View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA 119, 246–259 (1988)

# Rewriting Products of Group Elements—II

RUSSELL D. BLYTH*

*University of Illinois, Urbana, Illinois 61801*

*Communicated by Peter M. Neumann*

Received June 25, 1987

## 1. INTRODUCTION

Let $n$ be an integer greater than 1. A group $G$ is said to be *n-rewriteable*, or to have the property

$$\mathbf{Q}_n$$

if for every subset $\{x_1, ..., x_n\}$ of $n$ elements of $G$ there exist distinct permutations $\sigma$ and $\tau$ in Sym($n$) such that

$$x_{\sigma(1)} \cdots x_{\sigma(n)} = x_{\tau(1)} \cdots x_{\tau(n)}.$$

A group is *rewriteable*, or has the property

$$\mathbf{Q}$$

if it is $n$-rewriteable for some $n > 1$.

The class of rewriteable groups was first considered in [2], where a characterization of all such groups is given:

STRUCTURE THEOREM. *A group $G$ is rewriteable if and only if it is finite-by-abelian-by-finite.*

The main object of this paper is to present two applications of the Structure Theorem. The reader should consult [2] for any undefined terms used in the sequel.

Although, as the abelian groups show, there is no bound on the order of a general $\mathbf{Q}_n$-group, there is such a bound for the class of semisimple groups (that is, the class of groups which have no nontrivial abelian normal subgroups).

* The results presented in this paper are excerpted from the author's Ph. D. dissertation submitted at the University of Illinois, Urbana-Champaign, 1987.

† Present address: St. Louis University, St. Louis, Missouri 63103.



0021-8693/88 $3.00

Copyright © 1988 by Academic Press, Inc.
All rights of reproduction in any form reserved.

THEOREM 1. *For each $n \geqslant 3$, there is a constant $J_n$, depending only on n, such that if G is an n-rewriteable semisimple group, then $|G| \leqslant J_n$.*

The 5-rewriteability of the nonsolvable group Alt(5) shows that the following result cannot be extended to any higher rewriting class.

THEOREM 2. *Every 4-rewriteable group is solvable.*

Thus there is at least limited agreement between an established measure of noncommutativity (solvability) and the use of the rewriting properties as measures of the degree of noncommutativity of a group. A similar result has been shown for the stronger property of total 4-rewriteability [1]; in fact, every totally 4-rewriteable group is metabelian [8]. The symmetric group on 4 letters shows that this latter result does not extend to 4-rewriteable groups.

The proofs of Theorem 1 and 2 each depend initially on a reduction using the Structure Theorem to a more restricted class of groups. For Theorem 1, we are left to show that the conclusion of the theorem holds for $n$-rewriteable nonabelian finite simple groups. We then use the classification of the finite simple groups and information about the structure of the groups of Lie type to find the required bounds. In Theorem 2, the reduction leaves us to show that no minimal simple group is 4-rewriteable. Machine calculations required to settle various particular cases were carried out using Cayley on the CYBER 175 system at the University of Illinois.

## 2. REWRITEABLE SEMISIMPLE GROUPS

Most of the proof of Theorem 1 lies in proving the result for nonabelian finite simple groups.

PROPOSITION 2.1. *For each $n \geqslant 3$, there is a constant $K_n$, depending only on n, such that if G is an n-rewriteable nonabelian finite simple group, then $|G| \leqslant K_n$.*

Indeed, suppose that 2.1 has been demonstrated, and let $G$ be a semisimple $\mathbf{Q}_n$-group. Since $G \in \mathbf{FAF}$ and $\mathbf{FA} \subseteq \mathbf{N}_2\mathbf{F}$, it follows easily that $G \in \mathbf{N}_2\mathbf{F}$ ($\mathbf{N}_2$ is the class of groups which are nilpotent of class at most 2). Thus, by semisimplicity, $G$ is finite. Every finite group has a unique nonabelian $CR$-radical $R$, which is a direct product of nonabelian finite simple groups. Each direct factor has order at most $K_n$, and by Proposition 2.6 of [2], there are at most $c_n = \binom{n}{2} - 1$ such factors. Hence

$$|R| \leqslant (K_n)^{c_n}.$$

Since $G$ is semisimple, the canonical homomorphism $G \to \mathrm{Aut}\, R$ is injective [10], and therefore

$$|G| \leqslant ((K_n)^{c_n})!.$$

This completes the proof of Theorem 1.

We utilize the classification of the finite simple groups to prove 2.1. We need not be concerned with the sporadic groups, since they are finite in number. Suppose that $\mathrm{Alt}(m)$ is $n$-rewriteable. From [2], we have that $m \leqslant n+1$. It remains for us to consider the groups of Lie type. We first study the projective special linear groups.

