Proving consistency of equational theories in bounded arithmetic

Arnold Beckmann*
Mathematical Institute, University of Oxford
24-29 St. Giles', Oxford OX1 3LB, UK†

August 30, 2000

Abstract

We consider equational theories for functions defined via recursion involving equations between closed terms with natural rules based on recursive definitions of the function symbols. We show that consistency of such equational theories can be proved in the weak fragment of arithmetic S^1_2. In particular this solves an open problem formulated by Takeuti (c.f. [5, p.5 problem 9.])

1 Introduction

Since the introduction of bounded arithmetic it has been and still is a major open problem if bounded arithmetic is finitely axiomatizable, or, equivalently, if the hierarchy of bounded arithmetic theories S^i_2 (c.f. [2]) is proper. One of the first ideas to attack this problem which comes into one's mind is to use consistency statements as separating sentences. However, up to now only negative results have been achieved in this direction. The usual notion of consistency is too strong as $S_2 \nvdash Con_{S^{-1}_2}$, c.f. [11], where S^{-1}_2 is the induction-free fragment of bounded arithmetic S_2. Also the weaker consistency statements $BDCon$ which refer to proofs that use only bounded formulas still is too strong: S. Buss [2] proved that $S^{i+1}_2 \vdash BDCon_{S^i_2}$ holds for at most one i, and P. Pudlák showed in [9] that $S_2 \nvdash BDCon_{S^1_2}$, hence only $S_2 \vdash BDCon_{S^0_2}$ remains to be possible. The reason why usual approaches for proving consistency do not work in weak arithmetic is that it is impossible to feasibly evaluate closed terms from the language of bounded arithmetic – their values grow exponentially in their Gödel-numbers in general. This leads to the plausible conjecture raised by

*Supported by the Deutschen Akademie der Naturforscher Leopoldina grant #BMBF-LPD 9801-7 with funds from the Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie.
†email: Arnold.Beckmann@math.uni-muenster.de

G. Takeuti, c.f. [5, p.5 problem 9.]: "Let $S_2^{-\infty}$ be the equational theory involving equations $s = t$, where s, t are closed terms in the language of S_2, with natural rules based on recursive definitions of the function symbols. Show that $S_2 \nvdash Con(S_2^{-\infty})$. […]"

If this conjecture would be true then it would be likely that consistency statements cannot be used to negatively answer the finitely axiomatizability problem of bounded arithmetic. In this paper we will disprove this conjecture, thus there is hope that consistency statements can lead to a negative answer.

More generally we will consider equational theories for functions defined via recursion involving equations between closed terms with natural rules based on recursive definitions of the function symbols. The recursion can be defined very general. On the one hand it can depend on several kinds of numerals like natural numbers, binary words, or k-adic numbers (trees will not be allowed). On the other hand, in a recursive definition of a function symbol f the symbol itself may occur with unrestricted arguments (thus the recursion may not be terminating). So the axioms have the general form

$$f(\vec{x}) = t(\lambda \vec{y}.f(\vec{y}), \vec{x})$$

where t involves some previously defined function symbols. Examples of such equational theories will be given for the primitive recursive functions, the μ-recursive (or partial recursive) functions, and Cook's system PV (c.f. [6]) without the substitution and induction rule for the polynomial time computable functions, see Example 2.3. Let Ax be such a set of axioms defining the functions, then $\mathrm{EqT}(Ax)$ is the equational theory given by (closed) instances of Ax, the definition of equality as an equivalence relation, and the compatibility of function symbols with equality.

We will show that the consistency of such equational theories can be proved in the fragment S_2^1 of bounded arithmetic.

Main Theorem 1.1 *S_2^1 proves the consistency of* $\mathrm{EqT}(Ax)$*, i.e. that* $0 = 1$ *is not derivable in* $\mathrm{EqT}(Ax)$.

Remark 1.2 *Our result is quite remarkable when compared with known results about unprovability of consistency statements. In [3] it is shown that $PV \nvdash$* $\mathrm{Con}(PV^-)$*, where PV^- is related to* Cook*'s equational theory PV without induction. But one has to be careful, because on the one hand in this article we study equational theories without substitution rule only, and on the other hand the version of PV^- in [3] contains some additional axioms, i.e. finitely many equations, beside the defining equations according to the recursive definition of the function symbols.*

Acknowledgments: I would like to thank Jan Krajíček, who reminded me of the problem raised by Takeuti (c.f. [5]), and for many valuable suggestions and remarks on a first version of this article; Alex Wilkie for his hospitality during my stay at the Mathematical Institute of the University of Oxford, and for a lot of discussions and remarks; Sam Buss for many valuable suggestions and discussions leading to the final version of this article.

2 Equational theories based on recursion

A typical equational theory, which is a kind of prototype for the ones we will consider, is given by the following small example which defines a kind of exponentiation over the natural numbers.

Example 2.1 *Let* $\mathcal{F}_{\widetilde{\exp}}$ *be the set of function symbols consisting of* $0, \mathrm{S}, +, \cdot, \widetilde{\exp}$ *where* 0 *is zero-ary denoting the constant zero,* S *is unary denoting the successor function, and* $+, \cdot, \widetilde{\exp}$ *are binary denoting addition, multiplication and, respectively, a kind of exponentiation. These symbols are recursively axiomatized by the following equations forming the set* $Ax_{\widetilde{\exp}}$*:*

$$
\begin{array}{rr}
0 + x_1 = x_1 & \qquad (\mathrm{S}\,x_0) + x_1 = \mathrm{S}(x_0 + x_1) \\
0 \cdot x_1 = 0 & \qquad (\mathrm{S}\,x_0) \cdot x_1 = (x_0 \cdot x_1) + x_1 \\
\widetilde{\exp}(0, x_1) = x_1 & \qquad \widetilde{\exp}(\mathrm{S}\,x_0, x_1) = x_1 \cdot \widetilde{\exp}(x_0, x_1)
\end{array}
$$

We are going to show (by applying our general results to this special example) that S^1_2 proves the consistency of the equational theory for $\mathcal{F}_{\widetilde{\exp}}$, i.e. that $0 = \mathrm{S}\,0$ is not derivable.

As mentioned in the introduction our result even holds for equational theories which base on general recursive axioms over general numerals. In order to make this more precise we start fixing numerals as free algebras over some set of constructors. First some general remarks. Throughout this paper we assume familiarity with the theories of bounded arithmetic and general notions introduced in [2]. A ":" attached to one side of the equality sign in an equation indicates that the expression on the side where ":" occurs is defined by the expression on the other side. I.e., $u := v$, or $v =: u$, respectively, indicates that u is defined by v. With $\mathcal{N}$ we denote the set of non-negative integers.

Let $\mathcal{F}$ be a set of function symbols with arities $\mathrm{ar}(f)$ for $f \in \mathcal{F}$. With $\mathcal{T}(\mathcal{F})$ we denote the set of terms over $\mathcal{F}$, which can be inductively defined by

$$
f \in \mathcal{F} \quad \text{and} \quad t_1, \dots, t_{\mathrm{ar}(f)} \in \mathcal{T}(\mathcal{F}) \quad \Rightarrow \quad (f t_1 \dots t_{\mathrm{ar}(f)}) \in \mathcal{T}(\mathcal{F}).
$$

The reader not interested in general equational theories, but rather wants to stick to Example 2.1, can skip the next two pages and go on reading with Example 2.3 on page 5. For the ongoing discussion he should think of $\mathcal{C}$ *as* $\{0, \mathrm{S}\}$*, of* $\mathbb{A}$ *as* $\mathbb{N} =$ *"the numerals over* $\mathcal{C}$*", i.e.* $\mathcal{T}(\mathcal{C})$*, of* $\mathcal{F}$ *as* $\mathcal{F}_{\widetilde{\exp}}$*, and, respectively, of "a nice set of recursive axioms" as* $Ax_{\widetilde{\exp}}$*.*

Let $X = \{x_0, x_1, x_2, \dots\}$ be a set of free variables. For a subset Y of X let $\mathcal{T}(\mathcal{F}, Y)$ be $\mathcal{T}(\mathcal{F} \cup Y)$, viewing variables as function symbols of arity 0. If Y is a finite set $\{\vec{x}\}$, we will write $\mathcal{T}(\mathcal{F}, \vec{x})$ instead of $\mathcal{T}(\mathcal{F}, \{\vec{x}\})$. We will suppress brackets for a better readability. E.g. we will write $f\vec{t}$ instead of $(f\vec{t})$ and $\mathrm{S}\,\mathrm{S}\,\mathrm{S}\,x$ instead of $(\mathrm{S}(\mathrm{S}(\mathrm{S}\,x)))$.

Let $\mathcal{C} \subset \mathcal{F}$ be a finite set of *constructors* with arities $\mathrm{ar}(\mathrm{c}) \in \{0, 1\}$ for $\mathrm{c} \in \mathcal{C}$, which is not trivial, i.e. $\{\mathrm{ar}(\mathrm{c}) \ : \ \mathrm{c} \in \mathcal{C}\} = \{0, 1\}$. The *free algebra* $\mathbb{A} = \mathbb{A}(\mathcal{C})$ over $\mathcal{C}$ is defined by $\mathcal{T}(\mathcal{C})$. Examples are the algebra $\mathbb{N}$ of natural numbers with constructors 0, S of arity 0, respectively, 1; the algebra $\mathbb{W}$ of binary words over the alphabet $\{0,1\}$ with constructors ϵ of arity 0 and S_0, S_1 of arity 1 (their intended meaning is: $\epsilon =$ empty word, $\mathrm{S}_i(w) = wi$); or the algebra $\mathbb{D}_k$ of k-adic numbers with constructors 0 of arity 0, S_1, ... ,S_k of arity 1 (their intended meaning is: $\mathrm{S}_i(n) = kn + i$). Elements from $\mathbb{A}$ will also be called *numerals*.

By $s_x(t)$ we denote the result of replacing all occurrences of x in s by t.

The function symbols from $\mathcal{F} \setminus \mathcal{C}$ represent functions over $\mathbb{A}$. We assume that they are axiomatized in the restricted way defined next which makes our arguments easier (e.g., the recursion argument is always the first one), but which is still general enough, i.e. captures all interesting examples (see Examples 2.3).

