EMBEDDINGS INTO SIMPLE FREE PRODUCTS

DAVID MEIER

ABSTRACT. We prove that a countable group G can be embedded into a two-generator simple group S which is an amalgamated free product of groups $G * F_1$ and F , where F and F_1 are free groups on two generators. S is also the product of two commuting free subgroups. If G has solvable word problem, then we can construct a recursive presentation for S .

1. Introduction. It is well known that every countable group is a subgroup of a simple two-generator group (see [3] and [7]). The main result of our paper is

THEOREM A. (a) *A countable group G can be embedded into a simple two-generator group S which is an amalgamated free product of $G * F_1$ and F , where F and F_1 are both free groups on two generators. S is also the product of two commuting free subgroups.*

(b) *If G has solvable word problem, we can construct the group S of (a) with a recursive presentation.*

It was first shown by R. J. Thompson [8] by a construction completely different from ours that a countable group with solvable word problem is a subgroup of a recursively presented finitely generated simple group. Our construction of the group S is similar to the construction of the simple free products of R. Camm [1], or see [6] for a slightly simplified version.

2. The construction of the group S . Let H be a countable infinite group with an element x of order at least 5, and assume that the elements of H are numbered by the integers, $H = \{g_i, i \in \mathbf{Z}\}$, such that $g_0 = 1$, $g_1 = x$, $g_2 = x^2$, $g_3 = x^3$, $g_4 = x^4$. Let $A = \langle a \rangle$ and $F = \langle b, c \rangle$ be free groups on a and b, c , respectively. Then the subgroup U of $A * H$ generated by the elements of the form

$$u_i = a^i g_{\rho(i)}, \quad i \in \mathbf{Z} - \{0\},$$

where ρ is a permutation of $\mathbf{Z} - \{0\}$, is a free group freely generated by the elements u_i , $i \in \mathbf{Z} - \{0\}$, with transversal A in $A * H$. Similarly, the elements

$$v_j = b^j c^{\sigma(j)}, \quad j \in \mathbf{Z} - \{0\},$$

of F , where σ is a second permutation of $\mathbf{Z} - \{0\}$, freely generate a free subgroup V of F with transversal $B = \langle b \rangle$.

Received by the editors April 10, 1983.

1980 *Mathematics Subject Classification.* Primary 20E06, 20E32, 20F10.

©1985 American Mathematical Society
0002-9939/85 \$1.00 + \$.25 per page

We can therefore form the amalgamated free product

$$S = \langle A * H * F; u_i = v_{\tau(i)}, i \in \mathbf{Z} - \{0\} \rangle,$$

τ is a third permutation of $\mathbf{Z} - \{0\}$.

By the normal form theorem for amalgamated free products (see Theorem 4.4 in [5]), $S = U\langle a, b \rangle$, where $\langle a, b \rangle$ is free on a and b . S is therefore the product of two commuting free subgroups.

We now choose ρ, σ, τ in such a way that S is a simple two-generator group.

3. The permutations ρ, σ, τ . For $1 \leq i \leq 4$, ρ, σ, τ are defined by the equations

$$\begin{aligned} (1) \quad & ag_1 = bc, \\ (2) \quad & a^2g_2 = b^2c^3, \\ (3) \quad & a^3g_3 = b^4c^4, \\ (4) \quad & a^4g_4 = b^3c^2. \end{aligned}$$

For $-4 \leq i \leq -1$ we set $a^ig_i = b^ic^i$. Assume now that $z_i = a^{i_1}b^{j_1} \cdots b^{j_n}a^{i_{n+1}}$, $i = 0, 1, 2, \dots$, is a recursive enumeration of the elements of $\langle a, b \rangle$, $z_0 =$ identity element. For $|i| > 4$ the permutations are inductively defined by going through the list of elements z_i , beginning with z_1 , in the following way. Assume that n_0 is the smallest positive number for which ρ, σ, τ are not yet defined and $z_i = a^{i_1}b^{j_1} \cdots a^{i_n}b^{j_n}a^{i_{n+1}}$ is the next word on our list. Note that $i_1 = 0$ or $i_{n+1} = 0$ are allowed. Then set

$$x_i = a^{i_1}g_{j_1} \cdots a^{i_n}g_{j_n}a^{i_{n+1}}, \quad w_i = b^{i_1}c^{j_1} \cdots b^{i_n}c^{j_n}b^{i_{n+1}}.$$

