A SOLUTION TO A PROBLEM OF WIEGOLD

ATTILA MARÓTI AND M. CHIARA TAMBURINI BELLANI

Abstract. It is well known that a non-abelian finite simple group G can be generated by two elements, i.e. it is 2-generated. We show that the direct product of n copies of G is 2-generated, where n is the smallest integer larger than $2\sqrt{|G|}$. This answers a question of Wiegold.

1. Introduction

Let G be a non-abelian finite simple group. In 1936 Hall [12] showed that the largest non-negative integer $h(G,k)$ such that the direct product of $h(G,k)$ copies of G can be generated by k elements, i.e. it is k-generated, is $h(G,k) = \varphi(G,k)/|\operatorname{Aut}(G)| < |G|^{k-1}$, where $\varphi(G,k)$ is the number of k-tuples of elements of G that generate G. (For an alternative proof of this fact see [15, Corollary 7].) Since we know that G is 2-generated (see [1]), we have $h(G) = h(G,2) \geq 1$.

For a non-identity element g_1 of G let $d(g_1)$ be the number of elements g_2 in G such that $\langle g_1, g_2\rangle = G$. Put $d(G) = \min_{1\neq g\in G} d(g)$. If $d(G) \geq 1$ then we say that G has spread 1. Erfanian and Wiegold [7] showed that $h(G)$ tends to infinity as $|G|$ tends to infinity, assuming that G has spread 1. If $P(G) = \varphi(G,2)/|G|^2$ denotes the probability that a random ordered pair of elements generates G then [18, Theorem 1.6] says that $P(G) = 1 - O(1/m(G))$ where $m(G)$ denotes the minimal index of a proper subgroup of G. From this an asymptotic formula readily follows for $h(G)$. However, for applications, it would be useful to have an explicit lower bound for $h(G)$. In this paper we prove the following.

Theorem 1.1. *For any non-abelian finite simple group G we have $2\sqrt{|G|} < h(G)$.*

This answers [16, Problem 17.116] posed by Wiegold which is to show $\sqrt{|G|} \leq h(G)$. Note that in the abstract of [6] it is claimed that this problem is due to Erfanian and Wiegold dating back to 1996.

Problem 17.116 of [16] has been solved for projective special linear groups [5], for certain symplectic groups [6], and for alternating groups [19]. Our proof of Theorem 1.1 is independent from these papers. In fact, by Hall's result above, in the case when G is different from A_5 and A_6, Theorem 1.1 is a direct consequence of the following.

Theorem 1.2. *Let G be a non-abelian finite simple group different from A_5 and A_6. Then $(2\cdot|\operatorname{Aut}(G)|\sqrt{|G|})/(|G|-1) < d(G)$.*

Date: April 17, 2011.

2000 *Mathematics Subject Classification.* Primary 20B30; Secondary 20P05.

Key words and phrases. finite simple group, generation.

The research of the first author was mainly supported by a grant from INDAM-GNSAGA, and partly by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme, by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, and by OTKA K84233.

Our proof of Theorem 1.2 depends heavily on the papers of Guralnick, Kantor [10] and Breuer, Guralnick, Kantor [2]. We must also note that, as shown by Guralnick, Liebeck, Saxl, Shalev [11] and Fulman, Guralnick [9] one can asymptotically do much better than Theorem 1.2.

The reader will learn that the papers [10] and [2] would allow better explicit bounds in Theorems 1.1 and 1.2. However our main motivation was to answer Wiegold's question, keeping the paper short.

2. Preliminaries

Let $\mathcal{S}$ be the set of non-abelian finite simple groups whose members are $\mathrm{Sp}_{2m}(2)$ with $m \geq 3$, $\Omega_8^+(2)$, $A_6 \cong \mathrm{Sp}_4(2)'$, $\Omega_7(3)$, $\mathrm{P}\Omega_8^+(3)$, A_7, $\mathrm{PSp}_4(3) \cong \mathrm{SU}_4(2)$, A_5, and M_{11}. By a result of Breuer, Guralnick, Kantor [2, Theorem 1.1] for any non-abelian finite simple group G there exists a (given) conjugacy class C such that for any $1 \neq g \in G$ the number of elements s in C with $\langle s, g\rangle = G$ is at least $\lambda|C|$ where $\lambda = 13/42$ if $G \in \mathcal{S}$ and $\lambda = 2/3$ if $G \notin \mathcal{S}$.

For our proof of Theorem 1.2 we will need a lower bound for $|C|$, that is, an upper bound for $|C_G(s)|$ where s denotes a representative of C.

In Section 3 of this paper we recall general results about centralizer sizes of elements in classical groups. We apply these bounds to fill in the corresponding columns in the tables in Section 4. In Section 5 we give an upper bound for $|C_G(s)|$, when G is a non-classical non-abelian simple group. In Section 6, with the help of the various tables, we perform most of the necessary calculations to show that the inequality (2) of Theorem 6.1 is satisfied. The case of $\mathrm{PSL}_2(q)$, which needs a more detailed analysis, is postponed to Section 7. The last Section of this paper deals with the finitely many simple groups left out from the proof of Theorem 1.2.

The invariants $|G|$ and $|\operatorname{Out}(G)|$ will be taken from [17, Pages 170-171]. The first three columns of Table 9 will be taken from [10, Table III] and [20, Table 1]. In various cases the exact value of $|C_G(s)|$ will be taken from the Atlas [3].

3. Bounds for centralizers in classical groups

In this paper we set $q = p^f$, where p is a prime and f is an integer. Also $\mathrm{SU}_d(q)$ denotes the special unitary group defined over the field of order q^2.

For the reader's convenience, we recall some basic facts, used in the next section.