Definition 2.2 *Let Ax be a set of equations over $\mathcal{T}(\mathcal{F}, X)$. We call Ax a* nice set of recursive axioms *iff the following conditions are satisfied:*

i) Each function symbol $f \in \mathcal{F} \setminus \mathcal{C}$ is uniquely (i.e., deterministically) and completely defined by some equation from Ax. By this we mean that for each $f \in \mathcal{F} \setminus \mathcal{C}$ and each $\mathrm{c} \in \mathcal{C}$ there exists exactly one equation $s = t$ in Ax such that s has the form $f\,\mathrm{c}\,x_1 \dots x_{\mathrm{ar}(f)}$ if $\mathrm{ar}(\mathrm{c}) = 0$, or ,respectively, the form $f(\mathrm{c}\,x_0)x_1 \dots x_{\mathrm{ar}(f)}$ if $\mathrm{ar}(\mathrm{c}) = 1$.

With t^{c}_f we denote the t from the equation $s = t$ which is uniquely determined by f and c. Considering Example 2.1 we have, e.g., $t^0_+ = x_1$ and $t^{\mathrm{S}}_+ = \mathrm{S}(x_0 + x_1)$.

ii) The opposite inclusion also holds. Each equation in Ax is a recursive definition of some function symbol in $\mathcal{F} \setminus \mathcal{C}$. I.e., for each $s = t$ in Ax there exists $f \in \mathcal{F} \setminus \mathcal{C}$ and $\mathrm{c} \in \mathcal{C}$ such that either $\mathrm{ar}(\mathrm{c}) = 0$ and s has the form $f\,\mathrm{c}\,x_1 \dots x_{\mathrm{ar}(f)}$ and $t \in \mathcal{T}(\mathcal{F}, \{x_1 \dots x_{\mathrm{ar}(f)}\})$, or $\mathrm{ar}(\mathrm{c}) = 1$ and s has the form $f(\mathrm{c}\,x_0)x_1 \dots x_n$ and $t \in \mathcal{T}(\mathcal{F}, \{x_0 \dots x_{\mathrm{ar}(f)}\})$.

For $\mathrm{c} \in \mathcal{C}$ and $u, v \in \mathcal{T}(\mathcal{F})$ we write $u = \mathrm{c}(v)$ iff either $\mathrm{ar}(\mathrm{c}) = 0$ and $u = \mathrm{c}$, or $\mathrm{ar}(\mathrm{c}) = 1$ and $u = (\mathrm{c}\,v)$. This is a technical convenience which unifies some distinction of cases. For example, condition i) and ii) establish that there is a bijection between $(\mathcal{F} \setminus \mathcal{C}) \times \mathcal{C}$ and Ax, which is given by

$$f, \mathrm{c} \mapsto (f\,\mathrm{c}(x_0)x_1 \dots x_{\mathrm{ar}(f)} = t^{\mathrm{c}}_f).$$

In order to obtain formalizability in S^1_2 we assume in addition that syntax is GÖDEL*ized in a suitable way. In particular, we assume that the predicates $(u = v) \in Ax$, $f \in \mathcal{F}$, or the set of triples $(f, \mathrm{c}, t^{\mathrm{c}}_f)$, are Δ^b_1-definable in S^1_2, and that the code of f contains the code for t^{c}_f for each $\mathrm{c} \in \mathcal{C}$. With the last condition we mean the following: Given $f \in \mathcal{F} \setminus \mathcal{C}$ and $\mathrm{c} \in \mathcal{C}$, let $\tilde{t}$ be the term t^{c}_f, where all occurrences of f have been replaced by some new $\mathrm{ar}(f)$-ary function symbol. Then we assume that the code of $\tilde{t}$ is bounded by the code of f.*

Observe that f is allowed to occur in t^{c}_f *without* restriction on its arguments, hence this is more general than usual recursion or recurrence schemas. Of course this leads in general to non-terminating computations. E.g. let f be an unary function symbol, and let Ax be $\{(f0 = f0), (f(\mathrm{S}\, x) = fx)\}$, then Ax is a nice set of recursive axioms for $\{0, \mathrm{S}, f\}$ over $\mathbb{N}$, but $f0$ cannot be computed (in the sense that it is equal to some numeral).

Examples 2.3 *i)* $Ax_{\widetilde{\exp}}$ *is a nice set of recursive axioms for* $\mathcal{F}_{\widetilde{\exp}}$ *over* $\mathbb{N}$*.*

ii) *A nice set of recursive axioms over* $\mathbb{N}$ *for the primitive recursive functions can be defined as follows: For each* $n \in \mathbb{N}$ *and words* u, v *let* $f_{n,u,v}$ *be a new function symbol, e.g.* $\langle n, u, v\rangle$*. For* $f_{n,u,v}$ *the index* n *will indicate its arity, and indices* u, v *are terms which will be used to recursively define* $f_{n,u,v}$*. Let* $\mathcal{F}_0$ *be the set of constructors* $\{0, \mathrm{S}\}$ *of* $\mathbb{N}$*, and define inductively* $\mathcal{F}_{i+1}$ *by extending* $\mathcal{F}_i$ *by all function symbols* $f_{n+1,u,v}$ *with* $u \in \mathcal{T}(\mathcal{F}_i, x_1, \dots , x_n)$ *and* $v \in \mathcal{T}(\mathcal{F}_i, \{x_0, \dots , x_{n+1}\})$*, and let* $\mathrm{ar}(f_{n+1,u,v})$ *be* $n + 1$*. Let* $\mathcal{F}_{PR}$ *be* $\bigcup_i \mathcal{F}_i$*.*

Then a nice set of recursive axioms Ax_{PR} *for* $\mathcal{F}_{PR}$ *over* $\mathbb{N}$*, which defines exactly the primitive recursive functions, is given by all equations*

$$(f0x_1 \dots x_n) = u \qquad \text{and} \qquad (f(\mathrm{S}\, x_0)x_1 \dots x_n) = v_{x_{n+1}}(fx_0 \dots x_n)$$

for $f_{n+1,u,v} \in \mathcal{F}_{PR}$*.*

iii) Ax_{PR} *can be extended to a nice set of recursive axioms* $Ax_{\mu R}$ *over* $\mathbb{N}$ *which exactly defines the* μ*-recursive functions in the following way: modify the construction of* $\mathcal{F}_{i+1}$ *by adding symbols* μ_f *and* $\tilde{\mu}_f$ *of arity* $n + 1$*, respectively,* $n+2$ *for each* $f \in \mathcal{F}_i$ *of arity* $n+1$ *obtaining* $\mathcal{F}_{\mu R}$*. Then modify the construction of* R_{PR} *by replacing* $\mathcal{F}_{PR}$ *by* $\mathcal{F}_{\mu R}$ *and adding the equations*

$$\begin{aligned} \mu_f x_1 \dots x_n &= \tilde{\mu}_f(f0x_1 \dots x_n)0x_1 \dots x_n \\ \tilde{\mu}_f 0x_1 \dots x_{n+1} &= x_1 \\ \tilde{\mu}_f(\mathrm{S}\, x_0)x_1 \dots x_{n+1} &= \tilde{\mu}_f(f(\mathrm{S}\, x_1)x_2 \dots x_{n+1})(\mathrm{S}\, x_1)x_2 \dots x_{n+1} \end{aligned}$$

for each $f \in \mathcal{F}_{\mu R}$ *of arity* $n + 1$ *obtaining* $R_{\mu R}$*.*

iv) Cook*'s system PV (c.f. [6])* **without** *the substitution and induction rule, i.e. without the rules* $u = w \Rightarrow u_x(v) = w_x(v)$ *and*

$$\frac{\begin{array}{cc} f_1(0,\vec{x}) = g(\vec{x}) & f_2(0,\vec{x}) = g(\vec{x}) \\ f_1(\mathrm{S}_i(y),\vec{x}) = h_i(y,\vec{x}, f_1(y,\vec{x})) & f_2(\mathrm{S}_i(y),\vec{x}) = h_i(y,\vec{x}, f_2(y\vec{x})) \\ f_1(y,\vec{x}) \leq l(y,\vec{x}) & f_2(y,\vec{x}) \leq l(y,\vec{x}) \end{array}}{f_1(y,\vec{x}) = f_2(y,\vec{x})}$$

can be regarded as a nice set of recursive axioms Ax_{PV} *over* $\mathbb{D}_2$*.*

The equational theory for a nice set of recursive axioms Ax is given by (closed) instances of Ax, the definition of equality as an equivalence relation, and the compatibility of function symbols with equality. Let us define this formally.

Definition 2.4 *Let Ax be a nice set of recursive axioms for $\mathcal{F}$. The* equational theory $\mathrm{EqT}(\mathcal{F}, Ax)$ for $\mathcal{F}$ axiomatized by Ax *consists of all equations $u = v$ with $u, v \in \mathcal{T}(\mathcal{F})$ which can be derived by the following rules: let $u, v, w, \vec{u}, \vec{w} \in \mathcal{T}(\mathcal{F})$.*

(Ax) $s_{\vec{x}}(\vec{u}) = t_{\vec{x}}(\vec{u})$ *for* $(s = t) \in Ax$.

(E_1) $u = u$

(E_2) $u = w \Rightarrow w = u$

(E_3) $u = v, v = w \Rightarrow u = w$

(E_4) $u_1 = w_1, \dots, u_m = w_m \Rightarrow f\vec{u} = f\vec{w}$ *for* $f \in \mathcal{F}$ *with* $m = \mathrm{ar}(f)$.

Observe that $\mathrm{EqT}(\mathcal{F}, Ax)$ consists only of equations between closed terms and does **not** contain a substitution rule of the kind $u = w \Rightarrow u_x(v) = w_x(v)$. We will write $\mathrm{EqT}(Ax)$ if the $\mathcal{F}$ connected to Ax is clear or unimportant.

We assume that syntax is coded in a feasible way. Let E be some equational theory as considered above and let $\mathrm{Prf}_E(\pi, \ulcorner s = t \urcorner)$ denote that π codes a treelike proof in E of $s = t$. We assume that 0 and c' are some zero-ary, respectively, unary constructors, which are fixed for a given set of constructors $\mathcal{C}$. Let 1 be the numeral $\mathrm{c}'\,0$. Then $\mathrm{Con}(E)$ is the formula $\forall\pi\neg\,\mathrm{Prf}_E(\pi, \ulcorner 0 = 1 \urcorner)$. The main result in this paper will be the following

Main Theorem 2.5 *Let Ax be a nice set of recursive axioms. Then*

$$S^1_2 \vdash \mathrm{Con}(\mathrm{EqT}(Ax)).$$

The proof will be divided into two main steps. In the next section we will construct in S^1_2 from a given treelike proof in $\mathrm{EqT}(Ax)$ of $s = t$ a path going from s to t according to a rewriting relation associated with Ax. In section 4 we will prove in S^1_2 a feasible CHURCH-ROSSER-property for paths according to this rewriting relation which start from numerals. This shows in S^1_2 that there cannot be a path from 0 to 1 which, with the first step, yields the Main Theorem.

