University of Trento
Department of Mathematics

University of Gent
Department of Mathematics

University of Verona
Department of Computer Science

Ph.D. Thesis

Proof-Theoretical Aspects of Well Quasi-Orders

and

Phase Transitions in Arithmetical Provability

Candidate:
Gabriele Buriola

Supervisors:
Prof. Peter Schuster University of Verona
Prof. Andreas Weiermann University of Gent

Academic Year 2023 – 2024

Abstract

English

In this thesis we study the concept of *well quasi-order*, originally developed in order theory but nowadays transversal to many areas, in the over-all context of proof theory - more precisely, in reverse mathematics and constructive mathematics. Reversed mathematics, proposed by Harvey Friedman, aims to classify the strength of mathematical theorems by identifying the required axioms. In this framework, we focus on two classical results relative to well quasi-orders: Kruskal's theorem and Higman's lemma. Concerning the former, we compute the proof-theoretic ordinals of two different versions establishing their non equivalence. Regarding the latter, we study, over the base theory $\mathbf{RCA}_0$, the relations between Higman's original achievements and some versions of Kruskal's theorem. For what concerns constructive mathematics, which goes back to Brouwer's reflections and rejects the law of excluded middle in favour of more perspicuous reasoning principles, we scrutinize the main definitions of well quasi-order establishing their constructive nature; moreover, a new constructive proof of Higman's lemma is proposed paving the way for a systematic analysis of well quasi-orders within constructive means.

On top of all this we consider a peculiar phenomenon in proof theory, namely phase transitions in provability. Building upon previous results about provability in Peano Arithmetic, we locate the threshold separating provability and unprovability for statements regarding Goodstein sequences, Hydra games and Ackermannian functions.

Italiano

In questa tesi studiamo il concetto di *well quasi-order*, originariamente sviluppato nella teoria degli ordini ma oggi trasversale a molti ambiti, nel contesto generale della teoria della dimostrazione - più precisamente, in reverse mathematics e matematica costruttiva. La reverse mathematics, proposta da Harvey Friedman, mira a classificare la forza dei teoremi matematici individuando gli assiomi richiesti. In questo contesto, ci concentriamo su due risultati classici relativi ai well quasi-order: il teorema di Kruskal e il lemma di Higman. Per quanto riguarda il primo, abbiamo calcolato gli ordinali proof-teoretici di due diverse versioni stabilendone la non equivalenza. Per quanto riguarda il secondo, studiamo, sopra la teoria di base $\mathbf{RCA}_0$, le relazioni tra i risultati originali di Higman e alcuni versioni del teorema di Kruskal. Per quanto riguarda la matematica costruttiva, che si rifà alle riflessioni di Brouwer e rifiuta la legge del terzo escluso a favore di principi di ragionamento più perspicui, esaminiamo attentamente le principali definizioni di well quasi-order stabilendone la natura costruttiva; inoltre, viene proposta una nuova dimostrazione costruttiva del lemma di Higman aprendo la strada per una sistematica analisi dei well quasi-order all'interno di metodi costruttivi.

Oltre a questo consideriamo un fenomeno peculiare nella teoria della dimostrazione, vale a dire le transizioni di fase nella dimostrabilità. Basandoci su risultati precedenti sulla dimostrabilità nell'aritmetica di Peano, abbiamo individuato la soglia che separa dimostrabilità e indimostrabilità per enunciati riguardanti sequenze di Goodstein, Hydra games e funzioni ackermanniane.

Nederlands

In dit proefschrift bestuderen we het concept van *well quasi-order*, oorspronkelijk ontwikkeld in ordetheorie, maar tegenwoordig transversaal op veel gebieden, in de algemene context van bewijstheorie - meer precies, in omgekeerde wiskunde en constructief wiskunde. Omgekeerde wiskunde, voorgesteld door Harvey Friedman, heeft tot doel dit te bereiken classificeer de sterkte van wiskundige stellingen door de vereiste te identificeren axioma's. In dit raamwerk concentreren we ons op twee klassieke resultaten met betrekking tot putten quasi-orden: de stelling van Kruskal en het lemma van Higman. Wat het eerstgenoemde betreft, we berekenen de bewijstheoretische rangtelwoorden van twee verschillende versies hun niet-equivalentie. Wat dit laatste betreft, bestuderen we de basistheorie $\mathbf{RCA}_0$, de relaties tussen de oorspronkelijke prestaties van Higman en sommige versies van de stelling van Kruskal. Wat constructieve wiskunde betreft, die teruggrijpt op de reflecties van Brouwer en de wet van de uitgeslotenen verwerpt midden in het voordeel van meer doorzichtige redeneerprincipes, onderzoeken we de belangrijkste definities van quasi-orde die hun constructieve aard aantonen; bovendien wordt bestrating voorgesteld als een nieuw constructief bewijs van het lemma van Higman de weg voor een systematische analyse van quasi-ordes binnen constructief middelen.

Bovendien beschouwen we een eigenaardig fenomeen in de bewijstheorie: namelijk faseovergangen in de bewijsbaarheid. Voortbouwend op eerdere resultaten over bewijsbaarheid in Peano Arithmetic vinden we de drempel die de bewijsbaarheid scheidt en onbewijsbaarheid voor uitspraken over Goodstein-sequenties, Hydra-spellen en Ackermanniaanse functies.

Acknowledgements

First of all, I want to express my deepest appreciation to both my supervisors Peter Schuster and Andreas Weiermann for their suggestions and support in my research, but above all for their role as mentors at the beginning of my academic life. If I have achieved any results it is thanks to their guidance.

I want to thank also all the friends and colleagues I have met during this journey of almost four years into logic and mathematics, you have transformed work meetings into life meetings. In particular, I would like to mention some of the amazing persons I met, listed simply in alphabetic order: Toshiro Arai, Ulrich Berger, Stefania Centrone, Laura Crosilla, Anton Freund, Hugo Herbelin, Henri Lombardi, Ulrich Kohlenbach, Milly Maietti, Alberto Marcone, Sara Negri, Stefan Neuwirth, Eugenio Orlandelli, Iosif Petrakis, Michael Rathjen, Helmut Schwichtenberg, Monica Seisenberger, Matteo Tesi, and last, but not least, Margherita Zorzi.

I want to reserve a special mention to Giulio Fellin, my senpai in the doctoral programme in Verona; as well as to the co-authors of my already published articles: Ingo Blechschmidt and Stefano Berardi.

Regarding the groups with which I have had the honor of collaborating, a special place is reserved to the logic group at Ghent University which hosted me during my research period for the double degree; in particular I would like to thank Fedor Pakhomov for his suggestions always insightful, Giovanni Soldà for being the best office companion I could have had and of course Andreas Weiermann for leading the leading European group in proof theory.

A very special thank goes to the RDF* team: prof. Domenico Cantone, Gianluca Cincotti, prof. Eugenio Omodeo e Gaetano Spartà. Although our work does not appear in this thesis, our periodic meetings have been a precious source of advice.

I can't forget my long-time friends who stood by me along the way, I hope to have you by my side for a long time to come.

Last, but not least, I would like to thank my parents for their unconditional love and support and my brothers for their inexhaustible patience.

Contents

Chapter 1

Introduction and Preliminaries

1.1 The Background

The concept of proof is ubiquitous in mathematics and the flow from axioms to theorems through proofs may be recognized, as memories of high school, by many. Mathematicians have always been concerned about what are axioms and when we can assert that we have proved something; but, even when they were aware of the questionability of their axioms, e.g. Euclid with his famous fifth postulate [91], the focus was their acceptability and the persuasiveness of the proofs, more than their formal correctness or proper nature. Then the crisis in the foundations came. Stemmed from the lack of necessary rigor in the definitions of continuous function, real number and natural number, it quickly became an inquiry regarding the very concept of proof. A possible solution came from David Hilbert who, taking advantage of previous results in logic mainly due to Frege, proposed the creation of a "*Beweistheorie*": that is, a theory of proofs, or simply proof theory. Hilbert's idea was to use the instruments of mathematics itself to analyze mathematical theorems and their proofs; after a proper formalization, the latter indeed become mathematical objects. Proof theory thus has been a meta-mathematical enterprise from its very beginning. The original aspiration of Hilbert regarding a finitary proof of the consistency of the whole of mathematics was shattered by Gödel's incompleteness theorems [83].

Nevertheless, proof theory has turned out to be incredibly fruitful, and the meta-mathematical perspective is a constant of the present thesis. The main topics are *well quasi-orders*, in particular in *reverse mathematics* and *constructive mathematics*, and *phase transitions* in arithmetical provability.

1.2 The Theory of Well Quasi-Orders

Order relations, i.e. relations which are reflexive ($\forall x\, xRx$), antisymmetric ($\forall x,y\ xRy \wedge yRx \rightarrow x = y$), and transitive ($\forall x,y,z\ xRy \wedge yRz \rightarrow xRz$), have always played a remarkable role in mathematics, starting from the standard order $\leqslant$ between numbers. To fix some terminology, here is our first definition:

Definition 1.1 *Let P be a set and $\leqslant$ a binary relation over P.*

1. *$(P, \leqslant)$ is a* PARTIAL ORDER, po, *if $\leqslant$ is a reflexive, antisymmetric, transitive relation;*

2. *$(P, \leqslant)$ is a* TOTAL, *or* LINEAR ORDER, lo, *if it is a partial order such that, in addition, $\forall p, q \in P\, (p \leqslant q \vee q \leqslant p)$;*

3. *$(P, \leqslant)$ is a* QUASI-ORDER, qo, *if $\leqslant$ is a reflexive and transitive relation.*

From the definition it is clear that every linear order is a partial order, which in turn is a quasi-order; moreover, po and qo are tightly connected. In fact, given a qo $(P, \leqslant)$, we can consider the following equivalence relation over P: $p \sim q$ iff $p \leqslant q$ and $q \leqslant p$; then the quotient set $P/\!\sim$ is a partial order with respect to the relation induced by $\leqslant$. This connection allows to extend to qo many definitions referring to po simply taking the quotient. Finally, for what concerns notation, we frequently talk about a po, or qo, P omitting the underlying order relation and, as usual, we denote: by $<$ the corresponding strict order, i.e. $p < q$ iff $p \leqslant q$ and $q \nleqslant p$; by $\geqslant$ the reverse order, namely $q \geqslant p$ iff $p \leqslant q$, and by $p \sim q$ equivalent elements, i.e. $p \leqslant q \wedge q \leqslant p$.

The concept of total order, i.e. an order in which any two elements are comparable, is a natural and reasonable strengthening of the one of partial order; on the other hand, quasi-orders may seem strange. By weakening partial to quasi-orders one allows cycles which are commonly one of the features we do not want in something called "an order". Nevertheless, the concept of quasi-order turns out to be the right one for our theoretical purposes. In particular, we will focus on a specific refinement of qo's, *well quasi-orders*, wqo, which are the analogue, in the context of qo, of well orders; namely total orders in which every non empty subset has a minimum or, equivalently, containing no infinite strictly descending chains (the paradigmatic example is $(\mathbb{N}, \leqslant)$). Well quasi-orders have proved extremely fruitful and thus they were frequently rediscovered as tracked by Kruskal in his classical survey [107]. To appreciate the vastness of the sectors where they have been applied, it may be helpful to count the number of different, yet equivalent, definitions which have been proposed; to present them we need some preliminary concepts we will use throughout the thesis.

Definition 1.2 *For every quasi-order* $(Q, \leqslant)$,

- *the* CLOSURE *of a subset* B *of* Q *is given by* $\uparrow B = \{q \in Q \mid \exists b \in B\, b \leqslant q\}$*;*
- *a subset of* Q *is* CLOSED *if it equals its own closure, and a closed subset is* FINITELY GENERATED *if it is the closure of a finite set;*
- *a* SEQUENCE $(q_k)_k$ *(of elements) in* Q *is a function from* $\mathbb{N}$ *to* Q*;*
- *an* ANTICHAIN *in* Q *is a sequence* $(q_k)_k$ *in* Q *such that* q_i *and* q_j *are incomparable whenever* $i \neq j$*;*
- *an* EXTENSION *of* $(Q, \leqslant)$ *is a* qo $\preccurlyeq$ *on* Q *extending* $\leqslant$ *in the sense that* $p \leqslant q \Rightarrow p \preccurlyeq q$ *and such that for all* p *and* q, $p \preccurlyeq q \wedge q \preccurlyeq p \Rightarrow p \sim q$*;*
- $(Q, \leqslant)$ *is* WELL-FOUNDED*, if it has no infinite strictly descending chains* $q_1 > q_2 > q_3 > \dots$

Although there are many equivalent definitions for wqo, the following is commonly consider the "standard" one.

Definition 1.3 *A* qo $(Q, \leqslant)$ *is a* WELL QUASI-ORDER*, wqo, if for every sequence* $(q_k)_k$ *in* Q *there exist two indexes* $i < j$ *such that* $q_i \leqslant q_j$.

A sequence $(q_k)_k$ in Q with such a property, i.e. $\exists i < j \; q_i \leqslant q_j$, is called *good*, otherwise is called *bad*; thus a qo Q is a wqo if it has no infinite bad sequences.

We can now state the following equivalence result which collects together the most frequent properties used as definition of wqo.

Proposition 1.1 *Given a* qo $(Q, \leqslant)$*, the following are equivalent:*

1. Q *is a wqo;*
2. *every sequence* $(q_k)_k$ *in* Q *has a weakly increasing subsequence* $q_{i_1} \leqslant q_{i_2} \leqslant q_{i_3} \leqslant \dots$ *with* $i_1 < i_2 < i_3 < \dots$*;*
3. Q *is well-founded and has no infinite antichains;*
4. *every closed subset of* Q *is finitely generated;*
5. *every subset* B *of* Q *is contained in the closure of a finite subset of* B*;*
6. *the set of closed subsets has no infinite ascending chains with respect to inclusion* $\subseteq$*;*

7. *every extension of $\leqslant$ is well-founded;*

8. *every linear extension of $\leqslant$ is a well-order.*

Proof see [92, Theorem 2.1], [77, Lemma 2.4] and [42, Proposition 1.1].[1] □

The previous properties, in particular the first three, can be understood as termination properties for sequences in Q and this fact has been extensively exploited in computer science to prove termination of algorithms [26, 58, 59]. For a recent survey on the many areas of use of wqo see [159]. Given their useful applications, a standard problem in the theory of wqo is how to generate new ones; the following results are nowadays classical.

Proposition 1.2 *Given two* wqo $(P, \leqslant_P)$ *and* $(Q, \leqslant_Q)$ *then the following are* wqo*:*

1. *Disjoint union:* $(P \dot{\cup} Q, \leqslant_{P \cup Q})$ *with*

$$p \leqslant_{P \dot{\cup} Q} q \;\equiv\; p \leqslant_P q \vee p \leqslant_Q q;$$

2. *Intersection:* $(P \cap Q, \leqslant_{P \cap Q})$ *with*

$$p \leqslant_{P \cap Q} q \;\equiv\; p \leqslant_P q \wedge p \leqslant_Q q;$$

3. *Product:* $(P \times Q, \leqslant_{P \times Q})$ *with*

$$(p_1, q_1) \leqslant_{P \times Q} (p_2, q_2) \;\equiv\; p_1 \leqslant_P p_2 \wedge q_1 \leqslant_Q q_2.$$

Lemma 1.1 (Higman's lemma) *Given a* wqo $(Q, \leqslant_Q)$*, then* Q^**, the set of finite sequences in* Q*, is a* wqo *with respect to the following* qo $\leqslant_Q^*$*:*

$$p_1 \ldots p_n \leqslant_Q^* q_1 \ldots q_m \;\equiv\; \exists\, 1 \leqslant i_1 < \ldots < i_n \leqslant m \,:\, p_k \leqslant_Q q_{i_k} \text{ for all } 1 \leqslant k \leqslant n.$$

Proof see [92]. □

Theorem 1.1 (Kruskal's theorem) *Given a* wqo $(Q, \leqslant_Q)$*, then* $\mathbb{T}(Q)$ *the set of finite trees with labels in* Q *is a* wqo *under tree embeddability.*[2]

Proof see [106]. □

These last results, for which we refer also to [9], are crucial in the theory of wqo and the core part of this thesis is dedicated to analyze them in two different frameworks: Reverse Mathematics and Constructive mathematics which are briefly introduced in the next sections.

[1] It is interesting to note how the name of these results about equivalences changed, from "theorem" to "proposition", as the concept has became more and more common.

[2] See Def. 2.7 for the definition of tree embeddability.

1.3 Reverse Mathematics

As the working mathematician already knows, in order to prove a property or a statement the very first step is often to wonder which hypotheses suffice to obtain that statement and this reverse path from a thesis to the hypotheses required to prove it, or more generally from theorems to the axioms, is almost as ancient as mathematics itself. Nevertheless, by *Reverse Mathematics*, we do not mean this theoretical process; instead, we refer to the programme pioneered by Harvey Friedman [73], and subsequently developed by Stephen Simpson and others [168, 169, 173], aiming to classify "ordinary mathematics" statements using as benchmark suitable axioms, mainly existential axioms, in the language of second order arithmetic.

Given its goal, the reverse mathematics programme is specified in different areas, such as reverse algebra, reverse analysis and so on; nevertheless, there are two phenomenona almost ubiquitous in reverse mathematics which we briefly highlight. The first one regards the connection between the minimal axioms needed in order to prove a theorem and the theorem itself; quoting the founding father of reverse mathematics Harvey Friedman [73, pag. 1]: "When the theorem is proved from the right axioms, the axioms can be proved from the theorem". The second one, instead, concerns the general structure formed by these axioms. Given the numerous fields of mathematics, the final picture may lack any regularity; but actually, the majority of ordinary mathematics theorems turns out to be equivalent to one of four specific subsystems or provable in a fifth one (the base theory), these systems are called the "Big Five" of reverse mathematics (RCA_0, WKL_0, ACA_0, ATR_0 and Π^1_1-CA_0); moreover, the Big Five turn out to be linearly ordered.

Our novel results regarding wqo inside the general framework of reverse mathematics concern mainly two topics: ordinal analysis of Kruskal's theorems and the equivalence between Higman's and Kruskal's theorems. Regarding the latter, the starting point is the original article by Higman [92] where he proved a general version, concerning abstract algebras, of his celebrated lemma. It is already known that this result, dubbed here Higman's theorem, is equivalent to Kruskal's theorem [138]; our goal is to carry out this equivalence over the weak base theory RCA_0. For what concerns ordinal analysis of Kruskal's theorems, we compute the following two proof-theoretical ordinals, $|\mathrm{RCA}_0 + \mathrm{KT}_\ell(\omega)| = \vartheta(\Omega^{\omega+1})$ and $|\mathrm{RCA}_0 + \forall n\, \mathrm{KT}_\ell(n)| = \vartheta(\Omega^\omega + \omega)$, where $\mathrm{KT}_\ell(\omega)$ denotes standard Kruskal's theorem (see Theorem 2.9) and $\mathrm{KT}_\ell(n)$ a restricted version concerning bounded trees. Roughly speaking, ordinal analysis measures the strength of theories and theorems using large countable ordinals, see [142] for an introduction to the topic. In this thesis, we extend previous investigations made by Rathjen and Weiermann [149] to obtain the aforementioned estimations; in doing so, we take advantages from some recent achievements by Arai [10, 12] regarding the ordinal analysis of well-ordering principles. The novel content of this chapter is based on two joint papers with Andreas Weiermann which have not yet been published.

1.4 Constructive Mathematics

As previously said, one of the core elements in the birth of modern mathematics starting from the early 1900s is the crisis of foundations. The main solution that marked the subsequent developments was Hilbert's formalism with the creation of a theory of proofs, in order to reduce the whole mathematics to finitistic, and thus trustful, means. Nevertheless, other proposals were made. One of the most fruitful was *intuitionism* [96], stemmed from the philosophical reflections of the Dutch mathematician L.E.J. Brouwer. Intuitionism has three main aspects: philosophical, logical and mathematical. As a philosophy of mathematics, intuitionism emphasizes the role of human mind in the construction of mathematical objects which exist as products of our thought; thus it differs from the other two principal philosophical proposals: platonism [109] and formalism [193]. From the logical point of view, intuitionism gives a different interpretation of logical connectives, in particular disjunction and existential quantifier; this interpretation is commonly called the BHK interpretation (from the names of the three mathematicians who developed it: Brouwer, Heyting, Kolmogorov). This reinterpretation of logical connectives is reflected in the mathematical point of view, i.e. daily mathematical practice, where we can see one of the most peculiar characteristics of intuitionism (and constructive mathematics[3] [30] in general): the rejection of the *Law of Excluded Middle*, LEM. This position derives immediately from the intuitionistic interpretation of disjunction: to prove $\varphi \vee \psi$ means to prove either φ or ψ; thus, if we are not able to prove φ nor to refute it (which is the actual situation for the Riemann Hypothesis for example), then we can not assert $\varphi \vee \neg\varphi$. A similar peculiarity holds for the intuitionistic existential quantifier which, to be proved, does not require a proof of mere existence, but a concrete witness. We treat these topics in the first section of Chapter 3.

For what concerns wqo's, reasoning constructively has three main consequences: firstly, some classical definitions are intuitionistically useless, in the sense that only the trivial set with one element satisfies them; secondly, and similarly to what happens in reverse mathematics, equivalences between different definitions no longer hold, or at least they are no longer trivial. This establishes a very rich, and not yet fully charted, picture of the implications between different definitions and the second section of Chapter 3 is dedicated to explore this landscape on the base of a joint work with Ingo Blechschmidt and Peter Schuster [37]. The

[3] Regarding nomenclature, although intuitionism and constructivism are not synonyms, given our constraints and results we reserve to use them as if they were.

third consequence regards the classical proofs of standard results in wqo theory, such as Higman's lemma and Kruskal's theorem, which are not intuitionistically acceptable. The search for constructive proofs started soon and from the early nineties a plethora of results have been obtained [48, 121, 155, 162, 186]; given their applications in computer science, the extraction of the computational content from these proofs [139, 140, 160] also soon began. Following this stream, in Sec. 3.4 we propose a novel constructive definitions for wqo based on bars and prove the corresponding version of Higman's lemma for finite alphabets; these results stem from a joint work with Stefano Berardi e Peter Schuster [19].

Given the limitations of intuitionistic reasoning, inductive approaches (such as the use of bars) are commonly applied in constructive mathematics. In Sec. 3.3, we survey the set theoretical foundation of inductive definitions in the context of constructive set theory [52], exposing under which conditions an inductive definition gives rise to a set.

1.5 Phase Transitions in Proof Theory

Gödel's incompleteness theorems [83] not only shattered Hilbert's programme, at least in its ultimate goal of a finitary foundation of all mathematics, but also revealed the existence of true, yet unprovable, statements. Given the logical nature of Gödel's original sentences a thorough search for finding proper mathematical statements, and not only "artificial" logical ones, which show the undecidability phenomenon soon began. The quest was far from being easy, but finally Paris and Harrington [132], using some previous results due to Kirby and Paris [100] regarding models of Peano Arithmetic, discovered a theorem, concerning colouring of finite subsets, provable in ZFC but not in PA. Soon after, further undecidable results were found, for example the work of Kirby and Paris [101], which will play a relevant role in our results, and the miniaturization of theorems due to Harvey Friedman [89]; Friedman's achievements in particular paved the way for the topic of the fourth and last chapter: Phase Transitions in Proof Theory.

In general terms, a phase transition is a type of behavior wherein small changes of a parameter of a system cause dramatic shifts in some globally observed behavior of the system itself, such shifts being usually marked by a sharp 'threshold point'. (An everyday life example of such thresholds are ice melting and water boiling temperatures.) This kind of phenomena occurs throughout many mathematical and computational disciplines: statistical physics, evolutionary graph theory, percolation theory, computational complexity, artificial intelligence etc.

Since the main relation in proof theory is provability, $T \vdash \varphi$, phase transitions in this context amount mainly to a shift from provability to unprovability. Given an arithmetical assertion $A(r)$ depending on a real parameter $r > 0$, we may ask for which values of r $A(r)$ is provable over a (presumably consistent) arithmetical theory T. Let us suppose that $A(r)$ is true for every $r > 0$, but T-provable only for small values of r; under the additional hypothesis that unprovability is "monotone", namely $T \nvdash A(r)$ and $r' > r$ imply $T \nvdash A(r')$, our goal is to classify the exact real value t at which the transition from T-provability to T-unprovability happens.

An example of such phenomenon is furnished by Friedman's miniaturization of Kruskal's theorem FKT [170] with respect to PA. Although Kruskal's theorem is a second-order statement, since it treats infinite sequences of trees, a miniaturization suitable to first-order is obtainable by restricting the thesis to arbitrary long, but finite, sequences. In the following, $|\cdot|$ denotes the number of nodes and $\preccurlyeq$ tree embeddability (see Def. 2.7):

Theorem 1.2 *(FKT) For every K, there is a number N such that for all finite sequences $T^1, \ldots, T^N$ of finite trees with $|T^i| \leqslant K + i$ for all $i \leqslant N$, there exist indexes i, j such that $1 \leqslant i < j \leqslant N$ and $T^i \preccurlyeq T^j$.*

Theorem 1.2 is true, but unprovable over PA. A parametrized version of FKT is also possible.

Theorem 1.3 *(FKT_r) For every K, there is a number N such that for all finite sequences $T^1, \ldots, T^N$ of finite trees with $|T^i| \leqslant K + r \cdot \log_2(i)$ for all $i \leqslant N$, there exists indexe i, j such that $1 \leqslant i < j \leqslant N$ and $T^i \preccurlyeq T^j$.*

Theorem 1.3 is true for every real number $r \geqslant 0$, but even for $r = 4$ it is not provable in PA; the threshold value ρ in this case it is approximately $0.639578\ldots$ [189] (which is currently not known to be rational, irrational, algebraic or transcendental).

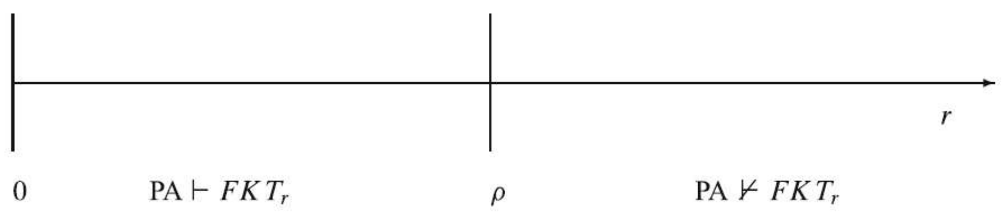


Figure 1.1: Phase transition for FKT_r [118].

In the fourth and last chapter, we treat a generalization of such phenomenon relatively to a statement $A(f)$ parametrized by a number-theoretic function f (assumed to be elementary recursive) instead of a number. Previous hypotheses regarding monotonicity and provability would in this case by applied to f and the phase transition threshold would then be given, not by a number, but by a growing rate.

More precisely, we extend some previous results [118, 130] regarding such phase transitions for the Kirby-Paris principles about Goodstein sequences and Hydra games, as well as for the primitive recursiveness of an Ackermaniann hierarchy. Goodstein sequences and Hydra games concern sequences of, respectively, natural numbers and countable ordinals smaller than ε_0; PA may not be able to prove the termination of such sequences and the phase transition regards this lack of provability. In the case of the Ackermannian hierarchy, the transition is between primitive recursiveness and non primitive recursiveness of the resulting diagonal function. The two problems are closely linked inasmuch they share the same phase transition threshold, consisting in a suitable inverse function obtained from the Hardy hierarchy H_α of fast growing functions [74]. The novel content of this final chapter is based on a joint paper with Andreas Weiermann which has not yet been published.

1.6 Notations and Conventions

We adopt the ordinary notations and conventions of standard mathematics. For example, if I, J are sets, then $I \times J = \{(x, y) \mid x \in I, y \in J\}$ denotes their Cartesian product and, given a binary relation R on I, J, we write R^{-1} for the inverse binary relation $\{(y, x) \in J \times I \mid (x, y) \in R\}$, using the notation $R(x, y)$ or xRy for $(x, y) \in R$. If $\leqslant$, or a similar symbol such as $\preccurlyeq$, denotes an order relation, then the specular symbol denotes the inverse relation; namely $y \geqslant x$ is equivalent to $x \leqslant y$. We use also the common abbreviations for logic systems, such as PA for Peano's arithmetic and ZFC for Zermelo-Fraenkel plus Axiom of Choice; some of these systems will be formally introduced too. For what concerns logic formulas, we adopt the standard notation regarding bounded quantifiers and complexity hierarchies. Namely, given a formula φ in a language $\mathcal{L}$, $\forall x \in a\, \varphi$, $\exists x \in a\, \varphi$, $\forall n < m\, \varphi$ and $\exists n < m\, \varphi$ denote the following abbreviations:

$$\forall x \in a\, \varphi \equiv \forall x\, (x \in a \to \varphi), \qquad \exists x \in a\, \varphi \equiv \exists x\, (x \in a \wedge \varphi),$$
$$\forall n < m\, \varphi \equiv \forall n\, (n < m \to \varphi), \quad \exists n < m\, \varphi \equiv \exists n\, (n < m \wedge \varphi).$$

Moreover, we inductively define the sets Π^0_n, Σ^0_n and Δ^0_n as follows[4]:

1. $\Pi^0_0 = \Sigma^0_0 = \Delta^0_0$ is the set of formulas with only bounded quantifiers;

[4]We observe how, depending on the context, not all bounded quantifiers may be available at once; e.g., in the language of set theory we have, in principle, only $\forall x \in a$ and $\exists x \in a$. In this case we denote the set of the complexity hierarchy simply by Π_n, Σ_n and Δ_n.

2. if $\varphi \in \Pi^0_n$ (resp. Σ^0_n), then $\exists x\, \varphi$ (resp. $\forall x\, \varphi$) is an element of Σ^0_{n+1} (resp. Π^0_{n+1});

3. $\varphi \in \Delta^0_n$ if φ is provably equivalent, with respect to the system under consideration, both to a formula in Π^0_n and in Σ^0_n.

Similarly, we treat the alternation of second-order quantifiers such as $\forall X \varphi$ or $\exists X \varphi$, if they are available; in this case, the corresponding hierarchies are denoted by Π^1_n, Σ^1_n and Δ^1_n. We observe that, in the case of second order arithmetic Z_2, Δ^1_0 is just the set of all arithmetical formulas; i.e. formulas without set quantifiers, but possibly with set parameters.

Finally, we adopt the standard notation for ordinals, e.g., denoting with ω the first infinite ordinals and with Ω the first uncountable ordinal.

Chapter 2

Higman's and Kruskal's Theorems in Reverse Mathematics

This chapter is dedicated to two milestones in the theory of well quasi-orders, Higman's lemma and Kruskal's theorem, and their analysis in the framework of reverse mathematics. By "Reverse Mathematics" we refer to the programme pioneered by Harvey Friedman [73], and subsequently developed by Stephen Simpson and others [168, 169, 173], regarding the classification of "ordinary mathematics" statements by using as benchmark suitable axioms, mainly existential axioms, in the language of second order arithmetic. The reverse path from theorems to the axioms required to prove them is almost as ancient as mathematics itself, one topic for all is the role and the story of Euclid's fifth postulate [91]; nevertheless, the foundational revolution of the first years of twentieth century called for a formal study of this reverse approach. The general aim of reverse mathematics is conceptually simple, quoting Simpson [169, pag. 1]:

> We are especially interested in the question of which set existence axioms are needed to prove the known theorems of mathematics. The scope of this initial question is very broad, but we can narrow it down somewhat by dividing mathematics into two parts. On the one hand there is set-theoretic mathematics, and on the other hand there is what we call "non-set-theoretic" or "ordinary" mathematics. By *set-theoretic mathematics*[1] we mean those branches of mathematics that were created by the set-theoretic revolution which took place approximately a century ago. [...] We identify as *ordinary* or *non-set-theoretic* that body of mathematics which is prior to or independent of the introduction of abstract set-theoretic concepts. [...] We therefore formulate our Main

[1] Here and below the italic is in the original source.

> Question as follows: *Which set existence axioms are needed to prove the theorems of ordinary, non-set-theoretic mathematics*?

The classical reference for reverse mathematics is Simpson's book [169]; for computability and combinatorics in reverse mathematics see Hirschfeldt [94]; whereas for two more recent introductions see Stillwell [173] and Dzhafarov and Mummert [64].

Inside the reverse mathematics programme there are two phenomena which deserved to be highlighted, both regarding the set existential axioms cited by Simpson. The first amounts to the equivalence between the minimal axioms needed in order to prove a theorem and the theorem itself; quoting the founding father of reverse mathematics Harvey Friedman [73, pag. 1]: "When the theorem is proved from the right axioms, the axioms can be proved from the theorem". The second, instead, regards the structure these axioms form. In principle, we could end up with a very intricate and chaotic net; but actually, the majority of ordinary mathematics theorems is equivalent to one of four specific subsystems or provable in a fifth one (the base theory), they are the so-called "Big Five" of reverse mathematics, which in turn are linearly ordered. These two aspects will be briefly explored in the next sections.

In this chapter we work within the "standard" framework of reverse mathematics, namely second order arithmetic and classical logic; nevertheless, there are, at least, two other possible approaches which have been fruitfully explored in the last decades. The first is higher-order reverse mathematics initiated by Ulrich Kohlenbach [102]. As the name suggests, we leave second order arithmetic Z_2 to consider arithmetic in all finite types Z^ω; this greatly expands the expressivity of the language. This higher-order approach have been recently applied by Dag Norman and Sam Sanders in a series of papers [127, 128, 129]. The second is constructive reverse mathematics proposed by Hajime Ishihara [98] and quickly developed by the community of constructive mathematicians [22, 124, 187]; see [61] for a recent survey. Using classical logic, reverse mathematics is not able to discern principles or results which are classically, but not constructively, equivalent; to manage this task, intuitionistic logic is needed. Following this principle, instead of existential axioms, constructive reverse mathematics classifies constructive and non-constructive results with respect to some fixed non-constructive principle such as the Limited Principle of Omniscience, LPO, and its weaker versions (see Chapter 3 dedicated to constructive mathematics for more details regarding LPO).

As the title states, the content of this chapter, whose novel achievements are based on two joint papers with Andreas Weiermann which have not yet been published, regards mainly Higman's and Kruskal's results in Reverse Mathematics. More precisely: previous proof-theoretic investigations concerning Kruskal's theorem [149] are extended in order to treat trees with labels and to compute the proof-theoretic ordinal for the corresponding version of Kruskal's theorem; regarding Higman's results, their connections over RCA_0 with other wqo statements, namely Kruskal's theorem and Dickson's lemma, are explored. For what concerns the structure, the first section is a gentle introduction to reverse mathematics which emphasizes the main technical points needed to work in second order arithmetic; section two is dedicated to Kruskal's theorem in reverse mathematics and in particular to the computation of the proof-theoretic ordinal of the theory RCA_0 extended with two different versions of Kruskal's theorem; the third and last section explores the connection between Higman's and Kruskal's results, establishing their already known equivalence [138] also over the weak base theory RCA_0.

2.1 A Brief Introduction to Reverse Mathematics

To also allow the reader not acquainted with reverse mathematics to benefit from this chapter, we briefly introduce the language of second order arithmetic, list the Big Five of reverse mathematics, expose some classical theorems equivalent to them, and, both as introduction and application, present some results relatively to well quasi-orders.

This section is not meant to be a formal introduction to reverse mathematics nor a compendium of reverse mathematics results for which we refer to [168, 169, 173]; the main goal is to emphasize some technical restrictions related to reverse mathematics, fixing some recurring concepts throughout the chapter.

2.1.1 The Language of Second Order Arithmetic

The formal framework in which standard reverse mathematics works is second order arithmetic and its subsystems which we now present; in this and the next subsection we mainly follow [169, I.2].

Reverse mathematics uses the *language of second order arithmetic* L_2 which is a two-sorted language. The two distinct sorts of variable are: *number variables*, denoted by $a, b, c, \ldots,\ i, j, k, n, m \ldots$ and intended to range over the set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of natural numbers, and *set variables*, denoted by $X, Y, Z \ldots$ and intended to range over some subsets of $\mathbb{N}$. From this two types of variable, numerical terms and atomic formulas are obtained as follows: *numerical terms* are built from number variables using two binary function symbols $+$ and $\cdot$, together with two constant symbols 0 and 1, e.g. if t is a numerical term, then $t + 0$ and $t \cdot 1$ are numerical terms; *atomic formulas* are given by $t_1 = t_2$, $t_1 < t_2$ and $t_1 \in X$, where t_1, t_2 are numerical terms and X a set variable. The intended meaning of function symbols, constants and atomic formulas are respectively: addition, multiplication, the numbers 0 and 1, equality betweens terms, order relation between terms and membership. *Formulas* are built from atomic formulas using: *propositional connectives* $\wedge, \vee, \neg, \rightarrow$; *number quantifiers* $\forall n, \exists n$; and *set quantifiers* $\forall X, \exists X$. The meanings of logical connectives are the standard ones; for what concerns set quantifiers, they range, depending on the model under consideration, over a subset of the power set of the domain of discourse, thus the systems of reverse mathematics are actually two-sorted first order systems. Finally, a *sentence* is a formula without free variables.

Having at our disposal only number variables representing natural numbers and set variables representing sets of natural numbers, a key step in the treatment of ordinary mathematical results, not concerning directly number theory, is an appropriate translation of their statements in the language of L_2, together with a suitable coding in the natural numbers of the mathematical objects they refer to. For example, if we are talking about groups or real functions, then we need to code in L_2 what a group or a real function is; in the latter case this can be highly non trivial (see [169, Definition I.4.6]). For finite trees, with or without labels, the encoding is quite simple; for abstract algebras, presented in Subsec. 2.3.1, some extra caution will be needed.

By *second order arithmetic* Z_2 we mean the set of formulas in L_2 closed under logical deduction and containing the universal closure of the following formulas:

1. Basic axioms:
$$\begin{array}{l} n+1 \neq 0 \\ m+1 = n+1 \;\rightarrow\; m = n \\ m+0 = m \\ m+(n+1) = (m+n)+1 \\ m \cdot 0 = 0 \\ m \cdot (n+1) = (m \cdot n) + m \\ \neg m < 0 \\ m < n+1 \leftrightarrow (m < n \vee m = n) \end{array}$$

2. Induction axiom[2]:
$$0 \in X \;\wedge\; \forall n\,(n \in X \rightarrow n+1 \in X) \;\rightarrow\; \forall n\,(n \in X)$$

3. Comprehension schema:
$$\exists X\, \forall n\, (n \in X \leftrightarrow \varphi(n))$$
where $\varphi(n)$ is any formula in L_2 in which X does not occur free.

[2]Differently from Peano Arithmetic, having at our disposal set variables and comprehension schema, we can express full induction with a single axiom, instead of an axiom schema.

Z_2 is a relatively strong theory, being commonly believed that all theorems of ordinary mathematics are provable in Z_2.[3] Such a theory is thus too strong to serve as a classification tool; namely, a theory T which proves both φ and ψ is not appropriate to establish the proof-theoretical relations between φ and ψ. Hence we consider subsystems of Z_2. A *subsystem* of Z_2 is given by a subset of formulas of Z_2 which is closed under logical deduction; we consider in particular subsystems which are axiomatized by some fragments of the axioms of Z_2.

It turns out that, among the infinite subsystems of Z_2, only a handful are useful in reverse mathematics; the most relevant five are exposed in the next section. Before moving to the Big Five, some model theoretic notes regarding L_2 are in order.

A *model* of L_2 is given by a tuple $M = (|M|, \mathcal{S}_M, +_M, \cdot_M, 0_M, 1_M, <_M)$ which defines the range $|M|$ of number quantifiers, the range $\mathcal{S}_M$ of set quantifiers (a family of subsets of $|M|$) and the interpretations for function symbols, constants ad $\leqslant$ (equality is always interpreted as the diagonal relation). Obviously, the *intended model* $(\mathbb{N}, \mathcal{P}(\mathbb{N}), +, \cdot, 0, 1, <)$ is given by the set $\mathbb{N}$ together with its power set and its standard operations and relations.[4] An ω-*model* is a L_2 model in which the first order part is the standard $\mathbb{N}$, i.e. a model of the form $(\mathbb{N}, \mathcal{S}, +, \cdot, 0, 1, <)$ with $\mathcal{S} \subseteq \mathcal{P}(\mathbb{N})$ and $+, \cdot, 0, 1, <$ interpreted in the standard way; the study of ω-models plays a relevant role in reverse mathematics and we refer to [169] for further considerations.

2.1.2 The "Big Five" of Reverse Mathematics

We list now, from the weakest to the strongest, the Big Five: five subsystems of Z_2 which commonly appear in reverse mathematics. For each, we briefly present: the defining axioms; some metamathematical considerations; some equivalent theorems in ordinary mathematics; and its Π^1_1 proof-theoretical ordinal. Regarding the axioms, since all the five subsystems share the basic ones about the standard arithmetical properties of $+, \cdot, 0, 1, <$, we explicitly state only the remaining ones. For the last point concerning the Π^1_1 ordinal, we refer to Subsec. 2.2.2 for the definition. Finally, given their relevance in this thesis, we focus in particular on RCA_0 and ACA_0.

From now on, we use notations and definitions regarding *bounded* quantifiers $\forall t < n, \exists t < n$ and hierarchies of formulas (e.g. $\Pi^1_2, \Sigma^0_2, \Pi^0_1, \dots$) exposed in Sec. 1.6.

[3] Actually, even more has been supposed, see Harvey Friedman's *grand conjecture* [13].

[4] To keep the notation uniform along the thesis, differently from [169], we denote with $\mathbb{N}$ the "real" set of natural numbers

$\mathbf{RCA_0}$

RCA_0, which stands for Recursive Comprehension Axiom, is the weakest of the Big Five and thus is routinely used as base theory to compare stronger systems or results; namely many results in reverse mathematics have the form $\mathrm{RCA}_0 \vdash \varphi \leftrightarrow \psi$ meaning that, over RCA_0, φ and ψ are equivalent. RCA_0 is obtained by adding to the basic axioms the following:

1. Σ^0_1 induction schema:

$$\varphi(0) \wedge \forall n\, (\varphi(n) \rightarrow \varphi(n+1)) \;\rightarrow\; \forall n\, \varphi(n)$$

   where $\varphi(n)$ is a Σ^0_1 formula;

2. Δ^0_1 comprehension schema:

$$\forall n\, (\varphi(n) \leftrightarrow \psi(n)) \;\rightarrow\; \exists X\, \forall n\, (n \in X \leftrightarrow \varphi(n))$$

   where $\varphi(n)$ is a Σ^0_1 formula and $\psi(n)$ a Π^0_1 formula.

For RCA_0, as well as the other subsystems, the subscript 0 denotes the fact that the system does not have *full induction*, $\varphi(0) \wedge \forall n\, (\varphi(n) \rightarrow \varphi(n+1)) \rightarrow \forall n\, \varphi(n)$ with $\varphi \in L_2$, but only a restricted form of it. In RCA_0 and WKL_0 this amounts to Σ^0_1 induction; whereas the other three systems have the same set induction as Z_2. The name "recursive comprehension" derives from the fact that Δ^0_1 comprehension ensures the existence of recursive subsets of the model; in particular the family REC of all recursive subset of $\mathbb{N}$ is exactly the minimal ω-model of RCA_0 in the sense that the second-order part of every ω-model of RCA_0 contains REC, see [169, Corollary II.1.8].

For a short list of results in ordinary mathematics provable in RCA_0 we have:

Theorem 2.1 *The following ordinary mathematical theorems are provable in RCA_0:*

1. *the Baire category theorem;*
2. *the intermediate value theorem;*
3. *Urysohn's lemma and the Tietze extension theorem for complete separable metric spaces;*
4. *the soundness theorem and a version of Gödel's completeness theorem in mathematical logic;*
5. *the existence of an algebraic closure of a countable field;*

6. *the existence of a unique real closure of a countable ordered field;*

7. *the Banach/Steinhaus uniform boundedness principle.*

Proof see [169, Theorem I.8.3]. □

Given its strong connections with computability theory and Turing machines, and despite the use of excluded middle and other differences [169, Remark I.8.9], RCA_0 corresponds to some extend to Bishop's constructive mathematics [24](regarding this correspondence see also [75]). Finally, for what concerns an ordinal measure of the strength of RCA_0, the Π^1_1 ordinal of RCA_0 is ω^ω.

$\mathbf{WKL_0}$

WKL_0, which stands for Weak König's Lemma, is the second subsystem of Z_2 we briefly consider. As the name suggests, its definition is connected with the weak König's lemma which we now state. Let $2^{<\mathbb{N}}$ denote the full binary tree, i.e. the set of (codes for) finite sequences of 0's and 1's which is definable in RCA_0; *weak König's lemma* reads: "Every infinite subtree of $2^{<\mathbb{N}}$ has an infinite path". WKL_0 amounts to RCA_0 plus weak König's lemma.

We now list a series of results equivalent to WKL_0 over RCA_0.

Theorem 2.2 *Over RCA_0, WKL_0 is equivalent to each of the following ordinary mathematical statements:*

1. *Every continuous real-valued function on* $[0, 1]$*, or on any compact metric space, is bounded;*

2. *Every continuous real-valued function on* $[0, 1]$*, or on any compact metric space, is uniformly continuous;*

3. *The maximum principle: Every continuous real-valued function on* $[0, 1]$*, or on any compact metric space, has a supremum;*

4. *The local existence theorem for solutions of ordinary differential equations;*

5. *Gödel's completeness theorem: every finite, or countable, set of sentences in the predicate calculus has a countable model;*

6. *Every countable commutative ring has a prime ideal;*

7. *Every countable field (of characteristic 0) has a unique algebraic closure;*

8. *Every countable formally real field is orderable;*

9. *Every countable formally real field has a (unique) real closure;*

10. *Brouwer's fixed point theorem: Every uniformly continuous function* $\phi\colon [0,1]^n \to [0,1]^n$ *has a fixed point.*

Proof see [169, Theorem I.10.3]. □

From a metamathematical perspective [169, Remark IX.3.18], WKL_0 corresponds to some extend to Hilbert's programme of finitistic reductionism [93] (regarding this correspondence see also [167]). Differently from RCA_0, WKL_0 does not have a minimal ω-model [169, Corollary VIII.2.8]; nevertheless, its Π^1_1 ordinal is the same of RCA_0, namely ω^ω.

$\mathbf{ACA}_0$

ACA_0, which stands for Arithmetical Comprehension Axiom, is the third subsystem of the Big Five and, together with RCA_0, plays a prominent role in reverse mathematics. Its axioms are the same of Z_2, but with the comprehension schema restricted to arithmetical formulas (hence the name); we recall that a formula is arithmetical if it has no set quantifier (set variables are nonetheless allowed as parameters). As before, we shortly list some results equivalent to ACA_0 over RCA_0.

Theorem 2.3 *Over* RCA_0*,* ACA_0 *is equivalent to each of the following ordinary mathematical statements:*

1. *Every bounded, or bounded increasing, sequence of real numbers has a least upper bound;*

2. *The Bolzano/Weierstraß theorem: Every bounded sequence of real numbers, or of points in* $\mathbb{R}^n$*, has a convergent subsequence;*

3. *Every sequence of points in a compact metric space has a convergent subsequence;*

4. *The Ascoli lemma: Every bounded equicontinuous sequence of real-valued continuous functions on a bounded interval has a uniformly convergent subsequence;*

5. *Every countable commutative ring has a maximal ideal;*

6. *Every countable vector space over* $\mathbb{Q}$*, or over any countable field, has a basis;*

7. *Every countable field of characteristic 0 has a transcendence basis;*

8. *Every countable Abelian group has a unique divisible closure;*

9. *König's lemma: Every infinite, finitely branching tree has an infinite path;*

10. *Ramsey's theorem for colourings of* $[\mathbb{N}]^3$*, or of* $[\mathbb{N}]^4$*,* $[\mathbb{N}]^5$*, . . .*

Proof see [169, Theorem I.9.3]. □

Given its relevance in this thesis, we separately mention the fact that also Higman's lemma is equivalent, over RCA_0, to ACA_0 [169, Theorem X.3.22].[5]

ACA_0 is tightly connected with Peano Arithmetic [169, Remark I.3.3]. More precisely, ACA_0 is a *conservative extension* of PA; this means that, for any sentence σ in the language of first order arithmetic, σ is a theorem of PA if and only if σ is a theorem of ACA_0. Said in other words, PA is the first order part of ACA_0.

Finally, the Π^1_1 ordinal of ACA_0 is ε_0, the same as the ordinal of PA.

ATR_0

ATR_0, which stands for Arithmetical Transfinite Recursion is the fourth subsystem of Z_2 we briefly consider. Given the technical nature of its defining axiom schema, namely the Arithmetical Transfinite Recursion schema, and the fact that we do not use ART_0 in this thesis, we omit the formal presentation of the axiom schema.

For a short list of results equivalent to ATR_0 we have

Theorem 2.4 *Over* RCA_0*,* ATR_0 *is equivalent to each of the following ordinary mathematical statements:*

1. *Any two countable well orderings are comparable;*
2. *Ulm's theorem: Any two countable reduced Abelian p-groups which have the same Ulm invariants are isomorphic;*
3. *The perfect set theorem: Every uncountable closed, or analytic, set has a perfect subset;*
4. *Lusin's separation theorem: Any two disjoint analytic sets can be separated by a Borel set;*
5. *The domain of any single-valued Borel set in the plane is a Borel set;*
6. *Every open, or clopen, subset of* $\mathbb{N}^{\mathbb{N}}$ *is determined;*
7. *Every open, or clopen, subset of* $[\mathbb{N}]^{\mathbb{N}}$ *has the Ramsey property.*

Proof see [169, Theorem I.11.5]. □

Finally, the Π^1_1 ordinal of ATR_0 is Γ_0, see [77] for a survey on this specific ordinal.

[5] In this reference, Higman's lemma is dubbed "Higman's theorem".

Π^1_1-CA$_0$

Π^1_1-CA$_0$, which stands for Π^1_1 Comprehension Axiom, is the last and strongest subsystem of the Big Five. Its axioms are the same of Z_2, but with the comprehension schema restricted to Π^1_1 formulas.

For a short list of results equivalent to Π^1_1-CA$_0$ we have

Theorem 2.5 *Over RCA$_0$, Π^1_1-CA$_0$ is equivalent to each of the following ordinary mathematical statements:*

1. *Every tree has a largest perfect subtree;*
2. *The Cantor/Bendixson theorem: Every closed subset of $\mathbb{R}$, or of any complete separable metric space, is the union of a countable set and a perfect set;*
3. *Every countable Abelian group is the direct sum of a divisible group and a reduced group;*
4. *Every difference of two open sets in the Baire space $\mathbb{N}^{\mathbb{N}}$ is determined;*
5. *Every G_δ set in $[\mathbb{N}]^{\mathbb{N}}$ has the Ramsey property.*

Proof see [169, Theorem I.9.4]. □

Regarding ordinal analysis, the Π^1_1 ordinal of Π^1_1-CA$_0$ is $\psi_\Omega(\Omega_\omega)$, see [176] for this non trivial result.

Other subsystems, in particular weaker than RCA$_0$, have been studied in Reverse Mathematics [169, X.4.]. Finally, given the abundance of different subsystems, we adopt the standard notation in Reverse Mathematics literature regarding the subsystem in which a result is obtained; namely if a statement starts with one of the aforementioned subsystems in parenthesis, then the proof can be made in that subsystem.

2.1.3 Well Quasi-Orders in Reverse Mathematics

Given the crucial role played by well quasi-orders in our results, we dedicate this paragraph to their formal introduction in RCA$_0$ as well as to a first analysis of their properties. All definitions are given in RCA$_0$.

Definition 2.1 *A* QUASI-ORDER, qo, $(|Q|, \leqslant)$ *is given by a subset* $|Q| \subseteq \mathbb{N}$ *together with a binary relation* $\leqslant \subseteq |Q| \times |Q|$ *which is reflexive and transitive; if in addition* $\leqslant$ *is antisymmetric, then* $(Q, \leqslant)$ *is a* PARTIAL ORDER, po.

In the following, we denote $|Q|$ simply by Q and we may denote with Q also the qo $(Q, \leqslant)$, omitting the quasi-order relation $\leqslant$. Moreover, we can take Def. 1.2, regarding auxiliary concepts for qo, and Def. 1.3 for wqo as they stand since they are already suitable for RCA_0.

As already mentioned in Proposition 1.1, many different definitions have been proposed for well quasi-orders; in his classical historical survey [107], J. Kruskal referred to wqo as a frequently discovered concept. It is therefore natural to ask if all these definitions are equivalent even in Reverse Mathematics, in particular over weak theories like RCA_0, or WKL_0. This problem has been thoroughly treated by Cholak et al. [43] and by Marcone [113, 114]; we now briefly summarize their results.

Let us consider the following definitions for wqo.

