

MONOID PRESENTATIONS OF GROUPS BY FINITE SPECIAL STRING-REWRITING SYSTEMS *

DUNCAN W. PARKES^{1,2}, V. YU. SHAVRUKOV^{1,3}
AND RICHARD M. THOMAS¹

Abstract. We show that the class of groups which have monoid presentations by means of finite special $[\lambda]$ -confluent string-rewriting systems strictly contains the class of plain groups (the groups which are free products of a finitely generated free group and finitely many finite groups), and that any group which has an infinite cyclic central subgroup can be presented by such a string-rewriting system if and only if it is the direct product of an infinite cyclic group and a finite cyclic group.

Mathematics Subject Classification. 20E06, 20F05, 20F10, 68Q42.

1. INTRODUCTION

Several results have been proved giving algebraic characterizations of the groups which can be presented by certain classes of finite string-rewriting system: a general account of this subject may be found in [6]. Recall that a string-rewriting system is said to be special if every rule rewrites a string to the empty word. In [2], Cochet shows that a group has a presentation by a finite special confluent string-rewriting system if and only if it is the free product of finitely many (finite

Keywords and phrases. Group, monoid presentation, Cayley graph, special string-rewriting system, word problem.

* *The research of the second author was supported by EPSRC grant GR/L37175/01.*

¹ Department of Mathematics and Computer Science, University of Leicester, University Road, Leicester, LE1 7RH, England; e-mail: rmt@mcs.le.ac.uk

² *Current address:* School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, Scotland; e-mail: dparkes@mcs.st-and.ac.uk

³ *Current address:* IT-Universitetet i København, Glentevej 67, 2400 København NV, Denmark; e-mail: volodya@itu.dk

and infinite) cyclic groups. A string-rewriting system is said to be $[\lambda]$ -confluent if it is confluent on the Thue-congruence class containing the empty word. Madlener and Otto, in [6], prove that a group can be presented by a finite special string-rewriting system R which is $[\lambda]$ -confluent and which provides inverses of length one for every letter (that is, for every generator x there exists a generator y such that $xy \rightarrow \lambda$ and $yx \rightarrow \lambda$ are rules of R), if and only if it is a plain group (the free product of a finitely generated free group and finitely many finite groups).

There is at present no known algebraic characterization of the groups presented by finite special $[\lambda]$ -confluent string-rewriting systems which do not necessarily provide inverses of length one (the class $C_{\text{sp},1}$ from [6]). We shall show in Section 3 that this class strictly contains the class of plain groups (thereby answering a question of Madlener and Otto) and, in Section 4, that a group which has an infinite cyclic central subgroup has a presentation by a finite special $[\lambda]$ -confluent string-rewriting system if and only if it is the direct product of one finite and one infinite cyclic group (Th. 4.6). In Section 5 we give some further examples of groups which can be presented by finite special $[\lambda]$ -confluent string-rewriting systems.

2. PRELIMINARIES

In this section we recall some of the concepts we need from group theory and the theory of string-rewriting systems and fix notation. In general, definitions from group theory may be found in [5] or [7], and those from string-rewriting may be found in [1].

A set X , where each $x \in X$ represents an element of a group G , is said to be a *monoid generating set* for G if every element of G is represented by a word from X^* . The *word problem* $W_X(G)$ of G with respect to a monoid generating set X is the set of words in X^* which are equal to the identity in G . The *irreducible word problem* $I_X(G)$ of G with respect to a monoid generating set X is the subset of the word problem consisting of those non-empty words which have no non-empty proper subword which is equal to the identity.

We shall use the expression $v \equiv w$ to mean that the words v and w are identical as strings of symbols, and $v = w$ to mean that v and w represent the same element of the appropriate group. The length of the word w will be denoted by $|w|$, and $|w|_x$ will denote the number of occurrences of the symbol x in w . If $w \equiv uv$, then u is said to be a *prefix* of w , and v is said to be a *suffix* of w . We shall denote the *empty word* (the word of length zero) by λ .

Given a finite alphabet Σ , a *string-rewriting system* R over Σ is a set of rules $u \rightarrow v$, where u and v are in Σ^* . We shall only be interested in finite string-rewriting systems here.

We define the *reduction relation* \Rightarrow_R^* to be the reflexive transitive closure of \Rightarrow_R , where $w_1uw_2 \Rightarrow_R w_1vw_2$ if $w_1, w_2 \in \Sigma^*$ and $u \rightarrow v \in R$. If $w_1 \Rightarrow_R^* w_2$ then we say that w_2 is an (R) -*descendant* of w_1 . The transitive symmetric closure of \Rightarrow_R^* ,

written as \Leftrightarrow_R^* , is a monoid congruence and is called the *Thue congruence* of R . The congruence class of a word w is then denoted by $[w]$.

