Undecidability results for simple induction proofs

Sebastian Eberhard* Stefan Hetzl **

March 17, 2014

Abstract

In our [4] an algorithm IndProof has been proposed which automatically produces inductive proofs of Σ_1 sequents of the form $\Sigma[\alpha] := \Gamma \Rightarrow B[\alpha]$ with α only occurring in the quantifier-free formula B. The input of IndProof is given as a collection of Herbrand sequents of instances $\Sigma[\overline{n}]$ for $n \in \mathbb{N}$. Undecidability of certain problems plays an important role in the design of the algorithm IndProof of [4]. In this paper we deliver proofs of the undecidability of these problems which were skipped in [4] because of lack of space.

IndProof uses a two-phased strategy. The first step of IndProof is FindGram which produces a schematic grammar from the input Herbrand sequents. However, FindGram does not give a guarantee that all instance grammars G_n of the output schematic grammar produce Herbrand sequents of $\Gamma \Rightarrow B[\overline{n}]$ for $n \in \mathbb{N}$ since this property is undecidable in general. The second step of IndProof is FindFml which involves an *unbounded* search for a quantifier-free formula solving a specific schematic form of sip. This is because the logical complexity of formulas solving a given schematic form of sip cannot be bounded in general and the problem whether a solution exists at all is undecidable.

The results of this paper are also of some interest independently of [4] since they nicely fit into active research areas of propositional schemata and second-order quantifier elimination.

1 The undecidability results

Remark 1 *This paper is premarily designed as completion of our [4] where the proofs of some lemmas were not given because of lack of space. For the definitions of the concepts used in this paper we refer to [4].*

We will prove three undecidability results. The first undecidability result is given as follows.

*Institute of Discrete Mathematics and Geometry, Vienna University of Technology, Wiedner Hauptstrae 8-10, AT-1040 Wien, Austria. Email: eberhard@iam.unibe.ch.

**Institute of Discrete Mathematics and Geometry, Vienna University of Technology, Wiedner Hauptstrae 8-10, AT-1040 Wien, Austria. Email: stefan.hetzl@tuwien.ac.at. Homepage: http://www.logic.at/staff/hetzl/

Theorem 2 *Assume* $\Sigma[\alpha] := \Gamma \Rightarrow B[\alpha]$ *is a* Σ_1 *sequent with* α *only occurring in the quantifier-free formula* B*. Then, it is undecidable whether for an input schematic grammar* G*, all of its instance grammars* G_n *produce Herbrand sequents of* $\Sigma[\overline{n}]$*.*

This theorem was mentioned in [4] on page (TODO: insert number) and explains why the algorithm FindGram defined in [4] does not check whether its output grammar is a schematic grammar for the whole $\mathbb{N}$. The second undecidability result is given as follows.

Theorem 3

- *It is undecidable whether an input schematic form of sip is solvable.*
- *It is undecidable whether an input schematic form of sip produced from a grammar* G *with sequent* $\Gamma \Rightarrow B[\alpha]$ *with* G_n *producing a Herbrand sequent of* $\Gamma \Rightarrow B[\overline{n}]$ *for all* $n \in \mathbb{N}$ *is solvable.*

This theorem was mentioned on page (TODO: insert number) in [4]. The second statement of the theorem which clearly implies the first one is of particular importance for [4] since in the context of algorithm IndProof, it only makes sense to solve schematic forms of sip produced from schematic grammars which fulfil the above stated correctness condition. The theorem justifies that the algorithm $\mathsf{FindFml}^c$ defined in [4] searches for solutions of unbounded logical complexity of the schematic form of sip of its input schematic grammar. The third undecidability result is given as follows.

Theorem 4 *Let* $\Gamma \Rightarrow B[\alpha]$ *be a* Σ_1 *sequent with* α *only occurring in the quantifier-free formula* B*. Then, it is undecidable whether there exists a simple induction proof with conclusion* $\Gamma \Rightarrow B[\alpha]$*.*

This result justifies the fact that in [4] the main algorithm IndProof does not yield a decision procedure for the question whether there is a simple induction proof with an input Σ_1 sequent $\Gamma \Rightarrow B[\alpha]$ given as before as conclusion.

All three undecidability results are proved by reductions of Post's correspondence problem (PCP) to the mentioned decision problems.

2 Related research

The first and second undecidability result are of interest independently of [4]. Let us cite some related research.

An undecidability result similar to our first undecidability result has been obtained by Aravantinos, Caferra, and Peltier in [2]. The authors analyse schemas S which from an input natural number n produce a propositional formula $S(n)$ for each $n \in \mathbb{N}$. They proved undecidability of the question whether there is an $n \in \mathbb{N}$ such that $S(n)$ is satisfiable. We will set this result into relation to our first undecidability result later.

Let us now switch to our second undecidability result. Schematic forms of sip S are given as list of three sequents, S_1, S_2, S_3. Let the formula F_S be given as $S_1 \wedge S_2 \wedge S_3$. Note

that F_S is a quantifier-free formula possibly containing free first-order variables $\alpha, \beta, \nu, \gamma$[1]. The solvability of a schematic form of sip S can be reformulated as follows: Is the sentence $\exists X \forall \overline{y} F_S[X, \vec{y}]$ valid in second-order logic with equality, where the quantifier $\exists X$ is restricted to predicates defined by quantifier-free formulas, and where $\overline{y} = \alpha, \beta, \nu, \gamma$? For F being an arbitrary quantifier-free formula, it can be proved easily that the validity of $\exists X \forall \overline{y} F_S[X, \overline{y}]$ is undecidable independently of whether the second order quantifier is restricted. This is acomplished by choosing F such that it formalises the term transformation rules of the lambda calculus. The undecidability then follows from undecidability of certain properties of the lambda calculus. The difficulty of this paper was to show undecidability of validity of $\exists X \forall \vec{y} F[X, \vec{y}]$ already for F restricted to formulas obtained as F_S for some schematic form of sip S.

Several authors analysed the validity of statements of the form $\exists X \forall \vec{y} F[X, \vec{y}]$ in second order logic with equality, for first-order formulas F with parameter X of varying complexity, and $\overline{y}$ being an arbitrary vector of free variables. The authors we cite in the following did not restrict the second order quantifier in any way. For $F[X]$ being a closed quantifier-free formula, Weller proved in [6] that there always exists a witness G_F such that $\exists X F[X] \leftrightarrow F[G_F]$ is valid in second order logic with equality. Since the witness G_F can be constructed primitive recursively from F, this result yields the decidability of the validity of sentences of the form $\exists X F[X]$ for F closed, and quantifier-free.

The $SCAN$ algorithm presented and implemented by Gabbay and Ohlbach in [5] produces for an input formula of the form $\exists X \forall \vec{y} F[X, \vec{y}]$ for F being a first order formula with parameter X a set $\mathcal{S}$ of logical consequences of $\exists X \forall \vec{y} F[X, \vec{y}]$ in second order logic with equality without occurrences of X. A Skolemisation of F is used for this purpose. By transferring a proof of a similar result by Ackermann [1], it can be shown that the conjunction of all formulas in $\mathcal{S}$ is equivalent to $\exists X \forall \vec{y} F[X, \vec{y}]$ in second order logic with equality. For quantifier-free formulas F, the $SCAN$ algorithm yields a decision strategy for the validity of $\exists X \forall \vec{y} F[X, \vec{y}]$ whenever the set $\mathcal{S}$ can be computed effectively. Especially, for closed quantifier-free formulas F, $SCAN$ decides the validity of $\exists X F[X]$. As long as $\mathcal{S}$ is a finite set, the $SCAN$ algorithm find first-order formulas equivalent to the given second order formula of the form $\exists X \forall \vec{y} F[X, \vec{y}]$. This is of great interest for modal logic where this strategy yields a translation of modal axioms into frame conditions in many cases of practical interest.

