Ordinal Arithmetic through Infinitary Term Rewriting

Marek Kwiatkowski
Free University, Amsterdam, The Netherlands
Jagiellonian University, Kraków, Poland
st.huck@gmail.com

Master Thesis in Computer Science
written under the supervision of:

Prof. Dr. Jan Willem Klop
Dr. Roel de Vrijer
prof. dr hab. Marek Zaionc

31 May 2006

Abstract

In this thesis an infinitary term rewriting system for ordinal arithmetic is studied. This system, called the Dedekind TRS, implements addition, multiplication, exponentiation and stacking on countable ordinals below ε_ω. After necessary restrictions on the considered terms it is shown to satisfy infinitary normalisation and confluence. A semantic function mapping the terms to ordinal numbers is given and its properties are investigated.

KEYWORDS: *infinitary term rewriting, ordinal arithmetic, tree ordinals*

Contents

Chapter 1

Introduction

This essay is an attempt to give a term-rewriting perspective on the arithmetic of ordinal numbers. Usually this would mean providing a term rewriting system whose terms can be interpreted as ordinal numbers, equipped with syntactical constructs to express arithmetical operations. This term rewriting system – or TRS for short – should be sound and complete in the sense that two terms should have identical normal forms if and only if they both denote the same ordinal number.

Not surprisingly, this has already been done. IJsbrand Oudshoorn gave such a TRS in his interesting and useful Bachelor Thesis [Oud05]. His research is precisely a realisation of the program outlined above. Ordinal numbers, however, are inherently infinite objects and (finite) ordinal notations used to represent them tend to blur their nature. It would therefore be desirable to have a more direct notational system for ordinals to use in a term rewriting system.

As the reader might have already guessed – probably with the help of the hint provided by the title of this thesis – this is possible if we drop the requirement that the denotations of ordinals are finite. This decision, however, makes the classical term rewriting not applicable, as the terms of a finitary TRS have to be finite. What comes to rescue here is a fairly recent theory of infinitary term rewriting, where both terms and reduction sequences can be infinite. It is now possible to represent ordinals via *fundamental sequences* (see below), which are very intuitive and in principle allow to express every countable ordinal.

All of this is not for free, though. It is tricky to justify the use of infinite objects in what is meant to be a direct model of computation. I am not going to do it here, as it can be found elsewhere, in several places. Let me just mention that the motivation is the study of functional programming languages with the so-called *lazy evaluation*.

I am thus going to provide an infinitary term rewriting system for ordinal arithmetic and study its properties. Ordinals are going to be denoted by their fundamental sequences, but I am not going to take full advantage of the expressive power of this notation. I will content myself with implementation of ordinal arithmetic up to ε_ω at the reward of having a nice rewriting setup that eliminates some pathologies introduced by the infinitary framework.

Before proceeding to an introduction to infinitary term rewriting I have a couple of organisational remarks. I assume familiarity with first-order term rewriting. As a general reference, the reader may consult [Baa98] or [Ter03]. The rewriting-related notation I use is that of [Ter03] (hence for example $\equiv$ stands for syntactic equality of terms and $\twoheadrightarrow$ for the reflexive and transitive closure of $\rightarrow$). Knowledge of ordinal numbers together with their arithmetic is also treated as a prerequisite. My favourite textbooks here are [Dev93] and [Kur68]. [Sie65] is the ultimate reference on cardinals and ordinals. The class of ordinal numbers is denoted by **ON**. Two very important non-standard definitions are stated below.

As the reader must have already noted I dropped the use of "we" in the storytelling as I consider it a bit schizophrenic in case of a paper having only one author.

Definition 1.1 *The* ordinal stacking $\sqsupset$ *is a ternary function on ordinal numbers defined by transfinite induction on the last argument as follows:*

(a) $\sqsupset(\alpha, \beta, 0) \overset{df}{=} \alpha$

(b) $\sqsupset(\alpha, \beta, \gamma + 1) \overset{df}{=} \beta^{\sqsupset(\alpha,\beta,\gamma)}$

(c) $\sqsupset(\alpha, \beta, \lambda) \overset{df}{=} \lim_{\xi<\lambda} \sqsupset(\alpha, \beta, \xi)$*, where* λ *is a limit.*

Definition 1.2 *A* fundamental sequence *for a limit ordinal* λ *is a strictly increasing function* $\xi : \omega \to \lambda$ *with* $\lim \xi(i) = \lambda$*.*

Recall that every countable limit ordinal has a fundamental sequence.

1.1 Infinitary Term Rewriting

Infinitary term rewriting is an extension of the classical theory of term rewriting that allows the terms to be infinite and defines limits for some of the infinite reduction sequences. My presentation of this theory follows roughly Chapter 12 of [Ter03], but I dropped everything that is not going to be needed in future chapters.

All considered terms are closed, with the exception of left- and right-hand sides of the rules.

Definition 1.3 *Let Σ be a signature. Define d: $Ter(\Sigma) \times Ter(\Sigma) \to \mathbb{R}$ by $d(t_1, t_2) \stackrel{df}{=} 2^{-n}$, where n is the depth of the first level on which t_1 and t_2 differ, or $d(t_1, t_2) \stackrel{df}{=} 0$ if $t_1 \equiv t_2$.*

Example 1.4 Fix a signature with a constant 0, unary symbol S and binary A. The following hold:

$$d(0, S(S((0)))) = 2^{-1} = \frac{1}{2}$$

$$d(S(A(0, S(0)))), S(A(0, 0))) = 2^{-3} = \frac{1}{8}$$

$$d(S(S(0)), S(S(0))) = 0$$

Proposition 1.5 *For a fixed Σ, $\langle Ter(\Sigma), d\rangle$ is a metric space.*

Proof Straightforward. $\square$

Definition 1.6 *Denote by $Ter^{\infty}(\Sigma)$ the metric completion of $\langle Ter(\Sigma), d\rangle$.*

The above definition it is not easy to use. It is not very difficult to prove, however, that the elements from $Ter^{\infty}(\Sigma) \setminus Ter(\Sigma)$ can be seen as infinite, finitely branching trees satisfying two conditions:

(1) every node is labelled with a symbol from the signature and the number of its children equals the arity of this symbol,

(2) every infinite path has order type ω (when the root is considered the *smallest* element of the tree).

The notion of the infinitary TRS – or iTRS for short – that is going to be adopted here allows neither for infinite rules nor for an infinite number of them. Thus any TRS can be seen as an iTRS. The iTRSs are equipped with an additional relation $\twoheadrightarrow$ on $Ter^{\infty}(\Sigma)$, that is going to be introduced now.

Definition 1.7 *Let ρ be an ordinal number. Fix a term $t \in Ter^{\infty}(\Sigma)$ and a sequence $\langle t_i \to t_{i+1}\rangle_{i<\rho}$ of rewrite steps. This sequence is called a* convergent reduction sequence of length ρ from t_0 to t *if the following conditions are met:*

(a) *For every limit ordinal $\lambda < \rho$, $\langle t_i \to t_{i+1} \rangle_{i<\lambda}$ is a convergent reduction sequence from t_0 to t_λ,*

(b) *The sequence $\langle t_i \rangle_{i<\rho}$ of terms converges to t in the metric sense (that is, $t_{\rho-1} \equiv t$ if ρ is a successor ordinal and every cofinal ω-subsequence converges to t if ρ is a limit).*

(c) *There are only finitely many steps at every depth.*

When there is a convergent reduction sequence of length ρ from t to r, the notation $t \twoheadrightarrow_\rho r$ is used. When the length of the reduction is not important, the subscript on $\twoheadrightarrow$ is dropped. A reduction sequence that satisfies (a) and (b) but not (c) is called divergent.

The first clause is a recursive reference to the definition and this recursion is well-founded thanks to the well-ordering of ordinal numbers. The second clause makes sure that t is indeed the limit, and the last clause ensures that the depth of the steps performed tends to infinity at every limit ordinal less than ρ, and also along the whole reduction sequence if ρ is a limit.

Example 1.8 Consider the iTRS with a constant 0, unary operator I and the single rewrite rule $I(x) \to I(I(x))$. Consider the reduction sequence:

$$\begin{array}{ccccccc} I & & I & & I & & I \\ \vert & \to & \vert & \to & \vert & \to \cdots & \vert \\ 0 & & I & & I & & I \\ & & \vert & & \vert & & \vert \\ & & 0 & & I & & I \\ & & & & \vert & & \vert \\ & & & & 0 & & I \\ & & & & & & \vert \\ & & & & & & \cdots \end{array}$$

Let $I^n(0)$ stand for the application of I to 0 n times. Does the sequence $\langle I^n(0) \rangle$ really converges to the limit $I^\omega \stackrel{\mathrm{df}}{=} I(I(I(I(\ldots$ as displayed in the picture? The answer is: it depends. Check all three clauses of the definition:

(a) void, as $\rho = \omega$ in this case.

(b) satisfied.

(c) this is the tricky part. Observe that the rule $I(x) \to I(I(x))$ allows to make the step $I^n(0) \to I^{n+1}(0)$ at any depth between 1 and n. Hence the sequence of depths can be $(1, 2, 3, \ldots)$, but it can also be for example $(1, 1, 1, \ldots)$. In the first case the reduction sequence was convergent, in the second it was not. Note that Definition 1.7 requires the reduction steps to be fixed to prevent this kind of confusion.

Observe that the term I^ω is not a normal form, as $I^\omega \to I^\omega$. How would this example change if the rule $I(x) \to I(I(x))$ were replaced by $I(0) \to I(I(0))$?

The following theorem is the cornerstone of the theory of infinitary term rewriting:

Theorem 1.9 (Compression Lemma) *Let $t \twoheadrightarrow_\rho r$ in a left-linear iTRS. There exists an ordinal $\alpha \leq \omega$ with $t \twoheadrightarrow_\alpha r$.*

Proof A rather straightforward proof by transfinite induction on ρ can be found in [Ter03]. □

The origin of the name "Compression Lemma" should be clear. Observe that it may be possible for the infinite reduction sequences to be compressed to finite length. The Compression Lemma will be used in this essay many times and without a warning.

I hope that the notion of convergent sequence is now more or less clear to the reader. I will now proceed to the generalisation of the classical rewriting properties to the infinitary setting. This same material is also outlined in [Klo05].

Definition 1.10 *Let $\mathcal{R}$ be an iTRS. $\mathcal{R}$ is* infinitarily confluent *(notation: $\mathcal{R} \models \mathrm{CR}^\infty$) if for every $t, r, u \in Ter^\infty(\mathcal{R})$ with $t \twoheadrightarrow r$ and $t \twoheadrightarrow u$, there is $v \in Ter^\infty(\mathcal{R})$ with $r \twoheadrightarrow v$ and $u \twoheadrightarrow v$.*

Definition 1.11 *Let $\mathcal{R}$ be an iTRS. $\mathcal{R}$ has* infinitary uniqueness of normal forms *(notation: $\mathcal{R} \models \mathrm{UN}^\infty$) if for every $t, u, v \in Ter^\infty(\mathcal{R})$ where u and v are normal forms, $t \twoheadrightarrow u$ and $t \twoheadrightarrow v$ implies $u \equiv v$.*

The proof of the following proposition can be found in [Ter03].