A string-rewriting system is said to be *special* if every rule is of the form $u \rightarrow \lambda$, for some $u \in \Sigma^+$. A string-rewriting system R over Σ is said to be $[\lambda]$ -confluent if, whenever $u, w_1, w_2 \in [\lambda]$, with $u \Rightarrow_R^* w_1$ and $u \Rightarrow_R^* w_2$, then there exists $v \in [\lambda]$ such that $w_1 \Rightarrow_R^* v$ and $w_2 \Rightarrow_R^* v$. A special string-rewriting system is $[\lambda]$ -confluent if $u \in [\lambda]$ implies that $u \Rightarrow_R^* \lambda$. For a special string-rewriting system R , a word u is called (R) -irreducible if u has no R -descendants other than u .

We say that string-rewriting system R over Σ *presents* the monoid

$$\langle \Sigma : \{u = v : (u \rightarrow v) \in R\} \rangle,$$

which is isomorphic to the monoid $\Sigma^* / \Leftrightarrow_R^*$. We are interested here in the situation where the monoid presented by R is a group.

When we wish to discover whether or not a group may be presented by a finite special $[\lambda]$ -confluent string-rewriting system, we shall not generally work with string-rewriting systems directly, but shall use instead the following observation, implicit in [6].

Proposition 2.1. *Let G be a group, and X a finite monoid generating set for G . Then G can be presented by a finite special $[\lambda]$ -confluent string-rewriting system over X if and only if it has finite irreducible word problem with respect to X .*

Proof. Let R be a finite special $[\lambda]$ -confluent string-rewriting system over X which presents G . If $w \in I = I_X(G)$ then, since $w \in W_X(G)$, there is a rule $u \rightarrow \lambda$ which can be applied to w . Now u is a non-empty subword of w which is equal to the identity, so $u \equiv w$. We have shown that, for any $w \in I$, there must be a rule $w \rightarrow \lambda$ in R . Since R has only finitely many rules, I must be finite.

Conversely, let G be a group with finite monoid generating set X such that $I = I_X(G)$ is finite. Then $\{w \rightarrow \lambda : w \in I\}$ is a finite special $[\lambda]$ -confluent string-rewriting system which presents G . \square

When we refer to the *Cayley graph* of a group we shall mean the right Cayley graph, that is, for a group G with monoid generating set X , the graph Γ whose vertices are the elements of G , and which has an edge labelled by $x \in X$ from vertex g_1 to vertex g_2 exactly when $g_1x = g_2$. For each vertex g of Γ , any word $w \in X^*$ labels a path starting at g . The path labelled by the word w is said to be *closed* if it starts and ends at the same vertex (closed paths are also known as *loops*) and *simple* if no non-empty proper subword of w labels a loop.

It is noted in [3] that a non-empty word w labels a simple loop in the Cayley graph of G with respect to X if and only if it is in the irreducible word problem of G with respect to X .

3. SPECIAL REWRITING FOR $C_\infty \times C_k$

We know from [6] that a group can be presented by a finite special $[\lambda]$ -confluent string-rewriting system which provides inverses of length one for each generator if and only if it is a plain group, but it is left open there as to whether or not this continues to be the case if the condition on inverses is dropped. Our task here is to give an example to show that this is not the case.

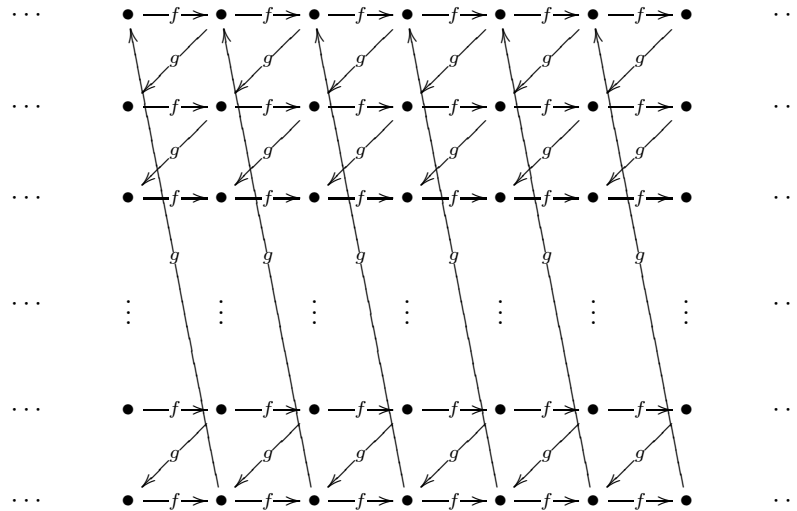


FIGURE 1. The Cayley graph of $C_\infty \times C_k = \langle f : \rangle \times \langle a : a^k \rangle$ with respect to the monoid generating set $\{f, g\}$, where $g = af^{-1}$.

