Arch. math. Logik 22 (1982), 51–60

SOME DIOPHANTINE FORMS OF GÖDEL'S THEOREM *

Verena H. Dyson, James P. Jones, and John C. Shepherdson

1. Introduction

Gödel's famous incompleteness theorems [6] are often formulated in terms of R.M.Robinson's theories R and Q (see [13]), the theory PA (Peano Arithmetic) or A.Cobham's fragment R_0 (described in Vaught [14]). For these theories we have $R_0 \subset R \subset Q \subset PA$. So a very general form of Gödel's first theorem is the following:

Gödel's Incompleteness Theorem. *Let T be any axiomatizable ω-consistent extension of R_0. Then there exists a sentence S of elementary number theory such that S is undecidable in T.*

Gödel's proof is constructive and such a sentence may in principle be written down. But if one were to follow the procedure implicit in the proof, then the sentence S would be extremely long. Of course by Gödel's second theorem on consistency we can (at least if $PA \subset T$) take the statement Con_T for S. But Con_T is also arithmetically very complicated. A simpler example for the case $T = PA$ would be the undecidable statement of Paris and Harrington [9]. This is a combinatorial statement, very distinguished by its clear mathematical content, although still very complicated if written arithmetically.
In this paper we establish the undecidability, in various theories, of a certain arithmetical statement constructed earlier by one of the authors, Jones [7]. Although the mathematical content is not so readily understood, the sentence has a simple arithmetical form. In fact it is equivalent to a diophantine sentence.

Theorem 1. *Let T be any axiomatizable ω-consistent extension of R_0. Then there exists a non-negative integer n such that the following sentence, $S(\bar{n})$, is undecidable in T:*

$$\exists ab \forall i_{\leqq \bar{n}} \exists swpq \forall jv \exists eg \{(s+w)^2 + 3w + s = 2i \wedge ([j = w \wedge v = q] \vee [j = 3i \wedge v = p + q] \\ \vee [j = s \wedge (v = p \vee (i = \bar{n} \wedge v = q + \bar{n}))] \vee [j = 3i + 1 \wedge v = pq] \rightarrow a = v + e + ejb \\ \wedge v + g = jb)\}.$$

---

* Eingegangen am 6.7.1979.

The above formula, $S(\bar{n})$ is written in prenex normal form. There are eleven quantified variables in the prefix; $a, b, i, s, w, p, q, j, v, e, g$. These are understood to range over the non-negative integers. The matrix of $S(n)$ contains the logical symbols "$\wedge$" (and), "$\vee$" (or), and "$\rightarrow$" (implication). Since the associative laws are not provable in R_0, we ought to indicate the bracketings of sums and products. But it will be seen that it makes no difference how this is done.
The proposition $S(\bar{n})$ also contains a numeral, $\bar{n}$. The value of n depends upon T. The theorem is that for any theory T a suitable value of n may be found. For example, for some value of n, $S(\bar{n})$ is undecidable in Peano Arithmetic, PA. For some other value of n, $S(\bar{n})$ is undecidable in ZF, etc.
It would be interesting to know an actual specific value of n for which $S(\bar{n})$ is undecidable in PA. We have not yet been able to do this. Perhaps the least such n is very large. But in the case of R_0, R or Q we can give such an n, namely $n=1$. [It follows from [7] that $S(\bar{1})$ is false in classical arithmetic. But in Section 4 we construct a model M for Q in which $S(\bar{1})$ is true.]
In addition to this example of an arithmetical incompleteness, this paper also contains some more general results about diophantine forms of the Gödel-Rosser theorem. In particular we produce a number theory S, a good deal stronger than Q, in which Matijasevič's theorem is provably not formalizable.

2. Proof of Theorem 1

The theories R, Q, and PA are defined in [13, pp. 51–53]. The theory R_0 is essentially R with the axiom schema Ω_5 deleted (see [14]). We shall use the notation of [13] with the exception of using $\bar{n}$ for the numerals Δ_n.
The sentence $S(\bar{n})$ was first constructed in the paper of Jones [7] where it was proved to have the property

$$(2) \qquad n \in W_n \Leftrightarrow S(\bar{n}) \qquad \text{(for all } n\text{)}.$$

