A Slick Proof of the Unsolvability of the Word Problem for Finitely Presented Groups

Stephen G. Simpson

First draft: May 17, 2005
This draft: May 18, 2005

Abstract

A famous theorem of P. Novikov 1955 and W. W. Boone 1959 asserts the existence of a finitely presented group with unsolvable word problem. In my Spring 2005 topics course (MATH 574, Topics in Mathematical Logic), I presented Boone's proof, as simplified by J. L. Britton, 1963. In this seminar I shall present a truly slick, streamlined proof, due to S. Aanderaa and D. E. Cohen, 1980. Instead of Turing machines or register machines, the Aanderaa-Cohen proof uses another kind of machines, called modular machines, which I shall discuss in detail. In addition, the Aanderaa-Cohen proof uses Britton's Lemma. I shall omit the proof of Britton's Lemma, which can be found in my course notes [3] at http://www.math.psu.edu/simpson/notes/.

We present the Aanderaa-Cohen [1] simplified proof of the unsolvability of the word problem for finitely presented groups.

Like the original Boone-Britton proof, the Aanderaa-Cohen proof is based on HNN extensions and Britton's Lemma. The statement and proof of Britton's Lemma are in [3]. Here we mention some consequences of Britton's Lemma which we shall need.

Definition 1. Let G be any group, and let $\phi_i : H_i \cong K_i$, $i \in I$, be a family of isomorphisms between subgroups of G. Then the group

$$G' = \langle G, p_i, i \in I \mid p_i^{-1} h p_i = \phi_i(h), h \in H_i, i \in I \rangle$$

is called an *HNN extension* of G with *stable letters* $p_i, i \in I$. By Britton's Lemma, $G \subseteq G'$.

Definition 2. A *good subgroup* of G is a subgroup $A \subseteq G$ such that $\phi_i(A \cap H_i) = A \cap K_i$ for all $i \in I$. Let A' be the subgroup of G' generated by $A, p_i, i \in I$, i.e., A plus the stable letters. By Britton's Lemma, A' is an HNN extension of A with the same stable letters, and $A' \cap G = A$.

Instead of Turing machines or register machines, the Aanderaa-Cohen proof uses another kind of machines, called modular machines.

Definition 3. A *modular machine* $\mathcal{M}$ consists of an integer $M > 1$ and a finite set of quadruples of the form (a, b, c, R) and (a, b, c, L) where $M > a \geq 0$ and $M > b \geq 0$ and $M^2 > c \geq 0$. We require that for each (a, b) there is at most one quadruple of $\mathcal{M}$ beginning with (a, b).

A *modular machine configuration* is an ordered pair $(\alpha, \beta) \in \mathbb{N}^2$. We write $(\alpha, \beta) \xrightarrow{\mathcal{M}} (\alpha_1, \beta_1)$ if and only if $\alpha = uM + a$ and $\beta = vM + b$ and there exists c such that either

1. $(a, b, c, R) \in \mathcal{M}$ and $\alpha_1 = uM^2 + c$ and $\beta_1 = v$, or
2. $(a, b, c, L) \in \mathcal{M}$ and $\alpha_1 = u$ and $\beta_1 = vM^2 + c$.

Note that the action of $\mathcal{M}$ on (α, β) depends on the class of (α, β) modulo M. This is why we call $\mathcal{M}$ a "modular machine."

We write $(\alpha, \beta) \overset{\mathcal{M}}{\longrightarrow}{}^{*} (\overline{\alpha}, \overline{\beta})$ if there exists a finite sequence

$$(\alpha, \beta) = (\alpha_0, \beta_0) \xrightarrow{\mathcal{M}} (\alpha_1, \beta_1) \xrightarrow{\mathcal{M}} \cdots \xrightarrow{\mathcal{M}} (\alpha_n, \beta_n) = (\overline{\alpha}, \overline{\beta}) .$$

Such a sequence is called a *computation* of $\mathcal{M}$.

Theorem 4. *There is a modular machine $\mathcal{M}$ such that the halting set*

$$H_{\mathcal{M}} = \left\{ (\alpha, \beta) \,\middle|\, (\alpha, \beta) \overset{\mathcal{M}}{\longrightarrow}{}^{*} (0, 0) \right\}$$

is nonrecursive.

