Annals of Pure and Applied Logic 61 (1993) 63–73
North-Holland

Hilbert's tenth problem for weak theories of arithmetic

Richard Kaye
Jesus College, Oxford OX1 3DW, United Kingdom

Communicated by D. van Dalen
Received 24 September 1991
Revised 3 February 1992

Abstract

Kaye, R., Hilbert's tenth problem for weak theories of arithmetic, Annals of Pure and Applied Logic 61 (1993) 63–73.

Hilbert's tenth problem for a theory T asks if there is an algorithm which decides for a given polynomial $p(\bar{x})$ from $\mathbb{Z}[\bar{x}]$ whether $p(\bar{x})$ has a root in some model of T. We examine some of the model-theoretic consequences that an affirmative answer would have in cases such as T = Open Induction and others, and apply these methods by providing a negative answer in the cases when T is some particular finite fragment of the weak theories IE_1 (bounded existential induction) or IU_1^- (parameter-free bounded universal induction).

1. Introduction

Hilbert's famous tenth problem asked if there is an algorithm A which, when given a polynomial $p(\bar{x})$ from $\mathbb{Z}[\bar{x}]$, returns the output 'yes' or 'no' depending on whether there is $\bar{a}$ in $\mathbb{N}$ such that $p(\bar{a}) = 0$. In 1970, Matijasevič [8], using previous work by J. Robinson, Davis and Putnam answered this question negatively, proving:

Result 1 (The MRDP theorem). *For all r.e. predicates $\theta(\bar{x})$ there is a polynomial $p(\bar{x}, \bar{y})$ from $\mathbb{Z}[\bar{x}, \bar{y}]$ such that for all $\bar{x} \in \mathbb{N}$, $\theta(\bar{x})$ holds just in case $\exists \bar{y}\, p(\bar{x}, \bar{y}) = 0$.*

Even more famously, Hilbert also asked if certain strong theories of arithmetic (such as PA) were decidable. The well-known negative answer to this last question given by Gödel and Rosser led Skolem, Kreisel, Schoenfield and Shepherdson in the 1950s and 60s to look at the free-variable system of arithmetic formulated in the usual language of arithmetic with nonlogical symbols $+, \cdot, <, 0, 1, \dot{-}$, variables, and the usual logical connectives $=, \wedge, \vee, \neg, \rightarrow$, *but no*

Correspondence to: R. Kaye, Jesus College, Oxford OX1 3DW, United Kingdom.

quantifiers. The usual basic axioms, PA^-, for the nonnegative parts of discretely ordered rings can be expressed in this language, and induction can be given as a rule rather than an axiom scheme. The first and most basic question along Hilbert's lines is: is this quantifier-free fragment of PA decidable?

In an obvious way, all theorems of the free-variable PA can be regarded as universal (or $\forall_1$) statements about the standard model $\mathbb{N}$. Shepherdson [11] showed that in fact this system has exactly the same $\forall_1$ consequences as the $\mathscr{L}_A$-theory *IOpen*, where $\mathscr{L}_A$ is the full language of arithmetic with nonlogical symbols $+$, $\cdot$, $\dot{-}$, $<$, 0, 1 and quantifiers, and *IOpen* is axiomatized by PA^- together with the usual axiom scheme of induction on all quantifier-free (or open) formulas θ:

$$\forall \bar{a}\,((\theta(0, \bar{a}) \wedge \forall x\,(\theta(x, \bar{a}) \rightarrow \theta(x+1, \bar{a}))) \rightarrow \forall x\,\theta(x, \bar{a})).$$

It is easy to check that any $\forall_1$ formula $\varphi(\bar{x})$ in $\mathscr{L}_A$ is equivalent (in PA^-) to a formula of the form $\forall \bar{y}\, p(\bar{x}, \bar{y}) \neq 0$, where $p(\bar{x}, \bar{y})$ is a polynomial with coefficients from $\mathbb{Z}$. For example, $u < v$ is equivalent to $\forall w\, v + w - u \neq 0$, while $p(\bar{u}) \neq 0 \vee q(\bar{v}) \neq 0$ is equivalent to $p(\bar{u})^2 + q(\bar{v})^2 \neq 0$, and $p(\bar{u}) \neq 0 \wedge q(\bar{v}) \neq 0$ is equivalent to $p(\bar{u}) \cdot q(\bar{v}) \neq 0$. Thus, by Shepherdson's result, the question about decidability of the free-variable PA is equivalent to asking whether there is an algorithm A such that, on input $p(\bar{x}) \in \mathbb{Z}[\bar{x}]$, A answers 'yes' if there is $\bar{a}$ and $\bar{a} \in M \models IOpen$ with $M \models p(\bar{a}) = 0$ (i.e., if $IOpen \not\vdash \forall \bar{x}\, p(\bar{x}) \neq 0$) and answers 'no' otherwise. Because of its close similarity with Hilbert's tenth problem, I shall refer to this as *Hilbert's tenth problem for IOpen*, or the *diophantine problem for IOpen*, and the analogous problem when *IOpen* is replaced by another theory T, *Hilbert's tenth problem for T*. Since the reduction above of $\forall_1$ formulas to formulas stating that a polynomial has no root, 'Hilbert's tenth problem for *IOpen*' is equivalent to asking whether the set of $\forall_1$ consequences of *IOpen*, $\forall_1(IOpen)$, is recursive. Notice that the set of $p(\bar{x})$ solvable in some model of *IOpen* is a co-r.e. set: the problem is to decide if it is r.e.