Here $W_1, W_2, \ldots$ is a list of all recursively enumerable sets of non-negative integers. (This result, (2) was based on an idea of Julia Robinson [10] and the solution of Hilbert's tenth problem by Yu.V. Matijasevič, Julia Robinson, Martin Davis, and Hilary Putnam [3, 8].)
Since the universally quantified variables j and v of $S(\bar{n})$, are given a finite number of explicit values, it is clear that for each fixed n, $S(\bar{n})$ is provably equivalent to an existential sentence. That is, for each fixed n we have

$$(3) \qquad \vdash_{R_0} S(\bar{n}) \leftrightarrow \exists x_1, x_2, \ldots, x_k \mathscr{S}(x_1, x_2, \ldots, x_k),$$

where $\mathscr{S}$ and k both depend upon n. ($\mathscr{S}$ is a conjunction of $7n+9$ polynomial equations and $k=10n+4$.)
Our proof will use (2) and (3) but no other properties of $S(n)$. Hence the result will hold for any sentence with these two properties, in particular for the existential sentence associated with any universal diophantine equation.

Now by (3), for each fixed n we have

(4) $$\neg S(\bar{n}) \Rightarrow \vdash_{R_0} \neg \mathscr{S}(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_k) \quad (\text{for all } n_1, n_2, \ldots, n_k).$$

This is because R_0 proves (disproves) any substitution instance of correct (incorrect) equations. For the same reason we also have

(5) $$S(\bar{n}) \Rightarrow \vdash_{R_0} S(\bar{n}) \quad (\text{for all } n).$$

Now if T is an axiomatizable theory, then the set $\{n\colon \vdash_T \neg S(\bar{n})\}$ is recursively enumerable. Hence by (2) an index n_0 exists such that

(6) $$S(\bar{n}_0) \Leftrightarrow \vdash_T \neg S(\bar{n}_0).$$

According to (5) and (6), $S(\bar{n}_0)$ implies the inconsistency of T. Therefore $\neg S(\bar{n}_0)$, and so by (6) $\nvdash_T \neg S(\bar{n}_0)$. Also by (4)

(7) $$\vdash_T \neg \mathscr{S}(\bar{n}_1, \bar{n}_2, \ldots, \bar{n}_k) \quad (\text{for all } n_1, n_2, \ldots, n_k).$$

It follows from (3) that $\vdash_T S(\bar{n}_0)$ would imply

(8) $$\vdash_T \exists x_1, x_2, \ldots, x_k \mathscr{S}(x_1, x_2, \ldots, x_k).$$

Conditions (7) and (8) constitute what might be called an instance of an "ω^k-inconsistency". Hence the proof will be completed by establishing the following lemma.

Lemma. *Suppose $R_0 \subseteqq T$. If T is ω-consistent, then T is ω^k-consistent, for all k.*

Proof. Suppose we could find a formula $\Phi(x_1, \ldots, x_k, z)$ with the two properties

(9) $$\vdash_T \forall x_1, \ldots, x_k (\Phi(x_1, \ldots, x_k, \bar{m}) \rightarrow x_1 \leqq \bar{m} \wedge \ldots \wedge x_k \leqq \bar{m}), \quad \text{for all } m,$$

and

(10) $$\vdash_T \forall x_1, \ldots, x_k \exists z \Phi(x_1, \ldots, x_k, z).$$

Then given any $\mathscr{S}(x_1, \ldots, x_k)$ satisfying (7) and (8), we could define $\mathscr{S}'(z)$ by

(11) $$\mathscr{S}'(z) = \exists x_1, \ldots, x_k (\Phi(x_1, \ldots, x_k, z) \wedge \mathscr{S}(x_1, \ldots, x_k)).$$

Then (7) and (9) would imply $\vdash_T \neg \mathscr{S}'(\bar{m})$, for every m, whereas (8) and (10) would imply that $\vdash_T \exists z \mathscr{S}'(z)$. Thus the problem is reduced to finding a formula $\Phi(x_1, \ldots, x_k, z)$ satisfying (9) and (10). This is not difficult if $T \supseteqq PA$. We may simply take $\Phi(x_1, \ldots, x_k, z)$ to be $x_1 \leqq z \wedge x_2 \leqq z \wedge \ldots \wedge x_k \leqq z$. It is also not difficult when $T \supseteqq Q$. We may then take $\Phi(x_1, \ldots, x_k, z)$ to be $(\ldots((x_1 + x_2) + x_3) + \ldots) + x_k = z$. However, given only $T \supseteqq R$, the problem is more difficult. In this case we find it necessary to first define $x \leqq' y$ by $x \leqq y \vee \neg y \leqq x$. We then have

$$\vdash x \leqq' x, \quad \vdash x \leqq' y \vee y \leqq' x \quad \text{and} \quad \vdash_R x \leqq' \bar{n} \rightarrow x \leqq \bar{n}.$$

