N}^{\circledast}$ such that $x \geq y$ for all $y \in M$, and let $I \in \mathit{Idl}(\mathbb{N})$ and $\boldsymbol{B} \in \mathit{Idl}(\mathbb{N})^{\circledast}$ such that $I \supseteq K$ for any $K \in \boldsymbol{B}$, and let $J \in \mathit{Idl}(\mathbb{N})$ and $\boldsymbol{C} \in \mathit{Idl}(\mathbb{N})^{\circledast}$ such that $J \supseteq K$ for any $K \in \boldsymbol{C}$. Finally, let $D, E \in \mathit{Down}(\mathbb{N})$ and assume that $|\boldsymbol{B}| = |\boldsymbol{C}|$, that $D \subseteq K$ for any $K \in \boldsymbol{B}$ and that $E \subseteq K$ for any $K \in \boldsymbol{C}$. We have:

$$\begin{aligned}&\{\!|x|\!\} + M \in \downarrow_{\in} [\{\!|I|\!\} + \boldsymbol{B}] \oplus D^{\circledast} \cap \downarrow_{\in} \{\!|J|\!\} + \boldsymbol{C} \oplus E^{\circledast} \\ &\qquad\qquad\qquad\qquad \Leftrightarrow x \in I \cap J \wedge M \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} \cap \downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast}\end{aligned}$$

Left to right implication follows from the fact I and J are greater than ideals from $\boldsymbol{B}$ and $\boldsymbol{C}$, and greater than D and E. Right to left implication holds since x is greater than any elements of M. Now by induction hypothesis, M is in $\downarrow_{\in} \{\!|(I_1 \cap J_1) \cdots (I_n \cap J_n)|\!\} \oplus (D \cap E)^{\circledast}$, assuming $\boldsymbol{B} = \{\!|I_1 \cdots I_n|\!\}$ where elements are sorted, and similarly for $\boldsymbol{C}$. Thus this is equivalent to $\{\!|x|\!\} + M \in \downarrow_{\in} \{\!|(I \cap J) \cdot (I_1 \cap J_1) \cdots (I_n \cap J_n)|\!\} \oplus (D \cap E)^{\circledast}$. $\square$

7.1.4 Related Work

The WQO $(X^{\circledast}, \leq_{\mathrm{emb}})$ appears naturally to order configurations of some Petri Net extensions. The structure of its ideals and its ideally effectiveness are used in [18] for a forward algorithm to semi-decide reachability in timed Petri Nets, and in [27] to derive tight complexity upper bounds of the coverability problem for ν-Petri Nets. In the first case, $(X, \leq)$ is a finite alphabet, while in the second case it is $(\mathbb{N}^k, \leq_{\times})$.

Here also, these results have been generalized to Noetherian spaces in [13].

7.2 Multisets under the Manna-Dershowitz Ordering

Let $(X, \leq)$ be a WQO such that $\leq$ is antisymmetric. Such an ordering is often called well partial-order, abbreviated WPO.

The *multiset ordering* $N \leq_{\mathrm{ms}} M$, on the set $X^{\circledast}$ of finite multisets over $(X, \leq)$, has been introduced by Manna and Dershowitz in 1979 in the context of proving termination for rewriting systems ([35]). It is also called *domination ordering*, or the *multiset extension of* $<$ (all terms would induce a risk of confusion with the quasi-orderings of Section 7.1).

It is known that $(X^{\circledast}, \leq_{\mathrm{ms}})$ is a linear ordering whenever $(X, \leq)$ is. More precisely, if $(X, \leq)$ is isomorphic to some ordinal α, then $(X^{\circledast}, \leq_{\mathrm{ms}})$ is isomorphic to ω^{α}.

Before we give the formal definition of $\leq_{\mathrm{ms}}$, let us introduce some notations. Operations $+$ and $-$ on multisets introduced at the beginning of this chapter, do not act as inverse, and in particular are not associative (as in the case of $\mathbb{N}$). For instance $(A + B) - C \neq A + (B - C)$. Subsequently, we adopt the convention of a left-association, i.e. we write $A + B - C$ for $(A + B) - C$. With this convention for instance, $A + B - C = A - (C - B) + (B - C)$.

Definition 7.2.1. *The multiset ordering is equivalently defined by one of the following statements. The second formulation is the original definition, while the first one comes from [36].*

(Def 1) $\forall x \in X.\ N(x) > M(x) \Rightarrow (\exists y > x.\ M(y) > N(y))$

(Def 2) $\exists S, T \in X^{\circledast}.\ S \subseteq M\ \wedge\ N = M - S + T\ \wedge\ S$ *dominates* T
where a multiset S *dominates another multiset* T *if* $\forall x \in T\ \exists y \in S.\ x < y$*, see [35].*

(Def 3) $M - N$ *dominates* $N - M$

(Def 4) $N = \{\!|x_1 \cdots x_n|\!\}, M = \{\!|y_1 \cdots y_m|\!\}, \exists f : [n] \to [m] :$
$\forall i \in [n].\ ((x_i < y_{f(i)}) \vee (x_i \leq y_{f(i)} \wedge \forall j \neq i.\ f(j) \neq f(i)))$.
Intuitively, $N \leq_{\mathrm{ms}} M$ *if* N *embeds in* M *as in the previous section, but we don't require that the embedding is injective when an element is mapped to a strictly greater element.*

Proof. Equivalence between the four definitions.

First observe that for any two multisets M and N, we have $N = M - (M - N) + (N - M)$ (with implicit left parenthesizing). Implication (3) $\Rightarrow$ (2) directly follow from this observation.

(1) $\Rightarrow$ (3) Let M and N as in the first definition. Let x in $N - M$. Since $0 < \max(0, N(x) - M(x))$, we have $N(x) > M(x)$. According to the first definition, this implies that there exists $y > x$ with $M(y) > N(y)$, which means $y \in M - N$. This shows $M - N$ dominates $N - M$.

(2) $\Rightarrow$ (1) Assume $N = M - S + T$ with $S \subseteq M$ and S dominates T. Let $x \in X$ such that $N(x) > M(x)$, that is $M(x) - S(x) + T(x) > M(x)$, i.e. $T(x) > S(x)$. In particular, $x \in T$, hence there exists $y \in S$ such that $x < y$. Take y maximal in S with this property (S is finite), then $T(y) = 0$. Indeed, if not, there must be $z \in S$ with $z > y$, which contradicts the maximality of y. Now since $T(y) = 0$, $N(y) = M(y) - S(y) < M(y)$ since $y \in S$, which proves $N \leq_{\mathrm{ms}} M$ for the first definition.

(2) $\Rightarrow$ (4) Let $N \leq_{\mathrm{ms}} M$ according to the second definition, there are $S, T \in X^{\circledast}$ such that $S \subseteq M$, $N = M - S + T$ and S dominates T. That is, we can write $N = \{\!|y_1 \cdots y_m \cdot t_1 \cdots t_n|\!\}$ and $M = \{\!|y_1 \cdots y_m \cdot s_1 \ldots s_r|\!\}$. Define $f : [m+n] \to [m+r]$ by $f(i) = \begin{cases} i & \text{if } i \leq m \\ \epsilon_i & \text{otherwise} \end{cases}$, where ϵ_i for $i \in [n]$ is such that $t_i < s_{\epsilon_i}$ (it exists by the domination hypothesis). It is obvious that f satisfies the requirements from the

fourth definition, its restriction to $[m]$ is injective, and its restriction to $m + [n]$ is a domination.

(4) $\Rightarrow$ (2) Assume $N = \{\!|x_1 \cdots x_n|\!\} \leq_{\mathrm{ms}} M = \{\!|y_1 \cdots y_m|\!\}$, and let $f : [n] \to [m]$ be a function satisfying the requirements of the fourth definition. Define $S = \{\!|y_j \mid j \notin Im(f) \vee (\exists i \in [n].\ x_i < y_j = y_{f(i)})|\!\}$ and $T = \{\!|x_i \mid x_i < y_{f(i)}|\!\}$. Then obviously $S \subseteq M$. Moreover, $M - S = \{\!|y_j \mid \exists i \in [n].\ f(i) = j \wedge x_i = y_j|\!\}$, hence $N = M - S + T$ (indeed, every element in N is either equal to its image or strictly smaller). Finally, S dominates T, proving that $N \leq_{\mathrm{ms}} M$ according to the second definition.

$\square$

Note that we require $(X, \leq)$ to be a *partial*-order, and in this case, $(X^{\circledast}, \leq_{\mathrm{ms}})$ is a partial-order as well. From the fourth definition, it is obvious that $\leq_{\mathrm{emb}} \subseteq \leq_{\mathrm{ms}}$. Hence, $\leq_{\mathrm{ms}}$ is a WQO (when X is) and Section 4.1 applies. However function $\mathcal{C}l_{\mathrm{I}}$ is not computable here (this is shown in Section 8.3.2). The reason is the same as in Section 5.4: we cannot decide in general whether a given ideal is principal. Nonetheless, in this case, we can show that $(X^{\circledast}, \leq_{\mathrm{ms}})$ is ideally effective, but of course, for a different representation of ideals. Let us now define this representation of ideals. By Proposition 4.1.1, $Idl(X^{\circledast}, \leq_{\mathrm{ms}}) = \{\downarrow_{\leq_{\mathrm{ms}}} \boldsymbol{I} \mid \boldsymbol{I} \in Idl(X^{\circledast}, \leq_{\mathrm{emb}})\}$. This helps proving the following proposition:

Proposition 7.2.2. *Let $(X, \leq)$ be a WPO. Then,*

$$Idl(X^{\circledast}, \leq_{\mathrm{ms}}) = \{\downarrow_{\mathrm{ms}} B + D^{\circledast} \mid B \in X^{\circledast}, D \in Down(X)\}$$

Warning: unlike in the previous section, here B is a multiset of elements of X, not of ideals. Observe that $\downarrow B + D^{\circledast} = \{M_1 + M_2 \mid M_1 \leq_{\mathrm{ms}} B \wedge M_2 \in D^{\circledast}\} = \{M \mid M \setminus D \leq_{\mathrm{ms}} B\}$.

Proof. ($\supseteq$) We show that given $B \in X^{\circledast}$ and $D \in Down(X)$, $\downarrow B + D^{\circledast}$ is an ideal.

- It is downward-closed: let $N \leq_{\mathrm{ms}} M \in \downarrow B + D^{\circledast}$. Obviously, this implies that $N \setminus D \leq_{\mathrm{ms}} M \setminus D$ and by assumption $M \setminus D \leq_{\mathrm{ms}} B$. Thus, by transitivity, $N \setminus D \leq_{\mathrm{ms}} B$.
- It is directed: let $M_1, M_2 \in \downarrow B + D^{\circledast}$. Let $N = B + M_{1|D} + M_{2|D}$. Then $N \in \downarrow B + D^{\circledast}$ and $M_i \leq_{\mathrm{ms}} N$.

($\subseteq$) Let $\boldsymbol{J} \in Idl(X^{\circledast}, \leq_{\mathrm{ms}})$, $\boldsymbol{J} = \downarrow_{\leq_{\mathrm{ms}}} \boldsymbol{I}$ for some $\boldsymbol{I} \in Idl(X^{\circledast}, \leq_{\mathrm{emb}})$, and $\boldsymbol{I} = \downarrow_{\in} \boldsymbol{C} \oplus E^{\circledast} = \{M \mid M \setminus E \in_{\mathrm{emb}} \boldsymbol{C}\}$ for some $\boldsymbol{C} \in Idl(X)^{\circledast}$ and $E \in Down(X)$. Write $\boldsymbol{C}$ as $\{\!|I_1 \cdots I_k \cdot \downarrow x_1 \cdots \downarrow x_m|\!\}$ where the I_i's are limit ideals (i.e. not principal). Define $B = \{\!|x_1 \cdots x_m|\!\}$ and $D = E \cup I_1 \cup \cdots \cup I_k$. We show that $\boldsymbol{J} = \downarrow_{\leq_{\mathrm{ms}}} \boldsymbol{I} = \downarrow B + D^{\circledast}$.

- ($\subseteq$) It is simple to see that $\boldsymbol{I} \subseteq \downarrow B + D^{\circledast}$ and since $\downarrow B + D^{\circledast}$ is downward-closed, we have one inclusion.

- $(\supseteq)$ To show the second inclusion, let $M \in \downarrow B + D^{\circledast}$. Since each ideal I_i is directed and unbounded, while M is finite, it is possible to pick in each I_i an element strictly greater than any of the elements in $M_{|I_i}$. Putting these elements together, we define a multiset $M' \in_{\mathrm{emb}} \{\!|I_1 \cdots I_k|\!\}$. Now the following holds: $M \leq_{\mathrm{ms}} B + M' + M_{|E}$ (cf. definition 4 for instance), and since $B + M' \in_{\mathrm{emb}} \boldsymbol{C}$, it proves that $M \in \downarrow_{\leq_{\mathrm{ms}}} \boldsymbol{I}$.

□

According to this proposition, we can represent ideals of $(X^{\circledast}, \leq_{\mathrm{ms}})$ as pairs $(B, D) \in X^{\circledast} \times Down(X)$, the semantic being the set $\downarrow_{\mathrm{ms}} B + D^{\circledast}$. Elements of $X^{\circledast}$ are represented as in the previous section. We can now state the main result of this section.

Theorem 7.2.3. *With aforementioned representations, the finite multiset extension with domination ordering is an ideally effective construction. It is not polynomial-time in general. Given a polynomial-time presentation of an ideally effective WQO $(X, \leq)$, we can compute an exponential-time presentation of $(X^{\circledast}, \leq_{\mathrm{ms}})$.*

Let $(X, \leq)$ designates an ideally effective WPO. The rest of this section is dedicated to the proof of the theorem. Here is the outline:

(OD), (PI) Any of the four equivalent definition of $\leq_{\mathrm{ms}}$ provide a procedure to decide $\leq_{\mathrm{ms}}$. The third one is the most convenient to notice that when $(X, \leq)$ is given by a polynomial-time presentation, $\leq_{\mathrm{ms}}$ can be decided in polynomial-time.

(PI) The function $M \mapsto \downarrow_{\mathrm{ms}} M$ is trivial with our representation of ideals: it outputs the pair $(M, \emptyset)$. This procedure obviously runs in polynomial-time when $(X, \leq)$ is given by a polynomial-time presentation.

(ID), In Section 7.2.1, we give a procedure to decide ideal inclusion. This procedure runs in polynomial time when $(X, \leq)$ is given by a polynomial-time presentation. We will also define canonical representations for ideals of $(X^{\circledast}, \leq_{\mathrm{ms}})$.

(CF),(II),(IF) In subsections 7.2.2, 7.2.4 and 7.2.5, we give procedures to complement filters, intersect ideals and intersect filters, respectively. These procedures run in polynomial-time when $(X, \leq)$ is given by a polynomial-time presentation.

(II) In Section 7.2.3, we give a procedure to complement ideals. This procedure runs in exponential-time when $(X, \leq)$ is given by a polynomial-time procedure. In this same subsection, we prove that a matching lower bound. We also provide a polynomial-time procedure some specific WQOs.

- It will be obvious that the procedures mentioned above are computable from a presentation of $(X, \leq)$.

(XF) The set of all finite multisets is the upward-closure of the empty multiset.

(XI) As a downward-closed set, $X^{\circledast}$ is its own ideal decomposition, since it is an ideal.

In the following subsections, $(X, \leq)$ always designates a WQO.

7.2.1 Ideal Inclusion (ID)

Proposition 7.2.4. *Given $B_1, B_2 \in X^{\circledast}$ and $D_1, D_2 \in Down(X)$:*

$$\begin{aligned}\downarrow B_1 + D_1^{\circledast} \subseteq \downarrow B_2 + D_2^{\circledast} \textit{ iff } & B_1 \setminus D_2 \leq_{\mathrm{ms}} B_2 \textit{ and} \\ & D_1 \subseteq D_2 \cup \downarrow_< Supp(B_2 - B_1)\end{aligned}$$

If $(X, \leq)$ is an (polynomial-time) ideally effective WQO, the above characterization of inclusion leads to a (polynomial-time) procedure to decide inclusion.

Proof. $(\Rightarrow)$ First, $B_1 \in \downarrow B_1 + D_1^{\circledast} \subseteq \downarrow B_2 + D_2^{\circledast}$, thus $B_1 \setminus D_2 \leq_{\mathrm{ms}} B_2$.

For the second part, let $x \in D_1$, consider the multiset $M = B_1 \setminus D_2 + \{\!| x \cdots x |\!\}$ with $|B_2| + 1$ copies of x. Obviously, $M \in \downarrow B_1 + D_1^{\circledast} \subseteq \downarrow B_2 + D_2^{\circledast}$ and thus $M \setminus D_2 \leq_{\mathrm{ms}} B_2$. Now, if $x \notin D_2$, then $x \in M \setminus D_2$ and $M(x) = B_1(x) + |B_2| + 1 > |B_2| \geq B_2(x)$, thus there exists $y > x$ such that $B_2(y) > M(y) = B_1(y)$. This implies that $y \in Supp(B_2 - B_1)$ and $x < y$.

$(\Leftarrow)$ Let $M \in \downarrow B_1 + D_1^{\circledast}$, i.e. $M \setminus D_1 \leq_{\mathrm{ms}} B_1$. We want to show $M \setminus D_2 \leq_{\mathrm{ms}} B_2$. Decompose M in two parts: $M \setminus D_2 = (M \setminus D_2) \setminus D_1 + (M \setminus D_2)_{|D_1}$. For the first part, $(M \setminus D_2) \setminus D_1 = (M \setminus D_1) \setminus D_2 \leq_{\mathrm{ms}} B_1 \setminus D_2$. Besides, by the third definition of $\leq_{\mathrm{ms}}$, $B_1 \setminus D_2 = B_2 - S + T$ for $S = B_2 - (B_1 \setminus D_2)$ and $T = (B_1 \setminus D_2) - B_2$, and S dominates T.

For the second part, observe that $D_2 \cup \downarrow_< Supp(B_2 - B_1) = D_2 \cup \downarrow_< Supp(B_2 - (B_1 \setminus D_2))$ and thus $D_1 \setminus D_2 \subseteq \downarrow_< Supp(S)$. It follows that $(M \setminus D_2)_{|D_1}$ is dominated by S, and we obtain:

$$\begin{aligned} M \setminus D_2 &= (M \setminus D_2) \setminus D_1 + (M \setminus D_2)_{|D_1} \\ &\leq_{\mathrm{ms}} B_1 \setminus D_2 + (M \setminus D_2)_{|D_1} \\ &= B_2 - S + (T + (M \setminus D_2)_{|D_1}) \\ &\leq_{\mathrm{ms}} B_2 \end{aligned}$$

Computability: Assuming $(X, \leq)$ is a (polynomial-time) ideally effective WQO, the objects $B_1 \setminus D_2$ and $D_2 \cup \downarrow_< Supp(B_2 - B_1)$ can be computed (in polynomial-time), and $\leq_{\mathrm{ms}}$ and $\subseteq$ on $Down(X)$ can be decided (in polynomial-time). □

Notice that as in the case of finite multisets with the embedding ordering, this representation is not unique, and we now provide a canonical representation for each ideal.

Proposition 7.2.5. *For every ideal $\boldsymbol{I}$ of $(X^{\circledast}, \leq_{\mathrm{ms}})$, there exists a unique representation $\boldsymbol{I} = \downarrow B + D^{\circledast}$ such that $B_{|D} = \emptyset$.*

Besides, when $(X, \leq)$ is an (polynomial-time) ideally effective WQO, this canonical representation *is computable (in polynomial-time) from any other representation.*

Proof. Given $\boldsymbol{I} = \downarrow B + D^{\circledast}$, the canonical representation of $\boldsymbol{I}$ is $\downarrow(B \setminus D) + D^{\circledast}$, which is obviously computable using $|B| \cdot |D|$ membership tests in $(X, \leq)$.

Now for uniqueness, assume $\downarrow B_1 + D_1^{\circledast} = \downarrow B_2 + D_2^{\circledast}$ and for $i \in \{1, 2\}$, $B_{i|D_i} = \emptyset$. By contradiction, assume there exists $x \in B_1 - B_2$, and assume x maximal.

- Either $x \in D_2$: but since $D_2 \subseteq D_1 \cup \downarrow_< Supp(B_1 - B_2)$ and $x \notin D_1$ by assumption, it implies that there exists $y > x$ such that $B_1(y) > B_2(y)$. This contradicts the maximality of x.
- Or $x \notin D_2$: then since $B_1 \smallsetminus D_2 \leq_{\mathrm{ms}} B_2$, there must be $y > x$ such that $B_2(y) > B_1(y)$. Once again, we can pick y maximal.
  - Either $y \in D_1$: but $D_1 \subseteq D_2 \cup \downarrow_< Supp(B_2 - B_1)$, but by maximality, y cannot be in $\downarrow_< Supp(B_2 - B_1)$. On the other hand, y is in B_2, and thus cannot be in D_2 either. Contradiction.
  - Or $y \notin D_1$: and since $B_2 \smallsetminus D_1 \leq_{\mathrm{ms}} B_1$, this implies the existence of $z > y > x$ such that $B_1(z) > B_2(z)$, contradicting the maximality of x.

Using the symmetry of the situation, we have proved $B_1 = B_2$. Thus $B_1 - B_2 = B_2 - B_1 = \emptyset$, which entails $D_1 = D_2$.

□

7.2.2 Complementing Filters (CF)

Proposition 7.2.6. *Given $N \in X^{\circledast}$ and $x \in X$, define $N_x = N_{|\uparrow x} - \{\!|x|\!\}$.*
The complement of $\uparrow N$ is given by:

$$X^{\circledast} \smallsetminus \uparrow N = \bigcup_{x \in Supp(N)} \downarrow N_x + (X \smallsetminus \uparrow x)^{\circledast}$$

From this expression, we easily derive a (polynomial-time) procedure to complement filters when $(X, \leq)$ is a (polynomial-time) ideally effective WQO.

Proof. $(\subseteq)$ Let $M \notin \uparrow N$, by negating the first definition, this is equivalent to

$$\exists x \in N.\ N(x) > M(x) \wedge \forall y > x.\ M(y) \leq N(y)$$

Then $M \in \downarrow N_x + (X \smallsetminus \uparrow x)^{\circledast}$ directly follows from the fact that $\forall y \in X.\ M_{|\uparrow x}(y) \leq N(y)$.

$(\supseteq)$ Let $x \in Supp(N)$ and $M \in \downarrow N_x + (X \smallsetminus \uparrow x)^{\circledast}$. We show that there exists y such that $N(y) > M(y)$ and for all $z > y$, $N(y) \geq M(y)$. Let S, T be two multisets such that $M_{|\uparrow x} = N_x - S + T$ and S dominates T. We consider two cases:

1. If x is maximal in S, then take $y = x$. By domination, for any $z \in T$, $z \ngeq x$, hence forall $z \geq x$, $M(z) = N_x(z)$. In particular, $M(x) = N_x(x) < N(x)$ and $M(z) \leq N_x(z) = N(z)$ for $z > x$.

2. Otherwise, take a maximal $y \in S$ such that $y \geq x$. In particular, $T(y) = 0$ and $S(y) \geq 1$, which implies that $M(y) = N_x(y) - S(y) + T(y) < N_x(y) \leq N(y)$. Besides, given $z > y$, $M(z) = N_x(z) - 0 + 0 \leq N(z)$.

□

7.2.3 Complementing Ideals (CI)

Proposition 7.2.7. *Let $B \in X^{\circledast}$ and $D \in Down(X)$.*
Given $x \in X$, define $B_x = B_{|\uparrow x} + \{\!|x|\!\}$ Then:

$$X^{\circledast} \smallsetminus (\downarrow B + D^{\circledast}) = \bigcup_{S \subseteq Supp(B)} \uparrow\{B_x \mid x \in \min(X \smallsetminus (D \cup \downarrow S))\}$$

The above expression is clearly computable (in exponential-time) when $(X, \leq)$ is a (polynomial-time) ideally effective WQO.

Proof. ($\subseteq$) Let $M \notin \downarrow B + D^{\circledast}$. Let $N = M \smallsetminus D$, by assumption $N \not\leq_{\text{ms}} B$. Thus, there exists $x \in X$ such that $N(x) > B(x)$ and for all $y > x$, $N(y) \geq B(y)$ (negation of the first definition of $\leq_{\text{ms}}$). Since $N(x) > 0$, $x \notin D$. Let S be the largest subset of $Supp(B)$ such that $x \notin \downarrow S$. It exists since $x \notin \emptyset$ and the property is stable by union. The element x is thus in $X \smallsetminus (D \cup \downarrow S)$ and there exists $y \in \min(X \smallsetminus (D \cup \downarrow S))$ such that $y \leq x$.

We now prove that $B_y \leq_{\text{ms}} M$. Observe that, by maximality of S, for all $z \in Supp(B) \smallsetminus S$, $x \leq z$. Thus, $B_{|\uparrow x} = B_{|\uparrow y}$ which proves that $B_y \leq_{\text{ms}} B_x$. On the other hand, for any $z \in X$, $B_x(z) \leq M(z)$. This is immediate for $z \not\geq x$. For $z = x$, $M(x) = N(x) > B(x) = B_x(x) - 1$. And for $z > x$, $M(z) = N(z) \geq B(z) = B_x(z)$. This proves $B_y \leq_{\text{ms}} B_x \leq_{\text{ms}} M$ which concludes this direction of the proof.

($\supseteq$) For any $x \in X$, $B_x \not\leq_{\text{ms}} B$: this is immediate by negating the first definition of $\leq_{\text{ms}}$ and instantiating with x. Thus, for any $x \notin D$, $B_x \notin \downarrow B + D^{\circledast}$, which proves the desired inclusion.

□

We now provide a matching lower bound on the operation of complementing ideals, proving that the procedure given by Proposition 7.2.7 is asymptotically optimal in general. Notice that for a finite alphabet A, $(A^{\circledast}, \leq_{\text{emb}}) = (A^{\circledast}, \leq_{\text{ms}})$, since there are no elements $x, y \in A$ such that $x < y$. Thus, $(A^{\circledast}, \leq_{\text{ms}}) \equiv (\mathbb{N}^{|A|}, \leq_{\times})$ and all operations can be performed in polynomial-time. Besides, as stated in the introduction of this chapter, $(\mathbb{N}, \leq_{\text{ms}})$ is isomorphic to the ordinal ω^{ω}, for which all operations are computable in polynomial-time as well.

The next natural candidate would be $\mathbb{N}^2$, but then it suffices to take union over subsets of size 2 of $Supp(B)$ in the formula of Proposition 7.2.7, which results in polynomial-time complexity. More generally:

Proposition 7.2.8. *For $(X, \leq) = (\mathbb{N}^k, \leq_{\times})$, there is a polynomial-time procedure to complement ideals, described by the following expression: Given $B \in X^{\circledast}$ and $D \in Down(X)$,*

$$X^{\circledast} \smallsetminus (\downarrow B + D^{\circledast}) = \bigcup_{\substack{S \subseteq Supp(B) \\ |S| \leq k}} \uparrow\{B_x \mid x \in \min(X \smallsetminus (D \cup \downarrow S))\}$$

The only difference with the general expression is that it suffices to take the union over subsets of $Supp(B)$ that have size at most k, leading to a polynomial-time implementation.

Proof. We show that for every minimal elements x of $X \smallsetminus (D \cup \downarrow S)$ for some $S \subseteq Supp(B)$ such that $|S| > k$, x is also a minimal element of $X \smallsetminus (D \cup \downarrow S')$ for some $S' \subseteq Supp(B)$ with $|S'| \leq k$.

Indeed, denote by e_i the element of $\mathbb{N}^k$ that has a 1 on the i-th component, zeros elsewhere. Since x is minimal in $X \smallsetminus (D \cup \downarrow S)$, for every $i \in [1,k]$, $x_i = x - e_i$ is either in D, or in $\downarrow S$, or $x_i \notin \mathbb{N}^k$ (if the i-th component of x is 0). Therefore, we can define a subset $S' \subset S$ of size at most k such that for every $i \in [1,k]$, $x_i \in D$ or $x_i \in \downarrow S'$, or $x_i \notin \mathbb{N}^k$. Obviously, x is still in $X \smallsetminus (D \cup \downarrow S')$, and is still minimal since for every i, $x_i \in (D \cup \downarrow S')$ (if $x_i \in \mathbb{N}^k$).

□

Finally, the lower bound is proved using the polynomial-time ideally effective WQO $(\mathcal{P}_f(\mathbb{N}^2), \sqsubseteq_{\mathcal{H}})$ (cf. Section 7.3).

Proposition 7.2.9. *Let $(X, \leq) = (\mathcal{P}_f(\mathbb{N}^2), \sqsubseteq_{\mathcal{H}})$ where $\mathbb{N}^2$ is ordered with the product ordering. For $n \in \mathbb{N}$, $i \in [1,n]$ and $U \subseteq [1,n]$, define:*

$$\begin{aligned} x_i &= \langle i-1, n-i \rangle \\ S_U &= \{x_i \mid i \in U\} \\ T_i &= S_{[1,n]\smallsetminus\{i\}} = \{x_j \mid j \neq i\} \\ B &= \{\!| T_1 \cdots T_n |\!\} \\ D &= \mathcal{P}_f(\bigcup_{i=1}^{n-1} \langle i-1, n-1-i \rangle) \end{aligned}$$

The upward-closed set $X^{\circledast} \smallsetminus (\downarrow B + D^{\circledast})$ has at least $2^n - 1$ minimal elements. In particular, any procedure for (CI) *runs in exponential-time in the worst case.*

Proof. The elements $(x_i)_{1 \leq 1 \leq n}$ form an antichain of size n of $\mathbb{N}^2$. The downward-closed set D is chosen so that any set which is both smaller than $S_{[1,n]}$ and in $\complement D$ is equal to S_U for some $U \in [1,n]$.

Recall from Proposition 7.2.7 that minimal elements of $X^{\circledast} \smallsetminus (\downarrow B + D^{\circledast})$ are of the form B_S, where $B_S = B_{|\uparrow S} + \{\!|S|\!\}$. We here show that multisets B_{S_U} all are minimal elements of $X^{\circledast} \smallsetminus (\downarrow B + D^{\circledast})$ when U ranges over *strict* subsets of $[1,n]$. Given $U \subseteq [1,n]$, B_{S_U} will be denoted B_U for readability. Since $(x_i)_{1 \leq i \leq n}$ is an antichain, given $U, V \subseteq [1,n]$, $S_U \sqsubseteq_{\mathcal{H}} S_V \Leftrightarrow S_u \subseteq S_V \Leftrightarrow U \subseteq V$. Thus B_U has one copy of each T_i such that $i \notin U$, and an extra copy of S_U.

For any $U \subsetneq [1,n]$, $S_U \notin D$, thus $B_U \notin (\downarrow B + D^{\circledast})$ (cf. second part of the proof of Proposition 7.2.7). It remains to show that each B_U is minimal. Let $U \subsetneq [1,n]$ and M be some multiset such that $M <_{\mathrm{ms}} B_U$. According to the second definition of $\leq_{\mathrm{ms}}$, there exists multisets P and Q such that $\emptyset \neq P \subseteq B_U$, $M = B_U - P + Q$ and P dominates Q. Without loss of generality, we can assume that $Supp(M) \cap D = \emptyset$. Subsequently, we show that $M \leq_{\mathrm{ms}} B$. Assume $M(S) > B(S)$ for some $S \in X$. By case analysis:

- If $S \in Q$, then there exists $T \in P$ such that $S \sqsubseteq_{\mathcal{H}} T$. In particular $T \in B_U$.

1. If $T = S_U$: from $S \notin D$ and $S \sqsubseteq_{\mathcal{H}} S_U$, we deduce that $S = S_V$ for some $V \subsetneq U$ (D has been chosen for this property). Therefore, there exists $i \in U \smallsetminus V$, hence $S = S_V \sqsubseteq_{\mathcal{H}} T_i$, while $T = S_u \not\sqsubseteq_{\mathcal{H}} T_i$. However, $B_U(R) = 0$ for any $T_i \sqsubseteq_{\mathcal{H}} R$, thus $M(T_i) = 0 < 1 \leq B(T_i)$.
2. Otherwise, $T = T_i$ for some $i \notin U$, and we can assume that $S_U \neq T_i$. Then $M(T_i) = 0 < B(T_i) = 1$.

- If $x \notin Q$, then we have $B_U(S) \geq M(S) > B(S)$ and by definition of B_U this is only possible for $S = S_U$ in which case $B_U(S) = M(S) = B(S) + 1$. From $B_U(S) = M(S)$ we deduce that $S \notin P$, and P is not empty, thus there is some i such that $T_i \in P$. Note that this T_i cannot be equal to S_U since $B_U(S_U) = M(S_U)$. Thus, $S_U \sqsubset_H T_i$ and $M(T_i) = 0 < B(T_i) = 1$.

In conclusion, the exponential-time procedure described in Proposition 7.2.7 is optimal in the general.

□

7.2.4 Intersecting Ideals (II)

Proposition 7.2.10. *Let $\downarrow B_0 + D_0^{\circledast}$ and $\downarrow B_1 + D_1^{\circledast}$ be two ideals given by their canonical representation, that is for $i \in \{0,1\}$, $B_{i|D_i} = \emptyset$. For $i \in \{0,1\}$, define $\bar{\imath} = 1 - i$ and:*

$$\begin{aligned} B'_i &= B_i \smallsetminus D_{\bar{\imath}} - B_0 \cap B_1 \\ S_i &= \{x \in B'_i \mid \exists z \in B'_{\bar{\imath}}.\, z > x \wedge \forall t \in B'_i.\, t \not> z\} \\ B &= B_0 \cap B_1 + B'_{0|S_0} + B'_{1|S_1} + B_{0|D_1} + B_{1|D_0} \\ D &= \bigcup_{\substack{x \in B_0 - B \\ y \in B_1 - B}} (\downarrow x \cup D_0) \cap (\downarrow y \cup D_1) \end{aligned}$$

The intersection of two ideals is an ideal:

$$(\downarrow B_0 + D_0^{\circledast}) \cap (\downarrow B_1 + D_1^{\circledast}) = \downarrow B + D^{\circledast}$$

When $(X, \leq)$ is an (polynomial-time) ideally effective WQO, this leads to a (polynomial-time) procedure to intersect ideals, in particular because in this case, we can compute the canonical representation in polynomial-time.