3 Viewing proofs as term rewriting

Rewrite systems are directed equations used to simplify expressions by repeatedly replacing subterms of a given expression with equal terms.[1] Term rewriting has also been used to investigate recursive function theory, c.f. [4, 10, 1]. Here we use term rewriting to prove consistency of equational theories defined by nice recursive axioms.

We start by briefly defining term rewriting adapted to our setting. Throughout the rest of this paper let Ax be some nice set of recursive axioms for $\mathcal{F}$ over $\mathbb{A}$, e.g. $Ax_{\widehat{\exp}}$ for $\mathcal{F}_{\widehat{\exp}}$ over $\mathbb{N}$ from Example 2.1. Terms in which no variable occur,

[1] See [7] for a general introduction to the theory of rewrite systems.

i.e. from $\mathcal{T}(\mathcal{F})$, are called *closed* or *ground*. A *ground substitution* is a mapping σ from a finite set of variables into the set of ground terms $\mathcal{T}(\mathcal{F})$. It is common to write $s\sigma$ instead of $\sigma(s)$ for terms s.

Equations from Ax have – the way we defined them – the property that they are "simplifying from left to right", which is also the direction how the functions defined by them are computed. This is also reflected through the direction of the rewriting relation in the next definition.

Definition 3.1 *The* one-step rewriting relation $\longrightarrow^1_{Ax}$ *is the binary relation on* $\mathcal{T}(\mathcal{F})$ *defined as follows for ground terms* u, v*:* $u \longrightarrow^1_{Ax} v$ *holds iff there exists an axiom* $s = t$ *in* Ax *and a ground substitution* σ *such that* $s\sigma$ *is a ground term and* v *is the result of replacing exactly one occurence of* $s\sigma$ *in* u *by* $t\sigma$*.*

Then $\longrightarrow^n_{Ax}$, $\longrightarrow^*_{Ax}$ *are defined to be the* n*-step rewriting relation, respectively, the reflexive and transitive closure of* $\longrightarrow^1_{Ax}$*.*

The symmetric one-step rewriting relation $\longleftrightarrow^1_{Ax}$ *is defined by*

$$u \longleftrightarrow^1_{Ax} v \quad \textit{iff} \quad u \longrightarrow^1_{Ax} v \;\; \textit{or} \;\; v \longrightarrow^1_{Ax} u$$

and then $\longleftrightarrow^n_{Ax}$, $\longleftrightarrow^*_{Ax}$ *again are defined to be the* n*-step symmeteric rewriting relation, respectively, the reflexive and transitive closure of* $\longleftrightarrow^1_{Ax}$*.*

Observe that equations $s = t$ from nice sets of recursive axioms always fulfill that the variables of t occur under those of s, hence if $s\sigma$ is a ground term, then so is $t\sigma$. Thus, starting from a ground term, $\longrightarrow^*_{Ax}$ only produces ground terms. Furthermore, it is easy to see that $\longleftrightarrow^*_{Ax}$ is an equivalence relation (provable in S^1_2).

As said before we consider a feasible GÖDELization of syntax as in [2]. I.e., after GÖDELizing all symbols in a suitable way, terms are coded by

$$\ulcorner(ft_1 \dots t_m)\urcorner = \langle \ulcorner(\urcorner, \ulcorner f\urcorner\rangle {}^\frown \ulcorner t_1\urcorner {}^\frown \dots {}^\frown \ulcorner t_m\urcorner {}^\frown \langle \ulcorner)\urcorner\rangle.$$

Hence the number of symbols in a term is proportional to the code of that term.

Equational theories are strongly connected to corresponding symmetric rewriting relation. It is possible to feasibly extract from a given proof of an equation $u = v$ in some equational theory a path from u to v according to the corresponding symmetric rewriting relation.

Theorem 3.2 (S^1_2) *If* $u = v$ *is provable in* $\mathrm{EqT}(Ax)$*, then* $u \longleftrightarrow^*_{Ax} v$*.*

Proof. We prove the assertion by induction on the $\mathrm{EqT}(Ax)$-proof of $u = v$.

If $u = v$ is an axiom concerning (Ax), then $u = v$ is an instance of some equation $s = t$ from Ax. By mapping each variable in s, t to its instance in u, v we obtain a ground substitution σ such that

$$u = s\sigma \longrightarrow^1_{Ax} t\sigma = v.$$

If the last inference have been one of (E_1), (E_2) or (E_3), then the assertion is obvious, because $\longleftrightarrow^*_{Ax}$ is an equivalence relation, provable in S^1_2.

If the last inference has been (E_4), then u has the form $fu_1 \dots u_m$, and v has the form $fv_1 \dots v_m$, and we have subproofs π_i in π of $u_i = v_i$. By induction hypothesis we obtain $u_i \longleftrightarrow^*_{Ax} v_i$, which we use successively to obtain

$$u = fu_1 \dots u_m \longleftrightarrow^*_{Ax} fv_1 u_2 \dots u_m \longleftrightarrow^*_{Ax} fv_1 v_2 \dots u_m \longleftrightarrow^*_{Ax} \dots \longleftrightarrow^*_{Ax} v.$$

In order to see that this proof is formalizable in S^1_2 we have to check that the constructed path from u to v concerning $\longleftrightarrow^1_{Ax}$ is polynomially bounded in the original proof π. But it is easy to see that the number of steps from u to v is bounded by the number of symbols in π, and all terms on that path are bounded by π. (Both bounds are only very rough upper bounds.) $\square$

4 A kind of Church-Rosser-property

We start this section with an example. Assume we have a path $a \longleftrightarrow^*_{Ax} u$ starting from some numeral $a \in \mathbb{A}$. At each step of this path we will convince ourselves that the term at this point has value a, thus there cannot be a path from 0 to 1. The first idea for solving this problem, which comes to ones mind, is to prove in S_2 that $\longrightarrow^1_{Ax}$ has the Church-Rosser-property, i.e. to show

$$u \longleftrightarrow^*_{Ax} v \quad \Rightarrow \quad \exists w (u \longrightarrow^*_{Ax} w \ \& \ v \longrightarrow^*_{Ax} w).$$

This solves the problem, because numerals are irreducible under $\longrightarrow^1_{Ax}$. But it is, to the author's best knowledge, an open problem if this general form of the Church-Rosser-property is provable in S_2, and the author conjectures that this is not the case.

We will solve this problem, in case that u is a numeral and $u \longleftrightarrow^*_{Ax} v$ holds, by reducing v to u according to a modified reduction relation. This modification is a combination of "approximation" and "calculation". For "approximation" we introduce a new symbol $*$. If a subterm is replaced by $*$, it is blocked out from the ongoing computation (we think of its value as "arbitrary" or "unknown"). Now "calculating" means reducing according to $\longrightarrow^1_{Ax}$, which is viewed in this setting as a rewriting relation over $\mathcal{T}(\mathcal{F}, *)$.

Example 4.1 *Let us return to $Ax = Ax_{\widetilde{\exp}}$ from Example 2.1. The corresponding rewriting relation $\longrightarrow^1_{Ax}$ is given by*

$$\begin{aligned} 0 + y &\longrightarrow^1_{Ax} y & (\mathrm{S}\, x) + y &\longrightarrow^1_{Ax} \mathrm{S}(x + y) \\ 0 \cdot y &\longrightarrow^1_{Ax} 0 & (\mathrm{S}\, x) \cdot y &\longrightarrow^1_{Ax} x \cdot y + y \\ \widetilde{\exp} 0 y &\longrightarrow^1_{Ax} y & \widetilde{\exp}(\mathrm{S}\, x) y &\longrightarrow^1_{Ax} y \cdot (\widetilde{\exp} x y) \end{aligned}$$

Consider the following reduction chain according to $\longrightarrow^1_{Ax}$:

$$0 \longleftarrow^1_{Ax} 0 \cdot (\widetilde{\exp}(s + t) 0) \longleftarrow^1_{Ax} \widetilde{\exp}(\mathrm{S}(s + t)) 0 \longleftarrow^1_{Ax} \widetilde{\exp}((\mathrm{S}\, s) + t) 0 \qquad (1)$$

We now show how this approximation and calculation stuff works by considering successively the terms in the chain (from left to right).

i) "0". *Nothing to do.*

ii) "$0\cdot(\widetilde{\exp}(s+t)0)$". *Approximate* $\widetilde{\exp}(s+t)0$ *by* $*$, *then calculate* $0\cdot * \longrightarrow^1_{Ax} 0$.

iii) "$\widetilde{\exp}(\mathrm{S}(s+t))0$". *For the subterm* $\mathrm{S}(s+t)$ *approximate* $s+t$ *by* $*$ *which yields* $\mathrm{S}\,*$. *Calculate* $\widetilde{\exp}(\mathrm{S}\,*)0 \longrightarrow^1_{Ax} 0\cdot(\widetilde{\exp}*0)$, *approximate* $(\widetilde{\exp}*0)$ *by* $*$ *and use information from ii) that* $0\cdot *$ *approximates and calculates to* 0. *Hence* $\widetilde{\exp}(\mathrm{S}\,*)0$ *approximates and calculates to* 0.

iv) "$\widetilde{\exp}((\mathrm{S}\,s)+t)0$". *For the subterm* $(\mathrm{S}\,s)+t$ *approximate* s *and, respectively,* t *by* $*$, *then calculate* $(\mathrm{S}\,*)+* \longrightarrow^1_{Ax} \mathrm{S}(*+*)$ *and approximate* $*+*$ *by* $*$, *thus* $(\mathrm{S}\,s)+t$ *approximates and calculates to* $\mathrm{S}\,*$. *Use information from iii) that* $\widetilde{\exp}(\mathrm{S}\,*)0$ *approximates and calculates to* 0.

