Bull. Aust. Math. Soc. **91** (2015), 426–434
doi:10.1017/S0004972715000015

ON GROUPS PRESENTED BY MONADIC REWRITING SYSTEMS WITH GENERATORS OF FINITE ORDER

ADAM PIGGOTT

(Received 19 November 2014; accepted 30 November 2014; first published online 6 March 2015)

Abstract

We prove that the groups presented by finite convergent monadic rewriting systems with generators of finite order are exactly the free products of finitely many finite groups, thereby confirming Gilman's conjecture in a special case. We also prove that the finite cyclic groups of order at least three are the only finite groups admitting a presentation by more than one finite convergent monadic rewriting system (up to relabelling), and these admit presentation by exactly two such rewriting systems.

2010 *Mathematics subject classification*: primary 20F10; secondary 20E99.

Keywords and phrases: group, monoid presentation, rewriting system, monadic system, plain group.

1. Introduction

A string rewriting system for a group G comprises a set Σ of monoid generators for the group and a set T of rewriting rules which proclaim that certain forbidden words in the generators may be replaced by other preferred words that spell the same group element. Viewed in this way, group elements are equivalence classes of words, with words equivalent if they are related in the reflexive, symmetric and transitive closure of the rewriting rules. Words with no forbidden subwords are natural candidates for normal forms. Under certain hypotheses one may understand how to apply rewriting rules to solve the word problem, and related problems, in G. A program exists to characterise algebraically those groups that admit presentation by various subclasses of string rewriting systems.

Finite convergent monadic rewriting systems provide a particularly fast solution to the word problem because in such systems rewriting rules are length reducing and each equivalence class of words contains a unique irreducible (normal form) which is necessarily the shortest word in the equivalence class. To compute the irreducible for an arbitrary word $w \in \Sigma^*$ one repeatedly replaces a forbidden subword by a single generator or the empty word until no forbidden subwords remain. The existence of

This work was partially supported by a grant from the Simons Foundation (#317466 to Adam Piggott).

such a simple and efficient solution to the word problem has significant algebraic consequences. For example, any group G admitting such a solution to the word problem is virtually free [5, Theorem 5].

In 1984 Gilman conjectured that a group G can be described by a finite convergent monadic rewriting system if and only if G is a plain group [6]. A group is plain if it can be decomposed as a free product of finitely many finite groups and finitely many infinite cyclic groups. The plain groups form a proper subclass of the finitely generated virtually free groups [5, Corollary 1]. Gilman's conjecture is known to hold in a number of special cases. In particular, it holds:

- if all forbidden words are to be replaced by the empty word [4] (see also [9]), in which case G decomposes as a free product of finitely many cyclic groups;
- if $|\Sigma| \leq 2$, in which case G is either a finite group or an infinite cyclic group or a free product of a finite cyclic group and a cyclic group [8, Theorem 3.4];
- if G is torsion-free, because a torsion-free virtually free group is necessarily a free group [10, Theorem 11];
- if G is virtually abelian [5];
- if every element of Σ has a group inverse in Σ [1]; or
- if all forbidden words have length two [2].

Despite this excellent progress, Gilman's conjecture in its full generality is yet to be confirmed or refuted. Perhaps this is surprising given the number of other known or suspected characterisations of the plain groups. The plain groups are exactly:

- the fundamental groups of finite graphs of groups in which vertex groups are finite and edge groups trivial [12];
- the groups admitting a finite group presentation with a simple reduced word problem [7];
- the groups presented by finite rewriting systems that are convergent on at least the equivalence class containing the empty word and in which all forbidden words are to be replaced by the empty word and every element of Σ has an inverse in Σ [9].

Shapiro [13] asked whether or not the plain groups are exactly the groups admitting a finite group generating set with respect to which the Cayley graph is geodetic.

In the present paper we prove that the groups presented by finite convergent monadic rewriting systems with generators of finite order are exactly the free products of finitely many finite groups, thereby confirming that Gilman's conjecture holds in another special case. We also prove that a normalised finite convergent monadic rewriting system (Σ, T) which presents a finite group G is either the nontrivial part of the multiplication table for G, or $|\Sigma| = |T| = 1$ and G is a finite cyclic group of order at least three. It is therefore easy to determine whether or not the group presented by a normalised finite convergent monadic rewriting system is finite.

https://doi.org/10.1017/S0004972715000015 Published online by Cambridge University Press

2. Rewriting systems

In this section we recall standard notation, vocabulary and well-known results concerning rewriting systems. A comprehensive account of the results mentioned can be found in [3].