Fig. 7.1 may help the understanding of the above expression. The multiset B, depicted by the areas dashed in red on the figure, consists of the intersection $B_0 \cap B_1$, restrictions $B_{i|D_{\bar{\imath}}}$, plus the red clouds. Note that, as shown on the picture, these 3 parts of the definition of B are pairwise disjoint. Indeed, we assume that ideals $\downarrow B_i + D_i^{\circledast}$ are given by their canonical representations, hence there are no elements from D_i in B_i. Thus $B_0 \cap B_1 \cap B_{i|D_{\bar{\imath}}} \subseteq B_{\bar{\imath}|D_{\bar{\imath}}} = \emptyset$. The red clouds are disjoint from the two aforementioned parts by construction: we restrict our attention to what is left of the two multisets, which we denote B'_i. Of these multisets B'_i, we only keep in B elements from sets S_i. These sets consist of elements of B'_i that are dominated by elements in

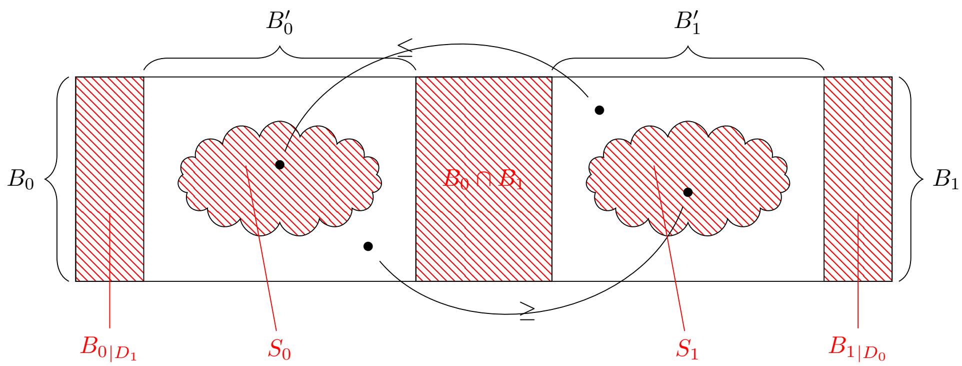

Figure 7.1: Intersection of Ideals

$B_{\bar{\imath}}'$ that are not themselves dominated in B_i'. In other words, for every $x \in S_i$ (point in the cloud), there exists some $y > x$ which is in $B_{\bar{\imath}}'$, but not in $S_{\bar{\imath}}$, i.e. not in the other cloud.

Proof. First of all, notice from the construction that for any $x \in X$, $B(x) \in \{B_0(x), B_1(x)\}$. Indeed, consider the following cases:

- If $x \in D_0$: then $B_0(x) = 0$ since we assumed ideals given by their canonical representations. Thus $B(x) = \min(0, B_1(x)) + 0 + B'_{1|S_1}(x) + 0 + B_{1|D_0}(x)$. By definition, $B_1'(x) = 0$ and $B_{1|D_0}(x) = B_1(x)$. Thus $B(x) = B_1(x)$.
- Similarly if $x \in D_1$, $B(x) = B_0(x)$.
- Otherwise, $x \notin D_0 \cup D_1$. Note that $S_0 \cap S_1 = \emptyset$ by construction. Three cases remain:
  - If $x \in S_0$, then $x \notin S_1$ thus $B'_{0|S_0}(x) = B_0'(x)$ and $B'_{1|S_1}(x) = 0$. Thus, $B(x) = (B_0 \cap B_1)(x) + (B_0 \smallsetminus D_1)(x) - (B_0 \cap B_1)(x) = B_0(x)$.
  - Similarly if $x \in S_1$, $B(x) = B_1(x)$.
  - Otherwise, $B(x) = \min(B_0(x), B_1(x)) \in \{B_0(x), B_1(x)\}$.

($\subseteq$) Let $M \in ({\downarrow} B_0 + D_0^{\circledast}) \cap ({\downarrow} B_1 + D_1^{\circledast})$. We want to show $M \smallsetminus D \leq_{\mathrm{ms}} B$. Let $x \notin D$ such that $M(x) > B(x)$. We distinguish two cases:

1. Either $B(x) = \max(B_0(x), B_1(x))$. Four possibilities:

   (a) $x \notin D_0 \cup D_1$. In that case, since $M \smallsetminus D_0 \leq_{\mathrm{ms}} B_0$ and $M \smallsetminus D_1 \leq_{\mathrm{ms}} B_1$, there exist $y > x$ and $z > x$ such that $M(y) < B_0(y)$ and $M(z) < B_1(z)$. Now, if $B_0(y) > B(y)$ and $B_1(z) > B(z)$ hold simultaneously, then $x \in {\downarrow} y \cap {\downarrow} z \subseteq D$ which is a contradiction. Thus, at least one of the previous inequality does not hold, implying either $B(y) > M(y)$ or $B(z) > M(z)$.

   (b) $x \in D_0 \smallsetminus D_1$. In that case, we only have the existence of $z > x$ such that $B_1(z) > M(z)$. Again, if $B_1(z) > B(z)$ then $x \in {\downarrow} z \cap D_0 \subseteq D$, which is a contradiction. Thus $B(z) \geq B_1(z) > M(z)$.

(c) $x \in D_1 \smallsetminus D_0$ is symmetrical.

(d) Finally, $x \in D_0 \cap D_1$ is impossible, since $D_0 \cap D_1 \subseteq D$.

2. Or $B_i(x) > B(x) = B_{\bar{\imath}}(x)$. Without loss of generality, we assume $i = 0$. From $B_0(x) > B(x) \geq B_{0|D_1}(x)$ we deduce $x \notin D_1$. Since $M \smallsetminus D_1 \leq_{\mathrm{ms}} B_1$, there exists $y > x$ such that $B_1(y) > M(y)$. If $B_1(y) > B(y)$, then $y \in B_1 - B$, and since $x \in B_0 - B$, this would imply $x \in \downarrow x \cap \downarrow y \subseteq D$, which is a contradiction. Thus, $B(y) \geq B_1(y) > M(y)$.

($\supseteq$) We show $\downarrow B + D^{\circledast} \subseteq \downarrow B_i + D_i^{\circledast}$, for $i \in \{0, 1\}$, using Proposition 7.2.4. We thus want to show that:

1. $B \smallsetminus D_i \leq_{\mathrm{ms}} B_i$

2. $D \subseteq D_i \cup \downarrow_< \mathit{Supp}(B_i - B)$

We prove the result for $i = 0$, the case $i = 1$ being symmetrical. To prove the first point, assume some $x \notin D_0$ is such that $B(x) > B_0(x)$. By our preliminary remark, it implies $B(x) = B_1(x) > B_0(x)$, which also implies $x \in B_1$, and thus $x \notin D_1$. Now, since we are in the case $B(x) = \max(B_0(x), B_1(x)) = B_1(x)$, by definition $B'_{1|S_1}(x) \neq 0$, and thus: $x \in S_1$, i.e. $\exists z \in B'_0.\ z > x$, and $\nexists t \in B'_1.\ t > z$. From the last condition we deduce that $B'_{0|S_0}(z) = 0$, therefore $B(z) = \min(B_0(z), B_1(z))$. Furthermore, from $z \in B'_0$ we deduce that $B_0(z) > B_1(z)$, and conclude $B_0(z) > B(z)$.

For the second point, distributing the intersection over the unions leads to four cases to consider:

1. Given $x \in B_0 - B$ and $y \in B_1 - B$, $\downarrow x \cap \downarrow y \subseteq \downarrow_< \mathit{Supp}(B_0 - B)$ follows from $x \neq y$. This itself follows from $B_0 \cap B_1 \subseteq B$.

2. Given $x \in B_0 - B$, by construction of B, $x \notin D_1$. Thus for any z in $\downarrow x \cap D_1$, $z < x$, and $z \in \downarrow_< \mathit{Supp}(B_0 - B)$.

3. Given $y \in B_1 - B$, it is obvious that $\downarrow y \cap D_0 \subseteq D_0$.

4. Finally, $D_0 \cap D_1 \subseteq D_0$, obviously.

□

7.2.5 Intersecting Filters (IF)

Proposition 7.2.11. *Given two multisets M_0 and M_1, and $i \in \{0, 1\}$, we write $\bar{\imath}$ for $1 - i$, and define $S_i = \{x \in M_i \mid \forall z \in M_{\bar{\imath}} - M_i.\ z > x \Rightarrow \exists t \in M_i - M_{\bar{\imath}}.\ t > z\}$.*

The intersections of two filters is a filter:

$$\uparrow M_0 \cap \uparrow M_1 = \uparrow (M_{0|S_0} \cup M_{1|S_1})$$

When $(X, \leq)$ is an (polynomial-time) ideally effective WQO, this leads to a (polynomial-time) procedure to intersect filters.

It is easier to understand this complicated condition on examples. Take $X = \mathbb{N}^2$. If $M_0 = [(1,1)(2,1)]$ and $M_1 = [(1,2)]$, then $M_{0|S_0} \cup M_{1|S_1} = [(1,2)(2,1)]$, which is indeed greater than both M_0 and M_1. On the other hand, if $M_0 = [(1,1)(2,2)]$ and $M_1 = [(2,2)]$, then $M_{0|S_0} \cup M_{1|S_1} = [(1,1)(2,2)]$. Notice how $(1,1)$ is not part of the final result in the second example, while it is in the second. Intuitively, the condition expresses that an element x from M_0 will not be in the final result if it is dominated by some $z \in M_1$ such that z is in the final result. The fact that z is in the final result is expressed by negating the existence of a t in M_0 that dominates z. The condition on the multiplicities of z and t becomes clear when considering the case $M_0 = [(1,1)(2,2)]$ and $M_1 = [(2,2)(2,2)]$ and comparing it to the second example.

Proof. Define $M'_i = M_{i|S_i}$ and $M = M'_0 \cup M'_1$, that is for all $x \in X$, $M(x) = \max(M'_0(x), M'_1(x))$.

($\subseteq$) Let $N \in \uparrow M_0 \cap \uparrow M_1$. To prove $M \leq_{\text{ms}} N$, assume $N(x) < M(x) = \max(M'_1(x), M'_2(x))$ for some x. This implies that $M'_i(x) > N(x)$ for some $i \in \{0,1\}$, and without loss of generality, we assume $i = 0$. This implies $M'_0(x) > 0$, thus $x \in S_0$ and $M'_0(x) = M_0(x)$. Since $M_0 \leq_{\text{ms}} N$, there exists $y > x$ such that $M_0(y) < N(y)$.

If $M'_1(y) < N(y)$, then $M(y) < N(y)$, which concludes the proof. We now prove that the other case, $M'_1(y) \geq N(y)$ is impossible. It in particular implies $y \in S_1$ and thus $M_1(y) \geq N(y) > M_0(y)$. Recall that $x \in S_0$, therefore $\forall z \in M_1 - M_0.\, z > x \Rightarrow \exists t \in M_0 - M_1.\, t > z)$. Instantiated with $z = y$, it gives the existence of $t \in M_0 - M_1$ such that $t > y$. Besides, we can consider this t maximal. Similarly, we instantiate with $z = t$ in the condition of $y \in S_1$, to obtain the existence of $u \in M_1 - M_0$ such that $u > t$. Now, we instantiate one more time the condition given by $x \in S_0$, but with $z = u$. This gives the existence of $v \in M_0 - M_1$ such that $v > u > t$, which contradicts the maximality of t. Thus this case is impossible, and $M \leq_{\text{ms}} N$.

($\supseteq$) We show that $M_0 \leq_{\text{ms}} M$, the other case being symmetrical. Assume $M_0(x) > M(x) = \max(M'_0(x), M'_1(x))$. This implies that $M'_0(x) = 0$ and $M'_1(x) < M_0(x)$. From $M'_0(x) = 0$, we deduce the existence of $z \in M_1 - M_0$ such that $z > x$ and for any $t \in M_0 - M_1$, $t \leq z$. This last part implies that $z \in S_1$, thus $M'_1(z) = M_1(z)$ and therefore $M(z) = \max(M'_0(z), M'_1(z)) = M'_1(z) = M_1(z) > M_1(z)$. $\square$

7.3 Finitary powerset over X

When $(X, \leq)$ is a QO, a natural quasi-ordering on $\mathcal{P}(X)$, the powerset over X, is the *Hoare quasi-ordering* (also called *domination quasi-ordering*), denoted $\sqsubseteq_{\mathcal{H}}$, and defined by

$$S \sqsubseteq_{\mathcal{H}} T \overset{\text{def}}{\Leftrightarrow} \forall x \in S : \exists y \in T : x \leq y.$$

A convenient characterization of this quasi-ordering is the following: $S \sqsubseteq_{\mathcal{H}} T$ iff $S \subseteq \downarrow_X T$.

Note that $(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ is in general not antisymmetric even when $(X, \leq)$ is. For example $S \equiv_{\mathcal{H}} \downarrow_X S$ for any $S \subseteq X$. Actually, $(\mathcal{P}(X)/\equiv_{\mathcal{H}}, \sqsubseteq_{\mathcal{H}})$ is order-isomorphic to $(Down(X), \subseteq)$. It is sometimes stated that $(X, \leq)$ is a WQO if and only if

$(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ is well-founded. With the above remark, this is exactly (WQO7) from the definition of WQO we gave in Chapter 2. In particular, $(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ needs not be a WQO, see Section 9.2 for more details. However, $(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{H}})$ is a WQO, where $\mathcal{P}_f(X)$ denotes the set of all *finite subsets* of X. Indeed, it is the quotient of $(X^*, \leq_{\mathrm{st}})$ (see Section 6.2) by the relation $\simeq$ defined by $\boldsymbol{u} \simeq \boldsymbol{v}$ iff $Supp(\boldsymbol{u}) = Supp(\boldsymbol{v})$, where $Supp(\boldsymbol{u})$ is the finite set of elements of X that appear in the finite sequence $\boldsymbol{u} \in X^*$. Moreover, $\simeq \circ \leq_{\mathrm{st}} = \leq_{\mathrm{st}} \circ \simeq$, and Section 4.2 applies. However, procedures for this WQO are rather simple to obtain directly, and more efficient than if relying on Section 4.2.

Since $(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{H}})$ can be obtained as a quotient of $(X^*, \leq_{\mathrm{st}})$ its ideals are exactly the closure under $\simeq$ of the ideals of $(X^*, \leq_{\mathrm{st}})$. The latter has been shown to be sets of the form $D_1^* \cdots D_k^*$ (cf. Section 6.2), and thus their closure under $\simeq$ is $(D_1 \cup \cdots \cup D_k)^*$. In terms of sets, this is exactly $\mathcal{P}_f(D_1 \cup \cdots \cup D_k)$, the set of finite subsets of $D_1 \cup \cdots \cup D_k$.

Lemma 7.3.1. *The ideals of $(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{H}})$ are exactly the sets of the form $\mathcal{P}_f(D)$, where D is a downward-closed subset of X.*

Proof. In complement of the sketch of proof that precedes the lemma, we present below a direct and simple proof:

$(\Leftarrow)$: $\emptyset \in \mathcal{P}_f(D)$, so $\mathcal{P}_f(D)$ is nonempty. It is downward-closed, since if $S \sqsubseteq_{\mathcal{H}} T \in \mathcal{P}_f(D)$, then $S \subseteq \downarrow_X T \subseteq \downarrow_X D = D$. It is directed, since if $S, T \in \mathcal{P}_f(D)$, then $S \cup T \in \mathcal{P}_f(D)$.

$(\Rightarrow)$: Let $\mathcal{J}$ be an ideal of $\mathcal{P}_f(X)$. Let $D = \bigcup \mathcal{J} = \bigcup_{S \in \mathcal{J}} S$. Then clearly $\mathcal{J} \subseteq \mathcal{P}_f(D)$. Since $\mathcal{J}$ is downward-closed under $\sqsubseteq_{\mathcal{H}}$, D is downward-closed under $\leq$ and $\{x\} \in \mathcal{J}$ for all $x \in D$. Since $\mathcal{J}$ is nonempty (it is an ideal), $\emptyset \in \mathcal{J}$. Finally, if $S, T \in \mathcal{J}$, then there is some $U \in \mathcal{J}$ such that $S, T \sqsubseteq_{\mathcal{H}} U$. Thus $S \cup T \sqsubseteq_{\mathcal{H}} U$, and $S \cup T \in \mathcal{J}$. Therefore, $\mathcal{J}$ has the empty set and singletons, and is closed under finite unions, and so is equal to $\mathcal{P}_f(D)$. $\square$

We now turn to ideal effectiveness. Assume we have encodings for X and $Idl(X)$. Finite sets of X are represented as the explicit list of the encoding of their elements. Once again, this corresponds to the representation suggested by Section 4.2: finite sets are equivalence classes of finite sequences.

Moreover, Lemma 7.3.1 suggests a very simple representation for ideals of $(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{H}})$: the ideal $\mathcal{P}_f(D)$ for some $D \in Down(X)$ is simply encoded with the encoding of D, which we know how to encode whenever we have an encoding for $Idl(X)$.

Theorem 7.3.2. *The Hoare Extension is a polynomial-time ideally effective construction.*

Proof. Let $(X, \leq)$ be an ideally effective WQO.

Given $S \in \mathcal{P}_f(X)$, the notation $\downarrow S$ could represent the downward-closure of S as a subset of X, or the downward-closure of $\{S\}$ as a subset of $\mathcal{P}_f(X)$. We therefore annotate every occurrence of a closure: $\downarrow_X S$ denotes the downward-closure of S as a subset of X, while $\downarrow_{\mathcal{H}} S$ denotes the downward-closure of S in $\mathcal{P}_f(X)$.

(OD) The quasi-ordering $S \sqsubseteq_{\mathcal{H}} T$ can be tested using at most $|S| \cdot |T|$ comparisons of elements of S and T.

(ID) Given $D_1, D_2 \in Down(X)$, checking $\mathcal{P}_f(D_1) \subseteq \mathcal{P}_f(D_2)$ boils down to checking $D_1 \subseteq D_2$.

(PI)**:** Given $S \in \mathcal{P}_f(X), \downarrow_{\mathcal{H}} S = \mathcal{P}_f(\downarrow_X S)$ (obvious when considering the alternative definition of $\sqsubseteq_{\mathcal{H}}$ given at the beginning of this chapter). Note that $\downarrow_X S = \bigcup_{x \in S} \downarrow x$ is computable.

(CF)**:** Given $S \in \mathcal{P}_f(X)$, the complement of $\uparrow_{\mathcal{H}} S$ is given by:

$$\begin{aligned} \mathcal{P}_f(X) \smallsetminus \uparrow_{\mathcal{H}} S &= \bigcup_{x \in S} \mathcal{P}_f(X) \smallsetminus \uparrow_{\mathcal{H}} \{x\} \\ &= \bigcup_{x \in S} \mathcal{P}_f(X \smallsetminus \uparrow x) \end{aligned}$$

(II)**:** To intersect ideals: $\mathcal{P}_f(D_1) \cap \mathcal{P}_f(D_2) = \mathcal{P}_f(D_1 \cap D_2)$.

(IF)**:** Filters may be intersected using $\uparrow S \cap \uparrow T = \uparrow(S \cup T)$.

(CI)**:** Given D a downward-closed set of X, $\mathcal{P}_f(X) \smallsetminus \mathcal{P}_f(D)$ consists of the set that contain at least one element not in D. That is:

$$\mathcal{P}_f(X) \smallsetminus \mathcal{P}_f(D) = \uparrow_{\mathcal{H}} \{\{x\} \mid x \in \min(X \smallsetminus D)\}$$

All of the above expressions trivially lead to (polynomial-time) procedures when $(X, \leq)$ is an (polynomial-time) ideally effective WQO. This proves that $(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{H}})$ is an (polynomial-time) ideally effective WQO when $(X, \leq)$ is. Moreover, the procedures above are obviously computable from a presentation of $(X, \leq)$. Besides, (XI) The whole set $\mathcal{P}_f(X)$ is an ideal since X is downward-closed, and (XF) the filter decomposition of $\mathcal{P}_f(X)$ is the empty set: $\uparrow_{\mathcal{H}} \emptyset$ (not to be confused with the empty filter decomposition, which denotes the empty upward-closed set of $\mathcal{P}_f(X)$).

Therefore, the Hoare extension is a polynomial-time ideally effective construction.

$\square$

Chapter 8

A Minimal Set of Axioms

8.1 Shortly Effective WQOs

The main notion of this part of the manuscript, Ideal Effectiveness (Definition 3.1.1), is defined through a list of requirements. A question that might occur to the reader, is whether some of the requirements are unnecessary, that is, whether some requirement is automatically fulfilled when the others are.

When we are only interested in computability, and not complexity, the answer is (surprisingly ?) yes. Let us formally prove this.

Definition 8.1.1. *A* short presentation *of a WQO $(X, \leq)$ is a list of:*

- *Representations for X and $Idl(X)$;*
- *Algorithms for the operations* (ID)*,* (PI)*,* (CF)*,* (II)*;*
- *The ideal decomposition of X.*

We say that a WQO equipped with some representation for X and $Idl(X)$ is shortly effective *if it has a short presentation.*

Note that a short presentation of $(X, \leq)$ is obtained from one of its presentation by dropping procedures to decide $\leq$ (OD), to intersect filters (IF), to complement ideals (CI) and by dropping the filter decomposition of X.

Theorem 8.1.2. *Given a short presentation of a WQO $(X, \leq)$, one can compute a presentation of $(X, \leq)$. In particular, a WQO is shortly effective if and only if it is ideally effective.*

Proof. We explain how to obtain the missing procedures:

(OD)**:** The quasi-ordering $\leq$ can be tested using (ID) and (PI): given $x, y \in X$, $x \leq y$ if and only if $\downarrow x \subseteq \downarrow y$.

(CI): We actually show a stronger statement, denoted CD, that complementing an arbitrary downward-closed set is computable. This strengthening is necessary for (IF).

Let D be an arbitrary downward-closed set. We compute $\complement D$ as follows:

1. Initialize $U := \emptyset$;
2. While $\complement U \not\subseteq D$ do
   (a) pick some $x \in \complement U \cap \complement D$;
   (b) set $U := U \cup \uparrow x$
3. Return U.

Every step of this high-level algorithm is computable. The complement $\complement U$ is computed using the procedure to complement filters composed with the procedure to intersect ideals: $\complement \bigcup_{i=1}^{n} \uparrow x_i = \bigcap_{i=1}^{n} \complement \uparrow x_i$ which is computed with (CF) and (II) (or with (XI) in case $n = 0$, i.e., for $U = \emptyset$). Then, inclusion $\complement U \subseteq D$ is tested with (ID). If this test fails, then we know $\complement U \cap \complement D$ is not empty, and thus we can enumerate elements $x \in X$ by brute force, and test membership in U and in D. Eventually, we will find some $x \in \complement U \cap \complement D$.

To prove partial correctness we use the following loop invariant: U is upward-closed and $U \subseteq \complement D$. The invariant holds at initialization and is preserved by the loop's body since if $\uparrow x$ is upward-closed and since $x \notin D$ and D downward-closed imply $\uparrow X \subseteq \complement D$. Thus when/if the loop terminates, one has both $\complement U \subseteq D$ and the invariant $U \subseteq \complement D$, i.e., $U = \complement D$.

Finally, the algorithm terminates since it builds a strictly increasing sequence of upward-closed sets, which must be finite by Eq. (WQO6).

(IF): This follows from (CF) and CD, by expressing intersection in terms of complement and union.

(XF): Using CD we can compute $\complement \emptyset$.

□

Remark 8.1.3 (On Theorem 8.1.2)**.** *The above methods are generic but in many cases there are simpler and more efficient ways of implementing* (CI)*,* (IF)*, etc. for a given WQO. This is why Definition 3.1.1 lists eight requirements instead of just four: we wanted to provide efficient procedures for all main operations in concrete cases. In particular, this theorem does not state that a polynomial-time presentation can be computed from a polynomial-time short presentation.*

As seen in the above proof, the fact that (CF), (II), (PI) and (XI) entail (CI) is non-trivial. The algorithm for CD computes an upward-closed set U from an oracle answering queries of the form "Is $U \cap I$ empty?" for ideals I. This is an instance of the Generalized Valk-Jantzen Lemma [37], an important tool for showing that some upward-closed sets are computable.

The existence of such a non-trivial redundancy in our definition led us to the question of whether there are other redundancies. The following proposition answers negatively.

Proposition 8.1.4. *A presentation of a WQO cannot be computed from a short presentation where one component (other than the encodings of X and $Idl(X)$ has been dropped. In other words, the requirements listed to define short effectiveness are minimal to capture the notion of ideal effectiveness.*

Proof. To prove this proposition, we prove the following statement:

(ID) There exists a WQO $(X, \leq)$ such that there exist algorithms to perform operations (PI), (CF) and (II), but ideal inclusion is undecidable.

(PI) There exists a WQO $(X, \leq)$ such that there exist algorithms to perform operations (ID), (CF) and (II), but function $x \mapsto \downarrow x$ is not computable.

(CF) There exists a WQO $(X, \leq)$ such that there exist algorithms to perform operations (ID), (PI) and (II), but there are no algorithm to complement filters.

(II) There exists a WQO $(X, \leq)$ such that there exist algorithms to perform operations (ID), (PI) and (CF), but there are no algorithm to intersect ideals.

(XI) There are no algorithm such that for all WQO $(X, \leq)$, given a list containing encodings for X and $Idl(X)$ as well as procedures for (ID), (PI), (CF) and (II), the algorithm computes the ideal decomposition of X.

Observe that the first four statements are stronger than the statement we need to prove. Indeed, there cannot be an algorithm that produces an algorithm for (ID) given the rest of a short presentation for any WQO $(X, \leq)$, since there is a specific WQO for which this algorithm does not even exist.

In the case of (XI) however, we cannot prove such a stronger statement since for each specific WQO, the ideal decomposition of the whole set is a constant, hence always computable.

Before we proceed to prove the five statements above, let us introduce the general idea, as well as some notations. In this remainder of this chapter, we build WQOs equipped with encodings for X and $Idl(X)$ for which some operation is not computable. To prove non-computability of an operation, we always reduce the halting problem for Turing machines. More precisely, from now on we fix an enumeration $(T_i)_{i \in \mathbb{N}}$ of Turing machines, such that there is a universal Turing Machine that can simulate T_i when given i as input. We use the following version of the halting problem: given i, decide whether T_i halts on the empty input (i.e. starting with an empty tape). This problem is well-known to be undecidable. Also define $t_i \in \mathbb{N} \cup \{\omega\}$ to be the halting time of machine T_i (on the empty input). For illustration purposes, we will assume that our enumeration is such that T_0 and T_1 halt ($t_0 < \omega$, $t_1 < \omega$) but not T_2 ($t_2 = \omega$).

All the WQOs given subsequently are built along the same idea: an element of the WQO intuitively corresponds to some execution step of some Turing machine T_i. Elements are ordered such that an element corresponding to step t of the execution of machine T_i is greater or equal to an element corresponding to step t' of the execution of machine T_j whenever $i > j$ or $i = j$ and $t' > t$. The simplest WQO satisfying these conditions is the ordinal ω^2 (equivalently, the lexicographic ordering over $\mathbb{N}^2$). WQOs presented in this chapter are often obtained by modifying the shape of ω^2 around elements corresponding to steps t_i (halting steps), so that some set-theoretic operation on the WQO is able to spot the difference: it is then possible to compute t_i using an oracle for this operation, which proves the operation to be non computable. This is often done by quotienting the natural ordering on the ordinal ω^2 by a well-chosen equivalence relation. Therefore, it is advised to read Section 3.2.3 and Section 4.2 before the remainder of this chapter.

In all our examples, it is crucial that despite being undecidable, the halting problem is semi-decidable. In particular, given a time t and a machine number i, one can decide whether $t \leq t_i$. It suffices to simulate the machine T_i for t steps: if it halted before, then $t_i < t$, otherwise $t \leq t_i$.

The remainder of the proof of Proposition 8.1.4 is split over the five next subsections, one for each of the five statements from the beginning of the proof. □

8.1.1 Ideal Inclusion (ID)

Let $X = \boldsymbol{\omega^2}$. According to the Cantor Normal form, elements of X can be written $\omega \cdot i + j$ for some $i, j \in \mathbb{N}$. We let $\leq$ denote the usual linear ordering on ordinals.

Define E as the smallest equivalence relation such that:

$$(\omega \cdot i + t)E(\omega \cdot i + t + 1) \text{ when } t \neq t_i$$

As in Section 4.2, this defines a quasi-ordering $\leq_E = \leq \circ E$ over X. Note that E is indeed compatible with $\leq$, that is to say $\leq_E = \leq \circ E = E \circ \leq$).

For a visual definition of E, see Fig. 8.1: an edge between two points means these two elements are equivalent with respect to $\leq_E$, otherwise, greater elements are drawn above smaller elements.

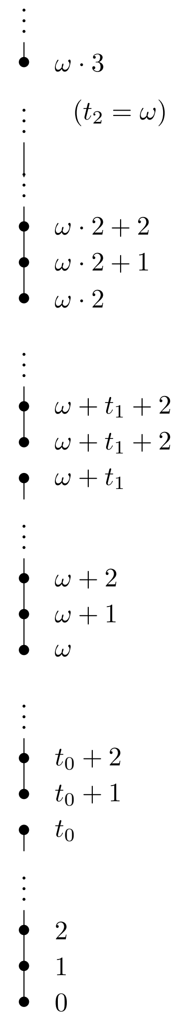

Figure 8.1: WQO for (ID), (CF) and (PI)

Here is an intuition behind the definition of the structure $(X, \leq_E)$. Associate to each Turing Machine T_i a copy of $\mathbb{N}$ where each natural number represents an execution time of the machine T_i. The WQO X is made of ω copies (one per Turing machine) on top of one another: this is a countable lexicographic sum, otherwise seen as the lexicographic product of ω by $\mathbb{N}$. In this QO, we interpret the ordinals $\omega \cdot i + t$ as the Turing machine T_i running for t steps. Then, the equivalence relation E is gluing some elements together in each copy of $\mathbb{N}$ so that each copy has only one or two equivalence class(es): the class of all elements smaller or equal to t_i, and if t_i is finite, the class of all elements strictly above. Therefore, the copy associated with T_i has two equivalence classes if and only if T_i halts (and one otherwise).

Below, we show that the WQO $(X, \leq_E)$ is almost shortly effective: (ID) cannot be decided, but (PI), (CF) and (II) are computable. This proves that in general, a procedure to decide ideal inclusion cannot be computed from procedures to compute (PI), (CF) and (II). The representations we use for elements of X is clear: elements of X are of the form $\omega \cdot i + t$. For ideals, we rely on the standard representation of ideals of a quotient defined in Section 4.2, that is ideals of $(X, \leq_E)$ are represented as ideals of $(\boldsymbol{\omega^2}, \leq)$, but denote their closure under E. Remember the ideals of $\boldsymbol{\omega^2}$ are exactly sets $\boldsymbol{\alpha} = \{\beta \mid \beta < \alpha\}$ for $\alpha < \omega^2 + 1$.

(OD): Let us mention that the quasi-ordering is decidable: $\omega \cdot i + t \leq_E \omega \cdot i' + t'$ iff $i < i'$; or $i = i'$ and $t, t' < t_i$; or $i = i'$ and $t_i \leq t, t'$. Conditions $t, t' < t_i$ and $t_i \leq t, t'$ are decidable by simulating T_i for $\max(t, t')$ steps.

(PI): Ideals of $(X, \leq_E)$ are encoded as ideals of $(\boldsymbol{\omega^2}, \leq)$ and thus $\downarrow_{\leq_E} x$ for $x \in X$ is encoded as $\downarrow_{\leq} x$ which is computable according to Section 3.2.3.

(CF): Given $\omega \cdot i + t \in X$, it is possible to test whether $t \leq t_i$. If $t \leq t_i$, then $\omega \cdot i + t$ is in the lower equivalence class of the i-th copy of $\mathbb{N}$ (the upper equivalence class might be reduced to $\emptyset$ if T_i does not halt). Therefore:

$$X \smallsetminus \uparrow_{\leq_E} \omega \cdot i + t = \boldsymbol{\omega \cdot i}$$

Otherwise, $t > t_i$, and t_i has been found (we run T_i for t steps, and T_i halted in less than t steps). Therefore we can output:

$$X \smallsetminus \uparrow_{\leq_E} \omega \cdot i + t = \boldsymbol{\omega \cdot i + t_i}$$

(II): Ideals are linearly quasi-ordered by inclusion, thus intersection consists in taking the minimum for inclusion. Although we cannot decide inclusion of ideals of $(X, \leq_E)$, observe that it suffices to always output the minimum for inclusion of ideals of $(\boldsymbol{\omega^2}, \leq)$. In other words, given $I, J \in \mathit{Idl}(\boldsymbol{\omega^2}, \leq)$ and denoting $\overline{S}$ the closure under E of some $S \subseteq X$, we have:

$$\overline{I} \cap \overline{J} = \overline{I \cap J}$$

Finally, observe that machine T_i does not halt if and only if $\overline{\boldsymbol{\omega \cdot i + 1}} = \overline{\boldsymbol{\omega \cdot (i + 1)}}$. Therefore, there can be no algorithm to decide ideal inclusion.

8.1.2 Complementing Filters (CF)

The WQO for which we cannot compute (CF), but for which we can decide (ID) and compute (PI) and (II) is the same WQO $(X, \leq_E)$ as before ! Only, we change our representation of its ideals. This (surprising) result shows the importance of the chosen encoding of sets when dealing with computability questions.

As observed in the previous subsection, each copy of the natural numbers has only one or two equivalence classes for $\equiv_E = \leq_E \cap \geq_E$. Therefore, the only limit ideal of $(X, \leq_E)$ is the whole set X itself. All other ideals are principal. We thus encode ideals of $(X, \leq_E)$ using encodings of elements of X, plus an extra symbol for the ideal X itself.

With these representations of X and $\mathit{Idl}(X)$, we now show that (ID), (PI) and (II) are computable.

(OD): Note that we have not changed our representation of X, and thus the quasi-ordering $\leq_E$ is still decidable.

(ID): Inclusion is now decidable since it is essentially the same as the quasi-ordering, with the extra element ω^2 which is greater than any other.

(PI): With our representation of ideals, the function $x \mapsto \downarrow x$ is the identity function.

(II): Ideals are linearly quasi-ordered by inclusion, and thus, intersection consists of taking the minimum for inclusion, which is now decidable.

However, assume we have an algorithm to complement filters: on input $\uparrow(\omega\cdot(i+1))$ for some $i \in \mathbb{N}$, it returns some $\downarrow(\omega \cdot i + t)$ For this algorithm to be correct, it must be the case that $\downarrow_{\leq_E}(\omega \cdot i + t) = \downarrow_{\leq_E}(\omega \cdot i + t')$ for all $t' \geq t$, i.e. $\omega \cdot i + t$ and $\omega \cdot i + t'$ are equivalent. Thus, $t_i < \omega$ if and only if $t_i < t$, and the halting problem could be decided by bounded simulation.

8.1.3 Principal Ideals (PI)

For (PI), we again consider the same WQO $(X, \leq_E)$, taking yet another representation of its ideals. If the ordinals α and β are E-equivalent, then $\downarrow\alpha$ and $\downarrow\beta$ are two representations of the same ordinal. We thus make representations of ideals unique by allowing only two types of ideals:

- the limit ordinals of $\boldsymbol{\omega^2+1}$, that is $\boldsymbol{\omega^2} = X$ and $\boldsymbol{\omega\cdot i} = \{\alpha \mid \alpha < \omega \cdot i\}$ for $i \in \mathbb{N}$;
- and the successor ordinals of the form $\boldsymbol{\omega\cdot i + t_i + 1}$ for $i \in \mathbb{N}$.

The set of ideals is still recursive, since given i and t, it is possible to check whether $t = t_i + 1$. Ideal inclusion corresponds to a sub-order of the natural ordering on ordinals, and is thus decidable. The inclusion on ideals being linear, intersecting ideals again corresponds to taking the minimum, and hence is computable.

However, we now have a procedure for (CF):

- $X \smallsetminus \uparrow(\omega \cdot i + t) = \boldsymbol{\omega\cdot i}$ if $t \leq t_i$.
- $X \smallsetminus \uparrow(\omega \cdot i + t) = \boldsymbol{\omega\cdot i + t_i + 1}$ if $t > t_i$. Note that if $t > t_i$, then t_i has been found, and thus it can be output.

But there are no procedures for (PI) anymore: if there were, one could compute $\downarrow\omega \cdot i$ that should be mapped to $\boldsymbol{\omega\cdot i + t_i + 1}$ if T_i halts, and to $\boldsymbol{\omega\cdot(i+1)}$ otherwise.