For the rest of this section let $\mathcal{C}$, $\mathbb{A}$ and $\mathcal{F}$ be fixed and Ax be a nice set of recursive axioms for $\mathcal{F}$ over $\mathbb{A}$, e.g. $\{0,\mathrm{S}\}$, $\mathbb{N}$, $\mathcal{F}_{\widetilde{\exp}}$, $Ax_{\widetilde{\exp}}$ from Example 2.1. Example 4.1 shows that we want to suppress parts of a term which are unessential for a certain reduction path. We do this by replacing such unessential subterms of a term s by a new (fixed) symbol $*$. The result of such a replacement will be an approximation to s.

More precise, let $*$ be a new zero-ary constructor. Define $\mathcal{C}_* := \mathcal{C}\cup\{*\}$, $\mathcal{F}_* := \mathcal{F}\cup\{*\}$ and $\mathbb{A}_* := \mathcal{T}(\mathcal{C}_*)$. Elements of $\mathbb{A}_*$ are called *generalized numerals.* We define a binary relation $\lhd$ on $\mathcal{T}(\mathcal{F}_*)$ which will have the meaning that $s \lhd t$ holds if t is an approximation to s, i.e., if t is the result of replacing some (possibly none) subterms of s by $*$. Read "$s \lhd t$" as "s is approximated by t".

Definition 4.2 *We define the relation* $\lhd$ *on* $\mathcal{T}(\mathcal{F}_*)$ *inductively by*

i) $s \lhd *$ *holds for all* $s \in \mathcal{T}(\mathcal{F}_*)$.

ii) If $f\in\mathcal{F}$ *and* $s_i \lhd t_i$ *for* $i=1,\dots,\mathrm{ar}(f)$, *then* $f\vec{s} \lhd f\vec{t}$.

The definition of $\lhd$ *as a* Δ^b_1*-predicate in* S^1_2 *is left to the reader as an exercise.*

Observe that ii) implies $f \lhd f$ for $f\in\mathcal{F}_*$ with $\mathrm{ar}(f)=0$, therefore we obtain $u \lhd u$ for all $u\in\mathcal{T}(\mathcal{F}_*)$. We state some properties which follow immediately from the definition.

Let us remind ourselves that for $\mathrm{c}\in\mathcal{C}$ and a term u we have fixed the convention that in case that c is zero ary the writing $\mathrm{c}(u)$ denotes the term c, and in case that c is unary the writing $\mathrm{c}(u)$ denotes the term $(\mathrm{c}\,u)$. For $\mathcal{F}_{\widetilde{\exp}}$ from Example 2.1 the only possibilities are $0(u)$ denoting 0 and $\mathrm{S}(u)$ denoting $(\mathrm{S}\,u)$. To see that this convention often helps reducing cases we observe that Observation 4.3 ii) for $\mathcal{F}_{\widetilde{\exp}}$ is equivalent to

$$\mathrm{S}\,u \lhd \mathrm{S}\,v \Rightarrow u \lhd v \quad \textit{and} \quad \mathrm{S}\,u \not\lhd 0 \quad \textit{and} \quad 0 \not\lhd \mathrm{S}\,v.$$

Observations 4.3 (S^1_2)

i) If $u \lhd v$ *and* $v\in\mathcal{T}(\mathcal{F})$, *then* $u=v$.

ii) *If* $\mathrm{c}(u) \lhd \mathrm{c}'(v)$ *and* $\mathrm{c}, \mathrm{c}' \in \mathcal{C}$*, then* $\mathrm{c} = \mathrm{c}'$ *and* $u \lhd v$.

iii) *If* $u \lhd v \lhd u$*, then* $u = v$.

iv) $\lhd$ *is transitive.*

v) *If* $u \lhd v$ *and* $t \in \mathcal{T}(\mathcal{F}_*, x)$*, then* $t_x(u) \lhd t_x(v)$. □

The following Lemma is simple but essential for the layout of our proofs. It would be wrong if the set of constructors would contain an element with arity bigger than one.

Lemma 4.4 (S^1_2)
If $w \lhd u$*,* $w \lhd v$ *and* $u, v \in \mathbb{A}_*$*, then* $u \lhd v$ *or* $v \lhd u$.

Proof. We essentially use $\{\mathrm{ar}(\mathrm{c}) : \mathrm{c} \in \mathcal{C}\} = \{0, 1\}$. We prove the assertion by induction on the definition of $w \lhd u$. If $u = *$, then $v \lhd u$. If $u = \mathrm{c} \in \mathcal{C}$, then $w = u$, hence $u \lhd v$.

Otherwise $u = \mathrm{c}\, u'$, $\mathrm{c} \in \mathcal{C}$, hence $w = \mathrm{c}\, w'$ and $w' \lhd u'$. In case $v = *$ we get $u \lhd v$. Otherwise we have $v = \mathrm{c}\, v'$ and $w' \lhd v'$ because of $w = \mathrm{c}\, w' \lhd v$. By induction hypothesis we obtain $u' \lhd v'$ or $v' \lhd u'$, hence $u \lhd v$ or $v \lhd u$. □

As in Example 4.1 we view $\longrightarrow^1_{Ax}$ also as the rewriting relation over $\mathcal{T}(\mathcal{F}_*)$. This way we already described a new way for computing (generalized) values of closed terms by a method we called "approximation and calculation". As in Example 4.1 we can construct from a given path according to our rewrite system the essence which let us feasibly approximate and calculate values of the terms of the path. In the example this essence has the form

$$0 \cdot * \rightsquigarrow 0\,, \quad f(\mathrm{S}\,*)0 \rightsquigarrow 0\,, \quad (\mathrm{S}\,*) + * \rightsquigarrow \mathrm{S}\,*\,.$$

We call this sequence $\mathfrak{e}$ an *evidence* (it includes that it is "correctly derived" using the underlying rewriting system). Using evidence $\mathfrak{e}$ we can feasibly argue that each term on the path has value 0. We say that, for example, 0 is an $\mathfrak{e}$-approximation to $f((\mathrm{S}\,s) + t)0$. (We use the wording "approximation" because we will also consider paths starting from generalized numerals w, so that w will only be an approximation in the sense of Definition 4.2 to the value of each term of the path.)

Furthermore, we will also control the depths of all generalized numerals occurring in approximations and evidences. The *depth* $\mathrm{dp}(t)$ of a term $t \in \mathcal{T}(\mathcal{F}_*)$ is defined as usual inductively by

$$\mathrm{dp}(f t_1 \dots t_m) = \begin{cases} 0 & \text{if } m = 0, \\ 1 + \max_{i=1,\dots,m} \mathrm{dp}(t_i) & \text{if } m > 0. \end{cases}$$

We consider a feasible coding of sequences, which can be handled in S^1_2, as done for example in [2]. Especially we have a predicate Seq for the set of all sequence numbers, and we assume $0 \notin \mathrm{Seq}$. We write $\langle a_1, \ldots, a_n \rangle$ for the code of the sequence $a_1, \ldots, a_n$. With $\mathrm{l}(\sigma)$, $(\sigma)_i$, $\mathrm{maxel}(\sigma)$, $\sigma ^\frown \tau$, $\sigma \restriction j$, $\mathrm{SqBd}(a, b)$ we denote the length of a sequence σ, its i-th element, the maximum of its elements, the concatenation of σ with the sequence τ, the restriction of σ to its first j elements, i.e. $\sigma \restriction j := \langle (\sigma)_0, \ldots, (\sigma)_{j-1} \rangle$, respectively, an upper bound to all sequences σ with $\mathrm{l}(\sigma) \leq |a|$ and $\mathrm{maxel}(\sigma) \leq b$. Here $|a|$ denotes the number of bits in the binary representation of a, i.e. $\lceil \log_2(n+1) \rceil$. With $\sigma \sqsubseteq \tau$ we mean that σ is a subsequence of τ, i.e.

$$\exists i_1 < \ldots < i_{\mathrm{l}(\sigma)} < \mathrm{l}(\tau) \quad \forall j < \mathrm{l}(\sigma) \quad (\sigma)_j = (\tau)_{i_{j+1}} .$$

Then $\sigma \sqsubset \tau$ is the strict form of $\sqsubseteq$, i.e. it means $\sigma \sqsubseteq \tau$ and $\sigma \neq \tau$. With $a \in \sigma$ we mean that a occurs under the elements of σ. All these predicates and functions are Δ^b_1-definable, respectively, Σ^b_1-definable in S^1_2. Furthermore S^1_2 can prove all necessary properties, see [2].

We now define formally that a generalized numeral w approximates a term under a given (hypothetic) evidence $\mathfrak{e}$, and afterwards that $\mathfrak{e}$ is an evidence. We have to define the notions in this order because an evidence also carries the information that it is correct under the underlying rewriting system, and this correctness is expressed using approximations. In the following we always identify symbols with their GÖDEL-numbers.

Definition 4.5 *We define by induction on $t \in \mathcal{T}(\mathcal{F}_*)$ that w is an* $\mathfrak{e}, k$-approximation for t *iff $w \in \mathbb{A}_*$, $\mathfrak{e} \in \mathrm{Seq}$, and*

i) $w = *$, *or*

ii) $\mathrm{dp}(w) \leq k$, *t has the form $f t_1 \ldots t_m$, and there are $\mathfrak{e}, k$-approximations w_i for t_i for $i = 1, \ldots, m$ such that either $f \in \mathcal{C}_*$ and $f \vec{w} \lhd w$, or $f \notin \mathcal{C}_*$ and there is some $v \lhd w$ such that $\langle f, \vec{w}, v \rangle \in \mathfrak{e}$.*

Let us remind ourselves the convention of writing t^{c}_f. There is a bijection between $(\mathcal{F} \setminus \mathcal{C}) \times \mathcal{C}$ and Ax, which is given in the following way: for each $f \in \mathcal{F} \setminus \mathcal{C}$ and each $\mathrm{c} \in \mathcal{C}$ there is exactly one equation $s = t$ in Ax with $s = f\,\mathrm{c}(x_0) x_1 \ldots x_{\mathrm{ar}(f)}$, and then t^{c}_f denotes t. Considering Example 2.1 we have, e.g., $t^0_+ = x_1$ and $t^{\mathrm{S}}_+ = \mathrm{S}(x_0 + x_1)$.

