Ackermann's Substitution Method (remixed) [1]

Georg Moser

University of Innsbruck, Computational Logic
Technikerstraße 21a
A-6020 Innsbruck, Austria

Abstract

We aim at a conceptually clear and technically smooth investigation of Ackermann's substitution method: W. Ackermann (Mathematische Annalen, 117:162–194, 1944). Our analysis provides a direct classification of the provably recursive functions of $\mathsf{PA}(\varepsilon)$, i.e. Peano Arithmetic framed in the ε-calculus.

Key words: Epsilon substitution method, Provably recursive functions.
1991 MSC: 03F30, 03F05, 03F15

1 Introduction

A classification of the provably recursive functions of Peano Arithmetic (PA) in terms of Kreisel's class of ordinal recursive functions was suggested in [1]. This class can in turn be characterised by hierarchies of number-theoretic functions defined by transfinite recursion up-to the ordinal ε_0, cf. [2]. Kreisel's solution of the classification problem for the provably recursive function of PA is based on *Ackermann's consistency proof* of arithmetic [3], framed in Hilbert's ε-calculus.

Hilbert's ε-calculus [4, 5, 6] is based on an extension of the language of predicate logic by a term-forming operator ε_x. This operator is governed by the *critical axiom*

$$A(t) \supset A(\epsilon_x A(x)) \ ,$$

where t is an arbitrary term. Within the ε-calculus quantifiers become definable by $\exists x A(x) \Leftrightarrow A(\epsilon_x A(x))$ and $\forall x\ A(x) \Leftrightarrow A(\epsilon_x \neg A(x))$. The expression $\epsilon_x A(x)$ is called *ε-term*.

Email address: `georg.moser@uibk.ac.at` (Georg Moser).
[1] Work partially supported by Marie Curie grant no. HPMF-CT-2002-015777.

When considering arithmetical systems the ε-substitution method [3, 4] provides an analogue to Gentzen's famous extension [7, 8] of his cut-elimination method. Tait [9] describes the substitution method as the general problem of associating with a formal system S, admitting quantifiers, a free-variable system $S^\star$ without quantifiers and to give an effective procedure of transforming statements A in (the language of) S into statements $A^\star$ in (the language of) $S^\star$. Assume S proves A, then the transform of A is to be an *ε-substitution instance* $A^\star$ of A. It is obtained by replacing ε-terms by terms in the language of $S^\star$. For Peano Arithmetic coached in the ε-calculus, this procedure of eliminating bounded variables from arbitrary proofs, is sufficient to establish consistency (and even 1-consistency). The difficult part is to show that the substitution method terminates.

Let $\mathsf{PA}(\varepsilon)$ denote Peano arithmetic framed in the ε-calculus. Based on Gentzen's work, revealing the role played by transfinite induction up to ε_0, Ackermann [3] presented a constructive termination proof of the substitution method for $\mathsf{PA}(\varepsilon)$. As an important achievement he defined functions, ordinal recursive in ε_0, that bound the *complexity* of the transformation procedure.[2] It is a direct consequence of Ackermann's proof, firstly observed by Kreisel [1], that the provably recursive functions of PA are primitive recursive in some $\prec \epsilon_0$-recursive functions. Thus [3] renders a Π^0_2-analysis of PA and establishes 1-consistency of PA; see also [10].

We analyse Ackermann's solution and in particular the given complexity analysis of the substitution method. In our presentation we follow the original treatment closely. The novelty being that we are able to measure the complexity of the substitution method directly in terms of the fast-growing *Hardy hierarchy* (see [11]), i.e., functions from the Hardy hierarchy replace the specific ordinal recursive functions—seemingly ad-hoc defined—employed in [3]. Thus we show that any provably recursive function of $\mathsf{PA}(\varepsilon)$ can be elementarily defined in some H_α, $\alpha \prec \varepsilon_0$ and therefore the class of provably recursive functions of $\mathsf{PA}(\varepsilon)$ equals the Hardy class $\mathcal{H}$. The same machinery is applied to characterise the provably recursive functions of a weak arithmetic theory without induction axiom (or rule); here the Hardy hierarchy can be replaced by the *slow-growing hierarchy*. We have replaced the set-theoretical ordinals employed in Ackermann's proof by (structured) tree-ordinals.

The reader may wonder why we have based our investigation on the original—quite old—treatment of the substitution method; the work by Arai [12, 13], Avigad [10], Buchholz, Mints, and Tupailo [14], Mints [15, 16], and Tait [17, 9] spring to mind as more adequate starting points. However, to our surprise, it turned out that once we understood how to replace Ackermann's original repre-

[2] By *complexity* of the substitution method we understand the maximal number of approximation steps necessary till the final substitution is rendered.

sentation and codings of (set-theoretical) ordinals by structured tree-ordinals, the desired results followed quite easily. Thus by changing the employed ordinal notation we can establish the direct characterisation result, but still follow the original presentation closely enough to render a modern presentation of Ackermann's ideas.

In contrast to Gentzen-style proof theory by cut-elimination the substitution method is less dependent on the structure of a given derivation in S. We employ this fact to separate the actual substitution method and the ε-calculus. This allows us to make an abstract assessment of the transformation procedure incorporated in the substitution method apart from the ε-calculus trade. In the next section we define a class of tautologies $\mathcal{S}$ and we re-formulate the problem of the substitution method accordingly. Only after we have studied the behaviour of the transformation procedure with respect to the class $\mathcal{S}$ in some detail, we relate our findings to a suitable axiomatisation of Peano arithmetic in the ε-calculus and thus obtain the main result of this work.

2 The formal system $\mathcal{S}$

We assume an arbitrary but fixed *language* $\mathcal{L}$ of arithmetic, such that $\mathcal{L}$ does not contain quantifiers. Instead of including $\neg$ as a logical connective, negation is defined by asserting that atomic formulas $R(t_1, \ldots, t_n)$ occur in complementary pairs $\overline{R}(t_1, \ldots, t_n)$. Note that $\overline{\overline{R}}(\ldots) := R(\ldots)$. In this sense the classical double negation law becomes a syntactic equality. Using de Morgan's laws this definition is lifted to the general level.

It is notationally convenient to distinguish between *bound* $(x, y, z, \ldots)$ and *free* variables $(a, b, c, \ldots)$, respectively. Bound variables are collected in the set BV, while free variables are collected in the set FV; we set $\mathcal{V} := \mathsf{FV} \cup \mathsf{BV}$. *Terms* in $\mathcal{L}$ are constructed from *constants*, *free variables*, and *function symbols* as usual. *Semi-terms* are like terms but may also contain *bound* variables. *Formulas* are defined with the proviso that only bound variables are allowed to be quantified and only free variables may occur free. *Semi-formulas* are similar to formulas with the exception that both free and bound variables may occur free in a semi-formula. An *expression* is either a (semi-)term or a (semi-)formula.

We use the metasymbols $f, g, h, \ldots$ to denote function symbols, while the metasymbols $P, Q, R, \ldots$ vary through predicate symbols. We write $\mathrm{ar}(f)$ $(\mathrm{ar}(P))$ to denote the arity of a function (predicate) symbol f (P). Within this text we are eager to use only the symbols k, l, m, n, p, q as denotations of natural numbers. Deviations from this convention will be clearly marked. We write $[1, n]$ to denote the interval of natural numbers from 1 to n. Occasionally we abbreviate tuples of terms $(t_1, \ldots, t_n)$ as $\overline{t}$. The length of the tuple will always be clear from the context.

We need not be very specific on atoms, however we assume that in the standard-model ($\mathcal{N}$)

$$\langle \mathbb{N}, 0, \mathrm{S}, \ldots, R_j^{\mathbb{N}}, \ldots \rangle ,$$

they are to be interpreted as *elementary* relations. [3] With respect to the specific atomic formulas that we will encounter below, this requirement is met; S denotes the successor function.

A substitution σ—denoted as $\{a_1 \mapsto t_1, \ldots, a_n \mapsto t_n\}$—is a mapping from the set of variables to the set of terms such that $\sigma(a_i) = t_i$ and $\sigma(a) = a$, for almost all a. Let A be a formula and $t_1, \ldots, t_n$ terms. If there exists a formula B and n distinct variables $a_1, \ldots, a_n$ s.t. A is equal to $B\{a_1 \mapsto t_1, \ldots, a_n \mapsto t_n\}$ then for each $i \in [1, n]$, the occurrences of t_i in A resulting from this replacement are said to be *indicated* in A. This fact is also expressed (less accurately) in writing B as $B(a_1, \ldots, a_n)$ and A as $B(t_1, \ldots, t_n)$. We say that a term t is *fully indicated* in A if every occurrence of t in A can be obtained by such an replacement (from some formula B, $n = 1$ and $t = t_1$), cf. [8]. It is easy to see how this notion is generalised to arbitrary expressions.

Below we introduce a set of quasi-tautologies, denoted as $\mathcal{S}$, based on an extensions $\mathcal{L}^{\mathrm{ext}}$ of the language $\mathcal{L}$ by new function symbols $f_1, \ldots, f_q$ of fixed arity. The arity of a function symbol f is denoted as $\mathrm{ar}(f)$. Each such function symbol f_i will be called *defined.* Before we can define the class of quasi-tautologies $\mathcal{S}$ precisely, we have to introduce specific *quantifier-free formulas*, which will be present in all studied quasi-tautologies and govern the defined functions symbols.

The *definition formulas* for f_i, $\mathrm{ar}(f_i) = l$, are substitution instances of

$$A(t, s_1, \ldots, s_l) \supset A(f_i(s_1, \ldots, s_l), s_1, \ldots, s_l) , \tag{1}$$

where A is quantifier-free. By $A(f_i(\overline{s}), \overline{s})$ we denote the replacement of the indicated occurrences of t in $A(t, \overline{s})$ by $f_i(\overline{s})$. The term t is called *critical.*

Furthermore we want to express that the defined function symbols fulfil certain minimality constraints. To that avail we consider instances of

$$A(t, s_1, \ldots, s_l) \supset f_i(s_1, \ldots, s_l) \leq t , \tag{2}$$

for each defined f_i. This formula is called *second definition formula* or *minimality formula* for f_i.

[3] A function f is called *elementary* (in a function g) if f is definable explicitly from $0, 1, +, \cdot, \dot{-}$ (and g), using bounded sum, and product. The elementary functions are collected in the class ELEM. A predicate is *elementary*, if its characteristic function is.

As we want $\leq$ to be interpreted in its usual sense, we need the presence of formulas defining basic relations between terms. Thus we will employ substitution instances of the weak arithmetical axioms given in Table 1.

Table 1
Arithmetical axioms

$N1.$	$\mathrm{S}(s) \neq 0$	$N6.$	$s \cdot \mathrm{S}(t) = (s \cdot t) + s$
$N2.$	$\mathrm{S}(s) = \mathrm{S}(t) \supset s = t$	$N7.$	$s \not< 0$
$N3.$	$s + 0 = s$	$N8.$	$s < \mathrm{S}(t) \Leftrightarrow s \leq t$
$N4.$	$s + \mathrm{S}(t) = \mathrm{S}(s + t)$		
$N5.$	$s \cdot 0 = 0$		

To deal properly with equality, instances of the axioms given in Table 2 have to be considered, together with instances of the following *identity formulas*

$$s = t \supset f_i(u_1, \ldots, u_{i-1}, s, u_{i+1}, \ldots, u_l) = f_i(u_1, \ldots, u_{i-1}, t, u_{i+1}, \ldots, u_l) \ . \tag{3}$$

for all defined function symbols f_i.