LEMMA 2.2. *Let $F \cong GF(q)$, where $q = p^m$, $p$ prime. Suppose that the group $G$ is either*

(i) $F^* \ltimes F^+$, *or*

(ii) $F^*/(-1) \ltimes F^+$,

*where in each case $x \in F^*$ or $x \in F^*/(-1)$ acts on $F^+$ via multiplication by $x^2$. If $G$ is $n$-rewriteable $(n > 1)$, then*

(a) $q \leqslant (n-1)\, n!(n!-1)$, *and*

(b) $m \leqslant M_p(n) = n(n+(-1)^p)/2$; *in fact, if $p \geqslant n$, then $m \leqslant n-1$.*

*Proof.* (a) Suppose that $G$ is $n$-rewriteable. Unless $q < n$ (in which case we are done), fix $a_1, ..., a_n$ to be distinct elements of $F^+$. Let $x \in F^*$, and consider the subset $\{(x, a_1), ..., (x, a_n)\}$ of $n$ elements of $G$. Since $G$ is a $\mathbf{Q}_n$-group, we have

$$(x, a_{i_1}) \cdot \cdots \cdot (x, a_{i_n}) = (x, a_{j_1}) \cdot \cdots \cdot (x, a_{j_n})$$

for some $(i_1, ..., i_n) \neq (j_1, ..., j_n)$, where each $n$-tuple is an arrangement chosen from the set $\{1, ..., n\}$. Hence

$$\begin{aligned}(x^n, x^{2(n-1)}a_{i_1} + x^{2(n-2)}a_{i_2} + \cdots + a_{i_n}) \\ = (x^n, x^{2(n-1)}a_{j_1} + x^{2(n-2)}a_{j_2} + \cdots + a_{j_n}),\end{aligned}$$

and so it follows that $x$ is a root of the polynomial

$$(a_{i_1} - a_{j_1})X^{2(n-1)} + (a_{i_2} - a_{j_2})X^{2(n-2)} + \cdots + (a_{i_n} - a_{j_n}).$$

This is a nontrivial polynomial of degree at most $2(n-1)$ with coefficients in $F$. The number of distinct polynomials that can arise in this fashion is at most $n!(n!-1)$, and each such polynomial has at most $2(n-1)$ distinct roots in $F$. Since transposing $(i_1, ..., i_n)$ and $(j_1, ..., j_n)$ merely negates the coefficients of the corresponding polynomial, there are at most

$(n-1)\,n!(n!-1)$ distinct roots in $F$ of all of these polynomials. Moreover, 0 is a root of one of these polynomials, for example, of the polynomial $(a_2-a_1)X^{2(n-1)}+(a_1-a_2)X^{2(n-2)}$ arising from $(i_1, ..., i_n)=(2, 1, 3, ..., n)$ and $(j_1, ..., j_n)=(1, 2, 3, ..., n)$. It follows that if $F$ has more than $(n-1)\,n!(n!-1)$ elements, then there is an element $x\in F^*$ which is not a root of any of these polynomials. The existence of such an $x$ would contradict the $n$-rewriteability of $G$.

(b) $F^*$ is cyclic, so set $F^*=\langle z\rangle$. Let $a$ be a nonzero element of $F^+$, and consider the subset $\{(z, a), (z^2, a), ..., (z^n, a)\}$, if $p=2$, or $\{(1, a), (z, a), ..., (z^{n-1}, a)\}$, if $p>2$, of $n$ elements of $G$. Since $G$ is a $\mathbf{Q}_n$-group, we have

$$(z^{i_1}, a)\cdot(z^{i_2}, a)\cdot\cdots\cdot(z^{i_n}, a)=(z^{j_1}, a)\cdot(z^{j_2}, a)\cdot\cdots\cdot(z^{j_n}, a)$$

for some $(i_1, ..., i_n)\neq(j_1, ..., j_n)$, where each $n$-tuple is an arrangement chosen from the set $\{1, 2, ..., n\}$, if $p=2$, or $\{0, 1, ..., n-1\}$, if $p>2$. Hence

$$\begin{aligned}&(z^{M_p(n)}, (z^{2\sum_{k=2}^{n} i_k}+z^{2\sum_{k=3}^{n} i_k}+\cdots+z^{2i_n}+1)a)\\&\quad=(z^{M_p(n)}, (z^{2\sum_{k=2}^{n} j_k}+z^{2\sum_{k=3}^{n} j_k}+\cdots+z^{2j_n}+1)a)\end{aligned}$$

and therefore,

$$\begin{aligned}&(z^{2\sum_{k=2}^{n} i_k}+z^{2\sum_{k=3}^{n} i_k}+\cdots+z^{2i_n}+1)\\&\quad-(z^{2\sum_{k=2}^{n} j_k}+z^{2\sum_{k=3}^{n} j_k}+\cdots+z^{2j_n}+1)=0.\end{aligned}$$

Thus, since $(i_1, i_2, ..., i_n)\neq(j_1, j_2, ..., j_n)$ if and only if $(\sum_{k=2}^{n} i_k, \sum_{k=3}^{n} i_k, ..., i_n)\neq(\sum_{k=2}^{n} j_k, \sum_{k=3}^{n} j_k, ..., j_n)$, $z^2$ satisfies a nontrivial polynomial of degree at most $M_p(n)$ over the prime subfield $F_0$. It follows that $\deg(\mathrm{Irr}_{F_0}(z^2))\leqslant M_p(n)$, from which we obtain $|F_0(z^2)|\geqslant p^{M_p(n)}$. On the other hand, $|z|=p^m-1$, which gives

$$|z^2|=\begin{cases}\frac{1}{2}(p^m-1) & \text{if } p>2\\ p^m-1 & \text{if } p=2.\end{cases}$$

In either case $|z^2|\geqslant\frac{1}{2}(p^m-1)$. Thus $\frac{1}{2}(p^m-1)\leqslant|z^2|\leqslant p^{M_p(n)}-1$, and so $p^m\leqslant 2p^{M_p(n)}-1$. We conclude that $m\leqslant M_p(n)$.