8.1.4 Intersecting Ideals (II)

Let $Y = (\mathbb{N} \sqcup \mathbb{N}) + (\mathbf{1} \sqcup \mathbf{1})$ quasi-ordered with the sum quasi-orderings introduced in Chapter 5. The set Y consists of two copies of $\mathbb{N}$, augmented with two top elements that will be denoted $\langle 1, \omega\rangle$ and $\langle 2, \omega\rangle$, that are incomparable with each other, but greater than any other element of Y. In particular, note that for any $a \in \{1, 2\}$ and $n \in \mathbb{N}$,

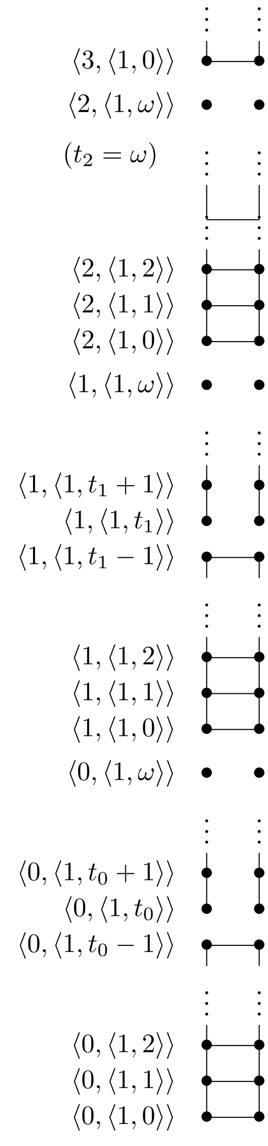

Figure 8.2: WQO for (II)

$\langle i, \langle a, \omega\rangle\rangle > \langle i, \langle 3-a, n\rangle\rangle$. In other words, Y is not quasi-ordered as $\boldsymbol{\omega+1} \sqcup \boldsymbol{\omega+1}$, although it has the same support.

Define $X = \mathbb{N} \times Y$ equipped with the lexicographic quasi-ordering $\leq_{\text{lex}}$ defined in Section 5.4. Intuitively, X is the WQO obtained by putting ω copies of Y on top of each other. Elements of X are of the form $\langle i, \langle a, n\rangle\rangle$ where $i \in \mathbb{N}$ designates the copy of Y (the floor of the tower), $a \in \{1, 2\}$ designates the disjoint copy (left or right) and $n \in (\boldsymbol{\omega+1})$. Due to space constraints, only the left copy is labeled on Fig. 8.2). Once again, we extend the quasi-ordering by an equivalence relation E defined by :

- $\langle i, (a, n)\rangle E \langle i, (b, m)\rangle$ for $i \in \mathbb{N}$, $a, b \in \{1, 2\}$ and $n, m \in \mathbb{N}$ and $n, m < t_i$.
- $\langle i, (a, n)\rangle E \langle i, (a, m)\rangle$ for $i \in \mathbb{N}$, $a \in \{1, 2\}$ and $n, m \in \mathbb{N}$ and $n, m \geq t_i$.

Note that each copy of Y has either 3 or 5 equivalence classes (depending on whether T_i halts).

The representation of the elements of X is the one described above. For ideals, we again rely on the fact that the equivalence relation E is "gluing" many elements, and thus there are no infinite strictly increasing sequence of elements within a copy of Y. Thus, the only limit ideal is X itself. All other ideals are principal, hence represented by $\downarrow x$ for $x \in X$.

We now show that for these representations, the operations (ID), (PI) and (CF) are computable, but not (II).

(OD)**:** The quasi-ordering is decidable, as in previous cases by bounded simulations of Turing machines.

(ID)**:** Inclusion is then trivially decidable: it is the same as the quasi-ordering (plus the maximal element X).

(PI)**:** Computing principal ideals is again the identity function.

(CF)**:** To complement filters:

$\complement\uparrow\langle 0, \langle a, n\rangle\rangle = \emptyset$ when $n \in \mathbb{N}$ and $n < t_0$ and $a \in \{1, 2\}$.

$\complement\uparrow\langle i+1, \langle a, n\rangle\rangle = \downarrow\langle i, \langle 1, \omega\rangle\rangle \cup \downarrow\langle i, \langle 2, \omega\rangle\rangle$ when $n \in \mathbb{N}$ and $n \leq t_{i+1}$ and $a \in \{1, 2\}$.

$\complement\uparrow\langle i, \langle a, n\rangle\rangle = \downarrow\langle i, \langle 3-a, n\rangle\rangle$ when $\omega \geq n \geq t_i$ and $a \in \{1, 2\}$.

Finally, observe that $\downarrow\langle i, \langle 1, \omega\rangle\rangle \cap \downarrow\langle i, \langle 2, \omega\rangle\rangle$ is an ideal if and only if T_i does not halt. Thus, if intersections were computable, the size of the ideal decomposition of the result would decide the halting problem.

8.1.5 Ideal Decomposition of X (XI)

As mentioned at the beginning of this subsection, the result for (XI) is a little weaker, as for a given X, its ideal decomposition is a constant, hence computable. Thus we here provide an infinite collection of WQOs $(X_i, \leq_i)_{i\in\mathbb{N}}$ such that one cannot compute

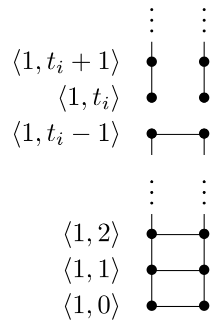

Figure 8.3: X_i when T_i halts. $(X_i, \leq_i \circ E_i)$ is isomorphic to $\mathbf{1} \oplus (\mathbf{1} \sqcup \mathbf{1})$.

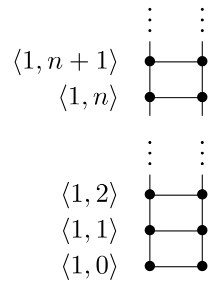

Figure 8.4: X_i when T_i does not halt. $(X_i, \leq_i \circ E_i)$ is isomorphic to $\mathbf{1}$.

the ideal decomposition of X_i given $i \in \mathbb{N}$, while (PI), (CF) and (II) are computable for each X_i.

Define $X_i = \mathbb{N} \sqcup \mathbb{N}$ with the natural ordering extended with relation E_i defined by (cf. Figures 8.3 and 8.4):

- $\langle a, n\rangle E_i \langle b, m\rangle$ for $a, b \in \{1, 2\}$ and $n, m < t_i$.
- $\langle a, n\rangle E_i \langle a, m\rangle$ for $a \in \{1, 2\}$ and $n, m \geq t_i$.

First of all, for any $i \in \mathbb{N}$, $(X_i, \leq_i)$ is ideally effective, where the representation for X is the usual one for disjoint sum, and we represent ideals as elements, since they are all principal ($X_i / \equiv_i$ is a finite WQO for every i).

(OD)**:** As in the other cases, the quasi-ordering is decidable by bounded simulations.

(ID)**:** Ideal inclusion is then the same as the quasi-ordering on X_i.

(PI)**:** The ideal $\downarrow x$ has the same representation as x, for $x \in X_i$.

(CF)**:** Complements of filters are computed using:

$$\begin{aligned} \complement \uparrow\langle a, n\rangle &= \emptyset && \text{if } n < t_i \\ \complement \uparrow\langle a, n\rangle &= \downarrow\langle 3 - a, t_i\rangle && \text{if } n \geq t_i \end{aligned}$$

(II)**:** Ideal intersections are computed using:

$$\downarrow\langle a, n\rangle \cap \downarrow\langle a, m\rangle = \downarrow\langle a, \min(n, m)\rangle;$$
$$\downarrow\langle a, n\rangle \cap \downarrow\langle 3 - a, m\rangle = \begin{cases} \downarrow\langle 1, \min(n, m)\rangle & \text{when } \min(n, m) < t_i \\ \downarrow\langle 1, 0\rangle & \text{otherwise.} \end{cases}$$

However, the function that maps $i \in \mathbb{N}$ to the ideal decomposition of X_i is not computable, since otherwise it would decide the halting problem. Indeed, X_i is an ideal if and only if T_i does not halt.

8.2 Effective Extensions

Given $(X, \leq)$ an ideally effective WQO and $\leq'$ an extension of $\leq$, we have given in Theorem 4.1.2 sufficient conditions for $(X, \leq')$ to be ideally effective. In this section, we prove the following stronger theorem:

Theorem 8.2.1. *Let $(X, \leq)$ be an ideally effective WQO and $\leq'$ an extension of $\leq$. Then, $(X, \leq')$ is ideally effective (for the encodings of X and $Idl(X, \leq')$ described in Section 4.1), whenever the following function is computable:*

$$\begin{aligned} \mathcal{C}l_{\mathrm{I}} \quad : Idl(X, \leq) \quad &\to Down(X, \leq) \\ I \quad &\mapsto {\downarrow_{\leq'}} I \end{aligned}$$

Moreover, under these assumptions, a presentation of $(X, \leq')$ can be computed from a presentation of $(X, \leq)$ and algorithms realizing $\mathcal{C}l_{\mathrm{I}}$.

Proof. It suffices to show that, under these assumptions, we can compute function $\mathcal{C}l_{\mathrm{F}}$:

$$\begin{aligned} \mathcal{C}l_{\mathrm{F}} \quad : (X, \leq) \quad &\to Up(X, \leq) \\ x \quad &\mapsto {\uparrow_{\leq'}} x \end{aligned}$$

Indeed, if $\mathcal{C}l_{\mathrm{F}}$ is computable, we can conclude with Theorem 4.1.2. The idea to compute $\mathcal{C}l_{\mathrm{F}}$ using only $\mathcal{C}l_{\mathrm{I}}$ and operations in $(X, \leq)$ is quite similar to the algorithm to compute CD using the other operations presented in the proof of Theorem 8.1.2. In particular, our algorithm relies on brute force enumeration of elements of X, and we will not get a complexity upper bound for $\mathcal{C}l_{\mathrm{F}}$, even if $\mathcal{C}l_{\mathrm{I}}$ is polynomial-time. This is why we dropped the conclusion about polynomial-time presentation in the formulation of the theorem above (compared to Theorem 4.1.2).

Let $x \in X$. We can compute ${\uparrow_{\leq'}} x$ as follows:

1. Initialize $U := {\uparrow_{\leq}} x$
2. While $\mathcal{C}l_{\mathrm{F}}(x) \not\subseteq U$ do:
   (a) find $y \in \mathcal{C}l_{\mathrm{F}}(x) \setminus U$,
   (b) set $U := U \cup {\uparrow_{\leq}} y$
3. Return U.

Every step of this high-level algorithm is computable. Step 1 can be performed using (PI) for $(X, \leq)$. To test the conditional part of the while loop, we use the following equivalence: for any $x \in X$ and $U \in Up(X, \leq)$,

$$\begin{aligned} \mathcal{C}l_{\mathrm{F}}(x) \not\subseteq U &\iff {\uparrow_{\leq'}} x \not\subseteq U \\ &\iff X \setminus {\uparrow_{\leq'}} x \not\supseteq X \setminus U \\ &\iff X \setminus {\uparrow_{\leq'}} x \not\supseteq \mathcal{C}l_{\mathrm{I}}(X \setminus U) \\ &\iff {\uparrow_{\leq'}} x \not\subseteq X \setminus \mathcal{C}l_{\mathrm{I}}(X \setminus U) \end{aligned}$$

Observe that the implication $X \smallsetminus \uparrow_{\leq'} x \not\supseteq \mathcal{C}l_{\mathrm{I}}(X \smallsetminus U) \Rightarrow X \smallsetminus \uparrow_{\leq'} x \not\supseteq X \smallsetminus U$ holds because $X \smallsetminus \uparrow_{\leq'}$ is already downward-closed for $\leq'$. For a downward-closed set D, it is equivalent to contain an arbitrary subset S or its downward-closure $\downarrow S$.

Now, we can test this last condition $\uparrow_{\leq'} x \not\subseteq X \smallsetminus \mathcal{C}l_{\mathrm{I}}(X \smallsetminus U)$ by computing a finite basis of the upward-closed set (for $\leq$) $X \smallsetminus \mathcal{C}l_{\mathrm{I}}(X \smallsetminus U) = \bigcup_{i \in I} \uparrow x_i$ and testing whether $x \geq' x_i$ for some $i \in I$. Computing such a finite basis is possible since $U \in Up(X, \leq)$, on which we can perform complements ((CF) and (II)), then we can compute function $\mathcal{C}l_{\mathrm{I}}$ which outputs a downward-closed set of $(X, \leq)$,on which we know how to compute complements ((CI) and (IF)). Finally, the ordering $\leq'$ is decidable using $x \leq' y \iff x \in \mathcal{C}l_{\mathrm{I}}(\downarrow_{\leq} y)$.

Therefore, if entering the while loop, it means that $\mathcal{C}l_{\mathrm{F}}(x) \not\subseteq U$, and there exists some $y \in X$ such that $y \in \mathcal{C}l_{\mathrm{F}}(x) \smallsetminus U$. To find such an element, it suffices to enumerate elements of X and for each test whether it is greater than x for $\leq'$ (possible since $\leq'$ is decidable) and if it belongs to U.

Besides, observe that since at step 2b we know that $y \notin U$, the sequence of upward-closed sets built by the while loop is strictly increasing, therefore finite (Eq. (WQO6)). Thus, the program terminates.

To prove correction, observe that $U \subseteq \mathcal{C}l_{\mathrm{F}}(x)$ is an invariant of the program, and whenever the program terminates (and it will), the conditional of the while loop is false, that is $\mathcal{C}l_{\mathrm{F}}(x) \subseteq U$. Therefore, the return value U is indeed the upward-closed set of $\mathcal{C}l_{\mathrm{F}}(x) \in Up(X, \leq)$.

□

We have just proved that function $\mathcal{C}l_{\mathrm{F}}$ can be computed from function $\mathcal{C}l_{\mathrm{I}}$. The asymmetry between upward- and downward-closed sets of a WQO strikes again, and we can show that the converse is not true: we cannot compute $\mathcal{C}l_{\mathrm{I}}$ from $\mathcal{C}l_{\mathrm{F}}$. Indeed, consider again the WQO $(X, \leq_E)$ from Section 8.1.1. It is obtained as a quotient of the ordinal $(\boldsymbol{\omega^2}, \leq)$, which is ideally effective. Below, we show that function $\mathcal{C}l_{\mathrm{F}} : \boldsymbol{\omega^2} \to Up(\boldsymbol{\omega^2}, \leq)$ is computable. Of course $\mathcal{C}l_{\mathrm{I}}$ cannot be computable, otherwise $(X, \leq_E)$ would be ideally effective for the representations we used in Section 8.1.1.

Remember that given $x \in \boldsymbol{\omega^2}$, $\mathcal{C}l_{\mathrm{F}}(x)$ is the filter decomposition of $\uparrow_{\leq_E} \overline{x}$, where $\overline{x}$ is the equivalence class under E of x. Here, since the ordering $\leq$ is linearly ordered, $\overline{x}$ has a unique minimal element. Let $x = \omega \cdot i + t \in \boldsymbol{\omega^2}$. If $t \leq t_i$ then $\overline{x} = \{\omega \cdot i + j \mid 0 \leq j \leq t_i\}$, in which case $\mathcal{C}l_{\mathrm{F}}(x) = \uparrow_{\leq_E} \omega \cdot i + t = \uparrow_{\leq} \omega \cdot i$. Otherwise, when $t > t_i$, $\overline{x} = \{\omega \cdot i + j \mid j > t_i\}$, and $\mathcal{C}l_{\mathrm{F}}(x) = \uparrow_{\leq_E} \omega \cdot i + t = \uparrow_{\leq} \omega \cdot i + t_i + 1$. Therefore, $\mathcal{C}l_{\mathrm{F}}$ is computable.

Let us also mention that removing any assumption in Theorem 8.2.1 breaks the theorem. In particular, the situation above provides an example of an ideally effective WQO $(X, \leq)$ and a decidable relation E such that $(X, \leq \circ E)$ is not ideally effective. This legitimate the introduction of the function $\mathcal{C}l_{\mathrm{I}}$.

On the other hand, function $\mathcal{C}l_{\mathrm{I}}$ is not a necessary condition in the following sense: there exists an ideally effective WQO $(X, \leq)$ such that the function $\mathcal{C}l_{\mathrm{I}}$ associated to the extension from $(X^{\circledast}, \leq_{\mathrm{emb}})$ to $(X^{\circledast}, \leq_{\mathrm{ms}})$ is not computable (see Section 8.3.2), but the WQO $(X^{\circledast}, \leq_{\mathrm{ms}})$ is still ideally effective. However, note that $(X^{\circledast}, \leq_{\mathrm{ms}})$ is ideally effective for another representation of ideals than the one fixed in Section 4.1. Otherwise, $\mathcal{C}l_{\mathrm{I}}$ is really necessary: let $(X, \leq)$ be an ideally effective WQO and $\leq'$ an extension of $\leq$. Assume $(X, \leq')$ is ideally effective when representing its ideals as ideals of $(X, \leq)$. Then given $I \in Idl(X, \leq)$, we can enumerate $D \in Down(X)$ and check whether $D = \mathcal{C}l_{\mathrm{I}}(I)$ as follows: with (ID) for $\leq'$ we can check that $\downarrow_{\leq'} I = \downarrow_{\leq'} D$, and with (CI) for $\leq$ and $\leq'$ we can check that $X \smallsetminus D = X \smallsetminus (\downarrow_{\leq'} I)$. If it is the case, it means $X \smallsetminus D$ is upward-closed for $\leq'$, and thus D is downward-closed for $\leq'$.

Last remark: as in the case of Theorem 8.1.2, we have presented only Theorem 4.1.2 in Section 4.1 (and not the version above without the function $\mathcal{C}l_{\mathrm{F}}$) for complexity reasons. In practical cases, it is important to have an efficient version of $\mathcal{C}l_{\mathrm{F}}$.

8.3 Deciding whether an Ideal is Principal

We prove that in general, one cannot decide whether an ideal of an ideally effective WQO is principal. The counter-example is again built following the same idea. Define $X = \omega^2$, and extend the natural ordering so that for any given $i \in \mathbb{N}$, elements $\omega \cdot i + t$ for $t \geq t_i$ form an equivalence class (Fig. 8.5). We show that $(X, \leq_E)$ is ideally effective using Section 4.2.

- $\mathcal{C}l_{\mathrm{I}}(\boldsymbol{\omega \cdot i + j}) = \boldsymbol{\omega \cdot (i + 1)}$ if $j > t_i$,
- $\mathcal{C}l_{\mathrm{I}}(\boldsymbol{\omega \cdot i + j}) = \boldsymbol{\omega \cdot i + j}$ otherwise.
- $\mathcal{C}l_{\mathrm{F}}(\omega \cdot i + j) = \omega \cdot i + t_i$ if $j \geq t_i$,
- $\mathcal{C}l_{\mathrm{F}}(\omega \cdot i + j) = \omega \cdot i + j$ otherwise.

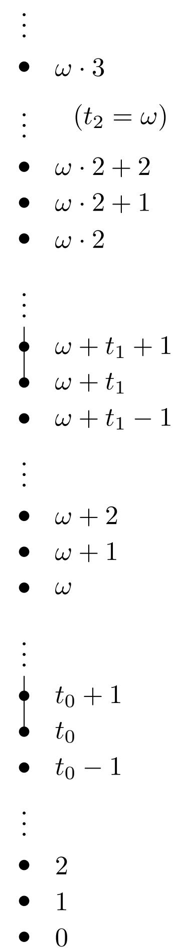

Figure 8.5: WQO for Subsection 8.3

The functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ being computable, $(X, \leq_E)$ is ideally effective. However, $\boldsymbol{\omega \cdot (i + 1)}$ is a principal ideal if and only if T_i halts, hence, one cannot decide whether an ideal is principal.

This is yet another independence result: one could add the axiom "principality of ideals is decidable" to our definition of ideal effectiveness, and the axiomatic system would still be minimal (no axiom is implied by the others). Note that to actually prove this statement, one should also check that the other axioms remain independent in the presence of the new one. This is the case: for every WQOs considered in the proof of Proposition 8.1.4, it is decidable whether a given ideal is principal.

Nonetheless, we decided not to include this as an axiom: a priori, deciding whether an ideal is principal does not seem related to our original motivation: handling closed subsets. It turned out to be sometimes related, for instance in Section 5.4 where it is crucial to be able to decide whether an ideal is principal to prove ideal effectiveness of the lexicographic quasi-ordering. This is further discussed in Section 8.3.1. Another case where the inability to test whether an ideal is principal affected our work is discussed in Section 8.3.2. Because of these two examples mostly, we considered adding this requirement to our definition. However, the WQO defined above is obtained as a quotient of an ideally effective WQO, that in addition satisfies the extra assumptions of Section 4.1. This proves that the ability to decide ideal principality is not preserved under quotient. We favored the generality of our results on quotient over the specific lexicographic quasi-ordering, and decided to exclude this axiom from Definition 3.1.1.

8.3.1 The Lexicographic Quasi-Ordering Is Not Ideally Effective

In this section, we prove that the lexicographic quasi-ordering introduced in Section 5.4 is not ideally effective in general. More precisely, in Section 5.4 we proved that $(X_1 \times X_2, \leq_{\text{lex}})$ is ideally effective provided that $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are ideally effective WQOs, and that we can decide whether an ideal of X_1 is principal. Subsequently, we justify the necessity of this last assumption.

Let $(X_1, \leq_1)$ be the WQO defined in the previous section, in particular it is undecidable given $I \in \mathit{Idl}(X_1)$ whether I is principal. Let X_2 be the finite set $\{a, b\}$ ordered with equality. What matters most here is that X_2 is not an ideal.

Lemma 8.3.1. *Given $I \in \mathit{Idl}(X_1)$, the downward-closed set $I \times X_2$ is an ideal of $(X_1 \times X_2, \leq_{\text{lex}})$ if and only if I is not principal.*

Proof. ($\Rightarrow$) By contraposition, if $I = \downarrow x$ is a principal ideal for some $x \in X_1$, then the elements $\langle x, a\rangle$ and $\langle x, b\rangle$ have no common upper bound in $I \times X_2$.

($\Leftarrow$) Let $\langle x, c\rangle, \langle y, d\rangle \in I \times X_2$. Since I is not principal (but directed), there exists $z \in I$ such that z is *strictly* greater than both x and y. Then $\langle z, a\rangle \in I \times X_2$, and is greater for $\leq_{\text{lex}}$ than both $\langle x, c\rangle, \langle y, d\rangle$. $\square$

Theorem 8.3.2. *Let $(X_1, \leq_1)$ and $(X_2, =)$ be the two WQOs defined above. We represent elements of $X_1 \times X_2$ as pairs of encodings of X_1 and X_2. Then, for any representation of ideals of $(X_1 \times X_2, \leq_{\text{lex}})$, the lexicographic product $(X_1 \times X_2, \leq_{\text{lex}})$ is not ideally effective.*

Proof. Fix some representation of ideals of $(X_1 \times X_2, \leq_{\text{lex}})$.

Recall that both $(X_1, \leq_1)$ and $(X_2, =)$ are ideally effective. Therefore, given $I \in \mathit{Idl}(X_1)$, we can compute its complement $U \stackrel{\text{def}}{=} X_1 \smallsetminus I$. We can then compute $V \stackrel{\text{def}}{=} U \times \{a\} \cup U \times \{b\} \in \mathit{Up}(X_1 \times X_2)$. Indeed, if $U = \bigcup_{i \in I} \uparrow_1 x_i$, then $V = \bigcup_{i \in I} \uparrow_{\text{lex}} \langle x_i, a\rangle \cup \uparrow_{\text{lex}} \langle x_i, b\rangle$. Assuming $(X_1 \times X_2, \leq_{\text{lex}})$ is ideally effective, we can compute $(X_1 \times X_2) \smallsetminus V = I \times X_2$. In particular, we can decide whether $I \times X_2$ is an ideal. According to the previous lemma, this is impossible. $\square$

8.3.2 The Domination Ordering on Multisets Does Not Effectively Extend the Embedding Quasi-Ordering

Let $(X, \leq)$ be a WPO. Recall from Section 7.2 the definition of its finite multiset extension under the domination ordering $(X^{\circledast}, \leq_{\text{ms}})$. Also, remember that $\leq_{\text{ms}}$ is an extension of $\leq_{\text{emb}}$, where $(X^{\circledast}, \leq_{\text{emb}}$ is the finite multiset extension under the embedding ordering, shown ideally effective in Section 7.1.

Proving $(X^{\circledast}, \leq_{\text{ms}})$ to be ideally effective following the approach of Section 4.1 would require to show that the functions $\mathcal{C}l_{\text{I}}$ and $\mathcal{C}l_{\text{F}}$ associated to this extension are computable. Subsequently, we show that this is not the case in general. This justifies that ideal effectiveness was shown from scratch in Section 7.2, with a better encoding of ideals of $(X^{\circledast}, \leq_{\text{ms}})$ than the one from Section 4.1.

Recall that ideals of $(X^{\circledast}, \leq_{\text{emb}})$ are elements $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$ for $\boldsymbol{B} \in (\mathit{Idl}(X)^{\circledast}$ and $D \in \mathit{Down}(X)$, where $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} = \{M \mid M \smallsetminus D \in_{\text{emb}} \boldsymbol{B}\}$. Observe that when characterizing $\downarrow_{\mathrm{ms}}[\downarrow_\in \boldsymbol{B} \oplus D^\circledast]$ in Proposition 7.2.2, it was crucial to distinguish principal ideals from limit ideals. Suppose $\boldsymbol{B} = \{\!| \downarrow x_1, \ldots, \downarrow x_n, I_1, \ldots, I_m |\!\}$ where $I_1, \ldots, I_m$ are limit ordinals, then it was proved in Proposition 7.2.2 that $\downarrow_{\mathrm{ms}}[\downarrow_\in \boldsymbol{B} \oplus D^\circledast] = \downarrow_{\mathrm{ms}}\{\!| x_1 \cdots x_n |\!\} + (D \cup I_1 \cup \cdots \cup I_m)^\circledast$.

Applying this to the WQO X from Section 8.3:

$$\mathcal{C}l_{\mathrm{I}}(\downarrow_\in \{\!| \boldsymbol{\omega \cdot (i+1)} |\!\}) = \begin{cases} \downarrow_{\mathrm{ms}}\{\!| \omega \cdot i + t_i + 1 |\!\} & \text{if } T_i \text{ halts} \\ [\boldsymbol{\omega \cdot (i+1)}]^\circledast & \text{otherwise} \end{cases}$$
$$= \begin{cases} \downarrow_\in \{\!| \boldsymbol{\omega \cdot (i+1)} |\!\} \cup [\boldsymbol{\omega \cdot i + t_i}]^\circledast & \text{if } T_i \text{ halts} \\ [\boldsymbol{\omega \cdot (i+1)}]^\circledast & \text{otherwise} \end{cases}$$

8.4 Deciding whether an Ideal is Adherent

Finally, we show that adherence cannot be decided in general. Remember from Section 4.3 that given $Y \subseteq X$, an ideal $I \in \mathit{Idl}(X)$ is adherent to Y if and only if $\downarrow_X(I \cap Y) = I$.

Below, we define a WQO $(X, \leq)$ and a recursive subset $Y \subseteq X$ such that deciding whether a given ideal of X is adherent to Y is undecidable. Moreover, we show that this WQO is not ideally effective, proving that some extra assumptions are necessary for induced WQOs to be ideally effective (however, this does not prove that the extra assumptions made in Section 4.3 are necessary).

Define $X = \omega^2$ ordered by the natural ordering. $(X, \leq)$ is ideally effective since it is an ordinal, as proved in Section 3.2.3. Consider the subset $Y = \{\omega \cdot i + t \mid i, t \in \mathbb{N}, t \leq t_i\}$. This is a recursive subset of X Observe that the ideal $\boldsymbol{\omega \cdot (i+1)}$ is adherent to Y if and only if T_i halts. Therefore, adherence to Y is undecidable. Moreover, $Y \smallsetminus \uparrow_Y \omega \cdot (i+1)$ gives the halting time t_i of T_i, hence $(Y, \leq)$ is not ideally effective.

Chapter 9

Toward Ideally Effective BQOs

We motivate our introduction of *Better Quasi-Orderings* with yet another construction: that of taking infinite sequences over a WQO $(X, \leq)$. By infinite, we mean sequences of length ω.

9.1 Infinite Sequences of WQOs

Let $(X, \leq)$ be a QO. We consider the QO $(X^\omega, \leq_\omega)$ where X^ω denotes the set of infinite sequences over X, and $\leq_\omega$ denotes the embedding relation introduced in Chapter 2 restricted to X^ω. Formally, if $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ and $\boldsymbol{v} = (v_i)_{i\in\mathbb{N}}$, we have:

$$\boldsymbol{u} \leq_\omega \boldsymbol{v} \overset{\text{def}}{\Leftrightarrow} \text{There exists a strictly increasing mapping } f : \mathbb{N} \to \mathbb{N}.\ \forall i \in \mathbb{N}.\ u_i \leq v_{f(i)}$$

If $|X| > 1$, the set X^ω has uncountably many elements, and thus we cannot represent all its elements algorithmically. However, if $(X, \leq)$ is a WQO, then $(X^\omega, \leq_\omega)$ has countably many equivalence classes for $\equiv_\omega$. This relies on the following characterization of $\leq_\omega$ over X^ω.

For the remainder of this section, let $(X, \leq)$ designates a WQO.

Proposition 9.1.1. *Given $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}} \in X^\omega$, define the* tail *of $\boldsymbol{u}$ as $D(\boldsymbol{u}) = \bigcap_{i\in\mathbb{N}} \bigcup_{j\geq i} \downarrow u_j$, and the* head *of $\boldsymbol{u}$ as the finite prefix $h(\boldsymbol{u}) = u_0 \cdots u_j$ of $\boldsymbol{u}$, where j is the smallest natural number such that $\forall k > j.\ u_k \in D(\boldsymbol{u})$.*

Then, for all $\boldsymbol{u} \in X^\omega$: $\downarrow \boldsymbol{u} = (\downarrow_* h(\boldsymbol{u})) \cdot D(\boldsymbol{u})^\omega$.

Corollary 9.1.2. *Given $\boldsymbol{u}, \boldsymbol{v} \in X^\omega$,*

$$\boldsymbol{u} \leq_\omega \boldsymbol{v} \Leftrightarrow h(\boldsymbol{u}) \in (\downarrow h(\boldsymbol{v})) \cdot D(\boldsymbol{v})^* \wedge D(\boldsymbol{u}) \subseteq D(\boldsymbol{v})$$

Proof. Of Proposition 9.1.1 and Corollary 9.1.2.
Let $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}} \in X^\omega$. Intuitively, $D(\boldsymbol{u})$ consists of all elements of X that will be covered infinitely often in $\boldsymbol{u}$. The sequence $D_i = \bigcup_{j\geq i}(\downarrow u_j)$ is a decreasing sequence of downward-closed subsets of $(X, \leq)$. Thus since $(X, \leq)$ is WQO, $(D_i)_{i\in\mathbb{N}}$ stabilizes to some element D_{i_0}, and its limit is $D(\boldsymbol{u}) = D_{i_0} \neq \emptyset$. Hence, $h(\boldsymbol{u})$ is well defined.

Let $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}, \boldsymbol{v} = (v_i)_{i\in\mathbb{N}} \in X^\omega$. We show the following:

$$\boldsymbol{u} \in \downarrow \boldsymbol{v} \iff \boldsymbol{u} \in (\downarrow h(\boldsymbol{v})) \cdot D(\boldsymbol{v})^\omega.$$

($\Rightarrow$) Assume $\boldsymbol{u} \leq_\omega \boldsymbol{v}$ and let $f : \mathbb{N} \to \mathbb{N}$ be a witness of this embedding. Let i_0 be the greatest index such that $f(i) \leq |h(\boldsymbol{v})|$. Then $u_1 \cdot u_2 \cdots u_{i_0} \leq_* h(\boldsymbol{v})$ ($\leq_*$ is the embedding quasi-ordering on X^*, see Section 6.1). Moreover, by definition of $h(\boldsymbol{v})$: for every $i > i_0$, $v_{f(i)} \in D(\boldsymbol{v})$. Thus $u_i \in D(\boldsymbol{v})$.

($\Leftarrow$) Assume $\boldsymbol{u} \in (\downarrow h(\boldsymbol{v})) \cdot D(\boldsymbol{v})^\omega$. Let $\boldsymbol{u} = \boldsymbol{u}_1\boldsymbol{u}_2$ with $\boldsymbol{u}_1 \in \downarrow h(\boldsymbol{v})$ and $\boldsymbol{u}_2 \in D(\boldsymbol{v})^\omega$. We define $f : \mathbb{N} \to \mathbb{N}$ that witnesses $\boldsymbol{u} \leq_\omega \boldsymbol{v}$. For indexes up to $|\boldsymbol{u}_1|$, f is defined as a witness of $\boldsymbol{u}_1 \leq_* h(\boldsymbol{v})$. The remainder of f is defined inductively: for every $i > |\boldsymbol{u}_1|$, pick for $f(i)$ an index j such that $j > \max\{i, f(1), f(2), \ldots, f(i-1)\}$ and $v_j \geq u_i$. Such an index j exists since $u_i \in D(\boldsymbol{v})$ and $D(\boldsymbol{v})$ consists of all the elements of X that are covered infinitely often in $\boldsymbol{v}$, that is: $x \in D(\boldsymbol{v}) \Leftrightarrow \forall i \in \mathbb{N}.\, \exists j > i.\, x \leq v_j$.

Proof of Corollary 9.1.2

$$\begin{aligned}
\boldsymbol{u} \leq_\omega \boldsymbol{v} &\Leftrightarrow \downarrow \boldsymbol{u} \subseteq \downarrow \boldsymbol{v} \\
&\Leftrightarrow (\downarrow h(\boldsymbol{u})) \cdot D(\boldsymbol{u})^\omega \subseteq (\downarrow h(\boldsymbol{v})) \cdot D(\boldsymbol{v})^\omega \\
&\Leftrightarrow (\downarrow h(\boldsymbol{u})) \cdot D(\boldsymbol{u})^\omega \subseteq (\downarrow h(\boldsymbol{v})) \cdot D(\boldsymbol{v})^* \cdot D(\boldsymbol{v})^\omega \\
&\Leftrightarrow h(\boldsymbol{u}) \in \downarrow h(\boldsymbol{v}) \cdot D(\boldsymbol{v})^* \wedge D(\boldsymbol{u}) \subseteq D(\boldsymbol{v})
\end{aligned}$$

$\square$

Corollary 9.1.3. *The set $X^\omega/\equiv_\omega$ is countable.*

Proof. It follows from Proposition 9.1.1 that

$$u \not\equiv_\omega v \Leftrightarrow h(\boldsymbol{u}) \neq h(\boldsymbol{v}) \vee D(\boldsymbol{u}) \neq D(\boldsymbol{v})$$

Since X^* and $Down(X)$ are countable (X is assumed countable), so is $X^\omega/\equiv_\omega$. $\square$

Finally, one last property is directly implied by Proposition 9.1.1:

Corollary 9.1.4. *$(X^\omega, \leq_\omega)$ is a WQO if and only if $(Down(X), \subseteq)$ is.*

Note that (WQO7) in Section 2.3 only gives well-foundedness of $(Down(X), \subseteq)$. And indeed, $(Down(X), \subseteq)$ may not be a WQO. Hence, neither is $(X^\omega, \leq_\omega)$. This matter is discussed in Section 9.2.