For a nonempty set Σ, we write Σ^* for the set of finite words in symbols from Σ (including the empty word λ). Equipped with the operation of concatenation, Σ^* is the free monoid on Σ. We write $\equiv$ for equality in Σ^*. For all $w \in \Sigma^*$, we write $|w|$ for the length of w, and we write w^j to represent the concatenation of j copies of w.

A rewriting system (Σ, T) comprises a nonempty set Σ of *letters*, and a set $T \subseteq \Sigma^* \times \Sigma^*$ of *rewriting rules*. The set $\mathrm{dom}(T) := \{\ell \in \Sigma^* \mid (\ell, r) \in T \text{ for some } r \in \Sigma^*\}$ is the *domain* of the rewriting system. The elements of $\mathrm{dom}(T)$ are called *forbidden words*. For $u, v \in \Sigma^*$ we write $u \to v$ if there exist $x, y \in \Sigma^*$ and $(\ell, r) \in T$ such that $u \equiv x\ell y$ and $v \equiv xry$; that is, v is obtained from u by replacing a forbidden subword by the preferred word indicated by a rewriting rule. A word $u \in \Sigma^*$ is *reducible* if there exist $x, y \in \Sigma^*$ and $\ell \in \mathrm{dom}(T)$ such that $u \equiv x\ell y$, and *irreducible* otherwise. We write $\to^*$ for the reflexive and transitive closure of $\to$. We say that $v \in \Sigma^*$ is a *reduction* of u if $u \to^* v$. We write $\leftrightarrow^*$ for the symmetric closure of $\to^*$. It follows that $\leftrightarrow^*$ is an equivalence relation respecting concatenation, and $G = \Sigma^* / \leftrightarrow^*$ is a monoid with identity element represented by λ. We say that G is *presented by the rewriting system* (Σ, T). We are interested in the case where G is a group. This holds if and only if for all $a \in \Sigma$ there exists $w_a \in \Sigma^*$ such that $aw_a \leftrightarrow^* \lambda \leftrightarrow^* w_a a$.

A general rewriting system may be unwieldy, or ineffective for solving the word problem. Some addition properties are desirable. We say that (Σ, T) is: *terminating* (or *Noetherian*) if there is no infinite sequence of words $u_0, u_1, \ldots, \in \Sigma^*$ such that $u_i \to u_{i+1}$ for all i; *Church–Rosser* if whenever $u \leftrightarrow^* v$, there exists $x \in \Sigma^*$ such that $u \to^* x$ and $v \to^* x$; and *convergent* if it is both terminating and Church–Rosser. If (Σ, T) is a convergent rewriting system and $u, v \in \Sigma^*$, then rewriting rules can be used to demonstrate $u \leftrightarrow^* v$ whenever it holds. To also be able to demonstrate $u \not\leftrightarrow^* v$ whenever it holds, one needs a method to demonstrate $u \not\leftrightarrow^* v$ when u and v are irreducibles.

We say that (Σ, T) is: *finite* if Σ and T are finite sets; *monadic* if $r \in \Sigma \cup \{\lambda\}$ for all $(\ell, r) \in T$; and *normalised* (or *reduced*) if for all $(\ell, r) \in T$ we have that $|\ell| \geq 2$, no proper subword of ℓ is reducible, r is irreducible, and $(\ell, r') \in T$ implies $r \equiv r'$. It is well known that for any finite convergent rewriting system (Σ, T) presenting a monoid G, we may by an effective procedure construct a normalised finite convergent rewriting system (Σ', T') that presents an isomorphic monoid G'. Further, the construction is such that (Σ', T') is monadic if (Σ, T) is monadic. It follows that when it is the monoid G of interest, we do not lose generality by assuming that any finite convergent monadic rewriting system presenting G is normalised. In such a system, each reduction reduces the length of a word, and each irreducible $g \in \Sigma^*$ is the unique minimal length word representing the corresponding element of G. It is therefore easy to determine whether or not $u \leftrightarrow^* v$ for an arbitrary pair of words $u, v \in \Sigma^*$. For each $u \in \Sigma^*$ we write $\mathrm{irr}(u)$ for the irreducible that is $\leftrightarrow^*$-equivalent to u.

https://doi.org/10.1017/S0004972715000015 Published online by Cambridge University Press

3. Generators of finite order

We henceforth assume that (Σ, T) is a normalised finite convergent monadic rewriting system presenting a group G, and that every letter $a \in \Sigma$ has finite order. We write m_a for the order of a, and for each $1 \leq j < m_a$ we write a_j for the irreducible representing a^j. We write $\Sigma_a := \Sigma \cap \{a_1, \ldots, a_{m_a-1}\}$. We say that (Σ, T) *contains the nontrivial part of the multiplication table for* $\langle a \rangle$ if $\Sigma_a = \{a_1, \ldots, a_{m_a-1}\}$, from which it follows that $a_j a_k \in \mathrm{dom}(T)$ for all $1 \leq j, k < m_a$.