Lemma 3.1. *Let X be an absolutely irreducible subgroup of $\mathrm{GL}_d(q)$ with center Z. For $x \in X$, set $s = Zx$. Then*

$$|C_{X/Z}(s)| \leqslant |C_X(x)| \leqslant |C_{\mathrm{GL}_d(q)}(x)|.$$

Proof. The group Z consists of scalar matrices, by the absolute irreducibility of X. Thus the preimage of $C_{X/Z}(s)$ in X is the group $\overline{C} = \{g \in X \mid x^g = \rho x,\ \rho I \in Z\}$. The map $g \mapsto \rho$ is a homomorphism from $\overline{C}$ into Z, with kernel $C_X(x)$. Hence $\left|\overline{C}\right| \leqslant |C_X(x)|\,|Z| \leqslant \left|C_{\mathrm{GL}_d(q)}(x)\right|\,|Z|$. Our claim follows from $C_{X/Z}(s) = \overline{C}/Z$. □

Assume first that x is an irreducible element of $\mathrm{GL}_d(q)$. The rational canonical form of x must be a companion matrix. It follows that the characteristic polynomial $m(t)$ is also the minimum polynomial of x. In particular $m(t)$ is irreducible in $\mathrm{F}_q[t]$ since, by Schur's Lemma, $C_{\mathrm{Mat}_d(q)}(x)$ is a division algebra. Thus the subalgebra $\mathrm{F}_q[x]$, generated by x, is a field of order q^d. Actually $\mathrm{F}_q[x] = C_{\mathrm{Mat}_d(q)}(x)$, since this centralizer has dimension d over F_q, by a formula of Frobenius (see [14, Theorem 3.16, p. 207]). Thus $C_{\mathrm{GL}_d(q)}(x)$ is cyclic of order $q^d - 1$.

When X is a classical group, we need the more precise upper bounds for $|C_X(x)|$, given in Table 1. They were determined by B. Huppert in [13]. In this table we assume $x \in X$, with x irreducible, having centralizer of maximal order.

Table 1

X	d	$\lvert C_X(x)\rvert$
$\mathrm{SL}_d(q)$	any	$(q^d-1)/(q-1)$
$\mathrm{SU}_d(q)$	odd	$(q^d+1)/(q+1)$
$\mathrm{Sp}_d(q)$, $\mathrm{SO}^-_d(q)$, $\mathrm{GO}^-_d(q)$	even	$q^{d/2}+1$
$\Omega^-_d(q)$	even	$(q^{d/2}+1)/(2,q+1)$

Let us explain row one of Table 1. If $x \in \mathrm{SL}_d(q)$ is irreducible, then there exists an element y in $C_{\mathrm{GL}_d(q)}(x)$ of order q^d-1. If $\alpha \in \mathrm{F}_{q^d}$ is an eigenvalue of y, the other eigenvalues are $\alpha^q, \ldots, \alpha^{q^{d-1}}$. It follows that α has order q^d-1. Hence $\det y = \alpha^{1+q+\cdots+q^{d-1}}$ has order $q-1$ and generates F_q^*. This explains why $\left|C_{\mathrm{SL}_d(q)}(x)\right| = \left(q^d-1\right)/\left(q-1\right)$.

Now let $d = d_1 + \cdots + d_k$ and x belong to $\mathrm{GL}_{d_1}(q) \times \cdots \times \mathrm{GL}_{d_k}(q)$. Clearly $\mathrm{F}_q^d = V_1 \oplus \cdots \oplus V_k$, where each V_i is an $\langle x\rangle$-module, of dimension d_i. In this case we write $x = \mathrm{blockdiag}(x_1, \ldots, x_k)$. If V is endowed with a non-singular scalar product J such that V_i is orthogonal to V_j for all $i \neq j$, we say that x is of type $d_1 \perp \cdots \perp d_k$. This follows the notation of the paper [2].

Lemma 3.2. *Let $x = \mathrm{blockdiag}(x_1, \ldots, x_k)$ where x_1, …, x_k are irreducible, with pairwise different characteristic polynomials of degrees d_1, …, d_k. Then*

$$C_{\mathrm{GL}_d(q)}(x) = C_{\mathrm{GL}_{d_1}(q)}(x_1) \times \cdots \times C_{\mathrm{GL}_{d_k}(q)}(x_k). \tag{1}$$

If x belongs to a classical group X, preserving a non-singular scalar product J, and x is of type $d_1 \perp \cdots \perp d_k$, then for all $i \leqslant k$:

(i) *the restriction J_i of J to V_i is non-singular;*

(ii) *for any $c \in C_X(x)$, its projection c_i in $\mathrm{GL}_{d_i}(q)$ preserves J_i.*

Proof. Let $V = \mathrm{F}_q^d$. Clearly $V = V_1 \oplus \cdots \oplus V_k$, where the V_i-s are irreducible, pairwise non-isomorphic $\langle x\rangle$-modules. If W is an $\langle x\rangle$-submodule isomorphic to V_i, for some $i \leqslant k$, then $W = V_i$. To see this, we may assume $i = 1$ and put $U = V_1 \oplus \cdots \oplus V_{k-1}$. From $W/(W \cap U) \cong (W+U)/U \leq V/U \cong V_k$ we have $W \leq U$. By induction on k we conclude that $W = V_1$.

For any $c \in C_{\mathrm{GL}_d(q)}(x)$, the map $w \mapsto cw$ is an $\langle x\rangle$-isomorphism from V_i to cV_i. Thus $cV_i = V_i$ for all $i \leqslant k$, whence (1).

As to the second part of the statement, we may assume that J is the matrix of the form with respect to the canonical basis. Under our assumptions we get $J = \mathrm{blockdiag}(J_1, \ldots, J_k)$. Part (i) follows immediately. To say that $g \in X$ preserves J means that $g^T J g^\sigma = J$, for a fixed automorphism σ of F_q of order 1 or 2. Part (ii) also follows. □

Remark. In the paper we apply Lemma 3.2 only for $k \leq 3$. On the other hand, in one occasion we need to deal with the slightly different case in which $x = \mathrm{blockdiag}(x_1, x_2, x_2)$ where x_1 and x_2 are irreducible, with different characteristic polynomials of degrees d_1 and d_2. As the centralizer of x must preserve the homogeneous components of the natural module, it is easy to see that

$$C_{\mathrm{GL}_d(q)}(x) = C_{\mathrm{GL}_{d_1}(q)}(x_1) \times \mathrm{GL}_2(q^{d_2}).$$

For further use we recall the standard embedding of $\mathrm{GL}_m(q)$ into $\mathrm{SO}^+_{2m}(q)$, given by $A \mapsto \mathrm{blockdiag}(A^t, A^{-1})$. Here we assume that $\mathrm{SO}^+_{2m}(q)$ preserves the quadratic form $\sum_{i=1}^m x_i x_{-i}$. Under this embedding $\mathrm{SL}_m(q)$ maps into $\Omega^+_{2m}(q) = \mathrm{SO}^+_{2m}(q)'$.