Proposition 1.12 *Let $\mathcal{R}$ be an orthogonal iTRS. Then $\mathcal{R} \models \mathrm{UN}^\infty$ but not necessarily $\mathcal{R} \models \mathrm{CR}^\infty$.*

Definition 1.13 *Let $\mathcal{R}$ be a iTRS. $\mathcal{R} \models \mathrm{WN}^\infty$ if for every $t \in Ter^\infty(\mathcal{R})$ there is a normal form $r \in Ter^\infty(\mathcal{R})$ with $t \twoheadrightarrow r$.*

The generalisation of SN turns out to be less straightforward. I adopt the definition from [Klo05].

Definition 1.14 *If for every reduction sequence in an iTRS $\mathcal{R}$ the conditions (a) and (b) of the Definition 1.7 imply (c), then $\mathcal{R}$ is said to satisfy* infinitary strong normalisation *(notation: $\mathcal{R} \models \mathrm{SN}^\infty$). In other words: $\mathcal{R} \models \mathrm{SN}^\infty$ if there are no divergent reductions in $\mathcal{R}$.*

The following surprising result is proven in [Klo05].

Theorem 1.15 *Let $\mathcal{R}$ be an orthogonal iTRS. Then $\mathcal{R} \models \mathrm{WN}^\infty$ iff $\mathcal{R} \models \mathrm{SN}^\infty$.*

The following result is an easy generalisation of the above theorem. The notation $A \models P$ where A is a class of terms and P is a property means that P is satisfied if all quantifiers in its definition are restricted to A.

Proposition 1.16 *Let $\mathcal{R}$ be an orthogonal iTRS and let $A \subseteq Ter(\mathcal{R})$ be a reduction- and subterm-closed class of terms. Then $A \models \mathrm{WN}^\infty$ iff $A \models \mathrm{SN}^\infty$.*

Proof The proof of Theorem 1.15 given in [Klo05] is applicable if instead of arbitrary terms only A-terms are considered. $\square$

1.2 Overview

Now I give a brief outline of the thesis.

Chapter 1 In the first chapter I give the reader a perspective on the research carried out in the later chapters as well as a brief description of the contents of this essay, but the core part is an introduction to infinitary term rewriting.

Chapter 2 The second chapter contains the specification of the term rewriting system I am working with. I included also some examples of terms and their reductions to give the reader the feeling of how this TRS works. The last part is devoted to some simple observations about basic properties of the TRS.

Chapter 3 The third chapter has two distinct parts. First, I make a strategic decision about the angle from which I am going to analyse the TRS, and try to justify it. Then I prove the main result of this thesis: a certain subclass of terms of the TRS satisfies both infinitary confluence and infinitary normalisation. The latter is achieved by giving an algorithm of normalisation.

Chapter 4 In the last chapter the focus is finally shifted from syntax to semantics: I provide a function mapping the terms of the TRS to ordinal numbers and analyse its properties. It turns out that the ordinals that can be expressed in the system form an initial segment of the class of ordinal numbers, with supremum equal to ε_ω. A side product here is the Theorem 4.8 asserting that the normal forms of the terms from the subclass defined in Chapter 3 are so-called *tree ordinals* – syntactic representations of ordinal numbers, relevant to proof theory.

1.3 Acknowledgements

There are a few people without whom this work could not be done and others who in various ways made it easier. I want to take the opportunity and thank all of them here:

First of all, I am indebted to my Dutch advisors: Jan Willem Klop and Roel de Vrijer. They suggested a very interesting topic and, what is more important, gave me the independence of making all strategic decisions in the course of the research. Thanks to this I gained invaluable experiences in scientific work.

I wrote this thesis in Amsterdam. I am therefore very thankful to Professor Marek Zaionc for the confidence he must have had in me when he agreed to be my "remote" supervisor at the Jagiellonian University. I also appreciate his enthusiasm for my research he was expressing during our scarce meetings.

I want to express my gratitude to Ariya Ishihara, who solved an important problem of the expressivity of the Dedekind TRS. Without this result this thesis would be incomplete.

I have also profited from inspiring discussions with IJsbrand Oudshoorn. IJsbrand also gave a direct proof of Theorem 2.7 that can be found in this essay.

Finally, I am grateful to all my friends I lived with in Amsterdam. They created a wonderful atmosphere and made this stay truly memorable. Special thanks here go to Jaap Weel – for many overnight discussions and for technical support.

Pictures of trees were generated with the `synttree` package by Matijs van Zuijlen.

Chapter 2

The Dedekind TRS

In this chapter the reader will be introduced to the Dedekind TRS, an infinitary term rewriting system which is the subject of the research conducted in this thesis. The chapter begins with the specification of the TRS which is then followed by some examples of terms and their reductions. It is concluded by a couple of simple observations regarding some basic properties of this rewrite system.

This TRS was given by J. W. Klop. The first four rewrite rules of this TRS are traditionally attributed to R. Dedekind and his famous book [Ded88] – hence the name of the system.[1] Instead of writing "The Dedekind TRS" I will often write simply $\mathcal{D}$.

2.1 Specification of the TRS

The signature of the Dedekind TRS is given in the Table 2.1. This TRS is meant to provide a framework for ordinal arithmetic, hence the signature contains constructs for representing ordinals as well as symbols to represent arithmetical operations. The intended meaning of every symbol is briefly stated in the Table 2.1; I will now explain it in more detail.

The constants 0 and ω stand for ordinal numbers 0 and ω, respectively – nothing to comment on here.

The unary symbol S stands for ordinal successor. It means that whenever there is a term t representing an ordinal number α, then the term $S(t)$ represents the ordinal number $\alpha + 1$. A term of the form $S^n(0)$ – i.e. a finite number of applications of S to 0 – is called a *numeral* for the natural number n.

[1] It seems that H. Grassmann arrived at the same ideas some 25 years before Dedekind.

symbol	arity	infix notation	function / intended meaning
0	0	none	the ordinal 0
ω	0	none	the ordinal ω
S	1	none	ordinal successor
$nats$	1	none	stream generator
P	2	:	pairing operator (cons)
A	2	$+$	ordinal addition
M	2	$\cdot$	ordinal multiplication
exp	2	superscript	ordinal exponentiation
$\sqsupset$	3	none	ordinal stacking

Table 2.1: The signature

The symbols A, M, exp and $\sqsupset$ represent arithmetical operations of ordinal addition, multiplication, exponentiation and stacking, respectively. For example, when for given t and r, the term $M(t,r)$ (which will usually be written as $t \cdot r$) is to be seen as denoting the ordinal obtained by multiplying the ordinal denoted by t by the ordinal denoted by r. These four symbols will be called *arithmetical* when considered en bloc.

The pairing symbol P (written more often in the infix notation as colon :) should be seen as the list forming operator. Thus $P(0, P(S(0), S(S(0))))$ – or $0 : S(0) : S(S(0))$ – is the list of length 3, having 0 as the first, $S(0)$ as the second and $S(S(0))$ as the third element. Not the finite lists, however, but the infinite ones will be of great importance in this essay and P is going to be used to form these as well. An infinite list (also called a *stream*) is an infinite term of the form $t_0 : t_1 : t_2 : \dots$, where every t_i can be arbitrary. The brackets are dropped when the : notation is used.

The last symbol, *nats*, is a generator of the stream of natural numbers. This auxiliary symbol will serve to obtain the stream $0 : S(0) : S(S(0)) : \dots$ – see Example 2.1.

The rewrite rules for the Dedekind TRS are given in the Table 2.2. The rules (1)–(12) are syntactical analogues of the definitions of the operations of ordinal arithmetic by transfinite induction: (1), (3), (5) and (7) model the zero case, (2), (4), (6) and (8) the successor case and (9)–(12) the limit case. This will hopefully become clearer in the next section, where sample reductions are performed. The rules (13) and (14) allow to expand the constant ω into its canonical fundamental sequence $0 : 1 : 2 : \dots$.

1.	$x + 0$	$\rightarrow$	x
2.	$x + S(y)$	$\rightarrow$	$S(x + y)$
3.	$x \cdot 0$	$\rightarrow$	0
4.	$x \cdot S(y)$	$\rightarrow$	$x \cdot y + x$
5.	x^0	$\rightarrow$	$S(0)$
6.	$x^{S(y)}$	$\rightarrow$	$x^y \cdot x$
7.	$\sqsupset(x, y, 0)$	$\rightarrow$	x
8.	$\sqsupset(x, y, S(z))$	$\rightarrow$	$y^{\sqsupset(x,y,z)}$
9.	$x + y : z$	$\rightarrow$	$(x + y) : (x + z)$
10.	$x \cdot y : z$	$\rightarrow$	$(x \cdot y) : (x \cdot z)$
11.	$x^{y:z}$	$\rightarrow$	$(x^y) : (x^z)$
12.	$\sqsupset(x, y, u : z)$	$\rightarrow$	$\sqsupset(x, y, u) : \sqsupset(x, y, z)$
13.	ω	$\rightarrow$	$nats(0)$
14.	$nats(x)$	$\rightarrow$	$x : nats(S(x))$

Table 2.2: The rules

2.2 Examples

The following examples should give the reader a grip on the ways the Dedekind TRS works and point out some of its peculiarities. The active redex is underlined and subscripts on arrows indicate the rules used. Numerals are replaced by the corresponding numbers for readability.

Example 2.1 The simplest infinite reduction:

$$\begin{aligned} \underline{\omega} &\rightarrow_{13} \underline{nats(0)} \\ &\rightarrow_{14} 0 : \underline{nats(1)} \\ &\rightarrow_{14} 0 : 1 : \underline{nats(2)} \\ &\twoheadrightarrow_{14} 0 : 1 : 2 : 3 : \ldots \end{aligned}$$

Thus, as promised, the constant ω rewrites to the stream of natural numbers.

Example 2.2 The ordinal $\omega + 1$:

$$\begin{aligned} \underline{\omega + 1} &\rightarrow_{2} S(\underline{\omega + 0}) \\ &\rightarrow_{1} S(\underline{\omega}) \\ &\twoheadrightarrow S(0 : 1 : 2 : 3 : \ldots) \end{aligned}$$

The normal form of $\omega + 1$ is therefore different of the normal form of ω – a result that could have been expected.

Example 2.3 The ordinal $1+\omega$ and its reduction of length $\omega \cdot 3$:

$$\begin{array}{rll} 1+\underline{\omega} & \twoheadrightarrow & \underline{1+0:1:2:3:\ldots} \\ & \to_9 & (1+0):(\underline{1+1:2:3:\ldots}) \\ & \twoheadrightarrow & (1+0):(1+1):(1+2):(1+3)\ldots \\ & \twoheadrightarrow & 1:2:3:4:\ldots \end{array}$$

This is probably a surprise for the reader: although the ordinal number $1+\omega$ is equal to ω, normal forms of the terms denoting these ordinals are different. A quick glance reveals, however, that they both encode fundamental sequences for the same ordinal. This cannot be said of the normal forms of ω and $\omega+1$.