However, the $SCAN$ algorithm does not determine the decidability of the solvability of schematic forms of sip. This is because for S being a schematic form of sip, in general $SCAN$ produces an infinite set $\mathcal{S}$ for the input $\exists X \forall \vec{y} F_S[X, \vec{y}]$. In addition, $SCAN$ does not restrict the second order quantifier to predicates having quantifier free definitions.

In his [3], van Benthem devides sentences of the form $\exists X \forall \vec{y} F[X]$ for F being a quantifier-free first-order formula with parameter X into three classes according to their complexity.

- Sentences of the form $\exists X \exists \vec{y} F[X, \vec{y}]$ are always equivalent to some first-order sentence.
- Sentences of the form $\exists X \forall \vec{y} F[X, \vec{y}]$ are equivalent to some infinite disjunction of infinite conjunctions of first-order sentences.

[1]For the argumentation it is irrelevant that schematic forms of sip may contain arbitrary additional variables.

- Sentences of the form $\exists X \forall \vec{y} \exists \vec{z} F[X, \vec{y}, \vec{z}]$ are equivalent to some Σ_1^1 sentence.

For each class C_1 of higher complexity than a class C_2 there is a sentence in C_1 not fulfilling the above mentioned property of sentences of class C_2.

3 Post's correspondence problem

For technical reasons, we will work with two versions of Post's correspondence problem (PCP). The standard PCP and the modified PCP. These two versions will be defined in the following.

Notations 5 *Words are produced as usual from the empty word* 0 *by applying unary successor functions. For* $n \in \mathbb{N}$*, n-ary words are produced using the successors* $\mathsf{s}_1, \cdots, \mathsf{s}_n$*. Binary words are produced using the successors* $\mathsf{s}_1, \mathsf{s}_2$*. For a words* v, w *we write* $v * w$ *for the concatenation of* v *and* w*.*

Both versions of PCP share the notion of instance.

Definition 6 (Instance of standard/modified PCP) *An instance* $\mathcal{P}$ *of the standard/modified PCP is given as a list of words*

$$< w_1, v_1 >, \cdots, < w_{|\mathcal{P}|}, v_{|\mathcal{P}|} >$$

for $|\mathcal{P}| \in \mathbb{N}$ *where* $|\mathcal{P}| \geq 2$*, and where* $w_1 \neq v_1$ *and* $w_1, v_1 \neq 0$*.*

The difference between the original PCP and its modification is what counts as a solution.

Definition 7 (Solution of instance of standard PCP) *Let* $\mathcal{P}$ *be an instance of PCP. We say that* $n \in \mathbb{N}$ *with* $n > 0$ *is a solution of* $\mathcal{P}$ *if there are* $1 \leq q_1, q_2, \cdots, q_n \leq |\mathcal{P}|$ *such that*

$$w_{q_1} * w_{q_2} * \cdots * w_{q_n} = v_{q_1} * v_{q_2} * \cdots * v_{q_n}.$$

Definition 8 (Solution of instance of modified PCP) *Let* $\mathcal{P}$ *be an instance of the modified PCP. We say that* $n \in \mathbb{N}$ *is a solution of* $\mathcal{P}$ *if there are* $1 \leq q_1, q_2, \cdots, q_n \leq |\mathcal{P}|$ *such that*

$$w_{q_1} * w_{q_2} * \cdots * w_{q_n} * w_1 = v_{q_1} * v_{q_2} * \cdots * v_{q_n} * v_1.$$

The formalisation of the membership problem for Turing machines yields the undecidability of the modified PCP. The modified PCP can be reduced to the standard PCP which in total yields the following well-known theorem.

Theorem 9 *It is undecidable whether an input instance* $\mathcal{P}$ *of the standard/modified PCP has a solution.*

4 Undecidability whether instance grammars produce quasi-tautologies

In this section, we give the tedious proof of the following theorem.

Theorem 10 *Assume $\Sigma[\alpha] := \Gamma \Rightarrow B[\alpha]$ is a Σ_1 sequent with α only occurring in the quantifier-free formula B. Then, it is undecidable whether for an input schematic grammar G, all of its instance grammars G_n produce Herbrand sequents of $\Sigma[\overline{n}]$.*

Notations 11 *For an instance grammar G_n of a schematic grammar G, we say that a formula is derivable from $\mathcal{L}(G_n)$ if it is derivable in predicate logic with equality from the conjunction of the formulas corresponding to the language $\mathcal{L}(G_n)$ as described in [4] on page (TODO: insert number).*

For the proof of the theorem, we fix an arbitrary instance $\mathcal{P}$ of the standard PCP. We will produce a schematic grammar G such that for each $n \in \mathbb{N}$ G_n produces a Herbrand sequent of $\Sigma[\overline{n}]$ for a certain Σ_1 sequent Σ exactly if n is no solution of $\mathcal{P}$. It follows that the instance grammar G_n produces a Herbrand sequent of $\Sigma[\overline{n}]$ for all $n \in \mathbb{N}$ exactly if $\mathcal{P}$ does not have a solution. This property is undecidable for some instances $\mathcal{P}$ of PCP which yields theorem 10. Our strategy is as follows: Lists of n pairs of $\mathcal{P}$ are formalised as $pair_{q_1}(pair_{q_2}(\cdots pair_{q_n}(0)\cdots))$ for unary constants $pair_{q_1}, \cdots, pair_{q_n}$ and the empty word 0. Functions lw (leftword), and rw (rightword) will allow us to extract the words $w_{q_1} * w_{q_2} * \cdots * w_{q_n}$ and $v_{q_1} * v_{q_2} * \cdots * v_{q_n}$ from the pair chain displayed above. Let us call the sequent the instance grammar G_n for $n \in \mathbb{N}$ produces instances of $\Gamma \Rightarrow B[\alpha]$. Γ will contain i.a. axioms for lw, rw and the *pair* constants, and G_n will produce instances of these axioms to simplify terms of the form $\mathsf{lw}(pair_{q_1}(pair_{q_2}(\cdots pair_{q_i}(0)\cdots)))$ or $\mathsf{rw}(pair_{q_1}(pair_{q_2}(\cdots pair_{q_i}(0)\cdots)))$ for $0 \leq i \leq n$. Finally, $B[\overline{n}]$ is chosen such that it follows from $\mathcal{L}(G_n)$ exactly if for all lists of pairs p of $\mathcal{P}$ of length n, the words $\mathsf{lw}(p)$ and $\mathsf{rw}(p)$ are not equal. In more detail, $B[\overline{n}]$ is given as $P[\overline{n}] \to Q[\overline{n}]$ for propositional variables P, Q. Its proof will require a chain of implications of length $|\mathcal{P}|^n$ which is exactly the number of lists of word pairs of $\mathcal{P}$ of length n. Each such list $pair_{q_1}(pair_{q_2}(\cdots pair_{q_n}(0)\cdots))$ will have a corresponding piece of the implication chain which will be derivable from $\mathcal{L}(G_n)$ exactly if

$$w_{q_1} * w_{q_2} * \cdots * w_{q_n} \neq v_{q_1} * v_{q_2} * \cdots * v_{q_n}.$$

Accordingly, the whole implication chain will be derivable from $\mathcal{L}(G_n)$ exactly if n is no solution of $\mathcal{P}$.