Proposition 3.1. *Let G be the direct product of the infinite cyclic group and a finite cyclic group. Then G can be presented by a finite special $[\lambda]$ -confluent string-rewriting system, but G is not plain.*

Proof. Firstly, we note that G cannot be plain, since a group cannot be both a non-trivial direct product and a non-trivial free product: see for example [5], p. 177 or [7], Problem 4.1.22.

The standard group presentation for G is $\langle f : \rangle \times \langle a : a^k \rangle$. Let $X = \{f, g\}$, where $g = af^{-1}$. The Cayley graph of G with respect to X is shown in Figure 1. We claim that X is a monoid generating set for G with respect to which the irreducible word problem of G is finite.

Any element of G can be written in terms of the symbols f , f^{-1} and a . Since $f \in X$, $a = fg$ and $f^{-1} = f^{k-1}g^k$, we see that X is a monoid generating set for G .

A word w is in $W_X(G)$ if and only if it satisfies $|w|_f = |w|_g$ and $|w|_g \equiv 0 \pmod k$. Together these conditions give that $|w|_f = |w|_g = nk$, and $|w| = 2nk$, for some

$n \geq 0$. We shall show that if $n > 1$ then w cannot be in $I = I_X(G)$, so that I is just the set of words which contain exactly k instances of f and k instances of g , and is thus a finite set.

Assume that $w \equiv z_1 \dots z_{2nk} \in I$ and that $n > 1$. Consider the word $z_1 \dots z_{2k}$. This subword of w must contain different numbers of instances of f and g , or else it would be equal to the identity in G . We may therefore assume without loss of generality that it contains more instances of f than it does of g . Now suppose that, for some i , the subword $z_i \dots z_{i+2k-1}$ contains more instances of f than of g . The difference between $|z_i \dots z_{i+2k-1}|_f$ and $|z_{i+1} \dots z_{i+2k}|_f$ must be at most 1, and so $|z_{i+1} \dots z_{i+2k}|_f \geq k$. We cannot have $|z_{i+1} \dots z_{i+2k}|_f = k$ because this would mean that $z_{i+1} \dots z_{i+2k}$ is equal to the identity; so $|z_{i+1} \dots z_{i+2k}|_f > k$. By induction we see that every subword of w consisting of $2k$ consecutive symbols contains more instances of f than it does instances of g . Since $|w|$ is a multiple of $2k$, we may consider w as the concatenation of n words of $2k$ symbols, and it is clear that $|w|_f > |w|_g$, a contradiction. \square

4. INFINITE CYCLIC CENTRAL SUBGROUPS

Having demonstrated that the class of groups which may be presented by finite special $[\lambda]$ -confluent string-rewriting systems strictly contains the plain groups, the obvious question is:

Question 4.1. Which groups can be presented by finite special $[\lambda]$ -confluent string-rewriting systems?

We shall answer this question for groups which have an infinite cyclic central subgroup. We start with two lemmas.

Lemma 4.2. *Let X be a finite monoid generating set for the group G . Suppose there are a finite set $S \subseteq G$, an element $g \in G$, and an infinite set P of pairs of words over X such that, for all $(u_1, u_2) \in P$, both u_1 and u_2 have no non-empty subwords equal to the identity, $u_1 g u_2 \in S$, and $u_+ g u_- = 1$ implies $u_+ \equiv u_- \equiv \lambda$ whenever u_+ is a suffix of u_1 and u_- is a prefix of u_2 . Then $I_X(G)$ is infinite.*

Proof. For each $s \in S$, let the word \bar{v}_s represent some fixed path in the Cayley graph Γ of G connecting s to 1 so that $\bar{v}_s = s^{-1}$. Since S is finite, there is an integer B such that the length of each such path does not exceed B . Let $C = |v_g|$, where v_g is a word representing g .

Suppose $I_X(G)$ were finite. By Proposition 2.1 there is then a finite special $[\lambda]$ -confluent string-rewriting system R over X presenting G . Let M be larger than the length of the left hand side of any rule in R . Observe that an application of any R -rule to the label of any path in Γ corresponds to the removal from that path of a loop of length less than M .

