

Relatively Diophantine Correct Models of Arithmetic

BONNIE GOLD*

A model M of Peano arithmetic is called *diophantine correct* if every polynomial which has a root in M already has a root in \mathbf{N} (the standard natural numbers). Lipshitz [2] has shown that if M is a countable nonstandard model of Peano arithmetic, then M is diophantine correct if and only if for every nonstandard $\alpha \in M$ there is an embedding of M onto an initial segment of $[0, \alpha] = \{x \in M \mid x \leq \alpha\}$. In this paper we extend this result to the case of a countable model M being diophantine correct relative to a submodel N (see definition in Section 1 below).¹

I We are repeatedly going to talk about N -polynomials $p(\bar{x})$, where N is a countable model of Peano arithmetic, and about the result of substituting a sequence of elements \bar{a} (usually in a larger model M) into $p(\bar{x})$, getting $p(\bar{a})$. By an N -polynomial $p(\bar{x})$ we mean a nonstandard polynomial which is coded by its Gödel-number $\ulcorner p(\bar{x}) \urcorner$. Notice that N -polynomials will, in general, have a nonstandard number of variables, as well as nonstandard sums, products, and coefficients. When phrases such as “the polynomial $p(\bar{x})$ ” or “ $p(\bar{a}) = b$ ” appear in formulas the reader is to understand that the formula actually is one involving the Gödel numbers of such polynomials. We shall repeatedly use the fact that the sets of Gödel numbers of polynomials, and of formulas “ $p(\bar{x}) = y$ ”, are defined by Σ_1 formulas and, using the results of Matijasevič [3], by π_1 formulas. We will assume the reader is familiar with the basic model theory and coding techniques used in the study of nonstandard models of arithmetic (see, e.g., Pillay [5]).

Let M and N be models of Peano arithmetic. M is *N -diophantine correct* if for every N -polynomial $p(\bar{x})$, if $p(\bar{x})$ has a zero in M then it already has one in N .

Wilkie [6] has shown that every countable model N of Peano arithmetic has an end extension M such that $N \approx M$ and such that M solves a diophantine equation with coefficients in N that is not solvable in N . Hence, every countable non-

*I would like to thank the referee for helping make Proposition 3 less convoluted. I would like to thank L. Lipshitz for suggesting the problem to me.

standard model N has an end extension which is diophantine correct with respect to standard polynomials but which is not N -diophantine correct.

On the other hand, by just taking an elementary end extension via the MacDowell Specker theorem one also gets an N -diophantine correct end extension.

An observation of M. Kaufmann permits us to confine our attention to N an initial segment of M .

Proposition 1 (Kaufmann) *If $N \subset M$ are models of Peano arithmetic and \bar{N} is the initial segment of M with which N is cofinal, then M is N -diophantine correct if and only if M is \bar{N} -diophantine correct.*

Proof: \Leftarrow By a theorem of Gaufman's [1], N is an elementary submodel of \bar{N} . If M is \bar{N} -diophantine correct and $p(\bar{x})$ is an N -polynomial with a zero in M , then $\bar{N} \models (\exists \bar{x})(p(\bar{x}) = 0)$, so $N \models (\exists \bar{x})(p(\bar{x}) = 0)$. Thus $p(\bar{x})$ has a root in N , and so M is N -diophantine correct.

\Rightarrow Let $p(\bar{x})$ be an \bar{N} -polynomial and \bar{a} a sequence from M such that $M \models p(\bar{a}) = 0$. Assume M is N -diophantine correct. We must find a root of $p(\bar{x})$ in \bar{N} . Let $b \in N$ be greater than the Gödel number of $p(\bar{x})$. Let $c \in N$ code the smallest zeroes of N -polynomials whose Gödel numbers are less than b ; that is, if $q(\bar{x})$ is an N -polynomial whose Gödel number is less than b , then $M \models q(\bar{c})_{\uparrow q} = 0$. Then $N \models (\text{for all polynomials } q \text{ with Gödel number less than } b) (\exists \bar{z}(q(\bar{z}) = 0) \Rightarrow q(\bar{c})_{\uparrow q} = 0)$. Notice that this is a Π_1 statement over N ; that is, it is of the form $(\forall \bar{y})\phi(\bar{y})$ where ϕ just involves bounded quantifiers. Hence, since M is N -diophantine correct, it is true in M . Thus for every M - (or equivalently, \bar{N} -) polynomial q with $\ulcorner q \urcorner < b$, $M \models [(\exists \bar{z})(q(\bar{z}) = 0) \rightarrow q(\bar{c})_{\uparrow q} = 0]$. Hence $(\bar{c})_{\uparrow p}$ is a zero of $p(\bar{x})$ in \bar{N} . Thus M is \bar{N} -diophantine correct.

