ON PROVING CONSISTENCY OF EQUATIONAL THEORIES IN BOUNDED ARITHMETIC

ARNOLD BECKMANN AND YORIYUKI YAMAGATA

August 23, 2022

ABSTRACT. We consider pure equational theories that allow substitution but disallow induction, which we denote as **PETS**, based on recursive definition of their function symbols. We show that the Bounded Arithmetic theory S_2^1 proves the consistency of **PETS**. Our approach employs models for **PETS** based on approximate values resembling notions from domain theory in Bounded Arithmetic, which may be of independent interest.

1. INTRODUCTION

The question whether the hierarchy of Bounded Arithmetic theories is strict or not, is an important open problem due to its connections to corresponding questions about levels of the Polynomial Time Hierarchy [2]. One obvious route to address this problem is to make use of Gödel's 2nd Incompleteness Theorem, using statements expressing consistency for Bounded Arithmetic theories. Early lines of research aimed to restrict the formulation of consistency suitably to achieve this aim [2, 8].

One particular programme is to consider consistency statements based on equational theories. Buss and Ignjatović [4] have shown that the consistency of an induction free version of Cook's equational theory PV [5] is not provable in S_2^1, where S_2^1 is the Bounded Arithmetic theory related to polynomial time reasoning. Their version of induction free PV is formulated in a system that allows, in addition to equations, also inequalities between terms, and Boolean formulas. Furthermore, a number of properties have been stated as axioms.

On the other hand, in a pure equational setting, where lines in derivations are equations between terms, axioms are restricted to recursive definition of function symbols, and induction is not allowed, consistency becomes provable in Bounded Arithmetic: The first author has shown in [1] that the consistency of pure equational theories, in which substitution is not allowed, is provable in S_2^1 – in particular this result applies to Cook's PV [5] without substitution and induction. The second author of this paper has improved on this result in [9] by showing that the consistency of PV without induction but with substitution is provable in S_2^2, the second level of the hierarchy of Bounded Arithmetic theories.

In this paper, we extend both our previous results [1, 9]. With **PETS**(Ax) we denote the pure equational theory with substitution but without induction, based on some nice set of axioms Ax – Cook's original PV [5] without induction but with substitution is one example of such a theory. The main aim of this paper is to show that the consistency of **PETS**(Ax) is provable in S_2^1, thus improving on both [1, 9]. To this end we employ a novel method of defining models in Bounded Arithmetic based on approximate values, which may be of independent interest. Our approach

1

resembles elements from domain theory, however we leave a full treatment of domain theory in Bounded Arithmetic to future research.

In the next section, we briefly introduce Bounded Arithmetic and fix some notions used throughout the paper. In Section 3 we define pure equational theories **PETS**(Ax), which will be more general than PV without induction in that arbitrary recursive functions may be considered. This is followed in Section 4 by an introduction of approximate values and semantics based on approximation, leading to feasible evaluations of terms based on such approximation semantics. Section 5 then defines models for equational theories based on approximation semantics, including a suitably restricted version which can be expressed as a bounded formula and used in induction arguments inside Bounded Arithmetic. A key notion will be a way of updating such models with further information about approximate values of functions, in a way that preserves the notion of being a model, provably in S_2^1. In Section 6 we prove our first main theorem showing a form of soundness for **PETS**(Ax) based on approximation semantics in S_2^2– an immediate consequence will be that S_2^2 proves the consistency of **PETS**(Ax). The final sections improve on this approach to obtain proofs in S_2^1: In Section 7 we introduce instructions that allow to encode sequences of terms and operations on them, which are extracted from derivations in **PETS**(Ax). In this way we obtain an explicit way of describing model constructions related to **PETS**(Ax) derivations, which allows us to reduce the bounded quantifier complexity of induction assertion in the proof of our second main theorem in Section 8 to show an improved soundness property for **PETS**(Ax) provable in S_2^1.

2. BOUNDED ARITHMETIC

2.1. **Language of Bounded Arithmetic.** We give a brief introduction to Bounded Arithmetic to support the developments in this paper. For more in depth discussions and results we refer the interested reader to the literature [2, 6]. Theories of Bounded Arithmetic are first order theories of arithmetic similar to Peano Arithmetic, their domain of discourse are the non-negative integers. For the purpose of this paper we can assume that the language of Bounded Arithmetic contains a symbol for each polynomial time computable function, including 0, 1, $+$, $\cdot$, $|.|$, $\#$, representing zero, one, addition, multiplication, the binary length function $|x|$ that computes the number of bits in a binary representation of x and can be defined by $|x| = \lceil \log_2(x+1) \rceil$, and smash $\#$ computing $x \# y = 2^{|x| \cdot |y|}$.

2.2. **Theories of Bounded Arithmetic.** Theories of Bounded Arithmetic contain suitable defining axioms for its function symbols. The main differentiator are various forms of induction for various classes of bounded formulas, which we will define next.

Bounded quantifiers are defined as follows:

$$(\forall x \leq t)A \quad \text{abbreviates} \quad (\forall x)(x \leq t \rightarrow A)$$
$$(\exists x \leq t)A \quad \text{abbreviates} \quad (\exists x)(x \leq t \wedge A)$$

If the bounding term t of a bounded quantifier is of the form $|t'|$, then the quantifier is called *sharply bounded*.

Classes of bounded formulas Σ_i^b and Π_i^b are defined in [2] by essentially counting alternations between existential and universal bounded quantifiers. Predicates defined by Σ_i^b and Π_i^b formulas define computational problems in corresponding

classes of the Polynomial Time Hierarchy of decision problems Σ_i^{p} and Π_i^{p}, respectively. For example, those defined by Σ_1^{b} correspond exactly to NP.

In particular, the Σ_i^{b} and Π_i^{b} classes include the following formulas:

- $\Sigma_0^{\mathrm{b}} = \Pi_0^{\mathrm{b}}$ is the class of formulas build from atomic formulas and closed under Boolean connectives and sharply bounded quantification.
- $\Sigma_{i+1}^{\mathrm{b}}$ includes all formulas of the form $(\exists x \leq t)A$ with $A \in \Pi_i^{\mathrm{b}}$.
- Π_{i+1}^{b} includes all formulas of the form $(\forall x \leq t)A$ with $A \in \Sigma_i^{\mathrm{b}}$.

The theories S_2^i, $i \geq 0$, of Bounded Arithmetic have been defined in [2], establishing a close relationship between fragments of Bounded Arithmetic and levels of the Polynomial Time Hierarchy of functions. More precisely, the $\Sigma_{i+1}^{\mathrm{b}}$-definable functions of S_2^{i+1}, that is the functions whose graph can be described by a $\Sigma_{i+1}^{\mathrm{b}}$ formula, and whose totality is provable in S_2^{i+1}, form exactly the $i+1$-st level of the Polynomial Time Hierarchy of functions, $\mathrm{FP}^{\Sigma_i^{\mathrm{p}}}$.

Instead of defining the theory S_2^i, we state some characteristic properties about induction provable in them. Let $\Sigma_i^{\mathrm{b}}{-}\mathrm{IND}$ be the schema of induction for Σ_i^{b}-properties, consisting of formulas of the form

$$A(0) \wedge (\forall x)(A(x) \to A(x+1)) \to (\forall x)A(x)$$

for $A \in \Sigma_i^{\mathrm{b}}$. The schema of *logarithmic induction* $\Sigma_i^{\mathrm{b}}{-}\mathrm{LIND}$ is then obtained by restricting the conclusion of induction to logarithmic values, that is

$$A(0) \wedge (\forall x)(A(x) \to A(x+1)) \to (\forall x)A(|x|)$$

for $A \in \Sigma_i^{\mathrm{b}}$. We have the following:

Theorem 1 ([2]). *The instances of $\Sigma_i^{\mathrm{b}}{-}\mathrm{LIND}$ and $\Pi_i^{\mathrm{b}}{-}\mathrm{LIND}$ are provable in S_2^i.*

We already mentioned the intricate relationship between Bounded Arithmetic theories and the Polynomial Time Hierarchy in terms of definable functions. Furthermore, it is know that a collapse of the hierarchy of Bounded Arithmetic theories is equivalent to a collapse of the Polynomial Time Hierarchy, provable in Bounded Arithmetic [3,7,10]; With T_2^i denoting the theory $\Sigma_i^{\mathrm{b}}{-}\mathrm{IND}$ we have that $\mathrm{T}_2^i = \mathrm{S}_2^{i+1}$ is equivalent to $\Sigma_{i+1}^{\mathrm{p}} \subseteq \Pi_{i+1}^{\mathrm{p}}/poly$ provable in T_2^i.

The Bounded Arithmetic theory S_2^1 is able to formalize meta-mathematics and essential constructions to prove Gödel's Incompleteness Theorems [2]. A basis for such formalization is a feasible encoding of sequences of numbers. For this paper we assume that a suitable encoding of sequences and operations on them can be formalized in S_2^1 as done in [2]. We assume the following notation:

- With $\langle x_1, \ldots, x_k \rangle$ we denote the encoding of sequence $x_1, \ldots, x_k$. We will use σ, τ etc to range over sequence encodings.
- With ' :: ' we denote concatenation of sequences:

$$\langle x_1, \ldots, x_k \rangle :: \langle x_{k+1}, \ldots, x_{k+\ell} \rangle \quad = \quad \langle x_1, \ldots, x_k, x_{k+1}, \ldots, x_{k+\ell} \rangle$$

- With ' : ' we denote the function that adds an element to the left or right of a sequence:

$$x : \sigma \quad = \quad \langle x \rangle :: \sigma$$
$$\sigma : x \quad = \quad \sigma :: \langle x \rangle$$

The predicate 'being a sequence encoding', as well as the operations ' : ' and ' :: ', can be defined in S_2^1 with their usual properties proven.

In the following we will concentrate on bounding the number of symbols in transformations and constructions. For an object o we will define its length $\mathbf{l}(o)$ to be the number of symbols occurring in o. As all our constructions will happen in the context of a given derivation $\mathcal{D}$, we obtain that the size of the Gödelization of object o can then be bounded by $\mathbf{l}(o)$ times the size of the Gödelization of $\mathcal{D}$.

Furthermore, the constructions for defining o in the context of $\mathcal{D}$ will always be explicit and simple enough to be formalizable in S_2^1, similar to constructions in [2] dealing with meta-mathematical notions. In those cases where more involved induction is needed (as in Theorems 40 and 51) these will be analyzed carefully.

2.3. **Notations.** In the remaining part of this section we will fix some notation used throughout this paper. We use $\equiv$ for equality of syntax.

- With $\#S$ we denote the cardinality of a set S.
- For a function f, $\mathrm{dom}(f)$ denotes its domain, $\mathrm{rng}(f)$ its range.
- We will use the abbreviation $\bar{x}$ for a sequence $x_1, \ldots, x_n$ of objects.
- For a set X, tuples in X^n are denoted with $(x_1, \ldots, x_n)$.
- $\max(X)$ computes the maximum (according to a given order) of the elements in X. $\max$ is applied to a tuple by computing the maximal component in it.

Tuples and sequences. Technically, there is a difference between a tuple of the form $(s_1, \ldots, s_n)$, which is an element of S^n, and the sequence $s_1, \ldots, s_n$, which is a formal list used e.g. as the arguments to an n-ary function. We will identify both and write $s \in S^n$ and $f(s)$ in the same context, as long as it does not lead to confusion, in which case we will choose a more precise differentiation.