Since P is infinite, there is a pair $(u_1, u_2) \in P$ with $|u_1 u_2| > M(B+C)$. Consider the word $u_1 v_g u_2 \bar{v}_s$, where $u_1 v_g u_2 = s \in S$ so that $u_1 v_g u_2 \bar{v}_s = 1$. As $(u_1, u_2) \in P$, the application of any R -rule to (any R -descendant of) the word $u_1 v_g u_2 \bar{v}_s$ must remove at least one edge of the loop $u_1 v_g u_2 \bar{v}_s$ outside the subpaths labelled by u_1

and u_2 . Therefore one reaches an R -irreducible descendant w of $u_1v_gu_2\bar{v}_s$ in at most $B + C$ steps. Hence,

$$|w| \geq |u_1v_gu_2\bar{v}_s| - M(B + C) \geq |u_1u_2| - M(B + C) > 0.$$

Since $w = u_1v_gu_2\bar{v}_s = 1$, this contradicts the $[\lambda]$ -confluence of R and completes the proof. \square

Lemma 4.2 has the following consequence:

Lemma 4.3. *Let X be a finite monoid generating set for the group G . Suppose there are a finite set $S \subseteq G$ and an infinite set U of words over X such that no $u \in U$ has a non-empty proper subword equal to the identity, and every $u \in U$ is equal in G to an element of S . Then $I_X(G)$ is infinite.*

Proof. We may clearly assume that no element of U is equal to the identity. Then Lemma 4.2 applies with $g = 1$ and $P = \{(\lambda, u) : u \in U\}$. \square

We may now characterize the groups which may be presented by finite special $[\lambda]$ -confluent string-rewriting systems amongst those groups which are split extensions with infinite cyclic quotient and finite kernel.

Proposition 4.4. *A group G which is of the form $H \rtimes F$, where H is a finite normal subgroup of G and F is an infinite cyclic subgroup, can be presented by a finite special $[\lambda]$ -confluent string-rewriting system if and only if $G = H \times F$ and H is cyclic.*

Proof. Proposition 3.1 tells us that the “if” part of the theorem is true.

To prove the “only if” direction, we shall assume that G is not of the form $H \times F$ for any finite cyclic group H , and deduce that G has infinite irreducible word problem with respect to any monoid generating set.

Let X be a finite monoid generating set for G . We may assume that there are no redundant elements in X , since if $I_X(G)$ is infinite, then adding more elements to X is certainly not going to make it finite.

Fix a generator f (not necessarily in X) of the infinite cyclic group F and let $\phi : G \rightarrow F$ be the natural projection of G onto F . We start by partitioning X into three sets, P , N , and Z , where $P = \{x \in X : x\phi = f^i \text{ and } i > 0\}$, $N = \{x \in X : x\phi = f^i \text{ and } i < 0\}$, and $Z = \{x \in X : x\phi = 1\} = X \cap H$. We must have $P \neq \emptyset$ and $N \neq \emptyset$ in order that we have in X^* both words which are equal to f and words which are equal to f^{-1} .

We shall split the proof that $I_X(G)$ is infinite into several cases.

CASE 1. $Z \neq \emptyset$.

Fix $a \in Z$, $x \in P$ and $y \in N$. We shall construct a sequence $(w_r : r \geq 0)$ of distinct words which satisfy the following conditions:

- (i) $w_r \in H \setminus \{1\}$;
- (ii) w_r has no non-empty proper subword which is equal to the identity;
- (iii) every x in w_r occurs to the left of the first y .

Let $m, n > 0$ be minimal such that $x^m y^n \in H$. We cannot have both $x^m y^n = 1$ and $x^m a y^n = 1$, since a would then be redundant. We may therefore choose w_0 to be either $x^m y^n$ or $x^m a y^n$ so that it satisfies condition (i). The minimality of m and n tells us that w_0 satisfies condition (ii), and it is clear that w_0 satisfies condition (iii).

Assume that we have constructed w_r which satisfies conditions (i), (ii) and (iii). We cannot have both $x^m w_r y^n = 1$ and $x^m w_r a y^n = 1$, so we may choose w_{r+1} to be $x^m w_r y^n$, if this is not the identity, and $x^m w_r a y^n$ otherwise, so that w_{r+1} satisfies condition (i). We need to check that w_{r+1} satisfies condition (ii). If $w_{r+1} \equiv x^m w_r y^n$ then (ii) for w_{r+1} is easily established by considering ϕ -images of subwords of w_{r+1} . If $w_{r+1} \equiv x^m w_r a y^n$, then we must have $x^m w_r y^n = 1$, and hence $y^n x^m w_r = 1$. The only non-empty subword of w_{r+1} which can be equal to the identity is $w_r a$, but if this is the case then $y^n x^m = y^n x^m w_r a = a$, and a is redundant. Condition (iii) for w_r , and the fact that all of the new instances of x are introduced on the left, and all of the new instances of y on the right, ensure that w_{r+1} satisfies condition (iii).