Lemma 3.3. *The following inequalities hold for all q.*

1. *Let k and n be integers with $1 \leq k \leq n/2$. Then $(q^{n-k}+1)(q^k+1) \leq 2q^n$.*
2. *Let k_1, k_2, n be integers with $2 \leq k_1 \leq k_2 \leq n-k_1-k_2$. Then we have $(q^{k_1}+1)(q^{k_2}+1)(q^{n-k_1-k_2}+1) \leq 2q^n$.*

(3) $(q+1)(q^2+1)(q^4+1) \leq 2q^7$.

Proof.

(1) This is equivalent to show that $q^{n-k}+q^k+1 \leq q^n$, that is to see that $1+(1/q^k) \leq q^{n-2k}(q^k-1)$. For $(k,q) \neq (1,2)$ the claim follows from $1+(1/q^k) \leq q^k-1$. For $(k,q)=(1,2)$ it can be checked directly.

(2) Observe that $q^i+1 \leq \sqrt[3]{2} \cdot q^i$ whenever $i = k_1$, k_2, or $n-k_1-k_2$. Now multiply together the left and right-hand sides of the three inequalities.

(3) The inequality is equivalent to $(q^7-1)/(q-1) < q^7$ which is clear. □

4. Classical groups

Let X be a linear classical group, with center Z, such that $G = X/Z$ is a non-abelian finite simple group. For $x \in X$ we denote by $s = Zx$ its projective image in G. In this section, for each conjugacy class C of G described in [2, Section 5], we call s a representative of C and find a convenient upper bound for $|C_G(s)|$. In finding this upper bound we use the ideas of Section 3. It is worth noting that our x corresponds to s in the notation of [2, Section 5].

For positive integers n and m we write (n,m) both for the ordered pair and for the greatest common divisor of n and m. Confusion should not arise.

Table 2

G	type of s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \operatorname{Out}(G)\rvert$
$\mathrm{PSp}_{2m}(q)$ q even $(m,q) \neq (2,2)$	A2	q^m+1	$q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$	$\leq 2f$
$\mathrm{PSp}_{2m}(q)$ q odd $m \geq 5$	B2	$2q^m$	$\frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$	$2f$
$\mathrm{PSp}_{2m}(q)$ q odd, $2 \leq m \leq 4$ $(m,q) \neq (2,3),(3,5),(3,7)$	A2	q^m+1	$\frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$	$2f$
$\mathrm{PSp}_6(q)$, $q=5,\,7$	B2	$2q^3$	$\frac{1}{2}q^9\prod_{i=1}^{3}(q^{2i}-1)$	2

The groups $\mathrm{PSp}_2(q) \cong \mathrm{PSL}_2(q)$ and $\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$ will be treated in Table 8 and Table 7 respectively. We also have $\mathrm{PSp}_4(2) \cong S_6$.

Types A2. In rows one and three of Table 2, let x be an irreducible element in $\mathrm{Sp}_{2m}(q)$ of order q^m+1. In this case, by Lemma 3.1 and Table 1, $|C_G(s)| \leq q^m+1$.

Type B2. In rows two and four of Table 2, setting $\delta = (2,m)$, let x be an element in $\mathrm{Sp}_{2m}(q)$ of type $2\delta \perp (2m-2\delta)$ and order $\mathrm{lcm}(q^\delta+1, q^{m-\delta}+1)$. By Lemmas 3.1, 3.2 and Table 1 we have $|C_G(s)| \leq (q^\delta+1)(q^{m-\delta}+1) \leq 2q^m$, where the second inequality follows from Lemma 3.3.

Table 3

G	type of s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \operatorname{Out}(G)\rvert$
$\mathrm{P}\Omega^+_{2m}(q)$ $m > 4$	A3	$2q^m$	$\geq \frac{1}{4}q^{m(m-1)}(q^m-1)\prod_{i=1}^{m-1}(q^{2i}-1)$	$\leq 8f$
$\mathrm{P}\Omega^+_8(q)$ $q \geq 5$	B3	$8q^8$	$\geq \frac{1}{4}q^{12}(q^2-1)(q^4-1)^2(q^6-1)$	$\leq 24f$
$\mathrm{P}\Omega^+_8(2)$	C3	15	$2^{12}\cdot 3^5\cdot 5^2\cdot 7$	6
$\mathrm{P}\Omega^+_8(3)$	D3	20	$2^{12}\cdot 3^{12}\cdot 5^2\cdot 7\cdot 13$	24
$\mathrm{P}\Omega^+_8(4)$	A3	$5\cdot 65$	$2^{24}\cdot 3^5\cdot 5^4\cdot 7\cdot 13\cdot 17^2$	12

The groups $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$ are treated in Table 8 and the groups $\mathrm{P}\Omega_4^+(q)$ and $\mathrm{P}\Omega_2^+(q)$ are not simple.

Type A3. Consider rows one and five of Table 3. Let x be an element of $\Omega_{2m}^+(q)$ of type $(m-\delta)^- \perp (m+\delta)^-$ and order $(q^{(m-\delta)/2}+1)(q^{(m+\delta)/2}+1)/(4,q-1)$ where $\delta = 1$ if m is odd and $\delta = 2$ if m is even. By Lemmas 3.1, 3.2 and Table 1 we have $|C_G(s)| \leq (q^{(m-\delta)/2}+1)(q^{(m+\delta)/2}+1)$. For row one this is at most $2q^m$ by Lemma 3.3. In row five the exact upper bound is $5 \cdot 65$.

