J. Austral. Math. Soc. (*Series A*) **48** (1990), 333–346

ON PRESENTATIONS OF $PSL(2, p^n)$

C. M. CAMPBELL, E. F. ROBERTSON and P. D. WILLIAMS

(Received 6 January 1988)

Communicated by H. Lausch

Abstract

We give presentations for the groups $PSL(2, p^n)$, p prime, which show that the deficiency of these groups is bounded below. In particular, for $p = 2$ where $SL(2, 2^n) = PSL(2, 2^n)$, we show that these groups have deficiency greater than or equal to -2. We give deficiency -1 presentations for direct products of $SL(2, 2^{n_i})$ for coprime n_i. Certain new efficient presentations are given for certain cases of the groups considered.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 20 F 05; Secondary 20 D 06, 20 G 40.

1. Introduction

For any field F let $SL(2, F)$ denote the group of 2×2 matrices of determinant 1 over F and let $PSL(2, F)$ denote the factor of $SL(2, F)$ by its centre. When $F = GF(p^n)$ we write $SL(2, p^n)$ and $PSL(2, p^n)$ respectively. Considerable effort has, over the years, been put into finding presentations of $PSL(2, p)$ with a small number of defining relations; see [15], [18]. However, except for a few cases of particular values of p and n, nothing appears in the literature on the corresponding problem of finding presentations with a small number of defining relations for $PSL(2, p^n)$, $n \geq 2$.

Presentations of $PSL(2, p^n)$ with the number of defining relations increasing with n are given by Bussey [3], Todd [16], Sinkov [14] and Beetham [1]. The Beetham presentation is particularly pleasing because of the symmetry

P. D. Williams wishes to thank the Carnegie Trust for the Universities of Scotland for a grant enabling him to carry out this work at the University of St Andrews.

displayed. In order to describe a lower bound on the number of defining relations we introduce some terminology (see [12]).

Let G be a finite group. If G has a finite presentation $\langle X|R\rangle$ then the *deficiency of the presentation* is $|X|-|R|$. The *deficiency* of G is the maximum of the deficiencies of all finite presentations of G and is denoted by $\operatorname{def} G$. An upper bound for $\operatorname{def} G$ is given in terms of the rank of the Schur multiplier $M(G)$ of G,

$$-\operatorname{def} G \geq \text{ minimal number of generators of } M(G). \tag{1.1}$$

A group G is said to be *efficient* if equality holds in (1.1). The Schur multiplier of $PSL(2,p^n)$ is given in [10]. We have that $M(PSL(2,p^n))$ is a non-trivial cyclic group if p is odd or $p=2$ and $n=2$ while for $n \geq 3$, $M(PSL(2,2^n)) = 1$. Note that $PSL(2,2^n) = SL(2,2^n)$.

We consider the deficiency of $PSL(2,p^n)$, p odd, and $SL(2,2^n)$ in Sections 2 and 3 respectively. Although we are unable to show that these groups are efficient in general we show in both cases that the deficiency does not decrease with n. In particular, we show that

$$-2 \leq \operatorname{def}(SL(2,2^n)) \leq 0.$$

Indeed for many values of n, Theorem 3.4 shows that $\operatorname{def}(SL(2,2^n)) \geq -1$. The methods of Sections 2 and 3 are used in Section 4 to give deficiency -1 presentations for direct products of $SL(2,2^{n_i})$ for coprime n_i.

The notation used is standard, for example $[x,y] = x^{-1}y^{-1}xy = x^{-1}x^y$. The field notation and terminology is as in Cohn [9] except the definition of the period of the polynomial $f(t)$ which is the least l such that $f(t)$ divides $t^l - 1$, see [2].

2. Presentations of $PSL(2,p^n)$, p an odd prime, $n \geq 2$

Let p be an odd prime and let α be a primitive zero of the irreducible polynomial $m(t)$ over $GF(p)$ where

$$m(t) = t^n - \sum_{i=0}^{n-1} a_i t^i.$$

Consider the matrices

$$\overline{W} = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, \quad \overline{X} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \overline{Y} = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}, \quad \overline{Z} = \begin{bmatrix} \alpha & \alpha^{-1} \\ 0 & \alpha^{-1} \end{bmatrix},$$

over the field $GF(p^n)$ and denote by W, X, Y and Z respectively their images under the canonical morphism from $SL(2,p^n)$ onto $PSL(2,p^n)$. Let $S_{2i} =$

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

Z^iXZ^{-i}, $0 \le i \le [(n+1)/2]$ and $S_{2i+1} = Z^iYZ^{-i}$, $0 \le i \le [n/2]$. It is easy to check that $\{W, X, Y, Z\}$ is a set of generators for $PSL(2,p^n)$ and satisfy the relations of the group

(2.1)

$$G = \Big\langle w,x,y,z \mid w^3 = (wz)^2 = (wx)^2 = (wyz)^3 = x^p = y^p = z^{(p^n-1)/2} = 1,$$
$$s_{2i} = z^ixz^{-i}, 0 \le i \le [(n+1)/2], s_{2i+1} = z^iyz^{-i}, 0 \le i \le [n/2],$$
$$[x,s_i] = [y,s_i] = 1, 1 \le i \le n-1, s_n = \prod_{i=0}^{n-1} s_i^{a_i}, s_{n+1} = \prod_{i=0}^{n} s_i^{a_{i-1}} \Big\rangle.$$

It is shown in [14] that in fact $G \cong PSL(2,p^n)$.