Although the definition of N -diophantine correct involves all N -polynomials, we can restrict our attention to standard polynomials (that is, a standard number of variables, sums, and products) with coefficients from N .

Proposition 2 *Let $N \subset M$ be models of Peano arithmetic. M is N -diophantine correct if and only if every standard polynomial $q(\bar{x})$ with coefficients from N which has a root in M already has a root in N .*

Proof: \Rightarrow obvious.

\Leftarrow The assertion “ x is the value of the polynomial with Gödel-number y evaluated at the sequence with Gödel number z ” is a Σ_1 formula. Hence, by the results of Matijasevič [3], it is equivalent to some formula $\exists \bar{u}(p(x, y, z, \bar{u}) = 0)$ where p is a standard polynomial. Hence if $q(\bar{z})$ is an N -polynomial with a root \bar{a} in M , say $q(\bar{z})$ has Gödel number $n \in N$. Then $M \models \exists \bar{u}[p(0, n, a, \bar{u}) = 0]$ (where a is the Gödel number of \bar{a}), and thus there is a $\bar{b} \in M$ for which $M \models p(0, n, a, \bar{b}) = 0$. Notice that $p(0, n, z, \bar{u})$ can be thought of as $p_1(z, \bar{u})$, a standard polynomial with coefficients (the n) from N . Now, $p_1(z, \bar{u})$ has a root, (a, \bar{b}) , in M . So by our hypothesis $p_1(z, \bar{u})$ has a root (a_1, \bar{b}_1) in N . That is, $N \models p(0, n, a_1, \bar{b}_1) = 0$ and thus $N \models \exists \bar{u}(p(0, n, a_1, \bar{u}) = 0)$. Hence, \bar{a}_1 is a root of $q(\bar{z})$ in N . Therefore, M is N -diophantine correct.

Let $N \subset M$ be models of Peano arithmetic, and let f be a function from M into itself. f is an N -embedding if f is a standard homomorphism of M which keeps N fixed. Note: we call it an N -embedding rather than simply an N -

homomorphism because *any* homomorphism of a model of arithmetic is an embedding (since “ $a < b$ ” is existential).

Proposition 3 *Let $N \subset M$ be models of Peano arithmetic, and let f be a map from M into itself. Then f is an N -embedding if and only if (1) for every N -sequence from M with Gödel-number a , $f(a)$ is an N -sequence of the same length, and (2) if $p(\bar{x})$ is an N -polynomial and \bar{a} is an N -sequence, $M \models p(\overline{f(\bar{a})}) = f(p(\bar{a}))$.*

Proof: $\Rightarrow (\bar{x})_i = y$ is Σ_1 and hence by Matijasevič [3] is existential; thus it is preserved by N -embeddings. So $f(\bar{x})$ is a sequence of the same length as \bar{x} for all N -sequences \bar{x} . Similarly, “the polynomial coded by x evaluated at the sequence coded by y equals z ” is Σ_1 and hence $f(p(\bar{a})) = p(\overline{f(\bar{a})})$ for all N -polynomials $p(\bar{x})$ and all N -sequences of the correct length \bar{a} .

\Leftarrow Using $x^2 - x$ and $x^2 - 2x$ it is clear from (2) that $f(0) = 0$ and then $f(1) = 1$. It then follows from (2) that f is a standard homomorphism of M . Now, let $n \in N$ and let $p_n(x_1 \dots x_n) = x_1 + \dots + x_n$. Then $M \models p(1, \dots, 1) = 1 + \dots + 1 = n$; hence $M \models p(f(1), \dots, f(1)) = f(1) + \dots + f(1) = nf(1) = n = f(p(1, \dots, 1)) = f(n)$. Hence, f keeps N fixed.

2 We are now ready to state and prove the main theorem.

Theorem *Let $N \subset M$ be countable models of Peano arithmetic. M is N -diophantine correct if and only if for every $\alpha \in M$ which is bigger than everything in N there is an N -embedding of M onto an initial segment of $[0, \alpha]$.*

Proof: The proof follows the general outline of Lipshitz [2], but details are provided since the proof there is rather brief and some of the steps are a little different in our case.

