SOME UNDECIDABLE PROBLEMS IN GROUP THEORY

GEORGE S. SACERDOTE[1]

ABSTRACT. In this paper we obtain general results for un-decidable first order decision problems about groups (that is, problems about elements in a particular group, such as the word and conjugacy problems). We shall describe a class Ω of such decision problems and a construction Δ such that if P is a problem in Ω, then $\Delta(P)$ will be a finitely presented group in which P is recursively undecidable. This work then yields an analog of the Adjan-Rabin theorem for quotient-closed properties.

In the past 20 years there has been a rash of undecidability results for finitely presented groups. Some of these are the conjugacy problem [12], the word problem ([4,] [13]), the isomorphism problem ([1], [14]), the center problem [2], and many others (see [2] for a collection of other examples). With the single exception of the Adjan-Rabin theorem, which shows the undecidability of the isomorphism problem, each of these results is obtained by providing a construction for the particular problem in question, and then concluding the desired unsolvability from peculiarities of the construction. The Adjan-Rabin theorem, on the other hand, gives a general construction which can be applied to any Markov property P of finitely presented groups, and from which one can conclude the impossibility of deciding which presentations present groups enjoying P.

In this paper we obtain general results for undecidable first order decision problems (that is, problems about elements in a particular group, such as the word and conjugacy problems). We shall describe a class Ω of such decision problems and a construction Δ such that if P is a problem in Ω, then $\Delta(P)$ will be a finitely presented group in which P is recursively undecidable.

The following list tabulates some problems in Ω (the $(?x)(\cdots)$ notation

231

is explained in §1):

$(?x)(x = 1)$ word problem;

$(?x)(?y)(\exists z)(z^{-1}xz = y)$ conjugacy problem;

$(?x)(x^n = 1), n \neq 0$ nth order problem;

$(?x)(\forall y)(xy = yx)$ center problem;

$(?x)(\exists y)(x = y^n), |n| \neq 1$ nth root problem;

$(?x, y)(x^m = y^n), n \neq 0$ power problem;

$(?x)(\exists y)(\exists z)(x = y^{-1}z^{-1}yz)$ commutator problem;

$(?x, y)(\exists z)(\sim x = y \ \& \ z^{-1}xz = y)$ conjugacy of distinct elements;

$(?x)(\forall y)(\forall z)(xy = yx \lor [x, y, z] = 1)$.

As a consequence of the work on first order decision problems in §3 of this paper, we are able to obtain an analog of the Adjan-Rabin theorem; the analog bears a relationship to first-order quotient closed properties similar to that which the Adjan-Rabin theorem bears to subgroup-hereditary properties.

1. The *basic language L* of this paper is the first order language of group theory with individual variables $(x_1, x_2, \cdots, y_1, y_2, \cdots, z_1, z_2, \cdots)$, an individual constant 1, operation symbols $\cdot$ and $^{-1}$, the predicate $=$, and the logical symbols $\&$, $\lor$, $\sim$, $\forall$, and $\exists$. All formulas will be taken to be in prenex normal form, with matrices in disjunctive normal form, and with atomic subformulas in the form $W=1$, where W is a term. Given a group G the language L^G is obtained from L by adding a new constant 'g' (name of g) for each element g of G. Given a homomorphism h from G to H, sentences of L^G can be interpreted in H by letting the symbol 'g' name hg. Ordinarily we will use the same symbol to denote an element of G and its name in L^G. A sentence of one of these languages will be called *positive* if it is logically equivalent to one which does not involve the negation symbol $\sim$. Given a formula Φ of one of these languages, Φ^+ is obtained from Φ by replacing each subformula of the form $\sim W=1$ by the formula $1=1$.

A *finite presentation of a group* $\pi = \langle S; D \rangle$ consists of a finite *alphabet* (or *generating set*) S, and a finite set of words on the symbols $a^{\pm 1}$, where a is in S, called *relators*. The group G_π is the quotient of the free group F_S on S by the normal closure in F_S of the elements of D. By an abuse of notation, this will be abbreviated $G_\pi = F_S/D$. A group is called *finitely presented* if it possesses such presentation.