Now $\langle S_0, S_1, S_2, \ldots, S_{n-1}\rangle$ is the image of the upper triangular subgroup of $SL(2,p^n)$ in $PSL(2,p^n)$ so $U = \langle s_0, s_1, s_2, \ldots, s_{n-1}\rangle$ is abelian and $\theta: s_i \to \alpha^i$, $0 \le i \le n-1$ induces an isomorphism onto the additive group of $GF(p^n)$. Now the elements of $GF(p^n)$ are of the form $f(\alpha)$ where $f(t)$ is a polynomial over $GF(p)$ of the form

$$f(t) = c_0 + c_1t + \cdots + c_{r-1}t^{r-1}.$$

The inverse image of $f(\alpha)$ under θ is $s_0^{c_0}s_1^{c_1}\cdots s_{n-1}^{c_{n-1}}$ and we denote this preimage by s^f. Notice that in this notation the last two relations of (2.1) may be written as $s^{m(t)} = 1$ and $s^{tm(t)} = 1$. Notice also that if $f(t)$ is any polynomial over $GF(p)$ with $f(\alpha) = 0$ then $s^{f(t)} = 1$ in (2.1). Further, $H = \langle U, z\rangle = \langle x, y, z\rangle$ is isomorphic to the image of the upper triangular subgroup of $SL(2,p^n)$ in $PSL(2,p^n)$ and has order $p^n(p^n-1)/2$. The presentation (2.1) contains $2n+7$ relations some of which could be easily eliminated but we aim to make a substantial reduction in the number of relations. In order to do this we introduce the groups K

$$\langle a, b_0, b_1 \mid a^l = b_0^p = b_1^p = [b_0, b_j] = [b_1, b_{j+1}] = 1, b_k = b_0^d b_j^e, b_{k+1} = b_1^d b_{j+1}^e\rangle$$

where

(K1) p is an odd prime and $l = (p^n-1)/2$;

(K2) $e^2 \not\equiv (d-1)^2 \pmod p$ if k is even,
$d^2 \not\equiv (e-1)^2 \pmod p$ if k is odd;

(K3) j is odd and $(j,l) = 1$;

(K4) $b_{2i} = a^ib_0a^{-i}$, $b_{2i+1} = a^ib_1a^{-i}$.

The next theorem relates the order of the derived group of K to the number of distinct zeros of a trinomial. It uses a method of proof similar to that in [7, Theorem 3].

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

THEOREM 2.1. *The group K is metabelian with K' elementary abelian of order p^ν where ν is the number of distinct zeros in $GF(p^n)$ of the trinomial $d + et^j - t^k$ over $GF(p)$.*

PROOF. Modulo K', using (K3), we have $b_j = b_1$, $b_{j+1} = b_0$. Now the conditions (K2) imply that, modulo K', $b_0 = b_1 = 1$ so $b_0, b_1 \in K'$. Hence K/K' is cyclic of order l. We use the Reidemeister-Schreier algorithm to give a presentation for K' on the Schreier generators

$$r_i = a^{i-1}b_0a^{1-i}, \quad s_i = a^{i-1}b_1a^{1-i} \qquad (1 \le i \le l).$$

The following presentation is obtained:

$$(2.2)\quad K' = \langle r_i, s_i | r_i^p = s_i^p = [r_i, s_{i+h}] = [r_{i+h+1}, s_i] = 1, v_i = r_i^d s_{i+h}^e, \\ w_i = s_i^d r_{i+h+1}^e, 1 \le i \le l \rangle$$

where $h = (j-1)/2$ and if $k = 2m$ say, $v_i = r_{i+m}$, $w_i = s_{i+m}$ while if $k = 2m+1$ then $v_i = s_{i+m}$, $w_i = r_{i+m+1}$ where the subscripts are reduced modulo l. A similar argument to that used in [4, Theorem 3.3] shows that K' is abelian. Finally, we obtain the order of K' where k is even, the case for k odd being similar. The relation matrix for K' has the form $\begin{bmatrix} M \\ pI \end{bmatrix}$ where I is the $2l \times 2l$ identity matrix and M is a $2l \times 2l$ circulant matrix formed as follows. Let the odd columns of M be indexed by the r_i and the even columns indexed by the s_i. The first row of M contains the integers d, e, -1 in positions 1, j, $k-1$ respectively and zero elsewhere. Now the rank of M is $2l - \nu$ which can be proved by taking the product of M and the Vandermonde matrix with rows $1, \beta, \ldots, \beta^{2l-1}$, $\beta \in GF(p^n) \setminus \{0\}$, (see [9, page 211]). Hence $|K'| = p^\nu$.