3. Equational Theories

3.1. **Domain of discourse.** The intended domain of discourse $\mathbb{B}$ will be binary strings representing numbers. $\mathbb{B}$ can be defined inductively as follows:

$$v ::= \epsilon \mid v0 \mid v1$$

We will also use terms denoting binary strings, which are formed from constant ϵ using unary function symbols s_0 and s_1 to add a single digit to the right of a string. We also use $t0$ to denote $\mathrm{s}_0(t)$, and $t1$ for $\mathrm{s}_1(t)$ for terms t.

Remark. Our results are not restricted to binary strings, but can be applied to general free algebras as domains of discourse as done in [1]. However, for sake of simplicity we will only consider binary strings in this paper.

3.2. **Terms.** We fix the language we use for equational theories.

Definition 2 (Language for Equational Theories)**.** We have the following basic ingredients:

- A countable set $\mathcal{X}$ of *variables;* we use $x, y, x_1, x_2, \ldots$ to denote variables.
- A countable set $\mathcal{F}$ of *function symbols;* we use $f, g, h, f_1, f_2, \ldots$ to denote function symbols. Each function $f \in \mathcal{F}$ comes with a non-negative integer $\mathrm{ar}(f)$ called its *arity*. We assume that ϵ, s_0 and s_1 are included in $\mathcal{F}$; ϵ, s_0 and s_1 form the set $\mathcal{B}$ of *basic function symbols*.

Remark. A function with arity 0 is called a *constant.* For example, ϵ is a constant.

Definition 3 (Terms). Let $X \subseteq \mathcal{X}$ and $F \subseteq \mathcal{F}$. The set $\mathcal{T}(X, F)$ of *terms over F and X*, or simply *terms*, is defined inductively as follows:

- All variables in X are terms.
- If $f \in F$ has arity n and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

We will use s, t, u to denote terms.

The *length* $\mathbf{l}(t)$ *of term t* is defined in the following way: The length of a variable is 1, and, recursively,

$$\mathbf{l}(f(t_1, \ldots, t_n)) = \mathbf{l}(t_1) + \cdots + \mathbf{l}(t_n) + 1 \ .$$

With $\mathrm{Var}(t)$ we denote the *set of variables* that are occurring in a term t.

Definition 4 (Substitution). Let t, u be terms and x be a variable. The *substitution of u for x in t*, denoted $t[u/x]$, is obtained by replacing any occurrence of x in t by u.

We extend substitution to sequences of variables and terms of the same length by successively substituting terms: $t[\overline{u}/\overline{x}]$ stands for $t[u_1/x_1][u_2/x_2] \ldots [u_n/x_n]$.

Definition 5 (Instance). A *substitution instance*, or *instance*, of an equation $s = t$ is any $s[\overline{u}/\overline{x}] = t[\overline{u}/\overline{x}]$ for sequences of variables $\overline{x}$ and terms $\overline{u}$ of the same length.

3.3. **Nice axiom systems.** We will consider axioms consisting of equations that satisfy particular conditions, which have been called *nice* in [1].

Definition 6 (Axioms). Let Ax be a *set of nice axioms for $\mathcal{F}$*. That is, each equation in Ax must be of one of the following forms, for some $f \in \mathcal{F} \setminus \mathcal{B}$, some $t, t_\epsilon \in \mathcal{T}(\mathcal{F}, \{\overline{x}\})$, and $t_0, t_1 \in \mathcal{T}(\mathcal{F}, \{x, \overline{x}\})$:

$$f(\overline{x}) = t$$
$$f(\epsilon, \overline{x}) = t_\epsilon$$
$$f(x0, \overline{x}) = t_0$$
$$f(x1, \overline{x}) = t_1.$$

Furthermore, the left-hand side of an equation is occurring at most once among equations in Ax, also modulo substitution.

Remark. The definition implies that for any $t = u$ in Ax we have $\mathrm{Var}(u) \subseteq \mathrm{Var}(t)$.

Remark. Consider a term $f(\overline{t})$ with $f \in \mathcal{F} \setminus \mathcal{B}$. The property of Ax being nice implies that there is at most one axiom $t = u$ in Ax such that $f(\overline{t})$ can be written as a substitution instance of t.

Remark. The definition of a nice axiom system in [1] also contains a completeness condition, requiring that each function symbol in $\mathcal{F} \setminus \mathcal{B}$ is defined by an equation, and that the case distinction in the latter part is complete. We omit this form of completeness, as it is not needed for our developments.

The left-hand side of an equation in Ax is of a very special form: an argument to the out-most function symbol can either be a variable, ϵ, or $\mathrm{s}_i(x)$ for some variable x. We capture these forms in the following definition.

Definition 7 (Generalized variable). A *generalized variable* is a term which either is a variable, or ϵ, or of the form $\mathrm{s}_i(x)$ for some variable x.

Remark. Consider an axiom $t = u$ in Ax. It follows that t must be of the form $f(\bar{t})$, that each t_i is a generalized variable, hence each t_i contains at most one variable. Furthermore, the same variable cannot occur simultaneously in t_i and t_j for $i \neq j$.

Definition 8 (Rules for equational reasoning)**.** Let $s, t, u, s_1, \ldots, s_n, t_1, \ldots, t_n$ be terms. The following are the rules that can be used to derive equations:

> **Axiom:** $\vdash t = u$, where $t = u$ is an instance of an equation in Ax.
> **Reflexivity:** $\vdash t = t$
> **Symmetry:** $t = u \vdash u = t$
> **Transitivity:** $t = s, s = u \vdash t = u$
> **Compatibility:** $t = u \vdash s[t/x] = s[u/x]$
> **Substitution:** $t = u \vdash t[s/x] = u[s/x]$.

In the case of Substitution as stated above, we say that the application of Substitution binds the variable x.

Remark. We also make use of a display style for presenting rules, like

$$\frac{}{t = t}$$

for Reflexivity Rule, or

$$\frac{t = s \qquad s = u}{t = u}$$

for Transitivity Rule.

Definition 9 (Derivations)**.** A *derivation* is a finite tree whose nodes are labelled with instances of rules for equational reasoning, such that for each node, the premises of the rule at that node coincide with the conclusions of rules at corresponding child nodes.

Derivations can also be defined inductively from rules for equational reasoning: Any instance of an Axiom or Reflexivity Rule is a derivation ending in the equation given by that rule. If R is a unary rule (like Symmetry, Compatibility or Substitution) with premise e' and conclusion e, and $\mathcal{D}'$ a derivation ending in e', then

$$R \, \frac{\overset{\mathcal{D}'}{e'}}{e}$$

is a derivation ending in e. The only binary rule we are considering is the Transitivity Rule. If $\mathcal{D}_1$ a derivation ending in $t = s$, and $\mathcal{D}_2$ a derivation ending in $s = u$, then

$$\text{Transitivity} \, \frac{\overset{\mathcal{D}_1}{t = s} \qquad \overset{\mathcal{D}_2}{s = u}}{t = u}$$

is a derivation ending in $t = u$.

The *length* $\mathbf{l}(\mathcal{D})$ *of a derivation* $\mathcal{D}$ is defined as the sum of the lengths of the equations occurring in it, plus the length of any additional syntax needed to identify applications of rules — for example, for an application of Substitution $t = u \vdash t[s/x] = u[s/x]$ we add $\mathbf{l}(t, s, x, u, s, x)$ to avoid complications in cases where x is not occurring in t or u. The length $\mathbf{l}(t = u)$ of an equation $t = u$ is set to $\mathbf{l}(t) + \mathbf{l}(u) + 1$. With $\mathrm{Var}(\mathcal{D})$ we denote the set of variables occurring in $\mathcal{D}$. $\mathrm{BVar}(\mathcal{D})$ is the set of variables occurring in $\mathcal{D}$ that are bound by an application of the Substitution Rule.

Definition 10 (Pure Equational Theories)**.** The *pure equational theory* $\mathbf{PET}(\mathrm{Ax})$ consists of all equations that can be derived using the Axiom, Reflexivity, Symmetry, Transitivity and Compatibility Rules. The *pure equational theory with substitution* $\mathbf{PETS}(\mathrm{Ax})$ is obtained by additionally allowing the Substitution Rule in the derivation of equations.

An instance $s[\overline{u}/\overline{x}] = t[\overline{u}/\overline{x}]$ of $s = t$ in Ax is called an *injective renaming* of $s = t$, iff the variables $\overline{x}$ are pairwise distinct, they satisfy $\{\overline{x}\} = \mathrm{Var}(s, t)$, and $\overline{u}$ is a list of pairwise distinct variables.

Proposition 11 (Variable Normal Form)**.** *For* $\mathbf{PETS}(\mathrm{Ax})$ *derivations, we can assume the following normal form:*

(1) *Axiom* $\vdash t = u$ *only occur in the form where* $t = u$ *is obtained by injectively renaming variables of an equation in* Ax*. This implies that* t *is of the form* $f(\overline{t})$ *with each* t_i *a generalized variable, and that the same variable is not occurring in both* t_i *and* t_j *for* $i \neq j$.

(2) *Each variable occurring in a normal derivation is either occurring in the equation in which the derivation ends, or is removed in exactly one application of Substitution (as the variable which is bound by that application of Substitution).*

Furthermore, if $\mathcal{D} \vdash t = u$*, then there exists* $\mathcal{D}'$ *in Variable Normal Form such that* $\mathcal{D}' \vdash t = u$ *and* $\mathbf{l}(\mathcal{D}') = \mathrm{O}(\mathbf{l}(\mathcal{D})^2)$.

Proof. For (1), consider an equation $t = u$ in Ax. As Ax is nice, we have that t is of the form $f(t_1, \ldots, t_n)$ with each t_i a generalized variable potentially containing one variable x_i, and that these variables are pairwise distinct. Consider terms $s_1, \ldots, s_n$, and the instance $\vdash t[\overline{s}/\overline{x}] = u[\overline{s}/\overline{x}]$ of the Axiom Rule. This can be replaced by $\vdash t[\overline{y}/\overline{x}] = u[\overline{y}/\overline{x}]$ where $\overline{y}$ is a list $y_1 \ldots, y_n$ of fresh, pairwise distinct variables, followed by applications of the Substitution Rule for successively applying substitutions $[s_1/y_1], [s_2/y_2], \ldots, [s_n/y_n]$.

For (2), we observe that we can replace all occurrences of a fixed variable by a fresh variable throughout a derivation ending in an equation e, obtaining a similar derivation of the equation e potentially with the former variable being renamed to the latter fresh variable.

The above transformation at most squares the length of a derivation. $\square$

Definition 12 (Formal Consistency)**.** With $\mathrm{Cons}(\mathbf{PETS}(\mathrm{Ax}))$ we denote the sentence in the language of Bounded Arithmetic which expresses that there is no derivation in $\mathbf{PETS}(\mathrm{Ax})$ ending in $0 = 1$, where 0 denotes $\mathrm{s}_0(\epsilon)$ and 1 denotes $\mathrm{s}_1(\epsilon)$.

4. Approximation Semantics

Infeasible values, although finite, can be considered as infinite bit strings within theories of feasibility like Bounded Arithmetic. This is relevant when evaluating functions formally in Bounded Arithmetic. Thus we will make use of notions from domain theory to define a method for evaluating terms occurring in equational proofs.

4.1. **Approximate values.** The notion of approximate values v is defined in [9], which adds 'unknown value' of a term [1], denoted with '$*$', to bit-strings.