Proof. Let $\mathcal{T}$ be a Turing machine such that the set of eventually halting configurations of $\mathcal{T}$ is nonrecursive. We may safely assume that, whenever $\mathcal{T}$ halts, the tape is empty. We construct a modular machine $\mathcal{M}$ which simulates $\mathcal{T}$. Let A be the tape alphabet of $\mathcal{T}$. Let Q be the set of internal states of $\mathcal{T}$. Let M be the cardinality of the set $A \cup Q$. We may safely assume that $A = \{1, \ldots, n\}$ and $Q = \{n+1, \ldots, M\}$. To each configuration $a_k \cdots a_1 q a b_1 \cdots b_l$ of $\mathcal{T}$, we associate two modular machine configurations $(uM + q, vM + a)$ and $(uM + a, vM + q)$, where $u = \sum_{i=1}^{k} a_i M^{i-1}$ and $v = \sum_{j=1}^{l} b_j M^{j-1}$. For each quintuple $qaq'a'D$ of $\mathcal{T}$, where $D \in \{R, L\}$, we let $\mathcal{M}$ have quadruples $(q, a, a'M + q', D)$ and $(a, q, a'M + q', D)$. The details are left to the reader. $\square$

We shall use $\mathcal{M}$ to construct a finitely presented group with unsolvable word problem. We begin with the particular group

$$G = \langle t, x, y \mid xy = yx \rangle .$$

For $\alpha, \beta \in \mathbb{Z}$ put

$$t(\alpha, \beta) = x^{-\alpha} y^{-\beta} t x^{\alpha} y^{\beta} .$$

Note that the subgroup

$$T = \langle t(\alpha,\beta) \mid \alpha,\beta \in \mathbb{Z}\rangle$$

is free on these generators.

For any $M > a \geq 0$ and $N > b \geq 0$, consider the subgroup

$$\begin{aligned} T_{ab}^{MN} &= \langle t(\alpha,\beta) \mid \alpha \equiv a \bmod M, \beta \equiv b \bmod N\rangle \\ &= \langle t(uM+a, vN+b) \mid u,v \in \mathbb{Z}\rangle \end{aligned}$$

of T. Note that there is a canonical isomorphism $T_{ab}^{MN} \cong T$. In addition, let G_{ab}^{MN} be the subgroup of G generated by $t(a,b), x^M, y^N$. Again, there is a canonical isomorphism $G_{ab}^{MN} \cong G$.

Lemma 5. $T_{ab}^{MN} = T \cap G_{ab}^{MN}$.

Proof. For $\subseteq$, note that $t(uM+a, vN+b) = x^{-uM}y^{-vN}t(a,b)x^{uM}y^{vN} \in G_{ab}^{MN}$. For $\supseteq$, note that $x^M t(\alpha,\beta) = t(\alpha - M, \beta)x^M$ and $y^N t(\alpha,\beta) = t(\alpha,\beta - N)y^N$, hence any element of G_{ab}^{MN} is of the form $gx^{uM}y^{vN}$ where $g \in T_{ab}^{MN}$ and $u,v \in \mathbb{Z}$. If this element is in T, then clearly $u = v = 0$, hence it is in T_{ab}^{MN}. $\square$

Definition 6. Given a modular machine

$$\mathcal{M} = \{(a_i,b_i,c_i,R) \mid i \in I\} \cup \{(a_j,b_j,c_j,L) \mid j \in J\},$$

we construct an HNN extension $G'_{\mathcal{M}}$ of G. For each $i \in I$ we introduce a stable letter r_i and specify that $g \mapsto r_i^{-1}gr_i$ extends the canonical isomorphism $\phi_i : G_{a_ib_i}^{MM} \cong G_{c_i,0}^{M^2,1}$. For each $j \in J$ we introduce a stable letter l_j and specify that $g \mapsto l_j^{-1}gl_j$ extends the canonical isomorphism $\psi_j : G_{a_jb_j}^{MM} \cong G_{0,c_j}^{1,M^2}$. Thus, the stable letters of $G'_{\mathcal{M}}$ are r_i, $i \in I$, and l_j, $j \in J$. Note that $G'_{\mathcal{M}}$ is finitely presented.

By Lemma 5, T is a good subgroup of G with respect to the HNN extension $G' = G'_{\mathcal{M}}$. It follows that $T = T' \cap G$. Consider also the subgroup

$$T_{\mathcal{M}} = \langle t(\alpha,\beta) \mid (\alpha,\beta) \in H_{\mathcal{M}}\rangle.$$

Note that if $\phi_i(t(\alpha,\beta)) = t(\alpha_1,\beta_1)$ or $\psi_j(t(\alpha,\beta)) = t(\alpha_1,\beta_1)$, then $(\alpha,\beta) \xrightarrow{\mathcal{M}} (\alpha_1,\beta_1)$, hence $t(\alpha,\beta) \in T_{\mathcal{M}} \iff (\alpha,\beta) \in H_{\mathcal{M}} \iff (\alpha_1,\beta_1) \in H_{\mathcal{M}} \iff t(\alpha_1,\beta_1) \in T_{\mathcal{M}}$. From this it follows that $T_{\mathcal{M}}$ is again a good subgroup of G with respect to G'. Therefore, $T_{\mathcal{M}} = T'_{\mathcal{M}} \cap G$.