Example 2.4 The ordinal ε_0:

$$\begin{array}{rll} \sqsupset(\omega,\omega,\underline{\omega}) & \twoheadrightarrow & \underline{\sqsupset(\omega,\omega,0:1:2:\ldots)} \\ & \to_{12} & \sqsupset(\omega,\omega,0):\underline{\sqsupset(\omega,\omega,1:2:\ldots)} \\ & \twoheadrightarrow & \underline{\sqsupset(\omega,\omega,0)}:\sqsupset(\omega,\omega,1):\sqsupset(\omega,\omega,2):\ldots \\ & \to_7 & \omega:\underline{\sqsupset(\omega,\omega,1)}:\sqsupset(\omega,\omega,2):\ldots \\ & \to_8 & \omega:\underline{\omega^{\sqsupset(\omega,\omega,0)}}:\sqsupset(\omega,\omega,2):\ldots \\ & \to_7 & \omega:\omega^{\omega}:\underline{\sqsupset(\omega,\omega,2):\ldots} \\ & \twoheadrightarrow & \omega:\omega^{\omega}:\omega^{\omega^{\omega}}:\ldots \end{array}$$

Example 2.5 This example shows that the streams produced by the Dedekind TRS are not always non-decreasing:

$$\begin{array}{rll} 0^{\underline{\omega}} & \twoheadrightarrow & \underline{0^{0:1:2:\ldots}} \\ & \to_{11} & 0^0:\underline{0^{1:2:\ldots}} \\ & \twoheadrightarrow_{11} & \underline{0^0}:0^1:0^2:\ldots \\ & \to_5 & 1:\underline{0^1}:0^2:\ldots \\ & \to_6 & 1:\underline{0^0\cdot 0}:0^2:\ldots \\ & \to_3 & 1:0:\underline{0^2:\ldots} \\ & \twoheadrightarrow & 1:0:0:\ldots \end{array}$$

There are not many decreasing streams that are at the same time reducts of finite terms. All examples known to the author are variants of the above – they all involve 0 raised to the power α, where α is a term that reduces to a stream with 0 as the first element.

2.3 An important subsystem

I will now isolate a subsystem of $\mathcal{D}$. This subsystem will be of importance in the next chapter, where it will be used to prove, under certain restrictions, normalisation of $\mathcal{D}$.

Definition 2.6 *$\mathcal{D}_0$ is the (finitary) term rewriting system whose signature consists of all symbols from the signature of $\mathcal{D}$ except for ω and nats, and whose set of rules consists of the rules (1)–(12) of $\mathcal{D}$.*

$\mathcal{D}_0$ is suitable for computations with finite lists of natural numbers. Such computations do not belong to the scope of this thesis and hence $\mathcal{D}_0$ will be used for technical purposes only. More precisely, I will make use of the fact that it is normalising.

Theorem 2.7 $\mathcal{D}_0 \models \mathrm{SN}$.

Proof The following proof is due to IJsbrand Oudshoorn. It uses the IPO method of [Klo02]. The reader who is not familiar with IPO may prefer to use an automated termination tool like the Tyrolean Termination Tool[2] to convince him- or herself of the termination of $\mathcal{D}_0$.

To show that $\mathcal{D}_0$ is terminating I rewrite in the IPO system all the left hand sides of the rules to their right hand sides. The order on the signature of $\mathcal{D}_0$ is as follows: $S < P < A < M < \mathit{exp} < \sqsupset$. The cases (10)–(12) are analogous to (9).

(1) $A(x,0) \to_{put} A^\star(x,0) \to_{select} x$

(2) $A(x,S(y)) \to_{put} A^\star(x,S(y)) \to_{copy} S(A^\star(x,S(y))) \to_{down} S(A(x,S^*(y)))$
$\to_{select} S(A(x,y))$

(3) $M(x,0) \to_{put} M^\star(x,0) \to_{select} 0$

(4) $M(x,S(y)) \to_{put} M^\star(x,S(y)) \to_{copy} A(M^\star(x,S(y),M^\star(x,S(y))$
$\to_{down} A(M(x,S^\star(y)),M^\star(x,S(y))) \to_{select} A(M(x,y),M^\star(x,S(y)))$
$\to_{select} A(M(x,y),x)$

(5) $\mathit{exp}(x,0) \to_{put} \mathit{exp}^\star(x,0) \to_{copy} S(\mathit{exp}^\star(x,0)) \to_{select} S(0)$

(6) $\mathit{exp}(x,S(y)) \to_{put} \mathit{exp}^\star(x,S(y)) \to_{copy} M(\mathit{exp}^\star(x,S(y)),\mathit{exp}^\star(x,S(y)))$
$\to_{down} M(\mathit{exp}(x,S^\star(y)),\mathit{exp}^\star(x,S(y))) \to_{select} M(\mathit{exp}(x,y),\mathit{exp}^\star(x,S(y)))$
$\to_{select} M(\mathit{exp}(x,y),x)$

(7) $\sqsupset(x,y,0) \to_{put} \sqsupset^\star(x,y,0) \to_{select} x$

(8) $\sqsupset(x,y,S(z)) \to_{put} \sqsupset^\star(x,y,S(z)) \to_{copy} \mathit{exp}(\sqsupset^\star(x,y,S(z)),\sqsupset^\star(x,y,S(z)))$
$\to_{select} \mathit{exp}(y,\sqsupset^\star(x,y,S(z))) \to_{down} \mathit{exp}(y,\sqsupset(x,y,S^\star(z)))$
$\to_{select} \mathit{exp}(y,\sqsupset(x,y,z))$

(9) $A(x,P(y,z)) \to_{put} A^\star(x,P(y,z)) \to_{copy} P(A^\star(x,P(y,z)),A^\star(x,P(y,z)))$
$\to_{down} P(A(x,P^\star(y,z)),A^\star(x,P(y,z))) \to_{select} P(A(x,y),A^\star(x,P(y,z)))$
$\to_{down} P(A(x,y),A(x,P^\star(y,z))) \to_{select} P(A(x,y),A(x,z))\Box$

[2] `http://cl2-informatik.uibk.ac.at/ttt/`

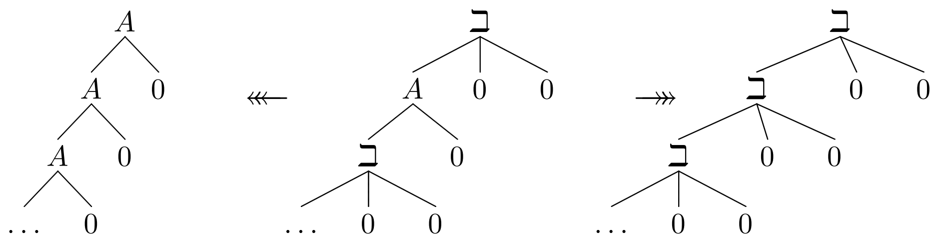

Figure 2.1: Counterexample for $\mathcal{D} \models \mathrm{CR}^\infty$

2.4 Negative results

$\mathcal{D}$ is orthogonal and therefore confluent in the finitary sense. Orthogonality implies also UN^∞. It is clear that $\mathcal{D}$ is not finitarily normalising, with ω being the simplest term admitting an infinite reduction. The failure of normalisation is of course planned, as $\mathcal{D}$ is supposed to be a "proper" infinitary TRS and have infinite reduction sequences. What comes as a surprise is that $\mathcal{D}$ satisfies neither SN^∞ nor CR^∞. The first fact follows from a general observation.

Proposition 2.8 *Let $\mathcal{R}$ be an infinitary TRS containing a collapsing rule. Then $\mathcal{R}$ is not infinitarily normalising.*

Proof The collapsing rule is of the form $C[x] \to x$, where $C[\cdot]$ is a context for the variable x. Consider the term t defined by $t = C[t]$. Clearly $t \to t$, so $\mathcal{R}$ is not normalising. $\square$

Corollary 2.9 *$\mathcal{D}$ is not infinitarily normalising.*

A counterexample for CR^∞ can be obtained in a similar way.

Proposition 2.10 *$\mathcal{D}$ is not infinitarily confluent.*

Counterexample Term t satisfying $t = \beth(t+0, 0, 0)$ reduces transfinitely (in ω steps) to $t' = \beth(t', 0, 0)$ and (again in ω steps) to $t'' = t'' + 0$. t' and t'' are distinct and reduce only to themselves, so the fork cannot be joined.

Chapter 3

Meaningful terms

I ended the last chapter with a sort of a cliffhanger: The Dedekind TRS was shown to be neither normalising nor (infinitarily) confluent and hence unsuitable for any reasonable computations. In this chapter it is made usable despite these flaws.

The implemented solution stems from the observation that the counterexamples for SN^∞ and CR^∞ are pathological terms, in the sense that they do not denote any ordinal numbers. Another example of such term can be the full infinite binary tree with each node labelled by P (or any other binary symbol for that matter). This is a valid infinite term over the signature of $\mathcal{D}$, and yet it would be much desired to get rid of it somehow because it clearly does not stand for any ordinal number. I will therefore define a class that contains enough terms to express a considerable number of countable ordinals and does not contain any of the pathological terms described above. This class will be referred to as the class of meaningful terms[1] and the bulk of this chapter will be devoted to proving that inside it both SN^∞ and CR^∞ hold.

3.1 Definitions

First, I define a class of finite terms that will serve as the source for all the meaningful terms. What it exactly means will be made clear in a moment.

Definition 3.1 *Define $Ker \subseteq Ter(\mathcal{D})$ inductively:*

(a) $0 \in Ker$ *and* $\omega \in Ker$.

[1]There is a formal concept of "meaninglessness" in the theory of infinitary term rewriting. My use of this word is rather informal and does refer to this idea.

(b) if $t, r, u \in Ker$ then $S(t), t + r, t \cdot r, t^r, \sqsupset(t, r, u) \in Ker$.

The class of the meaningful terms can now be defined as the closure of Ker under finite and transfinite convergent reduction sequences.

Definition 3.2 $\mathcal{B} \stackrel{df}{=} \{t \in Ter^{\infty}(\mathcal{D})\colon \exists(t_0 \in Ker)(t_0 \twoheadrightarrow t)\}$.

In the due course of this thesis the attention will be restricted to the terms from $\mathcal{B}$. The choice of this class was quite arbitrary and therefore deserves some justification. This justification will not have a formal character because at this point it would be quite tedious to define what it means for a term to be "meaningful", i.e. to denote an ordinal. Intuitively, all terms in Ker are meaningful: there is an obvious mapping from Ker to **ON** (it will be the starting point of the discussion of semantics in the next chapter). Hence excluding the Ker-terms from the considerations would be a bad choice. Intuitively still, the reduction should preserve "meaningfulness" and this is why it is expected that every term from $\mathcal{B}$ denotes an ordinal number.

Observe that there is no clause stating that $t, r \in Ker$ implies $t : r \in Ker$ in the definition of Ker. This is because the Dedekind TRS is meant to model computations with ordinal numbers rather than with lists of ordinal numbers. Had this clause been included, the semantics of the TRS would require some reworking, but it can be expected that the normalisation would still hold, although the proof given in this chapter would not be directly applicable.

Remark 3.3 It would be naïve to expect $\mathcal{B}$ to contain every term that can be seen as denoting an ordinal number. To show that, assume that there is an uniform procedure that brings any $\mathcal{B}$-term to its unique normal form in ω steps or less. This going to be proven by the end of this chapter, of course independently of this discussion. Take any undecidable subset $A \subseteq \mathbb{N}$. A can be ordered into a strictly ascending sequence $a_0 < a_1 < a_2 < \ldots$. For any $n \in \mathbb{N}$, let $\underline{n}$ denote the corresponding numeral (i.e. $S^n(0)$). Consider the term $t \equiv \underline{a_0} : \underline{a_1} : \underline{a_2} : \ldots$. It is a legal infinite term over the signature of $\mathcal{D}$. Moreover, it clearly encodes a fundamental sequence for the ordinal ω. Now suppose that $t \in \mathcal{B}$. It means that there is a term $t_0 \in Ker$ such that $t_0 \twoheadrightarrow t$. t_0 can be reduced to t in ω steps so every $\underline{a_i}$ can be obtained in finite time. This yields, however, a decision procedure for A: take n as an input and start reducing t_0 according to the normalisation strategy mentioned above.[2] Answer "yes" when $\underline{n}$ is encountered in the reduct. Answer

[2]This is a little bit more tricky: there is no simple way to find t_0 for a given A. The procedure given above is a program scheme, giving $\aleph_0$ programs – one for every possible source from Ker. Since $t_0 \in Ker$, one of these programs is the decision procedure for A.

