Notre Dame Journal of Formal Logic
Volume 34, Number 3, Summer 1993

On Propositional Quantifiers in Provability Logic

SERGEI N. ARTEMOV and LEV D. BEKLEMISHEV

Abstract The first order theory of the Diagonalizable Algebra of Peano Arithmetic (DA(PA)) represents a natural fragment of provability logic with propositional quantifiers. We prove that the first order theory of the 0-generated subalgebra of DA(PA) is decidable but not elementary recursive; the same theory, enriched by a single free variable ranging over DA(PA), is already undecidable. This gives a negative answer to the question of the decidability of provability logics for recursive progressions of theories with quantifiers ranging over their ordinal notations. We also show that the first order theory of the free diagonalizable algebra on n independent generators is undecidable iff $n \neq 0$.

1 Introduction Gödel was probably the first to consider the *provability interpretation of modal logic*: according to it the modality $\Box$ is understood as the standard arithmetical Σ_1-predicate $Pr(\cdot)$ expressing provability in Peano arithmetic PA (cf. [15]). A complete axiomatization together with a decision procedure for the propositional modal logic of provability was given in Solovay [21]. On the other hand, it was shown in Artemov [2] and Vardanyan [23] that predicate provability logic has no r.e. axiom systems.

One of the most interesting remaining problems in this area is that of axiomatizability and decidability of the Provability Logic with Propositional Quantifiers (PLPQ). Informally speaking, PLPQ is the set of all formulas in a modal language with quantifiers over propositions, which are true in the standard model of PA under the interpretation of propositional variables as (the Gödel numbers of) arbitrary arithmetic sentences, and $\Box$ as $Pr(\cdot)$. For example, PLPQ contains the "usual" Hilbert–Bernays derivability conditions

$$\forall p, q\ \Box(\Box(p \to q) \to (\Box p \to \Box q)), \quad \forall p\ \Box(\Box p \to \Box\Box p),$$

formalized Löb's theorem

$$\Box\ \forall p\ (\Box(\Box p \to p) \to \Box p)$$

Received July 20, 1992

and many other nontrivial principles:

$$\forall p, q\, \exists r \Box((\Box p \vee \Box q) \leftrightarrow \Box r) \quad \textit{(Goldfarb's Principle),}$$

$$\exists p\, \Box((\Box p \vee \Box \neg p) \rightarrow \Box \bot) \quad \textit{(Rosser's Principle), etc.}$$

There are some difficulties in providing arithmetical interpretations for formulas in the language of PLPQ. For example, $\forall p(\Box p \rightarrow p)$ cannot be naturally interpreted as a single arithmetical sentence, and hence it is not clear what the expression

$$\Box \forall p(\Box p \rightarrow p)$$

could mean. The following algebraic construction, however, gives rise to a robust and natural fragment of PLPQ.

A *Diagonalizable Algebra* (DA) is, by definition, a boolean algebra enriched by a unary operator τ such that

$$\tau 1 = 1,\ \tau x \wedge \tau(x \rightarrow y) \leq \tau y;\ \tau x \leq \tau\tau x;\ \tau(\tau x \rightarrow x) \leq \tau x.$$

The main example of a DA is DA(PA), that is the Lindenbaum boolean algebra of Peano Arithmetic, with the provability formula $Pr(\cdot)$ as the operator τ. The equational theory of DA(PA) can be identified with the propositional provability logic GL (see e.g. Boolos [6] and Smoryński [20]). Solovay's Second Arithmetical Completeness Theorem implies that the universal (and hence, the existential) theory of DA(PA) is decidable.

The full first order theory of DA(PA) represents a fragment of PLPQ, where all propositions occur inside the scopes of $\Box$'s, whereas any quantifiers may only occur outside. The question whether the first order theory of DA(PA) is decidable remains open. The first order theory of the variety of all DA's is undecidable (cf. Montagna [18]), but so far practically nothing is known about the decidability of the first order theories of individual (infinite) DA's.

Let us consider the 0-generated subalgebra $\mathrm{DA(PA)}_0$ of DA(PA). An independent description of $\mathrm{DA(PA)}_0$ was given in Friedman [13], where Problem 35 asks whether the term equality problem for closed terms of $\mathrm{DA(PA)}_0$ is decidable (the affirmative solution was obtained independently by Boolos, Bernardi and Montagna and van Benthem, as noted in [20]).

Theorems 3.4 and 3.7 of this paper state that $Th(\mathrm{DA(PA)}_0)$, i.e. the first order theory of $\mathrm{DA(PA)}_0$, is decidable but not elementary recursive; the decision procedure and nonelementary lower bounds are obtained by a mutual interpretation of this theory and Büchi's weak second order arithmetic WS1S.

Theorem 4.1 says that the theory obtained by adding free variables ranging over DA(PA) to the language of $Th(\mathrm{DA(PA)}_0)$ is undecidable. (Actually, only one such variable is necessary.) This yields the following reduction:

If $\mathrm{DA(PA)}_0$ is first order definable[1] in DA(PA), then $Th(\mathrm{DA(PA)})$ is undecidable.

This theorem has been first proved by Shavrukov, and we have obtained his kind permission to publish (a somewhat sharpened version of) his result with our proof.

As an application of the results of 4.1, Theorem 5.1 gives a negative answer to a question by Feferman[2] on the decidability of propositional provability logics for recursive progressions of theories based on iteration of consistency, with modal

operators corresponding to the theories of a given progression, and with quantifiers ranging over their ordinal notations. We also indicate how to extend this result to other natural types of recursive progressions.

The arithmetical interpretation of the propositional modal language induces a natural isomorphism of $\mathrm{DA(PA)_0}$ and $\mathrm{DA(GL)_0}$ (i.e. the 0-generated free DA). Hence, by Theorem 3.4, $Th(\mathrm{DA(GL)_0})$ is a decidable theory. In Theorem 6.1 we show that, for each $n > 0$, the first order theory of the free DA on n independent generators is (hereditarily) undecidable. A similar result for the free DA on countably many generators could also be easily obtained by methods of Rybakov [19].

2 Canonical Representation of DA(PA)$_0$ In this section we review some well-known results concerning the atomless fragment of propositional provability logic and reformulate them in terms of DA's.

The language of propositional modal logic is that of the ordinary propositional calculus enriched by a unary modal operator $\Box$. The system GL (after Gödel and Löb) is defined by the axioms:

classical tautologies in the modal language;
$\Box(P \to Q) \to (\Box P \to \Box Q)$;
$\Box P \to \Box\Box P$;
$\Box(\Box P \to P) \to \Box P$;

and rules

$P,\ P \to Q \vdash Q$ *(modus ponens);*
$P \vdash \Box P$ *(necessitation).*

Solovay's logic S can be axiomatized by all theorems of GL and the modal reflection schema

$$\Box P \to P,$$

with *modus ponens* as the sole inference rule.

The system GL is complete with respect to finite irreflexive transitive Kripke models (cf. [20]). The First Arithmetical Completeness Theorem for GL due to Solovay [21] states that GL derives exactly those modal formulas which are provable in PA under the interpretation of propositional variables as arbitrary arithmetic sentences, and $\Box$ as $Pr(\ulcorner\cdot\urcorner)$. Solovay's Second Theorem states that, under the same interpretation, the system S axiomatizes the set of all universally true provability schemata.

Visser (preceeded by Boolos in [7]) suggested a convenient format for Kripke semantics for S (cf. [24]). A Kripke model $\mathcal{K} = (K, \prec, \Vdash)$ is called a *tail-model* iff there is a node $r \in K$ such that:

1. $\{x \in K \mid x \prec r\}$ is a linearly ordered subset of K of order type $(\omega + 1)^*$;
2. the set $\{x \in K \mid r \preceq x\}$ is a finite tree;
3. for any $x \in K$ such that $x \prec r$, and for every propositional variable p

$$x \Vdash p \quad \text{iff} \quad r \Vdash p.$$

The set $\{x \in K \mid x \prec r\}$ is usually referred to as the "tail" of the model $\mathcal{K}$. It is not difficult to show that, for any modal formula Q, $S \vdash Q$ iff Q is forced at the lowermost node of every tail-model.

