ON THE CHARACTERIZATION OF RECURSIVELY ENUMERABLE SETS AS PSEUDO-DIOPHANTINE

KOSTAS SKANDALIS

(Communicated by Andreas Blass)

ABSTRACT. In 1989 L. Blum, M. Shub, and S. Smale stated a problem whether the recursively enumerable sets can be characterized as pseudo-diophantine definable (Bull. Amer. Math. Soc. (N.S.) **21** (1989), 1–46, Problem 9.2). An example shows that such a characterization is impossible. Nevertheless, a somewhat different characterization holds for the recursively enumerable sets over reals.

INTRODUCTION

We assume the reader is familiar with the notion of function which is computable by some machine or programme (cf. [1, 2]). The domains of such functions are called recursively enumerable sets. Problem 9.2 of [1] asks the question whether every recursively enumerable set over an ordered ring R has a pseudo-diophantine definition, i.e., can be defined in the form:

$$(1) \qquad X_{\Omega, \bar{c}} = \{\overline{x} \in R^n : (\exists q \in \Omega) q(\overline{x}, \overline{c}) \leq 0\}$$

where $\bar{c} \in R^m$ and $\Omega \subseteq \mathbf{Z}[\overline{x}, \overline{y}]$ is a pseudo-diophantine set of polynomials with integer coefficients.

In §1 we give an example of a recursively enumerable set over the ordered field **R** of reals which cannot be defined in the form (1).

The example shows that a conjunction of two inequalities cannot be expressed by a countable disjunction of inequalities. But, over the reals (and any archimedean ordered field) the effective disjunctions of pairs of inequalities are sufficient to characterize the recursively enumerable sets. We prove this in §2.

1. THE EXAMPLE

Proposition 1. Let $B = \{\langle x, y \rangle \in \mathbf{R}^2 : x \geq 0 \land y \geq 0\}$. Then B is a recursively enumerable set but has no pseudo-diophantine definition.

Proof. B is clearly a recursively enumerable set. It is the domain of the function computed by the following programme:

$$\textbf{while } (x < 0) \textbf{ do } x := x \, ; \textbf{ while } (y < 0) \textbf{ do } y := y \, .$$

The pseudo-diophantine definable sets are countable unions of sets of the form:

$$A(q) = \{\langle x, y \rangle \in \mathbf{R}^2 : q(x, y) \leq 0\},$$

where $q \in \mathbf{R}[x, y]$.

Suppose that for some polynomials $f_n \in \mathbf{R}[x, y] (n \in \mathbf{N})$ we have $B = \bigcup_n A(f_n)$. It follows that

$$(2) \qquad \{x \in \mathbf{R} : x \geq 0\} = \bigcup_n \{x \in \mathbf{R} : f_n(x, 0) = 0\}.$$

Indeed, if $x \geq 0$, then $f_n(x, 0) \leq 0$ for some $n \in \mathbf{N}$. But $f_n(x, h) > 0$ for $h < 0$, since $\langle x, h \rangle \notin B$. By the continuity of f_n, it follows that $f_n(x, 0) \geq 0$. Hence $f_n(x, 0) = 0$.

But the equality (2) is impossible for any polynomials $f_n(x, 0)$. It follows that B has no pseudo-diophantine definition. □

2. The characterization

Let $\langle P_n^l : n \in \mathbf{N} \rangle$ be an effective enumeration of $\mathbf{Z}[x_1, \ldots, x_l]$. Let α, β be recursive functions. Let $c_1, \ldots, c_j \in \mathbf{R}$. Consider the set, which we call $\mathscr{D}_2$ type,

$$(3) \quad X(\alpha, \beta; \overline{c}) = \{\overline{x} \in \mathbf{R}^m : (\exists n \in \mathbf{N})(p_{\alpha(n)}^{m+j}(\overline{x}, \overline{c}) \leq 0 \wedge P_{\beta(n)}^{m+j}(\overline{x}, \overline{c}) \leq 0)\}.$$

We shall prove that the recursively enumerable sets over reals can be characterized as $\mathscr{D}_2$ sets.

Note 1. The class $\mathscr{D}_2$ generalizes the class of pseudo-diophantine definable sets. Indeed, if $\Omega \subseteq \mathbf{Z}[x_1, \ldots, x_l]$ is pseudo-diophantine (cf. [1, §9]) then for some recursive function γ we have $\Omega = \{P_{\gamma(n)}^l : n \in \mathbf{N}\}$. Conversely, for any recursive function γ the set $\Omega = \{P_{\gamma(n)}^l : n \in \mathbf{N}\}$ (as a set of integers coding the coefficients of polynomials) is recursively enumerable. Hence, by the Davis-Matijasevic-Robinson characterization, Ω can be defined as $\{q \in \mathbf{Z}[x_1, \ldots, x_l] : (\exists \overline{k} \in \mathbf{Z}^i)(h(\overline{k}, q) = 0)\}$, for some polynomial h with integer coefficients. So Ω is pseudo-diophantine in the sense of [1].

It follows that the sets definable in the form (1) can be defined as

$$(4) \qquad X(\gamma; \overline{c}) = \{\overline{x} \in R^m : (\exists n \in \mathbf{N})(P_{\gamma(n)}^{m+j}(\overline{x}, \overline{c}) \leq 0)\}$$

for some recursive function γ and $\overline{c} \in R^j$. It is clear that (3) is a generalization of (4).