Definition 2.2 *Let $(Q, \leqslant)$ be a qo, then Q is:*

1. *a* SEQUENTIALLY WELL QUASI-ORDER, *wqo(set), if every sequence $(q_k)_k$ in Q has an infinite ascending subsequence, i.e. there are indices $k_0 < k_1 < \dots$ such that $q_{k_i} \leqslant q_{k_j}$ whenever $i < j$;*

2. *an* ANTICHAIN WELL QUASI-ORDER, *wqo(anti), if Q has no infinite descending chains and no infinite antichains.*

3. *an* EXTENSIONAL WELL QUASI-ORDER, *wqo(ext), if every linear extension $\preccurlyeq$ of $\leqslant$ is well-founded;*

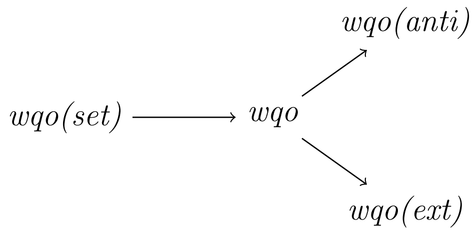
4. *wqo(fbp) if Q has the* FINITE BASIS PROPERTY, *i.e. every closed subset is finitely generated.*

With some slight and harmless variations, to take into account constructive logic, these and other definitions will be considered in Chapter 3, more precisely in Subsec. 3.2.2.

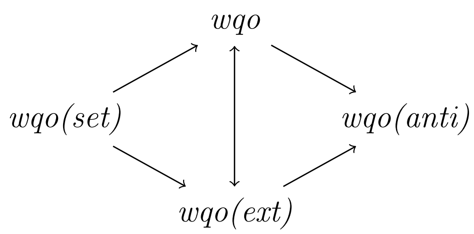
For what concerns the relations over RCA_0, WKL_0 and ACA_0 between these definitions, the results in [43, 113, 114] can be summarized in the following theorem.

Theorem 2.6 *(Cholak, Marcone, Solomon) Consider the previous definitions: wqo, wqo(set), wqo(anti), wqo(ext), wqo(fbp). Then:*

RCA_0 *wqo is equivalent to wqo(fbp) and all the other relations are exhaustively exposed in the following schema, namely no arrow can be inverted.*



$\mathbf{WKL}_0$ *The exact implications over WKL_0 are exposed in the following schema.*



$\mathbf{ACA}_0$ *All the definitions are equivalent.*

Proof see [43, 113, 114]. □

Given their good properties, one of the main problems in the theory of well quasi-orders concerns how to obtain new wqo's or, equivalently, how to preserve the property of being wqo. Two standard operations on qo are *product* and *(disjoint) union.*

Definition 2.3 *Let $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$ be* qo*, then we define:*

1. *the* (DISJOINT) UNION $(P \dot{\cup} Q, \leqslant_{P \dot{\cup} Q})$ *with*

$$p \leqslant_{P \dot{\cup} Q} q :\Leftrightarrow (p, q \in P \wedge p \leqslant_P q) \vee (p, q \in Q \wedge p \leqslant_Q q);$$

2. *the* PRODUCT $(P \times Q, \leqslant_{P \times Q})$ *with*

$$(p_1, q_1) \leqslant_{P \times Q} (p_2, q_2) :\Leftrightarrow p_1 \leqslant_P p_2 \wedge q_1 \leqslant_Q q_2.$$

We may omit the word "disjoint"; for other possible quasi-order operations, e.g., the *sum* $P + Q$, see [114].

We consider now the closure of wqo under product, union and subsets, starting with the good behavior of union.

Lemma 2.1 *(Marcone) Let $\mathcal{P}$ be any of the property* wqo*,* wqo*(set),* wqo*(anti) or* wqo*(ext); if $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$ satisfy property $\mathcal{P}$, then RCA_0 suffices to prove that $(P \dot{\cup} Q, \leqslant_{P \dot{\cup} Q})$ has property $\mathcal{P}$.*

Proof see [114]. □

Except for wqo(ext), a similar well behavior hold for subsets.

Lemma 2.2 *Let $\mathcal{P}$ be any of the property wqo, wqo(set), wqo(anti); if $(Q, \leqslant_Q)$ satisfy property $\mathcal{P}$ and $P \subseteq Q$, then RCA_0 suffices to prove that $(P, \leqslant_Q)$ has property $\mathcal{P}$.*

Proof see [114]. □

The statement of the previous lemma for wqo(ext) is still open, see [114, Question 2.15]; similarly, it is still open in the context of constructive mathematics, see Subsec. 3.2.2. In the case of the product the situation is far more complex, more precisely we have the following.

Theorem 2.7 *(Cholak, Marcone, Solomon) Let $\mathcal{P}$ be any of the property wqo, wqo(anti) or wqo(ext). The following hold:*

- *if $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$ are wqo(set), then RCA_0 suffices to prove that $(P \times Q, \leqslant_{P\times Q})$ is wqo(set);*
- *if $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$ have property $\mathcal{P}$, then WKL_0 does not suffice to prove that $(P \times Q, \leqslant_{P\times Q})$ has property $\mathcal{P}$.*

Proof see [43, 114]. □

This limitations regarding the product of wqo will partially affect the proof of Theorem 2.24. We consider now preservation of wqo with respect to functions, starting with the following definition.

Definition 2.4 *Given two qo $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$, a function $\phi\colon P \to Q$ is:*

1. ORDER-PRESERVING *if $p_1 \leqslant_P p_2$ implies $\phi(p_1) \leqslant_Q \phi(p_2)$;*
2. ORDER-REFLECTING *if $\phi(p_1) \leqslant_Q \phi(p_2)$ implies $p_1 \leqslant_P p_2$;*
3. *an* ORDER ISOMORPHISM *if it is an order-preserving, order-reflecting bijection.*

Regarding wqo preservation with respect to such order functions, we have the following result which, to the best of our knowledge, it is novel in the current literature.

Proposition 2.1 *(RCA_0) Let $\mathcal{P}$ be any of properties wqo, wqo(set), wqo(anti) or wqo(ext) and let P and Q be two qo and let ϕ be a function $\phi\colon P \to Q$,*

1. *if P has the property $\mathcal{P}$ and ϕ is an order-preserving surjection then Q has the property $\mathcal{P}$;*

2. *if Q has the property $\mathcal{P}$, with $\mathcal{P} \neq$ wqo(ext), and ϕ is an order-reflecting map then P has the property $\mathcal{P}$.*

Proof We start with the first point, i.e. ϕ order-preserving surjection, considering all the cases for $\mathcal{P}$.

[P wqo] Let $(q_k)_k$ be an infinite sequence in Q, since ϕ is surjective we can find (also in RCA_0) an infinite sequence $(p_k)_k$ in P such that for all n, $\phi(p_n) = q_n$; but P is wqo, thus there exist indexes $i < j$ such that $p_i \leqslant_P p_j$ and, since ϕ is order-preserving, we obtain $q_i = \phi(p_i) \leqslant_Q \phi(p_j) = q_j$.

[P wqo(set) or P wqo(anti)] The previous strategy works here too.

[P wqo(ext)] In order to keep the notation readable we consider the case P, Q partial orders. Let $\preccurlyeq_Q$ be a linear extension of $\leqslant_Q$, we have to prove $\preccurlyeq_Q$ well-founded. For each element $q \in Q$, we consider the subset $P_q = \{p \in P \mid \phi(p) = q\}$ together with the restriction to P_q of $\leqslant_P$; by Szpilrajn's theorem, available in RCA_0 ([62, Observation 6.1], see also [76]), we can consider for each $q \in Q$ a linear extension $\trianglelefteq_q$ of $(P_q, \leqslant_P \downharpoonleft P_q)$. We define now the following order on P:

$$p_1 \preccurlyeq_P p_2 :\Leftrightarrow \phi(p_1) \prec_Q \phi(p_2) \vee (\phi(p_1) = \phi(p_2) \wedge p_1 \trianglelefteq_{\phi(p_1)} p_2).$$

It is a straightforward verification to check that $\preccurlyeq_P$ is a linear extension of $\leqslant_P$ and $p_1 \preccurlyeq_P p_2$ implies $\phi(p_1) \preccurlyeq_Q \phi(p_2)$.

Since $\preccurlyeq_P$ is a linear order extending $\leqslant_P$ and P is wqo(ext), then $\preccurlyeq_P$ is a well-order. Let us assume, by contradiction, that $q_1 \succ_Q q_2 \succ_Q \ldots$ is a strictly descending chain in $(Q, \preccurlyeq_Q)$, since ϕ is surjective we can find a sequence $p_1, p_2, \ldots$ such that $\phi(p_n) = q_n$ for all n; but $\preccurlyeq_P$ is a well-order, thus there exist $i < j$ such that $p_i \preccurlyeq p_j$ and then $\phi(p_i) \preccurlyeq_Q \phi(p_j)$, contradiction.

Let us consider the second point, namely ϕ order-reflecting.

[Q wqo] Let $(p_k)_k$ be an infinite sequence in P, then $(\phi(p_k))_k$ is an infinite sequence in Q and thus there exist indexes $i < j$ such that $\phi(p_i) \leqslant_Q \phi(p_j)$; but, since ϕ is order-reflecting, this implies $p_i \leqslant_P p_j$.

[P wqo(set) or P wqo(anti)] The previous strategy works here too. □

As before, the case wqo(ext) is still open for an order-reflecting map ϕ. Finally, the fact that, even in classical mathematics, not all operations preserve the property of being a wqo (for example if we consider infinite sequences [141]), is one of the main reasons which motivated the introduction of *better quasi-orders* [42, 123].

2.2 Kruskal's Theorem in Reverse Mathematics

Kruskal's theorem [106] is a milestone in the theory of well-quasi orders, with ramified applications in many different areas, such as term rewriting [58, 59] and mathematical logic [77, 165]. This section, based on a joint work with Andreas Weiermann which has not yet been published, is dedicated to one of the main results of the thesis, namely the computation of the proof-theoretic ordinal of various versions of Kruskal's theorem.

Extending previous proof-theoretic investigations on this topic (mainly [149]), we calculate the Π^1_1 ordinals of two different versions of labelled Kruskal's theorem. More precisely, the following ordinal estimations are obtained: $|\mathrm{RCA}_0 + \forall n\, \mathrm{KT}_\ell(n)| = \vartheta(\Omega^\omega + \omega)$ and $|\mathrm{RCA}_0 + \mathrm{KT}_\ell(\omega)| = \vartheta(\Omega^{\omega+1})$. In the previous formulas, ϑ is a so-called collapsing function (see [149] for a detailed introduction) used in ordinal notations for large countable ordinals [33, 35]; while $\forall n\, \mathrm{KT}_\ell(n)$ and $\mathrm{KT}_\ell(\omega)$ denote, respectively, the conjunction of all the cases of labelled Kruskal's theorem for trees with an upper bound on the branching degree, i.e. labelled trees with a fixed upper bound on the number of children of each node, and the standard Kruskal's theorem for labelled trees, see Theorem 2.9. The two ordinals imply that the conjunction of all the finite cases, i.e. $\forall n\, \mathrm{KT}_\ell(n)$, is strictly weaker then the infinite case, $\mathrm{KT}_\ell(\omega)$; thus, the situation differs from the unlabelled case, thoroughly treated by Michael Rathjen and Andreas Weiermann in their proof-theoretical investigations [149], where, over RCA_0, $\forall n\, \mathrm{KT}(n)$ and $\mathrm{KT}(\omega)$ are equivalent.

In order to perform the above calculations, a key step is to move from Kruskal's theorem, which concerns preservation of wqo's, to an equivalent Well-Ordering Principle (WOP), dealing with instead preservation of well-orders; for an introduction to WOP see [7] and [150]. Roughly speaking, given an ordinal function $g : \Omega \to \Omega$, $\mathrm{WOP}(g)$ amounts to $\forall \mathfrak{X}\, [\mathrm{WO}(\mathfrak{X}) \to \mathrm{WO}(g(\mathfrak{X}))]$, where $\mathrm{WO}(\mathfrak{X})$ stands for "$\mathfrak{X}$ is a well-ordering", i.e. $\mathfrak{X}$ is a well-founded total order.[6] In our case, the two ordinal functions involved are $g_\forall(\mathfrak{X}) := \sup_n \vartheta(\Omega^n \cdot \mathfrak{X})$ and $g_\omega(\mathfrak{X}) := \vartheta(\Omega^\omega \cdot \mathfrak{X})$. The main tool used to achieve a proper analysis of the two related WOPs is an extension of a result, due to Arai [12, Theorem 3], regarding the proof-theoretic ordinal of a Well-Ordering Principle; namely, keeping the same thesis, we weaken the hypotheses of Arai's theorem to include the two ordinal functions risen from Kruskal's theorem. Given our proof of the aforementioned extension, i.e. a careful rereading of Arai's one, having at hand [12] could be very helpful.

2.2.1 Trees and Kruskal's Theorem in RCA_0

We start by recalling some standard definitions regarding trees, tree embedding and branching degree; as before, all definitions are stated in RCA_0.

Definition 2.5 *Given a set Q, we inductively define the set $\mathbb{T}(Q)$ of (finite ordered)* TREES *with* LABELS *in Q as follows:*

[6] We use the new font $\mathfrak{X}$ instead of X to emphasize that $\mathfrak{X}$ is a set with an associated order and to comply with a common notation in the literature [150, 145].

1. *for each* $q \in Q$, $q[]$ *is an element of* $\mathbb{T}(Q)$*;*

2. *if* $t_1, \ldots, t_k$*, with* $k > 0$*, is a sequence of elements of* $\mathbb{T}(Q)$ *and* $q \in Q$*, then* $t := q[t_1, \ldots, t_n]$ *is an element of* $\mathbb{T}(Q)$*.*

Since all trees we consider are finite and ordered, we omit these specifications. Connected to labelled trees, there are the following definitions.

Definition 2.6 *Let* Q *and* $\mathbb{T}(Q)$ *be as before, then:*

- *if* $t = q[t_1, \ldots, t_n]$*, then* q *is the* LABEL *of the root and* $t_1, \ldots, t_n$ *are called the* (IMMEDIATE) SUBTREES *of* t*;*

- *if* Q *is a singleton, then* $\mathbb{T} := \mathbb{T}(Q)$ *is the set of* UNLABELLED *trees;*

- *if* $t \in \mathbb{T}(Q)$*, we inductively define the set* $\mathcal{N}(t)$ *of* NODES[7] *of* t*:*

  1. *if* $t = q[]$*, then* $\mathcal{N}(t) := \{q[]\}$*;*
  2. *if* $t = q[t_1, \ldots, t_n]$*, then* $\mathcal{N}(t) := \{q[t_1, \ldots, t_n]\} \cup \mathcal{N}(t_1) \cup \cdots \cup \mathcal{N}(t_n)$*.*

Starting from a qo Q allows to define an embeddability relation.

Definition 2.7 *Given a qo* $(Q, \leqslant_Q)$ *and* $t, s \in \mathbb{T}(Q)$*, we inductively define the embeddability relation* $\preccurlyeq$ *on* $\mathbb{T}(Q)$ *a follows;* $t \preccurlyeq s$ *holds if:*

1. $t = p[]$, $s = q[]$ *and* $p \leqslant_Q q$*; or*

2. $s = q[s_1, \ldots, s_m]$ *and* $t \preccurlyeq s_i$ *for some* $1 \leqslant i \leqslant m$*; or*

3. $t = p[t_1, \ldots, t_n]$, $s = q[s_1, \ldots, s_m]$, $p \leqslant_Q q$ *and there exist* $1 \leqslant i_1 < \cdots < i_n \leqslant m$ *such that* $t_k \preccurlyeq s_{i_k}$ *for all* $1 \leqslant k \leqslant n$*.*

We observe that $(\mathbb{T}(Q), \preccurlyeq)$ is a quasi-order.

Before stating Kruskal's theorems, we need one last definition: branching degrees.

Definition 2.8 *Let* $t \in \mathbb{T}(Q)$ *and let* $s = p[s_1, \ldots, s_m]$ *be a node of* t*, then we define:*

- $l(s) := p$ *is the* LABEL *of* s*;*

- $deg(s) := m$ *is the* DEGREE *of* s*;*

[7]This is not the standard definition of nodes, e.g. the tree $q\,[p[], p[]]$ has only two nodes $q\,[p[], p[]]$ and $p[]$; nevertheless, it fits our definition of branching degree.

- *$Deg(t) := \max\{deg(s) \mid s \in \mathcal{N}(t)\}$ is the* BRANCHING DEGREE *of the tree t.*

Moreover, for every $n \in \mathbb{N}$ and every set Q, we define:

- *$\mathbb{T}_n$ is the set of unlabelled trees with branching degree less or equal to n;*
- *$\mathbb{T}_n(Q)$ is the set of trees with labels in Q and branching degree less or equal to n.*

Since we consider only finite trees, *deg* and *Deg* are always well defined.

We can now state the various versions of Kruskal's theorem we are interested in; each of them is denoted by an abbreviation, possibly with a number parameter.

Theorem 2.8 *The following statements hold with n a natural number:*

KT(n): *$(\mathbb{T}_n, \preccurlyeq)$ is a wqo;*

KT(ω): *$(\mathbb{T}, \preccurlyeq)$ is a wqo;*

KT$_\ell$(n): *if Q is a wqo, then $(\mathbb{T}_n(Q), \preccurlyeq)$ is a wqo;*

KT$_\ell$(ω): *if Q is a wqo, then $(\mathbb{T}(Q), \preccurlyeq)$ is a wqo.*

Starting from the original paper by Kruskal [106], proofs of Kruskal's theorem, or its variation, are ubiquitous in the literature [87, 122, 171, 186]. For what concerns its strength from the reverse mathematics point of view, by a result due to Harvey Friedman [165](see also [77]), it is known that even Kruskal's theorem for unlabelled trees (KT(ω) in our notation), as well as its finite miniaturization [165, 170], is not provable in ATR_0. A thorough investigation of the unlabelled versions of Kruskal's theorem has been carried out by Rathjen and Weiermann [149], their main results can be summarized in the following theorem

Theorem 2.9 *(Rathjen and Weiermann)*

$$RCA_0 \vdash \forall n\, KT(n) \leftrightarrow KT(\omega) \leftrightarrow WO(\vartheta\Omega^\omega) \leftrightarrow \Pi^1_1\text{-}RFN(\Pi^1_2\text{-}BI_0).$$

In the previous statement, Π^1_1-$RFN(\Pi^1_2$-$BI_0)$ denotes the *uniform reflection principle* for Π^1_1 formulas of the theory Π^1_2-BI_0, which amounts to RCA_0 extended with bar induction for Π^1_2 formulas, see [149, Section 11] for more details. $\mathrm{WO}(\vartheta\Omega^\omega)$ instead denotes the well-orderedness of the countable ordinal $\vartheta\Omega^\omega$, where ϑ is a so-called *collapsing function*, see [33, 149, 184] for an introduction to such and similar functions.

In the next paragraph, we extend the results concerning proof ordinals to the labelled case.

2.2.2 Ordinal Analysis and Well-Ordering Principles

We first briefly introduce two central concepts in our results, *Ordinal Analysis* and *Well-Ordering Principles.*

The origin of ordinal analysis can be tracked back to Gentzen [79, 80] who showed that transfinite induction up to the ordinal

$$\varepsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \dots\}$$

suffices to prove the consistency of PA; moreover, he proved that ε_0 is the best possible choice in the sense that PA proves transfinite induction up to α for arithmetic formulas for any $\alpha < \varepsilon_0$. Thus, the idea is that ε_0 in some sense "measures" the consistency strength of PA.

From the seminal works of Gentzen, ordinal analysis has grown enormously both in results and methods; still, one of the goals, probably the most known, is roughly to "attach ordinals in a given representation system to formal theories" [142, Pag. 1]. The most commonly attached ordinal is the Π^1_1 ordinal which, for most "natural" theories T,[8] equals the supremum of the provable recursive well-orderings of T, namely

$$|T|_{\Pi^1_1} := \sup\{ot(\prec) \mid \prec \text{ is recursive and } T \vdash \mathrm{WO}(\prec)\},$$

where $ot(\prec)$ is the *order type* of $\prec$ (see [55, 158]), and the encoding of $\prec$ and $\mathrm{WO}(\prec)$ may change on the base of T, e.g. if T is a first- or second-order theory. By Spector's Σ^1_1-boundedness theorem, $|T|_{\Pi^1_1} < \omega_1^{ck}$ whenever T is Σ^1_1-sound, where the Church-Kleene ordinal ω_1^{ck} denotes the least non-recursive ordinal. For sake of readability, we denote $|T|_{\Pi^1_1}$ simply by $|T|$; for further readings on ordinal analysis, we refer to [11, 142, 144].

Well-ordering principles, which regard the preservation of well-orderedness by an ordinal function, are a crucial tool for our ordinal analysis of Kruskal's theorem; their precise definition is as follows.

Definition 2.9 *Given an ordinal function $\mathfrak{g}\colon \Omega \to \Omega$, and denoted with $WO(\mathfrak{X})$ the well-ordering of $\mathfrak{X}$, the* WELL-ORDERING PRINCIPLE *of $\mathfrak{g}$, $WOP(\mathfrak{g})$, amounts to the following statement*

$$\forall \mathfrak{X}\ [WO(\mathfrak{X}) \to WO(\mathfrak{g}(\mathfrak{X}))]\,.$$

The study of well-ordering principles can be traced back to Girard [81] where the following equivalence was obtained

[8] A formal and rigorous definition of naturalness for a logical theory is still an open problem.

Theorem 2.10 *(Girard[81]) Over RCA_0, ACA_0 is equivalent to WOP($\lambda\mathfrak{X}.\omega^{\mathfrak{X}}$).*[9]

Similar equivalences for other subsystems of second order arithmetic have been achieved; for example the following two, whose original proofs were based on a recursion-theoretic approach.

Theorem 2.11 *(Marcone and Montalbán[115]) Over RCA_0, ACA_0^+ is equivalent to WOP($\lambda\mathfrak{X}.\varepsilon_{\mathfrak{X}}$).*

Theorem 2.12 *(Friedman, Montalbán and Weiermann) Over RCA_0, ATR_0 is equivalent to WOP($\lambda\mathfrak{X}.\varphi\mathfrak{X}0$).*

The connections between well-ordering principles and existence of suitable ω-models have been subsequently explored by Michael Rathjen and co-authors in a series of papers [7, 145, 146, 147, 148, 150]; more recently, Anton Freund studied how Π^1_1-comprehension and well-ordering principles are correlated [68, 69, 71]. The results in the aforementioned articles, e.g., $|\mathrm{ACA}_0| = |\mathrm{WOP}(\lambda\mathfrak{X}.\omega^{\mathfrak{X}})| = \varepsilon_0$ [81], $|\mathrm{ATR}_0| = |\mathrm{WOP}(\lambda\mathfrak{X}.\varphi\mathfrak{X}0)| = \Gamma_0$ on one side and $|\mathrm{ACA}_0^+| = |\mathrm{WOP}(\lambda\mathfrak{X}.\varepsilon_{\mathfrak{X}})|$ [115], $|\mathrm{ATR}_0^+| = |\mathrm{WOP}(\lambda\mathfrak{X}.\Gamma_{\mathfrak{X}})|$ [145] on the other, suggest the existence of some general schemas. Such schemas have been exposed by Arai in [10, 12] where, for a normal function g satisfying suitable term conditions [12, Def.3 and Def.4] and its derivative g' (i.e. the function which enumerates the fixed points of g), the following theorems have been proven:

Theorem 2.13 *(Arai[12]) $|ACA_0 + WOP(g)| = g'(0) = \min\{\alpha \mid g(\alpha) = \alpha\}$.*

Theorem 2.14 *(Arai[12]) Over ACA_0, the following are equivalent:*

- *WOP(g');*
- *(WOP(g))$^+$;*

where (WOP(g))$^+$ means that every set is contained in a countable coded ω-model of ACA_0 + WOP(g), see [12, Definition 2] for a detailed definition.

We develop now the theoretical tools needed for our goal. As already mentioned in the introductory part of this section, a key step in our ordinal analysis of labelled Kruskal's theorem is to move from Kruskal's result, which is about preservation of wqo, to an equivalent well-ordering principle, regarding instead well-orders.

[9] Here and below we use the λ-notation, namely $\lambda\mathfrak{X}.\phi(\mathfrak{X})$, with $\phi(\mathfrak{X})$ an ordinal term containing $\mathfrak{X}$, represents the function $\phi\colon \Omega \to \Omega$ sending α to $\phi(\alpha)$. For example $\lambda\mathfrak{X}.\varepsilon_{\mathfrak{X}}$ is the ordinal function "counting" the epsilon numbers, i.e. ε_0 is the first epsilon number, ε_1 the second one and so on.

Although the literature regarding well-ordering principles is already well established [7, 10, 12, 69, 81, 115, 145, 146, 147, 148, 150], the WOP's required for our case, and their proof-theoretic analysis, have not been presented yet; the gap is filled in this section where the following ordinal estimation

$$|\mathrm{ACA}_0 + \mathrm{WOP}(\mathsf{g})| = \mathsf{g}'(0) = \sup_n \mathsf{g}^n(0) = \min\{\alpha > 0 \mid \forall \beta < \alpha \ \mathsf{g}(\beta) < \alpha\}$$

is achieved for a class of ordinal functions g larger than the one studied by Arai in [12], e.g., the two ordinal functions considered below.

We obtain the aforementioned estimation by extending a previous result due to Arai [12, Theorem 3]; moreover, preparing this section, we glimpsed another possible approach which instead uses an equivalence lemma, proved by Pakhomov and Walsh [131, Lemma 3.8], relating well-ordering principles and well-ordering rules.

Extending a result by Arai

In [12], Arai studied the proof-theoretic ordinal of $\mathrm{ACA}_0 + \mathrm{WOP}(\mathsf{g})$ for a *normal function* g, namely for a strictly increasing and continuous ordinal function. More precisely, given a normal function g and denoting with g' its derivative, i.e. the ordinal function enumerating the fixed points of g, if g and g' satisfy some term properties [12, Def. 3 and Def. 4], then the following ordinal computation holds [12, Theorem 3]:

$$|\mathrm{ACA}_0 + \mathrm{WOP}(\mathsf{g})| = \mathsf{g}'(0) = \min\{\alpha \mid \mathsf{g}(\alpha) = \alpha\}$$

We aim to extend this result, weakening the conditions required for g.

Keeping the same notation as in [12], we consider a computable function $\mathsf{g}\colon \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ which sends a linear order $<_X = \{(n,m) \mid \langle n,m\rangle \in X\}$ to a linear order $<_{\mathsf{g}(X)} = \{(n,m) \mid \langle n,m\rangle \in \mathsf{g}(X)\}$[10]; however, since we consider functions which may not be normal, we define $\mathsf{g}'(0)$ not as its first fixed point (which might not exist), but directly as the first ordinal closed under g, namely $\mathsf{g}'(0) := \sup_n \mathsf{g}^n(0) = \min\{\alpha > 0 \mid \forall \beta < \alpha \ \ \mathsf{g}(\beta) < \alpha\}$. Differently from [12], for g we require only the following properties:

1. g is weakly increasing, i.e. $\alpha \leqslant \beta \ \Rightarrow \ \mathsf{g}(\alpha) \leqslant \mathsf{g}(\beta)$;
2. $\mathsf{g}'(0)$ is an epsilon number, i.e. $\omega^{\mathsf{g}'(0)} = \mathsf{g}'(0)$.

[10] By $\langle n,m\rangle$ we denote the encoding in $\mathbb{N}$ of pairs of natural numbers. Moreover, with a slight and harmless abuse of notation, we denote with g both the function from $\mathcal{P}(\mathbb{N})$ to $\mathcal{P}(\mathbb{N})$ and its restriction $\mathsf{g}\colon \Omega \to \Omega$ which sends countable ordinals to countable ordinals.

Thus, with respect to Arai's conditions for g, we drop normality as well as the term structure requirements (for this point see also Remark 2.1). Moreover, we emphazise how property 2. ensures $g'(0) > 0$.

Our extended version of [12, Theorem 3] can now be stated:

Theorem 2.15 *Given an ordinal function g as above, then:*

$$|ACA_0 + WOP(g)| = g'(0)$$

Proof: the easy direction can be immediately proven considering the following ordinal succession: $\alpha_0 = 0, \alpha_1 = g(0)$ and $\alpha_{n+1} = g(\alpha_n)$. By definition, we have that $\sup_n \alpha_n = \sup_n g^n(0) = g'(0)$; but, using finitely many iterations of WOP(g), each α_n is a well order and thus $|\mathrm{ACA}_0 + \mathrm{WOP}(g)| \geqslant g'(0)$.

For the other direction, i.e. $\leqslant$, we resort to a thorough analysis of [12, Theorem 3] and its proof in order to extract the key points where the properties of g are actually used, and subsequently, check that our weaker hypotheses for g are indeed sufficient. Given the structure of our proof, all the references in the remaining part of this section refer to Arai's article [12].

For sake of clarity, we briefly summarize Arai's proof (cf. [12, pag. 266-268]). Assume that ACA_0 + WOP(g) proves WO($\prec$) for a linear relation $\prec$. One can obtain a derivation of $\Delta_0, E_\prec(x)$ in $G_2 + (VJ) + (prg) + (WPL)$, where Δ_0 is a set of negated axioms and $E_\prec$ a fresh new variable related to $\prec$. Next, $G_2 + (VJ) + (prg) + (WPL)$ is embedded into $(prg)^\infty + (WP) + (cut)_{1^{st}}$, an intermediate infinitary calculus obtained from $(prg)^\infty + (WP)$ adding a first-order cut rule; from $G_2 + (VJ) + (prg) + (WPL) \vdash \Delta_0, E_\prec(x)$, we move to $(prg)^\infty + (WP) + (cut)_{1^{st}} \vdash^{\omega^2}_{d,p} \Delta_0, E_\prec(n)$ for all n, where ω^2 bounds derivation length, d the number of nested applications of (WP) and p the rank of cut formulas. Applying cut elimination, we arrive at $(prg)^\infty + (WP) \vdash^\beta_c E_\prec(n)$ for all n, with $\beta < \varepsilon_0$ and $c < \omega$. By Theorem 5, in $Diag(\emptyset) + (prg)^\emptyset$ it holds that $\{n\} \vdash^\alpha E_\prec(n)$ for all n, with $\alpha = F(\beta, c) + \beta$. Finally, thanks to Theorem 6 and Proposition 2, we can extract an order-preserving injection $f\colon |\prec| \to \omega^{\alpha+1}$ such that $n \prec m$ implies $f(n) < f(m) < \omega^{\alpha+1} = \omega^{F(\beta,c)+\beta+1} < \omega^{g'(0)} = g'(0)$; thus $ot(\prec) \leqslant g'(0)$.

All in all, Arai's proof revolves around three main ingredients: three different calculi for second order arithmetic, two of which infinitary; a bounding function F defined from g, used to control derivation length and whose properties are ensured by Arai's Proposition 2 and two theorems, Theorem 5 and Theorem 6 which he uses to move from one calculus to another and to extract, together with F, the final upper bound for the proof-theoretic ordinal. We consider them one by one.

For what concerns the three main calculi used in the proof[11], $G_2 + (VJ) + (prg) + (WPL)$, $(prg)^\infty + (WP)$ and $Diag(\emptyset) + (prg)^\emptyset$, these are defined without any concrete reference to the properties of g; thus, we can keep them as they are.

For the function F, we can use Arai's definition which we briefly recall. Given g, we define $\beta, \alpha \mapsto F(\beta, \alpha)$ by induction on α as follows: $F(\beta, 0) = \omega^{1+\beta}$, $F(\beta, \alpha + 1) = F(\mathsf{g}(\omega^{F(\beta,\alpha)+\beta+1}), \alpha) + 1$, and $F(\beta, \lambda) = \sup\{F(\beta, \alpha) + 1 \,|\, \alpha < \lambda\}$ for λ limit ordinal. From our hypotheses for g, the following weaker, yet sufficient, version of Arai's Proposition 2 can be obtained:
CLAIM. If $F(\beta, \alpha)$ is defined as above, then:

1. if $\alpha \leqslant \gamma$ and $\beta \leqslant \delta$, then $F(\beta, \alpha) \leqslant F(\delta, \gamma)$;
2. if $\beta < \mathsf{g}'(0)$ and $c < \omega$, then $F(\beta, c) < \mathsf{g}'(0)$.

Proof of the Claim. 1. derives from the fact that each function $\beta \mapsto \beta + \alpha$, $\beta \mapsto \omega^\beta$ and $\beta \mapsto \mathsf{g}(\beta)$ is weakly increasing; *2.* is proved by induction on c, using the closure of $\mathsf{g}'(0)$ with respect to g. *This concludes the proof of the Claim.*

Regarding the role of Proposition 2 in Arai's proof, respectively the previous Claim in ours, *1.* is extensively used to majorize derivation length, whereas *2.* is used in the very last step to have $\mathsf{g}'(0)$ as upper bound.

For what concerns Arai's Theorems 5 and 6, the situation is as follows. Theorem 6 allows to extract, from a derivation in $Diag(\emptyset) + (prg)^\emptyset$ of the well-foundedness of a linear relation $\prec$, an upper bound for the order type of $\prec$; since both Theorem 6 and its proof do not refer to g, they remain untouched. Theorem 5, which plays a crucial role in Arai's proof, is a WP-elimination result, it allows to avoid the use of the rule (WP) (which is a well-ordering principle in the form of a rule) in a formal derivation. More precisely, Theorem 5 states that, under some side conditions, from a derivation of a set of formulas Γ in $(prg)^\infty + (WP)$ one can obtain a derivation of Γ in $Diag(\emptyset) + (prg)^\emptyset$. The proof of Arai's Theorem 5 is preceded by two auxiliary lemmas, Lemma 1 and Lemma 2 [12, pag. 272], which again do not refer to g and thus are untouched. Considering the proof of Theorem 5 itself, a key step is obtaining, from an embedding, i.e. an injective order-preserving function, $f : <^\emptyset_A \to \omega^{F(\gamma,\alpha)+\gamma+1}$, an embedding $F : <^\emptyset_{\mathsf{g}(A)} \to \mathsf{g}(\omega^{F(\gamma,\alpha)+\gamma+1})$ with $\mathsf{g}(\omega^{F(\gamma,\alpha)+\gamma+1})$ well-ordered by $\mathrm{WOP}(\mathsf{g})$. In Arai's proof, this step is ensured by Proposition 1. Here instead, this fact is derived from the property of g of being weakly increasing: if f is such an embedding, then $ot(<^\emptyset_A) < \omega^{F(\gamma,\alpha)+\gamma+1}$, thus $\mathsf{g}(ot(<^\emptyset_A)) \leqslant \mathsf{g}(\omega^{F(\gamma,\alpha)+\gamma+1})$

[11] In Arai's article, the last two calculi, which are the infinitary ones, refer also to a subsidiary set $\mathcal{P}$; this set is needed only for the second main result of the paper ([12, Theorem 4]) and thus it is negligible here.

and we can consider as $F : <^{\emptyset}_{g(A)} \to g(\omega^{F(\gamma,\alpha)+\gamma+1})$ the identity function[12]. In the end, also Theorem 5 holds under our weaker hypotheses for g and so Arai's proof. □

Remark 2.1 *Differently from Arai, we do not resort to term structures for denoting ordinals in the domain and codomain of* g *[12, Definition 3]; as a minor drawback, our proof is not directly formalizable in* ACA_0*. Instead, we need a metatheory strong enough to treat directly ordinals, such as ZFC.*

2.2.3 Ordinal Analysis of Kruskal's Theorem(s)

In this section, using Theorem 2.15, we prove the aforementioned estimations for the proof-ordinals of Kruskal's theorem, namely:

$$|\mathrm{RCA}_0 + \forall n\, \mathrm{KT}_\ell(n)| = \vartheta(\Omega^\omega + \omega) \text{ and } |\mathrm{RCA}_0 + \mathrm{KT}_\ell(\omega)| = \vartheta(\Omega^{\omega+1}).$$

Instrumental to our goal, we prove the following equivalences:

Theorem 2.16 *(RCA_0) The following are equivalent:*

1. $KT_\ell(\omega)\colon \forall Q\, [Q \text{ wqo} \to \mathbb{T}(Q) \text{ wqo}]$;
2. $\forall \mathfrak{X}\, [WO(\mathfrak{X}) \to WO(\vartheta(\Omega^\omega \cdot \mathfrak{X}))]$.

For each n, the following are equivalent:

1. $KT_\ell(n)\colon \forall Q\, [Q \text{ wqo} \to \mathbb{T}_n(Q) \text{ wqo}]$;
2. $\forall \mathfrak{X}\, [WO(\mathfrak{X}) \to WO(\vartheta(\Omega^n \cdot \mathfrak{X}))]$.

Proof: we consider the equivalence between the first two points reasoning in ACA_0, since they both imply ACA_0 over RCA_0.

1) ⇒ 2) Let $\mathfrak{X}$ be a well-order, then $\mathfrak{X}$ is a wqo and, by 1), also $(\mathbb{T}(\mathfrak{X}), \preccurlyeq)$ is a wqo, in particular any extension of the tree embeddability $\preccurlyeq$ is well-founded. But, since $\preccurlyeq$ can be extended over $\mathbb{T}(\mathfrak{X})$ to a linear order order-isomorphic to $\vartheta(\Omega^\omega \cdot \mathfrak{X})$ [149], $\vartheta(\Omega^\omega \cdot \mathfrak{X})$ is a well-founded linear order and thus is well-ordered.

2) ⇒ 1) Let Q be a wqo, then the tree T_B of bad sequences in Q is well-founded and, provable in ACA_0 [169, lemma V.1.3], the Kleene-Brouwer linearization $\mathfrak{X}$ of T_B is a well-order. Thus Q admits a reification by the well-order $\mathfrak{X}$, i.e. there is a function $f\colon T_B \to \mathfrak{X}$ such that if the bad sequence a extends the bad sequence b,

[12] We warn the reader not to be baffled by the two distinct roles played here by the function letter F: binary ordinal function, $F(\alpha, \beta)$, and embedding, $F : <^{\emptyset}_{g(A)} \to g(\omega^{F(\gamma,\alpha)+\gamma+1})$; we use the same letter to keep the notation as equal as possible to Arai's article.

then $f(a) \geqslant f(b)$. By [149], this implies the existence of a reification of $\mathbb{T}(Q)$ by $\vartheta(\Omega^\omega \cdot \mathfrak{X})$ which, thanks to 2), is a well-order; thus $\mathbb{T}(Q)$ is a wqo since it has no infinite bad sequences.
For each n, the second part is proved analogously. □

From the second equivalence of the previous theorem, we can easily obtain:

Proposition 2.2 *(RCA_0) The following are equivalent:*

- $\forall n\, KT_\ell(n) : \forall n \forall Q\, [Q \text{ wqo} \rightarrow \mathbb{T}_n(Q) \text{ wqo}]$;
- $\forall n \forall \mathfrak{X}\, [WO(\mathfrak{X}) \rightarrow WO(\vartheta(\Omega^n \cdot \mathfrak{X}))]$;
- $\forall \mathfrak{X}\, [WO(\mathfrak{X}) \rightarrow \forall n\, WO(\vartheta(\Omega^n \cdot \mathfrak{X}))]$;
- $\forall \mathfrak{X}\, [WO(\mathfrak{X}) \rightarrow WO(\sup_n(\vartheta(\Omega^n \cdot \mathfrak{X})))]$.

Proof: Straightforward. □

Having Theorem 2.15, Theorem 2.16 and Proposition 2.2 at our disposal, the last step is to prove that both the ordinal functions $g_\omega(\mathfrak{X}) = \vartheta(\Omega^\omega \cdot \mathfrak{X})$ and $g_{\forall n}(\mathfrak{X}) = \sup_n \vartheta(\Omega^n \cdot \mathfrak{X})$ satisfy the hypotheses of Theorem 2.15 and, subsequently, computing $g'_\omega(0)$ and $g'_{\forall n}(0)$.

Proposition 2.3 *Let α, β be countable ordinals. Both $g_\omega(\mathfrak{X}) = \vartheta(\Omega^\omega \cdot \mathfrak{X})$ and $g_{\forall n}(\mathfrak{X}) = \sup_n \vartheta(\Omega^n \cdot \mathfrak{X})$ satisfy the following properties:*

1. *$\alpha \leqslant \beta$ implies $g(\alpha) \leqslant g(\beta)$;*
2. *$\omega^{g'(0)} = g'(0)$.*

Proof: both properties derive directly from the definitions of g_ω and $g_{\forall n}$, together with the properties of the collapsing function ϑ [149, Lemma 1.2], e.g., $\vartheta(\alpha)$ is always an epsilon number, namely $\omega^{\vartheta(\alpha)} = \vartheta(\alpha)$. □

Next, we compute $g'_\omega(0)$ and $g'_{\forall n}(0)$.

Proposition 2.4 *$g'_\omega(0) = \vartheta(\Omega^{\omega+1})$ and $g'_{\forall n}(0) = \vartheta(\Omega^\omega + \omega)$.*

Proof: we focus on the second case, $g'_{\forall n}(0) = \vartheta(\Omega^\omega + \omega)$, which is the most involved. Let us define the following increasing sequence $\alpha_0 = \omega$ and $\alpha_{k+1} = \sup_n \vartheta(\Omega^n \cdot \alpha_k)$; given the definition of ϑ [149, pag. 51], one can compute its first elements, i.e. $\alpha_1 = \sup_n \vartheta(\Omega^n \cdot \omega) = \vartheta(\Omega^\omega)$ and $\alpha_2 = \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega)) = \vartheta(\Omega^\omega + 1)$. We prove by induction on k, with the base case given by α_1, that $\alpha_{k+1} = \vartheta(\Omega^\omega + k)$, from this $g'_{\forall n}(0) = \sup_k \alpha_k = \vartheta(\Omega^\omega + \omega)$ easily follows.

First we prove $a_{k+1} \leqslant \vartheta(\Omega^\omega + k)$. So let $k \geqslant 1, \alpha_k = \vartheta(\Omega^\omega + k - 1)$ and $\alpha_{k+1} = \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1))$; by definition of ϑ, $\vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1)) < \vartheta(\Omega^{n+1} \cdot \vartheta(\Omega^\omega + k - 1)) < \vartheta(\Omega^\omega + k)$ holds for all n and thus $a_{k+1} = \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1)) \leqslant \vartheta(\Omega^\omega + k)$. For the other direction, $a_{k+1} \geqslant \vartheta(\Omega^\omega + k)$, we resort to an equivalent definition for ϑ, namely $\vartheta(\alpha) = \min\{\xi \in E \mid \alpha^* < \xi \text{ and } \forall \beta < \alpha\, (\beta^* < \xi \to \vartheta(\beta) < \xi)\}$ [184, pag. 15], where E is the set of epsilon numbers and, given an ordinal γ, γ^* is the maximum epsilon number, apart from Ω, in the Cantor normal form of γ. Keeping in mind the aforementioned alternative definition for $\vartheta(\alpha)$, since $\alpha_{k+1} = \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1))$ is an epsilon number and $(\Omega^\omega + k)^* = 0$, to prove $\alpha_{k+1} \geqslant \vartheta(\Omega^\omega + k)$ it remains to check that, for all $\beta < \Omega^\omega + k$, if $\beta^* < a_{k+1}$, then $\vartheta(\beta) < \alpha_{k+1}$. Let us assume that $\beta < \Omega^\omega + k$ and $\beta^* < \alpha_{k+1} = \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1))$, the first condition amounts to $\beta < \Omega^\omega$ or $\beta \in \{\Omega^\omega, \Omega^\omega + 1, \ldots, \Omega^\omega + k - 1\}$. The latter case case is the simplest one, if $\beta \in \{\Omega^\omega, \Omega^\omega + 1, \ldots, \Omega^\omega + k - 1\}$ then $\beta = \Omega^\omega + r$ with $0 \leqslant r \leqslant k - 1$ and in this case $\vartheta(\beta) \leqslant \vartheta(\Omega^\omega + k - 1) = \alpha_k \leqslant \alpha_{k+1}$. We consider now the former, if $\beta < \Omega^\omega = \sup_n(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1))$ and $\beta^* < \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1))$, then there exists a natural number $\bar{n}$ such that $\beta < \Omega^{\bar{n}} \cdot \vartheta(\Omega^\omega + k - 1)$ and $\beta^* < \vartheta(\Omega^{\bar{n}} \cdot \vartheta(\Omega^\omega + k - 1))$; but, since $\vartheta(\Omega^{\bar{n}} \cdot \vartheta(\Omega^\omega + k - 1))$ is a ϑ number, then $\vartheta(\beta) < \vartheta(\Omega^{\bar{n}} \cdot \vartheta(\Omega^\omega + k - 1)) < \sup_n \vartheta(\Omega^n \cdot \vartheta(\Omega^\omega + k - 1)) = \alpha_{k+1}$. Thus $\alpha_{k+1} \geqslant \vartheta(\Omega^\omega + k)$ and so $\alpha_{k+1} = \vartheta(\Omega^\omega + k)$.

The case $g'_\omega(0) = \vartheta(\Omega^{\omega+1})$ where $g'_\omega(0) := \min\{\alpha > 0 \mid \forall \beta < \alpha\ \vartheta(\Omega^\omega \cdot \beta) < \alpha\}$ is treated in an analogous way considering this time the sequence $\alpha_0 = \omega$ and $\alpha_{k+1} = \vartheta(\Omega^\omega \cdot \alpha_k)$. □

Finally, we obtain our main result:

Theorem 2.17

$$|RCA_0 + \forall n\, KT_\ell(n)| = \vartheta(\Omega^\omega + \omega) \text{ and } |RCA_0 + KT_\ell(\omega)| = \vartheta(\Omega^{\omega+1}).$$

Proof: we simply apply together Theorem 2.15, Theorem 2.16, Proposition 2.2, Proposition 2.3 and Proposition 2.4. RCA_0 can be taken as base theory, differently from Arai who uses ACA_0, because both $\text{KT}_\ell(\omega)$ and $\forall n\, \text{KT}_\ell(n)$ imply Arithmetical Comprehension over RCA_0. □

For sake of completeness, we report the results for the unlabelled case together with a lemma and some corollaries.

Theorem 2.18 $RCA_0 \vdash \forall n\, KT(n) \leftrightarrow KT(\omega) \leftrightarrow WO(\vartheta(\Omega^\omega))$

Proof: [149]. □

Lemma 2.3 *(Carlucci, Mainardi, Rathjen) If $\omega \cdot \sigma = \sigma$ then $|RCA_0 + WO(\sigma)| = \sigma^\omega$.*

Proof [41]. □

Corollary 2.1

1. $|RCA_0 + KT(\omega)| = \vartheta(\Omega^\omega)^\omega$;
2. $RCA_0 \nvdash KT(\omega) \rightarrow \forall n\, KT_\ell(n)$;
3. $RCA_0 \nvdash \forall n\, KT_\ell(n) \rightarrow KT_\ell(\omega)$.

Proof: 1. derives from Theorem 2.18 together with Lemma 2.3; *2.* and *3.* derive from Theorem 2.17 and Theorem 2.18. □

Future Work

Regarding future work, the proof-theoretic investigations on Kruskal's theorem by Rathjen and Weiermann [149] still point the way. As already said, beside the proof-ordinal calculation, $\mathrm{RCA}_0 \vdash \mathrm{KT}(\omega) \leftrightarrow \mathrm{WO}(\vartheta\Omega^\omega)$, they sized the proof-theoretic strength of Kruskal's theorem for unlabelled trees in term of reflection principles.

Theorem 2.19 *(Rathjen and Weiermann [149])* $RCA_0 \vdash KT(\omega) \leftrightarrow \Pi^1_1\text{-}RFN(\Pi^1_2\text{-}BI_0)$.

$\Gamma\text{-}RFN(T)$ denotes the theory T extended with the uniform reflection principle $\forall x\,(Pr_T(\ulcorner\varphi(\bar{x})\urcorner) \rightarrow \varphi(x))$ for all formula φ in Γ having at most one free variable, and $\Pi^1_2\text{-}BI_0$ the theory $\mathrm{ACA}_0 + \Pi^1_2\text{-}BI$, with $\Pi^1_2\text{-}BI$ the bar induction schema for Π^1_2 formulas. For further readings regarding reflection principles, we refer to [16, 17, 18].

Consequentially, the next step is to obtain a similar classification also for $\mathrm{KT}_\ell(\omega)$ and $\mathrm{KT}_\ell(n)$. During the preparation of the thesis, the two following conjectures arise:

Conjecture 2.1

- $RCA_0 \vdash KT_\ell(\omega) \leftrightarrow \Pi^1_2\text{-}\omega RFN(\Pi^1_2\text{-}BI_0 \restriction \Pi^1_3)$ *[F. Pakhomov]*
- $RCA_0 \vdash \forall n\, KT_\ell(n) \leftrightarrow \Pi^1_2\text{-}RFN(\Pi^1_2\text{-}BI_0)$ *[A. Freund].*

Further work will also be required to extend the present results to other embeddability relations between trees, such as Friedman's gap condition [70]; finally, for a recent survey on modern perspectives in Proof Theory see [8].

2.3 Proof-Theoretical Relations between Various Results for Wqo

Higman's lemma and Kruskal's theorem are two of the most celebrated results in the theory of well quasi-orders. In his seminal paper [92] Higman obtained what is known as Higman's lemma as a corollary of a more general theorem, dubbed here Higman's theorem. Whereas the lemma deals with finite strings over a well quasi-order (and so, implicitly, with only the binary operation of juxtaposition), the theorem regards abstract operations of arbitrary high arity, covering a much broader spectrum of situations.

Kruskal was well aware of this general set up; in his time-honoured paper [106] not only did he use Higman's lemma in crucial steps of the proof of his own theorem, but also followed the same proof schema as Higman. Moreover, in the very end of his article, Kruskal explicitly stated that Higman's theorem is a special version of Kruskal's tree theorem; namely a restriction to trees of finite branching degree, i.e. trees with an upper bound regarding the number of immediate successors of each node. Although no proof of the reduction is provided, he presented a glossary to properly translate concepts from the tree context of his paper to the algebraic context of Higman's work. The equivalence between restricted versions has subsequently been exposed by Schmidt [158]; whereas Pouzet [138] gave, together with that equivalence, an infinite version of Higman's theorem which proves equivalent to the general Kruskal's theorem.

In this section, based on a joint work with Andreas Weiermann which has not yet been published, we revisit the aforementioned equivalences to obtain a clearer view of the proof-theoretical relations between the different versions of Higman's and Kruskal's theorem, paying particular attention to the former's algebraic formulation. More precisely, we establish, over the base theory RCA_0, the equivalence of the finite and infinite versions of Higman's and Kruskal's theorem. The ultimate goal is to complete the picture within the frame of reverse mathematics and ordinal analysis, following [149].

2.3.1 Abstract Algebras and Higman's Theorem in $\mathbf{RCA}_0$

This paragraph is devoted to introduce *abstract algebras* and *Higman's theorem.* As before all the definitions are given in RCA_0; however, since dealing in RCA_0 with sets of operations, i.e. sets of functions and thus sets of sets, required some care, the following definition is slightly more involved than its classical counterpart [92].

Definition 2.10 *An n-ARY (ABSTRACT) ALGEBRA $(|A|, M)$ is given by a set $|A| \subseteq \mathbb{N}$ together with a finite list $M = (M_i)_i$ with $1 \leqslant i \leqslant n$ of sequences, possibly* *finite or empty, of operations over $|A|$; for each i, M_i is a sequence of i-ary functions from $|A|^i$ to $|A|$.*

As for qo, we tacitly write A instead of $|A|$, omitting also the term "abstract"; moreover, although it does not exist as a set, we use M to informally refer to the family of all the operations of the algebra.

Remark 2.2 *Since each operation μ is uniquely determined by its arity r, i.e. $\mu \in M_r$ for some $r \in \{1, \dots, n\}$, and its position d in the sequence M_r, we can uniquely assign a natural number $|\mu|$ to each operation, allowing us to consider also the set $|M_i|$ of the operation codes of element of M_i; moreover, we can also require that codes for operations and codes for elements of A are disjoint. Given this bijection, at least in the metatheory, in the following we write μ for both an operation and the corresponding code relying on the context to make clear the exact meaning; similarly for M_i and $|M_i|$.*

We can give the following generalization:

Definition 2.11 *An* (ABSTRACT) ALGEBRA $(|A|, M, d)$ *is given by a set $|A| \subseteq \mathbb{N}$ together with a sequence M of operations over $|A|$ and an arity function $d \colon M \to \mathbb{N}$ which associates to every operation $f \in M$ its arity $d(f)$.*

As before, we simply write A instead of $|A|$, omitting the word "abstract"; we frequently omit also the arity operator d. In analogy with the previous case, we can associate an unique code to each operation of M (and thus considering the code set $|M|$), requiring these codes to be different from the codes of elements of A. Finally, we underline how an n-ary algebra can be seen as an algebra placing $M = M_1 \cup \dots \cup M_n$ and $d(f) = i$ if $f \in M_i$.

For algebras, there are the following auxiliary definitions.

Definition 2.12 *Given an algebra (A, M):*

- *(B, M) is a* SUBALGEBRA *of (A, M) if $B \subseteq A$ and B is closed with respect to M, i.e. for every μ in M of arity $d(\mu)$ and every $b_1, \dots, b_{d(\mu)}$ in B, $\mu(b_1, \dots, b_{d(\mu)}) \in B$;*
- *$C \subseteq A$ is a* GENERATING SET *of A, and A is* GENERATED *by C, if for every subalgebra (B, M) of (A, M), $C \subseteq B$ implies $B = A$.*

We can now link together quasi orders and abstract algebras.