Our argument is structured as a sequence of lemmas. Our first two lemmas establish a dichotomy of behaviour for the cyclic subgroups generated by letters.

Lemma 3.1. *Suppose that* $a \in \Sigma$. *If* $\Sigma_a \neq \{a\}$, *then* $m_a > 2$ *and* (Σ, T) *contains the nontrivial part of the multiplication table for* $\langle a \rangle$.

Proof. Suppose that $\Sigma_a \neq \{a\}$. Then $m_a > 2$ and there exists an integer s such that $1 < s < m_a$ and $a_s \in \Sigma$.

Let p be the maximum integer such that $1 < p < m_a$ and $a_p \in \Sigma$. Suppose that $p < m_a - 1$. Since $a_1 a_p \leftrightarrow^* a_p a_1 \leftrightarrow^* a^{p+1}$, the words $a_1 a_p$ and $a_p a_1$ are distinct words representing the same group element. Because irreducibles are the unique words of minimal length representing the corresponding group element, $a_1 a_p$ and $a_p a_1$ are reducible. Thus $|a_{p+1}| \leq 1$. Because $p < m_a - 1$, $a_{p+1} \not\equiv \lambda$. Thus $a_{p+1} \in \Sigma$, contradicting the maximality of p. Thus $p = m_a - 1$.

Now let q be the minimum integer such that $1 < q < m_a$ and $a_q \in \Sigma$. Suppose that $q > 2$. Since $a_{m_a-1} a_q \leftrightarrow^* a_q a_{m_a-1} \leftrightarrow^* a^{q-1}$, the words $a_{m_a-1} a_q$ and $a_q a_{m_a-1}$ are distinct words representing the same group element. As above, it follows that $|a_{q-1}| \leq 1$. Because $q > 2$, $a_{q-1} \not\equiv \lambda$. Thus $a_{q-1} \in \Sigma$, contradicting the minimality of q. Thus $q = 2$. □

Lemma 3.2. *Suppose that* $a \in \Sigma$.

(1) *If* (Σ, T) *does not contain the nontrivial part of the multiplication table for* $\langle a \rangle$, *then* $\Sigma_a = \{a\}$, $m_a > 2$ *and* $a_j \equiv a^j$ *for all* $1 \leq j < m_a$.

(2) *We have* $a_j \in \Sigma_a^*$ *for all* $1 \leq j < m_a$; *in particular,* $\mathrm{irr}(a^{m_a-1}) \in \Sigma_a^*$.

(3) *If* $a^j \in \mathrm{dom}(T)$ *for some integer* $j \geq 3$, *then* $j = m_a$.

Proof. The first statement follows immediately from Lemma 3.1 and the observation that $\Sigma_a = \{a_1, \ldots, a_{m_a-1}\}$ when $m_a = 2$. The second statement follows immediately from the first. We now prove the third statement. Suppose that $\ell \equiv a^j \in \mathrm{dom}(T)$ for some integer $3 \leq j < m_a$. Because (Σ, T) is monadic, $\mathrm{irr}(a^j) \in \Sigma_a \cup \{\lambda\}$. Because (Σ, T) is normalised, every proper subword of ℓ is irreducible. Hence a^2 is irreducible. By (1), a^i is irreducible for all $1 \leq i < m_a$. Hence $j \geq m_a$. Because every proper subword of ℓ is irreducible, and a^{m_a} is reducible, $j = m_a$. □

The next two lemmas establish that forbidden words have a very structured form.

Lemma 3.3. *Suppose that* $\ell \in \mathrm{dom}(T)$.

(1) *If* $\ell \equiv uba^j$ *for some* $a \in \Sigma$, $1 \leq j < m_a$, $b \in \Sigma \backslash \{a\}$ *and* $u \in \Sigma^*$, *then* $u \equiv \lambda$.

(2) *If* $\ell \equiv a^j bu$ *for some* $a \in \Sigma$, $1 \leq j < m_a$, $b \in \Sigma \backslash \{a\}$ *and* $u \in \Sigma^*$, *then* $u \equiv \lambda$.

https://doi.org/10.1017/S0004972715000015 Published online by Cambridge University Press

Proof. We prove the first statement. The second is proved similarly. Suppose that $\ell \equiv uba^j$ for some for some $a \in \Sigma$, $1 \leq j < m_a$, $b \in \Sigma \backslash \{a\}$ and $u \in \Sigma^*$.