We have constructed an infinite sequence of words w_r of increasing length which are equal to elements of the finite group H and which have no non-empty subword equal to the identity, and we may therefore appeal to Lemma 4.3 to see that $I_X(G)$ is infinite.

CASE 2. $|P| = |N| = 1, Z = \emptyset$.

Let $P = \{x\}$ and $N = \{y\}$ so that $X = \{x, y\}$. If x and y commute, then G is the direct product of an infinite cyclic group and a finite cyclic group, so we may assume that they do not commute. Let $i > 0$ and $j < 0$ be such that $x\phi = f^i$ and $y\phi = f^j$.

If there is no $k \geq 0$ such that $y^{-1}xy^k$ is equal to a power of x then no element of the form $x^l y^{-1}xy^k$ with any integer l and $k \geq 0$ is equal to the identity. Elementary arithmetic involving i and j shows that for each $k \geq 0$ there exists an $l_k \geq 0$ satisfying $x^{l_k} y^{-1}xy^k \in \bigcup_{0 < r \leq i-j} f^r H$. Since $x^{l'} y^{-1} \neq 1 \neq y^{-1}xy^{k'}$ for all integers l', k' , Lemma 4.2 applies with $P = \{(x^{l_k}, xy^k) : k \geq 0\}$, $S = \bigcup_{0 < r \leq i-j} f^r H$, and $g = y^{-1}$ to establish that $I_X(G)$ is infinite.

We may therefore choose t that is smallest among $k \geq 0$ such that $y^{-1}xy^k$ is a power of x . We also fix s such that $y^{-1}xy^t = x^s$.

Observe that $t > 0$ lest y be a power of x , which would cause x and y to commute. If $t = 1$ then $y^{-1}xy = x^s$. By considering the ϕ -images of both sides, we have that $s = 1$ so that x and y commute. Therefore $t > 1$. Applying this consideration to the ϕ -images of $y^{-1}xy^t = x^s$, we have $s < 1$. Since x is not equal to any power of y , we cannot have $s = 0$. Thus $s < 0$.

We are going to apply Lemma 4.2 with

$$P = \{(x^{-sk}, (xy^{t-1})^k) : k \geq 0\}, \quad S = \{y^{-1}\}, \quad \text{and} \quad g = y^{-1}.$$

First, observe that by the definition of s and t we have $x^{-s}y^{-1}xy^{t-1} = y^{-1}$. From this it follows by induction on k that

$$x^{-sk}y^{-1}(xy^{t-1})^k = y^{-1} \in S.$$

Clearly, x^{-sk} has no non-empty subwords equal to the identity. We verify that neither does $(xy^{t-1})^k$. Any subword of $(xy^{t-1})^k$ that is not a string of y 's has the form $y^{n_1}(xy^{t-1})^mxy^{n_2}$ with $n_i, m \geq 0$. If such a word is equal to the identity then so is $(xy^{t-1})^mxy^n$, where $n = n_1 + n_2 \geq 0$. Observe that $m \neq 0$, for otherwise $xy^n = 1$ so x and y would have to commute. Since $xy^{t-1} = yx^sy^{-1}$, we have

$$(yx^sy^{-1})^mxy^n = 1.$$

Applying ϕ , we get

$$ism + i + jn = 0.$$

As $j < 0$ and $n \geq 0$, we have $jn \leq 0$, and therefore $i(sm + 1) \geq 0$. Next, $sm \geq -1$ because $i > 0$. In view of $s < 0 < m$, the only possibility for this to hold is if $s = -1$, $m = 1$, and $n = 0$. Hence $yx^{-1}y^{-1}x = 1$, which implies that x and y commute. Thus no non-empty subword of $(xy^{t-1})^k$ is equal to the identity. Observe that $m \neq 0$, for otherwise $xy^n = 1$ so x and y would have to commute. Finally, suppose that $u_+y^{-1}u_- = 1$, where u_+ is a suffix of x^{-sk} and u_- is a prefix of $(xy^{t-1})^k$. Note that u_- cannot be empty for otherwise $x^ly^{-1} = 1$ for some $l \geq 0$. Thus

$$x^ly^{-1}(xy^{t-1})^mxy^n = 1$$

for some $l, m \geq 0$ and $0 \leq n \leq t - 1$. Since $xy^{t-1} = yx^sy^{-1}$ we then have

$$1 = x^ly^{-1}(yx^sy^{-1})^mxy^n = x^{l+sm}y^{-1}xy^n,$$

and therefore $y^{-1}xy^n$ is equal to a power of x . Since $0 \leq n \leq t - 1$, this contradicts the minimality requirement on t . Therefore $u_+y^{-1}u_- \neq 1$. Thus all conditions of Lemma 4.2 on P , S , and g are met, and hence $I_X(G)$ is infinite.