9.1.1 Encodings for X^ω and its Ideals

Subsequently, let $(X, \leq)$ designates an ideally effective WQO such that $(Down(X), \subseteq)$ is also a WQO. In this setting, $(X^\omega, \leq_\omega)$ is a WQO as well.

We have argued that it is hopeless to represent every element of X^ω, and we will therefore focus on the ideal effectiveness of its quotient $(X^\omega/\equiv_\omega, \leq_\omega)$. The above results suggest to represent equivalence classes of $X^\omega/\equiv_\omega$ as pairs from $X^* \times$

$Down(X)$. Intuitively, we want a pair $\langle \boldsymbol{u}, D\rangle \in X^* \times Down(X)$ to encode the equivalence class of infinite sequences that have head $\boldsymbol{u}$ and tail D. There are three issues with this representation:

1. If $D = \emptyset$, there are no infinite sequences with tail D. We therefore define $Down'(X) = Down(X) \smallsetminus \{\emptyset\}$, the set of non-empty downward-closed subsets of X. Note that working with $X^* \times Down(X)$ amounts to represent $X^{\leq\omega}$, the set of sequences of length at most ω. Subsequently, we will restrict our attention to $X^* \times Down'(X)$.

2. If $\boldsymbol{u}$ has a non-empty suffix in D, then there are no infinite sequence of head $\boldsymbol{u}$ and tail D, since we defined the head to be as small as possible. We therefore want $\langle \boldsymbol{u}, D\rangle$ to denote any infinite sequence in $\boldsymbol{u} \cdot D^\omega$.

3. However, all the elements of $\boldsymbol{u} \cdot D^\omega$ do not belong to the same equivalence class. For instance, if $X = \{a, b, c\}$ is a finite alphabet, and if $\boldsymbol{u} = aaba$ and $D = \{a, c\}$, then $aaba(a + c)^\omega$ contains the word $aabaa^\omega$, which is strictly smaller than $aaba(ca)^\omega$ for instance. The reason is that $D(aabaa^\omega) = \{a\} \subsetneq D$. The solution is to restrict our attention to the maximal elements of $\boldsymbol{u} \cdot D^\omega$: they are all equivalent, and thus represent a unique element of $X^\omega/ \equiv_\omega$. This is proved in the next proposition.

Proposition 9.1.5. *1. Let $\boldsymbol{u}, \boldsymbol{v} \in X^\omega$. If $\boldsymbol{u} \equiv_\omega \boldsymbol{v}$, then $h(\boldsymbol{u}) = h(\boldsymbol{v})$ and $D(\boldsymbol{u}) = D(\boldsymbol{v})$. We can thus define the* head *and* tail *of an equivalence class $\boldsymbol{S} \in X^\omega/ \equiv_\omega$. They will be denoted $h(\boldsymbol{S})$ and $D(\boldsymbol{S})$ respectively.*

2. Given an equivalence class $\boldsymbol{S}$ of $X^\omega/ \equiv_\omega$, $\boldsymbol{S}$ consists exactly of the maximal elements of $h(\boldsymbol{S}) \cdot (D(\boldsymbol{S}))^\omega$.

3. Given $\langle \boldsymbol{u}, D\rangle \in X^* \times Down'(X)$, the maximal elements of $\boldsymbol{u} \cdot D^\omega$ all are equivalent for $\equiv_\omega$. Let $\boldsymbol{S}$ be the equivalence class they all belong to. We have $D(\boldsymbol{S}) = D$ and $h(\boldsymbol{S}) = \boldsymbol{u}_1$, where $\boldsymbol{u} = \boldsymbol{u}_1\boldsymbol{u}_2$ and $\boldsymbol{u}_2$ is the longest suffix of $\boldsymbol{u}$ which is in D^*.

According to the third point of the proposition above, we let $\langle \boldsymbol{u}, D\rangle \in X^* \times Down'(X)$ represent the equivalence class $\boldsymbol{S} \in X^\omega/ \equiv_\omega$ to which every maximal element of $\boldsymbol{u} \cdot D^\omega$ belongs. Note that in general the maximal elements of $\boldsymbol{u} \cdot D^\omega$ are strictly included in $\boldsymbol{S}$. For instance, in the case introduced before: if $X = \{a, b, c\}$ is a finite alphabet, and if $\boldsymbol{u} = aaba$ and $D = \{a, c\}$, the infinite sequence $aab(ca)^\omega$ is equivalent to maximal elements of $\boldsymbol{u} \cdot D^\omega$, but does not belong to it.

Moreover, an equivalence class $\boldsymbol{S}$ has several representations. In light of the proposition, we define $\langle h(\boldsymbol{S}), D(\boldsymbol{S})\rangle$ to be its *canonical representation*. According to the third point, this representation is computable from any other representation $\langle \boldsymbol{u}, D\rangle$: it suffices to remove the suffix of $\boldsymbol{u}$ which is in D.

Proof. Of Proposition 9.1.5

1. According to Corollary 9.1.2, we immediately get that $D(\boldsymbol{u}) = D(\boldsymbol{v})$ by double inclusion. Moreover, we have $h(\boldsymbol{u}) \in \downarrow h(\boldsymbol{v}) \cdot D(\boldsymbol{u})^*$, but by definition of $h(\boldsymbol{u})$,

its last symbol is not in $D(\boldsymbol{u})$. Therefore $h(\boldsymbol{u}) \leq_* h(\boldsymbol{v})$. By symmetry we get $h(\boldsymbol{u}) = h(\boldsymbol{v})$.

2. Any element $\boldsymbol{u} \in X^\omega$ belongs to $h(\boldsymbol{u}) \cdot D(\boldsymbol{u})^\omega$. Therefore, elements of $\boldsymbol{S}$ belong to $h(\boldsymbol{S}) \cdot D(\boldsymbol{S})^\omega$. Conversely, if $\boldsymbol{u} \in h(\boldsymbol{S}) \cdot D(\boldsymbol{S})^\omega$ then $h(\boldsymbol{u}) \in (\downarrow h(\boldsymbol{S})) \cdot D(\boldsymbol{S})^*$ and $D(\boldsymbol{u}) \subseteq D(\boldsymbol{S})$. Therefore, by Corollary 9.1.2, $\boldsymbol{u}$ is smaller than any element of $\boldsymbol{S}$.

3. Given $\boldsymbol{u} \in X^*$ and $D \in \mathit{Down}'(X)$, decompose $\boldsymbol{u} = \boldsymbol{u}_1 \boldsymbol{u}_2$ where $\boldsymbol{u}_2$ is the longest suffix of $\boldsymbol{u}$ which is in D. Any maximal word $\boldsymbol{v}$ of $\boldsymbol{u} \cdot D^\omega$ can be written $\boldsymbol{u}_1 \boldsymbol{v}'$ with $\boldsymbol{v} \in D^\omega$. Since $\boldsymbol{u}_1$'s last element is not in D, $h(\boldsymbol{v}) = \boldsymbol{u}_1$ and $D(\boldsymbol{v}) = D$. Therefore, they are all equivalent, and we denote by $\boldsymbol{S}$ their equivalence class. We have proved that $\boldsymbol{S}$ is the class of elements of head $\boldsymbol{u}_1$ and tail D.

□

The decidability of $\leq_\omega$ on this representation follows from Corollary 9.1.2, and the computability of the canonical representation, the quasi-ordering $\leq$ on X, the inclusion of ideals of $(X^*, \leq_*)$ and the inclusion of downward-closed subsets of X.

We denote by the same symbol $\leq_\omega$ the quasi-ordering on $X^* \times \mathit{Down}'(X)$ defined by: $\langle \boldsymbol{u}, D \rangle \leq_\omega \langle \boldsymbol{v}, E \rangle$ if all the equivalent maximal sequences of $\boldsymbol{u} \cdot D^\omega$ are smaller than all the equivalent maximal sequences of $\boldsymbol{v} \cdot E^\omega$. This new quasi-ordering $\leq_\omega$ is decidable since we can always compute the canonical representations, and then use Corollary 9.1.2. Instead, we prove that Corollary 9.1.2 is also valid in this more general setting:

Proposition 9.1.6. *Given two pairs $\langle \boldsymbol{u}, D \rangle, \langle \boldsymbol{v}, E \rangle \in X^* \times \mathit{Down}'(X)$,*

$$\langle \boldsymbol{u}, D \rangle \leq_\omega \langle \boldsymbol{v}, E \rangle \iff \boldsymbol{u} \in (\downarrow \boldsymbol{v}) \cdot E^* \wedge D \subseteq E$$

Proof. Let $\boldsymbol{S}$ and $\boldsymbol{T}$ be the two equivalence classes of $X^\omega / \equiv_\omega$ represented by $\langle \boldsymbol{u}, D \rangle$ and $\langle \boldsymbol{v}, E \rangle$ respectively. By Proposition 9.1.5, we know that $D = D(\boldsymbol{S})$ and $E = D(\boldsymbol{T})$ on the one hand, and that $\boldsymbol{u} = h(\boldsymbol{S}) \cdot \boldsymbol{u}'$ and $\boldsymbol{v} = h(\boldsymbol{T}) \cdot \boldsymbol{v}'$ for some $\boldsymbol{u}' \in D^*$ and some $\boldsymbol{v}' \in E^*$.

($\Rightarrow$) If $\langle \boldsymbol{u}, D \rangle \leq_\omega \langle \boldsymbol{v}, E \rangle$, by Corollary 9.1.2:

$$h(\boldsymbol{S}) \in (\downarrow h(\boldsymbol{T})) \cdot D(\boldsymbol{T})^* \wedge D(\boldsymbol{S}) \subseteq D(\boldsymbol{T}),$$

which is equivalent to $h(\boldsymbol{S}) \in (\downarrow h(\boldsymbol{T})) \cdot E^* \wedge D \subseteq E$. The left conjunct implies $h(\boldsymbol{S})\boldsymbol{u}' \in (\downarrow h(\boldsymbol{T})) \cdot (\downarrow \boldsymbol{u}') \cdot E^*$, and since $\boldsymbol{u}' \in D^* \subseteq E^*$, this simplifies to $\boldsymbol{u} \in (\downarrow h(\boldsymbol{T})) \cdot E^* \subseteq (\downarrow \boldsymbol{v}) \cdot E^*$.

($\Leftarrow$) Conversely, because $\boldsymbol{u} = h(\boldsymbol{S})\boldsymbol{u}'$ and $\boldsymbol{u}' \in D^* \subseteq E^*$, $\boldsymbol{u} \in (\downarrow \boldsymbol{v}) \cdot E^*$ implies $h(\boldsymbol{S}) \in (\downarrow h(\boldsymbol{T})\boldsymbol{v}') \cdot E^*$. But since $\boldsymbol{v}' \in E^*$, the right-hand-side simplifies to $(\downarrow h(\boldsymbol{T})) \cdot E^*$, entailing the desired condition:

$$h(\boldsymbol{S}) \in (\downarrow h(\boldsymbol{T})) \cdot D(\boldsymbol{T})^* \wedge D(\boldsymbol{S}) \subseteq D(\boldsymbol{T})$$

□

9.1.2 Ideal Effectiveness of the Infinite Sequences Extension

It follows from the previous proposition that the relation $\leq_\omega$ on $X^* \times Down'(X)$ extends the classical product ordering $\leq_\times$ (it is actually be obtained as a composition with an equivalence relation, as defined in Section 4.2). Therefore, Section 4.1 applies to the quasi-ordering $\leq_\omega$, and we therefore once again turn to the functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$.

Lemma 9.1.7. *Given* $\boldsymbol{I} \in Idl(X^*, \leq_*)$*,* $\mathcal{J} \in Idl(Down(X), \subseteq)$*,* $\boldsymbol{u} \in X^*$ *and* $D \in Down(X)$*:*

$$\mathcal{C}l_{\mathrm{I}}(\boldsymbol{I} \times \mathcal{J}) \overset{def}{=} {\downarrow_\omega}(\boldsymbol{I} \times \mathcal{J}) = (\boldsymbol{I} \cdot (\bigcup \mathcal{J})^*) \times \mathcal{J}$$

$$\mathcal{C}l_{\mathrm{F}}(\langle \boldsymbol{u}, D\rangle) \overset{def}{=} {\uparrow_\omega}\langle \boldsymbol{u}, D\rangle = \bigcup_{\boldsymbol{u}=\boldsymbol{u}_1\boldsymbol{u}_2} {\uparrow_\times}\langle \boldsymbol{u}_1, D \cup {\downarrow} Supp(\boldsymbol{u}_2)\rangle$$

Proof. Let $\langle \boldsymbol{u}, D\rangle \in \boldsymbol{I} \times \mathcal{J}$ and $\langle \boldsymbol{v}, E\rangle \leq_\omega \langle \boldsymbol{u}, D\rangle$, that is $\boldsymbol{v} \in ({\downarrow}\, \boldsymbol{u}) \cdot D^*$ and $E \subseteq D$. Since $D \in \mathcal{J}$ and $\boldsymbol{u} \in \boldsymbol{I}$ which is downward-closed, $\boldsymbol{v} \in \boldsymbol{I} \cdot (\bigcup \mathcal{J})^*$. Finally, since $\mathcal{J}$ is downward-closed, $E \in \mathcal{J}$ and $\langle \boldsymbol{v}, E\rangle \in I \cdot (\bigcup \mathcal{J})^*) \times \mathcal{J}$.

Conversely, given $\langle \boldsymbol{v}, E\rangle \in \boldsymbol{I} \cdot (\bigcup \mathcal{J})^*) \times \mathcal{J}$, decompose $\boldsymbol{v} = \boldsymbol{u}\boldsymbol{w}$ with $\boldsymbol{u} \in \boldsymbol{I}$ and $\boldsymbol{w} \in (\bigcup \mathcal{J})^*$. Since $\boldsymbol{w}$ is finite, it actually belongs to a finite union $(\bigcup_i D_i)^*$ of downward-closed sets of $\mathcal{J}$. Since $\mathcal{J}$ is directed, $D \overset{\mathrm{def}}{=} E \cup \bigcup_i D_i$ is in $\mathcal{J}$. Therefore, $\langle \boldsymbol{v}, E\rangle \leq_\omega \langle \boldsymbol{u}, D\rangle \in \boldsymbol{I} \times \mathcal{J}$.

Let $\langle \boldsymbol{v}, E\rangle \geq_\omega \langle \boldsymbol{u}, D\rangle$, that is $\boldsymbol{u} \in ({\downarrow_*}\, \boldsymbol{v}) \cdot E^*$ and $D \subseteq E$. Decompose $\boldsymbol{u} = \boldsymbol{u}_1\boldsymbol{u}_2$ with $\boldsymbol{u}_1 \leq_* \boldsymbol{v}$ and $\boldsymbol{u}_2 \in E^*$: $\langle \boldsymbol{u}_1, D \cup {\downarrow} Supp(\boldsymbol{u}_2)\rangle \leq_\times \langle \boldsymbol{v}, E\rangle$.

Conversely, if $\boldsymbol{u} = \boldsymbol{u}_1\boldsymbol{u}_2$, then trivially $\boldsymbol{u} \in ({\downarrow_*}\, \boldsymbol{u}_1) \cdot ({\downarrow} Supp(\boldsymbol{u}_2))^*$ and $D \subseteq D \cup {\downarrow} Supp(\boldsymbol{u}_2)$. Thus, according to Corollary 9.1.2, $\langle \boldsymbol{u}_1, D \cup Supp(\boldsymbol{u}_2)\rangle \in {\uparrow_\omega}\langle \boldsymbol{u}, D\rangle$. $\square$

Now according to Sections 4.1, 5.3 and 6.1, $(X^\omega, \leq_\omega)$ is ideally effective provided that:

1. $(X, \leq)$ is ideally effective,
2. $(Down'(X), \subseteq)$ is ideally effective,
3. Functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ are computable.

The first condition is the basic assumption we have made throughout other sections. The second one however is novel: indeed, $(Down(X), \subseteq)$ might not even be a WQO in general, making its ideal effectiveness a non-relevant question. The necessity of this extra assumption will be further discussed in the next section. Finally, we could neither prove that the third condition follows from the two first conditions, nor that it was independent. The two operations we use in Lemma 9.1.7 whose computability does not follow *a priori* from the two first conditions listed above are $\bigcup \mathcal{J}$ (used in the expression of $\mathcal{C}l_{\mathrm{I}}$) and ${\downarrow} Supp(\boldsymbol{u})$ (used in the expression of $\mathcal{C}l_{\mathrm{F}}$). We have already used the second one earlier, and it seems obviously computable, since $Supp(\boldsymbol{u})$ (for $\boldsymbol{u}$ a finite word) is a finite set, ${\downarrow} Supp(\boldsymbol{u}) = \bigcup_{x \in Supp(\boldsymbol{u})} {\downarrow} x$. However, this expression will output a downward-closed set represented as a list of ideals of X. But, we need this downward-closed set to be represented according to the encoding chosen to show that $(Down(X), \subseteq)$ is ideally effective. Indeed, assuming that both $(X, \leq)$ and $(Down'(X), \subseteq)$ are ideally effective is not enough, we need to ensure that the representations used for downward-closed sets of $(X, \leq)$ can be translated into representations of elements of $Down'(X)$.

In other words, we want to assume that the following *transfer* function is computable:

$$\begin{cases} Down(X) & \to & Down'(X) \\ D & \mapsto & D \end{cases}$$

Similarly, the operation $\bigcup \mathcal{J}$ is a way to link the representations in the other direction: going from ideals of $Down'(X)$ back to ideals of X. We thus assume the computability of the *flattening* function:

$$\begin{cases} Idl(Down'(X)) & \to & Down(X) \\ \mathcal{J} & \mapsto & \bigcup \mathcal{J} \end{cases}$$

Finally, we obtain the following theorem:

Theorem 9.1.8. *Let $(X, \leq)$ a WQO such that $(Down(X), \subseteq)$ is a WQO. Then $(X^\omega / \equiv_\omega, \leq_\omega)$ is an ideally effective WQO provided that:*

- *$(X, \leq)$ is ideally effective for some representations of X and $Idl(X)$,*
- *$(Down'(X), \subseteq)$ is ideally effective, for some representations of $Down'(X)$ and $Idl(Down'(X))$,*
- *The transfer function is computable. It maps a non-empty list $[I_1, \ldots, I_n]$ of ideals of X (encoded according to the representation of the first condition) to an element $D \in Down'(X)$ (encoded according to the representation of the second condition) such that $D = \bigcup_{i=1}^n I_i$.*
- *The flattening function is computable. It maps $\mathcal{J} \in Idl(Down'(X))$ to a list $[I_1, \ldots I_n]$ of ideals of X (encoded according to the first condition) such that $\bigcup \mathcal{J} = \bigcup_{i=1}^n I_i$.*

The next chapter is devoted to a deeper understanding of the assumptions that $(Down(X), \subseteq)$ is a WQO, and furthermore an ideally effective one.

Remark 9.1.9. *It is natural to assume that we represent the elements of $Down'(X)$ using the same representation we have used so far, thus rendering the transfer function trivial. Note that in the expression of $\mathcal{Cl}_{\mathrm{F}}$, we also perform unions of downward-closed sets, which is trivial with our usual representation, but might not be for an arbitrary one. Thankfully, union of downward-closed sets corresponds to intersection of filters:*

$$\uparrow D_1 \cap \uparrow D_2 = \uparrow (D_1 \cup D_2)$$

Unions of downward-closed sets are therefore computable when $Down'(X)$ is ideally effective.

However, even if we assume the usual representation for $Down'(X)$, we could not prove that the computability of the flattening function is implied by the other assumptions (namely ideal effectiveness of both X and $Down(X)$). Nor could we prove that it is independent (in the fashion of Chapter 8).

However, we would like to point out that the flattening function allows to test whether an ideal is principal: $\mathcal{J} \in Idl(Down(X))$ is principal if and only if $\bigcup \mathcal{J} \in \mathcal{J}$. This does not suffice to prove that the flattening function is not computable in general since the counter-example for deciding whether an ideal is principal given in Section 8.3 takes place in a more general setting. In other words, the flattening function allows to decide whether an ideal is principal only in WQOs that are the ideal space of another WQO.

Furthermore, assume we represent downward-closed sets as finite sets of ideals. Then, the flattening allows to decide whether an ideal of X is principal. Indeed, given an ideal of X, one can compute $\downarrow_{\subsetneq} I \stackrel{def}{=} \{J \in Idl(X) \mid J \subsetneq I\}$. Indeed, this set can be obtained as $\downarrow_{Idl(X)} I \cap (Idl(X) \smallsetminus \uparrow_{Idl(X)} I)$. We claim that $\bigcup(\downarrow_{\subsetneq} I) = I$ if and only if I is not principal in $Idl(X)$. Indeed, if I is principal, $I = \downarrow x$ for some $x \in X$. Then for every $J \in \downarrow_{\subsetneq} I$, $x \notin J$, and therefore $x \notin \bigcup \downarrow_{\subsetneq} I$, but $x \in I$. Conversely, if $x \in I$ but $x \notin \bigcup(\downarrow_{\subsetneq} I)$, then $\downarrow x \subseteq I$ but $\downarrow x \not\subsetneq I$, i.e. $\downarrow x = I$.

Once again, this is not enough to conclude that the flattening function is not computable in general: it might be the case the the assumption $Down'(X)$ is ideally effective implies that we can test whether an ideal of X is principal. In particular, for all ideally effective WQOs $(X, \leq)$ we know of such that we cannot decide whether an ideal is principal, $Down'(X)$ is not ideally effective.

9.2 Better Quasi-Orderings

Chapters 5 to 7 provide an effective algebra of ideally effective WQOs: any WQO obtained as sums of products of finite sequences of finite subsets of finite multisets of ordinals and/or finite WQOs is an ideally effective WQO. And procedures for set-theoretic operations in this WQO do not only exist, they can be computed from the structure of the WQO.

However, the operations of taking the infinite sequences of a WQO (quasi-ordered with embedding), or the infinite powerset (quasi-ordered with $\sqsubseteq_{\mathcal{H}}$) are not *a priori* part of this algebra. Indeed, these two operations do not preserve the WQO property. This was first proved by Rado in [38]: he exhibited a WQO $(X, \leq)$ such that $(X^\omega, \leq_\omega)$ is not WQO. This WQO is now commonly known as *Rado's structure*. Moreover, this counter example is minimal: given a WQO $(X, \leq)$, $(X^\omega, \leq_\omega)$ is WQO if and only if $(X, \leq)$ does not embed Rado's structure.

Inspired by this characterization, Nash-Williams [39, 40] defined the notion of *Better Quasi-Orderings* (BQO), that notably satisfies the following property: if $(X, \leq)$ is a BQO, then the ordinal sequences over X, quasi-ordered with embeddability is a WQO. Alternatively, Section 9.1 has shown that $\mathcal{P}(X)$ is WQO if and only if X^ω is, and thus, Rado provided a sufficient and necessary condition for $\mathcal{P}(X)$ to be WQO. What Nash-Williams intended are conditions on $(X, \leq)$ such that $\mathcal{P}(X)$, $\mathcal{P}^2(X) \stackrel{\text{def}}{=} \mathcal{P}(\mathcal{P}(X))$,

$\mathcal{P}^3(X)$, and so on iterating transfinitely all are WQOs.

Many positive results on BQOs followed, the intuitive rule being that whenever an order-construction preserves WQO, its infinitary version preserves BQO: if $(X, \leq)$ is WQO, then the set of finite sequences over X is WQO (Higman's Theorem), while if it is BQO, the set of sequences over a countable ordinal is BQO. Similar results for sets and trees have been proved.

Of course, BQOs are *better* WQOs, that is a BQO is in particular a WQO, and indeed the original definition was given in a similar way: $(X, \leq)$ is BQO if any application $f : B \to X$ from a barrier B to X is good, that is there exists $s \lhd t \in B$ such that $f(s) \leq f(t)$. The formal definitions of barriers and $\lhd$ are too technical and out of the scope of this thesis, and will therefore not be given, we simply stress the similarities with (WQO1): the application $f : B \to X$ is a generalization of an infinite sequence (application from $\mathbb{N}$ to X). For that matter, $\mathbb{N}$ is a barrier on which $\lhd$ coincides with the natural ordering, which proves that any BQO is WQO.

Jullien [41] later provided an alternative definition of BQOs, which is proved equivalent in [42, 11]. This definition uses the notion of indecomposability of an ordinal sequence (which we solely call sequence from now on, see Chapter 2 for definitions, terminology and notations. In particular, in what follows, $\leq$ denotes sequence embedding). A sequence $\boldsymbol{s}$ is said to be *indecomposable* if for any sequences $\boldsymbol{s}_1, \boldsymbol{s}_2$ such that $\boldsymbol{s} = \boldsymbol{s}_1 \cdot \boldsymbol{s}_2$ and $\boldsymbol{s}_2 \neq \epsilon$, $\boldsymbol{s} \leq \boldsymbol{s}_2$, that is indecomposable sequences embed in all their non-empty suffixes. Note that an indecomposable sequence necessarily has an indecomposable length, where an ordinal α is *indecomposable* if it cannot be written $\alpha = \beta + \gamma$ with $0 \neq \gamma < \alpha$, or equivalently, $\alpha = \omega^\beta$ for some ordinal β.

Definition 9.2.1. *Jullien [41] A QO $(X, \leq)$ is BQO if any non-empty sequence $\boldsymbol{s}$ over X of countable length can be written $\boldsymbol{s} = \boldsymbol{s}_1 \cdot \boldsymbol{s}_2$ with $\boldsymbol{s}_2$ non-empty and indecomposable, i.e. $\boldsymbol{s}$ has an indecomposable suffix.*

In this chapter, we are looking for sufficient conditions on $(X, \leq)$ to ensure that $(X^\omega, \leq_\omega)$ is an ideally effective WQO. In particular, we need $(Down(X), \subseteq)$ to be WQO (cf. Corollary 9.1.4). Note that since every construction presented in the previous chapters that preserve WQOs also preserve BQOs, and since our basic WQOs (namely natural numbers and finite quasi-orderings) are BQOs, our effective algebra of WQOs is actually an algebra of BQOs. Thus, we can also close this algebra under the construction of the infinite sequences (which preserves BQO), or the full powerset construction. But what about effectiveness ? To prove that $(X^\omega, \leq_\omega)$ is an ideally effective WQO, we need that $(Down(X), \subseteq)$ is not only a WQO, but an ideally effective one. In other words, we want to show that $Down$ is an ideally effective construction on BQOs. It cannot be an ideally effective construction on WQOs since it does not even preserve WQOs. In Section 9.4, we will actually show a stronger statement. But first, we introduce a finer notion than BQO.

9.3 α-WQO

Observe that Definition 9.2.1 can be naturally layered: X is a BQO if *all* ordinal sequences over X satisfy some property. In the following definition, we only ask that this property holds for ordinal sequences up to some length. The following definition can be found in [11]:

Definition 9.3.1. *[11], Chapter 8*
Given an indecomposable ordinal α, a QO $(X, \leq)$ is α-WQO if any β-sequence $\boldsymbol{s}$ over X for $\beta \leq \alpha$ can be written $\boldsymbol{s} = \boldsymbol{s}_1 \cdot \boldsymbol{s}_2$ with $\boldsymbol{s}_2$ non-empty and indecomposable.

Note that the notion of α-WQO when α is not indecomposable coincides with the notion β-WQO if there exists γ such that $\alpha = \gamma + \beta$. Indeed, if $(X, \leq)$ is β-WQO, then any sequence $\boldsymbol{s} \in X^\alpha$ can be decomposed $\boldsymbol{s} = \boldsymbol{uv}$ with $\boldsymbol{v} \in X^\beta$, and thus $\boldsymbol{v}$ has an indecomposable suffix. This is the reason we are only interested in α-WQOs for indecomposable ordinals α.

With this definition, a QO is BQO if and only if it is α-WQO for every countable ordinal α. Moreover, the notion of WQO coincides with ω-WQO, which provides a simple proof that BQOs are WQOs.

Proposition 9.3.2. *$(X, \leq)$ is WQO if and only if it is ω-WQO.*

Proof. Observe that ω-sequences have been introduced in the previous chapter.

($\Rightarrow$) If $(X, \leq)$ is WQO, and $\boldsymbol{s}$ is an ω-sequence, then the decomposition of $\boldsymbol{s}$ is given by its head and tail which were introduced in Proposition 9.1.1. Indeed, let $\boldsymbol{s}'$ be the ω-sequence such that $\boldsymbol{s} = h(\boldsymbol{s}) \cdot \boldsymbol{s}'$. It is not hard to see that $\boldsymbol{s}'$ is indecomposable since it is made of elements that are covered infinitely often in $\boldsymbol{s}$.

($\Leftarrow$) If $(X, \leq)$ is ω-WQO, and $\boldsymbol{s} \in X^\omega$, let $\boldsymbol{s} = \boldsymbol{s}_1\boldsymbol{s}_2$ be the decomposition given by Definition 9.3.1, and let x be the first element of s_2. Since $\boldsymbol{s}_2$ is indecomposable, x must be smaller than some subsequent element of $\boldsymbol{s}_2$.

□

We are mainly interested in this finer definition for the following property: $(Down(X), \subseteq)$ is WQO if and only if $(X, \leq)$ is ω^2-WQO. This is proved in the following proposition, among other characterizations:

Proposition 9.3.3. *Let $(X, \leq)$ be a QO. The following are equivalent:*

1. *$(X, \leq)$ is ω^2-WQO,*
2. *$(Idl(X), \subseteq)$ is WQO,*
3. *$(Down(X), \subseteq)$ is WQO,*
4. *$(Up(X), \supseteq)$ is WQO,*
5. *$(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ is WQO,*
6. *$(\mathcal{P}(X), \sqsubseteq_{\mathcal{S}})$ is WQO,*
7. *$(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{S}})$ is WQO,*
8. *$(X^\omega, \leq_\omega)$ is WQO,*
9. *$X^{<\omega^2}$ is WQO for the sequence embedding quasi-ordering,*

10. *X^{ω^2} is well-founded for the sequence embedding quasi-ordering,*

11. *$(X, \leq)$ is a WQO and does not contain Rado's structure,*

where $\sqsubseteq_{\mathcal{S}}$ is the Smyth quasi-ordering on $\mathcal{P}(X)$, defined by: $S \sqsubseteq_{\mathcal{S}} T \overset{def}{\Leftrightarrow} \forall y \in T.\ \exists x \in S.\ x \leq y$.

Proof. $2 \iff 3$: follows from the isomorphism between $(Down(X), \subseteq)$ and $(\mathcal{P}_f(Idl(X))/{\equiv_{\mathcal{H}}}, \sqsubseteq_{\mathcal{H}})$, and the fact that $(Y, \leq)$ is WQO if and only if $(\mathcal{P}_f(Y), \sqsubseteq_{\mathcal{H}})$ is.

$5 \iff 3 \iff 4$: also follows from aforementioned isomorphisms (notably at the end of Chapter 2).

$4 \iff 6 \iff 7$: dual of $\sqsubseteq_{\mathcal{H}}$ which coincides with inclusion for downward-closed sets, $\sqsubseteq_{\mathcal{S}}$ coincides with $\supseteq$ for upward-closed set: $S \sqsubseteq_{\mathcal{S}} T$ if and only if $\uparrow S \supseteq \uparrow T$. Besides, any subset S is equivalent for $\sqsubseteq_{\mathcal{S}}$ to its upward-closure, which is equivalent to its finite basis.

$3 \iff 8$: follows from Corollary 9.1.4

$9 \Rightarrow 8$: X^{ω} is a subset of $X^{<\omega^2}$.

$8 \Rightarrow 9$: The embedding quasi-ordering on $X^{<\omega^2}$ is an extension of Higman's quasi-ordering on $(X^{\omega})^*$, which is a WQO by Higman's Lemma.

$10 \Rightarrow 1$: Let $\boldsymbol{s} \in X^{\omega^2}$. Consider the set of all non-empty suffixes of $\boldsymbol{s}$. Since X^{ω^2} is well-founded, this set has a minimal element. It is simple to see that this minimal element is an indecomposable suffix of $\boldsymbol{s}$.

$1 \Rightarrow 8$: Let Y be the set of indecomposable sequences of X^{ω}. We show that Y is a WQO. It follows that $X^* \times Y$ is a WQO, since by Proposition 9.3.2, $(X, \leq)$ is WQO. Moreover, since $(X, \leq)$ is ω^2-WQO, any ω-sequence $\boldsymbol{s}$ can be decomposed $\boldsymbol{s} = \boldsymbol{s}_1\boldsymbol{s}_2$ with $\boldsymbol{s}_2$ indecomposable. Therefore, X^{ω} is isomorphic to an extension of $X^* \times Y$, and as such is WQO.

We proceed to show that Y is WQO. An infinite sequence $\boldsymbol{S} = (\boldsymbol{s}_i)_{i<\omega}$ of elements of Y can be *flattened* as a sequence $\boldsymbol{s} = \prod_{i<\omega} \boldsymbol{s}_i \in X^{\omega^2}$. This sequence can be written $\boldsymbol{s} = \boldsymbol{u}\boldsymbol{v}$ with $\boldsymbol{v}$ indecomposable, and we can further assume that the length of $\boldsymbol{u}$ is a multiple of ω, that is $\boldsymbol{u} = \boldsymbol{s}_0\boldsymbol{s}_1 \cdots \boldsymbol{s}_n$ for some $n < \omega$. Now we can *unflatten* $\boldsymbol{v}$ to see it back as an ω-sequence $\boldsymbol{V} = \boldsymbol{s}_{n+1}\boldsymbol{s}_{n+2} \cdots$ over Y. Since $\boldsymbol{v}$ is indecomposable, $\boldsymbol{s}_{n+1}$ embeds in some finite prefix of what remains of $\boldsymbol{V}$, i.e. $\boldsymbol{s}_{n+1} \leq \boldsymbol{s}_{n+2} \cdots \boldsymbol{s}_m$ for some $m < \omega$. But since $\boldsymbol{s}_{n+1}$ is an infinite sequence, by the pigeon-hole principle an infinite suffix of $\boldsymbol{s}_{n+1}$ embeds in $\boldsymbol{s}_i$ for some $n+2 \leq i \leq m$, and since $\boldsymbol{s}_{n+2}$ is indecomposable, $\boldsymbol{s}_{n+1} \leq \boldsymbol{s}_i$. This is an increasing pair of $\boldsymbol{S}$, which proves Y is a WQO.

$3 \Rightarrow 10$: This implication follows from an analysis of the embedding relation between ordinal sequences which is very similar to the one we conducted in Proposition 9.1.1, but we failed to provide a proof that uses this analysis without replaying it. As previously observed, the "unflattening" defines a reflection from X^{ω^2} to $(X^{\omega})^{\omega}$ which is in general not an embedding. Therefore, the image of the embedding quasi-ordering on X^{ω^2} is an extension of the embedding on $(X^{\omega})^{\omega}$. However, if extensions of a WQO are WQOs, extensions of a well-founded quasi-orderings may not be well-founded. As a result, we cannot deduce the well-foundedness of X^{ω^2} from the well-foundedness of $(X^\omega)^\omega$ (which follows from Section 9.1 when X^ω is a WQO).