\Leftarrow Assume that M is not N -diophantine correct. Then there is an N -polynomial $p(\bar{x})$ which has a root in M but none in N . Since $N \not\prec \bar{N}$, $p(\bar{x})$ has no roots in \bar{N} . It follows that there is an $\alpha \in M \setminus \bar{N}$ (i.e., greater than everything in N) such that $p(\bar{x})$ has no roots less than α . For, let $\phi(y)$ be the formula $(\exists \bar{x} < y)(p(\bar{x}) = 0)$. (Notice that, since p is a nonstandard polynomial this is actually a formula involving Gödel numbers.) If $p(\bar{x})$ had roots arbitrarily close to \bar{N} in M , $\phi(x)$ would be false for all $x \in \bar{N}$ but true for all $x \in M \setminus \bar{N}$, violating induction in M .

Thus there can't be an N -embedding of M into $[0, \alpha]$, since if \bar{a} is a root of $p(\bar{x})$ and f is an N -embedding, $p(\overline{f(\bar{a})}) = f(p(\bar{a})) = f(0) = 0$ so $\overline{f(\bar{a})}$ would be a root of $p(\bar{x})$ which would be less than α .

\Rightarrow Assume M is N -diophantine correct, and let $\alpha > N$ be fixed. We wish to find an N -embedding of M onto an initial segment of $[0, \alpha]$. By Proposition 1, we can assume N is an initial segment of M , since an \bar{N} -embedding is a fortiori an N -embedding. By Proposition 3 it will suffice to find a standard homomorphism which keeps N fixed. To do this it will suffice to find a function onto an initial segment of $[0, \alpha]$ keeping N fixed such that for every standard polynomial $p(\bar{a}, \bar{x})$, \bar{a} constants from M , with coefficients in N which has a root in M , $p(\overline{f(\bar{a})}, \bar{x})$ has a root in that initial segment.

Now, let $\{c_i\}_{i < \omega}$ be a list of $M \setminus N$, $\{d_i\}_{i < \omega}$ a list of $[0, \alpha] \setminus N$. Define $f(n) = n$ for all $n \in N$. We will define a_i, b_i ($i \geq 1$) and $f(a_i)$ by induction so

that $f(a_i) = b_i$, a_i exhausts $M \setminus N$ (using odd i 's), and b_i exhausts some initial segment of $[0, \alpha] \setminus N$ (using even i 's).

Assume $a_1, \dots, a_{2j}, b_1, \dots, b_{2j}$, and $f(a_1), \dots, f(a_{2j})$ have been defined so that $a_i \in M \setminus N$, $b_i \in [0, \alpha] \setminus N$, and $f(a_i) = b_i$ for each i ; and such that

(**) for every N -polynomial $p(x_1, \dots, x_{2j}, \bar{y})$ if $M \models (\exists \bar{y}) [p(a_1, \dots, a_{2j}, \bar{y}) = 0]$ then $M \models (\exists \bar{y} < \alpha) [p(b_1, \dots, b_{2j}, \bar{y}) = 0]$.

Notice that for $j = 0$, (**) is true, since if $p(\bar{x})$ is an N -polynomial, either: (a) the roots of $p(\bar{x})$ are bounded in N , say by n_0 , in which case, since M is N -diophantine correct, $p(\bar{x})$ can have no roots in $M \setminus N$ (consider the polynomial $q(\bar{x})$ which says " $p(\bar{x})$ and $x > n_0$ ": $q(\bar{x})$ has no roots in N , but if $p(\bar{x})$ had a root in $M \setminus N$, $q(\bar{x})$ would have a root in M , violating N -diophantine correctness); or (b) the roots of $p(\bar{x})$ are unbounded in N , in which case by induction in M there are roots of $p(\bar{x})$ between N and α (otherwise the formula $\chi(y)$ which says $[y < \alpha$ and $(\exists \bar{x} > y)(p(\bar{x}) = 0)]$ would be true in M for all $y \in N$ but false for all $y \in M \setminus N$, violating induction in M).