In case $p\geqslant n$, the $n$ elements $a_1, a_2, ..., a_n$ in (a) may all be chosen to lie in $F_0$, and therefore the polynomials arising there have coefficients in $F_0$. In particular, $z^2$ must be a root of a nontrivial polynomial over $F_0$ of degree at most $n-1$, and so $\deg(\mathrm{Irr}_{F_0}(z^2))\leqslant n-1$. As in the argument above, we conclude that $m\leqslant n-1$. This completes the proof.

COROLLARY 2.3. *Suppose that $G$ is either the group $SL(2, q)$ or the group $PSL(2, q)$, where $q = p^m$. If $G$ is $n$-rewriteable $(n > 1)$, then*

(a) $q \leqslant (n-1)\,n!(n!-1)$, *and*

(b) $m \leqslant M_p(n) = n(n+(-1)^p)/2$; *in fact, if $p \geqslant n$, then $m \leqslant n-1$.*

*Proof.* Let $G \cong GF(q)$. In the group $SL(2, q)$, the subgroup $U = \{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right) \mid b \in F\}$ is isomorphic to $F^+$, and $X = \{\left(\begin{smallmatrix}\lambda^{-1} & 0\\ 0 & \lambda\end{smallmatrix}\right) \mid \lambda \in F^*\}$ is a subgroup isomorphic to $F^*$. Moreover, the action of $x = \left(\begin{smallmatrix}\lambda^{-1} & 0\\ 0 & \lambda\end{smallmatrix}\right)$ on $a = \left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right)$ is given by $a^x = \left(\begin{smallmatrix}1 & \lambda^2 b\\ 0 & 1\end{smallmatrix}\right)$, so that $x$ acts on $U$ via $x \mapsto x^2$. It follows that $\langle X, U\rangle \cong F^* \ltimes F^+$, under the action of 2.2. Finally, since $U \cap \langle -1_2\rangle = 1$, we have $\langle X, U\rangle/\langle -1_2\rangle \cong (F^*/\langle -1\rangle) \ltimes F^+$.

We are now equipped to deal with the general group of Lie type. The order of a group of Lie type depends on two parameters: the rank $l$ of the group, and the number of elements $q$ in the underlying field. If the group $L$ is $n$-rewriteable, we can provide bounds for each parameter which depend only on $n$, and hence bound the order of $L$.

PROPOSITION 2.4. *Suppose that $L$ is a group of Lie type of rank $l$ of one of the types $A_l(q)$, $B_l(q)$, $C_l(q)$, $D_l(q)$, ${}^2A_l(q)$, or ${}^2D_l(q)$ which is $n$-rewriteable $(n > 1)$.*

(i) *If $L$ is of type $A_l(q)$, then $l \leqslant n-1$.*

(ii) *If $L$ is of type $B_l(q)$, $C_l(q)$, or $D_l(q)$, then $l \leqslant n$.*

(iii) *If $L$ is of type ${}^2A_l(q)$, with $l$ odd, then $l \leqslant 2n-1$.*

(iv) *If $L$ is of type ${}^2A_l(q)$, with $l$ even, then $l \leqslant 2n$.*

(v) *If $L$ is of type ${}^2A_l(q)$, then $l \leqslant n+1$.*

*Proof.* Since $L$ is $n$-rewriteable, it follows that the monomial subgroup $N$ of $L$ is $n$-rewriteable. The Weyl group $W(L)$ is isomorphic to the quotient group $N/H$, where $H$ is the diagonal subgroup of $L$, and thus $W$ is a $\mathbf{Q}_n$-group. The Weyl groups of interest are [3, 4]

$$W(L) = \begin{cases} \mathrm{Sym}(l+1) & \text{if } L \text{ is of type } A_l(q), \\ \mathrm{Sym}(l) \ltimes (\mathbb{Z}/2\mathbb{Z})^l & \text{if } L \text{ is of type } B_l(q) \text{ or } C_l(q), \\ \mathrm{Sym}(l) \ltimes (\mathbb{Z}/2\mathbb{Z})^{l-1} & \text{if } L \text{ is of type } D_l(q), \\ \mathrm{Sym}\left(\dfrac{l+1}{2}\right) \ltimes (\mathbb{Z}/2\mathbb{Z})^{(l+1)/2} & \text{if } L \text{ is of type } {}^2A_l(q),\ q \text{ odd}, \\ \mathrm{Sym}\left(\dfrac{l}{2}\right) \ltimes (\mathbb{Z}/2\mathbb{Z})^{l/2} & \text{if } L \text{ is of type } {}^2A_l(q),\ q \text{ even}, \\ \mathrm{Sym}(l-1) \ltimes (\mathbb{Z}/2\mathbb{Z})^{l-1} & \text{if } L \text{ is of type } {}^2D_l(q). \end{cases}$$

The conclusion of the result now follows from the fact that Sym($m$) is $n$-rewriteable if and only if $m \leqslant n$ (see [2]).

The proof of the next result follows the method of Jones [7].