Type B3. Consider row two of Table 3. Let $x \in X = \Omega_8^+(q)$ be as in [2, Lemma 5.15]. By [2, Lemma 3.6], we have $|C_X(x)| \leq 4q^2(q^4-1)(q^2-1) < 8q^8$. Whence $|C_G(s)| < 8q^8$ by Lemma 3.1.

Type C3. Consider row three of Table 3. Let x be an element of $\Omega_8^+(2)$ of order 15, arising from the embedding of $\mathrm{SL}_4(2)$ into $\Omega_8^+(2)$. Then s has order 15 and is self-centralizing in G (see also the Atlas [3]).

Type D3. Consider row four of Table 3. Let x be an element of $\Omega_8^+(3)$ of order 40, arising from the embedding of $\mathrm{SL}_4(3)$ into $\Omega_8^+(3)$. Then s has order 20 and is self-centralizing in G (see also the Atlas [3]).

Table 4

G	type of s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
$\mathrm{P}\Omega_{2m}^-(q)$ $m \geq 11$	A4	$2q^m$	$\geq \frac{1}{4}q^{m(m-1)}(q^m+1)\prod_{i=1}^{m-1}(q^{2i}-1)$	$\leq 8f$
$\mathrm{P}\Omega_{2m}^-(q)$ $m \geq 7$ odd $(m,q) \neq (7,2)$	B4	$2q^m$ if $m \neq 9$ q^{21} if $m = 9$	$\geq \frac{1}{4}q^{m(m-1)}(q^m+1)\prod_{i=1}^{m-1}(q^{2i}-1)$	$\leq 8f$
$\mathrm{P}\Omega_{2m}^-(q)$ $m \in \{4,5,6,8,10\}$	C4	q^m+1	$\geq \frac{1}{4}q^{m(m-1)}(q^m+1)\prod_{i=1}^{m-1}(q^{2i}-1)$	$\leq 8f$
$\mathrm{P}\Omega_{14}^-(2)$	C4	2^7+1	$2^{42} \cdot 3^9 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 43$	2

We have $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$ and $\mathrm{P}\Omega_4^-(q) \cong \mathrm{PSL}_2(q^2)$. These groups will be treated in Tables 6 and 8 respectively. The groups $\mathrm{P}\Omega_2^-(q)$ are not simple. Note that the groups $G = \mathrm{P}\Omega_{2m}^-(q)$ with $m \geq 11$ odd are considered both in rows one and two.

Type A4. Consider row one of Table 4. Let x be an element of $\Omega_{2m}^-(q)$ of type $(2m-10)^- \perp 6^- \perp 4^-$ and order $\mathrm{lcm}(q^{m-5}+1, q^3+1, q^2+1)/(2,q-1)$. By Lemmas 3.1, 3.2 and Table 1, we have $|C_G(s)| \leq (q^{m-5}+1)(q^3+1)(q^2+1)$. By Lemma 3.3, this is at most $2q^m$.

Type B4. In row two of Table 4, let $x \in X = \Omega_{2m}^-(q)$ of type $(m+1)^- \perp (m-5)^- \perp 4^-$ and order $\mathrm{lcm}(q^{(m+1)/2}+1, q^{(m-5)/2}+1, q^2+1)/(2,q-1)$. For $m \neq 9$ the same argument used in type A4 leads to the same upper bound. Let $m = 9$. Then, by Lemma 3.1, Table 1 and by the remark after Lemma 3.2, we have that $|C_G(s)| \leq |C_X(x)| \leq (q^5+1)|\,\mathrm{GL}_2(q^4)|/(q-1)$. If $q > 2$ then this is clearly less than q^{21} while for $q = 2$ it is less than 2^{21}.

Type C4. Consider rows three and four of Table 4. Let x be an irreducible element of $\Omega_{2m}^-(q)$ of order $(q^m+1)/(2,q-1)$. By Lemma 3.1 and Table 1, we have $|C_G(s)| \leq q^m+1$.

Table 5

G	type of s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
$\Omega_{2m+1}(3)$ $m \geq 4$ even	A5	3^{m+1}	$\frac{1}{2}3^{m^2}\prod_{i=1}^{m}(3^{2i}-1)$	2
$\Omega_{2m+1}(3)$ $m \geq 5$ odd	B5	3^{m+1}	$\frac{1}{2}3^{m^2}\prod_{i=1}^{m}(3^{2i}-1)$	2
$\Omega_{2m+1}(q)$ $q > 3$ odd $m \geq 3$	A5	q^{m+1}	$\frac{1}{2}q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$	$2f$
$\Omega_7(3)$	A5	3^4	$2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$	2

For q even we have $\Omega_{2m+1}(q) \cong \mathrm{PSp}_{2m}(q)$ and for all q we have $\Omega_5(q) \cong \mathrm{PSp}_4(q)$. These groups were treated in Table 2.

Type A5. Consider rows one, three and four of Table 5. Let $x = s$ be an element of $\Omega_{2m+1}(q)$ of type $1 \perp 2m^-$ and order $(q^m+1)/2$. By Table 1 and Lemma 3.2, $|C_G(s)| \leq (q-1)(q^m+1) < q^{m+1}$.

Type B5. Consider row two of Table 5. Let $x = s$ be an element of $\Omega_{2m+1}(3)$ of type $[3] \perp (2m-2)^-$ (here the first component is not irreducible) and order $3(3^{m-1}+1)/2$. Using Table 1 it is easy to see that $|C_G(s)| \leq 3(3^{m-1}+1) \leq 3^{m+1}$.