Definition 4.6 *We define that $\mathfrak{e}$ is a k-*evidence *iff $\mathfrak{e} \in \mathrm{Seq}$ and for all $i < \mathrm{l}(\mathfrak{e})$ there are f, with arity $m > 0$, and $w_1, \ldots, w_m, w$ such that $(\mathfrak{e})_i$ has the form $\langle f, w_1, \ldots, w_m, w \rangle$, $w, \vec{w} \in \mathbb{A}_*$, $\mathrm{dp}(w), \mathrm{dp}(\vec{w}) \leq k$, w_1 has the form $\mathrm{c}(v)$ with $\mathrm{c} \in \mathcal{C}$, and w is an $(\mathfrak{e} \restriction i), k$-approximation for $t^{\mathrm{c}}_f(v, w_2, \ldots, w_m)$.*

Going back to Example 4.1 we have the following list of level l, terms t and evidences $\mathfrak{e}$ such that $\mathfrak{e}$ is an l-evidence and 0 an $\mathfrak{e}, l$-approximation of t.

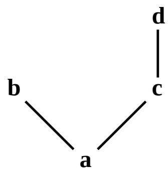
term	level	evidence
0	0	$\langle\rangle$
$0 \cdot (f(s+t)0)$	0	$\langle\langle \cdot, 0, *, 0 \rangle\rangle$
$f(\mathrm{S}(s+t))0$	1	$\langle\langle \cdot, 0, *, 0 \rangle, \langle f, \mathrm{S}\,*, 0, 0 \rangle\rangle$
$f((\mathrm{S}\,s)+t)0$	1	$\langle\langle \cdot, 0, *, 0 \rangle, \langle f, \mathrm{S}\,*, 0, 0 \rangle, \langle +, \mathrm{S}\,*, *, \mathrm{S}\,* \rangle\rangle$

On the next one and a half pages we will argue that the last definitions can be formalized in a suitable way in S^1_2. The reader who believes this already, or does not want to go into so much detail, can skip these and go on reading with Observation 4.7 on page 14.

Let $\mathrm{B}_{\mathbb{A}_*}(k)$ be an upper bound to the GÖDEL-numbers of elements from $\mathbb{A}_*$ whose depths are not bigger that k, which can be chosen to fulfill $|\,\mathrm{B}_{\mathbb{A}_*}(k)| = O(k)$.

We now argue that the just defined notions can be given by Σ^b_1-formulas such that S^1_2 proves the properties given in the above definitions. As "$\mathfrak{e}$ is a k-evidence" is not inductively defined but explicitly based on "w is an $\mathfrak{e}, k$-approximation for t" it suffices to argue for the last notion which has been defined in Definition 4.5. We first have to fix some functions and predicates on coded trees which can be seen to be Σ^b_1-definable in S^1_2, respectively, Δ^b_1 in S^1_2 similar to [2].

E.g., let us consider the following tree



which is coded as $t = \ulcorner(a(b)(c(d)))\urcorner$. A node in t is given either by an index k of the sequence t, or by a position $p \in \mathrm{Seq}$ which reflects the path from the root to that node. E.g. the nodes of t have the following indices and positions:

node	a	b	c	d
index in t	1	3	6	8
position in t	$\langle\rangle$	$\langle 0\rangle$	$\langle 1\rangle$	$\langle 1,0\rangle$

Let $\mathrm{tcb}(w, s_1, \dots, s_l) := \langle\ulcorner(\urcorner, w\rangle \frown s_1 \frown \dots \frown s_l \frown \langle\ulcorner)\urcorner\rangle$ (tcb stands for tree-combine), i.e. $\mathrm{tcb}(w, s_1, \dots, s_l)$ codes the tree whose root is labeled with w, and which has l children $s_1, \dots, s_l$. E.g. $t = \mathrm{tcb}(a, \ulcorner(b)\urcorner, \ulcorner(c(d))\urcorner)$. In the following we often replace unimportant terms by one or several dots.

For $p \in \mathrm{Seq}$ let the *p-th subtree of s* be defined by

$$\mathrm{st}(p,s) := \begin{cases} s & \text{if } p = \langle\rangle \\ \mathrm{st}(p', s_i) & \text{if } p = \langle i\rangle \frown p' \text{ and } s = \mathrm{tcb}(., s_0, \dots, s_{l-1}) \text{ and } i < l \\ \langle\rangle & \text{otherwise.} \end{cases}$$

E.g. $\mathrm{st}(\langle 0\rangle, t) = \ulcorner(b)\urcorner$. Let

$$\mathrm{val}(s) := \begin{cases} \langle w\rangle & \text{if } s = \mathrm{tcb}(w, \dots) \\ \langle\rangle & \text{otherwise,} \end{cases}$$

then the *p-th value of s* is defined by $\mathrm{val}(p, s) := \mathrm{val}(\mathrm{st}(p, s))$. E.g. $\mathrm{val}(\langle 1\rangle, t) = \langle c\rangle$ and $\mathrm{val}(\langle 1, 0\rangle, t) = \langle d\rangle$.

We also need some kind of inverse function to $\mathrm{val}(p, s)$, which computes the position of a node in a tree. The *position* of a node $(t)_k$ in a tree t can be computed via

$$\begin{aligned}
&\mathrm{pos}(k, t) = 0 \qquad \text{if } t \neq \mathrm{tcb}(\dots) \\
&\mathrm{pos}(k, \mathrm{tcb}(., s_0, \dots, s_{l-1})) \\
&\quad = \begin{cases} \langle\rangle & \text{if } k = 1 \\ \langle m\rangle ^\frown \mathrm{pos}(k \dot{-} n, s_m) & \text{if } m < l,\ n = 2 + \sum_{j<m} \mathrm{l}(s_j) \\ & \ \text{and } n \leq k < n + \mathrm{l}(s_m) \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

For our example we have

index k	0	1	2	3	4	5	6	7	8	9	10	11
k-th char. in t	(	a	(	b	)	(	c	(	d	)	)	)
$\mathrm{pos}(k, t)$	0	$\langle\rangle$	0	$\langle 0\rangle$	0	0	$\langle 1\rangle$	0	$\langle 1, 0\rangle$	0	0	0

Observe that $\mathrm{l}(\mathrm{pos}(k, t)) \leq \mathrm{l}(t)$ and $\mathrm{maxel}(\mathrm{pos}(k, t)) \leq \mathrm{l}(t)$, hence $\mathrm{pos}(k, s) \leq \mathrm{SqBd}(t, |t|)$. For $p := pos(k, t) \in \mathrm{Seq}$ we have $\mathrm{val}(p, t) = (t)_k$, because $0 \notin \mathrm{Seq}$. Furthermore, if $p = \mathrm{pos}(k, t) \in \mathrm{Seq}$ and $\mathrm{st}(p ^\frown \langle l\rangle, t) \neq \langle\rangle$, then there is some $k' > k$ such that $\mathrm{pos}(k', t) = p ^\frown \langle l\rangle$.

We say that s *has the same tree-structure as* t iff s and t are trees which differ at most at the labels of their nodes, i.e. $\mathrm{l}(s) = \mathrm{l}(t)$ and

$$\forall i < \mathrm{l}(t) \big[(t)_i \in \{ \ulcorner (\urcorner, \ulcorner) \urcorner \} \Rightarrow (s)_i = (t)_i \big].$$

We now define a Σ^b_1-formula stating that τ is an $\mathfrak{e}, k$-approximation tree for t, which, for τ having the same tree-structure as t, means that the labels of τ are $\mathfrak{e}, k$-approximations for the corresponding subterms in t.

$$\begin{aligned}
\mathit{approxtree}(\mathfrak{e}, k, t, \tau) \ :\Leftrightarrow \forall j < |t| \Big[& \text{ if } p := \mathrm{pos}(j, t) \in \mathrm{Seq} \\
& \text{let } f := \mathrm{val}(p, t), w' := \mathrm{val}(p, \tau), m := \mathrm{ar}(f), \\
& w_i := \mathrm{val}(p ^\frown \langle i \dot{-} 1\rangle, \tau) \text{ for } i = 1, \dots, m, \\
& \text{then } w', \vec{w} \in \mathbb{A}_*, \mathrm{dp}(w'), \mathrm{dp}(\vec{w}) \leq k, \\
& \quad (f \in \mathcal{C}_* \Rightarrow f\vec{w} \lhd w') \quad \text{ and} \\
& \quad (f \notin \mathcal{C}_* \Rightarrow \exists v \leq \mathfrak{e} (v \lhd w' \ \& \ \langle f, \vec{w}, v\rangle \in \mathfrak{e})) \Big]
\end{aligned}$$

For $w \in \mathbb{A}_* \setminus \{*\}$, $\mathfrak{e} \in \mathrm{Seq}$, $t \in \mathcal{T}(\mathcal{F}_*)$ we then can define that w is an $\mathfrak{e}, k$-approximation for t iff there exists a sequence $\tau \leq \mathrm{SqBd}(t, \max(\mathfrak{e}, t))$ such that τ has the same tree-structure as t and $\mathit{approxtree}(\mathfrak{e}, k, t, \tau)$ and $\mathrm{val}(\langle\rangle, \tau) = \langle w\rangle$. Obviously this is defined by a Σ^b_1-formula.

The following observations follow immediately from the definitions.

Observations 4.7 (S^1_2)

i) *w is a $\langle\rangle, k$-approximation for t iff $w \in \mathbb{A}_*$, $\mathrm{dp}(w) \leq k$ and $t \lhd w$.*

ii) *If w is an $\mathfrak{e}, k$-approximation for $t \in \mathbb{A}_*$, then $t \lhd w$.*

iii) *If w is an $\mathfrak{e}, k$-approximation for $\mathrm{c}(t)$, $\mathrm{c} \in \mathcal{C}$, then $w = *$ or $w = \mathrm{c}(w')$.*

iv) *If $(\mathrm{c}\, w)$ is an $\mathfrak{e}, k$-approximation for $(\mathrm{c}\, t)$, then w is an $\mathfrak{e}, k$-approximation for t.*

v) *If v is an $\mathfrak{e}, k$-approximation for t and $v \lhd w$, then w is an $\mathfrak{e}, k$-approximation for t (because $v \lhd w \Rightarrow \mathrm{dp}(w) \leq \mathrm{dp}(v)$).*

vi) *If w is an $\mathfrak{e}, k$-approximation for t and $\mathfrak{e} \sqsubseteq \mathfrak{e}'$, $k \leq k'$, then w is an $\mathfrak{e}', k'$-approximation for t.* □

Our general plan is to construct, from a given path $a \longleftrightarrow^*_{Ax} v$ starting from some numeral $a \in \mathbb{A}_*$, a number k and a k-evidence $\mathfrak{e}$ such that a is an $\mathfrak{e}, k$-approximation for v. But if also $v \in \mathbb{A}_*$, this implies $v \lhd a$ by Observation 4.3 ii). Hence, as $1 \not\lhd 0$, there cannot be a path $0 \longleftrightarrow^*_{Ax} 1$. This will prove the consistency of $\mathrm{EqT}(Ax)$.