Consider first the case where $b \in \Sigma_a$. By Lemma 3.1, (Σ, T) contains the nontrivial part of the multiplication table for $\langle a \rangle$. Hence ba is reducible. Since every proper subword of ℓ is irreducible, $\ell \equiv ba$. Hence $u \equiv \lambda$ (and $j = 1$).

Now consider the case where $b \notin \Sigma_a$. By Lemma 3.2(2), $ub \not\equiv a_{m_a-j}$. Since ub is a proper subword of a word in the domain of T, it is irreducible. Because distinct irreducible words represent distinct group elements, $ub \not\leftrightarrow^* a_{m_a-j}$. It follows that $(uba^j, d) \in T$ for some $d \in \Sigma$. Now $ub = \mathrm{irr}(uba^j a_{m_a-j})$, but $uba^j a_{m_a-j} \rightarrow^* da_{m_a-j}$. By Lemma 3.2(2), $a_{m_a-j} \in (\Sigma_a)^*$. Since a_{m_a-j} is irreducible and $a_{m_a-j} \in (\Sigma_a)^*$ and (Σ, T) is monoidal, any reduction of da_{m_a-j} of length at least two has last letter from Σ_a. Since $b \notin \Sigma_a$ and ub is a reduction of da_{m_a-j}, $|ub| \leq 1$. Thus $u \equiv \lambda$. □

Lemma 3.4. *Suppose that $\ell \in \mathrm{dom}(T)$. If $|\ell| > 2$, then $\ell \equiv a^{m_a}$ and for some $a \in \Sigma$.*

Proof. We prove the contrapositive. Suppose that $\ell \not\equiv a^{m_a}$ for all $a \in \Sigma$. Consider first the case where $\ell \equiv a^j$ for some $a \in \Sigma$ and some positive integer j. By Lemma 3.2(3), $j = 2$ and hence $|\ell| = 2$. Now consider the case where no such a, j exist. It follows that $\ell \equiv uba^j$ for some $a \in \Sigma$, $1 \leq j < m_a$, $b \in \Sigma \backslash \{a\}$ and $u \in \Sigma^*$. By Lemma 3.3(1), $u \equiv \lambda$ and $\ell \equiv ba^j$. By Lemma 3.3(2), $j = 1$. Thus $\ell \equiv ba$ and $|\ell| = 2$. □

In light of Lemma 3.4, it is natural to construct a digraph $\Delta = \Delta(\Sigma, T)$ in which vertices correspond to letters and a directed edge from a to b (with $a \not\equiv b$) indicates that $ab \in \mathrm{dom}(T)$. Distinct connected components of Δ correspond to sub-rewriting systems of (Σ, T) that generate free factors of G. The remaining lemmas establish that the connected components of Δ are in fact complete digraphs.

Lemma 3.5. *Suppose that $a, b \in \Sigma$.*

(1) *If $xb \in \mathrm{dom}(T)$ for some $x \in \Sigma_a$, then $ub \in \mathrm{dom}(T)$ for all $u \in \Sigma_a$.*
(2) *If $ay \in \mathrm{dom}(T)$ for some $y \in \Sigma_b$, then $av \in \mathrm{dom}(T)$ for all $v \in \Sigma_b$.*
(3) *If $xy \in \mathrm{dom}(T)$ for some $x \in \Sigma_a$ and $y \in \Sigma_b$, then $uv \in \mathrm{dom}(T)$ for all $u \in \Sigma_a$ and $v \in \Sigma_b$.*

Proof. We prove the first statement. The second statement is proved similarly. The first and second statements combine to give the third.

Suppose that $xb \in \mathrm{dom}(T)$ for some $x \in \Sigma_a$. Then $(xb, d) \in T$ for some $d \in \Sigma \cup \{\lambda\}$. If $\Sigma_a = \{a\}$ there is nothing to prove, so suppose that $u \in \Sigma_a \backslash \{x\}$. By Lemma 3.1, $m_a > 2$ and (Σ, T) contains the nontrivial part of the multiplication table for $\langle a \rangle$. Hence $x \equiv a_j$ and $u \equiv a_k$ for some $1 \leq j, k < m_a$. Let i be the remainder when $k - j$ is divided by m_a. Because $x \not\leftrightarrow^* \lambda$, $b \not\equiv d$. Now $a_i xb \rightarrow a_i d$ and $a_i xb \rightarrow a_k b$. Since $a_i d, a_k b$ are distinct words that spell the same group element and $|a_i d| \leq |a_k b|$, the word $a_k b$ is reducible. Because (Σ, T) is normalised, a reducible word of length two is necessarily in $\mathrm{dom}(T)$. Hence $a_k b \in \mathrm{dom}(T)$, and the claim is proved. □

