Bull. Aust. Math. Soc. **93** (2016), 61–72
doi:10.1017/S0004972715000763

THE (2,3)-GENERATION OF THE CLASSICAL SIMPLE GROUPS OF DIMENSIONS 6 AND 7

MARCO ANTONIO PELLEGRINI

(Received 10 April 2015; accepted 22 April 2015; first published online 5 August 2015)

Dedicated to M. C. Tamburini on the occasion of her 70th birthday

Abstract

In this paper, we prove that the finite simple groups $\mathrm{PSp}_6(q)$, $\Omega_7(q)$ and $\mathrm{PSU}_7(q^2)$ are $(2,3)$-generated for all q. In particular, this result completes the classification of the $(2,3)$-generated finite classical simple groups up to dimension 7.

2010 *Mathematics subject classification*: primary 20G40; secondary 20F05.

Keywords and phrases: generation, classical groups.

1. Introduction

Given a finite group, it is very natural to ask for a minimal set of generators. For finite nonabelian simple groups it is well known that they can be generated by a pair X, Y of suitable elements: for alternating groups this is an old result of Miller [12], for groups of Lie type it is due to Steinberg [18] and for sporadic groups to Aschbacher and Guralnick [2].

Since nonabelian simple groups have even order, on many occasions group theorists require that one of these two elements, say X, is an involution. It was conjectured (for example, see [5]) that every finite nonabelian simple group can be generated by an involution X and an element Y of order ≥ 3. For alternating and sporadic groups the answer was already provided in [12] and [2], respectively. Groups of Lie type attracted the interest of many authors: among them, Malle *et al.* proved in [10] the validity of the conjecture (at least for $G \neq \mathrm{PSU}_3(9)$), taking Y to be strongly real. Their result clearly implies that every finite nonabelian simple group different from $\mathrm{PSU}_3(9)$ is generated by a set of three involutions. For $G = \mathrm{PSU}_3(9)$, a direct computation shows that this group can be generated by an involution and an element of order 7.

Considering simple groups of Lie type, one can require, for instance, that Y is contained in few maximal subgroups, as done for instance in [6], or that the order of Y is a prime. In particular, we say that a group is $(2,p)$-generated if it can be generated by two elements X, Y of respective orders 2 and p, where p is a prime. Since groups generated by two involutions are dihedral, we must have $p \geq 3$. It seems that the difficulties increase when one investigates the $(2, p)$-generation for some fixed small prime p. The choice $p = 3$ is the most natural, since $(2, 3)$-generated groups are, along with the groups of order at most 3, the homomorphic images of $\mathrm{PSL}_2(\mathbb{Z})$.

A key result for this kind of problem is due to Liebeck and Shalev, who proved in [7] that, apart from the infinite families $\mathrm{PSp}_4(2^m)$, $\mathrm{PSp}_4(3^m)$ and ${}^2B_2(2^{2m+1})$, all finite nonabelian simple groups are $(2, 3)$-generated with a finite number of exceptions. However, their result relies on probabilistic methods and does not provide any estimates on the number or the distribution of such exceptions. The exceptional groups of Lie type were studied by Lübeck and Malle [8] and so the problem of finding the exact list of simple groups which are not $(2, 3)$-generated reduces to the classical groups, where it is still wide open (see [11, Problem 18.98]). In view of papers such as [17, 22, 23], we have to consider only groups of small dimension, say less than 13 for $\mathrm{PSL}_n(q)$ and less than 88 for the other classical groups.

In [9], Macbeath dealt with the groups $\mathrm{PSL}_2(q)$. For classical groups of dimensions 3 and 5, the groups which are not $(2, 3)$-generated are described in [14] and for dimension 4 in [16].

With this paper we conclude the classification of the $(2, 3)$-generated finite classical simple groups up to dimension 7. The $(2, 3)$-generation of $\mathrm{SL}_6(q)$, $\mathrm{SL}_7(q)$ and $\mathrm{SU}_6(q^2)$ (and their projective images) for all q was proved in [19], [20] and [13], respectively. When q is odd, the symplectic groups $\mathrm{Sp}_6(q)$ are not $(2, 3)$-generated (see [26]), but the simple groups $\mathrm{PSp}_6(q)$ are $(2, 3, 7)$-generated for $q > 3$ (see [24]) and $\mathrm{PSp}_6(3)$ is $(2, 3)$-generated, for instance, by the projective images of the following matrices:

$$x = \begin{pmatrix} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

The remaining cases, studied in this paper, are the groups $\mathrm{Sp}_6(q)$ for q even, $\Omega_7(q)$ for q odd and $\mathrm{SU}_7(q^2)$ for all q (our notation for the classical groups accords with [4]). Observe that among these classes of groups only $\mathrm{PSU}_7(p^{n_7})$, for any prime $p \neq 7$ such that its order n_7 modulo 7 is even, are $(2, 3, 7)$-generated; see [15, 21].

From Theorems 2.5, 3.8 and 3.12 and Propositions 3.7 and 3.11 below, we deduce the following theorem.

Theorem. *The finite simple groups* $\mathrm{PSp}_6(q)$, $\Omega_7(q)$ *and* $\mathrm{PSU}_7(q^2)$ *are* $(2, 3)$-*generated for all* q.