Given a sequence $\boldsymbol{s} \in X^{\omega^2}$, we denote by $\boldsymbol{s}_i \in X^\omega$ the ω-sequences such that $\boldsymbol{s} = \boldsymbol{s}_1\boldsymbol{s}_2\cdots$, that is $\forall i, j \in \mathbb{N}$, $\boldsymbol{s}_i(j) = \boldsymbol{s}(\omega \cdot i + j)$. Recall from Section 9.1 the notion of *tail* of an ω-sequence. The *tail* of a sequence $\boldsymbol{s} \in X^{\omega^2}$, denoted $\mathcal{D}(\boldsymbol{s}) \in Down(Down(X))$, is defined by $\mathcal{D}(\boldsymbol{s}) = \bigcap_{i<\omega} \bigcup_{j \geq i} \downarrow D(\boldsymbol{s}_i)$, where $\downarrow D$ denotes $\{E \in Down(X) \mid E \subseteq D\}$, that is the downward-closure is taken over $Down(Down(X))$, and $\downarrow D$ is a principal ideal of downward-closed sets. Assuming $Down(X)$ is a WQO, $Down(Down(X))$ is well-founded ((WQO7)) and a infinite increasing subsequence can be extracted from the ω-sequence $(D(\boldsymbol{s}_i))_{i<\omega}$, implying that $\mathcal{D}(\boldsymbol{s}) \neq \emptyset$. It remains to show that whenever two ω^2-sequences $\boldsymbol{s}$ and $\boldsymbol{t}$ are ordered $\boldsymbol{s} \leq \boldsymbol{t}$, then $\mathcal{D}(\boldsymbol{s}) \subseteq \mathcal{D}(\boldsymbol{t})$. Let $\boldsymbol{s}, \boldsymbol{t}$ be such two sequences and $f : \boldsymbol{\omega^2} \to \boldsymbol{\omega^2}$ be a witness of the embedding $\boldsymbol{s} \leq \boldsymbol{t}$. Let $i \in \mathbb{N}$. The image of $f(\omega \cdot (i+1))$ is in $\boldsymbol{\omega^2}$, thus it is some $\omega \cdot n + m$. This means that $\boldsymbol{s}_i \leq \boldsymbol{t}_0\boldsymbol{t}_1 \cdots \boldsymbol{t}_n\boldsymbol{t}_{n+1}$. Therefore, by the pigeon-hole principle, there exists $j \leq n+1$ and an infinite suffix $\boldsymbol{s}'_i$ of $\boldsymbol{s}_i$ such that $\boldsymbol{s}'_i \leq \boldsymbol{t}_j$. Observe that $D(\boldsymbol{s}'_i) = D(\boldsymbol{s}_i)$, and by Proposition 9.1.1, $D(\boldsymbol{s}'_i) \subseteq D(\boldsymbol{t}_j)$.

In the end, if $D \in \mathcal{D}(\boldsymbol{s})$, it is covered by infinitely many $D(\boldsymbol{s}_i)$, and thus by infinitely many $D(\boldsymbol{t}_j)$, and is thus a member of $\mathcal{D}(\boldsymbol{t})$.

Lastly, for Item 11, we cannot provide a proof since we did not define Rado's structure. 11 $\iff$ 8: is proved in the Rado's original article [38]. The right-to-left direction can also be found in [43, 11] (with a nice illustration of Rado's structure in [43]). Otherwise, a direct proof of 11 $\iff$ 6: can be found in [44]. $\square$

Many of the equivalences above generalize to countable ordinals.

Proposition 9.3.4. *Given an indecomposable countable ordinal α, $(X, \leq)$ is α-WQO if and only if $(X^{<\alpha}, \leq)$ is WQO [11, 45].*

The above generalizes items 1 and 9. Items 2, 3,4, 5, 6 and 7 are generalized as the equivalence between [46]:

- *$(X, \leq)$ is $(\alpha \cdot \omega)$-WQO,*
- *$(Idl(X), \subseteq)$ is α-WQO,*
- *$(Down(X), \subseteq)$ is α-WQO,*
- *$(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ is α-WQO,*
- *$(\mathcal{P}(X), \sqsubseteq_{\mathcal{S}})$ is α-WQO,*
- *$(\mathcal{P}_f(X), \sqsubseteq_{\mathcal{S}})$ is α-WQO,*
- *$(Up(X), \supseteq)$ is α-WQO.*

The generalization of Item 11 is what led Nash-Williams to the original definition of BQOs, with the notion of blocks. This intuition of blocks is formalized in [42], Theorem III-3.3. Concerning Item 10, the implication X^α well-founded $\Rightarrow X$ α-WQO is proved in [11], the general proof being as simple as the one above. However, we were unable to find mention of the converse implication in the literature, and have been unable to prove it or disprove it. It seems possible to generalize the proof given above for $\alpha = \omega^2$ to indecomposable ordinals of the form $\omega^{\alpha+1}$. Indeed, we essentially used that if X is $\omega^{\alpha+1}$-WQO, then $Y \stackrel{\text{def}}{=} X^{\omega^\alpha}$ is WQO, and then $X^{\omega^{\alpha+1}}$ can be approximated by Y^ω. But in the case X is ω^λ-WQO, with λ a limit ordinal, we cannot use the same methods.

Finally, let us mention that all the order-constructions mentioned in the previous chapters that preserve WQO also preserve α-WQO. For $\alpha = \omega^2$, this will be a trivial consequence of our analysis in the next section. In the general case, and for more details on BQO theory, we redirect the reader to the following surveys [43, 45, 42, 11].

9.4 Ideally Effective ω^2-WQOs

In this section, we extend our notion of effectiveness to ω^2-WQOs.

If $(X, \leq)$ is an ordinal, then so is $(\mathit{Idl}(X), \subseteq)$ (Section 3.2.3), and therefore it is ideally effective (successor of a recursive ordinal is recursive). Similarly, if $(X, \leq)$ is finite, then $(\mathit{Idl}(X), \subseteq)$ is isomorphic to $(X, \leq)$ and is thus ideally effective. Recall that $(\mathit{Down}(X), \subseteq)$ is ideally effective whenever $(\mathit{Idl}(X), \subseteq)$ is (Section 7.3). Thus in these cases, $(X^\omega, \leq_\omega)$ is ideally effective. It remains to show that the constructions we have considered will preserve these properties. The properties we are formally interested in are formalized in the next definition.

Definition 9.4.1. *A ω^2-WQO $(X, \leq)$ further equipped with representations for X, $\mathit{Idl}(X)$ and $\mathit{Idl}(\mathit{Idl}(X))$ is Idl^2-*effective *if:*

- *$(X, \leq)$ is an ideally effective WQO for the given representations of X and $\mathit{Idl}(X)$,*
- *$(\mathit{Idl}(X), \subseteq)$ is an ideally effective WQO for the given representations of $\mathit{Idl}(X)$ and $\mathit{Idl}(\mathit{Idl}(X))$.*
- *The* flattening *function defined below is computable:*

$$\begin{cases} \mathit{Idl}(\mathit{Idl}(X)) & \to & \mathit{Idl}(X) \\ \boldsymbol{J} & \mapsto \bigcup & \boldsymbol{J} \end{cases}$$

The basic WQOs from Section 3.2 are examples of Idl^2-effective ω^2-WQOs.

- For a finite WQO $(X, \leq)$, ideals of X are isomorphic to X itself, and thus so are ideals of ideals. This proves that $(X, \leq)$ is an ω^2-WQO. We thus represent the three sets X, $\mathit{Idl}(X)$ and $\mathit{Idl}(\mathit{Idl}(X))$ using the same encoding, computability of set-theoretic operations then follow from the ideal effectiveness of finite WQOs. Finally, the flattening function is the identity.
- The set of ideals of an ordinal $(\boldsymbol{\alpha}, \leq)$ ordered with inclusion is isomorphic to $\boldsymbol{\alpha} + \mathbf{1}$. Therefore, the set of ideals of ideals of $\boldsymbol{\alpha}$ is isomorphic to $\boldsymbol{\alpha} + \mathbf{2}$, and $(\boldsymbol{\alpha}, \leq)$ is indeed a ω^2-WQO. According to Section 3.2.3, both $(\boldsymbol{\alpha}, \leq)$ and $(\boldsymbol{\alpha} + \mathbf{1}, \leq)$ are Idl^2-effective. For the flattening function, given a successor ordinal $\beta + 1 \in \boldsymbol{\alpha} + \mathbf{2}$, $\bigcup(\boldsymbol{\beta} + \mathbf{1}) = \boldsymbol{\beta}$, and given a limit ordinal $\lambda \in \boldsymbol{\alpha} + \mathbf{2}$, $\bigcup \boldsymbol{\lambda} = \boldsymbol{\lambda}$.

Next, we prove that when $(X, \leq)$ is an Idl^2-effective ω^2-WQO, $(X^\omega, \leq_\omega)$ is an ideally effective WQO. The previous definition has been designed to this end.

Proposition 9.4.2. *Let $(X, \leq)$ be an Idl^2-effective ω^2-WQO. Then $(\mathit{Down}(X), \subseteq)$, $(\mathcal{P}(X), \sqsubseteq_\mathcal{H})$ and $(X^\omega, \leq_\omega)$ are ideally effective WQOs.*

Proof. The ideal effectiveness of $(\mathit{Down}(X), \subseteq)$ follows from the isomorphism between the latter and $(\mathcal{P}_f(\mathit{Idl}(X)), \sqsubseteq_\mathcal{H})$, as a result of Section 7.3. In this same section, we have also argued that $(\mathcal{P}(X)/\equiv_\mathcal{H}, \sqsubseteq_\mathcal{H})$ is isomorphic to $(\mathit{Down}(X), \subseteq)$.

To establish the ideal effectiveness of $(X^\omega, \leq_\omega)$, we use Theorem 9.1.8. Obviously, $(X, \leq)$ is ideally effective, and $(\mathit{Down}(X), \subseteq)$ as well according to what precedes. Since we have shown that $(\mathit{Down}(X), \subseteq)$ is ideally effective using the standard representation for downward-closed sets (i.e. finite sets of ideals), the *transfer* function is trivial. Finally, we have to show that the following function is computable:

$$\begin{cases} \mathit{Idl}(\mathit{Down}(X)) & \to & \mathit{Down}(X) \\ \boldsymbol{J} & \mapsto & \bigcup \boldsymbol{J} \end{cases}$$

However, Definition 9.4.1 only provides the computability of this function:

$$\begin{cases} \mathit{Idl}(\mathit{Idl}(X)) & \to & \mathit{Idl}(X) \\ \boldsymbol{J} & \mapsto & \bigcup \boldsymbol{J} \end{cases}$$

Recall from Section 7.3 that ideals of $\mathit{Down}(X) \equiv \mathcal{P}_f(\mathit{Idl}(X))$ are of the form $\mathcal{P}_f(\boldsymbol{D})$ for $\boldsymbol{D} \in \mathit{Down}(\mathit{Idl}(X))$, and therefore simply encoded as elements of $\mathit{Down}(\mathit{Idl}(X))$. Let $\boldsymbol{J}$ be an actual ideal of $\mathit{Down}(X)$ (i.e. its semantic), and $\boldsymbol{D}$ be its representation (its syntax). Then, $\bigcup \boldsymbol{J} = \bigcup \boldsymbol{D}$. Indeed, $\boldsymbol{D}$ stands for $\mathcal{P}_f(\boldsymbol{D}) = \{E \in \mathcal{P}_f(\mathit{Idl}(X)) \mid E \subseteq D\}$, and an element $E \in \mathcal{P}_f(\mathit{Idl}(X))$ actually stands for $\bigcup E$, that is the downward-closed set obtained as the union of the ideals members of E. Therefore, $\boldsymbol{J} = \{\bigcup E \mid E \in \mathcal{P}_f(\mathit{Idl}(X)) \text{ and } E \subseteq D\}$.

Let $x \in \bigcup \boldsymbol{J}$, there exists a downward-closed set $F \in \mathit{Down}(X)$ such that $x \in F \in \boldsymbol{J}$. Therefore, x is in some ideal $I \in \mathit{Idl}(X)$ which appears in the canonical decomposition of F, and by definition, $I \in \boldsymbol{D}$. Thus $x \in I \in \boldsymbol{D}$, proving $\bigcup \boldsymbol{J} \subseteq \bigcup \boldsymbol{D}$.

For the other direction, let $x \in \boldsymbol{D}$, there exists $I \in \mathit{Idl}(X)$ such that $x \in I \in \boldsymbol{D}$. Therefore $\{I\} \subseteq \boldsymbol{D}$ and the downward-closed set I is a member of $\boldsymbol{J}$. It follows that $x \in I \in \boldsymbol{J}$ and $\bigcup \boldsymbol{D} \subseteq \bigcup \boldsymbol{J}$.

It now remains to prove that $\bigcup \boldsymbol{D}$ is computable. Remember $\boldsymbol{D} \in \mathit{Down}(\mathit{Idl}(X))$, and it therefore has an ideal decomposition $\boldsymbol{D} = \boldsymbol{I}_1 \cup \cdots \boldsymbol{I}_n$ for some $\boldsymbol{I}_1, \ldots, \boldsymbol{I}_n \in \mathit{Idl}(\mathit{Idl}(X))$. We can similarly prove $\bigcup \boldsymbol{D} = \bigcup_{i=1}^n \bigcup \boldsymbol{I}_i$, and given $\boldsymbol{I} \in \mathit{Idl}(\mathit{Idl}(X))$, $\bigcup \boldsymbol{I}$ is computable by Definition 9.4.1. □

We now want to show that our algebra of ideally effective WQOs is actually an algebra of Idl^2-effective ω^2-WQOs. In particular, this would imply that $(X^\omega, \leq_\omega)$ is ideally effective for every WQO $(X, \leq)$ in our algebra. Since we have shown that our basic WQOs introduced in Chapter 3 are Idl^2-effective ω^2-WQOs, it now suffices to show that each of the constructions introduced in the previous chapters not only preserve WQOs and ideal effectiveness, but also ω^2-WQOs and Idl^2-effectiveness.

Definition 9.4.3. *An order-theoretic WQO and ω^2-WQO-preserving construction C is said to be Idl^2*-effective *if, for every Idl^2-effective ω^2-WQOs $(X_1, \leq_1), \ldots, (X_n, \leq_n)$:*

- *$C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ is an Idl^2-effective ω^2-WQO, and*
- *Presentations of $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ and $Idl(C[(X_1, \leq_1), \ldots, (X_n, \leq_n)])$ are computable from presentations of the $(X_i, \leq_i)$ and the $(Idl(X_i), \subseteq)$ $(i = 1, \ldots, n)$.*
- *The flattening function for $C[(X_1, \leq_1), \ldots, (X_n, \leq_n)]$ is computable from flattening functions for the $(X_i, \leq_i)$ $(i = 1, \ldots, n)$.*

Theorem 9.4.4. *The following constructions are ω^2-WQO-preserving and Idl^2-effective:*

- *Disjoint Sum (Section 5.1),*
- *Lexicographic Sum (Section 5.2),*
- *Cartesian Product with Dickson's quasi-ordering (Section 5.3),*
- *Finite Sequences extension with Higman's quasi-ordering (Section 6.1),*
- *Finite Sequences extension with Stuttering quasi-ordering (Section 6.2),*
- *Finite Multisets extension with Embedding quasi-ordering (Section 7.1)*
- *Finite Powerset with Hoare quasi-ordering (Section 7.3),*

Proof. First, observe that proving that a construction C is ω^2-WQO-preserving and Idl^2-effective is equivalent to proving the conjunction of the following statements:

1. C is WQO-preserving.
2. C is ideally effective.
3. C is ω^2-WQO-preserving.
4. For every Idl^2-effective ω^2-WQOs $(X_1, \leq_1), \ldots, (X_n, \leq_n)$, $Idl(C[(X_1, \leq_1), \ldots, (X_n, \leq_n)])$ is an ideally effective WQO.
5. A presentation of $Idl(C[(X_1, \leq_1), \ldots, (X_n, \leq_n)])$ is computable from presentations of the $(X_i, \leq_i)$ and the $(Idl(X_i), \subseteq)$ $(i = 1, \ldots, n)$.
6. For every Idl^2-effective ω^2-WQOs $(X_1, \leq_1), \ldots, (X_n, \leq_n)$, the flattening function for $Idl(C[(X_1, \leq_1), \ldots, (X_n, \leq_n)])$ is computable.
7. A procedure for this flattening function is computable from procedures for the flattening functions for $(Idl(X_i), \subseteq)$ $(i = 1, \ldots, n)$.

For each of the constructions C mentioned in the theorem, the first two statements are already proved in the section dedicated to construction C. We therefore focus, for each construction, on proving statements three to seven. Statement three will always be proved by showing that $Idl(C[(X_1, \leq_1), \ldots, (X_n, \leq_n)])$ is a WQO when the $(X_i, \leq_i)$ are ω^2-WQOs. Statements five and seven will always be trivial from the rest, and we will not mention them.

Let $(X, \leq)$, $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be ideally effective ω^2-WQOs. In particular, $(Idl(X), \subseteq)$ and $(Down(X), \subseteq)$ are ideally effective.

Disjoint Sum: In Section 5.1 we have proved that the set $Idl(X_1 \sqcup X_2, \sqcup)$ ordered with inclusion is isomorphic to the disjoint sum of $Idl(X_1)$ and $Idl(X_2)$. Therefore, it is a WQO, and the disjoint sum construction is ω^2-WQO-preserving. Moreover, since $Idl(X_1)$ and $Idl(X_2)$ are ideally-effective, Section 5.1 proves that $(Idl(X_1 \sqcup X_2), \subseteq) \cong (Idl(X_1), \subseteq) \sqcup (Idl(X_2), \subseteq)$ is ideally effective as well. Finally, the flattening function for the sum simply is the sum of the flattening functions for X_1 and X_2: given an ideal of $Idl(Idl(X_1 \sqcup X_2))$, it is of the form $\langle i, \boldsymbol{I} \rangle$ for some $i \in \{1, 2\}$ and some $\boldsymbol{I} \in Idl(Idl(X_i))$. Therefore, $\bigcup \langle i, \boldsymbol{I} \rangle = \langle i, \bigcup \boldsymbol{I} \rangle$.

Lexicographic Sum: Here also, the lexicographic sum is ω^2-WQO-preserving and the ideal effectiveness of $Idl(X_1 \oplus X_2) \cong Idl(X_1 \ \subseteq) \oplus Idl(X_2, \subseteq)$ follows from Section 5.2. The flattening function is exactly the same as before, but keep in mind that the representation $\langle 2, \bigcup \boldsymbol{I} \rangle$ actually stands for the set $X_1 \cup \bigcup \boldsymbol{I}$.

Cartesian Product with Dickson's Quasi-Ordering: Again, Cartesian Product is ω^2-WQO-preserving and Idl^2-effective because this construction commutes with the ideal construction: $Idl(X_1 \times X_2) \cong Idl(X_1, \subseteq) \times Idl(X_2, \subseteq)$. For the flattening function: given $\boldsymbol{I} \in Idl(Idl(X_1))$ and $\boldsymbol{J} \in Idl(Idl(X_2))$, $\bigcup(\boldsymbol{I} \times \boldsymbol{J}) = (\bigcup \boldsymbol{I}) \times (\bigcup \boldsymbol{J})$.

Finite Sequences with Higman's Quasi-Ordering: In this case, the set $Idl(X^*)$ is in bijection with $(Idl(X) \sqcup Down(X))^*$, but inclusion on the former does not correspond to the natural quasi-ordering $\leq_* (\leq_\sqcup)$ on the latter, instead it corresponds to an extension of this natural QO.

The Atom Construction Preserves Ideal Effectiveness: We first deal with the atoms $Atm(X)$ (see Section 6.1 for the definition): the set of atoms is isomorphic to an extension of $(Idl(X) \sqcup Down(X), \subseteq_\sqcup)$. Actually, the atom $\emptyset^*$ can always be removed from an atom decomposition of an ideal of $Idl(X^*)$ (see Definition 6.1.11). We therefore work with $(Idl(X) \sqcup Down'(X), \subseteq_\sqcup)$ instead, where $Down'(X) \stackrel{\text{def}}{=} Down(X) \smallsetminus \{\emptyset\}$. Let $\sqsubseteq$ be the image of the inclusion quasi-ordering on the atoms of

X^* by the isomorphism above, that is:

$$\begin{aligned}
\langle 1, I\rangle \sqsubseteq \langle 1, J\rangle &\iff I + \epsilon \subseteq J + \epsilon && \iff I \subseteq J \\
\langle 1, I\rangle \sqsubseteq \langle 2, D\rangle &\iff I + \epsilon \subseteq D^* && \iff I \subseteq D \\
\langle 2, D\rangle \sqsubseteq \langle 2, D'\rangle &\iff D^* \subseteq D'^* && \iff D \subseteq D' \\
\langle 2, D\rangle \sqsubseteq \langle 1, I\rangle &\iff D^* \subseteq I + \epsilon && \text{which is never true } (D \neq \emptyset
\end{aligned}$$

With this notation, $(Atm(X), \subseteq)$ is isomorphic to $(Idl(X) \sqcup Down(X), \sqsubseteq)$. We show that the latter is ideally effective using Section 4.1, since $\subseteq_\sqcup\ \subseteq\ \sqsubseteq$: it suffices to show that function $\mathcal{C}l_\mathrm{F}$ and $\mathcal{C}l_\mathrm{I}$ are computable. To compute $\mathcal{C}l_\mathrm{F}$, use the following equations:

$$\begin{aligned}
\mathcal{C}l_\mathrm{F}(\langle 1, I\rangle) &= \uparrow_\sqcup\langle 1, I\rangle \cup \uparrow_\sqcup\langle 2, I\rangle \\
\mathcal{C}l_\mathrm{F}(\langle 2, D\rangle) &= \uparrow_\sqcup\langle 2, D\rangle
\end{aligned}$$

Regarding function $\mathcal{C}l_\mathrm{I}$, recall from Section 5.1 that the set of ideals of $(Idl(X) \sqcup Down(X), \leq_\sqcup)$ is the disjoint sum of the set of ideals of $Idl(X)$ and of the set of ideals of $Down(X)$, that is, an ideal of $(Idl(X) \sqcup Down(X), \leq_\sqcup)$ is either of the form $\langle 1, \boldsymbol{I}\rangle$ for $\boldsymbol{I} \in Idl(Idl(X))$ or of the form $\langle 2, \boldsymbol{J}\rangle$ for $\boldsymbol{J} \in Idl(Down(X))$. Note that $Down(X)$ is ideally effective according to Proposition 9.4.2.

We can now show that $\mathcal{C}l_\mathrm{I}$ is computable:

$$\begin{aligned}
\mathcal{C}l_\mathrm{I}(\langle 1, \boldsymbol{I}\rangle) &\stackrel{\text{def}}{=} \downarrow_\sqsubseteq\langle 1, \boldsymbol{I}\rangle = \langle 1, \boldsymbol{I}\rangle \\
\mathcal{C}l_\mathrm{I}(\langle 2, \boldsymbol{J}\rangle) &\stackrel{\text{def}}{=} \downarrow_\sqsubseteq\langle 2, \boldsymbol{J}\rangle = \langle 2, \boldsymbol{J}\rangle \cup \bigcup_{i=1}^{n}\langle 1, \boldsymbol{I}_i\rangle
\end{aligned}$$

where $\bigcup_{i=1}^n \boldsymbol{I}_i$ is the ideal decomposition of $\bigcup \boldsymbol{J}$ where $\boldsymbol{J}$ is seen as an ideal of $\mathcal{P}_f(Idl(X))$.

Let us argue the correctness and computability of the second equation. The ideal $\boldsymbol{J} \in Idl(Down(X))$ is actually encoded as an element of $Idl(\mathcal{P}_f(Idl(X)))$, according to our representation of downward-closed sets of X. Therefore, $\bigcup \boldsymbol{J} = \bigcup_{S \in \boldsymbol{J}} S$ is a downward-closed set of ideals of X, which admits a decomposition into ideals of ideals of X. This is precisely the decomposition $\bigcup_{i=1}^n \boldsymbol{I}_i$ we use in the equation above.

It remains to show that this particular decomposition can be computed from the actual encoding of $\boldsymbol{J}$. Remember from Section 7.3 that the ideals of $\mathcal{P}_f(Idl(X))$ are of the form $\mathcal{P}_f(\boldsymbol{D})$ for $\boldsymbol{D} \in Down(Idl(X))$, and therefore $\boldsymbol{J}$ is actually encoded as $\boldsymbol{D}$ (as in the proof of Proposition 9.4.2). We now prove that semantically, $\boldsymbol{D} = \bigcup_{S \in \boldsymbol{J}} S$, which concludes the proof since the ideal decomposition of $\boldsymbol{D}$ can be computed.

Let $I \in \boldsymbol{D}$, then $S \stackrel{\text{def}}{=} \{I\} \in \mathcal{P}_f(\boldsymbol{D}) = \boldsymbol{J}$ which proves that $I \in S \in \boldsymbol{J}$. Conversely, given some $I \in \boldsymbol{J}$, there exists some $S \in \boldsymbol{J} = \mathcal{P}_f(\boldsymbol{D})$ such that $I \in S \subseteq \boldsymbol{D}$. Therefore, $I \in \boldsymbol{D}$.

In conclusion, functions $\mathcal{C}l_\mathrm{I}$ and $\mathcal{C}l_\mathrm{F}$ being computable, $(Atm(X), \sqsubseteq)$ is ideally effective.

Back to the Idl^2-effectiveness of X^*, the ideals of X^* are finite sequences of atoms. Unfortunately, the quasi-ordering on these sequences does not coincide with one of the three quasi-ordering on X^* that we have shown to be ideally effective. Indeed, when embedding a sequence of atoms into another, we are allowed to stutter (in the sense of Section 6.2) on atoms of the form $\langle 2, D\rangle$ for $D \in \mathit{Down}(X)$, but not on atoms of the form $\langle 1, I\rangle$ for $I \in \mathit{Idl}(X)$. Hence, we introduce a quasi-ordering on sequences which generalizes both the Higman quasi-ordering and the stuttering quasi-ordering. We call it the *partial stuttering quasi-ordering*, and we now show that it is an ideally effective construction (for any ideally effective WQO $(X, \leq)$, not only for atoms, which is the case we are ultimately interested in).

The Partial Stuttering Quasi-Ordering is Ideally Effective: Given an ideally effective WQO $(X, \leq)$ and an upward-closed set $A \subseteq X$, define the *partial stuttering quasi-ordering on A* by:

$$x_1 \cdots x_n \leq_{\mathrm{st}}^A y_1 \cdots y_m \overset{\text{def}}{\Leftrightarrow} \exists f : [n] \to [m].\ \forall i \in [n].\ x_i \leq y_{f(i)}$$
$$\text{and } \forall i \neq j \in [n].\ f(i) = f(j) \Rightarrow y_{f(i)} \in A.$$

This QO generalizes both the Higman quasi-ordering (from Section 6.1) and the stuttering quasi-ordering (from Section 6.2): if $A = \emptyset$, then $\leq_{\mathrm{st}}^A = \leq_*$ and when $A = X$, $\leq_{\mathrm{st}}^A = \leq_{\mathrm{st}}$. In all generality, the following holds: $\leq_* \subseteq \leq_{\mathrm{st}}^A \subseteq \leq_{\mathrm{st}}$. In particular, this QO is an extension of $\leq_*$, and we can use Section 4.1 to prove it ideally effective.

Since A is upward-closed, $\leq_{\mathrm{st}}^A$ is transitive: it suffices to compose the witnesses of the embeddings. Moreover, it is also still possible to concatenate witnesses, that is if $u \leq_{\mathrm{st}}^A u'$ and $v \leq_{\mathrm{st}}^A v'$ then $u \cdot v \leq_{\mathrm{st}}^A u' \cdot v'$ ($\leq_{\mathrm{st}}^A$ is *compatible* with concatenation). In particular, it is still the case that $(\downarrow_{\mathrm{st}}^A \boldsymbol{P}_1) \cdot (\downarrow_{\mathrm{st}}^A \boldsymbol{P}_2) = \downarrow_{\mathrm{st}}^A (\boldsymbol{P}_1 \cdot \boldsymbol{P}_2)$, for $\boldsymbol{P}_1, \boldsymbol{P}_2$ ideals of $(X^*, \leq_*)$. Therefore, it only remains to compute $\mathcal{C}l_{\mathrm{I}}$ on atoms.

$$\begin{aligned} \mathcal{C}l_{\mathrm{I}}(I + \epsilon) &= I^* && \text{when } I \cap A \neq \emptyset \\ \mathcal{C}l_{\mathrm{I}}(I + \epsilon) &= I + \epsilon && \text{otherwise} \\ \mathcal{C}l_{\mathrm{I}}(D^*) &= D^* \end{aligned}$$

Proof. If $A \cap I \neq \emptyset$ then:

- $\downarrow_{\mathrm{st}}^A I \subseteq I^*$: if $\boldsymbol{u} \leq_{\mathrm{st}}^A \boldsymbol{x}$ for some $x \in I$, then $\boldsymbol{u} \in (\downarrow x)^* \subseteq I^*$. The case $\boldsymbol{u} \leq_{\mathrm{st}}^A \epsilon$ is trivial.
- $I^* \subseteq \downarrow_{\mathrm{st}}^A I$: given $\boldsymbol{u} \in I^*$, since $\boldsymbol{u}$ is finite and I is directed, we can find $x \in I$ such that x is greater than every element of $\boldsymbol{u}$. Moreover, since I is directed, there exists $z \in I$ which is greater than all elements of $\boldsymbol{u}$ (greater than x) and which is in A (pick any $y \in A \cap I$). It satisfies $\boldsymbol{u} \leq_{\mathrm{st}}^A \boldsymbol{z}$.

If $A \cap I = \emptyset$ then: for any $\boldsymbol{u} \leq_{\mathrm{st}}^A \boldsymbol{x}$ for some $x \in I$, since $x \notin A$, $|\boldsymbol{u}| \leq 1$ and therefore $\boldsymbol{u} = \epsilon$, or $\boldsymbol{u} = \boldsymbol{y}$ for $y \leq x \in I$. The other inclusion is trivial. So is the third equation. □

Observe that the condition $I \cap U \neq \emptyset$ for $I \in \mathit{Idl}(X)$ and $U \in \mathit{Up}(X)$ is decidable. Indeed, $I \cap \uparrow x \neq \emptyset \iff x \in I$: the right-to-left direction is trivial, and if there exists $y \in I \cap \uparrow x$, then $x \leq y \in I$ which implies $x \in I$ since I is downward-closed.

Emptiness of the intersection with an upward-closed is then tested by distributing the intersection over the unions. Therefore, $\mathcal{C}l_{\mathrm{I}}$ is computable.

As in Section 6.2, function $\mathcal{C}l_{\mathrm{F}}$ is more complicated: let $\boldsymbol{u} = x_1 \cdots x_n$,

$$\mathcal{C}l_{\mathrm{F}}(\boldsymbol{u}) \;=\; \uparrow_{\mathrm{st}} \boldsymbol{u} \;=\; \uparrow_{*} \left\{ y_1 \cdots y_k \;\middle|\; \begin{array}{c} 0 \leq k \leq n \\ 0 = i_0 < i_1 < \cdots < i_k = n \\ \forall j \in [k].\ y_i \in \min(\bigcap_{i_{j-1} < \ell \leq i_j} \uparrow_X x_\ell) \\ \forall j \in [k].\ (i_j = i_{j-1} + 1 \vee y_j \in A) \end{array} \right\}$$

Remember the intuition given in Section 6.2: if $\boldsymbol{u} \leq_{\mathrm{st}} bw$, we can extract the image $\boldsymbol{v} = y_1 \cdots y_k$ of an embedding witnessing $\boldsymbol{u} \leq_{\mathrm{st}} \boldsymbol{w}$ ($\boldsymbol{v}$ is a subsequence of $\boldsymbol{w}$). This induces a factorization $\boldsymbol{u} = \boldsymbol{u}_1 \cdots \boldsymbol{u}_k$ of $\boldsymbol{u}$ where $\boldsymbol{u}_i \leq_{\mathrm{st}} y_i$ for all $i \in [k]$. Now for $\leq_{\mathrm{st}}^{A}$, we must also ensures that either $y_i \in A$ (it can embeds several elements), or $|\boldsymbol{u}_i| = 1$. The proof is left to the reader.

In conclusion, $\mathcal{C}l_{\mathrm{F}}$ is computable as well, which proves that $(X^*, \leq_{\mathrm{st}}^{A})$ is ideally effective for any $A \in \mathit{Up}(X)$ whenever $(X, \leq)$ is ideally effective. In our case, $(\mathit{Idl}(X^*), \subseteq)$ is isomorphic to $(\mathit{Atm}(X)^*, \leq_{\mathrm{st}}^{\langle 2, \mathit{Down}'(X) \rangle})$, where as expected, $\langle 2, \mathit{Down}'(X) \rangle$ designates $\{\langle 2, D \rangle \mid D \in \mathit{Down}'(X)\} \in \mathit{Up}(\mathit{Atm}(X))$. The latter is ideally-effective according to what precedes.

To establish the Idl^2-effectiveness of $(X^*, \leq_*)$, it remains to prove the computability of the flattening function. Let $\boldsymbol{\mathcal{P}} \in \mathit{Idl}(\mathit{Idl}(X^*))$. It is encoded as an ideal of $(\mathit{Atm}(X)^*, \leq_{\mathrm{st}}^{\langle 2, \mathit{Down}'(X) \rangle})$. These ideals are themselves encoded as sequences of some particular atoms of $\mathit{Atm}(X)$, which we will subsequently call *higher atoms*. Given $\boldsymbol{I} \in \mathit{Idl}(\mathit{Idl}(X))$, then $\langle 1, \boldsymbol{I} \rangle \in \mathit{Idl}(\mathit{Atm}(X))$ and $\langle 1, \boldsymbol{I} \rangle + \epsilon$ is a higher atom. If $\boldsymbol{D} \in \mathit{Down}(\mathit{Idl}(X))$, then $\langle 1, \boldsymbol{D} \rangle \in \mathit{Down}(\mathit{Atm}(X))$ and $\langle 1, \boldsymbol{D} \rangle^*$ is a higher atom. Lastly, given $\boldsymbol{E} \in \mathit{Down}(\mathit{Down}(X))$, $\langle 2, \boldsymbol{E} \rangle \in \mathit{Down}(\mathit{Atm}(X))$ and $\langle 2, \boldsymbol{E} \rangle^*$ is a higher atom. Moreover, these are the only types of higher atoms.

Now, any $\boldsymbol{\mathcal{P}} \in \mathit{Idl}(\mathit{Idl}(X^*))$ is encoded as a product $\boldsymbol{\mathcal{A}}_1 \cdots \boldsymbol{\mathcal{A}}_n$ of higher atoms, and the flattening of $\boldsymbol{\mathcal{P}}$ is the product of flattening of its higher atoms:

$$\bigcup \boldsymbol{\mathcal{P}} = (\bigcup \boldsymbol{\mathcal{A}}_1) \cdots (\bigcup \boldsymbol{\mathcal{A}}_n)$$

It thus remain to prove that the flattening of higher atoms is computable. Let $\boldsymbol{\mathcal{A}}$ be an higher atom.

- If $\boldsymbol{\mathcal{A}} = \langle 1, \boldsymbol{I} \rangle + \epsilon$, then $\bigcup \boldsymbol{\mathcal{A}} = \langle 1, \bigcup \boldsymbol{I} \rangle$.
- If $\boldsymbol{\mathcal{A}} = \langle 1, \boldsymbol{D} \rangle^*$, then $\bigcup \boldsymbol{\mathcal{A}} = \langle 1, \bigcup \boldsymbol{D} \rangle^*$. Indeed, if $\boldsymbol{u} \in \bigcup \boldsymbol{\mathcal{A}}$ then there exists some ideals $I_1, \ldots, I_n \in \boldsymbol{D} \subseteq \mathit{Idl}(X)$ for $n = |u|$ such that $\boldsymbol{u} \in (I_1 + \epsilon) \cdots (I_n + \epsilon)$. But since for every i, $I_i \subseteq \bigcup \boldsymbol{D}$, $\boldsymbol{u} \in (\bigcup \boldsymbol{D})^*$.