In this section, we are mainly interested in the atomless fragment of GL. *Atomless modal formulas* are those containing no propositional variables, i.e. built up from $\bot$ (falsum) using $\Box$ and boolean connectives. The arithmetical interpretation $*$ of such formulas is defined inductively as follows:

$\bot^* = (0 = 1)$;
$*$ commutes with boolean connectives;
$(\Box Q)^* = Pr(\ulcorner Q^* \urcorner)$.

Thus, by Solovay's First Theorem we have:

$$\mathrm{GL} \vdash Q \quad \text{iff} \quad \mathrm{PA} \vdash Q^*,$$

for every atomless modal formula Q.

The Kripke Completeness Theorem for the atomless fragment of GL could be reformulated in a strengthened form. Consider the structure $(\omega, >)$ as a reverse well-founded Kripke frame. The forcing relation $\Vdash$ of atomless modal formulas on ω is defined uniquely by stipulating that for every $n \in \omega$ $n \nVdash \bot$, $n \Vdash (\cdot)$ commutes with boolean connectives, and

$$n \Vdash \Box Q \Leftrightarrow (\forall m < n \;\; m \Vdash Q).$$

Lemma 2.1 *For every atomless modal formula Q,*

$$\mathrm{GL} \vdash Q \quad \text{iff} \quad \forall m \in \omega \;\; m \Vdash Q.$$

Proof: Easy.

The useful notion of the *trace* of a modal formula is developed in Artemov [1],[3]. For technical reasons we shall deal here with the dual notion of the *spectrum*.

Definition 2.2 The *spectrum* of an atomless formula Q is the set

$$sp(Q) \rightleftharpoons \{n \in \omega \mid n \Vdash Q\}.$$

Lemma 2.3 ([1]) *For any atomless modal formulas Q, R*

1. *$GL \vdash Q \Leftrightarrow sp(Q) = \omega$;*
   $sp(Q \vee R) = sp(Q) \cup sp(R)$,
   $sp(\neg Q) = \omega \setminus sp(Q)$;
2. *$sp(\Box^{n+1}\bot) = \{0, \ldots, n\}$ for all $n \in \omega$;*
3. *$sp(Q)$ is either a finite or a cofinite subset of ω;*
4. *$sp(Q)$ is finite iff Q^* is false.*

Proof: Statement 1 is equivalent to Lemma 2.1; 2 and 3 are obvious; 4 is verified by an easy induction on the build-up of Q. To prove 5 it is sufficient to check the "only if" part of the statement. Suppose that $sp(Q)$ is finite. Then for some $n \in \omega$

$$sp(Q) \subseteq \{0, \ldots, n\}$$

and hence by Statement 3

$$sp(Q) \subseteq sp(\Box^{n+1}\bot).$$

Statements 1 and 2 imply that

$$GL \vdash Q \to (\Box^{n+1}\bot).$$

By the Arithmetical Completeness Theorem

$$\mathrm{PA} \vdash Q^* \to (\Box^{n+1}\bot)^*,$$

consequently if Q^* were true, so would be $(\Box^{n+1}\bot)^*$, which is not the case.

Now we turn to diagonalizable algebras. One of the simplest examples of a DA is the *free DA on n independent generators* $\mathrm{DA(GL)}_n$. It can be described as the Lindenbaum boolean algebra of GL in the language with exactly n propositional variables, the diagonal operator τ being defined in the natural way:

$$\tau([Q]_{\mathrm{GL}}) \rightleftharpoons [\Box Q]_{\mathrm{GL}}.$$

(Here $[Q]_{\mathrm{GL}}$ denotes the equivalence class of a formula Q modulo GL-provable equivalence.) In particular, for $n = 0$ we obtain the Lindenbaum diagonalizable algebra $\mathrm{DA(GL)}_0$ of the atomless fragment of GL. The full Lindenbaum algebra DA(GL) is identified with the free DA on countably many independent generators.

The arithmetical interpretation $*$ induces a natural homomorphism of $\mathrm{DA(GL)}_0$ into DA(PA):

$$[Q]_{\mathrm{GL}} \longmapsto [Q^*]_{\mathrm{PA}}.$$

The First Arithmetical Completeness Theorem ensures that for any atomless modal formulas Q and R

$$\mathrm{PA} \vdash Q^* \leftrightarrow R^* \quad \text{iff} \quad \mathrm{GL} \vdash Q \leftrightarrow R.$$

Hence $*$ is a monomorphism. Clearly, the arithmetical interpretations of atomless modal formulas constitute (modulo PA-provable equivalence) exactly the 0-generated subalgebra $\mathrm{DA(PA)}_0$ of DA(PA). We immediately obtain the following.

Corollary 2.4 $\mathrm{DA(PA)}_0$ *is isomorphic to* $\mathrm{DA(GL)}_0$.

For a subset $X \subseteq \omega$ define:

$$m(X) \rightleftharpoons \{0, \ldots, \min(\omega \setminus X)\},$$

where we assume $\min \varnothing = \infty$ and thus $m(\omega) = \omega$.

Lemma 2.5 *For every atomless modal formula* Q

$$sp(\Box Q) = m(sp(Q)).$$

Proof: This is just a reformulation of one of the inductive clauses of the definition of forcing on ω.

Corollary 2.6 *The boolean algebra* DA_0 *of the finite and cofinite subsets of* ω *together with the operator* m *is a* DA, *and* $sp(\cdot)$ *is an isomorphism of* $\mathrm{DA(GL)}_0$ *and* DA_0.

Proof: By Lemmas 2.3 and 2.5 $sp(\cdot)$ is a homomorphism of $\mathrm{DA(GL)}_0$ into DA_0. Lemma 2.1 ensures that $sp(\cdot)$ is a monomorphism. To show that $sp(\cdot)$ is onto, for every $n \in \omega$ and every finite $X \in \omega$ consider the following atomless formulas:

$$C_n \rightleftharpoons \Box^{n+1} \bot \wedge \neg \Box^n \bot$$

and

$$C_X \rightleftharpoons \bigvee_{n \in X} C_n.$$

An easy calculation using Lemma 2.3 shows that

$$sp(C_n) = \{n\} \qquad \text{and} \qquad sp(C_X) = X.$$

Hence all finite (and consequently, all cofinite) subsets of ω are within the range of $sp(\cdot)$.

Corollaries 2.4 and 2.6 combined together imply that $\mathrm{DA(PA)}_0$ is isomorphic to DA_0. This isomorphism is called the *canonical representation* of $\mathrm{DA(PA)}_0$. From now on we do not distinguish $\mathrm{DA(PA)}_0$ or $\mathrm{DA(GL)}_0$ from DA_0.

3 An equivalence between Th(DA$_0$) and WS1S We begin this section with an explicit description of formal languages involved.

The language $\mathcal{L}_1$ of the first order theory of DA_0 contains variables $x_0, x_1, \ldots$ ranging over the finite and cofinite subsets of ω; constants $\mathbf{0}$ and $\mathbf{1}$ (for the empty set and for ω respectively); functional symbols for boolean operations $\cap, \cup, -$; a functional symbol m for the diagonal operator, and $=$ as the only predicate symbol. The theory $Th(\mathrm{DA}_0)$ is the collection of all $\mathcal{L}_1$-formulas valid in ω under the natural interpretation.