We divide this general plan into two parts according to the direction of the rewriting steps $t \longleftrightarrow^1_{Ax} t'$ on the path. If we already have an evidence $\mathfrak{e}$ and an $\mathfrak{e}$-approximation w for t and $t \longrightarrow^1_{Ax} t'$, then the same $\mathfrak{e}$ yields that w is an $\mathfrak{e}$-approximation for t'. This is the easier part.

In the second part, if $t \longleftarrow^1_{Ax} t'$, we will construct a new evidence $\mathfrak{e}'$ such that w is an $\mathfrak{e}'$-approximation for t'. In this step the depth of the stored generalized numerals will eventually raise by one.

Let s, t be terms and x be a variable, then by $s_x(t)$ we denote the result of replacing all occurrences of x in s by t. With $s(x)$ we denote some occurrences of x in s (possibly none).

For the first part we only have to show that enough information is stored in evidences. E.g. returning to Example 2.1, if $\mathfrak{e}$ is an evidence and w an $\mathfrak{e}$-approximation for $\widetilde{\exp}(\mathrm{S}\, s, t)$, then by definition there are $\mathfrak{e}$-approximations u, v for s, respectively t, such that w is an $\mathfrak{e}$-approximation for $t^{\mathrm{S}}_{\widetilde{\exp}}(u, v) = v \cdot \widetilde{\exp}(u, v)$, using that $\mathfrak{e}$ is an evidence. Hence, we only have to show that u, v can be replaced by s, respectively t. The next lemma states such a composition property for approximations.

At the end of the proof of some of the next lemmas and propositions we will indicate how the proofs can be formalized in S^1_2. The reader who already believes in the formalizability, or does not want to go into so much detail, may skip these remarks and go on reading after those proofs. Let us remind ourselves that $\mathrm{B}_{\mathbb{A}_*}(k)$ is an upper bound to all (Gödel-numbers of) numerals of $\mathbb{A}_*$ of depth not greater than k.

Lemma 4.8 (S^1_2) *Assume w_i is an $\mathfrak{e}, k$-approximation for t_i, for $i = 1, \ldots, m$, and w is an $\mathfrak{e}, k$-approximation for $a(\vec{w})$, where $a(\vec{x}) \in \mathcal{T}(\mathcal{F}_*, \vec{x})$. Then w is an $\mathfrak{e}, k$-approximation for $a(\vec{t})$.*

Proof. Let w_i be an $\mathfrak{e}, k$-approximation for t_i, for $i = 1, \ldots, m$. We prove

$$\forall w \leq \mathrm{B}_{\mathbb{A}_*}(k) \big[\, w \text{ is an } \mathfrak{e}, k\text{-approximation for } a(\vec{w}) \\ \Rightarrow w \text{ is an } \mathfrak{e}, k\text{-approximation for } a(\vec{t}) \,\big]$$

by induction on the definition of the term $a(\vec{x})$.

If $a \in \mathcal{C}_*$ the assertion is obvious.

In case $a(\vec{x}) = x_i$ we have that w is an $\mathfrak{e}, k$-approximation for w_i, hence with Observation 4.7 ii) $w_i \lhd w$. Thus using the assumptions we obtain from Observation 4.7 v) that w is an $\mathfrak{e}, k$-approximation for t_i.

Finally assume that $a(\vec{x})$ is $f b_1(\vec{x}) \ldots b_n(\vec{x})$. If $w = *$ we are done. Otherwise there is v_i being an $\mathfrak{e}, k$-approximation for $b_i(\vec{w})$, for $i = 1, \ldots, n$. By induction hypothesis we obtain that v_i is an $\mathfrak{e}, k$-approximation for $b_i(\vec{t})$, for $i = 1, \ldots, n$. Then the same reason for w being an $\mathfrak{e}, k$-approximation for $a(\vec{w})$ also shows that w is an $\mathfrak{e}, k$-approximation for $a(\vec{t})$.

Concerning formalizability the induction described so far is equivalent to $LIND$ over some Π^b_2-formula which is not available in S^1_2. In order to see that this proof can be done in S^1_2, we would have to proceed as follows. Fix some term $a(\vec{x})$ and w being an $\mathfrak{e}, k$-approximation for $a(\vec{w})$. I.e., there is some τ having the same tree-structure as $a(\vec{w})$ such that $\mathrm{val}(\langle\rangle, \tau) = \langle w \rangle$ and $approxtree(\mathfrak{e}, k, a(\vec{w}), \tau)$ holds. Now we prove

$$\forall i < |a(\vec{x})| \Big(j \leq i \;\&\; p := \mathrm{pos}(i, a(\vec{x})) \in \mathrm{Seq} \\ \Rightarrow (\mathrm{val}(p, \tau))_0 \text{ is an } \mathfrak{e}, k\text{-approximation for } \mathrm{st}(p, a(\vec{t})) \Big)$$

by backwards induction on j using the fact that if $p = \mathrm{pos}(i, a(\vec{x})) \in \mathrm{Seq}$ and s is the $(l+1)$-th direct subterm of $\mathrm{st}(p, a(\vec{x}))$, then $\mathrm{st}(p ^\frown \langle l \rangle, a(\vec{x})) = s$ and there is some $i' > i$ such that $\mathrm{pos}(i', a(\vec{x})) = p ^\frown \langle l \rangle$. □

The structures of most of the following proofs are the same as the one from the last proof. They will mostly rely on an induction on terms $a(\vec{x}) \in \mathcal{T}(\mathcal{F}_*, \vec{x})$. We will therefore only consider those cases where something new happens, i.e. which are not the same as in the last proof, or do not follow directly from the induction hypothesis.

Theorem 4.9 (S^1_2) *Assume that $\mathfrak{e}$ is a k-evidence, w is an $\mathfrak{e}, k$-approximation for t, and $t \longrightarrow^1_{Ax} t'$. Then w is an $\mathfrak{e}, k$-approximation for t'.*

Proof. Let $\mathfrak{e}$ be a k-evidence, and fix some $f \in \mathcal{F} \setminus \mathcal{C}$, $\mathrm{c} \in \mathcal{C}$ and $b, \vec{c} \in \mathcal{T}(\mathcal{F}_*)$, $a(x) \in \mathcal{T}(\mathcal{F}_*, x)$. Remember that $f\, \mathrm{c}(b)\vec{c} \longrightarrow^1_{Ax} t^{\mathrm{c}}_f(b, \vec{c})$. We prove the assertion for $a(f\, \mathrm{c}(b)\vec{c}) \longrightarrow^*_{Ax} a(t^{\mathrm{c}}_f(b, \vec{c}))$. Let w be an $\mathfrak{e}, k$-approximation for $a(f\, \mathrm{c}(b)\vec{c})$.

We only consider the case that $a(x) = x$. Then there are $\mathfrak{e}, k$-approximations $w', \vec{w}_c$ for $\mathrm{c}(b), \vec{c}$. As $f \notin \mathcal{C}_*$ there exists some $v \lhd w$ such that $\langle f, w', \vec{w}_c, v\rangle \in \mathfrak{e}$. $\mathfrak{e}$ is a k-evidence, hence $w' = \mathrm{c}(w_b)$, same c, by Observation 4.7 iii), and v is an $\mathfrak{e}, k$-approximation for $t^{\mathrm{c}}_f(w_b, \vec{w}_c)$. From this, $v \lhd w$ and Observation 4.7 v), it follows that w is an $\mathfrak{e}, k$-approximation for $t^{\mathrm{c}}_f(w_b, \vec{w}_c)$. Hence the assertion follows by Lemma 4.8, as w_b is an $\mathfrak{e}, k$-approximation for b by Observation 4.7 iv). $\square$

This Theorem finishes the first part of our general plan. The second one is more involved, here we have to construct new approximations. E.g. returning to Example 2.1, let $\mathfrak{e}$ be an evidence and w be an $\mathfrak{e}$-approximation for $t^{\mathrm{S}}_{\widetilde{\exp}}(s,t) = t \cdot \widetilde{\exp}(s,t)$. Then we have to construct an evidence $\mathfrak{e}'$ such that w is an $\mathfrak{e}'$-approximation of $\widetilde{\exp}(\mathrm{S}\, s, t)$. To do so, we first have to find $\mathfrak{e}$-approximations u, v for s, respectively t. Here lies the crucial point, which is very similar to the general Church-Rosser-property, but which can now be handled in S^1_2. From the assumption that w is an $\mathfrak{e}$-approximation for $t \cdot \widetilde{\exp}(s,t)$ we obtain for several occurrences of t in general several $\mathfrak{e}$-approximations v, v' for t. The main part is now to prove that v and v' are comparable with respect to $\lhd$. In particular, this implies that 0 and 1 *cannot* be $\mathfrak{e}$-approximations of the same term at the same time. Assuming that $v \lhd v'$, it is then easy to conclude that w is an $\mathfrak{e}$-approximation for $v \cdot \widetilde{\exp}(u, v)$. Hence we can extend $\mathfrak{e}$ by a new entry $\langle \widetilde{\exp}, \mathrm{S}\, u, v, w\rangle$ obtaining an evidence $\mathfrak{e}'$ which solves our problem. In the following we make this precise.

We start with a simple Lemma.

Lemma 4.10 (S^1_2) *Assume w is an $\mathfrak{e}, k$-approximation for $a(v)$ with $a(x) \in \mathcal{T}(\mathcal{F}_*, x)$, and $u \lhd v \in \mathbb{A}_*$. Then w is an $\mathfrak{e}, k$-approximation for $a(u)$.*

Proof. Let $u \lhd v \in \mathbb{A}_*$, $a(x) \in \mathcal{T}(\mathcal{F}_*, x)$, and w be an $\mathfrak{e}, k$-approximation for $a(v)$. We only consider the case that $a(x) = x$. Then w is an $\mathfrak{e}, k$-approximation for $v \in \mathbb{A}_*$. Observation 4.7 ii) yields $v \lhd w$, thus $u \lhd w$ by transitivity of $\lhd$. Furthermore, $w \in \mathbb{A}_*$ and $\mathrm{dp}(w) \leq k$, hence by Observation 4.7 i) w is a $\langle\rangle, k$-approximation for u. With Observation 4.7 vi) this yields that w is an $\mathfrak{e}, k$-approximation for u. $\square$

As explained before the next proposition is central for our investigation. It shows that S^1_2 can prove the correctness of our approximations, i.e. that several approximations for the same term are comparable.