In his 1964 paper, Shepherdson [12] constructed models of *IOpen* and showed in particular that *IOpen* cannot prove the irrationality of $\sqrt{2}$,

$$\forall x, y\,(x+1)^2 \neq 2(y+1)^2,$$

nor Fermat's Last theorem for exponent 3,

$$\forall x, y, z\,(x+1)^3 + (y+1)^3 \neq z^3,$$

and in his 1965 paper [13] he announced a free-variable system with no induction axioms and the same $\forall_1$ consequences as *IOpen*. Wilkie [15] found a much more useful algebraic characterization of $\forall_1(IOpen)$, and van den Dries [2] used Wilkie's characterization to find an algorithm that decides for each two-variable polynomial $p(x, y)$ for $\mathbb{Z}[x, y]$ whether or not there is a ring Z whose nonnegative

part is a model of *IOpen* and $p(x, y)$ has a zero in Z.[1] Note that the *original* tenth Hilbert problem for two-variable polynomials and solvability over $\mathbb{N}$ (or $\mathbb{Z}$) is still open!

Despite a great deal of work, Hilbert's tenth problem for *IOpen* is still unsolved. The theory *IOpen* is known not to prove the MRDP theorem on the diophantine representation of r.e. predicates, but this seems to be of little help here. Both Wilkie and van den Dries have provided strong evidence that diophantine equations over *IOpen* should be decidable, and so they conjecture that $\forall_1(IOpen)$ is a recursive set of formulas. My object in this paper, however, is to examine this conjecture from what may seem to be a rather 'negative' point of view: I shall examine what it means for a theory T to have a *decidable* diophantine problem. In this way I shall derive independence results of a rather general nature from the van den Dries–Wilkie conjecture, and also show that rather modest-seeming extensions of *IOpen*—extensions that are known not to prove the MRDP theorem—have undeciable diophantine problem. As the referee has commented this article can be read as a discussion about how independence results of this kind can be attained for weak theories—whether one agrees with my approach or not.

The techniques I shall use combine the negative solution to Hilbert's original problem for the standard model $\mathbb{N}$ by Matijasevič, J. Robinson, Davis and Putnam, Tennenbaum's method of showing a nonstandard model of arithmetic to be nonrecursive, and a model-theoretic construction going back to A. Robinson and Henkin applied to this setting in a careful way. These methods will allow the role of the induction axioms to be investigated, and it will turn out that a sufficient condition for $\forall_1(T)$ not to be recursive is if T together with a rather strong induction rule applied to an $\exists_1$ formula can prove a fragment of the MRDP theorem. The main undecidability result of the paper, that neither the theory IE_1 of Wilmers [16] nor IU_1^- of Kaye [5] have decidable diophantine problem then follows from this and the main result of Kaye [6]. This undecidability result was first announced in Kaye [5] and its proof appears here for the first time.

The results and ideas in this paper formed the basis for my talk at Utrecht, and I gave an earlier exposition of these ideas at the weekend conference at Baruch College, New York, in December 1988. I am grateful to the organizers of both conferences for their invitations and hospitality, and to the organizers of the Utrecht meeting in particular for arranging that the conference proceedings could be published in the present form.

[1] There is a minor technical detail here concerning the difference between solvability in the full ring and in the nonnegative part of the ring. For solvability in $\mathbb{N}$, the two problems are equivalent by Lagrange's theorem that every nonnegative integer is the sum of four squares. It turns out that these two problems are also equivalent even in the case of *IOpen*, since by a result of Otero [10], the $\forall_1$ consequences of *IOpen* and of *IOpen* + *Langrange's theorem* are identical. It is not clear to me if van den Dries' result applies to solvability of two-variable polynomials in the nonnegative part of the rings associated with models of *IOpen*.

The rest of this introduction recalls some definitions that have become more-or-less standard in the study of models of arithmetic and the Tennenbaum phenomena. For more details on the notation used here, see Kaye [6].