The fact that (2.2) defines an abelian group allows us to replace most of the commutators in presentation (2.1) by two relations.

THEOREM 2.2. *Let α be a primitive element of $GF(p^n)$ which is a zero of the irreducible polynomial $m(t)$ over $GF(p)$. There exists some trinomial $f(t)$ over $GF(p)$*

$$f(t) = d + et^j - t^k$$

satisfying (K1), (K2) *and* (K3) *with $f(\alpha) = 0$. Then $PSL(2, p^n)$ has presentation*

$$(2.3)\quad \langle w, x, y, z | w^3 = (wx)^2 = (wz)^2 = (wyz)^3 = x^p = y^p = z^l \\ = [x, s_j] = [y, s_{j+1}] = s^{m(t)} = s^{tm(t)} = s^{f(t)} = s^{tf(t)} = 1 \rangle$$

where s_i is defined as in (2.1).

PROOF. Since α is primitive in $GF(p^n)$ there is a positive integer k for which $1 + \alpha = \alpha^k$ so $f(t) = 1 + t - t^k$ is an appropriate trinomial. Note that

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

there may be other such trinomials f and we need only assume the conditions on f as in the statement of the theorem. Since $f(\alpha)=0$ we have noted that $s^{f(t)}=s^{tf(t)}=1$ are consequences of the relations of (2.1). We adjoin these relations. Now $z=a$, $x=b_0$, $y=b_1$ satisfy the relations of K so the proof of Theorem 2.1 shows that all the commutator relations $[x,s_i]=[y,s_i]=1$, $1\le i\le n-1$, are redundant except the two relations $[x,s_j]=[y,s_{j+1}]=1$ and this completes the proof.

Notice that the presentation (2.3) has a fixed number of relations in contrast to those previously known for $PSL(2,p^n)$ where the number of relations increases with n, see for example [1] and [14]. With some additional conditions a further reduction in the number of relations is possible.

COROLLARY 2.3. *If the trinomial $d+et^j-t^k$ has precisely n zeros in $GF(p^n)$ then the relations $s^{m(t)}=s^{tm(t)}=1$ are redundant in* (2.3). *Moreover, if $p^n\equiv -1 \pmod 4$ the relation $(wyz)^3=1$ is also redundant.*

PROOF. Let G be the group presented by (2.3) with $s^{m(t)}=s^{tm(t)}=1$ omitted. Let $L=\langle s^{m(t)}, s^{tm(t)}\rangle$, $N=L^G$ and $H=\langle x,y,z\rangle$. By Theorem 2.2, $G/N\cong PSL(2,p^n)$. Clearly $L\le H\cap N$ but HN/N, being isomorphic to the canonical image of the upper triangular matrices in $PSL(2,p^n)$, has order $p^n(p^n-1)/2$. Now, using Theorem 2.1,

$$|H|\le |K|=((p^n-1)/2)|K'|=p^n(p^n-1)/2.$$

Therefore $|H|\le |HN/N|$ and so $H\cap N=1$. Hence $L=1$ as required. The proof that the relation $(wyz)^3=1$ is redundant when $p^n\equiv -1 \pmod 4$ is given in [16].

The case where $p^n\equiv -1 \pmod 4$ is particularly amenable and a considerable shortening can be achieved beyond that given in Corollary 2.3. We give a deficiency -4 presentation in this case.

THEOREM 2.4. *Suppose $p^n\equiv -1 \pmod 4$, α is a primitive element of $GF(p^n)$ and a zero of the irreducible polynomial $m(t)$. Let k be such that $1+\alpha=\alpha^k$. Thus $PSL(2,p^n)$ may be presented by*

(2.4)

$$\langle w,x,z \mid w^3=(wx)^2=(wz)^2=s^{m(t)}=[x,z^qxz^{-q}]=1,\ z^l=x^p,\ z^rxz^{-r}=u\rangle$$

where $l=(p^n-1)/2$, $q=(p^n+1)/4$, $r=[k/2]$ and $u=xz^{(-1)^kq}x^{-1}z^{(-1)^{k+1}q}$. In (2.4) *$s^{m(t)}$ is to be interpreted as a word in x,y as above with y replaced by $z^qx^{-1}z^{-q}$.*

PROOF. First note that $2q=l+1$. As α is primitive in $GF(p^n)$, $\alpha^l=-1$ and so $\alpha^{2q}=-\alpha$. Now (2.3) defines $PSL(2,p^n)$ and working with matrices

modulo $\{\pm I\}$ we see that

$$z^q x z^{-q} = y^{-1} \tag{2.5}$$

and we add this relation to (2.3). Use (2.5) to eliminate y. The defining relations of (2.3) become

$$\begin{cases} w^3 = (wx)^2 = (wz)^2 = [x, z^q x z^{-q}] = z^l = x^p = s^{m(t)} = 1, \\ s_k = x z^q x^{-1} z^{-q}, \end{cases} \tag{2.6}$$

$$s^{tm(t)} = [z^q x z^{-q}, z x z^{-1}] = 1, s_{k+1} = z^q x^{-1} z^{1-q} x z^{-1}. \tag{2.7}$$