  Conversely, let $\boldsymbol{u} = x_1 \cdots x_n \in (\bigcup \boldsymbol{D})^*$. In particular, for each i, $x_i \in \bigcup \boldsymbol{D}$, and there exists an ideal such that $x_i \in I_i \in \boldsymbol{D}$. Therefore, $\boldsymbol{u} \in (I_1 + \epsilon) \cdots (I_n + \epsilon) \in \langle 1, \boldsymbol{D} \rangle^*$.

  Besides, we can compute $\boldsymbol{D} = \boldsymbol{I}_1 \cup \cdots \cup \boldsymbol{I}_m$ the ideal decomposition of $\boldsymbol{D}$, with $\boldsymbol{I}_i \in \mathit{Idl}(\mathit{Idl}(X))$, and we have

$$\bigcup \boldsymbol{D} = (\bigcup \boldsymbol{I}_1) \cup \cdots \cup (\bigcup \boldsymbol{I}_m)$$

This last expression is computable using the flattening function for $\mathit{Idl}(\mathit{Idl}(X))$.

- Lastly, if $\boldsymbol{\mathcal{A}} = \langle 2, \boldsymbol{E} \rangle^*$ for some $\boldsymbol{E} \in \mathit{Down}(\mathit{Down}(X))$, then $\bigcup \boldsymbol{\mathcal{A}} = \langle 2, \bigcup \boldsymbol{E} \rangle^*$. The proof is similar to the previous one. Besides, the expression $\bigcup \boldsymbol{E}$ for $\boldsymbol{E} \in \mathit{Down}(\mathit{Down}(X))$ has already been shown computable in Proposition 9.4.2.

Finite Sequences with Stuttering: In this case, $\mathit{Idl}(X^*, \leq_{\mathrm{st}})$ is isomorphic to $(\mathit{Down}(X)^*, \subseteq_{\mathrm{st}})$. which is ideally effective since $(\mathit{Down}(X), \subseteq)$ is (cf. Section 6.2).

Note that the quasi-ordering $\leq_{\mathrm{st}}^A$ on X^* introduced in the previous paragraph generalizes both $\leq_*$ $(A = \emptyset)$ and $\leq_{\mathrm{st}}$ $(A = X)$. Therefore, the Idl^2-effectiveness of these two constructions follows from the Idl^2-effectiveness of $(X^*, \leq_{\mathrm{st}}^A)$, which can be proved following the lines of the previous case.

Finite Multisets with the Embedding Quasi-Ordering: In this case, $\mathit{Idl}(X^{\circledast}, \leq_{\mathrm{emb}})$ is isomorphic to an extension of $(\mathit{Idl}(X)^{\circledast} \times \mathit{Down}(X), \leq_{\times})$. The latter is ideally effective according to Sections 5.3 and 7.1. We show that its extension is ideally effective using Section 4.1.

Let $\sqsubseteq$ denotes the image of $\subseteq$ by the function that maps an ideal $\boldsymbol{I} \in \mathit{Idl}(X^{\circledast})$ to $\langle \boldsymbol{B}, D \rangle \in \mathit{Idl}(X)^{\circledast} \times \mathit{Down}(X)$ where $\boldsymbol{I} = {\downarrow_{\in}} \boldsymbol{B} \oplus D^{\circledast}$, that is:

$$\langle \boldsymbol{B}, D \rangle \sqsubseteq \langle \boldsymbol{C}, E \rangle \overset{\text{def}}{\Leftrightarrow} \boldsymbol{B} \smallsetminus E \subseteq_{\mathrm{emb}} \boldsymbol{C} \wedge D \subseteq E$$

Function $\mathcal{C}l_{\mathrm{F}}$ is easily seen computable: given $\langle \boldsymbol{B}, D \rangle$ an ideal of $(\mathit{Idl}(X)^{\circledast} \times \mathit{Down}(X), \leq_{\times})$,

$$\mathcal{C}l_{\mathrm{F}}(\langle \boldsymbol{B}, D \rangle) = \bigcup_{\boldsymbol{C} \subset \boldsymbol{B}} \uparrow_{\times} \langle \boldsymbol{C}, D \cup {\downarrow} \mathit{Supp}(\boldsymbol{B} - \boldsymbol{C}) \rangle$$

For function $\mathcal{C}l_{\mathrm{I}}$: recall from Section 5.3 that ideals of $(\mathit{Idl}(X)^{\circledast} \times \mathit{Down}(X), \leq_{\times})$ are pairs of ideals of $\mathit{Idl}(X)^{\circledast}$ and of ideals of $\mathit{Down}(X)$. Using the results of Section 7.1, the ideals of $\mathit{Idl}(X)^{\circledast}$ are of the form ${\downarrow_{\in}} \boldsymbol{\mathcal{B}} \oplus \boldsymbol{D}^{\circledast}$ for $(\boldsymbol{\mathcal{B}}, \boldsymbol{D}) \in \mathit{Idl}(\mathit{Idl}(X))^{\circledast} \times \mathit{Down}(\mathit{Idl}(X))$. Let $\langle {\downarrow_{\in}} \boldsymbol{\mathcal{B}} \oplus \boldsymbol{D}^{\circledast}, \boldsymbol{I} \rangle$ be an ideal of $(\mathit{Idl}(X)^{\circledast} \times \mathit{Down}(X), \leq_{\times})$:

$$\mathcal{C}l_{\mathrm{I}}(\langle {\downarrow_{\in}} \boldsymbol{\mathcal{B}} \oplus \boldsymbol{D}^{\circledast}, \boldsymbol{I} \rangle) = \langle {\downarrow_{\in}} \boldsymbol{\mathcal{B}} \oplus (\boldsymbol{D} \cup {\downarrow_{\subseteq}} \{I_1, \ldots, I_n\})^{\circledast}, \boldsymbol{I} \rangle$$

where $I_1 \cup \cdots \cup I_n$ is a decomposition of the downward-closed set $\bigcup \boldsymbol{I}$, and ${\downarrow_{\subseteq}}$ here designates the downward-closure of a set of ideals within $\mathit{Down}(\mathit{Idl}(X))$, i.e. ${\downarrow_{\subseteq}} \boldsymbol{S} = \{I \in \mathit{Idl}(X) \mid \exists J \in \boldsymbol{S}.\ I \subseteq J\}$. It has been shown before that the expression $\bigcup \boldsymbol{I}$ is computable for $\boldsymbol{I} \in \mathit{Idl}(\mathit{Down}(X))$.

Proof. Let $\boldsymbol{B} \in {\downarrow_{\in}} \boldsymbol{\mathcal{B}} \oplus \boldsymbol{D}^{\circledast} \subseteq \mathit{Idl}(X)^{\circledast}$ and $D \in \boldsymbol{I} \subseteq \mathit{Down}(X)$, so that ${\downarrow_{\in}} \boldsymbol{B} \oplus D^{\circledast}$ is an element of $\mathit{Idl}(X^{\circledast})$. Let ${\downarrow_{\in}} \boldsymbol{C} \oplus E^{\circledast} \subseteq {\downarrow_{\in}} \boldsymbol{B} \oplus D^{\circledast}$ be a smaller ideal. Then by Proposition 7.1.6, $\boldsymbol{C} \smallsetminus \mathit{Down}(D) \subseteq_{\mathrm{emb}} \boldsymbol{B}$ and $E \subseteq D$. Let $I_1 \cup \cdots \cup I_n$ be the ideal decomposition of the downward-closed set $\bigcup \boldsymbol{I}$. Since $\boldsymbol{C}$ is a multiset of ideals, $\boldsymbol{C} \smallsetminus \mathit{Down}(D) = \boldsymbol{C} \smallsetminus \mathit{Idl}(D)$. Indeed, remember that since D is downward-closed, its ideals are exactly the ideals of X that are subsets of D. Moreover, since $D \in \boldsymbol{I}$, then $D \subseteq \bigcup \boldsymbol{I} = I_1 \cup \cdots \cup I_n$. That is, $\mathit{Idl}(D) \subseteq {\downarrow_{\subseteq}} \{I_1, \ldots, I_n\}$. Hence, $\boldsymbol{C} \in {\downarrow_{\in}} \boldsymbol{\mathcal{B}} \oplus (\boldsymbol{D} \cup {\downarrow_{\subseteq}} \{I_1, \ldots, I_n\})^{\circledast}$ and obviously $E \in \boldsymbol{I}$.

The other inclusion is clear. $\square$

Regarding the flattening function: let $\mathcal{J} \in Idl(Idl(X^{\circledast}))$. It is encoded as $\langle \downarrow_{\in} \mathcal{B} \oplus \boldsymbol{D}^{\circledast}, \boldsymbol{I} \rangle$ where $\mathcal{B} \in Idl(Idl(X))^{\circledast}$, $\boldsymbol{D} \in Down(Idl(X))$ and $\boldsymbol{I} \in Idl(Down(X))$.

We claim that:

$$\bigcup \mathcal{J} = \downarrow_{\in} \{\!| \bigcup \boldsymbol{I}_1, \ldots, \bigcup \boldsymbol{I}_n |\!\} \oplus (\bigcup \boldsymbol{D} \cup \bigcup \boldsymbol{I})^{\circledast}$$

where $\mathcal{B} = \{\!| \boldsymbol{I}_1, \ldots, \boldsymbol{I}_n |\!\}$, for some $\boldsymbol{I}_1, \ldots, \boldsymbol{I}_n \in Idl(Idl(X))$.

Indeed, let $M \in \bigcup \boldsymbol{J}$, there exists an ideal of $X^{\circledast}$ $\downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast} \in \boldsymbol{J}$ such that $M \in \downarrow_{\in} \boldsymbol{B} \oplus D^{\circledast}$. By definition of $\mathcal{J}$, $D \in \boldsymbol{I}$ and $\boldsymbol{B} \in \downarrow_{in} \mathcal{B} \oplus \boldsymbol{D}^{\circledast}$. Decompose $M = M_1 + M_2$ with $M_1 \in_{\text{emb}} \boldsymbol{B}$ and $M_2 \in D^{\circledast}$. Firstly, since $D \in \boldsymbol{I}$, $M_2 \in \bigcup \boldsymbol{I}$. Secondly, decompose $\boldsymbol{B} = \boldsymbol{B}_1 + \boldsymbol{B}_2$ with $\boldsymbol{B}_1 \in_{\text{emb}} \mathcal{B}$ and $\boldsymbol{B}_2 \in \boldsymbol{D}^{\circledast}$. Further decompose $M_1 = M_1' + M_1''$ such that $M_1' \in_{\text{emb}} \boldsymbol{B}_1$ and $M_1'' \in_{\text{emb}} \boldsymbol{B}_2$. Composing embeddings that witness $M_1' \in_{\text{emb}} \boldsymbol{B}_1$ and $\boldsymbol{B}_1 \in_{\text{emb}} \mathcal{B}$, it follows that $M_1' \in \{\!| \bigcup \boldsymbol{I}_1, \ldots, \bigcup \boldsymbol{I}_n |\!\}$. Indeed, if an element $x \in M_1'$ belongs to an ideal $I \in \boldsymbol{B}_1$, which itself belongs to an ideal of ideals $\boldsymbol{J} \in \mathcal{B}$, then $x \in \bigcup \boldsymbol{J}$.

Finally, for every $x \in M_1''$, there exists an ideal $I \in \boldsymbol{B}_2$ such that $x \in I$, and since $\boldsymbol{B}_2 \in \boldsymbol{D}^{\circledast}$, $I \in \boldsymbol{D}$. Therefore $x \in \bigcup \boldsymbol{D}$ and $M_1'' \in (\bigcup \boldsymbol{D})^{\circledast}$.

Conversely, let $M = M_1 + M_2 + M_3$ with $M_1 \in_{\text{emb}} \{\!| \bigcup \boldsymbol{I}_1, \ldots, \bigcup \boldsymbol{I}_n |\!\}$ and $M_2 \in (\bigcup \boldsymbol{D})^{\circledast}$ and $M_3 \in (\bigcup \boldsymbol{I})^{\circledast}$. Let $k = |M_1| \le n$, write $M_1 = \{\!| x_1 \cdots x_k |\!\}$ such that for every $i \in [k]$, $x_i \in \bigcup \boldsymbol{I}_i$. Thus, for each i, there exists $I_i \in \boldsymbol{I}_i$ such that $x_i \in I_i$. Define I_j to be an arbitrary ideal of $\boldsymbol{I}_j$ for $j \in [k+1, n]$, and define $\boldsymbol{B} = \{\!| I_1, \ldots, I_n |\!\}$. We have $M_1 \in_{\text{emb}} \boldsymbol{B} \in_{\text{emb}} \mathcal{B}$.

Moreover, let $M_2 = \{\!| y_1 \cdots y_\ell |\!\}$ and $\boldsymbol{B}' = \{\!| \downarrow y_1, \ldots, \downarrow y_\ell |\!\} \in (Idl(X))^{\circledast}$. Since $M_2 \in (\bigcup \boldsymbol{D})^{\circledast}$, $\boldsymbol{B}' \in \boldsymbol{D}^{\circledast}$, and $\boldsymbol{B} + \boldsymbol{B}' \in \downarrow_{\in} \mathcal{B} \oplus \boldsymbol{D}^{\circledast}$. Finally, we can similarly prove that there exists $D \in \boldsymbol{I} \subseteq Down(X)$ such that $M_3 \in D^{\circledast}$, ultimately proving that $M \in \bigcup \mathcal{J}$.

Finite Powerset with Hoare Quasi-Ordering: In this case, $Idl(\mathcal{P}_f(X), \subseteq)$ is isomorphic to $(Down(X), \subseteq)$, which has been shown to be ideally effective in Proposition 9.4.2. The computability of the flattening function has also been proved there.

□

Unfortunately, we did not finish our investigation in time to include all the results in this manuscript, but we have recently obtained that:

- Under extra assumptions, $(X, \le')$ is Idl^2-effective when $(X, \le)$ is, where $\le \subseteq \le$.
- These extra assumptions are met in the case of $(X^*, \le_{\text{cj}})$ which is thus Idl^2-effective.
- The domination ordering on finite multisets is also Idl^2-effective.

Remark 9.4.5. *As the reader may have noticed, constructions that "commute" with the ideal constructions are particularly easy to show Idl^2-effective. For instance, for the cartesian product, $Idl(X_1 \times X_2) = Idl(X_1) \times Idl(X_2)$ and therefore, the Idl^2-effectiveness comes for free with the ideal-effectiveness.*

In the case of sequences, we have seen that ideals of X^* are some kind of "higher" sequences as well, but the ordering on these sequences is not the classical embedding ordering. Therefore, we introduced a quasi-ordering $\leq_{\mathrm{st}}^A$ on sequences that generalizes the Higman quasi-ordering, and that almost commutes with the ideal construction. In particular, Chapter 6 should have presented $(X^*, \leq_{\mathrm{st}}^A)$ first, and proved its ideal effectiveness. Then, the ideal effectiveness of $(X^*, \leq_*)$ and $(X^*, \leq_{\mathrm{st}})$ would have been obtained as a corollary.

The answer to the Idl^2-effectiveness of extensions ($\leq \subseteq \leq'$, see Section 4.1) follows a similar path: the ideals of $(X, \leq')$ is not an extension of the ideals of $(X, \leq)$, essentially because the support of the QO is not the same: $Idl(X, \leq) \neq Idl(X, \leq')$. What we found to be the good notion that generalizes extensions is the setting where there exists a surjective and monotone function $f : (X, \leq_X) \to (Y, \leq_Y)$. In this case, $(X, \leq_X)$ is ideally effective, and functions $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ (similar definitions) are computable, then $(Y, \leq_Y)$ is ideally effective. Moreover, it is now possible to show that this setting is preserved under the ideal construction: the existence of f always imply the existence of a surjective and monotone map $g : Idl(X, \leq_X) \to Idl(Y, \leq_Y)$. Thanks to this more general notion, we were able to show that $(X^*, \leq_{\mathrm{cj}})$ is Idl^2-effective.

9.5 Perspectives

In conclusion, we have provided an effective algebra of ideally effective ω^2-WQOs, whose set-theoretic operations in these ω^2-WQOs can be automatically computed. Most of the commonly used WQOs fall in this algebra, but this inductive approach becomes particularly handy for WQOs that consist of a high number of iterations of these constructions. This is for instance the case of the quasi-ordering used for *priority channel systems* [47], which essentially is the n-th iteration of Higman's extension of the one element WQO, for a fixed $n \in \mathbb{N}$.

Note that this algebra is not closed under taking infinite sequences. Indeed, this construction is not Idl^2-effective as it does not even preserve ω^2-WQOs. However, given any quasi-ordering in this algebra, the set of infinite sequences over this WQO is ideally effective, and procedures for set-theoretic operations can be computed. The same can be said for taking the powerset $(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ of a quasi-ordering in this algebra. This has applications in verification: some algorithms to verify WSTS [48, 49] rely on $(\mathcal{P}(X), \sqsubseteq_{\mathcal{H}})$ being an effective WQO. Also in [29], the authors define the *completion* of a WSTS which is a transition system whose states are the ideals of the original set of states. For this system to be well-structured, we need that the original WQO is ω^2-WQO, and to apply e.g. forward analysis, it is crucial that $Idl(X)$ be an ideally effective WQO.

Extending the Algebra One of the most natural extension of our work would be to add more classical constructions to our algebra, the most relevant being trees and graphs. In these two cases, the objects at hand are more complex, and therefore so are the ideals, and a fortiori operations manipulating them. Already characterizing the structure of the ideals is difficult, and finding convenient representations becomes tough as well. Moreover, there are several classes of trees to consider, each of which can be quasi-ordered with several variants (bounded/unbounded width, bounded/unbounded height, ranked/unranked trees, etc.). The case of graphs is no simpler: already the minor relation is not simple to manipulate, and in practice many variants of this quasi-ordering are used, that are sometimes only WQOs on certain classes of graphs.

In conclusion, a complete investigation of these two cases would be long and difficult, and the results would be quite technical. In the case of trees, some cases have been shown effective (in some sense close to ours) in [13] and [30] for instance.

Infinite Sequences. If we want the infinite sequences construction to be part of our algebra, we need a class of WQOs that is preserved by this construction. Section 9.1 shows that this is the same as being preserved by the construction $Down$. From Proposition 9.3.4 we deduce that the smallest such class is that of α-WQOs for $\alpha < \omega^\omega$.

This motivates the following inductive definition:

Definition 9.5.1. *Given $n \in \mathbb{N}$, $(X, \leq)$ is Idl^n-WQO if:*

- *$(X, \leq)$ is ω^n-WQO,*
- *$(X, \leq)$ is an ideally effective WQO,*
- *$(Idl(X), \subseteq)$ is Idl^{n-1}-effective,*
- *The representation of ideals of X coincides in the two lines above.*
- *The flattening function from $Idl(Idl(X))$ to $Idl(X)$ is computable.*

$(X, \leq)$ is Idl^ω-effective if it is Idl^n-effective for every $n \in \mathbb{N}$.

Note that from Proposition 9.3.4, it is simple to derive that if $(X, \leq)$ is ω^n-WQO, then $Idl^n(X)$ is a WQO, where $Idl^n(X)$ is the n-th composition of the ideal completion of X. Note that X ω^ω-WQO is not equivalent to X being ω^n-WQO for every n. Indeed, Proposition 9.3.4 shows that if X is ω^n-WQO for every n, then so is $Idl(X)$. However, $Idl(X)$ is ω^ω-WQO if and only if X is $\omega^{\omega+1}$-WQO. Therefore, the two conditions are not equivalent since it is proved in [45] that α-WQO and β-WQO are two different notions when α and β are two distinct indecomposable countable ordinals.

However, for our purpose, being ω^n-WQO for every $n \in \mathbb{N}$ seems sufficient: it allows any finite number of application of the infinite sequences construction to a WQO of our algebra, provided all of our constructions are Idl^n-effective (similar definition)

Disjoint and lexicographic sums, and cartesian products are obviously Idl^ω effective. But this is less clear for finite sequences for instance, since $Idl(X^*)$ is not directly expressible with our constructions (we had to use an extension).

A promising first step would be to generalize Section 4.1 to Idl^n-effective WQOs. Does assuming the computability of $\mathcal{C}l_{\mathrm{I}}$ and $\mathcal{C}l_{\mathrm{F}}$ at the first level is enough to show that an extension is still Idl^n-effective, or do we need such functions for each level $Idl^m(X)$ for $m \leq n$?

Ideally Effective BQOs. What about a notion of effectiveness for BQOs? The characterization X ω^n-WQO if and only if $Idl^n(X)$ WQO is convenient to inductively define Idl^n-effectiveness. But does it generalizes further ? There is a classical definition of the transfinitely iterated powerset $\mathcal{P}^\alpha(X)$ in BQO theory, which can be adapted to $Idl^\alpha(X)$, and it is well known that X is BQO if and only if $\mathcal{P}^{\omega_1}(X)$ is WQO. However, we did not find any layered version of this theorem, that is: X $\omega^{\alpha+1}$-WQO if and only if $\mathcal{P}^\alpha(X)$ WQO. With such a property, we could for instance define Idl^α-effectiveness as $Idl^\beta(X)$ being ideally effective for every $\beta \leq \alpha$. It would probably also be necessary to assume that representations used for each $Idl^\beta(X)$ are compatible, in the sense that the representation for ideals of $Idl^\beta(X)$ is the same as the representation for the elements of $Idl^{\beta+1}(X)$; and to have some uniformity assumptions of the form: the function that to $\beta \in \boldsymbol{\alpha}$ associates a full presentation of $Idl^\beta(X)$ is computable.

Minimality of the Definition Is Definition 9.4.1 minimal ? Does there exists a ω^2-WQO $(X, \leq)$ such that $(Idl(X), \subseteq)$ is not ideally effective ? A starting point would be to investigate the domination ordering on finite multisets or the lexicographic product, since we were unable to prove these constructions to be Idl^2-effective.

Part II

First-Order Logic over an Ideally Effective WQOs

Joint work with Ph. Schnoebelen and G. Zetzsche

Results on the expressiveness and decidability of first-order theories, and in particular first-order theories over some fixed structure abound. One of the simplest structures one can think of are quasi-ordered sets, and indeed many such structures have been studied in the last decades (see [50, 51, 52, 53, 54, 55, 56] and references therein). In the following chapters, we investigate first-order logics over well quasi-ordered sets. More precisely, given a WQO $(X, \leq)$, we consider the first-order logic with $\leq$ as the only predicate, denoted $\mathsf{FO}(X, \leq)$, where $\leq$ is interpreted as the quasi-ordering $\leq$ over X. We can for instance express the following properties:

- $\forall x, y, z.\ x \leq y \land y \leq z \to x \leq z$. This expresses that $\leq$ is transitive, which is true for any QO $(X, \leq)$
- $\forall x, y.\ \exists u.\ x \leq u \land y \leq u \land [\forall z.\ (x \leq z \land y \leq z) \to u \leq z]$. This expresses that $(X, \leq)$ is a semi-lattice. This formula is for instance satisfied on the structure $(\mathbb{N}^k, \leq_\times)$ but not on $(A^*, \leq_*)$.
- $\exists x, y, z, u, v, w.\ x \leq u \land x \leq v \land x \not\leq w \land y \leq u \land y \not\leq v \land y \leq w \land z \not\leq u \land z \leq v \land z \leq w \land x \perp y \land x \perp z \land y \perp z \land u \perp v \land u \perp w \land v \perp w$, where $x \perp y$ is an abbreviation for $x \not\leq y \land y \not\leq x$. This formula expresses that some finite ordering embeds into $(X, \leq)$. For instance, this particular finite ordering does not embed into $\mathbb{N}^2$, but does embed into $\mathbb{N}^k$ for $k \geq 3$.

We also consider formulas that include constants from X, that is we consider the first-order theory with $\leq$ as the only predicate, and a (potentially infinite) set of constants $\mathtt{X}$, interpreted over X. This logic will be denoted $\mathsf{FO}(X, \leq, \mathtt{X})$. For instance, the formula

$$\forall x.\ (x \geq \langle 2, 3\rangle \land x \geq \langle 3, 2\rangle) \leftrightarrow x \geq \langle 3, 3\rangle$$

expresses that over $\mathbb{N}^2$, $\uparrow\langle 2, 3\rangle \cap \uparrow\langle 3, 2\rangle = \uparrow\langle 3, 3\rangle$.

More generally, we can represent any upward-closed set $U = \bigcup_{i=1}^{n} \uparrow x_i$ as a formula $\varphi_U(x) = \bigvee_{i=1}^{n} x \geq \mathtt{x}_i$ with one free variable x, such that for any element $\mathtt{x}$ of X, $\mathtt{x} \in U$ if and only if $X, x \mapsto \mathtt{x} \models \varphi(x)$. Therefore, the logic provides a representation for upward-closed sets, and also for downward-closed sets using the *excluded minor* representation. Moreover, the logic can express that a "set" (represented as a formula with one free variable) is closed, or directed:

$$\forall x, y.\ \varphi(x) \land y \geq x \Rightarrow \varphi(y)$$
$$\forall x, y. \varphi(x) \land \varphi(y) \Rightarrow \exists z.\ \varphi(z) \land z \geq x \land z \geq y$$

As a result, if $\mathsf{FO}(X, \leq, \mathtt{X})$ is decidable, we can compute unions, intersections and complements of closed subsets. In the following chapters, we investigate connections between this representation of closed subsets and the notion of effectiveness introduced in the first part. Of course, the decidability of the full logic $\mathsf{FO}(X, \leq, \mathtt{X})$ seems to be a much stronger property, and this is confirmed by the undecidability of $\Sigma_2(A^*, \leq_*)$, proved in [55] already for A a two-elements alphabet. In the following chapters, we thus mostly study sub-fragments of the existential fragment $\Sigma_1(X, \leq, \mathtt{X})$. The existential fragment of a structure remains an important piece of the logic, notably due to the success of SMT solvers over the past decades. It corresponds to constraint solving, which has many applications in theorem proving and rewriting theory for instance [50].

In Chapter 10, we prove that the *positive existential fragment* of $\mathsf{FO}(X, \leq, \mathtt{X})$ is decidable for any ideally effective WQO $(X, \leq)$. In [50], it is shown that the positive existential fragment of first-order logic interpreted over terms on a finite signature, and where the only predicate $\leq$ is interpreted as tree embedding, is decidable. In these terms, we extend this result to the case where the set of terms is generated by an infinite signature, but with no symbols of arity greater than 0 (i.e. only constants). In this case, the ordering on terms (trees) coincides with the ordering over the elements.

In Chapter 11, we show that our result cannot be extended to the full existential fragment, since $\Sigma_1(A^*, \leq_*, \mathtt{A}^*)$ is already undecidable for a two-symbols alphabet A, while $(A^*, \leq_*)$ is ideally effective (Section 6.1).

The first-order structure of words (over a finite alphabet) is of particular importance in computer science, and it has been studied for various orderings, although the most studied structure on words probably is $(A^*, \cdot, =)$ where $\cdot$ is interpreted as concatenation. Its Σ_2 fragment is undecidable [57, 58], but its existential fragment has been shown decidable by Makanin [59], and has been intensively studied since, notably because its exact complexity is still an open problem [60, 61]. In [54], first-order logics over A^* with several orderings are considered. It is in particular shown that $\Sigma_3(A^*, \leq_*)$ is undecidable. This result is improved in [55]: $\Sigma_2(A^*, \leq_*)$ is undecidable. Note that in the case of A^*, it is possible to define constants (up to permutation of the letters of A) in the Σ_2 fragment, as shown in [55]. However, without constants, $\Sigma_1(A^*, \leq_*)$ is decidable (this is discussed in Section 10.3). In Section 11.1, we close the gap, showing that in the presence of constants, $\Sigma_1(A^*, \leq_*, \mathtt{A}^*)$ is undecidable.

Chapter 11 is based on the article [62]: only parts of the article are rewritten here. A brief overview of the results of [62] that are not presented in this thesis is given in conclusion.

Chapter 10

Constraints Solving on an Ideally Effective WQO

10.1 Definitions

In this section, we define formally all the notions discussed in the previous introduction that will be used in the subsequent sections of this chapter. The main object is the first-order logic over the structure $(X, \leq)$ with constants, denoted $\mathsf{FO}(X, \leq, \mathtt{X})$.

Syntax. The syntax of this logic consists of all first-order formulas over the signature with predicate $\leq$ and a constant symbol $\mathtt{u}$ for each $u \in X$. We use the font $\mathtt{u}$ to distinguish constants from variables in the formulas. These formulas are generated by the following grammars:

- Terms: $t ::= x \mid \mathtt{u}$
  where $\mathtt{u} \in \mathtt{X}$ and $x \in \mathrm{Var}$, a countably infinite set of variables.
- Formulas: $\varphi ::= t \leq t \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists x.\, \varphi$

The notation $\mathsf{FO}(X, \leq)$ denotes the first-order logic over X without constant symbols, i.e. where terms are restricted to be variables from Var.

Semantic. We interpret these formulas over a WQO $(X, \leq)$: a *valuation* is a function from Var to X. A formula φ is said to be *satisfied* by a valuation $V : \mathrm{Var} \to X$, denoted by $X, V \models \varphi$, if:

$$
\begin{array}{ll}
X, V \models t_1 \leq t_2 & \overset{\text{def}}{\Leftrightarrow} V(t_1) \leq V(t_2) \text{, where } V \text{ is extended to constants by } V(\mathtt{u}) \overset{\text{def}}{=} u \\
X, V \models \neg\varphi & \overset{\text{def}}{\Leftrightarrow} X, V \not\models \varphi \\
X, V \models \varphi_1 \wedge \varphi_2 & \overset{\text{def}}{\Leftrightarrow} X, V \models \varphi_1 \text{ and } X, V \models \varphi_2 \\
X, V \models \varphi_1 \vee \varphi_2 & \overset{\text{def}}{\Leftrightarrow} X, V \models \varphi_1 \text{ or } X, V \models \varphi_2 \\
X, V \models \exists x.\, \varphi & \overset{\text{def}}{\Leftrightarrow} \text{ there exists } z \in X \text{ such that } X, V \uplus (x \mapsto z) \models \varphi
\end{array}
$$

where $V \uplus (x \mapsto z)$ denotes the valuation such that for any $y \in \mathrm{Var} \setminus \{x\}$, $V \uplus (x \mapsto z)(y) = V(y)$ and $V \uplus (x \mapsto z)(x) = z$.

Truth Problems. A formula is said to be:

- *satisfiable* if there exists a valuation $V : \mathrm{Var} \to X$ such that $X, V \models \varphi$;
- *valid* if for any valuation $V : \mathrm{Var} \to X$, $X, V \models \varphi$

The set of *free variables* of a formula φ will be denoted $\mathsf{fv}(\varphi)$. We sometimes write $\varphi(x_1, \ldots, x_n)$ to emphasize that $\mathsf{fv}(\varphi) = \{x_1, \ldots, x_n\}$ where the x_i's are distinct. When such an enumeration $x_1, \ldots, x_n$ of $\mathsf{fv}(\varphi)$ is understood, we denote the *solutions* of φ by $[\![\varphi]\!]$, defined by:

$$[\![\varphi]\!] \overset{\text{def}}{=} \{(z_1, \ldots, z_n) \in X^n \mid X, \biguplus_{i \in [n]} (x_i \mapsto z_i) \models \varphi\}$$

Note that with this definition, a formula φ is satisfiable if and only if $[\![\varphi]\!] \neq \emptyset$; and valid if and only if $[\![\varphi]\!] = X^n$. As a consequence, observe that a formula is satisfiable if and only if its negation is not valid.

A formula is said to be *closed* if it has no free variables. In this case, satisfiability and validity coincide (the only valuation being the empty valuation), and the two notions will be used interchangeably.

In the remainder of Part II, we study satisfiability and validity over fragments of $(X, \leq)$: given a *fragment* (i.e. subset) $\mathcal{F}$ of $\mathsf{FO}(X, \leq, \mathtt{X})$, define the following problems,

SATISFIABILITY OF THE $\mathcal{F}$ FRAGMENT

INPUT: A first-order formula $\varphi \in \mathcal{F}$

QUESTION: Is φ satisfiable ?

VALIDITY OF THE $\mathcal{F}$ FRAGMENT

INPUT: A first-order formula $\varphi \in \mathcal{F}$

QUESTION: Is φ valid ?

If $\mathcal{F}$ consists of closed formulas only (and it will always be the case), then the two problems coincide, and we will say that $\mathcal{F}$ is decidable (resp. undecidable) to express that both problems are decidable (resp. undecidable).

Equivalence and Normal Forms Two formulas φ and ψ are said to be *equivalent*, denoted $\varphi \Leftrightarrow \psi$, if $[\![\varphi]\!] = [\![\psi]\!]$.

We assume the reader is familiar with the following normal forms:

- Alpha-renaming: if φ is quantifier-free and $y \notin \mathsf{fv}(\varphi)$, then the formulas $\exists x.\ \varphi$ and $\exists y.\ \varphi[x \leftarrow y]$ are equivalent, where $\varphi[x \leftarrow y]$ denotes the syntactical substitution of variable y for variable x in φ. In particular, we can always assume that a variable is not quantified twice in a first-order formula.

- Prenex normal form: any formula φ is equivalent to a formula in *prenex normal form*, that is with all quantifiers in front; i.e. of the form $Qx_1.\ Qx_2 \dots Qx_n.\ \psi$ where ψ is quantifier-free and $Q \in \{\exists, \forall\}$. Given a formula, one can compute an equivalent formula in prenex normal form.

- Finally, quantifier-free formulas can be put in *disjunctive (resp. conjunctive) normal form*, that is as a disjunction of conjunctions of litterals, where a *litteral* is either an atomic formula or its negation.

Since the problems we study are closed under equivalence, we can always assume that the input formulas of our problems are given in such forms.

Fragments. The main fragments we are interested in are fragments where the quantifier alternation is controlled. Let Σ_i be the set of closed formulas in prenex normal form that start with a certain number of consecutive existential quantifiers, then a certain number of consecutive universal quantifiers, and so on alternating at most i times between consecutive blocks of each type of quantifiers. The fragment Π_i is defined analogously, but we ask that formulas start with universal quantifiers. By convention, $\Sigma_0 = \Pi_0$ is the set of quantifier-free formulas.

The fragment Σ_i of $\mathsf{FO}(X, \leq, \mathtt{X})$ will be denoted $\Sigma_i(X, \leq, \mathtt{X})$.

Syntactic Sugar. In the subsequent chapters, we will use the usual syntactic abbreviations for logical operators (notably for the universal quantification $\forall$), as well as the following shortcuts:

- Not smaller: $x \not\leq y \overset{\text{def}}{\Leftrightarrow} \neg(x \leq y)$.

- Order equivalence: $x \equiv y \overset{\text{def}}{\Leftrightarrow} x \leq y \wedge y \leq x$. The symbol $\equiv$ will be denoted $=$ if $(X, \leq)$ is anti-symmetric.

- Incomparability: $x \perp y \overset{\text{def}}{\Leftrightarrow} x \not\leq y \wedge y \not\leq x$.

- Membership in an upward-closed set: if $U = \bigcup_i \uparrow u_i$, $x \in U \overset{\text{def}}{\Leftrightarrow} \bigvee_i x \geq \mathtt{u}_i$.

- Membership in a downward-closed set: if D is downward-closed, its complement $\complement D = X \smallsetminus D$ is upward-closed, and the previous abbreviation can be used: $x \in D \overset{\text{def}}{\Leftrightarrow} \neg(x \in \complement D)$.