The language $\mathcal{L}_2$ of WS1S contains two sorts of variables: $a_0, a_1, \ldots$ for natural numbers and $A_0, A_1, \ldots$ for finite subsets of ω; a constant 0 (for the number 0); binary predicate symbols $<$ and $=$ for the standard relations on natural numbers and a binary predicate symbol $\in$. WS1S is the collection of all valid $\mathcal{L}_2$-formulas.[3]

To define an embedding of $Th(\mathrm{DA}_0)$ into WS1S we need an auxiliary language $\mathcal{L}_1'$ obtained by adding to $\mathcal{L}_1$ an infinite list of new variables $A_0, A_1, \ldots$ ranging over the finite subsets of ω. A translation α of $\mathcal{L}_1$-formulas to $\mathcal{L}_1'$-formulas is defined inductively by specifying that α preserves atomic formulas; α commutes with boolean connectives and for all $\mathcal{L}_1$-formulas F,

$$\alpha(\forall x_i\ F(x_i)) \rightleftharpoons \forall A_i\ (\alpha(F)(A_i) \wedge \alpha(F)(-A_i)).$$

Lemma 3.1 *For every $\mathcal{L}_1$-sentence Q*

$$\omega \vDash Q \text{ iff } \omega \vDash \alpha(Q).$$

Proof: Follows by a straightforward induction on the build-up of Q.

Note that for any $\mathcal{L}_1$-formula Q, all the quantifiers occurring in $\alpha(Q)$ actually range over the finite subsets of ω. Therefore, if Q is a sentence, $\alpha(Q)$ does not contain other variables than $A_0, A_1, \ldots$.

We shall define a translation β of $\mathcal{L}_1'$-formulas in the alphabet $A_0, A_1, \ldots$ into the language $\mathcal{L}_2$ of WS1S. For every $\mathcal{L}_1'$-term $t(A_0, \ldots, A_n)$ a $\mathcal{L}_2$-formula "$a \in t(A_0, \ldots, A_n)$" is defined by induction on the build-up of t as follows:

$$\text{“}a \in A_i\text{”} \rightleftharpoons (a \in A_i);$$

$$\text{“}a \in \mathbf{0}\text{”} \rightleftharpoons (0 \neq 0), \qquad \text{“}a \in \mathbf{1}\text{”} \rightleftharpoons (0 = 0);$$

$$\text{“}a \in t \cup s\text{”} \rightleftharpoons (\text{“}a \in t\text{”} \vee \text{“}a \in s\text{”}), \text{“}a \in t \cap s\text{”} \rightleftharpoons (\text{“}a \in t\text{”} \wedge \text{“}a \in s\text{”});$$

$$\text{“}a \in -t\text{”} \rightleftharpoons \neg\text{“}a \in t\text{”};$$

$$\text{“}a \in m(t)\text{”} \rightleftharpoons \forall b\ (b < a \rightarrow \text{“}b \in t\text{”}).$$

By definition, the translation β commutes with boolean connectives and quantifiers of the form $\forall A_i(\cdot)$ and $\exists A_i(\cdot)$, and for atomic formulas β is defined as follows: for any terms t and s in the alphabet $A_0, A_1, \ldots$

$$\beta(t = s) \rightleftharpoons \forall a(\text{“}a \in t\text{”} \leftrightarrow \text{“}a \in s\text{”}).$$

Lemma 3.2 *For each $\mathcal{L}_1'$-sentence Q containing variables for finite subsets of ω only,*

$$\omega \vDash Q \text{ iff } \omega \vDash \beta(Q).$$

Proof: Since β commutes with quantifiers and boolean connectives, it suffices to verify the lemma for atomic formulas Q. By Lemmas 2.3 and 2.5, for every $\mathcal{L}_1'$-term t in $A_0, A_1, \ldots$ the formula "$a \in t$" adequately expresses the fact that a belongs to a subset of ω denoted by t. Hence $\beta(t = s)$ means that t and s have exactly the same elements, which is equivalent to $t = s$.

Putting Lemmas 3.1 and 3.2 together one obtains the following.

Corollary 3.3 *For every $\mathcal{L}_1$-sentence Q*

$$Q \in Th(\mathrm{DA}_0) \text{ iff } \beta(\alpha(Q)) \in \mathrm{WS1S}.$$

Theorem 3.4 *The first order theory of* $\mathrm{DA(PA)}_0$ *is decidable.*

Proof: This is a combination of the previous corollary and Büchi's result on decidability of WS1S ([8]).

Note that the given proof of Theorem 3.4 does not provide a *feasible* decision procedure for $Th(\mathrm{DA}_0)$. The translation α already causes an exponential growth of lengths of formulas, and we have to use an extremely inefficient decision algorithm for WS1S afterwards. Our next result shows that the decision problem for $Th(\mathrm{DA}_0)$ really is of high complexity: we shall describe a natural translation of WS1S into $Th(\mathrm{DA}_0)$, which increases the lengths of formulas only linearly . This will allow us to extend to $Th(\mathrm{DA}_0)$ the nonelementary lower bounds on computational complexity of a decision procedure for WS1S, obtained by Meyer in [17].

Working within the language $\mathcal{L}_1$, fix an auxiliary variable z along with two infinite lists of distinct variables: $u_0, u_1, \ldots$ and $v_0, v_1, \ldots$. Define:

$$x \subseteq y \rightleftharpoons x \cap -y = \mathbf{0};$$

$$\text{"}u_i \textit{ is a singleton}\text{"} \rightleftharpoons u_i \neq \mathbf{0} \wedge \forall z(z \subseteq u_i \leftrightarrow z = \mathbf{0} \vee z = u_i);$$

$$\text{"}v_i \textit{ is finite}\text{"} \rightleftharpoons \exists z(z \neq \mathbf{1} \wedge v_i \subseteq m(z)).$$

A translation γ from $\mathcal{L}_2$ into $\mathcal{L}_1$ is defined inductively as follows:

- for atomic formulas

$$\gamma(0 \in A_i) \rightleftharpoons (m\mathbf{0} \subseteq v_i), \quad \gamma(a_j \in A_i) \rightleftharpoons (u_j \subseteq v_i);$$

$$\gamma(a_i < a_j) \rightleftharpoons (u_j \subseteq -m(-u_i)), \quad \gamma(0 < a_j) \rightleftharpoons (u_j \subseteq -m\mathbf{0});$$

$$\gamma(a_i = a_j) \rightleftharpoons (u_i = u_j), \quad \gamma(a_i = 0) \rightleftharpoons (u_i = m\mathbf{0});$$

$$\gamma(a_i < 0) \rightleftharpoons (\mathbf{0} \neq \mathbf{0}), \quad \gamma(0 = 0) \rightleftharpoons (\mathbf{0} = \mathbf{0});$$

- γ commutes with boolean connectives;
- $\gamma(\forall a_i\ Q) \rightleftharpoons \forall u_i$ ("u_i *is a singleton*" $\rightarrow \gamma(Q)$);
- $\gamma(\forall A_i\ Q) \rightleftharpoons \forall v_i$ ("v_i *is finite*" $\rightarrow \gamma(Q)$).

It is clear that $u_0, u_1, \ldots$ imitate variables over natural numbers, and $v_0, v_1, \ldots$ play the role of those over finite subsets of ω. This fact is formally established by the following.

Lemma 3.5 *Suppose $Q(a_0, \ldots, a_k, A_0, \ldots, A_m)$ is an arbitrary $\mathcal{L}_2$-formula. Then for any $n_0, \ldots, n_k \in \omega$ and any finite subsets $X_0, \ldots, X_m$ of ω,*

$$\omega \vDash Q(n_0, \ldots, n_k, X_0, \ldots, X_m) \text{ iff } \omega \vDash \gamma(Q)(\{n_0\}, \ldots, \{n_k\}, X_0, \ldots, X_m).$$

Proof: Routine induction on the build-up of Q.

Corollary 3.6 *For every $\mathcal{L}_2$-sentence Q*

$$Q \in \text{WS1S} \quad \text{iff} \quad \gamma(Q) \in Th(\text{DA}_0).$$

Theorem 3.7 *$Th(\text{DA}_0)$ is not elementary recursive.*

Proof: It is easily seen that the translation γ gives only a linear increase of lengths of formulas. By a well-known result of Meyer [17] WS1S has a nonelementary lower bound on the complexity of a decision procedure, hence $Th(\text{DA}_0)$ is not elementary recursive as well.

