PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 2, February 1996

DEGREES OF UNSOLVABILITY OF FIRST ORDER DECISION PROBLEMS FOR FINITELY PRESENTED GROUPS

OLEG V. BELEGRADEK

(Communicated by Andreas R. Blass)

ABSTRACT. We show that for any arithmetical m-degree $\mathbf{d}$ there is a first order decision problem $\mathbf{P}$ such that $\mathbf{P}$ has m-degree $\mathbf{d}$ for the free 2-step nilpotent group of rank 2. This implies a conjecture of Sacerdote.

Let $\varphi(\mathbf{v})$ be a formula of the first order language of group theory L and π a finite group presentation in an alphabet X. The first order decision problem $(?\mathbf{v})\varphi(\mathbf{v})$ for G_π, the group defined by π, is the problem of deciding for arbitrary tuple of words $\mathbf{u}$ in X whether or not the sentence $\varphi(\mathbf{u})$ holds in G_π. For example, $(?v)v = 1$ is the word problem and $(?xy)(\exists z)x^z = y$ is the conjugacy problem. It is easy to see that for a finitely presented group G the type of recursive isomorphism of the problem $(?\mathbf{v})\varphi(\mathbf{v})$ is independent of which finite presentation of G one chooses.

Sacerdote [**S1**] posed the following problem: which Turing degrees of unsolvability are the degrees of first order decision problems for finitely presented groups? For any atomic formula $\varphi(\mathbf{v})$ the problem $(?\mathbf{v})\varphi(\mathbf{v})$ is recursively enumerable; therefore any first order decision problem for any finitely presented group is arithmetical. Boone suggested that all first order decision problems for finitely presented groups have recursively enumerable Turing degrees. Sacerdote [**S2**] showed that it is not so. He constructed an *ad hoc* rather complicated example of a finitely presented group G and a formula $\varphi(\mathbf{v})$ with four free variables such that the problem $(?\mathbf{v})\varphi(\mathbf{v})$ has degree $\mathbf{0}''$ for G. He suggested the following

Conjecture. *Let $\mathbf{D}$ be an arithmetical degree of unsolvability. Then there exist a first order decision problem $\mathbf{P}$ and a finitely presented group G such that $\mathbf{P}$ has degree $\mathbf{D}$ for G.*

The aim of the present note is to prove this conjecture in a stronger form.

Theorem. *Let F be the free 2-step nilpotent group of rank 2. Then for any arithmetical m-degree $\mathbf{d}$ there is an L-formula $\varphi_{\mathbf{d}}(v)$ with one free variable such that the problem $(?v)\varphi_{\mathbf{d}}(v)$ has m-degree $\mathbf{d}$ for F.*

Note that F is finitely presented: if a_1 and a_2 freely generate F, then the relations $[a_1, a_2, a_1] = 1$ and $[a_1, a_2, a_2] = 1$ define F.

Received by the editors August 19, 1994.
1991 *Mathematics Subject Classification.* Primary 03D40, 03D30, 20F10, 20F18.
Key words and phrases. First order decision problem, m-degree.
The author was partially supported by the AMS fSU Aid Fund.

For a proof of the theorem we need some known facts.

(A) Every group word in a_1, a_2 can be effectively reduced in F to the form $a_2^k a_1^l c^m$, where $c = [a_1, a_2]$; the presentation of any element in this form is unique.

(B) A pair of elements (h_1, h_2) is said to be a *base* in a group H if

(1) H is 2-step nilpotent,

(2) $C_H(h_1)$ and $C_H(h_2)$ are abelian,

(3) $C_H(h_1, h_2) = Z(H)$,

(4) $[C_H(h_1), h_2] = [h_1, C_H(h_2)] = Z(H)$.

Note that there is an L-formula $\beta(x_1, x_2)$ such that, for any group H and its elements h_1 and h_2, the pair (h_1, h_2) is a base in H iff $\beta(h_1, h_2)$ holds in H.

The following construction is due to Mal′tsev [**M**]. Let (h_1, h_2) be a base in H. Define binary operations $+$ and $\times$ on $Z(H)$ as follows. For z_1, z_2 in $Z(H)$, $z_1 + z_2$ is just $z_1 z_2$, and $z_1 \times z_2$ is defined to be $[g_1, g_2]$, where $g_i \in C_H(h_i)$ for $i = 1, 2$, $[g_1, h_2] = z_1$, $[h_1, g_2] = z_2$. It turns out that $\times$ is well defined and $(Z(H), +, \times)$ is a ring with identity; denote the ring by $\mathrm{Ring}(H, h_1, h_2)$. Clearly, the ring is definable in H with parameters h_1, h_2. Therefore for any formula $\psi(\mathbf{v})$ of $\mathcal{L}$, the first order language of ring theory, one can effectively construct an L-formula $\psi^*(\mathbf{v}, x_1, x_2)$ such that, for any group H with a base (h_1, h_2) and any tuple $\mathbf{z}$ in $Z(H)$, the formula $\psi(\mathbf{z})$ holds in $\mathrm{Ring}(H, h_1, h_2)$ iff the formula $\psi^*(\mathbf{z}, h_1, h_2)$ holds in H.