(1) Let a_{2j+1} be the first of the c_i which is not in $\{a_1, \dots, a_{2j}\}$. Let $\phi_1^j(n)$ be $(\exists z < \alpha)$ [for all polynomials $p(\bar{y}, \bar{x})$ of length $\leq n$, if $(\exists \bar{x})(p(a_1, \dots, a_{2j}, a_{2j+1}, \bar{x}) = 0)$ then $(\exists \bar{x} < \alpha)(p(b_1, \dots, b_{2j}, z, \bar{x}) = 0)$]. Notice that $\phi_1^j(n)$ is actually a messy statement involving the Gödel numbers of the polynomials and sequences involved, and also that if $n \in N$, all such polynomials are N -polynomials. We will show that $M \models \phi_1^j(n)$ for all $n \in N$. Fix $n \in N$. Let p_1, \dots, p_s ($s \in N$) be all N -polynomials of Gödel-number $\leq n$ such that $M \models \exists \bar{x}(p(a_1, \dots, a_{2j}, a_{2j+1}, \bar{x}) = 0)$. (This may be an infinite number of polynomials, but is an N -finite number of them). Then the sum $\sum_{i=1}^s p_i^2(y_1, \dots, y_{2j+1}, \bar{x}_i)$ (where the \bar{x}_i involve distinct variables for distinct p_i) is an N -polynomial $q(\bar{y}, \bar{z})$. By the definition of the p_i 's, $M \models \exists \bar{z}[q(\bar{a}, a_{2j+1}, \bar{z}) (=q(a_1, \dots, a_{2j}, a_{2j+1}, \bar{z})) = 0]$. Hence, $M \models \exists \bar{z}, z[q(\bar{a}, z, \bar{z}) = 0]$. By (**), $M \models (\exists \bar{z}, z < \alpha)[q(\bar{b}, z, \bar{z}) = 0]$. Hence $M \models (\exists z < \alpha) \left(\bigwedge_{i=1}^s (\exists \bar{x}_i < \alpha)[p_i(b_1, \dots, b_{2j}, z, \bar{x}_i) = 0] \right)$. That is, $M \models \phi_1^j(n)$. Since $M \models \phi_1^j(n)$ for all $n \in N$, by induction in M there is an $m \in M \setminus N$ such that $M \models \phi_1^j(m)$. Let b_{2j+1} be the z for $\phi_1^j(m)$ and let $f(a_{2j+1}) = b_{2j+1}$. Then (**) is now true for $2j + 1$.

(2) Now let b_{2j+2} be the first d_i which does not appear among $\{b_1, \dots, b_{2j+1}\}$ but which is less than some one of them; say $b_{2j+2} < b_k$. (If there is no such d_i , let $a_{2j+2} = a_{2j+1}$, $b_{2j+2} = b_{2j+1}$, and continue.) Let $\phi_2^j(n)$ be $(\exists z < a_k)$ [for all N -polynomials $p(x_1, \dots, x_{2j+2}, \bar{y})$ of length $\leq n$, if $(\neg \exists \bar{y} < \alpha)[p(b_1, \dots, b_{2j+1}, b_{2j+2}, \bar{y}) = 0]$ then $\neg \exists \bar{y}[p(a_1, \dots, a_{2j+1}, z, \bar{y}) = 0]$].

We shall again show that for all $n \in N$, $M \models \phi_2^j(n)$. Let p_1, \dots, p_r ($r \in N$) be all the N -polynomials p of Gödel-number $\leq n$ such that $M \models (\neg \exists \bar{y} < \alpha)[p(\bar{b}, b_{2j+2}, \bar{y}) = 0]$. (Again, there are just N -finitely many.) Then $M \models (\exists z < b_k)(\forall \bar{y} < \alpha) \bigwedge_{i=1}^r [p_i(\bar{b}, z, \bar{y}) \neq 0]$. Let $\theta(\bar{w})$ be $(\exists z < w_k)(\forall \bar{y} < \alpha) \bigwedge_{i=1}^r [p_i(\bar{w}, z, \bar{y}) \neq 0]$, where w_k is the k th element of the sequence \bar{w} ; then $M \models \theta(\bar{b})$. Observe that $\vdash \neg \theta(w) \leftrightarrow (\forall z < w_k)(\exists \bar{y} < \alpha) \bigvee_{i=1}^r [p_i(\bar{w}, z, \bar{y}) = 0]$. The two quantifiers on the right can be coded into a function \bar{u} on $[0, w_k]$ so that