Table 2
Identity axioms

$E1.$ $s = s$

$E2.$ $s = t \supset g(u_1, \ldots, u_i, s, u_{i+1}, \ldots, u_l) = g(u_1, \ldots, u_i, t, u_{i+1}, \ldots, u_l)$
if $g \in \mathcal{L}$ and $\mathrm{ar}(f) = l$

$E3.$ $s = t \supset R(u_1, \ldots, u_i, s, u_{i+1}, \ldots, u_l) \supset R(u_1, \ldots, u_i, t, u_{i+1}, \ldots, u_l)$
if $R \in \mathcal{L}$ and $\mathrm{ar}(R) = l$

Finally we are in a position to give the definition of the class of quasi-tautologies $\mathcal{S}$.

Suppose $T \in \mathcal{L}^{\text{ext}}$ is a quasi-tautology which can be written in the form

$$A_1 \wedge \cdots \wedge A_m \wedge B_1 \wedge \cdots \wedge B_n \supset F \ , \tag{4}$$

such that each A_i is an instance of formulas of the form (1)—(3), while each B_i is an instance of the axioms given in Table 1 or Table 2. Then T belongs to the class $\mathcal{S}$ and no formula which cannot be defined in this way belongs to $\mathcal{S}$.

In this abstract setting the substitution method can be reformulated as the following problem.

> *Can we (effectively) replace the defined function symbols in F by functions $\mathbb{N}^n \to \mathbb{N}$ such that the resulting formula $F^\star$ is valid in the standard-model $\mathcal{N}$.*

Firstly assume that only instances of the axioms given in Table 1 or Table 2 are present as assumptions in a tautology $T \in \mathcal{S}$. Then $\mathcal{N} \models B_i$ for all $i = 1, \ldots, n$ and we obtain $\mathcal{N} \models F$. Hence, to solve the problem it is sufficient to define an assignment Ψ of defined functions such that Ψ transforms each A_i to a true arithmetical formula. Moreover it is sufficient to concentrate on those defined function symbols that actually occur in A_i $(i = 1, \ldots, m)$: Assume these form a proper subset of all occurring defined function symbols in T and we are given an assignment Ψ of functions for this subset: Such an assignment is extended by assigning to all other function symbols the constant function 0.

The formulas (1)–(3) are called *critical axioms*. If we need to distinguish between them, then axioms of the form (1) will be called *critical axioms of first kind*, axioms of form (2) will be called *minimality axioms* or *critical axioms of second kind*, and the axioms of form (3) will be called *critical identity axioms*.

Suppose $T(a_1, \ldots, a_k) \in \mathcal{S}$ is arbitrary but fixed and all free variables in T are indicated. Let $(n_1, \ldots, n_k)$ be an arbitrary tuple of natural numbers and $n = \max\{n_1, \ldots, n_k\}$. In the sequel, we consider the quasi-tautology $T(n_1, \ldots, n_k)$. The set of critical axioms A_i occurring in T is denoted by $\mathcal{C}$. W.l.o.g. we denote the set of defined function symbols occurring in $\mathcal{C}$ by

$$f_1, f_2, \ldots, f_q \ ,$$

and assume that f_i $(i = 1, \ldots, q)$ always refers to a defined function symbol. Note that during the substitution method n is not changed, as only the evaluation of terms of form $f_j(\overline{s})$ may change.

We assume the sequence of function symbols to be ordered in a suitable way. Let f_i be governed by a critical axiom of the form

$$A(r(t), \overline{s}) \supset A(r(f_i(\overline{s})), \overline{s}) \ .$$

If u with leading function symbol f_j occurs in $r(a)$, then we assume that f_j precedes f_i in the chosen order, i.e. $j < i$ holds.

Remark 2.1 *At the time being, we cannot decide whether a total order on the defined function symbols exits, fulfilling the requirement. We will see later that this assumption can be met, when we apply the abstract method to* $\mathsf{PA}(\varepsilon)$*, where the defined function symbols will be replaced by* ε*-matrices, see Section 6.*

3 Structured Ordinals

We use ‘structured’ ordinals in the treatment of the substitution method. By a ‘structured’ countable ordinal, we mean an ordinal with an arbitrary but fixed fundamental sequence $\langle\lambda_x\rangle_{x\in\mathbb{N}}$ for any limit λ. We follow [11] in our presentation. For proofs of Lemmas and Propositions of this section see [11]. The set Ω of countable *tree-ordinals* is inductively defined as (i) $0 \in \Omega$, (ii) $\alpha \in \Omega$ implies $\alpha + 1 := \alpha \cup \{\alpha\} \in \Omega$, and (iii) $\forall x \in \mathbb{N}\ (\alpha_x \in \Omega)$ implies $\alpha := \langle a_x\rangle_{x\in\mathbb{N}} \in \Omega$. We use lower case Greek letters $\alpha, \beta, \gamma, \lambda, \dots$ to denote tree-ordinals (with the exception of ε and μ). We use the convention that λ always denotes a limit: $\lambda := \langle\lambda_x\rangle_{x\in\mathbb{N}}$. Alternatively, we write $\lambda = \sup \lambda_x$.

The order $\prec$ on tree-ordinals is defined according to the rules (for $\alpha, \lambda \in \Omega$). (i) $\alpha \prec \alpha + 1$, and (ii) $\lambda_m \prec \lambda$, for all $m \in \mathbb{N}$. Note, that $\prec$ constitutes a partial order. We identify $n \in \mathbb{N}$ with $0 + \overbrace{1 + \cdots + 1}^{n-\text{times } 1}$. We define $\omega_0 := \sup\langle x\rangle$; $\omega := \sup\langle 1 + x\rangle$. Clearly ω_0 and ω are $\prec$-incomparable.

Let $n \in \mathbb{N}, \alpha, \lambda \in \Omega$. The finite set $\alpha[n]$ of *n-predecessors* of α is recursively defined. (i) $0[n] := \emptyset$, (ii) $(\alpha+1)[n] := \alpha[n] \cup \{\alpha\}$, and (iii) $\lambda[n] := \lambda_n[n]$. The *immediate n-predecessor* of α, the $\prec$-maximal element of $\alpha[n]$, if $\alpha[n] \neq \emptyset$, is denoted by $P_n(\alpha)$. (If $\alpha[n] = \emptyset$, then $P_n(\alpha) := 0$.) The set of *structured* tree-ordinals Ω^S consists of all $\alpha \in \Omega$ such that $\forall\lambda \preceq \alpha, x \in \mathbb{N}\ \lambda_x \in \lambda[x + 1]$.

Lemma 3.1 *For every $\alpha \in \Omega^S$ we have (i) $\alpha[0] \subseteq \cdots \subseteq \alpha[n] \subseteq \alpha[n+1] \subseteq \cdots$, (ii) $\beta \prec \alpha$ iff $\beta \in \alpha[n]$ for some $n \in \mathbb{N}$, and (iii) $\beta \in \alpha[n]$ implies $\beta[n] \subset \alpha[n]$.*

Addition, multiplication and exponentiation on Ω are defined in the obvious way.

$$\begin{array}{lll}
\alpha + 0 := \alpha & \alpha + (\beta + 1) := (\alpha + \beta) + 1 & \alpha + \lambda := \sup(\alpha + \lambda_x)\ , \\
\alpha \cdot 0 := 0 & \alpha \cdot (\beta + 1) := (\alpha \cdot \beta) + \alpha & \alpha \cdot \lambda := \sup(\alpha \cdot \lambda_x)\ , \\
\alpha^0 := 1 & \alpha^{\beta+1} := \alpha^\beta \cdot \alpha & \alpha^\lambda := \sup(\alpha^{\lambda_x})\ .
\end{array}$$

We need to know that these operations are well-defined on (structured) tree-ordinals. This is accomplished by the following two lemmas.

Lemma 3.2 *Let α, β, and $\gamma \in \Omega$. Then $\gamma \in \beta[n]$ implies (i) $\alpha+\gamma \in (\alpha+\beta)[n]$, (ii) $\alpha \cdot \gamma \in (\alpha \cdot \beta)[n]$ if $0 \in \alpha[n]$, and (iii) $\alpha^\gamma \in \alpha^\beta[n]$ if $1 \in \alpha[n]$.*

Lemma 3.3 *Let α, β, and $\gamma \in \Omega$. Then $\alpha, \beta \in \Omega^S$ implies (i) $\alpha + \beta \in \Omega^S$, (ii) $\alpha \cdot \beta \in \Omega^S$ if $0 \in \alpha[n]$, and (iii) $\alpha^\beta \in \Omega^S$ if $1 \in \alpha[n]$.*

We usually drop the brackets in $(\alpha + \beta)[n], (\alpha \cdot \beta)[n]$, respectively and write $\alpha+\beta[n], \alpha\cdot\beta[n]$, instead. Clearly $\omega_0, \omega \in \Omega^S$. Simple applications of the lemmas gives: If $\alpha_1, \dots, \alpha_r \in \Omega^S$, then $\omega^{\alpha_1} \cdot n_1 + \cdots + \omega^{\alpha_r} \cdot n_r$ is structured. We obtain that $\omega^\alpha[n]$ contains all ordinals of the form

$$\omega^{\beta_1} \cdot m_1 + \omega^{\beta_2} \cdot m_2 + \cdots + \omega^{\beta_k} \cdot m_k\ ,$$

such that $\beta_1 \succ \cdots \succ \beta_k$ and $\beta_i \in \alpha[n]$, furthermore $m_i \leq n$. We define

$\exp_\alpha(\beta) := \alpha^\beta$ and the n-iterate of that $\exp^n_\alpha(\beta) := \alpha^{\cdot^{\cdot^{\cdot^{\alpha^\beta}}}} \}_{n-\text{times }\alpha}$. We define $\varepsilon_0 := \sup(1, \omega, \omega^\omega, \ldots)$; clearly $\varepsilon_0 \in \Omega^S$. Moreover $\alpha \prec (\varepsilon_0)_n$ iff α can be written in Cantor normal form $\omega^{\beta_1} \cdot m_1 + \omega^{\beta_2} \cdot m_2 + \cdots + \omega^{\beta_k} \cdot m_k$, $\beta_k \prec \beta_{k-1} \prec \cdots \prec \beta_1 \prec (\varepsilon_0)_{n-1}$.

For each unary function f, f^n denotes its n^{th} iterate, defined by $f^0(a) = a, f^{n+1}(a) = f(f^n(a))$. Sometimes we use the operator J to denote the n^{th} iteration of f. Then $f^n(a)$ is written $J(f,n)(a)$.

We define three subrecursive hierarchies of number-theoretic functions. We start with the *slow-growing functions*

$$\mathrm{G}_0(n) := 0 \qquad \mathrm{G}_\alpha(n) := \mathrm{G}_{P_n(\alpha)}(n) + 1 \ .$$

The *Hardy functions* are defined as follows

$$\mathrm{H}_0(n) := n \qquad \mathrm{H}_\alpha(n) := \mathrm{H}_{P_n(\alpha)}(n+1) \ .$$

Finally we define the *fast growing functions.*

$$\mathrm{F}_0(n) := n+1 \qquad \mathrm{F}_\alpha(n) := \mathrm{F}^{n+1}_{P_n(\alpha)}(n) \ .$$

Lemma 3.4 *Let $\alpha \in \Omega^S$. Then (i) G_α is increasing (strictly increasing if α is infinite), and if $\beta \in \alpha[n]$, then $\mathrm{G}_\beta(n) < \mathrm{G}_\alpha(n)$. Furthermore (ii) H_α (F_α) is strictly increasing and if $\beta \in \alpha[n]$, then $\mathrm{H}_\beta(n) < \mathrm{H}_\alpha(n)$ ($\mathrm{F}_\beta(n) < \mathrm{F}_\alpha(n)$).*

Lemma 3.5 *For all non-zero $\alpha \in \Omega^S$ $\mathrm{G}_\alpha(n) < \mathrm{H}_\alpha(n) < \mathrm{F}_\alpha(n)$.*

It is interesting to note that the slow-growing hierarchy $\bigcup_{\alpha<\epsilon_0} \mathrm{G}_\alpha$ captures the elementary functions. Note that $\mathrm{H}_{\alpha+\beta} = \mathrm{H}_\alpha \circ \mathrm{H}_\beta$ and $\mathrm{H}_{\omega^\alpha} = \mathrm{F}_\alpha$.

