DIOPHANTINE CORRECT MODELS OF ARITHMETIC

L. LIPSHITZ¹

ABSTRACT. A countable nonstandard model of arithmetic is diophantine correct if and only if it can be embedded in arbitrarily short nonstandard initial segments of itself.

A model M of Peano arithmetic is called *diophantine correct* if the same diophantine equations have solutions in M and $\mathbb{N}$ (the natural numbers). The purpose of this note is to prove the following theorem, which was suggested to the author by S. Tennenbaum.

THEOREM. *Let M be a countable nonstandard model of Peano arithmetic. Then M is diophantine correct if and only if for every nonstandard $\lambda \in M$ there is an embedding of M into the initial segment $[0, \lambda] = \{x \in M \mid x \leq \lambda\}$.*

The reader will notice that the existence of such embeddings for arbitrary countable models of Peano arithmetic would have given a positive solution for Hilbert's tenth problem. The proofs of the Theorem and the Remark below are similar to the proof of Theorem 4.2 of [1].

PROOF OF THE THEOREM. If M is not diophantine correct then there is a polynomial $p(x_1, \dots, x_n)$ with integer coefficients such that $p(x_1, \dots, x_n)$ has a solution in M but has no solution in $\mathbb{N}$. Choose $\lambda \in M$ nonstandard so that $p(x_1, \dots, x_n) = 0$ has no solution with $x_1, \dots, x_n < \lambda$. Then there is no embedding of M into the initial segment $[0, \lambda]$. Conversely suppose that M is countable and diophantine correct. Let $M = \{a_1, a_2, \dots\}$, and let $\lambda \in M$ be nonstandard. Notice that for any polynomial $p(x_1, \dots, x_n)$ (with integer coefficients) either $p(x_1, \dots, x_n) = 0$ has only finitely many solutions, which are all standard, or for every nonstandard γ there is a nonstandard solution less than γ . We shall define partial embeddings $\rho_n: \{a_1, \dots, a_n\} \rightarrow [0, \lambda]$ by induction so that for all $n \in \omega$ (i) $\rho_n \subset \rho_{n+1}$ and (ii) for every polynomial $p(x_1, \dots, x_n, y_1, \dots, y_k)$ if $\exists y_1, \dots, y_k [p(a_1, \dots, a_n, y_1, \dots, y_k) = 0]$ then $\exists y_1, \dots, y_k < \lambda [p(\rho_n(a_1), \dots, \rho_n(a_n), y_1, \dots, y_k) = 0]$. We take $\rho_0 = \emptyset$. Suppose that ρ_n is defined and has properties (i) and (ii). Consider the following formula $\psi(m) = \exists z < \lambda$ [for all polynomials $p(x_1, \dots, x_n, u, y_1, \dots, y_k)$ of length $\leq m$ if $\exists y_1, \dots, y_k (p(a_1, \dots, a_n, a_{n+1}, y_1, \dots, y_k) = 0)$ then $\exists y'_1, \dots, y'_k < \lambda [p(b_1, \dots, b_n, z, y'_1, \dots, y'_k) = 0]$, where $b_i = \rho_n(a_i)$].

Received by the editors May 25, 1977.

AMS (MOS) subject classifications (1970). Primary 02H20, 10N15.

¹Supported in part by National Science Foundation Grant MCS76-06357.

0002-9939/79/0000-0022/\$01.50
© 1979 American Mathematical Society

Using the fact that a system of polynomial equations ($\bigwedge_i p_i(x) = 0$) is equivalent to one polynomial equation ($\sum_i (p_i(x))^2 = 0$) it follows from property (ii) for ρ_n that $M \models \psi(\underline{m})$ for each $m \in \omega$. Hence for some nonstandard γ , $M \models \psi(\gamma)$. Let b_{n+1} be a corresponding $z < \lambda$, and set $\rho_{n+1} = \rho_n \cup \{\langle a_{n+1}, b_{n+1} \rangle\}$. It is clear that $\rho = \bigcup_{n < \omega} \rho_n$ is the required embedding.

