Записки научных
семинаров ПОМИ
Том 377, 2010 г.

M. Davis

REPRESENTATION THEOREMS FOR R.E. SETS AND A CONJECTURE RELATED TO POONEN'S LARGES SUBRING OF $\mathbb{Q}$

Abstract. It is remarked that unsolvability results can often be extended to yield novel "representation" theorems for the set of all recursively enumerable sets. In particular it is shown that analysis of the proof of the unsolvability of Hilbert's 10th Problem over Poonen's large subring of $\mathbb{Q}$ can provide such a theorem. Moreover, applying that theorem to the case of a simple set leads to a conjecture whose truth would imply the unsolvability of Hilbert's 10th Problem over $\mathbb{Q}$.

The word problem

A group G is *finitely generated* if there is a finite sequence of its elements $x_1, x_2, \ldots, x_n$ such that every element of G can be written $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ for some $m_1, m_2, \ldots, m_n \in Z$. It is also *recursively presented* if the set

$$\{\langle m_1, m_2, \ldots, m_n\rangle \mid x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} = e\}$$

is r.e. Finally it is *finitely presented* if the group is determined by a finite number of equations of the form $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n} = e$. The *word problem* for a finitely presented group is to find an algorithm to determine whether a given product $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ is equal to the identity.

Novikov–Boone theorem [4, 1]**.** *There is a finitely presented group with an unsolvable word problem.*

Higman representation theorem [2, 7]**.** *A finitely generated group is recursively presented if and only if it is a subgroup of a finitely presented group.*

Whereas the Novikov–Boone theorem provides an example of an unsolvable word problem, the Higman theorem does much more: it provides

Key words and phrases. Simple set, Poonen, Hilbert's tenth problem for the rational numbers.

a characterization of recursive enumerability in terms of group theory. Such representation theorems are often available in connection with unsolvability theorems.

Hilbert's tenth problem

The solution of Hilbert's 10th Problem was by means of a representation theorem for recursively enumerable sets.

Matiyasevich/MRDP/DPRM theorem. *A set of natural numbers is recursively enumerable (r.e.) if and only if it has a Diophantine definition* [3].

Such theorems provide an equivalent of r.e. set in a particular subject domain. They open the possibility of a two-way interchange between the subject domain and computability theory. Work on unsolvability of Hilbert's 10th Problem (H10) over domains other than the integers has typically not sought general representation theorems, though often, they are readily available.

We write $\mathbb{N}$ for the set of natural numbers, and $\mathbb{Q}$ for the set of rationals. As usual let $\pi(x)$ stand for the number of prime numbers $\leqslant x$. If A is a set of primes, let $\pi_A(x)$ be the number of elements of A that are $\leqslant x$.

Making use of elliptic curves, Bjorn Poonen has proved:

Theorem (Poonen [5])**.** *There is a computable set A of prime numbers such that*

$$\lim_{x\to\infty} \frac{\pi_A(x)}{\pi(x)} = 1$$

and Hilbert's 10th problem is unsolvable over the ring $\mathcal{U}$ of all rational numbers whose denominators are products of primes in A.

Definition. *Let $\mathcal{R}$ be a subring of $\mathbb{Q}$. A set $W \subseteq \mathcal{R}^m$ is Diophantine over $\mathcal{R}$ if there is a polynomial p with coefficients in $\mathcal{R}$ such that*

$$W = \{a \in \mathcal{R}^m \mid (\exists x \in \mathcal{R}^k)[p(a,x) = 0]\}.$$

Poonen's Lemma. *There is a computable map $n \to y_n$ of $\mathbb{N}$ into $\mathcal{U}$ such that the sets of triples $\{\langle y_a, y_b, y_{a+b}\rangle \mid a,b \in \mathbb{N}\}$ and $\{\langle y_a, y_b, y_{ab}\rangle \mid a,b \in \mathbb{N}\}$ are both Diophantine over $\mathcal{U}$.*

Poonen's Theorem is an immediate consequence of this lemma.

Let

$$S = \{a \in \mathbb{N} \mid (\exists x \in \mathbb{N}^k)[q(a,x) = 0]\},$$

where q is a polynomial with integer coefficients, be a Diophantine definition of some recursively enumerable (r.e.) set. Using Poonen's lemma we see that there exists a polynomial p with coefficients in $\mathcal{U}$ such that

$$S = \{a \in \mathbb{N} \mid (\exists x \in \mathcal{U}^\ell)[p(y_a, x) = 0]\}.$$

Writing

$$\widehat{S}_p = \{a \in \mathbb{N}) \mid (\exists x \in \mathbb{Q}^\ell)[p(y_a, x) = 0]\},$$

we have $S \subseteq \widehat{S}_p \subseteq \mathbb{N}$.