We point out that there are only eight exceptions for simple classical groups of dimension ≤ 7. To our knowledge the only exceptions in higher dimension are $\Omega_8^+(2)$

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

and $P\Omega_8^+(3)$ (see Vsemirnov, 2012). Furthermore, our generators were constructed in a uniform way starting from the generators provided in [14] and following the inductive method described in [13]. The idea is to construct the $(2,3)$-generators of dimension n from those of dimension $n-1$. In fact, dimensions 6 and 7 can be considered the basis of this induction process for what concerns unitary, symplectic and odd-dimensional orthogonal groups in any characteristic.

Throughout this paper, for any fixed power q of the prime p, $\mathbb{F}_q$ denotes the finite field of q elements and $\mathbb{F}$ is its algebraic closure. Furthermore, the set $\{e_1, e_2, \ldots, e_n\}$ is the canonical basis of $\mathbb{F}^n$. For a description of the maximal subgroups of the low-dimensional classical groups, we refer to [3]. Finally, ω is an element of $\mathbb{F}$ of order 3 if $p \neq 3$, $\omega = 1$ otherwise.

2. The groups Sp(6, q), q even

In order to prove the $(2,3)$-generation of the groups $\mathrm{Sp}_6(q)$ for q even, we first construct our pair x, y of $(2,3)$-generators. Take $a \in \mathbb{F}_q^*$, with q even, and define $H = \langle x, y\rangle$, where

$$x = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & a & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & a & 1 & 1 & 1 & 1 \\ 0 & a & 1 & 0 & 1 & 0 \end{pmatrix}. \tag{2.1}$$

Observe that $x^2 = y^3 = I$ and that $H \leq \mathrm{Sp}_6(q)$ since they fix the following Gram matrix (that is, $x^{\mathrm{T}}Jx = y^{\mathrm{T}}Jy = J = J^{\mathrm{T}}$):

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & a & a+1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & a & 1 & 0 & 1 & 1 \\ 0 & a+1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

The invariant factors of x and y are, respectively,

$$(t^2+1), (t^2+1), (t^2+1) \quad \text{and} \quad (t^3+1), (t^3+1). \tag{2.2}$$

The minimum polynomial of $z = xy$ coincides with its characteristic polynomial

$$\chi_z(t) = t^6 + (a+1)t^5 + t^4 + t^3 + t^2 + (a+1)t + 1. \tag{2.3}$$

Proposition 2.1. *The subgroup H is absolutely irreducible.*

Proof. It suffices to prove the irreducibility of H viewed as a subgroup of $\mathrm{Sp}_6(\mathbb{F})$, where $\mathbb{F}$ denotes the algebraic closure of $\mathbb{F}_q$ (so the parameter a in (2.1) is an element

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

of $\mathbb{F}^*$). Suppose that $W \neq V$ is an H-invariant subspace of $V = \mathbb{F}^6$. Observe firstly that for all $v \in V$ the vector $v + yv + y^2v$ always belongs to the subspace $U = \langle e_1, e_2 + ae_6\rangle$. So, assume that, for some $w \in W$, we have $u = w + yw + y^2w \neq 0$ (hence $0 \neq u \in W \cap U$). We will show that this implies the contradiction $W = V$.

Let $u = (x_1, x_2, 0, 0, 0, ax_2)^{\mathrm{T}} \neq 0$. Replacing, if necessary, w by a suitable scalar multiple, without loss of generality, we may assume that either $(x_1, x_2) = (1, 0)$ or $x_2 = 1$. If $(x_1, x_2) = (1, 0)$, then the matrix M_1, whose columns are

$$M_1 = (u \mid xu \mid yxu \mid xyxu \mid (yx)^2u \mid x(yx)^2u),$$

has determinant $a \neq 0$ and hence the H-submodule generated by u is the whole space V, contradicting the fact that it is contained in the proper subspace W. If $x_2 = 1$, then the matrix M_2, whose columns are

$$M_2 = (u \mid xu \mid yxu \mid xyxu \mid xy^2xu \mid y^2xu),$$

has determinant $a^3(x_1 + a + 1)^2$, which is nonzero if $x_1 \neq a + 1$. In this case, as before, the H-submodule generated by u is the whole space V, producing the contradiction $V \leq W$. So, assume further that $x_1 = a + 1$. In this case, if a has order 3 we obtain the contradiction $V = \langle u, xu, yxu, xy^2xu, (yx)^2u, (xy)^2yxu\rangle \leq W$ and for the other choices of $a \neq 0$ we get the contradiction $V = \langle u, xu, yxu, y^2xu, xy^2xu, yxy^2xu\rangle \leq W$.

Hence, we have proved that $W \cap U = \{0\}$ or, in other words, that all the elements w of W satisfy the condition

$$w + yw + y^2w = 0. \tag{2.4}$$

It follows that every element w of W has shape $w = (x_1, 0, x_3, x_4, x_5, x_1 + x_5)^{\mathrm{T}}$. Fix such a $w \in W$. Since $xw \in W$ also satisfies (2.4), we obtain $x_4 = 0$ and $x_3 = x_1 + ax_5$. Next, considering $xyxw \in W$, we get $x_1 = 0$ and $(a^2 + a + 1)x_5 = 0$. Finally applying (2.4) to $(xy)^2xw \in W$, we obtain $(a + 1)x_5 = 0$, whence $x_5 = 0$ and so $w = 0$ (that is, $W = \{0\}$). □

Now, we want to analyse when H is contained in a maximal subgroup of $\mathrm{Sp}_6(q)$. For a description of these subgroups, see [3, Tables 8.28 and 8.29].

