Lifting $(2,k)$-generators of linear groups

A. MARÓTI

MTA Alfréd Rényi Institute of Mathematics
Reáltanoda utca 13-15, H-1053, Budapest, Hungary
e-mail: maroti@renyi.hu

C. TAMBURINI BELLANI

Dipartimento di Matematica e Fisica
Università Cattolica
Via Musei 41, Brescia, Italy
e-mail: c.tamburini@dmf.unicatt.it

Dedicated to Karl Gruenberg

Let $\ell = kh$, where k, h are orders of arbitrary elements of $\mathrm{SL}_2(q)$ subject to $k \geq 3$, $h \geq 3$ and $(k,h) = 1$. For q even allow also $k = 4$ or $h = 2$. We describe $(2,\ell)$-generating pairs of $\mathrm{PSL}_n(q)$, for all $n \geq 5$ and $q > 2$.

Keywords: $(2,\ell)$-generating pairs; Finite simple groups.

1. Introduction

A $(2,\ell)$-generating pair of a group G consists of two elements, of respective orders 2 and ℓ, which generate G. Clearly $\ell \geq 3$, unless G is abelian or dihedral. The authors of [2] study the problem of finding uniform $(2,k)$-generating pairs for the finite classical groups $\mathrm{PSL}_4(q)$, $\mathrm{PSp}_4(q)$ and $\mathrm{PSU}_4(q^2)$, with $k \geq 3$ the order of some element of $\mathrm{SL}_2(q)$, including $k = 4$ when q is even. In Theorem 3.1 of this paper we lift their $(2,k)$-generating pairs of $\mathrm{PSL}_4(q)$ to $(2,\ell)$-generating pairs of $\mathrm{PSL}_n(q)$, for all $n \geq 5$. Here $\ell = kh$, where k, h are orders of arbitrary elements of $\mathrm{SL}_2(q)$ subject to $k \geq 3$, $h \geq 3$ and $(k,h) = 1$. For q even we allow also $k = 4$ or $h = 2$. Most likely the same construction, with $\ell = k$ and σ in (2) of order h dividing k, produces $(2,k)$-generating pairs of $\mathrm{PSL}_n(q)$, $n \geq 5$. This would be the best possible generalization. But the proof becomes much more intricate.

Let $\mathbb{F}_q$ be the Galois field of order $q = p^a$, where p is a prime, and $\mathbb{F}_q^*$ be the set of its non-zero elements. For k as above, except in the case $(k, q) = (4, 2^a)$, let $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix}$ be a rational canonical form of $\mathrm{SL}_2(q)$ having order k, and consider the matrices:

$$x = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ d & 0 & 0 & 0 \\ 0 & d & 0 & 0 \end{pmatrix}, \ d = \pm 1, \quad y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & r \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & s \end{pmatrix}, \ r \in \mathbb{F}_q^*. \tag{1}$$

Clearly $x^2 = dI$. Moreover y has the same order k of γ, except when $s = 0$ and $q = 2^a$, in which case y has order 4. When necessary, we identify x, y with their projective images, of respective orders 2 and k.

Lemma 1.1. *If $q > 3$, for fixed $s \in F_q$ and $d = \pm 1$, there exists $r \in \mathbb{F}_q^*$ such that $\mathbb{F}_q = \mathbb{F}_p\left[s, r^2\right]$ and $r \neq \pm\sqrt{d}\,(s-2)$.*

The easy proof can also be deduced from Lemma 5.3 of [2], where the following result is proved (Theorem 11.1):

Theorem 1.1. *Assume that x, y are defined as in (1) with $s \in \mathbb{F}_q$, $r \in \mathbb{F}_q^*$ such that $\mathbb{F}_q = \mathbb{F}_p\left[s, r^2\right]$ and $r \neq \pm\sqrt{d}\,(s-2)$. Then*

$$\langle x, y \rangle = \mathrm{SL}_4(q).$$

In particular the groups $\mathrm{SL}_4(q)$, $q > 3$, and $\mathrm{PSL}_4(q)$, $q > 2$, are $(2, k)$-generated for all $k \geq 3$ which correspond to the order of some element of $\mathrm{SL}_2(q)$, including $k = 4$ when q is even.

For the reader's convenience, we note that the assumptions on k are equivalent to the following: $k \geq 3$, k divides $q-1$ or k divides $q+1$ or $k \in \{p, 2p\}$.

2. Definition of the $(2, \ell)$-generating pairs

Let $\ell = kh$, where k, h are orders of arbitrary elements of $\mathrm{SL}_2(q)$ subject to the conditions $k \geq 3$, $h \geq 3$ and $(k, h) = 1$. For q even allow also $k = 4$ or $h = 2$. For all $n \geq 5$, we lift any $(2, k)$-generating pair (x, y) of $\mathrm{PSL}_4(q)$ to a $(2, \ell)$-generating pair (X, Y) of $\mathrm{PSL}_n(q)$ via the following blocks:

$$\sigma := \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}, \quad \pi_\lambda := \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}, \ \lambda = \pm 1. \tag{2}$$

Here $t \in \mathbb{F}_q$ is such that σ has order h.

Denoting by $e_1, \dots, e_4$ the canonical basis of $\mathbb{F}_q^4$, let y_3 be the restriction of y in (1) to $\langle e_2, e_3, e_4 \rangle$, namely:

$$y_3 := \begin{pmatrix} 1 & 0 & r \\ 0 & 0 & -1 \\ 0 & 1 & s \end{pmatrix}, \quad r \in \mathbb{F}_q^*. \tag{3}$$

For $n = 2m + 3 \geq 5$, in (2) take $\lambda = 1$ and define

$$X := \begin{pmatrix} \pm 1 & & & & \\ & \pi_1 & & & \\ & & \dots & & \\ & & & \pi_1 & \\ & & & & x \end{pmatrix}, \qquad Y := \begin{pmatrix} \sigma & & & \\ & \dots & & \\ & & \sigma & \\ & & & y_3 \end{pmatrix} \tag{4}$$

where x is as in (1) with $d = 1$, π_1 and σ are as in (2), and the sign $\pm$ is chosen so that $\det X = 1$. In (4) the number of blocks π_1 is $m - 1$ and the number of blocks σ is m.