4 A two-sorted undecidable quantified provability logic In this section we will show that the first order theory of DA(PA) enriched by a unary predicate defining the 0-generated subalgebra DA(PA)_0 of DA(PA) is undecidable. In fact, we shall get an even stronger result: the theory obtained by adding to the language of $Th(\text{DA(PA)}_0)$ just one *free* variable ranging over arbitrary arithmetic sentences is already undecidable. Thus, two decidable theories—the universal theory of DA(PA) and the first order theory of DA(PA)_0—combined together yield an undecidable one. This result also provides a negative answer to a question on the decidability of quantified propositional provability logics for progressions of theories, raised by Feferman.

Let $\mathcal{L}_3$ be the language of DA(PA)_0 enriched by an infinite list of new (Greek) variables $\alpha, \beta, \gamma, \ldots$ ranging over (equivalence classes) of arbitrary arithmetic sentences. Small Latin variables $x_0, x_1, \ldots$ are reserved for elements of DA(PA)_0. Thus, $\mathcal{L}_3$ extends both the languange of DA(PA)_0 and that of DA(PA).

We shall keep the notation

$$\text{DA(PA)} \vDash Q(\alpha_0, \ldots, \alpha_k, x_0, \ldots, x_m)$$

for arbitrary $\mathcal{L}_3$-formulas Q and arbitrary elements $\alpha_0, \ldots, \alpha_k$ and $x_0, \ldots, x_m$ of their respective algebras. For the sake of readability we shall identify terms of $\mathcal{L}_3$ and quantifier-free modal formulas in the two-sorted alphabet, and also ignore the distinction between arithmetic sentences and elements of DA(PA). The boolean ordering on DA(PA) will be denoted $\subseteq$, i.e. for any sentences α and β

$$\text{DA(PA)} \vDash \alpha \subseteq \beta \text{ iff } PA \vdash \alpha \to \beta.$$

Let $\mathcal{L}_3^0$ denote the fragment of $\mathcal{L}_3$ consisting of those $\mathcal{L}_3$-formulas, which do not contain quantifiers over the Greek variables.

Theorem 4.1 *The set of all $\mathcal{L}_3^0$-formulas $Q(\alpha_0, \ldots, \alpha_k, x_0, \ldots, x_m)$ such that*

$$\text{DA(PA)} \vDash \forall\alpha_0 \ldots \alpha_k \forall x_0 \ldots x_m Q(\alpha_0, \ldots, \alpha_k, x_0, \ldots, x_m)$$

is undecidable.

Proof: We apply a common method of obtaining undecidability results of this sort. We shall define a *parametric relative interpretation* of a well-known hereditarily undecidable[4] theory—the first order theory of finite partially ordered sets—in the set of formulas in question. More specifically, we shall exhibit two $\mathcal{L}_3^0$-formulas $U(\alpha, x)$ and $R(\beta, x, y)$ such that for any given finite (irreflexive) partial ordering $\mathcal{P} = (P, \prec)$ one can find arithmetic sentences α and β such that the binary relation $R(\beta, \cdot, \cdot)$ defines on $\{x \mid \mathrm{DA(PA)} \vdash U(\alpha, x)\}$ a partial ordering isomorphic to $\mathcal{P}$.

Clearly, for these particular α and β and for every sentence Q in the language of the theory of partially ordered sets, we shall have:

$$\mathcal{P} \vDash Q \text{ iff } \mathrm{DA(PA)} \vdash \overline{Q}(\alpha, \beta),$$

where $\overline{Q}(\alpha, \beta)$ is obtained from Q by relativizing all quantifiers to $U(\alpha, \cdot)$ and translating $x \prec y$ as $R(\beta, x, y)$. (Note that α and β are the only Greek variables occurring in $\overline{Q}(\alpha, \beta)$.) Consequently, the set of all sentences Q in the language of partially ordered sets such that

$$\mathrm{DA(PA)} \vdash \forall \alpha, \beta\ (\exists x U(\alpha, x) \to \overline{Q}(\alpha, \beta))$$

is a subtheory of the theory of finite partial orderings, and hence is undecidable. As $\overline{Q}(\alpha, \beta)$ is constructed effectively from Q, the result will follow.

Now we proceed to an explicit construction. We are able to write out the formulas $U(\alpha, x)$ and $R(\beta, x, y)$ at once:

$$U(\alpha, x) \rightleftharpoons (x \neq \mathbf{0} \wedge \forall y\ (y \subseteq x \to y = x \vee y = \mathbf{0}) \wedge x \subseteq \alpha),$$

$$R(\beta, x, y) \rightleftharpoons (\beta \wedge x \subseteq \Diamond(\beta \wedge y)),$$

where, as usual, $\Diamond(\cdot)$ stands for $\neg\Box\neg(\cdot)$.

Let a finite irreflexive partial ordering $\mathcal{P} = (P, \prec)$ be given. Without loss of generality assume that $P \subseteq \omega$ and that $\prec$ agrees with the standard ordering $>$ on natural numbers in the sense that

$$\forall a, b \in P\ \ (a \prec b \Rightarrow a > b).$$

We seek arithmetic sentences α and β such that $U(\alpha, x)$ and $R(\beta, x, y)$ define a similar ordering within DA(PA).

Clearly, the formula $U(\alpha, x)$ asserts that x is an atom of $\mathrm{DA(PA)}_0$ which lies below α. By the results of Section 2 we know that atoms of $\mathrm{DA(PA)}_0$ are exactly the arithmetical interpretations of atomless modal formulas

$$C_i \rightleftharpoons (\Box^{i+1}\bot \wedge \neg\Box^i\bot),\ i \in \omega.$$

Hence for

$$\alpha \rightleftharpoons C_P^* \rightleftharpoons \bigvee_{i \in P} C_i^*,$$

$U(\alpha, \cdot)$ selects exactly the set $\{C_i^* \mid i \in P\}$ of elements of DA(PA). The proof of Theorem 4.1 will be completed, if we manage to find an arithmetic sentence β such that for all $i, j \in P$

$$i \prec j \text{ iff } \mathrm{DA(PA)} \vdash \beta \wedge C_i \subseteq \Diamond(\beta \wedge C_j).$$

The sentence β is constructed by methods of Solovay: we shall transform the partial ordering $\mathcal{P}$ into a Kripke model $\mathcal{P}^*$ and invoke the Second Arithmetical Completeness Theorem.

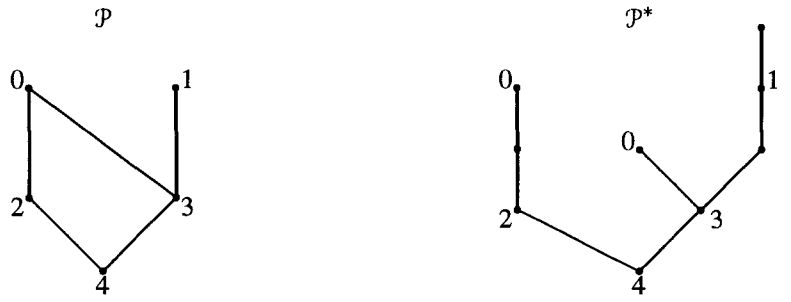

Figure 1: Transformation of $\mathcal{P}$ into $\mathcal{P}^*$. Nodes of $\mathcal{P}^*$ marked by numbers are precisely those where the variable p is forced. Numbers themselves indicate depths of the nodes.

Lemma 4.2 *There is a finite irreflexive treelike Kripke model*

$$\mathcal{P}^* = (P^*, \prec^*, \Vdash)$$

such that for all $i, j \in P$

$$i \prec j \quad \textit{iff} \quad \forall x \in P^* \; x \Vdash p \wedge C_i \to \Diamond(p \wedge C_j),$$

p being a fixed propositional variable.

Proof: The proof is long but rather straightforward. The reader will probably grasp the idea more quickly by looking at a typical example (Fig. 1), than by inspecting our detailed presentation.