Lemma 2.2. *The subgroup H is not monomial.*

Proof. Let $\mathcal{B} = \{v_1, \dots\}$ be a basis on which H acts monomially. Considering transitivity and canonical forms (2.2), the permutation induced by x is the product of three 2-cycles. Furthermore, we may assume that

$$v_2 = yv_1, \quad v_3 = yv_2, \quad v_4 = xv_1, \quad v_5 = yv_4, \quad v_6 = yv_5.$$

We have the following cases.

(i) $xv_2 = \lambda v_5$ and $xv_3 = \mu v_6$; in this case $\chi_{xy}(t) = t^6 + 1$, in contradiction with (2.3).
(ii) $xv_2 = \lambda v_6$ and $xv_3 = \mu v_5$; in this case $\chi_{xy}(t) = t^6 + ((\lambda^2\mu + \mu^2 + \lambda)/\lambda\mu)t^4 + ((\lambda\mu^2 + \lambda^2 + \mu)/\lambda\mu)t^2 + 1$ and comparison with (2.3) gives a contradiction.
(iii) $xv_2 = \lambda v_3$ and $xv_5 = \mu v_6$; in this case $\chi_{xy}(t) = t^6 + ((\lambda + \mu)/\lambda\mu)t^5 + (1/\lambda\mu)t^4 + (\lambda\mu)t^2 + (\lambda + \mu)t + 1$ and, once again, we obtain a contradiction with (2.3). □

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

LEMMA 2.3. *The subgroup H is not contained in an orthogonal group $\mathrm{SO}_6^{\pm}(q)$.*

PROOF. Suppose that $H \leq \mathrm{SO}_6^{\pm}(q)$ and let Q be a quadratic form fixed by H. This means that for all $v \in \mathbb{F}_q^6$, $Q(xv) = Q(v)$ and $Q(yv) = Q(v)$. Recall further that $Q(v_1 + v_2) + Q(v_1) + Q(v_2) = v_1^{\mathrm{T}} J v_2$.

From $Q(e_5) = Q(xe_5) = Q(e_5 + ae_6)$, $Q(e_6) = Q(ye_6) = Q(e_5)$ and $Q(e_1) = Q(xe_1) = Q(e_3)$, we get respectively $Q(e_6) = 1/a$, $Q(e_5 + e_6) = 1$ and $Q(e_1 + e_3) = 0$. Now, $Q(e_4) = Q(ye_4) = Q((e_1 + e_3) + (e_4 + e_5))$, which implies that $Q(e_4) = Q(e_1 + e_3) + Q(e_4 + e_5) + 1 = Q(e_4) + Q(e_5) + 1 + 1$, whence $0 = Q(e_5) = Q(e_6) = 1/a$, which is a contradiction. □

LEMMA 2.4. *The subgroup H is not contained in a subgroup M isomorphic to $G_2(q)$.*

PROOF. We first observe that the discriminant of the characteristic polynomial of $z = xy$ is 1 and so the eigenvalues of z are pairwise distinct. Suppose that H is contained in a subgroup $M \cong G_2(q)$. We may embed H in $\mathfrak{G} = G_2(\mathbb{F})$ and by the previous observation z is a semisimple element of $\mathfrak{G}$, that is, it belongs to a maximal torus of $\mathfrak{G}$. By [1], z is conjugate to $s = \mathrm{diag}(\alpha, \beta, \alpha\beta, \alpha^{-1}, \beta^{-1}, (\alpha\beta)^{-1})$, where $\alpha, \beta \in \mathbb{F}^*$. Let $\chi_s(t) = t^6 + \sum_{j=1}^{5} f_j t^j + 1$ be the characteristic polynomial of s. It is easy to see that $f_3 = f_1^2$. Comparison with (2.3) gives $1 = (a+1)^2$, that is, $a = 0$. □

THEOREM 2.5. *Take x, y as in (2.1), with $a \in \mathbb{F}_q^*$, q even, such that $\mathbb{F}_p[a] = \mathbb{F}_q$. Then $H = \langle x, y\rangle = \mathrm{Sp}_6(q)$. In particular, the groups $\mathrm{Sp}_6(q)$ are $(2,3)$-generated for all q.*

PROOF. We already observed that $H \leq \mathrm{Sp}_6(q)$. Let M be a maximal subgroup of $\mathrm{Sp}_6(q)$ which contains H. By Proposition 2.1, H is absolutely irreducible and so $M \notin C_1 \cup C_3$. Moreover, M cannot belong to C_2 by Lemma 2.2. Since $a + 1$ is a coefficient of the characteristic polynomial of z, the assumption $\mathbb{F}_p[a] = \mathbb{F}_q$ implies that the matrix z cannot be conjugate to elements of $\mathrm{Sp}_6(q_0)$ for any $q_0 < q$. Thus, $M \notin C_5$. By Lemmas 2.3 and 2.4, M cannot be in $C_8 \cup \mathcal{S}$. We conclude that $H = \mathrm{Sp}_6(q)$. □

3. The 7-dimensional classical groups

In order to prove that the groups $\mathrm{SU}_7(q^2)$ and $\Omega_7(q)$ are $(2,3)$-generated, we provide a pair of uniform generators. Consider the following matrices:

$$x = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & a \\ 1 & 0 & 0 & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & -1 & 0 & -1 & 0 & a+b-1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}, \tag{3.1}$$

where either

$$b = a \in \mathbb{F}_q \quad \text{and} \quad H \leq \mathrm{SL}_7(q) \tag{3.2}$$