Definition 13 (Approximate values). The set $\mathbb{D}$ of *approximate values* is defined inductively as follows:
$$v ::= \epsilon \mid v0 \mid v1 \mid *$$
The *gauge* $\mathbf{g}(v)$ of $v \in \mathbb{D}$ is defined recursively:
$$\mathbf{g}(\epsilon) = \mathbf{g}(*) = 1$$
$$\mathbf{g}(v0) = \mathbf{g}(v1) = \mathbf{g}(v) + 1$$
For a tuple $\overline{w} = (w_1, \ldots, w_n) \in \mathbb{D}^n$, its *gauge* is given as $\mathbf{g}(\overline{w}) = \max\{\mathbf{g}(w_1), \ldots, \mathbf{g}(w_n)\}$, and its *extent* as $\mathbf{e}(\overline{w}) = n$.

4.2. **Approximation relation.** A relation $\unlhd$ has been defined in [1]. Here we will consider the converse $\sqsubseteq$ of $\unlhd$.

Definition 14 (Approximation relation). The *approximation relation* $\sqsubseteq$ is a binary relation over $\mathbb{D}$, defined inductively as follows:

- $* \sqsubseteq v$ for any $v \in \mathbb{D}$.
- $\epsilon \sqsubseteq \epsilon$.
- if $v_1 \sqsubseteq v_2$, then $v_10 \sqsubseteq v_20$ and $v_11 \sqsubseteq v_21$.

We pronounce '$v \sqsubseteq w$' as 'v approximates w'.
   We extend $\sqsubseteq$ to tuples: $(v_1, \ldots, v_n) \sqsubseteq (w_1, \ldots, w_n)$ iff $v_i \sqsubseteq w_i$ for each i.

Proposition 15. $\sqsubseteq$ *is a partial order on* $\mathbb{D}^n$, *that is, it is reflexive, anti-symmetric and transitive.* $\qquad\square$

Definition 16 (Compatible). $u, v \in \mathbb{D}$ are *compatible* if $u \sqsubseteq v$ or $v \sqsubseteq u$. $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ in $\mathbb{D}^n$ are compatible if each u_i and v_i are. We denote $\overline{u}$ and $\overline{v}$ being compatible with $\overline{u} \triangle \overline{v}$.

   The following lemma has already been proven in [1]:

Lemma 17. *If* $\overline{u}, \overline{v}, \overline{w} \in \mathbb{D}^n$ *and* $\overline{u}, \overline{v} \sqsubseteq \overline{w}$, *then* $\overline{u} \triangle \overline{v}$. $\qquad\square$

Lemma 18. *Any finite subset S of $\mathbb{D}$ of pairwise compatible elements has a maximal element w.r.t.* $\sqsubseteq$ *which we denote with* $\max_{\sqsubseteq}(S)$, *where* $\max_{\sqsubseteq}(\emptyset) = *$. $\qquad\square$

Definition 19 (Generator). A *generator* for $\mathbb{D}^n \to \mathbb{D}$ is a mapping $\overline{u} \mapsto v$ with $\overline{u} \in \mathbb{D}^n$ and $v \in \mathbb{D} \setminus \{*\}$.

Definition 20 (Consistent set). A *consistent set* $\tilde{f}$ of $\mathbb{D}^n \to \mathbb{D}$ is a finite set of generators satisfying the following condition:
   if $\overline{x} \mapsto y, \overline{u} \mapsto v \in \tilde{f}$ and $\overline{x} \triangle \overline{u}$, then $y \triangle v$.

Definition 21 (Finitely generated maps). A consistent set $\tilde{f}$ defines a mapping, which we call a *finitely generated map* or just *map*, via
$$\tilde{f}(\overline{x}) = \max_{\sqsubseteq}\{v \mid \exists \overline{w}, \overline{w} \sqsubseteq \overline{x} \text{ and } \overline{w} \mapsto v \in \tilde{f}\}.$$
We sometimes write $\tilde{f}[\overline{x}]$ to denote the set
$$\{v \mid \exists \overline{w}, \overline{w} \sqsubseteq \overline{x} \text{ and } \overline{w} \mapsto v \in \tilde{f}\}$$
so that $\tilde{f}(\overline{x}) = \max_{\sqsubseteq} \tilde{f}[\overline{x}]$.

To see that maps are well-defined, consider two generators $\overline{w} \mapsto v$ and $\overline{w}' \mapsto v'$ in $\tilde{f}$ with $\overline{w}, \overline{w}' \sqsubseteq \overline{x}$. With Lemma 17 we obtain $\overline{w} \bigtriangleup \overline{w}'$. Hence $v \bigtriangleup v'$ as $\tilde{f}$ is consistent. Thus, using Lemma 18, the set

$$\tilde{f}[\overline{x}] = \{v \mid \exists \overline{w}, \overline{w} \sqsubseteq \overline{x} \text{ and } \overline{w} \mapsto v \in \tilde{f}\}$$

has a maximal element w.r.t. $\sqsubseteq$.

Lemma 22 (Expansion property of maps). *Let $\tilde{f}_1$ and $\tilde{f}_2$ be consistent sets of $\mathbb{D}^n \to \mathbb{D}$. If $\tilde{f}_1 \subseteq \tilde{f}_2$, then $\tilde{f}_1(\overline{v}) \sqsubseteq \tilde{f}_2(\overline{v})$ for $\overline{v} \in \mathbb{D}^n$.*

Proof. From $\tilde{f}_1 \subseteq \tilde{f}_2$ we immediately obtain $\tilde{f}_1[\overline{v}] \subseteq \tilde{f}_2[\overline{v}]$. Hence the assertion follows. $\square$

For $\overline{x} \sqsubseteq \overline{y}$ we have $\tilde{f}[\overline{x}] \subseteq \tilde{f}[\overline{y}]$, thus we obtain that finitely generated maps are monotone.

Lemma 23 (Monotonicity of finitely generated maps). *Finitely generated maps are monotone w.r.t. $\sqsubseteq$.* $\square$

Remark. There are monotone maps which cannot be represented by finite consistent sets. For example, the identity function from $\mathbb{D}$ to $\mathbb{D}$ is monotone but cannot be represented by a finite consistent set.

Definition 24 (Measures for consistent sets). We define two measures for consistent sets $\tilde{f}$:

- The gauge $\mathbf{g}(\tilde{f})$ is given as

$$\max\{\mathbf{g}(\overline{v}), \mathbf{g}(w) \mid \overline{v} \mapsto w \in \tilde{f}\} \ .$$

- The extent $\mathbf{e}(\tilde{f})$ is given as

$$\max\{\mathbf{e}(\overline{v}) \mid \overline{v} \mapsto w \in \tilde{f}\} \ .$$

Remark. Using the above measures, the length of $\tilde{f}$, $\mathbf{l}(\tilde{f})$, in some natural serialization of $\tilde{f}$, can be bounded by $\mathbf{l}(\tilde{f}) = \mathrm{O}(\#\tilde{f} \cdot \mathbf{e}(\tilde{f}) \cdot \mathbf{g}(\tilde{f}))$.

Definition 25 (Frame). A *frame* F is a partial, finite mapping of function symbols $f \in \mathcal{F} \setminus \mathcal{B}$ to consistent sets. We extend F to all $f \in \mathcal{F} \setminus \mathcal{B}$ by setting $F(f) = \bot$ for $f \notin \mathcal{B} \cup \mathrm{dom}(F)$, where $\bot$ denotes the empty set $\emptyset$.

The set of frames is partially ordered by

$$F_1 \sqsubseteq F_2 \iff \forall f, F_1(f) \subseteq F_2(f) \ .$$

A frame F defines an *evaluation* $F(f)(v)$ for $f \in \mathcal{F}$ and $\overline{v} \in \mathbb{D}^{\mathrm{ar}(f)}$ as follows:

- If $f \in \mathcal{B}$, let $F(f)(\overline{v}) = f(\overline{v})$
- If $f \notin \mathcal{B}$ and $F(f) = \tilde{f}$, let $F(f)(\overline{v}) = \tilde{f}(\overline{v})$.

Observe that for $f \notin \mathrm{dom}(F) \cup \mathcal{B}$, we have $F(f) = \bot$, hence $F(f)(\overline{v}) = \bot(\overline{v}) = *$.

Definition 26 (Measures for frames). We use the following measures for frames:

- The width of F is given by $\mathbf{w}(F) = \max\{\#F(f) \mid f \in \mathrm{dom}(F)\}$.
- The gauge of F is given by $\mathbf{g}(F) = \max\{\mathbf{g}(f) \mid f \in \mathrm{dom}(F)\}$.
- The extent of F is given by $\mathbf{e}(F) = \max\{\mathbf{e}(f) \mid f \in \mathrm{dom}(F)\}$.

Remark. Using the above measures, the length of F, $\mathbf{l}(F)$, in some natural serialization of F, can be bounded by $\mathbf{l}(F) = \mathrm{O}(\#\,\mathrm{dom}(F) \cdot \mathbf{w}(F) \cdot \mathbf{e}(F) \cdot \mathbf{g}(F)) \ .$

Definition 27 (Assignments). An *assigment* ρ is a partial, finite mapping from variables $\mathcal{X}$ to approximations $\mathbb{D}$. We extend assignments outside their domain, by setting $\rho(x) = *$ for $x \notin \mathrm{dom}(\rho)$.

We extend the approximation order $\sqsubseteq$ to assignments pointwise:

$$\text{Let} \quad \rho_1 \sqsubseteq \rho_2 \quad \text{iff} \quad \forall x, \rho_1(x) \sqsubseteq \rho_2(x) \ .$$

With $\rho[x \mapsto v]$ we denote the assignment that behaves like ρ but maps variable x to approximation v:

$$\rho[x \mapsto v](y) \quad = \quad \left\{ \begin{array}{ll} v & : \ \text{if } y = x \\ \rho(y) & : \ \text{otherwise.} \end{array} \right.$$

We apply assignments to generalized variables in the natural way, e.g., $\rho(\mathrm{s}_i(x)) = \mathrm{s}_i(\rho(x))$.

Definition 28 (Measures for assignments). We use the following measures for assignments:

- The width of ρ is given by $\mathbf{w}(\rho) = \# \mathrm{dom}(\rho)$.
- The gauge of ρ is given by $\mathbf{g}(\rho) = \max\{\mathbf{g}(v) \mid v \in \mathrm{rng}(\rho)\}$.

Remark. Using the above measures, the length of ρ, $\mathbf{l}(\rho)$, in some natural serialization of ρ, can be bounded by $\mathbf{l}(\rho) = \mathrm{O}(\mathbf{w}(\rho) \cdot \mathbf{g}(\rho))$.

Definition 29 (Evaluation). Let ρ be an assignment, F a frame, and t a term. The *evaluation* $[\![t]\!]_{F,\rho}$ of t under F, ρ is defined recursively as follows:

$$[\![x]\!]_{F,\rho} \ = \ \rho(x) \quad \text{for a variable } x \in \mathcal{X};$$
$$[\![f(t_1, \ldots, t_n)]\!]_{F,\rho} \ = \ F(f)([\![t_1]\!]_{F,\rho}, \ldots, [\![t_n]\!]_{F,\rho}) \ .$$

We have the following immediate properties of evaluations.

Lemma 30.   (1) $[\![t]\!]_{F,\rho} \in \mathbb{D}$
    (2) $[\![t]\!]_{F,\rho}$ *is monotone in F and ρ w.r.t.* $\sqsubseteq$.

Proof. (1) follows immediately from the definition.