Definition 2.13 *Given an algebra (A, M) and a quasi-order $\leqslant$ over A:*

1. $(A, M, \leqslant)$ *is an* ORDERED ALGEBRA *if for any function* $\mu \in M$ *with arity* $d(\mu)$
$$\forall i \leqslant d(\mu)\ a_i \leqslant b_i \quad \textit{implies} \quad \mu(a_1, \ldots, a_{d(\mu)}) \leqslant \mu(b_1, \ldots, b_{d(\mu)});$$

2. $\leqslant$ *is a* DIVISIBILITY ORDER *if, in addition, for any function* $\mu \in M$ *with arity* $d(\mu)$
$$\forall i \leqslant d(\mu)\ \ a_i \leqslant \mu(a_1, \ldots, a_{d(\mu)});$$

3. $\leqslant$ *is* COMPATIBLE *with a qo* $\trianglelefteq$ *on* M *if for any* μ, λ *in* M
$$a_1 \ldots a_{d(\lambda)} \leqslant^* b_1 \ldots b_{d(\mu)} \text{ and } \lambda \trianglelefteq \mu \text{ imply } \lambda(a_1, \ldots, a_{d(\lambda)}) \leqslant \mu(b_1, \ldots, b_{d(\mu)}),$$
for the definition of $\leqslant^*$ *see Lemma 1.1.*

This definition can be given almost untouched for an n-ary algebra too, the only concrete modification is for compatibility. In an n-ary algebra, we could have different qo's $\trianglelefteq_r$, one for each operation set M_r; compatibility is then stated separately for each arity, i.e. if λ, μ belong to M_r then
$$\forall i \leqslant r\ a_i \leqslant b_i \text{ and } \lambda \trianglelefteq_r \mu \text{ imply } \lambda(a_1, \ldots, a_r) \leqslant \mu(b_1, \ldots, b_r).$$

Properties 1. and 2. of previous definition, or their equivalents, can be found also in other contexts. A function over ordinals satisfying those conditions is commonly called, respectively, *monotonic* and *increasing* [158, def. 4.5 p.379]; while, talking about natural numbers, such a function is dubbed, respectively, *weakly increasing* and *inflationary* [191, p.178]

Remark 2.3 *(cf. Remark 2.2) Formally speaking in the third point of Def. 2.13 (compatibility), given a qo* $\trianglelefteq$ *over* $|M|$*, we are requiring that* $\leqslant$ *preserves this order, namely*
$$a_1 \ldots a_{d(\lambda)} \leqslant^* b_1 \ldots b_{d(\mu)} \text{ and } |\lambda| \trianglelefteq |\mu| \text{ imply } \lambda(a_1, \ldots, a_{d(\lambda)}) \leqslant \mu(b_1, \ldots, b_{d(\mu)}).$$

The finite and the infinite versions of Higman's theorem can now be stated; the former can be found in the seminal paper of Higman [92], while the latter is stated in [138]. For each $n \in \mathbb{N}$, we have the corresponding version of the following theorem:

Theorem 2.20 (n-finite Higman's theorem) *Given an* n*-ary ordered algebra* $(A, M, \leqslant)$*, if* $(M_r, \trianglelefteq_r)$ *is a wqo for each* r*,* $\leqslant$ *is a divisibility order compatible with the qo's of* M *and* (A, M) *is generated by a wqo set* $C \subseteq A$*, then* $(A, \leqslant)$ *is wqo.*

Using a notation similar to the one reserved for the various versions of Kruskal's theorem, each n-version of the previous theorem is denoted by HT(n), e.g. HT(3) states that the theorem holds for each 3-ary ordered algebra. Given this notation, the original theorem stated by Higman [92] simply reads as follows.

Theorem 2.21 (Original Higman's theorem) $\forall n\, HT(n)$.

Using abstract algebras, we can state an infinite version of Higman's theorem, denoted by HT(ω).

Theorem 2.22 (Infinite Higman's theorem) *Given an ordered algebra* $(A, M, \leqslant)$*, if* $(M, \trianglelefteq)$ *is a wqo,* $\leqslant$ *is a divisibility order compatible with* $\trianglelefteq$ *and* (A, M) *is generated by a wqo set* $C \subseteq A$*, then* $(A, \leqslant)$ *is wqo.*

The crucial difference between the finite version and the infinite one is the presence in the former of an arbitrary high, but fixed, upper bound on the arity of the operations of M. The main references for abstract algebras are Higman's original paper [92] and the book of Cohn [46].

2.3.2 Equivalence between Higman's and Kruskal's Theorems

Adapting to the framework of reverse mathematics the proof by Pouzet [138] (see also [158]), we prove that, regarding abstract algebras and structured labelled trees, Higman's and Kruskal's theorems are two sides of the same coin. We first consider the fine case, HT(n) and $\mathrm{KT}_\ell(n)$; our goal is to prove the following equivalence.

Theorem 2.23 $RCA_0 \vdash \forall n\, HT(n) \longleftrightarrow \forall n\, KT_\ell(n)$.

We obtain the previous result as immediate consequence of the following lemma.

Lemma 2.4 *(RCA_0)* $\forall n\ HT(n) \longleftrightarrow KT_\ell(n)$.

Proof We prove Lemma 2.4 by fixing n and considering separately each direction. First of all we set down some notation:

- $\leqslant$ will be the qo over the set A, representing an n-ary algebra, whose elements will be denoted by $a, b, c \ldots$; $\leqslant$ will be also the usual order over $\mathbb{N}$.
- $\trianglelefteq$ will be the qo over M_r for each r, whose elements will be denoted by $\mu, \lambda, \ldots$; for sake of readability, we use the same symbol $\trianglelefteq$ for each set M_r, $1 \leqslant r \leqslant n$.

- $\preccurlyeq$ will be the embeddability relation between finite structured labelled trees, which will be denoted by $t, s, \ldots$; if necessary, trees will be also denoted by the extended notation $t = q[t_1, \ldots, t_k]$.

"$\mathrm{HT}(n) \Rightarrow \mathrm{KT}_\ell(n)$"

Given a wqo $(Q, \leqslant)$, we must prove that $(\mathbb{T}_n(Q), \preccurlyeq)$ is well quasi-ordered by $\preccurlyeq$. For each $1 \leqslant r \leqslant n$ and $q \in Q$, we define the following operation over $\mathbb{T}_n(Q)$:

$$\bigoplus_{r,q} : \mathbb{T}_n(Q)^r \to \mathbb{T}_n(Q) \text{ by } \bigoplus_{r,q}(t_1, \ldots, t_r) := q[t_1, \ldots, t_r]$$

where $q[t_1, \ldots, t_r]$ is the tree whose root is labelled by q and whose immediate subtrees, are $t_1, \ldots, t_r$. We informally dubbed $\bigoplus_{N,Q}$ (which is isomorphic to $\{1 \ldots, n\} \times Q$) the family of all these operations and we quasi-order each set $\bigoplus_{r,Q} = \{\bigoplus_{r,q} \mid q \in Q\}$ (of codes) of r-ary operations in the following way: $\bigoplus_{r,q} \trianglelefteq_r \bigoplus_{r,p}$ iff $q \leqslant p$; with such quasi-orders each $(\bigoplus_{r,Q}, \trianglelefteq_r)$ is a wqo, since also Q is.

CLAIM. $(\mathbb{T}_n(Q), \bigoplus_{N,Q}, \preccurlyeq)$ is an ordered n-ary algebra with $\preccurlyeq$ a divisibility order compatible with $\trianglelefteq$; moreover $C = \{q[] \mid q \in Q\}$ is a generating set for $\mathbb{T}_n(Q)$.

Proof of the Claim: Since $\bigoplus_{N,Q}$ is a family of at most n-ary operations, we need to check the three properties of Def. 2.13 regarding the quasi order $\preccurlyeq$ and the generation of $\mathbb{T}_n(Q)$ by C.

Ordered algebra: given $1 \leqslant r \leqslant n$, $q \in Q$ and $t_i \preccurlyeq s_i$ for all $1 \leqslant i \leqslant r$, then $q[t_1, \ldots, t_r] \preccurlyeq q[s_1, \ldots, s_r]$ holds by the third condition of Def. 2.7, and so $\bigoplus_{r,q}(t_1, \ldots, t_r) \preccurlyeq \bigoplus_{r,q}(s_1, \ldots, s_r)$.

Divisibility: given $1 \leqslant r \leqslant n$ and $q \in Q$, $t_i \preccurlyeq q[t_i, \ldots, t_r]$ holds by the second condition of Def. 2.7, and so $t_i \preccurlyeq \bigoplus_{r,q}(t_1, \ldots, t_r)$ for all $1 \leqslant i \leqslant r$.

Compatibility: given $1 \leqslant r \leqslant n$, $\bigoplus_{r,q} \trianglelefteq \bigoplus_{r,p}$ and $t_i \preccurlyeq s_i$ for all $1 \leqslant i \leqslant r$, then $q \leqslant p$ and $q[t_1, \ldots t_r] \preccurlyeq p[s_1, \ldots, s_r]$ holds by the third case of Def. 2.7, thus $\bigoplus_{r,q}(t_1, \ldots t_r) \preccurlyeq \bigoplus_{r,p}(s_1, \ldots, s_r)$

Generation: obviously $C \subseteq \mathbb{T}_n(Q)$; we need to prove that, given a subset $B \subseteq \mathbb{T}_n(Q)$, closed with respect to $\bigoplus_{N,Q}$, if $C \subseteq B$ then $B = \mathbb{T}_n(Q)$. Let $C \subseteq B$ and $t \in \mathbb{T}_n(Q)$, if $t \in C$, i.e. $t = q[]$ with $q \in Q$, then $t \in B$; else t is obtained by a finite number of elements of C, the leaves of t, and a finite number of applications of operations in $\bigoplus_{N,Q}$, since B is closed with respect to $\bigoplus_{N,Q}$, $t \in B$ and thus $B = \mathbb{T}_n(Q)$. *End of the proof of the Claim.*

To conclude, since $\trianglelefteq$ is a wqo on $\bigoplus_{N,Q}$, we can apply $\mathrm{HT}(n)$ to obtain that $(\mathbb{T}_n(Q), \preccurlyeq)$ is a wqo.

"$\mathrm{KT}_\ell(n) \Rightarrow \mathrm{HT}(n)$"

Let $(A, M, \leqslant)$ be an n-ary ordered algebra satisfying all the hypotheses of Higman's theorem: each set of r-ary operations M_r is a wqo; $\leqslant$ is a divisibility order compatible with the wqo $\trianglelefteq$ of each M_r; there is a wqo generating set C. We must prove $(A, \leqslant)$ wqo.

Since M is a wqo (given by the finite union $M_1 \cup \cdots \cup M_n$ of wqo's) and C is a wqo, so it is $C \cup M$, by Lemma 2.1, and applying $\mathrm{KT}_\ell(n)$ so it is $(\mathbb{T}_n(C \cup M), \preccurlyeq)$. Over $C \cup M$ we consider the *grade function* $g : C \cup M \to \mathbb{N}$ defined as $g(x) := 0$ if $x \in C$ and $g(x) := r$ if $x \in M_r$. Finally, we define inside $\mathbb{T}_n(C \cup M)$ the subset $\mathbb{T}^g_n(C \cup M)$ of *graded trees*, i.e. the trees t satisfying the following grade condition

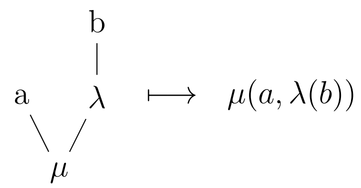
$$\forall s \in t \ d(s) = g(l(s)).$$

In other words, we are considering trees such that, for each node, the degree d of the node is equal to the grade g of the label of the node. The functions g, d and $\mathbb{T}^g_n(C \cup M)$ are all definable in RCA_0; moreover, $\mathbb{T}^g_n(C \cup M)$ is well quasi-ordered by $\preccurlyeq$.

We construct now an order-preserving function ϕ between $(\mathbb{T}^g_n(C \cup M), \preccurlyeq)$ and $(A, M, \leqslant)$, defined by recursion over the tree structure of the elements of $\mathbb{T}^g_n(C \cup M)$:

$$\phi(t) = \begin{cases} q & \text{if } t = q[] \text{ with } q \in C; \\ \mu(\phi(t_1), \ldots, \phi(t_r)) & \text{if } t = \mu[t_1, \ldots, t_r] \text{ with } \mu \in M_r. \end{cases}$$

Since we are considering graded trees, the label of a leaf is always an element of C; whereas the label of a node of degree r is always (the code of) an operation of (A, M) of arity r, i.e. an element of M_r. This, together with the fact that we are treating ordered trees (i.e. $\lambda[t_1, t_2] \neq \lambda[t_2, t_1]$, unless $t_1 = t_2$), ensures that ϕ is well definite. An instance of ϕ is depicted below



We prove by induction that ϕ is order-preserving, i.e. $t \preccurlyeq s \Rightarrow \phi(t) \leqslant \phi(s)$, considering the three defining cases of Def. 2.7. Given $t, s \in \mathbb{T}^g_n(C \cup M)$ then:

1. if $t \preccurlyeq s$ with $t = q[], s = p[]$, then $q \leqslant p$ and thus $\phi(t) \leqslant \phi(s)$;

2. if $t \preccurlyeq s$ with $s = \mu[s_1, \ldots, s_r]$, $\mu \in M_r$ and $t \preccurlyeq s_i$ for some $i \in \{1, \ldots, r\}$, then, by induction, $\phi(t) \leqslant \phi(s_i)$ and, since $\leqslant$ is a divisibility order, $\phi(t) \leqslant \mu(\phi(s_1), \ldots, \phi(s_r))$, thus $\phi(t) \leqslant \phi(s)$;

3. if $t \preccurlyeq s$ with $t = \mu[t_1, \ldots, t_r]$, $s = \lambda[s_1, \ldots, s_k]$, $\mu \in M_r$, $\lambda \in M_k$, $\mu \trianglelefteq \lambda$ and there exist $1 \leqslant i_1 < \ldots < i_r \leqslant k$ such that $t_1 \preccurlyeq s_{i_1}, \ldots, t_r \preccurlyeq s_{i_r}$, then, by

definition of $\trianglelefteq$, $r = k$ and, by induction, $\phi(t_1) \leqslant \phi(s_1), \dots, \phi(t_r) \leqslant \phi(s_r)$, thus, since $\leqslant$ is compatible with $\trianglelefteq$, $\mu(\phi(t_1), \dots, \phi(t_r)) \leqslant \lambda(\phi(s_1), \dots, \phi(s_r))$, i.e. $\phi(t) \leqslant \phi(s)$.

In order to conclude by applying Theorem 2.1, we need to prove that ϕ is also surjective. Let us consider $\phi(\mathbb{T}^g_n(C \cup M)) \subset A$, obviously $C \subseteq \phi(\mathbb{T}^g_n(C \cup M))$; since C is a generating set it suffices to check that $\phi(\mathbb{T}^g_n(C \cup M))$ is closed under M. Given $a_1, \dots, a_r \in \phi(\mathbb{T}^g_n(C \cup M))$ and $\mu \in M_r$, there exist $t_1, \dots, t_r \in \mathbb{T}^g_n(C \cup M)$ such that $\phi(t_1) = a_1, \dots, \phi(t_r) = a_r$; but now $\mu[t_1, \dots, t_r]$, i.e. the tree with the root labelled by μ and with immediately subtrees $t_1, \dots, t_r$ is an element of $\mathbb{T}^g_n(C \cup M)$ and, by definition, $\phi(\mu[t_1, \dots, t_r]) = \mu(\phi(t_1), \dots, \phi(t_r)) = \mu(a_1, \dots, a_r)$, thus $\mu(a_1, \dots, a_r) \in \phi(\mathbb{T}^g_n(C \cup M))$. So $\phi(\mathbb{T}^g_n(C \cup M)) = A$, i.e. ϕ is surjective, and we can apply Theorem 2.1 to conclude that $(A, \leqslant)$ is wqo □

We consider now the infinite case of the previous equivalence.

Theorem 2.24 *$RCA_0 \vdash HT(\omega) \longleftrightarrow KT_\ell(\omega)$*

Proof The general context is quite similar, the main differences regarding the background are the following:

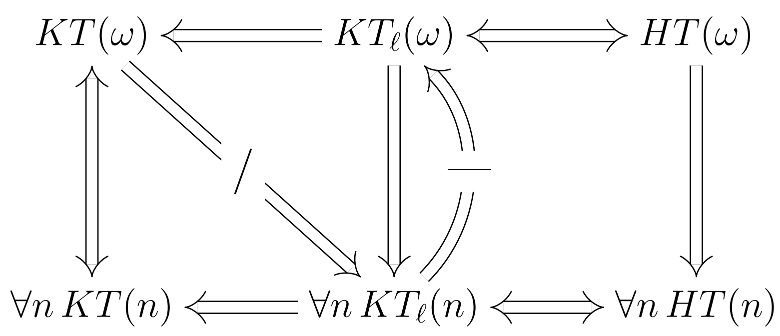
- We are dealing with abstract algebras rather than n-ary algebras; this means that we could have operations of any finite arity. In particular, since an infinite union of wqo's is not in general a wqo, we do not consider a wqo $\trianglelefteq_r$ for each set M_r of r-ary operations as before; conversely, we have one single wqo $\trianglelefteq$ over the set M.
- We are dealing with trees of, possibly, any finite branching degree, i.e. we consider $\mathbb{T}(Q)$ and $\mathbb{T}^g(Q)$ rather than $\mathbb{T}_n(Q)$ and $\mathbb{T}^g_n(Q)$.

For what concerns the proof, we briefly highlight the required adaptations.
"HT(ω) $\Rightarrow$ KT$_\ell$(ω)": the main difference involves the operations $\bigoplus_{r,q}$ which are now define for each natural number $r \in \mathbb{N}$; the family $\bigoplus_{\mathbb{N},Q}$ is well quasi-ordered by the "quotient order" over Q, i.e. $\bigoplus_{n,q} \trianglelefteq \bigoplus_{m,p}$ iff $q \leqslant p$ (we can not take directly $\mathbb{N} \times Q$ since, by Theorem 2.7, RCA$_0$ does not prove in general that $\mathbb{N} \times Q$ is a wqo). We have then a corresponding version of the claim.
CLAIM. $(\mathbb{T}(Q), \bigoplus_{\mathbb{N},Q}, \preccurlyeq)$ is an ordered algebra with $\preccurlyeq$ a divisibility order compatible with $\trianglelefteq$; moreover $C = \{q[\,] \mid q \in Q\}$ is a generating set for $\mathbb{T}(Q)$.
The proof of the claim, as well as the rest of this direction, is almost equal; a minor modification occurs for compatibility since, through $\trianglelefteq$, we can compare operations $\bigoplus_{r,q}$ and $\bigoplus_{s,p}$ with different arities, i.e. $r \neq s$.

"KT$_\ell$(ω) $\Rightarrow$ HT(ω)": in this case, M is directly a wqo and we apply KT$_\ell$(ω) to obtain the well-quasi-orderedness of $(\mathbb{T}(C \cup M), \preccurlyeq)$. The grade function g is now an extension of the arity function d of the abstract algebra under consideration, namely $g : C \cup M \to \mathbb{N}$ is defined as $g(x) = 0$ if $x \in C$ and $g(x) = d(x)$ if $x \in M$. The remaining minor changes are relative to notation. $\square$

Previous equivalences, in particular the finite one, allow for another possible proof of point *2.* of Corollary 2.1, namely $\mathrm{RCA}_0 \nvdash \mathrm{KT}(\omega) \to \forall n\, \mathrm{KT}_\ell(\mathrm{n})$.[13]
Alternative Proof of Corollary 2.1 Suppose, by contradiction, that the implication holds, then, by Theorem 2.23, we obtain $\mathrm{RCA}_0 \vdash \mathrm{KT}(\omega) \to \forall n\, \mathrm{HT}(n)$. From $\forall n\, \mathrm{HT}(n)$, one can easily deduce Higman's lemma, HL, which correspond to a particular case of HT(2), and so $\mathrm{RCA}_0 \vdash \mathrm{KT}(\omega) \to \mathrm{HL}$; this means that every model of RCA_0 satisfying $\mathrm{KT}(\omega)$ must satisfy also Higman's lemma. But now we obtain a contradiction because REC, the minimal ω-model of RCA_0 given by recursive sets, satisfies $\mathrm{KT}(\omega)$ (since $\mathrm{KT}(\omega)$ is a Π^1_1 statement); whereas REC does not satisfy Higman's lemma, for it is not a model of ACA_0 which is equivalent, over RCA_0, to Higman's lemma [169, Theorem X.3.22]. $\square$

We can sum up all previous results regarding Higman and Kruskal (including Theorem 2.17) in the following proof-relation schema where all the implications are over RCA_0:



2.3.3 Equivalence between Higman's and Dickson's Lemmas

Despite having been subsequently overtaken by Kruskal's theorem, Higman's and Dickson's lemma remain two remarkable milestones in the history of well quasi-order theory. In this section, we collect together the main proof theoretic results regarding this two achievements. For both clarity and brevity, we adopt the following abbreviations where A^* denotes the set of finite strings over A:

Definition 2.14

[13]We thank Anton Freund for suggesting this approach.

- *HL: standard Higman's lemma, i.e.* $\forall Q\,(Q\,wqo \to Q^*\,wqo)$*;*
- *HL*(ω)*:* $\mathbb{N}^*$ *is wqo, with the order on* $\mathbb{N}$ *given by the standard natural order* $\leqslant$*.*
- *HL*(n)*:* $\{0,\ldots,n-1\}^*$ *is wqo, with the order on* $\{0,\ldots,n-1\}$ *given by the equality, i.e.* $n \leqslant m$ *iff* $n = m$*.*
- *DL: Dickson's lemma, i.e.* $\mathbb{N}^n$ *is wqo for each* n*.*

Collecting several findings present in the literature [41, 45, 81, 90, 166, 169], we obtain the following summarizing result.

Theorem 2.25 *The following proof-ordinal estimations hold:*

1. $|RCA_0 + HL| = \varepsilon_0$*;*
2. $|RCA_0 + HL(\omega)| = |RCA_0 + \forall n\, HL(n)| = \omega^{\omega^{\omega+1}}$*;*
3. *for all* n $|RCA_0 + HL(n)| = \omega^{\omega^n}$*.*

The proof of the previous estimations derives mainly from the following three lemmas together with Lemma 2.3.

Lemma 2.5 *(Simpson, Girard)* $RCA_0 \vdash HL \longleftrightarrow ACA_0$*.*

Proof [169, Theorem X.3.22], see also [166, 81]. □

Lemma 2.6 *(Simpson, Clote)* $RCA_0 \vdash \forall n\, HL(n) \longleftrightarrow HL(\omega) \longleftrightarrow WO(\omega^{\omega^\omega})$*.*

Proof [45, Theorem 5], see also [166]. □

Lemma 2.7 *(Simpson, Hasegawa)* $RCA_0 \vdash HL(n) \longleftrightarrow WO(\omega^{\omega^{n-1}})$*.*

Proof In [90] R. Hasegawa proves it improving a well known result due to G. Simpson [166, sublemma 4.8]. □

Given the above results we easily obtain

Corollary 2.2 *Over* RCA_0 *the following chain of implications is provable:*

$$HL \to HL(\omega) \leftrightarrow \forall n\, HL(n) \ \to \ldots \to HL(n{+}1) \ \to \ HL(n) \to \ldots \to HL(2) \leftrightarrow DL.$$

The only proof-theoretical relation which does not derive immediately from the aforementioned results is the last one, namely $\mathrm{RCA}_0 \vdash \mathrm{HL}(2) \leftrightarrow \mathrm{DL}$. This can be obtained indirectly through another result by Simpson [169, Theorem X.3.20], i.e. $\mathrm{RCA}_0 \vdash \mathrm{DL} \leftrightarrow \mathrm{WO}(\omega^\omega)$. Nevertheless, we give an explicit proof adapting a constructive proof by J. Berger [21] for the framework of reverse mathematics. Since all the following definitions and results are stated or proved in RCA_0, we omit the usual notation (RCA_0).

Proposition 2.5 $RCA_0 \vdash HL(2) \leftrightarrow DL$.

Proof Denoted by $\mathbb{N}_+$ the set of positive integer and by $\{0,1\}^*_0$ the set of finite strings of 0 and 1 starting with a 0, we actually prove the equivalence over RCA_0 of the two following statements:

DL'**:** for all n, $\mathbb{N}^n_+$ is a wqo;

$HL'(2)$**:** $\{0,1\}^*_0$ is a wqo;

whose equivalence with, respectively, "DL" and "$HL(2)$" is apparent.

We denote by u, v, w the elements of $\{0,1\}^+_0$, by i an element of $\{0,1\}$ and by n, m, k, l the elements of $\mathbb{N}$; with an harmless abuse of notation, we denote by 0 both the natural number and the string consists only of the number 0. Moreover, by ui, we denote the string obtained from u by adding as final letter i and by $|u|$ the length of u, i.e. its number of letters.[14] We recall also that the quasi-order $\sqsubseteq$ over $\{0,1\}^*_0$ is given by substrings, namely $v \sqsubseteq w$ if $v = v_1 \dots v_p,\ w = w_1 \dots w_q$ and there exist $1 \leqslant r_1 < \cdots < r_p \leqslant q$ such that $v_j = w_{r_j}$ for all $1 \leqslant j \leqslant p$; whereas the quasi-order $\leqslant$ over $\mathbb{N}^n_+$ is given component-wise, i.e. $(k_1, \dots k_n) \leqslant (k'_1, \dots, k'_n)$ if $k_j \leqslant k'_j$ for all $1 \leqslant j \leqslant n$.

We define $\lambda\colon \{0,1\}^+_0 \to \{0,1\}$ as

$$\lambda(0) := 0 \text{ and } \lambda(ui) := i$$

i.e. $\lambda(w)$ is just the last letter of w.

We define $\Phi\colon \{0,1\}^*_0 \to \mathbb{N}$ as

$$\Phi(0) := 1 \ \text{ and } \Phi(ui) := \begin{cases} \Phi(u) & \text{if } \lambda(u) = i, \\ \Phi(u) + 1 & \text{if } \lambda(u) \neq i. \end{cases}$$

$\Phi(w)$ is called the *weight* of w and amounts to the number of "blocks" of 0's and 1's in w, e.g.,

$$\Phi(00) = 1, \quad \Phi(01100) = 3, \quad \Phi(011011100) = 5.$$

[14] Given the extensive use of strings we make in Sec. 3.4, there we adopt some different notations.

Moreover, we inductively define $F\colon\{0,1\}_0^* \to \bigcup_{n\geqslant 1} \mathbb{N}_+^n$ as

$$F(0) := 1 \text{ and } F(ui) := \begin{cases} (k_1,\dots,k_m+1) & \text{if } \lambda(u)=i, \\ (k_1,\dots,k_m,1) & \text{if } \lambda(u)\neq i, \end{cases} \quad \text{if } F(u)=(k_1,\dots,k_m).$$

F is a bijection which converts a string of weight m into an m-tuple counting the occurrences of 0's and 1's, e.g.,

$$F(00)=(2),\quad F(01100)=(1,2,2),\quad F(011011100)=(1,2,1,3,2).$$

Since we are dealing with finite strings of natural numbers, λ, Φ and F are all definable in RCA_0.

Fixed $n\in\mathbb{N}_+$, we denote by $\mathcal{W}_n$ the elements of $\{0,1\}_0^*$ with weight n and by F_n the restriction of F to $\mathcal{W}_n$. Thus, given the previous definitions we easily obtained the following claim.

CLAIM 1. $F_n\colon\mathcal{W}_n \to \mathbb{N}_+^n$ is an order isomorphism between $(\mathcal{W}_n, \sqsubseteq)$ and $(\mathbb{N}_+^n, \leqslant)$.

Proof of Claim 1. Straightforward.

We define also a length-normalizing function $G_n\colon\bigcup_{m\geqslant 1} \mathbb{N}_+^m \to \mathbb{N}_+^n$ as

$$G_n(k_1,\dots,k_m) = \begin{cases} (k_1,\dots,k_m,1,\dots,1) & \text{if } m<n, \\ (k_1,\dots,k_n) & \text{if } n\leqslant m. \end{cases}$$

For $u\in\{0,1\}_0^*$, we set

$$u!_n = F_n^{-1}(G_n(F(u))). \tag{2.1}$$

CLAIM 2. The following properties hold:

- $\Phi(u!_n) = n$;
- if $\Phi(u)=n$ then $u!_n = u$;
- if $\Phi(u)<n$ then $|u!_n| < |u|$;
- $G_n(F(u)) = F_n(u!_n)$.

Proof of Claim 2. Straightforward.

Before the main result, we state and prove two other claims.

CLAIM 3. For all v, w in $\{0,1\}_0^*$, we have

$$(2\cdot|v|\leqslant\Phi(w)) \;\Rightarrow\; v\sqsubseteq w$$

Proof of CLAIM 3. We reason by contradiction. Let $v=v_1\dots v_n$, $w=w_1\dots w_m$ with $\Phi(w)=k$, $2n\leqslant k$, but $v\not\sqsubseteq w$. We consider the word $u=01\dots01$ of length and weight $2n$; since for all $1\leqslant j\leqslant n$ $v_j=u_{2j-1}$ or $v_j=u_{2j}$, then $v\sqsubseteq u$. Moreover,

since $\Phi(u) = 2n \leqslant k = \Phi(w)$, we have that $u_j = \bar{w}_j$ where $\bar{w}_j$ is the first letter of the j-th block of w, and so $u \sqsubseteq w$. Thus $v \sqsubseteq u \sqsubseteq w$, contradiction. *This concludes the proof of Claim 3.*
CLAIM 4. For all v, w in $\{0,1\}^*_0$, we have

$$\Phi(v) \leqslant \Phi(w) \leqslant n \wedge v!_n \sqsubseteq w!_n \;\Rightarrow\; v \sqsubseteq w.$$

Proof of Claim 4. Let $k = \Phi(v)$. By $v!_n \sqsubseteq w!_n$ we obtain $G_n(F(v)) \leqslant G_n(F(w))$ and therefore

$$F_k(v) = G_k(F(v)) \leqslant G_k(F(w)) = F_k(w!_k),$$

thus

$$v \sqsubseteq w!_k.$$

Since $k \leqslant \Phi(w)$, $w!_k \sqsubseteq w$ holds and by transitivity $v \sqsubseteq w$. *This concludes the proof of Claim 4.*

We can now prove the main result of this section considering separately the two directions.
"$HL'(2) \Rightarrow DL'$": fix $n \in \mathbb{N}_+$ and an infinite sequence $f : \mathbb{N} \to \mathbb{N}^n_+$. By applying $HL'(2)$ to $F_n^{-1} \circ f$ we obtain $k < l$ with

$$F_n^{-1} \circ f(k) \sqsubseteq F_n^{-1} \circ f(l),$$

and thus, applying F, $f(k) \leqslant f(l)$.
"$DL' \Rightarrow HL'(2)$": fix an infinite sequence $g : \mathbb{N} \to \{0,1\}^*_0$ and set $n = 2 \cdot |g(0)|$. Then, applying DL', we obtain $k < l$ such that

$$(F_n(g(k)!_n), \Phi(g(k))) \leqslant (F_n(g(l)!_n), \Phi(g(l))).$$

If $n < \Phi(g(l))$, we have $g(0) \sqsubseteq g(l)$ by CLAIM 3. Otherwise, we have

$$\Phi(g(k)) \leqslant \Phi(g(l)) \leqslant n \text{ and } g(k)!_n \sqsubseteq g(l)!_n,$$

thus $g(k) \sqsubseteq g(l)$ by CLAIM 4. $\square$

Chapter 3

Well Quasi-Orders in Constructive Mathematics

In this chapter, we continue our journey in the theory of well quasi-orders exploring the topic from a completely different point of view: constructive mathematics. Constructive mathematics is a branch of mathematics where the underling classical logic is substituted by intuitionistic logic, which, roughly speaking, rejects the Law of Excluded Middle, LEM.

The content of this chapter, whose novel results are based on two joint articles respectively with Schuster and Blechschmidt [37] and Berardi and Schuster [19], mainly regards definitions and properties of wqo in a constructive setting; more precisely, we explore different definitions of Noetherianity (in particular the ascending chain conditions) and well quasi-orders, establishing their constructive nature and relations, and we present another constructive version of Higman's lemma regarding bars. For what concerns the structure, the first section is a gentle introduction to constructive mathematics which emphasizes the key points of constructive reasoning as well as some of its main subtleties (particularly in algebra); section two is dedicated to a constructive description of Noetherianity and well quasi-orders, focusing on their definitions and relations; in section three, we explore inductive definitions in constructive set theories; the fourth and last section exposes some constructive results in wqo theory regarding in particular Higman's lemma.

For an introduction to intuitionism, and more generally constructive mathematics, we refer to [183] and to the corresponding entries in the Stanford Encyclopedia, namely intuitionism [96] and constructive mathematics [30]; for what concerns proper constructive mathematical results instead, a classical reference are the two volumes by van Dalen and Troelstra [181, 182]. Regarding nomenclature, although intuitionism and constructivism are not synonyms, e.g. due to Brouwer's reflections on sequences or the nature of intuitionistic real numbers, given our constraints and results we reserve to use them as if they were.

3.1 A Brief Introduction to Constructive Mathematics

Given the constructive setting which characterizes this chapter and its results, we briefly summarize some salient points of constructive reasoning. This section is not meant to be a formal introduction to intuitionistic logic nor a compendium of constructive results for which we refer to [181, 182, 183]; the main goal is to emphasize some subtleties of the constructive approach, fixing some recurring concepts throughout the chapter.

3.1.1 The Constructive Framework

To clarify the peculiarities of constructive reasoning, we start with a non-constructive proof of a nevertheless constructively provable result.

Proposition 3.1 *There exist irrational numbers $a, b \in \mathbb{R} \setminus \mathbb{Q}$, such that a^b is rational, i.e. $a^b \in \mathbb{Q}$.*

Proof The classical approach uses excluded middle to reason by cases. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we take $a = b = \sqrt{2}$; if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$, obtaining $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$. In both cases we are done. □

This high-school-level proof leaves an utterly legitimate question: which case does actually hold? Thanks to the previous reasoning, we only know that at least one pair among $(\sqrt{2}, \sqrt{2})$ and $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$, in fact exactly one, satisfies the property; but without knowing *which* one. On the other hand, a constructive proof of Proposition 3.1 would furnish an explicit witness for the required property. For the curious reader, the right answer is $(\sqrt{2}^{\sqrt{2}}, \sqrt{2})$, being $\sqrt{2}^{\sqrt{2}}$ irrational by Gelfond–Schneider theorem [78].

Constructive mathematics can be seen as the practical application of a novel approach to the foundational issues raised in the beginning of the 20th century, an approach called *Intuitionism.* Stemming from the philosophical reflections of the Dutch mathematicians L.E.J. Brouwer[1](1881-1966) and based on a different

[1]For Brouwer's philosophical and logic writings we refer the reader to [32], whereas for the mathematical writings to [31].

conception regarding the interplay between thought, logic and mathematics, intuitionism proposes a new interpretation for the mathematical process and even for mathematical truths. Differentiating both from the platonic view [109], where mathematical entities exist per se in some hyperuranic world, and from the formalist approach [193], for which mathematics is just a game with pen and paper, intuitionism emphasizes the role of human mind which creates mathematical objects through its thought, starting from the "pure intuition of time" [32, pag. 127-128]. Mathematical objects exist, but as a product of our minds; we *construct* them. Thus, they, as well as our knowledge of them, are limited and we can not pretend to have a complete access to the properties of mathematical entities which we have not discovered, or better created, yet.

Considering mathematics independent from logic, Brouwer contributed a little to the formal foundation of constructive logic, but his teachings have not been lost. His most eminent student Arend Heyting (1898-1980) formalized intuitionistic logic, studying moreover the intuitionistic version of PA, nowadays called Heyting Arithmetic HA; for a survey on the scientific work of Heyting see [178]. After a period of quiescence in the second part of the first half of last century, a rebirth of constructive mathematics happened thanks to the works of Errett Bishop (1928-1983), in particular [24]. Bishop focused on a constructive approach toward "standard mathematics" results rather than built a new mathematical structure on a different grounding; thus setting aside all the philosophical debates regarding the "right" foundational view. In this short historical detour, also the Russian constructive recursive school, which studied recursion theory and computability using intuitionistic logic, deserves to be cited [108, 116]; similarly, we mention the constructive nature of Martin-Löf type theory [63] which has a foundational proposal different from set theory and revealed a strong connection between proofs and programs, the so-called Curry-Howard isomorphism [188]. For an historical survey regarding constructivism we refer to [180].

On the concrete level of daily mathematical practise, the most relevant characteristic of constructive mathematics is the rejection of the *Law of Excluded Middle* LEM; namely, given a formula p, it does not hold that either p or $\neg p$ is true, formally speaking $p \vee \neg p$ is not in general an intuitionistic axiom. From this other logic principles, implying or equivalent to LEM, are judged not valid: first of all *Double Negation Elimination* DNE, from $\neg\neg p$ we can not derive p, i.e. $\neg\neg p \to p$ is not valid; since DNE is not accepted, similarly are not accepted proofs by contradiction; even some non-logical axioms are excluded from constructive proofs, for example the Axiom of Choice [60]. Given only these formal restrictions, it is not always clear which is the essence of intuitionism in mathematical practise. To convey a comprehension of constructive reasoning, a standard tool is the so-called BHK *interpretation*, from the initials of the three mathematicians (Brouwer, Heyting and

Kolmogorov) who, partially independently, developed it. The BHK interpretation provides an informal explanation of the intuitionistic meaning of logical connectives, using an undefined concept of *proof*. Let p and q be two mathematical statements and denote the absurdity with $\perp$, then:

- a proof of $p \wedge q$ is given by a proof of p together with a proof of q;
- a proof of $p \vee q$ is by a proof of p or a proof of q together with the specification of which proposition among p, q is proved;
- a proof of $p \to q$ is a construction which converts any proof of p in a proof of q;
- $\perp$ has no proof;
- a proof of $\neg p$ is a proof of $p \to \perp$, i.e., it is a construction showing the impossibility of a proof of p.

If the statement considered involves quantifiers the interpretation is as follows:

- a proof of $\forall x\, p(x)$ is a construction which converts any element d of the domain of discourse D into a proof of $p(d)$;
- a proof of $\exists x\, p(x)$ is given by a witness $d \in D$ and a proof of $p(d)$.

A consequence of the last two points is that, differently from classical logic, for an intuitionistic mathematician $\neg\forall x\, \neg p(x)$ is not equivalent to $\exists x\, p(x)$; the fact that is absurd that all x do not satisfy p ($\neg\forall x\, \neg p(x) \equiv \forall x\, \neg p(x) \to \perp$) does not suffice to state the existence of a witness for p. Other counterintuitive facts of intuitionistic reasoning will be presented and analysed later.

Given all these restrictions on what constitutes constructive reasoning, a legitimate question is about what we earn from such an approach. Beside to settle the original philosophical issues which stimulated the birth of intuitionism, the most remarkable aspect regards the deeper comprehension of a result, even a classical one, obtained by applying a constructive approach; quoting Henry Lombardi [111, pag. 2]: "[...] when one cannot use magic tools as the law of excluded middle (LEM), it is necessary to understand what is the true content of a classical proof. Also, usual shortcuts allowed in classical proofs introduce sometimes useless detours. In order to understand clearly a problem, prescience may be a handicap." Another fruitful product became apparent with the computer science revolution, the absence of "prescience" allows for a far more easily implementation of constructive results inside programs; more precisely, from the constructive proof of a statement it is possible to mechanically extract an algorithmic witness of the statement itself, with the correctness of such an algorithm ensures by the correctness of the proof. More generally, the use of intuitionistic techniques allows "to mine" bounds and informations even from a classical proof. For a survey on this second aspect, we refer to [120, 164] for program extraction and to [103, 104] for the so-called "proof mining" project. The connection between constructive reasoning and computation can be effectively used to prove that some results are not constructively provable, something more about this relation and its usefulness can be found in Subsec. 3.1.2.

Finally, although the aforementioned restrictions depict intuitionistic logic as a proper subset of classical logic, the so-called *double negation translation* [82, 84][2] overturns this picture furnishing an embedding of the latter into the former; in this view intuitionistic logic, distinguishing more cases then the classical one (e.g. separating p and $\neg\neg p$), can be seen not as a subcase, but as an extension.

Although the use of excluded middle may be particularly subtle sometimes, its most common direct applications are given by case distinction, such as in the proof of Proposition 3.1, and proof by contradiction: if $\neg p$ leads to a contradiction, then p holds. It is not tough to detect an appeal to these techniques, since normally it is explicitly stated; however, it ought to be remarked that the proof of a negation may be mistaken for a proof by contradiction. More precisely, since $\neg p$ is an abbreviation of $p \to \bot$, to prove $\neg p$ we *do assume* p in order to derive a contradiction and thus $\bot$.

As already said, there are axioms which are not acceptable in constructive mathematics; the archetype is the Axiom of Choice which implies excluded middle [60], but many other properties or principles fall in this category. A standard way to obtain that a specific result is not constructive consists in proving, from the result under consideration, a non-constructive principle or consequence; we will repeatedly use this technique afterwards.

Given its relevance in our results, the notion of *constructively meaningful definition* deserves some comments. First of all is not a formal definition, or better a formal meta-definition, but rather an heuristic concept: it denotes the definitions which have a sensible use in constructive mathematics, here is an example. Suppose that a definition regarding sets is given, so a set is "X-special" if it satisfies some conditions; if the only set for which we can constructively prove that is X-special is the empty set, then X-special is not a constructively acceptable definition, or shortly, its not a constructive definition. The idea is that a definition can have classical applications and yet being constructively useless, having constructively only trivial examples. Given its informal nature, we might be a little sloppy when referring to non-constructive definitions.

[2] Through the years, many different "negative translations" have been proposed, see [67] for a systematic study.

3.1.2 Ordinary Mathematics Constructively

We start with a relevant definition which, as opposed to "constructively acceptable", can be formally stated.

Definition 3.1 *A set A is* FINITELY ENUMERABLE*, or simply* FINITE*, if there exists, constructively, a natural number $n \geqslant 0$ such that all the elements of A can be listed as $\{a_1, \ldots, a_n\}$, possibly with repetitions.*

With this definition, adopted also in [66, 156, 194], we slightly deviate from the prevalent terminology of constructive mathematics and set theory [5, 6, 24, 119] for which *finite* means in bijection with $\{1, \ldots, n\}$ for a unique $n \geqslant 0$. Regarding this point see also footnote 4 of [194] and page 11 of [119].

After having introduced the formal intuitionistic system in which our results could be in principle formalized, we will see a puzzling example of the subtleties of constructive reasoning: the subsets of a finite set need not to be finite!

There are many different frameworks which can be adopted as formal foundations for constructive mathematics such as Martin-Löf Type Theory [63] or Category theory [112, 117]; here we briefly expose a set theoretical proposal: *Intuitionistic Zermelo Fraenkel*, IZF. Originally developed by Harvey Friedman [157], IZF amounts to an intuitionistically acceptable version of Zermelo-Fraenkel set axioms, ZF; more precisely, ZF is equivalent to IZF plus the Law of Excluded Middle. The main reference we follow is [6]; for further references and details see [52].

Given the sensitivity of intuitionistic logic to non-logical axioms, ZF axioms, as they stand, are not a valid choice; for example, the foundation axiom $\forall a\, (\exists x\, x \in a \rightarrow \exists x \in a\, (x \cap a = \emptyset))$ implies a restricted form of LEM; thus it must be substituted by set induction schema which is classically, but not intuitionistically, equivalent. The axioms of IZF are formulated in first order intuitionistic logic with a binary predicate $\in$ as only non logical symbol; we use the notation introduced in Sec. 1.6.

Definition 3.2 *The axioms of IZF are as follows:*

Extensionality

$$\forall a\, \forall b\, [\forall z\, (z \in a \leftrightarrow z \in b) \rightarrow a = b];$$

Pairing

$$\forall a\, \forall b\, \exists y\, \forall z\, [z \in y \leftrightarrow (z = a \vee z = b)];$$

Union

$$\forall a\, \exists y\, \forall z\, [z \in y \leftrightarrow \exists x \in a\, (z \in x)];$$

Powerset

$$\forall a\, \exists y\, \forall z\, [z \in y \leftrightarrow z \subseteq a];$$

Infinity

$$\exists a\,[\exists x\, x \in a \;\wedge\; \forall x \in a\, \exists y \in a\, (x \in y)];$$

Set Induction Schema

$$\forall a\,[(\forall x \in a\, \phi(x)) \rightarrow \phi(a)] \rightarrow \forall a\, \phi(a),$$

for all formulas $\phi(a)$*;*

Separation Schema

$$\forall a\, \exists y\, \forall z\, [z \in y \leftrightarrow z \in a \wedge \phi(z)],$$

for all formulas $\phi(x)$ *where* y *is not free;*

Collection Schema

$$\forall x \in a\, \exists y\, \phi(x, y) \rightarrow \exists b\, \forall x \in a\, \exists y \in b\, \phi(x, y),$$

for all formulas $\phi(x, y)$ *where* b *is not free.*

In this context, another intuitionistically acceptable system, weaker than IZF, well deserves to be mentioned, namely *Constructive Zermelo Fraenkel*, CZF [6]. CZF differs from IZF for three axioms: separation schema is restricted to *bounded* formulas; collection schema is strengthened to a strong collection schema; and powerset is replaced by a subset collection schema. This separation and powerset substitutions ensure the *predicativity* of CZF, in contrast with the impredicativity of IZF, see Subsec. 3.3.2 for more regarding this point.

As previously anticipated, we present now a non-finite subset of a finite set. Let $\mathbb{B} = \{0, 1\}$ and let φ be the statement of an open problem, such as the Riemann's Hypothesis; we define a set A in the following way

$$A := \{x \mid x = 0 \;\vee\; (x = 1 \wedge \varphi)\}.$$

The set A exists by separation axiom, is a subset of $\mathbb{B}$, but is not finite; since, if it were, then we could list its elements, i.e. $A = \{a_1, \ldots, a_n\}$, with each element being 0 or 1, thus we could take the maximal value. If it is 0, then the only element of A is 0 and φ is false, if it is 1, 1 is an element of A and φ must be true; but we do not know if φ is true or false. This example should warn about the application of classical logical principles which might seems in principle harmless.

We consider now algebra and relations, particularly order relations, in a constructive setting; for a thorough exposition of constructive algebra we refer to [119].

As for sets, reasoning constructively regarding relations requires some cautions. The first one regards *decidable* relations.

Definition 3.3 *Given a binary relation R, R is* DECIDABLE *if for all x, y*

$$xRy \ \vee \ \neg xRy.$$

Classically this is a trivial application of excluded middle, but constructively this means that we have an effective procedure to establish which one, among xRy and $\neg xRy$, holds. Obviously not all relations are decidable, e.g. if a Turing machine halts or not on a given input (which is just the Halting Problem); in particular, it may happen that even equality, i.e. establishing if two elements are the same, is not decidable [151, 152]. Thus, requiring decidable relations in a statement is a strengthening of the hypotheses from an intuitionistic point of view.

Focusing on order relations, this means that moving between the strict $<$ and large version $\leqslant$ of a partial order is not always granted. Namely, if the order relation is decidable, then everything works as in classical logic; if not, we can still construct the other version of a given order, but it may have different properties.

If we restrict ourself to natural numbers, something more can be said. More precisely, the standard order relation $\leqslant$ on $\mathbb{N}$ is decidable, as well as any relation expressed by a bounded formula. Nevertheless, although $\leqslant$ is decidable, some simple and seemingly harmless principles regarding $\leqslant$ are not constructive; we give two example of such principles.

The first one is the *minimum principle*, i.e. "every non empty subset of $\mathbb{N}$ as a minimum". The proof of the non-constructivity of this principle is similar to the existence of non-finite subsets of a finite set; it suffices to consider the set $B = \{x \mid (x = 0 \wedge \varphi) \vee x = 1\}$ for a yet unproven and not disproven sentence φ.

The second is the *Limited Principle of Omniscience* LPO elaborated by Bishop [24] which is used subsequently. The most common version of LPO states that, for every infinite binary sequence α, α consists only of zeroes or there exists an index n such that $\alpha(n) = 1$; formally

$$LPO :\Leftrightarrow \forall \alpha \colon \mathbb{N} \to \{0,1\}(\forall n\, \alpha(n) = 0 \ \vee \ \exists n\, \alpha(n) = 1),$$

again this is classically obtained by excluded middle.

For sake of completeness, there exist also the *Weak* Limited Principle of Omniscience WLPO, $\forall \alpha \colon \mathbb{N} \to \{0,1\}(\forall n\, \alpha(n) = 0 \ \vee \ \neg\forall n\, \alpha(n) = 0)$, and the *Lesser* Limited Principle of Omniscience LLPO, $\forall \alpha, \beta \colon \mathbb{N} \to \{0,1\}\, [\neg(\exists n\, (\alpha(n) \neq 0) \wedge \exists n\, (\beta(n) \neq 0)) \to \neg\exists n\, (\alpha(n) \neq 0) \vee \neg\exists n\, (\beta(n) \neq 0)]$; for a thorough analysis of these principles we refer to [98].

Even in algebra, reasoning constructively imposes some restrictions, as we can see from the following proposition which extends the previous example regarding finite sets to algebraic structures.

Proposition 3.2 *The field with two elements $\mathbb{F}_2$ does not satisfy the* FINITE BASIS PROPERTY, *i.e., $\mathbb{F}_2$ has ideals which are not finitely generated.*

Proof consider the same subset as before

$$A := \{x \mid x = 0 \lor (x = 1 \land \varphi)\}.$$

This subset is an ideal of $\mathbb{F}_2$, even constructively, but it is not finitely generated. □

This lack of $\mathbb{F}_2$ is one of the starting points for the next section.

3.2 A Constructive Picture of Noetherianity and Well Quasi-Orders

In this section, based on a joint article with Peter Schuster and Ingo Blechschmidt [37], we analyse, from an intuitionistic point of view, the main definitions for *well quasi-orders*, wqo, present in the literature together with the related constructively viable concepts of Noetherian ring. Despite being all equivalent to each other in the classical setting, their constructive contents are different, as we have already seen in Subsec. 2.1.3 for the reverse mathematics context. Our goal is to carry out a first joint analysis of Noetherianity and well quasi-order theory, in such a way that the rich literature of the former can be usefully applied to the latter. We thus aim for a more comprehensive picture of partial and quasi-order properties in the spirit of intuitionistic and constructive reverse mathematics [98, 124, 187].

3.2.1 Noetherianity in a Constructive Setting

The concept of a Noetherian ring or module is ubiquitous in abstract algebra. Not least for its important role in computational algebra, e.g., for the termination of Buchberger's algorithm, from the half of the last century Noetherianity has been studied also in constructive algebra [119, 153, 161] up to Gröbner bases [51, 195]. The initial challenge for the latter setting was that, with intuitionistic logic, only the trivial ring can be proved Noetherian according to the classical definitions.

Nevertheless, many constructively sensible definitions are present in the literature. We start off with the one given by Richman [153] and Seidenberg [161] reworking an idea of Tennenbaum's [177], and with how it differs from the classical concept.

Definition 3.4 *A commutative ring R has the property*

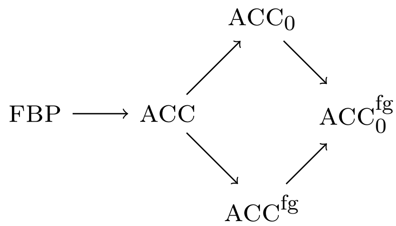
1. FBP (FINITE BASIS PROPERTY) *if every ideal of R is finitely generated;*
2. ACC *if in R every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$* STABILIZES *in that there exists an index n such that $I_n = I_{n+1} = \dots;$*

3. ACC$^{\text{fg}}$ *if in R every ascending chain of finitely generated ideals $I_1 \subseteq I_2 \subseteq \dots$ stabilizes in that there exists an index n such that $I_n = I_{n+1} = \dots$;*

4. ACC$_0$ *if in R every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$* STALLS *in that there exists an index n such that $I_n = I_{n+1}$.*

5. ACC$_0^{\text{fg}}$ *if in R every ascending chain of (finitely generated) ideals $I_1 \subseteq I_2 \subseteq \dots$ stalls in that there exists an index n such that $I_n = I_{n+1}$.*

The relations above these definitions can be schematized as follows:



where ACC is derived from FBP by considering, for a given ascending chain of ideals $I_1 \subseteq I_2 \subseteq \dots$, a finite generating subset $\{a_1, \dots, a_r\}$ of the union $\bigcup_n I_n$ (which is an ideal and thus finitely generated by FBP) and then the least index $\bar{n}$ such that $\{a_1, \dots, a_r\} \subset I_{\bar{n}}$; thus, $I_{\bar{n}} = I_{\bar{n}+1} = \bigcup_n I_n$.

The classical *ascending chain condition* due to Noether is ACC, whereas ACC$_0^{\text{fg}}$ is Richman's and Seidenberg's constructive substitute [153, 161], thus often dubbed *RS-Noetherian*. The latter was motivated by the observation that FBP, ACC and ACC$^{\text{fg}}$ cannot be verified with intuitionistic logic but for the trivial ring [53, 153].

While the Noetherian conditions listed in Def. 3.4 are classically equivalent, their known constructive relations are displayed in the figure above, and we conjecture that none of the implications can be reversed with the arrows from ACC$_0^{\text{fg}}$ to ACC$^{\text{fg}}$ and from ACC$^{\text{fg}}$ to ACC having already counterexamples. We now show that the hybrid condition ACC$_0$—referring to arbitrary ideals but requiring only stalling, not stabilizing—is not constructively sensible, thus settling an issue raised by the late Ray Mines.[3] The idea is to prove that if ACC$_0$ holds for a non trivial field, namely the two-element field, then we can derive a non-constructive principle, i.e., every increasing sequence of truth values stalls

Proposition 3.3 *The field with two elements satisfies the condition* ACC$_0$ *if and only if every increasing sequence of truth values stalls; but there are topological models which falsify this principle.*

[3] Personal communication by Hajime Ishihara, January 2023.