PROPOSITION 2.5. *Suppose that $L$ is an $n$-rewriteable group of Lie type over the field $GF(q)$ of $q$ elements.*

(i) *If $L$ is a Chevalley group, or of type ${}^2F_4(q)$ or ${}^2G_2(q)$, then $q \leqslant (n-1)\,n!\,(n!-1)$.*

(ii) *If $L$ is of type ${}^2A_l(q)$, ${}^2D_l(q)$, or ${}^2E_6(q)$, then $q \leqslant [(n-1)\,n!\,(n!-1)]^2$.*

(iii) *If $L$ is of type ${}^3D_4(q)$, then $q \leqslant [(n-1)\,n!\,(n!-1)]^3$.*

(iv) *If $L$ is of type ${}^2B_2(q)$, then $q \leqslant 2^{n(n+1)/2}$.*

*Proof.* Consider first the case that $L$ is a Chevalley (nontwisted) group, and let $r$ be a positive root of $L$. The epimorphism

$$\varphi_r\colon SL(2, q) \to \langle X_r, X_{-r}\rangle$$

defined by sending

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mapsto x_r(t) \qquad \text{and} \qquad \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \mapsto x_{-r}(t)$$

has kernel of order at most 2 (see [5]), which shows that $\langle X_r, X_{-r}\rangle$ is isomorphic either to $SL(2, q)$ or to $PSL(2, q)$. In either case, by 2.3(a), $q \leqslant (n-1)\,n!\,(n!-1)$.

Consider next the case that $L$ is a Steinberg group, that is, one of the types ${}^2A_l(q)$, ${}^2D_l(q)$, ${}^3D_4(q)$, or ${}^2E_6(q)$. Each of these groups is the subgroup of the corresponding Chevalley group fixed by an automorphism $\sigma$ which maps each generator $x_r(t)$ to $x_{r'}(t')$, where the map $r \mapsto r'$ is a symmetry of the root system and $t \mapsto t'$ is an automorphism of $GF(q)$. The map $\sigma$ has order 2, 2, 3, and 2, respectively. Inspection of the Dynkin diagrams shows that in all cases except ${}^2A_l(q)$, with $l$ even, there is at least one fundamental root fixed by the root symmetry. In the case of ${}^2A_l(q)$, with $l$ even, there are two adjacent fundamental roots which are transposed by the graph symmetry, and thus the positive root which is their sum is fixed by the symmetry. Thus in all cases the symmetry fixes at least one positive root $s$. Consider the epimorphism

$$\varphi_s\colon SL(2, q) \to \langle X_s, X_{-s}\rangle.$$

The elements $x_s(t)$ fixed by $\sigma$, and thus contained in $L$, are those for which $t$ is fixed by the automorphism of $GF(q)$. These elements $t$ form a subfield

$GF(q')$ of $GF(q)$, where $q'$ is $q^{1/2}$, $q^{1/2}$, $q^{1/3}$, and $q^{1/2}$, respectively. Restricting $\varphi_s$ to the subgroup $SL(2, q')$ of $SL(2, q)$, we observe that

$$\varphi_s|_{SL(2,q')}: SL(2, q') \to \langle X_s, X_{-s} \rangle \cap L$$

is a homomorphism with kernel of order at most 2. It follows, as before, that $q' \leqslant (n-1)\,n!(n!-1)$, and therefore the Steinberg group case is complete.

According to [13], the group $L = {}^2F_4(q)$ has a subgroup isomorphic to PSL(2, $q$). The group ${}^2G_2(q)$ contains a centralizer $G_b$ of some $q+1$ of its elements which is a direct product of $PSL(2, q)$ and $\mathbb{Z}/2\mathbb{Z}$ (see [11]). Thus the cases ${}^2F_4(q)$ and ${}^2G_2(q)$ are complete, by 2.3(a).

Finally, for the Suzuki groups ${}^2B_2(q) = Sz(q)$, where $q = 2^{2m+1}$, we carry out direct calculations (see [8]). Consider the subset $\{xa, x^2a, ..., x^na\}$ of $n$ elements of $Sz(q)$, where $a = S(1, 0)$ and $x = M(\omega)$. Here $\omega$ is a root of the primitive irreducible polynomial defining $F = GF(q)$; thus $\omega$ generates $F^*$. Using the action $S(a, b)^{M(\lambda)} = S(\lambda a, \lambda(\lambda\pi)b)$, the typical product is

$$x^{i_1}a \cdot x^{i_2}a \cdot \cdots \cdot x^{i_n}a = x^{n(n+1)/2} S(\omega^{\sum_{j=2}^{n} i_j} + \omega^{\sum_{k=3}^{n} i_j} + \cdots + \omega^{i_n} + 1, \mu),$$

where $(i_1, ..., i_n)$ is an arrangement chosen from $\{1, ..., n\}$ and $\mu \in F$. We note that different choices of $(i_1, ..., i_n)$ give rise to different $(n-1)$-tuples $(\sum_{j=2}^{n} i_j, \sum_{j=3}^{n} i_j, ..., i_n)$, and therefore, as formal sums, the expressions

$$\omega^{\sum_{j=2}^{n} i_j} + \omega^{\sum_{j=3}^{n} i_j} + \cdots + \omega^{i_n} + 1$$

are all distinct. They remain distinct in $F$ if, in particular,

$$\sum_{j=2}^{n} i_j < \text{degree of } F \text{ over } GF(2)$$
$$= 2m + 1.$$

This is certainly the case if $n(n+1)/2 < 2m+1$. Since this would contradict the $n$-rewriteability of $Sz(q)$, it follows that $n(n+1)/2 \geqslant 2m+1$.