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

or

$$b = a^q \in \mathbb{F}_{q^2} \quad \text{and} \quad H \leq \mathrm{SL}_7(q^2). \tag{3.3}$$

The invariant factors of x and y are respectively

$$(t+1), (t^2-1), (t^2-1), (t^2-1); \quad (t^2+t+1), (t^2+t+1), (t^3-1), \tag{3.4}$$

and the characteristic polynomial of $z = xy$ is

$$\chi_{xy}(t) = t^7 - t^5 + (1-a)t^4 + (b-1)t^3 + t^2 - 1.$$

Lemma 3.1. *If H is absolutely irreducible, then the characteristic polynomial $\chi_z(t)$ of z coincides with its minimum polynomial. Furthermore, under hypothesis (3.2) we have $H \leq \mathrm{SO}_7(q)$ and under hypothesis (3.3) we have $H \leq \mathrm{SU}_7(q^2)$.*

Proof. Observe that $\dim C(x) = 25$, $\dim C(y) = 19$ and $\dim C(z) = 7$. From the Frobenius formula, it follows that z has a unique invariant factor, whence our first claim. In particular, the triple (x, y, z) is rigid (see [16]) and by [16, Theorem 3.1] we obtain $H \leq \mathrm{SO}_7(q)$ when (3.2) holds and $H \leq \mathrm{SU}_7(q^2)$ when (3.3) holds. □

Proposition 3.2. *Take x, y as in (3.1). Then the subgroup $H = \langle x, y\rangle$ is absolutely irreducible if and only if the following conditions hold:*

(i) $a^2 - ab + b^2 + 2a + 2b + 4 = \prod_{j=1}^{2}(b + \omega^j a - 2\omega^{2j}) \neq 0$;
(ii) $(a+b)^3 - 8(a+b-2)^2 - 8ab \neq 0$.

Proof. We consider the irreducibility of H viewed as a subgroup of $\mathrm{SL}_7(\mathbb{F})$ (so the parameters a, b in (3.1) are elements of $\mathbb{F}$).

First, assume that $b = -\omega^j a + 2\omega^{2j}$ for some $j = 1, 2$ and consider the element $w = (a + \omega^{2j}, -\omega^{2j}, 1, -1, \omega^j, \omega^{2j}, -1)^{\mathrm{T}} \neq 0$. We have $yw = \omega^j w$ and $xw = -w$. Thus, $W = \langle w\rangle$ is a 1-dimensional H-invariant subspace of $V = \mathbb{F}^7$.

Next, assume that $(a+b)^3 - 8(a+b-2)^2 - 8ab = 0$. If $p = 2$, then $a = b$. Taking $w = (1, 1, 1, 1, 1, 1, 0)^{\mathrm{T}}$, the subspace $\langle w, yw, xyw, yxyw, (xy)^2 w, y(xy)^2 w\rangle$ is H-invariant. Assume that $p \neq 2$. If $a = b = 2$, then consider $w = (1, 1, 2, 2, 1, 1, 0)^{\mathrm{T}}$; the subspace $\langle w, yw, xyw, yxyw\rangle$ is H-invariant. If $(a, b) \neq (2, 2)$, taking $w = (x_1, x_1, x_2, x_2, x_3, x_3, 0)^{\mathrm{T}}$, where $x_1 = -\frac{1}{2}((a+b)^2 - 6a - 10b + 16)$, $x_2 = 2b - 4$ and $x_3 = a + b - 4$, we obtain that $w \neq 0$ and the subspace $\langle w, yw\rangle$ is H-invariant.

Now, assume that Conditions (i) and (ii) both hold and let $W \neq V$ be an H-invariant subspace of V. Straightforward calculation shows that, for all $v \in V$, the element $v + yv + y^2 v = (I + y + y^2)v$ always belongs to the subspace $\langle e_1\rangle$. On the other hand, note that

$$xe_1 = e_2, \quad ye_2 = e_3, \quad xe_3 = e_4, \quad ye_4 = e_5, \quad xe_5 = e_6, \quad ye_6 = e_7. \tag{3.5}$$

It follows that if for some $w \in W$ we have $u = w + yw + y^2 w \neq 0$, then the H-submodule generated by u is the whole space V, in contradiction with the assumption $W \neq V$. Hence, every element w of W satisfies the following condition:

$$w + yw + y^2 w = 0. \tag{3.6}$$

We will show that this condition implies $W = \{0\}$.

Case (a). Suppose that $w + xw = 0$ for all $w \in W$. Then all vectors in W have shape $(x_1, -a(x_5 + x_6) - x_1, x_3, -x_3, x_5, x_6, x_5 + x_6)^{\mathrm{T}}$. We fix a nonzero $w \in W$. From $yw + xyw = 0$ and $y^2w + xy^2w = 0$, we see that expression (i) must be 0, which is a contradiction.