CASE 3. $|P| = 1$, $|N| \geq 2$, $Z = \emptyset$.

Let $P = \{x\}$, with $x\phi = f^i$ and $i > 0$. We construct inductively a sequence $(w_r : r \geq 0)$ of words such that no prefix of w_r is equal to a negative power of x . Let w_0 be a single letter word consisting of an element of N which is not equal to a negative power of x . Such an element must exist, since if each element of N is equal to a power of x then G must be generated by the set $\{x, x^{-1}\}$, which clearly cannot be the case. Let w_{r+1} be $w_r y$ where y is an element of N such that $x^l w_r y \neq 1$ for all $l \geq 0$. Such a y must exist, since there are at least two elements in N , and if y_1 and y_2 are elements of N , and l_1 and l_2 are natural numbers, with $l_2 \geq l_1$, such that $x^{l_1} w_r y_1 = x^{l_2} w_r y_2 = 1$, then $y_1 x^{l_1} w_r = y_2 x^{l_2} w_r$, and thus $y_1 = y_2 x^{l_2 - l_1}$, and y_1 is redundant. There can therefore be only one element y' of N such that $x^l w_r y' = 1$ for some $l \geq 0$, and the other elements of N must be suitable candidates for y . Note that $w_r \in N^*$, so that w_r labels a simple path.

For each w_r , let $t_r \geq 0$ be minimal such that $(x^{t_r}w_r)\phi = f^j$ with $j \geq 0$. Clearly each word $x^{t_r}w_r$ labels a simple path, and for any $r \geq 0$ we have $x^{t_r}w_r \in f^kH$ with $i > k \geq 0$, so we may apply Lemma 4.3 with $S = \bigcup_{0 \leq k < i} f^kH$ to settle this case.

CASE 4. $|P| \geq 2, |N| = 1, Z = \emptyset$.

This case is similar to Case 3.

CASE 5. $|P| \geq 2, |N| \geq 2$.

We construct words w_r inductively as follows; each w_r will be of the form w_+w_- with $w_+ \in P^*$ and $w_- \in N^*$. Let $w_0 \equiv x$, for some $x \in P$. If $w_r\phi = f^i$ with $i \geq 0$, then let $w_{r+1} \equiv w_ry$ for some $y \in N$ such that w_ry has no suffix equal to 1. If $w_r\phi = f^i$ with $i < 0$, then let $w_{r+1} \equiv xw_r$ for some $x \in P$ such that xw_r has no prefix equal to 1. We must now check that we can do this. If y_1 and y_2 are distinct elements of N such that $vy_1 = 1$ for some suffix v of w_r , and $uvy_2 = 1$ for some suffix uv of w_r , then $y_1 = y_2u$, where $u \in P^*$, and y_1 is redundant. The situation is similar when we prefix w_r by an element of P .

We now have an infinite set $\{w_r : r \geq 0\}$ of words, none of which has a subword equal to the identity, and each of which is equal to an element of the finite set $S = \bigcup_{|l| \leq M} f^lH$, where M is minimal such that $X \subseteq \bigcup_{|l| \leq M} f^lH$. We may therefore apply Lemma 4.3.

This case completes the proof of Proposition 4.4. □

We shall need the following observation; for completeness we include a proof.

Lemma 4.5. *If G is a virtually free group containing an infinite cyclic central subgroup Z , then G is a semi-direct product $H \rtimes F$ where H is a finite normal subgroup of G and F is an infinite cyclic subgroup.*

Proof. By definition, G contains a free subgroup F of finite index. Since G is infinite, F is non-trivial.

If F is non-cyclic, then $Z(F) = 1$, so that $F \cap Z = 1$ (as $F \cap Z \leq Z(F)$). But then G contains the subgroup $F \times Z$, contradicting the fact that F has finite index in G . So F is infinite cyclic and then G is virtually cyclic.

By Theorems 5.1 and 5.4 of [4], G has a finite normal subgroup H such that G/H is isomorphic to C_∞ or to $C_2 * C_2$. In the latter case, G/H would have trivial centre, contradicting the fact that ZH/H must be an infinite central subgroup of G/H . So G/H is isomorphic to C_∞ .