Proof In classical logic, a sequence $(\Psi_i)_{i\in\mathbb{N}}$ of truth values which is "increasing", in that $\Psi_i \Rightarrow \Psi_{i+1}$ for all $i \in \mathbb{N}$, always *stalls*: There always exists a number n such that $\Psi_n \Leftrightarrow \Psi_{n+1}$. Indeed, if $\neg\Psi_2$, then $\Psi_2 \Rightarrow \Psi_1$, and if Ψ_2, then $\Psi_3 \Rightarrow \Psi_2$.

This principle is not constructively acceptable, for in the topological model of intuitionistic logic given by the Heyting algebra of opens in the real line, the ascending sequence $((-n, n))_{n\in\mathbb{N}}$ does not stall (for a brief introduction to topological models see, e.g., [174, Section 4]). The intervals $(-n, n)$ are the truth values of the sentences "$|\xi| < n$", where ξ is the generic real number of the topological model (the identity function $\mathbb{R} \to \mathbb{R}$).

In contrast, if the field $\mathbb{F}_2 = \{0, 1\}$ with two elements validates ACC_0, then every increasing sequence $(\Psi_i)_i$ of truth values does stall. We build the ascending chain of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ where $\mathfrak{a}_i = \{x \in \mathbb{F}_2 \mid x = 0 \vee \Psi_i\}$. By ACC_0, this sequence stalls, that is there exists a number $\bar{n}$ such that $\mathfrak{a}_{\bar{n}} = \mathfrak{a}_{\bar{n}+1}$; hence $1 \in \mathfrak{a}_{\bar{n}+1} \Rightarrow 1 \in \mathfrak{a}_{\bar{n}}$ and thus, by definition of these ideals, $\Psi_{\bar{n}+1} \Rightarrow \Psi_{\bar{n}}$.

The converse direction rests on the fact that two ideals $\mathfrak{a}, \mathfrak{a}' \subseteq \mathbb{F}_2$ are equal iff the truth values of $1 \in \mathfrak{a}$ and $1 \in \mathfrak{a}'$ agree. □

Our next result is a source of countermodels for the converse of the implication $\text{ACC}^{\text{fg}} \Rightarrow \text{ACC}_0^{\text{fg}}$ since the field with two elements verifies ACC_0^{fg}, but models of constructive mathematics which falsify Bishop's *limited principle of omniscience* (LPO) abound. Here, we take this principle to mean that every infinite descending binary sequence $\mathbb{N} \to \mathbb{B}$ is either constantly one or contains a zero. For instance, LPO is falsified in the effective topos (see [29, Section 4.2] for a survey and the references [14, 95, 136, 185]).

Proposition 3.4 *The field with two elements validates* ACC^{fg} *iff* LPO *holds.*

Proof For the "only if" direction, let $\alpha : \mathbb{N} \to \mathbb{B}$ be an infinite descending binary sequence. Then the family $(\mathfrak{a}_n)_{n\in\mathbb{N}}$ given by $\mathfrak{a}_n := (1 - \alpha(0), \ldots, 1 - \alpha(n)) \subseteq \mathbb{F}_2$ (where we identify the two elements of $\mathbb{B}$ with the zero and unit element of $\mathbb{F}_2$) is an ascending sequence of finitely generated ideals. By assumption, this sequence stabilizes at some index n. Either $\mathfrak{a}_n = (0)$ or $\mathfrak{a}_n = (1)$. If the former, then α is constantly one. If the latter, then α has a zero among the terms 0 to n.

The "if" direction follows from the observation that every finitely generated ideal of $\mathbb{F}_2$ is either (0) or (1). □

Bauer [15] first considered the variant of the effective topos which is built using the infinite-time Turing machines of Hamkins, Kidder and Lewis [88]. This topos provides a countermodel for the reversal of the implication $\text{ACC} \Rightarrow \text{ACC}^{\text{fg}}$; for background on realizability toposes, we refer to [185].

Proposition 3.5 *In the realizability topos corresponding to infinite-time Turing machines, the field with two elements validates* ACC^{fg} *but not* ACC.

Proof This realizability topos is known to validate the limited principle of omniscience [15], so its field with two elements validates $\textsc{acc}^{\text{fg}}$ by Proposition 3.4. Assuming that it also validates $\textsc{acc}$, we obtain a contradiction as follows, arguing internally to the topos.

If M is any infinite-time Turing machine, then because the ascending chain

$$\{x \in \mathbb{F}_2 \mid x = 0 \vee (M \text{ halts on at least one of the inputs } 0, \ldots, n)\}$$

stabilizes, there is a number $n_M \in \mathbb{N}$ such that M halts on at least one of the inputs $0, \ldots, n_M$ iff there is at least one input $k \geqslant n_M$ on which it terminates. By countable choice (available in the topos even if it is not on the meta level), we obtain a map $M \mapsto n_M$ and an infinite-time Turing machine E computing this map.

The following description then defines a self-referencing machine P defeating E: "Read a number n as input. Simulate E on input P. Compare n with n_P. If $n > n_P$, then terminate. Else go into an infinite loop." (The self-reference is resolved by Kleene's second recursion theorem, whose textbook proof carries over step for step to infinite-time Turing machines.) This machine terminates on input $n_P + 1$, but does not terminate on any of the inputs $0, \ldots, n_P$. □

Topological countermodels for the reversal of the implication $\textsc{acc} \Rightarrow \textsc{acc}^{\text{fg}}$ also exist; for the required background, we refer to [174, Section 4] and to [28].

Proposition 3.6 *In the topological model over the real line, there is a ring validating* $\textsc{acc}^{\text{fg}}$ *but not* $\textsc{acc}_0$ *(hence also not* $\textsc{acc}$*).*

Proof Let M be the subset, internally speaking, of the naturals which contains n with truth value the open interval $(-1/n, 1/n)$ as in [25, Example 2]. The polynomial ring $\mathbb{Z}[M]$ over this set validates $\textsc{acc}^{\text{fg}}$ but not $\textsc{acc}$. It validates $\textsc{acc}^{\text{fg}}$ because, due to connectedness of open intervals, a finitely generated sheaf of ideals over an open interval is globally generated over every slightly smaller open interval. It falsifies $\textsc{acc}$, and also $\textsc{acc}_0$, because the sequence of ideals generated by $M \cap {\downarrow}(n)$ neither stabilizes nor stalls. □

Beyond RS-Noetherianity, we consider now five other constructive versions of Noetherianity, namely: *ML-Noetherianity*, proposed by Martin-Löf (from whom the letters ML are derived) and applied by Jacobsson and Löfwall [99]; *strong Noetherianity*, developed by Perdry [133]; *inductive Noetherianity*, considered by Coquand, Lombardi and Persson [47, 49, 50]; and *tree Noetherianity* and *processly Noetherianity*, tailored for nondeterministic algorithms and originally proposed respectively by Richman [154] and by Blechschmidt [27, Section 3.9].
For some of the above definitions we need the following auxiliary properties :

Definition 3.5 *Let* $(E, \leqslant)$ *be a partial order and* $<$ *the associated strict order.*

1. *A subset* $H \subseteq E$ *is* HEREDITARY *iff* $\forall x \in E\,(\{y\,|y<x\} \subseteq H \Rightarrow x \in H)$.

2. *The poset* E *is* HEREDITARILY WELL-FOUNDED, hwf, *if the only hereditary subset* H *of* E *is* $H = E$.

3. *The poset* E *is a* HEREDITARILY WELL-ORDER *iff it is a hereditarily well-founded linear order.*

4. *An* ASCENDING TREE *with values in* E *is a family* $(x_i)_{i\in I}$ *of elements of* E *such that* I *is a tree (in the sense of [154, Section 1]) and such that* $j < k$ *in* I *implies* $x_j \leqslant x_k$. *Such a tree* STALLS *iff there are indices* $j < k$ *such that* $x_j = x_k$.

5. *An* ASCENDING PROCESS *with values in* E *consists of an initial value* $x_0 \in E$ *and a function* $f : E \to \mathcal{P}(E)$ *such that for every* $x \in E$ *and every* $y \in f(x)$, $x \leqslant y$, *and: (1) the set* $f(x_0)$ *is inhabited; (2) for every number* n *and for all elements* $x_1, \ldots, x_n$ *such that* $x_{i+1} \in f(x_i)$ *for* $i = 0, \ldots, n-1$, *the set* $f(x_{n+1})$ *is inhabited. Such a process* STALLS *iff there exists a number* n *and elements* $x_1, \ldots x_n$ *such that* $x_{i+1} \in f(x_i)$ *for* $i = 0, \ldots, n-1$ *and such that* $x_n \in f(x_n)$.

6. *For a predicate* P *on ascending finite lists* σ *of elements of* E, *we inductively generate the predicate "*$P \mid \sigma$*" (pronounced "*P *bars* σ*") by the following clauses:*

   (a) *If* $P(\sigma)$, *then* $P \mid \sigma$.

   (b) *If* $P \mid \sigma x$ *for all elements* $x \in E$ *such that* $x \geqslant \sigma$, *then* $P \mid \sigma$.

   Here and in the following, by "$x \geqslant \sigma$*" we mean that* $x \geqslant y$ *for all terms* y *of* σ.

Part 7 of Def. 3.5 is to be read within generalized inductive definitions [1, 5, 6, 143](see also Sec. 3.3) according to which $P \mid \sigma$ is the least predicate on ascending finite list σ of elements of E which satisfies the clauses (a) and (b) (see also Sec. 3.3). In particular, $P \mid \sigma$ is tantamount to: If Q is a predicate on ascending finite lists σ of elements of E such that

1. if $P(\sigma)$, then $Q(\sigma)$, and

2. if $Q(\sigma x)$ for all $x \in E$ such that $x \geqslant \sigma$, then $Q(\sigma)$,

then $Q([\,])$.

As, e.g., in [134] we now consider Noetherian conditions for arbitrary partial orders, not necessarily stemming from ideals of commutative rings.

Definition 3.6 *A partial order* $(E, \leqslant)$ *is*

1. NOETHERIAN *iff for every ascending chain* $e_1 \leqslant e_2 \leqslant \dots$ *in* E *there exists a number* n *such that* $e_n = e_{n+1} = e_{n+2} = \dots$*;*

2. RS-NOETHERIAN *iff for every ascending chain* $e_1 \leqslant e_2 \leqslant \dots$ *in* E *there exists a number* n *such that* $e_n = e_{n+1}$*;*

3. ML-NOETHERIAN *if the* REVERSE *order* $(E, \geqslant)$ *is hereditarily well-founded;*

4. STRONGLY NOETHERIAN *iff there exists an hereditarily well-order* W *and a map* $\phi : E \to W$ *which is* STRICTLY DESCENDING*: that is,* $e < f \Rightarrow \phi(f) < \phi(e)$*;*

5. PROCESSLY NOETHERIAN *iff every ascending process with values in* E *stalls;*

6. TREE NOETHERIAN *iff every ascending tree with values in* E *stalls;*

7. INDUCTIVELY NOETHERIAN *iff* Stalls | [ ]*, where* Stalls(σ) *expresses that the ascending finite list* σ *of elements of* E *contains repeated terms.*

Consequently, a ring is Noetherian (resp. RS-Noetherian, . . .) if the partially ordered set of its finitely generated ideals is Noetherian (resp. RS-Noetherian, . . .). Although we will focus on the applications of these definitions in the specific case of the family of closed subsets of a well quasi-order, further abstract developments are possible [134]. Moreover, the tree and the process condition are equivalent [27, p. 36].

A first analysis unveils quite a complex picture of relations between these notions. For instance, inductive Noetherian implies ML-Noetherian, but ML-Noetherian implies RS-Noetherian only in the case that equality of comparable elements is decidable. On the other hand, inductive Noetherian implies RS-Noetherian also without any decidability condition. Hence the conditions seem not fit into a linear hierarchy. The picture is clarified when we introduce a classically equivalent but constructively stronger relation $\leqslant'$ derived from $\leqslant$: $x \leqslant' y$ iff $x = y \vee x < y$. We then obtain the following two-dimensional picture.

Theorem 3.1 *Let* $(E, \leqslant)$ *be a partial order. Let* E' *be the partial order with the same underlying set as* E *but with* $\leqslant'$ *as ordering relation. Then:*

$$
\begin{array}{ccccccc}
 & & \text{ind} \Longrightarrow & \text{tree} \Longrightarrow & \text{RS} & & \text{for } E \\
 & & \Uparrow\Downarrow & \Uparrow\Downarrow & \Uparrow\Downarrow & & \\
 & & \text{ind} \Longrightarrow & \text{tree} \Longrightarrow & \text{RS} & & \text{for } E' \\
 & & \Updownarrow & & & & \\
\text{strong} & \Longrightarrow & \text{ML} & & & & \text{for } E \text{ and for } E'
\end{array}
$$

The dotted implications hold whenever equality of comparable elements is decidable for E, that is if $x \leqslant y \Rightarrow (x = y \vee x < y)$; in this case $\leqslant$ and $\leqslant'$ agree.

Proof The conditions "strong" and "ML" are equivalent for E and E' because these only refer to the induced strict orders $<$ and $<'$, which coincide.

"Ind implies tree": For ascending finite lists σ of elements of E, we define the predicate $Q(\sigma)$ stating that every ascending tree $(x_i)_{i\in I}$ with a path in which all terms of σ occur stalls. Assume that Stalls $|$ [ ], we need to verify $Q([\,])$ and do so by induction.

1. If Stalls(σ), i.e. σ contains repeated terms, then trivially $Q(\sigma)$.

2. Assume that $Q(\sigma a)$ holds for all $a \geqslant \sigma$. To prove $Q(\sigma)$, let $(x_i)_{i\in I}$ be an ascending tree containing a path in which all terms of σ occur. By the tree condition, this path can be enlarged to a path containing a further term a. Hence $(x_i)_{i\in I}$ is an ascending tree which has a path containing all terms of σa and hence stalls by $Q(\sigma a)$.

"Tree implies RS": Every ascending sequence is also an ascending tree.
"Strong implies ML": [133, p. 517].
"Ind for E' implies ML": For ascending finite lists σ of elements of E', we define the predicate $Q(\sigma)$ stating that:

> For every hereditary subset $H \subseteq E'$ and for every element $x \in E'$, if the list σx is ascending and does not contain repeated terms, then $x \in H$.

Using the induction principle available by the assumption that E' is inductively Noetherian, we will prove $Q([\,])$, thereby validating that E' is ML-Noetherian.

1. If σ contains repeated terms, then $Q(\sigma)$ by ex falsum quodlibet.

2. Assume that $Q(\sigma x)$ holds for all $x \in E'$ such that $x \geqslant' \sigma$, i.e. σx is ascending. To prove $Q(\sigma)$, let $H \subseteq E'$ be a hereditary subset and let $x \in E'$ be an element such that σx is an ascending list without repeated terms. To verify $x \in H$, we show $y \in H$ for every element $y > x$. This follows from $Q(\sigma x)$, for the list $\sigma x y$ is ascending and without repeated terms.

"ML implies ind for E'": Let Q be a property of finite ascending lists σ of elements of E' such that (1) Stalls(σ) $\Rightarrow Q(\sigma)$ and (2) $(\forall (x \geqslant' \sigma)\ Q(\sigma x)) \Rightarrow Q(\sigma)$. It suffices to verify that the set $H := \{x \in E \,|\, \forall(\sigma \leqslant' x)\, Q(\sigma x)\}$ is hereditary; in fact, if $H = E$ by ML, then $Q(\sigma)$ for all σ by property (2).

So let an element $x \in E$ be given and assume that $y \in H$, for all $y > x$. To prove $x \in H$, let σ be an ascending list such that $\sigma \leqslant' x$, i.e. σx is also an ascending list. We verify $Q(\sigma x)$ by making use of property (2).

So let $y \geqslant' x$ be given. Hence either $y = x$ or $y > x$. In the first case, we have Stalls(σxy) and hence $Q(\sigma xy)$ by property (1). In the second case, we have $Q((\sigma x)y)$ by $y \in H$. □

We conjecture that none of the solid implications can be constructively reversed. The question whether "strong ⇒ ML" could be reversed is already raised in [134, p. 123]. Blass gave an example falsifying "RS ⇒ ML" in a topological model [25, Example 2]; his example also falsifies "tree ⇒ ML". Because there the ordering relation is decidable, there is no difference between ML and inductive Noetherian.

On ML-Noetherian, which for important applications such as the Hilbert basis theorem requires that equality of comparable elements is decidable, Richman writes [154]: "This seems necessary and is reasonable for a theory that emphasizes strict inclusion of ideals. I have yet to learn to love this approach although I have tried, off and on, for many years." With his proposed ascending tree condition he can indeed do without decidability assumptions; however, for his version of the Hilbert basis theorem he still requires an additional coherence hypothesis.

The cleanest form of the Hilbert basis theorem is instead obtained for inductive Noetherian: If R is inductively Noetherian, then so is $R[X]$ [50, Corollary 16]. Our Theorem 3.1 puts this state of affairs into a wider context: The tree condition is already on the right track because it uses $\leqslant$ instead of $\leqslant'$. On the other hand, it is slightly too weak—the ML condition is better from this point of view. Since ML is just inductive Noetherian for $\leqslant'$, the resolution is to use inductive Noetherian, but for $\leqslant$; that is, the Noetherian condition of Coquand and Persson.

3.2.2 Wqo Definitions and their Relations

We will treat now, within the same constructive spirit of the previous subsection, well quasi-orders and their relations.

By moving from partial orders to quasi-orders one leaves out the antisymmetry requirement. As usual we omit the subscript Q from the qo when there is no ambiguity, i.e. we write just Q for a qo if the relation over it is clear from the context. Moreover we recall, from Sec. 1.2 some notation, namely we abbreviate as follows: $p<q$ is a shorthand for $p\leqslant q \wedge q\nleqslant p$;[4] $p\geqslant q$ stands for $q\leqslant p$; $\perp$ denotes *incomparability*, i.e., $q \perp p$ iff $q\nleqslant p \wedge p\nleqslant q$; and $\sim$ denotes *equivalent* elements, i.e., $p \sim q$ iff $p\leqslant q \wedge q\leqslant p$. Notice that, even constructively, if $(Q, \leqslant_Q)$ is a qo, then the quotient set $Q/\sim$ with the relation induced by $\leqslant_Q$ is a partial order. We freely use also the concepts introduced in Def. 1.2, with the exception of well-foundedness which, in the next definition, is stated in more suitable way for a constructive context.

[4]The standard definition $p<q := p\leqslant q \wedge p \neq q$ is not appropriate for quasi-orders which are not antisymmetric. One could have $p\leqslant q \wedge q\leqslant p$, although $p \neq q$; obtaining in this case $p<q \wedge q<p$, which is commonly unwanted.

As already mentioned, the weak antisymmetry requirement on extensions ensures that there is a canonical bijection between the linear extensions of Q as a qo and the linear partial orders on $Q/{\sim}$ which contain $\leqslant$. Some of the next definitions regarding well quasi-orders (e.g., wqo(set) or wqo(anti)), are adopted from the context of reverse mathematics, where a thorough analysis of wqo's has already been done [43, 113, 114] (cf. Subsec. 2.1.3).

We consider now the main definitions of a *well quasi-order* findable in literature, namely the ones in Def. 2.2, together with others coming from the foregoing reflections on constructive Noetherianity. Except for the first two ones, which are only about well-foundedness, all of them are equivalent within classical logic [92, Theorem 2.1], see also [77, Lemma 2.4].

Definition 3.7 *A quasi-order* $(Q, \leqslant)$ *is*

1. WELL-FOUNDED, wf, *if, for every descending chain* $q_0 \geqslant q_1 \geqslant \dots$ *in* Q *there are* $i < j$ *such that* $q_i \leqslant q_j$ *and thus* $q_i \sim q_j$;[5] *in this sense every strictly descending chain in* Q *is finite (cf. Def. 3.5);*

2. SEQUENTIALLY WELL-FOUNDED, wf*(set), if every descending chain* $q_1 \geqslant q_2 \geqslant \dots$ *in* Q *has an infinite subsequence of equivalent elements, i.e., there are indices* $k_0 < k_1 < \dots$ *such that* $q_{k_i} \leqslant q_{k_j}$ *and thus* $q_{k_i} \sim q_{k_j}$ *whenever* $i < j$*;*

3. *a* WELL QUASI-ORDER, *wqo, if for every sequence* $(q_k)_k$ *in* Q *there are* $i < j$ *such that* $q_i \leqslant q_j$*;*

4. *a* SEQUENTIALLY WELL QUASI-ORDER, *wqo(set), if every sequence* $(q_k)_k$ *in* Q *has an infinite ascending subsequence, i.e., there are indices* $k_0 < k_1 < \dots$ *such that* $q_{k_i} \leqslant q_{k_j}$ *whenever* $i < j$*;*

5. *an* ANTICHAIN WELL QUASI-ORDER, *wqo(anti), if* Q *is well-founded and if, for every sequence* $(q_k)_k$ *of equal or incomparable elements, there exist* $i < j$ *such that* $q_i = q_j$*; namely every strictly descending chain and every antichain are finite;*

6. *an* EXTENSIONAL WELL QUASI-ORDER, *wqo(ext), if every linear extension* $\preccurlyeq$ *of* $\leqslant$ *is well-founded;*

7. *wqo(fbp) if* Q *has the* FINITE BASIS PROPERTY*, i.e., every closed subset is finitely generated;*

8. *wqo(acc) if the set of closed subsets is Noetherian;*

[5]By transitivity, an equivalent condition is that there is an index i such that $q_i \leqslant q_{i+1}$.

9. *wqo(RS), wqo(ML), wqo(str), wqo(ind), wqo(prc) if the set of finitely generated closed subsets is RS-Noetherian (resp. ML, strong, inductively, processly).*

Remark 3.1

1. *For quasi-orders, we have the following implications:*
   (a) wf*(set) implies* wf*, and* wqo*(set) implies* wqo*;*
   (b) wqo*(set) implies* wf*(set), and* wqo *implies* wf.
2. *Let* $(E, \leqslant)$ *be a* PARTIAL *order,*
   (a) $(E, \leqslant)$ *is well-founded iff* $(E, \geqslant)$ *is RS-Noetherian;*
   (b) $(E, \leqslant)$ *is sequentially well-founded iff* $(E, \geqslant)$ *is Noetherian;*
   (c) $(E, \leqslant)$ *is hereditarily well-founded iff* $(E, \geqslant)$ *is ML-Noetherian.*

At least two of the above definitions are worth some further remarks. By Theorem 3.1, hereditarily well-founded implies well-founded, but not the other way round [25, Example 2]. While wqo(anti) is commonly found as the negative statement "there is no infinite strictly descending chain nor any infinite antichain", here we propose a constructively suitable and to some extent positive version.

Theorem 3.2 *The conditions* wqo*(set),* wf*(set),* wqo*(fbp) and* wqo*(acc) are constructively unprovable already for partial orders.*

Proof Endow $\mathbb{B} = \{0, 1\}$ with the partial order $0 \leqslant 1$. While there is a Brouwerian counterexample to $\mathbb{B}$ being wqo(set) [186], we show that if $\mathbb{B}$ is wf(set), then LPO holds. To this end let $a_0 \geq a_1 \geq \dots$ in $\mathbb{B}$. If there are $k_0 < k_1 < \dots$ such that $a_{k_0} \leqslant a_{k_1} \leqslant \dots$ too, then actually $a_{k_0} = a_{k_1} = \dots$ Now if $a_{k_0} = 1$, then $a_i = 1$ for all i, simply because $i \leqslant k_i$ for every i.

We next show that if $\mathbb{B}$ is wqo(fbp), then the law of excluded middle (LEM) holds. To do so, we carry over from rings to orders the argument that LEM follows from "every ideal of the two-element field $\mathbb{F}_2$ is finitely generated". Let φ be a truth value. We resort to the "fishy set" $F_\phi := \{x \in \mathbb{B} \mid (x = 0 \wedge \phi) \vee x = 1\}$ and suppose that $\uparrow F_\phi = \uparrow\{b_1, \dots, b_n\}$. Now if $b_i = 1$ for all i, then $F_\phi \subseteq \uparrow F_\phi = \uparrow\{1\} = \{1\}$ and thus $0 \notin F_\phi$, which is to say that $\neg\phi$; if $b_i = 0$ for some i, then $0 \in \uparrow F_\phi$, that is, $p \leqslant 0$ for some p in F_ϕ, which means $0 \in F_\phi$ and thus ϕ.[6]

[6]While we generally work in IZF, in CZF we would get LEM only for formulas φ of set theory which are *bounded*: that is, every bound variable x occurring in ϕ ranges over a set as in $\forall x \in y$ and $\exists x \in y$. By this restriction, F_ϕ would be a set also in CZF where the separation axiom scheme is limited to bounded formulas.

Finally, LPO follows from $\mathbb{B}$ being wqo(acc) along the route to LPO from "the two-element field $\mathbb{F}_2$ is Noetherian" [53].[7] □

We now analyse the implications among the constructively sensible conditions: wqo, wqo(anti), wqo(ext), wqo(RS), wqo(ML) and wqo(str); for wqo see, e.g., [162]

Theorem 3.3 *The following implications hold:*

$$\begin{array}{ccc} & & \text{wqo(anti)} \\ & & \nearrow \\ \text{wqo(str)} \rightarrow \text{wqo(ML)} \rightarrow \text{wqo(RS)} \longrightarrow & \text{wqo} & \\ & & \searrow \\ & & \text{wqo(ext)} \end{array}$$

Proof For what concerns the first two implications they are consequence of Theorem 3.1; so let us focus on the last three.

"$\mathsf{wqo}(RS) \Rightarrow \mathsf{wqo}$" Let Q be a qo. For every infinite sequence $q_0, q_1, \dots$ in Q consider the ascending chain of closed subsets $\uparrow\{q_0\} \subseteq \uparrow\{q_0, q_1\} \subseteq \dots$. If Q is wqo(RS), then there is n such that $\uparrow\{q_0, \dots, q_n\} = \uparrow\{q_0, \dots, q_n, q_{n+1}\}$; thus $q_{n+1} \in \uparrow\{q_0, \dots, q_n\}$ and there exists $i \in \{0, \dots, n\}$ such that $q_i \leqslant q_{n+1}$.

"$\mathsf{wqo} \Rightarrow \mathsf{wqo}$(anti)" Notice first that every wqo is well-founded. If $q_0, q_1, \dots$ is an infinite sequence in a wqo Q such that any given q_i and q_j are equal or incomparable, then there are $i < j$ such that $q_i \leqslant q_j$ and thus $q_i = q_j$.

"$\mathsf{wqo} \Rightarrow \mathsf{wqo}$(ext)" Let $(Q, \leqslant)$ be a wqo, and $(Q, \preccurlyeq)$ a linear extension (in fact any extension whatsoever would do [77, Lemma 2.4]). Given any $\preccurlyeq$-descending chain $q_0 \succcurlyeq q_1 \succcurlyeq q_2 \succcurlyeq \dots$, since $\leqslant$ is wqo, there are $i < j$ such that $q_i \leqslant q_j$ and thus $q_i \preccurlyeq q_j$. By transitivity, $q_i \succcurlyeq q_j$; whence $q_i \sim q_j$, i.e., $\preccurlyeq$ is wf. □

Remark 3.2 *There is a certain similarity between the constructive implications and the implications over* RCA$_0$ *which, regarding wqo(set), wqo, wqo(anti) and wqo(ext), are depicted below, where no other implications hold (see Theorem 2.6). Differently from reverse mathematics (where there are counterexamples to each direction), we do not know which relation, if any, holds constructively between wqo(anti) and wqo(ext); the correspondence between* RCA$_0$ *and constructive mathematics may suggest a likewise incomparable situation.*

$$\begin{array}{ccc} & & \mathit{wqo(anti)} \\ & & \nearrow \\ \mathit{wqo(set)} \longrightarrow & \mathit{wqo} & \\ & & \searrow \\ & & \mathit{wqo(ext)} \end{array}$$

[7] Similarly one could consider something like $\mathsf{wqo}(\mathrm{acc}^{\mathrm{fg}})$ or $\mathsf{wqo}(\mathrm{acc}_0)$.

We conclude with a study of the closure properties of wqo's under subsets; for the argument's sake, we include some constructively bland concepts. Given a quasi-/partial order $(Q, \leqslant)$, let every subset $P \subseteq Q$ be endowed with the induced quasi-/partial order, and denote the respective closures with $\uparrow_Q$ and $\uparrow_P$.

Lemma 3.1

1. *Let $(Q, \leqslant)$ be a qo, and $P \subseteq Q$. If $B \subseteq P$, then $\uparrow_P B = P \cap \uparrow_Q B$. In particular, $B_1 \subseteq B_2$ if and only if $\uparrow_Q B_1 \subseteq \uparrow_Q B_2$ for all* CLOSED *subsets B_1, B_2 of P.*

2. *If a partial order $(E, \leqslant)$ is* hwf*, then $(E_0, \leqslant)$ is* hwf *for every subset $E_0 \subseteq E$.*

Proof The first item is straightforward. As for item 2, let $H_0 \subseteq E_0$ be hereditary. Then $H = \{x \in E \,|\, x \in E_0 \Rightarrow x \in H_0\}$ is a hereditary subset of E such that $H_0 = E_0 \Leftrightarrow H = E$. □

Proposition 3.7 *Let $\mathcal{P}$ be any of the properties* wf*,* wf*(set),* wqo*,* wqo*(set),* wqo*(anti),* wqo*(acc),* wqo*(RS),* wqo*(ML),* wqo*(str). If the qo $(Q, \leqslant)$ has property $\mathcal{P}$ and $P \subseteq Q$, then $(P, \leqslant)$ has property $\mathcal{P}$.*

Proof We consider separately each case: While the cases wf, wf(set), wqo, wqo(set) and wqo(anti) are straightforward, the cases wqo(acc) and wqo(RS) follow from Lemma 3.1. As for wqo(ML) and wqo(str), let $\mathcal{F}_P$ and $\mathcal{F}_Q$ consist of the finitely generated closed subsets of P and Q. The map $\mathcal{F}_P \to \mathcal{F}_Q$ with $B \mapsto \uparrow_Q B$ is strictly increasing (Lemma 3.1). In particular, if $\mathcal{F}_Q$ is hwf, then so is $\mathcal{F}_P$ [119, Chapter I, Theorem 6.2]. □

Future work

In Proposition 3.7, we left out wqo(ext) on purpose: this is an open problem just as it is in reverse mathematics over RCA_0 [114, Question 2.15], see also Lemma 2.2. Several other closure conditions equally deserve attention from a constructive angle, e.g., preservation of wqo under products. A deeper analysis would further call for a thorough distinction between a well-order as in Def. 3.5, i.e., a *hereditarily* well-founded linear order, and a well-order in the customary understanding: that is, a linear order which is well-founded in the sense of Def. 3.7. Finally, a few implications related to Def. 3.4 and Theorem 3.1 ought to be considered, as well as the ones regarding our novel wqo definition proposed in Sec. 3.4.

3.3 Inductive Definitions in Constructive Mathematics

Given their crucial role in constructive mathematics, as exemplified by inductive Noetherianity in Def. 3.6 and bar induction in the next section Def. 3.17, we dedicate this section to an exposition regarding inductive definitions and their properties, summarizing the main results present in literature. Firstly we describe, in a classical setting, three main approaches to inductive definitions: *operators*, *rules* and *operations*. Subsequently, we explore to which extent these definitions can fruitfully be applied in constructive frameworks, in particular IZF and CZF, see Def. 3.2 for their axioms. For a general introduction to inductive definitions we refer to [1]; whereas regarding the non trivial problem of constructivity of inductive definitions our main source is [143].

3.3.1 General Inductive Definitions

Starting from the induction principle over $\mathbb{N}$, the recursive construction of terms in first-order logic and generated substructures in algebra, induction and its properties are ubiquitous in mathematics. This abundance reverberates into the many different, yet equivalent, ways to introduce and treat inductive definitions; we consider three of them: operators, rules and operations. For sake of simplicity, here we work in a classical framework (such as ZFC), postponing to the next paragraph the constructive analysis of these definitions.

Monotone Operators

First we consider inductive definitions stemming from *set operators*.

Definition 3.8 *Let M be a set and $\Phi : \mathcal{P}(M) \to \mathcal{P}(M)$ a function, which Φ is called an* OPERATOR. *We say that:*

1. *Φ is* MONOTONE *if $X \subseteq Y \subseteq M$ implies $\Phi(X) \subseteq \Phi(Y)$;*
2. *Φ is* EXPANSIVE *if $X \subseteq M$ implies $X \subseteq \Phi(X)$;*
3. *Φ is* CONTRACTIVE *if $X \subseteq M$ implies $\Phi(X) \subseteq X$;*
4. *$X \subseteq M$ is Φ-*CLOSED *if $\Phi(X) \subseteq X$;*
5. *$X \subseteq M$ is a Φ-*FIXED POINT *if $\Phi(X) = X$.*

Obviously M is Φ-closed, as well as every fixed point of Φ; moreover, if Φ is expansive, then every Φ-closed subset of M is a fixed point of Φ.

Definition 3.9 *Let M be a set and $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ a monotone operator; we say that the subset*

$$I(\Phi) := \bigcap \{X \in \mathcal{P}(M) \mid \Phi(X) \subseteq X\},$$

i.e. the intersection of all Φ-closed subsets of M, is INDUCTIVELY DEFINED *by Φ.*

The following results highlight some crucial properties of $I(\Phi)$.

Theorem 3.4 *$I(\Phi)$ is the least Φ-closed subset of M.*

Proof Let $\mathcal{C} = \{X \in \mathcal{P}(M) \mid \Phi(X) \subseteq X\}$ and $I_\Phi = I(\Phi)$, so $I_\Phi = \bigcap \mathcal{C} = \bigcap_{X \in \mathcal{C}} X$. For every $X \in \mathcal{C}$, we thus have $I_\Phi \subseteq X$; in particular $\Phi(I_\Phi) \subseteq \Phi(X) \subseteq X$ as Φ is monotone. Hence $\Phi(I_\Phi) \subseteq \bigcap_{X \in \mathcal{C}} X = I_\Phi$, so $I_\Phi \in \mathcal{C}$. Clearly $I_\Phi \subseteq X$ for every $X \in \mathcal{C}$. □

Corollary 3.1 *$I(\Phi)$ is the least fixed point of Φ.*

Proof Again let $I_\Phi = I(\Phi)$; from $\Phi(I_\Phi) \subseteq I_\Phi$ we get $\Phi(\Phi(I_\Phi)) \subseteq \Phi(I_\Phi)$ by monotonicity of Φ, so $\Phi(I_\Phi)$ is Φ-closed and thus $I_\Phi \subseteq \Phi(I_\Phi)$. In all, $\Phi(I_\Phi) = I_\Phi$. □

Remark 3.3 *As $I(\Phi) \in \mathcal{C} = \{X \in \mathcal{P}(M) \mid \Phi(X) \subseteq X\}$, and thus $I(\Phi)$ is one of the $X \in \mathcal{C}$ which are used for the very definition of $I(\Phi)$ as $\bigcap_{X \in \mathcal{C}} X$, the definition of $I(\Phi)$ is* IMPREDICATIVE *inasmuch it is* CIRCULAR *(the definiendum occurs in its own definiens).*

Despite its impredicativity, Def. 3.9 allows for the following inductive principle.

Corollary 3.2 *(Φ-induction) Let $P(x)$ be a property of $x \in M$. If $\{x \in M \mid P(x)\}$ is Φ-closed, then* EVERY *$x \in I(\Phi)$ has the property $P(x)$, i.e. $\forall x \in I(\Phi)\, P(x)$.*

Proof Set $X_P = \{x \in M \mid P(x)\}$. If X_P is Φ-closed, then $I(\Phi) \subseteq X_P$ by Theorem 3.4, i.e. $\forall x \in I(\Phi)\, P(x)$. □

We can give a slight improvement of this last result, in which, for sake of readability, $I(\Phi)$ is again denoted by I_Φ.

Corollary 3.3 *Let $M, \mathcal{P}(M), \Phi$ as before. For every $X \in \mathcal{P}(M)$, if $\Phi(I_\Phi \cap X) \subseteq X$, then $I_\Phi \subseteq X$.*

Proof As $I_\Phi \cap X \subseteq I_\Phi$ and Φ is monotone, we have $\Phi(I_\Phi \cap X) \subseteq \Phi(I_\Phi)$. By Theorem 3.4, $\Phi(I_\Phi) \subseteq I_\Phi$ and so $\Phi(I_\Phi \cap X) \subseteq I_\Phi$. Hence, if $\Phi(I_\Phi \cap X) \subseteq X$, then $\Phi(I_\Phi \cap X) \subseteq I_\Phi \cap X$, i.e. $I_\Phi \cap X$ is Φ-closed and thus, again by Theorem 3.4, $I_\Phi \subseteq I_\Phi \cap X \subseteq X$ as required. □

In other words, to get $P(x)$ for every $x \in I_\Phi$ as in Corollary 3.2, it is enough to verify $\Phi(I_\Phi \cap X_P) \subseteq X_P$ rather than $\Phi(X_P) \subseteq X_P$.

Example 3.3.1 *For an example of an inductive definition according to Def. 3.9, let us consider the linear subspace generated by a subset of a vector space. Let M be a vector space over the field K and let $N \subseteq M$. Define $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ by setting*

$$\Phi(X) := \{0\} \cup N \cup \{x + y \mid x, y \in X\} \cup \{\lambda x \mid x \in X, \lambda \in K\}.$$

For every $X \in \mathcal{P}(M)$, we have $\Phi(X) \subseteq X$ precisely when $N \subseteq X$ and X is a linear subspace of M, that is $0 \in X$, $x, y \in X \Rightarrow x + y \in X$ and $x \in X, \lambda \in X \Rightarrow \lambda x \in X$. Hence the inductively defined subset $I(\Phi)$ of M is nothing but the linear span of N in M, for short span(N), i.e. the least linear subspace of M containing N.

Remark 3.4 *One can avoid this impredicative definition by defining span(N) as the set of linear combinations stemming from N, that is*

$$\mathit{span}(N) := \left\{ \sum_{i=0}^{n} \lambda_i x_i \mid n \geqslant 0, \lambda_1, \ldots, \lambda_n \in K, x_1, \ldots, x_n \in N \right\}.$$

Before moving to induction by rules, we present an alternative definition, exploiting ordinals, for the set inductively generated by a set operator, which is suitable also for non-monotone operators. Let $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ be an operator on M, not necessarily monotone, we define $\Phi^\lambda \subseteq M$ by transfinite recursion on the ordinal λ as follows:

$$\Phi^\lambda := \bigcup_{\mu<\lambda} \Phi^\mu \,\cup\, \Phi\left(\bigcup_{\mu<\lambda} \Phi^\mu \right),$$

finally, we put $\Phi^\infty := \bigcup_\lambda \Phi^\lambda$ where λ ranges over all ordinals.

For Φ monotone we regain the set inductively defined from Φ.

Proposition 3.8 *Let M a set and $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ a monotone operator, then $I(\Phi) = \Phi^\infty$.*

Proof [1, Proposition 1.3.1]. □

Based on this property, and the fact that the definition of Φ^∞ does not require monotonicity, we call Φ^∞ the *set inductively generated from* Φ even for a non-monotone operator. From this definition, a fruitful theory of non-monotone inductive definitions can be developed, see [137, Chapter 13].

Rules

Another approach to induction, commonly found in formal logic, is given by *rules.*

Definition 3.10

1. *A* RULE *is a pair* (X, x) *where* X *is a set, called the set of* PREMISES*, and* x *is the* CONCLUSION*; the rule* (X, x) *will be denoted by* $X \to x$.[8]

2. *If* Φ *is a set of rules, also called a* RULE SET*, then a set* A *is* Φ-CLOSED *if each rule in* Φ *whose premisses are in* A *also has its conclusion in* A*. We write* $\Phi\colon X \to x$ *to denote that the rule* $X \to x$ *is in* Φ*, then* A *is* Φ*-closed if* $X \subseteq A$ *and* $\Phi\colon X \to x$ *imply* $x \in A$.

3. *A rule set* Φ *is* FINITARY *if each rule* $\Phi : X \to x$ *has a finite set* X *of premisses.*

4. *If* Φ *is a rule set, then* $I(\Phi)$*, the* SET INDUCTIVELY DEFINED BY Φ*, is given by* $I(\Phi) := \bigcap\{A \mid A \text{ is } \Phi\text{-closed}\}$.

Example 3.3.2 *An insightful example of induction by rules is given by the set of theorems deductible in a formal system. If we consider a formal system* H *à la Hilbert, we operate on the set of well-formulated formulas, which again can be inductively defined from atomic formulas and logic connectives (and quantifiers for the first-order version). We have then two types of rules: axioms, which can be seen as rules without premisses, i.e. pure introductory rules such as* $\emptyset \to \varphi \vee \neg\varphi$ *for an instance of LEM, and applications of modus ponens where the set of premisses has the form* $X = \{\varphi, \varphi \to \psi\}$[9] *and the conclusion* x *amounts to the formula* ψ*. From the formal system* H*, we thus obtain a rule set* Φ_H *given by the rule versions of axioms and modus ponens, and the deductive closure of theorems deducible in* H *is nothing but* $I(\Phi_H)$.

Remark 3.5 *Whereas* Φ_H *in the previous example is a finitary rule set (every rule has zero or two premisses), we observe how, using infinitary rule sets, also infinitary deduction systems, e.g. one including the* ω*-rule [97], can be formalized in the previous setting.*

For a finitary rule set Φ, we can generalize the standard concept of "proof" for formal systems, such as H in the previous example.

Definition 3.11 $a_0, \ldots, a_n$ *is a* Φ*-proof of* b *if:*

1. $a_n = b$,

2. *for all* $m \leqslant n$ *there exists* $X \subseteq \{a_i \mid i < m\}$ *such that* $\Phi\colon X \to a_m$.

---

[8] Other notations are possible, such as $\frac{X}{x}$ used in [143].

[9] We warn the reader not to mistake the syntactic arrow of $\phi \to \psi$, with the notational arrow $X \to x$ of a rule; although from a conceptual point of view they are clearly related.

Proposition 3.9 *For a finitary rule set* Φ*,*

$$I(\Phi) = \{b \mid b \text{ has a } \Phi\text{-proof}\}.$$

Proof See [1, Proposition 1.1.4.]. □

Remark 3.6 *The two approaches previously exposed, operators and rules, are actually equivalent. Namely given a monotone operator* $\Phi_{op}\colon \mathcal{P}(M) \to \mathcal{P}(M)$ *there is the rule set* $\bar{\Phi}_{op}$

$$\bar{\Phi}_{op} := \{X \to x \mid X \subseteq M \text{ and } x \in \Phi_{op}(X)\}$$

for which $I(\Phi_{op}) = I(\bar{\Phi}_{op})$*. Viceversa, given a rule set* Φ_r *on* M *(i.e. such that* $X \cup \{x\} \subseteq M$ *for every rule* $\Phi : X \to x$*), we can define a monotone operator* $\tilde{\Phi}_r\colon \mathcal{P}(M) \to \mathcal{P}(M)$ *by*

$$\tilde{\Phi}_r(Y) := \{x \in M \mid \Phi_r\colon X \to x \text{ for some } X \subseteq Y\},$$

for which again $I(\Phi_r) = I(\tilde{\Phi}_r)$*. Moreover, the two operations are each the inverse of the other, namely* $\tilde{\bar{\Phi}}_{op} = \Phi_{op}$ *and* $\bar{\tilde{\Phi}}_r = \Phi_r$*.*

Monotone operators, in particular the ordinal version, allow to define "formal proof" also for infinitary rule sets using transfinite sequences [1, Definition 1.4.1.]; although even trees can be used to formalize infinitary proof, see definition 1.4.3. and 1.4.4. in [1].

Operations

In the case of finitary rules, there is another way to express and treat induction: *partial operations* over an algebra.

Definition 3.12 *A (partial)* ALGEBRA (M, O) *à la Birkhoff* [10] *is given by:*

- *a carrier set* M*;*
- *a set* $O = \bigcup_{n \geqslant 0} O_n$ *of (partial) operations, for each* $n \geqslant 0$ *the set* O_n *consists of the* n*-ary (partial) operations on* M*, i.e. (partial) maps* $M^n \to M$*.*

In the case $n = 0$, we have $M^0 = \{\varepsilon\}$ for the empty list ε; by identifying $\varphi \in O_0$ with $\varphi(\varepsilon) \in M$, the nullary operations in O_0 correspond to certain elements of M, called the *distinguished elements* of M.

[10] Cf. with Def. 2.11.

The connection between finitary rules and partial operators should be apparent, the finitary rule $\varphi\colon \{x_1,\ldots,x_n\} \to x$ on M corresponds to the partial operation $\varphi\colon M^n \to M$, $\varphi(x_1,\ldots,x_n) = x$.

Over (M, O), we may consider also the following set operator

$$\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M),\ X \mapsto \bigcup_{n\geqslant 0} \bigcup_{\varphi\in O_n} \varphi\left(X^n\right),$$

for $n = 0$, we have $X^0 = \{\varepsilon\}$ and $\varphi(X^0) = O_0$.

This operator is monotone, and $\Phi(X) \subseteq X$ if and only if X is *closed* under every $\varphi \in O_n$ for every $n\geqslant 0$: that is $\varphi(X^n) \subseteq X$ or, more explicitly, $x_1,\ldots,x_n \in X$ implies $\varphi(x_1,\ldots,x_n) \in M$; in particular, if $\Phi(X) \subseteq X$, then X contains all the distinguished elements of M. Thus, the Φ-closed sets $X \subseteq M$ are the (partial) *subalgebras* of (M, O), i.e. the $X \subseteq M$ to which the (partial) operations can be restricted, and $I(\Phi)$ is the *least* subalgebra of (M, O). By redefining O_0 as $O_0 \cup N$ for any given $N \subseteq M$ and dubbing Φ_N the corresponding operator, one achieves $N \subseteq X$ for every Φ_N-closed set $X \subseteq M$, whence $I(\Phi_N)$ is the (partial) *subalgebra generated* by N.

Example 3.3.3 *If $(M, e, \circ)$ is a group and $N \subseteq M$, then we set $O = O_0 \cup O_1 \cup O_2$ with $O_0 = \{e\} \cup N$, $O_1 = \{\rho\}$ and $O_2 = \{\mu\}$ where $\rho(x) := x^{-1}$ and $\mu(x, y) := x \circ y$. In this case, $I(\Phi)$ is the subgroup of M generated by N. Alternatively we may set $O = O_0 \cup O_2$ with again $O_0 = \{e\} \cup N$ and $O_2 = \{\eta\}$ where $\eta(x, y) := x^{-1} \circ y$; also, $O_0 = N$ suffices whenever N has any element at all. If we instead set $O_1 = \{\rho\} \cup \{\gamma_z \mid z \in M\}$ where $\gamma_z(x) := z^{-1} \circ x \circ z$, then $I(\Phi)$ is the normal subgroup generated by N, also called normal closure of N in M.*

3.3.2 General Inductive Definitions, Constructively

In the previous paragraph, we have reasoned in classical logic; now instead we address the following problem: given an inductive definition Φ, stemming from an operator or some rules, when is $I(\Phi)$ a set even in constructive mathematics?

We consider this problem in the two main constructive frameworks in set theory: IZF, Intuitionistic Zermelo Fraenkel, and CZF, Constructive Zermelo Fraenkel (see Def. 3.2). Here we briefly recall that, whereas IZF has both Powerset and full Separation axioms, i.e. $\mathcal{P}(a)$ and $\{x\in a \mid \phi(a)\}$ are sets for every set a and every formula ϕ, CZF has only Bounded Separation; namely $\{x\in a \mid \phi(a)\}$ is a set only if a is a set and ϕ is a bounded formula (i.e. all quantifiers have the form $\forall x\in z$ or $\exists x\in z$ with z a set).

Since $I(\Phi)$ is strictly connected with the intersection of a family of sets, we start with the following question: given a class C, when is $\bigcap C = \{x \mid \forall y\in C\,(x\in y)\}$ a set in constructive mathematics?

If C has an element z, then $\bigcap C = \{x \in z \mid \varphi(x)\}$ with $\varphi(x) \equiv \forall y \in C\,(x \in y)$; whence if C is inhabited, then $\bigcap C$ is a set:

- in IZF always by Full Separation;
- in CZF by Bounded Separation whenever C is a set in which case φ is bounded.

What if $C = \{y \in D \mid P(y)\}$ for a class D and a formula P? In this case $\bigcap C = \{x \in \bigcup D \mid \forall y \in D\,(P(y) \to x \in y)\}$ and, if $z \in C$, we obtain as before $\bigcap C = \{x \in z \mid \varphi(x)\}$ with $\varphi(x) \equiv \forall y \in D\,(P(y) \to x \in y)$; moreover, φ is bounded if and only if D is a set and P is bounded.

We can apply these findings to the inductive case. Let M be a set and $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ a monotone operator and take $\mathcal{P}(M)$ as D, which is a set in IZF but not in general in CZF. Let $P(y)$ be "y is Φ-closed", which in concrete cases may well be bounded. In any case, not only $M \in D$, but also $M \in C$. So $I(\Phi)$ always is a set in IZF, but not in general in CZF even when "y is Φ-closed" is bounded.

It is no surprise that $I(\Phi)$ is not in general a set in CZF; in fact, CZF does not have the Powerset axiom and only has the axiom schema of Bounded Separation, differently from IZF which has both Powerset and Full Separation. Moreover, CZF is a predicative inasmuch as it is tied together, [2, 3, 4], with Martin-Löf Type Theory; and IZF is impredicative inasmuch as it tolerates circular definitions in which the definiendum occurs within the definiens.

Despite previous considerations, for some classes of inductive definitions $I(\Phi)$ is a set even in CZF; one of such classes is given by continuous operators. We recall that $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ is *continuous* if $\Phi\left(\bigcup_{i\in I} X_i\right) = \bigcup_{i\in I} \Phi\left(X_i\right)$ for every directed family $(X_i)_{i\in I}$ in $\mathcal{P}(M)$; moreover, we observe how the inclusion $\supseteq$ in the previous equality is equivalent to Φ monotone, i.e. $X \subseteq Y \subseteq M \Rightarrow \Phi(X) \subseteq \Phi(Y)$. The following construction is due to Kleene for the least fixed point of a continuous endomorphism of a dcpo (directed-complete partial order[11]), as e.g. in [175, Theorem 3.7].

Theorem 3.5 *(CZF) If M is a set and $\Phi : \mathcal{P}(M) \to \mathcal{P}(M)$ is a continuous operator, then $I(\Phi)$ is a set.*

Proof Let $I_\Phi^0 = \emptyset, I_\Phi^{k+1} = \Phi\left(I_\Phi^k\right), I_\Phi^\infty = \bigcup_{k\geqslant 0} I_\Phi^k$ and denote $I(\Phi)$ by I_Φ; we prove $I_\Phi = I_\Phi^\infty$. By induction on k (and the axiom scheme of replacement) I_Φ^k is a set for every k. (If A is a set and B, F are classes such that $F\colon A \to B$ is a function, then $F(A)$ is a set by replacement.) Again by replacement, $I_\Phi^\infty = \bigcup\{I_\Phi^k \mid k \in \mathbb{N}\}$ is a set, so $I_\Phi^\infty \in \mathcal{P}(M)$. Moreover, we obtain $I_\Phi^\infty = I_\Phi$ proving the double inclusion:

[11] A po $(P, \leqslant)$ is a dcpo if every directed subset has a supremum, where a subset S is *directed* if it is inhabited and every pair of elements in S has an upper bound in S.

$\supseteq$ by Corollary 3.1 and $\Phi(I_\Phi^\infty) = I_\Phi^\infty$; the latter equality follows from the fact that $I_\Phi^0 \subseteq I_\Phi^1 \subseteq \ldots$ is a chain, whence by continuity

$$\Phi(I_\Phi^\infty) = \Phi\left(\bigcup_{k\geqslant 0} I_\Phi^k\right) = \bigcup_{k\geqslant 0} \Phi\left(I_\Phi^k\right) = \bigcup_{k\in\mathbb{N}} I_\Phi^{k+1} = I_\Phi^\infty .$$

$\subseteq$ for this direction, we show by induction on k that $I_\Phi^k \subseteq X$ for any Φ-closed subset X and every $k \geqslant 0$. Namely, for $k = 0$ we have $\emptyset \subseteq X$; for the inductive step, from $I_\Phi^k \subseteq X$, we obtain $I_\Phi^{k+1} = \Phi(I_\Phi^k) \subseteq \Phi(X) \subseteq X$. □

Note that we have not really made use of the specific form of $\mathcal{P}(M)$; the whole treatment could perhaps be generalized to other classes, even the universal class V. For a recent result regarding constructive inductive definitions over poset, more precisely a constructive version of Tarski's fixed point theorem, we refer to [54].