We have now completed the proof of (2.1).

## 3. Solvability of 4-Rewriteable Groups

The bulk of the proof of Theorem 2 resides in considering the minimal simple groups.

Proposition 3.1. *No minimal simple group is 4-rewriteable.*

Indeed, suppose that 3.1 is established. By the Structure Theorem, if

there is an insolvable $\mathbf{Q}_4$-group, then there is a finite one. Let $G$ be a finite insolvable $\mathbf{Q}_4$-group of smallest order. Then $G$ must be minimal simple, contradicting 3.1. This disposes of Theorem 2.

We recall the classification of the minimal simple groups, due to Thompson [12].

PROPOSITION 3.2. *The minimal simple groups are*

(a) $PSL(2, 2^m)$, $m$ *a prime,*

(b) $PSL(2, 3^l)$, $l$ *an odd prime,*

(c) $PSL(2, p)$, $p = 5$, *or* $p$ *a prime* $> 5$ *congruent to* $\pm 2$ (modulo 5),

(d) $PSL(3, 3)$, *and*

(e) $Sz(2^{2m+1})$, $2m+1$ *a prime.*

We shall investigate each type of minimal simple group in turn; in fact, we obtain more general results.

PROPOSITION 3.3. *The group* $PSL(2, 2^m)$ *is 4-rewriteable if and only if* $m = 1$.

*Proof.* On the one hand, $\mathrm{PSL}(2, 2) \cong \mathrm{Sym}(3)$ is 4-rewriteable. On the other hand, suppose that $PSL(2, 2^m)$ is 4-rewriteable. By 2.3(b), we must have $m \leqslant 10$; thus $PSL(2, 2^m)$ does not have $\mathbf{Q}_4$ for $m > 10$. Since $PSL(2, 2^r)$ is a subgroup of $PSL(2, 2^s)$ whenever $r$ divides $s$ (see [11]), it remains to investigate $PSL(2, 2^2)$, $PSL(2, 2^3)$, $PSL(2, 2^5)$, and $PSL(2, 2^7)$. The group $PSL(2, 2^2) \cong \mathrm{Alt}(5)$ is not 4-rewriteable [2]. For the group $PSL(2, 2^3)$, we take the elements of the underlying field $GF(2^3)$ to be $\{a + b\omega + c\omega^2 \mid a, b, c \in GF(2)\}$, where $\omega$ is a root of the primitive irreducible polynomial $x^3 - x - 1$ over $GF(2)$. Machine computations show that the subset

$$\left\{\begin{pmatrix} \omega^2+1 & 0 \\ 0 & \omega \end{pmatrix}, \begin{pmatrix} \omega^2+1 & \omega^2+1 \\ 0 & \omega \end{pmatrix}, \begin{pmatrix} \omega^2+\omega & \omega^2+\omega \\ \omega & \omega+1 \end{pmatrix}, \begin{pmatrix} \omega^2+1 & 0 \\ \omega & \omega \end{pmatrix}\right\}$$

of elements of $SL(2, 2^3)$ is not rewriteable. For the group $PSL(2, 2^5)$, we take the elements of the underlying field $GF(2^5)$ to be $\{a + b\omega + c\omega^2 + d\omega^3 + e\omega^4 \mid a, b, c, d, e \in GF(2)\}$, where $\omega$ is a root of the primitive irreducible polynomial $x^5 - x^2 - 1$ over $GF(2)$. The subset

$$\left\{\begin{pmatrix} \omega^2+1 & 0 \\ 0 & \omega^4+\omega^2+\omega+1 \end{pmatrix}, \begin{pmatrix} \omega^2+1 & \omega^2+1 \\ 0 & \omega^4+\omega^2+\omega+1 \end{pmatrix},\right.$$
$$\left.\begin{pmatrix} \omega^4 & \omega^4 \\ 0 & \omega^3+\omega+1 \end{pmatrix}, \begin{pmatrix} \omega^2+1 & 0 \\ \omega^4+\omega^2+\omega+1 & \omega^4+\omega^2+\omega+1 \end{pmatrix}\right\}$$

of elements of $SL(2, 2^5)$ is not rewriteable. Finally, for the group $PSL(2, 2^7)$, we take the elements of the underlying field $GF(2^7)$ to be $\{a+b\omega+c\omega^2+d\omega^3+e\omega^4+f\omega^5+g\omega^6 \mid a,b,c,d,e,f,g \in GF(2)\}$, where $\omega$ is a root of the primitive irreducible polynomial $x^7-x-1$ over $GF(2)$. The subset

$$\left\{\begin{pmatrix}\omega^6+1 & 0\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}\omega^6+1 & \omega^6+1\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}\omega^2+1 & \omega^2+1\\ 0 & \omega^5+\omega^3+\omega\end{pmatrix}, \begin{pmatrix}\omega^6+1 & 0\\ \omega & \omega\end{pmatrix}\right\}$$

of elements of $SL(2, 2^7)$ is not rewriteable. Since $PSL(2, 2^r) \cong SL(2, 2^r)$, the proof is complete.