Notations 12

- *In the following, we will work in a setting of $|\mathcal{P}|$-ary words, and just call them words in the following.*
- *Let max denote the maximal length of a word contained in one of the pairs of $\mathcal{P}$.*
- *Let the function q enumerate all pairs $< w, v >$ of $|\mathcal{P}|$-ary words such that $|w|, |v| \leq max$. Let us assume that $dom(q) = [1, m]$ for $m \in \mathbb{N}$. If $q(n) =< w, v >$, then $q_0(n) := w$ and $q_1(n) := v$. Let us assume that q restricted to $[1, |\mathcal{P}|]$ enumerates exactly the pairs of $\mathcal{P}$.*

- *We assume that the successor on numbers* s *and* s_1 *are identical symbols.* $\overbrace{\mathsf{s}_1 \cdots \mathsf{s}_1}^{n \text{ times}}(0)$ *is abbreviated as usually by* $\overline{n}$*.*

Notations 13
- *Remember that the* Σ_1 *sequent the instance grammars* G_n *will produce instantiations of is denoted as* $\Gamma \Rightarrow B[\alpha]$*.*
- *For a formula of the form* $\forall x B[x]$*, we refer to* $B[t]$ *as* t *instance of* $\forall x B[x]$ *or of* $B[x]$*.*
- lw *(leftword),* rw *(rightword),* Ord *(order),* s_ℓ *(lexicographic successor) denote pairwise different fresh unary constants.*

Definition 14 Γ *is given as the collection of the following formulas which will be defined in the following:*

- lw *axioms,* rw *axioms,* Ord *axioms,* s_ℓ *axioms, successor axioms, Post axioms, zero case axiom.*

We list these axioms in the following, omitting the quantifier over the variable x *in each axiom.*

- *The* lw *axioms are given as follows where for all* $1 \leq i \leq m$ $pair_i$ *is a fresh unary constant.*

$$\begin{array}{l} \mathsf{lw}(pair_1 x) = q_0(1) * (\mathsf{lw}x) \\ \cdots \\ \mathsf{lw}(pair_m x) = q_0(m) * (\mathsf{lw}x) \\ \mathsf{lw}(0) = 0 \end{array}$$

- *The* rw *axioms are given analogously.*

$$\begin{array}{l} \mathsf{rw}(pair_1 x) = q_1(1) * (\mathsf{rw}x) \\ \cdots \\ \mathsf{rw}(pair_m x) = q_1(m) * (\mathsf{rw}x) \\ \mathsf{rw}(0) = 0 \end{array}$$

- *The* Ord *axioms are given as follows.*

$$\begin{array}{l} \mathsf{Ord}(pair_1 x) = \mathsf{s}_1(\mathsf{Ord}x) \\ \cdots \\ \mathsf{Ord}(pair_{|\mathcal{P}|} x) = \mathsf{s}_{|\mathcal{P}|}(\mathsf{Ord}x) \\ \mathsf{Ord}(0) = 0 \end{array}$$

- *The* s_ℓ *axioms are given as follows.*

$$\begin{array}{l} \mathsf{s}_\ell(\mathsf{s}_1 \mathsf{lw}x) = \mathsf{s}_2 \mathsf{lw}x \\ \mathsf{s}_\ell(\mathsf{s}_2 \mathsf{lw}x) = \mathsf{s}_3 \mathsf{lw}x \\ \cdots \\ \mathsf{s}_\ell(\mathsf{s}_\mathcal{P} \mathsf{lw}x) = \mathsf{s}_1 \mathsf{s}_\ell \mathsf{lw}x \\ \mathsf{s}_\ell(0) = 0 \end{array}$$

- *The successor axioms are given as follows.*

$$\begin{array}{ll} \mathsf{s}_i\mathsf{lw}x \neq 0 & \text{for } 1 \leq i \leq m \\ \mathsf{s}_i\mathsf{lw}x \neq \mathsf{s}_j\mathsf{rw}x & \text{for } 1 \leq i \neq j \leq m \\ \mathsf{s}_i\mathsf{lw}x = \mathsf{s}_i\mathsf{rw}x \rightarrow \mathsf{lw}x = \mathsf{rw}x & \text{for } 1 \leq i \leq m \end{array}$$

- *The post axioms are given as follows where P, Q denote unary propositional variables.*

$$\begin{array}{l} \mathsf{lw}x \neq \mathsf{rw}x \rightarrow (P(\mathsf{Ord}(x)) \rightarrow Q(\mathsf{s}_\ell\mathsf{Ord}(x)) \\ \mathsf{lw}x \neq \mathsf{rw}x \rightarrow (Q(\mathsf{Ord}(x)) \rightarrow Q(\mathsf{s}_\ell\mathsf{Ord}(x)) \end{array}$$

- *The zero case axiom is given as follows.*

$$P(0) \rightarrow Q(0)$$

We will use the next few pages to explain the meaning of the axioms of Γ. This will typically be achieved by proving simple lemmas about the axioms of Γ.

The functions lw and rw allow to obtain words from chains composed of *pair* constants. Note that a *pair* constant is present for each pair of words with length bounded by max.

Notations 15
- *Let $\mathcal{L}_n$ and $\mathcal{R}_n$ denote the set of instances $pair_{q_1}(\cdots pair_{q_i}(0)\cdots)$ for $0 \leq i \leq n$ and $1 \leq q_1, \cdots, q_i \leq m$ of the lw axioms or the rw axioms, respectively.*
- *A term of the form $pair_{q_1}(\cdots pair_{q_i}(0)\cdots)$ is called a pair chain in the following. We drop the brackets in pair chains in the following.*

Lemma 16 *Let $< w, v >$ be a pair of words with $|w|, |v| \leq n \cdot max$ for $n \in \mathbb{N}$. Then, there exists a term $t := pair_{q_1} \cdots pair_{q_n} 0$ such that $\mathsf{lw}(t) = w$ and $\mathsf{rw}(t) = v$ are logically[2] implied by $\mathcal{L}_n \cup \mathcal{R}_n$.*

Proof. Note that finding a term t such that the equations hold is a trivial instance of PCP where all possible pairs of words with bounded length are available. t can be found by intersecting w and v arbitrary and independently into n pieces of length at most max. This uniquely fixes a pair chain. It is easy to see that in order to prove $\mathsf{lw}(t) = w$ only instances of the axioms for lw contained in $\mathcal{L}_n$ have to be used. Analogously for $\mathsf{rw}(t) = v$. □

Let us explain the purpose of the Ord- and s_ℓ-axioms: They will allow us to derive pieces of the earlier mentioned implication chain necessary to derive the consequent $P[\overline{n}] \rightarrow Q[\overline{n}]$.

Remark 17 *The function Ord translates a term of the form $pair_{q_1} \cdots pair_{q_n} 0$ with $1 \leq q_1, \cdots, q_n \leq |\mathcal{P}|$ into the word $\mathsf{s}_{q_1} \cdots \mathsf{s}_{q_n} 0$. Note that only pair chains are translated into words which correspond to possible solutions of $\mathcal{P}$. A term $\mathsf{Ord}(pair_i x)$ for $i > |\mathcal{P}|$ cannot be simplified using the given axioms.*

[2] We always work in predicate logic with equality.