First, we have to fix some notation concerning finite partial orderings. The *depth* function d on a partial ordering $\mathcal{P} = (P, \prec)$ is a mapping of P to natural numbers, uniquely determined by the following condition: for all $x \in P$

$$d(x) \rightleftharpoons \max \{d(y) + 1 \mid x \prec y\},$$

where we assume $\max \varnothing = 0$. The *height* $h(\mathcal{P})$ of a partial ordering $\mathcal{P}$ is

$$\max \{d(y) \mid y \in P\}.$$

For a given element $a \in P$, $\mathcal{P}[a]$ is the restriction of the ordering $\prec$ on P to a subset

$$P[a] \rightleftharpoons \{x \in P \mid a \preceq x\}.$$

Clearly, $h(\mathcal{P}[a]) < h(\mathcal{P})$ unless a is the infimum of $\mathcal{P}$.

The required Kripke model $\mathcal{P}^*$ is constructed by recursion on the height of $\mathcal{P}$, assuming without loss of generality that $\mathcal{P}$ has an infimum. At each step we shall guarantee in addition that $h(\mathcal{P}^*) = \inf(\mathcal{P})$. (Recall that $P \subseteq \omega$ and hence $\inf(\mathcal{P})$ is just a natural number.)

Basis. P is a singleton $\{n\}$. Take $P^* \rightleftharpoons \{0, \ldots, n\}$, $\prec^* \rightleftharpoons <$ and for each element $x \in P^*$ let

$$x \Vdash p \text{ iff } x = 0.$$

Inductive Step. Let a_0 be the infimum of $\mathcal{P}$, and let $a_1, \ldots, a_k$ enumerate all the immediate successors of a_0 (with respect to $\prec$) in decreasing order (with respect to $<$). Since $\prec$ agrees with $>$, obviously $a_0 > a_1$.

By Induction Hypothesis one can construct Kripke models

$$\mathcal{P}[a_i]^* \rightleftharpoons (P[a_i]^*, \prec_i, \Vdash_i), \quad i = 1, \ldots, k$$

of heights $a_1, \ldots, a_k$ respectively. Without loss of generality assume all $P[a_i]^*$ pairwise disjunctive.

To construct the required model $\mathcal{P}^*$ pick a linearly ordered set $(T, <_T)$ of $a_0 - a_1$ elements, disjunctive with all the $P[a_i]$, and put

$$P^* \rightleftharpoons T \cup \bigcup_{i=1}^{k} P[a_i]^*.$$

The ordering $\prec^*$ on P^* is the transitive closure of all the orderings $\prec_i$ together with $<_T$ and the following relations:

$x \prec^* y$ for all $x \in T$, $y \in P[a_1]$;
$b \prec^* y$ for all $y \in P^*$, $y \neq b$,

where b is the minimum of T. Finally, define $\Vdash$ as $\Vdash_i$ on each $P[a_i]^*$, and for $x \in T$ put

$$x \Vdash p \text{ iff } x = b.$$

It is easy to see that the height of $\mathcal{P}^*$ equals a_0 as required, so the whole construction is correct.

Next we formulate and successively prove the following auxiliary lemmas:

Lemma 4.3 *$h(\mathcal{P}^*) = \inf(\mathcal{P})$ and the variable p is forced at the root of the model $\mathcal{P}^*$.*

Proof: Trivial.

Lemma 4.4 $\forall x \in P^* \; (x \Vdash p \Rightarrow d(x) \in P)$.

Proof: By induction on $h(\mathcal{P})$.

Lemma 4.5 $\forall a \in P \; \exists x \in P^* \;\; \mathcal{P}[a]^* \simeq \mathcal{P}^*[x]$.

Proof: By induction on $h(\mathcal{P})$.

Lemma 4.6 $\forall a \in P \; \exists x \in P^* \; (x \Vdash p \;\; \& \;\; d(x) = a)$.

Proof: Follows from Lemmas 4.3 and 4.5.

Lemma 4.7 $\forall x \in P^* \; (x \Vdash p \;\&\; d(x) = a \;\Rightarrow\; \mathcal{P}^*[x] \simeq \mathcal{P}[a]^*)$.

Proof: We argue by induction on the height of $\mathcal{P}$. Suppose that $x \in \mathcal{P}^*$ and $x \Vdash p$, then either x is the root of $\mathcal{P}^*$, $a = a_0 = \inf(\mathcal{P})$ and hence

$$\mathcal{P}^*[x] \simeq \mathcal{P}^* \simeq \mathcal{P}[a]^*;$$

or $x \in P[a_i]^*$ and then

$$\mathcal{P}^*[x] \simeq (\mathcal{P}[a_i]^*)[x] \simeq \mathcal{P}[a]^*$$

by Induction Hypothesis.

Lemma 4.8 *For all $i, j \in P$, if $i \prec j$ then*

$$\forall x \in P^* \ \ x \Vdash p \wedge C_i \to \Diamond(p \wedge C_j).$$

Proof: Suppose $x \Vdash p \wedge C_i$, then $d(x) = i$ and by 4.7

$$\mathcal{P}^*[x] \simeq \mathcal{P}[i]^*.$$

Since $j \in P[i]$, by Lemma 4.6 there is an $y \in P[i]^*$ such that $y \Vdash p$ and $d(y) = j$. Hence for some $y' \in P^*[x]$, $y' \Vdash p$ and $d(y') = j$, ergo $y' \Vdash p \wedge C_j$. It follows that $x \Vdash \Diamond(p \wedge C_j)$.

Lemma 4.9 *For all $i, j \in P$, if $i \not\prec j$ then*

$$\exists x \in P^* \ \ (\ x \Vdash p \wedge C_i \ \ \& \ \ x \nVdash \Diamond(p \wedge C_j)\ ).$$

Proof: Since $i \in P$, by Lemma 4.5the model $\mathcal{P}[i]^*$ has the form $\mathcal{P}^*[x]$ for some $x \in P^*$. Since $h(\mathcal{P}[i]^*) = i$, clearly $x \Vdash p \wedge C_i$. On the other hand, if $y \in P^*[x]$ and $y \Vdash p$, then $d(y) \in P[i]$ by Lemma 4.4. It follows that either $j = i$ and $y = x$, or $j \notin P[i]$ and then $y \Vdash \neg C_j$. Thus, we have shown that $x \Vdash \Box(p \to \neg C_j)$.

Lemmas 4.8 and 4.9 complete the proof of Lemma 4.2.

Lemma 4.10 *There is an arithmetic sentence β such that for all $i, j \in P$*

$$i \prec j \quad \textit{iff} \quad \mathrm{DA(PA)} \vDash \beta \wedge C_i \subseteq \Diamond(\beta \wedge C_j).$$

Proof: With the given partial ordering $\mathcal{P}$ we associate the following modal formula $Q_{\mathcal{P}}(p)$:

$$\bigwedge_{i \prec j} \Box(p \wedge C_i \to \Diamond(p \wedge C_j)) \ \wedge \ \bigwedge_{i \not\prec j} \neg\Box(p \wedge C_i \to \Diamond(p \wedge C_j)).$$

We claim that $\neg Q_{\mathcal{P}}(p)$ is not derivable in Solovay's logic S. Indeed, for the model $\mathcal{P}^*$ constructed in Lemma 4.2 obviously

$$\forall x \in P^* \ \ x \Vdash Q_{\mathcal{P}}(p).$$

By appending at the root of $\mathcal{P}^*$ a tail T such that for every $x \in T$ $x \nVdash p$, the model $\mathcal{P}^*$ is transformed into a tail-model validating $Q_{\mathcal{P}}(p)$.

Solovay's Second Theorem guarantees that there exists an arithmetical interpretation $*$ such that $Q^*_{\mathcal{P}}$ is true, i.e. for all $i, j \in P$

$$\mathrm{PA} \vdash p^* \wedge C_i^* \to \Diamond(p \wedge C_j)^* \ \text{ if } \ i \prec j$$

and

$$\mathrm{PA} \nvdash p^* \wedge C_i^* \to \Diamond(p \wedge C_j)^* \ \text{ if } \ i \not\prec j.$$

Take $\beta = p^*$.