Table 6

G	type of s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
$\mathrm{PSU}_{2m+1}(q)$ $(m,q) \neq (1,3),$ $(1,5),(2,2)$	A6	$\frac{q^{2m+1}+1}{q+1}$	$\frac{1}{(2m+1,q+1)}q^{(2m+1)m}\prod_{i=2}^{2m+1}(q^i-(-1)^i)$	$2(2m+1,q+1)f$
$\mathrm{PSU}_{2m}(q)$ $m \geq 2$ $(m,q) \neq (2,2),$ $(2,3),(3,2)$	B6	$q^{2m-1}+1$	$\frac{1}{(2m,q+1)}q^{(2m-1)m}\prod_{i=2}^{2m}(q^i-(-1)^i)$	$\leq 2(2m,q+1)f$

Table 7

G	$\lvert s\rvert$	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
$\mathrm{PSU}_3(3)$	6	12	$2^5 \cdot 3^3 \cdot 7$	2
$\mathrm{PSU}_3(5)$	10	10	$2^4 \cdot 3^2 \cdot 5^3 \cdot 7$	6
$\mathrm{PSU}_4(2)$	9	9	$2^6 \cdot 3^4 \cdot 5$	2
$\mathrm{PSU}_4(3)$	7	7	$2^7 \cdot 3^6 \cdot 5 \cdot 7$	8
$\mathrm{PSU}_5(2)$	11	11	$2^{10} \cdot 3^5 \cdot 5 \cdot 11$	2
$\mathrm{PSU}_6(2)$	11	11	$2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$	6

The group $\mathrm{PSU}_3(2)$ is not simple.

Type A6. In row one of Table 6, let x be an irreducible element of $\mathrm{SU}_{2m+1}(q)$ and order $(q^{2m+1}+1)/(q+1)$. Then by Table 1 and Lemma 3.1, we have $|C_G(s)| \leq (q^{2m+1}+1)/(q+1)$.

Type B6. In row two of Table 6, let x be an element of $\mathrm{SU}_{2m}(q)$ of type $1 \perp (2m-1)$ of order $q^{2m-1}+1$. Then by Table 1 and Lemmas 3.1 and 3.2, we have $|C_G(s)| \leq q^{2m-1}+1$.

Type A8. Consider row one of Table 8. Let x be an element of $\mathrm{SL}_d(q)$ of type $e \oplus (d-e)$ and order $\mathrm{lcm}(q^e-1, q^{d-e}-1)/(q-1)$ where e is $(d+1)/2$ if d is odd, is $d/2+2$ if $d \equiv 2 \pmod 4$, and is $d/2+1$ if $d \equiv 0 \pmod 4$. By Lemmas 3.1, 3.2, and Table 1, we have $(q-1)|C_G(s)| \leq (q^e-1)(q^{d-e}-1) \leq q^d-1$.

Type B8. Consider rows two and four to ten of Table 8. Let x be an irreducible element in $\mathrm{SL}_d(q)$ of order $(q^d-1)/(q-1)$. By Table 1 we see that x is self-centralizing. The bound for $|C_G(s)|$ follows by Lemma 3.1.

Type C8. Consider row three of Table 8. Let x be an element in $X = \mathrm{SL}_6(q)$ of type $1 \oplus 5$ and order q^5-1. By Lemma 3.2 and Table 1, we have $|C_X(x)| = q^5-1$. The bound for $|C_G(s)|$ follows by Lemma 3.1.

Table 8

G	type of s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
$\mathrm{PSL}_d(q)$ $d \geq 8$, $d \neq 11$ $(d,q) \neq (8,2),(10,2)$	A8	$\frac{q^d-1}{q-1}$	$\frac{1}{(d,q-1)} q^{d(d-1)/2} \prod_{i=2}^{d}(q^i-1)$	$2(d,q-1)f$
$\mathrm{PSL}_d(q)$ $d=2$, $q \neq 4,5,7,9$ or $d=3$, $q \neq 4$ or $d=4,5,7,11$	B8	$\frac{q^d-1}{q-1}$	$\frac{1}{(d,q-1)} q^{d(d-1)/2} \prod_{i=2}^{d}(q^i-1)$	$\leq 2(d,q-1)f$
$\mathrm{PSL}_6(q)$ $q \geq 7$	C8	q^5-1	$\frac{1}{(6,q-1)} q^{15} \prod_{i=2}^{6}(q^i-1)$	$\leq 2(6,q-1)f$
$\mathrm{PSL}_{10}(2)$	B8	1023	$2^{45} \cdot 3^6 \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127$	2
$\mathrm{PSL}_8(2)$	B8	255	$2^{28} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 17 \cdot 31 \cdot 127$	2
$\mathrm{PSL}_6(5)$	B8	3906	$2^{13} \cdot 3^4 \cdot 5^{15} \cdot 7 \cdot 11 \cdot 13 \cdot 31^2 \cdot 71$	4
$\mathrm{PSL}_6(4)$	B8	1365	$2^{30} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 31$	12
$\mathrm{PSL}_6(3)$	B8	364	$2^{11} \cdot 3^{15} \cdot 5 \cdot 7 \cdot 11^2 \cdot 13^2$	4
$\mathrm{PSL}_6(2)$	B8	63	$2^{15} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$	2
$\mathrm{PSL}_3(4)$	B8	21	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	12

We have $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$, $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ and $\mathrm{PSL}_2(9) \cong A_6$. The alternating groups will be treated in Table 12.

5. The remaining simple groups

In this section we consider non-classical, non-abelian finite simple groups. For each such group G we describe the conjugacy class C (taken from [10] or [2]) by giving a representative s of the class. Then we give bounds for $|C_G(s)|$.