Remark 18 *The function* s_ℓ *reminds of a lexicographic successor on words. The reason for the presence of* lw *in the axioms is that for* x *being instantiated by pair chains, the axioms will yield the expected calculation rules for words due to lemma 16 as intended. This will become clearer later.*

Remark 19 *The following sequence of terms, to be read from the left to the right, is produced by applying* s_ℓ *repeatedly starting from* $\mathsf{s}_1 \cdots \mathsf{s}_1 0$.

$$\begin{array}{l}
\mathsf{s}_1 \cdots \mathsf{s}_1 0, \mathsf{s}_2 \mathsf{s}_1 \cdots \mathsf{s}_1 0, \cdots, \mathsf{s}_{|\mathcal{P}|} \mathsf{s}_1 \cdots \mathsf{s}_1 0, \\
\mathsf{s}_1 \mathsf{s}_2 \mathsf{s}_1 \cdots \mathsf{s}_1 0, \cdots, \mathsf{s}_{|\mathcal{P}|} \mathsf{s}_2 \mathsf{s}_1 \cdots \mathsf{s}_1 0, \\
\cdots \\
\mathsf{s}_1 \mathsf{s}_{|\mathcal{P}|} \mathsf{s}_1 \cdots \mathsf{s}_1 0, \cdots, \mathsf{s}_{|\mathcal{P}|} \mathsf{s}_{|\mathcal{P}|} \mathsf{s}_1 \cdots \mathsf{s}_1 0, \\
\mathsf{s}_1 \mathsf{s}_1 \mathsf{s}_2 \cdots \mathsf{s}_1 0, \cdots \\
\cdots \\
\mathsf{s}_1 \mathsf{s}_{|\mathcal{P}|} \cdots \mathsf{s}_{|\mathcal{P}|} 0, \cdots, \mathsf{s}_{|\mathcal{P}|} \mathsf{s}_{|\mathcal{P}|} \cdots \mathsf{s}_{|\mathcal{P}|} 0, \\
\mathsf{s}_1 \cdots \mathsf{s}_1 0
\end{array}$$

Note that the by repeatedly applying s_ℓ *to a* $|\mathcal{P}|$*-ary word* x*, we will finally obtain* x *again. In addition, each word of length* n *can be obtained by repeatedly applying* s_ℓ *to an arbitrary word of length* n *for all* $n \in \mathbb{N}$.

Next, we explain the successor axioms. They force us to treat syntactically different words as unequal objects.

Lemma 20 *Let* $\mathcal{S}_n$ *denote the set of instances* $pair_{q_1} \cdots pair_{q_i} 0$ *for* $0 \leq i \leq n$ *and* $1 \leq q_1, \cdots, q_i \leq m$ *of the successor axioms. Let* w, v *be two syntactically different words with* $|w|, |v| \leq n \cdot max$.

Then $w \neq v$ *is logically implied by* $\mathcal{S}_n \cup \mathcal{L}_n \cup \mathcal{R}_n$.

Proof. First, assume that w, v are of the form $\mathsf{s}_i w', \mathsf{s}_j v'$ for $i \neq j$. Lemma 16 yields a pair chain t of length smaller or equal n such that $\mathsf{lw}(t) = w'$ and $\mathsf{rw}(t) = v'$ follow from $\mathcal{L}_n$ or $\mathcal{R}_n$, respectively. The corresponding instance of the second successor axiom yields $w \neq v$.

Second, assume that w, v are of the form $\mathsf{s}_i w', \mathsf{s}_i v'$. Again, lemma 16 yields a pair chain t with the same properties as before. The corresponding instance of the third successor axiom yields $w = v \rightarrow w' = v'$. The argumentation is repeated until we

- either deduce that if $w = v$ then two words of the form $\mathsf{s}_i \hat{w}$ and $\mathsf{s}_j \hat{v}$ for $i \neq j$ are equal.
- or deduce that $\mathsf{s}_i \hat{w} = 0$ for a word $\hat{w}$.

The first case has been treated above, yielding that w and v are unequal. The second case is treated similarly using the first successor axiom. □

Let us explain the Post axioms. Their consequens represents pieces of the earlier mentioned chain of implications. Note that each piece of the implication chain will be derivable from Γ exactly if a certain pair chain does not yield a solution of $\mathcal{P}$. Finally, the purpose of the zero case axioms is to turn $\mathcal{L}(G_0)$ into a quasi-tautology.

This concludes the enumeration of the formulas contained in Γ.

Lemma 21 Γ *is a consistent set of formulas.*

Proof. We will build a closed term model $\mathcal{M}$ of Γ. The elements of $\mathcal{M}$ are the equivalence classes of closed terms relative to the equations of Γ for $\mathsf{lw}, \mathsf{rw}, \mathsf{Ord}, \mathsf{s}_\ell$. So, e.g. $[\mathsf{s}_\ell(\mathsf{s}_1\mathsf{lw}0)]_=$ is an element of $\mathcal{M}$ which is equal to $[\mathsf{s}_2 0]_=$. P, Q are interpreted as true propositions in $\mathcal{M}$. $\mathcal{M}$ trivially fulfils all formulas of Γ except of the successor axioms. We prove in the following that $\mathcal{M}$ also fulfils them.

The axioms of the form $s = t$ for $\mathsf{lw}, \mathsf{rw}, \mathsf{Ord}, \mathsf{s}_\ell$ induce a reduction relation R reducing s to t. It can be checked easily that R has the single step diamond property. This implies that R has the Church-Rosser property. Therefore, if $[t_0]_= = [t_1]_=$ the closed terms t_0, t_1 must have a common reduct. Clearly, for any term t all reducts of $\mathsf{s}_i(\mathsf{lw}t)$ are of the form $\mathsf{s}_i(\cdot)$ for all $1 \leq i \leq m$. This immediately implies that the first and second successor axiom hold. The third successor axiom is trivially fulfilled in $\mathcal{M}$. $\square$

Remember that the consequent $B[\alpha]$ is given as $P(\alpha) \to Q(\alpha)$. Note that to derive $B[\overline{n}]$ for $n > 0$ from Γ, we will have to derive $P(\overline{n}) \to Q(\mathsf{s}_\ell\overline{n})$ and $Q(w) \to Q(\mathsf{s}_\ell w)$ for all words w of length n except of $\overline{n}$. This is only possible, if all corresponding instances of $\mathsf{lw}x \neq \mathsf{rw}x$ are true. But this can only be the case if n is not a solution of $\mathcal{P}$. We have to define a schematic grammar G such that this argumentation goes through using only instances of axioms of Γ produced by G_n for each $n \in \mathbb{N}$.

Definition 22 (Grammar G**)** *The schematic grammar G contains exactly the following productions.*

- *For all formulas A whose universal closure is present in Γ, productions of the form $\tau \to \mathsf{r}_{\forall xA[x]}(\beta)$ and $\tau \to \mathsf{r}_{\forall xA[x]}(\gamma)$ are contained in G.*
- $\gamma \to pair_i\gamma$ *for* $1 \leq i \leq m$
- $\gamma_{end} \to 0$

Observe that from productions of G_n, we obtain $pair_{q_1} \cdots pair_{q_i} 0$ instances of all axioms of Γ for $0 \leq i \leq n$. This yields the following lemma.

Lemma 23 *For all $n \in \mathbb{N}$ we have*

$$\mathcal{S}_n \cup \mathcal{L}_n \cup \mathcal{R}_n \subset \mathcal{L}(G_n).$$

Lemma 24 *Assume that n is a solution of $\mathcal{P}$. Then, G_n does not produce a Herbrand sequent of $\Gamma \Rightarrow P[\overline{n}] \to Q[\overline{n}]$.*

Proof. Note that $n > 0$. If n is a solution of $\mathcal{P}$, there exists a certain term $t := pair_{q_1} pair_{q_2} \cdots pair_{q_n} 0$ with $1 \leq q_1, \cdots, q_n \leq |\mathcal{P}|$ for which we can clearly derive

$$\mathsf{lw}pair_{q_1} pair_{q_2} \cdots pair_{q_n} 0 = \mathsf{rw}pair_{q_1} pair_{q_2} \cdots pair_{q_n} 0 := s_1 = s_2$$

from $\mathcal{L}_n \cup \mathcal{R}_n$ with $\mathcal{L}_n \cup \mathcal{R}_n \subseteq \mathcal{L}(G_n)$ because of lemma 23. Because of the consistency of $\mathcal{L}(G_n)$ we cannot derive $s_1 \neq s_2$ from $\mathcal{L}(G_n)$. The consistency of $\mathcal{L}(G_n)$ together with

lemma 20 implies that we cannot prove that two syntactically different $|\mathcal{P}|$-ary words both of length n are equal. This easily yields that $P(\overline{n}) \to Q(\overline{n})$ can only be derived if we can derive $P(\overline{n}) \to Q(\mathsf{s}_\ell\overline{n})$ and $Q(w) \to Q(\mathsf{s}_\ell w)$ for all $|\mathcal{P}|$-ary words w of length n except of $\overline{n}$. This implies that $P(\overline{n}) \to Q(\overline{n})$ cannot be derived from $\mathcal{L}(G_n)$. $\square$

