EXTENSIONS AND COROLLARIES OF RECENT WORK ON HILBERT'S TENTH PROBLEM[1]

BY
MARTIN DAVIS

This paper consists of three separate notes related only in that each of the three either extends or employs the results of [2], with which acquaintance is assumed.

1. A sharpening of Kleene's normal form theorem

By a form of Kleene's normal form theorem (cf. [1] or [3]) we may understand the following assertion:

THEOREM. *There is a function $U(y)$ and a predicate $T(z, x, y)$ both belonging to the class Q such that a function $f(x)$ is partially computable if and only if for some number e*

$$f(x) = U(\min_y T(e, x, y)).$$

In its original form, this result was stated with Q the class of primitive recursive functions and predicates. It is well known (cf. [3] and [6]) that smaller classes Q suffice. We wish to point out here that (assuming variables to range over the positive integers) we may take for Q the following extremely modest class:

(1) *A function f belongs to Q if and only if f can be obtained by repeated application of the operation of composition to the functions*: 2^x, $x \cdot y$, $N(x) = 0$, $U_i^n(x_1, \cdots, x_n) = x_i$, $K(x)$, $L(x)$, *where $K(x)$, $L(x)$ are recursive pairing functions.*

(2) *A predicate $R(x_1, \cdots, x_n)$ belongs to Q if*

$$R(x_1, \cdots, x_n) \leftrightarrow f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n)$$

where $f, g \in Q$.

In fact, we may even take $U(y) = K(y)$.

To see this we begin by noting that by Corollary 5 of [2], (or rather the immediate extension thereof to predicates), we have

$$\begin{aligned} \bigvee_y T_2(z, x, u, y) &\leftrightarrow \bigvee_{x_1,\cdots,x_n} P(z, x, u, x_1, \cdots, x_n, 2^{x_1}, \cdots, 2^{x_n}) = 0 \\ &\leftrightarrow \bigvee_{x_1,\cdots,x_n} \Big\{ \textstyle\sum_{j=1}^m f_j(z, x, u, x_1, \cdots, x_n, 2^{x_1}, \cdots, 2^{x_n}) \\ &\qquad = \textstyle\sum_{j=1}^m g_j(z, x, u, x_1, \cdots, x_n, 2^{x_1}, \cdots, 2^{x_n}) \Big\}, \end{aligned}$$

Received November 22, 1961.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command.

where $f_j, g_j \in Q$, $j = 1, 2, \cdots, m$. Now, using the fact that

$$\sum A_j = \sum B_j \leftrightarrow 2^{\Sigma A_j} = 2^{\Sigma B_j}$$
$$\leftrightarrow \prod 2^{A_j} = \prod 2^{B_j},$$

we see that

$$\bigvee_y T_2(z, x, u, y) \leftrightarrow \bigvee_{x_1, \cdots, x_n} R(z, x, u, y, x_1, \cdots, x_n),$$

where $R \in Q$. Now, let

$$q_1(t) = K^{n-1}(t),$$
$$q_j(t) = L(K^{n-j}(t)), \qquad j = 2, 3, \cdots, n,$$

where the exponent on K indicates iterated application, so that $q_j(t) \in Q$, $j = 1, 2, \cdots, n$. Thus

$$\bigvee_y T_2(z, x, u, y) \leftrightarrow \bigvee_t R(z, x, u, y, q_1(t), \cdots, q_n(t))$$
$$\leftrightarrow \bigvee_t S(z, x, u, y, t),$$

where $S \in Q$.

Let $f(x)$ be any partially computable function. Then the predicate $u = f(x)$ is semicomputable (recursively enumerable). Hence, for some e,

$$u = f(x) \leftrightarrow \bigvee_y T_2(e, x, u, y)$$
$$\leftrightarrow \bigvee_t S(e, x, u, t).$$

Finally,

$$f(x) = K(\min_y S(e, x, K(y), L(y))).$$

So, we have derived Kleene's normal form theorem with

$$T(z, x, y) \leftrightarrow S(z, x, K(y), L(y)) \quad \text{and} \quad U(y) = K(y).$$

2. Negative solution to a problem of Quine

In [4], Quine proposed the following problem:

Let us consider schemata constructed from the following ingredients: numerals, variables ranging over the nonnegative integers, the symbols of sum, product and power, =, and the truth-function signs.