10.2 Positive Existential Fragment

We begin our investigation with a very simple fragment of $\mathsf{FO}(X, \leq, \mathtt{X})$, which we call the *extended positive existential fragment*. As its name indicates, it is a sub-fragment of the more common *existential fragment* $\Sigma_1(X, \leq, \mathtt{X})$. In this section, we show the decidability of the extended positive existential fragment, under the assumption that $(X, \leq)$ is an ideally effective WQO.

Definition 10.2.1. *The* extended positive existential fragment *of* $\mathsf{FO}(X, \leq, \mathtt{X})$ *is defined by the following grammar:*

$$\varphi ::= \mathtt{u} \leq x \mid \mathtt{u} \not\leq x \mid x \leq \mathtt{u} \mid x \not\leq \mathtt{u} \mid x \leq y \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists x.\, \varphi$$

where $c \in X$ *and* $x, y \in \mathrm{Var}$.

We call it extended due to the presence of negation in some atomic formulas. Observe that it suffices to add the predicate "$x \not\leq y$" to this grammar to generate the full existential fragment of $\mathsf{FO}(X, \leq, \mathtt{X})$.

Theorem 10.2.2. *If* $(X, \leq)$ *is an ideally effective WQO, then the extended positive existential fragment of* $\mathsf{FO}(X, \leq, \mathtt{X})$ *is decidable.*

Our first observation is that the four atomic formulas $x \bowtie \mathtt{u}$ (for $x \in \mathrm{Var}$ a variable, $\mathtt{u} \in \mathtt{X}$ a constant and $\bowtie \in \{\leq, \geq, \not\leq, \not\geq\}$) can be reformulated as $x \in U$ for some upward-closed set $U \subseteq X$ or as $x \in D$ for some downward-closed set $D \subseteq X$. Indeed:

$$\mathtt{u} \leq x \Leftrightarrow x \in \uparrow u \qquad\qquad \mathtt{u} \not\leq x \Leftrightarrow x \in \neg\uparrow u$$
$$x \leq \mathtt{u} \Leftrightarrow x \in \downarrow u \qquad\qquad x \not\leq \mathtt{u} \Leftrightarrow x \in \neg\downarrow u$$

Since $(X, \leq)$ is an ideally effective WQO, we can compute these sets (which actually are principal ideals and filters). We push this approach beyond atomic formulas: given a closed formula of the extended positive existential fragment, we can compute its prenex normal form, and put the quantifier-free part of the formula in Disjunctive Normal Form. We obtain a formula $\varphi = \exists x_1 \cdots \exists x_k.\ \bigvee_{i=1}^{p} \bigwedge_{j=1}^{q_i} \varphi_{i,j}$ where the $\varphi_{i,j}$ are atomic. Moreover, since $(X, \leq)$ is ideally effective, we can compute intersections of closed subsets. Thus for each $i \in [p]$ and each $j \in [q_i]$, there exist formulas ψ_1 and ψ_2 such that $\bigwedge_{j=1}^{q_i} \varphi_{i,j}$ is equivalent to $\psi_1 \wedge \psi_2$, ψ_1 is a conjunction of exactly one constraint of the form $x \in U_x \cap D_x$ per $x \in \mathrm{Var}(\varphi)$, for some upward-closed set U_x and some downward-closed set D_x, and ψ_2 is a conjunction of constraints of the form $x \leq y$ for some $x, y \in \mathrm{Var}(\varphi)$. In the end, satisfiability of a conjunction $\bigwedge_{j=1}^{q_i} \varphi_{i,j}$ reduces to the following problem we call *Partial-Embeddability under constraints*:

<u>PARTIAL-EMBEDDABILITY UNDER CONSTRAINTS</u>

INPUT: A finite quasi-ordering $(V, \leq)$, a collection of upward-closed sets $(U_v)_{v \in V}$ of X, and a collection of downward-closed sets $(D_v)_{v \in V}$ of X.

QUESTION: Does there exist a monotone $f : V \to X$ such that $\forall v \in V.\ f(v) \in U_v \cap D_v$?

Indeed, we take $V = \bigcup_{j=1}^{q_i} \mathsf{fv}(\varphi_{i,j})$; ψ_2 induces a quasi-ordering on V, that is, $x \leq y$ in V if and only if $x \leq y$ is a conjunct of ψ_2. Finally, ψ_1 gives a collection of upward-closed sets $(U_v)_{v \in V}$ and a collection of downward-closed sets $(D_v)_{v \in V}$. Subsequently, we show that this problem is decidable, which proves the decidability of the extended positive existential fragment since it then suffices to solve an instance of the Partial-Embeddability under constraints problem for each $\bigwedge_{j=1}^{q_i} \varphi_{i,j}$.

Lemma 10.2.3. *The Partial-Embeddability under constraints problem is decidable.*

Proof. The algorithm to solve the Partial-Embeddability under constraints problem is based on the following observation: given $v_1, v_2 \in V$ such that $v_1 \leq v_2$, the function f we seek to define must satisfy the following conditions:

1. $f(v_1) \leq f(v_2)$ (f is monotone),
2. $f(v_1) \in U_{v_1} \cap D_{v_1}$,
3. $f(v_2) \in U_{v_2} \cap D_{v_2}$.

But, 1 and 3 together imply that $f(v_1) \in D_{v_2}$, and 1 and 2 together imply that $f(v_2) \in U_{v_1}$. That is to say, our instance is equi-satisfiable with the same instance where D_{v_1} is replaced by $D_{v_1} \cap D_{v_2}$ and U_{v_2} is replaced by $U_{v_2} \cap U_{v_1}$.

This motivates the following definition: an instance of the Partial-Embeddability problem under constraints is said to be *resolved* if:

R1: for every $v_1, v_2 \in V$, $v_1 \leq v_2 \Rightarrow U_{v_2} \subseteq U_{v_1}$,

R2: for every $v \in V$, U_v is a filter,

R3: for every $v_1, v_2 \in V$, $v_1 \leq v_2 \Rightarrow D_{v_1} \subseteq D_{v_2}$,

R4: for every $v \in V$, D_v is an ideal.

Observe that the satisfiability status of a resolved instance $\mathcal{I} = (V, \leq, (\uparrow x_v)_{v \in V}, (I_v)_{v \in V})$ is immediate, hence the name:

$$\begin{aligned} \mathcal{I} \text{ is a yes-instance } &\Leftrightarrow \forall v \in V.\ \uparrow x_v \cap I_v \neq \emptyset \\ &\Leftrightarrow \forall v \in V.\ x_v \in I_v \end{aligned}$$

This last condition is decidable. The left-to-right direction of the first equivalence is trivial. For the left-to-right direction of the second equivalence: if there exists some $y \in \uparrow x_v \cap I_v$, then in particular $x_v \leq y \in I_v$, thus $x_v \in I_v$ since I_v is downward-closed. Finally, if $x_v \in I_v$ for every $v \in V$, then the mapping $f(v) = x_v$ is a solution to $\mathcal{I}$. Indeed:

- for $v \in V$, $x_v \in \uparrow x_v \cap I_v$.
- given $v_1, v_2 \in V$, if $v_1 \leq v_2$ then $\uparrow x_{v_2} \subseteq \uparrow x_{v_1}$,
  i.e. $x_{v_1} = f(v_1) \leq x_{v_2} = f(v_2)$.

Now to conclude the proof, we show how to reduce the satisfiability of any instance to the satisfiability of a finite number of resolved instances. This process is essentially the one described in our first observation: if an instance is not resolved, then there exists a pair $(v_1, v_2) \in V^2$ such that $v_1 \leq v_2$ and either $U_{v_2} \not\subseteq U_{v_1}$ or $D_{v_1} \not\subseteq D_{v_2}$, or both. In this case, we can update U_{v_2} to $U_{v_2} \cap U_{v_1} \subseteq U_{v_1}$ (respectively D_{v_1} to $D_{v_1} \cap D_{v_2} \subseteq D_{v_2}$). In this instance, the pair (v_1, v_2) no longer violates conditions R1 and R3 of the definition of resolved (we will deal with conditions R2 and R4 later).

However, this new instance might not be resolved because of another pair (v_3, v_4), and it might be the case that v_3 or v_4 is actually equal to v_1 or v_2. Then, performing the same update for (v_3, v_4) might break again the property $U_{v_2} \subseteq U_{v_1} \wedge D_{v_1} \subseteq D_{v_2}$. Therefore we must be careful in which order the updates are performed.

Observe that the update for a pair (v_1, v_2) does not change D_{v_2} and U_{v_1}. We thus have to consider the upward-closed sets and the downward-closed sets independently, and update upward-closed sets following a non-decreasing order with respect to $(V, \leq)$, while updating downward-closed sets following a non-increasing order with respect to $(V, \leq)$.

Besides, to ensure conditions R2 and R4, we use the decomposition of upward-closed sets (resp. downward-closed sets) as a union of filters (resp. ideals). If $U = \bigcup_i F_i$ and $D = \bigcup_j I_j$, then $x \in U \cap D$ is equivalent to $\bigvee_{i,j} x \in F_i \cap I_j$. Because of this disjunction, one instance will be reduced into several, which will all be further reduced until all the instances are resolved. The original instance is satisfiable if and only if one of the resulting resolved instances is satisfiable.

Formally, given an unresolved instance $(V, \leq, (U_v)_{v \in V}, (D_v)_{v \in V})$, let $n = |V|$ and label the elements of V as $v_1, \ldots, v_n$ such that $\forall i, j \in [n], i < j \Rightarrow v_i \not\geq v_j$. In other words, $v_1 \preccurlyeq v_2 \preccurlyeq \cdots \preccurlyeq v_n$ is a linearization of $\leq$. We then run the following algorithm:

1. Let L be a singleton list containing the original instance.
2. Let L' be an empty list, that will be used as a temporary variable.
3. for $j = 1$ to n:
   (a) for each instance $\mathcal{I}$ in L:
      i. Update $U_{v_j} := U_{v_j} \cap \bigcap_{i<j} U_{v_i}$ in $\mathcal{I}$.
      ii. For each $x \in \min(U_{v_j})$, add a version of $\mathcal{I}$ updated with $U_{v_j} := \uparrow x$ to L'.
   (b) $L := L'$.
4. for $i = n$ down to 1:
   (a) for each instance $\mathcal{I}$ in L:
      i. Update $D_{v_i} := D_{v_i} \cap \bigcap_{i<j} D_{v_j}$ in $\mathcal{I}$.
      ii. For each ideal I in the canonical ideal decomposition of D_{v_i}, add a version of $\mathcal{I}$ updated with $D_{v_i} := I$ to L'.
   (b) $L := L'$.

5. Return L.

As observed at the beginning of this proof, steps 3(a)i and 4(a)i preserve satisfiability, and steps 3(a)ii and 4(a)ii simply transform unions into disjunction over multiple instances. The first loop (at line 3) updates upward-closed sets, while the second loop (at line 4) updates downward-closed sets. After the first loop is executed for index j, the following holds for every instance of L:
$\forall v \in V.\ v \leq v_j \Rightarrow U_v \subseteq U_{v_j}$, and the upward-closed sets U_v for $v \leq v_j$ will no longer be modified. Moreover, U_{v_j} is a filter, and will no longer be modified. Thus conditions R1 and R2 hold at the end of the algorithm. A similar invariant holds for the second loop. Hence, at the end of the algorithm, all instances in L are resolved, and the original instance is satisfiable if and only if one of the resolved instances of L is. $\square$

10.3 Full Existential Fragment

In the previous section, we have established the decidability of a sub-fragment of the existential fragment of $\mathsf{FO}(X, \leq, \mathtt{X})$. As observed earlier, it suffices to add the predicate $x \not\leq y$ to the grammar of Definition 10.2.1 to obtain a grammar for the full existential fragment of $\mathsf{FO}(X, \leq, \mathtt{X})$ (this grammar produces existential formulas whose negations have been pushed down to the atoms).

The same approach we used for the extended positive existential fragment can be applied to the full existential fragment:

- push the negations of φ in,
- convert predicates $x \bowtie c$ into constraints $x \in U$ and $x \in D$,
- put in prenex normal form, with the quantifier-free part in DNF.

We obtain a formula

$$\varphi = \exists x_1 \cdots \exists x_k.\ \bigvee_{i=1}^{p} \left(\bigwedge_{x \in \mathrm{Var}} x \in U_x^{i,j} \cap D_x^{i,j} \right) \wedge \psi_{i,j}$$

for some collections of upward-closed sets $(U_x)_{x \in \mathrm{Var}}$ and downward-closed sets $(D_x)_{x \in \mathrm{Var}}$. However this time, formulas $\psi_{i,j}$ are conjuncts of predicates of the form $x \leq y$ for some $x, y \in \mathrm{Var}$ (as before) but also of the form $x \not\leq y$. Thus, if we interpret $\psi_{i,j}$ as a quasi-ordering on Var, some monotone mapping from Var to X might actually not satisfy $\psi_{i,j}$. We need the stronger notion of *embedding*: $x \leq y$ if and only if $f(x) \leq f(y)$. We obtain a reduction to the following problem:
<u>EMBEDDABILITY UNDER CONSTRAINTS</u>

INPUT: A finite quasi-ordering $(V, \leq)$, and two collections $(U_v)_{v \in V}$ and $(D_v)_{v \in V}$ of upward-closed and downward-closed sets of X respectively.
QUESTION: Does there exists an <u>embedding</u> $f : V \to X$ such that $\forall v \in V.\ f(v) \in U_v \cap D_v$?

Note that since $\psi_{i,j}$ might not fully define a quasi-ordering on Var (i.e. ψ does not enforce exactly one among $x < y$, $x = y$ or $x \perp y$), we have to make an additional disjunction in φ over all finite quasi-orderings satisfying $\psi_{i,j}$ before reducing to this problem.

Replacing the monotone mapping by an embedding induces some changes: we say that an instance $(V, \leq, (U_v)_{v \in V}, (D_v)_{v \in V})$ of the Embeddability under constraints problem is *resolved* if:

1. for every $v_1, v_2 \in V$, $v_1 \leq v_2 \Rightarrow U_{v_2} \subseteq U_{v_1}$,
2. for every $v \in V$, U_v is a filter,
3. for every $v_1, v_2 \in V$, $v_1 \leq v_2 \Rightarrow D_{v_1} \subseteq D_{v_2}$,
4. for every $v \in V$, D_v is an ideal.
5. for every $v_1, v_2 \in V$, $v_1 \not\leq v_2 \Rightarrow U_{v_2} \not\subseteq U_{v_1}$

Once again, a resolved instance $\mathcal{I} = (V, \leq, (\uparrow x_v)_{v \in V}, (I_v)_{v \in V})$ can be easily solved:

$$\begin{aligned} \mathcal{I} \text{ is a yes-instance if and only if } & \forall v \in V.\ \uparrow x_v \cap I_v \neq \emptyset \\ \text{if and only if } & \forall v \in V.\ x_v \in I_v \end{aligned}$$

Indeed, if $\forall v \in V.\ x_v \in I_v$, then the mapping $f(v) = x_v$ is a solution to instance $\mathcal{I}$. Here again, $f(v) \in \uparrow x_v \cap I_v$ by construction. Moreover, it is an embedding:

- if $v_1 \leq v_2$, then $\uparrow x_{v_2} \subseteq \uparrow x_{v_1}$, i.e. $x_{v_1} \leq x_{v_2}$.
- if $v_1 \not\leq v_2$, then $\uparrow x_{v_2} \not\subseteq \uparrow x_{v_1}$, i.e. $x_{v_1} \not\leq x_{v_2}$.

Now, to reduce an unresolved instance to resolved instances as in the previous section, we need to handle pairs of elements of V such that $v_1 \not\leq v_2$. This was not the case with the Partial-Embeddability problem since monotone mappings may lose that information. Observe that given a pair $(v_1, v_2) \in V^2$ such that $v_1 \not\leq v_2$, and $U_{v_2} \subseteq U_{v_1}$, if U_{v_2} is a filter (say $U_{v_2} = \uparrow x_2$) then we can update U_{v_1} with $U_{v_1} \cap \complement(\downarrow x_2)$. This operation is sound and complete. Indeed, if the original instance has a solution f, then $f(v_2) \geq x_2$. Therefore, if $f(v_1) \in \downarrow x_2$, then $f(v_1) \leq f(v_2)$, and f would not be a solution. Thus, $f(v_1) \in U_{v_1} \cap \complement(\downarrow x_2)$.

At this point, one can see how this affects the rest of the proof: while in the case of partial-embeddability, we could update upward-closed sets in a certain order on V that was ensuring termination, here there could be a pair $(v_1, v_2) \in V^2$ such that $v_1 \not\leq v_2 \not\leq v_1$ for which the sequence of updates described above never reaches a resolved instance. This suspicion will be confirmed in the next chapter, where the following is proved:

Theorem 10.3.1. *For $(X, \leq) = (A^*, \leq_*)$, where $(A, =)$ is a two-symbol alphabet and $\leq_*$ is the Higman quasi-ordering introduced in Section 6.1: $\Sigma_1(A^*, \leq, \mathtt{A}^*)$ is undecidable.*

This result contrasts with the NP-completeness of $\Sigma_1(A^*, \leq_*)$, proved in [54]. Note that more generally, the decidability of $\Sigma_1(X, \leq)$ reduces to the embeddability problem without constraints, that is given a finite quasi-ordering, does it embed in $(X, \leq)$? This problem in the case of $(\mathbb{N}^k, \leq_\times)$ is called *the dimension problem* [63]. In the case of $(A^*, \leq_*)$ for a finite alphabet A, every instance is positive [54].

Chapter 11

First-Order Logic over the Subword Ordering

11.1 Undecidability of $\Sigma_1(A^*, \leq_*, \mathtt{A}^*)$

This section is dedicated to the proof of undecidability of the existential fragment of $\mathsf{FO}(A^*, \leq_*, \mathtt{A}^*)$ where $A = \{a, b\}$ is a two-symbol alphabet, i.e. ordered with equality.

More precisely we prove the following:

Theorem 11.1.1. *For each recursively enumerable set $S \subseteq \mathbb{N}$, there is a Σ_1 formula φ over the structure $\mathsf{FO}(A^*, \leq_*, \mathtt{A}^*)$ with one free variable such that $[\![\varphi]\!] = \{a^k \mid k \in S\}$. In particular, $\Sigma_1(A^*, \leq_*, \mathtt{A}^*)$ is undecidable.*

To prove Theorem 11.1.1, we use the following result on recursively enumerable sets:

Theorem 11.1.2 ([64])**.** *Let $S \subseteq \mathbb{N}$ be a recursively enumerable set. Then there is a finite set of variables $\{x_0, \ldots, x_m\}$ and a finite set E of equations, each of the form*

$$x_i = x_j + x_k \qquad\qquad x_i = x_j \cdot x_k \qquad\qquad x_i = 1$$

with $i, j, k \in [0, m]$, such that

$$S = \{y_0 \in \mathbb{N} \mid \exists y_1, \ldots, y_m \in \mathbb{N} \colon (y_0, \ldots, y_m) \text{ satisfies } E\}.$$

Proof. Of Theorem 11.1.1

The proof consists in building more and more complex predicates that can be expressed in the existential fragment of $\mathsf{FO}(A^*, \leq_*, \mathtt{A}^*)$. The new predicates we express are described in the meta language of mathematics. For each of them, we provide an existential first-order formula in our logic extended with the predicates built so far. Recall that $A = \{a, b\}$. As in the rest of the manuscript, elements in A^* are denoted $\boldsymbol{u}, \boldsymbol{v}, \ldots$ in bold font. For variables in the formulas, we use letters x, y, z, u, v, w. When proving the correctness of the formulas we provide, we identify a variable and its valuation, infringing the previous rule.

The following predicates can be expressed in $\Sigma_1(A^*, \leq_*, \mathtt{A}^*)$:

1. Simple languages membership: $x \in \boldsymbol{u}a^*\boldsymbol{v}b^*\boldsymbol{w}$, or simply $x \in \boldsymbol{u}a^*\boldsymbol{v}$.

   In the rest of the proof, we will write $\exists x \in L$ for several languages L of the form $\boldsymbol{u}a^*\boldsymbol{v}b^*\boldsymbol{w}$, for some $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in A^*$ and $a, b \in A$. This can indeed be expressed in our logic since we have seen that we can express membership in upward-closed sets and downward-closed sets, and $\boldsymbol{u}a^*\boldsymbol{v}b^*\boldsymbol{w} = \uparrow(\boldsymbol{uvw}) \cap (\downarrow \boldsymbol{u})a^*(\downarrow \boldsymbol{v})b^*(\downarrow \boldsymbol{w})$ (see Section 6.1 for the structure of downward-closed sets of $(A^*, \leq_*)$). Similarly, $\boldsymbol{u}a^*\boldsymbol{v} = \uparrow(\boldsymbol{uv}) \cap (\downarrow \boldsymbol{u})a^*(\downarrow \boldsymbol{v})$.

2. Occurrence comparison (strict): $|u|_a < |v|_a$.
   Recall $|u|_a$ denotes the number of occurrences of a in u.

$$\exists x \in a^* \colon x \leq_* v \wedge x \not\leq_* u.$$

   The correctness of this expression follows from the observation that for $x \in a^*$, $x \leq_* u$ is equivalent to $|x| \leq |u|_a$.

3. Successor (weak version 1): $\exists n \colon u = a^n \wedge v = a^{n-1}b$.

$$u \in aaa^* \wedge v \in a^*b \wedge \exists x \in a^*baa \colon |v|_a < |u|_a \wedge v \not\leq_* x \wedge u \leq_* x.$$

   Note that the above formula is actually equivalent to "$\exists n \geq 2 \colon u = a^n \wedge v = a^{n-1}b$", from which it is not difficult to build a formula for the actual predicate we want to express.

   Correctness:
   $(\Rightarrow)$ If $u = a^n$ and $v = a^{n-1}b$ for some $n \geq 2$, then the formula is satisfied with $x = a^{n-2}baa$.

   $(\Leftarrow)$ Conversely, suppose the formula is satisfied with $u = a^n$, $x = a^\ell baa$ and $v = a^m b$ for some $\ell, m, n \in \mathbb{N}$. Then $|v|_a < |u|_a \wedge v \not\leq_* x \wedge u \leq_* x$ translates as $m < n \wedge \ell < m \wedge n \leq \ell + 2$, i.e. $\ell < m < n \leq \ell + 2$ which implies $n = m + 1 = \ell + 2$.

4. Letter occurrence comparison (equality, weak version): $u, v \in A^*b \wedge |u|_a = |v|_a$.

$$\exists x \in a^* \colon \exists y \in a^*b \colon \left[\exists n \colon x = a^n \wedge y = a^{n-1}b\right]$$
$$\wedge\, y \leq_* u \;\wedge\; y \leq_* v \;\wedge\; x \not\leq_* u \;\wedge\; x \not\leq_* v.$$

   Correctness:
   $(\Rightarrow)$ If $u, v \in A^*b$ with $|u|_a = |v|_a$, then the formula is satisfied with $n = |u|_a + 1$.

   $(\Leftarrow)$ Suppose the formula is satisfied. Then $a^{n-1}b \leq_* u$ and $a^n \not\leq_* u$ together imply $|u|_a = n - 1$. Moreover, if u ended in a, then $a^{n-1}b \leq_* u$ would entail $a^n \leq_* u$, which is not the case. Since $|u| \geq 1$, we therefore have $u \in A^*b$. By symmetry, we have $|v|_a = n - 1$ and $v \in A^*b$. Hence, $|u|_a = n - 1 = |v|_a$.

5. Successor (weak version 2): $\exists n \colon u = aaba^n b \wedge v = aba^{n+1}b \wedge w = ba^{n+2}b$.

$$u \in aaba^*b \wedge v \in aba^*b \wedge w \in ba^*b$$
$$\wedge\; [u, v, w \in \{a, b\}^*b \wedge |u|_a = |v|_a = |w|_a]\,.$$

6. Successor (weak version 3): $\exists n\colon u = ba^n b \wedge v = ba^{n+1}b$.

$$\begin{aligned}\exists x, y, z\colon\ &\left[\exists m\colon x = aaba^m b \wedge y = aba^{m+1}b \wedge z = ba^{m+2}b\right]\\ &\wedge u, v \in ba^*b \ \wedge\ u \leq_* y \ \wedge\ u \not\leq_* x \ \wedge\ v \leq_* z \ \wedge\ v \not\leq_* y.\end{aligned}$$

   Again, observe that the formula only works for $n \geq 1$.

   Correctness:
   ($\Rightarrow$) If $u = ba^n b$ and $v = ba^{n+1}b$ for some $n \geq 1$, then the formula is satisfied with $m = n - 1$.

   ($\Leftarrow$) Suppose the formula is satisfied for $u = ba^k b$ and $v = ba^\ell b$. Then $u \leq_* y \wedge u \not\leq_* x$ imply $k = m + 1$; and $v \leq_* z \wedge v \not\leq_* y$ imply $\ell = m + 2$

7. Successor: $\exists n\colon u = a^n \wedge v = a^{n+1}$.

$$\begin{aligned}\exists x, y, z\colon\ &\left[\exists m\colon x = ba^m b \wedge y = ba^{m+1}b\right]\\ &\wedge \left[\exists k\colon y = ba^k b \wedge z = ba^{k+1}b\right]\\ \wedge u, v \in a^* \ \wedge\ u \leq_* y \ \wedge\ u \not\leq_* x \ \wedge\ v \leq_* z \ \wedge\ v \not\leq_* y.&\end{aligned}$$

   Correctness of the above formula (for $n \geq 1$) is similar to the previous one. Note that because of the word y, k has to be equal to $m + 1$.

8. Occurrence comparison (equality): $|u|_a = |v|_a$.

$$\exists x, y\colon \left[\exists n\colon x = a^n \wedge y = a^{n+1}\right] \wedge x \leq_* u \wedge y \not\leq_* u \wedge x \leq_* v \wedge y \not\leq_* y$$

   As for the second predicate, correctness relies on the equivalence
   $x \leq_* u \Leftrightarrow |x| \leq |u|_a$ for $x \in a^*$.

9. Unary concatenation (weak version): $u \in a^* \wedge v = bu$.

$$u \in a^* \wedge v \in ba^* \wedge |v|_a = |u|_a.$$

   The predicate $u \in a^* \wedge v = ub$ is similarly expressible.

10. Addition: $|w|_a = |u|_a + |v|_a$.

$$\begin{aligned}&\exists x, y \in a^*\colon |x|_a = |u|_a \wedge |y|_a = |v|_a\\ \wedge\exists z \in a^*ba^*\colon\ &xb \leq_* z \wedge xab \not\leq_* z \wedge by \leq_* z \wedge bya \not\leq_* z\\ &\wedge |w|_a = |z|_a\end{aligned}$$

    Note that we can define xa and ya thanks to Successor and xb, $(xa)b$, by and $b(ya)$ thanks to Unary concatenation (Items 7 and 9).
    Correctness:
    ($\Rightarrow$) Obvious.

    ($\Leftarrow$) the constraints on the second line enforce that $z = xby$ and hence $|z|_a = |x|_a + |y|_a = |u|_a + |v|_a$.

11. Longest unary suffix: v is the longest suffix of u which is in a^*, which we will later denote by $v = \mathrm{ls}(u, a)$.

$$\begin{gathered} v \in a^* \wedge\ \exists x \in b^*a^* \colon \exists y \in b^*a^* \colon \\ |x|_b = |y|_b = |u|_b\ \wedge\ |y|_a = |x|_a + 1 \\ \wedge\ x \leq_* u\ \wedge\ y \not\leq_* u\ \wedge\ |v|_a = |x|_a. \end{gathered}$$

Correctness: there are two cases: either $u \in a^*$, or $u = u'ba^n$ for some $u' \in A^*$ and $n \in \mathbb{N}$. The first case is left to the reader.

($\Rightarrow$) If $v = a^n$, then the formula is satisfied with $x = b^{|u'|_b}ba^n$ and $y = xa$.

($\Leftarrow$) Suppose the formula is satisfied, then $v = a^m, x = b^k a^m, y = b^k a^{m+1}$ for $k = |u|_b$ and for some $m \in \mathbb{N}$. Moreover, since $x \leq_* u$, $m \leq n$. And since $y \not\leq_* u$, $m + 1 \not\leq n$, from which we derive $m = n$, and $v = a^n$.

12. Unary concatenation: $v \in a^* \wedge w = uv$.

$$\begin{aligned} & v \in a^* \wedge \\ & \wedge\ \exists x, y \in a^*\ \colon x = \mathrm{ls}(u, a)\ \wedge\ y = \mathrm{ls}(w, a) \\ (11.1) \qquad & \wedge\ |w|_b = |u|_b\ \wedge\ u \leq_* w \\ (11.2) \qquad & \wedge\ |y|_a = |x|_a + |v|_a\ \wedge\ |w|_a = |u|_a + |v|_a \end{aligned}$$

Correctness:
($\Rightarrow$) If $v \in a^*$ and $w = uv$, then the formula is satisfied with $x = \mathrm{ls}(u, a)$ and $y = \mathrm{ls}(w, a)$.

($\Leftarrow$) Let $v = a^n$, $x = a^p$ and $y = a^q$. The implication being clear if $|u|_b = 0$ or $|w|_b = 0$, we write $u = u'ba^k$ and $w = w'ba^\ell$. The second line implies that $k = p$ and $\ell = q$. Moreover, $y = xv$ (forth line), and thus $w = w'bxv$. Hence, $u \leq_* w$ implies $u \leq_* w'bx$. Thus, w and uv have the same number of occurrences of both a and b, and one is subword of the other: they are therefore equal.

13. Perfect alternation: $u \in (ab)^*$.

$$\exists v \colon v = uab \wedge v = abu$$

Note that the equation $v = uab$ can be obtained using twice Item 12.

Correctness:
($\Rightarrow$) Obvious.

($\Leftarrow$) Assume $abu = uab$. If $u = \epsilon$, then $u \in (ab)^*$. Otherwise, $u = abu'$ for some $u' \in A^*$, and the equation becomes $ababu' = abu'ab$, which is equivalent to $abu' = u'ab$. By induction, we can prove that $u \in (ab)^*$.

14. Occurrence comparison of different letters: $|u|_a = |v|_b$.

$$\exists x \in (ab)^* \colon |u|_a = |x|_a \wedge |v|_b = |x|_b.$$

15. Multiplication: $\exists m, n\colon u = a^n \wedge v = a^m \wedge w = a^{m\cdot n}$.

$$\begin{aligned} & u, v, w \in a^* \\ \wedge\ \exists x\colon [\exists y, z\colon\ y = bu\ \wedge\ z = yx\ \wedge\ z = xy] & \\ \wedge\ |x|_b = |v|_a\ \wedge\ |w|_a = |x|_a. & \end{aligned}$$

Here again $y = bu$, $z = yx$ and $z = xy$ results from several applications of Item 12.

Correctness:
($\Rightarrow$) The formula is satisfied with $x = (bu)^m$.

($\Leftarrow$) The conditions in brackets require $(bu)x = x(bu)$. As in Item 13, a simple induction proves that this implies $x \in (bu)^*$. If $u = a^n$ and $v = a^m$, then the condition $|x|_b = |v|_a$ entails $x = (bu)^m$. Finally, $|w|_a = |x|_a = |u|_a{\cdot}m = n{\cdot}m$.

16. Recursively Enumerable sets: $\varphi_S(u) = \exists n \in S : u = a^n$, for any set $S \subseteq \mathbb{N}$ which is recursively enumerable.

We use the fact that every recursively enumerable set of natural numbers is Diophantine. Applying Theorem 11.1.2 to S yields a finite set E of equations over the variables $\{x_0, \ldots, x_m\}$. The formula φ_S is of the form

$$\exists x_1, x_2, \ldots, x_m \in a^*\colon \psi,$$

where ψ is a conjunction of the following formulas:

- for each equation $x_i = 1$, we add $x_i = a$;
- for each equation $x_i = x_j + x_k$, we add a formula expressing $|x_i|_a = |x_j|_a + |x_k|_a$,
- for each equation $x_i = x_j \cdot x_k$, we add a formula expressing $x_i = a^{|x_j|\cdot|x_k|}$. Then we clearly have $[\![\varphi_S]\!] = \{a^k \mid k \in S\}$. $\square$

11.2 Alternation Bounded Fragments of $\mathsf{FO}(A^*, \leq_*, \ldots)$

In this section, we refine the usual Σ_i fragments ($i \in \mathbb{N}$) with the notion of *letter alternation*. A language $L \subseteq A^*$ over some alphabet $A = \{a_1, \ldots, a_n\}$ is *alternation-bounded* if $L \subseteq (a_1^* \cdots a_n^*)^\ell$ for some $\ell \in \mathbb{N}$. Intuitively, the number of alternations between two distinct letters of a word of L is bounded by $\ell{\cdot}n$. Equivalently, the number of factors of the form ab for $a, b \in A$, $a \neq b$ is bounded by $\ell \cdot n$.

The motivation behind this notion is the observation that if all variables of a Σ_1 formula are restricted to belong to an alternation-bounded language, then the validity of such formulas reduces to Presburger arithmetic, the first-order theory of natural numbers with addition. Indeed, a word of $(a_1^* \cdots a_n^*)^\ell$ can be encoded using $\ell \cdot n$ integer variables, one for each maximal factor of the form a^*, for $a \in A$. It is thus of interest to investigate the effect of letter alternation on decidability: while Σ_i bounds the quantifier alternation of a formula, the fragment $\Sigma_{i,j}$ also bounds the number of variables whose (letter) alternation is not bounded.

Before defining the $\Sigma_{i,j}$ fragments, we need to formalise the possibility to restrict quantified variables to alternation-bounded languages. In this section, we will therefore use first-order logic formulas over the following extended syntax:

$$\begin{aligned}\varphi ::= t \leq t \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists x.\, \varphi \mid \forall x.\, \varphi \\ \mid \exists x \in (a_1^* \cdots a_n^*)^\ell.\, \varphi \mid \forall x \in (a_1^* \cdots a_n^*)^\ell.\, \varphi\end{aligned}$$

Note that the language $(a_1^* \cdots a_n^*)^\ell$ is downward-closed, therefore this extended logic is not more expressive than the one we used until now.

Definition 11.2.1. *Given a closed first-order formula φ and a variable $x \in \mathrm{Var}$, we say that x is* alternation-bounded *in φ if all quantifications over x occurring in φ are guarded by a language $(a_1^* \cdots a_n^*)^\ell$ for some ℓ, that is are of the form $Qx \in (a_1^* \cdots a_n^*)^\ell.\, \psi$ for $Q \in \{\forall, \exists\}$. Otherwise, x is said to be* alternation-unbounded*.*

The fragment $\Sigma_{i,j}$ consists of all Σ_i closed formulas with at most j alternation-unbounded variables.

In the next subsection, we formalise the intuition given above, proving that $\Sigma_{1,0}$ is decidable. We then prove the decidability of $\Sigma_{1,1}$ in Section 11.2.2, by reduction to $\Sigma_{1,0}$.

11.2.1 Decidability of $\Sigma_{1,0}$

Theorem 11.2.2. *The $\Sigma_{1,0}$ fragment is decidable.*

We reduce $\Sigma_{1,0}$ to existential Presburger arithmetic, the first-order theory of natural numbers with ordering and addition (but no multiplication). This logic has been proved decidable by Mojzesz Presburger in his Master thesis in 1929.