For $\Phi(x_1, \ldots, x_k, z)$ we may then take the formula $\varphi(x_1, x_2, \ldots, x_k, z)$, defined by

$$\varphi(x_1, \ldots, x_k, z) = \bigvee_{\sigma \in \Pi} x_{\sigma(1)} \leqq' x_{\sigma(2)} \wedge x_{\sigma(2)} \leqq' x_{\sigma(3)} \wedge \ldots \wedge x_{\sigma(k-1)} \leqq' x_{\sigma(k)} \wedge x_{\sigma(k)} \leqq' z .$$

Here Π denotes the set of all permutations of $\{1, 2, \ldots, k\}$. It is a straight forward exercise to check that the formula $\varphi(x_1, \ldots, x_k, z)$ has properties (9) and (10) for $T = R$.

To construct a formula $\Phi(x_1, x_2, \ldots, x_k, z)$ such that conditions (9) and (10) hold for $T = R_0$, we first define an auxiliary formula $N(x)$ by writing

$$N(x) = 0 \leqq x \wedge (\forall y)(y \leqq x \rightarrow S(y) \leqq x \vee x \leqq S(y)).$$

Here $S(y)$ denotes the successor of y. Now it is not difficult to see that for each n

$$\vdash_{R_0} N(\bar{n}), \quad \vdash_{R_0} N(x) \rightarrow (x \leqq \bar{n} \vee \bar{n} \leqq x), \quad \text{and} \quad \vdash_{R_0} N(x) \rightarrow (x \leqq' \bar{n} \rightarrow x \leqq \bar{n}).$$

Hence for $\Phi(x_1, x_2, \ldots, x_k, z)$ we may take the formula

$$N(z) \rightarrow N(x_1) \wedge N(x_2) \wedge \ldots \wedge N(x_k) \wedge \varphi(x_1, x_2, \ldots, x_k, z),$$

where φ is given by (12). This completes the proof of the Lemma and hence the proof of Theorem 1. As a corollary we have

Corollary 1. *Let T be any axiomatizable ω-consistent extension of R_0. Then some diophantine sentence is undecidable in T.*

By a *diophantine sentence* we have in mind a statement of the form $\exists x_1, x_2, \ldots, x_n (P(x_1, x_2, \ldots, x_n) = Q(x_1, x_2, \ldots, x_n))$ where P and Q are polynomials with non-negative integer coefficients. The theory R_0 is not strong enough to prove the usual equivalence of single equations with conjunctions and disjunctions of equations. Thus an existential sentence, such as that in (3), is not necessarily equivalent in R_0 to a diophantine sentence. Nevertheless, there is no reason why we cannot begin with such a sentence initially. Properties (2) and (3) were all that we required in the proof of Theorem 1.

3. Decision Problem for $S(n)$

It follows from (2) that $S(n)$ is also undecidable as a predicate, in the recursive sense that there exists no algorithm to determine the truth or falsity of $S(n)$ for general n. The same is true as regards the decision problem for provability of $S(n)$. It follows from (3), (4), (5) and ω-consistency that

$$(13) \qquad S(n) \Leftrightarrow \vdash_T S(\bar{n}) \quad \text{(for all } n).$$

Hence the provability of $S(\bar{n})$ in each ω-consistent extension of R_0 is undecidable. We shall see in the next section that the ω-consistency hypothesis is very important here. It cannot be replaced by simple consistency.

Remark. If we take $T=Q$ in (13) and let $\mathcal{Q}$ denote the logical conjunction of the seven axioms of Q, then we obtain

(14) $$S(n) \Leftrightarrow \vdash \mathcal{Q} \rightarrow S(\bar{n}).$$

Thus we obtain a visualizable form of Church's theorem. There is no decision method to decide the *logical* validity of $\mathcal{Q} \rightarrow S(\bar{n})$, for general n.

4. Rosser Form of Theorem 1

In 1936 J. Barkley Rosser [11] obtained a famous strengthened form of Gödel's Incompleteness Theorem in which Gödel's ω-consistency hypothesis was replaced by the weaker hypothesis of (simple) consistency. One might suppose that this would be possible in our Theorem 1. However it is *not*. Theorem 1 is false with this change, even if we replace R_0 by R or Q. For we can prove.