Case (b). There exists $\overline{w} \in W$ such that $\overline{w} + x\overline{w} \neq 0$. Then $\overline{w} + x\overline{w} = w$ has shape $(x_1, x_1, x_3, x_3, x_5, x_5, 0)^{\mathrm{T}}$. Equation (3.6) gives $2x_3 = 2x_1 + cx_5$, with $c = a + b - 2$. Suppose that $p = 2$. If $c = 0$ (that is, $a = b$), expression (ii) is 0, which is a contradiction. If $c \neq 0$, then $x_5 = 0$ and application of (3.6) to xyw and to $(xy)^2w$, which are in W, leads to $W = \{0\}$. Thus, $p \neq 2$ and $x_3 = x_1 + (c/2)x_5$. After this substitution, (3.6) applied to xyw gives

$$(c-2)x_1 = (-\tfrac{1}{2}(a+b)^2 + 3a + 5b - 8)x_5. \tag{3.7}$$

Assume that $c = 2$ (that is, $b = 4 - a$). Then $(a - 2)x_5 = 0$. If $a = 2$ (and so $b = 2$), then expression (ii) is 0, which is a contradiction. If $a \neq 2$, we get $x_5 = 0$. In this case, applying (3.6) to $(xy)^2w \in W$, we obtain $W = \{0\}$. Assume that $c \neq 2$. Using (3.7) to eliminate x_1 and applying (3.6) to $(xy)^2w$, we see that expression (ii) must be 0, which is a contradiction. □

Lemma 3.3. *Assume that H is absolutely irreducible. If $(xy)^k$ is a diagonal matrix, then $k \geq 13$.*

Proof. For $k \leq 3$, our claim follows from (3.5). Let $D(k) = (xy)^k$. For $k = 4, 5, 6$ we have $D(k)_{3,2} = \pm 1$ and for $k = 7$ we have $D(k)_{3,1} = 1$. If $k = 8$, we obtain $D(8)_{3,1} = a - 2$, but for $a = 2$ we get $D(8)_{7,2} = -1$. For $k = 9$, $D(9)_{7,1} = -2a + 3$ and hence $p \neq 2$. In this case, $a = \frac{3}{2}$ yields $D(9)_{7,5} = -1$. For $k = 10, 11, 12$ we have $D(10)_{3,4} = D(11)_{3,2} = D(12)_{3,1} = (2 - a)(a + 2b - 5)$. Assume first that $a = 2$. For $k = 10, 12$, we obtain $D(10)_{5,3} = D(12)_{6,4} = 2 - b$, whence $b = 2$. However, by Proposition 3.2(ii), H is reducible. For $k = 11$ we have $D(11)_{7,1} = 2(b - 2)$. If $b = 2$, as before, H is reducible and if $p = 2$ we get $D(11)_{2,1} = 1$. Assume now that $a = 5 - 2b$. In this case, $D(10)_{3,5} = 1 - b$; however, $b = 1$ leads to $D(10)_{4,1} = 7$ and $D(10)_{4,7} = 5$. Moreover, $D(11)_{3,4} = D(12)_{3,2} = (b - 2)(9b - 13)$. We can exclude $b = 2$ (which implies $a = 1$), since this produces the contradiction $D(11)_{1,4} = D(12)_{1,4} = 1$. So, take $9b = 13$ ($p \neq 3$). We then obtain the contradiction $D(11)_{3,5} = D(12)_{5,7} = \frac{1}{9}$. □

Now, we want to prove that H, when absolutely irreducible, is not contained in a maximal subgroup of $\Omega_7(q)$ or of $\mathrm{SU}_7(q^2)$. We refer to [3, Tables 8.37–8.40].

Lemma 3.4. *Assume that H is absolutely irreducible. Then H is not monomial.*

Proof. Let $\{v_1, \ldots, v_7\}$ be a basis on which H acts monomially and transitively. We may then assume that $yv_1 = v_2$, $yv_2 = v_3$, $yv_3 = v_1$, $yv_4 = v_5$, $yv_5 = v_6$ and $yv_6 = v_4$. However, this is in contradiction with the invariant factors (3.4) of y. □

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

Lemma 3.5. *Assume that H is absolutely irreducible. Then H is not conjugate to any subgroup of type $Z \times \mathrm{PSU}_3(3)$, where Z consists of scalar matrices.*

Proof. It suffices to notice that elements of $\mathrm{PSU}_3(3)$ have order $1, 2, 3, 4, 6, 7, 8$ or 12 and apply Lemma 3.3. □

Lemma 3.6. *Assume hypothesis (3.2) and that H is absolutely irreducible. Then H is not contained in a subgroup M isomorphic to $\mathrm{Sp}_6(2)$.*

Proof. Firstly, notice that the commutator between two elements of $\mathrm{Sp}_6(2)$ of orders respectively 2 and 3 has order 7. So, if $H \leq M$, then $[x, y]$ must have order 7. Set $D = [x, y]^7$. Since we are assuming that $b = a$, we obtain $D_{7,1} = (a-2)^2(1-a)$. However, for $a = 1, 2$ the subgroup is reducible by Proposition 3.2(ii). □

We can now prove the $(2, 3)$-generation of $\mathrm{SU}_7(q^2)$.

Proposition 3.7. *The group $\mathrm{SU}_7(4)$ is $(2, 3)$-generated.*

Proof. Take the following two matrices of $\mathrm{SL}_7(4)$:

$$x = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & \omega \\ 0 & 0 & 0 & 1 & 0 & \omega^2 & \omega \\ 0 & 0 & 0 & 0 & \omega & 1 & \omega^2 \\ 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Then $x^2 = y^3 = 1$. Moreover, $x^{\mathrm{T}} x^{\sigma} = y^{\mathrm{T}} y^{\sigma} = I$ (σ is the automorphism of $\mathrm{SL}_7(q^2)$ defined by $(\alpha_{i,j}) \mapsto (\alpha_{i,j}^q)$) and so $H = \langle x, y \rangle \leq \mathrm{SU}_7(4)$. Assume that H is contained in some maximal subgroup M of G. Since $g = (xy^2xy)^2(xy^2)^3$ has order 43, then g can be contained only in a maximal subgroup of class C_3: $M = ((2^7+1)/3) : 7$. However, $|M| = 7 \cdot 43$ and so $x \notin M$. Hence, $H = \mathrm{SU}_7(4)$. □

Theorem 3.8. *Take x, y as in (3.1) with $a \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and suppose that:*

(i) $a^{2q} - a^{q+1} + a^2 + 2a^q + 2a + 4 \neq 0$;
(ii) $(a + a^q)^3 - 8(a + a^q - 2)^2 - 8a^{q+1} \neq 0$ *when p is odd;*
(iii) $\mathbb{F}_{q^2} = \mathbb{F}_p[a^7]$.