Given a finite presentation of a group π and a formula $\Phi(x)$ of L^{G_π} all of whose free variables are among the t-tuple x, the *decision problem* $(?x)\Phi(x)$ for G_π is the problem of determining for which t-tuples u of words on the generators of π does the sentence $\Phi(u)$ hold in G_π. In this notation the word problem for a given finite group presentation is

$(?x)[x=1]$, the conjugacy problem is $(?x, y)(\exists z)[z^{-1}xzy^{-1}=1]$, and the center problem is $(?x)(\forall y)[x^{-1}y^{-1}xy=1]$.

It is easy to see that, given two distinct finite presentations π_1 and π_2 such that $G_{\pi_1} \cong G_{\pi_2}$, then the decision problems $(?x)\Phi(x)$ for these two presentations are Turing equivalent, because the isomorphism is effectively calculable. Consequently, given a finitely presented group G, we may speak of *the* decision problem $(?x)\Phi(x)$ for G (without explicitly mentioning the presentation).

Given a property P of finitely presented groups, we say that P is *L-definable* if there exists a sentence Φ of L such that for all finitely presented groups G, $P(G)$ if and only if G satisfies Φ.

The following lemma appears in [16].

LEMMA 1.1.   *Let F be a countable free group and let Φ be a positive sentence in L^F. Let G_1 $(\not\cong Z_2)$ and G_2 be nontrivial groups. Then there is an embedding of F into $G_1 * G_2$ such that Φ holds in F if and only if Φ holds in $G_1 * G_2$. Moreover, the embedding may be given by mapping each free generator δ_i of F to $W_i(a, b)$ where $W_i(x, y)$ is a freely reduced word on x and y and a and b may be taken to be any nontrivial elements of G_1 and G_2 respectively, such that $a^2 \neq 1$.*

LEMMA 1.2 (MERZLYAKOV [10]).   *Let F and F' be free groups where the rank of F is at least 2. Let Φ be a positive sentence of L^F. Φ holds in F if and only if Φ holds in $F * F'$.*

LEMMA 1.3 (LYNDON [7]).   *A sentence of L is equivalent to a positive sentence if and only if its truth is preserved under quotients.*

LEMMA 1.4.   *Let $\Phi(x)$ be a positive formula of L with at most t free variables. Let F be a free group of rank at least t.*

(i) *If $\Phi(x)$ is satisfiable in F, then $\Phi(1)$ holds in F.*

(ii) *If $\sim\Phi(x)$ is satisfiable in F, then $\sim\Phi(f)$ holds in F, where f is a t-tuple of free generators of F.*

PROOF.   (i) Since $\Phi(x)$ is satisfiable in F, it is satisfiable in F_ω, the free group of countable rank, by 1.2. Let w be a t-tuple of elements of F_ω such that $\Phi(w)$ holds. Let $f_1, \cdots, f_s$ be the generators F_ω appearing in elements of w. In the group $G = F_\omega/f_1 = 1 \& \cdots \& f_s = 1$, $\Phi(1)$ holds, by Lemma 1.3. But $G \cong F_\omega$. Therefore $\Phi(1)$ holds in F_ω and, by 1.2, $\Phi(1)$ holds in F.

(ii) Let w be elements of F such that $\sim\Phi(w)$ holds in F. Let $\beta_1, \cdots, \beta_t$ be new letters and let $\tilde{F} = F * \langle \beta_1, \cdots, \beta_t \rangle$. Since the map $h: \tilde{F} \to F$ defined by $hf = f$ for f in F and $h\beta_i = w_i$ is a homomorphism and $\Phi(x)$ is positive, $\tilde{F}$ satisfies $\sim\Phi(\beta)$. Further, since the map from $\tilde{F}$ to $\tilde{F}$ which interchanges the β's with the corresponding members of $f_1, \cdots, f_t$ and leaves all other

free generators of $\tilde{F}$ unchanged extends to an automorphism of $\tilde{F}$, $\tilde{F}$ satisfies $\sim\Phi(f)$. Applying 1.2 once again, F satisfies $\sim\Phi(f)$.