"no" if $\underline{k}$ is encountered for any $k > n$. This is a contradiction with the fact that A was picked to be undecidable, so $t \notin \mathcal{B}$.

The existence of fundamental sequences for ω that lie outside $\mathcal{B}$ is not worrying as there are many others that do belong to $\mathcal{B}$. However, the limitations introduced by the approach adopted in this thesis run deeper. It is easy to see that every countable ordinal can be represented by means of the signature of $\mathcal{D}$, but, as it will be shown in the next chapter, there is a countable upper bound on the ordinals denoted by $\mathcal{B}$-terms.

The above remark, apart from making its point, illustrates a technique of reasoning about $\mathcal{B}$ that will be used very often. Every term $t \in \mathcal{B}$ has a "source" $t_0 \in \mathit{Ker}$. The reduction $t_0 \twoheadrightarrow t$ can be then compressed to ω (or, if t is finite, less than ω) steps, yielding a sequence $t_0 \to t_1 \to t_2 \to \cdots t$. If we now want to prove something about t, we know that it is a limit of a reduction sequence of length ω of finite terms, first of them being an element of Ker.

$\mathcal{B}$ is not closed under subterms, what may be regarded as unnatural. Consider for example the term $0 : \mathit{nats}(S(0))$. It is an element of $\mathcal{B}$, but its subterm $\mathit{nats}(S(0))$ is not.[3] The class of all subterms of $\mathcal{B}$-terms is not going to be investigated in detail, but it will play a vital role later on.

Definition 3.4 $\mathcal{B}_{\subseteq} \stackrel{df}{=} \{t' \in \mathit{Ter}^{\infty}(\mathcal{D}) \colon \exists(t \in \mathcal{B})(t' \subseteq t)\}$.

Proposition 3.5 *$\mathcal{B}_{\subseteq}$ is closed under subterms, finite reductions and infinite convergent reductions.*

Proof Easy. □

The following theorem is an immediate consequence of the definitions stated above.

Theorem 3.6 *Let $t, r, u \in \mathcal{B}$. Then $S(t), t + r, t \cdot r, t^r, \sqsupset(t, r, u) \in \mathcal{B}$.*

Proof The proof is only for the case $t+r$ – the remaining cases are completely analogous. Let $t_0, r_0 \in \mathit{Ker}$ be such that $t_0 \twoheadrightarrow t$ and $r_0 \twoheadrightarrow r$. $t_0 + r_0 \in \mathit{Ker}$ and $t_0 + r_0 \twoheadrightarrow t + r$, so $t + r \in \mathcal{B}$ as required. □

3.2 The transformation Z

This section contains some of the most technical results in this essay. The reader will be forgiven for skipping the proofs and concentrating on appli-

[3] In Section 4.4 it is shown that $\mathcal{B}$ is closed under a relation that is a bit stricter that the subterm relation.

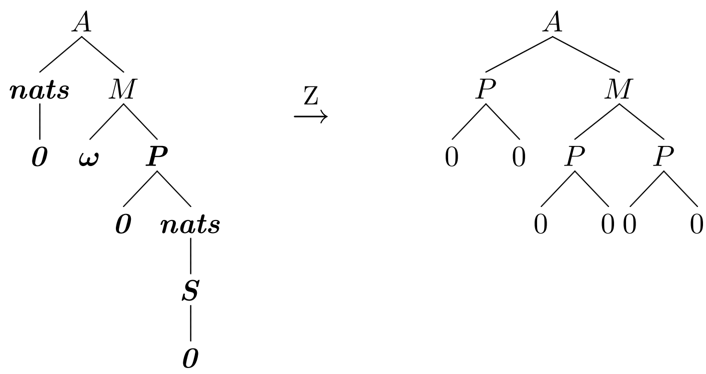

Figure 3.1: Application of Z to a sample term. Bold subtrees get replaced by $P(0,0)$.

cations of the results obtained here to the proof of normalisation which will be reached by the end of the chapter.

Definition 3.7 *Let $t \in Ter^{\infty}(\mathcal{D})$. Let $\{t_i\}_{i \in I}$ be the collection of all maximal subtrees of t having pairing or nats or ω as root (note that t_i's are pairwise disjoint). Define $Z(t)$ to be t with every t_i replaced by the constant term $P(0,0)$.*

Proposition 3.8 *Some basic properties of Z:*

(a) Let t be of the form $F(t_1, \ldots, t_n)$ where F is different from nats and P and ω. Then $Z(t) \equiv F(Z(t_1), \ldots, Z(t_n))$.

(b) Let $root(Z(t)) \equiv F$ for F different from P. Then $root(t) \equiv F$.

(c) Z is idempotent, i.e. for all t, $Z(Z(t)) \equiv Z(t)$.

Proof All of these properties follow directly from the definition and therefore proofs are omitted. □

Definition 3.9 *A reduction step $t \to r$ is called* top-level *if there is neither nats nor ω nor pairing on the path from the root of t to the root of the contracted redex (both included). The notation $t \to_{top} r$ is used to emphasise that the step is top-level. A step that is not top-level is called* low-level.

Note that every application of rule (13) or (14) is a low-level step. Again, the distinction between top-level and low-level steps is of technical nature.

Proposition 3.10 *Let $t \to r$ be a low-level step. Then $Z(t) \equiv Z(r)$.*

Proof (sketch) The claim follows from the observation that a redex active in a low-level step is always inside some subtree that gets eliminated (i.e. replaced by $0 : 0$) by Z and that the same is true of the reduct of this redex in r. $\Box$

Lemma 3.11 *If $t \to_{top} r$ then there exists a r' such that $Z(t) \to r'$ and $Z(r') \equiv Z(r)$.*

Proof Let $u \subseteq t$ be the active redex and $u' \subseteq r$ its reduct. Observe that because there is neither P nor ω nor *nats* on the path from the root of t to the root of u, Proposition 3.8a can be applied repeatedly to prove that $Z(u)$ is present in $Z(t)$ at the same position that u is in t. Thus it is enough to show that there is a r'' such that $Z(u) \to r''$ and $Z(r'') \equiv Z(u')$. The desired r' will then be $Z(r)$ with $Z(u')$ replaced by r''. Argue by cases:

(a) The applied rule is one of (1)-(8). Only the proof for the fourth rule is given and the reader is assured that for all of the remaining rules the very same argument applies:

Since the step is performed at the root of u, u must be of the form $t_1 \cdot S(t_2)$ for some t_1, t_2. Apply Proposition 3.8a twice to get $Z(u) \equiv Z(t_1) \cdot S(Z(t_2))$. Thus $Z(u) \to Z(t_1) \cdot Z(t_2) + Z(t_1)$. Put $r'' \stackrel{\text{df}}{=} Z(t_1) \cdot Z(t_2) + Z(t_1)$ and use Proposition 3.8ac to verify that $Z(r'') \equiv Z(u')$.

(b) The applied rule is one of (9)-(12). Again, the claim is proven only for rule (9):

$u \equiv t_1 + t_2 : t_3$. Thus $u' \equiv (t_1 + t_2) : (t_1 + t_3)$, so $Z(u') \equiv 0 : 0$. Moreover, $Z(u) \equiv Z(t_1) + 0 : 0$ so put $r'' \stackrel{\text{df}}{=} (Z(t_1) + 0) : (Z(t_1) + 0)$. Again, $Z(u) \to r''$ and $Z(r'') \equiv 0 : 0 \equiv Z(u')$. $\Box$

The next lemma is a dual to the previous one. It cannot, however, be guaranteed that a step from $Z(t)$ yields *one* step from t. This is because pairing symbols can appear in $Z(t)$ without being present in t, so t will first have to be reduced to a form in which the pairing symbols taking part in the reduction of $Z(t)$ are present. This is done in part (b) of the following proof.

Lemma 3.12 *If $Z(t) \to r$ then there exists a r' such that $t \to^+ r'$ and $Z(r) \equiv Z(r')$*

Proof I will proceed in the spirit of the proof of the previous lemma. Consider the active redex u in $Z(t)$ and its reduct u' in r. It is not difficult to see that $u \equiv Z(t')$ for a subterm $t' \subseteq t$ located at the same position in t that u is in $Z(t)$. The goal is now to find a r'' such that $t' \to^+ r''$ and moreover, $Z(r'') \equiv Z(u')$. r' will then be t with t' replaced by r''.

Observe that the step $Z(t) \to r$ cannot be the application of rule (13) or (14) because $Z(t)$ contains neither *nats* nor ω. Consider all of the other possibilities:

(a) The rule applied is one of (1)-(8). The proof presented here is for rule (2), all other rules follow the same pattern.

Since $Z(t')$ can be unified with $x + S(y)$, then by Proposition 3.8b (applied twice) the same is true of t'; thus $t' \equiv t_1 + S(t_2)$ and $Z(t') \equiv Z(t_1) + S(Z(t_2))$ for some t_1, t_2. Put $r'' \stackrel{\mathrm{df}}{=} S(t_1 + t_2)$. Obviously $t' \to r''$, and it follows from $u' \equiv S(Z(t_1) + Z(t_2))$ and Proposition 3.8ac that $Z(r'') \equiv Z(u')$, what proves the claim.

(b) The rule applied is one of (9)-(12). The difficulty here is that the rule patterns contain P and one cannot claim as above that since $Z(t')$ can be unified with the pattern then so can t' (consider for example $t' = \sqsupset(0, 0, \omega)$; $Z(t') \equiv \sqsupset(0, 0, 0 : 0)$ so there is a head step from $Z(t')$ but not from t'). The only reason for this mixup, however, is that the pairing symbol in $Z(t')$ has arisen from ω or $\mathit{nats}(x)$ in t'. The solution is then simple: reduce ω to $\mathit{nats}(0)$ and then to $0 : \mathit{nats}(0)$ (2 steps) and if the culprit was a term of the form $\mathit{nats}(x)$, then reduce it in one step to $x : \mathit{nats}(S(x))$. In this way t' was transformed to, say, t'' which is unifiable with the same pattern as $Z(t')$. If all of this was not necessary (i.e. t' was unifiable with the pattern from the beginning), then put $t'' \stackrel{\mathrm{df}}{=} t'$. Observe that $t' \twoheadrightarrow t''$ and $Z(t') \equiv Z(t'')$. After this preprocessing, the proof follows the same case as in (a); to reassure the reader, the claim is proven below for the rule (12):

$Z(t'') \equiv \sqsupset(t_1, t_2, 0 : 0)$ for some t_1, t_2, so $t'' \equiv \sqsupset(t'_1, t'_2, t_3 : t_4)$ (with $Z(t'_1) \equiv t_1$ and $Z(t'_2) \equiv t_2$). Put $r'' \stackrel{\mathrm{df}}{=} \sqsupset(t'_1, t'_2, t_3) : \sqsupset(t'_1, t'_2, t_4)$. Obviously $t'' \to r''$, which together with $t' \twoheadrightarrow t''$ gives $t' \to^+ r''$. Furthermore, $Z(t') \equiv Z(t'') \equiv 0 : 0 \equiv Z(r'')$. $\square$

The following theorem formalises the observation that when a term is being reduced, the pairing symbols always go “up” and eventually all the reduction steps become low-level, i.e. there is always a pairing symbol above the redex.