We prove (2) by induction on t, showing that for $F \sqsubseteq F'$ and $\rho \sqsubseteq \rho'$,

$$[\![t]\!]_{F,\rho} \sqsubseteq [\![t]\!]_{F',\rho'} \ .$$

If $t \equiv x$, the assertion holds because $\rho(x) \sqsubseteq \rho'(x)$. If $t \equiv f(t_1, \ldots, t_n)$, we compute

$$
\begin{aligned}
[\![f(t_1, \ldots, t_n)]\!]_{F,\rho} \ = \ & F(f)([\![t_1]\!]_{F,\rho}, \ldots, [\![t_n]\!]_{F,\rho}) \\
\sqsubseteq \ & F'(f)([\![t_1]\!]_{F,\rho}, \ldots, [\![t_n]\!]_{F,\rho}) \\
& \sqsubseteq \ F'(f)([\![t_1]\!]_{F',\rho'}, \ldots, [\![t_n]\!]_{F',\rho'}) \ = \ [\![t]\!]_{F',\rho'} \ ,
\end{aligned}
$$

where the first approximation uses the expansion property of maps, Lemma 22, and the second the induction hypothesis and monotonicity of maps, Lemma 23. $\square$

Lemma 31. *Let ρ be an assignment, F a frame, and t a term. Then*

$$\mathbf{g}([\![t]\!]_{F,\rho}) \ \leq \ \max(\mathbf{g}(\rho), \mathbf{g}(F)) + \mathbf{l}(t) \ .$$

Proof. By induction on t. If t is a variable x, we have

$$\mathbf{g}([\![t]\!]_{F,\rho}) \ = \ \mathbf{g}(\rho(x)) \ \leq \ \mathbf{g}(\rho) \ .$$

If t is ϵ we compute $\mathbf{g}(\llbracket t \rrbracket_{F,\rho}) = 1 = \mathbf{l}(t)$. For t of the form $\mathrm{s}_i(t_1)$ we have

$$\begin{aligned}
\mathbf{g}(\llbracket t \rrbracket_{F,\rho}) \;=\; \mathbf{g}(\mathrm{s}_i(\llbracket t_1 \rrbracket_{F,\rho})) \;&=\; \mathbf{g}(\llbracket t_1 \rrbracket_{F,\rho}) + 1 \\
&\leq\; \max(\mathbf{g}(\rho), \mathbf{g}(F)) + \mathbf{l}(t_1) + 1 \;=\; \max(\mathbf{g}(\rho), \mathbf{g}(F)) + \mathbf{l}(t) \;.
\end{aligned}$$

Finally, assume t is of the form $f(t_1, \ldots, t_n)$ with $f \notin \mathcal{B}$. Then we have $\mathbf{g}(\llbracket t \rrbracket_{F,\rho}) \leq \mathbf{g}(F)$. $\qquad\square$

Lemma 32 (Substitution Lemma)**.** $\llbracket t(u) \rrbracket_{F,\rho} = \llbracket t(x) \rrbracket_{F,\rho[x \mapsto \llbracket u \rrbracket_{F,\rho}]}$

Proof. The proof is by induction on t. $\qquad\square$

5. Frame Models

In this section we develop frames into models for equational theories based on nice axioms.

Definition 33 (Model)**.** A frame F is a *model of* Ax iff for any $t = u$ in Ax and any assignment ρ, $\llbracket t \rrbracket_{F,\rho} \sqsubseteq \llbracket u \rrbracket_{F,\rho}$.

Remark. In general, the notion of being a model cannot be expressed as a bounded formula, thus will usually be in Π_1, but not in Π_1^{b}.

We restrict the notion of being a model to obtain a bounded property. Let κ be a positive integer, which is intended to bound the gauge of approximations occurring in frames and assignments that need to be considered in the definition of models. Furthermore, we restrict the definition to axioms to those occurring in a particular derivation $\mathcal{D}$.

For the remainder of this section, we assume that κ and $\mathcal{D}$ are fixed. With $\mathrm{Var}(\mathcal{D})$ we denote the variables occurring in $\mathcal{D}$.

Definition 34 (κ-Model)**.** A frame F is a *κ-model of* $\mathcal{D}$ iff $\mathbf{g}(F) \leq \kappa$, and for any $t = u$ in Ax occurring in $\mathcal{D}$ and any assignment ρ with $\mathrm{dom}(\rho) \subseteq \mathrm{Var}(\mathcal{D})$ and $\mathbf{g}(\rho) \leq \kappa$, we have $\llbracket t \rrbracket_{F,\rho} \sqsubseteq \llbracket u \rrbracket_{F,\rho}$.

Remark. The notion of F being a κ-model of $\mathcal{D}$ can be written as a Π_1^{b} formula.

Lemma 35. *The empty frame is a κ-model of $\mathcal{D}$.*

Proof. Let F be the empty frame. Consider $t = u$ in Ax, and assignment ρ. Then t is of the form $f(\bar{t})$ for some f in $\mathcal{F} \setminus \mathcal{B}$. We have $F(f) = \bot$, hence $\llbracket f(\bar{t}) \rrbracket_{F,\rho} = * \sqsubseteq \llbracket u \rrbracket_{F,\rho}$. $\qquad\square$

We will now define the notion of *updates* that can be used to expand models based on axioms occurring in $\mathcal{D}$.

Definition 36 (Updates)**.** Let F be a κ-model of $\mathcal{D}$. An *update based on F, κ and $\mathcal{D}$* is any $f \in \mathcal{F} \setminus \mathcal{B}$ and generator $\bar{v} \mapsto w$, which we denote as $f \colon \bar{v} \mapsto w$, such that $\mathbf{g}(\bar{v}, w) \leq \kappa$ and there exists $t = u$ in Ax occurring in $\mathcal{D}$ and an assignment ρ satisfying that

- t is of the form $f(\bar{t})$,
- $v_i = \rho(t_i)$ for $i \leq \mathrm{ar}(f)$,
- and $w = \llbracket u \rrbracket_{F,\rho}$.

With $F * f\colon \overline{v} \mapsto w$ we denote the frame F' given by

$$F'(g) = F(g) \quad \text{if } g \neq f$$
$$F'(f) = F(f) \cup \{\overline{v} \mapsto w\}$$

The gauge of $f\colon \overline{v} \mapsto w$, denoted $\mathbf{g}(f\colon \overline{v} \mapsto w)$, is given by $\mathbf{g}(\overline{v}, w)$, its extent, denoted $\mathbf{e}(f\colon \overline{v} \mapsto w)$, by $\mathbf{e}(\overline{v})$.

Remark. The length of update $f\colon \overline{v} \mapsto w$, $\mathbf{l}(f\colon \overline{v} \mapsto w)$, can be bounded by

$$\mathbf{l}(f\colon \overline{v} \mapsto w) \;=\; \mathrm{O}(\mathbf{e}(f\colon \overline{v} \mapsto w) \cdot \mathbf{g}(f\colon \overline{v} \mapsto w)) \;.$$

Remark. The arguments $\overline{t}$ to f above are generalized variables, as Ax is nice. Thus $\rho(t_i)$ is well-defined. Furthermore, in each term of $\overline{t}$, at most one variable can occur, and such variables are distinct for different terms as Ax is nice, as remarked before. Hence, an update uniquely determines an axiom in Ax and substitution on which it is based.

Remark. For $F' = F * f\colon \overline{v} \mapsto w$ we compute

- $\#(F') \leq \#(F) + 1$,
- $\mathbf{w}(F') \leq \mathbf{w}(F) + 1$,
- $\mathbf{g}(F') = \max\{\mathbf{g}(F), \mathbf{g}(\overline{v}, w)\}$,
- $\mathbf{e}(F') = \max\{\mathbf{e}(F), \mathrm{ar}(f)\}$.

We now formulate and prove a crucial property of updates: They can be used to extend κ-models for $\mathcal{D}$.

Proposition 37 (S_2^1). *Let F be a κ-model of $\mathcal{D}$, $f\colon \overline{v} \mapsto w$ an update based on F, κ and $\mathcal{D}$, and $F' = F * f\colon \overline{v} \mapsto w$. Then F' is a κ-model of $\mathcal{D}$.*

Proof. We argue in S_2^1. Let the assumption of the proposition be given, and assume that $f\colon \overline{v} \mapsto w$ is given via $t = u$ in Ax and assignment ρ, where t is of the form $f(\overline{t})$ and $\overline{v} = \rho(\overline{t})$. W.l.o.g., $\mathrm{dom}(\rho) = \mathrm{Var}(t)$. We have $\mathbf{g}(\rho) \leq \kappa$.

In order to show that $F' = F * f\colon \overline{v} \mapsto w$ is a κ-model for $\mathcal{D}$, it suffices to show that

(1) $F'(f)$ is a consistent set, and
(2) for any $t' = u'$ in Ax occurring in $\mathcal{D}$, and any assignment ρ' with $\mathbf{g}(\rho') \leq \kappa$, we have $[\![t']\!]_{F',\rho'} \sqsubseteq [\![u']\!]_{F',\rho'}$.

For (1), consider $\overline{v}' \mapsto w' \in F(f)$ such that $\overline{v}' \bigtriangleup \overline{v}$. Then there exists $\overline{y}$ such that $\overline{v}, \overline{v}' \sqsubseteq \overline{y}$ and $\mathbf{g}(\overline{y}) \leq \kappa$ – we can choose y_i to be $\max_{\sqsubseteq}\{v_i, v_i'\}$, hence $\mathbf{g}(y_i) \leq \kappa$ follows from assumption $\mathbf{g}(\overline{v}_i), \mathbf{g}(\overline{v}_i') \leq \kappa$. Choose $\hat{\rho}$ with $\mathrm{dom}(\hat{\rho}) = \mathrm{Var}(t)$ such that $y_i = \hat{\rho}(t_i)$, which is possible since $\overline{v} \sqsubseteq \overline{y}$. We observe that $\rho \sqsubseteq \hat{\rho}$ and that $\mathbf{g}(\hat{\rho}) \leq \kappa$.

Let S be $F(f)[\overline{y}]$, that is

$$S \;=\; \{\tilde{w} \mid \exists \tilde{v}, \tilde{v} \sqsubseteq \overline{y} \text{ and } \tilde{v} \mapsto \tilde{w} \in F(f)\} \;.$$

We have $w' \in S$ as $\overline{v}' \sqsubseteq \overline{y}$, hence

$$w' \;\sqsubseteq\; \max_{\sqsubseteq} S \;=\; F(f)(\overline{y}) = [\![t]\!]_{F,\hat{\rho}} \;\sqsubseteq\; [\![u]\!]_{F,\hat{\rho}}$$

as F is a κ-model of $\mathcal{D}$. Furthermore,

$$w \;=\; [\![u]\!]_{F,\rho} \;\sqsubseteq\; [\![u]\!]_{F,\hat{\rho}}$$

as $\rho \sqsubseteq \hat{\rho}$. Hence $w \bigtriangleup w'$ using Lemma 17.

For (2), let $t' = u'$ be in Ax occurring in $\mathcal{D}$, and ρ' be an assignment with $\mathbf{g}(\rho') \leq \kappa$. If $t' = u'$ is not identical to $t = u$, then the assertion follows from F being a κ-model of $\mathcal{D}$: Ax being nice implies $[\![t']\!]_{F',\rho'} = [\![t']\!]_{F,\rho'}$ in this case, hence

$$[\![t']\!]_{F',\rho'} \;=\; [\![t']\!]_{F,\rho'} \;\sqsubseteq\; [\![u']\!]_{F,\rho'} \;\sqsubseteq\; [\![u']\!]_{F',\rho'}$$

as F is a κ-model of $\mathcal{D}$, and $F \sqsubseteq F'$.

Now consider $t' = u'$ being identical to $t = u$. Let y_i be $\rho'(t_i)$. If $\overline{v} \not\sqsubseteq \overline{y}$, then again $[\![t']\!]_{F',\rho'} = [\![t']\!]_{F,\rho'}$ and the assertion follows from F being a κ-model of $\mathcal{D}$ as before.