Note 2. The $\mathscr{D}_2$ sets are recursively enumerable over any field K containing $\mathbf{N}$. Indeed, over such a field the recursive functions are computable by some machines. There are also universal machines UT^l such that for any $n \in \mathbf{N}$ and $\overline{a} \in K^l$, the machine UT^l on input $\langle n, \overline{a} \rangle$ computes the value of $P_n^l(\overline{a})$ over K (cf. [1, 2]). It follows that the sets of the form (3) are domains of some machines over K.

Note 3. The domains of computable functions can be defined by effective countable disjunctions of open formulae (cf. [2]). If $I \subseteq K^m$ is the domain of some

computable function by a machine over a field K, then there exists a recursive function δ such that

$$\overline{x} \in I \quad \text{iff} \quad K \vDash \bigvee_n \Phi_{\delta(n)}^{m+j}(\overline{x}, \overline{c})$$

where $\langle \Phi_n^l : n \in \mathbf{N} \rangle$ is an effective enumeration of the open formulae of variables $x_1, \ldots, x_l$ of the language of ordered fields and $\overline{c} \in K^j$.

It follows that, in order to prove that the recursively enumerable sets of reals are $\mathscr{D}_2$ sets, it is sufficient to show that any effective countable disjunction of open formulae is equivalent over $\mathbf{R}$ to an effective disjunction of pairs of inequalities.

Let $\langle \Theta_n^l : n \in \mathbf{N} \rangle$ be an effective enumeration of formulae of the form

(5) $$q_1(\overline{x}) \leq 0 \wedge q_2(\overline{x}) \leq 0,$$

where $q_i \in \mathbf{Z}[x_1, \ldots, x_l]$.

We obtain the required characterization by showing that for any recursive function λ there exists a recursive function μ such that the formulae $\bigvee_n \Phi_{\lambda(n)}^l(\overline{x})$ and $\bigvee_n \Theta_{\mu(n)}^l(\overline{x})$ are equivalent over the reals. This follows from the proposition below.

Proposition 2. *Let $l \in \mathbf{N}$. There exists a recursive function ζ such that for all $i \in \mathbf{N}$*

$$\mathbf{R} \vDash \Phi_i^l(\overline{x}) \Leftrightarrow \bigvee_n \Theta_{\zeta(n)}^l(\overline{x}).$$

Proof. Any open formula ϕ is effectively equivalent to a finite disjunction of formulae of the form:

$$q_0(\overline{x}) = 0 \wedge \bigwedge_{i=1}^s q_i(\overline{x}) > 0,$$

where q_i's are polynomials with integer coefficients.

Since $q > 0$ is equivalent to $\bigvee_n (1 - nq \leq 0)$, we can express ϕ as an effective countable disjunction of formulae of the form:

(6) $$\bigwedge_{i=1}^t q_i(\overline{x}) \leq 0.$$

We show that any formula of type (6) is effectively equivalent to a countable disjunction of pairs of inequalities (i.e., type (5) formulae).

Let $\{\langle s_n, t_n \rangle : n \in \mathbf{N}\}$ be an effective enumeration of pairs of positive rationals. Set $r_n = \min(s_n, t_n)$. Note that $x \geq 0 \wedge y \geq 0 \wedge z \geq 0$ is equivalent to

$$(-x \leq 0 \wedge y^2 + z^2 \leq 0) \vee (-y \leq 0 \wedge z^2 + x^2 \leq 0) \vee (-z \leq 0 \wedge y^2 + x^2 \leq 0)$$

$$\vee \bigvee_n ((x - s_n)^2 + (y - t_n)^2 - r_n^2 \leq 0) \wedge (-z \leq 0)$$

$$\vee \bigvee_n ((y - s_n)^2 + (z - t_n)^2 - r_n^2 \leq 0) \wedge (-x \leq 0)$$

$$\vee \bigvee_n ((z - s_n)^2 + (x - t_n)^2 - r_n^2 \leq 0) \wedge (-y \leq 0).$$

This shows how 3-term inequalities can be effectively expressed as disjunctions of type (5) formulae.

By repetition of this procedure we can express any type (6) formula and, consequently, any open formula, in the required form. □

Corollary. *Any* $I \subseteq \mathbf{R}^m$ $(m \in \mathbf{N})$ *is recursively enumerable if and only if* $I \in \mathscr{D}_2$ *(i.e., can be defined in the form* (3)).

Final remark. The proved characterization holds also for *archimedean ordered fields*. In the proof of Proposition 2 we used the density of the rationals in the field and the property: $x > 0$ iff $(\exists n \in \mathbf{N})(x \geq \frac{1}{n})$. These properties are valid in any archimedean ordered field.

REFERENCES

1. L. Blum, M. Shub, and S. Smale, *On the theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines*, Bull. Amer. Math. Soc. (N.S.) **21** (1989), 1–46.

2. K. Skandalis, *Programmable real numbers and functions*, Fund. Inform. **7** (1984), 27–56.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CRETE, GREECE
E-mail address: kostek@grearn.bitnet