We have already mentioned that $\mathscr{L}_A$ denotes the usual first-order language of arithmetic, and PA^- the $\mathscr{L}_A$ theory axiomatizing the nonnegative parts of discretely ordered rings. The formulas classes $\exists_1$, $\forall_1$, E_1 and U_1 are, respectively, the classes of purely existential, universal, bounded existential, and bounded universal formulas of $\mathscr{L}_A$. Modulo PA^- these formula classes are equivalent to the classes of formulas of the form

$$\exists \bar{y}\, p(\bar{x}, \bar{y}) = q(\bar{x}, \bar{y})\ (\exists_1), \qquad \forall \bar{y}\, p(\bar{x}, \bar{y}) \neq q(\bar{x}, \bar{y})\ (\forall_1),$$

$$\exists \bar{y} < r(\bar{x})\, p(\bar{x}, \bar{y}) = q(\bar{x}, \bar{y})\ (E_1), \quad \text{and} \quad \forall \bar{y} < r(\bar{x})\, p(\bar{x}, \bar{y}) \neq q(\bar{x}, \bar{y})\ (U_1),$$

where p, q and r are terms involving $0, 1, +, \cdot$ only.

If Γ is a class of $\mathscr{L}_A$-formulas, $I\Gamma$ denotes the $\mathscr{L}_A$-theory with axioms PA^- and all induction axioms

$$\forall \bar{a}\, ((\theta(0, \bar{a}) \wedge \forall x\, (\theta(x, \bar{a}) \rightarrow \theta(x+1, \bar{a}))) \rightarrow \forall x\, \theta(x, \bar{a}))$$

for θ from Γ. $I\Gamma^-$ is the same, except the formulas θ in the induction axioms are not allowed to have any parameters $\bar{a}$. $L\Gamma$ and $L\Gamma^-$ are defined similarly except that the least number principle,

$$\forall \bar{a}\, (\exists x\, \theta(x, \bar{a}) \rightarrow \exists x\, (\theta(x, \bar{a}) \wedge \forall y < x \neg \theta(y, \bar{a})))$$

is used instead of the induction scheme.

An $\mathscr{L}_A$ structure $(M, +, \dot{-}, \cdot, 0, 1, <)$ is recursive iff there is an isomorphism $(M, +, \dot{-}, \cdot, 0, 1, <) \rightarrow (\mathbb{N}, \oplus, \ominus, \odot, n_0, n_1, \ll)$ where $\oplus, \ominus, \odot$ and $\ll$ are recursive operations on $\mathbb{N}$.

2. The results

Let T be an $\mathscr{L}_A$-theory. We say that T is *diophantine decidable* if it extends PA^- and Hilbert's tenth problem for T has an affirmative answer, equivalently if its universal consequence $\forall_1(T)$ forms a recursive set. Throughout the discussion in this section we shall fix attention on one such theory T and examine the effects for T, although for clarity we shall repeat the global assumptions on T in the statement of the theorems.

Given such a theory T, there is a rather standard way of building models of the $\forall\exists$ consequences of T, $\forall_2(T)$, which is due to A. Robinson (and is a modification of Henkin's proof of the completeness theorem), called *Robinson forcing* or, more descriptively, *model-theoretic forcing with quantifier-free conditions*. This construction and others like it are described in detail in Wilfrid Hodges' book, *Building models by games* [4]. I shall describe an effective version of the construction, and leave the reader to check that the resulting model K does indeed have the properties I claim.

The main ingredients for the construction are:

- a set of constants $W = \{w_0, w_1, w_2, \ldots\}$ called *witnesses*;
- a fixed recursive enumeration of all quantifier-free $\mathscr{L}_A(W)$ formulas $\theta_0(\bar{w}, \bar{x})$, $\theta_1(\bar{w}, \bar{x})$, $\theta_2(\bar{w}, \bar{x}), \ldots$.

At any stage i of the construction, we will have a *condition* $p_i(\bar{w})$, i.e., a finite set of quantifier-free $\mathscr{L}_A(W)$ *sentences* such that $T \cup p_i(\bar{w})$ is consistent. (We take p_0 to be the empty set.) At stage i the following is performed:

- if $T \cup p_i(\bar{w}) \cup \{\exists \bar{x}\, \theta_i(\bar{w}, \bar{x})\}$ is consistent, then let $p_{i+1}(\bar{w}, \bar{v})$ be $p_i(\bar{w}) \cup \{\theta_i(\bar{w}, \bar{v})\}$ where $\bar{v}$ is the first tuple of witnesses from W not already present in $p_i(\bar{w})$ or $\theta_i(\bar{w}, \bar{x})$; otherwise $p_{i+1}(\bar{w})$ is $p_i(\bar{w})$ itself, and if this happens, note that T proves $\forall \bar{y}\, (\bigwedge p_i(\bar{y}) \rightarrow \forall \bar{x} \neg \theta_i(\bar{y}, \bar{x}))$.