Below we will only be considered with *structured tree-ordinals*. Hence, we usually drop the references to Ω^S and simply speak of (tree-)ordinals.

4 Ackermann's Substitution Method

In this section we briefly state the termination proof of the ε-substitution method, cf. [3, 4]. We follow the presentation in [3] quite closely.

The starting idea of the substitution method is to replace the defined function symbols f_i by *functions of finite support.*[4] When we have assigned functions

[4] A function $\phi \colon \mathbb{N}^n \to \mathbb{N}$ is of finite support if $\phi(n_1, \ldots, n_l)$ is non-zero only for finitely many arguments $n_1, \ldots, n_l$.

to $f_1, \dots, f_q$ we are in a position to evaluate every formula in $\mathcal{C}$ either to a true or false formula in $\mathcal{N}$. Such an assignment is called a *(ε-)substitution*. A substitution S is *solving*, or *final* if all formulas in $\mathcal{C}$ are rendered true on the basis of S. By definition, every critical identity axiom is evaluated to a true formula. Hence the substitution method needs to be concerned with critical formulas of 1st and 2nd kind, only.

Let G_0 denote the *initial substitution*. This substitution instantiates all the $f_1, \dots, f_q$ by the *default value*, the constant function 0. Suppose we have already constructed a number of substitutions $G_0, \dots, G_i$ and G_i is not a solving substitution.

Definition 4.1 *Let S be a substitution, by recursion on the term structure we define the* value $|t|$ *of a term $f \in \mathcal{L}^{ext}$ with respect to S. If $t \in \mathcal{L}$, then $|t| \in \mathbb{N}$ is defined as usual, employing the recursive definitions of the function symbols in Table 1. Otherwise suppose $t = f_i(s_1, \dots, s_l)$. Then $|t| := \phi(n_1, \dots, n_l)$, where ϕ is the function assigned to f_i under S and $|s_i| = n_i$ for all $i = 1, \dots, l$.*

We write $t \hookrightarrow_S z$ to denote that the term t evaluates (in $\mathcal{N}$) to the natural number z with respect to the substitution S. Let $\overline{t} = (t_1, \dots, t_n)$ and $\overline{m} = (m_1, \dots, m_n)$. Then we write $\overline{t} \hookrightarrow_S \overline{m}$ as an abbreviation of $t_i \hookrightarrow_S m_i$ for all i.

We define the consecutive substitution G_{i+1}: Let the critical axioms in $\mathcal{C}$ be ordered in some arbitrary way, but fixed. We pick the first critical axiom of 1st kind that is false in $\mathcal{N}$ with respect to G_i. Suppose this axiom has the form

$$A(t, \overline{s}) \supset A(f_p(\overline{s}), \overline{s}) \ . \tag{5}$$

This critical axioms is called the *designated* critical axiom of G_{i+1}. If $t \hookrightarrow_{G_{n+1}} z$, then $A(z, \overline{s})$ is evaluated to true on the basis of the substitution G_i. Let $\overline{n}$ be the values of $\overline{s}$. We consider the sequence of formulas

$$A(1, \overline{n}), \dots, A(z, \overline{n}) \ , \tag{6}$$

and evaluate this sequence with respect to G_i. Let k be the smallest number such that $A(k, \overline{n})$ holds in $\mathcal{N}$. Let ϕ denote the function assigned to f_p by G_i. We define a new function ψ by modifying ϕ as follows. We write $m_1, \dots, m_l = n_1, \dots, n_l$ ($m_1, \dots, m_l \neq n_1, \dots, n_l$) to abbreviate $\forall i \; m_i = n_i$ ($\exists i \; m_i \neq n_i$).

$$\psi(m_1, \dots, m_l) := \begin{cases} \phi(m_1, \dots, m_l) & m_1, \dots, m_l \neq n_1, \dots, n_l \ , \\ k & m_1, \dots, m_l = n_1, \dots, n_l \ . \end{cases}$$

The substitution G_{i+1} is obtained by replacing the assignment of ϕ to f_p by ψ. The assignments for f_j, $j < p$ are left intact. Assignments to $f_j, j > p$ are changed to the default value 0. The following lemma follows easily from the definitions, see. [3]. As an immediate consequence of this lemma we obtain that in the process of consecutive constructed substitutions, only critical formulas of 1st kind can be evaluated to false, under a particular substitution S.

Lemma 4.1 *Let f_p be a l-ary defined function symbol. Let S denote an arbitrary substitution. The function assigned to f_p under the assignment S is denoted by ϕ. Then for all tuples $\overline{n} = n_1, \ldots, n_l$ either $\phi(\overline{n}) = 0$, or if $\phi(\overline{n}) = z > 0$, then $A(z, \overline{n})$ evaluates to true with respect to S, and for all $w < z$, $A(z, \overline{n})$ evaluates to false.*

Note that this lemma is only true when we throw away previously achieved assignments for function symbols f_j $j > p$. The lemma fails if this step is omitted. We give a slight reformulation of an example by v. Neumann to explain this, compare [18] and [4], pp. 123–125.

Example 4.1 *We write* S *for the successor and* P *for the predecessor. Let $n \in \mathbb{N}$ such that $n \geq 1$ and let f denote a unary defined function symbol and g a nullary defined function symbol, such that f is smaller than g in the assumed order on defined function symbols. Further set $A(a, b) :\Leftrightarrow a = b$ and $B(a) :\Leftrightarrow f(S(a)) = 0 \supset a = n$. Consider the following formulas.*

$$g = g \supset g = f(g) , \tag{7}$$
$$(f(S(n)) = 0 \supset n = n) \supset (f(S(g)) = 0 \supset g = n) , \tag{8}$$
$$(f(S(P(g)) = 0 \supset P(g) = n) \supset g \leq P(g) . \tag{9}$$

It is not difficult to see that (7) is the definition formula for f with respect to $A(a, g)$ such that g is the critical term. While (8) is a definition formula for g with respect to $B(n)$ so that n is the critical term. Furthermore (9) denotes a minimality formula with respect to $B(P(g))$, where $P(g)$ is the critical term.

We define a sequence of substitution steps starting with the initial substitution G_0. We write ψ and χ for the functions assigned to f and g respectively. By definition, G_1 sets ψ and χ to the constant function 0*. Hence (7) and (9) evaluate to true, but (8) evaluates to false. The next substitution S_1 is obtained by setting $\chi := n$. With respect to G_1 (8) and (9) evaluate to true, but (7) evaluates to false. Hence to obtain the next substitution S_2 we have to change the definition of ψ. We set $\psi(n) := n$ and $\psi(a) := 0$ for all $a \neq n$ and momentarily assume that χ is not changed. (Contrary to the above definition.)*

Now with respect to G_2 (7) and (8) evaluate to true, but (9) evaluates to false. Indeed on the basis of S_2 the value n for χ is no longer minimal, as $B(n-1)$ is true, too. Hence in the definition of G_3 we have to change the value of χ from n to $n - 1$. This contradicts Lemma 4.1.

On the other hand, if we apply the presented definition, then G_2 would set $\chi := 0$. Then (7) and (9) evaluate to true, but (8) evaluates to false and *the just described process can be repeated. It is not difficult to see that the final substitution assigns f the function ψ, s.t. ψ is defined as $\psi(m) := m$ if $m \in [1, n]$ and $\psi(m) := 0$ otherwise. The defined function symbol g is assigned 0.*

Definition 4.2 *Let S be a substitution different from the initial one. Let i be the maximal such that f_i is assigned a function different from the constant function 0. Then the* characteristic number *of S is $q - i + 1$, or alternatively the characteristic number of S is the position of f_i in the reversed order of the sequence $f_1, \ldots, f_q$. In the case where S denotes the initial substitution its characteristic number is defined as $q + 1$.*

The following lemma follows directly from the definitions.

Lemma 4.2 *Let $(S_1, \ldots, S_n)$ be an arbitrary consecutive sequence of substitutions. If all substitutions $S_2, \ldots, S_n$ have characteristic number less than m, then the functions assigned to the symbols $f_1, \ldots, f_{q-m+1}$ are equal for all $S_1, \ldots, S_n$.*

Let $A_1, \ldots, A_m$ be a sequence of formulas and let $t_1, \ldots, t_e$ be all the terms with a defined function symbol as leading function symbol occurring in this sequence. The sequence $(t_1, \ldots, t_e)$ is assumed to be ordered in such a way that all proper subterms of t_i occur to the left of t_i in the sequence.

Depending on the current substitution S we assign a binary string to the sequence: If t_i evaluates to 0 with respect to S, then the i^{th} entry in the string is 1, otherwise the i^{th} entry is 0. We want to code this string $\bar{s}$ by a natural number $\ulcorner \bar{s} \urcorner$. Although any coding fulfilling some natural restriction might do, the following has nice properties, which we will exploit later on. Let $\bar{s} = s_1 \cdots s_e$ be a $(0-1)$-string, then

$$\ulcorner \bar{s} \urcorner := 2^{e-1} \cdot s_1 + \cdots + 2^1 \cdot s_{e-1} + 2^0 \cdot s_e \, , \tag{10}$$

codes $\bar{s}$. Clearly $0 \leq \ulcorner \bar{s} \urcorner < 2^e$. The code of the binary string assigned to the sequence $(t_1, \ldots, t_e)$ is called the *index* of the sequence of formulas $(A_1, \ldots, A_m)$ (with respect to S). The index of $(A_1, \ldots, A_m)$ is denoted as $\mathrm{index}_S(A_1, \ldots, A_m)$.

In particular two specific sequences of formulas are of interest.

(1) The sequence of all formulas in our given set of critical axioms $\mathcal{C}$.
(2) Let $A(t, \overline{s}) \supset A(f_p(\overline{s}), \overline{s})$ be the designated critical axiom of a substitution S under consideration such that $s_1, \ldots, s_l \hookrightarrow_S n_1, \ldots, n_l$. Then the sequence (6), p. 9 will be the second formula-sequence of specific interest.

W.l.o.g. we can always assume that the number of terms $t_1, \ldots, t_e$ with a defined function symbol as leading function symbol in $\mathcal{C}$ is not zero. Let p

be a pairing function for the natural numbers with inverses u, v: $p(0,0) = 0$; $p(u(a), v(a)) = a$, $u(p(a,b)) = a$, and $v(p(a,b)) = b$. We use $\langle a, b\rangle$ as an abbreviation for $p(a,b)$. If a is the index with respect to the first formula-sequence, and b the index with respect to the second, then we assign the pair $\langle a, b\rangle$ to S. (The initial substitution G_0 is assigned the index $\langle a, 0\rangle$.) Let S be a substitution. If the pair $\langle a, b\rangle$ is assigned to S, then the *(ordinal) index of* S, denoted as $\text{ORD}(S)$, is the tree-ordinal $\omega a + b$.

Definition 4.3 *For all $i \in [1, q]$, let f_i be an arbitrary defined function symbol and let ϕ^i_S, ϕ^i_T be functions assigned to f_i under the substitutions S and T. Then T is* progressive *over S, if for all $\overline{n} = n_1, \ldots, n_l$*

(1) $\phi^i_S(\overline{n}) = 0$, *or*
(2) $\phi^i_S(\overline{n}) = \phi^i_T(\overline{n}) > 0$.