LEMMA 1.5. (i) *If $G \times H$ satisfies $\Phi(x)$, then G satisfies $\Phi^+(x)$ and H satisfies $\Phi^+(x)$.*

(ii) *If G satisfies $\Phi(x)$ and if H satisfies $(Qy)[D_1^+(x, y) \& \cdots \& D_k^+(x, y)]$ where $D_1, \cdots, D_k$ are the disjuncts of the matrix of $\Phi(x)$ and (Qy) is the prefix of $\Phi(x)$, then $G \times H$ satisfies $\Phi(x)$.*

PROOF. (i) Since $G \times H$ satisfies $\Phi(x)$, then $G \times H$ satisfies $\Phi^+(x)$. Since both G and H are quotients of $G \times H$, both of them satisfy $\Phi^+(x)$.

(ii) Let $D_i(x, y)$ be

$$U_{1i}(x, y) = 1 \& \cdots \& U_{ik_i}(x, y)$$
$$= 1 \& V_{i1}(x, y) \neq 1 \& \cdots \& V_{il_i}(x, y) \neq 1.$$

$G \times H$ satisfies $\Phi(x)$ if and only if

$$(Q_1\langle y_1, z_1 \rangle) \cdots (Q_s\langle y_s, z_s \rangle)$$

$$\left\{ \bigvee_i U_{i1}(a, y) =_G 1 \& \cdots \& U_{ik_i}(a, y) =_G 1 \& U_{i1}(b, z) \right.$$

$$=_H 1 \& \cdots \& U_{ik_i}(b, z)$$

$$=_H 1 \& [V_{i1}(a, y) \neq_G 1 \vee V_{i1}(b, z) \neq_H 1)] \& \cdots$$

$$\left. \& [V_{il_i}(a, y) \neq_G 1 \vee V_{il_i}(b, z) \neq_H 1]\right\},$$

for some vectors a and b of elements of G and H respectively. The latter condition holds if and only if

(1)
$$(Q_1 y_1 \in G)(Q_1 z_1 \in H) \cdots (Q_s y_s \in G)(Q_s z_s \in H)$$
$$\left\{ \bigvee_i [D_i(a, y) \& D_i^+(b, z)] \vee [\text{other terms}]\right\}.$$

The hypotheses indicate that

$$(Q_1 y_1 \in G) \cdots (Q_s y_s \in G)\left\{ \bigvee_i D_i(a, y)\right\}$$

$$\& (Q_1 z_1 \in H) \cdots (Q_s z_s \in H)\left\{ \&_i D_i^+(b, z)\right\}.$$

This is equivalent to

(2)
$$(Q_1 y_1 \in G)(Q_1 z_1 \in H) \cdots (Q_s y_s \in G)(Q_s z_s \in H)$$
$$\left\{ \bigvee_i [D_i(a, y)] \& D_1^+(b, z) \& \cdots \& D_m^+(b, z)\right\}.$$

It is clear that (2) implies (1).

2. THEOREM I.   *Let $\Phi(x)$ be a formula of L with free variables x. Suppose that there exist finitely presented groups K_0 and K_1 in which $\Phi(x)$ and $\sim\Phi^+(x)$ are satisfiable. Suppose further that $(Qy)[D_1^+(x,y)\&\cdots\&D_k^+(x,y)]$ is satisfiable in some nonabelian free group, where (Qy) is the prefix of $\Phi(x)$ and $D_1(x,y),\cdots, D_k(x,y)$ are the disjuncts of the matrix of $\Phi(x)$. Then $(?x)\Phi(x)$ is recursively unsolvable in some finitely presented group.*

PROOF.   Let u be elements of K_0 such that $\Phi(u)$ holds. Since $\sim\Phi^+(x)$ is satisfiable in K_1, $\sim\Phi^+(x)$ is satisfiable in F, a nonabelian free group of rank at least t (recall $t=$the number of free variables in Φ). Therefore $\sim\Phi^+(f)$ holds in F, where f is a t-tuple of free generators of F, by 1.4 (ii). Moreover, by 1.4 (i), $(Qy)[D_1^+(1,y)\&\cdots\&D_k^+(1,y)]$ holds in F. Call this last sentence Ψ. Ψ holds in any group, by Lemmas 1.2 and 1.3.