Lemma 25 *Assume that n is no solution of $\mathcal{P}$. Then, G_n produces a Herbrand sequent of $\Gamma \Rightarrow P[\overline{n}] \to Q[\overline{n}]$.*

Proof. Lemmas 20 and 23 imply that for two words w, v with $|w|, |v| \leq n \cdot max$ if they are syntactically unequal, they can be proved to be unequal from $\mathcal{L}(G_n)$. Together with the assumption of the lemma, this implies that

$$\mathsf{lw}(pair_{q_1} pair_{q_2} \cdots pair_{q_n} 0) \neq \mathsf{rw}(pair_{q_1} pair_{q_2} \cdots pair_{q_n} 0)$$

follows from $\mathcal{L}(G_n)$ for all $1 \leq q_1, \cdots, q_n \leq |\mathcal{P}|$. Therefore, using calculation rules for Ord contained in $\mathcal{L}(G_n)$ we can deduce

$$P(\overline{n}) \to Q(\mathsf{s}_\ell\overline{n}).$$

In addition, we can deduce $Q(w) \to Q(\mathsf{s}_\ell w)$ for all words w of length n. Clearly, the intended calculation rules for s_ℓ are contained in $\mathcal{L}(G_n)$ for $|\mathcal{P}|$-ary words with length smaller or equal n. The above mentioned properties therefore imply $P(\overline{n}) \to Q(\overline{n})$ as requested. $\square$

Finally, theorem 10 follows immediately from lemmas 24 and 25. This finishes the proof of the first undecidability result.

Let us now discuss a related undecidability result given in [2] by Aravantinos, Caferra, and Peltier. As we stated before, the authors analyse schemas S which from an input natural number n produce a propositional formula $S(n)$ with indexed propositional constants for each $n \in \mathbb{N}$. They proved undecidability of the question whether there is an $n \in \mathbb{N}$ such that $S(n)$ is satisfiable for the set of so called homothetic schemas, defined in chapter 6 of [2].

Note that a schematic grammar G also is a schema in the sense described above where $G(n)$ is the formula obtained by taking the conjunction over the formulas corresponding to the terms in $\mathcal{L}(G_n)$ in the sense of [4] page (TODO: insert number). The question whether $\mathcal{L}(G_n)$ produces a Herbrand sequent of $\Gamma \Rightarrow B[\overline{n}]$ for each $n \in \mathbb{N}$ can be reformulated as the question whether $G(n) \wedge \neg B[\overline{n}]$ is satisfiable for some $n \in \mathbb{N}$. Therefore, it makes sense to compare theorem 10 to the undecidability result of [2] presented in chapter 6.

A first major difference is that our logical setting is predicate logic with equality whereas in [2] it is propositional logic with indexed propositional constants (see section 2 of [2]). Indexed propositional constants p_i for $i \in \mathbb{N}$ can be easily simulated in our setting by $P(\bar{i})$ for a predicate P[3]. Nevertheless, homothetic schemata for which undecidability is proved in [2] cannot be simulated in our setting. This is because for homothetic schemata S the formula $S(n)$ may contain positive occurrences of disjunctions with a number of disjuncts growing in n. However, such disjunctions are not contained in formulas of the form $G(n) \wedge \neg B[\overline{n}]$. Because of this reasons, the undecidability results of [2] and theorem 10 seem to be independent.

[3] Also the arithmetic rules holding for indeces can be simulated in our setting.

5 Undecidability of the solvability of schemas

In this section, we give the tedious proof of the following theorem. Some notations similar to the ones of the previous section will be reused.

Theorem 26
- *It is undecidable whether an input schematic form of sip is solvable.*
- *It is undecidable whether an input schematic form of sip produced from a grammar G with sequent $\Gamma \Rightarrow B[\alpha]$ with G_n producing a Herbrand sequent of $\Gamma \Rightarrow B[\overline{n}]$ for all $n \in \mathbb{N}$ is solvable.*

Clearly, the second statement of the lemma implies the first one. We give a proof of the second statement in the following. We will fix an instance $\mathcal{P}$ of the *modified* PCP, and define a schematic form of sip $S_\mathcal{P}$ which has a solution exactly if $\mathcal{P}$ has one. $S_\mathcal{P}$ will satisfy the additional restriction for schemas mentioned in the second statement of the lemma.

The strategy of the proof of theorem 26 is as follows. The side formulas of the schematic form of sip $S_\mathcal{P}$ will contain instances of the axiom $(\forall x)(\mathsf{lw}(x) \neq \mathsf{rw}(x))$ for lw, rw given similarly as in the last section. Informally, it states that $\mathcal{P}$ does not have a solution. If in contrary $\mathcal{P}$ has a solution $n \in \mathbb{N}$, $\mathcal{L}(G_m)$ will be inconsistent for $m \geq n$. This will allow the definition of a solution of $S_\mathcal{P}$ by a finite definition by cases as we will show later. In the case that $\mathcal{P}$ does not have a solution, the axiom $(\forall x)(\mathsf{lw}(x) \neq \mathsf{rw}(x))$ will be without effect for the solvability of $S_\mathcal{P}$. In this case, $S_\mathcal{P}$ will not be solvable for essentially the same reasons as the schema whose unsolvability was demonstrated in the proof of lemma (TODO: insert number) in [4].

We give some notations to prepare the definition of the schematic form of sip $S_\mathcal{P}$ of $\mathcal{P}$.

Notations 27 *Let q be a function enumerating all pairs of words occurring in $\mathcal{P}$. We assume that $q(1)$ yields the first pair of words of $\mathcal{P}$. For $q(i) =< w, v >$, we define $q_0(i) := w$ and $q_1(i) := v$*[4].

Notations 28 *In the following, the successor s is assumed to be syntactically different from the successors $\mathsf{s}_1, \mathsf{s}_2$ occurring in the side formulas.*

Definition 29 (Schematic form of sip S) *The schematic form of sip S is defined as follows,*[5].

- $\mathsf{lw}{-}Ax[\beta], \mathsf{rw}{-}Ax[\beta], post{-}Ax[\beta], P(0) \Rightarrow X[\alpha, 0, \beta]$

  $\mathsf{lw}{-}Ax[\gamma], \mathsf{rw}{-}Ax[\gamma], post{-}Ax[\gamma], P(0), P(\gamma) \rightarrow P(\mathsf{s}\gamma)$
- $X[\alpha, \nu, \gamma], X[\alpha, \nu, pair_1(\gamma)], \cdots, X[\alpha, \nu, pair_m(\gamma)], X[\alpha, \nu, \mathsf{s}\gamma] \Rightarrow X[\alpha, \mathsf{s}\nu, \gamma]$
- $P(0), X[\alpha, \alpha, 0] \Rightarrow P(\alpha)$

[4] Note that in contrast to the proof of theorem 10 the function q does not enumerate all pairs of words of a bounded length.