Then $H = \langle x, y \rangle = \mathrm{SU}_7(q^2)$. Moreover, if $q^2 \neq 2^2$, then there exists $a \in \mathbb{F}_{q^2}^*$ satisfying Conditions (i)–(iii). In particular, the groups $\mathrm{SU}_7(q^2)$ and $\mathrm{PSU}_7(q^2)$ are $(2, 3)$-generated for all q.

Proof. By Conditions (i) and (ii), H is absolutely irreducible. From Lemma 3.1, it follows that $H \leq \mathrm{SU}_7(q^2)$. Let M be a maximal subgroup of $\mathrm{SU}_7(q^2)$ which contains H. Since H is absolutely irreducible, $M \notin C_1 \cup C_3$. Moreover, M cannot belong to C_2 by Lemma 3.4. Since z^6 is not scalar by Lemma 3.3, we may apply [14, Lemma 2.3]

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

to deduce that $M \notin C_6$. We have $\mathbb{F}_p[a^{7q}] = \mathbb{F}_p[a^7] = \mathbb{F}_{q^2}$, by (iii). Since $a^q - 1$ is a coefficient of the characteristic polynomial of z, the matrix z cannot be conjugate to any element of $\mathrm{SL}_7(q_0)Z$, with $q_0 < q^2$ and Z the centre of $\mathrm{SU}_7(q^2)$. Thus, $M \notin C_5$. Finally, M cannot be in class $\mathcal{S}$ by Lemma 3.5 (recall that we are taking $a \neq a^q$). We conclude that $H = \mathrm{SU}_7(q^2)$.

As to the existence of some a satisfying all the assumptions when $q > 2$, any element of $\mathbb{F}_{q^2}^*$ of order $q^2 - 1$ satisfies (iii) by [14, Lemma 2.3]. The elements in $\mathbb{F}_{q^2}^*$ which do not satisfy either (i) or (ii) are at most $3q + 2q = 5q$. If $q \geq 16$, there are at least $5q + 1$ elements in $\mathbb{F}_{q^2}^*$ having order $q^2 - 1$ (use [14, Lemma 2.1] for $q \geq 127$ and direct computations otherwise), whence the existence of a. For $3 \leq q \leq 13$, we may take a with minimum polynomial $m_a(t)$ over $\mathbb{F}_p$ as in the following table.

q	$m_a(t)$	q	$m_a(t)$	q	$m_a(t)$
$3, 13$	$t^2 + t - 2$	$4, 9$	$t^4 + t^3 - 1$	$5, 11$	$t^2 + t - 3$
7	$t^2 + t + 3$	8	$t^6 + t + 1$		

Then a satisfies (i)–(iii) and hence $H = \mathrm{SU}_7(q^2)$ for all $q > 2$. □

We now prove the $(2, 3)$-generation of $\Omega_7(q)$ for q odd.

Lemma 3.9. *Assume hypothesis (3.2) with q odd. Then H is contained in $\Omega_7(q)$ if and only if $a - 1$ is a square in $\mathbb{F}_q^*$.*

Proof. In Proposition 3.1, we already proved that $H \leq \mathrm{SO}_7(q)$. Furthermore, since $y = y^{-2}$, we have $H \leq \Omega_7(q)$ if and only if $x \in \Omega_7(q)$ if and only if the spinor norm of x is a square in $\mathbb{F}_q^*$ (for example, see [25, Theorem 11.51]). Set $V_x = \mathrm{Im}(x - Id)$. It is easy to see that $\{e_1 - e_2, e_3 - e_4, e_5 - e_6, -a(e_1 + e_2) + e_5 + e_6 + 2e_7\}$ is a basis of V_x. The Wall form of x (see [25, page 153]) with respect to this basis is given by the following matrix:

$$\begin{pmatrix} -4 & 0 & 2a & 4-4a \\ 0 & -2a & 0 & 4-2a \\ 2a & 0 & -4 & 2a^2-2a \\ 4-4a & 4-2a & 2a^2-2a & 4a-4-2a^2 \end{pmatrix},$$

whose determinant is $16(a-2)^2(a-1)(a+2)^2$. By [25, page 163], $x \in \Omega_7(q)$ if and only if $a - 1$ is a square in $\mathbb{F}_q^*$. □

Lemma 3.10. *Assume hypothesis (3.2) and q odd. If $a \neq 1, 2$, then H is not contained in a subgroup isomorphic to $G_2(q)$.*

Proof. Since we are assuming that $b = a$, the characteristic polynomial of $z = xy$ is

$$\chi_z(t) = t^7 - t^5 - (a-1)t^4 + (a-1)t^3 + t^2 - 1 \tag{3.8}$$

and the characteristic polynomial of $w = [x, y]$ is

$$\chi_w(t) = t^7 + t^6 + t^5 - (a^2 - 4a + 3)t^4 + (a^2 - 4a + 3)t^3 - t^2 - t - 1.$$

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

The discriminants of $\chi_z(t)$ and $\chi_w(t)$ are, respectively, $(a-1)(a-5)^3(27a^2-4a-148)^2$ and $(a-2)^6(a+2)^3(a-6)^3(27a^2-108a+76)^2$. Suppose that H is contained in a subgroup $M \cong G_2(q)$. Then we may embed H in $\mathfrak{G} = G_2(\mathbb{F})$.