In the case of closure under operations, the construction of $I(\Phi)$ following Theorem 3.5 yields the description well-known, e.g. in universal algebra [46, Lemma 5.1], of a generated subalgebra as the result of nested applications of the operations starting from the generators. To be more precise, let (M, O) be a (partial) algebra, and let $\Phi\colon \mathcal{P}(M) \to \mathcal{P}(M)$ denote the related monotone operator as before, i.e. $\Phi(X) = \bigcup_{n\geqslant 0} \bigcup_{\varphi\in O_n} \varphi(X^n)$. This operator is even continuous. In fact, if $(X_i)_{i\in I}$ is a directed family in $\mathcal{P}(M)$, then $\left(\bigcup_{i\in I} X_i\right)^n \subseteq \bigcup_{i\in I} X_i^n$ (for $(x_{i_1}, \ldots x_{i_n})$ with $x_{i_l} \in X_{i_l}$ pick $i_0 \in I$ such that $X_{i_0} \cup \cdots \cup X_{i_n} \subseteq X_{i_0}^n$ and thus $(x_{i_1}, \ldots, x_{i_n}) \in X_{i_0}^n$); whence

$$\Phi\left(\bigcup_{i\in I} X_i\right) = \bigcup_{n\geqslant 0} \bigcup_{\varphi\in O_n} \varphi\left(\left(\bigcup_{i\in I} X_i\right)^n\right) \subseteq \bigcup_{n\geqslant 0} \bigcup_{\varphi\in O_n} \bigcup_{i\in I} \varphi(X_i^n) = \bigcup_{i\in I} \Phi(X_i) .$$

Note that for this argument every φ needs to have finite arity n. Then $I_\Phi^0 = \emptyset$ and $I_\Phi^{k+1} = \{\varphi(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in I_\Phi^k, \varphi \in O_n, n \geqslant 0\}$. Hence I_Φ^∞ is the least subalgebra, i.e. the one generated by $\emptyset$; whereas, if $N \subseteq M$ is added to O_0, then I_Φ^∞ is the subalgebra generated by N, as $O_0 \subseteq I_\Phi^k$ for $k \geqslant 1$.

Although we did find a good class of inductive definitions for which $I(\Phi)$ is a set also in CZF, the question regarding the general conditions under which this happens remains. The problem was addressed by Rathjen in [143] and we briefly expose his findings. Let Φ be a *rule class*, i.e. a class of pairs (X, x) written as $X \to x$; the definitions of being Φ-closed and of $I(\Phi)$ can be easily extended to the class case. Obviously, $I(\Phi)$ will always be a class, but not necessarily a set. For any class A, let

$$\Gamma_\Phi(A) := \{x \mid \exists X (X \subseteq A \wedge \Phi\colon X \to x)\}.$$

Thus $\Gamma_\Phi(A)$ consists of all conclusions that can be drawn from a set of premisses comprised by A and using a single Φ-inference step. Given Γ_Φ, we could redefine

A to be Φ-closed as $\Gamma_\Phi(A) \subseteq A$. To obtain a thorough analysis of constructive inductive definitions, we need to add to CZF another axiom, namely the *Weakly Regular Extension Axiom*, first proposed by Aczel [4].

Definition 3.13 *An inhabited set A is* WEAKLY REGULAR *if A is transitive, i.e. $x \in a \in A$ implies $x \in A$, and for every $a \in A$ and every set $R \subseteq a \times A$, if $\forall x \in a\, \exists y\, (x, y) \in R$, then there is a set $b \in A$ such that $\forall x \in a\, \exists y \in b\, (x, y) \in R$. We write $\boldsymbol{wReg}(C)$ to denote that C is weakly regular. $\boldsymbol{wREA}$ is the axiom*

$$\forall x\, \exists y\, (x \subseteq y \wedge \boldsymbol{wReg}(y)).$$

Definition 3.14

1. *We call a rule class Φ* LOCAL *if $\Gamma_\Phi(X)$ is a set for all sets X.*
2. *We define a class B to be a* BOUND *for Φ if whenever $\Phi\colon X \to x$, then X is an image of a set $b \in B$; i.e., there is a function from b onto X.*
3. *We define Φ to be* (WEAKLY REGULAR) BOUNDED *if:*
   (a) *$\{y \mid \Phi\colon X \to y\}$ is a set for all sets X,*
   (b) *Φ has a bound that is a (weakly regular) set.*

We may now state the following results.

Proposition 3.10 *(CZF)*

1. *Every bounded rule class Φ is local;*
2. *If Φ is weakly regular bounded then $I(\Phi)$ is a set.*

Proof [5] Propositions 8.6 and 8.7. □

Theorem 3.6 *(CZF + $\boldsymbol{wREA}$) If Φ is bounded, then $I(\Phi)$ is a set.*

Proof [4, Theorem 5.2]. □

For further readings on the topics of this section, we refer to [1, 4, 5, 143], to [137], in particular Chapters 6 and 13, and the references therein.

3.4 A Constructive Version of Higman's Lemma for Bars

In this section, based on a joint article with Stefano Berardi and Peter Schuster [19], we enrich the collection of constructive versions of Higman's lemma; more precisely, we aim to a constructive form of Higman's lemma for bars.

Classically, a bar B for lists is a set of finite lists such that every infinite chain of one-step extensions meets B, i.e. has an element in B. Within intuitionistic logic we need and have a more perspicuous definition of bar (see Def. 3.17). Higman's lemma for bars now says: "for every bar B, every infinite sequence σ of words on a finite alphabet Σ has an infinite subsequence τ with a weakly increasing prefix τ_0 in B". Here we interpret $\tau_0 \in B$ as that τ_0 is "long enough for our purposes", with "our purposes" expressed by the choice of B.

E.g. if B is the set of lists of length 2 or more, then Higman's lemma for bars entails that every infinite sequence σ of words on Σ has an infinite subsequence τ with a weakly increasing prefix τ_0 in B, i.e. of two or more elements. This is the first of the desired consequences of Higman's lemma, all of which can be deduced from Higman's lemma for bars.

We will prove Higman's lemma for bars with intuitionistic logic. In fact, we prove a stronger version in which the requirement "σ is infinite" is replaced by one about the bar B. During our proof, we are able to constructively interpret several non-constructive classical theorems of the following form: for every sequence f there is an infinite sequence g such that $P(f, g)$. Higman's lemma for sequences is of course a typical case.

For instance, we rephrase the notion of wqo, the main ingredient of the classical proof of Higman's lemma, by quantification on bars and call "wqo(bar)" this novel notion of wqo. We have short proofs with intuitionistic logic that the concept wqo(bar) is closed by unions (provided that the union is a preorder), by products and by right-invertible morphisms; these are all properties of wqo typically occurring in a classical proof of Higman's lemma. With the notion of wqo(bar) at hand, we consider possible to develop a constructive version of the theory of wqo close to the classical one.

3.4.1 Higman's Lemma in Constructive Mathematics

The theory of well quasi-orders has found applications in many different fields, and so has Higman's lemma, one of this theory's milestones. Given the concrete character of Higman's lemma especially in the case of a finite alphabet, and its applicability in computer science, the search for a constructive and more perspicuous proof has started very early: not only to make possible program extraction from proofs, but also for a better understanding both of the original non-constructive proof of Higman's lemma and the short and elegant but still non-constructive proof by Nash-William [122]. To position the results of this section in the literature, we now briefly survey the existing constructive approaches to Higman's lemma and related results such as Kruskal's theorem. For an historical survey of well quasi-order broadly understood we refer to [107].

The presumably first constructive proof of Higman's lemma was obtained by Murthy and Russell [121] using a smart manipulation of finite strings. Richman and Stolzenberg [155] then proved Higman's lemma by induction on subsets. Coquand and Fridlender [48] instead used structural induction over inductive definitions; their results were extended by Seisenberger [162]. Fridlender [72] gave a type-theoretic version of Higman's lemma, and Veldman [186] an inductive intuitionistic proof. Worthy of mention is Berger's constructive proof [21] of the equivalence between Dickson's lemma and Higman's lemma for a two-element alphabet.

The connection between Higman's lemma and programs has been addressed several times. Schwichtenberg, Seisenberger, and Wiesnet [160] analyzed the computational content of Higman's lemma. Powell has successfully applied Gödel's Dialectica interpretation to well quasi-orders [140] and Higman's lemma [139]. Concerning computer-assisted theorem proving, Berghofer [23], has formalized a constructive proof of Higman's lemma in Isabelle, starting from the article by Coquand and Fridlender; more recently, Sternagel [172] used open induction to obtain a proof in Isabelle/HOL [125].

Finally, also Kruskal's theorem [106], the natural extension of Higman's lemma from strings to finite trees, has been put under constructive scrutiny by Veldman [186] and Seisenberger [163], whereas Goubault-Larrecq [87] gave a topological constructive version of Kruskal's theorem.

3.4.2 Lists, Words and Sequences

We start by recalling some well-known terminology about lists, sublists and labels, as well as notions related to alphabets and words.

Let $\mathbb{N}$ be the set of natural numbers and I any set. We call a *list* l on I any map l such that $l\colon [0,n[\to I$ for some $n \in \mathbb{N}$ or $l\colon \mathbb{N} \to I$. We set $\texttt{dom}(l) = [0,n[$, $\texttt{range}(l) = l([0,n[)$ in the first case and $\texttt{dom}(l) = \mathbb{N}$, $\texttt{range}(l) = l(\mathbb{N})$ in the second case; moreover, we call $\texttt{dom}(l)$ the set of indexes of l and $\texttt{range}(l)$ the set of elements of l, abbreviating $i \in \texttt{range}(l)$ with $i \in l$. The *length* of l, denoted $\texttt{len}(l)$, is $n \in \mathbb{N}$ in the first case and is ∞ (infinite) in the second case; in the first case we say that the list l is finite and in the second case that l is infinite. We call each $x \in \texttt{range}(l)$ an *element* of l and write $\texttt{Fin}(I)$ for the set of finite lists on I, $\texttt{Inf}(I)$ for the set of infinite lists, and $\texttt{List}(I) = \texttt{Fin}(I) \cup \texttt{Inf}(I)$ for the set of all lists on I.

We write a finite list $l \in \texttt{Fin}(I)$ of length $n = \texttt{len}(l)$ as $\langle l(0), \ldots, l(n-1)\rangle$, denoting with $\mathtt{Nil} = \langle\rangle$ the empty list, the unique list of length 0. For $l, m \in \mathtt{List}(I)$, we write $l \sqsubseteq m$, or "l is a sublist of m" for: there is a finite increasing list $f\colon [0, \mathtt{len}(l)[\to [0, \mathtt{len}(m)[$ of natural numbers such that $l(i) = m(f(i))$ for all $i \in [0, \mathtt{len}(a)[$; we call such an f an *embedding* of l in m. For instance, if I is the English alphabet, if $l = \langle w, o, r, d\rangle$, represents the word "word", and $m = \langle w, o, r, l, d\rangle$, represents the word "world", then $l \sqsubseteq m$. An embedding of l in m is $f : [0, 4[\to [0, 5[$ defined by $f(0) = 0, f(1) = 1$, $f(2) = 2$ and $f(3) = 4$. $\mathtt{range}(f)$ does not include 3, the index of the symbol "l" in "world". Another example: $l : \mathbb{N} \to \mathbb{N}$ defined by $l(i) = 2i$ is the list of all even numbers, $h : \mathbb{N} \to \mathbb{N}$ defined by $h(i) = i$ is the list of all natural numbers, and $f(i) = 2i$ is an embedding from l to h. Roughly speaking, we have $l \sqsubseteq h$ if and only if we can obtain l by skipping zero or more elements from h, without changing the order of the elements of h.

If X is a set and R a binary relation between I and J, the *R-upward cone* of X, denoted $R(X)$, is the set of $y \in J$ such that $\exists x \in X\, R(x, y)$; often abbreviating "upward cone" with "cone". If $x \in I$, we write $R(x)$ for $R(\{x\})$, and we call $R(x)$ the R-cone of x in J; moreover, we call $J \setminus R(x)$ the *anticone* of x in J: it is the cone of x with respect to the complement in $I \times J$ of the relation R.

We write $\sqsubseteq_{I,J}$ for the binary relation $\{(l, m) \in \mathtt{Fin}(I) \times \mathtt{Fin}(J) \mid l \sqsubseteq m\}$ defined by the sublist predicate restricted to $\mathtt{Fin}(I) \times \mathtt{Fin}(J)$ and we write $\sqsubseteq_I$ for $\sqsubseteq_{I,I}$ and $\sqsupseteq_{I,J}$ for the inverse binary relation $\{(l, m) \in \mathtt{Fin}(I) \times \mathtt{Fin}(J) \mid l \sqsupseteq m\}$

For any $i \in \mathbb{N}$, we define the restriction $l\lceil i \in \mathtt{Fin}(I)$ of l to $[0, i[$ by $(l\lceil i)(j) = l(j)$ for all $j < \mathtt{len}(l), j < i$ and $\mathtt{len}(l\lceil i) = \min(\mathtt{len}(l), i)$. When l is a restriction of some (possibly infinite) list m, then we say that l is a *prefix* of m and we write $l \leqslant m$.

We define the *concatenation* $m = l\star l'$ of two lists l, l' with l finite by: $m(i) = l(i)$ for all $i < \mathtt{len}(l)$ and $m(\mathtt{len}(l)+j) = l'(j)$ for all $j < \mathtt{len}(l')$. By definition we have $\langle l(0), \ldots, l(n-1)\rangle\star\langle l'(0), \ldots, l'(m-1), \ldots\rangle = \langle l(0), \ldots, l(n-1), l'(0), \ldots, l'(n'-1), \ldots\rangle$. The length of m is $\mathtt{len}(l) + \mathtt{len}(l')$ if l' is finite and ∞ if l' is infinite. If $m = l\star l'$ for some $l, l' \in \mathtt{Fin}(I)$, then we say that l' is a *suffix* of m.

Given $l, m \in \mathtt{Fin}(I)$, we write $l <_1 m$ if $m = l\star\langle i\rangle$ for some $i \in I$, i.e. m is obtained by adding the element i to the end of l. We write $<$ for the transitive closure of the relation $<_1$, observing that the prefix relation $\leqslant$ is the reflexive closure of $<$.

A finite alphabet Σ is any finite set Σ in bijection with $[0, n[$ for some natural number n and through some map f. Equality on Σ is provably decidable with intuitionistic logic, because $i = j$ in Σ if and only if $f(i) = f(j)$ in $\mathbb{N}$. We call the elements of Σ "symbols" of the language, and we denote them with the letters a, b, c and their variants, $a', a_1, \ldots$; the basic example is $\Sigma = \{0, 1\}$. A word on Σ is any finite list on Σ and we write $\Sigma^* = \mathtt{Fin}(\Sigma)$ for the set of words on Σ. We use `nil` for the empty word in Σ^*, this is just another name for $\texttt{Nil} = \langle\rangle$, and we denote words with the letters v, w, z and their variants, $v', v_1, \ldots$; moreover, with a slight and harmless abuse of notation, we use the expression $c \in w$ and $c \notin w$ to denote respectively that c is, or is not, one of the letters of w. If $v, w \in \Sigma^*$, when $v \sqsubseteq w$ we say that v is a *subword* of w and w a *superword* of v.

The following abbreviations are used only for words: if $c_1, \ldots, c_n \in \Sigma$, we denotes the word $w = \langle c_1, \ldots, c_n\rangle$ with $w = c_1 \ldots c_n$, written without spaces; if $v, w \in \Sigma^*$, the juxtaposition vw stands for the concatenation $v \star w$; if $c \in \Sigma$ and $w \in \Sigma^*$, we abbreviate $\langle c\rangle \star w$ with cw, and $w \star \langle c\rangle$ with wc.

We call a *sequence* of words in Σ, just a sequence for short, any list in Σ^*. A sequence is finite if it is a finite list, it is infinite if it is an infinite list. Within this terminology, $\texttt{Fin}(\Sigma^*)$ and $\texttt{Inf}(\Sigma^*)$ are the set of finite and infinite sequences in Σ^*. Finally, we adopt the following notation rule: finite sequences are denoted by Latin letters, whereas infinite sequences by Greek letters.

We characterize now the words which are superwords of a given word and those which are not. Let us fix any $v \in \Sigma^*$. We recall that $\not\sqsubseteq_\Sigma(v)$ denotes the anticone of v, which is the set of all $w \in \Sigma^*$ such that $v \not\sqsubseteq w$. The first step in our proof of Higman's lemma is to characterize the words in the anticone of v. To this aim, we need one preliminary step: we introduce a smaller set of words $\texttt{Slice}_\Sigma(v) \subseteq \Sigma^*$, dubbed the *slice* of v, consisting of all words $w \in \Sigma^*$ for which v is minimal among the words not embeddable in w.

Definition 3.15 (Slice of v) *For each word $v \in \Sigma^*$ we define $\texttt{Slice}_\Sigma(v)$ as the set of words in Σ^* which are superwords of all $v' < v$, but are not superwords of v.*

We characterize the words in $\texttt{Slice}_\Sigma(v)$. We have $\texttt{Slice}_\Sigma(\texttt{nil}) = \emptyset$, because all words are superlists of `nil`. Assume that $v = c_0 \ldots c_{k-1}$ is not empty, that is, that $k \geqslant 1$, then by definition unfolding we have:

$$\texttt{Slice}_\Sigma(v) = \{w \in \Sigma^* \mid (c_0 \ldots c_{k-2} \sqsubseteq w) \wedge (c_0 \ldots c_{k-1} \not\sqsubseteq w)\}.$$

To say otherwise, $\texttt{Slice}_\Sigma(v) = \sqsubseteq_\Sigma(c_0 \ldots c_{k-2}) \cap \not\sqsubseteq_\Sigma(c_0 \ldots c_{k-1})$, which is the set of words in Σ^* which are superwords of $c_0 \ldots c_{k-2}$ but not of $c_0 \ldots c_{k-1}$. We provide a detailed description of words in $\texttt{Slice}_\Sigma(v)$. Let us abbreviate $\Sigma_i = \Sigma \setminus \{c_i\}$, then Σ_i^* is the set of $w \in \Sigma^*$ such that $c_i \notin w$. We will prove that the words in $\texttt{Slice}_\Sigma(v)$ are exactly all the words of the form $w = w_0 c_0 w_1 c_1 \ldots c_{k-2} w_{k-1}$, such that $c_i \notin w_i$, that is, such that $w_i \in \Sigma_i^*$, for all $i < k$. Such a decomposition will be unique and, for all $i < k$, it will define a map α_i such that $w_i = \alpha_i(w)$. We first prove that we have a slightly different decomposition for the words of the cone of v, then we prove the required decomposition for the words of $\texttt{Slice}_\Sigma(v)$.

Lemma 3.2 (Characterization of cone and of slice) *Let $v = c_0 \ldots c_{k-1}$, $w \in \Sigma^*$.*

1. CONE. *If v is embedded in w through f, then there is a unique decomposition $w = w_0c_0w_1c_1 \dots w_{k-1}c_{k-1}w_k$, such that $c_i \notin w_i$, for all $i < k$. We have no requirement for w_k. Furthermore, if*

$$g(i) = \mathtt{len}(w_0c_0w_1c_1 \dots c_{i-1}w_i),$$

for all $i < k$, then g is the minimum embedding of v in w in the point-wise ordering: $g(i) \leqslant f(i)$ for all $i < k$.

2. SLICE. *If $k \geqslant 1$, then $\mathtt{Slice}_\Sigma(v)$ is the set of all words w such that $w = w_0c_0 \dots w_{k-2}c_{k-2}w_{k-1}$ and $c_i \notin w_i$ for all $i < k$. The decomposition of w if it exists, it is unique.*

Proof Let $v = c_0 \dots c_{k-1} \in \Sigma^*$, $w \in \Sigma^*$.

1. CONE. Assume that f is an embedding of v in w, we prove that there is a unique decomposition

$$w = w_0c_0w_1c_1 \dots w_{k-1}c_{k-1}w_k,$$

such that $c_i \notin w_i$, for all $i < k$. We explicitly stress that we have no requirement on w_k. Furthermore, if $g(i) = \mathtt{len}(w_0c_0w_1c_1 \dots w_{i-1}c_{i-1}w_i)$ for all $i < k$, we will prove that g is the minimum embedding of v in w in the point-wise ordering: $g(i) \leq f(i)$ for all $i < k$.

We reason by induction on k.

(a) Assume that $k = 0$. Then the decomposition $w = w_0$, with no conditions on w_0, exists and it is unique. f and g are maps with empty domain, therefore we trivially have that $g(i) \leq f(i)$ for all $i < 0$.

(b) Assume the thesis for $v' = c_0 \dots c_{k-2}$ in order to prove the thesis for $v = c_0 \dots c_{k-1}$. By induction hypothesis, there is a unique decomposition

$$w = w_0c_0w_1c_1 \dots w_{k-2}c_{k-2}w_{k-1},$$

such that $c_i \notin w_i$, for all $i < k-1$. If f' is the restriction of f to $[0, k-1[$ and $g'(i) = \mathtt{len}(w_0c_0w_1c_1 \dots c_{i-1}w_i)$ for all $i < k-1$, then by inductive hypothesis we have $g'(i) \leq f'(i) = f(i)$ for all $i < k-1$. For all $i < k-1$, we have $f(k-1) > f'(i) \geq g'(i)$. We deduce that $f(k-1)$ is the index of some c_{k-1} in w which is in the suffix w_{k-1}. Thus, there is a unique decomposition $w_{k-1} = w'_{k-1}c_{k-1}w'_k$ such that $c_{k-1} \notin w'_{k-1}$. We conclude that there is a unique decomposition $w = w_0c_0w_1c_1 \dots w_{k-2}c_{k-2}w'_{k-1}c_{k-1}\star w'_k$ such that $c_i \notin w_i$ for all $i < k-1$ and $c_{k-1} \notin w'_{k-1}$.

We have $g' \leq f'$ and we have still to prove that $g(k-1) \leq f(k-1)$. $f(k-1)$ is the index of some c_{k-1} in w which is in the suffix w_{k-1}. We have $c_{k-1} \notin w'_{k-1}$, therefore $f(k-1)$ is the index of some c_{k-1} in w which is in the suffix $c_{k-1}w'_k$. By assumption, $g(k-1) = \mathtt{len}(w_0c_0w_1c_1 \ldots w_{k-1})$, therefore $g(k-1)$ is the index of the FIRST $c_{k-1} \in w$ which is in the suffix $c_{k-1}w'_k$. We conclude that $g(k-1) \leq f(k-1)$, as wished.

2. SLICE. Assume that $k \geq 1$ and $w \in \mathtt{Slice}_\Sigma(v)$, $v = c_0 \ldots c_{k-1}$. By the previous point applied to $v' = c_0 \ldots c_{k-2}$ there is a unique decomposition $w = w_0c_0 \ldots w_{k-2}c_{k-2}w_{k-1}$ such that $c_i \notin w_i$ for all $i < k-1$, and an embedding g of v' in w such that g is empty or we have $g(i) \leq g(k-2) = \mathtt{len}(w_0c_0w_1 \ldots c_{k-3}w_{k-2})$ for all $i < k-1$.

   We have still to prove that $c_{k-1} \notin w_{k-1}$. Assume that $c_{k-1} \in w_{k-1}$; then we can extend g to an embedding h from v to w with $h(k-1) =$ "the first index of some c_{k-1} in w which is in the suffix w_{k-1}". The existence of h is in contradiction with $v \not\sqsubseteq w$. □

From the uniqueness of the decomposition of $w \in \mathtt{Slice}_\Sigma(v)$, we define the maps $\alpha_i(w)$ for $i < \mathtt{len}(v)$.

Definition 3.16 (The maps α_i) *Assume that $v = c_0 \ldots c_{k-1}$, $k \geqslant 1$ and $i < k$, as before let $\Sigma_i = \Sigma \setminus \{c_i\}$. Assume that $w = w_0c_0 \ldots w_{k-2}c_{k-2}w_{k-1}$, with $c_i \notin w_i$ for all $i < k$, is the unique decomposition given by the previous lemma, then we define $\alpha_i \colon \mathtt{Slice}_\Sigma(v) \to \Sigma_i^*$ by $\alpha_i(w) = w_i$.*

If X and Y are sets with binary relations R and S, respectively, then by a *morphism* $f \colon (X, R) \to (Y, S)$ we understand a map $f \colon X \to Y$ such that if xRx', then $f(x)Sf(x')$ (in the case R, S are order relations, such a function is called order-preserving, cf. Def. 2.4).

The "product" α of all α_i in Def. 3.16 defines a bijection, whose inverse is a morphism for $\sqsubseteq$; the map α plays a crucial role in the proof of Higman's lemma.

Lemma 3.3 (Product map and Slices) *The product map $\alpha = \alpha_1 \times \ldots \times \alpha_k \colon \mathtt{Slice}_\Sigma(v) \to \Sigma_0^* \times \ldots \times \Sigma_{k-1}^*$ is a bijection. Its inverse α^{-1} is a morphism from $(\Sigma_0^* \times \ldots \times \Sigma_{k-1}^*, \sqsubseteq \times \ldots \times \sqsubseteq)$ to $(\mathtt{Slice}_\Sigma(v), \sqsubseteq)$.*

Proof The product map α is right-invertible because $w = \alpha_0(w)c_0 \ldots \alpha_{k-1}(w)$ (Lemma 3.2).

We prove that α^{-1} is a morphism. If $w, w' \in \mathtt{Slice}_\Sigma(v)$ and we have $\alpha_1(w) \sqsubseteq \alpha_1(w'), \ldots, \alpha_{k-1}(w) \sqsubseteq \alpha_{k-1}(w')$, then $w = \alpha_0(w)c_0 \ldots \alpha_{k-1}(w) \sqsubseteq \alpha_0(w')c_0 \ldots \alpha_{k-1}(w') = w'$. □

Now we can characterize the anticone $\not\sqsubseteq_\Sigma(v)$ as a finite union of slices $\mathtt{Slice}_\Sigma(v')$.

Lemma 3.4 (Anticone) *$\not\sqsupseteq_\Sigma(v)$ is the union of all $\texttt{Slice}_\Sigma(v')$ for $v' \leqslant v$.*

Proof We prove both inclusions.

1. Assume that $w \in \texttt{Slice}_\Sigma(v')$ for some $v' \leq v$. We have to prove that $w \in \not\sqsupseteq_\Sigma(v)$, i.e. that $v \not\sqsubseteq w$. Assume for contradiction that $v \sqsubseteq w$; then, from $v' \leq v \sqsubseteq w$, we deduce $v' \sqsubseteq w$, contradicting $w \in \texttt{Slice}_\Sigma(v')$.

2. Assume that $w \in \not\sqsupseteq_\Sigma(v)$, namely that $v \not\sqsubseteq w$. We have to prove that $w \in \texttt{Slice}_\Sigma(v')$ for some $v' \leq v$. Let $v = c_0 \dots c_{k-1}$; by assumption $c_0 \dots c_{k-1} \not\sqsubseteq w$. There is a first $0 \leq i \leq k$ such that $c_0 \dots c_{i-1} \not\sqsubseteq w$, so let $v' = c_0 \dots c_{i-1}$. By the choice of i, we deduce $v' \not\sqsubseteq w$ and $v'' \sqsubseteq w$ for all $v'' < v'$; then, by definition of $\texttt{Slice}_\Sigma(v')$, we have $w \in \texttt{Slice}_\Sigma(v')$, as wished. □

These are all the properties we need about words, for what concerns bars we refer to the next section.

3.4.3 Bars: Definition and Properties

In this paragraph we define bars and their related notions, proving with intuitionistic logic the properties required in the rest of the section. The strongest property says that the Cartesian product of barred sets is barred by the union of the inverse image of the two projections. It is worth noticing that if we consider the empty bar, then from each result in this section about bars (except for "monotonicity", which only makes sense for bars) we obtain some well-known results about hereditary well-founded sets.

Given a *quasi-order* $(P, \leq)$, a sequence $(p_k)_k$, finite or infinite, over $(P, \leq)$ is *weakly increasing*, for short w.i., if, for every indices $i \leq j$, we have $p_i \leq p_j$.

A *labelling* of I on P is a map $\phi : I \to P$. A length n list $l = \langle l(0), \dots, l(n-1)\rangle \in \texttt{Fin}(I)$ can be turned into a list $\phi l = \langle \phi l(0), \dots, \phi l(n-1)\rangle \in \texttt{Fin}(P)$ on P, by composing with the labelling ϕ of I. When $I = P$, we also consider the identical label $\phi = \texttt{id}$, in which the list of labels of a list is the list itself. We write $\texttt{Incr}(\leq, \phi, I)$ for the set of finite lists $l \in \texttt{Fin}(I)$ such that ϕl is a weakly increasing list in P with respect to $\leq$.

We say that $B \subseteq \texttt{Fin}(I)$ is $<_1$-*closed*, or closed by one-step extension, if for all $l \in B$, $l <_1 m$ we have $m \in B$. Being closed by one-step extension is the same than being closed by $\leqslant$ (by extension).

We extend now the notion of a hereditarily well-founded set (see for instance [119, 133, 134] and compare with Def. 3.5) and define the one of *barred set*, both with respect to a given binary relation R. Our definitions are classically equivalent to the definition "all R-decreasing sequences intersect the bar", but in intuitionistic logic they allow to derive more results. Our bars generalize Troelstra's definition of bar ([179], page 77, Def. 1.9.20).

Definition 3.17 (Well-founded and Barred Sets) *Let P, X, B be sets and R be a binary relation.*

1. *P is X, R-*HEREDITARY *whenever, for all $x \in X$, if for all $x' \in X$ with $x'Rx$ we have $x' \in P$, then $x \in P$.*
2. *X is R-*WELL-FOUNDED *if for all P X, R-hereditary such that $P \subseteq X$ we have $P = X$.*
3. *B* BARS *X, R if for all P X, R-hereditary such that $B \cap X \subseteq P \subseteq X$ we have $P = X$.*
4. *B* BARS *x in X, R if for all P X, R-hereditary such that $B \cap X \subseteq P \subseteq X$ we have $x \in P$.*

Some comments on these definitions are in order. First, "X, R-hereditary" is exactly "X, R-inductive" from [20]. Next, B bars X, R if and only if B bars x in X, R for every $x \in X$.

In general, the subset consisting of the $x \in X$ such that B bars x in X, R is defined as the intersection of all X, R-hereditary $P \subseteq X$ such that $B \cap X \subseteq P$; and one can see (Proposition 3.11.2) that this intersection itself is X, R-hereditary. Hence "B bars x in X, R" coincides with the predicate $B \cap X \mid x$ from [48, 50]: that is, the inductively defined least X, R-hereditary predicate on X which contains $B \cap X$. B is often called the *inductively defined predicate* from X, R.

So "B bars x in X, R" can be interpreted as "x is accessible from B in X, R"; for $B = \emptyset$ this is nothing but the *accessibility predicate* [126, 162]. Accordingly, X is R-well-founded if and only if X, R is barred by $B = \emptyset$, or barred by any B such that $B \cap X = \emptyset$.

In Troelstra ([179], page 77, Def. 1.9.20) the definition of bar is given with $X =$ the set of all lists of natural numbers and $R =$ the one-step extension; it is also assumed that B is either decidable or closed by extensions. But the main difference is that the definition of bar is given as in classical mathematics, B is a bar if all infinite lists of natural numbers have some prefix in B. Instead, we defined B as the intersection of all X, R-hereditary properties, since we find this version more suitable for constructive proofs; this is the typical definition in the context of generalized inductive definitions [1, 143].

In the case we do not mention it, by R we mean $>_1$, the reverse of the one-step extension relation. In this case we say that B bars l in X, respectively that B bars X, meaning that B bars l in $X, >_1$, respectively that B bars $X, >_1$.

A subset B of X is said to be *R-downward-closed* if $x \in B$ and yRx imply $y \in B$. We have a puzzling point to stress here, if R is $>_1$, then R-downward-closed actually means that for all $x \in B$ if $y >_1 x$, then $y \in B$. That is, "R-downward-closed" in this case means "closed by one-step *extensions*". The reason is that in the literature, set of lists are often used to represent trees, and in the case of trees, it is customary to consider "smaller" a one-step-extension of a node of a tree, i.e. trees growing downward. We will still use the word "downward-closed" in this case, because it is a well-established terminology for inductive reasoning, but we point out that "downward-closed" in this case means "closed by one-step extensions".

A last warning. In our definition, bars for set of lists *do not have to be closed by extensions*. For instance, the set B of all finite lists on I having odd length is a bar for the set of all lists on I and $>_1$, because each list is either odd and barred by B, or has all one-step extensions odd and barred B, and in this case is barred because being barred is an hereditary predicate. Yet, each one-step extension of a list in B is some even length list, which is not in B. Closure of a bar for a set of lists by list extension is an useful feature in some proofs, nevertheless it is not strictly required in most cases.

We derive now some basic properties for bars, requiring little more than definition unfolding.

An *R-descending chain* in X is a finite or infinite list $x_0 R^{-1} x_1 R^{-1} x_2 R^{-1} \ldots$ of elements of X. For instance, a $<$-descending chain in $\mathbb{N}$ is any (necessarily finite) list $x_0 > x_1 > x_2 > \ldots$ of natural numbers. We will prove that if B bars X, R, then every infinite R-descending chain in X intersects B. Using classical logic and some choice, the two properties are equivalent, but with intuitionistic logic we only have the implication from the former to the latter.[12]

Proposition 3.11 (Infinite R-descending chains) *Let X, B be sets and R be a binary relation.*

1. *X is X, R-hereditary.*

2. *Any intersection $\cap\mathcal{F}$ of any inhabited family $\mathcal{F}$ of X, R-hereditary sets is X, R-hereditary.*

3. *The predicate "B bars x in X, R" on $x \in X$ is between $B \cap X$ and X and it is itself X, R-hereditary.*

4. *If B bars X, R, then every infinite R-descending chain in X intersects B in an infinite set of indexes.*

Proof

[12] We sketch a folk-lore proof. There is a model of Intuitionistic Logic in which all chain are recursive, while some order $<$ on some X has all infinite recursive $<$-descending chain finite and some non-recursive infinite $<$-descending chain infinite, with set of elements C. In this model all infinite $<$-descending chain in X intersects $\emptyset$, because no infinite $<$-descending chain exists. Yet, the set $P = X \setminus C$ is $X, <$-hereditary while $P \neq X$. Thus, it is not true that $\emptyset$ bars X, R.

1. Immediate by definition unfolding.

2. Assume that $\mathcal{F}$ is any inhabited family of X, R-hereditary sets, in order to prove that the intersection $\cap\mathcal{F}$ of $\mathcal{F}$ is X, R-hereditary. We assume that $x \in X$, $y \in \cap\mathcal{F}$ for all yRx, $y \in X$, and we have to prove that $x \in \cap\mathcal{F}$. From $y \in \cap\mathcal{F}$, we deduce that $y \in P$ for all yRx, $y \in X$ and for all $P \in \mathcal{F}$. We obtain that $x \in P$ because P is X, R-hereditary, and this for all $P \in \mathcal{F}$, thus $x \in \cap\mathcal{F}$.

3. Let $X_B = \{l \in X \mid B \text{ bars } l \text{ in } X, R\}$ be the set of elements of X which are barred by B in X, R, in order to prove that $B \cap X \subseteq X_B$ and X_B X, R-hereditary since, by definition, $X_B \subseteq X$. If $x \in B \cap X$, then x belongs to all X, R-hereditary sets which contain $B \cap X$; therefore it is barred by B and thus in X_B. To prove that X_B is X, R-hereditary, let us assume that $l \in X$ and that all $l' \in X$ with $l'Rl$ are barred by B, out goal is to prove that $l \in X_B$, i.e. also l is barred by B. Let P be an X, R-hereditary set such that $B \cap X \subseteq P \subseteq X$. Since all $l' \in X$ with $l'Rl$ are barred by B, they all are also in P; therefore $l \in P$, since P is X, R-hereditary, and thus l is barred by B.

4. Assume that B bars X, R and that $\sigma\colon \mathbb{N} \to X$ is some infinite R-descending chain in X which intersects B, in order to prove that σ intersects B infinitely many times. We have to prove that for all $x \in X$ and all $n \in \mathbb{N}$, if $x = \sigma(n)$, then there is $m \in \mathbb{N}$, $m \geq n$ such that $\sigma(m) \in B$. Let us define the set $P = \{x \in X \mid \forall n \in \mathbb{N}\ x = \sigma(n) \implies \exists m \in \mathbb{N}\ (m \geq n \wedge \sigma(m) \in B)\}$, then we prove: (a) $B \cap X \subseteq P$ and (b) P is X, R-hereditary. We will conclude that $x \in P$ for all $x \in X$ and our thesis follows.

   (a) Assume that $x \in B \cap X$ in order to prove that $x \in P$. For, assume that $n \in \mathbb{N}$, $x = \sigma(n)$. We choose $m = n$ and we deduce that $m \geq n$, $\sigma(m) \in B$; thus $x \in P$, as wished.

   (b) Let $x \in X$ be such that for all $y \in X$ with yRx we have $y \in P$, our goal is to prove that $x \in P$. By assumption, we have $x \in X$. Assume that $n \in \mathbb{N}$, $x = \sigma(n)$ in order to prove that, for some $m \in \mathbb{N}$, $m \geqslant n$, we have $\sigma(m) \in B$. Then, for all yRx, $y \in X$ we have $y \in P$, therefore for all $p \in \mathbb{N}$ if $y = \sigma(p)$, then for some $m \in \mathbb{N}$, $m \geq p$ we have $\sigma(m) \in B$. By assumption again we have $x = \sigma(n)R^{-1}\sigma(n+1)$, that is, $\sigma(n+1)R\sigma(n) = x$. If we choose $y = \sigma(n+1)$ and $p = n+1$, we conclude that $\sigma(m) \in B$ for some $m \geq n+1 > n$, as wished. □

If B bars X, R, then we can prove that a property $P \subseteq X$ holds for all $x \in X$ by bar-induction on B, X, R. Bar-induction is the following principle. Assume that $P \subseteq X$ and: *(i. base case)* for all $x \in B \cap X$ we have $x \in P$; *(ii. inductive* *case)* if for all $y \in X$ with yRx we have $y \in P$, then $x \in P$. Then we conclude that $P = X$. As an example, Proposition 3.11.4 is proved by bar-induction on B, X, R.

We give an interpretation of a proof by bar-induction of some property P on X. We think $B \cap X$ as the set of elements for which we can prove the property P directly. The one-step extension yRx of a sequence x are all elements "smaller" than x. In the inductive step of bar-induction, we have proved that if all elements "smaller" than any element x are in P, then x is in P. Eventually, if B bars X, R, then we conclude that $P = X$.

A tool for proving that B bars X, R is the notion of *simulation*. We say that x' is an R-predecessor of x if $x'Rx$. Roughly speaking, $V \subseteq X \times Y$ is a simulation between X, R and Y, S if whenever two elements are related by V, then any R-predecessor of the first element is V-related with some S-predecessor of the second element.

Definition 3.18 *We say that $V \subseteq X \times Y$ SIMULATES X, R in Y, S if for all $x, x' \in X$, $y \in Y$, if $x'Rx$ and xVy, then there is some $y' \in Y$, $y'Sy$ such that $x'Vy'$.*

We will prove that a simulation V, when V is everywhere defined (i.e. for every $x \in X$ there exists $y \in Y$ such that xVy), moves bars backwards from Y to X. By this we mean: if B bars Y, S, then $V^{-1}(B)$ bars X, R. In particular, simulation moves well-foundedness backwards: if we take $B = \emptyset$, we obtain that if Y is S-well-founded, then X is R-well-founded. We will prove the same result for morphisms: if $f \colon X \to Y$ maps pairs related by R into pairs related by S, then f^{-1} maps bars for Y, S into bars for X, R.

Lemma 3.5 (Simulation Lemma) *Let X, Y, B, C be sets and R, S be binary relations.*

1. (SIMULATION) *Assume that $V \subseteq X \times Y$ simulates X, R in Y, S, that V is everywhere defined and that C bars Y, S; then $B = V^{-1}(C)$ bars X.*
2. (MORPHISM) *Assume that $f \colon X, R \to Y, S$ is a morphism and C bars Y, then $f^{-1}(C)$ bars X.*

Proof Assume that X, Y, B, C are sets and R, S are binary relations.

1. (SIMULATION) Assume that $V \subseteq X \times Y$ simulates X, R in Y, S, V is everywhere defined and C bars Y, S in order to prove that $B = V^{-1}(C)$ bars X, R.

   Assume that $B \cap X \subseteq P \subseteq X$ and P is X, R-hereditary in order to prove that $P = X$. Define $Q := \{y \in Y \mid \forall x \in X\, (xVy \implies x \in P)\}$. We prove

$Q = Y$ by bar-induction on Y, S; it will follow for all $y \in Y$, all xVy we have $x \in P$. V is everywhere defined, therefore for all $x \in X$ there is some $y \in Y$ such that xVy. From $y \in Y = Q$ we will conclude that $x \in P$, and this for all $x \in X$, as wished.

Now we have to prove that Q includes C and is Y, S-hereditary.

Base Case. We have to prove that $C \cap Y \subseteq Q$. By definition of Q we assume that $y \in C \cap Y$, $x \in X$, xVy in order to prove that $x \in P$. From xVy we deduce that $x \in V^{-1}(C) = B$. From $B \cap X \subseteq P$ we conclude that $x \in B \cap X \subseteq P$, as wished.

Inductive Case. Assume that $y \in Y$, and for all $y'Sy$, $y' \in Y$ we have $y' \in Q$, in order to prove that $y \in Q$. By definition of Q we assume that $x \in X$, xVy in order to prove that $x \in P$. From P X, R-hereditary it is enough to prove that for all $x'Rx$, $x' \in X$ we have $x' \in P$. From V simulation there is some $y'Sy$, $y' \in Y$ such that $x'Vy'$. By assumption on y' we have $y' \in Q$, and by definition of Q and $x'Vy'$ we conclude that $x' \in P$, as wished.

2. (inverse image) Assume that $f : X \to Y$ is increasing with respect to R, S, and C bars Y. Then f is a simulation from X, R to Y, S, and f is everywhere defined because f is a function. From point 1 above we conclude that $B = f^{-1}(C)$ bars T. □

Now we prove that, if we extend a bar or we reduce the barred set and the relation, then the fact of being a bar is preserved. If we choose the empty bar we obtain a well-known result for well-founded relations, namely well-foundedness is preserved by moving to a subrelation. To say otherwise: if X is R-well-founded, with $Y \subseteq X$ and $S \subseteq R$, then Y is S-well-founded.

Lemma 3.6 (Monotonicity and Antimonotonicity) *Let X, Y, B, C be sets, and R, S binary relations.*

1. (monotonicity) *If B bars X, R and $B \cap X \subseteq C \cap X$, then C bars X, R.*
2. (antimonotonicity) *If B bars X, R and $Y \subseteq X$, $S \subseteq R$, then B bars Y, S.*

Proof Let X, Y, B, C be sets, and R, S binary relations.

1. (monotonicity) Immediate.
2. (antimonotonicity) Assume that B bars X, R and let $Y \subseteq X$, $S \subseteq R$. By $Y \subseteq X$, we have $\mathtt{id} : Y \to X$, which map is S, R-monotone since $S \subseteq R$. Lemma 3.5.2 yields that $B = \mathtt{id}^{-1}(B)$ bars Y, S. □

For every family of sets Y_x indexed by $x \in X$, we adopt from type theory the notation $\Sigma_{x\in X} Y_x$ for the set of pairs (x, y) such that $x \in X$ and $y \in Y_x$.

Now let R be a binary relation, and $S = \{S_x\}_{x\in X}$ an indexed family of binary relations on Y. We can think S as a ternary relation such that $S(x, y', y) \Leftrightarrow S_x(y', y)$ for all $x \in X$ and $y', y \in Y$. The *lexicographic product* $R \times S$ is the relation comparing (x', y') with (x, y) according to xRx', or, if $x = x'$, according to yS_xy'. Formally:

$$(x', y')(R \times S)(x, y) \quad \Leftrightarrow \quad x'Rx \ \vee \ (x' = x \ \wedge \ y'S_xy).$$

$R \times S$ is a partial order if R and all S_x are partial orders, in this case $R \times S$ is called the lexicographic order on pairs.

Assume that the dependency on $x \in X$ is trivial, that is, for some Z, T and for all $x \in X$ we have $Y_x = Z$, $S_x = T$. In this case we write $R \times T$ for $R \times S$. By definition unfolding, $R \times T$ is a relation on $\Sigma_{x\in X} Y_x = X \times Z$ defined by $(x', y')(R \times T)(x, y) \Leftrightarrow x'Rx \vee (x' = x \wedge y'Ty)$.

With the next lemma we define a bar D for $\Sigma_{x\in X} Y_x$, $R \times S$. When the dependency on $x \in X$ is trivial, D is a bar for $X \times Z$, $R \times T$. Our result generalises [119, Chapter I, Theorem 6.3], which is, in our terminology, the special case when D is the empty bar.

Lemma 3.7 (Lexicographic Product) *Let X, Y, B and C_x for $x \in X$ be sets, R a binary relation and S a ternary relation. Suppose that B bars X, R, and that C_x bars Y_x, S_x for all $x \in X$. Let D be the set of all pairs $(x, y) \in \Sigma_{x\in X} Y_x$ such that $x \in B$ or $y \in C_x$.*

1. *D bars $\Sigma_{x\in X} Y_x$ with $R \times S$, the lexicographic product of R, S.*
2. *If for some Z, T and for all $x \in X$ we have $Y_x = Z$, $S_x = T$, then D bars $X \times Z$, $R \times T$.*

Proof We assume that $Q \supseteq D \cap \Sigma_{x\in X} Y_x = D$ and Q is $\Sigma_{x\in X} Y_x, R \times S$-hereditary in order to prove that $Q = \Sigma_{x\in X} Y_x$.

We define $P := \{x \in X \mid \forall y \in Y_x \ \langle x, y\rangle \in Q\}$. By definition, $P \subseteq X$, and $x \in P$ says that all pairs of first component x satisfy Q. Then it is enough to prove $x \in P$ for all $x \in X$ in order to conclude that $Q = \Sigma_{x\in X} Y_x$. We argue by bar-induction on B and X, R. As auxiliary induction we will use bar-induction on C_x and Y_x, S_x.

Base Case. Assume that $x \in B \cap X$ in order to prove that $x \in P$. For, we assume that $y \in Y_x$ in order to prove that $\langle x, y\rangle \in Q$. From $x \in B \cap X$ we deduce that $\langle x, y\rangle \in (B \cap X) \times Y_x \subseteq D \cap \Sigma_{x\in X} Y_x$. From $D \cap (\Sigma_{x\in X} Y_x) \subseteq Q$ we conclude that $\langle x, y\rangle \in Q$, as wished.

Inductive Case. Assume that $x \in X$ and for all $x' \in X$, $x'Rx$ we have $x' \in P$, in order to prove that $x \in P$. By definition unfolding, let us assume that for all

$x' \in X$, $x'Rx$, all $y' \in Y_{x'}$ we have $\langle x', y'\rangle \in Q$; our goal is to prove that, for all $y \in Y_x$, we have $\langle x, y\rangle \in Q$. We have $D \subseteq Q$ and Q is $R \times S, \Sigma_{x\in X} Y_x$-hereditary, therefore in order to prove that $\langle x, y\rangle \in Q$, it is enough to prove that: for all $\langle x', y'\rangle \in \Sigma_{x\in X} Y_x$, $\langle x', y'\rangle R \times S\langle x, y\rangle$, we have $\langle x', y'\rangle \in Q$. By definition of $R \times S$ our thesis unfolds to: for all $x' \in X$, $y' \in Y_{x'}$ such that either $x'Rx$, or ($x' = x$ and $y'Sy$), we have $\langle x', y'\rangle \in Q$. In the case $x'Rx$, we have $\langle x', y'\rangle \in Q$ for all $y' \in Y_{x'}$ by assumption; it remains to prove that if $x' = x$ and $y'Sy$, then $\langle x', y'\rangle \in Q$. It is enough to prove a stronger property, namely that $\langle x, y'\rangle \in Q$ for *all* $y' \in Y_x = Y_{x'}$. Let define a set $Q' \subseteq Y_x$ by $y' \in Q' :\Leftrightarrow \langle x, y'\rangle \in Q$. Then we prove $y' \in Q'$ for all $y' \in Y_x$ by auxiliary bar-induction on the bar C_x for Y_x, S_x: this will imply that $\langle x, y'\rangle \in Q$ for all $y' \in Y$, as required.

Base case of second bar-induction. Assume that $y' \in C_x \cap Y_x$. Then $\langle x, y'\rangle \in D$. From $D \subseteq Q$ we deduce $\langle x, y'\rangle \in Q$, that is, $y' \in Q'$.

Inductive case of second induction. Assume that for all $y'' \in Y_x$, $y''S_x y'$ we have $y'' \in Q'$ in order to prove $y' \in Q'$. The assumption $y'' \in Q'$ for all $y''S_x y'$ unfolds to: $\langle x, y''\rangle \in Q$, for all $y''S_x y'$. By assumption, we have $\langle \bar{x}, y''\rangle \in Q$ for all $\bar{x} \in X$, $\bar{x}Rx$, and all $y'' \in Y_x$ and, by definition of $R \times S$, we deduce $\langle \bar{x}, y''\rangle \in Q$ for all $\langle \bar{x}, y''\rangle R \times S\langle x, y'\rangle$. Eventually, from Q inductive with respect to $\Sigma_{x\in X} Y_x, R \times S$ we deduce that $\langle x, y'\rangle \in Q$, that is, that $y \in Q'$, as wished. □

3.4.4 Higman's Lemma for Bars

In this section, we state Higman's lemma for bars, which is a constructive version of Higman's lemma for subsequences, and we argue why this version is stronger, within intuitionistic logic, than the versions proposed until now.

We briefly recall that, given any quasi-order $(P, \leqslant)$ and a labelling $\phi\colon I \to P$, $\mathtt{Fin}(I)$ denotes the set of finite lists over I and $\mathtt{Incr}(\phi, I)$ the subset $\mathtt{Incr}(\leqslant, \phi, I)$ of $\mathtt{Fin}(I)$ consisting of the finite lists ℓ in I such that $\phi\ell$ is a weakly increasing list in P for the order $\leqslant$. We introduce now the constructive version wqo(bar) of the notion of wqo;[13] more precisely, we present two equivalent definitions for wqo(bar), the latter one more suitable for practical applications.

Assume that $(P, \leq)$ is a quasi-order and $\phi\colon I \to P$ any labelling. We first define a binary relation $\mathtt{WI}_\phi(l, m)$ for any $l, m \in \mathtt{Fin}(I)$ as "m is a sublist of l and the ϕ-labelling of m is $\leq$-w.i.", formally:

$$\mathtt{WI}_\phi(l, m) \;\equiv\; l \sqsupseteq m \;\wedge\; m \in \mathtt{Incr}(\leq, \phi, I).$$

We formulate the notion of wqo(bar), saying that for all labelling $\phi\colon I \to P$ and all bars B for the set of ϕ-w.i. sublists of X, the set of lists having some ϕ-w.i. sublist in B is a bar for X. By unfolding definitions, $\mathtt{WI}_\phi(X)$ denotes the set of all ϕ-w.i. m

[13]For a constructive comparison of the customary concepts of wqo see Subsec. 3.2.2.

which are sublists of some list in X, and $\mathtt{WI}_\phi^{-1}(B)$ denotes the set of lists having some ϕ-w.i. sublist in B.

Definition 3.19 *A quasi-order $(P, \leqslant)$ is* wqo(bar) *if*

$$B \text{ bars } \mathtt{WI}_\phi(X) \implies \mathtt{WI}_\phi^{-1}(B) \text{ bars } X$$

for all labellings $\phi\colon I \to P$ of any set I by P, for every subsets $X \subseteq \mathtt{Fin}(I)$ and every set B.

Despite its formal elegance, the previous definition is not the right one for practical purposes. Thus, we introduce the notion of wqo(bar)*, proving subsequently the equivalence between the two definitions. A quasi-order $(P, \leqslant)$ is wqo(bar)* if for any set $X \subseteq \mathtt{Fin}(I)$, a bar B for the subset of X consisting of all w.i. lists (those in $\mathtt{Incr}(\phi, I)$) is a bar for the whole of X, provided that X is closed by sublists and B by superlists.

Definition 3.20 *A quasi-order $(P, \leqslant)$ is called* wqo(bar)* *if*

$$B \text{ bars } X \cap \mathtt{Incr}(\phi, I) \implies B \text{ bars } X \tag{3.1}$$

for all labellings $\phi\colon I \to P$ of any set I by P, for every subset $X \subseteq \mathtt{Fin}(I)$ closed by I-sublists and for every subset $B \subseteq \mathtt{Fin}(I)$ closed by I-superlists.

As before, "B bars ..." is meant for the converse $>_1$ of the one-step extension order $<_1$ on $\mathtt{Fin}(I)$.

Classically, (3.1) means that every infinite $<_1$-increasing chain $\sigma\colon \mathbb{N} \to X$ meets B if this is the case already for any such σ for which in addition we have $\phi\sigma(0) \leqslant \phi\sigma(1) \leqslant \ldots$ Again using classical logic, (3.1) is equivalent to the more commonly used notion of wqo(set): for every infinite list $\sigma\colon \mathbb{N} \to P$ there is a an infinite $\leqslant$-weakly increasing sublist $\tau\colon \mathbb{N} \to P$.

Before moving on, we prove the equivalence between wqo(bar) and wqo(bar)*; given the equivalence, after the lemma we will simply use the notation wqo(bar).

Lemma 3.8 *Let $(P, \leq)$ be a quasi order, then* wqo(bar) *is equivalent to* wqo(bar)**.*

Proof We prove the two directions separately.