Lemma 3.6. *For all $a, b \in \Sigma$, $ab \in \mathrm{dom}(T)$ if and only if $ba \in \mathrm{dom}(T)$.*

https://doi.org/10.1017/S0004972715000015 Published online by Cambridge University Press

Proof. Let $a, b \in \Sigma$. By symmetry it suffices to show only one direction of implication. Suppose that $ab \in \mathrm{dom}(T)$. If $a \equiv b$ there is nothing to prove, so suppose that $a \not\equiv b$. If $a, b \in \Sigma_c$ for some $c \in \Sigma$, then $\Sigma_c \neq \{c\}$ and the result follows from Lemma 3.1. So suppose that no such c exists. By Lemma 3.2(2), $a \not\leftrightarrow^* b^{m_b-1}$ and $b \not\leftrightarrow^* a^{m_a-1}$. It follows that $(ab, d) \in T$ for some $d \in \Sigma \backslash \{a, b\}$. Because $ab \leftrightarrow^* d$, $b_{m_b-1}a_{m_a-1} \leftrightarrow^* d_{m_d-1}$. Because d_{m_d-1} is irreducible, $b_{m_b-1}a_{m_a-1} \rightarrow^* d_{m_d-1}$.

Consider the case where $b_{m_b-1}a_{m_a-1} \equiv d_{m_d-1}$. Then $|d_{m_d-1}| = |b_{m_b-1}| + |a_{m_a-1}| > 1$. It follows by Lemma 3.2 that $m_d > 2$, $\Sigma_d = \{d\}$, $d_{m_d-1} \equiv d^{m_d-1}$ and $b_{m_b-1}, a_{m_a-1} \in \{d\}^*$. Because a, b, d are distinct, $b_{m_b-1} \not\equiv b^{m_b-1}$ and $a_{m_a-1} \not\equiv a^{m_a-1}$. By Lemma 3.2(1), $b_{m_b-1}, a_{m_a-1} \in \Sigma$. It follows that $b_{m_b-1} \equiv a_{m_a-1} \equiv d$. Then $ba_{m_a-1} \equiv bb_{m_b-1} \rightarrow^* \lambda$. Hence $ba_{m_a-1} \in \mathrm{dom}(T)$. By Lemma 3.5(2), $ba \in \mathrm{dom}(T)$.

Now consider the case where $b_{m_b-1}a_{m_a-1} \not\equiv d_{m_d-1}$. If $b_{m_b-1}, a_{m_a-1} \in \Sigma$, then $b_{m_b-1}a_{m_a-1} \in \mathrm{dom}(T)$ and the result follows from Lemma 3.5(3). If $a_{m_a-1} \in \Sigma$ but $b_{m_b-1} \notin \Sigma$, then $b_{m_b-1}a_{m_a-1} \equiv b^{m_b-1}a_{m_a-1}$. It follows from Lemma 3.4 that $ba_{m_a-1} \in \mathrm{dom}(T)$. The result follows from Lemma 3.4 again. Similarly, the result follows if $a_{m_a-1} \notin \Sigma$ but $b_{m_b-1} \in \Sigma$. Consider the case where $b_{m_b-1}, a_{m_a-1} \notin \Sigma$. Because $b_{m_b-1}a_{m_a-1} \equiv b^{m_b-1}a^{m_a-1}$ is reducible and b^{m_b-1}, a^{m_a-1} are irreducible and $a \not\equiv b$, Lemma 3.4 yields $ba \in \mathrm{dom}(T)$. □

Lemma 3.7. *Suppose that* $a, b, d \in \Sigma$. *If* $(ab, d_s) \in T$ *for some* $1 \leq s < m_d$, *then* $ad, da, bd, db \in \mathrm{dom}(T)$.

Proof. Suppose that $(ab, d_s) \in T$ for some $1 \leq s < m_d$. Note that this means $d_s \in \Sigma$ and $d_s \not\equiv a$. Since $ab \leftrightarrow^* d_s$, $a_{m_a-1}d_s \leftrightarrow^* b$. It follows that $a_jd_s \in \mathrm{dom}(T)$ for some $1 \leq j < m_a$. If $|a_j| > 1$, then $a_j \equiv a^j$ and, by Lemma 3.4, $ad_s \in \mathrm{dom}(T)$. If $|a_j| = 1$, then a_jd_s is a reducible word of length two, and hence $a_jd_s \in \mathrm{dom}(T)$. In either case, it follows from Lemma 3.5(3) that $ad \in \mathrm{dom}(T)$. By Lemma 3.6, $da \in \mathrm{dom}(T)$. The proof that $bd, db \in \mathrm{dom}(T)$ is similar. □

Lemma 3.8. *Suppose that* $a, b \in \Sigma$. *If* $ab \in \mathrm{dom}(T)$, *then* $\mathrm{irr}(a_jb_k) \in \Sigma \cup \{\lambda\}$ *for all* $1 \leq j < m_a$ *and* $1 \leq k < m_b$.