Assume first that $a \neq 5$ and $27a^2-4a-148 \neq 0$. Then the eigenvalues of z are pairwise distinct and so z is a semisimple element of $\mathfrak{G}$, that is, it belongs to a maximal torus of $\mathfrak{G}$. By [1], z is conjugate to $s = \mathrm{diag}(1, \alpha, \beta, \alpha\beta, \alpha^{-1}, \beta^{-1}, (\alpha\beta)^{-1})$, where $\alpha, \beta \in \mathbb{F}^*$. Let $\chi_s(t) = t^7 + \sum_{j=1}^{6} f_j t^j - 1$ be the characteristic polynomial of s. It is easy to see that $f_3 = f_1 + f_1^2 + f_2$. Comparison with (3.8) gives $(a-1) = 0 + 0^2 + 1$, contrary to the hypothesis $a \neq 2$.

Consider now the case $a = 5$ (and so $p \neq 3$). For this value of a, the discriminant of $\chi_w(t)$ is $-3^6 7^3 211^2$ and so, if $p \neq 7, 211$, w is a semisimple element of $\mathfrak{G}$. Proceeding as for z, we get the contradiction $8 = -1 + (-1)^2 + (-1)$. If $p = 7, 211$, we consider the element wz. We get $\chi_{wz}(t) = t^7 + 3t^6 - 16t^5 - 82t^4 + 82t^3 + 16t^2 - 3t - 1$, whose discriminant is nonzero. Hence, wz is a semisimple element of $\mathfrak{G}$, but we obtain the contradiction $82 = -3 + (-3)^2 + 16$.

Next, suppose that a is a root of $27a^2 - 4a - 148$. We show that for these values of a, the discriminant of $\chi_w(t)$ is nonzero, except when $p = 53$ and $a = -6$. First, notice that for $a = -2$ we get the contradiction $p = 2$, while $a = 6$ implies $p = 5$. Thus, $a = 1$. So, assume that a is a root of $27a^2 - 108a + 76$. This gives the conditions $p = 5, 53$ and $a = \frac{28}{13}$. However, for $p = 5$ we get the contradiction $a = 1$.

Assume that $p = 53$ and $a = 47$. In this case, $\chi_{wz^2}(t) = t^7 + 14t^6 + 25t^5 + 6t^4 - 6t^3 - 25t^2 - 14t - 1$ has nonzero discriminant. Hence, wz^2 is a semisimple element of $\mathfrak{G}$, but this gives the contradiction $-6 = -14 + (-14)^2 - 25$. In the other cases, w is a semisimple element of $\mathfrak{G}$ and this produces the contradiction $(a^2 - 4a + 3) = -1 + (-1)^2 - 1$, that is, $a = 2$. □

Proposition 3.11. *The groups $\Omega_7(3)$ and $\Omega_7(5)$ are $(2,3)$-generated.*

Proof. It suffices to take the following matrices of $\mathrm{SL}_7(p)$ for $p = 3, 5$:

$$x = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 7/2 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1/2 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 7/2 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 7 \\ 0 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

To prove that $H = \langle x, y \rangle = \Omega_7(p)$, we proceed as in Proposition 3.7. □

Theorem 3.12. *Let x, y as in (3.1) with $b = a \in \mathbb{F}_q$ and q odd. Suppose that:*

(i) $a \notin \{0, 1, \pm 2\}$;
(ii) $a - 1$ *is a square in* $\mathbb{F}_q^*$;
(iii) $\mathbb{F}_q = \mathbb{F}_p[a]$.

https://doi.org/10.1017/S0004972715000763 Published online by Cambridge University Press

Then $H = \langle x, y\rangle = \Omega_7(q)$. *Moreover, if* $q \geq 7$, *then there exists* $a \in \mathbb{F}_q$ *satisfying Conditions (i)–(iii) and the groups* $\Omega_7(q)$ *are* $(2, 3)$*-generated.*

Proof. By Condition (i) and Proposition 3.2, the subgroup H is absolutely irreducible. From Lemma 3.1, it follows that $H \leq \mathrm{SO}_7(q)$ and, by Condition (ii) and Lemma 3.9, $H \leq \Omega_7(q)$. Let M be a maximal subgroup of $\Omega_7(q)$ which contains H. Since H is absolutely irreducible, $M \notin C_1$. Moreover, M cannot belong to C_2 by Lemma 3.4. Also, by (iii) we have $\mathbb{F}_p[a] = \mathbb{F}_q$ and since $a - 1$ is a coefficient of the characteristic polynomial of xy (see (3.8)), the matrix xy cannot be conjugate to any element of $\mathrm{SO}_7(q_0)$, with $q_0 < q$. Thus, $M \notin C_5$. Finally, M cannot be in class $\mathcal{S}$. Indeed, H cannot be contained in a subgroup isomorphic to $\mathrm{Sp}_6(2)$, by Lemma 3.6, or isomorphic to $G_2(q)$, by Condition (i) and Lemma 3.10. We conclude that $H = \Omega_7(q)$.