Choose a to be an element of infinite order in G such that $G/H = \langle aH \rangle$; thus $G = \langle H, a \rangle$. Let $F = \langle a \rangle$, so that $G = HF$. Since F has no non-trivial finite subgroups, we have that $H \cap F = 1$ and so G is the semi-direct product $H \rtimes F$ as required. □

We are now in a position to prove the main result of this section:

Theorem 4.6. *A group G which has an infinite cyclic central subgroup can be presented by a finite special $[\lambda]$ -confluent string-rewriting system if and only if $G = H \times F$, where H is finite cyclic and F is infinite cyclic.*

Proof. A string-rewriting system is said to be *monadic* if every rule is of the form $u \rightarrow v$, where $|u| > |v|$, and $|v| \leq 1$. It is shown in [6] that the groups which can be presented by finite monadic $[\lambda]$ -confluent string-rewriting systems are exactly the finitely generated virtually free groups, so any group which can be presented by a finite special $[\lambda]$ -confluent string-rewriting system is certainly virtually free.

If G has an infinite cyclic central subgroup then, by Lemma 4.5, G is of the form $H \rtimes F$ where H is a finite normal subgroup of G and F is infinite cyclic. By Proposition 4.4, if G can be presented by a finite special $[\lambda]$ -confluent string-rewriting system, then G is the direct product of a finite and an infinite cyclic group.

The converse follows directly from Proposition 3.1. □

5. FURTHER EXAMPLES

In this last section we shall give several more examples of groups which may be presented by finite special $[\lambda]$ -confluent string-rewriting systems. The following example shows that there are non-abelian groups which are not plain and which can be presented by such a system.

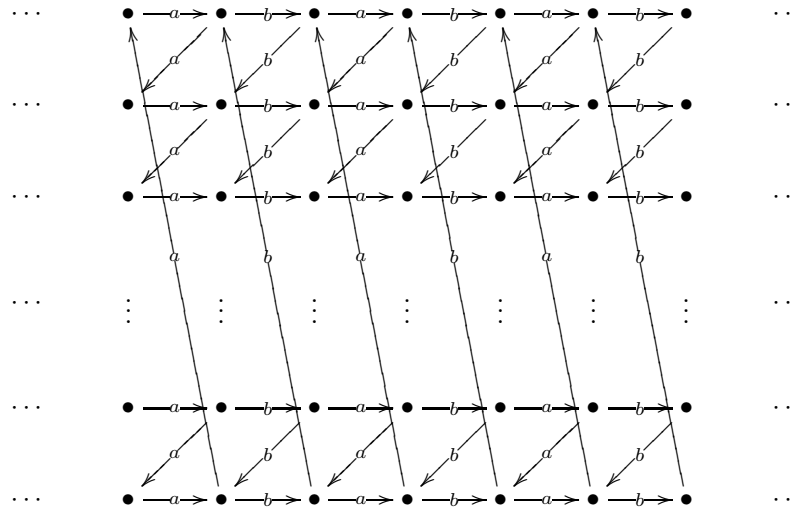


FIGURE 2. The Cayley graph of $C_{2k} *_{C_k} C_{2k} = \langle a, b : a^{2k}, a^2b^{-2} \rangle$ with respect to the monoid generating set $\{a, b\}$.

Example 5.1. The group $C_{2k} *_{C_k} C_{2k}$ can be presented by a finite special $[\lambda]$ -confluent string-rewriting system. If $k > 1$ this group is not plain.

Proof. The Cayley graph of $C_{2k} *_{C_k} C_{2k} = \langle a, b : a^{2k}, a^2b^{-2} \rangle$ with respect to the monoid generating set $\{a, b\}$ (pictured in Fig. 2) is isomorphic as an unlabelled graph to the Cayley graph of $C_\infty \times C_k = \langle f : \rangle \times \langle a : a^k \rangle$ with respect to $\{f, g\}$, where $g = af^{-1}$ (pictured in Fig. 1). The number of closed simple loops through any point in the two graphs must therefore be the same.

Clearly, $G_k = C_{2k} *_{C_k} C_{2k}$ is neither finite nor infinite cyclic. If $k > 1$, the group G_k has a non-trivial finite normal subgroup $C_k = \langle a^2 \rangle$. By [7] Problem 4.1.21(g), this implies that G_k cannot be a non-trivial free product, and hence G_k is not plain. \square

The next proposition gives us a way of constructing a new group which can be presented by a finite special $[\lambda]$ -confluent string-rewriting system from a group which has finite irreducible word problem with respect to a monoid generating set which contains a generator of order two.