Proof. Suppose that $ab \in \mathrm{dom}(T)$. If $a \equiv b$, then (Σ, T) contains the nontrivial part of the multiplication table for $\langle a \rangle$ and the result follows. Suppose that $a \not\equiv b$. If $\{a, b\} \subseteq \Sigma_c$ for some c, then the result follows from Lemma 3.1. Suppose that no such c exists. We now consider cases based on whether or not (Σ, T) contains the nontrivial parts of the multiplication tables for $\langle a \rangle$ and $\langle b \rangle$.

The result follows immediately from Lemma 3.5(3) in the case where (Σ, T) contains the nontrivial parts of the multiplication tables for $\langle a \rangle$ and $\langle b \rangle$.

Consider the case where $\Sigma_a = \{a\}$ and $m_a > 2$ and (Σ, T) contains the nontrivial part of the multiplication table for $\langle b \rangle$. By Lemma 3.5(2), $ab_k \in \mathrm{dom}(T)$ for all $1 \leq k < m_b$. Fix an integer $1 \leq k < m_b$. Since $ab_k \in \mathrm{dom}(T)$, $b_k \not\equiv a$. Since $a_{m_a-1} \equiv a^{m_a-1}$, $b_k \not\equiv \mathrm{irr}(a^{m_a-1})$. It follows that $(ab_k, d) \in T$ for some $d \in \Sigma \backslash \{a, b_k\}$. Now $a^{m_a}b_k \rightarrow a^{m_a-1}d$ and $a^{m_a}b_k \rightarrow^* b_k$. Because b_k is irreducible, $a^{m_a-1}d \rightarrow^* b_k$. Because a^{m_a-1} is irreducible, Lemma 3.4 gives that $(ad, e) \in T$ for some $e \in \Sigma \backslash \{a, d\}$. Thus $a^2b_k \rightarrow^* e$. Now we have

$a^{m_a}b_k \to a^{m_a-2}e$ and $a^{m_a}b_k \to^* b_k$. Applying this argument inductively, we conclude that $\mathrm{irr}(a^jb_k) \in \Sigma \cup \{\lambda\}$ for all $1 \le j < m_a$.

A similar argument proves that the result holds in the case where $\Sigma_b = \{b\}$ and $m_b > 2$ and (Σ, T) contains the nontrivial part of the multiplication table for $\langle a \rangle$.

Finally, consider the case where $\Sigma_a = \{a\}$ and $m_a > 2$ and $\Sigma_a = \{b\}$ and $m_b > 2$. Let j, k be such that $1 \le j < m_a$ and $1 \le k < m_b$. Because b^k and a^{m_a-j} are irreducible and distinct, $a^jb^k \nleftrightarrow^* \lambda$. An argument similar to that above gives that $a^jb^k \to^* db^{k-1}$ and $a^jb^k \to^* a^{j-1}e$ for some $d, e \in \Sigma\backslash\{a, b\}$. Because a^{j-1} is irreducible and $e \nleftrightarrow^* a^{m_a-j+1}$, any reduction of $a^{j-1}e$ has first letter a unless it has length one; because b^{k-1} is irreducible, any reduction of db^{k-1} has first letter equal in G to a^jb^p for some $1 \le p \le k$. Because $a^jb^k \nleftrightarrow^* a$, it must be that $a^{j-1}e$ reduces to a word of length one. Hence $\mathrm{irr}(a_jb_k) \in \Sigma$. □

Lemma 3.9. *Suppose that $a, b \in \Sigma$. If $ab \in \mathrm{dom}(T)$, then (Σ, T) contains the nontrivial parts of the multiplication tables of $\langle a \rangle$ and $\langle b \rangle$.*

Proof. Suppose that $ab \in \mathrm{dom}(T)$. By Lemma 3.6 it suffices to show that (Σ, T) contains the nontrivial part of the multiplication table of $\langle a \rangle$. Suppose not. By Lemma 3.1, $m_a > 2$ and $a_j \equiv a^j$ for all $1 \le j < m_a$. Because a^2 is irreducible and ab is reducible, $b \not\equiv a$. If $c \in \Sigma$ such that $a, b \in \Sigma_c$, then (Σ, T) contains the nontrivial part of the multiplication table of $\langle c \rangle$, and hence also $\langle a \rangle$. So no such c exists. By Lemma 3.6, $ba \in \mathrm{dom}(T)$. Let $x := \mathrm{irr}(b_{m_b-1}a)$ and $y := \mathrm{irr}(ab)$. By Lemma 3.8, $x, y \in \Sigma$. Because $ab \leftrightarrow^* y$ and $b \not\equiv \lambda$, $y \not\equiv a$. But then $yx \equiv \mathrm{irr}(ab)\mathrm{irr}(b_{m_b-1}a) \leftrightarrow^* a^2$. It follows that a^2 is reducible, which is impossible. □