Theorem 2. *There is a finitely axiomatizable consistent extension D of Q in which all diophantine sentences are decidable.*

Proof. Consider a slight variation on the nonstandard model for Q given on p. 55 of [13], viz the cardinal numbers $0, 1, 2, \ldots, \infty$, with $+$ and $\cdot$ interpreted as cardinal addition and multiplication and $S(\infty)=\infty$. Call this model M. Every diophantine equation $P(x_1, \ldots, x_n)=Q(x_1, \ldots, x_n)$ has a trivial solution in M unless P or Q are polynomials of degree zero. To obtain D it is enough to add three axioms to Q.

$$(D_1)\,\forall x, y(x+y=y+x), \qquad (D_2)\,\forall x, y(xy=yx), \qquad (D_3)\,\exists z \forall x(x+z=z).$$

Call this theory D. (It is ω-inconsistent.) From axioms D_1, D_2 and the axioms of Q, one can prove $x \leqq x+y$ and $y \leqq x+y$. Furthermore one can prove that $y \neq 0 \rightarrow x \leqq xy$. Here we are using the definition of $\leqq$ given in [13]. Therefore sentences of the form $\exists x_1, \ldots, x_n(P(x_1, \ldots, x_n)=\bar{m})$ are always decided correctly by D. Sentences of the form $\exists x_1, \ldots, x_n(P(x_1, \ldots, x_n)=Q(x_1, \ldots, x_n))$, where both P and Q are polynomials of positive degree, are always provable in D. This follows from the fact that an infinite element, ∞ [forced to exist by (D_3)], has the properties $x+\infty=\infty+x=\infty$, $S(\infty)=\infty$, and (for $x \neq 0$) $x\infty=\infty x=\infty$. Theorem 2 is proved.

Although the usual equivalence of conjunctions and disjunctions of equations to single equations is not provable in D it is not difficult to see that existential quantifications of such formulae are also decidable in D, i.e. Theorem 2 holds with this more general notion of diophantine sentence. On the other hand, sentences of the form

$$\exists x_1, \ldots, x_n[P(x_1, \ldots, x_n)=Q(x_1, \ldots, x_n) \wedge R(x_1, \ldots, x_n) \neq S(x_1, \ldots, x_n)]$$

are not in general decidable in D. However if we drop the condition of finite axiomatizability then we can obtain an extension of Q in which all existential sentences are decidable, including now as existential sentences, those with $\neg$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$ in the matrix, as well as $=$, $+$, $\cdot$, 0, and 1. In fact we can obtain such an extension of a theory far stronger than Q. We call this theory S.
The theory S is an elementary number theory essentially intermediate in strength between Q and PA. The theory S could be formulated in such a way that $Q \subset S \subset PA$ although we prefer to use here as nonlogical symbols 0, 1, $+$, $\cdot$, $=$, $<$ instead of 0, $+$, $\cdot$, S, $=$, traditionally associated with Q. The axiom system of S consists of the usual axioms of equality together with the following 21 sentences (not independent).

(1) $(x+y)+z=x+(y+z)$

(2) $(x\cdot y)\cdot z=x\cdot(y\cdot z)$

(3) $x+y=y+x$

(4) $x\cdot y=y\cdot x$

(5) $x(y+z)=xy+xz$

(6) $x+0=x$

(7) $x\cdot 0=0 \wedge x\cdot 1=x$

(8) $x+y=0 \rightarrow x=0 \wedge y=0$

(9) $xy=0 \rightarrow x=0 \vee y=0$

(10) $x+z=y+z \rightarrow x=y$

(11) $xz=yz \rightarrow (x=y \vee z=0)$

(12) $\neg(x<x)$

(13) $x<y \wedge y<z \rightarrow x<z$

(14) $x<y \vee x=y \vee y<x$

(15) $x=0 \vee 0<x$

(16) $x<y \leftrightarrow x+z<y+z$

(17) $0 \neq z \wedge x<y \rightarrow xz<yz$

(18) $0 \neq z \rightarrow \exists x(z=x+1)$

(19) $\exists z(z^2 \leqq x<(z+1)^2)$

(20) $x_1=x_2 \wedge y_1=y_2 \leftrightarrow x_1^2+x_2^2+y_1^2+y_2^2=2x_1x_2+2y_1y_2$

(21) $x_1=x_2 \vee y_1=y_2 \leftrightarrow x_1y_1+x_2y_2=y_1x_2+x_1y_2$.