1. Assume that $(P, \leq)$ is a wqo(bar)* and B bars $\mathtt{WI}_\phi(X)$ in order to prove that $\mathtt{WI}_\phi^{-1}(B)$ bars X. By $\mathtt{WI}_\phi^{-1}(B) \supseteq B$ and monotonicity of bars we obtain that $\mathtt{WI}_\phi^{-1}(B)$ bars $\mathtt{WI}_\phi(X)$; moreover, by definition we have $\mathtt{WI}_\phi^{-1}(B)$ closed by I-superlists and $\mathtt{WI}_\phi(X)$ closed by I-sublist. From $(P, \leq)$ wqo(bar)* we deduce that that $\mathtt{WI}_\phi^{-1}(B)$ bars $\mathtt{WI}_\phi(X)$. Finally, from $\mathtt{WI}_\phi(X) \supseteq X$ and antimonotonicity of bars we conclude that $\mathtt{WI}_\phi^{-1}(B)$ bars X.

2. Assume that $(P, \leq)$ is a $\texttt{wqo}$(bar), i.e. for all $X \subseteq \texttt{Fin}(I)$, all B, if B bars $\texttt{WI}_\phi(X)$ then $\texttt{WI}_\phi^{-1}(B)$ bars X; we prove that $(P, \leq)$ is $\texttt{wqo}$(bar)*. Assume that B is closed by I-superlists, X is closed by I-sublist and B bars $X \cap \texttt{Incr}(\leq, \phi, I)$ in order to prove that B bars X. By X closed by I-sublist, we have that $\texttt{WI}_\phi(X) = X \cap \texttt{Incr}(\leq, \phi, I)$; hence, B bars $\texttt{WI}_\phi(X)$. By assumption we obtain that $\texttt{WI}_\phi^{-1}(B)$ bars X. From B closed by I-superlist, we deduce that $\texttt{WI}_\phi^{-1}(B) \subseteq B$ and thus, by monotonicity of bars, B bars X. □

If we focus on partial orders $P = \Sigma^*$, given by the set of words for a finite alphabet Σ with the subword order $\sqsubseteq$ as $\leqslant$, then we can state the following result.

Theorem 3.7 (Higman's lemma for bars) *If Σ is a finite alphabet, then Σ^* is a $\texttt{wqo}$(bar).*

We postpone the proof of Theorem 3.7 to Subsec. 3.4.5. In the rest of this paragraph we derive with intuitionistic logic some corollaries of Theorem 3.7, in order to show the interest from a constructive viewpoint of stating the result in this form

Our corollaries are about functionals. We add a bottom element $\perp$ to $\mathbb{N}$ and consider total continuous functionals $\Phi\colon \texttt{Inf}(\Sigma^*) \to \mathbb{N} \cup \{\perp\}$ on infinite sequences of words, taking the canonical topology on $\texttt{Inf}(\Sigma^*) \to \mathbb{N} \cup \{\perp\}$.[14] Φ continuous roughly means that Φ, when converge, uses only a finite part of its input. Informally, a partial functional F explores larger and larger finite prefixes of an infinite sequence of words, until F finds a prefix long enough to compute some $n \in \mathbb{N}$. Formally, we define Φ from a map F as a map on *finite* lists, which can return the bottom element $\perp$, and if it returns $n \in \mathbb{N}$ on a finite list l then returns the same n on all extensions of l. If σ is infinite, then we set $\Phi(\sigma) = n$ if and only if $F(l) = n$ for some finite prefix l of σ; classically, F is called "total" if Φ returns some $n \in \mathbb{N}$ on all infinite lists. In order to make possible proofs with intuitionistic logic, we define totality through a bar instead and focus on the representation of Φ through a map F on finite sequences of words.

Definition 3.21 *1. The strict order $\prec$ on $\mathbb{N} \cup \{\perp\}$ is defined by $\perp \prec n$ for all $n \in \mathbb{N}$ with no others instances; $\preccurlyeq$ is the associated weak order.*

2. A PARTIAL CONTINUOUS FUNCTIONAL *is a map $F : \texttt{Fin}(\Sigma^*) \to \mathbb{N} \cup \{\perp\}$ which is monotone with respect to the prefix order $\leqslant$ and $\preccurlyeq$.*

[14] For any $l \in \texttt{Fin}(\Sigma^*)$, we define $O_l = \{m \in \texttt{Inf}(\Sigma^*) \mid l \leq m\}$; we then take on $\mathbb{N}$ the discrete topology, on $\texttt{Inf}(\Sigma^*)$ the topology generated by the sets O_l with $l \in \texttt{Fin}(\Sigma^*)$ and the function topology on $\texttt{Inf}(\Sigma^*) \to \mathbb{N} \cup \{\perp\}$.

3. *A partial continuous functional F is* (BAR-)TOTAL *if $F^{-1}(\mathbb{N})$ bars* $\texttt{Fin}(\Sigma^*)$.

4. *If F is a total continuous functional, then its* CANONICAL EXTENSION *to all $\sigma \in \texttt{Inf}(\Sigma^*)$ is given by $F(\sigma) = n$ if for some finite prefix l of σ we have $F(l) = n$.*[15]

Proposition 3.12 *If F is bar-total and $\sigma \in \texttt{Inf}(\Sigma^*)$, then $F(\sigma)$ exists, it is in $\mathbb{N}$ and it is unique.*

Proof From the fact that $F^{-1}(\mathbb{N})$ bars $\texttt{Fin}(\Sigma^*)$ and Lemma 3.11.4, every infinite list σ has some finite prefix l in the bar $F^{-1}(\mathbb{N})$, therefore $F(\sigma) = F(l) = n \in \mathbb{N}$ for some $n \in \mathbb{N}$. The value n is unique: if $F(\sigma) = F(l') = n' \in \mathbb{N}$ for another finite prefix of σ, then either $l \leqslant l'$ or $l' \leqslant l$, therefore $F(l) \preccurlyeq F(l')$ or $F(l') \preccurlyeq F(l)$, that is, $n \preccurlyeq n'$ or $n' \preccurlyeq n$. In both cases we conclude $n = n'$. □

Thus, if F is bar-total, then F is "total" with the usual classical definition: F returns some $n \in \mathbb{N}$ on all infinite lists. Classically, the reverse implication holds, but with intuitionistic logic bar-total is a stronger property.[16] From now on, by "total" we will always mean bar-total.

Let us fix any total functional F and any finite alphabet Σ. Higman's lemma for subsequences implies that for any infinite list σ on Σ^* there is some infinite sublist $\tau \sqsubseteq \sigma$ whose first $F(\tau)$ elements are in w.i. order. Classically, it is enough to take any infinite w.i. sublist τ of σ, then a finite prefix l of $F(\tau)$ elements. We call "F-long" the prefix of τ with $F(\tau)$-elements.

Informally speaking, this result means that we can provide infinite sublists τ having a w.i. prefix of any length, with the length $F(\tau)$ we require described by some bar-total continuous functional F applied to the very sublist τ we are defining. We can provide a proof within intuitionistic logic of this result as an immediate corollary of Higman's lemma for bars.

Corollary 3.4 (sublists with an F-long w.i. prefix) *Let Σ be a finite alphabet and $F\colon \texttt{Fin}(\Sigma^*) \to \mathbb{N} \cup \{\bot\}$ a bar-total continuous functional. Then every infinite sequence of words $\sigma \in \texttt{Inf}(\Sigma^*)$ has an infinite subsequence τ with the first $F(\tau)$ elements in w.i. order, i.e. such that τ has an F-long w.i. prefix.*

Proof Let $\phi = \mathrm{id}_I$, where $I = \Sigma^*$, $B_0 = \{\rho \in X \mid F(\rho) \in \mathbb{N}\}$ and set $X_0 = \texttt{Incr}(\phi, I)$ and $X = \texttt{Fin}(I)$. By the hypotheses on F, this B_0 bars X, and is

[15] The idea is that we can approximate an element of $\texttt{Inf}(\Sigma^*)$ considering all its initial segments which are elements of $\texttt{Fin}(\Sigma^*)$.

[16] We claim that there is some recursive functional F which is defined on all recursive sequences, but returning $\bot$ on some non-recursive sequence. The proof uses the folk-lore result there is some recursive tree, whose recursive branches are all finite, but having some infinite non-recursive branch.

upwards closed in X for the prefix order $\leqslant$; by the antimonotonicity of bars (Lemma 3.6.2), B_0 also bars $X_0 \subseteq X$. Let $B_1 = \{\rho \in B_0 \cap X_0 \mid \texttt{len}(\rho) \geqslant F(\rho)\}$.
CLAIM. B_1 bars X_0. To prove this, set $P = \{\rho \in X_0 \mid B_1 \text{ bars } \rho\}$. Then the Claim means $P = X_0$, which we show by bar induction with the bar B_0 for X_0. Since P is hereditary (Proposition 3.11), which is the induction step, we only need to verify the base case $B_0 \cap X_0 \subseteq P$. To this end, we show $\rho \in P$ for all $\rho \in B_0 \cap X_0$ by induction on $f(\rho) = \max(0, F(\rho) - \texttt{len}(\rho))$.

Case $f(\rho) = 0$: Then $F(\rho) \leqslant \texttt{len}(\rho)$ and thus $\rho \in B_1 \subseteq P$.

Case $f(\rho) = n+1$: For every $\rho' \in X_0$ with $\rho <_1 \rho'$ we have $\texttt{len}(\rho') = \texttt{len}(\rho)+1$, and $F(\rho) = F(\rho')$ by continuity, so $f(\rho') = n$. In addition, $\rho' \in B_0$ (because $\rho \in B_0$ and B_0 is upwards closed for $\leqslant \supseteq <_1$); whence $\rho' \in P$ by induction. As P is hereditary, $\rho \in P$ follows. *This ends the proof of the Claim.*

Now let $B = \{\rho \in X \mid \exists \eta \sqsubseteq \rho \, (\eta \in B_1)\}$. Then B is upwards closed for $\sqsubseteq$, i.e. closed by superlists; trivially, X is closed by sublists, and B bars $X_0 = X \cap \texttt{Incr}(\phi, I)$. The latter holds by the monotonicity of bars (Lemma 3.6.1); in fact B_1 bars X_0 by the Claim, and $B_1 \subseteq B$. All in all, Higman's lemma for bars (Theorem 3.7) applies, and yields that B bars X.

Now let $\sigma \in \texttt{Inf}(I)$. Since B bars X, the infinite list σ has a finite prefix $\sigma_0 \in B$. By definition of B, there is $\tau_0 \sqsubseteq \sigma_0$ such that $\tau_0 \in B_1$, which is to say that $\tau_0 \in X_0 = \texttt{Incr}(\phi, I)$, $F(\tau_0) \in \mathbb{N}$ and $\texttt{len}(\tau_0) \geqslant F(\tau_0)$. We extend τ_0 to any infinite sublist τ of σ and from $F(\tau_0) \in \mathbb{N}$, we get $F(\tau) = F(\tau_0) \leqslant \texttt{len}(\tau_0)$. Hence the first $F(\tau)$ entries of τ form a prefix of τ_0 and thus are in w.i. order. ☐

Example 3.4.1 *Let $\sigma \in \texttt{Inf}(\Sigma^*)$ be an infinite sequence of words over a finite alphabet Σ.*

1. *For all $k \in \mathbb{N}$ there is some w.i. length k subsequence of σ.*

2. *There are w.i. subsequences τ_1, τ_2, τ_3 of σ which have length $\texttt{len}(\tau_1(0)) + 1$, $\texttt{len}(\tau_2(0))^2 + 1$ and $2^{\texttt{len}(\tau_3(0))}$.*

Proof Apply Corollary 3.4 to the functionals defined by $F_0(\rho) = k$, $F_1(\rho) = \texttt{len}(\rho(0)) + 1$, $F_2(\rho) = \texttt{len}(\rho(0))^2 + 1$ and $F_3(\rho) = 2^{\texttt{len}(\rho(0))}$ where $\rho \in \texttt{Fin}(\Sigma^*)$, which are bar-total continuous. In fact, $F_0^{-1}(\mathbb{N}) = \texttt{Fin}(\Sigma^*)$ and $F_\nu^{-1}(\mathbb{N}) = \texttt{Fin}(\Sigma^*) \setminus \{\texttt{nil}\}$ for $\nu \in \{1,2,3\}$; whence $F_\nu^{-1}(\mathbb{N})$ bars $\texttt{Fin}(\Sigma^*)$ in all cases. ☐

The particular case $k = 2$ of Example 3.4.1 means that there are $i < j$ for which $\sigma(i) \sqsubseteq \sigma(j)$. This is Higman's lemma in its usual form.

3.4.5 A Constructive Proof of Higman's Lemma for Bars

In this section, we first prove some basic properties of wqo(bar): closure under finite products, finite unions and right-invertible morphisms. All these properties are classically true for the classically equivalent notion of wqo, see for example the original article by Higman [92]. Subsequently, we prove Higman's lemma for bars by induction on the finite language Σ. Namely, we assume that all Δ^* are wqo(bar), for all Δ smaller than Σ, in order to prove that Σ^* is a wqo(bar); the crucial step will be proving that the anticone of any $v \in \Sigma^*$ is a wqo(bar).

We start by giving two immediate examples, of a quasi-order which is wqo(bar) and a quasi-order which is not wqo(bar). For any set, $(I, =)$ is a quasi-order. Assume that Σ is any finite set, we can prove with intuitionistic logic that $(\Sigma, =)$ is a wqo(bar); whereas $(\mathbb{N}, =)$ is not.

Lemma 3.9 *Assume that Σ is any finite set. Then*

1. $(\Sigma, =)$ *is wqo(bar).*
2. $(\mathbb{N}, =)$ *is not wqo(bar).*

Proof

1. We assume that $X \subseteq \texttt{Fin}(I)$ is closed by I-sublist, that B is closed by I-superlists, and that B bars $X \cap \texttt{Incr}(=, \phi, I)$, in order to prove that B bars X. We argue by induction on Σ. Assume that $\Sigma = \{x\}$. Then all labelling (if any) are constantly equal to x, therefore are weakly increasing. We deduce that $X \cap \texttt{Incr}(=, \phi, I) = X$ and we conclude that B bars X. Assume that Σ has two or more elements; thus, $\Sigma = \Sigma_1 \cup \Sigma_2$ for some $\Sigma_1, \Sigma_2 \subset \Sigma$. Let $I_1 = \phi^{-1}(\Sigma_1)$ and $I_2 = \phi^{-1}(\Sigma_2)$. Then $I = I_1 \cup I_2$, and by antimonotonicity B bars $X \cap \texttt{Incr}(=, \phi, I_1)$ and B bars $X \cap \texttt{Incr}(=, \phi, I_2)$. By $X \subseteq \texttt{Fin}(I)$ closed by I-sublist, B is closed by I-superlists and Lemma 3.10 we conclude that B bars X.

2. $(\mathbb{N}, =)$ is a partial order. In order to prove that it is not a wqo(bar), we will provide some $X \subseteq \texttt{Fin}(I)$ closed by I-sublist, some B is closed by I-superlists, such that B bars $X \cap \texttt{Incr}(=, \phi, I)$ and B does not bars X. We choose $X =$ the set of non-repeating lists of length 1 words. X is closed by I-sublists and all its length ≥ 2 sublists are not increasing, because if $i \neq j$, then $\langle i \rangle \not\sqsubseteq \langle j \rangle$. Thus, $X \cap \texttt{Incr}(=, \phi, I)$ consists of all lists with 1 word of length 1. These lists are not comparable by $>_1$, therefore this set is trivially well-founded by $>_1$, and it is barred by $B = \emptyset$. However, B does not bar X, because the infinite list $\sigma = \langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \ldots$ in $\mathbb{N}$ does not intersect $\emptyset$. □

For comparison, if we use the notion of wqo(set), i.e. the existence of an infinite w.i. subsequence, point 1 above say that all infinite lists on a finite set Σ have an infinite constant sublist, while point 2 says there is an infinite list on $\mathbb{N}$ with no infinite constant sublist. Point 1 requires classical logic (this is why we avoid using the notion of wqo(set); Point 2 follows by taking the infinite list $0, 1, 2, 3, \ldots$.

In order to derive more basic properties of wqo(bar), we have first to find a constructive counterpart of the following classical property: given an infinite list σ in $\texttt{List}(I_1 \cup I_2)$, if σ_1 is the sublist obtained by restricting σ to the elements in I_1, and σ_2 is the sublist obtained by restricting σ to the elements in I_2, then either σ_1 is infinite or σ_2 is infinite. We propose to call this property the *Riffling Property for infinite lists*, because if I_1, I_2 are disjoint, then σ can be obtained from σ_1, σ_2 as when we riffle two decks of card in order to obtain a single deck of cards, while preserving the order we have in each deck. Riffling is not provable with intuitionistic logic, because we cannot decide whether we have an infinite sublist in $\texttt{Fin}(I_1)$ or in $\texttt{Fin}(I_2)$. In order to constructivise riffling, we prove a kind of contrapositive: if X is a set of lists and we bar with B the infinite I_1-lists in X and the infinite I_2-lists in X, then we bar with B the infinite $I_1 \cup I_2$-lists in X. When we state Riffling, we move from lists in X to sublists in X, and from sublists in the bar B to lists in the same B. Therefore Riffling requires two new assumptions, that B is closed by I-superlists and that X is closed by I-sublist; these are the same assumptions we have in the definition of wqo(bar).

Lemma 3.10 (Riffling for Bars) *Assume that the set X is closed by $I_1 \cup I_2$-sublists, and the set B is closed by $I_1 \cup I_2$-superlists. Then:*

$$B \text{ bars } X \cap \texttt{Fin}(I_1) \ \wedge\ B \text{ bars } X \cap \texttt{Fin}(I_2) \implies B \text{ bars } X \cap \texttt{Fin}(I_1 \cup I_2)$$

Proof We define an everywhere defined simulation relation V from $X \cap \texttt{Fin}(I_1 \cup I_2)$ with $>_1$ to $X \cap \texttt{Fin}(I_1) \times X \cap \texttt{Fin}(I_2)$ with the lexicographic product $>_1 \times >_1$. The thesis will follow from Lemma 3.5.1.

We require that $V(\sigma, \sigma_1, \sigma_2)$ selects for all σ some σ_1, σ_2 such that $\sigma_1, \sigma_2 \sqsubseteq \sigma$. The definition of V is by induction on σ. We set $V(\texttt{Nil}, \texttt{Nil}, \texttt{Nil})$, and if $\sigma\star\langle i\rangle \in X \cap \texttt{Fin}(I_1 \cup I_2)$ (hence $i \in I_1 \cup I_2$) and $V(\sigma, \sigma_1, \sigma_2)$, then we set: $V(\sigma\star\langle i\rangle, \sigma_1\star\langle i\rangle, \sigma_2)$ if $i \in I_1$, and $V(\sigma\star\langle i\rangle, \sigma_1, \sigma_2\star\langle i\rangle)$ if $i \in I_2$. By inductive hypothesis we have $\sigma_1, \sigma_2 \sqsubseteq \sigma$ and $\sigma_1 \in X \cap \texttt{Fin}(I_1)$, $\sigma_2 \in X \cap \texttt{Fin}(I_2)$. We deduce $\sigma_1\star\langle i\rangle, \sigma_2\star\langle i\rangle \sqsubseteq \sigma\star\langle i\rangle \in X$, therefore $\sigma_1\star\langle i\rangle, \sigma_2\star\langle i\rangle \in X$ by closure of X under $I_1 \cup I_2$-sublist. Furthermore, if $i \in I_1$, then $\sigma_1\star\langle i\rangle \in \texttt{Fin}(I_1)$, and if $i \in I_2$, then $\sigma_2\star\langle i\rangle \in \texttt{Fin}(I_2)$.

Therefore V is a well-defined relation from $X \cap \texttt{Fin}(I_1 \cup I_2)$ to $X \cap \texttt{Fin}(I_1) \times X \cap \texttt{Fin}(I_2)$, is a simulation between $>_1$ and the lexicographic product $>_1 \times >_1$ by construction and is everywhere defined by construction.

Assume that B is a bar for $X \cap \texttt{Fin}(I_1)$ and for $X \cap \texttt{Fin}(I_2)$. By Lemma 3.7, the set C of pairs of lists in $X \cap \texttt{Fin}(I_1) \times X \cap \texttt{Fin}(I_2)$ having at least one list in B is a bar for $X \cap \texttt{Fin}(I_1) \times X \cap \texttt{Fin}(I_2)$. By Lemma 3.5.1, $V^{-1}(C)$ is a bar for $X \cap \texttt{Fin}(I_1 \cup I_2)$. By monotonicity (Lemma 3.6.1), in order to prove that B bars $X \cap \texttt{Fin}(I_1 \cup I_2)$, it is enough to prove that $B \supseteq V^{-1}(C)$. For, assume that $\langle \sigma_1, \sigma_2 \rangle \in C$, that is, $\sigma_1 \in B$ or $\sigma_2 \in B$ and $V(\sigma, \sigma_1, \sigma_2)$, in order to prove that $\sigma \in B$. From $V(\sigma, \sigma_1, \sigma_2)$, we deduce $\sigma_1, \sigma_2 \sqsubseteq \sigma$ and conclude that $\sigma \in B$ from $\sigma_1 \in B$ or $\sigma_2 \in B$ and closure of B under $I_1 \cup I_2$-superlists. □

From the Riffling Property for Bars we deduce, within intuitionistic logic, that wqo(bar) are closed under binary compatible union.

Lemma 3.11 (Compatible union of wqo(bar)) *If $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$ are wqo(bar), $(P \cup Q, \leqslant_3)$ is a quasi-order and $\leqslant_P,\ \leqslant_Q \subseteq \leqslant_3$, then $(P \cup Q, \leqslant_3)$ is a wqo(bar).*

Proof Assume that $\phi : I \to P \cup Q$ and $X \subseteq \texttt{Fin}(I)$, X closed by I-sublists, B closed by I-superlists and B bars $X \cap \texttt{Incr}(\leq_3, \phi, I)$, in order to prove that B bars X. Let $I_1 = \phi^{-1}(P)$ and $I_2 = \phi^{-1}(Q)$. Then $I = I_1 \cup I_2$ and $X = X \cap \texttt{Fin}(I) = X \cap \texttt{Fin}(I_1 \cup I_2)$. Thus, it is enough to prove that B bars $X \cap \texttt{Fin}(I_1 \cup I_2)$. By X closed by I-sublists, B closed by I-superlists and Lemma 3.10 in order to prove that B bars $X \cap \texttt{Fin}(I_1 \cup I_2)$ it is enough to prove that B bars $X \cap \texttt{Fin}(I_1)$ and B bars $X \cap \texttt{Fin}(I_2)$. We assumed that $P, \leq_P$ and $Q, \leq_Q$ are wqo(bar), therefore it is enough to prove that B bars $X \cap \texttt{Fin}(I_1) \cap \texttt{Incr}(\leq_P, \phi, I_1)$ and B bars $X \cap \texttt{Fin}(I_2) \cap \texttt{Incr}(\leq_Q, \phi, I_2)$. These two sets are equal to $X \cap \texttt{Incr}(\leq_P, \phi, I_1)$ and to $X \cap \texttt{Incr}(\leq_Q, \phi, I_2)$, respectively. From $\leq_P, \leq_Q \subseteq \leq_3$, we deduce that they are both subsets of $X \cap \texttt{Incr}(\leq_3, \phi, I)$; therefore the thesis follows by B bars $X \cap \texttt{Incr}(\leq_3, \phi, I)$ and antimonotonicity of bars. □

The next step is to prove using intuitionistic logic that wqo(bar) are closed by componentwise product.

Lemma 3.12 (Componentwise product of wqo(bar)) *Assume that $(P, \leqslant_P)$ and $(Q, \leqslant_Q)$ are wqo(bar), then $(P \times Q, \leqslant_P \times \leqslant_Q)$ with the componentwise order is a wqo(bar).*

Proof Assume that $\phi : I \to P \times Q$ and $X \subseteq \texttt{Fin}(I)$, X closed by I-sublists, B closed by I-superlists and B bars $X \cap \texttt{Incr}(\leq_P \times \leq_Q, \phi, I)$, in order to prove that B bars X. Let $\phi_1 = \pi_1 \phi$ and $\phi_2 = \pi_2 \phi$. Then $\phi_1 : I \to P$, $\phi_2 : I \to Q$ and for all $i, j \in I$ we have $\phi(i) \leq \phi(j)$ if and only if $\phi_1(i) \leq_P \phi_1(j)$ and $\phi_2(i) \leq_Q \phi_2(j)$. We deduce that an I-list is ϕ-increasing if and only if it is ϕ_1-increasing and ϕ_2-increasing: that is, $\texttt{Incr}(\leq_P \times \leq_Q, \phi, I) = \texttt{Incr}(\leq_P, \phi_1, I) \cap \texttt{Incr}(\leq_Q, \phi_2, I)$. We deduce that B bars $X \cap \texttt{Incr}(\leq_P, \phi_1, I) \cap \texttt{Incr}(\leq_Q, \phi_2, I)$. From the assumption that $(Q, \leq_Q)$ is a wqo(bar), we deduce that B bars $X \cap \texttt{Incr}(\leq_P, \phi_1, I)$ and, from the assumption that $(P, \leq_P)$ is a wqo(bar), we conclude that B bars X, as wished. □

The last preliminary step is to prove constructively that wqo(bar)'s are closed by right-invertible morphisms. Again, this property is easily proved for the classical definition of wqo. Let assume we have a morphism $f\colon P \to Q$ with right inverse $g\colon Q \to P$ (i.e., $fg = \mathtt{id}_Q$) and $(P, \leqslant_P)$ is a wqo, then any infinite list $\sigma\colon \mathbb{N} \to Q$ is mapped by g into an infinite list $g\sigma\colon \mathbb{N} \to P$, which has an infinite w.i. sublist $\tau\colon \mathbb{N} \to P$, mapped by f into an infinite w.i. list $f\tau\colon \mathbb{N} \to Q$. From τ sublist of $g\sigma$ we deduce that $f\tau$ is a sublist of $fg\sigma$. From $fg\sigma = \sigma$ we conclude that $f\tau$ is an infinite w.i. sublist of σ. Using the notion of wqo(bar), we can provide an intuitionistic proof of the same result.

Lemma 3.13 (right-invertible morphism on a wqo(bar)) *Assume that* $(P, \leqslant_P)$ *is a wqo(bar),* $(Q, \leqslant_Q)$ *is a quasi-order and* $f\colon P \to Q$ *is a morphism with right inverse* g[17]*; then* $(Q, \leqslant_Q)$ *is a wqo(bar).*

Proof Assume that $\phi : I \to Q$ and $X \subseteq \mathtt{Fin}(I)$, X closed by I-sublists, B closed by I-superlists and B bars $X \cap \mathtt{Incr}(\leq_Q, \phi, I)$, in order to prove that B bars X. Define $\psi = g\phi : I \to P$. Then $f\psi = fg\phi = \phi$ because we assumed that $fg = \mathtt{id}_Q$. We first check that any list ψ-increasing for $\leq_Q$ is ϕ-increasing for $\leq_P$. Indeed, for all $i, j \in I$, if $\psi(i) \leq_P \psi(j)$, then $f\psi(i) \leq_Q f\psi(j)$ since f is increasing. From f morphism we deduce that $\phi(i) \leq_Q \phi(j)$. Then $\mathtt{Incr}(\leq_P, \psi, I) \subseteq \mathtt{Incr}(\leq_Q, \phi, I)$, and therefore $X \cap \mathtt{Incr}(\leq_P, \psi, I) \subseteq X \cap \mathtt{Incr}(\leq_Q, \phi, I)$. From the assumption B bars $X \cap \mathtt{Incr}(\leq_Q, \phi, I)$ and antimonotonicity, we deduce that B bars $X \cap \mathtt{Incr}(\leq_P, \psi, I)$ and, from the assumption that $P, \leq_P$ is a wqo(bar), we conclude that B bars X, as wished. □

Finally, we fix any labelling $\phi\colon I \to \Sigma^*$, and we assume that Δ^* is a wqo(bar) for all $\Delta \subset \Sigma$; from this assumptions, we prove that the anticone of any $v \in \Sigma^*$ is a wqo(bar). This is a crucial step in the proof of Higman's lemma for bars.

Lemma 3.14 (Slices and Anticones of a Word) *Assume that* Σ *is a finite alphabet and that, for all* $\Delta \subset \Sigma$*, the partial order* Δ^* *is a wqo(bar). Let* $v = c_1 \ldots c_k \in \Sigma^*$*, then:*

1. $\mathtt{Slice}_\Sigma(v)$*, the slice of* v*, is a wqo(bar).*
2. $\not\sqsupseteq_\Sigma(v)$*, the anticone of* v*, is a wqo(bar).*

Proof

1. Let $\Sigma_i = \Sigma \setminus \{c_i\}$ for $i = 1, \ldots, k$. We proved in Lemma 3.3 that there is a right-invertible morphism $\alpha : \Sigma_1^* \times \ldots \times \Sigma_k^* \to \mathtt{Slice}_\Sigma(v)$. By assumption, all Σ_i^* are wqo(bar) and, by Lemma 3.12, the componentwise product $\Sigma_1^* \times \ldots \times \Sigma_k^*$ is a wqo(bar). By Lemma 3.13 and α right-invertible morphism, we conclude that $\mathtt{Slice}_\Sigma(v)$ is a wqo(bar).

[17] Observe that g does not need to be a morphism.

2. By Lemma 3.4, $\not\sqsupseteq_\Sigma(v)$ is the finite union of all slices $\texttt{Slice}_\Sigma(v')$ with $v' \leq v$. We proved in point 1 above that all $\texttt{Slice}_\Sigma(v')$ are wqo's with respect to the subword relation. By closure under finite unions (Lemma 3.11), $\not\sqsupseteq_\Sigma(v)$ is a wqo(bar) with respect to the same subword relation. □

Suppose that $\phi\colon I \to P = \Sigma^*$ labels an arbitrary set I with words over a finite alphabet Σ, we introduce the last ingredient needed in the proof of Higman's lemma for bars. We extract from each finite list l with labels $\langle w_0, \ldots, w_{p-1}\rangle$ two disjoint sublists:

1. some ϕ-w.i. sublist $\texttt{Lex}(l,\phi)$ of l, with labels $w_{i_0} \sqsubseteq \ldots \sqsubseteq w_{i_{n-1}}$. $\texttt{Lex}(l,\phi)$ is obtained by selecting each time *the first element making the sublist ϕ-w.i.*;
2. the suffix $\texttt{Suff}(l,\phi)$ of l, with labels $\langle w_m, \ldots, w_{p-1}\rangle$ of l, such that $m = i_{n-1}+1$, and that $w_{i_{n-1}} \not\sqsubseteq w_m, \ldots, w_{p-1}$; if this is not possible, then $\texttt{Suff}(l,\phi)$ is the empty list.

In our terminology, the elements of $\texttt{Suff}(l,\phi)$ are in the anticone of $w_{i_{n-1}}$, where $w_{i_{n-1}}$ is the last element of $\texttt{Lex}(l,\phi)$; we will prove Higman's lemma for bars by bar induction on such pair of lists. The formal definition of the two sublists $\texttt{Lex}, \texttt{Suff}$, which used two auxiliary lists $\texttt{lex}, \texttt{suff}$, runs as follows.

Definition 3.22 (Decomposition of a list) *Assume l is any finite list on I, labelled by a map $\phi\colon I \to P = \Sigma^*$. Suppose $\phi l = \langle w_0, \ldots, w_{p-1}\rangle$ is the list of labels of l. By induction on l, we define $\texttt{lex}(l,\phi)$, $\texttt{suff}(l,\phi)$.*

1. *We define* $\texttt{lex}(\texttt{Nil},\phi) = \texttt{suff}(\texttt{Nil},\phi) = \texttt{Nil}$ *and* $\texttt{lex}(\langle i\rangle,\phi) = \langle 0\rangle$, $\texttt{suff}(\langle i\rangle,\phi) = \texttt{Nil}$.
2. *Suppose* $\texttt{len}(l) = p \geq 1$, $\texttt{lex}(l,\phi) = \langle i_0 \ldots, i_{n-1}\rangle$ *(an integer list) and* $x \in I$. *We define the clause for* $l\star\langle x\rangle$ *by cases on the condition: "*$w_{i_{n-1}} \sqsubseteq \phi(x)$*".*
   - (a) Assume $w_{i_{n-1}} \sqsubseteq \phi(x)$. *Then we set* $\texttt{lex}(l\star\langle x\rangle,\phi) = \texttt{lex}(l,\phi)\star\langle p\rangle$ *(we add the index p of x to* $\texttt{lex}$*) and* $\texttt{suff}(l\star\langle x\rangle,\phi) = \texttt{Nil}$ *(we reset* $\texttt{suff}$ *to* $\texttt{Nil}$*).*
   - (b) Assume $w_{i_{n-1}} \not\sqsubseteq \phi(x)$. *Then we set* $\texttt{lex}(l\star\langle x\rangle,\phi) = \texttt{lex}(l,\phi)$ *(*$\texttt{lex}$ *stays the same) and* $\texttt{suff}(l\star\langle x\rangle,\phi) = \texttt{suff}(l,\phi)\star\langle p\rangle$ *(we add the index p of x to* $\texttt{suff}$*).*

Finally, we define $\texttt{Lex}, \texttt{Suff}$*, the maps with capital* $\texttt{L}, \texttt{S}$*, by:* $\texttt{Lex}(l,\phi) = l\texttt{lex}(l,\phi)$ *and* $\texttt{Suff}(l,\phi) = l\texttt{suff}(l,\phi)$*.*

A (crucial) example: let $I = \Sigma^*$, $\phi = \mathtt{id}$ (labelling ϕl and list l coincide), and $l = \langle w_0, w_1, w_2, w_3, w_4 \rangle$, with

$$w_0 = a, \quad w_1 = ab, \quad w_2 = abb, \quad w_3 = bb, \text{ and } w_4 = bbb$$

According to Def.3.22 we obtain:

1. for $m = \mathtt{nil}$: $\mathtt{lex}(m, \phi) = \mathtt{nil}$.
2. for $m = \langle w_0 \rangle$: $\mathtt{lex}(m, \phi) =$ the index 0 of w_0
3. for $m = \langle w_0, w_1 \rangle$: $\mathtt{lex}(m, \phi) =$ the indexes $0, 1$ of w_0, w_1
4. for $m = \langle w_0, w_1, w_2 \rangle$: $\mathtt{lex}(m, \phi) =$ the indexes $0, 1, 2$ of w_0, w_1, w_2

When m increases to $m = \langle w_0, w_1, w_2, w_3 \rangle$, the new word w_3 added to m is discarded in $\mathtt{lex}(m, \phi)$. Indeed, we have $w_2 \not\sqsubseteq w_3, w_4$, therefore if $m = \langle w_0, w_1, w_2, w_3 \rangle$ then $\mathtt{lex}(m, \phi)$ is again equal to the indexes $0, 1, 2$ of w_0, w_1, w_2. The same when $m = \langle w_0, w_1, w_2, w_3, w_4 \rangle$: the new word w_4 added to m is again discarded, and we still have $\mathtt{lex}(m, \phi) =$ the integer list $0, 1, 2$.

The indexes of the discarded words are piled up in $\mathtt{suff}$. The first three values of $\mathtt{suff}(m, \phi)$ are: $\mathtt{nil}$, $\mathtt{nil}$, $\mathtt{nil}$. From $w_2 \not\sqsubseteq w_3, w_4$, we deduce the following values for $\mathtt{suff}$: $\mathtt{suff}(m, \phi) =$ the integer list whose only element is 3, and $\mathtt{suff}(m, \phi) =$ the integer list $3, 4$.

The outputs of $\mathtt{Lex}(m, \phi)$ and $\mathtt{Suff}(m, \phi)$ (with capital $\mathtt{L}, \mathtt{S}$) are the same, except that we take words instead of indexes of words. For the same values of m we obtain for $\mathtt{Lex}(m, \phi)$: $\mathtt{nil}$, $\langle w_0 \rangle$, $\langle w_0, w_1 \rangle$, $\langle w_0, w_1, w_2 \rangle$, then again $\langle w_0, w_1, w_2 \rangle$ and again $\langle w_0, w_1, w_2 \rangle$.

The words w_3, w_4 discarded from $\mathtt{Lex}(m, \phi)$ are piled up in $\mathtt{Suff}(m, \phi)$. Indeed, according to Def.3.22 we obtain for $\mathtt{Suff}(m, \phi)$: $\mathtt{nil}$, $\mathtt{nil}$, $\mathtt{nil}$, then $\langle w_3 \rangle$ and $\langle w_3, w_4 \rangle$. As a last example, let us suppose we add $w_5 = abb$ to m. In this case $w_2 \sqsubseteq w_5$, then w_5 is added to $\mathtt{Lex}(l, \phi)$ and we obtain $\mathtt{Lex}(l \star \langle w_5 \rangle, \phi) = \langle w_0 w_1 w_2 w_5 \rangle$. Instead, $\mathtt{Suff}$ is reset to $\mathtt{nil}$: according to Def. 3.22, we obtain $\mathtt{Suff}(l \star \langle w_5 \rangle, \phi) = \mathtt{nil}$.

The name we choose for the map $\mathtt{lex}$ comes from the fact that $f = \mathtt{lex}(l, \phi)$ is the minimum in the lexicographic ordering of all integer lists such that lf is a ϕ-w.i. sublist of l. However, we do not need a proof of this feature of f and we do not include further details.

The following properties of $f = \mathtt{lex}(l, \phi)$ and $g = \mathtt{suff}(l, \phi)$ are immediate from the definition. First, that $lf \in \mathtt{Incr}(\phi, I)$ for all $l \in \mathtt{Fin}(I)$. Second, if $l > \mathtt{Nil}$, $g = \mathtt{suff}(l, \phi)$, that lg is equal to the suffix of l after the last element of lf, and that lg is in the anticone of the last element of lf. Both properties can be proved by induction on l.

Finally, we prove Theorem 3.7 which for clarity we restate.

Theorem 3.8 (Higman's lemma for bars) *If Σ is any finite language, then Σ^* is a wqo(bar).*

Proof We argue by principal induction on Σ. If $\Sigma = \emptyset$ then $\Sigma^* = \texttt{Nil}$ and Σ^* is a wqo(bar) by Lemma 3.9. Assume Σ has some element and that for all $\Delta \subset \Sigma$ the partial order Δ^* is a wqo(bar), in order to prove that Σ^* is a wqo(bar). We assume that I is a set, $\phi : I \to \Sigma^*$ any labelling of elements of I by words, $X \subseteq \texttt{Fin}(I)$ is a set of finite I-lists closed by I-sublists, B is a set of finite I-lists closed by I-superlists, and B bars $X \cap \texttt{Incr}(\phi, I)$; our goal is to prove that B bars X.

Let $\texttt{Lex}, \texttt{Suff}$ be as in Def. 3.22, and $\sigma, l \in X$. We define a map $f(\sigma) = \texttt{Lex}(\sigma) \times \texttt{Suff}(\sigma)$ proving that $f : X \to Y$ is a morphism, where $Y := \Sigma_{l \in X \cap \texttt{Incr}(\phi,I)} Y_l$, for a family of sets $\{Y_l \mid l \in X \cap \texttt{Incr}(\phi, I)\}$ we are going to define. We will prove that Y is barred by some D such that $f^{-1}(D) \subseteq B$; "B bars X" follows from the Simulation Lemma (3.5) and monotonicity.

If $l = \texttt{Nil}$, we set $Y_{\texttt{Nil}} = \{\texttt{Nil}\}$. If $l \neq \texttt{Nil}$, we define each set Y_l as the set of all I-lists in X ϕ-labeled by words which are *not* super-words of (which are in the anticone of) the last word of ϕl. We formally define Y_l as follows. Let v be *the last element of* ϕl: then we set $Y_l := \texttt{Fin}(\phi^{-1}(\not\sqsupseteq_\Sigma(v))) \cap X$.

By definition of $\texttt{Lex}$, $\texttt{Suff}$ and the closure of X by I-sublists, we have $\texttt{Lex}(\sigma) \in X \cap \texttt{Incr}(\phi, I)$ and $\texttt{Suff}(\sigma) \in Y_l$. Moreover, by definition of $\texttt{Lex}$ and $\texttt{Suff}$, whenever we add one element i to l, either we add the same i to $\texttt{Lex}(\sigma, \phi)$, or $\texttt{Lex}(\sigma, \phi)$ stays the same and we add i to $\texttt{Suff}(\sigma, \phi)$. Thus, f is a morphism from $(X, >_1)$ to $\Sigma_{l \in X \cap \texttt{Incr}(\phi,I)} Y_l$ with relation the lexicographic product $>_1 \times >_1$. By Lemma 3.14.2 (Slices and Anticones), $\not\sqsupseteq_\Sigma(v)$ is a wqo(bar), since B bars $X \cap \texttt{Incr}(\phi, I)$ by assumption; then B bars the subset $\texttt{Fin}(\phi^{-1}(\not\sqsupseteq_\Sigma(v))) \cap X \cap \texttt{Incr}(\phi, I)$ by antimonotonicity. $\not\sqsupseteq_\Sigma(v)$ is a wqo(bar), therefore B bars $\texttt{Fin}(\phi^{-1}(\not\sqsupseteq_\Sigma(v))) \cap X$, which is Y_l. Let D be the set of pairs (l, m) such that $l \in B$ or $m \in B$. By Lemma 3.7 (Lexicographic Product), D bars $Y = \Sigma_{l \in X \cap \texttt{Incr}(\phi,I)} Y_l$, $>_1 \times >_1$. By Simulation Lemma (3.5) we deduce that $f^{-1}(D)$ bars X. In order to prove that B bars X, by monotonicity it is enough to prove that $f^{-1}(D) \subseteq B$.

Assume that $\sigma \in f^{-1}(D)$, then $f(\sigma) = \texttt{Lex}(\sigma) \times \texttt{Suff}(\sigma) \in D$, and by definition of D, we deduce that $\texttt{Lex}(\sigma) \in B$ or $\texttt{Suff}(\sigma) \in B$. From $\texttt{Lex}(\sigma), \texttt{Suff}(\sigma) \sqsubseteq \sigma$ and closure of B by I-superlists, we conclude that $\sigma \in B$, as wished. □

Future Work

Higman's lemma for sequences says that over a finite alphabet every infinite sequence of words has an infinite weakly increasing subsequence, and is inherently nonconstructive. As a constructive alternative we now have put forward what we call Higman's lemma for bars: over a finite alphabet, every bar for the weakly increasing finite lists of words which is closed by super-lists is already a bar for *all* finite lists. In particular, for every total continuous functional, every infinite sequence of such words has a weakly increasing finite sublist of length bounded below by the functional. We also proved the common form of Higman's lemma: the words over a finite alphabet form a well quasi-order, for our notion of well quasi-order. As we work as much as possible in settings more abstract than the one of words over a finite alphabet, we prepare for a constructive theory of well (quasi-)order, and, more in general, for a constructive version of classical theories dealing with Π^1_2-statements.

Chapter 4

Phase Transitions in Arithmetical Provability

In this Chapter, we treats a different topic than well quasi-orders, but still connected to proof theory: Phase Transitions in Proof Theory. In general terms, phase transition is a type of behavior wherein small changes of a parameter of a system cause dramatic shifts in some globally observed behavior of the system itself, such shifts being usually marked by a sharp 'threshold point'. (An everyday life example of such thresholds are ice melting and water boiling temperatures.) This kind of phenomena nowadays occurs throughout many mathematical and computational disciplines: statistical physics, evolutionary graph theory, percolation theory, computational complexity, artificial intelligence etc.

In the context of logic and proof theory the phase transition phenomenon can be exposed in the following way. Consider a familiar (presumably consistent) arithmetical theory T and a sufficiently complicated arithmetical assertion $A(r)$ depending on a real parameter $r>0$. Let us assume that $A(r)$ is true, T-provable for small values of r, T-unprovable for large values of r, and that A is monotone with respect to T-unprovability; namely the transition from provability to unprovability happens just once. We are interested in classifying the exact threshold point t at which the phase transition from T-provability to T-unprovability happens; that is, we wish to find t such that $A(r)$ is provable (unprovable) in T for $r<t$ $(r>t)$.

A concrete example of such behavior is given by Friedman's miniaturization of Kruskal theorem FKT [170] and PA. Treating infinite sequences of trees, Kruskal's theorem is a second-order statement; but, restricting the thesis to arbitrary long finite sequences allows the following first-order equivalent version, where $|\cdot|$ denotes the number of nodes and $\preccurlyeq$ tree embeddability:

Theorem 4.1 *(FKT) For every K, there is a number N such that for all finite sequences $T^1, \dots, T^N$ of finite trees with $|T^i| \leqslant K + i$ for all $i \leqslant N$, there exist* *indexes* i, j *such that* $1 \leqslant i < j \leqslant N$ *and* $T^i \preccurlyeq T^j$.

Theorem 4.1 is true, but unprovable over PA. A parametrized version of FKT is also possible.

Theorem 4.2 *(FKT_r) For every* K*, there is a number* N *such that for all finite sequences* $T^1, \ldots, T^N$ *of finite trees with* $|T^i| \leqslant K + r \cdot \log_2(i)$ *for all* $i \leqslant N$*, there exist indexes* i, j *such that* $1 \leqslant i < j \leqslant N$ *and* $T^i \preccurlyeq T^j$.

For every $r \geqslant 0$ this theorem is true, but even for $r = 4$ it is not provable in PA; the threshold value ρ for the phase transition of this logarithmic version (à la [110]) has approximate value $0.639578\ldots$ (which is currently not known to be rational, irrational, algebraic or transcendental) [189].

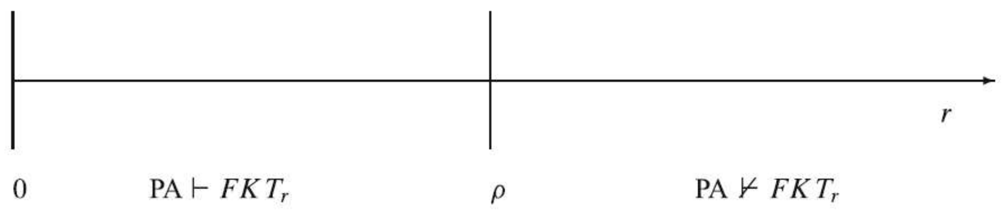


Figure 4.1: Phase transition for FKT_r [118].

A generalization of such phenomenon is given by a statement A_f parametrized by a number-theoretic function f (assumed to be elementary recursive) instead of a number. In this case, we assume A_f to be true for every f and to be provable in PA for a very slow growing f; moreover, and similarly as before, we assume that if A_f is unprovable in PA and g eventually majorizes f, then also A_g is unprovable in PA, with A_f unprovable for a reasonably fast growing function f. The phase transition threshold would then be given, not by a number, but by a growing rate.

Although it is a relatively recent topic, the literature on phase transitions in logic is already quite rich: Carlucci, Lee and Weiermann considered regressive Ramsey numbers and functions [39, 40]; Ramsey numbers have been treated also by Kojman et al. [105] and Weiermann and Van Hoof [192]; De Smet and Weiermann studied phase transitions related to weakly increasing sequences [56] and to the pigeonhole principle [57]; even Higman-style well-partial-orderings have been scrutinized in a paper by Gordeev and Weiermann [86]; finally, for a survey of these topics we refer the reader to [85] and [190].

Phase transitions over PA with respect to a function parameter are also the cases treated in this chapter. We consider such phase transitions for the Kirby Paris

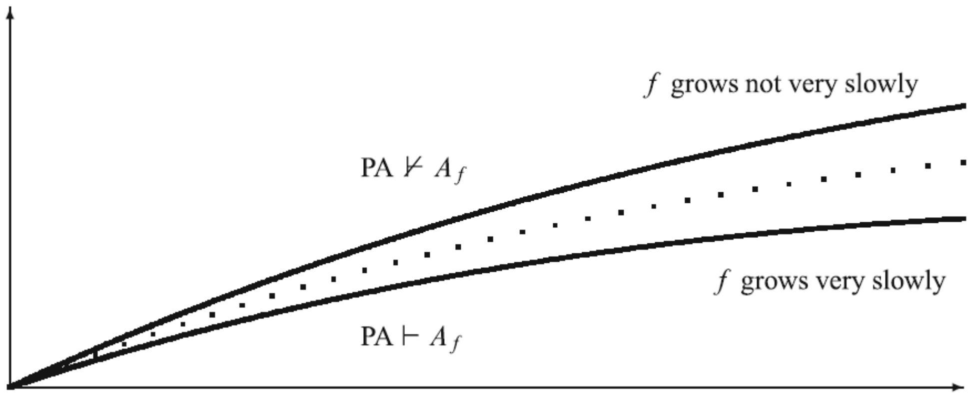


Figure 4.2: Phase transition for A_f [118].

principle about a generalized version of Goodstein sequences and Hydra games, and for a transfinite extension of Ackermaniann hierarchy; in both cases, the threshold is given by a suitable inverse function obtained from the Hardy hierarchy H_α of fast growing functions. Hardy functions H_α for $\alpha \leqslant \varepsilon_0$ classify the provably recursive, i.e. provably total, functions of PA [74] and this will be a key point in our analysis.

The novel content of this chapter, based on a joint paper with Andreas Weiermann which has not yet been published, generalizes the results of two previous articles, respectively due to Meskens and Weiermann [118] and Omri and Weiermann [130], treating the same topics. In both cases, we substitute the original successor function with the iterations of a strictly increasing primitive recursive function g satisfying the condition $g(x) \geqslant x+1$; more precisely, the steps of the Hydra Game, originally of type $\alpha_{f,i+1} = \alpha_{f,i}[1+f(i)]$, are now of the form $\alpha^{f,g}_{i+1} = \alpha^{f,g}_{i}[1+f(g^{i-1}(1))]$, while the steps of Goodstein sequences are changed from $m_{f,i+1} = m_{f,i}\,(1+f(i) \mapsto 1+f(i+1)) - 1$ to $m^{f,g}_{i+1} = m^{f,g}_{i}\,(1+f(g^{i-1}(1)) \mapsto 1+f(g^{i}(1))) - 1$. The new phase transition thresholds incorporate the starting function g. In the case of the Ackerman hierarchy, we consider also a transfinite extension. Concerning the structure, the first two sections extend Meskens' and Weiermann's achievements following the general scheme of their article and enlightening the needed modifications; the third and last section, instead, applies the results obtained in Sec. 4.2 to generalize and transfinitely expand the results obtained by Omri and Weiermann. Finally, differently from Chapter 2 and Chapter 3, here we work in classical mathematics, namely classical logic with possibly the axiom of choice.

4.1 Preliminaries

In this section we prepare the stage for the subsequent results recalling, and adapting when needed, proofs and notations of [118] to our case. For what concerns the standard association between the Hydras and ordinal numbers, we refer to the original article by Kirby and Paris [101] or to Buchholz's seminal paper [34]; moreover, we assume that hydras are represented by ordinals in Cantor normal form. Within this codification, a step in the Hydra game for hydra α at the move x corresponds in stepping down from α to $\alpha[x]$ with respect to the standard system of fundamental sequences for the ordinals below ε_0. Finally, if not mentioned otherwise, we adopt the following notation: natural numbers are denoted by Latin letters, big or small; ordinals smaller than ε_0, which are the only ones considered here, by small Greek letters, with λ reserved for limit ordinals and Lim denoting the set of limit ordinals below ε_0.

4.1.1 Main Definitions and Properties

We start with some standard notations regarding ordinals.

Definition 4.1 *For $0 < \alpha, \beta, \gamma < \varepsilon_0$ and $\omega \geqslant j \geqslant i \geqslant 2$ define:*

1. $\alpha =_{NF} \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ *if* $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ *and* $\alpha_1 \geqslant \ldots \geqslant \alpha_n$*;*

2. $NF(\beta, \gamma)$ *if* $\beta =_{NF} \omega^{\beta_1} + \cdots + \omega^{\beta_m}, \gamma =_{NF} \omega^{\gamma_1} + \cdots + \omega^{\gamma_n}$ *and* $\beta_m \geqslant \gamma_1$*;*

3. $\alpha =_{CNF} \omega^{\alpha_1} m_1 + \cdots + \omega^{\alpha_n} m_n$ *if* $\alpha = \omega^{\alpha_1} m_1 + \cdots + \omega^{\alpha_n} m_n, \alpha_1 > \cdots > \alpha_n$ *and* $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0\}$*;*

4. *if* $\alpha =_{CNF} \omega^{\alpha_1} m_1 + \cdots + \omega^{\alpha_n} m_n$*, then we define the* MAXIMAL COEFFICIENT *as* $mc(\alpha) := \max\{mc(\alpha_i), m_i \mid i = 1, \ldots, n\}$ *with* $mc(0) := 0$*.*

Working repeatedly with exponential towers and iterated logarithms it is practical to fix the following notations.

Definition 4.2 *For $\alpha, \beta < \varepsilon_0$ and nonnegative integers h, we define:*

1. $\alpha_0(\beta) := \beta, \alpha_{h+1}(\beta) := \alpha^{\alpha_h(\beta)}; \omega_h := \omega_h(1), 2_h := 2_h(1)$*.*

2. $|0| := 1, |i| := \lceil \log_2(i+1) \rceil$ *if* $i > 0$*;* $|i|_h := i$ *if* $h = 0$*,* $|i|_{h+1} := ||i|_h|$*.*

With this definitions, $|i|$ is the binary length of i and $|i|_h$ stands for the h-iterated binary length function.