Let G_1 and G_2 be distinct copies of a torsion-free group G with unsolvable word problem. In particular, neither G, nor G_1, nor G_2 is a 2-cycle. Let w be a variable ranging over words of G and let w_1 and w_2 be the images of w in the two copies. By Lemma 1.1, there are words $W_i(z_1, z_2)$ such that given any pair of nontrivial elements a_1 and a_2 of G_1 and G_2, the map defined by $\delta_i\to W_i(a_1, a_2)$ (the δ's are any fixed set of free generators for F) gives an embedding of F into $G_1 * G_2$ such that $\sim\Phi^+(f)$ holds in F if and only if it holds in the free product; moreover Ψ holds in $G_1 * G_2$. For each w in G, let $f_w=\langle W_1(w_1, w_2),\cdots, W_t(w_1, w_2)\rangle$. Thus, by Lemma 1.4, if $w\neq 1$ in G, $G_1 * G_2$ satisfies $\sim\Phi^+(f_w)$ and if $w=1$ in G, $G_1 * G_2$ satisfies $(Qy)D_1^+(f_w, y)\&\cdots\&D_k^+(f_w, y)$ because if $w=1$, $f_w=1$. Therefore by 1.5, $(G_1 * G_2)\times K_0$ satisfies

$$\Phi(\langle W_1(w_1, w_2), u_1\rangle,\cdots, \langle W_t(w_1, w_2), u_t\rangle)$$

if and only if $w=1$ in G. Since it is not possible to effectively decide when $w=1$ in G, $(?x)\Phi(x)$ is recursively unsolvable in $(G_1 * G_2)\times K_0$.

THEOREM II.   *Suppose that $\Phi(x)$ is a positive formula of L such that both $\Phi(x)$ and $\sim\Phi(x)$ are satisfiable in some nonabelian free group. Then $(?x)\Phi(x)$ is recursively unsolvable in some finitely presented group.*

PROOF.   Applying 1.4 we see that $\sim\Phi(f)$ and $\Phi(1)$ hold in F where F is free of rank greater than $t+1$ and f is a t-tuple of distinct free generators of F. Let G, G_1, G_2, w, w_1, and w_2 be as in the preceding proof. Let $W_1(z_1, z_2)$, $\cdots, W_t(z_1, z_2)$ be the words for Lemma 1.1 such that $\delta_i\to W_i(a_1, a_2)$ defines an embedding of F into $G_1 * G_2$ such that $\sim\Phi(\delta)$ holds in F if and only if it holds in $G_1 * G_2$ (recall that the δ's are a set of free generators for F, and a_1 and a_2 are any nontrivial words from G_1 and G_2 respectively).

Moreover, $\Phi(1)$ holds in all groups. For each word w of G, let f_w be $\langle W_1(w_1, w_2), \cdots, W_t(w_1, w_2)\rangle$. Thus $\Phi(f_w)$ holds in $G_1 * G_2$ if and only if $w = 1$ in G. Therefore, $(?x)\Phi(x)$ is recursively unsolvable in $G_1 * G_2$.

THEOREM III. *Suppose that $\Phi(x)$ is a quantifier free formula of L, and that there exist finitely presented groups K_0 and K_1 in which $\Phi(x)$ and $\sim\Phi(x)$ respectively are satisfiable. Then $(?x)\Phi(x)$ is recursively unsolvable in some finitely presented group.*

PROOF. *Case* (1). Each disjunct $D_i(x)$ of $\Phi(x)$ is of the form $U_i(x) = 1$ & $D_i'(x)$, where $U_i(x) = 1$ is a nontrivial atomic subformula. If F is a free group of rank at least t and if k includes the first t free generators of F, then $\sim\Phi(k)$ holds in F since $U_i(k) \neq 1$ for each i. On the other hand, for each i, $D_i^+(1)$ holds in F since each D_i^+ is simply a conjunction of equations of the type $U(x) = 1$ where U is a word on the variables. Finally $\Phi(u)$ holds in K_0, for some tuple u of elements of K_0. Therefore all of the hypotheses of Theorem I are satisfied. Consequently, there is a finitely presented group in which $(?x)\Phi(x)$ is recursively unsolvable.

