Math. Proc. Camb. Phil. Soc. (2006), **141**, 57
doi:10.1017/S0305004106009236 *Printed in the United Kingdom*

Subsemigroups of virtually free groups: finite Malcev presentations and testing for freeness

By ALAN J. CAIN,† EDMUND F. ROBERTSON and NIK RUŠKUC‡

School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS.

e-mail: alanc, edmund, nik@mcs.st-andrews.ac.uk

(*Received* 5 *July* 2004; *revised* 2 *March* 2005)

Abstract

This paper shows that, given a finite subset X of a finitely generated virtually free group F, the freeness of the subsemigroup of F generated by X can be tested algorithmically. (A group is virtually free if it contains a free subgroup of finite index.) It is then shown that every finitely generated subsemigroup of F has a finite Malcev presentation (a type of semigroup presentation which can be used to define any semigroup that embeds in a group), and that such a presentation can be effectively found from any finite generating set.

1. *Introduction*

The purpose of this paper is to study certain combinatorial and computational properties of finitely generated subsemigroups of finitely generated virtually free groups.

Let F be a finitely generated virtually free group. Let $X \subseteq F$ be finite. Let Z be a new alphabet in one-to-one correspondence $\phi: Z \to X$ with X. Let Z^{-1} be a set in bijection with Z under the involution $z \mapsto z^{-1}$; this involution is extended in the natural way to an anti-isomorphism from Z^* to $(Z^{-1})^*$. Extend ϕ to a homomorphism $\phi: Z^* \to \langle X \rangle$. Let

$$L(X) = \{uv^{-1} : u \in Z^+, v \in Z^*, u\phi = v\phi, u, v \text{ have no common suffix}\}.$$

The following theorem, proved in Section 2, is the principal technical result of the paper:

Theorem 1. *For any finite subset X of a virtually free group F, the language $L(X)$ is context-free, and a pushdown automaton recognizing $L(X)$ can be effectively constructed.*

In the remainder of the paper, two consequences of Theorem 1 are proved.

There are several well-known algorithms to determine whether a finitely generated subsemigroup of a given free monoid is free; two examples are due to Spehner [**14**] and Sardinas and Patterson [**13**]. Of course, a subsemigroup of a free group may be considerably more complex than those of a free monoid. Section 3 considers the

† Work supported by the Carnegie Trust for the Universities of Scotland.
‡ Partial financial support from INTAS 99/1224.

freeness of subsemigroups of free groups and more generally of virtually free groups, and contains the following result:

THEOREM 2. *There is an algorithm that, given a finite subset X of a virtually free group F, determines whether the subsemigroup of F generated by X is free.*

Although the above result generalizes those of [**13**, **14**], the proof uses a new methodology based on the properties of context-free languages.

A Malcev presentation is a particular species of semigroup presentation which can be used to define any semigroup that can be embedded in a group. Spehner [**16**] shows that every finitely generated subsemigroup of a free monoid has a finite Malcev presentation. Section 4 again uses the theory of context-free languages to strengthen this result to subsemigroups of free and virtually free groups:

THEOREM 3. *Every finitely generated subsemigroup of a virtually free group has a finite Malcev presentation. Moreover, such a presentation can be effectively found from any given finite generating set.*

Finitely generated subsemigroups of free groups need not be finitely presented. Markov [**11**, section III] gives an algorithm that takes a finite subset of a free semigroup and determines whether the subsemigroup it generates is finitely presented. Spehner [**15**, proposition 2·7 and theorem 2·14] gives an analogous condition for finitely generated submonoids of a free monoid. A natural question is whether there is an analogous algorithm for finitely generated subsemigroups of a free or virtually free group. At present, no such algorithm is known.

2. $L(X)$ *is context-free*

Facts from formal language theory will be stated as they are required; the reader is referred to [**7**] for proofs.

The word problem of a group G with respect to a generating set X is the set of words over $X \cup X^{-1}$ that represent the identity element of G. Muller and Schupp [**12**, lemma 3] proved that the word problem of a finitely generated virtually free group is a context-free language. Combining lemmas 2 and 3 of [**12**] and observing that all constructions used in their proofs are effective yields the following result:

PROPOSITION 2·1. *Any finitely generated subgroup of a finitely generated virtually free group has context-free word problem, and a pushdown automaton recognizing the word problem of the subgroup can be effectively found from a finite generating set.*

Recall the definition of ϕ as a bijection from the new alphabet Z to X. Extend ϕ to a homomorphism from $(Z \cup Z^{-1})^*$ to the subgroup of F generated by X by letting $(z^{-1})\phi = (z\phi)^{-1}$ for $z \in Z$.