The main part of the proof consists in proving that the relations (2.7) are implied by (2.6). First notice that $z^q s_{2i} z^{-q} = z^{q+i} x z^{-(q+i)} = z^i (z^q x z^{-q}) z^{-i} = s_{2i+1}^{-1}$ and similarly $z^q s_{2i+1} z^{-q} = s_{2i+2}^{-1}$. Thus

$$z^q s_i z^{-q} = s_{i+1}^{-1}. \tag{2.8}$$

(i) $s^{tm(t)} = 1$ is redundant. From (2.8) using the fact that the s_i's commute (see the proof of Theorem 2.2) we obtain

$$z^q s^{m(t)} z^{-q} = s^{-tm(t)}.$$

Since $s^{m(t)} = 1$ the proof of (i) is complete.

(ii) $[z^q x z^{-q}, z x z^{-1}] = 1$ is redundant. Using $z^{2q-1} = 1$ we have

$$[z^q x z^{-q}, z x z^{-1}]^{z^q} = [x, z^{1-q} x z^{q-1}] = [x, z^q x z^{-q}] = 1$$

so proving (ii).

(iii) The relation $s_{k+1} = z^q x^{-1} z^{1-q} x z^{-1}$ is redundant. From (2.8)

$$\begin{aligned} s_{k+1} &= z^q s_k^{-1} z^{-q} = z^q z^q x z^{-q} x^{-1} z^{-q} \\ &= z^q x^{-1} z^q x z^{-2q} = z^q x^{-1} z^{1-q} x z^{-1} \end{aligned}$$

as required.

Finally, we can combine the relations $z^l = x^p = 1$ into the single relation $z^l = x^p$. For x^p commutes with z and so raising $z^r x z^{-r} = u$ to the power p gives $x^p = 1$.

REMARK. In the case where $GF(p^n)$ has an element α satisfying a trinomial $m(t)$ (not necessarily irreducible) with properties (K1), (K2) and (K3) such that $m(t)$ has exactly n zeros in $GF(p^n)$ then the methods of Theorem 2.2 and Corollary 2.3 show that the last relation in the presentation given in the statement of Theorem 2.4 may be omitted.

EXAMPLE 2.5. The trinomial $t^3 - t - 2$ is irreducible over $GF(3)$ and is satisfied by a primitive element α of $GF(3^3)$. Now $1 + \alpha = \alpha^9$ and so from Theorem 2.4 we have the following presentation of $PSL(2, 3^3)$:

$$\langle w, x, z | w^3 = (wx)^2 = (wz)^2 = [x, z^7 x z^{-7}] = 1, z^{13} = x^3, \\ z^8 x^{-1} z^{-1} x z^{-7} x^{-2} = 1, z^4 x z^{-4} = x z^{-7} x^{-1} z^7 \rangle.$$

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

The trinomial t^9-t-1 has exactly three zeros in $GF(3^3)$ and by the preceding remark either of the last two relations may be omitted. Thus we have a deficiency -3 presentation of $PSL(2,3^3)$.

Although the results of this section show that $PSL(2,p^n)$ may in general be presented with three generators and a small number of relations we are able to show that for small values of p and n, the groups $PSL(2,p^n)$ are efficient, that is they have deficiency -1 presentations. An efficient presentation of $PSL(2,3^2)\cong A_6$ is given in [6]. Efficient presentations of $PSL(2,3^3)$, $PSL(2,5^2)$ and $PSL(2,7^2)$ are given in [8], see also [7].

We have used various computational techniques which are similar to those described in [8, Section 5] to obtain efficient presentations of $PSL(2,p^n)$ for other values of p^n. We have obtained efficient presentations for $PSL(2,3^4)$, $PSL(2,5^3)$, $PSL(2,11^2)$, $PSL(2,13^2)$ and $PSL(2,19^2)$. We list these together with two matrices which generate the corresponding group SL and whose images in PSL satisfy the given presentation.

(i)

$$PSL(2,3^4)=\langle a,b \mid a^2=b^3 = (ab)^2(ab^{-1})^4ab(ab^{-1})^3(ab)^5(ab^{-1})^3ab(ab^{-1})^4=1\rangle,$$

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix}\to a,\quad \begin{pmatrix}\alpha^{46}&\alpha^{73}\\ \alpha^{75}&\alpha^{35}\end{pmatrix}\to b,$$

where the minimum polynomial of α is $1+2t^3-t^4$.

$$PSL(2,3^4)=\langle a,b \mid a^2=b^3 = abab^{-1}(ab)^3ab^{-1}(ab)^3(ab^{-1})^4((ab)^3ab^{-1})^2=1\rangle,$$

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix}\to a,\quad \begin{pmatrix}\alpha&\alpha\\ \alpha^{33}&\alpha^{28}\end{pmatrix}\to b,$$

where the minimum polynomial of α is $1+2t^3-t^4$.