PROPOSITION 3.4. *The group $PSL(2, 3^l)$ is 4-rewriteable if and only if $l=1$.*

*Proof.* First, $PSL(2, 3) \cong \mathrm{Alt}(4)$ is 4-rewriteable. On the other hand, suppose that $PSL(2, 3^l)$ is 4-rewriteable. By 2.3(b), we observe that $l \leqslant 6$; thus for $l>6$ the group $PSL(2, 3^l)$ is not 4-rewriteable. It remains to investigate $PSL(2, 3^2)$, $PSL(2, 3^3)$, and $PSL(2, 3^5)$. The group $PSL(2, 3^2) \cong \mathrm{Alt}(6)$ is not 4-rewriteable [2]. For the group $PSL(2, 3^3)$, we take the elements of the underlying field $GF(3^3)$ to be $\{a+b\omega+c\omega^2 \mid a, b, c \in GF(3)\}$, where $\omega$ is a root of the primitive irreducible polynomial $x^3-x-2$ over $GF(3)$. The 24 possible products of the elements

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}2\omega^2+1 & 2\omega^2+1\\ 0 & \omega\end{pmatrix},$$

$$\begin{pmatrix}2\omega^2+2\omega+1 & 2\omega^2+2\omega+1\\ 0 & \omega^2\end{pmatrix}, \quad \text{and} \quad \begin{pmatrix}2\omega^2+1 & 0\\ \omega & \omega\end{pmatrix}$$

of $SL(2, 3^3)$ are all distinct modulo $Z(SL(2, 3^3)) = \langle -1_2 \rangle$. Hence $PSL(2, 3^3)$ is not 4-rewriteable. For the group $PSL(2, 3^5)$, take the elements of the underlying field $GF(3^5)$ to be $\{a+b\omega+c\omega^2+d\omega^3+e\omega^4 \mid a, b, c, d, e \in GF(3)\}$, where $\omega$ is a root of the primitive irreducible polynomial $x^5+x^4+x^2+1$ over $GF(3)$. The 24 possible products of the subset

$$\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}2\omega^4+2\omega^3+2\omega & 2\omega^4+2\omega^3+2\omega\\ 0 & \omega\end{pmatrix}, \begin{pmatrix}2\omega^3+2\omega^2+2 & 2\omega^3+2\omega^2+2\\ 0 & \omega^2\end{pmatrix}, \begin{pmatrix}2\omega^4+2\omega^3+2\omega & 0\\ \omega & \omega\end{pmatrix}\right\}$$

of elements of $SL(2, 3^5)$ are all distinct modulo $Z(SL(2, 3^5)) = \langle -1_2 \rangle$; thus $PSL(2, 3^5)$ is also not 4-rewriteable.

Although 2.3(a) shows that $PSL(2, p)$, $p$ prime, is not 4-rewriteable for $p > 1656$, using a different technique we are able to show that $PSL(2, p)$ is not 4-rewriteable for $p \geqslant 5$.

PROPOSITION 3.5. *For each prime $p \geqslant 5$ and positive integer $m$, the group $PSL(2, p^m)$ is not 4-rewriteable.*

*Proof.* It suffices to show that $PSL(2, p)$ is not rewriteable for each $p \geqslant 5$.

We first provide a generic example for $p > 7$. Choose $c$ to be a generator of the multiplicative subgroup of $GF(p)$ such that $c^2 \neq -2$ (modulo $p$) and $c^{-2} \neq -2$ (modulo $p$). The existence of such a $c$ is guaranteed provided that $\varphi(p-1) > 5$, where $\varphi(n)$ is the number of integers $i$, $1 \leqslant i \leqslant n$, such that $(i, n) = 1$. Since $\varphi(n) > 5$ for $n > 12$, $\varphi(p-1)$ is greater than 5 for $p > 13$. For $p = 11$, the choice $c = 2$ has the required properties, as does the choice $c = 2$ for $p = 13$. Therefore we can find a generator $c$ of the required type for each prime $p > 7$.

Choose the elements $A$, $B$, $C$, and $D$ of $SL(2, p)$ to be

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} c^{-1} & c^{-1} \\ 0 & c \end{pmatrix},$$

$$C = \begin{pmatrix} c^{-2} & c^{-2} \\ 0 & c^2 \end{pmatrix}, \quad \text{and} \quad D = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

We classify the 24 possible products arising by their (2, 1)-entries:

$$\text{I:} \quad \begin{pmatrix} c^{-3} & c^{-3}+c+c^3 \\ c^{-3} & c^{-3}+c+2c^3 \end{pmatrix}, \begin{pmatrix} c^{-3} & c^{-3}+c^{-1}+c^3 \\ c^{-3} & c^{-3}+c^{-1}+2c^3 \end{pmatrix},$$

$$\begin{pmatrix} c^{-3} & c^{-3}+2c \\ c^{-3} & c^{-3}+2c+c^3 \end{pmatrix}, \begin{pmatrix} c^{-3} & 2c^{-3}+c \\ c^{-3} & 2c^{-3}+c+c^3 \end{pmatrix},$$

$$\begin{pmatrix} c^{-3} & c^{-3}+2c^{-1} \\ c^{-3} & c^{-3}+2c^{-1}+c^3 \end{pmatrix}, \begin{pmatrix} c^{-3} & 2c^{-3}+c^{-1} \\ c^{-3} & 2c^{-3}+c^{-1}+c^3 \end{pmatrix},$$

$$\begin{pmatrix} 2c^{-3} & 2c^{-3}+2c+c^3 \\ c^{-3} & c^{-3}+c+c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3} & 2c^{-3}+2c^{-1}+c^3 \\ c^{-3} & c^{-3}+c^{-1}+c^3 \end{pmatrix}$$