THEOREM 1. *For any finite subset X of a virtually free group F, the language*

$$L(X) = \{uv^{-1} : u \in Z^+, v \in Z^*, u\phi = v\phi, u, v \text{ have no common suffix}\}$$

is context-free, and a pushdown automaton recognizing $L(X)$ can be effectively constructed.

Proof. The language

$$R = Z^+(Z^{-1})^* - \left[\bigcup_{z\in Z} Z^* z z^{-1} (Z^{-1})^*\right]$$

is clearly regular [**7**, chapter 2 and theorem 3·2]. The language

$$W(X) = \{w \in (Z \cup Z^{-1})^* : w\phi = 1_F\}$$

– which is the word problem for the subgroup of F generated by X – is context-free by Proposition 2·1. The intersection of a context-free language and a regular language is again context-free [**7**, theorem 6·5]. Hence $W(X) \cap R$ is context-free. Furthermore, $L(X) = W(X) \cap R$, because

$$\begin{aligned} uv^{-1} \in W(X) \cap R &\\ &\iff u \in Z^+, v \in Z^*, (uv^{-1})\phi = 1_F, uv^{-1} \text{ does not} \\ &\qquad\qquad \text{include any } zz^{-1} \text{ as a subword} \\ &\iff u \in Z^+, v \in Z^*, u\phi = v\phi, u \text{ and } v \text{ have no common suffix} \\ &\iff uv^{-1} \in L(X). \end{aligned}$$

So $L(X)$ is a context-free language. Observing that all the constructions are effective gives the result.

3. *An algorithm to determine freeness*

Proposition 3·1. *There is an algorithm that, given a finite subset X of a virtually free group F, determines whether the subsemigroup of F generated by X is free on X.*

Proof. Let S be the subsemigroup generated by X. Suppose that S were not free on X. Then some non-trivial relation would hold: there would be some $u, v \in Z^+$ with $u \neq v$ such that $u\phi = v\phi$. Without loss of generality, assume $|u| \geqslant |v|$. Suppose $u = u's$, $v = v's$, where $s \in Z^*$ is a common suffix of u and v of maximum length, and $u' \in Z^+, v' \in Z^*$. (Since this is a non-trivial relation, at most one of u' and v' can be the empty word ε and the length assumption shows that $u' \neq \varepsilon$.) Then $u'\phi = v'\phi$, since S is a subsemigroup of a group and therefore cancellative, and $u'(v')^{-1}$ cannot contain a subword zz^{-1}. Therefore, the language $L(X)$ would be non-empty. Conversely, if S is free on X there could be no such u, v and therefore $L(X)$ must be empty.

The ability to test the emptiness of $L(X)$ is therefore equivalent to testing the freeness of S on X. There is a known algorithm that takes a context-free grammar and tests whether the language it defines is empty [**7**, theorem 6·6]. Since a pushdown automaton can be converted to a context-free grammar [**7**, section 5·3], the result follows from Theorem 1.

In a free semigroup A^+, the generating set A is contained in every generating set. Hence A^+ is only free on A. Thus, if the subsemigroup S of F generated by X is free on some generating set Y, then it must be true that $Y \subseteq X$. There are only a finite number of subsets Y of X. If it is possible to determine which of these subsets generate S, then the algorithm of Proposition 3·1 can be applied to each one. The subsemigroup S will then be free if and only if some subset Y of X generates S and the algorithm finds that the subsemigroup S is free on Y.

Let $Y \subseteq X$ and let T be the subsemigroup generated by Y. Clearly, $T \subseteq S$ since $Y \subseteq X$. Answering the question of whether $S = T$ reduces to determining whether $X \subseteq T$.

For $x \in X$ and $Y \subseteq X$, let Z_Y be the subset of Z mapped onto Y by ϕ and let $z_x \in Z$ be such that $z_x\phi = x$. Let $M(x, Y)$ be the regular language $z_x((Z_Y)^{-1})^*$.