At the end of the construction, we take any model M of $T \cup \bigcup_i p_i$ and let $K \subseteq M$ be the submodel whose domain is the set of elements on M that realise one of the constants w_i.

Notice that the construction outlined above is effective, since the decision at stage i only depends on the consistency of a T together with a certain $\exists_1$ sentence of $\mathscr{L}_A$, and we assumed that $\forall_1(T)$ was recursive. It is easily checked that K satisfies $\forall_2(T)$ together with all $p_i(\bar{w})$. Thus the model K is recursive, for every basic atomic sentence of the form $w_i = w_j$, $w_i + w_j = w_k$, or $w_i \cdot w_j = w_k$ appears in the list θ_i ($i \in \mathbb{N}$), so it can be decided whether it is true in K or not by examining $p_i(\bar{w})$ for sufficiently large i. Putting all this together (and choosing the list θ_i so that θ_0 is the quantifier-free matrix of σ) we obtain:

Theorem 2. *Suppose T is a diophantine decidable $\mathscr{L}_A$-theory. Then for all $\exists_1$ sentences σ consistent with T there is a recursive model K of $\forall_2 T + \sigma$ such that:*

(i) *for all $\bar{a} \in K^{<\omega}$, the $\exists_1$ type of $\bar{a}$,*

$$\exists_1\text{-tp}_K(\bar{a}) \stackrel{\text{def}}{=} \{\varphi(\bar{x}) \in \exists_1 : K \models \varphi(\bar{a})\},$$

is recursive;

(ii) *K is existentially closed (e.c.) in the class of all models of T, i.e., if $\bar{a} \in K \subseteq L \models T$ and $L \models \exists \bar{x}\, \theta(\bar{a}, \bar{x})$ where θ is quantifier-free, then $K \models \exists \bar{x}\, \theta(\bar{a}, \bar{x})$.*

In the particular case of *IOpen*, note that *IOpen* is naturally $\forall_2$ axiomatized, and so the construction above gives a model of the full theory.

In general, the model K obtained by the construction depends on T and the choice of enumeration $\theta_i(\bar{x}, \bar{w})$ ($i \in \mathbb{N}$) of the quantifier-free $\mathscr{L}_A(W)$ formulas. For the remarks and results below, however, the ordering of the θ_i is immaterial, and I will refer to this model ambiguously as $K(T)$, or occasionally as $K(T, \sigma)$ when θ_0 is the quantifier-free matrix of the $\exists_1$ sentence σ.

Examining the model constructed in the last theorem then, we have:

Theorem 3. *Let T be diophantine decidable and let $K = K(T)$ as above. Then K is nonstandard. More generally, K satisfies overspill for $\exists_1$ formulas with parameters*

from K, i.e., whenever θ is quantifier-free, $\bar{a} \in K$, and

$$\mathbb{N} \subseteq \{x \in K: K \vDash \exists \bar{y}\, \theta(x, \bar{y}, \bar{a})\}$$

then

$$\mathbb{N} \subsetneq \{x \in K: K \vDash \exists \bar{y}\, \theta(x, \bar{y}, \bar{a})\}.$$

Proof. To see that K is nonstandard, note that if $K \cong \mathbb{N}$ then for each polynomial $p(\bar{x})$, $p(\bar{x})$ has a solution in $\mathbb{N}$ if and only if $\exists \bar{x}\, p(\bar{x}) = 0$ is in $\exists_1\text{-tp}_K(0)$. This type is recursive by supposition, contradicting the negative solution of Hilbert's tenth problem. The argument for $\exists_1$-overspill is similar: if $\mathbb{N} = \{x \in K: K \vDash \exists \bar{y}\, \theta(x, \bar{y}, \bar{a})\}$ then $p(\bar{x})$ has a solution in $\mathbb{N}$ if and only if

$$\exists \bar{x} \left(\bigwedge_i \exists \bar{y}\, \theta(x_i, \bar{y}, \bar{a}) \wedge p(\bar{x}) = 0 \right)$$