If $z_i = a^{i_1}$, if $i_1 = -i_{n+1}$, or if $i_1 = -i_{n+1} - 1$, proceed to (III), otherwise:

(I)(a) Choose distinct numbers p_i , $i = 1, \dots, 2n$, all $p_i \geq n_0$, such that $p_{2n} = p_0 - i_{n+1}$, where p_0 is defined by $p_1 = p_0 + i_1$, and such that $p_{2k-1} - p_{2k-2} = i_k$ for $k = 2, \dots, n$.

(I)(b) Choose distinct numbers π_i , $i = 1, \dots, 2n$, $|\pi_i| \geq n_0$ for all i , such that $g_{\pi_{2k-1}}g_{\pi_{2k}}^{-1} = g_{j_k}$ for $k = 1, \dots, n$.

(I)(c) Choose distinct numbers q_i , $i = 1, \dots, 2n$, $q_i \geq n_0$ such that $q_{2k-1} - q_{2k} = j_k$ for $k = 1, \dots, n$.

Then: set $n_1 = \max(p_i, |\pi_i|, q_i, i = 1, \dots, 2n)$ and $\rho(p_i) = \pi_i$, $\sigma(p_i) = q_i$ for $i = 1, \dots, 2n$; complete ρ and σ to permutations of $I_1 = [-n_1, -n_0] \cup [n_0, n_1]$; and set $\tau(i) = i$ for all i in I_1 .

(II)(a) Choose distinct numbers r_i , $i = 1, \dots, 2n$, $r_i > n_1$ for all i , such that $r_{2n} = r_0 - i_{n+1} - 1$, where r_0 is defined by $r_1 = r_0 + i_1$, and such that $r_{2k-1} - r_{2k-2} = i_k$ for $k = 2, \dots, n$.

(II)(b) Choose distinct numbers ρ_i , $i = 1, \dots, 2n$, $|\rho_i| > n_1$ for all i , such that $g_{\rho_{2k-1}}g_{\rho_{2k}}^{-1} = g_{j_k}$ for $k = 1, \dots, n$.

(II)(c) Choose distinct numbers σ_i , $i = 1, \dots, 2n$, $\sigma_i > n_1$ for all i , such that $\sigma_{2k-1} - \sigma_{2k} = j_k$ for $k = 1, \dots, n$.

Then: set $n_2 = \max(r_i, |\rho_i|, \sigma_i, i = 1, \dots, 2n)$ and $\rho(r_i) = \rho_i$, $\sigma(r_i) = \sigma_i$ for $i = 1, \dots, 2n$; complete ρ and σ to permutations of $I_2 = [-n_2, -n_1 - 1] \cup [n_1 + 1, n_2]$; and set $\tau(i) = i$ for all i in I_2 .

(III)(a) Choose numbers s_i , $i = 0, \dots, 2n+1$, $s_i > n_2$ for all i ,

$$s_i \text{ distinct for } \begin{cases} i = 1, \dots, 2n & \text{if } i_1 = 0 = i_{n+1}, \\ i = 0, \dots, 2n & \text{if } i_1 \neq 0 = i_{n+1}, \\ i = 1, \dots, 2n+1 & \text{if } i_1 = 0 \neq i_{n+1}, \\ i = 0, \dots, 2n+1 & \text{if } i_1 \neq 0 \neq i_{n+1}, \end{cases}$$

such that $s_{2k-1} - s_{2k-2} = -i_k$ for $k = 1, \dots, n+1$. Note that if $i_1 = 0$, then $s_0 = s_1$; and if $i_{n+1} = 0$, then $s_{2n} = s_{2n+1}$.

(III)(b) Choose distinct numbers v_i , $i = 1, \dots, 2n$, $v_i > n_2$ for all i , such that $v_{2k} - v_{2k-1} = -j_k$ for $k = 1, \dots, n$.