II: $\begin{pmatrix} 2c^{-3}+c+c^3 & c^{-3}+c+c^3 \\ c^3 & c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3}+c^{-1}+c^3 & c^{-3}+c^{-1}+c^3 \\ c^3 & c^3 \end{pmatrix},$

$\begin{pmatrix} 2c^{-3}+2c & c^{-3}+2c \\ c^3 & c^3 \end{pmatrix}, \begin{pmatrix} 3c^{-3}+c & 2c^{-3}+c \\ c^3 & c^3 \end{pmatrix},$

$\begin{pmatrix} 2c^{-3}+2c^{-1} & c^{-3}+2c^{-1} \\ c^3 & c^3 \end{pmatrix}, \begin{pmatrix} 3c^{-3}+c^{-1} & 2c^{-3}+c^{-1} \\ c^3 & c^3 \end{pmatrix},$

$\begin{pmatrix} 2c^{-3}+c & 3c^{-3}+2c \\ c^3 & 2c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3}+c^{-1} & 3c^{-3}+2c^{-1} \\ c^3 & 2c^3 \end{pmatrix}.$

III: $\begin{pmatrix} 2c^{-3}+c^{-1} & 2c^{-3}+c^{-1}+c+c^3 \\ c^{-1} & c^{-1}+c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3} & 2c^{-3}+3c \\ c^{-1} & c^{-1}+2c^3 \end{pmatrix},$

$\begin{pmatrix} 3c^{-3} & 3c^{-3}+2c \\ c^{-1} & c^{-1}+c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3} & 4c^{-3}+c \\ c^{-1} & 2c^{-1}+c^3 \end{pmatrix}.$

IV: $\begin{pmatrix} 2c^{-3}+c & 2c^{-3}+c^{-1}+c+c^3 \\ c & c+c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3} & 2c^{-3}+3c^{-1} \\ c & c+2c^3 \end{pmatrix},$

$\begin{pmatrix} 3c^{-3} & 3c^{-3}+2c^{-1} \\ c & c+c^3 \end{pmatrix}, \begin{pmatrix} 2c^{-3} & 4c^{-3}+c^{-1} \\ c & 2c+c^3 \end{pmatrix}.$

We observe first that products in different classes are distinct modulo $\langle -1_2 \rangle$, chiefly by comparing the (2, 1)-entries of the product matrices. The only situation not covered by comparing (2, 1)-entries arises when $p = 13$, for which $c^{-3} \equiv -c^3$ (modulo 13). In this case we chose $c = 2$, and explicit calculations give 0, 2, 4, 7, 1, 12, 2, and 7 (modulo 13) for the (2, 2)-entries of the matrices in class I, and 5 and 10 (modulo 13) for the additive inverses of the (2, 2)-entries of the matrices in class II. Thus it suffices to show that the products within each class are distinct. Since $2c^{-3}$, $2c^3$, $2c^{-1}$, and $2c$ are all nonzero (modulo $p$), two products within a class which are equal in $PSL(2, p)$ must be equal as elements of $SL(2, p)$. The details of the comparisons of the entries within each class are left to the reader; in the comparisons within classes I and II, the facts $c^2 \not\equiv -2$ (modulo $p$) and $c^{-2} \not\equiv -2$ (modulo $p$) are required. Since all 24 products are distinct as elements of $PSL(2, p)$, the group $PSL(2, p)$ is not 4-rewriteable for $p > 7$.

We observed in 3.3 that $PSL(2, 5) \cong \mathrm{Alt}(5)$ is not 4-rewriteable. Finally, the subset $\{\left(\begin{smallmatrix} 3 & 0 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 1 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 1 & 5 \end{smallmatrix}\right)\}$ of elements of $SL(2, 7)$ produces 24 products which are distinct modulo $Z(SL(2, 7)) = \langle -1_2 \rangle$. This completes the proof.

PROPOSITION 3.6. *The group $PSL(3, 3)$ is not 4-rewriteable.*

*Proof.* The subset

$$\left\{\begin{pmatrix}2&0&0\\0&1&0\\0&0&2\end{pmatrix},\begin{pmatrix}1&1&1\\0&1&2\\0&0&1\end{pmatrix},\begin{pmatrix}1&0&0\\0&2&0\\2&2&2\end{pmatrix},\begin{pmatrix}0&2&1\\1&0&1\\1&0&2\end{pmatrix}\right\}$$

of elements of $SL(3,3)\cong PSL(3,3)$ is not rewriteable.