(ii)

$$PSL(2,5^3)=\langle a,b \mid a^2=b^3=(ab)^4(ab^{-1})^{14}(ab)^4(ab^{-1})^{-7}=1\rangle,$$

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix}\to a,\quad \begin{pmatrix}\alpha^4&\alpha^{32}\\ \alpha^{35}&\alpha^{106}\end{pmatrix}\to b,$$

where the minimum polynomial of α is $3+4t^2-t^3$.

$$PSL(2,5^3)=\langle a,b \mid a^2=b^3=(ab)^3(ab^{-1})^{10}(ab)^3(ab^{-1})^{-21}=1\rangle,$$

$$\begin{pmatrix}0&-1\\1&0\end{pmatrix}\to a,\quad \begin{pmatrix}\alpha^2&\alpha^{17}\\ \alpha^{105}&\alpha^{51}\end{pmatrix}\to b,$$

where the minimum polynomial of α is $3+4t^2-t^3$.

(iii)

$$PSL(2,11^2) = \langle a,b \mid b^3 = a^{11},$$
$$(ba^4ba^7)^2 = ba^{-2}b^{-1}a^3ba^2b^{-1}a^3ba^{-2}b^{-1}a^{-3} = 1\rangle,$$
$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \to a, \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \to b,$$

where the minimum polynomial of α is $2 - t^2$.

(iv)

$$PSL(2,13^2) = \langle a,b \mid a^2 = b^3 = ((ab)^5(ab^{-1})^5)^2(ab)^6(ab^{-1})^8ab = 1\rangle,$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \to a, \quad \begin{pmatrix} \alpha^5 & \alpha^{41} \\ \alpha^{46} & \alpha^{21} \end{pmatrix} \to b,$$

where the minimum polynomial of α is $2 + t + t^2$.

(v)

$$PSL(2,19^2) = \langle a,b \mid a^2 = b^3 = (ab)^2(ab^{-1})^5(ab)^9(ab^{-1})^9(ab)^9(ab^{-1})^5 = 1\rangle,$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \to a, \quad \begin{pmatrix} \alpha^5 & \alpha^{141} \\ \alpha^{172} & \alpha^{104} \end{pmatrix} \to b,$$

where the minimum polynomial of α is $2 + t + t^2$.

3. Presentations of $SL(2,2^n)$, $n \geq 2$

Similar methods to those used in Section 2 work for $p = 2$. However, it is possible in this case to obtain neater presentations. With notation analogous to that in Section 2 a presentation for $SL(2,2^n)$ is

(3.1) $$\langle w,x,z \mid w^3 = (wx)^2 = (wz)^2 = z^l = x^2 = s^{m(t)} = [x, z^i x z^{-i}] = 1, 1 \leq i \leq n-1\rangle$$

where $l = 2^n - 1$ and $m(t)$ is an irreducible polynomial over $GF(2)$ satisfied by a primitive element α of $GF(2^n)$, see for example [14]. Matrices corresponding to the generators w, x and z may be taken to be, respectively,

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \alpha^{(l+1)/2} & \alpha^{(l-1)/2} \\ 0 & \alpha^{(l-1)/2} \end{pmatrix}.$$

In an analogous way to the definition of the groups K in Section 2 we define the groups K^*

$$K^* = \langle a,b \mid a^l = b^2 = 1, a^k b a^{-k} = b a^j b a^{-j}\rangle$$

where

(K*1) $$l = 2^n - 1,$$

(K*2) $$(j,l) = 1.$$

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

THEOREM 3.1. *K^* is a metabelian group and $K^{*\prime}$ is elementary abelian of order 2^ν where ν is the number of distinct zeros in $GF(2^n)$ of the trinomial $1+t^j+t^k$ over $GF(2)$.*

PROOF. The proof is essentially the same as that of Theorem 2.1 except that in this case the derived group of K^* is generated by the Schreier generators $r_i = a^{i-1}ba^{1-i}$, $i = 1,2,\ldots,l$, and a presentation for $K^{*\prime}$ on these generators is:

$$\langle r_1, r_2, \ldots, r_l | r_i^2 = 1, r_{i+k} = r_i r_{i+j}, i = 1,2,\ldots,l\rangle$$

where the subscripts are reduced modulo l.

Notice that since $K^{*\prime}$ is abelian any two conjugates of b by powers of a commute. We now add a relation to (3.1) so that $z = a, x = b$ satisfy the relations of K^*. This enables us to remove the $n-1$ commutator relations of (3.1).

THEOREM 3.2. *Let $l = 2^n - 1$ and let α be a primitive element of $GF(2^n)$ which is a zero of the irreducible polynomial $m(t)$ over $GF(2)$. Then there exists some trinomial*

$$f(t) = 1 + t^j + t^k$$

with $(j,l) = 1$ and $f(\alpha) = 0$. Then $SL(2,2^n)$ has a presentation

$$\langle w, x, z | w^3 = (wx)^2 = (wz)^2 = z^l = x^2 = s^{m(t)} = s^{f(t)} = 1\rangle. \tag{3.2}$$

PROOF. Since α is primitive in $GF(2^n)$ there exists a positive integer k for which $1+\alpha = \alpha^k$ so $f(t) = 1 + t + t^k$ is an appropriate trinomial. Add the redundant relation $s^{f(t)} = 1$ to (3.1) and use Theorem 3.1 to eliminate the $n-1$ commutator relations.