Case (2). Some disjunct D^* of Φ is of the form $\&_i V_i(x) \neq 1$. Each disjunct of the disjunctive normal form for $\sim\Phi$ is a conjunction of basic formulas; each of the basic formulas is the negation of a basic formula in Φ; moreover, each disjunct of Φ contributes precisely one basic formula to each disjunct of $\sim\Phi$. In particular each disjunct of $\sim\Phi$ is of the form $V^*(x) = 1$ & $D'(x)$, where $V^*(x) \neq 1$ is a basic formula of D^*. Thus $\sim\Phi$ meets the hypothesis of Case (1). Applying the argument for Case (1) and observing that $\sim\Phi(v)$ holds in K_1, for some tuple v of elements of K_1, we see that $(?x)\Phi(x)$ is recursively unsolvable in some finitely presented group.

THEOREM IV. *Let Φ be a sentence of L. Suppose that there exist finitely presented groups G and H such that G satisfies Φ and H satisfies $\sim\Phi^+$, respectively. Then $(?\pi)[G_\pi$ satisfies $\Phi]$ is recursively unsolvable, where the variable π ranges over finite presentations.*

PROOF. Since $\sim\Phi^+$ is satisfiable in H, $\sim\Phi^+$ holds in some finitely generated nonabelian free group F. Consequently, Φ is false in any free product of nontrivial torsion-free groups. We will show the desired unsolvability by giving a recursive class of presentations π_w indexed by words w of a group E with unsolvable word problem such that if $w = 1$ in E, then $\pi_w \cong G$ and if $w \neq 1$ in E, then π_w presents a group of the form $(G_1 * G_2) \times G$. Since $\sim\Phi^+$ holds in the free product, $\sim\Phi$ holds in the group presented by π_w, by Lemma 1.5.

Let Γ be a recursive family of finite presentations indexed by words of a

countable group E with unsolvable word problem, such that for each word w of E, if $w = 1$ in E, then the element γ_w of Γ presents the trivial group and if $w \neq 1$ in E, then γ_w presents a nontrivial torsion-free group. (See [11] for a detailed account of the construction of such a family Γ.) Let $\bar{\gamma}_w$ be obtained from γ_w by replacing each occurrence of each letter a in the generators and the relations of γ_w by a new letter $\bar{a}$. Then let π_w be: ⟨generators of γ_w and $\bar{\gamma}_w$, generators of G; relations of γ_w, $\bar{\gamma}_w$, and G, $[c, d]$, for each generator c of γ_w or $\bar{\gamma}_w$, for each generator d of G⟩. Thus π_w presents $(G_{\gamma_w} * G_{\bar{\gamma}_w}) \times G$. If $w = 1$ in E, the free product is trivial and π_w presents G. If $w \neq 1$ in E, then the free product is nontrivial and is not isomorphic to $Z_2 * Z_2$. Therefore, Φ^+ is false in $G_{\gamma_w} * G_{\gamma_w}$. Thus, if $w \neq 1$ in E, G_{π_w} is a group in which Φ is false. Thus $(?\pi)[G_\pi$ satisfies $\Phi]$ is recursively undecidable.

THEOREM V.   *Let P be a quotient-closed L-definable property of finitely presented groups. If P does not hold of all finitely presented groups, then $(?\pi)[P(G_\pi)]$ is recursively unsolvable.*

PROOF.   Let P be L-definable and quotient-closed. By Lyndon's theorem, there is a positive sentence Φ of L such that for all groups G, $P(G)$ if and only if G satisfies Φ. Since Φ is positive, Φ holds in a trivial group. Since P is a nontrivial property, it fails in some group; in particular, it fails in a finitely generated nonabelian free group, by Lyndon's theorem and Merzlyakov's theorem. That is, $\sim\Phi^+$ holds in some finitely presented group, since Φ is Φ^+. Therefore, by Theorem IV, the decision problem $(?\pi)[P(G_\pi)]$ is undecidable.