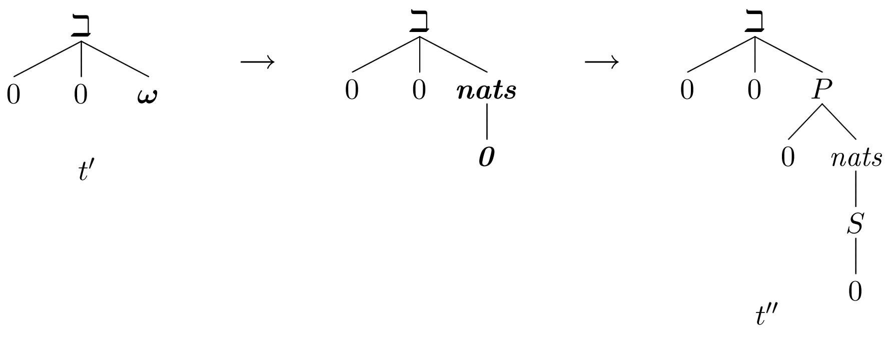

Figure 3.2: Preprocessing of t' in the proof of Lemma 3.12

Theorem 3.13 *Let $t \in Ter^{\infty}(\mathcal{D})$ be such that $Z(t)$ is finite. Let $t \twoheadrightarrow_{\omega} r$. This reduction contains only finitely many top-level steps.*

Proof Let the reduction $t \twoheadrightarrow_{\omega} r$ be of the form $t = t_0 \to t_1 \to \cdots r$. Suppose for a contradiction that it contains infinitely many top-level steps. I will inductively define a sequence of terms $\{u_n\}_{n=1}^{\infty}$ such that for all n, $u_n \to^{+} u_{n+1}$ and $Z(u_n) \equiv Z(t_{k+1})$ where $t_k \to t_{k+1}$ is the n'th top-level step (the second condition is here to strengthen the induction hypothesis). Since it will also be shown that $Z(t) \to u_1$, this will contradict termination of $\mathcal{D}_0$, as $Z(t) \in Ter(\mathcal{D}_0)$.

I start by defining u_1. Let $t_k \to_{top} t_{k+1}$ be the first top-level step. Use Lemma 3.11 to get a r s.t. $Z(t_k) \to r$ and $Z(r) = Z(t_{k+1})$. Put $u_1 \stackrel{\text{df}}{=} r$. Observe that $Z(t) \to u_1$ because by Proposition 3.10 $Z(t) = Z(t_k)$.

Now assume that u_n has already been defined. Let $t_l \to t_{l+1}$ be the nth and $t_k \to t_{k+1}$ the $n+1$st top-level step. $Z(u_n) \equiv Z(t_{l+1})$ (induction hypothesis) so by Proposition 3.10 $Z(u_n) = Z(t_k)$. Hence by Lemma 3.11 there is an r such that $Z(u_n) \to r$ and $Z(r) \equiv Z(t_{k+1})$. Now by Lemma 3.12 there is an r' with $u_n \to^{+} r'$ and $Z(r') \equiv Z(r) \equiv Z(t_{k+1})$. Put $u_{n+1} \stackrel{\text{df}}{=} r'$ to complete the construction. □

The requirement that $Z(t)$ is finite is always satisfied for $t \in \mathcal{B}$. This will be proven in the next section.

3.3 Completeness of reductions inside $\mathcal{B}$

Almost all of the tools needed to prove that reduction sequences inside $\mathcal{B}$ are infinitarily normalising and confluent have already been constructed. The last one is an important lemma about the placement of the pairing symbols in terms from $\mathcal{B}$.

Lemma 3.14 *Let $t \in \mathcal{B}$ and p be an infinite path in t. Then p contains pairing.*

Proof It is relatively easy to see that every path containing *nats* in a term in $\mathcal{B}$ is finite.[4] This observation will be used later on. Towards a contradiction suppose now that p does not contain pairing.

Since $t \in \mathcal{B}$, there is a reduction sequence $t_0 \to t_1 \to \cdots t$ for a $t_0 \in \mathit{Ker}$. Since this reduction is strongly convergent, it follows that from some t_k on there is no redex activity above the level at which p starts and that the first symbol of p is already fixed (i.e. from t_k on there is redex activity neither at the position where p starts nor above it).

Now consider a subterm t'_k of t_k having the first symbol of p as root. Clearly the subtree t' of t, having again the first symbol of p as root is an infinitary reduct of t'_k, so there is a reduction sequence $t'_k \to t'_{k+1} \to \cdots t'$ in which all the steps are steps of the reduction sequence $t_0 \to t_1 \to \cdots t$.

Call a step $t'_m \to t'_{m+1}$ in this sequence *generating* if the prefix of p without redex activity from t'_{m+1} on is longer that the prefix of p in t'_m without redex activity. A couple of observations can be made about generating steps; let $t'_m \to t'_{m+1}$ be generating:

(a) This step takes part on the fixed prefix of p or directly below it: indeed, if it were somewhere else, the length of the fixed prefix of p would be the same in t'_m and t'_{m+1}.

(b) The prefix of p from root of t_m to the root of the contracted redex (excluding the latter) is fixed in t'_m; to see this, consider the first position on p that is not yet fixed in t'_m but it is fixed in t'_{m+1}. This is a valid definition since the step is generating, but it means that this is the highest position on p that experiences redex activity during the step so it is precisely the root of the contracted redex.

(c) This step is top-level (in t'_m); indeed, by the above discussion the path from the root of active redex (excluded) to the root of t_m is a prefix of p and thus by the assumption in does not contain P. It does not contain *nats* either – because by the observation in the first line of this proof p would then be finite – and obviously does not contain ω. Moreover, since the position of the root of the active redex is already fixed in t'_{m+1}, it must be neither P (by the assumption) nor *nats* (again

[4]The reader may want to try to prove it using the methods of Section 4.4.

by first-line observation) so the step cannot be an application of either (13) or (14) because these rules introduce *nats* and P, respectively, as root of the reduct.

(d) There are infinitely many generating steps in the sequence $t'_k \to t'_{k+1} \to \cdots t'$. This follows from the fact that p is infinite but t'_m is finite: thus every generating step extends the fixed prefix of p only by a finite number of positions.

Thus the reduction $t'_m \twoheadrightarrow_\omega t'$ contains infinitely many top-level steps - a contradiction with Theorem 3.13. □

Corollary 3.15 *For every $t \in \mathcal{B}_\subseteq$, $Z(t)$ is finite.*

Proof Suppose that $Z(t)$ is infinite. Let r denote the $\mathcal{B}$-term with $t \subseteq r$.

By König's Lemma $Z(t)$ contains an infinite path. Obviously this path contains neither ω nor *nats*. It also does not contain the pairing symbol, because every pairing symbol in terms from the image of Z has 0 as both children and thus the considered path would be finite. Now use Proposition 3.8b to infer that this infinite path is present also in t, so it is also in r which is a contradiction with Lemma 3.14. □

Corollary 3.16 *Let $t \in \mathcal{B}$ be a normal form. Then t is built from 0, S and P only.*

Proof t contains neither ω nor *nats* because they give rise to redexes (rules (13) and (14)). Now suppose that t contains an arithmetical symbol. It is clear that the rightmost child of this symbol must be an arithmetical symbol again (for if it is not, then there is a redex again – cf. Table 2.2). Repeated application of this argument yields an infinite path of arithmetical symbols in t – a contradiction with Lemma 3.14. Since t contains neither *nats* nor ω nor arithmetical symbols, it is built exclusively from 0s, Ss and Ps. □

Now it is high time to prove that the reductions inside $\mathcal{B}$ are normalising.

Theorem 3.17 $\mathcal{B} \models \mathrm{WN}^\infty$. *Moreover, there is a procedure that brings every term $t \in \mathcal{B}$ to its normal form in at most ω steps.*

Proof I give an algorithm that in a finite number of steps brings every $t \in \mathcal{B}_\subseteq$ to a form where the root is 0, S or P. This algorithm, when applied top-down, level-by-level, to a $\mathcal{B}$-term yields a convergent reduction of length $\leq \omega$ whose limit is a normal form.

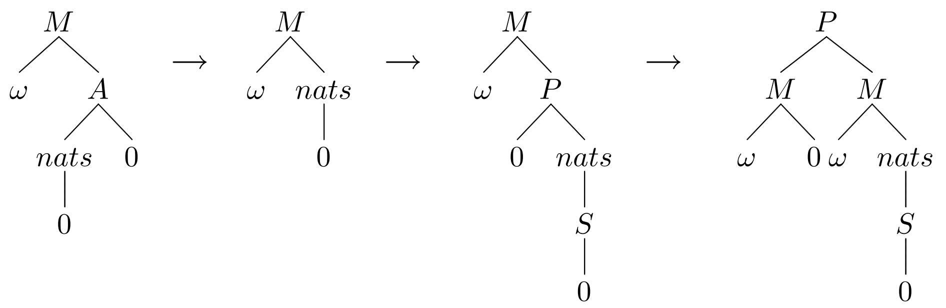

Figure 3.3: The head-normalisation algorithm applied to the term $\omega \cdot (nats(0) + 0)$. The first step is a top step that brings the term to a form where no further top steps are possible. The second step forces the rightmost path of arithmetical symbols to end with P and the last step brings this P to the root position.

Let $t \in \mathcal{B}_{\subseteq}$. All the algorithm has to do is to perform top-level steps in any order. By Theorem 3.13 it has to stop after a finite number of steps. If the root of the reduct is 0, S, or P, the required form was reached. If it is ω (or *nats*) then 2 head steps (or a single head step) bring pairing to the root position (cf. Fig. 3.2).

If the root is an arithmetical symbol, the situation is a bit more complicated. Since there is no top-level step, the rightmost child of the root has to be arithmetical again, the rightmost grandchild as well, and so on (cf. the proof of Corollary 3.16) until the path ends with ω or $nats(x)$ (this path has to be finite by Lemma 3.14 and any other terminating symbol would yield a top-level step). In this case the algorithm has to reduce ω or *nats* in the same way as before. Then, using exclusively the rules (9)–(12), it can bring pairing to the root position in n steps, where n was the number of arithmetical symbols on the considered path. $\square$

Corollary 3.18 $\mathcal{B} \models \mathrm{SN}^{\infty}$.

Proof The normalisation algorithm given in the proof of Theorem 3.17 works with any $t \in \mathcal{B}_{\subseteq}$, so $\mathcal{B}_{\subseteq} \models \mathrm{WN}^{\infty}$. Because $\mathcal{B}_{\subseteq}$ is subset- and reduction-closed, then by Proposition 1.16 $\mathcal{B}_{\subseteq} \models \mathrm{SN}^{\infty}$. This in conjunction with $\mathcal{B} \subseteq \mathcal{B}_{\subseteq}$ implies $\mathcal{B} \models \mathrm{SN}^{\infty}$.$\square$

A classical observation about finitary TRSs that WN and UN imply CR is transferable to the infinitary case: the implication $\mathrm{WN}^{\infty} \wedge \mathrm{UN}^{\infty} \Rightarrow \mathrm{CR}^{\infty}$ is true as well. $\mathcal{D} \models \mathrm{UN}^{\infty}$ because it is orthogonal, and $\mathcal{B} \models \mathrm{WN}^{\infty}$ has just been proven. This yields the infinitary confluence of reductions inside $\mathcal{B}$.