So assume $\overline{v} \sqsubseteq \overline{y}$. Let $\overline{x}$ be the list of variables occuring in t, then we have $\rho\!\upharpoonright_{\overline{x}} \sqsubseteq \rho'\!\upharpoonright_{\overline{x}}$. We compute

$$F'(f)(\overline{y}) \;=\; \max_{\sqsubseteq} F'(f)[\overline{y}] \;=\; \max_{\sqsubseteq}(\{w\} \cup F(f)[\overline{y}]) \;=\; \max_{\sqsubseteq}\{w, F(f)(\overline{y})\} \ .$$

We consider w and $F(f)(\overline{y})$ in turns: For $F(f)(\overline{y})$ we have

$$F(f)(\overline{y}) \;=\; [\![t]\!]_{F,\rho'} \;\sqsubseteq\; [\![u]\!]_{F,\rho'}$$

as F is a κ-model of $\mathcal{D}$. In case of w we have,

$$w \;=\; [\![u]\!]_{F,\rho} \;=\; [\![u]\!]_{F,\rho\upharpoonright_{\overline{x}}} \;\sqsubseteq\; [\![u]\!]_{F,\rho'\upharpoonright_{\overline{x}}} \;=\; [\![u]\!]_{F,\rho'}$$

using $\rho\!\upharpoonright_{\overline{x}} \sqsubseteq \rho'\!\upharpoonright_{\overline{x}}$. Hence $F'(f)(\overline{y}) \sqsubseteq [\![u]\!]_{F,\rho'}$. Thus

$$[\![t]\!]_{F',\rho'} \;=\; F'(f)(\overline{y}) \;\sqsubseteq\; [\![u]\!]_{F,\rho'} \;\sqsubseteq\; [\![u]\!]_{F',\rho'}$$

as $F \sqsubseteq F'$. $\qquad\square$

Definition 38. A *sequence of updates based on F, κ and $\mathcal{D}$* is a sequence σ of the form

$$\langle\, f_1\colon \overline{v}_1 \mapsto w_1\,,\ldots,\ f_\ell\colon \overline{v}_\ell \mapsto w_\ell \,\rangle$$

such that for

$$\begin{aligned} F_0 &:= F \\ F_{i+1} &:= F_i \,*\, f_{i+1}\colon \overline{v}_{i+1} \mapsto w_{i+1} \end{aligned}$$

we have that

$$f_{i+1}\colon \overline{v}_{i+1} \mapsto w_{i+1} \quad \text{is an update based on } F_i,\ \kappa \text{ and } \mathcal{D}.$$

Let $F * \sigma$ denote F_ℓ. The *sequence length of σ*, denoted $\mathbf{sql}(\sigma)$, is given by ℓ. The gauge of σ is given by $\mathbf{g}(\sigma) = \max\{\mathbf{g}(\overline{v}_1, w_1),\ldots,\mathbf{g}(\overline{v}_\ell, w_\ell)\}$, its extend by $\mathbf{e}(\sigma) = \max\{\mathrm{ar}(f_1),\ldots,\mathrm{ar}(f_\ell)\}$.

Remark. The length of σ, $\mathbf{l}(\sigma)$, can be bounded by $\mathbf{l}(\sigma) = \mathrm{O}(\mathbf{e}(\sigma) \cdot \mathbf{g}(\sigma) \cdot \mathbf{sql}(\sigma))$.

Remark. For $F' = F * \sigma$ we compute
- $\#(F') \leq \#(F) + \mathbf{sql}(\sigma)$,
- $\mathbf{w}(F') \leq \mathbf{w}(F) + \mathbf{sql}(\sigma)$,
- $\mathbf{g}(F') = \max\{\mathbf{g}(F), \mathbf{g}(\sigma)\}$,
- $\mathbf{e}(F') = \max\{\mathbf{e}(F), \mathbf{e}(\sigma)\}$.

Corollary 39 (S$_2^1$)**.** *Assuming the notions given by the previous definition, all F_i's are κ-models of $\mathcal{D}$, for $i \leq \ell$.*

Proof. The proof is by induction on $i \leq \ell$ using Proposition 37. $\qquad\square$

6. Soundness in S_2^2

We now prove a soundness property for equational reasoning using approximation semantics. The proof will be formalizable in S_2^2. This will be improved in the remaining sections to a proof formalizable in S_2^1 by introducing an additional property. To keep the exposition clearer, we first prove soundness based on the notions introduced so far.

Theorem 40 (S_2^2). *Assume $\mathcal{D} \vdash t = u$ is in Variable Normal Form. Let ρ be an assignment, and F a model for* Ax. *Let κ be $\max\{\mathbf{g}(F), \mathbf{g}(\rho)\} + \mathbf{l}(\mathcal{D})$. Then there are sequences σ_1 and σ_2 of updates based on F, κ and $\mathcal{D}$ such that*

$$[\![t]\!]_{F,\rho} \ \sqsubseteq \ [\![u]\!]_{F * \sigma_1, \rho}$$
$$[\![u]\!]_{F,\rho} \ \sqsubseteq \ [\![t]\!]_{F * \sigma_2, \rho}$$

To prove the previous theorem, we consider the following more general claim.

Claim 41 (S_2^2). *Fix some derivation $\mathcal{D}$ in Variable Normal Form, some model F for* Ax, *and some integer U such that $\mathbf{g}(F) + \mathbf{l}(\mathcal{D}) \leq U$.*

Let $\mathcal{D}_0 \vdash t = u$ be a sub-derivation of $\mathcal{D}$. Let ρ be an assignment, and σ a sequence of updates based on F, U, $\mathcal{D}$, satisfying

$$\mathrm{dom}(\rho) \ \subseteq \ \mathrm{Var}(\mathcal{D})$$
$$\mathbf{g}(\rho), \mathbf{g}(\sigma), \mathbf{e}(\sigma), \mathbf{sql}(\sigma) \ \leq \ U - \mathbf{l}(\mathcal{D}_0)$$

Then there are sequences σ_1 and σ_2 of updates based on F, U, $\mathcal{D}$ with

$$\mathbf{e}(\sigma_i), \mathbf{sql}(\sigma_i) \ \leq \ \mathbf{l}(\mathcal{D}_0)$$
$$\mathbf{g}(\sigma_i) \ \leq \ \max\{\mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\rho)\} + \mathbf{l}(\mathcal{D}_0)$$

such that

$$[\![t]\!]_{F,\rho} \ \sqsubseteq \ [\![u]\!]_{F' * \sigma_1, \rho}$$
$$[\![u]\!]_{F,\rho} \ \sqsubseteq \ [\![t]\!]_{F' * \sigma_2, \rho}$$

for $F' = F * \sigma$.

The Theorem follows from the Claim by letting $\mathcal{D}_0 = \mathcal{D}$, ρ as given, $\sigma = \langle\rangle$, and $U = \max\{\mathbf{g}(F), \mathbf{g}(\rho)\} + \mathbf{l}(\mathcal{D})$.

Proof of Claim 41. We argue in S_2^2. Let $\mathcal{D}$, F and U be given as in the Claim. We prove that for any $\mathcal{D}_0$, ρ, σ satisfying the conditions of the Claim, there are σ_1 and σ_2 satisfying the assertion of the Claim, by induction on $\mathbf{l}(\mathcal{D}_0)$. Thus this is proven by logarithmic induction (LIND) on a Π_2^b-property, which is available in S_2^2 by Theorem 1.

Let $\mathcal{D}_0$, ρ, σ be given, that are satisfying the conditions in the Claim. Let F' be $F * \sigma$. then F' is a U-model of $\mathcal{D}$ by Corollary 39.

We now consider cases according to the last rule applied in $\mathcal{D}_0$. If that is the **Reflexivity Rule** $\vdash t = t$, we can choose $\sigma_1 = \sigma_2 = \langle\rangle$ to satisfy the assertion of the Claim.

Axiom Rule: More interesting is the case of Axiom Rule $\vdash t = u$. As $\mathcal{D}$ is in Variable Normal Form we have that $t = u$ is an injective renaming of an equation in Ax. W.l.o.g. we can assume that $t = u$ is in Ax, as renamings of variables would make no difference to the following argument. As Ax is nice, we have that t is of the form $f(\bar{t})$ for some $f \in \mathcal{F} \setminus \mathcal{B}$ and generalized variables $\bar{t}$. Let v_i be $\rho(t_i)$ and $w = [\![u]\!]_{F',\rho}$. We compute $\mathbf{g}(v_i) \leq \mathbf{g}(\rho) + 1$ and, using Lemma 31,

$$\mathbf{g}(w) \ \leq \ \max\{\mathbf{g}(\rho), \mathbf{g}(F')\} + \mathbf{l}(u) \ < \ \max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma)\} + \mathbf{l}(\mathcal{D}_0) \ .$$

Let $\sigma_1 = \langle\rangle$ and $\sigma_2 = \langle f\colon \bar{v} \mapsto w\rangle$, then

$$\mathbf{e}(\sigma_i) \ \leq \ \mathrm{ar}(f) \ < \ \mathbf{l}(\mathcal{D}_0) \ ,$$
$$\mathbf{sql}(\sigma_i) \ \leq \ 1 \ < \ \mathbf{l}(\mathcal{D}_0) \ , \text{ and}$$
$$\mathbf{g}(\sigma_i) \ \leq \ \max\{\mathbf{g}(\sigma), \mathbf{g}(\rho), \mathbf{g}(F)\} + \mathbf{l}(\mathcal{D}_0) \ .$$

Furthermore, $[\![t]\!]_{F',\rho} \sqsubseteq [\![u]\!]_{F',\rho}$ as F' is U-model of $\mathcal{D}$, which proves the assertion for σ_1. For σ_2, let F'' be $F' * \sigma_2$, then we have

$$[\![u]\!]_{F',\rho} \ = \ w \ \sqsubseteq \ \max_{\sqsubseteq} F''(f)[\bar{v}] \ = \ F''(f)(\bar{v})$$
$$= \ F''(f)(\ldots, \rho(t_i), \ldots) \ = \ [\![t]\!]_{F'',\rho} \ .$$

Symmetry Rule: For the case of Symmetry Rule, let $\mathcal{D}_1$ be the sub-derivation of $\mathcal{D}_0$ ending in $u = t$. By induction hypothesis we obtain σ_1' and σ_2' satisfying the assertion for $\mathcal{D}_1$. By choosing $\sigma_1 = \sigma_2'$ and $\sigma_2 = \sigma_1'$ we immediately fulfill the assertion for $\mathcal{D}_0$.