The theory S is considerably stronger than Q. For example the axioms imply embeddability into an integral domain. Also axioms (20) and (21) imply that conjunctions and disjunctions of equations are equivalent to single equations. However the theory S is still not strong enough for the existential Gödel-Rosser theorem (and not strong enough to formalize the bounded quantifier theorem through to the Pell or Fibonacci development). For we can prove

Theorem 3. *There is a consistent axiomatizable extension of the theory S in which all existential sentences are decidable.*

Proof. As we are giving up the property of finite axiomatizability (possessed by the Theory D), it is clearly enough to produce a model M_1 for S such that the set of existential sentences true in M_1 is recursive. The model M_1 will be a certain subset of the positive elements of a real closed field. It is closely related to the model M_0 of Shepherdson [12]. It was noted there, in [12], that the field R_t of formal fractional power series in t^{-1}, i.e. expressions of the form

$$a_p t^{p/q} + a_{p-1} t^{(p-1)/q} + \ldots + a_0 + a_{-1} t^{-1/q} + a_{-2} t^{-2/q} + \ldots$$

with real coefficients (p, q being natural numbers with $q>0$) is real closed. The ordering of R_t is the non-archimedean one determined by saying that t is infinitely large. We take the set of elements of M_1 to be the subset of R_t consisting of all elements with $p>0$ and $a_p>0$, together with all natural numbers a_0 (i.e. all natural numbers and all elements greater than all natural numbers). Addition and multiplication are defined in M_1 as in R_t. Clearly this gives a model for S. We now complete the proof by giving an effective method for deciding which existential sentences are true in M_1.

Note that the ordering of M_1 is not the usual one defined in Q by

$$x \leqq y \leftrightarrow (\exists w)(w + x = y);$$

for example $t \leqq t + \frac{1}{2}$, but since $\frac{1}{2}$ is not in M_1 we do not have $(\exists w)(w + t = t + \frac{1}{2})$. However we shall allow $<$ as well as $+$, $\times$ to occur in what we call existential sentences, i.e. these are of the form

$$\exists x_1, \ldots, x_n \phi(x_1, \ldots, x_n),$$

where ϕ contains no quantifiers but may contain $<$ as well as $+$, $\times$, 0, 1, $=$, $\wedge$, $\vee$, $\neg$, $\rightarrow$, and $\leftrightarrow$.

Now let $\phi(x)$ be a formula (not necessarily quantifier free) containing only x free. The Tarski decision method allows us to replace $\phi(x)$ by a quantifier free formula $\chi(x)$ which is equivalent to it in all real closed fields. The formula $\chi(x)$ may be taken to be a Boolean combination of atomic formulae of the forms

$\alpha(x)=0$, $\alpha(x)>0$, where α is a polynomial with integer coefficients.

Now if $a_0, \ldots, a_n$ are integers and $a_n \neq 0$ and we put

$$N_\alpha = |a_0| + \ldots + |a_n|$$

then, for $x \geqq N_\alpha$,

$$\alpha(x) = a_0 + a_1 x + \ldots + a_n x^n$$

is of the same sign as a_n, i.e. $\alpha(x)=0$, $\alpha(x)>0$ are of constant truth value for $x \geqq N_\alpha$. So if we define N_χ to be the maximum N_α for all α occurring in χ, and finally put $N_\phi = N_\chi$ we have

$$(\exists x)\phi(x) \leftrightarrow (\exists x)_{\leqq N_\phi} \phi(x)$$

is true in all real closed fields, the bound N_ϕ being computable from ϕ.

The decision method for truth of existential sentences $\exists x_1, \ldots, x_n \phi(x_1, \ldots, x_n)$ is now defined by induction on n.

$n=0$. In this case ϕ has no variables and is a Boolean combination of numerical formulae whose truth value can be computed (it is the same in M_1 as in N).