Lemma 4.3 *Let T be progressive over S and let $(A_1, \ldots, A_m)$ be an arbitrary list of formulas. Then either $index_T(A_1, \ldots, A_m) < index_S(A_1, \ldots, A_m)$ or the evaluations of the terms $t_1, \ldots, t_e$ with leading function symbol f_i in the sequence $(A_1, \ldots, A_m)$ are the same under both substitutions.*

Theorem 4.1 *If G_l is progressive over G_k, then either* $\text{ORD}(G_l) \prec \text{ORD}(G_k)$ *or G_{l+1} is progressive over G_{k+1}.*

Proof. Let $\langle i_k, j_k\rangle, \langle i_l, j_l\rangle$ be the index pairs assigned to G_k, G_l, respectively. Apply Lemma 4.3 with respect to the sequence of formulas in $\mathcal{C}$. If $i_k > i_l$, then $\omega i_k + j_k \succ \omega i_l + j_l$ and the conclusion of the theorem follows.

If $i_k = i_l$, then according to the previous lemma the evaluation of the terms in $\mathcal{C}$ is the same, hence the designated critical axiom

$$A(t, \overline{s}) \supset A(f_p(\overline{s}), \overline{s})) ,$$

is the same for the substitutions G_k and G_l. (Here the assumed order on the critical axioms in $\mathcal{C}$ is needed.)

Suppose $t \hookrightarrow_{G_k} z$ (i.e., $t \hookrightarrow_{G_l} z$) and $\overline{s} \hookrightarrow_{G_k} \overline{n}$. By assumption, the formula-sequence (6) is the same for G_k and G_l. Applying the lemma again: Either $j_k > j_l$, or the evaluations of the terms in this sequence is equal. Then the smallest k such that $A(k, \overline{n})$ evaluates to true is the same for G_k, G_l. Hence $\phi_{G_k}(\overline{n}) = \phi_{G_l}(\overline{n})$. The progressivity of G_{l+1} over G_{k+1} follows from the assumption that G_l is progressive over G_k. $\square$

We need some further definitions: A 1-*sequence* of substitutions is simply a substitution. Let $(S_1, \ldots, S_n)$ be an arbitrary consecutive sequence of substitutions, $n \geq 1$. If the characteristic numbers of S_1, S_{n+1} are greater than or equal to m and the characteristic numbers of the substitutions $S_2, \ldots, S_n$ are strictly smaller than m, then $(S_1,\dots,S_n)$ constitutes an *m-sequence*. (If S_n is the last substitution in the maximal sequence of substitutions, we drop the condition for S_{n+1}.)

By definition, the sequence of all possible substitutions is a $q+1$-sequence. This sequences is called the *maximal* or *total* sequence. The following lemma is proven by induction on m.

Lemma 4.4 *Let R be an m-sequence $(S_1,\dots,S_n)$. Then either all the characteristic numbers of $S_2,S_3,\dots,S_n$ are less than $m-1$. In this case R constitutes also an $(m-1)$-sequence. Otherwise R decomposes into sub-sequences $T_1,\dots,T_r$, where the T_i are $(m-1)$-sequences meeting the condition: If S_{21},S_{31}, $\dots$,S_{r1} denote the first substitutions in $T_2,T_3,\dots T_r$ respectively, then the characteristic numbers of $S_{21},\dots,S_{r1}$ are $m-1$ respectively.*

The *(ordinal) index of an m-sequence*, $m>1$, is defined inductively: Let $(S_1,\dots,S_n)$ be substitutions constituting the m-sequence. Using Lemma 4.4 we find $(m-1)$-sequences $T_1,\dots,T_r$ that built the m-sequence. Assume for all $i\in[1,r]$ the indices of T_i are denoted as α_i. Then the (ordinal) index of $S_1,\dots,S_p$ is defined as $\omega^{\alpha_1}+\dots+\omega^{\alpha_r}$.

Theorem 4.2 *Let $(S_1,\dots,S_k)$ and $(S_{k+1},\dots,S_{k+l})$ denote the substitutions in two consecutive m-sequences, such that the characteristic number of S_{k+1} equals m. Let $\alpha_1,\alpha_2,\dots,\alpha_{k+l}$ be the indices of the substitutions $S_1,S_2,\dots,S_{k+l}$ respectively. Then there exists $i\in[1,l]$, such that $\alpha_{k+i}\prec\alpha_i$ and $\alpha_{k+j}=\alpha_j$, for all $j\in[1,i-1]$.*

Proof. First we show that S_{k+1} is progressive over S_1. We only prove the case where $k>1$, the other case is similar, but simpler Lemma 4.2 implies that all the $S_2,\dots,S_k$ change only the assignments for f_j, where $j>q-m+1$. As S_1, and S_{k+1} have characteristic number greater than or equal to m, this implies S_{k+1} changes the assignment to f_{q-m+1} and resets the previous assignments to $f_{q-m+2},f_{q-m+3},\dots,f_q$. Using Lemma 4.1 we see that this is only possible by changing a default value. Hence S_{k+1} is progressive over S_1.

Now we are in a position to apply Theorem 4.1: Either $\alpha_{k+1}\prec\alpha_1$ or conclude that $\alpha_{k+1}=\alpha_2$ and S_{k+2} is progressive over S_2. If $\alpha_{k+1}\prec\alpha_1$ then we are done. Otherwise the result that S_{k+2} is progressive over S_2 serves as the assumption for another application of Theorem 4.1, etc.

It remains to prove that there exists an $i\in[1,l]$ such that $\alpha_{k+i}\prec\alpha_i$. We concentrate on the case when $k=l$. Let $\alpha_k=\alpha_{k+l}$ and suppose S_{k+l+1} is progressive over S_{k+1}. It follows from $\alpha_k=\alpha_{k+l}$ and the proof of Theorem 4.1 that the designated critical axiom $A(t,\overline{s})\supset A(f_p(\overline{s}),\overline{s})$ is the same for S_{k+1},S_{k+l+1}. Suppose $\overline{s}\hookrightarrow_{S_k}\overline{n}$ By definition, S_{k+1} assigned a function ϕ to f_p such that $\phi(n_1,\dots,n_l)=u>0$. Suppose S_{k+l+1} assigns ψ to f_p s.t.

$\psi(n_1, \ldots, n_l) = v > 0$. Note that $u \neq v$, as otherwise $A(f_p(\overline{s}), \overline{s})$ is true under S_{k+l+1}. By the assumption the tuple $\overline{s}$ evaluates to $\overline{n}$ independently of the substitution S_{k+1}, S_{k+l+1}.

The characteristic number of S_{k+1} is equal to m which implies $p \leq q - m + 1$. However, the characteristic number of the substitutions $S_{k+2}, \ldots, S_{k+l}$ are less than m. Therefore none of this substitutions S_{k+i} can change the assignment to f_p. Hence S_{k+l+1} changes the assignment for f_p from ϕ to ψ such that $\phi(n_1, \ldots, n_l) = u$ and $\psi(n_1, \ldots, n_l) = v$ and $u \neq v$. (Note that v cannot equal u as otherwise the designated critical axioms would be true in S_{k+l}.) This contradicts Lemma 4.1. □

The substitutions S_i, S_{k+i} are the *designated substitutions* with respect to. the m-sequences $(S_1, \ldots, S_k)$ and $(S_{k+1}, \ldots, S_{k+l})$. All substitutions $S_j, S_{k+j}; 1 < j \leq i$ have pairwise the same characteristic number. This observation provides the basis for the next lemma.

Lemma 4.5 *Let $(S_1, \ldots, S_k)$ and $(S_{k+1}, \ldots, S_{k+l})$ be consecutive m-sequences s.t. the characteristic number of S_{k+1} equals m. Let S_i, S_{k+i} denote the designated substitutions. For $s \in [1, m]$, let $(\beta_1, \ldots, \beta_r)$ and $(\beta_{r+1}, \ldots, \beta_{r+z})$ denote the indices of the consecutive s-sequences in $(S_1, \ldots, S_k)$ and $(S_{k+1}, \ldots, S_{k+l})$. If S_i occurs in the s-sequences with index β_t, then S_{k+i} occurs in the s-sequence with index β_{r+t}. Moreover $\beta_1 = \beta_{r+1}, \beta_2 = \beta_{r+2}, \ldots, \beta_{t-1} = \beta_{r+t-1}$.*

Theorem 4.3 *Let $(S_1, \ldots, S_k)$ and $(S_{k+1}, \ldots, S_{k+l})$ be substitutions in two consecutive m-sequences such that the characteristic number of S_{k+1} equals m. For $s \in [1, m]$, let $(\beta_1, \ldots, \beta_r)$ and $(\beta_{r+1}, \ldots, \beta_{r+z})$ be the indices of included s-sequences. Then there exists $t \in [1, r]$ such that $\beta_{r+t} \prec \beta_t$ and $\beta_1 = \beta_{r+1}, \beta_2 = \beta_{r+2}, \ldots, \beta_{t-1} = \beta_{r+t-1}$.*

Proof. By induction on $s \leq m$. The case $s = 1$ is contained in Theorem 4.2.

Let $(\beta_1, \ldots, \beta_r)$ and $(\beta_{r+1}, \ldots, \beta_{r+z})$ be the indices of the $(s+1)$-sequences included in the two given m-sequences. Let S_i, S_{k+i} denote the distinguished substitutions with respect to $(S_1, \ldots, S_k)$ and $(S_{k+1}, \ldots, S_{k+l})$. By Lemma 4.5 there exists $t \in [1, r]$ such that if S_i occurs in the $(s+1)$-sequence R_t coded by β_t, then S_{k+i} occurs in the $(s+1)$-sequence R_{r+t} coded by β_{r+t}.

Using Lemma 4.4 we conclude that R_t and R_{r+t} are built up from s-sequences $(V_1, \ldots, V_u)$, $(W_1, \ldots, W_w)$ with indices $(\gamma_1, \ldots, \gamma_u)$, $(\delta_1, \ldots, \delta_w)$, respectively. Applying Lemma 4.5 for s on these s-sequences we conclude that the number of s-sequences preceding V_1 in $(S_1, \ldots, S_k)$ equals the number of s-sequences preceding W_1 in $(S_{k+1}, \ldots, S_{k+l})$. Furthermore the respective indices are pairwise the same.

We apply IH for s. Hence there exists $v \in [1,u]$ such that

$$\delta_v \prec \gamma_v \quad \text{and} \quad \delta_j = \gamma_j \quad \text{for all } j \in [1, v-1] \ . \tag{11}$$

We apply the theorem—setting $m = s$—successively for the pairs (V_1, V_2), (V_2, V_3), …, (V_{u-1}, V_u) and (W_1, W_2), (W_2, W_3), …, (W_{w-1}, W_w). This yields

$$\delta_w \prec \delta_{w-1} \prec \cdots \prec \delta_1 \qquad \gamma_u \prec \gamma_{u-1} \prec \cdots \prec \gamma_1 \ . \tag{12}$$

Putting (11) and (12) together we obtain, using $1 \in \omega[n]$ for arbitrary n.

$$\begin{aligned}\beta_{r+t} &= \omega^{\delta_1} + \cdots + \omega^{\delta_{v-1}} + \omega^{\delta_v} + \cdots + \omega^{\delta_w} \\ &\prec \omega^{\gamma_1} + \cdots + +\omega^{\gamma_{v-1}} + \omega^{\gamma_v} \preceq \beta_t \ .\end{aligned}$$

Hence the theorem follows. □

Corollary 4.1 *The substitution method terminates.*

Corollary 4.2 *Let $T \in \mathcal{S}$ be a tautology of the form* (4) *represented as*

$$A_1 \wedge \cdots \wedge A_m \wedge B_1 \wedge \cdots \wedge B_n \supset F(f_1, \ldots, f_q) \ ,$$

containing the defined function symbols $f_1, \ldots, f_q$. Then there exists a formula $F^\star$, quantifier-free, that is free of the defined function symbols $f_1, \ldots, f_q$ such that $\mathcal{N} \models F^\star$.