is in $\exists_1\text{-tp}_K(\bar{a})$. □

It is well known from Tennenbaum's theorem [14] and more recent work on this type of result that if a nonstandard model K has sufficient overspill it must be nonrecursive. In fact the argument in Wilmers [16] can be modified to show that, given some nonstandard model $M \vDash IOpen$ which satisfies overspill for both E_1 formulas and U_1 formulas, the addition function of the model is not recursive. This suggests a model-theoretic approach to Hilbert's tenth problem for weak theories, which seems particularly natural when one considers the tight relationship between Tennebaum's theorem and the Gödel–Rosser theorem (see Kaye [7, pp. 189–90]). But, unfortunately, a result due to Otero [10] shows that there is a U_1 formula $\psi(x)$ (more precisely, one can take $\psi(x)$ to be $\forall u, v, w < x$ $(3u^2 \neq v^2 + w^2 \vee uvw = 0)$) such that, in any e.c. model M of *IOpen*, the standard model $\mathbb{N}$ is definable by ψ, and so M fails to satisfy U_1-overspill. (Incidently, the same result, together with a simple compactness argument and the construction of e.c. models over a given model by a union-of-chains, shows that any e.c. model of *IOpen* satisfies $\exists_1$-overspill, irrespective of whether the van den Dries–Wilkie conjecture holds. Otero's result is, however, rather specific to *IOpen* and *IOpen + normality*, while I will want to use the last two theorems above in cases when T is not of this form.)

There is still some hope though of obtaining interesting results for, in $\mathbb{N}$ at least, the $\exists_1$-definable sets include all of the U_1-definable sets (by the MRDP theorem) and there may be ways of restricting the domain of the model $K(T)$ to mimic or (loosely speaking) 'interpret' a sufficient amount of the MRDP theorem for the Tennenbaum trick to work. The prototype argument (including the Tennenbaum trick) that we shall use is that in the next theorem, but first we need a definition.

Definition 4. A polynomial $p(\bar{u}; \bar{v}; w)$ over $\mathbb{Z}$ in the free-variables shown *bisects* disjoint r.e. sets A and B iff, for some polynomials $p_A(\bar{u}, w)$ and $p_B(\bar{v}, w)$ over $\mathbb{Z}$ we have

$$A = \{n \in \mathbb{N}: \mathbb{N} \vDash \exists \bar{u}\, p_A(\bar{u}, n) = 0\},$$
$$B = \{n \in \mathbb{N}: \mathbb{N} \vDash \exists \bar{v}\, p_B(\bar{v}, n) = 0\}$$

and

$$p(\bar{u}; \bar{v}; w) = p_A(\bar{u}, w)^2 + p_B(\bar{v}, w)^2.$$

Note that the definition depends on not just the polynomial, but also some partition $\bar{u}; \bar{v}; w$ of its free variables; when this partition is likely to be unclear, we shall indicate it using semicolons. Note also that if p does bisect disjoint sets A and B then p has no roots at all in $\mathbb{N}$.

Theorem 5. *Let K be a nonstandard model of* PA^-, *let A and B be disjoint, r.e., recursively inseparable subsets of $\mathbb{N}$, suppose $p(\bar{u}; \bar{v}; w)$ bisects A and B, $k = \mathrm{len}(\bar{u})$ and there is $\bar{b} \in K$ and an existential formula $\lambda(\bar{u}, \bar{b})$ such that*

$$\mathbb{N}^k \subseteq \{\bar{x} \in K^k: K \vDash \lambda(\bar{x}, \bar{b})\}$$

and, for all $\bar{l}$, $n \in \mathbb{N}$,

$$K \vDash \forall \bar{u}\ (\lambda(\bar{u}, \bar{b}) \rightarrow p(\bar{u}; \bar{l}; n) \neq 0).$$

Then the type $\exists_1\text{-tp}_K(\bar{b})$ is not recursive.

Proof. Let $p_A(\bar{u}, w)$ and $p_B(\bar{v}, w)$ be polynomials such that

$$A = \{n \in \mathbb{N}: \exists \bar{u}\, p_A(\bar{u}, n) = 0\},$$
$$B = \{n \in \mathbb{N}: \exists \bar{v}\, p_B(\bar{v}, n) = 0\}$$

and

$$p(\bar{u}; \bar{v}; w) = p_A(\bar{u}, w)^2 + p_B(\bar{v}, w)^2.$$

Then

$$\mathbb{N} \vDash \forall \bar{u}, \bar{v}, w\, p(\bar{u}, \bar{v}, w) \neq 0$$

since A and B are disjoint. Put $k = \mathrm{len}(\bar{u})$ and suppose that λ is as given in the statement of the theorem. Define

$$C = \{n \in \mathbb{N}: K \vDash \exists \bar{u}\ (\lambda(\bar{u}, \bar{b}) \wedge p_A(\bar{u}, n) = 0)\}.$$

Then $C \supseteq A$ since $K \vDash \lambda(\bar{u}, \bar{b})$ for all $\bar{u}$ in $\mathbb{N}^k$, and $B \cap C = \emptyset$ since $p(\bar{u}, \bar{l}, n) \neq 0$ for all $\bar{l}$, $n \in \mathbb{N}$ and all $\bar{u} \in K$ satisfying $K \vDash \lambda(\bar{u}, \bar{b})$. But C is Turing reducible to $\exists_1\text{-tp}_K(\bar{b})$, and separates A and B so is not recursive, hence $\exists_1\text{-tp}_K(\bar{b})$ cannot be recursive either. □

From the van den Dries–Wilkie conjecture and the results given so far, we can immediately deduce independence results for *IOpen*, the next corollary being a sample.