Table 9

G	$\lvert s\rvert$	$\frac{\lvert N_G(\langle s\rangle)\rvert}{\lvert s\rvert}$	$\lvert G\rvert$	$\lvert\operatorname{Out}(G)\rvert$
${}^2\mathrm{B}_2(q)$, $q=2^{2k+1}$, $k\geq 1$	$q_0^2+\sqrt{2}q_0+1$, $q_0=2^k\sqrt{2}$	4	$q^2(q^2+1)(q-1)$	f
${}^2\mathrm{G}_2(q)$, $q=3^{2k+1}$, $k\geq 1$	$q_0^2+\sqrt{3}q_0+1$, $q_0=3^k\sqrt{3}$	6	$q^3(q^3+1)(q-1)$	f
${}^2\mathrm{F}_4(q)$, $q=2^{2k+1}$, $k\geq 1$	$q_0^4+\sqrt{2}q_0^3+q_0^2+\sqrt{2}q_0+1$, $q_0=2^k\sqrt{2}$	12	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	f
$\mathrm{G}_2(q)$, $q\geq 5$	q^2-q+1	6	$q^6(q^6-1)(q^2-1)$	$\leq 2f$
${}^3\mathrm{D}_4(q)$	q^4-q^2+1	4	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	$3f$
$\mathrm{F}_4(q)$ $q\geq 4$	q^4-q^2+1	12	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	$\leq 2f$
$\mathrm{E}_6(q)$	q^6+q^3+1	9	$\geq \frac{1}{3}q^{36}\prod_{i\in\{12,9,8,6,5,2\}}(q^i-1)$	$\leq 6f$
${}^2\mathrm{E}_6(q)$ $q\geq 4$	q^6-q^3+1	9	$\geq \frac{1}{3}q^{36}\prod_{i\in\{12,9,8,6,5,2\}}(q^i-(-1)^i)$	$\leq 6f$
$\mathrm{E}_7(q)$ $q\geq 4$	$(q+1)(q^6-q^3+1)$	18	$\geq \frac{1}{2}q^{63}\prod_{i\{18,14,12,10,8,6,2\}}(q^i-1)$	$\leq 2f$
$\mathrm{E}_8(q)$	$q^8+q^7-q^5-q^4-q^3+q+1$	30	$q^{120}\prod_{i\in\{30,24,20,18,14,12,8,2\}}(q^i-1)$	f

Table 10

G	$\lvert s\rvert$	$\lvert C_G(s)\rvert\leq$	$\lvert G\rvert$	$\lvert\operatorname{Out}(G)\rvert$
$\mathrm{G}_2(3)$	13	13	$2^6\cdot 3^6\cdot 7\cdot 13$	2
$\mathrm{G}_2(4)$	13	13	$2^{12}\cdot 3^3\cdot 5^2\cdot 7\cdot 13$	2
${}^2\mathrm{F}_4(2)'$	13	13	$2^{11}\cdot 3^3\cdot 5^2\cdot 13$	2
$\mathrm{F}_4(2)$	17	17	$2^{24}\cdot 3^6\cdot 5^2\cdot 7^2\cdot 13\cdot 17$	2
$\mathrm{F}_4(3)$	73	$2^2\cdot 3\cdot 73$	$2^{15}\cdot 3^{24}\cdot 5^2\cdot 7^2\cdot 13^2\cdot 41\cdot 73$	1
${}^2\mathrm{E}_6(2)$	19	$3^2\cdot 19$	$2^{36}\cdot 3^9\cdot 5^2\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19$	6
${}^2\mathrm{E}_6(3)$	$19\cdot 37$	$\lvert\mathrm{SU}_3(27).3\rvert$	$2^{19}\cdot 3^{36}\cdot 5^2\cdot 7^3\cdot 13^2\cdot 19\cdot 37\cdot 41\cdot 61\cdot 73$	2
$\mathrm{E}_7(2)$	$43\cdot 3$	$3\cdot\lvert\mathrm{SU}_3(7)\rvert$	$2^{63}\cdot 3^{11}\cdot 5^2\cdot 7^3\cdot 11\cdot 13\cdot 17\cdot 19\cdot 31\cdot 43\cdot 73\cdot 127$	1
$\mathrm{E}_7(3)$	$4\cdot 19\cdot 37$	$12\cdot\lvert\mathrm{SU}_3(27)\rvert$	$2^{23}\cdot 3^{63}\cdot 5^2\cdot 7^3\cdot 11^2\cdot 13^3\cdot 19\cdot 37\cdot 41\cdot 61\cdot 73\cdot 547\cdot 757\cdot 1093$	2

We have ${}^2\mathrm{G}_2(3)' \cong \mathrm{PSL}_2(8)$ and $\mathrm{G}_2(2)' \cong \mathrm{PSU}_3(3)$. These groups were treated in Tables 8 and 7 respectively.

The bounds given in Table 10 for the centralizer sizes of elements s in $G=\mathrm{F}_4(2)$, $\mathrm{F}_4(3)$, ${}^2\mathrm{E}_6(2)$, ${}^2\mathrm{E}_6(3)$, $\mathrm{E}_7(2)$, and $\mathrm{E}_7(3)$ need an explanation. By [10, Table IV], in all cases there is exactly one maximal overgroup of $\langle s\rangle$ in G. These subgroups of G are $\mathrm{Sp}_8(2)$, ${}^3\mathrm{D}_4(3).3$, $\mathrm{SU}_3(8).3$, $\mathrm{SU}_3(27).3$, $\mathrm{SU}_8(2)$, and $2.{}^2\mathrm{E}_6(3).2$ in the respective cases. This gives the entry in column three for $G={}^2\mathrm{E}_6(3)$. An element of order 17 in $\mathrm{Sp}_8(2)$ is self-centralizing (see also [8]). This gives the corresponding entry for $G=\mathrm{F}_4(2)$. For $G=\mathrm{F}_4(3)$ we can choose the element s of order 73 to lie in ${}^3\mathrm{D}_4(3)$, and so by Table 9 it has centralizer in G of order at most $73\cdot 4\cdot 3$.

Table 11

G	s^G	$\lvert C_G(s)\rvert$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
M_{11}	11A	11	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	1
M_{12}	10A	10	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	2
M_{22}	11A	11	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	2
M_{23}	23A	23	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	1
M_{24}	21A	21	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	1
J_1	19A	19	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	1
J_2	10C	10	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	2
J_3	19A	19	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	2
J_4	29A	29	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	1
Fi_{22}	16A	32	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	2
Fi_{23}	23A	23	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	1
Fi'_{24}	29A	29	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 73 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	2
Co_3	21A	21	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	1
Co_2	23A	23	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	1
Co_1	35A	35	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	1
Suz	14A	28	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	2
McL	15A	30	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	2
He	14C	14	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	2
Ru	29A	29	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	1
Th	27A	27	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	1
HS	15A	15	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	2
HN	19A	19	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	2
O'N	31A	31	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	2
Ly	37A	37	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	1
B	47A	47	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	1
$\mathbb{M}$	59A	59	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot$ $13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	1

Now let $G = {}^2\mathrm{E}_6(2)$. By [8], an element of order 19 in $\mathrm{SU}_3(8).3$ has centralizer of size at most $3^2 \cdot 19$. Let $G = \mathrm{E}_7(2)$. In [10, Page 771] it is said that $C_G(s) \leq C_3 \times \mathrm{SU}_3(7)$.