REMARK. In the above we could have arranged that ρ be an isomorphism of M onto an initial segment of M contained in $[0, \lambda]$. Let $[0, \lambda] = \{c_1, c_2, \dots\}$. Define ρ satisfying (i) and (ii) above by induction as follows. If ρ_{2n} is defined obtain ρ_{2n+1} from ρ_{2n} in the same way that ρ_{n+1} was obtained from ρ_n above. Suppose that ρ_{2n+1} is defined. Let b be the first of the c_i 's not in the range of ρ_{2n+1} but less than something in the range ($\rho_{2n+1}(a'_i) = b_i$ say). (If no such c_i exists let $\rho_{2n+2} = \rho_{2n+1}$.) Let $\psi'(m) = \exists z_{< a'_i}$ [for any polynomial p of length $\leq m$ if $\neg \exists y_1, \dots, y_{k < \lambda} (p(b_1, \dots, b_l, b, y_1, \dots, y_k) = 0)$ then $\neg \exists y_1, \dots, y_k (p(a'_1, \dots, a'_l, z, y_1, \dots, y_k) = 0)$], where $\rho_{2n+1} = \{\langle a'_j, b_j \rangle \mid j = 1, \dots, l\}$. Next we shall show that for each $m \in \omega$, $M \models \psi'(\underline{m})$. Let $p_1, \dots, p_r$ be the polynomials of length $\leq m$ such that $M \models \neg \exists \bar{y}_{< \lambda} p_j(\bar{b}, b, \bar{y}) = 0$ for $j = 1, \dots, r$ where $\bar{b} = (b_1, \dots, b_l)$, $\bar{y} = (y_1, \dots, y_k)$ and $\bar{a} = (a'_1, \dots, a'_l)$. Then $M \models \exists z_{< b_i} \forall \bar{y}_{< \lambda} \bigwedge_{j=1}^r [p_j(\bar{b}, z, \bar{y}) \neq 0]$. By the results of [2] and the fact that these results can be formalized in Peano arithmetic there is a polynomial $p(\bar{b}, \bar{u}, \bar{v})$ such that $M \models \exists z_{< w_i} \forall \bar{y}_{< \lambda} \bigwedge_{j=1}^r [p_j(w, z, y) \neq 0] \leftrightarrow \neg \{\exists \bar{u}, \bar{v} (p(\bar{w}, \bar{u}, \bar{v}) = 0) \wedge \forall z_{< w_i} ((\bar{u})_z < \lambda)\}$ and $M \models \exists z_{< w_i} \forall \bar{y}_{< \lambda} \bigwedge_{j=1}^r [p_j(\bar{w}, z, \bar{y}) \neq 0] \leftrightarrow \neg \exists \bar{u}, \bar{v} (p(\bar{w}, \bar{u}, \bar{v}) = 0)$ where $\bar{w} = (w_1, \dots, w_l)$. Hence $M \models \neg \{\exists \bar{u}, \bar{v} (p(\bar{b}, \bar{u}, \bar{v}) = 0) \wedge \forall z_{< b_i} ((\bar{u})_z < \lambda)\}$ and hence $M \models \neg \exists \bar{u}, \bar{v}_{< \lambda} (p(\bar{b}, \bar{u}, \bar{v}) = 0)$. By property (ii) this gives us $M \models \neg \exists \bar{u}, \bar{v} (p(\bar{a}, \bar{u}, \bar{v}) = 0)$ and thus $M \models \exists z_{< a'_i} \forall \bar{y}_{< \lambda} \bigwedge_{j=1}^r [p_j(\bar{a}, z, \bar{y}) \neq 0]$, i.e. $M \models \psi'(\underline{m})$. Hence $M \models \psi'(\gamma)$ for some nonstandard $\gamma \in M$. Let a' be a corresponding value of z and set $\rho_{2n+2} = \rho_{2n+1} \cup \{\langle a', b \rangle\}$. It is clear that ρ_{2n+2} has properties (i) and (ii) and that $\rho = \bigcup_{n < \omega} \rho_n$ is the required isomorphism.

REFERENCES

1. Harvey Friedman, *Countable models of set theories*, Lecture Notes in Math., vol. 337, Springer-Verlag, Berlin and New York, 1973, pp. 539–573.
2. Yuri Matijasevič, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 = Soviet Math. Dokl. **11** (1970), 354–357.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907