Remark 3.10. The contrapositive of the lemma gives immediately that if $a \in \Sigma$ and (Σ, T) does not contain the nontrivial part of the multiplication table for $\langle a \rangle$, then $(\Sigma\backslash\{a\}, T\backslash\{(a_a^m, \lambda)\})$ is a normalised finite convergent monadic rewriting system presenting a group G_1 such that $G \cong G_1 * \mathbb{Z}/m_a\mathbb{Z}$.

Lemma 3.11. *Suppose that $a, b, c \in \Sigma$ and $ab, bc \in \mathrm{dom}(T)$ and $a \not\equiv c$. Then $ac \in \mathrm{dom}(T)$.*

Proof. If any two of the letters a, b, c are contained in Σ_d for some $d \in \Sigma$, then the result follows easily from Lemmas 3.1 and 3.5. Suppose that no such d exists. It follows that $a \not\equiv \mathrm{irr}(b^{m_b-1})$, and $b \not\equiv \mathrm{irr}(c^{m_c-1})$. Thus there exist $d, e \in \Sigma$ such that $(ab, d), (bc, e) \in T$. Since $b \not\equiv \lambda$, $c \not\equiv e$. By Lemma 3.8, $ab_{m_b-1} \to^* x$ for some $x \in \Sigma$. Now

$$ac \leftrightarrow^* ab_{m_b-1}bc \to ab_{m_b-1}e \to^* xe.$$

Because $c \not\equiv e$, $ac \not\equiv xe$. Because ac and xe are distinct words of equal length representing the same group element, they are reducible. Hence $ac \in \mathrm{dom}(T)$. □

We now prove our main results.

Theorem 3.12. *Let G be a group. Then G is presented by a finite convergent monadic rewriting system (Σ, T) such that every letter $a \in \Sigma$ has finite order in G if and only if G may be decomposed as a free product of finitely many finite groups.*

Proof. First suppose that $G = G_1 * \cdots * G_p$ for some finite groups $G_1, \ldots, G_p$. For each integer i such that $1 \leq i \leq p$, we let $\Sigma_i := G_i \backslash \{1_{G_i}\}$ (where 1_{G_i} denotes the identity element in G_i) and

$$\begin{aligned} T_i := &\{(ab, c) \mid a, b, c \in \Sigma_i \text{ such that } ab =_{G_i} c\} \\ &\cup \{(ab, \lambda) \mid a, b \in \Sigma_i \text{ such that } ab =_{G_i} 1_{G_i}\}. \end{aligned}$$

Let $\Sigma = \bigcup_{i=1}^{p} \Sigma_i$ and $T = \bigcup_{i=1}^{p} T_i$. It is then easily confirmed that (Σ, T) is a normalised finite convergent monadic rewriting system presenting G and every letter $a \in \Sigma$ has finite order in G.

Now suppose that G is presented by a finite convergent monadic rewriting system (Σ, T) such that every letter $a \in \Sigma$ has finite order in G. Without loss of generality we assume that (Σ, T) is normalised. For $a, b \in \Sigma$, we write $a \sim b$ if $a \equiv b$ or $ab \in \mathrm{dom}(T)$. By definition, the relation is reflexive. It is symmetric by Lemma 3.6, and transitive by Lemma 3.11. Thus $\sim$ is an equivalence relation on Σ. It follows that (Σ, T) may be partitioned into rewriting systems $(\Sigma_1, T_1), \ldots, (\Sigma_p, T_p)$ such that each Σ_i comprises the elements of one $\sim$-equivalence class (or, equivalently, the vertices of one connected component of Δ). Then $G \cong G_1 * \cdots * G_p$, where G_i denotes the group presented by (Σ_i, T_i) for $1 \leq i \leq p$. For $a, b \in \Sigma_i$ with $a \not\equiv b$, we have $ab, ba \in \mathrm{dom}(T)$. It follows that if $u \in \Sigma_i^*$ is irreducible and $|u| > 1$, then $u = a^j$ for some $a \in \Sigma_i$ and some $1 \leq j < m_a$. In turn it follows that there are finitely many irreducibles in (Σ_i, T_i), and hence finitely many elements in G_i. Thus G is a free product of finitely many finite groups. □

In [8, Theorem 2.7] it is shown that if (Σ, T) is a normalised finite convergent monadic rewriting system presenting a finite group G and every element of Σ has an inverse in Σ, then (Σ, T) is the nontrivial part of the multiplication table for G. It is also observed that for each integer $m \geq 3$ the finite cyclic group of order m is presented by the finite convergent monadic rewriting system $(\{a\}, \{(a^m, 1)\})$. It follows immediately from the above that these are the *only* examples of normalised finite convergent monadic rewriting systems describing finite groups.