We briefly recall also the standard assignment of fundamental sequences for ordinals below ε_0.

Definition 4.3 *If $\alpha \in \{0,1\}$, then $\alpha[k] := 0$; if $1 < \alpha < \varepsilon_0$, then write $\alpha =_{NF} \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}$ and define*

$$\alpha[k] := \begin{cases} \omega^{\alpha_1} + \cdots + \omega^{\alpha_{n-1}} & \text{if } \alpha_n = 0, \\ \omega^{\alpha_1} + \cdots + \omega^{\alpha_n - 1} \cdot (k+1) & \text{if } \alpha_n \notin Lim, \\ \omega^{\alpha_1} + \cdots + \omega^{\alpha_n[k]} & \text{if } \alpha_n \in Lim. \end{cases}$$

Lastly, put $\varepsilon_0[k] := \omega_k$.

In this definition, we define $\omega^{\alpha+1}[k] = \omega^\alpha \cdot (k+1)$, instead of the maybe more intuitive $\omega^{\alpha+1}[k] = \omega^\alpha \cdot k$, to guarantee the so-called Bachmann condition [36].

Finally, in order to concisely express Goodstein sequences, we adopt the following notation.

Definition 4.4 *Let $a \in \mathbb{N}$ and $2 \leqslant i \leqslant j$. If $a = i^{a_1} m_1 + \cdots + i^{a_n} m_n$ with $a_1 > \cdots > a_n$ and $i > m_k > 0$ for $k \in \{1, \ldots, n\}$, then $a(i \mapsto j) := j^{a_1(i \mapsto j)} m_1 + \ldots j^{a_n(i \mapsto j)} m_n$, else $a(i \mapsto j) := a$.*

For the rest of this chapter, let $f : \mathbb{N} \to \mathbb{N}$ denote a weakly increasing elementary recursive function and $g : \mathbb{N} \to \mathbb{N}$ a strictly increasing elementary recursive function such that $g(i) \geqslant i + 1$ for all $i \in \mathbb{N}$. Moreover, we define $\tilde{g}(i) := g^i(i)$, where the iterations of g are defined as $g^0(i) := i$ and $g^n(i) := g(g^{n-1}(i))$. In the sequel, we frequently consider the function $i \mapsto g^{i-1}(1)$ which, using the previous definition of iteration, is not well-defined for $i = 0$; instead, we set $g^{i-1}(1) := 0$ if $i = 0$. In this way, when g is the successor function, we obtain $g^{i-1}(1) = i$ for all $i \in \mathbb{N}$, and thus we recover all the results of [118] as special cases.

We define now the *predecessor operators* which represent one of the main tool of this chapter.

Definition 4.5 (Predecessor Operators) *For ordinals $\alpha, \lambda < \varepsilon_0$ and $n \geqslant 0$, we define:*

$$P^{f,g}_{n,x}(0) := 0, \qquad P^{f,g}_{n,x}(\alpha+1) := \alpha, \qquad P^{f,g}_{n,x}(\lambda) := P^{f,g}_{n,x}\left(\lambda\left[f\left(g^{n-1}(x)\right)\right]\right),$$
$$Q^{f,g}_{n,x}(0) := 0, \qquad Q^{f,g}_{n,x}(\alpha+1) := \alpha, \qquad Q^{f,g}_{n,x}(\lambda) := \lambda\left[f\left(g^{n-1}(x)\right)\right].$$

When f and g are respectively the identity function or the successor function, they are omitted.

The corresponding stepping down relations stemming from P and Q are defined as follows.

Definition 4.6 *For $R \in \{P, Q\}$, we define:*

1. $\alpha \succ^{R,0}_{f,g} \alpha$;
2. $\alpha \succ^{R,n}_{f,g} \beta :\iff \alpha > \beta$ *and* $\beta = R^{f,g}_{n,1} \dots R^{f,g}_{1,1}\alpha$ *with* $n \geqslant 1$;
3. $\alpha \succ^{R}_{f,g} \beta :\iff \exists n > 0 \left(\alpha \succ^{R,n}_{f,g} \beta\right)$;
4. $\alpha \succ^{R}_{k} \beta :\iff \alpha \succ^{R}_{f} \beta$ *where* f *is a constant function with value* k;
5. $\alpha \succcurlyeq^{R}_{k} \beta :\iff \alpha \succ^{R}_{f} \beta$ *or* $\alpha = \beta$ *where* $k \geqslant 0$.

Note that $R^{f,g}_{n,x}\beta = R_{f(g^{n-1}(x))}\beta$.

We define now a generalized version of Hydra steps and Goodstein Sequences.

Definition 4.7 (Hydra Steps) *Let* $\alpha < \varepsilon_0$*, we define*

$$\begin{aligned} \alpha^{f,g}_0 &:= \alpha, \\ \alpha^{f,g}_{i+1} &:= \alpha^{f,g}_i \left[1 + f\left(g^{i-1}(1)\right)\right], \end{aligned}$$

The Hydra principle (H^g_f) is the assertion $(\forall\alpha)(\exists i)\alpha^{f,g}_i = 0$. The Hydra principle is closely connected to iterations of the operator Q; schematically, after k Hydra steps the result is

$$\alpha^{f,g}_k = (\dots(\alpha[1 + f(0)])\dots)\left[1 + f\left(g^{k-1}(1)\right)\right]$$

Definition 4.8 (Goodstein Sequences) *Let* $m \geqslant 2$*, we define*

$$\begin{aligned} m^{f,g}_0 &:= m, \\ m^{f,g}_{i+1} &:= m^{f,g}_i(1 + f(g^{i-1}(1)) \mapsto 1 + f(g^{i}(1))) - 1. \end{aligned}$$

The Goodstein principle (G^g_f) is the assertion $(\forall m)(\exists i)m^{f,g}_i = 0$.

In Lemma 4.7 it is proved how Goodstein sequences are intrinsically connected to the operator P. In order to find the phase transition for the Hydra game (Q-steps), we will consider a faster and a slower process: the faster process is given by the Goodstein sequences (P-steps); whereas the slower corresponds to a Friedman style slowly well orderedness assertion with respect to a norm provided by the maximal coefficient ($mc(\cdot)$)[170].

We recall now the main results of [118] regarding the arithmetic of predecessor operators; *the novelty is given by the presence of the auxiliary function g instead of the successor function.* Except where explicitly stated, since not all the needed preliminaries contain the new function g, proofs are taken from the corresponding statements in [118]. As already pointed out by Meskens and Weiermann, a first indication that the Goodstein process is not lasting longer than a corresponding Hydra game is given in assertion 2 of the next lemma.

Lemma 4.1 *Let $\alpha, \beta, \lambda < \varepsilon_0$ and $R \in \{P, Q\}$, then the following assertions hold:*

1. $\alpha > 0 \Rightarrow \alpha \succcurlyeq_x^Q 1$, *and* $\alpha \succcurlyeq_x^P 0$;
2. $\alpha \succ_x^P \beta \Rightarrow \alpha \succ_x^Q \beta$;
3. $NF(\gamma, \beta)$ *and* $\beta > 0 \Rightarrow R_{n,x}^{f,g}(\gamma + \beta) = \gamma + R_{n,x}^{f,g}\beta$;
4. $NF(\gamma, \alpha)$ *and* $\alpha \succ_x^{R,m} \beta \Rightarrow \gamma + \alpha \succ_x^{R,m} \gamma + \beta$;
5. $x \geqslant 1$ *and* $\alpha \succ_x^{R,m} \beta \Rightarrow \exists n \geqslant m \left(\omega^\alpha \succ_x^{R,m} \omega^\beta\right)$.

Proof Assertions 1 and 2 follow by induction on α. For assertion 3 write $\beta =_{NF} \omega^{\beta_1} + \dots \omega^{\beta_m}$ and apply Def. 4.5. Assertion 4 follows from assertion 3. Assertion 5 follows from assertions 1 and 4 by induction on α. □

We prove now that

$$x \leqslant y,\ \lambda \in Lim \Rightarrow \lambda[y] \succcurlyeq_z^R \lambda[x] \tag{4.1}$$

for $z \geqslant 0$ and $R \in \{P, Q\}$. This follows by induction once we prove it for $y = x + 1$ and this case is treated in the next lemma. Moreover, assertion 4 of the next lemma gives a generalization of assertion 2 of Lemma 4.1.

Lemma 4.2 *Let $\alpha, \beta, \lambda < \varepsilon_0$ and $y \geqslant 0$, then the following assertions hold:*

1. $y > 0$ *and* $\lambda \in Lim \Rightarrow \lambda[x+1] \succcurlyeq_y^Q \lambda[x] + 1$;
2. $\alpha \succcurlyeq_x^Q \beta \succ_x^{P,m} \gamma \Rightarrow \exists n \geqslant m \left(\alpha \succ_x^{P,n} \gamma\right)$;
3. $y > 0$ *and* $\lambda \in Lim \Rightarrow \lambda[x+1] \succcurlyeq_y^P \lambda[x]$;
4. $\alpha > 0$ *and* $y \geqslant x > 0 \Rightarrow \alpha \succcurlyeq_y^Q P_x\alpha + 1$.

Proof Note that assertions 1 and 4 imply their strict versions if "+1" is omitted; this "+1′" will be needed in a crucial step of the proof of Proposition 4.3. Assertion 1 is proved by induction on λ. Indeed, if we write

$$\lambda =_{NF} \omega^{\lambda_1} + \dots + \omega^{\lambda_n},$$

then, because of Def. 4.3 and assertion 4 of Lemma 4.1, it suffices to prove

$$\omega^{\lambda_n}[x+1] \succ_y^Q \omega^{\lambda_n}[x] + 1.$$

If $\lambda_n \in Lim$, then the induction hypothesis yields $\lambda_n[x+1] \succcurlyeq_y^Q \lambda_n[x] + 1$, and therefore

$$\omega^{\lambda_n}[x+1] = \omega^{\lambda_n[x+1]} \succ_y^Q \omega^{\lambda_n[x]+1} \succcurlyeq_y^Q \omega^{\lambda_n}[x] + 1,$$

using assertion 5 of Lemma 4.1. Suppose now $\lambda_n = \alpha + 1$; by assertion 1 of Lemma 4.1 we obtain $\omega^\alpha \succcurlyeq_y^Q 1$, and this yield

$$\omega^{\lambda_n}[x+1] = \omega^\alpha(x+2) = \omega^\alpha(x+1) + \omega^\alpha \succcurlyeq_y^Q \omega^\alpha(x+1) + 1 = \omega^{\lambda_n}[x] + 1$$

by assertion 4 of Lemma 4.1.

Assertion 2 is also proved by induction on α, For the non trivial case, suppose $\alpha \neq \beta$. Then $\alpha[x] \succcurlyeq_x^Q \beta \succ_x^{P,m} \gamma$ which implies, by induction hypothesis, the existence of an $n \geqslant m$ such that

$$\alpha[x] \succ_x^{P,n} \gamma.$$

This yields $\alpha \succ_x^{P,k} \gamma$ with $k = n+1$ if $\alpha \notin Lim$ and with $k = n$ if $\alpha \in Lim$ since $P_x\alpha = P_x\alpha[x]$.

Proof of assertion 3 is as follows. From assertion 1 it follows that $\lambda[x+1] \succ_y^Q \lambda[x]$; because of $\lambda[x] + 1 \succ_y^P \lambda[x]$, assertion 2 yields $\lambda[x+1] \succ_x^P \lambda[x]$.

Assertion 4 is proved by induction on α using assertion 1 and is trivial for $\alpha \notin Lim$. If $\alpha \in Lim$, then

$$\alpha \succ_y^Q \alpha[y] \succcurlyeq_y^Q \alpha[x] \succcurlyeq_y^Q P_x\alpha[x] + 1 = P_x\alpha + 1.$$

Here the second inequality follows from assertion 1 by iteration iff $y > x$ (equality holds iff $y = x$), and the last inequality follows by the induction hypothesis. □

With the next lemma, we generalize [118, Lemma 3] considering also the function g.

Lemma 4.3 *Let $\alpha, \beta < \varepsilon_0$, $R \in \{P, Q\}$, $f, \bar{f} : \mathbb{N} \to \mathbb{N}$ be weakly increasing function and $g, \bar{g} : \mathbb{N} \to \mathbb{N}$ be strictly increasing function such that $g(x), \bar{g}(x) \geqslant x+1$, then the following assertions hold:*

1. $\alpha \succ_x^R \beta$ *and* $x \leqslant y \Rightarrow \alpha \succ_y^R \beta$;
2. $\forall i\, \bar{f}(i) \leqslant f(i),\ \bar{g}(i) \leqslant g(i)$ *and* $\alpha \succ_{\bar{f},\bar{g}}^{R,m} \beta \Rightarrow \exists n \geqslant m \left(\alpha \succ_{f,g}^{R,m} \beta\right)$.

Proof Asserion 1 is proved by induction on α and follows from $\alpha \succ_y^R \alpha[y] \succcurlyeq_y^R \alpha[x] \succcurlyeq_y^R \beta$. The second inequality holds because of Eq.(4.1) if $\alpha \in Lim$ (equality holds otherwise) and the last one follows from the induction hypothesis.

Assertion 2 is proved by induction on m. Assume that $\alpha \succ_{\bar{f},\bar{g}}^{R,m} \beta$; then there exists β_0 such that $\alpha \succ_{\bar{f},\bar{g}}^{R,m-1} \beta_0$ and $\beta = R_{f(g^{m-1}(1))}\beta_0$. The induction hypothesis yields an $n' \geqslant m-1$ such that $\alpha \succ_{f,g}^{R,n'} \beta_0$. We have to prove that there exists an $n > n'$ such that

$$\beta = R_{f(g^{n-1}(1))} R_{f(g^{n-2}(1))} \ldots R_{f\left(g^{n'}(1)\right)} \beta_0.$$

The assumption yields

$$f\left(g^{n-1}(1)\right) \geqslant \ldots \geqslant f\left(g^{n'}(1)\right) \geqslant \bar{f}\left(\bar{g}^{m-1}(1)\right)$$

for all $n \geqslant n' \geqslant m$. Put

$$z_i := f\left(g^{n'+i-1}(1)\right),$$

it suffices to show the relation $R_{z_1}\beta_0 \succcurlyeq^R_{z_1} \beta$ and the implication $R_{z_i} \ldots R_{z_1}\beta_0 \succ^R_{z_i} \beta \Rightarrow R_{z_i+1}R_{z_i} \ldots R_{z_1}\beta_0 \succcurlyeq^R_{z_i+1} \beta$.

Note first that $\beta = R_{\bar{f}(\bar{g}^{m-1}(1))}\beta_0$, hence $\beta_0 \succ^R_{\bar{f}(\bar{g}^{m-1}(1))} \beta$. Since $\bar{f}\left(\bar{g}^{m-1}(1)\right) < z_1$ assertion 1 yields $\beta_0 \succ^R_{z_1} \beta$.

Now assume that $R_{z_i} \ldots R_{z_1}\beta_0 \succ^R_{z_i} \beta$; then, by assertion 1, we have

$$R_{z_i} \ldots R_{z_1}\beta_0 \succ^R_{z_i+1} \beta,$$

thus

$$R_{z_i+1}R_{z_i} \ldots R_{z_1} \succcurlyeq^R_{z_i+1} \beta.$$

□

Finally, we are able to prove, extending [118, Corollary 1], that Goodstein sequences form a subsystem (subsequence) of the Hydra games even for the generalised versions.

Corollary 4.1 *If f, g are as before and $\alpha \succ^P_{f,g} \beta$, then $\alpha \succ^Q_{f,g} \beta$.*

Proof The assertion follows essentially from Lemma 4.2.3. We show the implication

$$\alpha \succ^{P,m}_{f,g} \beta \Rightarrow \exists n \geqslant m, \alpha \succ^{Q,n}_{f,g} \beta$$

by induction on m. For $m = 0$ is true by Def. 4.6. Assume that $\alpha \succ^{P,m}_{f,g} \beta$; then there exists β_0 such that

$$\alpha \succ^{P,m-1}_{f,g} \beta_0$$

and $\beta = P_{f(g^{m-1}(1))}\beta_0$. The induction hypothesis yields the existence of an $n' \geqslant m-1$ such that $\alpha \succ^{Q,n'}_{f,g} \beta_0$. We claim the existence of an $n \geqslant n'$ such that

$$Q_{f(g^{n-1}(1))} \ldots Q_{f(g^{n'}(1))}\beta_0 = \beta.$$

Let

$$z_i := f\left(g^{n'+i-1}(1)\right),$$

it suffice to show the relation $Q_{z_1}\beta_0 \succcurlyeq^Q_{z_1} \beta$ and the implication $Q_{z_i} \ldots Q_{z_1}\beta_0 \succ^Q_{z_i} \beta \Rightarrow Q_{z_i+1}Q_{z_i} \ldots Q_{z_1}\beta_0 \succ^Q_{z_i+1} \beta$.

First we have $\beta_0 \succ^P_{f(g^{m-1}(1))} \beta$, hence $\beta_0 \succ^Q_{f(g^{m-1}(1))} \beta$ according to assertion 2 of Lemma 4.1; since $z_1 \geqslant f(g^{m-1}(1))$, we obtain $\beta_0 \succ^Q_{z_1} \beta$, thus $Q_{z_1}\beta_0 \succ^Q_{z_1} \beta$.

Now assume $Q_{z_i} \dots Q_{z_1}\beta_0 \succ^Q_{z_i} \beta$. Assertion 1 of Lemma 4.3 yields

$$Q_{z_i} \dots Q_{z_1}\beta_0 \succ^Q_{z_i+1} \beta,$$

hence $Q_{z_i+1} \dots Q_{z_1}\beta_0 \succcurlyeq^Q_{z_i+1} \beta$. □

Given the crucial role of ω-towers of ordinals afterwards, we conclude this paragraph with some of their reductions.

Corollary 4.2 *Let $\alpha < \varepsilon_0$ and $x > 0$, then the following assertions hold:*

1. $\omega^{\alpha+1} \succ^Q_{x+1} \omega^\alpha \cdot 2$;
2. $\omega^{\alpha+1} \succ^Q_{x+1} \omega^\alpha + 1$;
3. $\omega_{h+1}(\alpha+1) \succ^Q_{x+1} \omega_h(\alpha) + \omega_{h+1}$ *if* $\alpha > 0$;
4. $x > 0 \Rightarrow \omega_{h+1} \succ^P_{x+1} \omega_h$.

Proof Assertion 1 is a direct consequence of assertions 1 and 4 of Lemma 4.1. Indeed, we have

$$\omega^{\alpha+1} \succ^Q_{x+1} \omega^\alpha(x+2) = \omega^\alpha 2 + \omega^\alpha x \succcurlyeq^Q_{x+1} \omega^\alpha 2.$$

Assertion 2 follows from assertion 1 by the assertions 1 and 4 of Lemma 4.1.

Assertion 3 is proved by induction on h. First note that an iteration of assertion 5 of Lemma 4.1 yields

$$\alpha \succ^Q_x \beta \Rightarrow \omega_h(\alpha) \succ^Q_x \omega_h(\beta). \tag{4.2}$$

Then note that the induction hypothesis implies

$$\omega_h(\alpha+1) \succ^Q_{x+1} \omega_h(\alpha) + 1 \tag{4.3}$$

by assertion 1 of Lemma 4.1. Further we have

$$\omega^{\omega_h(\alpha+1)} \succ^Q_{x+1} \omega^{\omega_h(\alpha)+1} \succ^Q_{x+1} \omega^{\omega_h(\alpha)}2 = \omega_{h+1}(\alpha)2 \succ^Q_{x+1} \omega_{h+1}(\alpha) + \omega_{h+1}.$$

The first inequality is obtained by assertion 5 of Lemma 4.1 applied to (4.3); the second one by assertion 1 and the last by (4.2).

Assertion 4 follows from $\omega \succ^Q_{x+1} 1$ and assertion 5 of Lemma 4.1. □

4.1.2 Generalized Hierarchies and Counting Functions

We recall now, extending their definitions, the standard subrecursive hierarchies which can be used to measure provability strengths with regard to provably recursive functions; more precisely, and similarly to the Goodstein sequences and Hydra games, we generalize their definition using an auxiliary function g. The Hardy hierarchy $(H_\alpha)_{\alpha\leqslant\varepsilon_0}$ will play a crucial role; whereas the slow growing hierarchy $x \mapsto G_x(\alpha)$ is used mainly for counting purposes.[1]

Definition 4.9 *Let f be a weakly increasing function and g a strictly increasing function with $g(n)\geqslant n+1$, let $\alpha,\lambda\leqslant\varepsilon_0$ with $\lambda\in Lim$; we define G, g, H, h as*

$$\begin{array}{rclrclrcl}
G_x(0) & := & 0 & G_x(\alpha+1) & := & G_x(\alpha)+1 & G_x(\lambda) & := & G_x(\lambda[x]) \\
g_x(0) & := & 0 & g_x(\alpha+1) & := & g_x(\alpha)+1 & g_x(\lambda) & := & g_x(\lambda[x])+1 \\
H_0^{f,g}(x) & := & x & H_{\alpha+1}^{f,g}(x) & := & H_\alpha^{f,g}(g(x)) & H_\lambda^{f,g}(x) & := & H_{\lambda[f(x)]}^{f,g}(x) \\
h_0^{f,g}(x) & := & x & h_{\alpha+1}^{f,g}(x) & := & h_\alpha^{f,g}(g(x)) & h_\lambda^{f,g}(x) & := & h_{\lambda[f(x)]}^{f,g}(g(x))
\end{array}$$

Again we suppress the subscript f or g in the definitions of H and h if $f(n)=n$ or $g(n)=n+1$.[2] In the last section of this chapter, we will see the connections between the Hardy hierarchy $(H_\alpha)_{\alpha<\varepsilon_0}$ and the Ackermann function A.

Some elementary, but crucial, properties of G, g, H and h for counting lengths of stepping down processes are provided by the following lemma which generalized [118, Lemma 4].

Lemma 4.4 *Let $0<\alpha<\varepsilon_0$, then*

1. $G_x(\alpha) = \min\{i \mid \alpha \succ_x^{P,i} 0\}$;
2. $g_x(\alpha) = \min\{i \mid \alpha \succ_x^{Q,i} 0\}$;
3. $H_\alpha^{f,g}(x) = g^{\bar{i}}(x)$ *where* $\bar{i} := \min\left\{i \mid P_{i-1,x}^{f,g} \dots P_{1,x}^{f,g}\alpha = 0\right\}$;
4. $h_\alpha^{f,g}(x) = g^{\bar{i}}(x)$ *where* $\bar{i} := \min\left\{i \mid Q_{i-1,x}^{f,g} \dots Q_{1,x}^{f,g}\alpha = 0\right\}$.

Proof All the assertions can be proved by induction on α. We treat only assertion 4 which, given our Def. 4.3 of fundamental sequences (in particular we have

[1] We use the notation $G_x(\alpha)$, instead of the more common $G_\alpha(x)$, because it fits better with our needs.

[2] We warn the reader not to confuse the counting function g_x, defined over ordinals, with the starting function g, defined over natural numbers.

$(\alpha+1)[n] = \alpha$ for every n), can be uniformly proved for all $0 < \alpha < \varepsilon_0$. Given $0 < \alpha < \varepsilon_0$, by definition we have

$$h^{f,g}_{\alpha}(x) = h^{f,g}_{\alpha[f(x)]}(g(x)) = h^{f,g}_{\alpha[f(x)][f(g(x))]}(g(g(x))) = \cdots = h_{\alpha[f(x)]\ldots[f(g^{\bar{i}-1}(x))]}\left(g^{\bar{i}}(x)\right) = g^{\bar{i}}(x)$$

where $\bar{i} = \min\{i \mid \alpha[f(x)][f(g(x))]\ldots[f(g^{i-1}(x))] = 0\}$; finally, by Def. 4.5 and Def. 4.6, we have

$$\min\{i \mid \alpha[f(x)][f(g(x))]\ldots[f(g^{i-1}(x))] = 0\} = \min\{i \mid Q^{f,g}_{i-1,x}\ldots Q^{f,g}_{1,x}\alpha = 0\}$$

$\square$

Remark 4.1 *If g is the successor function, points 3. and 4. of previous lemma reduce to*

1. $H^{f}_{\alpha}(x) = \min\left\{i \geqslant x \mid P^{f}_{i-1}\ldots P^{f}_{x}\alpha = 0\right\}$;
2. $h^{f}_{\alpha}(x) = \min\left\{i \geqslant x \mid Q^{f}_{i-1}\ldots Q^{f}_{x}\alpha = 0\right\}$.

In the following lemma, extending [118, Lemma 5], we prove that the Hydra games and Goodstein sequences do not differ that much, although their definitions imply huge differences in their counting functions (a P-step can contain many Q-steps). This is formalized by the additional "$g(x)$" in the definition of h compared with H which makes big differences because of recursion, but both functions bound each other. This means that their phase transitions will be closely related.

Lemma 4.5 *Let $\alpha, \beta < \varepsilon_0$ and f, g be as before, then*

1. $NF(\alpha,\beta) \Rightarrow H^{f,g}_{\alpha}\left(H^{f,g}_{\beta}(x)\right) = H^{f,g}_{\alpha+\beta}(x)$;
2. $F \in \{H,h\}, \alpha \succcurlyeq^{Q}_{f(x)} \beta \Rightarrow F^{f,g}_{\alpha}(x) \geqslant F^{f,g}_{\beta}(x)$;
3. $H^{f,g}_{\alpha}(x+1) \geqslant h^{f,g}_{\alpha}(x) \geqslant H^{f,g}_{\alpha}(x)$ *if f is strictly increasing;*
4. $H^{f,g}_{\omega^\alpha}(x) \geqslant H^{f,g}_{\alpha}(x)$ *if $f(x) \geqslant 1$.*

Proof All assertions are proved by induction on α, and possibly on β. As an example, we prove $H^{f,g}_{\alpha}(x+1) \geqslant h^{f,g}_{\alpha}(x)$. The cases $\alpha = 0$ and α successor are immediate; let us consider the limit step $\alpha = \lambda \in Lim$. In this case we have

$$\begin{aligned} H^{f,g}_{\lambda}(x+1) = H^{f,g}_{\lambda[f(x+1)]}(x+1) &\geqslant H^{f,g}_{\lambda[f(x)]+1}(x+1) \\ &\geqslant h^{f,g}_{\lambda[f(x)]+1}(x) = h^{f,g}_{\lambda[f(x)]}(g(x)) = h^{f,g}_{\lambda}(x). \end{aligned}$$

The first inequality holds by assertion 2 (by assertion 1 of Lemma 4.2 the condition is satisfied), the second inequality by the induction hypothesis; equalities hold by definition. □

We conclude this section with a useful tool for proving unprovability results; the idea is to bound the complexity of the Hydra game with maximal coefficients for a constant function. For this we need a relation between G and g; the required properties are contained in the following lemma.

Lemma 4.6 *Let* $\alpha, \beta < \varepsilon_0$*, then:*

1. $G_{x+1}(\alpha) \geqslant g_x(\alpha) \geqslant G_x(\alpha)$;
2. $\alpha < \beta,\ mc(\alpha) \leqslant x,\ \beta \notin Lim \Rightarrow \alpha \leqslant \beta[x+1]$ *and*
   $\alpha < \beta,\ mc(\alpha) \leqslant x,\ \beta \in Lim \Rightarrow \alpha < \beta[x+1]$;
3. $\#\{\alpha < \beta : mc(\alpha) \leqslant x\} \leqslant G_{x+1}(\beta)$;
4. $G_x(\alpha) = \alpha(\omega \mapsto x+1)$;
5. $\alpha < \beta, mc(\alpha) \leqslant x \Rightarrow H_\alpha(x) < H_\beta(x)$ *and* $G_x(\alpha) < G_x(\beta)$.

Proof Assertion 1 is proved by induction on x. Assertion 2 is proved by induction on β, assertion 3 is proved by induction on β using assertion 2. Assertion 4 and Assertion 5 are proved by induction on α. □

4.2 Phase Transition Results

In this section we will prove that, fixed a function g as before (i.e. g is an elementary recursive strictly increasing function from $\mathbb{N}$ to $\mathbb{N}$ with $g(n) \geqslant n+1$), the phase transition thresholds for the generalised Goodstein sequences, the generalised Hydra games and the generalised Friedman-style slowly wellfoundedness of ε_0 with regard to the maximal coefficient norm are the same. Given the previous discussion, it is sufficient to prove a sufficiently good lower bound of unprovability for the Goodstein sequences and a sufficiently good upper bound of provability for the Friedman style slowly well-foundedness. Proving (un)provability is done by determining whether the step counting function is provably recursive in the Hardy hierarchy. These statements are formalized in the following well known theorem.

Theorem 4.3 *Let T denote a standard primitive recursive Kleene predicate for the enumeration of the partial recursive functions. Let U be the corresponding primitive recursive function (producing the output of a terminating computation). Within the language of PA the T predicate is then of complexity Σ_1. Let*

$\Phi_e(m) := U(\min\{n \mid T(e,m,n)\})$. If Φ_e is provably recursive in the sense that PA $\vdash \forall x\, \exists y\, T(e,x,y)$, then there exists an $\alpha < \varepsilon_0$ such that Φ_e is primitive recursive in and bounded by h_α. The function h_{ε_0} therefore eventually dominates every provably recursive function of PA. Moreover for $\alpha < \varepsilon_0$, the functions $h_\alpha, H_\alpha, g_\alpha$ and G_α are all provably recursive in PA (and they are eventually dominated by the function h_{ε_0}).

Proof see e.g. [65]. □

Let us now investigate appropriate sub- and superprocesses for the generalised Hydra game in terms of ordinal sequences.

Definition 4.10 *Let f, g be as before, then we define:*

$$\begin{aligned} \left(\bar{G}^g_f\right) \quad &:\Longleftrightarrow \quad \forall K\, \exists M \left(\omega_K \succ^{P,M}_{f,g} 0\right) \\ \left(\bar{H}^g_f\right) \quad &:\Longleftrightarrow \quad \forall K\, \exists M \left(\omega_K \succ^{Q,M}_{f,g} 0\right) \\ \left(MC^g_f\right) \quad &:\Longleftrightarrow \quad \forall K\, \exists M\, \forall \alpha_0, \ldots \alpha_M \leqslant \omega_K \\ &\qquad\quad [\forall i \leqslant M\, (mc(\alpha_i) \leqslant K + f(g^{i-1}(1))) \Rightarrow \exists i < M\, (\alpha_{i+1} \geqslant \alpha_i)] \end{aligned}$$

Here MC^g_f is a generalised version of Friedman style slowly well-orderedness [170].

Corollary 4.3

$$PA \vdash (MC^g_f) \;\Rightarrow\; PA \vdash (\bar{H}^g_f) \;\Rightarrow\; PA \vdash (\bar{G}^g_f)$$

Proof The first implication is a direct consequence of the following bound regarding the maximal coefficient

$$mc(\alpha[x]) \leqslant \max(mc(\alpha), x+1),$$

which derives from Def. 4.1 and Def. 4.3. The second implication follows from Lemma 4.3 and Lemma 4.4. □

In the next lemma, representing the generalized version of [118, Lemma 7], the connection between Goodstein sequences and Hydra game and, respectively, P-steps and Q-steps is exposed.

Lemma 4.7 *Let f and g be as before, then:*

1. *$PA \vdash (G^g_f) \leftrightarrow (\bar{G}^g_f)$;*
2. *$PA \vdash (H^g_f) \leftrightarrow (\bar{H}^g_f)$.*

Proof The latter assertion derived immediately from Def. 4.7 since each $\alpha < \varepsilon_0$ is smaller than some ω_K. For the former, we proceed as follows. Firstly, for sake of readability, we fix $F(i) := f\left(g^{i-1}(1)\right)$; secondly, we recall from [44] that

$$G_x(P_x\alpha) = P_x(G_x\alpha) \tag{4.4}$$

holds for $\alpha < \varepsilon_0$, (4.4) can be proved by induction on α. Moreover, we note that if $\alpha = m_i^{f,g}(F(i)+1 \mapsto \omega)$, then

$$m_i^{f,g} = G_{F(i)}(\alpha),$$

and by definition

$$\begin{aligned} m_{i+1}^{f,g} &= \alpha(\omega \mapsto F(i+1)+1) - 1 \\ &= P_{F(i+1)}\alpha(\omega \mapsto F(i+1)+1) \\ &= P_{F(i+1)}G_{F(i+1)}(\alpha). \end{aligned}$$

Assume now that $(\forall m)(\exists i)m_i^{f,g} = 0$. From this assumption, let us prove the assertion $(\bar{G}_f^g)$ by elementary means. Let us assume that $F(0) = 1$ and that

$$e(m) := 2_m.$$

Then

$$PA \vdash (\forall m)(\exists i)e(m)_i^{f,g} = 0.$$

For a given $m \geqslant 2$, let

$$\alpha(m) := e(m)(2 \mapsto \omega) = \omega_m.$$

By induction on i, we show that

$$e(m)_i^{f,g} = G_{F(i)}\left(P_{F(i)} \ldots P_{F(1)}\alpha(m)\right).$$

Indeed, $e(m)_0^{f,g} = G_0\alpha(m)$ holds due to $F(0) = 1$; and, for $i > 0$, we have

$$\begin{aligned} e(m)_i^{f,g} &= P_{F(i)}e(m)_{i-1}^{f,g}(F(i-1)+1 \mapsto F(i)+1) \\ &= P_{F(i)}G_{F(i-1)}\left(P_{F(i-1)} \ldots P_{F(1)}\alpha(m)\right)(F(i-1)+1 \mapsto F(i)+1) \\ &= P_{F(i)}\left(P_{F(i-1)} \ldots P_{F(1)}\alpha(m)\right)(\omega \mapsto F(i-1)+1 \mapsto F(i)+1) \\ &= P_{F(i)}G_{F(i)}\left(P_{F(i-1)} \ldots P_{F(1)}\alpha(m)\right) \\ &= G_{F(i)}\left(P_{F(i)}P_{F(i-1)} \ldots P_{F(1)}\alpha(m)\right). \end{aligned}$$

The second inequality holds by induction hypothesis, the third and the fourth by Lemma 4.6.4, the last one by Eq. 4.4. Therefore

$$\min\{i \mid e(m)_i^{f,g} = 0\} = \min\left\{i \mid \alpha(m) \succ_F^{P,i} 0\right\} = \min\left\{i \mid \alpha(m) \succ_{f,g}^{P,i} 0\right\}$$

and we are done. The argument is clearly reversible and so from $(\bar{G}_f^g)$ we can also obtain (G_f^g) by elementary means. □

Remark 4.2 *In the current version of the previous lemma, f is needed to be weakly increasing, and as well as F inside the proof. Otherwise, the sequence of equality for proving $e(m)_i^{f,g} = G_{F(i)}\big(P_{F(i)} \dots P_{F(1)}\alpha(m)\big)$ may fail.*

Note that it suffices to prove termination of the processes under consideration for ordinals of the form ω_K. Moreover, because of assertion 3 of Lemma 4.5, it does not matter if the step counting function is primitive recursive in a function from $(h_\alpha)_{\alpha<\varepsilon_0}$ or from $(H_\alpha)_{\alpha<\varepsilon_0}$. In the following paragraphs we treat in order: unprovable results, provable results, and results concerning fragments of PA.

4.2.1 Unprovable Versions

To prove unprovability, we use the following strategy: we adjust the given ordinal by making a sufficiently big omega tower of it. Consequentially, its iterations will let the step counting function "explode", so that it dominates the function $K \mapsto H_{\omega_K}(1)$ which is not provably total in PA. In the following, we need the inverse of a function from $\mathbb{N}$ to $\mathbb{N}$ which, for $f\colon \mathbb{N} \to \mathbb{N}$, is defined as:

$$f^{-1}(n) := \min\{k \mid f(k) \geqslant n\}.$$

Observe that, if f is strictly increasing, then $f^{-1}(f(n)) = n$.

Proposition 4.1 *Let $f, g\colon \mathbb{N} \to \mathbb{N}$, where f is a weakly increasing function such that $f(n) \geqslant n$ and g is a strictly increasing function such that $g(n) \geqslant n+1$, then*

1. $PA \nvdash (G_f^g)$;
2. $PA \nvdash (\bar{G}_f^g)$;
3. $PA \nvdash (H_f^g)$;
4. $PA \nvdash (\bar{H}_f^g)$;
5. $PA \nvdash (MC_f^g)$.

Proof We only need to prove the second assertion which follows from [118, Proposition 1] and Lemma 4.3. □

The content of the next proposition will become clear inside the proof of Proposition 4.3, thus we postpone its demonstration.

Proposition 4.2 *Let $h \geqslant 1$ and g as before, we define a function $F\colon \mathbb{N} \to \mathbb{N}$ as $F(i) := |\tilde{g}^{-1}(g^{i-1}(1))|_h$. Moreover, define $j_0 := 0, j_{k+1} := (k+2)_h(k+2), b_0 := 0, b_{k+1} := b_k + j_{k+1}$, i.e. $b_k = j_0 + \cdots + j_k$, and a function $h\colon \mathbb{N} \to \mathbb{N}$ as $h(i) = k$ if $b_{k-1} < i \leqslant b_k$. Then, for all i, $h(i) \leqslant F(i)$.*

The following, which is a generalization of [118, proposition 2], is a key result to obtain unprovability.

Proposition 4.3 *Let $h \geqslant 1$, g be as before and set $f(i) := |\tilde{g}^{-1}(i)|_h$. For a given ordinal α, define $\beta := \omega_{h+1}(\alpha) + \omega_{h+1}$, then there exists an $i \geqslant H_\alpha(1)$ such that $\beta \succ^{P,i}_{f,g} \omega_{h+1}(0)$.*

Proof We mimic the proof in [118] adding a proper treatment of g and $\tilde{g}^{-1}$.
We know that $\min\left\{ i \,|\, \alpha \succ^{P,i-1}_{id} 0 \right\} = H_\alpha(1) =: L$. By definition we have $f(i) \geqslant 1$ for all i; moreover, we have

$$\begin{array}{rcl} \beta & \succ^P_1 & \omega_{h+1}(\alpha) + P_1 \omega_{h+1} \\ & \vdots & \\ & \succ^P_1 & \omega_{h+1}(\alpha) + \underbrace{P_1 \ldots P_1}_{2_h(2)} \omega_{h+1} \\ & = & \omega_{h+1}(\alpha) \end{array}$$

since, by Lemma 4.4.1 and Lemma 4.6.4, $\min\left\{ i \,|\, \omega_{h+1} \succ^{P,i}_1 0 \right\} = G_1(\omega_{h+1}) = 2_h(2)$. Thus, there exists $i_1 \geqslant 2_h(2)$ such that $\beta \succ^{P,i_1}_1 \omega_{h+1}(\alpha)$.

Define $\alpha_0 := \alpha, \alpha_k := P_k \alpha_{k-1}$. We prove by induction that

$$\omega_{h+1}(\alpha_{k-2}) \succ^{P,i_k}_k \omega_{h+1}(\alpha_{k-1}), \text{ for some } i_k \geqslant (k+1)_h(k+1), \tag{4.5}$$

for all $k = 2, \ldots, L$. Further we obtain

$$\begin{array}{rcl} \omega_{h+1}(\alpha_{k-1}) & \succcurlyeq^Q_{k+1} & \omega_{h+1}(P_k \alpha_{k-1} + 1) \\ & \succcurlyeq^Q_{k+1} & \omega_{h+1}(\alpha_k) + \omega_{h+1} \\ & \succcurlyeq^P_{k+1} & \omega_{h+1}(\alpha_k) + P_{k+1} \omega_{h+1} \\ & \vdots & \\ & \succcurlyeq^P_{k+1} & \omega_{h+1}(\alpha_k) + \underbrace{P_{k+1} \ldots P_{k+1}}_{(k+2)_h(k+2)} \omega_{h+1} \\ & = & \omega_{h+1}(\alpha_k) \end{array}$$

again since

$$\min\left\{ i \,|\, \omega_{h+1} \succ^{P,i}_{k+1} 0 \right\} = G_{k+1}(\omega_{h+1}) = (k+2)_h(k+2).$$

By assertion 2 of Lemma 4.2, this implies the existence of an $i_{k+1} \geqslant (k+2)_h(k+2)$ such that

$$\omega_{k+1}(\alpha_{k-1}) \succ^{P,i_{k+1}}_{k+1} \omega_{h+1}(\alpha_k).$$

We define now $i_0 := 0$, $\beta_0 := i_0$, $\beta_{k+1} := \beta_k + i_{k+1}$, i.e. $\beta_k = i_0 + \cdots + i_k$, and a function $h\colon \mathbb{N} \to \mathbb{N}$ as $h(i) = k$ if $\beta_{k-1} < i \leqslant \beta_k$, letting $M := \sum_{k=1}^{L} i_k$. Equation 4.5 yields

$$\beta \succ_h^{P,M} \omega_{h+1}(\alpha_{L-1}) = \omega_h.$$

By the definition of $\succ_{f,g}^{P,m}$ we have

$$\alpha \succ_{f,g}^{P,m} \beta \iff \beta = P_{m,1}^{f,g} \dots P_{1,1}^{f,g}\alpha \;=\; P_{f(g^{m-1}(1))} \dots P_{f(g(1))} P_{f(1)}\alpha,$$

and so

$$\alpha \succ_{f,g}^{P,m} \beta \iff \alpha \succ_F^{P,m} \beta \;\text{ with } F(i) := f\left(g^{i-1}(1)\right).$$

By Proposition 4.2, and the fact that $i_k \geqslant (k+1)_h(k+1)$, we obtain that, for all i, $h(i) \leqslant |\tilde{g}^{-1}(g^{i-1}(1))|_h = F(i)$ and, by Lemma 4.3, there exists $m \geqslant M > L$ such that $\beta \succ_F^{P,m} \omega_h$; finally, we have $\beta \succ_{f,g}^{P,m} \omega_h$ for some $m > L$. □

Hoping that its content has became apparent, we prove now Proposition 4.2.
Proof of 4.2 first we observe that

$$g^{i-1}(1) \geqslant g^{\lfloor \frac{i}{2} \rfloor}\left(g^{\lfloor \frac{i}{2} \rfloor - 1}(1)\right) \geqslant g^{\lfloor \frac{i}{2} \rfloor}\left(\left\lfloor \frac{i}{2} \right\rfloor\right) = \tilde{g}\left(\left\lfloor \frac{i}{2} \right\rfloor\right),$$

where the second inequality holds because g is strictly increasing and $g(x) \geqslant x+1$ and thus $g^n(x) \geqslant x+n$. From this we obtain

$$\tilde{g}^{-1}\big(g^{i-1}(1)\big) \geqslant \tilde{g}^{-1}\bigg(\tilde{g}\left(\left\lfloor \frac{i}{2} \right\rfloor\right)\bigg) = \left\lfloor \frac{i}{2} \right\rfloor,$$

and finally

$$F(i) = \left|\tilde{g}^{-1}\big(g^{i-1}(1)\big)\right|_h \geqslant \left|\left\lfloor \frac{i}{2} \right\rfloor\right|_h.$$

Thus, in the following we prove $h(i) \leqslant \left|\left\lfloor \frac{i}{2} \right\rfloor\right|_h$. For $i \leqslant 2_h 2 = i_1$, we have that $h(i) \leqslant 1 = F(i)$; the thesis for $i \geqslant 2_h 2$ easily derives from the following claim.

CLAIM: $\forall h, \forall i, \forall k \geqslant 1$, the following properties hold:

1. $2_h k \leqslant i < 2_h(k+1) \;\Rightarrow\; \left|\left\lfloor \frac{i}{2} \right\rfloor\right|_h = k$;
2. $b_{k-1} < i \leqslant b_k \;\Rightarrow\; h(i) = k$;
3. $2_h(k+1) \leqslant b_k$.

Properties 2. and 3. derive from the definitions of h and b_k, namely $2_h(k+1) \leqslant (k+1)_h(k+1) = j_k \leqslant b_k$. Property 1. is proved by induction over h using the definition of $|\cdot|$, i.e. $\left|\left\lfloor \frac{i}{2} \right\rfloor\right|_1 = \left\lceil \log_2\left(\left\lfloor \frac{i}{2} \right\rfloor + 1\right)\right\rceil$, and the properties of logarithms. □

To describe the threshold function for the phase transition resulting from the Hydra game it is useful to work with functional inverses of the Hardy functions H_α. Since H_α is strictly increasing, we have $H_\alpha^{-1}(H_\alpha(i)) = i$; moreover, for large α, H_α^{-1} grows very slowly and is elementary recursive.

The next lemma extends [118, Lemma 8].

Lemma 4.8 *Let g be as before, define*[3] $f(i) := |\tilde{g}^{-1}(i)|_{H_{\varepsilon_0}^{-1}(i)}$, $\bar{f}(i) := \max_{0 \leqslant k \leqslant i} f(k)$ *and fix* $m \geqslant 2$. *Let* $\alpha = \omega_{m+1}(\omega_m) + \omega_{m+1}$ *and* $i_0 = H_{\omega_m}(1)$, *then* $\alpha \succ^{P,i_0}_{\bar{f},g} \delta$ *for some* $\delta \geqslant \omega_m$.

Proof Let $f_m(i) := |\tilde{g}^{-1}(i)|_m$. For $i \leqslant i_0$, we have

$$H_{\varepsilon_0}^{-1}(i) \leqslant H_{\varepsilon_0}^{-1}(i_0) \leqslant m$$

since $H_{\omega_m}(1) \leqslant H_{\varepsilon_0}(m)$. Thus

$$\bar{f}(i) \geqslant f(i) = |\tilde{g}^{-1}(i)|_{H_{\varepsilon_0}^{-1}(i)} \geqslant f_m(i)$$

for all $i \leqslant i_0$. Then, by Proposition 4.3, there exists an $j_0 \geqslant i_0$ such that

$$\alpha \succ^{P,j_0}_{f_m,g} \omega_m.$$

Assertion 2 of Lemma 4.3 implies $\alpha \succ^{P,i_0}_{\bar{f},g} \delta$ for some $\delta \geqslant \omega_m$ since $\bar{f}(i) \geqslant f_m(i)$ for all $i \leqslant i_0$. □

The next theorem generalizes [118, Theorem 2] in the presence of g. In addition, it corrects a previous minor flaw; more precisely, the threshold function $f(i) := |i|_{H_{\varepsilon_0}^{-1}(i)}$ used in [118] is not weakly increasing[4] and this lack is not compatible with the current approach (see Remark 4.2). Nevertheless, we believe that a suitable treatment directly for $f(i) = |i|_{H_{\varepsilon_0}^{-1}(i)}$, or the g-version $f(i) = |\tilde{g}^{-1}(i)|_{H_{\varepsilon_0}^{-1}(i)}$, is achievable.

Theorem 4.4 (Phase Transition, Unprovable Version) *Let g be as before and define*

$$f(i) := \max_{0 \leqslant k \leqslant i} \left|\tilde{g}^{-1}(k)\right|_{H_{\varepsilon_0}^{-1}(k)}.$$

Then the following assertions hold:

1. $PA \nvdash (G_f^g)$;

[3] Here and below, we consider $\bar{f}$ instead of f because f is not in general weakly increasing, see also Remark 4.2.

[4]For example $f(H_{\varepsilon_0}(10)) = |H_{\varepsilon_0}(10)|_{10} > |H_{\varepsilon_0}(10) + 1|_{11} = f(H_{\varepsilon_0}(10) + 1)$.

2. $PA \nvdash (\bar{G}^g_f)$;
3. $PA \nvdash (H^g_f)$;
4. $PA \nvdash (\bar{H}^g_f)$;
5. $PA \nvdash (MC^g_f)$.

Proof As before, we adapt the proof proposed in [118] to include a suitable treatment of g. It suffices to prove assertion 1, which we prove by contradiction. Assume $PA \vdash (G^g_f)$ and let

$$e(m) := 2_{2m+1} + 2_{m+1}.$$

Then

$$PA \vdash \ (\forall m)(\exists i) e(m)^{f,g}_i = 0.$$

Given $m \geqslant m$, let

$$\alpha(m) := e(m)(2 \mapsto \omega) = \omega_{2m+1} + \omega_{m+1},$$

then, as seen in Lemma 4.7 and using the same notation $F(i) := f\left(g^{i-1}(1)\right)$,

$$e(m)^{f,g}_i = G_{F(i)}\left(P_{F(i)} \dots P_{F(1)} \alpha(m)\right).$$

This yields by Lemma 4.8

$$\min\{i \mid e(m)^{f,g}_i = 0\} = \min\{i \mid \alpha(m) \succ^{P,i}_{f,g} 0\} \geqslant H_{\omega_m}(1),$$

since $m \mapsto H_{\omega_m}(1)$ is not provably recursive in PA, we obtain a contradiction. □

4.2.2 Provable Versions

In assertion 3 of Lemma 4.6, given the fact that $x \mapsto G_x(\alpha)$ is provably total in PA for all $\alpha \leqslant \varepsilon_0$, we proved implicitly a first provable version for the Friedman style assertion MC^g_f for $g(n) = n + 1$ and a constant function f. This observation is used to obtain more general provable versions by stating an upper bound M for the lengths of descending sequences. The argument goes roughly as follows: if the function f is nondecreasing, then we have the constant function $f(M)$ as a majorization for f in the interval $[0, M]$; subsequently, we can apply assertion 2 of Lemma 4.3 and use the formula of assertion 4 of Lemma 4.6 to show that, if M is chosen sufficiently big and if f does not grow too quickly, then the number of possible descents is less than M.

We start with the following inequality used later.

Lemma 4.9 *Let $n, k > 0$, then $(2_n)_k \leqslant 2_{n+2(k-1)}$.*

Proof By induction on k. □

The next theorem generalizes [118, Theorem 3] in the presence of g; as before, for the threshold function we take the maximum over an initial segment of a suitable function involving $\tilde{g}^{-1}$.

Theorem 4.5 (Phase Transition, Provable Version) *Let g be as before, $\alpha < \varepsilon_0$ and define*

$$f_\alpha(i) := \max_{0 \leqslant k \leqslant i} \left|\tilde{g}^{-1}(k)\right|_{H_\alpha^{-1}(k)},$$

then the following assertions hold:

1. $PA \vdash \left(G^g_{f_\alpha}\right)$;
2. $PA \vdash \left(\bar{G}^g_{f_\alpha}\right)$;
3. $PA \vdash \left(H^g_{f_\alpha}\right)$;
4. $PA \vdash \left(\bar{H}^g_{f_\alpha}\right)$;
5. $PA \vdash \left(MC^g_{f_\alpha}\right)$.

Proof Again we mimic the corresponding proof in [118], adding a proper treatment of g and $\tilde{g}^{-1}$. We note that, by Corollary 4.3 and Lemma 4.7, it suffices to prove the last assertion. If $\alpha < \omega$, then $f_\alpha(i) \leqslant \alpha$ for all i, since H_α^{-1} is linear for $i \geqslant \alpha$, and we are done by Lemma 4.6.3. Generally speaking, given an α, if $\tilde{g}^{-1}(i)$ grows too slowly with respect to $H_\alpha(i)$, then $f_\alpha(i)$ is bounded and, again, we are done by Lemma 4.6.3. More precisely, from side considerations regarding the growth rate of H_α (e.g. Lemma 4.11), we have that at least for $\alpha < \omega^3$, $f_\alpha(i)$ is bounded and we are done.

Assume $\omega^3 \leqslant \alpha < \varepsilon_0$, let $\beta := \omega^{\alpha+4} \cdot 2$, suppose K is given and assume

$$\omega_K \geqslant \alpha_n > \cdots > \alpha_0$$

with $mc(\alpha_i) \leqslant K + f_\alpha(g^{i-1}(1))$. Put

$$M(K) := 2_{H_\alpha(H_\beta(K))}.$$

We prove $n < M(K)$ by contradiction. Assume otherwise; then we have $\alpha_{M(K)} > \cdots > \alpha_0$ with $mc(\alpha_i) \leqslant K + f_\alpha(g^{i-1}(1))$, and, since f_α is weakly increasing,

$$mc(\alpha_i) \leqslant K + f_\alpha\big(g^{M(K)-1}(1)\big) \tag{4.6}$$

for all $i \leqslant M(K)$.

Finally, we obtain that

$$\begin{aligned}
M(K) &\leqslant \#\{\alpha<\omega_K : mc(\alpha)<K+f_\alpha\big(g^{M(K)-1}(1)\big)\}\\
&\leqslant \omega_K(\omega\mapsto K+f_\alpha\big(g^{M(K)-1}(1)\big)+1)\\
&= \Big(K+1+\max_{0\leqslant k\leqslant g^{M(K)-1}(1)}|\tilde{g}^{-1}(k)|_{H_\alpha^{-1}(k)}\Big)_K(1)\\
&\leqslant \Big(K+1+|M(K)|_{H_\alpha^{-1}(M(K))}\Big)_K(1)\\
&= \left(K+1+\left|2_{H_\alpha\left(H_\beta(K)\right)}\right|_{H_\alpha^{-1}\left(2_{H_\alpha\left(H_\beta(K)\right)}\right)}\right)_K(1)\\
&\leqslant \left(K+1+\left|2_{H_\alpha\left(H_\beta(K)\right)}\right|_{H_{\omega^\alpha}(K)}\right)_K(1)\\
&= \Big(K+1+2_{H_\alpha\left(H_\beta(K)\right)-H_{\omega^\alpha}(K)}\Big)_K(1)\\
&< 2_{H_\alpha\left(H_\beta(K)\right)}\\
&= M(K),
\end{aligned}$$

which would yield a contradiction.