[5] For brevity we omit some formulas without occurrences of the variables β, ν, γ in the third sequent. This does not have any influence on the argument.

where the side formulas are given as follows:

- *For a variable x $\mathsf{lw}{-}Ax[x]$ denotes the conjunction of the following formulas where for all $1 \leq i \leq |\mathcal{P}|$ $pair_i$ denotes a fresh unary constant.*

$$\begin{array}{l}\mathsf{lw}(pair_1 x) = [q_0(1)](\mathsf{lw}x)\\ \ldots\\ \mathsf{lw}(pair_{|\mathcal{P}|} x) = [q_0(|\mathcal{P}|)](\mathsf{lw}x)\\ \mathsf{lw}(0) = [q_0(1)](0)\end{array}$$

- *For a variable x $\mathsf{rw}{-}Ax[x]$ denotes the conjunction of the following formulas.*

$$\begin{array}{l}\mathsf{rw}(pair_1 x) = [q_1(1)](\mathsf{rw}x)\\ \ldots\\ \mathsf{rw}(pair_|\mathcal{P}|x) = [q_1(|\mathcal{P}|)](\mathsf{rw}x)\\ \mathsf{rw}(0) = [q_1(1)](0)\end{array}$$

- *post$-Ax[x]$ is given as $\mathsf{lw}(x) \neq \mathsf{rw}(x)$.*

Let us explain the definition. In contrast to the proof of theorem 10 the definitions of lw and rw have been modified to deal with the modified PCP. Informally, the post axiom states that $\mathcal{P}$ does not have a solution. The reason to work with the modified PCP is to avoid that the instance 0 of the post axiom is always false.

Next, we prove lemma 32 which states that if $\mathcal{P}$ does not have a solution then $S_\mathcal{P}$ does not have a solution. Then, we prove lemma 40 which states that if $\mathcal{P}$ has a solution then $S_\mathcal{P}$ has a solution. Together, the two lemmas imply theorem 26. We just write S instead of $S_\mathcal{P}$ in the following.

Lemma 30 *S is the schematic form of sip of a schematic grammar G with sequent $\Gamma \Rightarrow B[\alpha]$ such that G_n produces a Herbrand sequent of $\Gamma \Rightarrow B[\overline{n}]$ for each $n \in \mathbb{N}$.*

Proof. S is the schematic form of sip of a schematic grammar G containing i.a. the following rules:

- $\tau \to \mathsf{r}_{P(0)}$
- $\tau \to \mathsf{r}_{\forall x(P(x)\to P(\mathsf{s}x))}(\gamma)$
- $\gamma \to \mathsf{s}\gamma$
- $\gamma_{end} \to 0$

It is easy to see that for each $n \in \mathbb{N}$ its instance grammar G_n produces the straightforward Herbrand sequent of

$$P(0), \forall x(P(x) \to P(\mathsf{s}x)) \Rightarrow P[\overline{n}].$$

This immediately implies the lemma. □

Notations 31
- *For $n \in \mathbb{N}$ and a term s, we write $chain_n(s)$ for an arbitrary term of the form $t_1(t_2(\cdots t_i(s)\cdots))$ where $t_q = \mathsf{s}, pair_1, \cdots, pair_{|\mathcal{P}|}$ for $1 \leq q \leq i$, and $1 \leq i \leq n$ or for the term s.*
- *For a term t, and a formula F, we write $F[chain_n(t)]^*$ for the conjunction of all $chain_n(t)$ instances of $\forall x F[x]$.*

Lemma 32 *If $\mathcal{P}$ does not have a solution, then S does not have a solution.*

Let us give a proof of the lemma in the following. We will need some auxiliary lemmas.

Lemma 33 *Assume that $F[x, y, z]$ is a solution of S. Then for any $n \in \mathbb{N}$ with $n > 0$, the sequent $\Theta(n)$ given as follows is a quasi-tautology.*

$$\begin{array}{l}\mathsf{lw}{-}Ax[chain_n(\gamma)]^*, \mathsf{rw}{-}Ax[chain_n(\gamma)]^*, post{-}Ax[chain_n(\gamma)]^*,\\ P(0), [P(chain_{n-1}(\gamma)) \to P(\mathsf{s}\ chain_{n-1}(\gamma))]^*, F[\alpha, \nu, chain_n(\gamma)]^* \Rightarrow\\ F[\alpha, \mathsf{s}^n\nu, \gamma]\end{array}$$

Proof. For $n, m \in \mathbb{N}$, let $[\nu/\mathsf{s}^m\nu, \gamma/chain_n(\gamma)]$ denote the set of substitutions obtained by substituting all ν occurrences by $\mathsf{s}^m\nu$ and in parallel, all γ occurrences by one of the terms abbreviated by $chain_n(\gamma)$ according to the notations 31. For $n \in \mathbb{N}$ with $n > 0$, carry out all of the substitutions displayed in the list below on the second sequent of $S[X\backslash F]$.

$$[\nu/\nu, \gamma/chain_{n-1}(\gamma)], [\nu/\mathsf{s}\nu, \gamma/chain_{n-2}(\gamma)], \ldots, [\nu/\mathsf{s}^{n-1}\nu, \gamma/\gamma]$$

From the quasi-tautologies resulting by the substitutions and the first sequent of $S[X/F]$, by using repeatedly cuts, we easily derive the sequent $\Theta(n)$. □

Lemma 34 *Assume that F is a solution of S. Then there is a solution F' of S with the same signature as S which is a conjunction of the formulas*

$$EQ_1 \to F_1, \cdots, EQ_n \to F_n$$

where EQ_i is a conjunction only containing (possibly negated) atoms of the form $s = t$ and F_i is a disjunction only containing (possibly negated) atoms of the form $P(\cdot)$.

Proof. Clearly, we can restrict ourselves to solutions in conjunctive normal form of the same signature as S. By rearranging each single clause, we obtain a solution of the required form. □

For the proof of lemma 32, we argue in a specific set of models $\mathcal{M}$.

Definition 35 (Set of models $\mathcal{M}$) *$\mathcal{M}$ denotes a set of models given as follows. The signature of the models in $\mathcal{M}$ is the signature of S:*

$$\{0, \mathsf{s}, \mathsf{s}_1, \mathsf{s}_2, pair_1, \cdots, pair_m, \mathsf{lw}, \mathsf{rw}, P\}$$

The universe of the models in $\mathcal{M}$ is the set of equivalence classes of closed terms relative to instances of the equations $\mathsf{lw}{-}Ax[x]$ and $\mathsf{rw}{-}Ax[x]$. Note that the described models only differ in their interpretation of P.

Notations 36 *We say that a formula F is true in $\mathcal{M}$ if it holds in all models of $\mathcal{M}$. For formulas F, we sometimes abbreviate 'F is true in $\mathcal{M}$' by 'F is true/holds' or just by F.*

Lemma 37 *Assume that $\mathcal{P}$ does not have a solution. Let $\Gamma, \Pi \Rightarrow \Delta$ be a sequent true in $\mathcal{M}$, where Π consists exclusively of instances of $post{-}Ax$, $\mathsf{lw}{-}Ax$ and $\mathsf{rw}{-}Ax$. Then the sequent $\Gamma \Rightarrow \Delta$ is true in $\mathcal{M}$.*

Proof. Note that since we assume that $\mathcal{P}$ does not have a solution, all instances of $post{-}Ax$ are true. The same holds for instances of $\mathsf{lw}{-}Ax$ and $\mathsf{rw}{-}Ax$ by definition of the models in $\mathcal{M}$. Therefore, if we drop these formulas from the antecedent of true sequents in $\mathcal{M}$ we again obtain true sequents in $\mathcal{M}$. □

Note that each term in the signature of the model in $\mathcal{M}$ contains at most one variable. Let us analyse the truth conditions of equations in $\mathcal{M}$ for terms $s[x], t[x]$ with x occurring in s and t. The following properties easily follow by similar arguments as the ones used on page 9 interpreting the equations holding in $\mathcal{M}$ as reduction relation with the one-step diamond property.