Let φ be a closed formula in $\Sigma_{1,0}$, and ℓ be the greatest alternation-bound appearing in φ. A word in $\boldsymbol{u} \in (a_1^* \cdots a_n^*)^\ell$ can be uniquely written $\boldsymbol{u} = \prod_{j=1}^{\ell} a_1^{x_1^j} a_2^{x_2^j} \cdots a_n^{x_n^j}$. Therefore, a variable x in φ will be encoded by $\ell \cdot n$ Presburger variables $(x_i^j)_{i \in [n], j \in [\ell]}$ following this decomposition. For variables with alternation bound $k < \ell$, it suffices to add the constraints $x_i^j = 0$ for $i \in [n]$ and $k < j \leq \ell$. In the other direction, given $\boldsymbol{x} = \langle x_1^1, \ldots, x_n^\ell \rangle \in \mathbb{N}^{\ell \cdot n}$, we denote by $w_{\boldsymbol{x}}$ the associated word $w_{\boldsymbol{x}} = \prod_{j=1}^{\ell} a_1^{x_1^j} \cdots a_n^{x_n^j}$.

Since $\leq_*$ is the only predicate in our logic, it suffices to build Presburger formulas for $x \leq_* y$ and $x \not\leq_* y$ with the above encoding of variables (notice that we can also use this encoding for constants). The rest of the reduction is straightforward: we replace every occurrence of $x \leq_* y$ or $x \not\leq_* y$ in φ by the adequate Presburger formula to obtain a Presburger formula which is equivalent to φ.

Proposition 11.2.3. *There are existential Presburger formulas $\psi_{\leq_*}$ and $\psi_{\not\leq_*}$ such that:*

$$\begin{aligned}\psi_{\leq_*}(x_1^1, \ldots, x_n^\ell, y_1^1, \ldots, y_n^\ell) &\iff w_{\boldsymbol{x}} \leq_* w_{\boldsymbol{y}}, \\ \psi_{\not\leq_*}(x_1^1, \ldots, x_n^\ell, y_1^1, \ldots, y_n^\ell) &\iff w_{\boldsymbol{x}} \not\leq_* w_{\boldsymbol{y}}.\end{aligned}$$

Proof. Let $I = [n] \times [\ell]$ and order the pairs $(i, j) \in I$ lexicographically: $(i', j') \preceq (i, j)$ if $j' < j$ or $j = j'$ and $i' < i$. This captures the order of the $a_i^{x_i^j}$ factors in

$w_{\boldsymbol{x}}$. We first define formulas τ and η that use extra free variables $t_{i,j,k}$ and $e_{i,j,k}$ for $(i,j,k) \in [n] \times [\ell] \times [\ell] \stackrel{\text{def}}{=} J$:

$$\tau \stackrel{\text{def}}{=} \bigwedge_{(i,j,k)\in J} t_{i,j,k} \quad = \begin{cases} 0 & \text{if } e_{i',j',k'} > 0 \text{ for some } (i',j') \preceq (i,j) \text{ and } k' > k \\ y_i^k - \sum_{j'=1}^{j-1} e_{i,j',k} & \text{otherwise} \end{cases}$$

$$\eta \stackrel{\text{def}}{=} \bigwedge_{(i,j,k)\in J} e_{i,j,k} \quad = \min\left(t_{i,j,k}\ ,\ x_i^j - \sum_{r=1}^{k-1} e_{i,j,r} \right)$$

These expressions define the leftmost embedding of $w_{\boldsymbol{x}}$ into $w_{\boldsymbol{y}}$: the variable $t_{i,j,k}$ describes how many letters from $a_i^{y_i^k}$ are available for embedding the $a_i^{x_i^j}$ factor of $w_{\boldsymbol{x}}$. The variable $e_{i,j,k}$ counts how many of these available letters are actually used for the $a_i^{x_i^j}$ factor in the left-most embedding of w_x into w_y.

We are now ready to define $\psi_{\leq_*}$ and $\psi_{\not\leq_*}$:

$$\psi_{\leq_*} \stackrel{\text{def}}{\Leftrightarrow} \exists (t_{i,j,k})_J \exists (e_{i,j,k})_J \colon \tau \wedge \eta \wedge \bigwedge_{(i,j)\in I} \left(x_i^j \leq \sum_{k=1}^{\ell} e_{i,j,k} \right)$$

$$\psi_{\not\leq_*} \stackrel{\text{def}}{\Leftrightarrow} \exists (t_{i,j,k})_J \exists (e_{i,j,k})_J \colon \tau \wedge \eta \wedge \bigvee_{(i,j)\in I} \left(x_i^j > \sum_{k=1}^{\ell} e_{i,j,k} \right)$$

Since formulas τ and η are inductive equations that uniquely define the values of $t_{i,j,k}$ and $e_{i,j,k}$ as functions of the x and y vectors, ψ is equivalent to the negation of φ (quantifying universally or existentially on the $t_{i,j,k}$ and $e_{i,j,k}$ yields equivalent formulas). Moreover, φ expresses that there is enough room to embed each factor $a_i^{x_i^j}$ in $w_{\boldsymbol{y}}$, i.e., that $w_{\boldsymbol{x}} \leq_* w_{\boldsymbol{y}}$ as claimed. $\square$

11.2.2 Decidability of $\Sigma_{1,1}$

Theorem 11.2.4. *The $\Sigma_{1,1}$ fragment is decidable.*

Decidability is obtained by reduction to $\Sigma_{1,0}$. In the fashion of a quantifier elimination procedure, we show that formulas of the form $\exists t\colon \varphi$ where $\varphi \in \Sigma_{1,0}$ and t is the only alternation-unbounded variable, are equivalent to some computable $\Sigma_{1,0}$ formula (next proposition). To compute an equivalent $\Sigma_{1,0}$ formula to any $\Sigma_{1,1}$ closed formula ψ, it then suffices to proceed by induction.

Proposition 11.2.5. *Let φ be a $\Sigma_{1,0}$ formula with a single free variable t. Then $\exists t\colon \varphi$ is equivalent to $\exists t \in (a_1^* \cdots a_n^*)^p \colon \varphi$ for some computable $p \in \mathbb{N}$.*

Proof. To prove this proposition, we exhibit a natural number p, computable from φ, such that for any word $\boldsymbol{u} \in A^*$, if $\boldsymbol{u} \notin (a_1^* \cdots a_n^*)^p$ and $\boldsymbol{u} \in [\![\varphi]\!]$, then there exists $\boldsymbol{v} \in [\![\varphi]\!]$ whose alternation is strictly smaller than $\boldsymbol{u}$'s (but not necessarily smaller than p). Thus, starting from any $\boldsymbol{u} \in [\![\varphi]\!]$, and by iterating the aforementioned property, we eventually get a solution to φ which is of alternation at most p.

However, the alternation decrease in each step are so small that we need a finer notion of alternation to prove that the alternation strictly decreases at each step. Any word $\boldsymbol{u} \in A^*$ can be factored into *blocks* of repeating letters, i.e. $\boldsymbol{u} = \prod_{i=1}^{k} {a_i}^{\ell_i}$ with $\ell_i > 0$ and $a_i \neq a_{i+1}$ for all i. By an *a-block of $\boldsymbol{u}$*, we mean an occurrence of a factor $a_i^{\ell_i}$ with $a_i = a$. Subsequently, we use the number of blocks of a word as a measure of alternation of the word. Note that if a word has k blocks, then it belongs to $(a_1^* \cdots a_n^*)^k$. Conversely, a word in $(a_1^* \cdots a_n^*)^\ell$ has at most $\ell \cdot n$ blocks. Therefore, alternation-bounded languages are the same for the two notions.

Without loss of generality, we assume φ to be in prenex form: $\varphi = \exists z_1 \ldots \exists z_k \colon \psi$. Further assume that ψ has no sub-formula of the form $t \bowtie \mathtt{u}$ for any constant $\mathtt{u}$. This can be assumed since we can always introduce a new alternation-bounded variable which is equal to $\mathtt{u}$. Let $(\boldsymbol{t}, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_k) \in [\![\psi]\!]$ be a solution to ψ. Let ℓ be the maximal number of blocks of the words $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_k$. We now show that if $\boldsymbol{t}$ has more than $p \stackrel{\text{def}}{=} k \cdot \ell + n$ blocks, then there exists $\boldsymbol{t}'$ such that $(\boldsymbol{t}', \boldsymbol{z}_1, \ldots, \boldsymbol{z}_k) \in [\![\psi]\!]$ and $\boldsymbol{t}'$ has strictly fewer blocks than $\boldsymbol{t}$.

Given $\boldsymbol{u} \in A^*$, we write $\operatorname{Im} \boldsymbol{u}$ for the image of the left-most embedding of $\boldsymbol{u}$ into $\boldsymbol{t}$. This is a set of positions in $\boldsymbol{t}$ and, in case $\boldsymbol{u} \not\leq_* \boldsymbol{t}$, these positions only account for the longest prefix of $\boldsymbol{u}$ that can be embedded in $\boldsymbol{t}$. In particular, $|\operatorname{Im} \boldsymbol{u}| = |\boldsymbol{u}|$ if and only if $\boldsymbol{u} \leq_* \boldsymbol{t}$ (and $|\operatorname{Im} \boldsymbol{u}| < |\boldsymbol{u}|$ otherwise).

Formally, if $\boldsymbol{u} = u_1 \cdots u_n$ and $\boldsymbol{t} = t_1 \cdots t_m$, define the left-most embedding f as follows: $f(1)$ is the smallest natural number k in $[1, m]$ such that $u_1 = t_k$, if it exists, $f(1)$ is left undefined otherwise. For $i \in [2, n]$, if $f(j)$ as been defined up to $i - 1$, let $f(i)$ be the smallest k in $[f(i-1), m]$ such that $u_i = t_k$, if it exists. In any other case, $f(i)$ is left undefined. In the end, $\operatorname{Im} \boldsymbol{u}$ is the set of all indexes $f(1), \ldots, f(n)$ that have been defined.

Let $\boldsymbol{b}_0$ be an a-block of $\boldsymbol{t}$. This block is said to be *irreducible* if and only if:

1. either it is the last, i.e. right-most, a-block of $\boldsymbol{t}$,

2. or writing $\boldsymbol{t}$ under the form $\boldsymbol{t} = \boldsymbol{t}_0 \boldsymbol{b}_0 \boldsymbol{t}_1 \boldsymbol{b}_1 \boldsymbol{t}_2$ where $\boldsymbol{b}_1$ is the next a-block, i.e. $a \notin \boldsymbol{t}_1$, one of the following holds:

   - there is some $i \in [k]$ such that:
   $$\boldsymbol{z}_i \leq_* \boldsymbol{t} \quad \text{and} \quad \boldsymbol{b}_0 \cap \operatorname{Im} \boldsymbol{z}_i \neq \emptyset \quad \text{and} \quad \boldsymbol{t}_1 \cap \operatorname{Im} \boldsymbol{z}_i \neq \emptyset.$$

   - there is $i \in [k]$ such that:
   $$\boldsymbol{z}_i \not\leq_* \boldsymbol{t} \quad \text{and} \quad \boldsymbol{b}_0 \cap \operatorname{Im} \boldsymbol{z}_i = \emptyset \quad \text{and} \quad \boldsymbol{t}_1 \cap \operatorname{Im} \boldsymbol{z}_i \neq \emptyset \quad \text{and} \quad \boldsymbol{b}_1 \cap \operatorname{Im} \boldsymbol{z}_i \neq \emptyset.$$

Otherwise $\boldsymbol{b}_0$ is said to be *reducible*.

The whole point of reducible blocks is that they can be swapped to the right: if $\boldsymbol{b}_0$ is a reducible a-block of $\boldsymbol{t}$, then $\boldsymbol{t}$ can be decomposed $\boldsymbol{t} = \boldsymbol{t}_0 \boldsymbol{b}_0 \boldsymbol{t}_1 \boldsymbol{b}_1 \boldsymbol{t}_2$ as above, and the word $\boldsymbol{t}' = \boldsymbol{t}_0 \boldsymbol{t}_1 \boldsymbol{b}_0 \boldsymbol{b}_1 \boldsymbol{t}_2$ satisfies the conditions we want. Indeed, since $\boldsymbol{b}_0$ and $\boldsymbol{b}_1$ are both blocks of the same letter, $\boldsymbol{b}_0 \boldsymbol{b}_1$ is now a single block of $\boldsymbol{t}'$, which means that $\boldsymbol{t}'$ has strictly less blocks than $\boldsymbol{t}$. Moreover, $(\boldsymbol{t}', \boldsymbol{z}_1, \ldots, \boldsymbol{z}_k) \in [\![\psi]\!]$: we show that for any $i \in [k]$, $\boldsymbol{z}_i \leq_* \boldsymbol{t}$ if and only if $\boldsymbol{z}_i \leq_* \boldsymbol{t}'$.

- Let $i \in [k]$ such that $\boldsymbol{z}_i \leq_* \boldsymbol{t}$, there is a unique decomposition $\boldsymbol{z}_i = \boldsymbol{u}_0\boldsymbol{u}_1\boldsymbol{u}_2\boldsymbol{u}_3\boldsymbol{u}_4$ of $\boldsymbol{z}_i$ such that $\operatorname{Im} u_0 \subseteq \boldsymbol{t}_0$, $\operatorname{Im} u_1 \subseteq \boldsymbol{b}_0$, $\operatorname{Im} u_2 \subseteq \boldsymbol{t}_1$, $\operatorname{Im} u_3 \subseteq \boldsymbol{b}_1$ and $\operatorname{Im} u_4 \subseteq \boldsymbol{t}_2$. Since $\boldsymbol{b}_0$ is reducible, one of $\operatorname{Im} \boldsymbol{u}_1$ or $\operatorname{Im} \boldsymbol{u}_2$ is empty. Thus one of $\boldsymbol{u}_1$ or $\boldsymbol{u}_2$ is the empty word, entailing $\boldsymbol{z}_i \leq_* \boldsymbol{t}'$.
- Let $i \in [k]$ such that $\boldsymbol{z}_i \not\leq_* \boldsymbol{t}$. Assume, by way of contradiction, that $\boldsymbol{z}_i \leq_* \boldsymbol{t}'$. Let $\boldsymbol{u}_1$ be the maximal prefix of $\boldsymbol{z}_i$ that embeds into $\boldsymbol{t}$. We proceed to show that $\boldsymbol{b}_0$ is irreducible (a contradiction).
  - Firstly, $\boldsymbol{b}_0 \cap \operatorname{Im} \boldsymbol{u}_1 = \emptyset$. Otherwise, since $a \notin \boldsymbol{t}_1$, the left-most embedding of $\boldsymbol{u}_1$ into $\boldsymbol{t}' = \boldsymbol{t}_0\boldsymbol{t}_1\boldsymbol{b}_0\boldsymbol{b}_1\boldsymbol{t}_2$ does not use t_1 at all and we would have $\boldsymbol{z}_i \leq_* \boldsymbol{t}_0\boldsymbol{b}_0\boldsymbol{b}_1\boldsymbol{t}_2 \leq_* \boldsymbol{t}$.
  - Secondly, $\boldsymbol{t}_1 \cap \operatorname{Im} \boldsymbol{u}_1$ is not empty. If it were, since $a \notin t_1$, the left-most embedding of $\boldsymbol{u}_1$ into $\boldsymbol{t}_0\boldsymbol{t}_1\boldsymbol{b}_0\boldsymbol{b}_1\boldsymbol{t}_2$ would not use $\boldsymbol{t}_1$ and again we would have $\boldsymbol{z}_i \leq_* \boldsymbol{t}_0\boldsymbol{b}_0\boldsymbol{b}_1\boldsymbol{t}_2 \leq_* \boldsymbol{t}$.
  - Lastly, $\boldsymbol{b}_1 \cap \operatorname{Im} \boldsymbol{u}_1 \neq \emptyset$. Otherwise, the already established condition $\boldsymbol{b}_0 \cap \operatorname{Im} \boldsymbol{u}_1 = \emptyset$ implies that $\boldsymbol{z}_i$ embeds not only in $\boldsymbol{t}'$ but in $\boldsymbol{t}_0\boldsymbol{t}_1\boldsymbol{t}_2$, which is a subword of $\boldsymbol{t}$.

Now to conclude the proof, it remains to show that $\boldsymbol{t}$ indeed has a reducible block. This results from our choice of p: every irreducible block is either a right-most a-block for some a (n possible blocks), or can be associated with a block alternation in some $\boldsymbol{z}_i$ ($\ell \cdot k$ possible blocks). Thus there are at most $\ell \cdot k + n = p$ irreducible blocks in $\boldsymbol{t}$. Since we assumed that $\boldsymbol{t}$ has more than p blocks, $\boldsymbol{t}$ must have some reducible blocks.

□

11.3 Concluding Remarks

Other Results from [62]. In the previous Section, we have introduced new fragments $\Sigma_{i,j}$ of the logic $\mathsf{FO}(A^*, \leq_*, \mathtt{A}^*)$ that refine the usual fragments Σ_i. We proved the decidability of $\Sigma_{1,0}$ by polynomial-time reduction to the existential fragment of Presburger's arithmetic, hence proving a NP upper bound for this fragment. The two problems are actually inter-reducible, settling the NP-completeness of $\Sigma_{1,0}$. The inter-reducibility further carries over any quantifier rank, and $\Sigma_{i,0}$ is inter-reducible with the Σ_i fragment of Presburger Arithmetic (see [62] for details). Recent results of Haase [65] on these fragments then settle the complexity of $\Sigma_{i,0}$ presented in Table 11.1. The notation Σ_n^{EXP} used in this table denotes the n-th level of the weak EXP hierarchy, which lies between NEXP and EXPSPACE [66, 67].

We then provided a polynomial-time reduction from $\Sigma_{1,1}$ to $\Sigma_{1,0}$ from which we derive that $\Sigma_{1,1}$ is NP-complete as well. A careful analysis of the proof of undecidability of Σ_1 in Section 11.1 actually reveals that already $\Sigma_{1,3}$ is undecidable. The gap is closed in [62]: $\Sigma_{1,2}$ is also decidable. However, only a NEXP upper bound is known, for the same NP lower bound. The exact complexity of this fragment remains an open problem.

$\Sigma_{i,j}$	0	1	2	3
1	NP	NP	in NEXP	U
$i \geq 2$	$\Sigma_{i-1}^{\mathsf{EXP}}$	U	U	U

Table 11.1: The cell in row i and column j shows the decidability/complexity of the fragment $\Sigma_{i,j}$, where U denotes undecidability.

All other fragments are undecidable, which follows either from the aforementioned undecidability of $\Sigma_{1,3}$ or from the undecidability of $\Sigma_{2,1}$, which is proved in [62]. These results are compiled in Table 11.1.

Perspectives. In Section 11.1, we proved that $\Sigma_1(A^*, \leq_*, \mathtt{A}^*)$ was already undecidable for A a two-symbol alphabet. This implies the undecidability for any alphabet of two or more symbols. We actually proved that it also implies the undecidability of $\Sigma_1(X^*, \leq_*, \mathtt{X}^*)$ for any finite ordering $(X, \leq)$ in which there exists an incomparable pair of elements $a \perp b$.

Therefore, the only finite orderings for which the decidability status of $\Sigma_1(X^*, \leq_*, \mathtt{X}^*)$ is not settled are the linear orderings. Observe that if X is a singleton, $\mathsf{FO}(X^*, \leq_*, \mathtt{X}^*)$ is the theory of integers with ordering, which is PSPACE-complete [68, 69]. Otherwise, X embeds the linearly-ordered set $(\{0,1\}, 0 \leq 1)$. We conjecture that $\Sigma_1(\{0,1\}^*, \leq_*, \{\mathtt{0},\mathtt{1}\}^*)$ is undecidable, which would imply that $\Sigma_1(X^*, \leq_*, \mathtt{X}^*)$ is undecidable for any order $(X, \leq)$ with $|X| \geq 2$. However, we could only prove that $\Sigma_2(\{0,1\}^*, \leq_*, \{\mathtt{0},\mathtt{1}\}^*)$ is undecidable, which already means that $\Sigma_2(X^*, \leq_*, \mathtt{X}^*)$ is undecidable for any partial order $(X, \leq)$ with $|X| \geq 2$.

From the perspective of Chapter 10, Theorem 11.1.1 shows that $\Sigma_1(X, \leq, \mathtt{X})$ cannot be decided in general for an arbitrary ideally effective WQO $(X, \leq)$. In order to find an extra sufficient criterion for an ideally effective WQO to have a decidable existential fragment, a promising angle would be to study other order constructions that preserve ideal effectiveness. This would once again result in an algebra of WQOs whose existential fragment is decidable. For instance, the Cartesian product preserves Σ_1 decidability. Another construction that would in addition be interesting in practice would be finite multisets. Since $(A^{\circledast}, \leq_{\mathrm{emb}})$ when $(A, =)$ is a finite alphabet is isomorphic to $(\mathbb{N}^k, \leq_\times)$, its first-order theory is decidable (using Presburger arithmetic). What about $\Sigma_1(\mathbb{N}^{\circledast}, \leq_{\mathrm{emb}})$ for instance ?

In the case some constructions turn out to preserve Σ_1 decidability, one can wonder about higher quantification alternation. For instance, is $\Sigma_2(X \times Y, \leq_\times, \mathtt{X} \times \mathtt{Y})$ decidable whenever $\Sigma_2(X, \leq_X, \mathtt{X})$ and $\Sigma_2(Y, \leq_Y, \mathtt{Y})$ are ?

Finally, what about the converse implication ? The natural way to represent downward-closed sets in logic is with "excluded minors", and as shown in Section 8.2, this representation may fail to distinguish ideals. However, directedness is a Π_2 formula, and therefore if $\Pi_2(X, \leq, \mathtt{X})$ is decidable, then it is decidable whether $[\![\varphi]\!]$ is an ideal. But otherwise, this is unlikely that decidability of the existential fragment, or positive existential fragment, imply ideal effectiveness in a general way. In particular because our definition requires downward-closed sets to be represented as finite union of ideals. This raises the question: can we find a non effective WQO whose first-order theory is decidable ? Or simply its existential fragment, or even positive existential fragment ?

Bibliography

[1] G. Higman. Ordering by divisibility in abstract algebras. *Proc. London Math. Soc. (3)*, 2(7):326–336, 1952.

[2] J. B. Kruskal. The theory of well-quasi-ordering: A frequently discovered concept. *Journal of Combinatorial Theory, Series A*, 13(3):297–305, 1972.

[3] Jean Goubault-Larrecq, Monika Seisenberger, Victor Selivanov, and Andreas Weiermann. Well quasi-orders in computer science (dagstuhl seminar 16031). In *Dagstuhl Reports*, volume 6. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[4] Alan Turing. Checking a large routine. In *The early British computer conferences*, pages 70–72. MIT Press, 1949.

[5] A. Finkel and Ph. Schnoebelen. Well-structured transition systems everywhere! *Theoretical Computer Science*, 256(1–2):63–92, 2001.

[6] S. Schmitz and Ph. Schnoebelen. The power of well-structured systems. In *CONCUR 2013, LNCS 8052*, pages 5–24. Springer, 2013.

[7] S. Schmitz and Ph. Schnoebelen. Algorithmic aspects of WQO theory. Lecture notes, 2012.

[8] Leonard Eugene Dickson. Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *American Journal of Mathematics*, 35(4):413–422, 1913.

[9] Neil Robertson and Paul D Seymour. Graph minors xxiii. nash-williams' immersion conjecture. *J. Comb. Theory, Ser. B*, 100(2):181–205, 2010.

[10] R. Bonnet. On the cardinality of the set of initial intervals of a partially ordered set. In *Infinite and Finite Sets, Colloquia Math. Soc. János Bolyai, Keszthely, Hungary, 1973*, pages 189–198. North-Holland, 1975.

[11] Roland Fraïssé. *Theory of relations*, volume 145. Elsevier, 2000.

[12] M. Kabil and M. Pouzet. Une extension d'un théorème de P. Jullien sur les âges de mots. *RAIRO Theoretical Informatics and Applications*, 26(5):449–482, 1992.

[13] A. Finkel and J. Goubault-Larrecq. Forward analysis for WSTS, part I: Completions. In *STACS 2009, LIPIcs 3*, pages 433–444. Leibniz-Zentrum für Informatik, 2009.

[14] P. Habermehl, R. Meyer, and H. Wimmel. The downward-closure of Petri net languages. In *ICALP 2010, LNCS 6199*, pages 466–477. Springer, 2010.

[15] Piotr Hofman, Sławomir Lasota, Ranko Lazić, Jérôme Leroux, Sylvain Schmitz, and Patrick Totzke. Coverability trees for Petri nets with unordered data. In *International Conference on Foundations of Software Science and Computation Structures*, pages 445–461. Springer, 2016.

[16] R. M. Karp and R. E. Miller. Parallel program schemata. *Journal of Computer and System Sciences*, 3(2):147–195, 1969.

[17] Parosh Aziz Abdulla, Ahmed Bouajjani, and Bengt Jonsson. On-the-fly analysis of systems with unbounded, lossy fifo channels. In *International Conference on Computer Aided Verification*, pages 305–318. Springer, 1998.

[18] P. A. Abdulla, J. Deneux, P. Mahata, and A. Nylén. Using forward reachability analysis for verification of timed Petri nets. *Nordic Journal of Computing*, 14(1–2):1–42, 2007.

[19] P. A. Abdulla, A. Collomb-Annichini, A. Bouajjani, and B. Jonsson. Using forward reachability analysis for verification of lossy channel systems. *Formal Methods in System Design*, 25(1):39–65, 2004.

[20] A. Finkel and J. Goubault-Larrecq. Forward analysis for WSTS, part II: Complete WSTS. In *ICALP 2009, LNCS 5556*, pages 188–199. Springer, 2009.

[21] R. Valk and M. Jantzen. The residue of vector sets with applications to decidability problems in Petri nets. *Acta Informatica*, 21(6):643–674, 1985.

[22] Alain Finkel, Pierre McKenzie, and Claudine Picaronny. A well-structured framework for analysing Petri net extensions. *Information and Computation*, 195(1-2):1–29, 2004.

[23] D. Zufferey, T. Wies, and T. A. Henzinger. Ideal abstractions for well-structured transition systems. In *VMCAI 2012, LNCS 7148*, pages 445–460. Springer, 2012.

[24] G. Geeraerts, J.-F. Raskin, and L. Van Begin. Expand, enlarge and check: New algorithms for the coverability problem of WSTS. *Journal of Computer and System Sciences*, 72(1):180–203, 2006.

[25] R. Diestel. Relating subsets of a poset, and a partition theorem for wqos. *Order*, 18(3):275–279, 2001.

[26] R. Lazić and S. Schmitz. The ideal view on Rackoff's coverability technique. In *RP 2015, LNCS 9328*, pages 76–88. Springer, 2015.

[27] R. Lazić and S. Schmitz. The complexity of coverability in ν-Petri nets. In *LICS 2016*, pages 467–476. ACM Press, 2016.

[28] J. Leroux and S. Schmitz. Demystifying reachability in vector addition systems. In *LICS 2015*, pages 56–67. IEEE Comp. Soc. Press, 2015.

[29] M. Blondin, A. Finkel, and P. McKenzie. Handling infinitely branching WSTS. In *ICALP 2014, LNCS 8573*, pages 13–25. Springer, 2014.

[30] J. Goubault-Larrecq and S. Schmitz. Deciding piecewise testable separability for regular tree languages. In *ICALP 2016, LIPIcs 55*, pages 97:1–97:15. Leibniz-Zentrum für Informatik, 2016.

[31] Georg Zetzsche. PTL-separability and closures for wqos on words. *arXiv preprint arXiv:1802.07397*, 2018.

[32] G. Delzanno and J.-F. Raskin. Symbolic representation of upward-closed sets. In *TACAS 2000, LNCS 1785*, pages 426–440. Springer, 2000.

[33] P. Jullien. Sur un théorème d'extension dans la théorie des mots. *C. R. Acad. Sci. Paris, Ser. A*, 266:851–854, 1968.

[34] P. Karandikar, M. Niewerth, and Ph. Schnoebelen. On the state complexity of closures and interiors of regular languages with subwords and superwords. *Theoret. Comput. Sci.*, 610:91–107, 2016.

[35] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Communications of the ACM*, 22(8):465–476, 1979.

[36] G. Huet and D. C. Oppen. Equations and rewrite rules: a survey. In R. Book, editor, *Formal Language Theory: Perspectives and Open Problems*, pages 349–405. Academic Press, 1980.

[37] J. Goubault-Larrecq. On a generalization of a result by Valk and Jantzen. Research Report LSV-09-09, Laboratoire Spécification et Vérification, ENS Cachan, France, May 2009.

[38] Richard Rado. Partial well-ordering of sets of vectors. *Mathematika*, 1(2):89–95, 1954.

[39] C St JA Nash-Williams. On better-quasi-ordering transfinite sequences. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 64, pages 273–290. Cambridge University Press, 1968.

[40] C St JA Nash-Williams. On well-quasi-ordering infinite trees. In *Mathematical proceedings of the cambridge philosophical society*, volume 61, pages 697–720. Cambridge University Press, 1965.

[41] Pierre Jullien. *Contribution à l'étude des types d'ordres dispersés*. Thèse de doctorat, Université de Marseille, 1969.

[42] Maurice Pouzet. Sur les prémeilleurordres. *Ann. Inst. Fourier (Grenoble)*, 22(2):1–19, 1972.

[43] Eric C Milner. Basic wqo-and bqo-theory. In *Graphs and order*, pages 487–502. Springer, 1985.

[44] P. Jančar. A note on well quasi-orderings for powersets. *Information Processing Letters*, 72(5–6):155–161, 1999.

[45] Alberto Marcone. Foundations of bqo theory. *Transactions of the American Mathematical Society*, 345(2):641–660, 1994.

[46] A. Marcone. Fine analysis of the quasi-orderings on the power set. *Order*, 18(4):339–347, 2001.

[47] Ch. Haase, S. Schmitz, and Ph. Schnoebelen. The power of priority channel systems. *Logical Methods in Comp. Science*, 10(4:4), 2014.

[48] P. A. Abdulla. Well (and better) quasi-ordered transition systems. *Bull. Symbolic Logic*, 16(4):457–515, 2010.

[49] Parosh Aziz Abdulla and Aletta Nylén. Better is better than well: On efficient verification of infinite-state systems. In *Logic in Computer Science, 2000. Proceedings. 15th Annual IEEE Symposium on*, pages 132–140. IEEE, 2000.

[50] A. Boudet and H. Comon. About the theory of tree embedding. In *Proc. TAPSOFT '93, LNCS 668*, pages 376–390. Springer, 1993.

[51] H. Comon and R. Treinen. Ordering constraints on trees. In *Proc. CAAP '94, LNCS 787*, pages 1–14. Springer, 1994.

[52] H. Comon and R. Treinen. The first-order theory of lexicographic path orderings is undecidable. *Theoret. Comput. Sci.*, 176(1–2):67–87, 1997.

[53] O. V. Kudinov, V. L. Selivanov, and L. V. Yartseva. Definability in the subword order. In *Proc. CiE 2010, LNCS 6158*, pages 246–255. Springer, 2010.

[54] D. Kuske. Theories of orders on the set of words. *RAIRO Theoretical Informatics and Applications*, 40(1):53–74, 2006.

[55] P. Karandikar and Ph. Schnoebelen. Decidability in the logic of subsequences and supersequences. In *Proc. FST&TCS 2015, LIPIcs 45*, pages 84–97. Leibniz-Zentrum für Informatik, 2015.

[56] R. Ramanujam and R. S. Thinniyam. Definability in first order theories of graph orderings. In Sergei Artemov and Anil Nerode, editors, *Logical Foundations of Computer Science*, pages 331–348, Cham, 2016. Springer International Publishing.

[57] W. V. Quine. Concatenation as a basis for arithmetic. *J. Symb. Logic*, 11(4):105–114, December 1946.

[58] Valery G. Durnev. Undecidability of the positive $\forall\exists^3$-theory of a free semigroup. *Sib. Math. J.*, 36(5):917–929, 1995.

[59] V. Diekert. Makanin's algorithm. In M. Lothaire, editor, *Algebraic Combinatorics on Words*, volume 90 of *Encyclopedia of Mathematics and Its Applications*, chapter 13, pages 387–442. Cambridge Univ. Press, 2002.

[60] W. Plandowski. Satisfiability of word equations with constants is in PSPACE. *J. ACM*, 51(3):483–496, 2004.

[61] Joel D. Day, Vijay Ganesh, Paul He, Florin Manea, and Dirk Nowotka. The satisfiability of extended word equations: The boundary between decidability and undecidability. *CoRR*, abs/1802.00523, 2018.

[62] Simon Halfon, Philippe Schnoebelen, and Georg Zetzsche. Decidability, complexity, and expressiveness of first-order logic over the subword ordering. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017.

[63] M. Yannakakis. The complexity of the partial order dimension problem. *SIAM J. Algebraic Discrete Meth.*, 3(3):351–358, 1982.

[64] Yuri V. Matiyasevich. *Hilbert's Tenth Problem*. MIT Press, Cambridge, Massachusetts, 1993.

[65] Christoph Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *Proc. CSL-LICS 2014*, pages 47:1–47:10. ACM, 2014.

[66] L. Hemachandra. The strong exponential hierarchy collapses. *J. Comput. System Sci.*, 39(3):299–322, 1989.

[67] G. Gottlob, N. Leone, and H. Veith. Second order logic and the weak exponential hierarchies. In *Proc. MFCS '95, LNCS 969*, pages 66–81. Springer, 1995.

[68] J. Ferrante and C. W. Rackoff. *The computational complexity of logical theories*, volume 718 of *Lecture Notes in Mathematics*. Springer, 1979.

[69] Larry Joseph Stockmeyer. *The complexity of decision problems in automata theory and logic*. PhD thesis, Department of Electical Engineering, MIT, July 1974. Available as Report MAC-TR-133.

Résumé

Avec des motivations venant du domaine de la Vérification, nous définissons une notion de WQO effectifs pour lesquels il est possible de représenter les ensembles clos et de calculer les principales opérations ensemblistes sur ces représentations. Dans une première partie, nous montrons que de nombreuses constructions naturelles sur les WQO préservent notre notion d'effectivité, prouvant ainsi que la plupart des WQOs utilisés en pratique sont effectifs. Cette partie est basée sur un article non publié dont Jean Goubault-Larrecq, Narayan Kumar, Prateek Karandikar et Philippe Schnoebelen sont co-auteurs.

Dans une seconde partie, nous étudions les conséquences qu'a notre notion sur la logique du première ordre interprété sur un WQO. Bien que le fragment existentiel positif soit décidable pour tous les WQOs effectif, les perspectives de généralisation sont limitées par le résultat suivant: le fragment existentiel de la logique du première ordre sur les mots finis, ordonnés par plongement, est déjà indécidable. Ce résultat a été publié à LICS 2017 avec Philippe Schnoebelen et Georg Zetzsche.

Abstract

With motivations coming from Verification, we define a notion of effective WQO for which it is possible to represent closed subsets and to compute basic set-operations on these representations. In a first part, we show that many of the natural constructions that preserve WQOs also preserve our notion of effectiveness, proving that a large class of commonly used WQOs are effective. This part is based on an unpublished article with Jean Goubault-Larrecq, Narayan Kumar, Prateek Karandikar and Philippe Schnoebelen.

In a second part, we investigate the consequences of our notion on first-order logics over WQOs. Although the positive existential fragment is decidable for any effective WQO, the perspective of extension to larger fragments is hopeless since the existential fragment is already undecidable for the first-order logic over words with the subword ordering. This last result has been published in LICS 2017 with Philippe Schnoebelen and Georg Zetzsche.