The existence of some a satisfying all the assumptions (when $q > 5$) is quite clear (take $a = \alpha^2 + 1$ for some suitable $\alpha \in \mathbb{F}_q^*$ of order $q - 1$). □

Remark 3.13. Taking $b = 0$ in (3.1) and proceeding as in the proof of the previous theorems, for all $q \geq 2$ it is always possible to find a value of $a \in \mathbb{F}_q$ such that the corresponding group H is $\mathrm{SL}_7(q)$. In other words, the elements x, y of (3.1) are uniform $(2, 3)$-generators for all classical groups of dimension 7.

References

[1] M. Aschbacher, 'Chevalley groups of type G_2 as the group of a trilinear form', *J. Algebra* **109**(1) (1987), 193–259.

[2] M. Aschbacher and R. Guralnick, 'Some applications of the first cohomology group', *J. Algebra* **90** (1984), 446–460.

[3] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Mathematical Society Lecture Note Series, 407 (Cambridge University Press, Cambridge, 2013).

[4] R. W. Carter, *Simple Groups of Lie Type*, Pure and Applied Mathematics, 28 (John Wiley, London–New York–Sydney, 1972).

[5] L. Di Martino and M. C. Tamburini, '2-Generation of finite simple groups and some related topics', in: *Generators and Relations in Groups and Geometries* (eds. A. Barlotti *et al.*) (Kluwer Academic, Dordrecht, 1991), 195–233.

[6] R. M. Guralnick and W. M. Kantor, 'Probabilistic generation of finite simple groups', *J. Algebra* **234**(2) (2000), 743–792.

[7] M. W. Liebeck and A. Shalev, 'Classical groups, probabilistic methods, and the (2, 3)-generation problem', *Ann. of Math.* (2) **144** (1996), 77–125.

[8] F. Lübeck and G. Malle, '(2, 3)-generation of exceptional groups', *J. Lond. Math. Soc.* (2) **59**(1) (1999), 109–122.

[9] A. M. Macbeath, 'Generators for the linear fractional groups', *Proc. Sympos. Pure Math.* **12** (1969), 14–32.

[10] G. Malle, J. Saxl and T. Weigel, 'Generation of classical groups', *Geom. Dedicata* **49**(1) (1994), 85–116.

[11] V. Mazurov and E. Khukhro, *Kourovka Notebook No. 18, Unsolved Problems in Group Theory*, arXiv:1401.0300.

[12] G. A. Miller, 'On the groups generated by two operators', *Bull. Amer. Math. Soc.* **7** (1901), 424–426.

[13] M. A. Pellegrini, M. Prandelli and M. C. Tamburini Bellani, 'The (2, 3)-generation of the special unitary groups of dimension 6', arXiv:1409.3411.

[14] M. A. Pellegrini and M. C. Tamburini Bellani, 'The simple classical groups of dimension less than 6 which are $(2,3)$-generated', *J. Algebra Appl.*, to appear, doi:10.1142/S0219498815501480.
[15] M. A. Pellegrini and M. C. Tamburini Bellani, 'Scott's formula and Hurwitz groups', arXiv:1501.07495.
[16] M. A. Pellegrini, M. C. Tamburini Bellani and M. A. Vsemirnov, 'Uniform $(2,k)$-generation of the 4-dimensional classical groups', *J. Algebra* **369** (2012), 322–350.
[17] P. Sanchini and M. C. Tamburini, '$(2,3)$-generation: a permutational approach', *Rend. Sem. Mat. Fis. Milano* **64** (1994), 141–158.
[18] R. Steinberg, 'Generators for simple groups', *Canad. J. Math.* **14** (1962), 277–283.
[19] K. Tabakov, '$(2,3)$-generation of the groups $\mathrm{PSL}_6(q)$', *Serdica Math J.* **37**(4) (2011), 365–370.
[20] K. Tabakov, $(2,3)$-generation of the groups $\mathrm{PSL}_7(q)$, *Proc. Forty Second Spring Conf. Union of Bulgarian Mathematicians*, Borovetz, 2–6 April 2013.
[21] M. C. Tamburini and M. Vsemirnov, 'Irreducible $(2,3,7)$-subgroups of $\mathrm{PGL}_n(F), n \leq 7$', *J. Algebra* **300** (2006), 339–362.
[22] M. C. Tamburini and J. S. Wilson, 'On the $(2,3)$-generation of some classical groups II', *J. Algebra* **176**(2) (1995), 667–680.
[23] M. C. Tamburini, J. S. Wilson and N. Gavioli, 'On the $(2,3)$-generation of some classical groups I', *J. Algebra* **168**(1) (1994), 353–370.
[24] M. C. Tamburini Bellani and M. Vsemirnov, 'Hurwitz generation of $\mathrm{PSp}_6(q)$', *Comm. Algebra*, to appear.
[25] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, 9 (Heldermann, Berlin, 1992).
[26] M. Vsemirnov, 'More classical groups which are not $(2,3)$-generated', *Arch. Math. (Basel)* **96**(2) (2011), 123–129.

MARCO ANTONIO PELLEGRINI, Dipartimento di Matematica e Fisica, Università Cattolica del Sacro Cuore, Via Musei 41, I-25121 Brescia, Italy
e-mail: marcoantonio.pellegrini@unicatt.it