LEMMA 3·2. *An element $x \in X$ is in T if and only if $L(X) \bigcap M(x, Y)$ is non-empty.*

Proof. Suppose $x \in T$. Then x can be expressed as a product $y_1 \cdots y_l$ of elements of Y. So there exists $w \in Z_Y^*$ such that $z_x\phi = w\phi$. Therefore $(z_x w^{-1})\phi = 1_F$ and so $z_x w^{-1} \in L(X) \bigcap M(x, Y)$.

Conversely, if $L(X) \bigcap M(x, Y) \neq \varnothing$, then there exists $w \in Z_Y^*$ such that $z_x\phi = w\phi$, so $x \in T$.

The language $L(X) \bigcap M(x, Y)$ is context-free, and a pushdown automaton recognizing it can be effectively constructed. The emptiness of $L(X) \bigcap M(x, Y)$, and so the question of whether $S = T$, can therefore be decided. The discussion following Proposition 3·1 gives:

THEOREM 2. *There is an algorithm that, given a finite subset X of a virtually free group F, determines whether the subsemigroup of F generated by X is free.*

4. *Finite Malcev presentations*

Malcev presentations were introduced by Spehner [**15**], though they are based on Malcev's necessary and sufficient condition for the embeddability of a semigroup in a group [**9**, **10**]. (Details of the embeddability condition can also be found in [**4**, chapter 12].) The necessary definitions regarding Malcev presentations are given below.

Definition 4·1. Let T be any semigroup. A congruence σ on T is a *Malcev congruence* if T/σ is embeddable in a group.

If $\{\sigma_i : i \in I\}$ is a set of Malcev congruences on T, then so is $\sigma = \bigcap_{i \in I} \sigma_i$. This is true because T/σ_i embeds in a group G_i for each $i \in I$, so T/σ embeds in $\prod_{i \in I} T/\sigma_i$, which in turn embeds in $\prod_{i \in I} G_i$. The following definition therefore makes sense.

Definition 4·2. Let Z^+ be a free semigroup; let $\rho \subset Z^+ \times Z^+$ be any binary relation on Z^+. Let σ be the smallest Malcev congruence containing ρ – namely,

$$\sigma = \bigcap \left\{ \tau : \tau \supseteq \rho, \tau \text{ is a Malcev congruence on } Z^+ \right\}.$$

Then $\langle Z \mid \rho \rangle$ is a *Malcev presentation* for [any semigroup isomorphic to] Z^+/σ. If both A and ρ are finite, the the Malcev presentation $\langle A \mid \rho \rangle$ is said to be finite.

Fix Z^+, ρ and σ as in the last definition and let $T = Z^+/\sigma$. Were $\langle Z \mid \rho \rangle$ an 'ordinary' semigroup presentation, two words $u, v \in Z^+$ would represent the same element of T if and only if there were a sequence

$$u = u_0 \to u_1 \to \ldots \to u_n = v \tag{4·1}$$

with $n \geqslant 0$, where, for each $i \in \{0, \ldots, n-1\}$, there exist $p_i, q_i, q_i', r_i \in Z^*$ such that $u_i = p_i q_i r_i$, $u_{i+1} = p_i q_i' r_i$, and $(q_i, q_i') \in \rho$ or $(q_i', q_i) \in \rho$. However, in dealing with a Malcev presentation, the fact that the semigroup in question must be embeddable in a group lends greater flexibility.

Let $Z^{\mathsf{L}}, Z^{\mathsf{R}}$ be two sets in bijection with Z under the mappings $z \mapsto z^{\mathsf{L}}$, $z \mapsto z^{\mathsf{R}}$, respectively, with $Z, Z^{\mathsf{L}}, Z^{\mathsf{R}}$ being pairwise disjoint. Two words in the Malcev presentation $\langle Z \mid \rho \rangle$ represent the same element of T if and only if there is a sequence (4·1) where, for each $i \in \{0, \ldots, n-1\}$, there exist $p_i \in (Z \cup Z^{\mathsf{L}})^*$, $r_i \in (Z \cup Z^{\mathsf{R}})^*$, $q_i, q_i' \in Z^*$, and $z \in Z$ such that either:

(i) $u_i = p_i q_i r_i$, $u_{i+1} = p_i q_i' r_i$, and $(q_i, q_i') \in \rho$ or $(q_i', q_i) \in \rho$;
(ii) $u_i = p_i r_i$, $u_{i+1} = p_i z^{\mathsf{L}} z r_i$;
(iii) $u_i = p_i r_i$, $u_{i+1} = p_i z z^{\mathsf{R}} r_i$;
(iv) $u_i = p_i z^{\mathsf{L}} z r_i$, $u_{i+1} = p_i r_i$; or
(v) $u_i = p_i z z^{\mathsf{R}} r_i$, $u_{i+1} = p_i r_i$.

The restriction on the letters that can appear in p_i and r_i simply means that no changes can be made to the left of a z^{L} or the right of a z^{R}. Such a sequence is called a *proper Malcev chain* from u to v, and it is said that (u, v) is a *Malcev consequence* of ρ. The insertion or deletion of $z^{\mathsf{L}} z$ or $z z^{\mathsf{R}}$ – transformations (ii)–(v) above – corresponds to the insertion or deletion of a generator of T and its inverse in a group in which T embeds.

(The definition of a 'Malcev chain' – which also links words representing the same element of T – is actually more complex than that of a 'proper Malcev chain' given above. A Malcev chain does not have the restriction on letters that can appear in the words p_i and r_i: instead insertions and deletions of $z^{\mathsf{L}} z$ or $z z^{\mathsf{R}}$ must obey certain rules [**16**, definition 2·3]. However, these rules follow as consequences of the restrictions on p_i and r_i. Every proper Malcev chain is thus a Malcev chain. Therefore, for brevity, the word 'proper' is omitted henceforth.)

It is clear that any set of relations $\mathcal{P} \subseteq Z^+ \times Z^+$ that are Malcev consequences of ρ (and thus known to hold in T) may be used instead of relations from ρ in a Malcev chain from u to v; (u, v) is then said to be a Malcev consequence of the relations in $\mathcal{P}$.

Spehner [**16**] shows that the insertion and deletion of $z^{\mathsf{L}} z$ and $z z^{\mathsf{R}}$ can be extended to words. Let $w = z_1 \cdots z_k \in Z^*$, with $z_i \in Z$, and define $w^{\mathsf{L}} = z_k^{\mathsf{L}} \cdots z_1^{\mathsf{L}}$ and $w^{\mathsf{R}} = z_k^{\mathsf{R}} \cdots z_1^{\mathsf{R}}$.

Lemma 4·3 ([**16**, proof of lemma 2·5]). *Let $u \in (Z \cup Z^{\mathsf{L}})^+$, $v \in (Z \cup Z^{\mathsf{R}})^+$. Then there is a valid chain of insertions that lead from uv to $uw^{\mathsf{L}}wv$ and from uv to $uww^{\mathsf{R}}v$ and a valid chain of deletions that lead from $uw^{\mathsf{L}}wv$ to uv and from $uww^{\mathsf{R}}v$ to uv.*

Proof. The chain

$$uv \to u z_k^{\mathsf{L}} z_k v \to u z_k^{\mathsf{L}} z_{k-1}^{\mathsf{L}} z_{k-1} z_k v \to \ldots \to u z_k^{\mathsf{L}} \cdots z_1^{\mathsf{L}} z_1 \cdots z_k v = u w^{\mathsf{L}} w v.$$

shows how to insert $w^{\mathsf{L}} w$; the reverse chain shows deletion. Insertion and deletion of $w w^{\mathsf{R}}$ can be proved similarly.

Theorem 3. *Every finitely generated subsemigroup of a virtually free group has a finite Malcev presentation. Moreover, such a presentation can be effectively found from any given finite generating set.*

Proof. Let F be a virtually free group; let X be a finite subset of F; let S be the subsemigroup of F generated by X. Observe that S has an ordinary presentation $\langle Z \mid \mathcal{R} \rangle$ in terms of the generating set X, where

$$\mathcal{R} = \{(u, v) : u \in Z^+, v \in Z^*, uv^{-1} \in L(X)\}.$$

This presentation is finite if and only if S is free on X. Assume therefore that S is not free on X, so that $\mathcal{R}$ is infinite and, in particular, non-empty.