Lemma 7. $T'_{\mathcal{M}} = \langle t\rangle'$.

Proof. The $\supseteq$ is obvious, because $t = t(0,0) \in T_{\mathcal{M}}$. To prove $\subseteq$, it suffices to show that $t(\alpha,\beta) \in \langle t\rangle'$ for all $(\alpha,\beta) \in H_{\mathcal{M}}$. We prove this by induction on the length of the computation putting (α,β) into $H_{\mathcal{M}}$. For $(\alpha,\beta) = (0,0)$ we have

$t(0,0) = t \in \langle t\rangle'$. Assume now that $(\alpha,\beta) \xrightarrow{\mathcal{M}} (\alpha_1,\beta_1)$ via (a_i,b_i,c_i,R). We have

$$\begin{aligned} t(\alpha,\beta) &= x^{-\alpha}y^{-\beta}tx^{\alpha}y^{\beta} \\ &= x^{-uM-a_i}y^{-vM-b_i}tx^{uM+a_i}y^{vM+b_i} \\ &= x^{-uM}y^{-vM}t(a_i,b_i)x^{uM}y^{vM}\,, \end{aligned}$$

hence

$$\begin{aligned} r_i^{-1}t(\alpha,\beta)r_i &= x^{-uM^2}y^{-v}t(c_i,0)x^{uM^2}y^{v} \\ &= x^{-uM^2-c_i}y^{-v}tx^{uM^2+c_i}y^{v} \\ &= t(uM^2+c_i,v) \\ &= t(\alpha_1,\beta_1)\,. \end{aligned}$$

If $(\alpha,\beta) \in H_{\mathcal{M}}$, then $(\alpha_1,\beta_1) \in H_{\mathcal{M}}$ by a shorter computation, hence by inductive hypothesis $t(\alpha_1,\beta_1) \in \langle t\rangle'$, hence $t(\alpha,\beta) = r_i t(\alpha_1,\beta_1) r_i^{-1} \in \langle t\rangle'$. If $(\alpha,\beta) \xrightarrow{\mathcal{M}} (\alpha_1,\beta_1)$ via (a_j,b_j,c_j,L), the proof is similar. □

It follows from the previous lemma that $T_{\mathcal{M}} = \langle t\rangle' \cap G$.

Theorem 8. *There is a finitely presented group with unsolvable word problem.*

Proof. Let $\mathcal{M}$ be a modular machine as in Theorem 4. Let $G'_{\mathcal{M}}$ be the HNN extension of G from Definition 6. Consider the further HNN extension

$$(G'_{\mathcal{M}})' = \langle G'_{\mathcal{M}}, k \mid k^{-1}hk = h, h \in \langle t\rangle'\rangle\,.$$

Since $\langle t\rangle'$ is finitely generated, $(G'_{\mathcal{M}})'$ is finitely presented. By Britton's Lemma, for all $g \in G'_{\mathcal{M}}$ we have $k^{-1}gk = g \iff g \in \langle t\rangle'$. In particular $k^{-1}t(\alpha,\beta)k = t(\alpha,\beta) \iff t(\alpha,\beta) \in \langle t\rangle' \iff t(\alpha,\beta) \in T_{\mathcal{M}} \iff (\alpha,\beta) \in H_{\mathcal{M}}$. Thus $H_{\mathcal{M}}$, the halting problem for $\mathcal{M}$, is reducible to the word problem for $(G'_{\mathcal{M}})'$. It follows that the latter problem is unsolvable. □

Remark 9. We have seen that the word problem for $(G'_{\mathcal{M}})'$ is unsovable. In addition, Aanderaa-Cohen [1] have shown that the word problem for $(G'_{\mathcal{M}})'$ is Turing equivalent to $H_{\mathcal{M}}$. Thus, there are finitely presented groups with word problem of any prescribed recursively enumerable degree of unsolvability. This result is originally due to Clapham, 1964.

References

[1] Stål Aanderaa and Daniel E. Cohen. Modular machines I, II. In [2], pages 1–18, 19–28, 1980.

[2] S. I. Adian, W. W. Boone, and G. Higman, editors. *Word Problems II: The Oxford Book*. Studies in Logic and the Foundations of Mathematics. North-Holland, 1980. X + 578 pages.

[3] Stephen G. Simpson. Topics in Mathematical Logic – Spring 2005. Unpublished lecture notes, Department of Mathematics, Pennsylvania State University, 75 pages, 2005.