Corollary 3.19 $\mathcal{B} \models \mathrm{CR}^\infty$.

This concludes the analysis of rewriting-related properties of $\mathcal{B}$. I have proven that the reductions of terms that I restricted my attention to are infinitarily normalising and confluent. This makes the Dedekind TRS an usable machinery for computing with ordinals. Now it is time to precisely define the connection between the terms of this TRS and the ordinal numbers. It will be done in the next chapter.

Chapter 4

Semantics

In this chapter I give a semantic function mapping $\mathcal{B}$ to the class **ON** of ordinal numbers.

The expression $\bar{t}$ for a $t \in \mathcal{B}$ will always denote the normal form of t. By the completeness results from the previous chapter this normal form exists and is unique, so this symbol is well-defined. Furthermore, I make no notational distinction between arithmetical operators as syntactical elements of terms and as operations of ordinal arithmetic. Their actual meaning is to be derived from the context. The same applies to the symbols 0 and ω: sometimes they stand for the constants of the Dedekind TRS, sometimes they denote "real" ordinal numbers.

4.1 Introduction

The task of giving semantics $[\![\cdot]\!] \colon \mathcal{B} \to \mathbf{ON}$ turns out to be a nontrivial one. The elements of $\mathcal{B}$ are often infinite, so the obvious inductive definition would not be well-founded. It should in principle be possible to define the semantics on $\mathcal{B}$ along some well-founded relation other than the subterm relation. One such (unsuccessful) attempt is described in Appendix A.

Before discussing other ways of setting up the semantic function for $\mathcal{B}$, it is a good idea to specify the requirements it should meet, since obviously not every map from $\mathcal{B}$ to **ON** is acceptable.[1] The first and most natural requirement is that the semantics of a term should be preserved under reduction, i.e. $t \twoheadrightarrow r$ should imply $[\![t]\!] = [\![r]\!]$. This condition can hardly be

[1] Actually there is only one function that satisfies the requirements that are going to be stated; one of the goals of this chapter is to give a more or less constructive definition of it.

challenged: it states that whenever we have a term denoting an ordinal number then by simplifying it (for in view of $\mathcal{B} \models \mathrm{SN}^{\infty}$ every reduction brings a term "closer" to its normal form) a term denoting the same ordinal number should be obtained.

The preservation of semantics by reduction sequences is by far not enough. For example, a constant function mapping every term to the ordinal number, say, ω^2, fulfills this condition but cannot be accepted as suitable. The other requirement that is going to be imposed on the semantic function essentially makes sure that every term is mapped to the right ordinal. First, a definition:

Definition 4.1 *Define sem*: $Ker \to \mathbf{ON}$ *by the inductive clauses:*

(a) $sem(0) \stackrel{df}{=} 0$ *and* $sem(\omega) \stackrel{df}{=} \omega$,

(b) *for any* $t, r, u \in Ker$,
$sem(S(t)) \stackrel{df}{=} sem(t) + 1$,
$sem(t + r) \stackrel{df}{=} sem(t) + sem(r)$,
$sem(t \cdot r) \stackrel{df}{=} sem(t) \cdot sem(r)$,
$sem(t^r) \stackrel{df}{=} sem(t)^{sem(r)}$ *and*
$sem(\sqsupset(t, r, u)) \stackrel{df}{=} \sqsupset(sem(t), sem(r), sem(u))$.

It is clear that whenever $t \in Ker$ then $[\![t]\!] = sem(t)$ should hold. This is precisely the second condition I want the semantic function for $\mathcal{B}$ to satisfy: $[\![\cdot]\!] \restriction Ker = sem$. Since all terms in $\mathcal{B}$ have their "source" in *Ker*, the first condition (the preservation of semantics by reduction sequences) will make sure that every term is mapped to the denotation of its "source" rather than some random value.

It is tempting – or rather it springs to mind immediately – to take this second condition as the starting point of the definition of $[\![\cdot]\!]$ and for a given $t \in \mathcal{B}$ define $[\![t]\!]$ to be $sem(t_0)$, where $t_0 \in Ker$ and $t_0 \twoheadrightarrow t$. This definition, however, has two serious flaws. The first one is that its correctness requires proving. For a given term there can be many terms in *Ker* that reduce to it and, although true, it is not evident that they all get mapped by *sem* to the same ordinal. Even if this difficulty were overcome, there is another problem: there is no effective method that for an arbitrary $t \in \mathcal{B}$ produces a $t_0 \in Ker$ with $t_0 \twoheadrightarrow t$. These difficulties are reasons for abandoning the idea of defining $[\![\cdot]\!]$ in terms of *sem*. The definition of $[\![\cdot]\!]$ is going to be stated in a somehow dual way that evades both problems. It requires, however, a study of the normal forms of the meaningful terms.

4.2 Normal forms of $\mathcal{B}$-terms

In this section I show that all normal forms of terms from $\mathcal{B}$ follow a particular structural pattern. This observation is crucial for the definition of $[\![\cdot]\!]$ that is given in the next section.

Definition 4.2 *Define the class $\mathcal{N} \subseteq Ter^{\infty}(\mathcal{D})$ by the inductive clauses:*

(a) $0 \in \mathcal{N}$*,*

(b) If $t \in \mathcal{N}$ then $S(t) \in \mathcal{N}$,

(c) If $t_0, t_1, t_2, \dots \in \mathcal{N}$ then $t_0 : t_1 : t_2 : \dots \in \mathcal{N}$.

Observe that whenever there is a term $t \in Ter^{\infty}(\mathcal{D})$ such that $\overline{t} \in \mathcal{N}$ and another term $r \in Ter^{\infty}(\mathcal{D})$ s. t. $t \twoheadrightarrow r$, then $\overline{r} \in \mathcal{N}$ and $\overline{r} \equiv \overline{t}$. This fact follows from the completeness results of the previous chapter and will be used throughout the rest of this thesis without a warning or further comment.

Remark 4.3 Elements of $\mathcal{N}$ are known in the literature under the name of *tree ordinals*. Sometimes there is an extra condition in the clause (c), requiring the streams to be increasing and/or recursive. Tree ordinals play an important role in proof theory – see e.g. [Bus98].

Now I am going to prove a sequence of lemmas. The proof of each lemma uses the previous lemma and follows the same pattern as the previous proof. This is why I get less precise as the proofs go on. In particular, the third inductive clause is omitted in the proofs of Lemmas 4.5 and 4.6 as completely analogous to the case (c) of the proof of Lemma 4.4 and the proof of Lemma 4.7 is omitted in the whole.

Lemma 4.4 *Let $t, r \in \mathcal{B}$ be such that $\overline{t}, \overline{r} \in \mathcal{N}$. Then $\overline{t+r} \in \mathcal{N}$.*

Proof I prove that for every $w \in \mathcal{N}$, $\overline{t+w} \in \mathcal{N}$. This proves the claim because $\overline{r} \in \mathcal{N}$ and $\overline{t+r} \equiv \overline{t+\overline{r}}$. The proof proceeds by induction on w:

(a) $w \equiv 0$. $t + w \to t$, so $\overline{t+w} \equiv \overline{t} \in \mathcal{N}$.

(b) $w \equiv S(w')$ for a $w' \in \mathcal{N}$. $t + w \to S(t + w')$. Therefore $\overline{t+w} \equiv \overline{S(t+w')} \equiv S(\overline{t+w'})$. But $\overline{t+w'} \in \mathcal{N}$ by the induction hypothesis, so $S(\overline{t+w'}) \in \mathcal{N}$ as well.

(c) $w \equiv w_0 : w_1 : w_2 : \ldots$ for $w_0, w_1, \cdots \in \mathcal{N}$. $t + w \twoheadrightarrow (t+w_0) : (t+w_1) : (t+w_2) : \ldots$. Thus $\overline{t+w} \equiv (\overline{t+w_0}) : (\overline{t+w_1}) : (\overline{t+w_2}) : \ldots$. For every i, $\overline{t+w_i} \in \mathcal{N}$ by the induction hypothesis, so $\overline{t+w} \in \mathcal{N}$ as well. $\Box$

Lemma 4.5 *Let $t, r \in \mathcal{B}$ be such that $\overline{t}, \overline{r} \in \mathcal{N}$. Then $\overline{t \cdot r} \in \mathcal{N}$.*

Proof Again, I prove that $\overline{t \cdot w} \in \mathcal{N}$ for every $w \in \mathcal{N}$ by induction on w:

(a) $w \equiv 0$. $t \cdot w \to 0$, so $\overline{t \cdot w} \equiv \overline{0} \equiv 0 \in \mathcal{N}$.

(b) $w \equiv S(w')$ for an $w' \in \mathcal{N}$. Thus $t \cdot w \to t \cdot w' + t$. $\overline{t \cdot w'} \in \mathcal{N}$ by the induction hypothesis and $\overline{t} \in \mathcal{N}$ is assumed, so apply Lemma 4.4 to get the claim.

(c) $w \equiv w_0 : w_1 : w_2 : \ldots$. Analogous to the case (c) of the previous proof. $\Box$

Lemma 4.6 *Let $t, r \in \mathcal{B}$ be such that $\overline{t}, \overline{r} \in \mathcal{N}$. Then $\overline{t^r} \in \mathcal{N}$.*

Proof I show $\overline{t^w} \in \mathcal{N}$ for any $w \in \mathcal{N}$ by induction on w:

(a) $w \equiv 0$. Thus $t^w \to S(0)$, so $\overline{t^w} \equiv \overline{S(0)} \equiv S(0) \in \mathcal{N}$.

(b) $w \equiv S(w')$ for an $w' \in \mathcal{N}$. Thus $t^w \to t^{w'} \cdot t$. $\overline{t^{w'}} \in \mathcal{N}$ by the induction hypothesis, so apply Lemma 4.5 to get the claim.

(c) $w \equiv w_0 : w_1 : w_2 : \ldots$. Analogous to the case (c) of the previous proof. $\Box$

Lemma 4.7 *Let $t, r, u \in \mathcal{B}$ be such that $\overline{t}, \overline{r}, \overline{u} \in \mathcal{N}$. Then $\overline{\beth(t, r, u)} \in \mathcal{N}$.*

Proof Omitted. $\Box$

The above lemmas will now serve to prove the theorem that is the goal of this section.

Theorem 4.8 *Let $t \in \mathcal{B}$. Then $\overline{t} \in \mathcal{N}$.*

Proof Since $t \in \mathcal{B}$, there is a $w \in Ker$ such that $w \twoheadrightarrow t$. Moreover, $\overline{w} \equiv \overline{t}$, so it is enough to prove that $\overline{w} \in \mathcal{N}$. This is done by induction on the structure of w:

(a) $w \equiv 0$. $\overline{w} \equiv 0 \in \mathcal{N}$.

(b) $w \equiv \omega$. $\overline{\omega} \equiv 0 : S(0) : S(S(0)) : \ldots$. For any n, $S^n(0) \in \mathcal{N}$, so $0 : S(0) : S(S(0)) : \cdots \in \mathcal{N}$ as well.

(c) $w \equiv S(w')$. Thus $\overline{w} \equiv S(\overline{w'}) \in \mathcal{N}$.