The strategy is to define an ordering on $\mathcal{R}$ and show that all except a finite number of elements of $\mathcal{R}$ are Malcev consequences of preceding elements in that order.

Let $\Gamma = (N, Z \cup Z^{-1}, P, O)$ be a context-free grammar that generates $L(X)$. The relevant definitions regarding context-free grammars are summarized: for further details, the reader is referred to [**7**, chapter 4].

In the grammar Γ, N is a finite alphabet of *non-terminals* or *variables*; $Z \cup Z^{-1}$ is the set of *terminals* – the alphabet of the language generated; $P \subseteq N \times (N \cup Z \cup Z^{-1})^*$ is a finite set of *productions*, denoted by $M \to \alpha$ for $M \in N$ and $\alpha \in (N \cup Z \cup Z^{-1})^*$; $O \in N$ is the distinguished *start symbol*.

If $M \to \alpha$ is a production, $\beta, \gamma \in (N \cup Z \cup Z^{-1})^*$, then it is said that $\beta M \gamma$ *directly derives* $\beta\alpha\gamma$ and this relation is denoted $\beta M \gamma \Rightarrow \beta\alpha\gamma$. The transitive closure of the relation $\Rightarrow$ is denoted by $\overset{*}{\Rightarrow}$. If $\beta \overset{*}{\Rightarrow} \gamma$ then it is said that β *derives* γ. A word $w \in (Z \cup Z^{-1})^*$ is in the language generated by Γ – namely $L(X)$ – if $O \overset{*}{\Rightarrow} w$ [**7**, section 4·2].

A *derivation tree* (or *parse tree*) is a tree whose internal vertices are labelled by non-terminals and whose leaves are labelled by terminals. In particular, the root is labelled by O. If an internal vertex is labelled by $M \in N$, then its children are labelled from left to right by the letters of α, where $M \to \alpha$ is a production. Reading the leaves from left to right gives a word in $L(X)$, and each word in this language possesses at least one derivation tree [**7**, section 4·3]. For the purposes of this paper, a path in a derivation tree from O to a terminal is referred to as a *derivation path*.

Let T be a derivation tree of a word in $L(X)$. Define

$$n(T) = \text{number internal vertices of } T.$$

For $w \in L(X)$, define

$$n(w) = \min\{n(T) : T \text{ is a derivation tree for } w\}.$$

It is now possible to define an order on $\mathcal{R}$ directly, but for convenience later in the proof, the ordering will be defined on $L(X)$ first of all, then switched to $\mathcal{R}$ in a natural manner.

Let $w_1, w_2 \in L(X)$. Define

$$w_1 \prec w_2 \iff n(w_1) < n(w_2).$$

For $(u_1, v_1), (u_2, v_2) \in \mathcal{R}$, let

$$(u_1, v_1) \prec (u_2, v_2) \iff u_1 v_1^{-1} \prec u_2 v_2^{-1}.$$

Let K be the subset of $L(X)$ consisting of all words that have a derivation tree in which no derivation path contains the same non-terminal more than twice. The set of such derivation trees is finite, since the lengths of their derivation paths are bounded by $2|N|$. Therefore K is finite. Let

$$\mathcal{Q} = \{(u, v) \in \mathcal{R} : uv^{-1} \in K\}.$$

It is clear that $\mathcal{Q}$ is finite. This set will form the finite set mentioned above: all relations in $\mathcal{R} - \mathcal{Q}$ will be shown to be a Malcev consequences of $\prec$-preceding elements of $\mathcal{R}$.

Let $(u, v) \in \mathcal{R} - \mathcal{Q}$. Consider the derivation of uv^{-1} in Γ. Let T be a derivation tree for uv^{-1} with $n(T) = n(uv^{-1})$. At least one derivation path in T must have

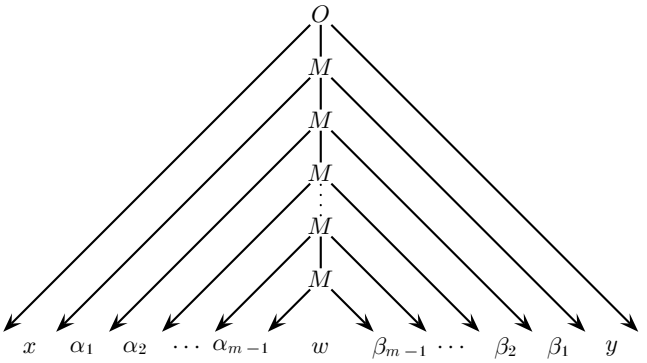

Fig. 1. Schematic of a derivation tree for $x\alpha_1 \cdots \alpha_{m-1} w \beta_{m-1} \cdots \beta_1 y$.