Lemma 38 *(A) Assume that the equation $s[\overline{n}] = q$ holds. Then, q is of the form $q'[\overline{n}]$.*

(B) For any $d, n, m \in \mathbb{N}$ we have $s[\overline{n}] = t[\overline{m}]$ exactly if $s[\overline{n+d}] = t[\overline{m+d}]$.

Lemma 39 *Assume that F is a solution of S. Let $m \in \mathbb{N}$ be an upper bound for the depth of terms occurring in F. For all q_1, q_2, n with $q_2 > q_1 > 2n$ and $n > m$ the following properties hold.*

- $EQ_i[\overline{q_1}, \overline{q_1}, 0] \leftrightarrow EQ_i[\overline{q_2}, \overline{q_2}, 0]$ *for all* $1 \leq i \leq n$.
- $EQ_i[\overline{q_1}, \overline{q_1 - n}, chain_n(0)] \leftrightarrow EQ_i[\overline{q_2}, \overline{q_1 - n}, chain_n(0)]$ *for all* $1 \leq i \leq n$.

Proof. We prove the first statement of the lemma. Whenever we write $s[u]$ or $s[v]$ for a term s and variables u, v in this proof, we assume that u, v occur in s. Analogously for $t[u], t[v]$. Because of property (A) of lemma 38, for equations of the form $s[u] = t$ occurring in $F[x, y, z]$ where $u = x, y$ with a closed term t the equation $s[\overline{q_i}] = t$ does not hold for $i = 1, 2$ since t has maximally depth n. For the same reason for equations of the form $s[u] = t[z]$ of $F[x, y, z]$ where $u = x, y$ the equation $s[\overline{q_i}] = t[0]$ does not hold for $i = 1, 2$.

For equations of the form $s[u] = t[v]$ of $F[x, y, z]$ where $u = x, y$ and $v = x, y$ we have that $s[\overline{q_1}] = t[\overline{q_1}]$ holds exactly if $s[\overline{q_2}] = t[\overline{q_2}]$ holds because of property (B) of lemma 38.

In total this implies the first statement of the lemma since we treated all types of equations possibly occurring in F. For the second statement of the lemma, we argue similarly. □

Finally, we are ready for the proof of lemma 32.

Proof.[of lemma 32]
We choose specific q_1, q_2, n as in lemma 39. Lemma 33 implies that the following sequent is a quasi-tautology:

$$\Theta(n)[\alpha/\overline{q_1}][\nu/\overline{q_1 - n}][\gamma/0]$$

According to lemma 37, from this sequent we obtain a sequent $\Theta'(n)$ true in $\mathcal{M}$ by dropping all instances of $\mathsf{lw}{-}Ax, \mathsf{rw}{-}Ax$ and $post{-}Ax$.

Using lemma 34, in $\Theta'(n)$, all of the formulas $F[\overline{q_1}, \overline{q_1 - n}, chain_n(0)]$ and the formula $F[\overline{q_1}, \overline{q_1}, 0]$ can be replaced by specific conjunctions of the form $F_{i_1} \wedge \cdots \wedge F_{i_k}$ which yields the formula $\tilde{\Theta}$, true in $\mathcal{M}$ only containing atoms of the form $P(\cdot)$. The interpretation of $P(t_0)$ and $P(t_1)$ for terms t_0 and t_1 which are unequal in $\mathcal{M}$ is completely independent in all models. Let E_0 and E_1 be the set of equivalent terms of t_0 or t_1, respectively, in $\mathcal{M}$. Therefore, if in a sequent Σ true in $\mathcal{M}$ all atoms of the form $P(q_0)$ with $q_0 \in E_0$ are replaced by $P(q_1)$ with $q_1 \in E_1$, we again obtain a sequent true in $\mathcal{M}$. Therefore, and because of property (A) and property (B) of lemma 38 the replacement of all occurrences of terms $\overline{N}$ with $q_1 \leq N$ by $\overline{N + q_2 - q_1}$ in $\tilde{\Theta}$ yields a formula true in $\mathcal{M}$. Note that on the left side of $\tilde{\Theta}$ exactly atoms are replaced which have been produced by replacing α. On the right side of $\tilde{\Theta}$ exactly atoms are replaced which have been produced by replacing α or ν. From the special choice of q_1, q_2, n, the previous lemma, and the truth of $\tilde{\Theta}$ in $\mathcal{M}$, we deduce that the formula Θ'' given as

$$P(0), (P(chain_{n-1}(0)) \to P(\mathsf{s}\ chain_{n-1}(0)))^*, F[\overline{q_2}, \overline{q_1 - n}, chain_n(0)]^* \Rightarrow F[\overline{q_2}, \overline{q_2}, 0]$$

is true in $\mathcal{M}$.

Assume that u is a term of the form $chain_n(0)$. A similar unfolding of the second sequent of $S[X/F]$ as in the proof of lemma 33 yields

$$P(0), (P(chain_{q_1-n-1}(u)) \to P(\mathsf{s}\ chain_{q_1-n-1}(u)))^* \Rightarrow F[\overline{q_2}, \overline{q_1 - n}, u],$$

using lemma 37. Together with Θ'' this yields

$$P(0), (P(chain_{q_1-1}(0)) \to P(\mathsf{s}\ chain_{q_1-1}(0)))^* \Rightarrow F[\overline{q_2}, \overline{q_2}, 0]$$

which finally yields, using the third sequent of $S[X/F]$, the following sequent.

$$P(0), (P(chain_{q_1-1}(0)) \to P(\mathsf{s}\ chain_{q_1-1}(0)))^* \Rightarrow P(\overline{q_2})$$

This sequent is not true in $\mathcal{M}$. A counter-model interprets P such that it holds exactly on numerals smaller than $\overline{q_2}$. This is a contradiction which rejects the assumption that the schematic form of sip S can be solved. $\square$

Lemma 40 *Assume that $\mathcal{P}$ has a solution. Then, also S has a solution.*

We need some auxiliary definitions and lemmas.

Notations 41 *Let S be the schematic form of sip defined in definition 29, given as usually as a list of sequents S_1, S_2, S_3 with side formulas $\Gamma_0, \Gamma_1, \Gamma_2$, step-terms t_i for $1 \leq i \leq n$ and cut terms u_i for $1 \leq i \leq m$. Since $\Gamma_1[\alpha, \nu, \gamma]$ does not contain α, ν, we just write $\Gamma_1[\gamma]$ instead. Analogously for Γ_0.*

Definition 42 ($C_{S,q}$) *We define a collection of formulas $C_{S,q}[z]$ for each $q \in \mathbb{N}$, and a variable z as follows.*

$$C_{S,0}[z] := \bigwedge \Gamma_0[z]$$
$$C_{S,q+1}[z] := \bigwedge \Gamma_1[z] \wedge \bigwedge_{1 \leq i \leq n} C_{S,q}[t_i[z]]$$

Lemma 43 *$C_{S,n}[0]$ implies $P(\overline{n})$ for each $n \in \mathbb{N}$.*

Proof. It is easy to see that $C_{S,n}[0]$ contains the conjuncts $P(0)$ and $P(\overline{k}) \to P(\overline{k+1})$ for all $0 \leq k \leq n-1$. Clearly, together they imply $P(\overline{n})$. $\square$

Lemma 44 *$C_{S,n}[\gamma]$ logically implies $C_{S,m}[\gamma]$ for $n > m$.*

Proof. This immediately follows from the fact that the empty term is one of the step-terms of S which means that $C_{S,q+1}[z]$ contains the conjunct $C_{S,q}[z]$ for all $q \in \mathbb{N}$. $\square$

Lemma 45 *Assume that $\ell \in \mathbb{N}$ is a solution of $\mathcal{P}$. Then, $C_{S,\ell}[0]$ is inconsistent.*