Then: set $n_3 = \max(s_i, v_j, i = 0, \dots, 2n+1, j = 1, \dots, 2n)$ and $\tau(s_i) = v_i$ for $i = 1, \dots, 2n$; complete τ to a permutation of $I_3 = [-n_3, -n_2 - 1] \cup [n_2 + 1, n_3]$; and set $\sigma(i) = \rho(i) = i$ for $i \in I_3$.

(III)(c) Choose numbers ρ_i , $i = 0, \dots, 2n+1$, $|\rho_i| > n_3$ for all i , ρ_i distinct whenever the s_i in (III)(a) are distinct, such that $g_{\rho_{2k}}^{-1} g_{\rho_{2k+1}} = g_{s_{2k}}^{-1} g_{s_{2k+1}}$ for $k = 0, \dots, n$.

Note that $s_0 = s_1$ implies $\rho_0 = \rho_1$ and $s_{2n} = s_{2n+1}$ implies $\rho_{2n} = \rho_{2n+1}$. Then: set $t_i = s_i + n_3 - n_2$ for $i = 0, \dots, 2n+1$; $\mu_i = v_i + n_3 - n_2$ for $i = 1, \dots, 2n$; $n_4 = \max(t_i, \mu_j, |\rho_i|, i = 0, \dots, 2n+1, j = 1, \dots, 2n)$; $\tau(t_i) = \mu_i$, $\sigma(\mu_i) = \mu_i$ for $i = 1, \dots, 2n$, $\rho(t_i) = \rho_i$ for $i = 0, \dots, 2n+1$; and complete τ, σ, ρ to permutations of $I_4 = [-n_4, -n_3 - 1] \cup [n_3 + 1, n_4]$.

Now proceed to word z_{i+1} .

Note that integers $p_i, \pi_i, q_i, r_j, p_j, \sigma_j, s_k, v_k, \rho_k$ satisfying the conditions of (I), (II), and (III), respectively, always exist, since at any stage of the construction we can choose from all but finitely many integers.

The case $z_i = a^{i_1}$ fits into the above construction with $n = 0$ if we omit the v and μ part in (III)(b) and (c).

Properties of ρ, σ, τ . (i) If $x_i = a^{i_1} g_{j_1} \dots a^{i_n} g_{j_n} a^{i_{n+1}}$ and $w_i = b^{i_1} c^{j_1} \dots b^{i_n} c^{j_n} b^{i_{n+1}}$ such that $x_i \neq a^{i_1}$ and $-i_{n+1} \neq -i_1 - 1$, then, in the notation of (I) and (II),

$$(a1) a^{p_0} x_i a^{-p_0} = u_{p_1} u_{p_2}^{-1} \dots u_{p_{2n-1}} u_{p_{2n}}^{-1};$$

$$(a2) b^{p_0} w_i b^{-p_0} = v_{p_1} v_{p_2}^{-1} \dots v_{p_{2n-1}} v_{p_{2n}}^{-1} \text{ and } u_{p_i} = v_{p_i} \text{ for } i = 1, \dots, 2n;$$

$$(b1) a^{r_0} x_i a^{-r_0} = u_{r_1} u_{r_2}^{-1} \dots u_{r_{2n-1}} u_{r_{2n}}^{-1} a^{-1};$$

$$(b2) b^{r_0} w_i b^{-r_0} = v_{r_1} v_{r_2}^{-1} \dots v_{r_{2n-1}} v_{r_{2n}}^{-1} b^{-1} \text{ and } u_{r_i} = v_{r_i} \text{ for } i = 1, \dots, 2n.$$

PROOF. We show (a1) and use the definitions of ρ, σ, τ in (I); (a2), (b1), and (b2) are similar.