Mal′tsev showed that (a_1, a_2) is a base in F; the ring $\mathrm{Ring}(F, a_1, a_2)$ consists of elements of the form c^n and is isomorphic to $\mathbf{Z}$ via $c^n \leftrightarrow n$.

(C) In F any two bases are conjugate by an automorphism [**B**, Theorem 5.11], even though in general it is not the case. So b_1, b_2 freely generate F iff $\beta(b_1, b_2)$ holds in F.

Proof. If $\mathbf{d}$ is the m-degree of the set of all natural numbers N we can take $v = v$ as $\varphi_{\mathbf{d}}(v)$. Suppose $\mathbf{d}$ is the m-degree of a proper arithmetical subset of N. Choose $A \subsetneq \mathbf{Z}$ of m-degree $\mathbf{d}$ such that $n \in A$ iff $-n \in A$, for any integer n. Due to the arithmeticity of A, there is an $\mathcal{L}$-formula $\psi(v)$ defining A in the ring $\mathbf{Z}$. We show that the L-formula $(\exists x_1 x_2)(\beta(x_1, x_2) \wedge \psi^*(v, x_1, x_2))$ can be taken as $\varphi_{\mathbf{d}}(v)$.

First we note that $n \in A$ iff $\varphi_{\mathbf{d}}(c^n)$ holds in F. Suppose $n \in A$. Then $\psi(n)$ holds in $\mathbf{Z}$. Therefore $\psi(c^n)$ holds in $\mathrm{Ring}(F, a_1, a_2)$, that is, $\psi^*(c^n, a_1, a_2)$ holds in F. So we can take a_1, a_2 as x_1, x_2. Now suppose that $\varphi_{\mathbf{d}}(c^n)$ holds in F. Then there are b_1, b_2 in F such that $\beta(b_1, b_2)$ and $\psi^*(c^n, b_1, b_2)$ hold in F. Because of (C), there is an automorphism τ of F sending b_i to a_i, for $i = 1, 2$. Then $\tau(c)^n$ satisfies $\psi^*(v, a_1, a_2)$ in F. The center of F is the infinite cyclic group generated by c. As $\tau(c)$ also generates the center, $\tau(c)$ is c or c^{-1}. Therefore $\psi(c^n)$ or $\psi(c^{-n})$ holds in $\mathrm{Ring}(F, a_1, a_2)$. So $\psi(n)$ or $\psi(-n)$ holds in $\mathbf{Z}$, that is, $n \in A$ or $-n \in A$. Then $n \in A$, by the choice of A.

Now it is clear that A is 1-reducible to the problem $(?v)\varphi_{\mathbf{d}}(v)$ for F. Fix an integer m_0 outside A. For a word w in a_1, a_2 put

$$g(w) = \begin{cases} m_0 & \text{if} \quad w = a_2^k a_1^l c^m \text{ in } F \text{ and } k \neq 0 \text{ or } l \neq 0, \\ m & \text{if} \quad w = c^m \text{ in } F. \end{cases}$$

Clearly, g is a recursive function, and $\varphi_{\mathbf{d}}(w)$ holds in F iff $g(w) \in A$. So the problem $(?v)\varphi_{\mathbf{d}}(v)$ for F is m-reducible to the set A. $\square$

References

[B] O. V. Belegradek, *The Mal′cev correspondence revisited*, Proc. Int. Conf. on Algebra Dedicated to the Memory of A. I. Mal′cev (L. A. Bokut′, Yu. L. Ershov, and A. I. Kostrikin, eds.), Contemp. Math., vol. 131, Amer. Math. Soc., Providence, RI, 1992, pp. 37–59. MR **93m:**03059

[M] A. I. Mal′tsev, *A correspondence between rings and groups*, Mat. Sb. (N.S.) **50** (1960), 257–266; English transl., *The metamathematics of algebraic systems. Collected papers: 1936–1967,* North-Holland, 1971, pp. 124–137.

[S1] G. S. Sacerdote, *Some unsolvable decision problems in group theory*, Proc. Amer. Math. Soc. **36** (1972), 231–238. MR **47:**8660

[S2] ______, *On a problem of Boone*, Math. Scand. **31** (1972), 111–117. MR **47:**6871

Kemerovo State University, Kemerovo 650043, Russia

E-mail address: `beleg@kaskad.kemerovo.su`