(d) $w \equiv w_1 + w_2, w \equiv w_1 \cdot w_2, w \equiv w_1^{w_2}, w \equiv \sqsupset(w_1, w_2, w_3)$ – apply Lemmas 4.4 to 4.7 above.

Let $\mathrm{NF}_{\mathcal{B}}$ denote the set $\{t \in \mathcal{B} \colon t \text{ is a normal form}\}$. The above theorem states precisely that $\mathrm{NF}_{\mathcal{B}} \subseteq \mathcal{N}$. The converse is not true. Instead of giving a concrete counterexample, we point out that whenever $\mathrm{NF}_{\mathcal{B}}$ contains a stream of natural numbers, this stream is recursive (see Remark 3.3 for a proof). There is no restriction on recursiveness in the definition of $\mathcal{N}$, however, so $\mathcal{N}$ contains all streams of natural numbers, including the non-recursive ones.

4.3 Semantics for $\mathcal{B}$

Clearly, every term in $\mathcal{N}$ can in a natural way be seen as an ordinal number:

Definition 4.9 *Define $\sigma \colon \mathcal{N} \to \mathbf{ON}$ by the following inductive clauses:*

(a) $\sigma(0) \stackrel{df}{=} 0$,

(b) $\sigma(S(t)) \stackrel{df}{=} \sigma(t) + 1$,

(c) $\sigma(t_0 : t_1 : t_2 : \ldots) \stackrel{df}{=} \bigcup_{i \in \omega} \sigma(t_i)$.

The semantic function $[\![\cdot]\!]$ is now going to be defined in terms of σ. The ordinal denoted by a given term $t \in \mathcal{B}$ is the one that is represented by the normal form of t.

Definition 4.10 *Define $[\![\cdot]\!] \colon \mathcal{B} \to \mathbf{ON}$ by $[\![t]\!] \stackrel{df}{=} \sigma(\overline{t})$.*

This definition satisfies both conditions stated in the previous section. Preservation of $[\![\cdot]\!]$ by reductions follows directly from $\mathcal{D} \models \mathrm{UN}^\infty$. To prove that $[\![\cdot]\!]$ restricted to *Ker* is equal to *sem* requires a little more work.

Lemma 4.11 *Let $t, r, u \in \mathcal{B}$. The following formulae hold for arbitrary $t, r, u \in \mathcal{B}$:*

(a) $[\![S(t)]\!] = [\![t]\!] + 1$

(b) $[\![t + r]\!] = [\![t]\!] + [\![r]\!]$

(c) $[\![t \cdot r]\!] = [\![t]\!] \cdot [\![r]\!]$

(d) $[\![t^r]\!] = [\![t]\!]^{[\![r]\!]}$

(e) $[\![\sqsupset(t, r, u)]\!] = \sqsupset([\![t]\!], [\![r]\!], [\![u]\!])$.

Proof (a) is elementary. Proofs of (b)–(e) all follow the same pattern. Every one of them uses the previous as well as continuity of an appropriate operation of ordinal arithmetic. Therefore only the proof of (d) is given; the use of the continuity, crucial for this proof, is marked by letters "ON" over the equality sign:

Observe that $[\![t^r]\!] = [\![t^{\overline{r}}]\!]$ since $r \twoheadrightarrow \overline{r}$. Thus it is enough to prove that $[\![t^w]\!] = [\![t]\!]^{[\![w]\!]}$ for any $w \in \mathcal{N}$. This is now done by induction on w:
ZERO: $w \equiv 0$. $t^w \to S(0)$ so $[\![t^w]\!] = [\![S(0)]\!] = 1 = [\![t]\!]^0 = [\![t]\!]^{[\![w]\!]}$.
SUCCESSOR: $w \equiv S(w')$ for a $w' \in \mathcal{N}$. $t^w \to t^{w'} \cdot t$ so $[\![t^w]\!] = [\![t^{w'} \cdot t]\!] \overset{(c)}{=} [\![t^{w'}]\!] \cdot [\![t]\!] \overset{\text{IH}}{=} [\![t]\!]^{[\![w']\!]} \cdot [\![t]\!] = [\![t]\!]^{[\![w']\!]+1} = [\![t]\!]^{[\![w]\!]}$.
STREAM: $w \equiv w_0 : w_1 : w_2 : \ldots$. $t^w \twoheadrightarrow (t^{w_0}) : (t^{w_1}) : (t^{w_2}) : \ldots$ so $[\![t^w]\!] = [\![(t^{w_0}) : (t^{w_1}) : (t^{w_2}) : \ldots]\!] = \bigcup_{i \in \mathbb{N}} [\![t^{w_i}]\!] \overset{\text{IH}}{=} \bigcup_{i \in \mathbb{N}} ([\![t]\!]^{[\![w_i]\!]}) \overset{\text{ON}}{=} [\![t]\!]^{\bigcup_{i \in \mathbb{N}} [\![w_i]\!]} = [\![t]\!]^{[\![w]\!]}$. $\square$

This is already enough to prove that $[\![\cdot]\!]$ fulfils the second condition.

Theorem 4.12 *For every $t \in Ker$, $[\![t]\!] = sem(t)$.*

Proof Induction on t:

(a) $t \equiv 0$. $[\![t]\!] = [\![\overline{0}]\!] = [\![0]\!] = 0 = sem(0)$.

(b) $t \equiv \omega$. $[\![t]\!] = \omega = sem(t)$.

(c) $t \equiv S(t_1), t \equiv t_1 + t_2, t \equiv t_1 \cdot t_2, t \equiv t_1^{t_2}, t \equiv \sqsupset(t_1, t_2, t_3)$ – apply Lemma 4.11 above. $\square$

4.4 Expressive power of the Dedekind TRS

The topic of this section is the image of $[\![\cdot]\!]$.

Definition 4.13 *Set $I \overset{df}{=} \{[\![t]\!] \colon t \in \mathcal{B}\}$.*

Proposition 4.14 *I has no greatest element.*

Proof Suppose $\alpha \in I$ is the greatest element of I. Then $\alpha = [\![t]\!]$ for a term $t \in \mathcal{B}$. There is a $t_0 \in Ker$ with $t_0 \twoheadrightarrow t$. $S(t_0) \in Ker \subseteq \mathcal{B}$, so $[\![S(t_0)]\!] \in I$, but $[\![S(t_0)]\!] = [\![t_0]\!] + 1 = [\![t]\!] + 1 = \alpha + 1$ and α is not the greatest element of I – a contradiction. □

Definition 4.15 *An* (unary) predicate *is a subset of* $Ter^{\infty}(\mathcal{D})$*. If* H *is a predicate, the notation* $H(t)$ *instead of* $t \in H$ *is used.*

Definition 4.16 *A predicate* $H \subseteq Ter^{\infty}(\mathcal{D})$ *is called* 1-stable *if* $H(t)$ *and* $t \to r$ *imply* $H(r)$*.*

Definition 4.17 *A predicate is called* ω-stable *if for every convergent* ω*-sequence* $t_0 \to t_1 \to \cdots t$ *with* $H(t_i)$ *for every* i*,* $H(t)$ *holds as well.*

These concepts are independent, for example "t is finite" is 1-stable but not ω-stable and "t is infinite" is ω-stable but not 1-stable.

Theorem 4.18 *Let* H *be an* 1*-stable and* ω*-stable predicate with* $Ker \subseteq H$*. Then* $\mathcal{B} \subseteq H$*.*

Proof Obvious. □

There is nothing revolutionary about the above observation. It is just an abstraction of a simple proof technique: in order to prove that all $\mathcal{B}$-terms have a certain property, prove that all terms from *Ker* have it (structural induction on terms can be useful here) and that it is preserved by finite (so in fact preservation by a single step is enough) and infinite reductions (here thanks to Compression Lemma, ω-long reductions are sufficient). I am now going to use this technique to prove that $\mathcal{B}$ is closed under a slightly strengthened subterm relation.

Definition 4.19 *Define the predicate* H *by*

$$H(t) \equiv t \in \mathcal{B} \wedge \forall (F \in \{S, A, M, exp, \sqsupset, P\}) \forall (F(t_1, \ldots, t_n) \subseteq t)(t_1 \in \mathcal{B})$$

Definition 4.20 *Define the predicate* G *by*

$$G(t) \equiv t \in \mathcal{B} \wedge \forall (\sqsupset(t_1, t_2, t_3) \subseteq t)(t_2 \in \mathcal{B})$$

Proposition 4.21 $Ker \subseteq H$ *and* $Ker \subseteq G$*.*

Proof Obvious, since *Ker* is closed under the usual subterm relation. □

Lemma 4.22 $\mathcal{B} \subseteq G$

Proof In view of Theorem 4.18, it suffices to show that G is both 1- and ω-stable.
1-STABLE: (sketch) Thanks to the fact that no rule *introduces* $\sqsupset$ (in the sense in which, for example, rule 4 introduces $+$), the second argument of this symbol can only be changed via a reduction inside it and this kind of change cannot force it outside $\mathcal{B}$.
ω-STABLE: Let $t_0 \to t_1 \to \cdots t$ and $G(t_i)$ for every i. Fix a subterm $\sqsupset(a, b, c)$ of t. There is an $n \in \mathbb{N}$ such that from t_n on, all reductions take place at the level that is lower than the position of b in t. Hence there is a subterm $\sqsupset(a', b', c') \subseteq t_n$, located at the same position that $\sqsupset(a, b, c)$ in t, and b is a reduct of b'. Since $b' \in \mathcal{B}$ from $G(t_m)$, $b \in \mathcal{B}$ as well.$\square$

Theorem 4.23 *H is 1-stable.*

Proof Let $t \to r$ and $H(t)$. Denote the active redex in t by u and its contractum in r by v. Let $F(r_1, \ldots, r_n) \subseteq r$. The goal is to show $r_1 \in \mathcal{B}$. Argue by cases:

(a) r_1 and v are disjoint. Then r_1 is present in t, also as the leftmost child of F, thus $r_1 \in \mathcal{B}$ follow from $H(t)$.

(b) $v \subseteq r_1$. Then r_1 is a reduct of a rightmost child of F in t. Hence $r_1 \in \mathcal{B}$, because $H(t)$ and $\mathcal{B}$ is closed under reductions.

(c) $r_1 \subsetneq v$. This is the critical case. Let us consider the exact position of r_1 in v, remembering that v is unifiable with one of 14 right-hand side rule patterns, each of depth at most 2.

   (i) If the entire term $F(r_1, \ldots, r_n)$ is inside a subterm of v that was unified with a variable, then $F(r_1, \ldots, r_n)$ was a subterm of t and the claim follows from $H(t)$.

   (ii) If r_1 was unified with a variable, then this variable appears on the left-hand side of the applied rule as a leftmost child of one of the symbols S, A, M, *exp*, $\sqsupset$, P and thus the claim follows from $H(t)$ again. The exception here is the 14^{th} rule, but in this case r_1 is simply a numeral of the form $S^n(0)$ and belongs to $\mathcal{B}$ as required.

   (iii) The last subcase is when $v \equiv F(r_1, \ldots, r_n)$. Confront Table 2.2 to see that either one of the above subcases is applicable or r_1 is of the form $\phi(t_1, ..., t_n)$ where for every i, $t_i \in \mathcal{B}$ – either by $H(t)$ or by $G(t)$ – and ϕ is arithmetical. Thus by Theorem 3.6 $r_1 \in \mathcal{B}$ as required. $\square$

Theorem 4.24 *$\mathcal{B} \subseteq H$.*

Proof It suffices to show that H is ω-stable. This is analogous to the second part of the proof of Lemma 4.22.$\square$

All these ugly syntactical results can now be used to prove something quite useful, yet not surprising: the meaningful streams are built from meaningful blocks.