Transitivity Rule: If $\mathcal{D}_0$ ends with an application of the Transitivity Rule, it must be of the form

$$\frac{\begin{array}{cc} \mathcal{D}_1 & \mathcal{D}_2 \\ t = s & s = u \end{array}}{t = u}$$

By induction hypothesis applied to $\mathcal{D}_1$, ρ and σ, we obtain some σ_1^1 satisfying

$$\mathbf{e}(\sigma_1^1), \mathbf{sql}(\sigma_1^1) \ \leq \ \mathbf{l}(\mathcal{D}_1) \ ,$$
$$\mathbf{g}(\sigma_1^1) \ \leq \ \max\{\mathbf{g}(\sigma), \mathbf{g}(\rho), \mathbf{g}(F)\} + \mathbf{l}(\mathcal{D}_1) \ , \text{ and}$$
$$[\![t]\!]_{F,\rho} \ \sqsubseteq \ [\![s]\!]_{F_1^1,\rho} \ \text{ for } F_1^1 = F' * \sigma_1^1 \ .$$

We compute

$$\mathbf{e}(\sigma * \sigma_1^1) \ \leq \ \max\{\mathbf{e}(\sigma), \mathbf{e}(\sigma_1^1)\} \ \leq \ U - \mathbf{l}(\mathcal{D}_0) + \mathbf{l}(\mathcal{D}_1) \ < \ U - \mathbf{l}(\mathcal{D}_2)$$
$$\mathbf{sql}(\sigma * \sigma_1^1) \ \leq \ \mathbf{sql}(\sigma) + \mathbf{sql}(\sigma_1^1) \ \leq \ U - \mathbf{l}(\mathcal{D}_0) + \mathbf{l}(\mathcal{D}_1) \ < \ U - \mathbf{l}(\mathcal{D}_2)$$

and

$$\mathbf{g}(\sigma * \sigma_1^1) \ \leq \ \max\{\mathbf{g}(F), \mathbf{g}(\rho), \mathbf{g}(\sigma)\} + \mathbf{l}(\mathcal{D}_1)$$
$$\leq \ U - \mathbf{l}(\mathcal{D}_0) + \mathbf{l}(\mathcal{D}_1) \ < \ U - \mathbf{l}(\mathcal{D}_2)$$

because $\mathbf{l}(\mathcal{D}_0) > \mathbf{l}(\mathcal{D}_1) + \mathbf{l}(\mathcal{D}_2)$. Thus, we can apply i.h. to $\mathcal{D}_2$, ρ and $\sigma * \sigma_1^1$, obtaining σ_1^2 satisfying

$$\mathbf{e}(\sigma_1^2), \mathbf{sql}(\sigma_1^2) \ \leq \ \mathbf{l}(\mathcal{D}_2) \ ,$$
$$\mathbf{g}(\sigma_1^2) \ \leq \ \max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma * \sigma_1^1)\} + \mathbf{l}(\mathcal{D}_2) \ , \ \text{and}$$
$$[\![s]\!]_{F_1^1,\rho} \ \sqsubseteq \ [\![u]\!]_{F_1^1 * \sigma_1^2,\rho} \ .$$

Let σ_1 be $\sigma_1^1 :: \sigma_1^2$, then we compute

$$\mathbf{e}(\sigma_1) \ = \ \max\{\mathbf{e}(\sigma_1^1), \mathbf{e}(\sigma_1^2)\} \ \leq \ \mathbf{l}(\mathcal{D}_1) + \mathbf{l}(\mathcal{D}_2) \ < \ \mathbf{l}(\mathcal{D}_0)$$
$$\mathbf{sql}(\sigma_1) \ = \ \mathbf{sql}(\sigma_1^1) + \mathbf{sql}(\sigma_1^2) \ \leq \ \mathbf{l}(\mathcal{D}_1) + \mathbf{l}(\mathcal{D}_2) \ < \ \mathbf{l}(\mathcal{D}_0)$$

and

$$\begin{aligned}
\mathbf{g}(\sigma_1) \ &= \ \max\{\mathbf{g}(\sigma_1^1), \mathbf{g}(\sigma_1^2)\} \\
&\leq \ \max\{\mathbf{g}(\sigma_1^1), \max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma :: \sigma_1^1)\} + \mathbf{l}(\mathcal{D}_2)\} \\
&= \ \max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\sigma_1^1)\} + \mathbf{l}(\mathcal{D}_2) \\
&\leq \ \max\{\mathbf{g}(F), \mathbf{g}(\rho), \mathbf{g}(\sigma)\} + \mathbf{l}(\mathcal{D}_1) + \mathbf{l}(\mathcal{D}_2) \\
&< \ \max\{\mathbf{g}(F), \mathbf{g}(\rho), \mathbf{g}(\sigma)\} + \mathbf{l}(\mathcal{D}_0)
\end{aligned}$$

Furthermore, $[\![t]\!]_{F,\rho} \ \sqsubseteq \ [\![s]\!]_{F_1^1,\rho} \ \sqsubseteq \ [\![u]\!]_{F_1^1 * \sigma_1^2,\rho} \ = \ [\![u]\!]_{F' * \sigma_1,\rho}$, because

$$F_1^1 * \sigma_1^2 \ = \ (F' * \sigma_1^1) * \sigma_1^2 \ = \ F' * (\sigma_1^1 :: \sigma_1^2) \ = \ F' * \sigma_1$$

which proves the assertion for σ_1. The construction for σ_2 is similar, starting with $\mathcal{D}_2$.

Compatibility Rule. In case of the last rule being the Compatibility Rule, $\mathcal{D}_0$ will have the following form:

$$\frac{\begin{array}{c} \mathcal{D}_1 \\ t = u \end{array}}{s[t/x] = s[u/x]}$$

Applying the i.h. to $\mathcal{D}_1$, ρ and σ, we obtain σ_1 and σ_2 satisfying the assertion for $\mathcal{D}_1$. Let $\rho_1^1 = \rho[x \mapsto [\![t]\!]_{F,\rho}]$ and $\rho_1^2 = \rho[x \mapsto [\![u]\!]_{F' * \sigma_1,\rho}]$. Then we have $\rho_1^1 \sqsubseteq \rho_1^2$. Employing the Substitution Lemma 32, we obtain

$$[\![s[t/x]]\!]_{F,\rho} \ = \ [\![s]\!]_{F,\rho_1^1} \ \sqsubseteq \ [\![s]\!]_{F' * \sigma_1,\rho_1^2} \ = \ [\![s[u/x]]\!]_{F' * \sigma_1,\rho}$$

which shows that σ_1 also satisfies the assertion for $\mathcal{D}_0$. Similar for σ_2 and $\mathcal{D}_0$.

Substitution Rule. If $\mathcal{D}_0$ ends in an application of Substitution, it will have the following form:

$$\frac{\begin{array}{c} \mathcal{D}_1 \\ t = u \end{array}}{t[s/x] = u[s/x]}$$

We only consider the case that x is occurring in $t = u$, the other case is trivial.

Let ρ' be $\rho[x \mapsto [\![s]\!]_{F,\rho}]$, then clearly $\mathrm{dom}(\rho') \subseteq \mathrm{Var}(\mathcal{D})$. Furthermore, using Lemma 31, we obtain

$$
\begin{aligned}
\mathbf{g}(\rho') \;&\leq\; \max\{\mathbf{g}(\rho), \mathbf{g}([\![s]\!]_{F,\rho})\} \\
&\leq\; \max\{\mathbf{g}(\rho), \max\{\mathbf{g}(\rho), \mathbf{g}(F)\} + \mathbf{l}(s)\} \\
&=\; \max\{\mathbf{g}(\rho), \mathbf{g}(F)\} + \mathbf{l}(s)
\end{aligned}
$$

hence

$$
\mathbf{g}(\rho') \;\leq\; U - \mathbf{l}(\mathcal{D}_0) + \mathbf{l}(s) \;<\; U - \mathbf{l}(\mathcal{D}_1)
$$

because

$$
\mathbf{l}(\mathcal{D}_0) \;=\; \mathbf{l}(\mathcal{D}_1) + \mathbf{l}(t[s/x] = u[s/x]) \;>\; \mathbf{l}(\mathcal{D}_1) + \mathbf{l}(s) \ .
$$

Thus we can apply the i.h. to $\mathcal{D}_1$, ρ' and σ, obtaining σ_1 and σ_2 such that

$$
\mathbf{e}(\sigma_i), \mathbf{sql}(\sigma_i) \;\leq\; \mathbf{l}(\mathcal{D}_1) \;<\; \mathbf{l}(\mathcal{D}_0)
$$

and

$$
\begin{aligned}
\mathbf{g}(\sigma_i) \;&\leq\; \max\{\mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\rho')\} + \mathbf{l}(\mathcal{D}_1) \\
&\leq\; \max\{\mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\rho)\} + \mathbf{l}(s) + \mathbf{l}(\mathcal{D}_1) \\
&<\; \max\{\mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\rho)\} + \mathbf{l}(\mathcal{D}_0)
\end{aligned}
$$

Furthermore,

$$
[\![t]\!]_{F,\rho'} \;\sqsubseteq\; [\![u]\!]_{F' * \sigma_1, \rho'}
$$

Now we can compute, employing the Substitution Lemma 32,

$$
\begin{aligned}
[\![t[s/x]]\!]_{F,\rho} \;&=\; [\![t]\!]_{F,\rho'} \;\sqsubseteq\; [\![u]\!]_{F' * \sigma_1, \rho'} \\
&=\; [\![u]\!]_{F' * \sigma_1, \rho[x \mapsto [\![s]\!]_{F,\rho}]} \\
&\sqsubseteq\; [\![u]\!]_{F' * \sigma_1, \rho[x \mapsto [\![s]\!]_{F' * \sigma_1, \rho}]} \;=\; [\![u[s/x]]\!]_{F' * \sigma_1, \rho}
\end{aligned}
$$

which proves the assertion for σ_1 and $\mathcal{D}_0$. Similar for σ_2 and $\mathcal{D}_0$. $\qquad \square$

Corollary 42. *The consistency of* **PETS**(Ax) *is provable in* S_2^2.

Proof. We argue in S_2^2. Assume $\mathcal{D}$ is a **PETS**(Ax) derivation ending in $0 = 1$. Using Proposition 11 we can assume that $\mathcal{D}$ is in Variable Normal Form. Let ρ be the empty assignment, and F the empty model for Ax. Let $\kappa = \mathbf{l}(\mathcal{D})$. By the previous Theorem 40, there is a sequence σ_1 of updates based on F, κ and $\mathcal{D}$ such that

$$
0 \;=\; [\![0]\!]_{F,\rho} \;\sqsubseteq\; [\![1]\!]_{F * \sigma_1, \rho} \;=\; 1
$$

which is impossible. $\qquad \square$

7. Instructions and Frame Models

In order to be able to prove our main theorem in S_2^1, we need to turn a proof tree consisting of equations using rules for equational reasoning into some linear sequence which describes how terms are transformed step by step in order to go from the term on the left-hand side of the final equation in the proof tree to the term on the right-hand side, and visa versa. This idea is similar to the one used in [1] where such proof trees (without the Substitution Rule) were turned into paths of a corresponding term rewriting relation. Here we use instructions storing the operation that should be applied to a term while moving through the tree.

We start by naming the instructions that will be considered.

Definition 43 (Instructions)**.** We define a set of *instructions* and their *length* as follows:

> **Axiom:** $A[t \to u]$ and $A[t \leftarrow u]$ are instructions, for any axiom $t = u \in \text{Ax}$. Their length is $\mathbf{l}(t) + \mathbf{l}(u) + 1$.
>
> **Substitution:** $S{\uparrow}[s, t/x]$ and $S{\downarrow}[s, t/x]$ are instructions, for terms s, t and variable x. Their length is $\mathbf{l}(s) + \mathbf{l}(t) + 1$.

Sequences of instructions will be denoted with τ. With $\mathbf{sql}(\tau)$ we denote the sequence length of τ, that is the number of instructions occurring in τ. With $\mathbf{l}(\tau)$ we denote the length of τ given as the sum of lengths of instructions occurring in them.

We now define the process of turning derivations into sequences of related instructions.

Definition 44. For a derivation $\mathcal{D}$, we define *sequences of instructions* $\overrightarrow{\text{Inst}}_{\mathcal{D}}$ and $\overleftarrow{\text{Inst}}_{\mathcal{D}}$ by recursion on $\mathcal{D}$ as follows.