Inductive Step

Let $\Phi \leftrightarrow \exists x_1, \ldots, x_n \phi(x_1, \ldots, x_n)$.
Use the Tarski decision method to see whether

$$(\forall z)(\exists x_1 \ldots x_n)(\phi(x_1, \ldots, x_n) \wedge x_1 > z \wedge \ldots \wedge x_n > z) \tag{17}$$

is true in all real closed fields. If so then it is true in R_t so taking $z = t$ we see that Φ is true in M_1 (since all elements of R_t which are $\geqq t$ are in M_1). Now ϕ is quantifier free, so if it holds in R_t for elements $x_1, \ldots, x_n$ of M_1 it also holds in M_1 for these elements. Now if (17) is not true in all real closed fields then

$$(\exists z)(\forall x_1 \ldots x_n)(\phi(x_1, \ldots, x_n) \rightarrow x_1 \leqq z \vee \ldots \vee x_n \leqq z) \tag{18}$$

is true in all real closed fields, in particular in R_t. Use the remark above to compute N so that

$$(\exists z)_{\leqq \bar{N}}(\forall x_1 \ldots x_n)(\phi(x_1, \ldots, x_n) \rightarrow x_1 \leqq z \vee \ldots \vee x_n \leqq z)$$

i.e.

$$(\forall x_1 \ldots x_n)(\phi(x_1, \ldots, x_n) \rightarrow x_1 \leqq \bar{N} \vee \ldots \vee x_n \leqq \bar{N})$$

is true in all real closed fields, in particular R_t. Since it is a universal statement it will also be true in M_1.
So, in M_1,

$$\Phi \leftrightarrow \exists x_1 \ldots x_n \phi(x_1, \ldots, x_n)$$

$$\leftrightarrow \bigvee_{j=0}^{N} (\exists x_2, \ldots, x_n) \phi(\bar{j}, x_2, \ldots, x_n) \vee \ldots \vee (\exists x_1, \ldots, x_{n-1}) \phi(x_1, \ldots, x_{n-1}, \bar{j}).$$

But, by the induction hypothesis we can decide the truth in M_1 of this last sentence, hence that of Φ. Theorem 3 is proved.
We have just seen that the Rosser form of Theorem 1 (and its Corollary) is false even if R_0 is replaced by a theory S, a good deal stronger than Q. But relying on unpublished work of Pridor and Julia Robinson we can show that the Rosser form of Theorem 1 is true if R_0 is replaced by PA.

Theorem 4. *Let T be any consistent axiomatizable extension of PA. Then some diophantine sentence is undecidable in T.*

Theorem 4 follows immediately from the next two lemmas.

Lemma 1. *Let T be any axiomatizable consistent theory in which each recursive set is numeralwise definable by one of the formulas $\Phi_n(x)$ (where the Gödel number of $\Phi_n(x)$ is a recursive function of n). Then for some n, $\Phi_n(n)$ is formally undecidable in T.*

Proof. Suppose not. Suppose that for each n, $\Phi_n(n)$ is decidable, i.e. provable or refutable in T. Put $V = \{n : \vdash_T \neg \Phi_n(n)\}$. Then V is an r.e. set. But the complement of

V is also r.e. So V is a recursive set. Hence there exists n_0 such that $\Phi_{n_0}(x)$ defines V in T. If $n_0 \in V$, then $\vdash_T \Phi_{n_0}(n_0)$, so not $\vdash_T \neg\Phi_{n_0}(n_0)$ and hence $n_0 \notin V$. If $n_0 \notin V$, then $\vdash_T \neg\Phi_{n_0}(n_0)$, so $n_0 \in V$. Hence a contradiction is obtained.

Lemma 1 is proved.

Lemma 2. *Every recursive set is numeralwise definable in PA by a diophantine formula.*

Proof. If A is a recursive set, then A and $\bar{A}$ are r.e. sets so by Davis et al. [3] and Matijasevič [8] there exist polynomials P, Q, P', and Q' (with positive integer coefficients) such that for all natural numbers a, both

(19) $$a \in A \Leftrightarrow \exists x_1, \ldots, x_n (P = Q),$$

and

(20) $$a \in \bar{A} \Leftrightarrow \exists y_1, \ldots, y_n (P' = Q').$$

(Using a universal diophantine equation P, Q, P', and Q' can be found uniformly for A.)