Corollary 6. *Suppose* $\forall_1(IOpen)$ *is recursive, and suppose further that* A, B *are r.e., recursively inseparable,*

$$A = \{n \in \mathbb{N}: \exists \bar{u}\, p_A(\bar{u}, n) = 0\}$$

and

$$B = \{n \in \mathbb{N}: \exists \bar{v}\, p_B(\bar{v}, n) = 0\}$$

where p_A *and* p_B *are polynomials over* $\mathbb{Z}$. *Then, for all* $\exists_1$ *sentences* σ *consistent with IOpen,*

$$IOpen + \sigma \nvdash \forall x, \bar{y}, \bar{z}\ (p_A(x, \bar{y})^2 + p_B(x, \bar{z})^2 \neq 0).$$

Proof. If not, take $K = K(IOpen, \sigma)$ and $\lambda(\bar{u})$ to be true for all $\bar{u}$ in K^k and apply Theorems 2 and 5. □

I consider the possibility of finding a suitable formula λ from a proof of (part of) the MRDP theorem to be much more important than the last corollary. From now on, we fix attention on a particular pair of r.e., recursively inseparable sets A and B and a bisecting polynomial $p(\bar{u}; \bar{v}; w) = p_A(\bar{u}, w)^2 + p_B(\bar{v}, w)^2$ as above. (No part of the following discussion will depend on the particular choice of A and B, although it is conceivable that future applications showing the diophantine problem for a specific theory T to be undecidable might depend on certain p_A and p_B being 'simple' in some sense.) We shall also use the tuple $\bar{x}$ to denote the concatenation $\bar{u}; \bar{v}; w$, writing $p(\bar{u}; \bar{v}; w)$ as $p(\bar{x})$.

Theorem 7. *Let* T *be a consistent* $\mathscr{L}_A$ *theory extending* PA^-, *suppose* $p(\bar{x})$ *is as above, and suppose that there are* $\exists_1$ *formulas* $\theta(y, \bar{z})$, $\psi(\bar{x}; y, \bar{z})$ *satisfying*:

(1) $\mathbb{N} \models \forall y\, ((\forall \bar{x} < y\, p(\bar{x}) \neq 0) \rightarrow \exists \bar{z}\, \theta(y, \bar{z}))$

(2) $T \vdash \forall y, \bar{z}\, \forall \bar{x} < y\, (\theta(y, \bar{z}) \wedge \psi(\bar{x}; y, \bar{z}) \rightarrow p(\bar{x}) \neq 0)$

(3) $T \vdash \forall y \neq 0\, \forall \bar{z}\, (\theta(y, \bar{z}) \rightarrow \psi(0, 0, \ldots, 0; y, \bar{z}))$

(4) *for all* $0 \leq i < k = \mathrm{len}(\bar{x})$ *and all* $n \in \mathbb{N}$,

$$T \vdash \forall \bar{x}, y, \bar{z}[(\theta(y, \bar{z}) \wedge \bar{x} < y \wedge n < y \wedge \psi(x_0, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_{k-1}; y, \bar{z})) \rightarrow \psi(x_0, \ldots, x_{i-1}, n, x_{i+1}, \ldots, x_{k-1}; y, \bar{z})].$$

Then T *has undecidable diophantine problem.*

Proof. We shall apply Theorem 5. Note first that all the sentences that T is required to prove in (2)–(4) above are $\forall_2$ so we may assume without loss of generality that $T = \forall_2(T)$, i.e., that T is $\forall_2$ axiomatized.

Assume that $\forall_1(T)$ is recursive. Then by Theorems 2 and 3 there is a non-standard model $K = K(T)$ of T with recursive $\exists_1$ types and $\exists_1$-overspill. Since $\mathbb{N} \models p(\bar{x}) \neq 0$ for all $\bar{x} \in \mathbb{N}$ we have from (1) that

$$\mathbb{N} \models \exists \bar{z}\ \theta(n, \bar{z})$$

for all $n \in \mathbb{N}$, so by the preservation upwards of $\exists_1$ formulas to extensions of $\mathbb{N}$ and by overspill in K there is $\alpha > \mathbb{N}$ and $\bar{\beta}$ in K so that $K \models \theta(\alpha, \bar{\beta})$. Now writing $\bar{x}$ as $\bar{u}; \bar{v}; w$ as before we consider the $\exists_1$ formula $\lambda(\bar{u}, \alpha, \bar{\beta})$ logically equivalent to