Proof. We have a pair chain t of length ℓ such that $\mathsf{lw}t = \mathsf{rw}t$. Since $C_{S,\ell}[0]$ contains all necessary calculation rules for rw and lw for arguments which are pair chains of length at most ℓ, we deduce $\mathsf{lw}t = \mathsf{rw}t$ from $C_{S,\ell}[0]$. Nevertheless, $C_{S,\ell}[0]$ also contains the conjunct $\mathsf{lw}t \neq \mathsf{rw}t$ which yields a contradition. $\square$

Proof.[of lemma 40] Assume that $\ell \in \mathbb{N}$ is a solution of $\mathcal{P}$. We claim that a solution $F[x, y, z]$ of S is given as follows.

$$\begin{array}{ll}
y = 0 \to & C_{S,0}[z] \wedge \\
y \neq 0 \wedge y = \overline{1} \to & C_{S,1}[z] \wedge \\
\cdots & \\
y \neq 0 \wedge y \neq \overline{1} \wedge \cdots \wedge y = \overline{\ell - 1} \to & C_{S,\ell-1}[z] \wedge \\
y \neq 0 \wedge y \neq \overline{1} \wedge \cdots \wedge y \neq \overline{\ell - 1} \to & C_{S,\ell}[z]
\end{array}$$

Since x does not occur in $F[x, y, z]$, we just write $F[y, z]$ instead. We have to prove that F is indeed a solution of S. $S_1[X/F]$ clearly is a quasi-tautology. For $S_2[X/F]$ we use a finite distinction by cases which can be justified by classical propositional logic. We have to prove $F[\mathsf{s}\nu, \gamma]$ from the antecedent of $S_2[X/F]$.

(Case 1) $\mathsf{s}\nu = 0$:
From finite distinction of cases, we deduce that $F[\nu, \gamma]$ implies $C_{S,i}[\gamma]$ for a $0 \leq i \leq \ell$. Lemma 44 yields $C_{S,0}[\gamma]$ as required.

(Case 2) $\mathsf{s}\nu = \overline{k}$ with $1 \leq k < \ell$ but $\mathsf{s}\nu \neq \overline{k-1}, \overline{k-2}, \cdots, 0$:
We deduce $\nu \neq \overline{k-2}, \overline{k-3}, \cdots, 0$. This implies that the antecedent of $S_2[X/F]$ logically implies

$$\Gamma_1[\gamma], \bigwedge_{1 \leq i \leq n} C_{S,q}[t_i[\gamma]]$$

for some $k-1 \leq q \leq \ell$. Lemma 44 yields

$$\Gamma_1[\gamma], \bigwedge_{1 \leq i \leq n} C_{S,k-1}[t_i[z]].$$

This is exactly the definition of $C_{S,k}[\gamma]$ which implies $F[\mathsf{s}\nu, \gamma]$.

(Case 3) The case where $\mathsf{s}\nu$ does not equal any numeral smaller than $\overline{\ell}$ is treated similarly.

We have to show that $S_3[X/F]$ is a quasi-tautology. This is done by a finite case distinction on the value of α justified by classical propositional logic.

(Case 1) $\alpha = 0$: The third premise trivially holds.

(Case 2) $\alpha = \overline{k}$ for $1 \leq k < \ell$ but $\alpha \neq \overline{k-1}, \overline{k-2}, \cdots, 0$:
The claim follows from lemma 43.

(Case 3) α does not equal any numeral which is smaller than $\overline{\ell}$: We have $C_{S,\ell}[0]$ which is inconsistent and therefore implies $P(\alpha)$.

□

From lemmas 32 and 40, we derive the following lemma.

Lemma 46 *The schematic form of sip S has a solution exactly if the instance $\mathcal{P}$ of the modified PCP has a solution.*

Since S can be constructed primitive recursively from $\mathcal{P}$, theorem 26 immediately follows from the previous lemma.

6 Undecidability of provability by simple induction proof

We move on to the last undecidability theorem.

Theorem 47 *Let $\Gamma \Rightarrow B[\alpha]$ be a Σ_1 sequent with α only occurring in the quantifier-free formula B. Then, it is undecidable whether there exists a simple induction proof with conclusion $\Gamma \Rightarrow B[\alpha]$.*

Proof. In essence, we prove that determining whether a Σ_1 sequent can be proved by a simple induction proof is not simpler than determining whether it is consistent. Let $\mathcal{F}$ represent a conjunction of the usual axioms for the factorial f defined by head recursion, and $\mathcal{M}$ and $\mathcal{A}$ represent conjunctions of usual axioms for multiplication and addition, respectively. Assume that $\mathcal{P}$ is a particular instance of the modified PCP, and let $\mathsf{lw}{-}Ax[x], \mathsf{rw}{-}Ax[x], post{-}Ax[x]$ be defined as in the last section. Let P be a predicate variable. We define $\Gamma \Rightarrow B[\alpha]$ as follows:

$$\mathcal{F}, \mathcal{M}, \mathcal{A}, \forall x \mathsf{lw}{-}Ax[x], \forall x \mathsf{rw}{-}Ax[x], \forall x post{-}Ax[x], P(0), \forall x(P(x) \to P(\mathsf{s}x)) \Rightarrow P(f(\alpha))$$

First, assume that $\mathcal{P}$ has a solution. This means that a certain collection C of instances of the axioms $\forall x \mathsf{lw}{-}Ax[x], \forall x \mathsf{rw}{-}Ax[x], \forall x post{-}Ax[x]$ is inconsistent. In this case a simple induction proof of $\Gamma \Rightarrow B[\alpha]$ can be defined as follows.

- The induction formula is given as $\bot$.
- π_b has the conclusion $C \Rightarrow \bot$
- π_s has the conclusion $\bot \Rightarrow \bot$
- π_c has the conclusion $\bot \Rightarrow P(f(\alpha))$

Second, assume that $\mathcal{P}$ does not have a solution. Then, for a class of models $\mathcal{M}'$ defined as $\mathcal{M}$ in definition 35 but satisfying in addition all instances of $\mathcal{F}, \mathcal{M}, \mathcal{A}$, we can prove an analogon of lemma 37. This lemma easily implies that the minimal number of instances of a Herbrand sequent of $\Gamma \Rightarrow B[\overline{n}]$ grows in n as fast as the factorial. This immediately implies that there is no schematic grammar with instance grammars producing these Herbrand sequents, since the size of the languages produced by the instance grammars G_n grows only exponentially in n. Therefore, there is no simple induction proof with conclusion $\Gamma \Rightarrow B[\alpha]$. $\Box$

References

[1] Ackermann, W. Untersuchungen über das entscheidungsproblem der mathematischen logik. *Mathematische Annalen 110* (1935), 390–413.

[2] Aravantinos, V., Caferra, R., and Peltier, N. Decidability and undecidability results for propositional schemata. *Journal of Artificial Intelligence Research 40* (2011), 599–656.

[3] Benthem, J., and Doets, K. Higher-order logic. In *Handbook of Philosophical Logic*, D. Gabbay and F. Guenthner, Eds., vol. 1 of *Handbook of Philosophical Logic*. Springer Netherlands, 2001, pp. 189–243.

[4] Eberhard, S., and Hetzl, S. Inductive theorem proving based on tree grammars. preprint available at http://www.logic.at/people/hetzl/research/.

[5] Gabbay, D. M., and Ohlbach, H. J. Quantifier elimination in second–order predicate logic. In *Principles of Knowledge Representation and Reasoning (KR92)* (1992), B. Nebel, C. Rich, and W. Swartout, Eds., Morgan Kaufmann, pp. 425–435. Also published as a Technical Report MPI-I-92-231, Max-Planck-Institut für Informatik, Saarbrücken, and in the *South African Computer Journal*, 1992.

[6] Weller, D. tba. preprint available at http://www.logic.at/people/hetzl/research/.