$$\begin{aligned} a^{p_0} x_i a^{-p_0} &= \underbrace{a^{p_0} a^{i_1}}_{= a^{p_i}} g_{j_1} a^{i_2} \dots a^{i_n} g_{j_n} \underbrace{a^{i_{n+1}} a^{-p_0}}_{= a^{-p_{2n}}} \\ &= a^{p_i} \overbrace{g_{\pi_1} g_{\pi_2}^{-1}}^{\overbrace{a^{-p_2} a^{p_3}} \dots a^{-p_{2n-2}} a^{p_{2n-1}}} \overbrace{g_{\pi_{2n-1}} g_{\pi_{2n}}^{-1}}^{\overbrace{a^{-p_{2n}}}} a^{-p_{2n}} \\ &= u_{p_1} u_{p_2}^{-1} u_{p_3} \dots u_{p_{2n-2}}^{-1} u_{p_{2n-1}} u_{p_{2n}}^{-1}. \end{aligned}$$

(ii) If $z_i = a^{i_1} b^{j_1} \dots a^{i_n} b^{j_n} a^{i_{n+1}}$, then, in the notation of §2,

(c) $z_i^{-1} u_{s_0} u_{t_0}^{-1} z_i = u_{s_{2n+1}} u_{t_{2n+1}}^{-1}$, with $s_0 \neq s_{2n+1}$.

PROOF. We use the notation of §2, (III).

$$\begin{aligned}
 z_i^{-1} u_{s_0} u_{t_0}^{-1} z_i &= \dots a^{-1_2} b^{-j_1} a^{-i_1} a^{s_0} g_{s_0} g_{\rho_0}^{-1} a^{-t_0} a^{i_1} b^{j_1} a^{i_2} \dots \\
 &= \dots a^{-i_2} b^{-j_1} a^{s_0-i_1} g_{s_0} g_{\rho_0}^{-1} a^{-(t_0-t_i)} b^{j_1} a^{i_2} \dots \\
 &= \dots a^{-i_2} b^{-j_1} a^{s_1} g_{s_1} \underbrace{\left(g_{\rho_0} g_{s_0}^{-1} g_{s_1} \right)^{-1}}_{a^{-t_1} b^{j_1} a^{i_2}} a^{-t_1} b^{j_1} a^{i_2} \dots \\
 &= \dots a^{-i_2} b^{-j_1} a^{s_1} g_{s_1} g_{\rho_1}^{-1} a^{-t_1} b^{j_1} a^{i_2} \dots \\
 &\quad \text{(now use the fact that } \tau(s_i) = \nu_i, \tau(t_i) = \mu_i \text{)} \\
 &= \dots a^{-i_2} b^{-j_1} b^{\nu_1} c^{\nu_1} c^{-\mu_1} b^{-\mu_1} b^{j_1} a^{i_2} \dots \\
 &= \dots a^{-i_2} b^{-j_1+\nu_1} c^{-j_1+\nu_1} c^{-(j_1+\mu_1)} b^{-(j_1+\mu_1)} a^{i_2} \dots \\
 &= \dots a^{-i_2} b^{\nu_2} c^{\nu_2} c^{-\mu_2} b^{-\mu_2} a^{i_2} \dots \\
 &= \dots a^{-i_2} a^{s_2} g_{s_2} g_{\rho_2}^{-1} a^{-t_2} a^{i_2} \dots \\
 &= \dots a^{-i_2} u_{s_2} U_{t_2}^{-1} a^{i_2} \dots
 \end{aligned}$$

By proceeding in the same manner we finally obtain

$$= u_{s_{2n+1}} u_{t_{2n+1}}^{-1}.$$

The choice of the s_i in (III)(a) guarantees that $s_0 \neq s_{2n+1}$ for any $z_i \neq 1$.

4. The group S is generated by two elements. Since for every element g_i in H , there is a relation of the form $a^r g_i = b^s c^t$, S is obviously generated by a , b , and c . If we rewrite (1)–(4) by using the fact that $g_1 = x, \dots, g_4 = x^4$, we get

- (1) $ax = bc$,
- (2) $a^2 x^2 = b^2 c^3$,
- (3) $a^3 x^3 = b^4 c^4$,
- (4) $a^4 x^4 = b^3 c^2$.

It is shown in [1, p. 76] that (1) and (2) can be used to express a , b , and c by $b^{-1}a$ and bc .