Thus, we have shown that the theory of finite partial orderings is parametrically interpretable in the set of all $\mathcal{L}_3^0$-formulas universally true in DA(PA). This completes the proof of Theorem 4.1.

Since the parameter α in the proof of Theorem 3 always belongs to $\mathrm{DA(PA)}_0$, it could be replaced by a Latin variable. Thus, we get the following corollary.

Corollary 4.11 *The set of all $\mathcal{L}_3^0$-formulas $Q(\alpha, x_0, \ldots, x_m)$, containing only one Greek variable α, such that*

$$\mathrm{DA(PA)} \vDash \forall\alpha\forall x_0 \ldots x_m\, Q(\alpha, x_0, \ldots, x_m),$$

is undecidable.

*5 **Provability logics for recursive progressions of theories*** As an application of techniques developed in the proof of Theorem 4.1, we shall now demonstrate that quantified propositional provability logics for recursive progressions of theories are, in the most natural cases, undecidable.

Recursive progressions are parametric families of theories of the form $(\mathcal{T}_z)_{z\in Z}$, where Z is a set of constructive ordinal notations. When speaking about progressions, we shall always assume that there exists an arithmetic Σ_1-formula $Pr_{\mathcal{T}}(z; x)$ adequately expressing the predicate "*x is provable in the theory $\mathcal{T}_z$*", and that the set Z is recursively enumerable[5] and gives exactly one notation to each finite ordinal.

The primary example of a recursive progression is (roughly) the following *transfinite recursive progression based on iteration of consistency*, first studied by Turing [22] and Feferman [11]:

$$\mathcal{T}_0 \rightleftharpoons \mathrm{PA}, \quad \mathcal{T}_{\lambda+1} \rightleftharpoons \mathcal{T}_\lambda + Con(\mathcal{T}_\lambda) \quad \text{and} \quad \mathcal{T}_\lambda \rightleftharpoons \bigcup_{\mu<\lambda} \mathcal{T}_\mu,$$

for λ a limit ordinal. (Here we identify Z with an initial segment of constructive ordinal numbers.)

Feferman suggested the following variant of a quantified provability logic for recursive progressions of theories. With the given system of ordinal notation Z we associate a language $\mathcal{L}(Z)$ containing two sorts of variables: $\alpha, \beta, \gamma, \ldots$ for arbitrary arithmetic sentences, and $x, y, z, \ldots$ for ordinal notations from Z. To each Latin variable x in $\mathcal{L}(Z)$, there corresponds a unary modal operator $[x]$. Formulas of $\mathcal{L}(Z)$ are built up from Greek variables using boolean connectives, modal operators and quantifiers over Latin variables in the natural way. *The arithmetical interpretation* $*$ with respect to a progression $(\mathcal{T}_z)_{z\in Z}$ translates Greek variables as arithmetic sentences, commutes with boolean connectives, and for every $\mathcal{L}(Z)$-formula Q

$$(\forall z\ Q)^* \rightleftharpoons (\forall z \in Z\ \ Q^*),$$

$$([z]Q)^* \rightleftharpoons Pr_{\mathcal{T}}(z; \ulcorner Q^* \urcorner).$$

Theorem 5.1 *Let $(\mathcal{T}_z)_{z\in Z}$ be a recursive progression based on iteration of consistency. Then the set of all $\mathcal{L}(Z)$-formulas, true under every arithmetical interpretation with respect to $(\mathcal{T}_z)_{z\in Z}$, is undecidable.*

Proof: The two-sorted language $\mathcal{L}_3$, which played a role in Theorem 4.1, could be given many other natural provability interpretations. In fact, one could let the Latin variables of $\mathcal{L}_3$ range over any specific subset D of DA(PA). Here we shall make use of the interpretation of Latin variables as iterated consistency assertions associated with $(\mathcal{T}_z)_{z\in Z}$:

$$D \rightleftharpoons \{Con(\mathcal{T}_z) \mid z \in Z\}.$$

We claim that the statement of Theorem 4.1 also holds for this modified interpretation. A proof closely follows the given proof of Theorem 4.1: it is easy to see that the first order theory of finite partial orderings is parametrically interpretable in the set of all universally true (in the new sense) formulas of $\mathcal{L}_3^0$.

Note that for every $i \in \omega$ the atom C^*_{i+1} of $\mathrm{DA(PA)}_0$ is PA-equivalent to the formula

$$Con(\mathcal{T}_i) \wedge Pr(\ulcorner \neg Con(\mathcal{T}_i) \urcorner).$$

It follows that, for $\alpha \not\supseteq C_0^*$, the formulas

$$U(\alpha, x) \rightleftharpoons (x \subseteq \alpha)$$

and

$$R(\beta, x, y) \rightleftharpoons (\beta \wedge x \wedge \Box\neg x \subseteq \Diamond(\beta \wedge y \wedge \Box\neg y))$$

define within DA(PA) exactly the same partial ordering as the one in the proof of Theorem 4.1. Hence the result.

Turning back to the provability logics for progressions of theories in the sense of Feferman, define a translation $\circ$ of the language $\mathcal{L}_3^0$ into $\mathcal{L}(Z)$ as follows:

- $\circ$ preserves Greek variables and commutes with boolean connectives and quantifiers;
- $(\Box Q)^\circ \rightleftharpoons (\forall z\, [z] Q^\circ)$;
- for any Latin variable x, $(x)^\circ \rightleftharpoons \neg[x]\bot$.

Clearly, for each $\mathcal{L}_3^0$-formula $Q(\alpha_1, \ldots, \alpha_n)$

$$DA(PA) \vdash \forall\alpha_1, \ldots, \alpha_n\ Q(\alpha_1, \ldots, \alpha_n)$$

iff for every arithmetical interpretation $*$

$$\omega \vdash (Q(\alpha_1, \ldots, \alpha_n)^\circ)^*.$$

This completes the proof of Theorem 5.1.

One can prove the analogue of Theorem 5.1 for other natural types of recursive progressions, such as those based on iteration of reflection principles, or for the natural progression $(I\Sigma_n)_{n\in\omega}$ of finitely axiomatizable subtheories of PA. (Here $I\Sigma_n$ denotes an arithmetical theory, axiomatized over PRA by the schema of induction for Σ_n-formulas.) Note that all these progressions satisfy the following property: for all $i, n \in \omega$

$$\mathcal{T}_0 + Con(\mathcal{T}_{i+1}) \vdash Con^n(\mathcal{T}_0 + Con(\mathcal{T}_i)),$$

where $Con^n(\mathcal{T})$ denotes the n times iterated consistency of a theory $\mathcal{T}$. Following the terminology of [5], this fact could be expressed by saying that for all i the sentence $Con(\mathcal{T}_{i+1})$ is *infinitely confident* in the theory $\mathcal{T}_0 + Con(\mathcal{T}_i)$.

Using the results of [5], for such progressions one can modify the construction of the model $\mathcal{P}^*$ in Lemma 4.2 and prove the following analogue of Lemma 4.10:

> For every finite partial ordering $\mathcal{P}$ there is an arithmetic sentence β such that for all $i, j \in P$
>
> $$i \prec j \quad \text{iff} \quad \mathrm{DA}(\mathcal{T}_0) \vdash \beta \wedge D_i \subseteq \Diamond(\beta \wedge D_j),$$
>
> where
>
> $$D_i \rightleftharpoons Con(\mathcal{T}_i) \wedge \Box\neg Con(\mathcal{T}_i).$$

With this modification, the proof of Theorem 5.1 goes through almost literally for any recursive progression satisfying the property of "infinite confidence" above.

It is probably worth mentioning here that we have actually proved a stronger statement than the one formulated in Theorem 5.1. Our proof shows that the fragment of the quantified provability logic for progressions of theories, consisting of $\mathcal{L}(Z)$-formulas with no occurrences of quantifiers inside modal operators, is undecidable.