5 Extraction of Bounds

Suppose the technical assumption on the order of the defined symbols $f_1, \ldots, f_q$ can be met. Then any tautology of form (4) in $\mathcal{S}$ can be transformed to a true arithmetical formula $F^\star$, free of defined function symbols. However, at the moment we only know that *some* functions of finite support ϕ_i are assigned to the f_i. This motivates the question whether we can describe these functions ϕ_i more precisely.

We define a subset of structural tree-ordinals $\Omega^I \subset \Omega^S$. Let $\alpha \in \Omega^S$ be given, then $\alpha \in \Omega^I$, if either

(1) $\alpha = \omega a + b$, where α denotes the ordinal index of a substitution, or
(2) $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_r}$, where α denotes the ordinal index of an m-sequence.

We call $\alpha \in \Omega^I$ *sequence coding*, or alternatively say that α *codes a sequence.* Let $\alpha \in \Omega^I$ due to case 2, such that α can be written as $\omega^{\alpha_1} + \cdots + \omega^{\alpha_r}$. Then each α_i codes a sequence and $\alpha_1 \succ \cdots \succ \alpha_r$; this follows from the results of Section 4.

We define a function $\mathrm{C}\colon \Omega \to \mathbb{N}$ as follows. Assume $\alpha \in \Omega^I$, then

$$\mathrm{C}(\alpha) := \begin{cases} 1 & \text{if } \alpha \in \Omega^I \text{ due to Case 1 above ,} \\ \mathrm{C}(\alpha_1) + \cdots + \mathrm{C}(\alpha_r) & \text{if } \alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_r} \text{ and Case 2 holds .} \end{cases}$$

Otherwise, if $\alpha \notin \Omega^I$, then $\mathrm{C}(\alpha) := 0$.

If α codes an m-sequence R then $\mathrm{C}(\alpha)$ measures the number of substitutions included in the sequence R. Note that C is not a *norm* in the sense of [19]. It violates the criteria $\forall\alpha\forall n\ \mathrm{Card}(\{\beta \prec \alpha\colon\ \mathrm{C}(\beta) \leq n\}) \prec \omega$.

Let S denote a substitution in the total sequence of substitutions $G_0, \ldots, G_i, G_{i+1}, \ldots$ Suppose the value of a term $f_j(\overline{s})$ $(j = 1, \ldots, q)$ under S is m. By our assumptions on $\mathcal{L}$ the value of any closed term in $\mathcal{C}$ can be bounded by an increasing elementary function $g(m)$. Recall that the set of critical axioms $\mathcal{C}$ is based on the tautology $T(n_1, \ldots, n_k)$, with $n := \max\{n_1, \ldots, n_k\}$. It follows by an easy induction that the value of any term $t \in \mathcal{C}$ with respect to G_i is less than or equal to $g^{i+1}(n)$.

Recall the definition of the binary string assigned to the sequence (6) with respect to a substitution G_i on page 11. Moreover recall the employed coding (10) of this string and the definition of the index of (6). If t denotes the critical term, then the length of the sequence (6) employed in the definition of G_i equals z, where $t \hookrightarrow_{G_{i-1}} z$. Suppose e denotes the number of terms of the form $f_j(\overline{s})$ in $\mathcal{C}$. Then the index with respect to (6) is smaller than $2^{J(g,i)(n)\cdot e}$.

Recall that during the substitution method n is not changed, only the evaluation of terms of form $f_j(\overline{s})$ may change. Let $h(a, b)$—parameterised in g—be a primitive recursive function, strictly increasing in both arguments, such that

$$h(a, b) \geq \max\left\{q + 1, 2a + b + 1, g^a(b), 2^{J(g,a)(b)\cdot e}\right\} .$$

The *position* of some substitution S in the total sequence $G_0, \ldots, G_i, G_{i+1}, \ldots$ is defined as the number i, s.t. $S = G_i$.

Theorem 5.1 *Let S_k and S_l be substitutions. Let p denote the position of S_l. If S_l is progressive over S_k, then either* $\mathrm{Ord}(S_l) \in \mathrm{Ord}(S_k)\,[h(p, n)]$ *or S_{l+1} is progressive over S_{k+1}.*

Proof. Using Theorem 4.1, we conclude that either S_{l+1} is progressive over S_{k+1} or $\mathrm{Ord}(S_l) \prec \mathrm{Ord}(S_k)$ holds. In the latter case, it remains to establish $\mathrm{Ord}(S_l) \in \mathrm{Ord}(S_k)\ [h(p, n)]$. We assume the notation of the proof of Theorem 4.1.

Let $\mathrm{Ord}(S_k) = \omega{\cdot}i_k{+}j_k$ and $\mathrm{Ord}(S_l) = \omega{\cdot}i_l{+}j_l$. Either (i) $i_k > i_l$ or (ii) $i_k = i_l$ and $j_k > j_l$, holds. Suppose $i_k > i_l$; It suffice to show $\omega \cdot i_l + j_l \in \omega \cdot i_k\ [h(p, n)]$.

Suppose $f_p(\overline{s}) \hookrightarrow_{S_l} z$. Using the above observations we see that $z \leq g^{p+1}(n)$ holds and therefore $j_l \leq h(p,n)$. Now the claim follows as

$$\omega \cdot i_l + j_l \in \omega \cdot (i_k - 1) + h(p,n) + 1\ [h(p,n)] = \omega \cdot i_k\ [h(p,n)]\ .$$

On the other hand suppose $i_k = i_l$ and $j_k > j_l$. Then the theorem follows from the definition of an n-predecessors, see Section 3 □

We fix some notation: Let $(S_1, \ldots, S_k)$ and $(S_{k+1}, \ldots, S_{k+l})$ be two consecutive m-sequences such that the characteristic number of S_{k+1} equals m. Suppose σ and ρ denotes the ordinal coding the first and second m-sequence. Furthermore we denote the position of S_1 by $a \in \mathbb{N}$, $a \geq 0$ and set $p := a + \mathrm{C}(\sigma)$.

Theorem 5.2 *Let $(S_1, \ldots, S_k)$, $(S_{k+1}, \ldots, S_{k+l})$ be consecutive m-sequences as defined above. Let $\alpha_1, \alpha_2, \ldots, \alpha_{k+l}$ denote the indices of S_1, $\ldots$, S_k, S_{k+1}, $\ldots$, S_{k+l}, respectively. Then there exists $i \in [1,k]$, such that $\alpha_{k+i} \in \alpha_i\ [h(p,n)]$ and $\alpha_{k+j} = \alpha_j$ for all $j \in [1, i-1]$.*

Proof. By Theorem 4.2, we conclude the existence of an i such that $\alpha_{k+i} \prec \alpha_i$. It is sufficient to show $\alpha_{k+i} \in \alpha_i\ [h(p,n)]$. We proceed by case-distinction: CASE $i = 1$. By definition $\mathrm{C}(\sigma)$ equals the number of substitutions included in $(S_1, \ldots, S_k)$. Hence the position of S_{k+1} equals $a + \mathrm{C}(\sigma)$ which equals p. Applying Theorem 5.1, we obtain $\alpha_{k+1} \in \alpha_1[h(p,n)]$.

CASE $i > 1$. Let S_i, S_{k+i} denote the designated substitutions of the two m-sequences. It follows from Lemma 4.3 that the evaluation for terms $f_l(\overline{s})$, $l = 1, \ldots, q$ is equal for all pairs (S_j, S_{k+j}), $1 \leq j < i$. Hence, if $A(t, \overline{s}) \supset A(f_p(\overline{s}), \overline{s})$ be the designated critical axiom of S_i and S_{k+i}, then the value $|t|$ of t under S_{i-1} (and more importantly with respect to S_{k+i-1}) is bounded by $g^{a+i}(n)$, and hence the second component of the index of S_{k+i} is less than $h(p,n)$. Applying similar reasoning as in Theorem 5.1 the result follows. □

We make use of a *parameterised Hardy function*:

$$\mathrm{H}[g]_0(n) := n \qquad \mathrm{H}[g]_\alpha(n) := \mathrm{H}[g]_{P_n(\alpha)}(g(n))\ .$$

Note that if $g(n) \leq \mathrm{H}_\alpha(n)$, for some $\alpha \prec \epsilon_0$, then $\mathrm{H}[g]_\beta(n) \leq \mathrm{H}_{\alpha \cdot \beta}(n)$. (This follows by an easy induction on β.) Below we make use of the parameterised Hardy functions only with respect to the specific function $h(a,a)$.

Theorem 5.3 *Let $(S_1, \ldots, S_k)$, $(S_{k+1}, \ldots, S_{k+l})$ be consecutive m-sequences, defined as above. For $s \in [1,m]$, let $(\alpha_1, \ldots, \alpha_r)$ and $(\alpha_{r+1}, \ldots, \alpha_{r+z})$ denote the indices of the s-sequences included. Then there exists a $t \in [1,r]$ such that $\alpha_{r+t} \in \alpha_t\ [\mathrm{H}[h]^s_{\alpha_t}(p+n)]$ and $\alpha_{r+j} = \alpha_j$ for all $j \in [1, t-1]$.*

Proof. For brevity, we write H_α instead of $\mathrm{H}[h]_\alpha$. Using Theorem 4.3 we conclude, for any s, the existence of a t such that $\alpha_{r+t} \prec \alpha_t$. It suffices to show

$\alpha_{r+t} \in \alpha_t\ [\mathrm{H}^s_{\alpha_t}(p+n)]$. The Theorem is proven by simultaneous induction on s; $s \leq m$ together with the following claim:

Claim 1 *Let $(T_1,\dots,T_p)$, $(T_{p+1},\dots,T_{p+q})$ be two consecutive s-sequences, such that the characteristic number of T_{p+1} equals s. Assume λ (μ) denotes the ordinal coding the first (second) s-sequence. Then $a+\mathrm{C}(\lambda)+\mathrm{C}(\mu)+n \leq \mathrm{H}^s_\lambda(a+\mathrm{C}(\lambda)+n)$.*

Base. By Theorem 5.2, we conclude, for some $t \in [1,r]$: $\alpha_{r+t} \in \alpha_t\ [h(p,n)]$ and $\alpha_{r+j} = \alpha_j$ for all $j \in [1,t-1]$. This entails $\alpha_{r+t} \in \alpha_t\ [\mathrm{H}_{\alpha_t}(p+n)]$ as $\alpha_t \neq 0$ and $h(p,n) \leq h(p+n,p+n) = \mathrm{H}_1(p+n) \leq \mathrm{H}_{\alpha_t}(p+n)$. Now consider the claim with respect to $s=1$. Let T_1, T_2 denote two consecutive 1-sequences, with indices λ, μ, respectively. By definition $\mathrm{C}(\lambda)=\mathrm{C}(\mu)=1$. We can apply the theorem for $s=m=1$ to the pair (T_1,T_2) to conclude $\mu \in \lambda\ [\mathrm{H}_\lambda(a+\mathrm{C}(\lambda)+n)]$; therefore $\lambda \neq 0$. Hence $a+\mathrm{C}(\lambda)+\mathrm{C}(\mu)+n \leq h(a+\mathrm{C}(\lambda)+n,n) \leq \mathrm{H}_\lambda(a+\mathrm{C}(\lambda)+n)$.