Proposition 4.11 (S^1_2) *Assume that $\mathfrak{e}$ is a k-evidence, and v, w are $\mathfrak{e}, k$-approximations for $t \in \mathcal{T}(\mathcal{F}_*)$. Then $v \lhd w$ or $w \lhd v$.*

Proof. Fix some k-evidence $\mathfrak{e}$ and some term $t \in \mathcal{T}(\mathcal{F}_*, X)$.

Define $a \in \mathit{Sub}(t, \mathfrak{e})$ iff a is a subterm of t, or there are $i < \mathrm{l}(\mathfrak{e})$ and $\mathrm{c} \in \mathcal{C}$ such that for $f := (\mathfrak{e})_{i0}$, which must be in $\mathcal{F}$ by definition of evidence, a is a subterm of t^{c}_f.

In order to get the induction through we have to prove a slightly more general assertion. We prove by main induction on $l \leq \mathrm{l}(\mathfrak{e})$ and side induction on the definition of $a(\vec{x}) \in Sub(t, \mathfrak{e})$ as a term – assuming that a only contains the variables $x_1, \ldots, x_n$ – that for all general numerals $v, v_1, \ldots, v_n, w, w_1, \ldots, w_n \leq \mathrm{B}_{\mathbb{A}_*}(k)$, if

$$\forall i = 1, \ldots, n \quad [v_i \lhd w_i \text{ or } w_i \lhd v_i],$$

v is an $(\mathfrak{e} \restriction l), k$-approximation for $a_{\vec{x}}(\vec{v})$, and w is an $(\mathfrak{e} \restriction l), k$-approximation for $a_{\vec{x}}(\vec{w})$, then $v \lhd w$ or $w \lhd v$.

Let $l \leq \mathrm{l}(\mathfrak{e})$, $a(\vec{x}) \in Sub(t, \mathfrak{e})$, and $v, w, \vec{v}, \vec{w} \leq \mathrm{B}_{\mathbb{A}_*}(k)$ with

$$\forall i = 1, \ldots, n[v_i \lhd w_i \text{ or } w_i \lhd v_i], \tag{2}$$

$$v \text{ is an } (\mathfrak{e} \restriction l), k\text{-approximation for } a(\vec{v}), \text{ and} \tag{3}$$

$$w \text{ is an } (\mathfrak{e} \restriction l), k\text{-approximation for } a(\vec{w}) \tag{4}$$

If $v = *$ or $w = *$ we are done. So let us assume that this is not the case. By Observation 4.3 ii) it suffices to find some u with $u \lhd v$ and $u \lhd w$.

If $a = \mathrm{c} \in \mathcal{C}_*$ and $\mathrm{ar}(c) = 0$, then $\mathrm{c} \lhd v$ and $\mathrm{c} \lhd w$ by Observation 4.7 ii) applied to assumptions (3), (4), hence we are done.

Assume $a(\vec{x}) = x_i$. W.l.o.g. we assume $v_i \lhd w_i$. Now (3) says that v is an $\mathfrak{e}, k$-approximation for $v_i \in \mathbb{A}_*$, hence Observation 4.7 ii) yields $v_i \lhd v$. Similarly we obtain from (4) $w_i \lhd w$. Hence $v_i \lhd w_i \lhd w$ and $v_i \lhd v$, and we are done.

Finally assume $a(\vec{x}) = f a_1(\vec{x}) \ldots a_m(\vec{x})$, $m > 0$. By assumption $v \neq * \neq w$, hence (3) and (4) yield some $u_1, \ldots, u_m, u'_1, \ldots, u'_m \leq \mathrm{B}_{\mathbb{A}_*}(k)$ such that

$$\begin{aligned} &u_j \text{ is an } (\mathfrak{e} \restriction l), k\text{-approximation for } a_j(\vec{v}) \\ &u'_j \text{ is an } (\mathfrak{e} \restriction l), k\text{-approximation for } a_j(\vec{w}) \end{aligned} \tag{5}$$

for $j = 1, \ldots, m$. As a_j is a subterm of $a \in Sub(t, \mathfrak{e})$, we have $a_j \in Sub(t, \mathfrak{e})$. This, (5), (2) and the side induction hypothesis yields

$$\forall j = 1, \ldots, m\, [u_j \lhd u'_j \text{ or } u'_j \lhd u_j]. \tag{6}$$

W.l.o.g. we assume $u_1 \lhd u'_1$.

In case $f \in \mathcal{C}_*$ with $\mathrm{ar}(f) = 1$, assumptions (3) and (4) show $f u_1 \lhd v$ and $f u'_1 \lhd w$, hence $f u_1 \lhd f u'_1 \lhd w$ and $f u_1 \lhd v$, and we are done.

Otherwise $f \notin \mathcal{C}_*$, hence (3) and (4) produce some $u \lhd v$ and $u' \lhd w$ such that

$$\langle f, \vec{u}, u \rangle, \langle f, \vec{u}', u' \rangle \in (\mathfrak{e} \restriction l). \tag{7}$$

In particular $l > 0$. The definition of an evidence shows that $u_1 = \mathrm{c}(\tilde{u}_1)$, $u'_1 = \mathrm{c}'(\tilde{u}'_1)$, for some $\mathrm{c}, \mathrm{c}' \in \mathcal{C}$, and

$$u \text{ is an } (\mathfrak{e} \restriction (l-1)), k\text{-approximation for } t_f^{\mathrm{c}}(\tilde{u}_1, u_2, \ldots, u_m) \tag{8}$$

$$u' \text{ is an } (\mathfrak{e} \restriction (l-1)), k\text{-approximation for } t_f^{\mathrm{c}'}(\tilde{u}'_1, u'_2, \ldots, u'_m) \tag{9}$$

As $u_1 \lhd u_1'$ we get $\mathrm{c} = \mathrm{c}'$ and $\tilde{u}_1 \lhd \tilde{u}_1'$, thus (9) can be rewritten as

$$u' \text{ is an } (\mathfrak{e} \restriction (l-1)), k\text{-approximation for } t_f^{\mathrm{c}}(\tilde{u}_1', u_2', \ldots, u_m') \tag{10}$$

Furthermore, $f = (\mathfrak{e})_{i0}$ for some $i < \mathrm{l}(\mathfrak{e})$, hence $t_f^{\mathrm{c}} \in Sub(t, \mathfrak{e})$. With (6), (8), (10) we can apply the main induction hypothesis obtaining $u \lhd u'$ or $u' \lhd u$. W.l.o.g. assume $u \lhd u'$, hence $u \lhd u' \lhd w$ and $u \lhd v$, thus we are done.

Concerning formalizability let $B_{t,\mathfrak{e}}$ be $\max(t, \mathrm{SqBd}(\mathfrak{e}, \mathfrak{e}))$. Then, by definition of a nice set of recursive axioms,

$$a \in Sub(t, \mathfrak{e}) \quad \Rightarrow \quad \ulcorner a \urcorner \leq B_{t,\mathfrak{e}} \tag{11}$$

This is clear if a is a subterm of t, because then $\ulcorner a \urcorner \leq \ulcorner t \urcorner$. Otherwise there are $i < \mathrm{l}(\mathfrak{e})$ and $\mathrm{c} \in \mathcal{C}$ such that $f := (\mathfrak{e})_{i0} \in \mathcal{F}$ and a is a subterm of t_f^{c}. By the definition of a nice set of recursive axioms, there is some $\tilde{t}(\star)$ with $\ulcorner \tilde{t}(\star) \urcorner \leq \ulcorner f \urcorner \leq \mathfrak{e}$ and $t_f^{\mathrm{c}} = \tilde{t}(f)$. Hence

$$\ulcorner t_f^{\mathrm{c}} \urcorner = \ulcorner \tilde{t}(\star) \urcorner_\star (\ulcorner f \urcorner) \leq \mathrm{SqBd}(\ulcorner f \urcorner, \ulcorner f \urcorner) \leq B_{t,\mathfrak{e}}.$$

Using (11) we see that the main and the side induction formulas are Π_1^b, hence this kind of Π_1^b-<-length-induction, which is equivalent to Σ_1^b-LMin, is available in S_2^1. $\square$

In the next Lemma we show a kind of converse of Lemma 4.8, i.e. that the approximations have a certain decomposition property.

Lemma 4.12 (S_2^1) *Assume that $\mathfrak{e}$ is a k-evidence, and w is an $\mathfrak{e}, k$-approximation for $t(b_1, \ldots, b_m) \in \mathcal{T}(\mathcal{F}_*)$. Then there are $w_1, \ldots, w_m$, such that w_j is an $\mathfrak{e}, k$-approximations for b_j, for $j = 1, \ldots, m$, and w is an $\mathfrak{e}, k$-approximation for $t(\vec{w})$.*

Proof. Let $\mathfrak{e}$ be a k-evidence and $b_1, \ldots, b_m \in \mathcal{T}(\mathcal{F}_*)$. We prove the assertion by induction on the definition of the term $t(\vec{x}) \in \mathcal{T}(\mathcal{F}_*, \vec{x})$.

If $w = *$ or $t \in \mathcal{C}_*$ we are done. So let us assume that this is not the case.

In case $t(\vec{x}) = x_i$ we have that w is an $\mathfrak{e}, k$-approximation for b_i. Let w_i be w, and w_j be $*$ for $j \neq i$. Then w_j is an $\mathfrak{e}, k$-approximation for b_j, for $j = 1, \ldots, m$, and w is an $\mathfrak{e}, k$-approximation for $w = t(\vec{w})$.