Although the proof of the previous theorem exhibits the existence of a particular trinomial, the generality in the statement of the theorem makes it more likely that a trinomial can be found with precisely n zeros in $GF(2^n)$. In that case we have

COROLLARY 3.3. *If the trinomial $f(t)$ has precisely n zeros in $GF(2^n)$ then the relation $s^{m(t)} = 1$ in (3.2) is redundant.*

The presentation for $SL(2,2^n)$ obtained from Corollary 3.3 corresponds to the presentation for the group $\theta(n,k)$ of [7] if we take $j = 1$, $a = x$, $b = x^{-1}z$, $c = wx$.

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

THEOREM 3.4. *The group $SL(2,2^n)$, $n \geq 3$, has a presentation on three generators and five relations given by*

$$\langle w, x, z | w^3 = (wx)^2, (wz)^2 = z^l = x^2, s^{m(t)} = s^{f(t)} = 1 \rangle. \tag{3.3}$$

Moreover, if $f(t)$ has exactly n zeros in $GF(2^n)$, the relation $s^{m(t)} = 1$ is redundant yielding a deficiency -1 presentation of $SL(2,2^n)$.

PROOF. Let G be the group given by (3.3). First note that x^2 is central since $x^2 = z^l$ shows $[x,z] = 1$ and $x^2 = (wz)^2$ shows $[x, wz] = 1$. From $w^3 = (wx)^2$ we obtain $w^{-1}xw = wx^{-1}$. So

$$x^2 = w^{-1}x^2w = wx^{-1}wx^{-1} = (wx)^2x^{-4} = w^3x^{-4}$$

showing that $x^6 = w^3$. Now $x^2 \in Z(G) \cap G'$ but $G/\langle x^2 \rangle \cong SL(2,2^n)$ by Theorem 3.2. Thus $x^2 \in M(SL(2,2^n))$ which is trivial since $n \geq 3$. This shows that $x^2 = w^3 = 1$ and so $G \cong SL(2,2^n)$. If $f(t)$ has exactly n zeros in $GF(2^n)$, $s^{m(t)} = 1$ is redundant by Corollary 3.3.

CONJECTURE 3.5. We conjecture that a trinomial

$$f(t) = 1 + t^j + t^k$$

where $(j, 2^n - 1) = 1$ having exactly n zeros in $GF(2^n)$ always exists.

EXAMPLE 3.6. The trinomial $1 + t^2 + t^{123}$ is irreducible over $GF(2)$ (see [19] for a complete list of irreducible trinomials over $GF(2)$ of degree less than 1000). From Theorem 3.4 a deficiency -1 presentation of $SL(2,2^{123})$ is

$$\langle w, x, z | w^3 = (wx)^2, (wz)^2 = z^l = x^2, z^{123}xz^{-123} = xz^2xz^{-2} \rangle$$

where $l = 2^{123} - 1$.

EXAMPLE 3.7. The trinomial $1 + t^2 + t^9$ is the product of irreducible polynomials as follows:

$$1 + t^2 + t^9 = (1 + t^3 + t^4)(1 + t^2 + t^3 + t^4 + t^5).$$

Hence from Theorem 3.4

$$\langle w, x, z | w^3 = (wx)^2, (wz)^2 = z^l = x^2, z^9xz^{-9} = xz^2xz^{-2} \rangle \tag{3.4}$$

is $SL(2,2^4)$ if $l = 2^4 - 1$ and $SL(2,2^5)$ if $l = 2^5 - 1$.

Note that since the Schur multiplier of $SL(2,2^n)$, $n \geq 3$, is trivial there is a possibility of a deficiency zero presentation of $SL(2,2^n)$. Indeed such presentations have been obtained for $SL(2,2^3)$, $SL(2,2^4)$, $SL(2,2^5)$ and $SL(2,2^6)$ (see [5], [8] and [11]). Since $SL(2,2^2) \cong PSL(2,5) \cong A_5$ it cannot have a deficiency zero presentation but efficient presentations of this group are well known.

4. Direct products

If we take $l = (2^4-1)(2^5-1)$ in presentation (3.4) of Example 3.7 we obtain a group clearly having $SL(2, 2^4)$ and $SL(2, 2^5)$ as homomorphic images and coset enumeration shows this group is $SL(2, 2^4) \times SL(2, 2^5)$. It is interesting to ask what happens in the general case if we relax the conditions on the polynomial $m(t)$.