Finally let $G = \mathrm{E}_7(3)$. Put $H = 2.{}^2\mathrm{E}_6(3)$. Then the group $H.2$ contains an element s of order $4 \cdot 19 \cdot 37$. In fact $t = s^4$ is contained in H. We clearly have

$$|C_G(s)| = |C_{H.2}(s)| \leq |C_{H.2}(t)| \leq 2 \cdot |C_H(t)|.$$

Let N be the normal subgroup of H of order 2. Then N is central in H and $\bar{t} = tN$ has order $19 \cdot 37$. By row seven of Table 10, we have $|C_{H/N}(\bar{t})| \leq |\mathrm{SU}_3(27).3|$. The entry in the last row of Table 10 now follows from $|C_H(t)| = 2 \cdot |C_{H/N}(\bar{t})|$.

Table 12

G	s	$\lvert C_G(s)\rvert \leq$	$\lvert G\rvert$	$\lvert \mathrm{Out}(G)\rvert$
A_n $n \geq 5$ $n \neq 6$	A12	$(n/2)^2$	$n!/2$	2
A_6	$\lvert s\rvert = 5$	5	$6!/2$	4

Type A12. Consider row one of Table 12. Let $n = 2m$ be even. Then let s be a permutation which is the product of two disjoint cycles, one of length $m-(2, m-1)$ and one of length $m + (2, m-1)$. If n is odd, then let s be an n-cycle.

6. Computations

Let $\mathcal{S}$, λ, C and s be as in Section 2.

Theorem 6.1. *Theorem* 1.2 *follows for the group G if the inequality*

$$\alpha \cdot |G| \geq |C_G(s)|^2 |\operatorname{Out}(G)|^2 \tag{2}$$

holds where $\alpha = 0.0225$ if $\lambda = 13/42$ and $\alpha = 0.1$ if $\lambda = 2/3$.

Proof. Suppose that G is a non-abelian finite simple group for which (2) holds where $s \in G$ is an element described in the previous sections. Notice that we have

$$\alpha < (\lambda/2)^2 (59/60)^2 \leq (\lambda/2)^2 ((|G|-1)/|G|)^2$$

since A_5 is the smallest non-abelian finite simple group. Applying this estimate to the left-hand side of (2) and taking square roots we get

$$(\lambda/2) \frac{|G|-1}{|G|} \sqrt{|G|} > |C_G(s)||\operatorname{Out}(G)|.$$

Multiplying both sides of this previous inequality by $|G|$, rearranging and using the fact that $|C| = |G|/|C_G(s)|$, one can deduce the inequality

$$\lambda |C| > \frac{2|\operatorname{Aut}(G)|\sqrt{|G|}|}{|G|-1}.$$

Now Theorem 1.2 follows by [2, Theorem 1.1]. □

The rest of this section is dedicated to analyze most of the non-abelian simple groups, in order to show that inequality (2) of Theorem 6.1 is satisfied. For the groups left out in this analysis, we show directly in Sections 7 and 8 that they satisfy Theorem 1.2 (with the exception of A_5 and A_6).

Theorem 6.2. *Let $G = \mathrm{PSp}_d(q)$ where $d \geq 4$ but $(d,q) \neq (4,2)$, $(4,3)$, and $(4,4)$. Let s be as in Table* 2*. Then we have*

$$0.0225 \cdot |G| \geq |C_G(s)|^2 |\operatorname{Out}(G)|^2.$$

Proof. Let $d = 2m$. Consider Table 2. In all cases we have $|C_G(s)| \leq 2 \cdot q^m$ and $|\operatorname{Out}(G)| \leq 2f$. Using these bounds it is sufficient to prove the inequality

$$q^{m^2-2m} \prod_{i=1}^{m} (q^{2i}-1) \geq (12800/9) \cdot f^2.$$

For $m = 2$ this holds for $q \geq 5$. Otherwise, for a fixed q, the minimum of the left-hand side occurs at $m = 3$. Hence it is sufficient to see $q^3(q^2-1)(q^4-1)(q^6-1) \geq (12800/9)f^2$ which is always the case. □

As said before, we do not consider the case $\mathrm{PSp}_4(2) \cong S_6$. The cases $\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$ and $\mathrm{PSp}_4(4)$, are treated in Theorem 6.6 and Section 8 respectively.

Theorem 6.3. *Let $G = \mathrm{P}\Omega_d^+(q)$ where $d \geq 8$. Let s be as in Table* 3*. Then we have*

$$0.0225 \cdot |G| \geq |C_G(s)|^2 |\operatorname{Out}(G)|^2.$$

Proof. Put $d = 2m$. First let $m > 4$. Then by the entries in Table 3 it is sufficient to show

$$q^{m(m-1)}(q^m-1) \prod_{i=1}^{m-1} (q^{2i}-1) \geq 45512 \cdot q^{2m} f^2.$$

After rearranging and using the bound $f < q$, it is sufficient to prove

$$q^{m^2-3m-2}(q^m-1) \prod_{i=1}^{m-1} (q^{2i}-1) \geq 45512.$$

The left-hand side of the previous inequality takes its minimum at $(m,q)=(5,2)$. After evaluating the left-hand side at this minimum we see that the inequality is valid.

Now let $m=4$ and $q\geq 5$. In this case it is sufficient to show the inequality

$$(q^2-1)(q^4-1)^2(q^6-1)\geq 6.6\cdot 10^6\cdot q^4f^2.$$

Now since $q^4f^2\leq q^6-1$, it is sufficient to show $(q^2-1)(q^4-1)^2\geq 6.6\cdot 10^6$. But this is clear for $q=5$.