5. The group S is simple. The strategy of the proof is as follows. We first show that $\langle S; a = b \rangle$ is trivial. Then we show that for any nontrivial element x in U , the additional relation $x = 1$ implies $a = b$. Finally, we show that for any nontrivial element s of S , the additional relation $s = 1$ implies a nontrivial relation $x = 1$ with x in U .

(i) $\langle S; a = b \rangle$ is trivial. Since S is generated by a , b , and c by §4, it is enough to show that $a = b$ implies $a = b = c = 1$. This follows easily from relations (1)–(4).

(ii) For any nontrivial $x_i = a^{i_1} g_{j_1} a^{i_2} \dots g_{j_n} a^{i_{n+1}}$ in U , $x_i = 1$ implies $a = b$. Since $x_i \in U$, $x_i = u_{k_1}^{\pm 1} u_{k_2}^{\pm 1} \dots u_{k_r}^{\pm 1}$. If we replace the relator x_i by a cyclically reduced conjugate in the u_i , and then by its inverse if necessary, we can assume that $x_i \neq a^{i_1}$ and $-i_{n+1} \neq i_1 \neq -i_{n+1} - 1$. As in §2 we set $w_i = b^{i_1} c^{j_1} b^{i_2} \dots c^{j_n} b^{i_{n+1}}$. We show next that the relator x_i implies a relator x_j with the property $x_j = w_j$. We use the

notation of the previous sections and claim that $x_j = a^{p_0} x_i a^{-p_0}$ has the desired properties. By (a1) in §3,

$$x_j = u_{p_1} u_{p_2}^{-1} \cdots u_{p_{2n-1}} u_{p_{2n}}^{-1} = v_{p_1} v_{p_2}^{-1} \cdots v_{p_{2n-1}} v_{p_{2n}}^{-1}.$$

Now use the definitions of ρ, σ, τ in (I) to rewrite x_j in $A * H$ and in F ; then

$$\begin{aligned} x_j &= a^{p_1} g_{j_1} a^{i_2} \cdots g_{j_n} a^{-p_{2n}} \quad \text{in } A * H \\ &= b^{p_1} c^{j_1} b^{i_2} \cdots c^{j_n} b^{-p_{2n}} \quad \text{in } F; \end{aligned}$$

therefore $x_j = w_j$. Note also that, since $p_1 = p_0 + i_1$ and $p_{2n} = p_0 - i_{n+1}$, the condition $i_1 \neq -i_{n+1} - 1$ for x_i implies $p_1 \neq p_{2n} - 1$ for x_j .

Now we use (II) of §2 and (b1) and (b2) in §3 for x_j and w_j to get

$$\begin{aligned} a^{r_0} x_j a^{-r_0} &= u_{r_1} u_{r_2}^{-1} \cdots u_{r_{2n}}^{-1} a^{-1}, \\ b^{r_0} w_j b^{-r_0} &= v_{r_1} v_{r_2}^{-1} \cdots v_{r_{2n}}^{-1} b^{-1}, \end{aligned}$$

and

$$u_{r_i} = v_{r_i} \quad \text{for } i = 1, \dots, 2n.$$

Therefore, ba^{-1} , the product of the relators $b^{r_0} w_j^{-1} b^{-r_0}$ and $a^{r_0} x_j a^{-r_0}$, is a relator of $\langle S; x_i = 1 \rangle$.

(iii) If s is a nontrivial element of S , then the additional relation $s = 1$ implies a nontrivial relation $x = 1$ for some x in U .

Since $S = U\langle a, b \rangle$, the element s is a product xz_i with x in U and $z_i = a^{i_1} b^{j_1} \cdots a^{i_n} b^{j_n} a^{i_{n+1}}$ with possibly $i_1 = 0$ or $i_{n+1} = 0$. The assertion is trivial if $z_i = 1$: we therefore assume $z_i \neq 1$. By property (c) in §3

$$z_i^{-1} u_{s_0} u_{t_0}^{-1} z_i = u_{s_{2n+1}} u_{t_{2n+1}}^{-1} \quad \text{with } s_0 \neq s_{2n+1} \text{ and } t_0 \neq t_{2n+1}.$$