The third inequality follows from the fact that $g^{M(K)-1}(1)\leqslant g^{M(K)}(M(K))=\tilde{g}(M(K))$ and that $g^{M(K)-1}(1)\geqslant M(K)$; the fourth inequality follows from $H_\alpha^{-1}\left(2_{H_\alpha(H_\beta(K))}\right)\geqslant H_{\omega^\alpha}(K)$, which is equivalent to $2_{H_\alpha(H_\beta(K))}\geqslant H_\alpha\left(H_{\omega^\alpha}(K)\right)$ which is trivially true. The last inequality

$$\big(K+1+2_{H_\alpha(H_\beta(K))-H_{\omega^\alpha}(K)}\big)_K(1)<2_{H_\alpha(H_\beta(K))}$$

follows by a side calculation which used Lemma 4.9. □

4.2.3 Results Concerning the Fragments of PA

In this paragraph, which extends [118, Section 4] with the generic starting function g, we consider restricted versions of Hydra principles which are related to the fragments $I\Sigma_n$ of Peano arithmetic where the induction scheme is restricted to formulas of quantifier complexity Σ_n; the phase transition thresholds derive mainly from the following property $I\Sigma_n\nvdash\forall x\,\exists y\,H_{\omega_{n+1}}(x)=y$, which is treated in full detail in [65] or [74]. Since the structure of the results of this section is the same as the previous one, proofs are basically a rewriting and thus are omitted. Finally, since the iteration functions of this subsection may not have values in $\mathbb{N}$, we adopt the following convention: for functions which have not values in $\mathbb{N}$, we tacitly consider their floor; i.e., if $f\colon\mathbb{N}\to\mathbb{R}$, by $f(i)$ we denote $\lfloor f(i)\rfloor$.

Definition 4.11 *Let $f, g\colon \mathbb{N} \to \mathbb{N}$ be as before; we define the following restricted versions of the principles in Def. 4.10*

$$
\begin{aligned}
\left(\bar{G}^n_{f,g}\right) &:\Longleftrightarrow \quad \forall K\, \exists M \left(\omega_n(K) \succ^{P,M}_{f,g} 0\right)\\
\left(\bar{H}^n_{f,g}\right) &:\Longleftrightarrow \quad \forall K\, \exists M \left(\omega_n(K) \succ^{Q,M}_{f,g} 0\right)\\
\left(MC^n_{f,g}\right) &:\Longleftrightarrow \quad \forall K\, \exists M\, \forall \alpha_0, \dots \alpha_M \leqslant \omega_n(K)\\
&\qquad\quad [\forall i \leqslant M\, (mc(\alpha_i) \leqslant K + f(g^{i-1}(1))) \Rightarrow \exists i < M\, (\alpha_{i+1} \geqslant \alpha_i)]
\end{aligned}
$$

For the principles $(G^n_{f,g})$ and $(H^n_{f,g})$ there exist corresponding combinatorial principles where the base representation of the numbers involved stops at height n and where the hydras are bounded in height by n (i.e. they are smaller than ω_{n+1}).

Corollary 4.4

$$I\Sigma_n \vdash (MC^n_{f,g}) \Rightarrow I\Sigma_n \vdash (\bar{H}^n_{f,g}) \Rightarrow I\Sigma_n \vdash (\bar{G}^n_{f,g}).$$

Proof Similarly as before. □

The following three statements correspond to Proposition 4.1, Proposition 4.3 and Lemma 4.8.

Proposition 4.4 *Let $f, g\colon \mathbb{N} \to \mathbb{N}$, where f is a weakly increasing function such that $f(n) \geqslant n$ and g is a strictly increasing function such that $g(n) \geqslant n + 1$, then*

1. $PA \nvdash (\bar{G}^n_{f,g})$;
2. $PA \nvdash (\bar{H}^n_{f,g})$;
3. $PA \nvdash (MC^n_{f,g})$;

Proof Similarly as before. □

Proposition 4.5 *Let $m \geqslant 1$, $n \geqslant 1$, g as before and put $f(i) := \sqrt[m]{|\tilde{g}^{-1}(i)|_{n-1}}$. For a given ordinal $\alpha < \omega_n(m)$, define $\beta := \omega_n(m) \cdot \alpha + \omega_n(m)$. Then there exists an $i \geqslant H_\alpha(1)$ and some $\delta > 0$ such that $\beta \succ^{P,i}_{f,g} \delta$.*

Proof similarly to Proposition 4.3. □

Lemma 4.10 *Let $m \geqslant 2$, $n \geqslant 1$, g as before and put $f(i) := \max_{0 \leqslant k \leqslant i} \sqrt[H^{-1}_{\omega_{n+1}}(k)]{|\tilde{g}^{-1}(k)|_{n-1}}$. Let $\alpha = \omega_n(m) \cdot \omega_n(m) + \omega_n(m)$ and $i_0 := H_{\omega_n}(1)$, then $\alpha \succ^{P,i_0}_{f,g} \delta$ for some $\delta > 0$.*

Proof similarly to Lemma 4.8, using this time Proposition 4.5. □

Finally, we can state the corresponding versions, for fragments of PA, of Theorem 4.4 and Theorem 4.5.

Theorem 4.6 (Phase Transition, Unprovable Version) *Let g be as before and fix*

$$f(i) := \max_{0 \leqslant k \leqslant i} \sqrt[H^{-1}_{\omega_{n+1}}(k)]{|\tilde{g}^{-1}(k)|_{n-1}},$$

then the following unprovability results hold:

1. $I\Sigma_n \nvdash (\bar{G}^n_{f,g})$;
2. $I\Sigma_n \nvdash (\bar{H}^n_{f,g})$;
3. $I\Sigma_n \nvdash (MC^n_{f,g})$.

Proof Similarly to Theorem 4.4, using this time Lemma 4.10. □

Theorem 4.7 (Phase Transition, Provable Version) *Let $\alpha < \omega_{n+1}$, g as before and fix*

$$f_\alpha(i) := \max_{0 \leqslant k \leqslant i} \sqrt[H^{-1}_{\alpha}(k)]{|\tilde{g}(k)|_{n-1}},$$

the the following provability results hold:

1. $I\Sigma_n \vdash (\bar{G}^n_{f_\alpha,g})$;
2. $I\Sigma_n \vdash (\bar{H}^n_{f_\alpha,g})$;
3. $I\Sigma_n \vdash (MC^n_{f_\alpha,g})$.

Proof Similarly to Theorem 4.5. □

4.3 Application to Transfinite Function Hierarchies

In this last section, we apply previous results, in particular the ones regarding phase transitions for fragments of PA, to obtain phase transition thresholds in combinatorics. More precisely, we study the transition between different levels of complexity (primitive recursive, recursive, multiply recursive [135]) for a suitable transfinite extension of Ackermann hierarchy. Firstly, we summarize previous results, mainly due to Omri and Weiermann [130], regarding the transition from primitive recursive to not primitive recursive for some versions of Ackermann function; secondly, we generalize the aforementioned results in the same spirit as before, namely we consider a further auxiliary function g and study the new phase transition threshold.

4.3.1 Ackermann Hierarchy and Previous Results

In this paragraph, we present the main definitions regarding Ackermann hierarchy together with the results already established by Omri and Weiermann to whom article [130] we refer for proofs. For what concerns notation, in order to keep it concordant with the previously one, we slightly differ from the one used in [130];[5] moreover, as before all functions are assume to have non negative integer values, if needed we implicitly consider their floor.

We start with one of the standard versions of Ackermann function.

Definition 4.12 *Let us define:*

$$A_0(n) := n+1,\ A_{k+1}(n) := A_k^{n+1}(n),\ A_\omega(n) := A_n(n),$$

then $Ack(n) = A_\omega(n)$ *is the* ACKERMANN FUNCTION.

It is well-know (see e.g. [38]) that each level A_k is primitive recursive and, moreover, each primitive recursive function is eventually majorized by some A_k; thus Ack, which eventually majorizes every level A_k, is not primitive recursive.

We now generalize the Ackermannian hierarchy considering two auxiliary functions g, f (having the same restrictions as before) with g being the new starting function and f the iteration function.

Definition 4.13 *Given* f *and* g *as before, we define:*

$$A[g,f]_0(n) := g(n),\ A[g,f]_{k+1}(n) := A[g,f]_k^{f(n)+1}(n),\ A[g,f]_\omega(n) := A[g,f]_n(n).$$

We some times denote $A[g,f]_k$ as $A_k^{f,g}$.[6]

Omri and Weiermann [130] investigated the transition between primitive recursiveness and recursiveness for the function $A[g,f]_\omega$, particularly with respect to the function parameter f; we briefly recall their results.

Theorem 4.8 *Let* $g(i) := i+1$ *and fix*

$$f_\alpha(i) := \sqrt[A_\alpha^{-1}(i)]{i}$$

then $A[g,f_\alpha]_\omega$ *is primitive recursive iff* $\alpha < \omega$.

Proof See [130, Theorem 1]. □

Theorem 4.9 *Given a natural number* l*, define*

$$g_l(i) := 2_l(|i|_l + 1) \text{ and } f_\alpha^l := \sqrt[A_\alpha^{-1}(i)]{|i|_l}$$

then $A[g_l,f_\alpha^l]_\omega$ *is primitive recursive iff* $\alpha < \omega$.

Proof This is a slight extension of Theorem 2 and Theorem 4 in [130]. □

[5] The three main changes are: the function symbol f instead of h for the iteration function; an additional "+1" and A instead of B in the definition of the Ackermann hierarchy.

[6] The usefulness of this inverted notation for f and g will be clear in the forthcoming Lemma 4.11.

4.3.2 Phase Transition Thresholds for Transfinite Hierarchies

In this last paragraph, we extend the aforementioned results along two paths: firstly, we generalize Theorem 4.8 to any strictly increasing starting function g; secondly, we consider phase transitions for the transfinite extension of the Ackermannian hierarchy. In both cases, a crucial role is played by the connection between the transfinite Ackermannian hierarchy and Hardy hierarchy; this connection allows to apply previous results about phase transitions in fragment of PA.

We start defining the generalize transfinite extension of the Ackermannian hierarchy $A^{f,g}_\alpha$; for sake of comparison, we recall also the Hardy hierarchy $H^{f,g}_\alpha$.

Definition 4.14 *Given f and g as before and $\alpha, \lambda < \varepsilon_0$, we define:*

$$A^{f,g}_0(x) := g(x) \qquad A^{f,g}_{\alpha+1}(x) := \left(A^{f,g}_\alpha\right)^{f(n)+1}(x) \qquad A^{f,g}_\lambda(x) := A^{f,g}_{\lambda[f(n)]}(x)$$

$$H^{f,g}_0(x) := x \qquad H^{f,g}_{\alpha+1}(x) := H^{f,g}_\alpha(g(x)) \qquad H^{f,g}_\lambda(x) := H^{f,g}_{\lambda[f(n)]}(x)$$

The tight connection between these two hierarchies is given by the first point of the following folklore lemma.

Lemma 4.11 *Let f and g be as before, then the followings hold:*

1. *for all $\alpha < \varepsilon_0$, $A^{f,g}_\alpha(x) = H^{f,g}_{\omega^\alpha}(x)$;*
2. *for all n, d, i, $H^{f,g}_{\omega_n(d)}(i) \leqslant H^{f,g}_{\omega_n(d+1)}(i)$.*

Proof By induction: on α the first point, on d the second. □

Before stating our main result of this section, we recall a classic theorem regarding the classification of primitive recursive functions, as well as some immediate consequences of our previous results regarding fragments of PA.

Theorem 4.10 *Let $h\colon \mathbb{N} \to \mathbb{N}$, then the following are equivalent*

1. *h is primitive recursive;*
2. *$I\Sigma_1 \vdash \forall K\, \exists M\, h(K) = M$.*

Namely, h is primitive recursive iff is provably total in $I\Sigma_1$.

Proof see for example [65]. □

Proposition 4.6 *Let $\alpha < \varepsilon_0$, g as before and define $f_\alpha(i) := \max_{0 \leqslant k \leqslant i} \sqrt[H_\alpha^{-1}(k)]{\tilde{g}^{-1}(k)}$, then the following are equivalent:*

1. *$I\Sigma_1 \vdash \bar{G}^1_{f_\alpha,g} : \forall K\, \exists M \left(\omega^K \succ^{P,M}_{f_\alpha,g} 0\right)$;*

2. *$I\Sigma_1 \vdash \forall K\, \exists M\, H^{f_\alpha,g}_{\omega^K}(1) = M$;*

3. *$K \mapsto H^{f_\alpha,g}_{\omega^K}(1)$ is a primitive recursive function:*

4. *$\alpha < \omega^\omega$.*

Proof 1. $\iff$ 2. $\iff$ 4. by Lemma 4.4, Theorem 4.6 and Theorem 4.7; 2. $\iff$ 3. by Theorem 4.10. □

Proposition 4.6 can be easily generalized to $I\Sigma_n$ for $n \geqslant 2$.

We are now able to extend Theorem 4.8 to a generic strictly increasing elementary recursive starting function g with $g(n) \geqslant n + 1$.

Theorem 4.11 *Let g be as before and define*

$$f_\alpha(i) := \max_{0 \leqslant k \leqslant i} \sqrt[A_\alpha^{-1}(k)]{\tilde{g}^{-1}(k)}$$

then $A[g, f_\alpha]_\omega$ is primitive recursive iff $\alpha < \omega$.

Proof By Lemma 4.11, it suffices to prove that $A[g, f_\alpha]_\omega(K) = A^{f_\alpha,g}_\omega(K) = H^{f_\alpha,g}_{\omega^\omega}(K)$ with $f_\alpha(i) = \max_{0 \leqslant k \leqslant i} \sqrt[A_\alpha^{-1}(k)]{\tilde{g}^{-1}(k)} = \max_{0 \leqslant k \leqslant i} \sqrt[H_{\omega^\alpha}^{-1}(k)]{\tilde{g}^{-1}(k)}$ is primitive recursive iff $\alpha < \omega$. We exploit now the striking resemblance with Proposition 4.6; more precisely we need to prove that:

1. for $\alpha < \omega$, $H^{f_\alpha,g}_{\omega^\omega}(K)$ is primitive recursive in $H^{f_\alpha,g}_{\omega^K}(1)$;

2. for $\alpha = \omega$, $H^{f_\alpha,g}_{\omega^K}(1)$ is primitive recursive in $H^{f_\alpha,g}_{\omega^\omega}(K)$.

We prove these two points separately; moreover, for sake of readability, we simply write f instead of f_α.

1. $[\alpha < \omega]$ In this case, for all $K \geqslant 2$, we have

$$\begin{aligned} H^{f,g}_{\omega^\omega}(K) &= H^{f,g}_{\omega^{f(K)+1}}(K) \\ &\leqslant H^{f,g}_{\omega^K}(K) \\ &\leqslant H^{f,g}_{\omega^K}\left(H^{f,g}_{\omega^K}(1)\right) \\ &= H^{f,g}_{\omega^K \cdot 2}(1) \\ &\leqslant H^{f,g}_{\omega^{K+1}}(1) \\ &\leqslant H^{f,g}_{\omega^{\left(H^{f,g}_{\omega^K}(1)\right)}}(1). \end{aligned}$$

The first equality is just the Def. 4.9; the first two and the last inequalities derived from Lemma 4.11.2 together with the fact that, for all K, $H^{f,g}_{\omega^K}$ is a weakly increasing function and $K < H^{f,g}_{\omega^K}(1)$; the second equality from Lemma 4.5 and the second-last inequality from Corollary 4.2 and Lemma 4.5.

Since for $\alpha < \omega$ the function $H^{f,g}_{\omega^K}(1)$ is primitive recursive and $H^{f,g}_{\omega^\omega}(K)$ is bounded by a double iteration of $H^{f,g}_{\omega^K}(1)$, then $H^{f,g}_{\omega^\omega}(K)$ is primitive recursive.

2. $[\alpha = \omega]$ Assume that $H^{f,g}_{\omega^\omega}(K)$ is primitive recursive. In this case, also the function $\mathbb{G}\colon \mathbb{N} \to \mathbb{N}$ define as

$$\mathbb{G}(K) := \tilde{g}\left(K^{H^{f,g}_{\omega^\omega}(K)}\right)$$

is primitive recursive, since g and $\tilde{g}$ are primitive recursive. In particular, there exists K_0 such that, for all $K \geqslant K_0$

$$\mathbb{G}(K) \leqslant H_{\omega^\omega}(K).$$

Since $H^{-1}_{\omega^\omega}$ is a weakly increasing function, for all $K \geqslant K_0$, we have

$$H^{-1}_{\omega^\omega}(\mathbb{G}(K)) \leqslant H^{-1}_{\omega^\omega}\left(H_{\omega^\omega}(K)\right) \leqslant K, \tag{4.7}$$

hence, for $K \geqslant K_0$, it holds that

$$f(\mathbb{G}(K)) = \max_{0 \leqslant k \leqslant K} \sqrt[H^{-1}_{\omega^\omega}(\mathbb{G}(k))]{\tilde{g}^{-1}(\mathbb{G}(k))} \geqslant \max_{0 \leqslant k \leqslant K} \sqrt[k]{k^{H^{f,g}_{\omega^\omega}(k)}} \geqslant K$$

where the inequalities come from (4.7) and the definition of $\mathbb{G}$.

Finally, for all $K \geqslant K_0$, we have

$$H^{f,g}_{\omega^K}(1) \leqslant H^{f,g}_{\omega^{f(\mathbb{G}(K))+1}}(1) \leqslant H^{f,g}_{\omega^{f(\mathbb{G}(K))+1}}(\mathbb{G}(K)) = H^{f,g}_{\omega^\omega}(\mathbb{G}(K)),$$

thus, if $H^{f,g}_{\omega^\omega}(K)$ is primitive recursive, so it is $H^{f,g}_{\omega^K}(1)$. □

The last theorem can be extended to the multiple recursive case to obtain the following.

Theorem 4.12 *Let g as above and define*

$$f_\alpha(i) := \max_{0 \leqslant k \leqslant i} \sqrt[A^{-1}_\alpha(i)]{|\tilde{g}^{-1}(i)|}$$

then $A[g,f_\alpha]_{\omega^\omega}$ is multiple recursive iff $\alpha < \omega^\omega$.

Proof The proof is analogous to Theorem 4.11. In this case we use the $I\Sigma_2$ version of Proposition 4.6 and the following characterization: $h\colon \mathbb{N} \to \mathbb{N}$ is multiple recursive iff $I\Sigma_2 \vdash \forall K\, \exists M\, h(K) = M$. □

Bibliography

[1] P. Aczel. An introduction to inductive definitions. In J. Barwise, editor, *Handbook of Mathematical Logic*, volume 90 of *Stud. Logic Found. Math.*, pages 739–782. North-Holland, 1977.

[2] P. Aczel. The Type Theoretic Interpretation of Constructive Set Theory. In *Logic Colloquium '77*, volume 96, pages 55–66. Elsevier, 1978.

[3] P. Aczel. The Type Theoretic Interpretation of Constructive Set Theory: Choice Principles. In A.S. Troelstra and D. van Dalen, editors, *The L. E. J. Brouwer Centenary Symposium*, volume 110 of *Studies in Logic and the Foundations of Mathematics*, pages 1–40. Elsevier, 1982.

[4] P. Aczel. The Type Theoretic Interpretation of Constructive Set Theory: Inductive Definitions. In Ruth Barcan Marcus, Georg J.W. Dorn, and Paul Weingartner, editors, *Logic, Methodology and Philosophy of Science VII*, volume 114 of *Studies in Logic and the Foundations of Mathematics*, pages 17–49. Elsevier, 1986.

[5] P. Aczel and M. Rathjen. Notes on constructive set theory. Technical report, Institut Mittag–Leffler, 2000. Report No. 40.

[6] P. Aczel and M. Rathjen. Constructive set theory. Book draft, 2010.

[7] B. Afshari and M. Rathjen. Reverse mathematics and well-ordering principles: A pilot study. *Annals of Pure and Applied Logic*, 160(3):231–237, 2009.

[8] J.P. Aguilera, F. Pakhomov, and A. Weiermann. Modern perspectives in Proof Theory. *Philosophical transactions of the Royal Society of London. Series A: Mathematical, physical, and engineering sciences*, 381(2248), 2023.

[9] E. Aichinger and F. Aichinger. Dickson's Lemma, Higman's Theorem and Beyond: A survey of some basic results in order theory. *Expositiones mathematicae*, 38(4):537–547, 2020.

[10] T. Arai. Derivatives of normal functions and ω-models. *Archive for mathematical logic*, 57(5-6):649–664, 2017.

[11] T. Arai. *Ordinal Analysis with an Introduction to Proof Theory*. Logic in Asia: Studia Logica Library. Springer Nature, Singapore, 1st edition 2020 edition, 2020.

[12] T. Arai. Proof-theoretic strengths of the well-ordering principles. *Archive for mathematical logic*, 59(3-4):257–275, 2020.

[13] J. Avigad. Number Theory and Elementary Arithmetic. *Philosophia Mathematica. Series III*, 3:257–284, 10 2003.

[14] A. Bauer. Realizability as the connection between computable and constructive mathematics, 2005. `http://math.andrej.com/asset/data/c2c.pdf`.

[15] A. Bauer. An injection from the Baire space to natural numbers. *Math. Structures Comput. Sci.*, 25(7):1484–1489, 2015.

[16] L.D. Beklemishev. Induction rules, reflection principles, and provably recursive functions. *Annals of pure and applied logic*, 85(3):193–242, 1997.

[17] L.D. Beklemishev. Proof-theoretic analysis by iterated reflection. *Archive for mathematical logic*, 42(6):515–552, 2003.

[18] L.D. Beklemishev. Reflection principles and provability algebras in formal arithmetic. *Russian mathematical surveys*, 60(2):197–268, 2005.

[19] S. Berardi, G. Buriola, and P. Schuster. A General Constructive Form of Higman's Lemma. In Aniello Murano and Alexandra Silva, editors, *32nd EACSL Annual Conference on Computer Science Logic (CSL 2024)*, volume 288 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:17, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[20] S. Berardi and S. Steila. Ramsey's Theorem for Pairs and k Colors as a sub-Classical Principle of Arithmetic. *J. Symbolic Logic*, 82(2):737–753, 2017.

[21] J. Berger. Dickson's Lemma and Higman's Lemma are Equivalent. *South American Journal of Logic*, 2(1):35–39, 2016.

[22] J. Berger and P. Schuster. Dini's Theorem in the Light of Reverse Mathematics. In *Logicism, Intuitionism, and Formalism*, Synthese Library, pages 153–166. Springer Netherlands, Dordrecht, 2009.

[23] S. Berghofer. A Constructive Proof of Higman's Lemma in Isabelle. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 3085 of *Lecture Notes in Computer Science*, pages 66–82, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[24] E. Bishop. *Foundations of Constructive Analysis.* New York, NY, USA: Mcgraw-Hill, 1967.

[25] A. Blass. Well-Ordering and Induction in Intuitionistic Logic and Topoi. In D.W Kueker, F.G.K. Lopez-Escobar, and C.H. Smith, editors, *Mathematical Logic and Theoretical Computer Science.* Taylor & Francis Group, United Kingdom, 1986.

[26] A. Blass and Y. Gurevich. Program termination and well partial orderings. *ACM Trans. Comput. Log.*, 9(3):18:1–18:26, 2008.

[27] I. Blechschmidt. *Using the internal language of toposes in algebraic geometry.* PhD thesis, University of Augsburg, 2017.

[28] I. Blechschmidt. Generalized spaces for constructive algebra. In K. Mainzer, P. Schuster, and H. Schwichtenberg, editors, *Proof and Computation II*, pages 99–187. World Scientific, 2021.

[29] I. Blechschmidt. Exploring mathematical objects from custom-tailored mathematical universes. In G. Oliveri, C. Ternullo, and S. Boscolo, editors, *Objects, structures, and logics: FilMat studies in the philosophy of mathematics.* Springer, 2022.

[30] D. Bridges, E. Palmgren, and H. Ishihara. Constructive Mathematics. In Edward N. Zalta and Uri Nodelman, editors, *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab, Stanford University, Fall 2022 edition, 2022. `https://plato.stanford.edu/archives/fall2022/entries/mathematics-constructive/`.

[31] L.E.J. Brouwer and H. Freudenthal. *L. E. J. Brouwer collected works: Geometry, analysis, topology and mechanics.* Number v. 2. North-Holland, 1976.

[32] L.E.J. Brouwer and A. Heyting. *L. E. J. Brouwer collected works: Philosophy and foundations of mathematics.* Number v. 1. North-Holland, 1975.

[33] W. Buchholz. A new system of proof-theoretic ordinal functions. *Annals of pure and applied logic*, 32(C):195–207, 1986.

[34] W. Buchholz. An independence result for $(\Pi^1_1 - CA) + BI$. *Annals of Pure and Applied Logic*, 33:131–155, 1987.

[35] W. Buchholz. A Survey on Ordinal Notations Around the Bachmann–Howard Ordinal. In *Feferman on Foundations*, volume 13 of *Outstanding Contributions to Logic*, pages 71–100. Springer International Publishing, Cham, 2018.

[36] W. Buchholz, A. Cichon, and A. Weiermann. A Uniform Approach to Fundamental Sequences and Hierarchies. *Mathematical Logic Quarterly*, 40(2):273–286, 1994.

[37] G. Buriola, P. Schuster, and I. Blechschmidt. A Constructive Picture of Noetherian Conditions and Well Quasi-orders. In Gianluca Della Vedova, Besik Dundua, Steffen Lempp, and Florin Manea, editors, *Unity of Logic and Computation*, pages 50–62, Cham, 2023. Springer Nature Switzerland.

[38] C. Calude. Theories of Computational Complexity. volume 35. Elsevier Science & Technology, The Netherlands, 1988.

[39] L. Carlucci, G. Lee, and A. Weiermann. Classifying the phase transition threshold for regressive Ramsey functions. 2006.

[40] L. Carlucci, G. Lee, and A. Weiermann. Sharp thresholds for hypergraph regressive Ramsey numbers. *Journal of combinatorial theory. Series A*, 118(2):558–585, 2011.

[41] L. Carlucci, L. Mainardi, and M. Rathjen. A Note on the Ordinal Analysis of $\mathrm{RCA}_0 + WO(\sigma)$. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 11558, pages 144–155, 2019.

[42] R. Carroy and Y. Pequignot. Well, Better and In-Between. In P. Schuster, M. Seisenberger, and A. Weiermann, editors, *Well-Quasi Orders in Computation, Logic, Language and Reasoning*, 2020.

[43] P. Cholak, A. Marcone, and R. Solomon. Reverse mathematics and the equivalence of definitions for well and better quasi-orders. *The Journal of symbolic logic*, 66(1):683–55, 2004.

[44] E.A. Cichon. A Short Proof of Two Recently Discovered Independence Results Using Recursion Theoretic Methods. *Proceedings of the American Mathematical Society*, 87(4):704–706, 1983.

[45] P. Clote. The metamathematics of Fraïssé's order type conjecture. In *Recursion Theory Week*, Lecture Notes in Mathematics, pages 41–56. Springer Berlin Heidelberg, Berlin, Heidelberg, 1990.

[46] P.M. Cohn. *Universal Algebra*. Springer Netherlands, 1981.

[47] T. Coquand. Notions invariant by change of basis, 2001. Unpublished Manuscript. `https://www.cse.chalmers.se/~coquand/base.ps`.

[48] T. Coquand and D. Fridlender. A proof of Higman's lemma by structural induction. Unpublished Manuscript. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.47.486`, November 1993.

[49] T. Coquand and H. Lombardi. Krull's Principal Ideal Theorem. Technical Report 30, Institut Mittag-Leffler, 2000/2001.

[50] T. Coquand and H. Persson. Gröbner bases in type theory. In T. Altenkirch, B. Reus, and W. Naraschewski, editors, *TYPES 1998: Types for Proofs and Programs*, volume 1657 of *Lecture Notes in Comput. Sci.*, pages 33–46. Springer, 1999.

[51] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate texts in mathematics. Springer International Publishing AG, Cham, 2015.

[52] L. Crosilla. Set Theory: Constructive and Intuitionistic ZF. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Summer 2020 edition, 2020.

[53] L. Crosilla and P. Schuster. Finite Methods in Mathematical Practice. In Godehard Link, editor, *Formalism and Beyond*, pages 351–410. De Gruyter, Berlin, München, Boston, 2014.

[54] G. Curi. On Tarski's fixed point theorem. *Proceedings of the American Mathematical Society*, 143(10):4439–4455, 2015.

[55] D.H.J. de Jongh and R. Parikh. Well-partial orderings and hierarchies. *Indagationes Mathematicae*, 39:195–207, 1977.

[56] M. De Smet and A Weiermann. Sharp Thresholds for a Phase Transition Related to Weakly Increasing Sequences. *Journal of logic and computation*, 22(2):207–211, 2012.

[57] M. De Smet and A. Weiermann. Phase Transitions Related to the Pigeonhole Principle. In Arnold Beckmann, Erzsébet Csuhaj-Varjú, and Klaus Meer, editors, *Language, Life, Limits*, pages 123–132, Cham, 2014. Springer International Publishing.

[58] N. Dershowitz. Orderings for term-rewriting systems. *Theoretical Computer Science*, 17(3):279–301, 1982.

[59] N. Dershowitz. Termination of rewriting. *Journal of Symbolic Computation*, 3(1):69–115, 1987.

[60] R. Diaconescu. Axiom of Choice and Complementation. *Proceedings of the American Mathematical Society*, 51(1):176–178, 1975.

[61] H. Diener and H. Ishihara. Bishop-Style Constructive Reverse Mathematics. In *Handbook of Computability and Complexity in Analysis*, Theory and Applications of Computability, pages 347–365. Springer International Publishing, Cham, 2021.

[62] R.G. Downey, D.R. Hirschfeldt, S. Lempp, and R. Solomon. Computability-theoretic and proof-theoretic aspects of partial and linear orderings. *Israel journal of mathematics*, 138(1):271–289, 2003.

[63] P. Dybjer and E. Palmgren. Intuitionistic Type Theory. In Edward N. Zalta and Uri Nodelman, editors, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Spring 2023 edition, 2023.

[64] D. Dzhafarov and C. Mummert. *Reverse Mathematics: Problems, Reductions, and Proofs*. Theory and Applications of Computability. Springer International Publishing AG, Cham, 1 edition, 2022.

[65] M. Fairtlough and S.S. Wainer. Hierarchies of provably recursive functions. In Samuel Buss, editor, *Handbook of proof theory*, volume 137, pages 149–207. Elsevier, Amsterdam, 1998.

[66] G. Fellin, P. Schuster, and D. Wessel. The jacobson radical of a propositional theory. *The bulletin of symbolic logic*, 28(2):163–181, 2022.

[67] G. Ferreira and P. Oliva. On various negative translations. *Electronic Proceedings in Theoretical Computer Science, EPTCS*, 47(Proc. CL & C 2010):21–33, 2011.

[68] A. Freund. *Type-Two Well-Ordering Principles, Admissible Sets, and* Π^1_1-*Comprehension*. PhD thesis, Univ. of Leeds, UK, 2018.

[69] A. Freund. Π^1_1-comprehension as a well-ordering principle. *Advances in Mathematics*, 355:106767, 2019.

[70] A. Freund. From Kruskal's theorem to Friedman's gap condition. *Mathematical Structures in Computer Science*, 30:952–975, 2020.

[71] A. Freund and M. Rathjen. Well ordering principles for iterated Π^1_1-comprehension. *Selecta mathematica (Basel, Switzerland)*, 29(5), 2023.

[72] D. Fridlender. *Higman's Lemma in Type Theory.* PhD thesis, Chalmers University of Technology, Göteborg, 1997.

[73] H. Friedman. Some systems of second order arithmetic and their use. In *in Proceedings of the International Congress of Mathematicians, Vancouver 1974*, pages 235–242, 1975.

[74] H. Friedman and M. Sheard. Elementary descent recursion and proof theory. *Annals of pure and applied logic*, 71(1):1–45, 1995.

[75] H. Friedman, S.G. Simpson, and R.L. Smith. Countable algebra and set existence axioms. *Annals of Pure and Applied Logic*, 25(2):141–181, 1983. Addendum, vol.28 (1985), pp. 320-321.

[76] E. Frittaion and A. Marcone. Linear extensions of partial orders and reverse mathematics. *Mathematical logic quarterly MLQ.*, 58(6):417–423, 2012.

[77] J.H. Gallier. What's so special about Kruskal's theorem and the ordinal Γ_0? A survey of some results in proof theory. *Annals of Pure and Applied Logic*, 53(3):199–260, 1991.

[78] A. Gelfond. Sur le septième problème de Hilbert. *Bulletin de l'Académie des Sciences de l'URSS. Classe des sciences mathématiques et na*, 4:623–634, 1934.

[79] G. Gentzen. Die Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische annalen*, 112(1):493–565, 1936.

[80] G. Gentzen. Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie. *Mathematische annalen*, 119(1):140–161, 1943.

[81] J. Girard. *Proof theory and logical complexity.* Studies in proof theory. Bibliopolis, Napoli, 1987.

[82] Y. Glivenko. Sur quelques points de la logique de M. Brouwer. *Bulletin de la Classe des sciences. Académie royale de Belgique*, 15(3):183–188, 1929.

[83] K. Gödel. Über formal unentscheidbare sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38(1):173–198, Dec 1931.

[84] K. Gödel. Zur intuitionistischen arithmetik und zahlentheorie. *Ergebnisse eines mathematischen Kolloquiums*, 4(1933):34–38, 1933. Reprinted in English translation as "On intuitionistic arithmetic and number theory" in *The Undecidable*, M. Davis, ed., pp. 75–81.

[85] L. Gordeev and A. Weiermann. Phase transitions in Proof Theory. *Discrete Mathematics and Theoretical Computer Science*, (Proceedings):343–358, 2010.

[86] L. Gordeev and A. Weiermann. Phase transitions of iterated Higman-style well-partial-orderings. *Archive for mathematical logic*, 51(1-2):127–161, 2012.

[87] J. Goubault-Larrecq. A Constructive Proof of the Topological Kruskal Theorem. In Krishnendu Chatterjee and Jirí Sgall, editors, *Mathematical Foundations of Computer Science 2013*, pages 22–41, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[88] J. Hamkins and A. Lewis. Infinite time Turing machines. *J. Symbolic Logic*, 65(2):567–604, 2000.

[89] L.A. Harrington, M.D. Morley, A. Šcedrov, and S. G. Simpson. *Harvey Friedman's Research on the Foundations of Mathematics.* Elsevier, 1985.

[90] R. Hasegawa. Well-Ordering of Algebra and Kruskal's Theorem. *Logic, Language and Computation. Festschrift in Honor of Satory Takasu*, 1994. volume 792 of *Lecture Notes in Computer Science* pages 133–172.

[91] T.L. Heath. *The Thirteen Books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix.* Dover Publications Inc., New York, 1956. Translated with introduction and commentary by Thomas L. Heath, 2nd ed.

[92] G. Higman. Ordering by divisibility in abstract algebras. *Proc. London Math. Soc. 3*, 2:326–336, 1952.

[93] D. Hilbert. On the Infinite. In J. van Heijenoort, editor, *From Frege to Gödel: A Source Book in Mathematical Logic, 1879-1931*, page 367–392. Harvard University Press, 1967. Translated by S. Bauer-Mengelberg.

[94] D.R. Hirschfeldt. *Slicing the Truth: On the Computable and Reverse Mathematics of Combinatorial Principles*. World Scientific, 2014.

[95] M. Hyland. The effective topos. In A. S. Troelstra and D. van Dalen, editors, *The L. E. J. Brouwer Centenary Symposium*, pages 165–216. North-Holland, 1982.

[96] R. Iemhoff. Intuitionism in the Philosophy of Mathematics. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Fall 2020 edition, 2020. `https://plato.stanford.edu/archives/fall2020/entries/intuitionism/`.

[97] Aleksandar Ignjatović. Hilbert's Program and the Omega-Rule. *The Journal of Symbolic Logic*, 59(1):322–343, 1994.

[98] H. Ishihara. Reverse mathematics in Bishop's constructive mathematics. *Philosophia Scientiae*, (CS 6):43–59, 2006.

[99] C. Jacobsson and C. Löfwall. Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. *Journal of symbolic computation*, 12(3):337–371, 1991.

[100] J. Kirby and J. Paris. Initial segments of models of Peano's axioms. In *Set theory and hierarchy theory, V (Proc. Third Conf., Bierutowice, 1976)*, page 211–226, 1977. Lecture Notes in Mathematics 619.

[101] L. Kirby and J. Paris. Accessible Independence Results for Peano Arithmetic. *The Bulletin of the London Mathematical Society*, 14(4):285–293, 1982.

[102] U. Kohlenbach. *Higher order reverse mathematics*, page 281–295. Lecture Notes in Logic. Cambridge University Press, 2005.

[103] U. Kohlenbach. *Applied proof theory: proof interpretations and their use in mathematics*. Springer monographs in mathematics. Springer, Berlin Heidelberg, 2008.

[104] U. Kohlenbach and O. Paulo. Proof Mining: A Systematic Way of Analysing Proofs in Mathematics. *BRICS Report Series*, 9(31), 2002.

[105] M. Kojman, G. Lee, E. Omri, and A. Weiermann. Sharp thresholds for the phase transition between primitive recursive and Ackermannian Ramsey numbers. *Journal of combinatorial theory. Series A*, 115(6):1036–1055, 2008.

[106] J.B. Kruskal. Well-quasi-ordering, the tree theorem, and Vazsonyi's conjecture. *Trans. Amer. Math. Soc.*, 95:210–225, 1960.

[107] J.B. Kruskal. The theory of well-quasi-ordering: A frequently discovered concept. *J. Comb. Theory A*, 13:297–305, 1972.

[108] B.A. Kushner and L.I.A. Leifman. *Lectures on constructive mathematical analysis*, volume 60 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, R.I, 1 edition, 1984.

[109] Ø. Linnebo. Platonism in the Philosophy of Mathematics. In Edward N. Zalta and Uri Nodelman, editors, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Summer 2023 edition, 2023.

[110] M. Loebl and J. Matoušek. On undecidability of the weakened Kruskal theorem. In *Logic and combinatorics (Arcata, Calif., 1985)*, volume 65, pages 275–280. Contemp. Math., Amer. Math. Soc., 1987.

[111] H. Lombardi. Algebra in Bishop's style: some major features of the book "A Course in Constructive Algebra" by Mines, Richman, and Ruitenburg, 2019. ArXiv preprint: `https://arxiv.org/abs/1903.04200`.

[112] S. Mac Lane. *Categories for the working mathematician*. Graduate texts in mathematics. Springer, New York, 2. ed edition, 1978.

[113] A. Marcone. Wqo and bqo theory in subsystems of second order arithmetic. In Stephen G. Simpson, editor, *Reverse mathematics 2001*, volume 21, pages 303–330, 2005. Assoc. Symbol. Logic, La Jolla, CA.

[114] A. Marcone. The Reverse Mathematics of wqos and bqos. In Peter M. Schuster, Monika Seisenberger, and Andreas Weiermann, editors, *Well-Quasi Orders in Computation, Logic, Language and Reasoning: A Unifying Concept of Proof Theory, Automata Theory, Formal Languages and Descriptive Set Theory*, pages 189–219, Cham, 2020. Springer International Publishing.

[115] A. Marcone and A. Montalbán. The Veblen functions for computability theorists. *The Journal of symbolic logic*, 76(2):575–602, 2011.

[116] A.A. Markov. *The theory of algorithms*, volume 42 of *Trudy Mat. Inst. Steklov.* Acad. Sci. USSR, Moscow-Leningrad, 1954.

[117] J. Marquis. Category Theory. In Edward N. Zalta and Uri Nodelman, editors, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Fall 2023 edition, 2023.

[118] F. Meskens and A. Weiermann. Classifying Phase Transition Thresholds for Goodstein Sequences and Hydra Games. In R. Kahle and M. Rathjen, editors,

Gentzen's Centenary, pages 455–478. Springer International Publishing, Cham, 2015.

[119] R. Mines, F. Richman, and W. Ruitenburg. *A Course in Constructive Algebra*. Universitext. Springer New York, 1988.

[120] C.R. Murthy. *Extracting constructive content from classical proof*. PhD thesis, Dep. of Comp. Science, Cornell Univ., Ithaca, New York, 1990.

[121] C.R. Murthy and J.R. Russell. A constructive proof of Higman's lemma. In *Proceedings of 5th Annual Symposium on Logic in Computer Science, Philadelphia PA*, pages 257–267, 1990.

[122] C.St.J.A. Nash-William. On well-quasi-ordering finite trees. *Proc. Cambridge Phil. Soc.*, 59:833–835, 1963.

[123] C.St.J.A. Nash-William. On better-quasi-ordering transfinite sequences. *Proc. Cambridge Phil. Soc.*, 64:273–290, 1968.

[124] T. Nemoto and S. Kentaro. A marriage of Brouwser's intuitionism and Hilbert's finitism I: arithmetic. *J. Symbolic Logic*, 87(2):437–497, 2022.

[125] T. Nipkow, L.C. Paulson, and M. Wenzel. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer, 2002.

[126] B. Nordström. Terminating general recursion. *BIT*, 28(3):605–619, 1988.

[127] D. Normann and S. Sanders. On the mathematical and foundational significance of the uncountable. *Journal of Mathematical Logic*, 19(1), 2019.

[128] D. Normann and S. Sanders. Pincherle's theorem in reverse mathematics and computability theory. *Annals of Pure and Applied Logic*, 171(5):102788, 2020.

[129] D. Normann and S. Sanders. The Biggest Five of Reverse Mathematics. *Journal of Mathematical Logic*, 09, 2023.

[130] E. Omri and A. Weiermann. Classifying the phase transition threshold for Ackermannian functions. *Annals of pure and applied logic*, 158(3):156–162, 2009.

[131] F. Pakhomov and J. Walsh. Corrigendum to Reducing ω-model reflection to iterated syntactic reflection. *Journal of Mathematical Logic*, 23, 03 2023.

[132] J. Paris and K. Harrington. A Mathematical Incompleteness in Peano Arithmetic. In *Studies in Logic and the Foundations of Mathematics*, volume 90, pages 1133–1142. 1977.

[133] H. Perdry. Strongly Noetherian rings and constructive ideal theory. *Journal of symbolic computation*, 37(4):511–535, 2004.

[134] H. Perdry and P. Schuster. Noetherian orders. *Mathematical structures in computer science*, 21(1):111–124, 2011.

[135] R. Peter. *Recursive Functions.* Academic Press, New York, 3rd ed., 1967.

[136] W. Phoa. An introduction to fibrations, topos theory, the effective topos and modest sets. Technical report, University of Edinburgh, 1992. `http://www.lfcs.inf.ed.ac.uk/reports/92/ECS-LFCS-92-208/`.

[137] W. Pohlers. *Proof theory: the first step into impredicativity.* Universitext. Springer, Berlin, 2009.

[138] M. Pouzet. Applications of well quasi-ordering and better quasi-ordering. In *Graphs and order*, pages 503–519. Springer, 1985.

[139] T. Powell. Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma. *Proceedings of Classical Logic and Computation (CLAC'12)*, volume 97 of *EPTCS*:49 –62, 2012.

[140] T. Powell. Well Quasi-orders and the Functional Interpretation. In Peter M. Schuster, Monika Seisenberger, and Andreas Weiermann, editors, *Well-Quasi Orders in Computation, Logic, Language and Reasoning: A Unifying Concept of Proof Theory, Automata Theory, Formal Languages and Descriptive Set Theory*, pages 339–350, Cham, 2020. Springer International Publishing.

[141] R. Rado. Partial well-ordering of sets of vectors. *Mathematika*, 1:89–95, 1954.

[142] M. Rathjen. The realm of ordinal analysis. In S. Barry Cooper and John K Truss, editors, *Sets and Proofs*, volume 258. Cambridge University Press, United States, 1999.

[143] M. Rathjen. Generalized inductive definitions in Constructive Set Theory. In L. Crosilla and P. Schuster, editors, *From Sets and Types to Topology and Analysis: Towards Practicable Foundations for Constructive Mathematics*, volume 48 of *Oxford Logic Guides*, chapter 16. Clarendon Press, 2005.

[144] M. Rathjen. The art of ordinal analysis. In *International Congress of Mathematicians, ICM 2006*, volume 2, pages 45–69, 2006.

[145] M. Rathjen. ω-models and well-ordering principles. In N. Tennant, editor, *Foundational Adventures: Essays in Honor of Harvey M. Friedman*, pages 179–212. College Publications, London, 2014.

[146] M. Rathjen. Well-Ordering Principles in Proof Theory and Reverse Mathematics. In F. Ferreira, R. Kahle, and G. Sommaruga, editors, *Axiomatic Thinking II*, pages 89–127. Springer International Publishing, Cham, 2022.

[147] M. Rathjen and I.A. Thomson. Well-ordering Principles, ω-models and Π^1_1-comprehension. In R. Kahle and M. Rathjen, editors, *The Legacy of Kurt Schütte*, pages 171–215. 2020.

[148] M. Rathjen and P.F.V. Vizcaíno. Well-Ordering Principles and Bar Induction. In R. Kahle and M. Rathjen, editors, *Gentzen's Centenary*, pages 533–561. Springer International Publishing, Cham, 2015.

[149] M. Rathjen and A. Weiermann. Proof-theoretic investigations on Kruskal's theorem. *Annals of Pure and Applied Logic*, 60:49–88, 1993.

[150] M. Rathjen and A. Weiermann. Reverse Mathematics and Well-ordering Principles. *Computability in Context*, pages 351–370, 02 2011.

[151] D. Richardson. Some undecidable problems involving elementary functions of a real variable. *J. Symb. Logic*, 33(4):514–520, 1968.

[152] D. Richardson and J. Fitch. The Identity Problem for Elementary Functions and Constants. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '94, page 285–290, New York, NY, USA, 1994. Association for Computing Machinery.

[153] F. Richman. Constructive Aspects of Noetherian Rings. *Proceedings of the American Mathematical Society*, 44(2):436–441, 1974.

[154] F. Richman. The ascending tree condition: Constructive algebra without countable choice. *Communications in algebra*, 31(4):1993–2002, 2003.

[155] F. Richman and G. Stolzenberg. Well quasi-ordered sets. *Advances in Mathematics*, 97:145–153, 1993.

[156] D. Rinaldi, P. Schuster, and D. Wessel. Eliminating disjunctions by disjunction elimination. *Indagationes Mathematicae*, 29(1):226–259, 2018.

[157] A. Ščedrov. Intuitionistic Set Theory. In L.A. Harrington, M.D. Morley, A. Ščedrov, and S.G. Simpson, editors, *Harvey Friedman's Research on the Foundations of Mathematics*, volume 117 of *Studies in Logic and the Foundations of Mathematics*, pages 257–284. Elsevier, 1985.

[158] D. Schmidt. Well-orderings and their maximal order types. 1979. Habilitationsschrift, Mathematisches Institut der Universitat Heidelberg. Also in P. Schuster, M. Seisenberger and A. Weiermann, editors, *Well-Quasi Orders in Computation, Logic, Language and Reasoning*, pages 351–391, 2020.

[159] P. Schuster, M. Seisenberger, and A. Weiermann. *Well-Quasi Orders in Computation, Logic, Language and Reasoning: A Unifying Concept of Proof Theory, Automata Theory, Formal Languages and Descriptive Set Theory*, volume 53 of *Trends in Logic*. Springer Nature, Cham, 1st edition 2020 edition, 2020.

[160] H. Schwichtenberg, M. Seisenberger, and F. Wiesnet. *Higman's Lemma and Its Computational Content*, pages 353–375. Springer International Publishing, Cham, 2016.

[161] A. Seidenberg. What is Noetherian? *Rendiconti del Seminario matematico e fisico di Milano*, 44(1):55–61, 1974.

[162] M. Seisenberger. An Inductive Version of Nash-Williams' Minimal-Bad-Sequence Argument for Higman's Lemma. *Types for Proofs and Programs*, *LNCS* Vol. 2277, 2001.

[163] M. Seisenberger. Kruskal's tree theorem in a constructive theory of inductive definitions. In P. Schuster, U. Berger, and H Osswald, editors, *Reuniting the Antipodes – Constructive and Nonstandard Views of the Continuum*, volume 306 of *Syntheses Library*, pages 241–255. Springer Verlag, 2001. Kluwer Academic Publisher.

[164] M. Seisenberger. *On the Constructive Content of Proofs*. PhD thesis, July 2003.

[165] S.G. Simpson. Nonprovability of certain combinatorial properties of finite trees. In L.A. Harrington, M.D. Morley, A. Šcedrov, and S. G. Simpson, editors, *Harvey Friedman's Research on the Foundations of Mathematics*, pages 87–117. Elsevier, 1985.

[166] S.G. Simpson. Ordinal numbers and the Hilbert basis theorem. *J. Symb. Logic*, 53:961–974, 1988.

[167] S.G. Simpson. Partial Realizations of Hilbert's Program. *Journal of Symbolic Logic*, 53(2):349–363, 1988.

[168] S.G. Simpson. *Reverse Mathematics 2001.* Lecture Notes in Logic. Cambridge University Press, 2005.

[169] S.G. Simpson. *Subsystems of Second Order Arithmetic.* Perspectives in Logic. Cambridge University Press, 2 edition, 2009.

[170] R.L. Smith. The Consistency Strengh of Some Finite Forms of the Higman and Kruskal Theorems. In L.A. Harrington, M.D. Morley, A. Šcedrov, and S. G. Simpson, editors, *Harvey Friedman's Research on the Foundations of Mathematics*, pages 87–117. Elsevier, 1985.

[171] C. Sternagel. Certified Kruskal's tree theorem. *Journal of Formalized Reasoning*, 7(1):45–62, 2014.

[172] C. Sternagel. A Mechanized Proof of Higman's Lemma by Open Induction. In Peter M. Schuster, Monika Seisenberger, and Andreas Weiermann, editors, *Well-Quasi Orders in Computation, Logic, Language and Reasoning: A Unifying Concept of Proof Theory, Automata Theory, Formal Languages and Descriptive Set Theory*, pages 339–350, Cham, 2020. Springer International Publishing.

[173] J. Stillwell. *Reverse mathematics: proofs from the inside out.* Princeton University Press, Princeton, 2018.

[174] T. Streicher. Introduction to Constructive Logic and Mathematics, 2001. Unpublished Manuscript. `https://www.mathematik.tu-darmstadt.de/~streicher/clm.pdf`.

[175] T. Streicher. *Domain-theoretic Foundations of Functional Programming.* World Scientific Publishing Company, Singapore, 2006.

[176] G. Takeuti. Consistency Proofs of Subsystems of Classical Analysis. *Annals of mathematics*, 86(2):299–348, 1967.

[177] J.B. Tennenbaum. *A constructive version of Hilbert's basis theorem.* PhD thesis, University of California, San Diego, California, 1973.

[178] A.S. Troelstra. The scientific work of A. Heyting. *Compositio Mathematica*, 20:3–12, 1968.

[179] A.S. Troelstra. Metamathematical Investigation of Intuitionistic Arithmetic and Analysis. *ILLC pre-publication series*, pages X–93–05, 1993.

[180] A.S. Troelstra. *History of constructivism in the 20th century*, page 150–179. Lecture Notes in Logic. Cambridge University Press, 2011.

[181] A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics, Vol 1*, volume 121. Elsevier Science & Technology, Oxford, 1988.

[182] A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics, Vol 2*, volume 123. Elsevier Science & Technology, Oxford, 1988.

[183] D. van Dalen. Intuitionistic Logic. In Lou Goble, editor, *The Blackwell Guide to Philosophical Logic*, pages 224–257. Oxford, UK: Blackwell, 2017.

[184] J. Van der Mereen. *Connecting the two worlds: well-partial-orders and ordinal notation systems*. PhD thesis, Univ. of Ghent, Belgium, 2015.

[185] J. van Oosten. *Realizability: An Introduction to its Categorical Side*, volume 152 of *Stud. Logic Found. Math.* Elsevier, 2008.

[186] W. Veldman. An Intuitionistic Proof of Kruskal's Theorem. *Archive for Mathematical Logic*, 43(2):215–264, 2004.

[187] W. Veldman. Brouwer's fan theorem as an axiom and as a contrast to Kleene's alternative. *Arch. Math. Logic*, 53:621–693, 2014.

[188] P. Wadler. Propositions as types. *Commun. ACM*, 58(12):75–84, nov 2015.

[189] A. Weiermann. An application of graphical enumeration to PA. *The Journal of symbolic logic*, 68(1):5–16, 2003.

[190] A. Weiermann. Analytic combinatorics, proof-theoretic ordinals, and phase transitions for independence results. *Annals of pure and applied logic*, 136(1):189–218, 2005.

[191] A. Weiermann. Classifying the Provably Total Functions of PA. *The bulletin of symbolic logic*, 12(2):177–198, 2006.

[192] A. Weiermann and W. Van Hoof. Sharp phase transition thresholds for the Paris Harrington Ramsey numbers for a fixed dimension. *Proceedings of the American Mathematical Society.*, 140(8):2913–2927, 2012.

[193] A. Weir. Formalism in the Philosophy of Mathematics. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Spring 2022 edition, 2022.

[194] D. Wessel and P. Schuster. Radical theory of Scott-open filters. *Theoretical Computer Science*, 945:113677, 2023.

[195] I. Yengui. *Constructive Commutative Algebra*. Springer Cham, 2015.