a non-terminal M appearing three times. Distinguish such a derivation path with $m \geqslant 3$ appearances of the non-terminal M. Suppose

$$uv^{-1} = x\alpha_1 \cdots \alpha_{m-1} w \beta_{m-1} \cdots \beta_1 y,$$

where x, y, w and the α_i and β_i (for $i \in \{1, \ldots, m-1\}$) are all words in $(Z \cup Z^{-1})^*$ such that

$$O \stackrel{*}{\Rightarrow} xMy, M \stackrel{*}{\Rightarrow} \alpha_i M \beta_i \text{ for each } i \in \{1, \ldots, m-1\}, M \stackrel{*}{\Rightarrow} w.$$

(See Figure 1 for a schematic illustration.)

Definition 4·4. The point in the word uv^{-1} where the subword $u \in Z^*$ ends and the subword $v^{-1} \in (Z^{-1})^*$ begins is called the *u–v^{-1} boundary*.

Lemma 4·5. *The u–v^{-1} boundary is in either x, w, or y (possibly at the end of x or w or the start of w or y).*

Proof. Suppose the u–v^{-1} boundary is in α_i for some $i \in \{1, \ldots, m-1\}$ (not at the start of α_1 or the end of α_{m-1}). Then there exist $s, t \in Z^+$ such that $\alpha_1 \cdots \alpha_{m-1} = st^{-1}$. By pumping derivation from M, it can be seen that

$$L(X) \ni x(\alpha_1 \cdots \alpha_{m-1})^2 w (\beta_{m-1} \cdots \beta_1)^2 y = xst^{-1}st^{-1}w\beta_{m-1} \cdots \beta_1 \beta_{m-1} \cdots \beta_1 y,$$

which is a contradiction, because this word is not in $Z^+(Z^{-1})^*$. A similar contradiction arises should the u–v^{-1} boundary be in some β_i, thus proving the lemma.

The relation (u, v) therefore takes one of the following three forms:

(i) $(x\alpha_1 \cdots \alpha_{m-1} w', y^{-1}\beta_1^{-1} \cdots \beta_{m-1}^{-1} w'')$, where $w = w'(w'')^{-1}$, if the u–v^{-1} boundary is in w;

(ii) $(x\alpha_1 \cdots \alpha_{m-1} w \beta_{m-1} \cdots \beta_1 y', y'')$, where $y = y'(y'')^{-1}$, if the u–v^{-1} boundary is in y;

(iii) $(x', y^{-1}\beta_1^{-1} \cdots \beta_{m-1}^{-1} w^{-1} \alpha_{m-1}^{-1} \cdots \alpha_1^{-1} x'')$, where $x = x'(x'')^{-1}$, if the u–v^{-1} boundary is in x.

The second and third cases are almost symmetrical – only the possibility that v (and so also y'') could be the empty word makes the second case more general than the third. It shall therefore suffice to prove that, in cases (i) and (ii), (u, v) is a Malcev consequence of $\prec$-preceding elements.

Observe that in Γ, since $m > 2$, $O \overset{*}{\Rightarrow} xMy$, $M \overset{*}{\Rightarrow} \alpha_1 \cdots \alpha_{m-2} M \beta_{m-2} \cdots \beta_1$, $M \overset{*}{\Rightarrow} \alpha_{m-1} M \beta_{m-1}$ and $M \overset{*}{\Rightarrow} w$, and therefore

$$x\alpha_1 \cdots \alpha_{m-2} w \beta_{m-2} \cdots \beta_1 y,$$
$$x\alpha_{m-1} w \beta_{m-1} y, xwy \in L(X). \tag{4·2}$$