The relation $s = 1$ implies $z_i^{-1} = x$; therefore

$$(*) \quad x u_{s_0} u_{t_0}^{-1} x^{-1} = u_{s_{2n+1}} u_{t_{2n+1}}^{-1}.$$

The elements $\dots, u_0, \dots, u_{s_0}, \dots, u_{s_{2n+1}}, \dots, u_{t_0}, \dots, u_{t_{2n+1}}, \dots$ are free generators of the subgroup U in G . Therefore the set

$$\dots, u_0, \dots, u_{s_0} u_{t_0}^{-1}, \dots, u_{s_{2n+1}} u_{t_{2n+1}}^{-1}, \dots, u_{t_0}, \dots, u_{t_{2n+1}}, \dots,$$

is also a free generating set of U . Since distinct free generators in a free group are not conjugate, $(*)$ is a nontrivial relation in U .

6. Proof of Theorem A. If G is a countable group, then $H = G * \langle x \rangle$, where $\langle x \rangle$ is infinite cyclic, has the properties required for the construction of the group S . Now write F_1 for the free group $\langle x, a \rangle$; then the proof of (a) is complete.

If G has solvable word problem, and $G = \langle T; R \rangle$ is a presentation of G with respect to which the word problem is solvable, then the word problem of $H = \langle T, x; R \rangle$ is solvable with respect to the given presentation, and we can therefore effectively enumerate the elements of H .

The permutations ρ, σ, τ are (almost) defined by an algorithm; thus, once we are able to effectively enumerate the elements of H , we can effectively produce the

relations $a^i g_{\rho(i)} = b^{\tau(i)} c^{\sigma(\tau(i))}$ of S . The relations of the presentation

$$S = \langle T, x, a, b, c; R, a^i g_{\rho(i)} = b^{\tau(i)} c^{\sigma(\tau(i))}, i \in \mathbf{Z} - \{0\} \rangle$$

are therefore recursively enumerable. This proves Theorem A(b). Theorem A(b), together with the well-known result of Kusnetsov [4, p. 191], gives a new proof of the following result of R. J. Thompson [8], which is in turn a sharpened version of a result of W. W. Boone and G. Higman [2].

COROLLARY B. *A finitely generated group G has solvable word problem if and only if it is a subgroup of a recursively presented finitely generated simple group.*

We close with three remarks.

1. Since G is a free factor of one of the factors of the amalgamated free product S , the embedding $G \rightarrow S$ has the following additional property: If the elements g_i and g_j of G are not conjugate in G , then they are not conjugate in S . Use Theorem 4.6 in [5]. It shares this property with the embedding constructed by R. J. Thompson [8].

2: The group S is an amalgamated free product, we have therefore control over the torsion elements of S . They are the conjugates of the torsion elements of G . Especially, if G is torsionfree, then S is torsionfree.

3. If G is the trivial group, then $H = G * \langle x \rangle$ is infinite cyclic and

$$S = \langle x, a, b, c; a^i x^{\rho(i)} = b^{\tau(i)} c^{\sigma(\tau(i))} \rangle.$$

This is the situation studied in [1] and [6].

REFERENCES

1. R. Camm, *Simple free products*, J. London Math. Soc. **28** (1953), 66–76.
2. W. W. Boone and G. Higman, *An algebraic characterization of the solvability of the word problem*, J. Austral. Math. Soc. **18** (1974), 41–53.
3. A. P. Goryushkin, *Imbedding of countable groups in two-generator groups*, Mat. Zametki **16** (1974), 231–235.
4. R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer-Verlag, Heidelberg, 1977.
5. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Wiley, New York, 1966.
6. D. Meier, *A note on simple free products*, Houston J. Math. **9** (1983), 501–504.
7. P. E. Schupp, *Embeddings into simple groups*, J. London Math. Soc. **13** (1976), 90–94.
8. R. J. Thompson, *Embeddings into finitely generated simple groups which preserve the word problem*, Word Problems. II, North-Holland, Amsterdam, 1980, pp. 401–441.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ALBERTA, EDMONTON, ALBERTA, T6G 2G1, CANADA

Current address: Pilgerweg 1, 8044 Zürich, Switzerland