6 First order theories of free diagonalizable algebras In this section we shall prove the following theorem:

Theorem 6.1 *For every $n > 0$, the first order theory of the free* DA *on n independent generators* $\mathrm{DA(GL)}_n$ *is undecidable.*

Proof: As in the proof of Theorem 4.1, we shall construct a parametric relative interpretation of the theory of finite partial orderings in the first order theory of $\mathrm{DA(GL)}_n$. Define:

$$U(\alpha, x) \rightleftharpoons (x \neq \mathbf{0} \wedge \forall y\, (y \subseteq x \rightarrow y = x \vee y = \mathbf{0}) \wedge x \subseteq \alpha),$$

$$R(x, y) \rightleftharpoons (x \subseteq \Diamond y).$$

As before, the formula $U(\alpha, x)$ distinguishes the set of atoms of $\mathrm{DA(GL)}_n$ below α, although now $R(x, y)$ is a fixed irreflexive transitive relation on the set of atoms of $\mathrm{DA(GL)}_n$. To demonstrate that U and R define the required parametric interpretation, we need some extra information on the structure of free diagonalizable algebras.

The fact that free DA's are atomic was discovered independently and in different set-ups by many authors (see e.g. [16],[4]). A useful characterization of atoms of $\mathrm{DA(GL)}_n$ in terms of *prime* Kripke models and their *defining formulas* (a notion similar to *characters* of [12],[14]) was suggested in [4]. In the sequel we shall work in the modal language with exactly n propositional variables $p_1, \ldots, p_n$ and use appropriate finite irreflexive treelike Kripke models. We write $\mathcal{K} \Vdash Q$ to indicate that the formula Q is forced at the root of the model $\mathcal{K}$.

Let a Kripke model $\mathcal{K} = (K, \prec, \Vdash)$ be given. A node $x \in K$ is called *dispensable* iff x is not the root of $\mathcal{K}$ and for every $y \prec x$ in $\mathcal{K}$, there is a node $z \succ y$ such that $z \neq x$ and the submodel $\mathcal{K}[z]$ is isomorphic to $\mathcal{K}[x]$. A model $\mathcal{K}$ is *prime* iff it does not contain any dispensable nodes.

Lemma 6.2 *To each model $\mathcal{K}$, there is a prime model $\mathcal{K}'$ such that for all the formulas Q in $p_1, \ldots, p_n$,*

$$\mathcal{K} \Vdash Q \quad \text{iff} \quad \mathcal{K}' \Vdash Q.$$

Proof: Just throw out successively all the submodels $\mathcal{K}[z]$ of $\mathcal{K}$ for dispensable nodes $z \in K$.

Corollary 6.3 *If the formulas Q and R are valid in the same prime models, then*

$$\mathrm{GL} \vdash Q \leftrightarrow R.$$

Lemma 6.4 *To any prime model $\mathcal{K}$, there exists a formula $\Phi_{\mathcal{K}}$* (defining formula) *such that for every prime model $\mathcal{K}'$*

$$\mathcal{K}' \Vdash \Phi_{\mathcal{K}} \quad \text{iff} \quad \mathcal{K}' \simeq \mathcal{K}.$$

Proof: See [4].

Corollary 6.5 *Atoms of* $\mathrm{DA(GL)}_n$ *are precisely the* GL*-equivalence classes of formulas of the form $\Phi_{\mathcal{K}}$ for prime models $\mathcal{K}$.*

Proof: Clearly, if $\mathrm{GL} \vdash Q \to \Phi_{\mathcal{K}}$, then by Lemma 6.4 Q is false in every prime model except $\mathcal{K}$. If $\mathcal{K} \Vdash \neg Q$, then by Lemma 6.2 $\mathrm{GL} \vdash \neg Q$. Otherwise, $\mathrm{GL} \vdash Q \leftrightarrow \Phi_{\mathcal{K}}$ by Corollary 6.3. Hence $\Phi_{\mathcal{K}}$ is an atom.

On the other hand, if $\mathrm{GL} \nvdash \neg Q$, then by Lemma 6.2 there is a prime model $\mathcal{K}$ such that $\mathcal{K} \Vdash Q$. By Lemma 6.4 $\mathrm{GL} \vdash \Phi_{\mathcal{K}} \to Q$, hence Q is not an atom, unless $\mathrm{GL} \vdash Q \leftrightarrow \Phi_{\mathcal{K}}$.

Let Ω_n denote the set of all (isomorphism classes) of prime Kripke models in the language with n propositional variables. For prime models $\mathcal{K}_1$ and $\mathcal{K}_2$ we shall write $\mathcal{K}_1 \lhd \mathcal{K}_2$ in case there exists a node x strictly above the root of $\mathcal{K}_1$ such that $\mathcal{K}_1[x]$ is isomorphic to $\mathcal{K}_2$. By Lemmas 6.2 and 6.4 $\mathcal{K}_1 \lhd \mathcal{K}_2$ is equivalent to

$$\mathrm{GL} \vdash \Phi_{\mathcal{K}_1} \to \Diamond \Phi_{\mathcal{K}_2};$$

hence the ordering $\lhd$ on Ω_n is isomorphic to the one defined by the relation

$$R(x, y) \rightleftharpoons (x \subseteq \Diamond y)$$

on the set of all atoms of $\mathrm{DA(GL)}_n$. Therefore, to complete the proof of Theorem 6.1 it suffices to prove the following

Lemma 6.6 *Every finite partial ordering is embeddable into* $(\Omega_n, \lhd)$.

Proof: Since each finite ordering is embeddable into a finite boolean algebra, it is sufficient to embed into Ω_n such algebras only. Besides, for $m < n$ the structure $(\Omega_m, \lhd)$ is embeddable into $(\Omega_n, \lhd)$ in the obvious way. Therefore we shall give the proof of Lemma 6.6 for $n = 1$, thus working in the language with exactly one propositional variable p.

The *sum*

$$\mathcal{K} \rightleftharpoons \bigoplus_{i=1}^{m} \mathcal{K}_i$$

of models $\mathcal{K}_i = (K_i, \prec_i, \Vdash_i)$, $i = 1, \ldots, m$ is defined as follows:

$$K \rightleftharpoons \{(x, i) \mid x \in K_i\} \cup \{0\};$$

$$(x, i) \prec (y, j) \text{ iff } (i = j \ \&\ x \prec_i y),$$

$$0 \prec (x, i) \quad \text{for all} \quad (x, i) \in K;$$

$$0 \Vdash p \quad \text{and for } x \in K_i \ ((x, i) \Vdash p \Leftrightarrow x \Vdash_i p).$$

In other words, taking the sum of models $\mathcal{K}_i$ amounts to attaching a new root 0 below those of all the $\mathcal{K}_i$ and stipulating that $0 \Vdash p$. Clearly, $\bigoplus_{i=1}^{m} \mathcal{K}_i$ is prime, whenever all the $\mathcal{K}_i$ are prime and incomparable with respect to $\lhd$.

Let B_n denote the boolean algebra of all subsets of a finite set $X = \{x_1, \ldots, x_n\}$. We construct an embedding of B_n into Ω_1 by stages. At stage i the prime models $F(Z)$ corresponding to subsets $Z \subseteq X$ of cardinality i are specified.

Stage 0. $F(\varnothing)$ is the linear model of height $n - 1$, p being forced at every node of $F(\varnothing)$.

Stage 1. $F(\{i\})$ is the model $\mathcal{A}_i = (A_i, \prec_i, \Vdash_i)$ of height n defined as follows. Put

$$A_i \rightleftharpoons \{0, \ldots, 2n\}$$

and for $x, y \in A_i$ let $x \prec_i y$ iff one of the following conditions hold:

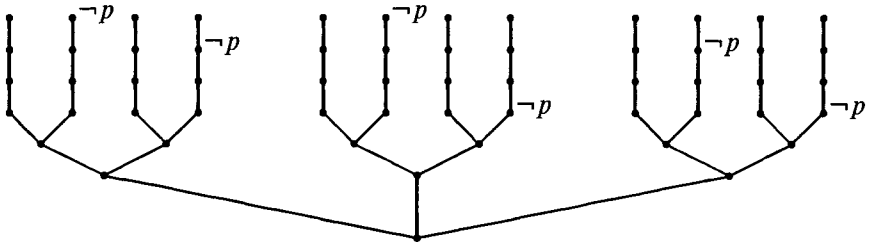

Figure 2: Embedding B_4 into Ω_1. This is the model $F(\{x_1, x_2, x_4\})$. The variable p is forced at all the nonlabelled nodes.