Furthermore, derivation trees with fewer than $n(uv^{-1}) = n(T)$ internal vertices exist for each of these words, as the following three derivations show:

$$O \overset{*}{\Rightarrow} xMy \overset{*}{\Rightarrow} x\alpha_1 \cdots \alpha_{m-2} M \beta_{m-2} \cdots \beta_1 y \overset{*}{\Rightarrow} x\alpha_1 \cdots \alpha_{m-2} w \beta_{m-2} \cdots \beta_1 y,$$
$$O \overset{*}{\Rightarrow} xMy \overset{*}{\Rightarrow} x\alpha_{m-1} M \beta_{m-1} y \overset{*}{\Rightarrow} x\alpha_{m-1} w \beta_{m-1} y,$$
$$O \overset{*}{\Rightarrow} xMy \overset{*}{\Rightarrow} xwy.$$

The words (4·2) therefore precede uv^{-1} in the $\prec$-ordering on $L(X)$.

(i) Firstly, observe that (4·2) implies that

$$(x\alpha_1 \cdots \alpha_{m-2} w', y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} w''),$$
$$(x\alpha_{m-1} w', y^{-1}\beta_{m-1}^{-1} w''), (xw', y^{-1}w'') \in \mathcal{R},$$

and that they each precede (u, v) in the $\prec$-ordering on $\mathcal{R}$. The following chain shows that (u, v) is a Malcev consequence of the given three elements:

$$\begin{aligned}
u &= x\alpha_1 \cdots \alpha_{m-1} w' \\
&\to x\alpha_1 \cdots \alpha_{m-2} w' (w')^{\mathsf{R}} \alpha_{m-1} w' \\
&\to y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} w'' (w')^{\mathsf{R}} \alpha_{m-1} w' \\
&\to y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} (y^{-1})^{\mathsf{L}} y^{-1} w'' (w')^{\mathsf{R}} \alpha_{m-1} w' \\
&\to y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} (y^{-1})^{\mathsf{L}} x w' (w')^{\mathsf{R}} \alpha_{m-1} w' \\
&\to y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} (y^{-1})^{\mathsf{L}} x \alpha_{m-1} w' \\
&\to y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} (y^{-1})^{\mathsf{L}} y^{-1} \beta_{m-1}^{-1} w'' \\
&\to y^{-1}\beta_1^{-1} \cdots \beta_{m-2}^{-1} \beta_{m-1}^{-1} w'' \\
&= v.
\end{aligned}$$

(ii) In this case, (4·2) means that

$$(x\alpha_1 \cdots \alpha_{m-2} w \beta_{m-2} \cdots \beta_1 y', y''),$$
$$(x\alpha_{m-1} w \beta_{m-1} y', y''), (xwy', y'') \in \mathcal{R}$$

and these precede (u, v) in the $\prec$-ordering on $\mathcal{R}$. Once again, the following chain shows that (u, v) is a Malcev consequence of these elements:

$$\begin{aligned}
u &= x\alpha_1 \cdots \alpha_{m-1} w \beta_{m-1} \cdots \beta_1 y' \\
&\to x\alpha_1 \cdots \alpha_{m-2} x^{\mathsf{L}} x \alpha_{m-1} w \beta_{m-1} \cdots \beta_1 y' \\
&\to x\alpha_1 \cdots \alpha_{m-2} x^{\mathsf{L}} x \alpha_{m-1} w \beta_{m-1} y' (y')^{\mathsf{R}} \beta_{m-2} \cdots \beta_1 y' \\
&\to x\alpha_1 \cdots \alpha_{m-2} x^{\mathsf{L}} y'' (y')^{\mathsf{R}} \beta_{m-2} \cdots \beta_1 y' \\
&\to x\alpha_1 \cdots \alpha_{m-2} x^{\mathsf{L}} x w y' (y')^{\mathsf{R}} \beta_{m-2} \cdots \beta_1 y' \\
&\to x\alpha_1 \cdots \alpha_{m-2} x^{\mathsf{L}} x w \beta_{m-2} \cdots \beta_1 y' \\
&\to x\alpha_1 \cdots \alpha_{m-2} w \beta_{m-2} \cdots \beta_1 y' \\
&\to y'' \\
&= v.
\end{aligned}$$

Therefore, (u, v) is a Malcev consequence of $\prec$-preceding elements, and this applies to all elements of $\mathcal{R} - \mathcal{Q}$. Hence the Malcev congruence generated by $\mathcal{Q}$ contains $\mathcal{R}$, and so $\langle Z \mid \mathcal{Q} \rangle$ is a finite Malcev presentation for S in terms of the generators X.