$M \models \neg \theta \leftrightarrow \exists \bar{u} [(\forall z < w_k) \bigvee_{i=1}^r [p_i(\bar{w}, z, (\bar{u})_z) = 0]] \wedge (\forall z < w_k) ((\bar{u})_z < \alpha)]$. Notice that $(\forall z < w_k) \bigvee_{i=1}^r [p_i(\bar{w}, z, (\bar{u})_z) = 0]$ has just bounded quantifiers, and so by the results of Matijasevič [3] and the fact that his results can be formalized in Peano arithmetic, there is some N -polynomial $q(\bar{w}, \bar{u}, \bar{v})$ such that $M \models [(\forall z < w_k) \bigvee_{i=1}^r (p_i(\bar{w}, z, (\bar{u})_z) = 0)] \leftrightarrow \exists \bar{v} (q(\bar{w}, \bar{u}, \bar{v}) = 0)$. Hence, (a) $M \models (\exists z < w_k) (\forall y < \alpha) \bigwedge_{i=1}^r (p_i(\bar{w}, z, \bar{y}) \neq 0) \leftrightarrow \neg \exists \bar{u} [\exists \bar{v} (q(\bar{w}, \bar{u}, \bar{v}) = 0) \wedge (\forall z < w_k) ((\bar{u})_z < \alpha)]$ and also (b) $M \models (\exists z < w_k) \forall y \bigwedge_{i=1}^r (p_i(\bar{w}, z, \bar{y}) \neq 0) \leftrightarrow \neg \exists \bar{u} \exists \bar{v} (q(\bar{w}, \bar{u}, \bar{v}) = 0)$. From (a), since $M \models \theta(\bar{b})$, $M \models \neg \exists \bar{u} [\exists \bar{v} q(\bar{b}, \bar{u}, \bar{v}) = 0 \wedge (\forall z < w_k) ((\bar{u})_z < \alpha)]$. So $M \models \neg (\exists \bar{u}, \bar{v} < \alpha) (q(\bar{b}, \bar{u}, \bar{v}) = 0)$. Hence, by (**) $M \models \neg \exists \bar{u}, \bar{v} (q(\bar{a}, \bar{u}, \bar{v}) = 0)$ and therefore, from (b), $M \models (\exists z < a_k) \forall y \bigwedge_{i=1}^r p_i(\bar{a}, z, \bar{y}) \neq 0$. Thus, $M \models \phi_2^j(n)$. As this is true for all $n \in N$, by induction in M there is an $m \in M \setminus N$ for which $M \models \phi_2^j(m)$. Let a_{2j+2} be the z for this m , and let $f(a_{2j+2}) = b_{2j+2}$.

Thus we have built up a map from M onto an initial segment of $[0, \alpha]$ with the required properties, and the theorem is proved.

The problem of how to generalize the theorem to uncountable models remains open. Clearly it is not true as it stands for *all* uncountable models, since if $N = \mathbf{N}$ (the standard natural numbers) and M is a diophantine-correct ω_1 -like model of Peano arithmetic, there will be no homomorphisms of M onto non- ω_1 -like initial segments. On the other hand, the proof could be formalized inside Peano arithmetic and so is true when M is “countable” from the view of an uncountable N .

NOTE

1. The referee pointed out that a related result due to Marker and Wilkie appears in [4]: that if M is a countable model of Peano arithmetic and $a \in M$, then there is an embedding of M onto an initial segment of $[0, a]$ iff for every Σ_1 -definable element m of M , $m \in a$.

REFERENCES

- [1] Gaifman, H., “A note on models and submodels of arithmetic,” Conference in Mathematical Logic, London, 1971, *Lecture Notes in Mathematics*, Springer-Verlag, vol. 255 (1972), pp. 128–144.
- [2] Lipshitz, L., “Diophantine correct models of arithmetic,” *Proceedings of the American Mathematical Society*, vol. 73, no. 1 (1979), pp. 107–108.
- [3] Matijasevič, Y., “Enumerable sets are diophantine,” *Doklady Akademii Nauk SSSR*, vol. 191 (1970), pp. 279–282 (translated as: *Soviet Mathematical Doklady*, vol. 11 (1970), pp. 354–357).

- [4] Mijajlovic, Z., "Submodels and definable points in models of Peano arithmetic," *Notre Dame Journal of Formal Logic*, vol. 24 (1983), pp. 417-425.
- [5] Pillay, A., "Models of Peano arithmetic (A survey of basic results)," pp. 263-269 in *Model Theory and Arithmetic*, ed. C. Berline, et al., *Lecture Notes in Mathematics*, Springer-Verlag, vol. 890 (1981).
- [6] Wilkie, A., "On models of arithmetic—answers to two problems raised by H. Gaifman," *The Journal of Symbolic Logic*, vol. 40, no. 1 (1975), pp. 41-47.

Mathematics Department
Wabash College
Crawfordsville, Indiana 47933