Let $m(t)$ be any polynomial of degree n and period l over $GF(2)$. Let $G = G(m(t))$ be the group with presentation

$$\langle w, x, z | w^3 = (wx)^2 = (wz)^2 = z^l = x^2 = s^{m(t)} = 1, C \rangle$$

where C denotes the commutator relations $[x, z^i x z^{-i}] = 1$, $1 \leq i \leq n-1$. Theorem 3.2 shows that if $m(t)$ is irreducible and satisfied by a primitive element α of $GF(2^n)$ then the relations C may be replaced by a single relation coming from a trinomial satisfied by α. Notice that in this case, all the zeros of $m(t)$ satisfy the same trinomial. However, if the conditions on $m(t)$ are relaxed, a trinomial satisfied by all the zeros of $m(t)$ may not exist. For example if

$$m(t) = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = (1 + t + t^3)(1 + t^2 + t^3)$$

there can be no trinomial $f(t)$ satisfied by all the zeros of $m(t)$.

The method of replacing C by a single trinomial relation clearly fails for such examples. In this case, coset enumeration shows that $G\left(\sum_{i=0}^{6} t^i\right) = SL(2, 2^3) \times SL(2, 2^3)$.

On the other hand, if $m(t)$ is reducible

$$m(t) = p_1(t)p_2(t) \cdots p_r(t)$$

with $p_i(t)$ irreducible of degree n_i, $n_i \geq 2$, and period $l_i = 2^{n_i} - 1$, $(l_i, l_j) = 1$ for $i \neq j$, then using the Chinese Remainder Theorem a trinomial $f(t)$ can be found which is satisfied by the zeros of $m(t)$. In fact we may choose the trinomial to be of the form $1 + t + t^k$ for some k and this allows C to be replaced by a single relation. Notice that $(l_i, l_j) = 1$ if and only if $(n_i, n_j) = 1$. When $m(t)$ itself is a trinomial satisfying these types of conditions we have the following theorem.

THEOREM 4.1. *Let $p_i(t)$, $1 \leq i \leq r$, be irreducible polynomials over $GF(2)$ of degree n_i. Suppose*

(i) *the period of $p_i(t)$ is $2^{n_i} - 1$, $1 \leq i \leq r$,*

(ii) *the n_i's are pairwise coprime,*

(iii) *$m(t) = \prod_{i=1}^{r} p_i(t) = 1 + t^j + t^n$ where $0 < j < n$,*

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

(iv) $(j,l) = 1$ *where* $l = \prod_{i=1}^{r}(2^{n_i} - 1)$.

The group presented by

$$\langle w, x, z | w^3 = (wx)^2 = (wz)^2 = z^l = x^2 = s^{m(t)} = 1 \rangle \tag{4.1}$$

is $SL(2, 2^{n_1}) \times SL(2, 2^{n_2}) \times \cdots \times SL(2, 2^{n_r})$.

Moreover, if $n_i \geq 3$ *for each* i, *then this group may be presented by the deficiency* -1 *presentation*

$$\langle w, x, z | w^3 = (wx)^2, (wz)^2 = z^l = x^2, s^{m(t)} = 1 \rangle. \tag{4.2}$$

PROOF. The proof consists of three steps.

(a) If $m(t)$ satisfies (i)–(iv) then $G(m(t)) \cong \mathrm{X}_{i=1}^{r} SL(2, 2^{n_i})$.

(b) If $m(t)$ satisfies (i)–(iv) then C can be replaced by the trinomial relation $s^{m(t)} = 1$ so is redundant.

(c) The six relations in (4.1) can be replaced by the four relations in (4.2) when $n_i \geq 3$, $1 \leq i \leq r$.

The proof of (c) is identical to that given in Theorem 3.4 while the argument required for (b) is essentially the same as in Sections 2 and 3. The proof of (a) is rather technical and we merely indicate the method. The approach is to enumerate the cosets of $H = \langle x, z \rangle$ in $G(m(t))$ which generalizes the technique of [16], see also Theorem 3.21 of [17]. This technique shows that H has at most $\prod_{i=1}^{r}(2^{n_i} + 1)$ cosets in $G(m(t))$. Also H has order at most $l2^n$. Finally, the proof is complete on showing that the following generators of the direct product of the SL's satisfy the relations of G:

$$(x_1, x_2, \ldots, x_r) \quad \text{where } x_i = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$(w_1, w_2, \ldots, w_r) \quad \text{where } w_i = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

$$(z_1, z_2, \ldots, z_r) \quad \text{where } z_i = \begin{pmatrix} \alpha_i^{t_i} & \alpha_i^{t_i - 1} \\ 0 & \alpha_i^{t_i - 1} \end{pmatrix}$$

with $t_i = 2^{n_i} - 1$, α_i primitive in $GF(2^{n_i})$ and a zero of $p_i(t)$.

An analogous argument in the case when p is odd gives less satisfactory results. For example one obtains a direct product of SL's factored by the central subgroup $\langle (-I, -I, \ldots, -I) \rangle$.