Now it is not difficult to understand (see e.g. [1, p. 340, Theorem 7.10]) that A is then numeralwise defined (in fact in R) by the formula

(21) $$\exists z[(\exists x_1, \ldots, x_n)_{<z}(P = Q) \wedge (\forall y_1, \ldots, y_n)_{<z}(P' \neq Q')].$$

Formula (21) is a diophantine analogue of the Rosser trick [11]. Now using pairing functions and replacing the predicate $P' \neq Q'$ by $\exists y[(P' - Q')^2 = y + 1]$, one finds that (21) is provably equivalent in PA to a formula of the form

(22) $$\exists z[(\exists x_1, \ldots, x_n)_{<z}(P = Q) \wedge (\forall y)_{<F(z)}(\exists y_1, \ldots, y_n)(\exists y)(P' = Q')],$$

where there is only one bounded universal quantifier and P, Q, P', Q', and F are polynomials with positive integer coefficients.

Now Julia Robinson has given a proof of (a modern version of, cf. [4]) the Bounded Quantifier Theorem of [3], by induction (unpublished). Also Pridor (see [5]) has shown that the Bounded Quantifier Theorem (and concomitant factorial to binomial coefficient to Pell or Fibonacci number development) is provable in PA. This result is also claimed in Carstens [2]. Relying on these results, it follows that the right conjunct of (22) is provably diophantine and hence that it may be replaced by an existential formula. (Theorem 3 shows that no such formalization can be carried out in the theory S.)

REFERENCES

[1] Bell, J., Machover, M.: A course in mathematical logic. Amsterdam: North-Holland 1977.

[2] Carstens, H.G.: The theorem of Matijasevič is provable in Peano's arithmetic by finitely many axioms. Logique et analyse **20**, 116–121 (1978).
[3] Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential diophantine equations. Ann. Math. **74**, 425–436 (1961).
[4] Davis, M., Matijasevič, Y., Robinson, J.: Hilbert's tenth problem. Diophantine equations. Positive aspects of a negative solution. Proceedings of the conference on the Hilbert problems, Dekalb, Illinois, May 1974 (Am. Math. Soc. 1976, pp. 323–378).
[5] Gaifman, H.: In Conference in Mathematical Logic, p. 132, London 1970, ed. W. Hodges. Berlin, Heidelberg, New York: Springer 1972. Gaifman also said in a letter dated 31/1/78 that he and his seminar students had again checked through the details of the proof of the bounded quantifier theorem in *PA*.
[6] Gödel, K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. I. Monatsh. Math. und Physik **38**, 173–198 (1931), [English translations: Gödel, K.: On formally undecidable propositions of principia mathematica and related systems. The undecidable. Davis, M. (ed.). Raven Press, 1965, pp. 5–38. (2) From Frege to Gödel, Jean Van Heijenoort (ed.), Harvard University Press, 1967, pp. 596–616.]
[7] Jones, J.P.: Three universal representations of recursively enumerable sets. J. Symbolic Logic **42**, 335–351 (1977)
[8] Matijasevič, Yu.V.: Enumerable sets are diophantine (Russian). Doklady Akademii Nauk SSSR **191**, 279–282 (1970). [English translation: Soviet Mathematics, Doklady **11**, 354–358 (1970).]
[9] Paris, J., Harrington, L.: A mathematical incompleteness in Peano arithmetic. Handbook of Mathematical Logic, J. Barwise (ed.), Studies in Logic and the Foundations of Mathematics, Vol. 90, pp. 1133–1142. Amsterdam: North-Holland 1977.
[10] Robinson, J.: Hilbert's tenth problem. Proc. Symp. Pure Math. **20**, 191–194 (1971).
[11] Rosser, J.B.: Extensions of some theorems of Gödel and Church. J. Symbolic Logic **1**, 87–91 (1936).
[12] Shepherdson, J.C.: A non-standard model for a free variable fragment of number theory. Bull. Acad. Polon. Sci: Ser. Math. Astronom. Phys. **12**, 79–86 (1964).
[13] Tarski, A., Mostowski, A., Robinson, R.: Undecidable theories, $ix+98$ pp. Amsterdam: North-Holland 1953.
[14] Vaught, R.L.: On a theorem of Cobham concerning undecidable theories. Logic, Methodology and Philosophy of Science, Proceedings of the 1960 International Congress, ed. by E. Nagel, P. Suppes, and A. Tarski, pp. 14–25. Stanford: Stanford University Press 1962.

Verena H. Dyson
James P. Jones
University of Calgary
Calgary, Alberta, Canada, T2N 1N4

John C. Shepherdson
School of Mathematics
University of Bristol
University Walk
Bristol, England, BS8 1TW