> **Axiom Rule:** If D is of the form
>
> $$\overline{t = u}$$
>
> let
>
> $$\overrightarrow{\text{Inst}}_{\mathcal{D}} := \langle A[t \to u] \rangle$$
> $$\overleftarrow{\text{Inst}}_{\mathcal{D}} := \langle A[t \leftarrow u] \rangle$$
>
> **Reflexivity Rule:** If D is of the form
>
> $$\overline{t = t}$$
>
> let
>
> $$\overrightarrow{\text{Inst}}_{\mathcal{D}} := \overleftarrow{\text{Inst}}_{\mathcal{D}} := \langle \rangle$$
>
> **Symmetry Rule:** Consider $\mathcal{D}$ of the form
>
> $$\frac{\begin{array}{c} \mathcal{D}_1 \\ u = t \end{array}}{t = u}$$
>
> Let $\overrightarrow{\text{Inst}}_{\mathcal{D}_1}$ and $\overleftarrow{\text{Inst}}_{\mathcal{D}_1}$ be given by i.h., then define
>
> $$\overrightarrow{\text{Inst}}_{\mathcal{D}} := \overleftarrow{\text{Inst}}_{\mathcal{D}_1}$$
> $$\overleftarrow{\text{Inst}}_{\mathcal{D}} := \overrightarrow{\text{Inst}}_{\mathcal{D}_1}$$
>
> **Transitivity Rule:** Consider $\mathcal{D}$ of the form
>
> $$\frac{\begin{array}{cc} \mathcal{D}_1 & \mathcal{D}_2 \\ t = s & s = u \end{array}}{t = u}$$
>
> Let $\overrightarrow{\text{Inst}}_{\mathcal{D}_1}$, $\overleftarrow{\text{Inst}}_{\mathcal{D}_1}$, $\overrightarrow{\text{Inst}}_{\mathcal{D}_2}$ and $\overleftarrow{\text{Inst}}_{\mathcal{D}_2}$ be given by i.h. Define
>
> $$\overrightarrow{\text{Inst}}_{\mathcal{D}} := \overrightarrow{\text{Inst}}_{\mathcal{D}_1} :: \overrightarrow{\text{Inst}}_{\mathcal{D}_2}$$
> $$\overleftarrow{\text{Inst}}_{\mathcal{D}} := \overleftarrow{\text{Inst}}_{\mathcal{D}_2} :: \overleftarrow{\text{Inst}}_{\mathcal{D}_1}.$$
>
> **Compatibility Rule:** If $\mathcal{D}$ is of the form

$$\begin{array}{c} \mathcal{D}_1 \\ \dfrac{t = u}{s[t/x] = s[u/x]} \end{array}$$

Let $\overrightarrow{\text{Inst}}_{\mathcal{D}_1}$ and $\overleftarrow{\text{Inst}}_{\mathcal{D}_1}$ be given by i.h., then define

$$\overrightarrow{\text{Inst}}_{\mathcal{D}} \; := \; \overrightarrow{\text{Inst}}_{\mathcal{D}_1}$$
$$\overleftarrow{\text{Inst}}_{\mathcal{D}} \; := \; \overleftarrow{\text{Inst}}_{\mathcal{D}_1}$$

Substitution Rule: If $\mathcal{D}$ is of the form

$$\begin{array}{c} \mathcal{D}_1 \\ \dfrac{t = u}{t[s/x] = u[s/x]} \end{array}$$

then let

$$\overrightarrow{\text{Inst}}_{\mathcal{D}} \; := \; \text{S}{\uparrow}[t, s/x] \; : \; \overrightarrow{\text{Inst}}_{\mathcal{D}_1} \; : \; \text{S}{\downarrow}[u, s/x]$$
$$\overleftarrow{\text{Inst}}_{\mathcal{D}} \; := \; \text{S}{\uparrow}[u, s/x] \; : \; \overleftarrow{\text{Inst}}_{\mathcal{D}_1} \; : \; \text{S}{\downarrow}[t, s/x]$$

Remark. We observe that $\mathbf{l}(\overrightarrow{\text{Inst}}_{\mathcal{D}}) = \mathbf{l}(\overleftarrow{\text{Inst}}_{\mathcal{D}}) \leq \mathbf{l}(\mathcal{D})$.

We will now describe a process of evaluating terms using approximations along sequences of instruction. We start with the most basic and also most interesting step of the reverse direction of an axiom instruction.

For the remainder of this section, we assume that κ and $\mathcal{D}$ are fixed.

Definition 45. Let $t = u$ be an axiom in $\mathcal{D}$, ρ an assignment, and F a κ-model of Ax. Define $\Psi(t \leftarrow u, \langle F, \rho \rangle)$ to be $f \colon \overline{v} \mapsto w$ satisfying

- t is of the form $f(\overline{t})$ for some terms $\overline{t}$;
- $v_i = \rho(t_i)$ for $i \leq \text{ar}(f)$;
- and $w = [\![u]\!]_{F,\rho}$.

For a sequence σ of updates based on F, κ and $\mathcal{D}$ we let $\Psi(t \leftarrow u, \langle F, \sigma, \rho \rangle)$ be $\Psi(t \leftarrow u, \langle F * \sigma, \rho \rangle)$.

Lemma 46. *Let $t = u$ be an axiom in* Ax, *κ' a positive integer with $\kappa' \leq \kappa - \mathbf{l}(u)$, ρ an assignment with $\mathbf{g}(\rho) \leq \kappa'$, and F a κ-model of $\mathcal{D}$ with $\mathbf{g}(F) \leq \kappa'$. Let $f \colon \overline{v} \mapsto w$ be given by $\Psi(t \leftarrow u, \langle F, \rho \rangle)$. Then $f \colon \overline{v} \mapsto w$ is an update based on F, κ and $\mathcal{D}$, satisfying that $\mathbf{g}(\overline{v}, w) \leq \kappa' + \mathbf{l}(u)$ and*

$$[\![u]\!]_{F,\rho} \; \sqsubseteq \; [\![t]\!]_{F \, * \, f \colon \overline{v} \mapsto w, \rho} \; .$$

Proof. As Ax is nice, we have that t is of the form $f(\overline{t})$ for some $f \in \mathcal{F} \setminus \mathcal{B}$ and generalized variables $\overline{t}$ (see Definition 7). Then $v_i = \rho(t_i)$ and $w = [\![u]\!]_{F,\rho}$. We compute $\mathbf{g}(v_i) \leq \mathbf{g}(\rho) + 1 \leq \kappa' + \mathbf{l}(u) \leq \kappa$, and, using Lemma 31,

$$\mathbf{g}(w) \; \leq \; \max\{\mathbf{g}(\rho), \mathbf{g}(F)\} + \mathbf{l}(u) \; \leq \; \kappa' + \mathbf{l}(u) \; \leq \; \kappa$$

Hence, $f \colon \overline{v} \mapsto w$ is an update based on F, κ and $\mathcal{D}$.

Furthermore, for $F' = F * f \colon \overline{v} \mapsto w$, we have

$$[\![u]\!]_{F,\rho} \; = \; w \; \sqsubseteq \; \max_{\sqsubseteq} F'(f)[\overline{v}] \; = \; F'(f)(\overline{v})$$
$$= \; F'(f)(\dots, \rho(t_i) \dots) \; = \; [\![t]\!]_{F',\rho} \; .$$

$\square$

Definition 47. Let τ be a sequence of instructions, ρ an assignment, F a κ-model for $\mathcal{D}$, and σ a sequence of updates based on F, κ and $\mathcal{D}$. Let $\alpha = \langle F, \sigma, \rho \rangle$. We define $\Phi(\tau, \alpha) = \langle F, \sigma', \rho' \rangle$ by induction on τ:

If τ is the empty sequence, let $\Phi(\langle\rangle, \alpha) = \alpha$

Otherwise, τ is of the form $\tau' : I$ for some instruction I. Let $\langle F, \sigma', \rho' \rangle = \Phi(\tau', \alpha)$ by i.h., and let F' be $F * \sigma'$. We consider cases according to the form of I:

Axiom: For $I = \mathrm{A}[t \to u]$ let $\Phi(\tau, \alpha) = \langle F, \sigma', \rho' \rangle$.
For $I = \mathrm{A}[t \leftarrow u]$ let $\nu = \Psi(t \leftarrow u, \langle F, \sigma', \rho' \rangle)$, and define

$$\Phi(\tau, \alpha) = \langle F, \sigma' * \nu, \rho' \rangle \ .$$

Substitution: If $I = \mathrm{S}{\uparrow}[t, s/x]$, let

$$\Phi(\tau, \alpha) = \langle F, \sigma', \rho'[x \mapsto [\![s]\!]_{F', \rho'}] \rangle \ .$$

If $I = \mathrm{S}{\downarrow}[t, s/x]$, let ρ'' be ρ' but with x removed from its domain: $\rho'' = \rho' \restriction_{\mathrm{dom}(\rho') \setminus \{x\}}$. Then let

$$\Phi(\tau, \alpha) = \langle F, \sigma', \rho'' \rangle \ .$$

Lemma 48. *Let τ be a sequence of instructions for $\mathcal{D}$, ρ an assignment, F a κ-model of $\mathcal{D}$, and σ a sequence of updates based on F, κ and $\mathcal{D}$, satisfying*

$$\max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma)\} + \mathbf{l}(\tau) \leq \kappa \ .$$

Let $\langle F, \sigma', \rho' \rangle$ be $\Phi(\tau, \langle F, \sigma, \rho \rangle)$. Then we have

(1) *σ' is a sequence of updates based on F, κ and $\mathcal{D}$;*
(2) *$\mathbf{sql}(\sigma') \leq \mathbf{sql}(\sigma) + \mathbf{sql}(\tau)$;*
(3) *$\mathbf{g}(\rho'), \mathbf{g}(\sigma') \leq \max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma)\} + \mathbf{l}(\tau)$.*
(4) *$\mathbf{e}(\sigma') \leq \mathbf{e}(\sigma) + \mathbf{l}(\tau)$;*

Proof. Let τ_i be the sequence consisting of the first i elements in τ, for $i = 0, \ldots, \mathbf{sql}(\tau)$. Let $\langle F, \sigma_i, \rho_i \rangle$ be $\Phi(\tau_i, \langle F, \sigma, \rho \rangle)$. We can show by induction on i that

(1) σ_i is a sequence of updates based on F, κ and $\mathcal{D}$;
(2) $\mathbf{sql}(\sigma_i) \leq \mathbf{sql}(\sigma) + \mathbf{sql}(\tau_i)$;
(3) $\mathbf{g}(\rho_i), \mathbf{g}(\sigma_i) \leq \max\{\mathbf{g}(\rho), \mathbf{g}(F), \mathbf{g}(\sigma)\} + \mathbf{l}(\tau_i)$.
(4) $\mathbf{e}(\sigma_i) \leq \mathbf{e}(\sigma) + \mathbf{l}(\tau_i)$;

For $i = 0$ there is nothing to show as $\sigma_0 = \sigma$ and $\rho_0 = \rho$.

In the induction step from i to $i+1$ we have $\tau_{i+1} = \tau_i : I$ for some instruction I. We consider cases according to I.

If $I = \mathrm{A}[t \to u]$ or $I = \mathrm{S}{\downarrow}[t, s/x]$, there is nothing to show as $\sigma_{i+1} = \sigma_i$ and $\mathbf{g}(\rho_{i+1}) \leq \mathbf{g}(\rho_i)$.