Theorem 4.25 *Let $t \equiv t_0 : t_1 : t_2 : \ldots \in \mathcal{B}$. Then for every i, $t_i \in \mathcal{B}$.*

Proof Fix i. Observe that $t_i : (t_{i+1} : t_{i+2} : \ldots) \subseteq t$. Then $t_i \in \mathcal{B}$ follows from $H(t)$.$\square$

This is already enough to show that I is downward-closed: another not surprising but nontrivial result.

Theorem 4.26 *Let $\beta \in I$ and $\alpha < \beta$. Then $\alpha \in I$.*

Proof Towards a contradiction, let β be the smallest element of I for which there is a smaller α outside I. There is a term $b \in \mathcal{N} \cap \mathcal{B}$ with $[\![b]\!] = \beta$. First I show that β must be a limit; for suppose it is not. Consider the possible forms of b: if $b \equiv S(b')$ for some b', then by Theorem 4.24 $b' \in \mathcal{B}$. Since $[\![b']\!] = [\![b]\!] - 1$, we have $\alpha \leq [\![b']\!]$. But $\alpha \notin I$, so $\alpha < (\beta - 1) \in I$ – a contradiction with the definition of β. Thus β is a successor ordinal denoted by the stream $b \equiv b_0 : b_1 : b_2 : \ldots$ (this is possible – cf. Example 2.5). Hence $[\![b_i]\!] = \beta$ for an i. By the above discussion b_i has to be a stream again, and repeating this argument ω times yields a contradiction with the definition of $\mathcal{N}$. Thus β is a limit ordinal and b is a stream.

The very same method allows to assume that there is a stream denoting β that is strictly increasing from some point on; if b does not have this property then one of its elements has to denote β and it has to be a stream itself, so either it is strictly increasing or one of its element has to denote β, etc. Without loss of generality assume that b is strictly increasing from some point on.

The last step of this proof is an easy one: since $\alpha < \beta$ and $[\![b]\!] = \beta$ then there is a b_i with $[\![b_i]\!] > \alpha$. The construction of b gives $[\![b_i]\!] < \beta$ and Theorem 4.25 yields $[\![b_i]\!] \in I$ – a contradiction with the definition of β. $\square$

There is only one more question left: how high can we go, i.e. what is the value of $\sup I$? The answer is ε_ω and is due to Ariya Ishihara. The following proofs are also due to Ariya, but any possible inaccuracies are mine as I changed his proofs a bit to suit my presentation.

Lemma 4.27 *For every $n \in \mathbb{N}$ there is an $e_n \in \mathcal{B}$ with $[\![e_n]\!] = \varepsilon_n$.*

Proof Define e_n inductively: $e_0 \stackrel{\text{df}}{=} \sqsupset(\omega, \omega, \omega)$, $e_{k+1} \stackrel{\text{df}}{=} \sqsupset(e_k+1, \omega, \omega)$. $[\![e_n]\!] = \varepsilon_n$ follows from the definition of epsilon numbers – consult [Sie65]. □

Corollary 4.28 $\sup I \geq \varepsilon_\omega$.

Lemma 4.29 *The equation $\sqsupset(\alpha, \beta, \gamma) = \varepsilon_{n+1}$ holds for any $n \in \mathbb{N}$ and for any α, β, γ with $\varepsilon_n < \alpha \leq \varepsilon_{n+1}$, $\omega \leq \beta < \varepsilon_{n+1}$ and $\omega \leq \gamma$.*

Proof Fix n, α and β as above. The proof proceeds by transfinite induction on γ:
BASE (ω): $\sqsupset(\alpha, \beta, \omega) = \lim(\alpha, \beta^\alpha, \beta^{\beta^\alpha}, \ldots)$. Every component in this sequence can be shown to be less than ε_{n+1}: $\alpha < \varepsilon_{n+1}$ is assumed, $\beta^\alpha < \varepsilon_{n+1}$ because $\beta < \varepsilon_{n+1}$ and $\alpha < \varepsilon_{n+1}$ (epsilon numbers are closed under exponentiation – see [Sie65] again), $\beta^{\beta^\alpha} < \varepsilon_{n+1}$ because $\beta < \varepsilon_{n+1}$ and $\beta^\alpha < \varepsilon_{n+1}$ and so on. Thus $\sqsupset(\alpha, \beta, \omega) \leq \varepsilon_{n+1}$. On the other hand $\sqsupset(\alpha, \beta, \omega) \geq \sqsupset(\varepsilon_n + 1, \omega, \omega) = \varepsilon_{n+1}$.
SUCCESSOR: $\sqsupset(\alpha, \beta, \gamma + 1) = \beta^{\sqsupset(\alpha,\beta,\gamma)} \stackrel{\text{IH}}{=} \beta^{\varepsilon_{n+1}} = \varepsilon_{n+1}$ where the last equality follows again from the basic properties of epsilon numbers.
LIMIT: If γ is a limit then the claim follows from the induction hypothesis and continuity of $\sqsupset$.□

Corollary 4.30 $\sup I \leq \varepsilon_\omega$

Proof The above lemma shows precisely that ε_ω cannot be obtained by the applications of stacking, but stacking is the strongest operation available in $\mathcal{D}$. Thus $\varepsilon_\omega \notin I$ and the claim follows from Theorem 4.26. □

Appendix A

Another approach to semantics

The definition of $[\![\cdot]\!]$ given in Chapter 4 has an obvious drawback that I was careful not to mention until now, although I am sure that the reader did spot it. Namely, to find the ordinal that is denoted by the given term, this term first has to be reduced to its normal form; it would be desirable, though, to have a definition that gives the semantics of a term "in place", so to say. The usual way of achieving this is to define the semantic function $[\cdot]$ inductively, by setting $[0] \stackrel{\text{df}}{=} 0$, $[\omega] \stackrel{\text{df}}{=} \omega$, $[S(t)] \stackrel{\text{df}}{=} [t]+1$, $[t+r] \stackrel{\text{df}}{=} [t]+[r]$, $\ldots$, $[t:r] \stackrel{\text{df}}{=} [t] \cup [r]$. It can easily be seen that this definition is not well-founded – it does not work for infinite terms. Now consider the following, slightly changed definition:

Definition A.1 *Define* $[\cdot] : \mathcal{B}_{\subseteq} \to \mathbf{ON}$ *recursively:*

(a) $[0] \stackrel{\textit{df}}{=} 0,\ [\omega] \stackrel{\textit{df}}{=} \omega$

(b) $[t+r] \stackrel{\textit{df}}{=} [t]+[r]$

(c) $[t \cdot r] \stackrel{\textit{df}}{=} [t] \cdot [r]$

(d) $[t^r] \stackrel{\textit{df}}{=} [t]^{[r]}$

(e) $[\sqsupset(t,r,u)] \stackrel{\textit{df}}{=} \sqsupset([t],[r],[u])$

(f) $[nats(x)] \stackrel{\textit{df}}{=} \omega$

(g) $[t:r] \stackrel{\textit{df}}{=} \begin{cases} [t] \cup [r] & \text{if } r \text{ is not a stream} \\ [t] \cup \bigcup_{i\in\mathbb{N}}[r_i] & \text{if } r \text{ is a stream of the form } r_0 : r_1 : r_2 : \ldots. \end{cases}$

The goal is to use $[\cdot]$ instead of $[\![\cdot]\!]$. This would be possible if the following propositions were established:

(1) Definition A.1 is well-founded

(2) $[\cdot]$ is preserved under reductions

(3) $[\cdot] \restriction \mathit{Ker} = \mathit{sem}$

The proof of (1) should probably start with a strengthening of Lemma 3.14 to assert that every infinite path in a $\mathcal{B}$-term contains *only* pairing from some point on. This seems to be true and yet turned out to be irritatingly difficult to prove. This condition, however, is not sufficient to guarantee the well-foundedness of the above definition (consider for example the full infinite binary tree labeled with P). A stronger result about "structural decency" of $\mathcal{B}$-terms would be needed, for example "every infinite path in a $\mathcal{B}$-term eventually turns out to be a stream", i.e. after a finite number of symbols it has only Ps and they are arranged in a way where every one is the right child of the previous. This seems to be true as well, and this is already enough for the Definition A.1 to be well-founded.

(2) seems to be easier than (1). Preservation of $[\cdot]$ by finite reductions looks straightforward, as all the rules are compatible with the Definition A.1, in the sense that $[\cdot]$ gives the same "metavalues" for left- and right-hand sides.[1] Preservation by infinite reductions looks a bit trickier, but it turns out that preservation by ω-sequences of terms starting in Ker is enough: for let $t \twoheadrightarrow r$ for $t, r \in \mathcal{B}$. Let $t_0 \in \mathit{Ker}$ be such that $t_0 \twoheadrightarrow t$. Thus $t_0 \twoheadrightarrow r$ and by Compression Lemma $t_0 \twoheadrightarrow_\omega t$ and $t_0 \twoheadrightarrow_\omega r$. If $[\cdot]$ is now preserved by ω-reductions starting in Ker, then $[t] = [t_0] = [r]$.

(3) is immediate, so if (1) and (2) are proven, then $[\cdot]$ will be shown to satisfy the requirements for the semantic function set in Section 4.1 and therefore equal to $[\![\cdot]\!]$.

[1] For example rule (4): $[x \cdot S(y)] = [x] \cdot [S(y)] = [x] \cdot ([y]+1) = [x] \cdot [y] + [x] = [x \cdot y] + [x] = [x \cdot y + x]$.

Bibliography

[Baa98] F. Baader and T. Nipkow *Term Rewriting and All That.* Cambridge University Press 1998.

[Bus98] S. R. Buss (editor) *Handbook of Proof Theory.* Elsevier 1998

[Ded88] R. Dedekind *Was sind und was sollen die Zahlen?* Vieweg 1888.

[Dev93] K. Devlin *The Joy of Sets. Fundamentals of Contemporary Set Theory.* Second Edition, Springer 1993.

[Klo02] J. W. Klop, V. van Oostrom, R. de Vrijer *Iterative Path Orders: Extended abstract*, 2002. Available at `http://www.phil.uu.nl/~oostrom/typcomp/01-02/ipo.pdf`.

[Klo05] J. W. Klop and R. C. de Vrijer *Infinitary Normalization.* In S. Artemov, H. Barringer, A. S. d'Avilla Garcez, L. C. Lamb and J. Woods (editors) *We Will Show Them: Essays in Honour of Dov Gabbay*, Vol. 2, College Publications 2005, pp. 169–192

[Kur68] K. Kuratowski and A. Mostowski *Set Theory.* PWN – Polish Scientific Publishers and North-Holland Publishing Company 1968.

[Oud05] IJ. Ph. Oudshoorn *Rekenen met ordinalen in een termherschrijfsysteem.* Bachelor Thesis, Free University, Amsterdam 2005 (in Dutch). Available at `http://www.cs.vu.nl/~ipoudsho/RekenenMetOrdinalen.pdf`.

[Sie65] W. Sierpiński. *Cardinal and Ordinal Numbers.* PWN – Polish Scientific Publishers 1965.

[Ter03] Terese (editors M. Bezem, J. W. Klop and R. de Vrijer) *Term Rewriting Systems.* Cambridge University Press 2003.