An r.e set $S \subseteq \mathbb{N}$ is *simple* if $\mathbb{N} - S$ is infinite but contains no infinite r.e. subset. Simple sets are obviously not computable. Applying the above to a simple set S we have: *either $\widehat{S}_p$ is itself simple or $\mathbb{N} - S_p$ is finite.*

Conjecture. *There is a Diophantine definition of a simple set S for which $\mathbb{N} - \widehat{S}_p$ is infinite, so that $\widehat{S}_p$ is also simple.*

This conjecture implies the unsolvability of H10 over $\mathbb{Q}$. The conjecture seems plausible because although it is easy to construct simple sets, and there are a number of ways to do so, and if the conjecture is false, then no matter how S is constructed, and no matter what Diophantine definition of S is provided, $\widehat{S}_p$ will differ from $\mathbb{N}$ by only finitely many elements. Because the additional primes permitted in denominators in the transition from $\mathcal{U}$ to $\mathbb{Q}$ form a sparse set, this seems implausible.

Post's construction of a simple set ([6])

Let $\omega_0, \omega_1, \omega_2, \ldots$ be a standard enumeration of the r.e. sets. For example, we may take

$$\omega_i = \{n \mid (\exists x_1, \ldots, x_k)[p(n, i, x_1, \ldots, x_k) = 0]\},$$

where $p(a, i, x_1, \ldots, x_n) = 0$ is a universal equation.

We set up an enumeration of the pairs

$$\{\langle n, i\rangle \mid n \in \omega_i\},$$

and we place certain of the numbers n in a set S we are constructing. Specifically, if $n \in \omega_i$ and $n > 2i$ and *no member of ω_i has already been placed in S, then we place n in S*. This set S is clearly r.e. We show that it is simple.

Lemma 1. *If ω_i is infinite, then $S \cap \omega_i \neq \varnothing$.*

Proof. Being infinite, ω_i has elements $> 2i$. □

Lemma 2. *$\mathbb{N} - S$ is infinite.*

Proof. We let θ_i be *the* element of ω_i placed in S if there is such; otherwise let θ_i be undefined. We ask: *for given n how many numbers θ_i are there with $\theta_i \leqslant 2n+2$?* Observing that for $i \geqslant n+1$ for which θ_i is defined, we have

$$\theta_i > 2i \geqslant 2n+2.$$

So we can restrict ourselves to $i \leqslant n$. Therefore there cannot be more than the $n+1$ numbers $\{\theta_i \mid i = 0, 1, \ldots, n\}$. Hence $\mathbb{N} - S$ contains at least $n+1$ numbers $> 2n+2$. □

Using the two lemmas, we see that S is simple.

It is clear that there is great flexibility in this construction. Any effort to prove the conjecture would have to begin with the details of Poonen's construction. The construction of the required simple set S would then need to satisfy requirements guaranteeing that the addition of new primes to the denominators of ring elements does not add too many elements to S.

References

1. W. Boone, *The Word Problem.* — Ann. Math. **70** (1959), 207–265.
2. G. Higman, *Subgroups of finitely presented groups.* — Proc. Royal Soc. London, Series A **262** (1961), 455–475.
3. Ю. В. Матиясевич, *Десятая проблема Гильберта.* Наука, Физматлит, Москва, 1993. *English translation: Hilbert's Tenth Problem.* MIT Press, Cambridge, Massachusetts 1993. *French translation: Le dixième problème de Hilbert.* Masson, 1995.
4. С. П. Новиков, *Об алгоритмической неразрешимости проблемы тождества слов в теории групп.* — Труды МИАН **44** (1955), 1–143. *English translation: On the algorithmic insolvability of the word problem in group theory.* — American Mathematical Society Translations, Ser. 2, **91**, 1–122 (1958).
5. B. Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$.* — J. Amer. Math. Soc. **16** (2003), No. 4, 981–990.
6. E. L. Post, *Recursively enumerable sets of positive integers and their decision problems.* — Bull. Amer. Math. Soc. **50** (1944), 284–316. *Reprinted:* Martin Davis, ed. "The Undecidable," Raven Press 1965 and Dover 2004, 305-337. *Reprinted:* Martin Davis, ed. "Solvability, Provability, Definability: The Collected Works of Emil L. Post," Birkhäuser 1994, 461–493.

7. J. Rotman, *An Introduction to the Theory of Groups*. Springer-Verlag, Berlin–New York (1994).

Courant Inst., NYU;
Visting Scholar, Univ. Calif. Berkeley

E-mail: martin@eipye.com

Поступило 10 мая 2010 г.