1. x, y are odd and $x < y$;
2. x, y are even and $x < y$;
3. $x = 0$ and $y \neq 0$.

Finally, for $x \in A_i$ define

$$x \Vdash_i p \quad \text{iff} \quad x \neq 2(n-i).$$

Clearly, all the $\mathcal{A}_i$ are prime and mutually incomparable with respect to $\lhd$.

Stage k+1. Suppose $Z \subseteq X$ and $|Z| = k+1$. Let $Z_1, \ldots, Z_{k+1}$ enumerate all the subsets of Z of cardinality k. Put

$$F(Z) \rightleftharpoons \bigoplus_{i=1}^{k+1} F(Z_i).$$

By induction on $|Z|$ one easily shows that for any subset $Z \subseteq X$

$$Z = \{x_i \mid \mathcal{A}_i \lhd F(Z) \text{ or } \mathcal{A}_i = F(Z)\}$$

and hence for all $Y \subseteq X$

$$Y \subset Z \quad \text{iff} \quad F(Y) \lhd F(Z).$$

It follows that for every $Z \subseteq X$ the model $F(Z)$ is prime, because at stage $k+1$ in the construction of $F(Z)$ one always takes the sum of models incomparable with respect to $\lhd$. Thus, F is an embedding of B_n into Ω_1 as required.

Now we complete the proof of Theorem 6.1. Let a finite partial ordering $(P, \prec)$ be given, and let Π denote a finite set of prime Kripke models given by Lemma 6.6 such that $(\Pi, \lhd)$ is isomorphic to $(P, \prec)$. Put

$$\alpha \rightleftharpoons \bigvee_{\mathcal{K} \in \Pi} \Phi_{\mathcal{K}}.$$

Clearly, by Corollary 6.5 the formula $U(\alpha, \cdot)$ defines exactly the set $\{\Phi_{\mathcal{K}} \mid \mathcal{K} \in \Pi\}$ of atoms of $\mathrm{DA(GL)}_n$, and $R(\cdot, \cdot)$ is a partial ordering on $\{\Phi_{\mathcal{K}} \mid \mathcal{K} \in \Pi\}$ isomorphic to $(P, \prec)$. Hence U and R define the required parametric relative interpretation, and consequently, the first order theory of $\mathrm{DA(GL)}_n$ is undecidable.

Acknowledgment We wish to thank Professor George Boolos who carefully read the manuscript of the paper and provided many constructive comments.

NOTES

1. However, such definability seems rather problematic.
2. Solomon Feferman asked this question in private discussions with the first of the authors.
3. For technical reasons we incorporate $<$ into the language of WS1S instead of a functional symbol for the successor operation, as in Büchi's original paper [8]. The two formulations are obviously equivalent.
4. This means that any subtheory of this theory is undecidable. See [10] and [9] for the details.
5. Actually, this requirment is superfluous, but it simplifies the construction of the uniform provability predicates $Pr_T(z; x)$ as well as the definition of arithmetical interpretations below.

REFERENCES

[1] Artemov, S. N., "Arithmetically complete modal theories," *Semiotika i Informatika*, vol. 14 (1980), pp. 115–133. English translation in *American Mathematical Society Translations 2*, vol. 135 (1987), pp. 39–54.

[2] Artemov, S. N., "Nonarithmeticity of truth predicate logics of provability," *Doklady Akad. Nauk SSSR*, vol. 284 (1985), pp. 270–271. English translation in *Soviet Mathematics Doklady*, vol. 33 (1985), pp. 403–405.

[3] Artemov, S. N., "On modal logics axiomatizing provability," *Izvestiya Akad. Nauk SSSR, ser. mat.*, vol. 49 (1985), pp. 1123–1154. English translation in: *Mathematics USSR Izvestiya*, vol. 27 (1986), pp. 401–429.

[4] Artemov, S. N., "Locally tabular propositional provability logics," pp. 9–12 in *Logical Methods of Constructing Efficient Algorithms*, Kalinin State University, Kalinin, 1986.

[5] Beklemishev, L. D., "On bimodal logics for Π_1-axiomatized extensions of arithmetical theories," ITLI Prepublication Series X–91–09, University of Amsterdam, 1991. To appear in *Annals of Pure and Applied Logic*.

[6] Boolos, G., *The Unprovability of Consistency; An Essay in Modal Logic*, Cambridge University Press, Cambridge, 1979.

[7] Boolos, G., "Provability, Truth and Modal Logic," *Journal of Philosophic Logic*, vol. 9 (1981), pp. 1–7.

[8] Büchi, J. R., "On a decision method in restricted second order arithmetic," pp. 1–11 in *Logic, Methodology and Philosophy of Science; Proceedings of the 1960 International Congress*, Stanford University Press, Palo Alto, 1962.

[9] Ershov, Y. L., *Decidability problems and constructive models*, Nauka, Moscow, 1980.

[10] Ershov, Y. L., Lavrov, I. A., Taimanov, A. D., and M. A. Taitslin, "Elementary theories," *Uspekhi Math. Nauk*, vol. 20 (1965), pp. 37–108.

[11] Feferman, S., "Transfinite recursive progressions of axiomatic theories," *The Journal of Symbolic Logic*, vol. 27 (1962), pp. 259–316.

[12] Fine, K., "Logics containing K4, Part 1," *The Journal of Symbolic Logic*, vol. 40 (1975), pp. 31–42.

[13] Friedman, H., "102 problems in mathematical logic," *The Journal of Symbolic Logic*, vol. 40 (1975), pp. 113–129.

[14] Gleit, Z., and W. Goldfarb. "Characters and fixed points in provability logic," To appear in *Notre Dame Journal of Formal Logic*.

[15] Gödel, K., "Eine Interpretation des intuitionistischen Aussagenkalkuls," *Ergebnisse Math. Kolloq.*, vol. 4 (1933), pp. 39–40, 1933.

[16] Grigolia, R. S., *Free Algebras of Non-classical Logics*. Metzniereba, Tbilissi, 1987.

[17] Meyer, A. R., "The inherent complexity of theories of ordered sets," pp. 477–482 in *Proceedings of the International Congress of Mathematics, Vancouver, 1974*, Canadian Mathematics Congress, 1975.

[18] Montagna, F., "Undecidability of the first order theory of diagonalizable algebras," *Studia Logica*, vol. 39 (1980), pp. 347–354.

[19] Rybakov, V. V., "Elementary theories of free topoboolean and pseudoboolean algebras," *Math. Zametki*, vol. 37 (1985), pp. 797–802.

[20] Smoryński, C., *Self-Reference and Modal Logic*. Springer–Verlag, Berlin, 1985.

[21] Solovay, R. M., "Provability interpretations of modal logic," *Israel Journal of Mathematics*, vol. 28 (1976), pp. 33–71.

[22] Turing, A. M., "System of logics based on ordinals," *Proc. London Math. Soc.*, ser. 2, vol. 45 (1939), pp. 161–228.

[23] Vardanyan, V. A., "Arithmetic comlexity of predicate logics of provability and their fragments," *Doklady Akad. Nauk SSSR*, vol. 288 (1986), pp. 11–14. English translation in *Soviet Mathematics Doklady* vol. 33 (1986), pp. 569–572.

[24] Visser, A., "The provability logics of recursively enumerable theories extending Peano Arithmetic at arbitrary theories extending Peano Arithmetic," *Journal of Philosophic Logic*, vol. 13 (1984), pp. 97–113.

Steklov Mathematical Institute
Vavilov str. 42
Moscow 117966
Russia