Such a schema is called *valid* if it becomes a true sentence whenever all of the variables occurring in it are replaced by numerals. The proposed problem is to give an algorithm for determining whether or not a given schema of this kind is valid.

We note here that the *recursive unsolvability of this problem* follows directly from the results of [2]. For, to each exponential Diophantine equation, $E = F$, there corresponds, mechanically, a "translation": $\Gamma = \Delta$ which is a schema of the kind being considered. Moreover, $E = F$ has a solution if and only if the schema $\sim(\Gamma = \Delta)$ is not valid. Hence, an algorithm for solving Quine's problem could be used to solve the decision problem for exponential Diophantine equations. But, by [2], there is no algorithm for solving this latter problem. Hence, Quine's problem is likewise unsolvable.

3. Diophantine representation of recursively enumerable sets in terms of a single predicate of exponential growth

A predicate $\rho(u, v)$ will be called a *Julia Robinson predicate* if

(1) $\rho(u, v) \rightarrow v \leqq u^u$,

(2) for each $k > 0$, there are u, v such that

$$\rho(u, v) \wedge v > u^k.$$

We shall prove the following

THEOREM. *Let S be a recursively enumerable set. Then there is a polynomial P such that*

$$S = \{x \mid \bigvee_{x_1, \cdots, x_n, u, v} [P(x, x_1, \cdots, x_n, u, v) = 0 \wedge \rho(u, v)]\}$$

for every Julia Robinson predicate $\rho(u, v)$.

Since, e.g., the predicate $v = 2^u \wedge u > 1$ is a Julia Robinson predicate, we have

COROLLARY 1. *Let S be a recursively enumerable set. Then, for some polynomial P,*

$$S = \{x \mid \bigvee_{x_1, \cdots, x_n, u} P(x, x_1, \cdots, x_n, u, 2^u) = 0\}.$$

This generalizes Corollary 5 of [2]. Moreover, the proof of Corollary 6 of [2], if applied to the present Corollary 1 instead of to Corollary 5 of [2], yields

COROLLARY 2. *For every recursively enumerable set S there is a function $P(x_1, \cdots, x_n, u, 2^u)$, where P is a polynomial, whose range (for positive integer values of the variables) consists of the members of S together with the non-positive integers.*

If in particular we choose for S, the set of positive primes, we obtain a curious "prime-representing" function!

It remains to prove the theorem stated above. In doing so we generalize the methods, relating to Pell's equation, of [5].[2] We recall the notation $x = a_n$, $y = a'_n$ for the successive solutions of the Pell equation

$$x^2 - (a^2 - 1)y^2 = 1.$$

LEMMA 1. *There is a Diophantine predicate $\psi(a, u)$ such that*

(1) $\psi(a, u) \rightarrow u \geqq a^a$,

(2) $a > 1 \rightarrow \bigvee_u \psi(a, u)$.

Proof. This is a weakening of Lemma 8 of [5].

[2] However, we are following [2] rather than [5] in taking variables to have the positive integers (rather than the nonnegative integers) as their range.

LEMMA 2. *There is a Diophantine predicate $D(c, y, z)$ such that*
(1) $a > c \wedge D(c, y, z) \rightarrow a > y^z$,
(2) $\bigwedge_{y,z} \bigvee_c D(c, y, z)$.

Proof. Let

$$D(c, y, z) \leftrightarrow \bigvee_b [b > y \wedge b > z \wedge \psi(b, c)].$$

Then

$$a > c \wedge D(c, y, z) \rightarrow \bigvee_b [a > c \geqq b^b > y^z].$$

LEMMA 3. *If $y > 1$ and $a > y^z$, then $y^z = [u/a_z]$ where*[3] *u is chosen as a solution of*

$$u^2 - (a^2y^2 - 1)v^2 = 1 \quad \textit{for which} \quad a_z \leqq u \leqq a \cdot a_z .$$

Proof. By Lemma 9 of [5], $y^z = [(ay)_z/a_z]$, and by Lemma 10 of [5], the number u is precisely $(ay)_z$.

LEMMA 4.

$$\bigwedge_{i \leqq m} (x_i = y_i^{z_i})$$
$$\leftrightarrow \bigvee_{r_1, \cdots, r_m} [\bigwedge_{i \leqq m} E(r_i , x_i , y_i , z_i , a) \wedge \bigwedge_{i \leqq m} (r_i = a_{z_i})],$$

where E is a Diophantine predicate, and where $a > c_1 , c_2 , \cdots , c_m , z_1 , \cdots , z_m$ with the $c_1 , \cdots , c_m$ satisfying $D(c_i , y_i , z_i)$.