PROPOSITION 3.7. *For each positive integer $m$, the Suzuki group $Sz(2^{2m+1})$ is not 4-rewriteable.*

*Proof.* For $m\geqslant 3$ we provide a generic example. Let $q=2^{2m+1}$ and $r=2^m$. The Suzuki group $G=Sz(q)$ has a cyclic subgroup $U_1=\langle a\rangle$ of order $q+2r+1$, with normalizer $N_G(U_1)=\langle U_1, x\rangle$, where $u^x=u^q$ for each $u\in U_1$, and $|N_G(U_1):U_1|=4$ (see [6]). Consider the subset $\{a, xa, xa^3, xa^5\}$ of elements in $\langle x\rangle\ltimes\langle a\rangle=N_G(U_1)$. Each of the 24 products arising may be expressed in the form $x^3a^z$, where $z$ is a linear combination of powers of $q$. Using $q^2\equiv -1$ (modulo $q+2r+1$) and $q\equiv -2r-1$ (modulo $q+2r+1$), we may reduce each $z$ to a linear expression in $r$. In this form it is easy to see that the powers $z$ arising are all distinct as integers as long as $r>4$, that is, for $m\geqslant 3$. Furthermore, the largest difference in powers $z$ arising is $12r+10$, which is less than $q+2r+1$ whenever $m\geqslant 3$. It follows that all 24 products are distinct as elements of $\langle x\rangle\ltimes\langle a\rangle$, and therefore that the group $Sz(2^{2m+1})$ is not 4-rewriteable for $m\geqslant 3$.

For the group $Sz(2^3)$, let the underlying field $GF(2^3)$ consist of elements of the form $a+b\omega+c\omega^2$, where $a, b, c\in GF(2)$ and $\omega$ is a root of the primitive irreducible polynomial $x^3-x-1$ over $GF(2)$. Let

$$S(1,1)=\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&1&1&0\\1&0&1&1\end{pmatrix},\qquad S(1,\omega)=\begin{pmatrix}1&0&0&0\\1&1&0&0\\\omega&1&1&0\\\omega^2+1&\omega+1&1&1\end{pmatrix},$$

$$M(\omega)=\begin{pmatrix}\omega+1&0&0&0\\0&\omega^2&0&0\\0&0&\omega^2+\omega+1&0\\0&0&0&\omega^2+\omega\end{pmatrix},$$

and

$$T=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix},$$

which are elements of $Sz(2^3)$. Computer calculations show that the subset $\{S(1, 1), T^{-1}S(1, \omega)\, T, M(\omega), T\}$ is not rewriteable. Finally, let $GF(2^5)$ consist of elements of the form $a + b\omega + c\omega^2 + d\omega^3 + e\omega^4$, where $a, b, c, d, e \in GF(2)$ and $\omega$ is a root of the primitive irreducible polynomial $x^5 - x^2 - 1$ over $GF(2)$. We choose the elements

$$S(1, 1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \qquad S(1, \omega) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \omega & 1 & 1 & 0 \\ \omega^3 + \omega^2 + \omega & \omega + 1 & 1 & 1 \end{pmatrix},$$

$$M(\omega) = \begin{pmatrix} \omega^2 + 1 & 0 & 0 & 0 \\ 0 & \omega^4 & 0 & 0 \\ 0 & 0 & \omega^3 + \omega + 1 & 0 \\ 0 & 0 & 0 & \omega^4 + \omega^2 + \omega + 1 \end{pmatrix},$$

and

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

of $Sz(2^5)$. The subset $\{S(1, 1), T^{-1}S(1, \omega)\, T, M(\omega), T\}$ of elements of $Sz(2^5)$ is not rewriteable.

This result completes the proof of 3.1.

## Acknowledgment

The author expresses his thanks to Professor Derek Robinson for his patient guidance as the author's Ph. D. thesis advisor from 1984 to 1987.

## References

1. M. Bianchi, R. Brandi, and A. G. B. Mauri, On the 4-permutational property for groups, *Arch. Math. (Basel)* **48** (1987), 281–285.
2. R. D. Blyth, Rewriting products of group elements—I, *J. Algebra* **116** (1988), 506–521.
3. N. Bourbaki, "Élements de Mathématique," Fasc. XXXIV, Groupes et algèbres de Lie IV–VI, Hermann, Paris, 1968.
4. R. W. Carter, "Simple Groups of Lie Type," Pure and Applied Mathematics, Vol. 28, Wiley, New York, 1972.

5. C. CHEVALLEY, Sur certains groupes simples, *Tôhoku Math. J. (2)* **7** (1955), 14–66.
6. B. HUPPERT AND N. BLACKBURN, "Finite Groups III," Grundlehren der mathematischen Wissenschaften, Band 243, Springer-Verlag, Berlin, 1982.
7. G. A. JONES, Varieties and simple groups, *J. Austral. Math. Soc.* **17** (1974), 163–173.
8. P. LONGOBARDI AND M. MAJ, Sui gruppi per cui ogni prodotto di quattro elementi è riordinabile, preprint.
9. H. LÜNEBURG, Some remarks concerning the Ree groups of type $(G_2)$, *J. Algebra* **3** (1966), 256–259.
10. D. J. S. ROBINSON, "A Course in the Theory of Groups," Graduate Texts in Mathematics, Vol. 80, Springer-Verlag, New York, 1982.
11. M. SUZUKI, "Group Theory I," Grundlehren der mathematischen Wissenschaften, Band 247, Springer-Verlag, Berlin, 1982.
12. J. G. THOMPSON, Nonsolvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.* **74** (1968), 383–437.
13. J. TITS, Les groupes simples de Suzuki et de Ree, *Séminaire Bourbaki* **13** (1960–1961), exposé 210.

*Printed in Belgium*