Proposition 5.2. *Let G be a group with a subgroup $C = \langle c \rangle$ of order two, X a finite monoid generating set for G , and suppose that $I_X(G)$ is finite and that $c \in X$. Let D be a cyclic group $\langle d \rangle$ of order four and let $P = G *_C D$ (where c is identified with d^2). Then $I_{X \cup \{d\}}(P)$ is finite.*

Proof. Let the word w represent a simple loop in the Cayley graph of P with respect to $X \cup \{d\}$. If the only symbol in w is d then clearly $|w| \leq 4$. If w contains any letters other than d then we may assume, by taking a cyclic permutation of w if necessary, that the last letter of w is not d .

Now, if w contains a subword of the form dd then the word obtained by replacing an occurrence of dd by c in w still is (labels) a simple loop. Applying similar replacements to the resulting word we eventually arrive at a word v with length at least half that of w and such that v does not contain any subwords of the form dd .

If d occurs in v then v has the form $du_1du_2 \dots du_n$, where the u_i are non-empty words over X . By the normal form theorem for amalgamated free products at least one of u_i has to satisfy $u_i \in C$ because $v = 1$. As v is a simple loop, $u_i \neq 1$. Hence $u_i = c$ and therefore $du_id = 1$. Since v is simple, this implies $n = 1$. But $du_1 \neq 1$; thus d does not occur in v . So $v \in X^*$ and therefore $|v|$ is bounded, as is $|w| \leq 2|v|$. \square

We give one further set of examples of groups with finite irreducible word problem. While the generator c in the following example is redundant, its presence both brings the situation under the scope of Proposition 5.2 and simplifies the proof.

Example 5.3. The direct product $P = \langle c : c^2 \rangle \times \langle f_1, f_2, \dots, f_n : \rangle \cong C_2 \times F_n$ has finite irreducible word problem with respect to the monoid generating set $\{f_1, \dots, f_n, c, g_1, \dots, g_n\}$ where $g_i = f_i^{-1}c$.

Proof. Let w be (the label of) a simple loop in the Cayley graph of P . Replace each occurrence of $g_i f_i$ and $f_i g_i$ in w by c and call the resulting word v . Since $g_i f_i = f_i g_i = c$, v is a simple loop. Observe that v has no proper subwords of the form cc for otherwise it cannot be simple.

Consider the word \tilde{v} obtained by deleting from v all occurrences of c and replacing each occurrence of g_i by the symbol f_i^{-1} . Since $v \mapsto \tilde{v}$ corresponds to the projection $C_2 \times F_n \rightarrow F_n$ and $v = 1$, we must have $\tilde{v} = 1$. If \tilde{v} is empty then $v \equiv cc$ so $|w| \leq 2|v| = 4$. Otherwise \tilde{v} must contain a subword of the form $f_i f_i^{-1}$ or $f_i^{-1} f_i$. Since neither $g_i f_i$ nor $f_i g_i$ nor cc can occur in v as (proper) subwords, a subword of the form $f_i c g_i$ or $g_i c f_i$ does. However $f_i c g_i = g_i c f_i = 1$ which, in view of the simplicity of v implies $|v| \leq 3$ and thus $|w| \leq 6$. \square

Acknowledgements. The referees' helpful comments allowed us to considerably simplify our treatment of Case 2 in the proof of Proposition 4.4. The third author would like to thank Hilary Craig for all her help and encouragement.

REFERENCES

- [1] R.V. Book and F. Otto, *String-Rewriting Systems*. Texts and Monographs in Computer Science, Springer-Verlag (1993).
- [2] Y. Cochet, Church-Rosser congruences on free semigroups, in *Algebraic Theory of Semigroups*, edited by G. Pollák. Colloquia Mathematica Societatis János Bolyai **20**, North-Holland Publishing Co. (1979) 51–60.
- [3] R.H. Haring-Smith, Groups and simple languages. *Trans. Amer. Math. Soc.* **279** (1983) 337–356.
- [4] T. Herbst and R.M. Thomas, Group presentations, formal languages and characterizations of one-counter groups. *Theoret. Comput. Sci.* **112** (1993) 187–213.
- [5] R.C. Lyndon and P.E. Schupp, *Combinatorial Group Theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete **89**, Springer-Verlag (1977).
- [6] K. Madlener and F. Otto, About the descriptive power of certain classes of finite string-rewriting systems. *Theoret. Comput. Sci.* **67** (1989) 143–172.
- [7] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, 2nd edn. Dover (1976).

Communicated by V. Diekert.

Received September 19, 2000. Accepted March 19, 2004.