We have obtained efficient presentations for a small number of direct products, for example, direct products involving fields of the same characteristic:

$$SL(2, 2^2) \times SL(2, 2^3) = \langle a, b | a^2 = b^3 = (ab)^2 (ab^{-1})^3 (ab)^3 (ab^{-1})^9 (ab)^3 (ab^{-1})^3 = 1 \rangle;$$

$$SL(2, 2^2) \times SL(2, 2^3) = \langle a, b | a^2 = b^3 = (abab^{-1}(ab)^3 ab^{-1})^2 (ab)^9 = 1 \rangle;$$

https://doi.org/10.1017/S1446788700035722 Published online by Cambridge University Press

$$PSL(2,5) \times PSL(2,5^2)$$
$$= \langle a, b | a^2 = b^3 = (ababab^{-1})^{12}$$
$$= (ab)^2(ab^{-1})^2(ab)^3(ab^{-1})^2(ab)^2(ab^{-1})^4(ab)^4(ab^{-1})^2(ab)^4(ab^{-1})^4 = 1\rangle;$$

Some direct products involving fields of different characteristics:

$$SL(2,2^3) \times PSL(2,29)$$
$$= \langle a, b | a^2 = b^3 = (ab(ab^{-1})^2)^2 abab^{-1}(ab)^2(ab^{-1})^8(ab)^2ab^{-1} = 1\rangle;$$
$$SL(2,2^2) \times PSL(2,3^2)$$
$$= \langle a, b | a^2 = b^5 = (abab^2ab^{-1})^3 = 1, (ab^2)^5 = (abab^{-1}ab^2)^3\rangle.$$

Notice that direct products of the form

$$PSL(2,p_1) \times PSL(2,p_2) \times \cdots \times PSL(2,p_r)$$

where the p_i are distinct primes are efficient since this direct product is $PSL(2, \mathbf{Z}_m)$ where $m = p_1p_2 \cdots p_r$ and $(m, 6) = 1$ (see [5], [13]).

References

[1] M. J. Beetham, 'A set of generators and relations for the groups $PSL(2, q)$, q odd', *J. London Math. Soc.* **3** (1971), 554–557.

[2] E. R. Berlekamp, *Algebraic coding theory* (McGraw-Hill, 1968).

[3] W. H. Bussey, 'Generational relations for the abstract group simply isomorphic with the group $LF[2, p^n]$', *Proc. London Math. Soc.* (2) **3** (1905), 296–315.

[4] C. M. Campbell and E. F. Robertson, 'Classes of groups related to $F^{a,b,c}$', *Proc. Roy. Soc. Edinburgh Sect. A* **78** (1978), 209–218.

[5] C. M. Campbell and E. F. Robertson, 'A deficiency zero presentation for $SL(2, p)$', *Bull. London Math. Soc.* **12** (1980), 17–20.

[6] C. M. Campbell and E. F. Robertson, 'The efficiency of simple groups of order $< 10^5$', *Comm. Algebra* **10** (1982), 217–225.

[7] C. M. Campbell and E. F. Robertson, 'On a class of groups related to $SL(2, 2^n)$', Computational Group Theory, edited by M. D. Atkinson, pp. 43–49 (Academic Press, London, 1984).

[8] C. M. Campbell, T. Kawamata, I. Miyamoto, E. F. Robertson, and P. D. Williams, 'Deficiency zero presentations for certain perfect groups', *Proc. Roy. Soc. Edinburgh Sect. A* **103** (1986), 63–71.

[9] P. M. Cohn, *Algebra*, Vol. 2 (Wiley, London, 1977).

[10] B. Huppert, *Endliche Gruppen* I (Springer-Verlag, Berlin, 1967).

[11] P. E. Kenne, 'Efficient presentations for three simple groups', *Comm. Algebra* **14** (1986), 797–800.

[12] E. F. Robertson, 'Efficiency of finite simple groups and their covering groups', *Contemp. Math.* **45** (1985), 287–294.

[13] E. F. Robertson and P. D. Williams, 'Efficient presentations of the groups $PSL(2, 2p)$ and $SL(2, 2p)$', *Bull. Canad. Math. Soc.* **32** (1989), 3–10.

[14] A. Sinkov, 'A note on a paper by J. A. Todd', *Bull. Amer. Math. Soc.* **45** (1939), 762–765.

[15] J. G. Sunday, 'Presentations of the groups $SL(2, m)$ and $PSL(2, m)$', *Canad. J. Math.* **24** (1972), 1129–1131.
[16] J. A. Todd, 'A second note on the linear fractional group', *J. London Math. Soc.* **2** (1936), 103–107.
[17] P. D. Williams, *Presentations of linear groups* (Ph. D. thesis, University of St. Andrews, 1982).
[18] H. J. Zassenhaus, 'A presentation of the groups $PSL(2, p)$ with three defining relations', *Canad. J. Math.* **21** (1969), 310–311.
[19] N. Zierler and J. Brillhart, 'On primitive trinomials (mod 2)', *Inform. and Control* **13** (1968), 541–554.

University of St. Andrews
North Haugh
St. Andrews
Fife KY16 9SS
Scotland

University of St. Andrews
North Haugh
St. Andrews
Fife KY16 9SS
Scotland

California State University
5500 University Parkway
San Bernardino, California 92407
U.S.A.