For $n = 2m + 4 \geq 6$, in (2) take $\lambda = 1$ if $n \equiv 0 \pmod 4$, $\lambda = -1$ if $n \equiv 2 \pmod 4$, and define:

$$X := \begin{pmatrix} \pi_\lambda & & & \\ & \dots & & \\ & & \pi_\lambda & \\ & & & x \end{pmatrix}, \qquad Y := \begin{pmatrix} 1 & & & & \\ & \sigma & & & \\ & & \dots & & \\ & & & \sigma & \\ & & & & y_3 \end{pmatrix} \tag{5}$$

where x is as in (1) with $d = \lambda$, σ and π_λ are as in (2). In (5) the number of blocks π_λ and σ is m.

Note that X^2 is scalar and Y has order $\ell = kh$.

3. The result

For each m such that $1 \leq m \leq n$, we consider the subgroup $S_m(q)$ of $\mathrm{SL}_n(q)$ defined as follows:

$$S_m(q) := \begin{pmatrix} I_{n-m} & \\ & \mathrm{SL}_m(q) \end{pmatrix}.$$

For the reader's convenience, we give a direct proof of a fact which is well known, namely:

Lemma 3.1. *Let σ and π_{-1} be defined as in (2). For all $n \geq 4$, set*

$$\Sigma := \begin{pmatrix} \sigma & \\ & I_{n-2} \end{pmatrix}, \quad \Pi := \begin{pmatrix} \pi_{-1} & \\ & I_{n-2} \end{pmatrix}.$$

Then $\mathrm{SL}_n(q) = \langle S_{n-1}(q), \Sigma\rangle = \langle S_{n-1}(q), \Pi\rangle$.

Proof. Consider the elementary transvection $\tau_1 := I + E_{2,3}$ and let $g \in \{\Sigma, \Pi\}$. Then $\tau_1^g = I + E_{1,3}$. Using the transitivity of $\mathrm{SL}_{n-1}(q)$ on the non-zero vectors of $\mathbb{F}_q^{n-1}$, it is easy to see that the conjugates of $I + E_{1,3}$ under $S_{n-1}(q)$ include all root subgroups $I + \mathbb{F}_q E_{1,j}$, $2 \le j \le n$.

In a similar way, consider the elementary transvection $\tau_2 := I + E_{3,2}$. Then $\tau_2^g = I + E_{3,1} \pmod{S_{n-1}(q)}$. As above, the conjugates of $I + E_{3,1}$ under $S_{n-1}(q)$ include all root subgroups $I + \mathbb{F}_q E_{j,1}$, $2 \le j \le n$. Since $\mathrm{SL}_n(q)$ is generated by the elementary root sugroups $I + \mathbb{F}_q E_{i,j}$, $i \ne j$, (see, e.g. [1]) our claim follows. □

Theorem 3.1. *Assume* $n \ge 5$. *Define* X, Y *respectively as in* (4) *or* (5) *according to* n *odd or even. If* $r \in \mathbb{F}_q^*$ *is such that* $\mathbb{F}_q = \mathbb{F}_p\left[s, r^2\right]$ *and* $r \ne \pm\sqrt{d}\,(s-2)$, *then:*

$$\langle X, Y\rangle = \mathrm{SL}_n(q).$$

In particular the group $\mathrm{SL}_n(q)$, $q > 3$ *and* $n \not\equiv 2 \pmod 4$ *if* q *is odd, is* $(2, \ell)$*-generated. The group* $\mathrm{PSL}_n(q)$, $q > 2$, *is* $(2, \ell)$*-generated.*

Proof. The subspace $U = \langle e_1, \dots, e_{n-3}\rangle$, generated by the first $n - 3$ vectors of the canonical basis, is Y-invariant. So we define:

$$Y_{n-3} := \begin{pmatrix} Y_{|U} & \\ & I_3 \end{pmatrix}, \qquad Y_3 := \begin{pmatrix} I_{n-3} & \\ & y_3 \end{pmatrix}.$$

By the assumption that k and h are coprime, we have:

$$\langle Y\rangle = \langle Y_{n-3}\rangle \times \langle Y_3\rangle\,.$$

It follows that $\langle X, Y\rangle$ contains the subgroup $H := \langle X, Y_3\rangle \le C_2 \times \mathrm{SL}_4(q)$. Using Theorem 1.1 and the fact that the group $\mathrm{SL}_4(q)$ is perfect, we get that $H' = S_4(q) \le \langle X, Y\rangle$. By induction we may assume that

$$S_{n-1}(q) \le \langle X, Y\rangle\,.$$

Noting that $\Sigma^{-1}Y \in S_{n-2}(q)$ if n is odd, and that either $\Pi X \in S_{n-1}(q)$ or $\Pi^{-1}X \in S_{n-1}(q)$ if n is even, we deduce $\Sigma \in \langle X, Y\rangle$ if n is odd, $\Pi \in \langle X, Y\rangle$ if n is even. Our claim follows from Lemma 3.1. □

References

1. R. Carter, Simple groups of Lie type, Wiley and Sons, London, 1972.
2. M. Pellegrini, C. Tamburini Bellani and M.A. Vsemirnov, Uniform $(2, k)$-generation of 4-dimensional classical groups (submitted).