Proof. We need only take

$$E(r_i , x_i , y_i , z_i , a) \leftrightarrow \bigvee_{u,v} [(u^2 - (a^2y_i^2 - 1)v^2 = 1) \wedge r_i \leqq u \leqq a \cdot r_i$$
$$\wedge r_ix_i \leqq u < r_i(x_i + 1)] \vee [x_i = y_i = 1].$$

LEMMA 5. *If $1 < r < a_a$ and $a > z$, then*

$$r = a_z \leftrightarrow \bigvee_s [r^2 - (a^2 - 1)(z + s(a - 1))^2 = 1].$$

Proof. This follows from Lemma 7 of [5].

LEMMA 6.

$$\bigwedge_{i \leqq m} (x_i = y_i^{z_i})$$
$$\leftrightarrow \bigvee_{a,d} [F(x_1 , \cdots , x_m , y_1 , \cdots , y_m , z_1 , \cdots , z_m , a, d) \wedge \rho(a, d)],$$

where F is a Diophantine predicate and ρ may be any Julia Robinson predicate.

Proof. We claim that, if we use the notation of Lemma 4,

$$\bigwedge_{i \leqq m} (x_i = u_i^{z_i}) \leftrightarrow \bigvee_{r_1, \cdots, r_m} \bigvee_a \{ \bigwedge_{i \leqq m} [E(r_i , x_i , y_i , z_i , a)$$
$$\wedge (a > z_i) \wedge \bigvee_{s_i} [r_i^2 - (a^2 - 1)(z_i + s_i(a - 1))^2 = 1]]$$
$$\wedge \bigvee_{c_1, \cdots, c_m} [\bigwedge_{i \leqq m} (D(c_i , y_i , z_i) \wedge a > c_i)]$$
$$\wedge \bigwedge_d [r_1 , \cdots , r_m \leqq d \wedge \rho(a, d)] \}.$$

[3] $[\cdots]$ here means, as usual, "the greatest integer $\leqq \cdots$".

For, if the right-hand side holds, then $r_1, \cdots, r_m \leqq d \leqq a < a_a$, so that by Lemma 5, $r_i = a_{z_i}$, and finally, by Lemma 6, $x_i = y_i^{z_i}$. Conversely, if the left-hand side holds, choose c_i so that $D(c_i, y_i, z_i)$ is satisfied, then let $z = \max_{i \leqq m} z_i$, and choose a, d so that $a > c_i$, $a > z$, $\rho(a, d)$, and $d > a_z$. Then

$$r_i = a_{z_i} \leqq a_z < d,$$

and the result follows by Lemmas 4 and 5.

LEMMA 7. *Let S be a recursively enumerable set. Then there is a polynomial P such that*

$$S = \{x \mid \bigvee_{x_1, \cdots, x_m} \bigvee_{y_1, \cdots, y_m} \bigvee_{z_1, \cdots, z_m} [P(x, x_1, \cdots, x_n, y_1, \cdots, y_m, z_1, \cdots, z_m) = 0] \wedge \bigwedge_{i \leqq m} (x_i = y_i^{z_i})\}.$$

Proof. This lemma is essentially a restatement of the main result of [2], namely that every recursively enumerable set is *exponential* Diophantine.

The theorem now follows at once from Lemmas 6 and 7.

REFERENCES

1. MARTIN DAVIS, *Computability and unsolvability*, New York, McGraw-Hill, 1958.
2. MARTIN DAVIS, HILARY PUTNAM, AND JULIA ROBINSON, *The decision problem for exponential Diophantine equations*, Ann. of Math. (2), vol. 74 (1961), pp. 425–436.
3. S. C. KLEENE, *Introduction to metamathematics*, New York, Van Nostrand, 1952.
4. W. V. QUINE, *On decidability and completeness*, Synthèse, vol. 7 (1949), pp. 441–446.
5. JULIA ROBINSON, *Existential definability in arithmetic*, Trans. Amer. Math. Soc., vol. 72 (1952), pp. 437–449.
6. RAYMOND M. SMULLYAN, *Theory of formal systems*, Annals of Mathematics Studies, no. 47, Princeton University Press, 1961.

YESHIVA UNIVERSITY
NEW YORK, NEW YORK