Step. Let $(\alpha_1,\dots,\alpha_r)$, $(\alpha_{r+1},\dots,\alpha_{r+z})$ denote the indices of the $(s+1)$-sequences such that α_t and $\alpha_{(r+t)}$ code the $(s+1)$-sequences that include the designated substitutions S_k, S_{k+i}. Let $\alpha_r = \omega^{\gamma_1}+\cdots+\omega^{\gamma_u}$ and $\alpha_{r+t} = \omega^{\delta_1}+\cdots+\omega^{\delta_w}$. By induction hypothesis (IH) for s, there exists $v \in [1,w]$ s.t. $\delta_v \in \gamma_v\ [\mathrm{H}^s_{\gamma_v}(p+n)]$. We show

$$\delta_v,\dots,\delta_w \in \gamma_v\ [\mathrm{H}^{s+1}_{\alpha_t}(p+n)]\ . \tag{13}$$

Assume (13) and set $z := \mathrm{H}^{s+1}_{\alpha_t}(p+n)$. Using Lemma 3.2 we conclude that $\omega^{\delta_v}+\cdots+\omega^{\delta_w} \in \omega^{\gamma_v}\ [z]$. Using Lemma 3.2 again we obtain

$$\begin{aligned}\alpha_{r+t} &= \omega^{\delta_1}+\cdots+\omega^{\delta_v}+\cdots+\omega^{\delta_w}\\ &\in \omega^{\gamma_1}+\cdots+\omega^{\gamma_v}\ [z]\\ &\subseteq \omega^{\gamma_1}+\cdots+\omega^{\gamma_u}\ [z] = \alpha_t\ [z]\ .\end{aligned}$$

To show (13), we assume that $v < w$; otherwise it holds trivially. Let $a^{(v+j)}$ denote the position of the first substitution in the s-sequence coded by $\delta_{(v+j)}$, for $j \in [0,w-v]$. Repeated application of the theorem for $m=s$ with respect to the pairs (δ_v,δ_{v+1}), $(\delta_{v+1},\delta_{v+2})$, …, (δ_{w-1},δ_w) yields:

$$\begin{gathered}\delta_w \in \delta_{w-1}\ [\mathrm{H}^s_{\delta_{w-1}}(a^{(w)}+n)]\ ,\\ \vdots\\ \delta_{v+1} \in \delta_v\ [\mathrm{H}^s_{\delta_v}(a^{(v+1)}+n)]\ .\end{gathered}$$

Let $j \in [1,w-v]$ and consider $(\delta_{v+j},\delta_{v+j-1})$. Set $b := a+\mathrm{C}(\alpha_1)+\cdots+\mathrm{C}(\alpha_r)+\mathrm{C}(\alpha_{r+1})+\cdots+\mathrm{C}(\alpha_{r+t-1})+\mathrm{C}(\delta_1)+\cdots+\mathrm{C}(\delta_{v-1})$. By application of IH on Claim 1 for s-sequences we have for all $j \in [0,w-v-2]$:

$$a^{(v+j+2)}+n \leq \mathrm{H}^s_{\delta_{v+j}}(a^{(v+j+1)}+n)\ .$$

Repeated application of this inequality for $j \in [0, w-v-2]$ yields:

$$\mathrm{H}^s_{\delta_{w-1}}(a^{(w)} + n) \leq \mathrm{H}^s_{\delta_{w-1}}(\cdots(\mathrm{H}^s_{\delta_v}(b + \mathrm{C}(\delta_v) + n))\cdots) .$$

Hence, we obtain for all $j \in [0, w-v-1]$:

$$\delta_{v+j+1} \in \delta_{v+j} \, [\mathrm{H}^s_{\delta_{v+j}}(\cdots(\mathrm{H}^s_{\delta_v}(b + \mathrm{C}(\delta_v) + n))\cdots)] .$$

Using Lemma 3.4, Lemma 3.5 and $s + 1 \leq q + 1 \leq h(0, 0)$:

$$\begin{aligned}
\mathrm{H}^s_{\delta_{w-1}}(\cdots(\mathrm{H}^s_{\delta_v}(b + \mathrm{C}(\delta_v) + n))\cdots) &< \mathrm{H}^s_{\omega^{\delta_{(w-1)}}}(\cdots(\mathrm{H}^s_{\omega^{\delta_v}}(b + \mathrm{C}(\delta_v) + n))\cdots) \\
&\leq \mathrm{H}_{\omega^{\delta_{(w-1)}+1}}(\cdots(\mathrm{H}^s_{\omega^{\delta_v}}(b + \mathrm{C}(\delta_v) + n))\cdots) \\
&\leq \mathrm{H}^{s+1}_{\omega^{\delta_{(w-2)}}}(\cdots(\mathrm{H}^s_{\omega^{\delta_v}}(b + \mathrm{C}(\delta_v) + n))\cdots) \\
&\leq \mathrm{H}^{s+1}_{\omega^{\delta_v}}(b + \mathrm{C}(\delta_v) + n) .
\end{aligned}$$

Employing $\delta_v \in \gamma_v \, [\mathrm{H}^s_{\gamma_v}(a + \mathrm{C}(\sigma) + n)]$, together with $c + \mathrm{C}(\alpha) \leq \mathrm{H}_\alpha(c)$ for $\alpha \neq 0$ and arbitrary c, and $b + n \leq 2a + n \leq h(a, n)$, we obtain:

$$\begin{aligned}
\mathrm{H}^{s+1}_{\omega^{\delta_v}}(b + \mathrm{C}(\delta_v) + n) &\leq \mathrm{H}^{s+2}_{\omega^{\delta_v}}(b + n) \leq \mathrm{H}^{s+2}_{\omega^{\delta_v}}(h(a + \mathrm{C}(\sigma), n)) \\
&\leq \mathrm{H}_{\omega^{\delta_v+1}}(h(a + \mathrm{C}(\sigma), n)) \\
&\leq \mathrm{H}_{\omega^{\delta_v+1}}(\mathrm{H}^s_{\omega^{\gamma_v}}(a + \mathrm{C}(\sigma) + n)) \\
&\leq \mathrm{H}^{s+1}_{\omega^{\gamma_v}}(a + \mathrm{C}(\sigma) + n) \\
&\leq \mathrm{H}^{s+1}_{\alpha_t}(p + n) .
\end{aligned}$$

On the other hand, we have:

$$\mathrm{H}^s_{\delta_v}(a + \mathrm{C}(\sigma) + n) \leq \mathrm{H}^{s+1}_{\omega^{\gamma_v}}(p + n) \leq \mathrm{H}^{s+1}_{\alpha_t}(p + n) .$$

This completes the proof of (13). The step case of Claim 1 follows by a generalisation of the base case, exploiting essentially the same sequence of inequalities as in the step case for the Theorem. □

The maximal sequence of substitutions is a $(q + 1)$-sequence. Suppose $\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_r}$ codes this sequence. From the proof of Theorem 5.3 we obtain:

$$\mathrm{C}(\alpha_1) + \cdots + \mathrm{C}(\alpha_r) \leq \mathrm{H}[h]_{\omega^{\alpha_1+1}}(n) .$$

This suffices to bound the value of a substitution instance for a defined function symbol f_i elementary in $\mathrm{H}_{\omega^{\alpha_1+1}}(n)$. To estimate α_1 we set

$$\overline{\omega}_m := \exp^{m-1}_\omega(\omega \cdot (2^e + 1)) .$$

(Recall that e denotes the number of terms $f_j(\overline{s})$ in $\mathcal{C}$.)

Lemma 5.1 *Suppose α codes an m-sequence $S_1, \ldots, S_k$. Let p denote the position of S_k in the maximal sequence R. Then $\alpha \in \overline{\omega}_m \, [\mathrm{H}^m_{\overline{\omega}_m}(p + n)]$.*

Proof. By induction on m using Theorem 5.1 and Theorem 5.3. $\square$

Theorem 5.4 *Let $(n_1, \dots, n_k)$ be an arbitrary tuple of natural numbers and $n = \max\{n_1, \dots, n_k\}$. Let $T(n_1, \dots, n_k) \in \mathcal{S}$ be a closed tautology of the form (4) represented as*

$$A_1 \wedge \cdots \wedge A_m \wedge B_1 \wedge \cdots \wedge B_n \supset F(f_1, \dots, f_q) \ ,$$

containing defined function symbols $f_1, \dots, f_q$ only. Define

$$\gamma = \begin{cases} \omega^\omega & \text{if } q = 1 \\ \omega_{q-1}(\omega^2) & \text{otherwise} \ . \end{cases}$$

Then there exists a quantifier-free formula $F^\star$, free of defined function symbols which is true in $\mathcal{N}$ such that the function ϕ_i substituted for f_i is elementary in $\mathrm{H}_\gamma(\max\{d, n\})$, where d depends on T only.

Proof. It suffices to show that each ϕ_i is elementary in $\mathrm{H}_\gamma(\max\{d, n\})$, where d depends on T only. During the proof we give sufficient criteria to fix this constant. We need some new ideas to establish the stated bound. We assume $q > 1$; the case $q = 1$ is similar, but simpler. By Theorem 5.3 we have for all $i \in [1, r-1]$:

$$\alpha_{i+1} \in \alpha_i \ [\mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{C}(\alpha_1) + n)] \subseteq \alpha_1 \ [\mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{C}(\alpha_1) + n)] \ .$$

The first goal is to find a suitable bound for $\mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{C}(\alpha_1) + n)$.

$$\begin{aligned} \mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{C}(\alpha_1) + n) &\leq \mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{H}[h]_{\alpha_1}(n)) \\ &\leq \mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{H}[h]_{\alpha_1}(\mathrm{H}[h]^{q}_{\overline{\omega}_q}(n))) \end{aligned}$$

By Lemma 5.1 this yields

$$\begin{aligned} \mathrm{H}[h]^{q \cdot i}_{\alpha_1}(\mathrm{C}(\alpha_1) + n) &\leq \mathrm{H}[h]^{q \cdot i}_{\overline{\omega}_q}(\mathrm{H}[h]_{\overline{\omega}_q}(\mathrm{H}[h]^{q}_{\overline{\omega}_q}(n))) \\ &\leq \mathrm{H}[h]^{q \cdot (i+2)}_{\overline{\omega}_q}(n) \ . \end{aligned}$$

We estimate $\mathrm{H}[h]^{q}_{\overline{\omega}_q}(n)$: As h is primitive recursive, $h(n, n) \leq \mathrm{H}_{\omega^l}(\max\{d, n\})$ for some numbers l and d. (Essentially $l = 3$ suffices, if we make sure that d is greater than e,q and the maximal depth of terms in T.) Using $q > 1$ and $d \geq l, q$, we see $h(n, n) \leq \mathrm{H}_{\overline{\omega}_q}(\max\{d, n\})$. We obtain:

$$\begin{aligned} \mathrm{H}[h]^{q}_{\overline{\omega}_q}(\max\{d, n\}) &\leq \mathrm{H}^{q}_{\overline{\omega}_q \overline{\omega}_q}(\max\{d, n\}) \\ &\leq \mathrm{H}_{\overline{\omega}_q^2 \omega}(\max\{d, n\}) \\ &\leq \mathrm{H}_{\overline{\omega}_q^3}(\max\{d, n\}) \ . \end{aligned}$$

For the second inequality we employ $\omega \in \overline{\omega}_q[\max\{d, n\}]$.

We set $\delta := \overline{\omega}_q^3$ and obtain $\mathrm{H}[h]^q_{\overline{\omega}_q}(n) \leq \mathrm{H}_\delta(\max\{d,n\})$, which implies $\alpha_1 \in \overline{\omega}_q\ [\mathrm{H}_\delta(\max\{d,n\})]$. Further, we obtain for each $i \in [1, r-1]$:

$$\mathrm{H}[h]^{q\cdot i}_{\alpha_1}(\mathrm{C}(\alpha_1)+n) \leq \mathrm{H}^{i+2}_\delta(\max\{d,n\}) \ . \tag{14}$$

We establish an upper bound for r, using the following lemma.