3. The following problem is suggested by this work.

Problem.   Which Turing degrees of unsolvability are the degrees of first order decision problems in the theory of finitely presented groups?

Up to now the principal partial results are that the recursively enumerable degrees are the degrees of word, conjugacy, and center problems. Boone has suggested that all first order decision problems for finitely presented groups have these degrees. However one must note that the conjugacy problem is Σ_1 in the word problem; thus it really adds no new evidence for this position. Similarly, for finitely presented groups, the center problem can be described by a sentence which is Σ_1 in the word problem. In particular, it is not clear that $(?x)(\forall y)[x^{-1}y^{-2}xy^2 = 1]$ must have r.e. degree in all such groups.[2]

---

[2] ADDED IN PROOF.   The author has recently constructed a finitely presented group G and a formula $\Phi(x)$ such that $(?x)\Phi(x)$ in G has degree of unsolvability $0''$. This work will appear shortly in Math. Scand.

References

1. S. I. Adjan, *On algorithmic problems in effectively complete classes of groups*, Dokl. Akad. Nauk SSSR **123** (1958), 13–16. (Russian) MR **21** #1998.

2. G. Baumslag, W. W. Boone and B. H. Neumann, *Some unsolvable problems about elements and subgroups of groups*, Math. Scand. **7** (1959), 191–201. MR **29** #1247.

3. W. W. Boone, *Certain simple, unsolvable problems of group theory*. I–VI, Nederl. Akad. Wetensch. Proc. Ser. A **57, 58, 60** = Indag. Math. **16** (1954), 231–237, 492–497; ibid. **17** (1955), 252–256, 571–577; ibid. **19** (1957), 22–27, 227–232. MR **16**, 564; MR **20** #5230; #5231.

4. ———, *The word problem*, Ann. of Math. (2) **70** (1959), 207–265. MR **31** #3485.

5. D. J. Collins, *On the word, order, and power problems in finitely presented groups*, Proc. Irvine Conference on Decision Problems in Group Theory (to appear).

6. M. Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Ann. **71** (1911), 116–144.

7. R. C. Lyndon, *Properties preserved under homomorphism*, Pacific J. Math. **9**. (1959), 143–154. MR **21** #7157.

8. ———, *On Dehn's algorithm*, Math. Ann. **166** (1966), 208–228. MR **35** #5499.

9. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Pure and Appl. Math., vol. 13, Interscience, New York, 1966. MR **34** #7617.

10. Ju. I. Merzljakov, *Positive formulae on free groups*, Algebra i Logika. Sem. **5** (1966), no. 4, 25–42. (Russian) MR **36** #5201.

11. C. F. Miller III, *On group-theoretic decision problems and their classification*, Ann. of Math. Studies, no. 68, Princeton Univ. Press, Princeton, N.J., 1971.

12. P. S. Novikov, *Unsolvability of the conjugacy problem in the theory of groups*, Izv. Akad. Nauk SSSR Ser. Mat. **18** (1954), 485–524. (Russian) MR **17**, 706.

13. ———, *On the algorithmic insolvability of the word problem in group theory*, Trudy Mat. Inst. Steklov. **44** (1955); English transl., Amer. Math. Soc. Transl. (2) **9** (1958), 1–122. MR **17**, 706; MR **19**, 1158.

14. M. O. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. of Math. (2) **67** (1958), 172–194. MR **22** #1611.

15. G. S. Sacerdote, *Elementary properties of free groups*, Trans. Amer. Math. Soc. (to appear).

16. ———, *Almost all free products have the same positive theory* (to appear).

17. P. E. Schupp, *On Dehn's algorithm and the conjugacy problem*, Math. Ann. **178** (1968), 119–130. MR **38** #5901.

Mathematical Institute, University of Oxford, Oxford, England

Current address: Institute for Advanced Study, Princeton, New Jersey 08540