$$\psi(\bar{u}; \bar{0}; 0; \alpha, \bar{\beta}) \wedge \bar{u} < \alpha$$

where $\bar{0}$ is a tuple of the same length as $\bar{v}$ and each entry being the constant 0. Then for all $\bar{m} \in \mathbb{N}$, $K \models \lambda(\bar{m}, \alpha, \bar{\beta})$ (by (3) and (4), and the choice of $\alpha > \mathbb{N}$), and if $\bar{l}$, $n \in \mathbb{N}$ and $\bar{u} \in K \models \lambda(\bar{u}, \alpha, \bar{\beta})$ then

$$K \models \psi(\bar{u}; \bar{l}; n; \alpha, \bar{\beta})$$

(by (3) and (4) again and the fact that α is nonstandard) and so

$$K \models p(\bar{u}, \bar{l}, n) \neq 0$$

(by (2)). Thus the conditions of Theorem 5 are satisfied, and we obtain the required contradiction. □

The conditions (1)–(4) in the last theorem may seem at first glance to be rather abstract and divorced from the MRDP theorem, but in fact they will hold if a part of the MRDP theorem is derivable from T together with a certain infinitary rule of derivation. Part (1) states that one direction of the equivalence

$$\forall y\ ((\forall \bar{x} < y\ p(\bar{x}) \neq 0) \leftrightarrow \exists \bar{z}\ \theta(y, \bar{z})) \tag{†}$$

is true in $\mathbb{N}$, that is: a U_1 formula is equivalent to an existential one, and the formula θ may be the usual one derived from the usual proof of the MRDP theorem, or indeed it may also include extra existential properties of the numbers y, $\bar{z}$ not derivable from T—provided of course that these properties are true in $\mathbb{N}$. Parts (2)–(4) state that the other direction of (†) is derivable in T together with a single application of an infinitary rule similar to the ω-rule or the rule for induction on the existential formula ψ. To see the relationship with induction, note that to verify (2)–(4) it would be sufficient to prove

$$\forall y\ ((\exists \bar{z}\ \theta(y, \bar{z})) \rightarrow (\forall \bar{x} < y\ p(\bar{x}) \neq 0)) \tag{‡}$$

using the axioms of T together with the induction rule

from $y \neq 0 \wedge \theta(y, \bar{z}) \rightarrow \psi(0, 0, \ldots, 0, y, \bar{z})$

and, for each i, $\theta(y, \bar{z}) \wedge \bar{x} < y \wedge x_i + 1 < y \wedge \psi(x_0, x_1, \ldots, x_{k-1}, y, \bar{z})$

$$\rightarrow \psi(x_0, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_{k-1}, y, \bar{z})$$

deduce $\bar{x} < y \wedge \theta(y, \bar{z}) \rightarrow \psi(\bar{x}, y, \bar{z})$

but, unfortunately, this rule can only be used once. However, it does suggest to me that Hilbert's tenth problem for weak theories is not so much about how much induction is present in the weak theory, but rather about whether the theory has enough to use this extra induction rule effectively. It is known [6] that the full MRDP theorem is provable in unrestricted parameter-free existential induction, but to prove undecidability results using this result and Theorem 7 needs extra knowledge about the theory T.

3. Applications to IE_1 and IU_1^-

In this section I will discuss some rather trivial applications of Theorem 7 to IE_1 and IU_1^-. Note that IU_1^- does not prove the MRDP theorem (indeed, the nonnegative part of the discretely ordered ring $\mathbb{Z}[X]$ satisfies IU_1^-) although whether IE_1 proves the MRDP theorem is still open. We start with IE_1. Recall the following ideas and result from [6].

Definition 8. Let $\phi(a, b, x, y)$ be the $\mathscr{L}_A$ formula

$$q(a, x, y) = 0 \wedge x \leqslant y \wedge x \equiv b \bmod(a-1) \wedge y \equiv b+1 \bmod(a-1)$$

where $q(a, x, y)$ is $x^2 + y^2 - 2axy - 1$. Let $\chi(a, b)$ be

$$\exists c \leqslant b\ \phi(a+2, a, c, b).$$

Note that χ is an $\exists_1$ $\mathscr{L}_A$ formula. The idea is that $\chi(a, b)$ states that b is 'exponentially larger' than a.