Lemma 5.2 *Suppose $f(n) \geq n+1$. Let μ_x denote the least number operator. Then*

$$\mathrm{H}[f]_\alpha(n) \geq \mu_k(P_{f^k(n)}P_{f^{k-1}(n)}\cdots P_n(\alpha)=0) \ .$$

Proof. One proves $\mathrm{H}[f]_\alpha(n) - n \geq \mu_k(P_{f^k(n)}P_{f^{k-1}(n)}\cdots P_n(\alpha)=0)$ by induction on α. □

By the above lemma and (14), we obtain:

$$\begin{aligned} r &\leq \mu_k(P_{\mathrm{H}^{k+2}_\delta(\max\{d,n\})}\cdots P_{\mathrm{H}^2_\delta(\max\{d,n\})}(\alpha_1)=0) \\ &\leq \mathrm{H}[\mathrm{H}_\delta]_{\alpha_1}(\mathrm{H}^2_\delta(\max\{d,n\})) \ . \end{aligned}$$

Furthermore

$$\begin{aligned} \mathrm{H}[\mathrm{H}_\delta]_{\alpha_1}(\mathrm{H}^2_\delta(\max\{d,n\})) = \mathrm{H}_{\delta\alpha_1}(\mathrm{H}^2_\delta(\max\{d,n\})) &\leq \mathrm{H}_{\delta\overline{\omega}_q}(\mathrm{H}^2_\delta(\max\{d,n\})) \\ &\leq \mathrm{H}_{\overline{\omega}_q^4+\overline{\omega}_q^3\omega}(\max\{d,n\}) \ . \end{aligned}$$

Summing up, we set $d \geq (2^e+1)^4$ and observe

$$\begin{aligned} \mathrm{C}(\alpha_1)+\cdots+\mathrm{C}(\alpha_r) &\leq \mathrm{H}[h]^{q(r-1)}_{\alpha_1}(\mathrm{C}(\alpha_1)+n) \\ &\leq \mathrm{H}^{r+1}_\delta(\max\{d,n\}) \\ &\leq \mathrm{H}_{\delta\omega}\mathrm{H}_{\overline{\omega}_q^4+\overline{\omega}_q^2\omega}(\max\{d,n\}) \\ &\leq \mathrm{H}_{\overline{\omega}_q^4+\overline{\omega}_q^4+\overline{\omega}_q^3\omega}(\max\{d,n\}) \\ &\leq \mathrm{H}_{\omega_q(\omega^2)}(\max\{d,n\}) = \mathrm{H}_\gamma(\max\{d,n\}) \ . \end{aligned}$$

Hence, the complexity of the Substitution Method is bounded by H_γ. We conclude, by similar considerations, that the value of a substitution instance for any defined function symbol is bounded by

$$\mathrm{H}_{\omega_{q-1}(\omega^2)}(\max\{d,n\}) \ .$$

Finally we set $w := \mathrm{H}_\gamma(\max\{d,n\})$. By definition of the substitution method, we obtain

$$\phi_i(n_1,\ldots,n_l) = \mu_{x\leq w}A(n_1,\ldots,n_l,x) \quad ,$$

for some elementary relation A. As bounded minimisation is elementary, ϕ_i is elementary in H_γ. □

Theorem 5.4 solves the problem ($\star$) posed in Section 1. It is easy to see that the employed machinery can be used also for a 'weaker' set of tautologies. We define a strict subset $\mathcal{S}' \subset \mathcal{S}$ in a similar fashion as the set of tautologies $\mathcal{S}$. However no reverence is made to a critical axiom of 2nd kind. This change allows us to alter the definition of substitution step.

The initial substitution S_0 assigns to all function symbols $f_1, \ldots, f_q$ the constant function 0. Suppose i substitutions have already be constructed. Let the critical axioms in $\mathcal{C}$ be ordered in some arbitrary way. The first critical axiom

$$A(t, \overline{s}) \supset A(f_p(\overline{s}), \overline{s}) \ ,$$

having truth value false is picked. Suppose $t \hookrightarrow_{G_i} z$, hence $A(z, \overline{s})$ is true in $\mathcal{N}$. The definition of the function ψ replacing the old instantiation ϕ for f_p becomes

$$\psi(m_1, \ldots, m_l) = \begin{cases} \phi(m_1, \ldots, m_l) & m_1, \ldots, m_l \neq n_1, \ldots, n_l \ , \\ z & m_1, \ldots, m_l = n_1, \ldots, n_l \ , \end{cases}$$

where $\overline{s} \hookrightarrow_{G_i} \overline{n}$.

The whole purpose of the index with respect to the sequence of formulas (6) is to control the respective part in the definition of substitution. Hence this index is not necessary, as no critical axioms of 2nd kind are present. This implies that the ordinal assigned to an arbitrary substitution is a natural number less than 2^e, where e is the maximum number of terms $f_i(s_1, \ldots, s_l)$ in $\mathcal{C}$. Based on this observation we can change the appropriate definitions and prove the key theorems for the restriction set of tautologies $\mathcal{S}'$.

Theorem 5.5 *Let $T(n_1, \ldots, n_k) \in \mathcal{S}'$ be a closed tautology of the form*

$$A_1 \wedge \cdots \wedge A_m \wedge B_1 \wedge \cdots \wedge B_n \supset F(f_1, \ldots, f_q) \ ,$$

containing defined function symbols $f_1, \ldots, f_q$.

Then there exists a quantifier-free formula $F^\star$, free of defined function symbols true in $\mathcal{N}$ such that the functions ϕ_i substituted for f_i are elementary in $J(g, \mathrm{G}_\gamma(1))(n)$, $\gamma < \epsilon_0$ and $n = \max\{n_1, \ldots, n_k\}$.

6 Peano Arithmetic coached in the ε-calculus

In this section the formal system $\mathsf{PA}(\varepsilon)$ is defined. The formalisation is chosen in such a form that the results of Section 4 and Section 5 can immediately be applied for $\mathsf{PA}(\varepsilon)$. In Section 7 we give an embedding of PA, into $\mathsf{PA}(\varepsilon)$. Our formalisation of Hilbert's ε-calculus and thus the axiomatisation of number theory is based on a Tait-style calculus.

Hilbert's ε-calculus centres around an extension of the basic first-order language $\mathcal{L}$ by the ε-symbol. We extend the definition of terms to include ε-terms. The extended language is called $\mathcal{L}(\varepsilon)$.

If $A(a)$ is a formula, not containing the bounded variable x, then the ε-term $\epsilon_x A(x)$ is a term. If on the other hand x does occur at positions $p_1, \ldots, p_k$ in $A(a)$, we obtain a *variant* A' by replacing x at p_i for all $i \in [1, k]$ by some other distinct bound variable y not already occurring in A. The variant A' is then used to form the ε-term $\epsilon_x A'(x)$. If $\epsilon_y A(y)$ is obtained from the expression $\epsilon_x A(x)$ by changing bound variables, as just described, then we call this change *admissible*. Two expressions are called *congruent* if one can be obtained from the other by a sequence of admissible changes of bound variables. Congruent expressions are considered to be equal.

A term $\epsilon_x A(x)$ is an *ε-matrix*—or simply a *matrix*—if all terms occurring in A are free variables each of which occurs exactly once. Clearly no expression in $A(x)$ containing x can be a term. We denote ε-matrices as $\epsilon_x A(x; a_1, \ldots, a_k)$ with the understanding that only the variables $a_1, \ldots, a_k$ occur and these are fully indicated. ε-matrices that differ only in the indicated tuples of variables are considered to be equal. Let E be some expression; a matrix $\epsilon_x A(x; a_1, \ldots, a_k)$ is said to *occur in E* if there exists a list of terms or semi-terms $s_1, \ldots, s_k$ such that $\epsilon_x A(x; s_1, \ldots, s_k)$ occurs in E. The *rank* of a matrix e (written $\mathrm{rank}(e)$) is defined inductively: If no matrix occurs inside e then $\mathrm{rank}(e) := 1$. Assume we already assigned ranks $r_1, \ldots, r_l$ to the l matrices occurring in e. Then $\mathrm{rank}(e) := \max\{r_1, \ldots, r_l\} + 1$.

Corresponding to each term $\epsilon_x A(x)$ there exists a unique matrix e: The matrix e is obtained by first replacing all maximal subterms occurring in $\epsilon_x A(x)$ by new free variables. In this newly obtained term we replace distinct occurrences of the same variable by different variables. The *rank of an ε-term*, written as $\mathrm{rank}(\epsilon_x A(x))$, is the rank of its matrix.

Example 6.1 *Suppose f, g denote binary function symbols; $a, b, x, y \in \mathcal{V}$. The rank of the ε-terms $\epsilon_x\{\epsilon_y(f(x,y) = \epsilon_z(g(x,z) = a)) = b\}$ and $\epsilon_x\{\epsilon_y(f(x,y) = \epsilon_z(g(y,z) = a)) = b\}$ is 2 and 3, respectively. The given ϵ-terms constitute their one ϵ-matrices.*

Note that the rank of $\epsilon_x A(x)$ can be lower than the rank of one of its subterms, i.e., the term depth of an ϵ-term is not necessary a bound for the rank, see [3, 4, 20] for further examples.

Based on the language $\mathcal{L}(\varepsilon)$, we define $\mathsf{PA}(\varepsilon)$ as a Tait-style sequent calculus.

A *sequent* is a line of the form

$$\vdash A_1, \dots, A_n \ ,$$

where each A_i is a formula. We conceive the line $A_1, \dots, A_n$ as a set of formulas. The *logical axioms* of $\mathsf{PA}(\varepsilon)$ have the form $\vdash \neg A, A$ and

$$\vdash \neg A(t), A(\epsilon_x A(x)) \ , \tag{15}$$

where t is an arbitrary term (over $\mathcal{L}(\varepsilon)$). The *identity axioms* are defined by suitable reformulation of the identity axioms in Table 2, together with instances of the following axiom of ε-identity:

$$\vdash b \neq c, \epsilon_x A(x; a_1, \dots, b, \dots, a_l) = \epsilon_x A(x; a_1, \dots, c, \dots, a_l) \ , \tag{16}$$

where $\epsilon_x A(x; a_1, \dots, a_l)$ denotes a representative of an ε-matrix of arity l. The *logical rules* and *structural rules* of $\mathsf{PA}(\varepsilon)$ are Tait-style formulations of the usual rules of the propositional fragment of predicate logic, see e.g. [21]. As non-logical axioms we employ (sequent reformulations of) the weak arithmetical axioms of Table 1 together with an axiom of *induction*. To formalise induction, the non-logical axiom

$$\vdash \neg A(t), \epsilon_x A(x) \leq t \qquad (\mathrm{Min}) \ , \tag{17}$$

is included, where A is an arbitrary formula in $\mathcal{L}(\varepsilon)$. This completes the definition of $\mathsf{PA}(\varepsilon)$. Within $\mathsf{PA}(\varepsilon)$ quantifiers become definable: $\exists x A(x) :\Leftrightarrow A(\epsilon_x A(x))$ and $\forall x A(x) :\Leftrightarrow A(\epsilon_x \neg A(x))$, compare [20].

Let Π be a derivation in $\mathsf{PA}(\varepsilon)$ of $\vdash A$ and suppose $e_1, \dots, e_q$ denote the ε-matrices of the ε-terms occurring in Π; let this sequence be fixed. The set of critical axioms $\mathcal{C}$ includes all *critical axioms* of the form (15) and (17). (We have already seen in Section 4 that the axioms of ε-identity need not be considered.) It is easy to see that the set of critical axioms $\mathcal{C}$ defined for a given proof in $\mathsf{PA}(\varepsilon)$ is a specialisation of the set of critical axioms of the system $\mathcal{S}$. Moreover it is clear that any proof Π in $\mathsf{PA}(\varepsilon)$, yields a tautology T which has the form studied in Section 4 and Section 5. The role played by the defined function symbols $f_1, \dots, f_q$ is taken up by the ε-matrices $e_1, \dots, e_q$.