In case $I = \mathrm{S}{\uparrow}[t, s/x]$ we have $\sigma_{i+1} = \sigma_i$ and $\rho_{i+1} = \rho_i[x \mapsto [\![s]\!]_{F * \sigma, \rho_i}]$. Thus assertion (1) and (2) follow immediately from i.h. For assertion (3) we compute, using Lemma 31,

$$\mathbf{g}([\![s]\!]_{F * \sigma, \rho_i}) \leq \max\{\mathbf{g}(F), \mathbf{g}(\sigma_i), \mathbf{g}(\rho_i)\} + \mathbf{l}(s) \ .$$

Hence, using i.h.

$$\begin{aligned}
\mathbf{g}(\rho_{i+1}) \ &\leq \ \max\{\mathbf{g}(\rho_i), \mathbf{g}([\![s]\!]_{F * \sigma, \rho_i})\} \\
&\leq \ \max\{\mathbf{g}(F), \mathbf{g}(\sigma_i), \mathbf{g}(\rho_i)\} + \mathbf{l}(s) \\
&\leq \ \max\{\mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\rho)\} + \mathbf{l}(\tau_i) + \mathbf{l}(s) \\
&< \ \max\{\mathbf{g}(F), \mathbf{g}(\sigma), \mathbf{g}(\rho)\} + \mathbf{l}(\tau_{i+1}) \ .
\end{aligned}$$

In case $I = \mathrm{A}[t \leftarrow u]$ we have $\rho_{i+1} = \rho_i$. Let $\nu = \Psi(t \leftarrow u, \langle F, \sigma_i, \rho_i \rangle)$. By Lemma 46 we obtain that ν is an update based on F, κ and $\mathcal{D}$, and that

$$\mathbf{g}(\nu) \ \leq \ \max\{\mathbf{g}(F), \mathbf{g}(\sigma_i), \mathbf{g}(\rho_i)\} + \mathbf{l}(u) \ .$$

The former immediately implies assertion (1) for σ_{i+1}. The latter implies, using i.h.

$$\begin{aligned}
\mathbf{g}(\sigma_{i+1}) \ &\leq \ \max\{\mathbf{g}(\sigma_i), \mathbf{g}(\nu)\} \\
&\leq \ \max\{\mathbf{g}(F), \mathbf{g}(\sigma_i), \mathbf{g}(\rho_i)\} + \mathbf{l}(u) \\
&\leq \ \max\{\mathbf{g}(F), \mathbf{g}(\rho), \mathbf{g}(\sigma)\} + \mathbf{l}(\tau_i) + \mathbf{l}(u) \\
&< \ \max\{\mathbf{g}(F), \mathbf{g}(\rho), \mathbf{g}(\sigma)\} + \mathbf{l}(\tau_{i+1}) \ .
\end{aligned}$$

Thus assertion (3) follows.

For assertion (2) we compute using i.h.

$$\begin{aligned}
\mathbf{sql}(\sigma_{i+1}) \ &= \ \mathbf{sql}(\sigma_i) + 1 \\
&\leq \ \mathbf{sql}(\sigma) + \mathbf{sql}(\tau_i) + 1 \ = \ \mathbf{sql}(\sigma) + \mathbf{sql}(\tau_{i+1}) \ .
\end{aligned}$$

For assertion (4) we compute using i.h.

$$\mathbf{e}(\sigma_{i+1}) \ = \ \max\{\mathbf{e}(\sigma_i), \mathbf{e}(\nu)\} \ \leq \ \mathbf{e}(\sigma) + \mathbf{l}(\tau_i) + \mathbf{l}(t) \ < \ \mathbf{e}(\sigma) + \mathbf{l}(\tau_{i+1}) \ .$$

$\square$

Lemma 49. *Consider* $\tau = \tau_1 :: \tau_2$. *Then*

$$\Phi(\tau, \langle F, \sigma, \rho \rangle) \ = \ \Phi(\tau_2, \Phi(\tau_1, \langle F, \sigma, \rho \rangle))$$

Proof. By induction on τ_1. $\square$

8. Soundness in S_2^1

We are now in the position to prove a form of soundness of pure equational reasoning in S_2^1. As a reminder, $\mathrm{BVar}(\mathcal{D})$ denotes the set of variables occurring in $\mathcal{D}$ that are bound by an application of substitution, see Definition 9.

Lemma 50. *Let $\mathcal{D}$ be a derivation in Variable Normal Form, ρ an assignment such that $\mathrm{dom}(\rho)$ and $\mathrm{BVar}(\mathcal{D})$ are disjoint. Let τ be $\overrightarrow{\mathrm{Inst}}_{\mathcal{D}}$ or $\overleftarrow{\mathrm{Inst}}_{\mathcal{D}}$, and let $\langle F, \sigma', \rho' \rangle$ be $\Phi(\tau, \langle F, \sigma, \rho \rangle)$. Then $\rho' = \rho$.*

Proof. By induction on $\mathcal{D}$. We only consider the case for $\overrightarrow{\mathrm{Inst}}_{\mathcal{D}}$, the case of $\overleftarrow{\mathrm{Inst}}_{\mathcal{D}}$ will be similar. The only rule which changes ρ is an application of Substitution. In this case, $\mathcal{D}$ will be of the form

$$\frac{\begin{array}{c} \mathcal{D}_1 \\ t = u \end{array}}{t[s/x] = u[s/x]}$$

and $\overrightarrow{\mathrm{Inst}}_{\mathcal{D}}$ has the form

$$\mathrm{S}{\uparrow}[t, s/x] : \overrightarrow{\mathrm{Inst}}_{\mathcal{D}_1} : \mathrm{S}{\downarrow}[u, s/x]$$

By assumption we obtain $x \notin \mathrm{dom}(\rho)$ as $x \in \mathrm{BVar}(\mathcal{D})$. The i.h. shows that the evaluation of $\overrightarrow{\mathrm{Inst}}_{\mathcal{D}_1}$ does not change the assignment. Evaluating $\mathrm{S}{\uparrow}[t, s/x]$ changes ρ by mapping x to some value, while evaluating $\mathrm{S}{\downarrow}[u, s/x]$ removes x from the domain of the assignment. Hence, the resulting overall assignment will be ρ again. □

Theorem 51 (S_2^1). *Let $\mathcal{D}$ be a derivation of $t = u$ in Variable Normal Form. Let ρ be an assignment with $\mathrm{dom}(\rho) \subseteq \mathrm{Var}(t, u)$, and F a model for* Ax. *Let σ_1, σ_2 be given by*

$$\langle F, \sigma_1, \rho \rangle = \Phi(\overrightarrow{\mathrm{Inst}}_{\mathcal{D}}, \langle F, \langle\rangle, \rho\rangle)$$
$$\langle F, \sigma_2, \rho \rangle = \Phi(\overleftarrow{\mathrm{Inst}}_{\mathcal{D}}, \langle F, \langle\rangle, \rho\rangle)$$

Then

$$[\![t]\!]_{F,\rho} \sqsubseteq [\![u]\!]_{F * \sigma_1, \rho}$$
$$[\![u]\!]_{F,\rho} \sqsubseteq [\![t]\!]_{F * \sigma_2, \rho}$$

Instead of proving the theorem directly, we prove the following stronger claim.

Claim 52 (S_2^1). *Fix some derivation $\mathcal{D}$ in Variable Normal Form, some model F for* Ax, *and some integer U such that $\mathbf{g}(F) + \mathbf{l}(\mathcal{D}) \leq U$. Let $\kappa = \mathbf{g}(F)$, and $X = \mathrm{Var}(\mathcal{D})$.*

Let $\mathcal{D}_0 \vdash t = u$ be a sub-derivation of $\mathcal{D}$. Let ρ be an assignment, and σ a sequence of updates based on F, U and $\mathcal{D}$ such that

$$\mathrm{dom}(\rho) \subseteq X \setminus \mathrm{BVar}(\mathcal{D}_0)$$
$$\mathbf{g}(\rho), \mathbf{e}(\sigma), \mathbf{g}(\sigma), \mathbf{sql}(\sigma) \leq U - \mathbf{l}(\mathcal{D}_0)$$

Let σ_1, σ_2 be given by

$$\langle F, \sigma_1, \rho \rangle = \Phi(\overrightarrow{\mathrm{Inst}}_{\mathcal{D}_0}, \langle F, \sigma, \rho\rangle)$$
$$\langle F, \sigma_2, \rho \rangle = \Phi(\overleftarrow{\mathrm{Inst}}_{\mathcal{D}_0}, \langle F, \sigma, \rho\rangle)$$

Then

$$[\![t]\!]_{F,\rho} \sqsubseteq [\![u]\!]_{F * \sigma_1, \rho}$$
$$[\![u]\!]_{F,\rho} \sqsubseteq [\![t]\!]_{F * \sigma_2, \rho} \ .$$

Theorem 51 follows from Claim 52 by letting $\mathcal{D}_0 = \mathcal{D}$, ρ as given, $\sigma = \langle\rangle$, and $U = \max\{\mathbf{g}(F), \mathbf{g}(\rho)\} + \mathbf{l}(\mathcal{D})$,

Proof of Claim 52. We argue in S_2^1. Let $\mathcal{D}$, F, κ, and X be given as in the Claim. We prove that for any $\mathcal{D}_0$, ρ, σ, σ_1 and σ_2 satisfying the conditions of the Claim, the assertion of the Claim holds, by induction on $\mathbf{l}(\mathcal{D}_0)$. Thus this is proven by logarithmic induction (LIND) on a Π_1^b-property, which is available in S_2^1 by Theorem 1.

We consider cases according to the last rule applied in $\mathcal{D}_0$. The details for each case follow the same lines as in the proof of Claim 41, except that now σ_1 and σ_2 are not chosen but given by the Φ-function applied to sequences of instances that are extracted from derivations. □

Corollary 53. *The consistency of* **PETS**(Ax) *is provable in* S_2^1.

Proof. We argue in S_2^1. Assume $\mathcal{D}$ is a **PETS**(Ax) derivation ending in $0 = 1$. Using Proposition 11 we can assume that $\mathcal{D}$ is in Variable Normal Form. Let ρ be the empty assignment, and F the empty model for Ax. Let σ_1 be given by

$$\langle F, \sigma_1, \rho \rangle \quad = \quad \Phi(\overrightarrow{\mathrm{Inst}}_{\mathcal{D}}, \langle F, \langle \rangle, \rho \rangle)$$

By the previous Theorem 51, we obtain

$$0 \quad = \quad [\![0]\!]_{F,\rho} \quad \sqsubseteq \quad [\![1]\!]_{F*\sigma_1,\rho} \quad = \quad 1$$

which is impossible. □

REFERENCES

[1] Arnold Beckmann, *Proving consistency of equational theories in bounded arithmetic*, Journal of Symbolic Logic **67** (2002mar), no. 1, 279–296.

[2] Samuel R. Buss, *Bounded arithmetic*, Bibliopolis, Naples, Italy, 1986. Revision of 1985 Princeton University Ph.D. thesis.

[3] _____, *Relating the bounded arithmetic and polynomial-time hierarchies*, Annals of Pure and Applied Logic **75** (1995), 67–77.

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

[5] Stephen A. Cook, *Feasibly constructive proofs and the propositional calculus*, Proceedings of the seventh annual acm symposium on theory of computing, 1975, pp. 83–97.

[6] Jan Krajíček, *Bounded arithmetic, propositional calculus and complexity theory*, Cambridge University Press, Heidelberg, 1995.

[7] Jan Krajíček, Pavel Pudlák, and Gaisi Takeuti, *Bounded arithmetic and the polynomial hierarchy*, Annals of Pure and Applied Logic **52** (1991), 143–153.

[8] Pavel Pudlák, *A note on bounded arithmetic*, Fundamenta Mathematicae **136** (1990), no. 2, 85–89.

[9] Yoyuki Yamagata, *Consistency proof of a fraement of pv with substitution in bounded arithmetic*, The Journal of Symbolic Logic **83** (2018), no. 3, 1063–1090.

[10] Domenico Zambella, *Notes on polynomially bounded arithmetic*, Journal of Symbolic Logic **61** (1996), 942–966.