Furthermore, since a context-free grammar Γ can be constructed from a pushdown automaton recognizing $L(X)$, and every derivation tree in Γ with at most two repetitions of any non-terminal in each derivation path can be found, the set $\mathcal{Q}$ can be constructed effectively if such a pushdown automaton is known. Therefore, a finite Malcev presentation for S can be found effectively if a finite generating set for S is known.

5. *Further observations*

Spehner [**16**] draws a parallel between his proof that every finitely generated subsemigroup of a free semigroup has a finite Malcev presentation and the proof of the Ehrenfeucht conjecture for regular languages given by Culik and Salomaa [**5**]. The proof of Theorem 3 bears a resemblance to the proof of Albert, Culik, and Karhumäki [**1**] of the Ehrenfeucht conjecture in the case of context-free languages. In particular, the idea of examining repeated non-terminals in a derivation tree is drawn from that source. (The Ehrenfeucht conjecture has since been proved independently by Albert and Lawrence [**2**] and by Guba [**6**].)

Given that free groups are coherent, it is natural to ask whether every finitely generated subsemigroup of a coherent group has a finite Malcev presentation. (Recall that a group is coherent if all its finitely generated subgroups are finitely presented.) The authors have shown [**3**] that this is not the case: the free product of a free group and an abelian group – which is coherent by the Kurosh subgroup theorem (see [**8**, section IV.1], for example) – can contain finitely generated subsemigroups that do not admit finite Malcev presentations.

REFERENCES

[**1**] J. Albert, K. Culik, II and J. Karhumäki. Test sets for context free languages and algebraic systems of equations over a free monoid. *Inform. and Control* **52** (1982), no. 2, 172–186.

[**2**] M. H. Albert and J. Lawrence. A proof of Ehrenfeucht's conjecture. *Theoret. Comput. Sci.* **41** (1985), no. 1, 121–123.

[**3**] A. J. Cain, E. F. Robertson and N. Ruškuc. Subsemigroups of groups: presentations, Malcev presentations, and automatic structures. *J. Group Theory*, to appear.

[**4**] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups – Vol. II* (Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1967).

[**5**] K. Culik, II and A. Salomaa. On the decidability of homomorphism equivalence for languages. *J. Comput. System Sci.* **17** (1978), no. 2, 163–175.

[**6**] V. S. Guba. Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems. *Mat. Zametki* **40** (1986), no. 3, 321–324, 428.

[**7**] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages and Computation* (Addison-Wesley Publishing Co., 1979).

[**8**] R. C. Lyndon and P. E. Schupp. Combinatorial group theory. *Ergeb. Math. Grenzgeb.* vol. 89 (1977).

[**9**] A. Malcev. On the immersion of associative systems in groups. *Mat. Sbornik* **6** (1939), no. 48, 331–336. (In Russian.)

[**10**] A. Malcev. On the immersion of associative systems in groups II. *Mat. Sbornik* **8** (1940), no. 50, 251–264. (In Russian.)

[**11**] A. A. Markov. On finitely generated subsemigroups of a free semigroup. *Semigroup Forum* **3** (1971/72), no. 3, 251–258.

[**12**] D. E. Muller and P. E. Schupp. Groups, the theory of ends and context-free languages. *J. Comput. System Sci.* **26** (1983), no. 3, 295–310.

[**13**] A. A. Sardinas and C. W. Patterson. A necessary and sufficient condition for the unique decomposition of coded messages. *Institute of Radio Engineers International Convention Records* **8** (1953), 104–108.

[**14**] J.-C. Spehner. Quelques constructions et algorithmes relatifs aux sous-monoïdes d'un monoïde libre. *Semigroup Forum* **9** (1974/75), no. 4, 334–353.

[**15**] J.-C. Spehner. Présentations et présentations simplifiables d'un monoïde simplifiable. *Semigroup Forum* **14** (1977), no. 4, 295–329.

[**16**] J.-C. Spehner. Every finitely generated submonoid of a free monoid has a finite Malcev's presentation. *J. Pure Appl. Algebra* **58** (1989), no. 3, 279–287.