Result 9 (Kaye [6]). (1) *The theory $I\Delta_0 + exp$ of Gaifman and Dimitracopoulos* [3] *is equivalent to $IE_1 + \forall x\, \exists y\, \chi(x, y)$.*

(2) *For all $\eta(\bar{x})$ in $\exists_1$, $I\Delta_0 + exp \vdash \forall \bar{x}\, \eta(\bar{x})$ if and only if there is $k \in \mathbb{N}$ such that*

$$IE_1 \vdash \forall \bar{y} \left[\bigwedge_{i=0}^{k-1} \chi(y_i, y_{i+1}) \rightarrow \forall \bar{x} < y_0\, \eta(\bar{x}) \right].$$

Theorem 10. *For some finite fragment T of IE_1, any consistent extension of T has undecidable diophantine problem.*

Proof. We check that the conditions of Theorem 7 are satisfied. Let $p(\bar{x})$ be given and take a quantifier-free $\theta'(y, \bar{z})$ such that

$$I\Delta_0 + exp \vdash \forall y\ (\forall \bar{x} < y\, p(\bar{x}) \neq 0 \leftrightarrow \exists \bar{z}\ \theta'(y, \bar{z}))$$

using the fact that $I\Delta_0 + exp$ proves the MRDP theorem [3]. By the result from [6] applied to

$$I\Delta_0 + exp \vdash \forall y, \bar{z}\ (\theta'(y, \bar{z}) \rightarrow \forall \bar{x} < y\, p(\bar{x}) \neq 0)$$

there is k so that

$$IE_1 \vdash \forall y, \bar{z}, \bar{w}\left(\theta'(y, \bar{z}) \wedge w_0 = \max(y, \bar{z}) + 1 \wedge \bigwedge_{i=0}^{k-1} \chi(w_i, w_{i+1}) \rightarrow \forall \bar{x} < y\, p(\bar{x}) \neq 0\right).$$

Then let $\theta(y, \bar{z}, \bar{w})$ be

$$\theta'(y, \bar{z}) \wedge w_0 = \max(y, \bar{z}) + 1 \wedge \bigwedge_{i=0}^{k-1} \chi(w_i, w_{i+1})$$

and ψ be $0 = 0$ and note that the conditions of Theorem 7 are satisfied. □

Corollary 11. *There is a finite fragment T of IU_1^- such that any consistent extension of it has an undecidable diophantine problem.*

Proof. The undecidability of the diophantine problem for IU_1^- follows by the conservation result in [5] that IU_1^- and IE_1 share the same $\forall_1$ consequences. The fact that this undecidability is also true of a finite fragment of IU_1^- is because, in the proof of the last theorem, the formula ψ was allowed to be trivial, and hence the only part of Theorem 7 that must be checked for IU_1^- is part (2), and this is a universal sentence. □

References

[1] L. van den Dries, Some model theory and number theory for models of weak systems of arithmetic, in: L. Pacholski et al., eds., Model Theory or Algebra and Arithmetic, Proceedings, Karpacz 1979, Lecture Notes in Math. 834 (Springer, Berlin, 1980) 346–362.

[2] L. van den Dries, Which curves over $\mathbb{Z}$ have points with coordinates in a discrete ordered ring?, Trans. AMS 264 (1981) 181–189.

[3] H. Gaifman and C. Dimitracopoulos, Fragments of Arithmetic and the MRDP Theorem, in: Logic and Algorithmic, Monographie No. 30 de L'Enseignement Mathèmatique (Genève, 1982) 187–206.

[4] W. Hodges, Building Models by Games, London Math. Soc. Student Texts 2 (Cambridge Univ. Press, Cambridge, 1986).

[5] R. W. Kaye, Parameter-free universal induction, Z. Math. Logik 35 (1989) 443–56.

[6] R. W. Kaye, Diophantine Induction, Ann. Pure Appl. Logic 46 (1990) 1–40.

[7] R. W. Kaye, Models of Peano Arithmetic, Oxford Logic Guides 15 (Oxford University Press, Oxford, 1991).

[8] Yu. Matijasevič, Enumerable sets are diophantine, Dokl. Akad. Nauk SSSR 191 (1970) 279–282.

[9] M. Otero, On diophantine equations solvable in models of open induction, J. Symbolic Logic 55 (1990) 779–786.

[10] M. Otero, Models of open induction, D. Phil Dissertation, Oxford University, 1991.

[11] J. C. Shepherdson, The rule of induction in the free variable arithmetic based on + and ·, Proceedings of the symposium at Clermont Ferrand, 1961.

[12] J. C. Shepherdson, A non-standard model for a free variable fragment of number theory, Bull. Polish Acad. Sci. 12 (1964) 79–86.

[13] J. C. Shepherdson, Non-standard models for fragments of number theory, in: J. W. Addison et al., eds., Symposium on the Theory of Models (North-Holland, Amsterdam, 1965) 342–358.

[14] S. Tennenbaum, Non-Archimedean models for arithmetic, Notices Amer. Math. Soc. 6 (1959) 270.

[15] A. J. Wilkie, Some results and problems on weak systems of arithmetic, in: A. Macintyre et al., eds., Logic Colloquium '77 (North-Holland, Amsterdam, 1978) 285–296.

[16] G. M. Wilmers, Bounded existential induction, J. Symbolic Logic 50 (1985) 72–90.