Finally assume $t(\vec{x}) = f t_1(\vec{x}) \ldots t_n(\vec{x})$. As $w \neq *$ and w is an $\mathfrak{e}, k$-approximation for $t(\vec{b})$, there are $v_1, \ldots, v_n \leq \mathrm{B}_{\mathbb{A}_*}(k)$ such that v_j is an $\mathfrak{e}, k$-approximation for $t_j(\vec{b})$, for $j = 1, \ldots, n$. By induction hypothesis there are $w_i^1, \ldots, w_i^n$ being $\mathfrak{e}, k$-approximations for b_i, for $i = 1, \ldots, m$, such that v_j is an $\mathfrak{e}, k$-approximation for $t_j(\vec{w}^j)$, for $j = 1, \ldots, n$. Using Proposition 4.11 we can choose $w_i \in \{w_i^1, \ldots, w_i^n\}$ which is minimal with respect to $\lhd$, $i = 1, \ldots, m$. Then Lemma 4.10 shows that v_j is an $\mathfrak{e}, k$-approximation for $t_j(\vec{w})$, for $j = 1, \ldots, n$. As in the proof of Lemma 4.8 the same reason for w being an $\mathfrak{e}, k$-approximation for $t(\vec{b})$ now shows w is an $\mathfrak{e}, k$-approximation for $t(\vec{w})$. $\square$

Theorem 4.13 (S^1_2) *Assume that* $\mathfrak{e}$ *is a* k*-evidence,* w *is an* $\mathfrak{e}, k$*-approximation for* t*, and* $t' \longrightarrow^1_{Ax} t$*. Then there are* $\ulcorner f \urcorner \leq \ulcorner t' \urcorner$*,* $\vec{v}, v \leq \mathrm{B}_{\mathbb{A}_*}(k+1)$ *such that* $\mathfrak{e}' := \mathfrak{e}^\frown\langle\langle f, \vec{v}, v\rangle\rangle$ *is a* $(k+1)$*-evidence, and* w *is an* $\mathfrak{e}', (k+1)$*-approximation for* t'*.*

Proof. Let $\mathfrak{e}$ be a k-evidence, $f \in \mathcal{F} \setminus \mathcal{C}$, $\mathrm{c} \in \mathcal{C}$ and $b, c_1, \dots, c_m \in \mathcal{T}(\mathcal{F}_*)$, $a(x) \in \mathcal{T}(\mathcal{F}_*, x)$. Furthermore, let w be an $\mathfrak{e}, k$-approximation for $a(t^{\mathrm{c}}_f(b, \vec{c}))$. We will construct an evidence $\mathfrak{e}'$ as claimed above such that w is an $\mathfrak{e}', (k+1)$-approximation for $a(f\,\mathrm{c}(b)\vec{c})$. This proves the Theorem.

The proof proceeds in several steps.

i) By Lemma 4.12 there is some v being an $\mathfrak{e}, k$-approximation for $t^{\mathrm{c}}_f(b, \vec{c})$, such that w is an $\mathfrak{e}, k$-approximation for $a(v)$. In particular $v \leq \mathrm{B}_{\mathbb{A}_*}(k)$.

ii) Again by Lemma 4.12 there are some $w_b, \vec{w}_c$ with w_b being an $\mathfrak{e}, k$-approximation for b and w_{c_i} being an $\mathfrak{e}, k$-approximation for c_i, for $i = 1, \dots, m$, and v being an $\mathfrak{e}, k$-approximation for $t^{\mathrm{c}}_f(w_b, \vec{w}_c)$.

iii) Let $\mathfrak{e}' := \mathfrak{e}^\frown\langle\langle f, \mathrm{c}(w_b), \vec{w}_c, v\rangle\rangle$, then $\mathfrak{e}'$ is a $(k+1)$-evidence, because $\mathrm{dp}(\mathrm{c}(w_b)) = \mathrm{dp}(w_b) + 1 \leq k + 1$, and by ii). This also implies $\mathrm{c}(w_b) \leq \mathrm{B}_{\mathbb{A}_*}(k+1)$.

iv) By the definition of $\mathfrak{e}'$ and ii) we immediately have that v is an $\mathfrak{e}', (k+1)$-approximation for $f\,\mathrm{c}(b)\vec{c}$.

v) From i) and Observation 4.7 vi) we obtain that w is an $\mathfrak{e}', (k+1)$-approximation for $a(v)$, hence with iv) and Lemma 4.8 we obtain w is an $\mathfrak{e}', (k+1)$-approximation for $a(f\,\mathrm{c}(b)\vec{c})$. □

This finishes the second (and last) part of our general plan. Now we put Theorem 4.9 together with the last one obtaining the main result of this section.

Theorem 4.14 (S^1_2) *Assume* $v, w \in \mathbb{A}_*$ *and* $v \longleftrightarrow^*_{Ax} w$*, then* $v = w$*.*

Proof. Assume $v, w \in \mathbb{A}_*$ and $v \longleftrightarrow^*_{Ax} w$. Let σ be the path from v to w. I.e., σ is a sequence, where the first element of σ is v, the last one is w, and two successive elements u, u' of σ fulfill $u \longleftrightarrow^1_{Ax} u'$. Let d be the depth of v. We prove that there exists some $\mathfrak{e}$ such that

$$\mathrm{l}(\mathfrak{e}) \leq j, \quad \mathrm{maxel}(\mathfrak{e}) \leq \mathrm{SqBd}(\sigma\restriction_{j+1}, \sigma\restriction_{j+1} + \mathrm{B}_{\mathbb{A}_*}(d+j)),$$
$$\mathfrak{e} \text{ is a } (d+j)\text{-evidence} \quad \text{and} \quad v \text{ is an } \mathfrak{e}, (d+j)\text{-approximation for } (\sigma)_j$$

by induction on $j < \mathrm{l}(\sigma)$. This induction is an application of Σ^b_1-LIND, because $\mathfrak{e}$ can obviously be bounded by $\mathrm{SqBd}(\sigma, \mathrm{SqBd}(\sigma, \sigma + \mathrm{B}_{\mathbb{A}_*}(d + \mathrm{l}(\sigma))))$.

If $j = 0$ let $\mathfrak{e} := \langle\rangle$ and the assertion is obvious as $(\sigma)_0 = v$.

Now assume $j + 1 < \mathrm{l}(\sigma)$ and by induction hypothesis there is some $\mathfrak{e}$ such that $\mathrm{l}(\mathfrak{e}) \leq j$, $\mathrm{maxel}(\mathfrak{e}) \leq \mathrm{SqBd}(\sigma\restriction_{j+1}, \sigma\restriction_{j+1} + \mathrm{B}_{\mathbb{A}_*}(d+j))$, $\mathfrak{e}$ is a $(d+j)$-evidence and v is an $\mathfrak{e}, (d+j)$-approximation for $(\sigma)_j$.

If $(\sigma)_j \longrightarrow^1_{Ax} (\sigma)_{j+1}$, then $\mathfrak{e}$ is also a $(d+j+1)$-evidence and Theorem 4.9 yields that v is an $\mathfrak{e},(d+j+1)$-approximation for $(\sigma)_{j+1}$.

Otherwise $(\sigma)_{j+1} \longrightarrow^1_{Ax} (\sigma)_j$. By Theorem 4.13 there are $f \leq (\sigma)_{j+1}$, $\vec{u}, u \leq \mathrm{B}_{\mathbb{A}_*}(d+j+1)$ such that $\mathfrak{e}' := \mathfrak{e}^\frown\langle\langle f,\vec{u},u\rangle\rangle$ is a $(d+j+1)$-evidence and v is an $\mathfrak{e}',(d+j+1)$-approximation for $(\sigma)_{j+1}$. Furthermore $\mathrm{l}(\mathfrak{e}') \leq \mathrm{l}(\mathfrak{e})+1 \leq j+1$ and

$$\langle f,\vec{u},u\rangle \leq \mathrm{SqBd}((\sigma)_{j+1},(\sigma)_{j+1}+\mathrm{B}_{\mathbb{A}_*}(d+j+1)),$$

hence the assertion follows.

Thus there is some $\mathfrak{e}$ such that v is an $\mathfrak{e},(d+\mathrm{l}(\sigma))$-approximation for w, thus $w \lhd v$ by Observation 4.7 ii). Similarly we obtain $v \lhd w$. Hence $v = w$ by Observation 4.3 iii). $\square$

***Proof* of the Main Theorem 2.5.** We argue in S^1_2. Let Ax be a nice set of recursive axioms and assume $\mathrm{Prf}_{\mathrm{EqT}(Ax)}(\pi,\ulcorner 0=1\urcorner)$. By Theorem 3.2 we obtain that $0 \longleftrightarrow^*_{Ax} 1$. But then Theorem 4.14 yields $0=1$, a contradiction. $\square$

Remark 4.15 *The consistency notion used in our results bases on treelike proofs. It is open whether the results still hold when considering daglike proofs, i.e. proofs coded as directed acyclic graphs. However, the proofs of Theorems 3.2 and 4.14 indicate that we can allow terms to be represented as dags.*

References

[1] Arnold Beckmann and Andreas Weiermann. A term rewriting characterization of the polytime functions and related complexity classes. *Arch. Math. Logic*, 36:11–30, 1996.

[2] Buss, Samuel R.: *Bounded arithmetic.* Studies in Proof Theory. Lecture Notes, 3. Bibliopolis, Naples, 1986.

[3] Buss, Samuel R.; Ignjatovič, Aleksandar: *Unprovability of consistency statements in fragments of bounded arithmetic.* Ann. Pure Appl. Logic 74 (1995), no. 3, 221–244.

[4] E. A. Cichon and A. Weiermann. Term rewriting theory for the primitive recursive functions. *Ann. Pure Appl. Logic*, 83(3):199–223, 1997.

[5] Clote, Peter; Krajíček, Jan: Open problems, in: *Arithmetic, proof theory, and computational complexity.* Papers from the conference held in Prague, July 2–5, 1991. Edited by Peter Clote and Jan Krajíček, pp. 1–9. Oxford Logic Guides, 23. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1993.

[6] Cook, Stephen A.: *Feasibly constructive proofs and the propositional calculus.* Seventh Annual ACM Symposium on Theory of Computing (Albuquerque, N.M., 1975), pp. 83–97. Assoc. Comput. Mach., New York, 1975.

[7] Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In Jan van Leeuwen, editor, *Handbook of theoretical computer science. Vol. B*, pages 243–320. Elsevier Science Publishers, Amsterdam, 1990. Formal models and semantics.

[8] Krajíček, Jan: *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Cambridge University Press, Heidelberg/New York, 1995.

[9] Pavel Pudlák. A note on bounded arithmetic. *Fund. Math.*, 136(2):85–89, 1990.

[10] Andreas Weiermann. Termination proofs for term rewriting systems with lexicographic path orderings imply multiply recursive derivation lengths. *Theoret. Comput. Sci.*, 139:355–362, 1995.

[11] Alex J. Wilkie and Jeff B. Paris. On the scheme of induction for bounded arithmetic formulas. *Ann. Pure Appl. Logic*, pages 261–302, 1987.