Definition 6.1 *We assume the following order on the $e_1, \dots, e_q$. Matrices of lower rank precede those of higher rank. It follows that e_j cannot occur in e_i for $i < j$. We make the additional assumption that if e_j is contained in the sequence, all matrices occurring in e_j are included in the sequence as well.*

It is easy to see that this order meets the technical assumption employed above on the order of the defined symbols $f_1, \dots, f_q$.

A function f is provably recursive in $\mathsf{PA}(\varepsilon)$, if there exists a primitive recursive predicate P and a primitive recursion function g such that $\mathsf{PA}(\varepsilon) \vdash$

$\forall y_1 \cdots \forall y_k \exists x P(y_1, \ldots, y_k, x)$ and f satisfies

$$f(n_1, \ldots, n_k) = g(\mu_x P(n_1, \ldots, n_k, x)) \ ,$$

where μ_x denotes the least number operator. For each $\alpha \prec \varepsilon_0$, let the Hardy class $\mathcal{H}$ be the smallest class of functions containing 0, S, all H_α, all projection functions $I_{n,i}(a_1, \ldots, a_n) = a_i$, and closed under primitive recursion and composition.

Corollary 6.1 *$\mathcal{H}$ is the class of all provably recursive functions in* $\mathsf{PA}(\varepsilon)$.

Proof. We will not give a full proof but restrict our attention to show that the class of provably recursive functions of $\mathsf{PA}(\varepsilon)$ is contained in $\mathcal{H}$. The other inclusion follows by the standard argumentation, cf. [8], employing the embedding of PA into $\mathsf{PA}(\varepsilon)$, shown in the next section. Making use of Theorem 5.4 we obtain a characterisation of the provably recursive functions in $\mathsf{PA}(\varepsilon)$. Let f be a function provably recursive in $\mathsf{PA}(\varepsilon)$ with proof Π. Then we can characterise f constructively. In the notations of Theorem 5.4.

$$f(n_1, \ldots, n_k) = \mu_{x \leq H(n_1, \ldots, n_k)} P(n_1, \ldots, n_k, x) \ ,$$

where $H(a_1, \ldots, a_k)$ abbreviates $\mathrm{H}_\gamma(\max\{d, a_1, \ldots, a_k\})$, where $\gamma < \epsilon_0$ and d depends on Π only. $\square$

7 Embedding Peano Arithmetic into $\mathsf{PA}(\varepsilon)$

We formalise PA in the form of a Tait-style sequent calculus. The language of PA is denoted as $\mathcal{L}(\mathsf{PA})$. The *logical axioms* of PA have the form $\vdash \neg A, A$. The *identity axioms* are given through a reformulation of the axioms in Table 2, while the *logical rules* and *structural rules* of PA are the usual rules of predicate logic, formulated in a Tait-style calculus, cf. [21].

This completes the definition of the logical system. To formalise Peano Arithmetic completely, it suffices to add induction, and sequent formulations of the weak arithmetical axioms in Table 1. Instead of the usual mathematical induction principle we include an equivalent principle of *order induction*.

$$\frac{\vdash \Gamma, \neg \forall y (y < a \supset A(y)), A(a)}{\vdash \Gamma, A(t)} \quad (\mathrm{Ind}) \ ,$$

where $a \in \mathcal{V}$ does not occur free in Γ and t is an arbitrary term. It remains to establish the embedding of usual PA into $\mathsf{PA}(\varepsilon)$. For any formula A in $\mathcal{L}(\mathsf{PA})$, we define a formula A^+ in $\mathcal{L}(\varepsilon)$:

$$\begin{aligned} A^+ &:= A \quad \text{if } A \text{ is an atomic formula} , \\ (A \odot B)^+ &:= A^+ \odot B^+ \quad \text{for } \odot \in \{\wedge, \vee\} , \\ (\exists x\, A(x))^+ &:= A^+(\epsilon_x A^+(x)] , \\ (\forall x\, A(x))^+ &:= A^+(\epsilon_x \neg A^+(x)) . \end{aligned}$$

Using the translation A^+ we are able to show

Theorem 7.1 *(1) If* PA $\vdash A$*, then* PA$(\varepsilon) \vdash A^+$
(2) If PA $\vdash A$*, such that A is a closed formula, then there exists a* PA(ε)*-derivation Π^+ of A^+ such that $var(\Pi^+) = \emptyset$.*

Proof. See [9] for a proof. □

Finally we obtain the following result as a corollary of Theorem 7.1 and Corollary 6.1. This theorem has first been proved in [22], see also [8].

Corollary 7.1 *$\mathcal{H}$ is the class of all provably recursive functions in* PA*.*

8 Conclusion and Further Work

Through the gained direct characterisation of the class of provably recursive functions of PA(ε), we can extract the content of proofs of purely existential formulas. Let $\exists\overline{x}A(\overline{c},\overline{x})$ be a closed Σ_1-formula. Suppose PA(ε) proves $\exists\overline{x}A(\overline{c},\overline{x}))^+$ with a derivation Π. The results of Section 5 allow us to pin-down, depending on information gathered from Π, numbers $n_1,\dots,n_l$ such that $A(\overline{c},\overline{n})$ is true in the standard-model $\mathcal{N}$.

The difference from usual Gentzen-style proof theory is that we need not consider the whole proof Π. It suffices to consider the set of critical axioms $\mathcal{C}$ occurring in Π. Following Ackermann's approach it seems natural to count the number of employed ε-matrices to measure the *length* of the proof Π. However, a close look at the results of Sections 4 and 5 shows that we can employ the following definition. We write $\Pi \vdash A$ to denote derivability of A (with a proof Π) in PA(ε).

Definition 8.1 *The* length *of Π such that $\Pi \vdash A$ is defined as the maximal rank of ε-matrices r in Π. We write $\Pi \vdash_r A$.*

This becomes possible, if we suitably change the definition of the *characteristic number*:

Definition 8.2 *Let S be a substitution different from the initial one, and let r denote the maximal rank of an ϵ-matrix occurring in $\mathcal{C}$. Suppose l is maximal such that $l = rank(e_i)$ and e_i denotes an ϵ-matrix that is assigned a function different from the constant function* 0 *under S. Then the* characteristic number *of S is $r + 1 - l$. In the case where S denotes the initial substitution its characteristic number is defined as $r + 1$.*

Although the definition of a characteristic number is central, all results of Sections 4 and 5 remain valid, when reformulated appropriately. We say a formula $A \in \mathcal{L}(\varepsilon)$ *is true at n*, if there exists an ε-substitution instance $A^\star$ of A such that all substitution instances of ε-terms occurring in A are bounded by n. In summary we obtain the following proposition.

Proposition 8.1 (Bounding Lemma) *Let $\exists\overline{x}A(\overline{c},\overline{x})$ be a closed Σ_1-formula. Suppose $\Pi \vdash_r (\exists\overline{x}A(\overline{c},\overline{x}))^+$. Then we have $(\exists\overline{x}A(\overline{c},\overline{x}))^+$ is true at $\mathrm{H}_\gamma(n)$, for n large enough, where*

$$\gamma = \begin{cases} \omega^\omega & \textit{if } r = 1 \\ \omega_{r-1}(\omega^2) & \textit{otherwise} . \end{cases}$$

An open problem is to relate our characterisation result of the provably recursive functions to the one obtained by Tait in [17, 9] and to Avigad [10]. As already mentioned the substitution method has recently received renewed attention. In particular, in [12] Arai observed a specific feature of Ackermann's proof. The construction used to prove the 1-consistency of $\mathsf{PA}(\varepsilon)$ can be employed to define an ordinal notation system. It turns out that this notation system has been reinvented much later by K. Schütte and S. Simpson for an investigation on independence results [23]. This is of interest as the latter can be shown to be equivalent to the algebraically motivated notation system introduced by Beklemishev [24].

Acknowledgements This paper grew out of a master project at the University of Leeds and I cordially thank Stan Wainer for his guidance during my time in Leeds. Moreover I would like to thank Toshiyasu Arai and Grigori Mints for comments on an earlier draft of this paper and useful discussions.

References

[1] G. Kreisel, Interpretation of non-finitist proofs I,II, J. Symbolic Logic 16,17 (1952) 241–267,43–58.

[2] S. S. Wainer, Ordinal Recursion, and a refinement of the extended Grzegorczyk hierarchy, J. Symbolic Logic (1972) 281–292.

[3] W. Ackermann, Zur Widerspruchsfreiheit der Zahlentheorie, Math. Annalen 117 (1940) 162–194.
[4] D. Hilbert, P. Bernays, Grundlagen der Mathematik II, Springer Verlag, Second Edition, 1970.
[5] A. Leisenring, Mathematical Logic and Hilbert's ϵ-symbol, MacDonald Technical and Scientific, London, 1969.
[6] J. Avigad, R. Zach, The Epsilon Calculus, in: E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Summer 2002 Edition), 2002, `http://plato.stanford.edu/archives/sum2002/entries/epsilon-calculus/`.
[7] G. Gentzen, Neue Fassung des Widerspruchsfreiheitsbeweises für die reine Zahlentheorie, Forschungen zur Logik und zur Grundlegung der exakten Wissenschaften 4.
[8] G. Takeuti, Proof Theory, 2nd Edition, North-Holland, Amsterdam, 1987.
[9] W. W. Tait, The Substitution Method, J. Symbolic Logic 30 (2) (1965) 175–192.
[10] J. Avigad, Update procedures and the 1-consistency of arithmetic, Math. Logic Quarterly 48 (2002) 3–13.
[11] M. Fairtlough, S. S. Wainer, Hierarchies of provably recursive functions, in: S. R. Buss (Ed.), Handbook of Proof Theory, Elsevier Science, 1998, pp. 149–207.
[12] T. Arai, Epsilon substitution method for theories of jump hierarchies, Archive for Mathematical Logic 41 (2002) 123–153.
[13] T. Arai, Epsilon substitution method for $ID_1(\Pi^0_1 \vee \Sigma^0_1)$, Annals of Pure and Applied Logic (2003) 163–208.
[14] W. Buchholz, G. Mints, S. Tupailo, Epsilon substitution method for elementary analysis, Archive for Mathematical Logic 35(2) (1996) 103–130.
[15] G. Mints, Hilbert's substitution method and Gentzen-type systems, in: Proc. of 9^{th} Int. Congress of Logic, Method. and Philos. of Sci., Uppsala, Sweden, 1994.
[16] G. Mints, A termination proof for epsilon substitution using partial derivations, Theoretical Computer Science (2003) 187–213.
[17] W. W. Tait, Functionals defined by transfinite recursion, J. Symbolic Logic 30 (2) (1965) 155–174.
[18] J. v. Neumann, Zur Hilbertschen Beweistheorie, Math Zeitschrift (1927) 1–46.
[19] W. Buchholz, A. Cichon, A. Weiermann, A uniform approach to fundamental sequences and hierarchies, Math. Logic Quarterly 40 (1994) 273–286.
[20] G. Moser, R. Zach, The Complexity of the Epsilon theorems, Studia Logica. To appear.
[21] H. Schwichtenberg, Some applications of cut-elimination, in: J. Barwise (Ed.), Handbook of Mathematical Logic, North Holland, 5^{th} edition, 1989, pp. 867–897.
[22] S. S. Wainer, A classification of the ordinal recursive functions, Archive

for Mathematical Logic 13 (1970) 136–153.
[23] K. Schütte, S. Simpson, Ein in der reinen Zahlentheorie unbeweisbarer Satz über endliche Folgen von natürlichen Zahlen, Archive for Mathematical Logic (1985) 75–89.
[24] L. Beklemishev, Provability algebras and proof-theoretic ordinals - part I, Annals of Pure and Applied Logic 128 (2004) 103–124.