Corollary 3.13. *Suppose that (Σ, T) is a normalised finite convergent monadic rewriting system presenting a group G. Then G is a finite group if and only if either $|\Sigma| = |T| = 1$ and $|G| \geq 3$ (in which case G is a finite cyclic group of order at least three), or (Σ, T) is the nontrivial part of the multiplication table for G. Therefore the finite cyclic groups of order at least three are the only finite groups admitting a presentation by more than one normalised finite monadic convergent rewriting system (up to relabelling), and these admit exactly two such rewriting systems.*

We note that, by Corollary 3.13, it is rather easy to determine whether or not a normalised finite convergent monadic rewriting system determines a finite group. In [11, Theorem 4.9] an algorithm is described which determines whether or not a finite convergent rewriting system with a unique irreducible representative for each $\leftrightarrow^*$-class determines a torsion-free group.

https://doi.org/10.1017/S0004972715000015 Published online by Cambridge University Press

Acknowledgement

The author wishes to thank the University of Wollongong for its hospitality as this work was undertaken.

References

[1] J. Avenhaus and K. Madlener, 'On groups defined by monadic Thue systems', in: *Algebra, Combinatorics and Logic in Computer Science, Vol. I, II (Győr, 1983)*, Colloquia Mathematica Societatis János Bolyai, 42 (North-Holland, Amsterdam, 1986), 63–71.

[2] J. Avenhaus, K. Madlener and F. Otto, 'Groups presented by finite two-monadic Church–Rosser Thue systems', *Trans. Amer. Math. Soc.* **297**(2) (1986), 427–443.

[3] R. V. Book and F. Otto, *String-Rewriting Systems*, Texts and Monographs in Computer Science (Springer, New York, 1993).

[4] Y. Cochet, 'Church—Rosser congruences on free semigroups', in: *Algebraic Theory of Semigroups (Proc. Sixth Algebraic Conf., Szeged, 1976)*, Colloquia Mathematica Societatis János Bolyai, 20 (North-Holland, Amsterdam, 1979), 51–60.

[5] V. Diekert, 'Some remarks on presentations by finite Church–Rosser Thue systems', *STACS 87, 4th Annual Symposium on Theoretical Aspects of Computer Science,* Passau, Germany, 1987, Lecture Notes in Computer Science, 247 (Springer, Berlin, 1987), 272–285.

[6] R. H. Gilman, 'Computations with rational subsets of confluent groups', *EUROSAM84, International Symposium on Symbolic and Algebraic Computation,* Cambridge, UK, 1984, Lecture Notes in Computer Science, 174 (Springer, Berlin, 1984), 207–212.

[7] R. H. Haring-Smith, 'Groups and simple languages', *Trans. Amer. Math. Soc.* **279**(1) (1983), 337–356.

[8] K. Madlener and F. Otto, 'On groups having finite monadic Church–Rosser presentations', in: *Semigroups, Theory and Applications (Oberwolfach, 1986)*, Lecture Notes in Mathematics, 1320 (Springer, Berlin, 1988), 218–234.

[9] K. Madlener and F. Otto, 'About the descriptive power of certain classes of finite string-rewriting systems', *Theoret. Comput. Sci.* **67**(2–3) (1989), 143–172.

[10] D. E. Muller and P. E. Schupp, 'Groups, the theory of ends, and context-free languages', *J. Comput. System Sci.* **26**(3) (1983), 295–310.

[11] F. Otto, 'Elements of finite order for finite monadic Church–Rosser Thue systems', *Trans. Amer. Math. Soc.* **291**(2) (1985), 629–637.

[12] J.-P. Serre, *Trees*, Springer Monographs in Mathematics (Springer, Berlin, 2003).

[13] M. Shapiro, 'Pascal's triangles in abelian and hyperbolic groups', *J. Austral. Math. Soc. Ser. A* **63**(2) (1997), 281–288.

ADAM PIGGOTT, Department of Mathematics, Bucknell University,
Lewisburg, PA 17837, USA
e-mail: adam.piggott@bucknell.edu

https://doi.org/10.1017/S0004972715000015 Published online by Cambridge University Press