Finally, for $(d,q)=(8,2)$, $(8,3)$, and $(8,4)$ the statement of the theorem can readily be checked from Table 3. □

Theorem 6.4. *Let $G=\mathrm{P}\Omega_d^-(q)$ where $d\geq 8$. Let s be as in Table 4. Then we have*

$$0.1\cdot|G|\geq|C_G(s)|^2|\operatorname{Out}(G)|^2.$$

Proof. Let $d=2m\geq 8$. First suppose that $m\neq 9$. Then $|C_G(s)|\leq 2q^m$ and $|\operatorname{Out}(G)|\leq 8f\leq 8q$. Using these bounds it is sufficient to verify the inequality

$$q^{m^2-3m-2}(q^m+1)\prod_{i=1}^{m-1}(q^{2i}-1)\geq 10240.$$

The left-hand side of this previous inequality takes its minimum at $(m,q)=(4,2)$ and this minimum is larger than 10240.

Now suppose that $m=9$. In this case we have a different upper bound on $|C_G(s)|$, namely q^{21}. Applying this estimate it is sufficient to show

$$q^{28}(q^9+1)\prod_{i=1}^{8}(q^{2i}-1)\geq 2560.$$

But this latter inequality is clear. □

Theorem 6.5. *Let $G=\Omega_d(q)$ where $d\geq 7$ is odd and $q\geq 3$. Let s be as in Table 5. Then we have*

$$0.1\cdot|G|\geq|C_G(s)|^2|\operatorname{Out}(G)|^2.$$

Proof. Let $d=2m+1$. Using the bound $|C_G(s)|\leq q^{m+1}$ and the fact that $|\operatorname{Out}(G)|=2f$ it is sufficient to show the inequality

$$q^{m^2-2m-2}\prod_{i=1}^{m}(q^{2i}-1)\geq 80f^2.$$

But this is clear for $m\geq 3$ and $q\geq 3$. □

Theorem 6.6. *Let $G=\mathrm{PSU}_d(q)$ where $d\geq 3$ and $(d,q)\neq(3,2),(3,8)$. Let s be as in Table 6. Then we have*

$$0.1\cdot|G|\geq|C_G(s)|^2|\operatorname{Out}(G)|^2$$

unless if $(d,q)=(4,2)$ in which case we have

$$0.0225\cdot|G|\geq|C_G(s)|^2|\operatorname{Out}(G)|^2.$$

Proof. The statements of the theorem can readily be checked if $(d,q)=(3,3)$, $(3,5)$, $(5,2)$, $(4,2)$, $(4,3)$, or $(6,2)$. So from now on assume that (d,q) is different from these tuples.

First assume that $d=2m+1$ is odd. Let $m\geq 2$. Then it is sufficient to consider the inequality

$$\frac{0.025}{(2m+1,q+1)}q^{(2m+1)m}\prod_{i=2}^{2m}(q^i-(-1)^i)\geq(q^{2m+1}+1)f^2.$$

To prove this for $m \geq 2$ it is sufficient to see that

$$q^{2(2m+1)}(q-1)(q^3+1)(q^4-1) \geq 40(q^{2m+1}+1)f^2$$

holds. But this is clear. Now let $m = 1$. Then it is sufficient to see the validity of the inequality

$$q^3(q^2-1)(q+1)^2 \geq 40(3,q+1)^3 f^2(q^3+1).$$

But this holds unless $q = 2$, 3, 5, or 8.

Now let $d = 2m$ be even with $m \geq 2$. Then it is sufficient to consider the inequality

$$q^{(2m-1)m}\Big(\prod_{i=2}^{2m-2}(q^i-(-1)^i)\Big)(q^{2m}-1) \geq 40(q^{2m-1}+1)f^2(2m,q+1)^3$$

which holds unless $(m,q) = (2,2)$ or $(2,3)$. □

As said before $\mathrm{PSU}_2(q) \cong \mathrm{PSp}_2(q)$ and the group $\mathrm{PSU}_3(2)$ is not simple.

Theorem 6.7. *Let $G = \mathrm{PSL}_d(q)$ with $d \geq 3$ and $(d,q) \neq (3,2)$, $(3,3)$, $(3,4)$, $(3,5)$, $(3,8)$, and $(4,2)$. Let s be as in Table 7. Then we have*

$$0.1 \cdot |G| \geq |C_G(s)|^2 |\operatorname{Out}(G)|^2.$$

Proof. First assume that $d \geq 4$. Since $|\operatorname{Out}(G)| \leq 2(q-1)q$ and $|C_G(s)| \leq (q^d-1)/(q-1)$, to prove the inequality in the statement of the theorem it is sufficient to consider the inequality

$$\frac{1}{40(q-1)} q^{d(d-1)/2} \prod_{i=2}^{d-1}(q^i-1) \geq (q^d-1)q^2.$$

To prove this inequality it is sufficient to consider the inequality

$$q^{d(d-1)/2} \prod_{i=2}^{d-1}(q^i-1) \geq 40 \cdot q^{d+3}. \tag{3}$$

If $d \geq 5$ then $d(d-1)/2-(d+3) \geq 2$, so in order to verify (3) for $d \geq 5$ it is sufficient to see $q^2 \prod_{i=2}^{d-1}(q^i-1) \geq 40$. But the left-hand side of this latter inequality takes its minimum for $(d,q) = (5,2)$ and $2^2 \prod_{i=2}^{4}(2^i-1) > 40$ so we are done. Now let $d = 4$. Then by (3) we have

$$(q^2-1)(q^3-1) \geq 40q$$

which is true for all $q \geq 3$.

Now let $d = 3$. Since $|\operatorname{Out}(G)| \leq 6f$ and $|C_G(s)| \leq (q^3-1)/(q-1)$, to prove the inequality in the statement of the theorem it is sufficient to consider the inequality

$$q^3(q^2-1)(q-1)^2 \geq 1080(q^3-1)f^2.$$

To prove this inequality it is sufficient to consider the following inequality

$$(q^2-1)(q-1)^2 \geq 1080f^2.$$

But this holds unless $q = 2$, 3, 4, 5, or 8. □

Theorem 6.8. *Let G be an exceptional simple group of Lie type, a sporadic simple group, or an alternating group of degree at least 9. Then the inequality (2) is satisfied.*

Proof. This follows by inspection of Tables 9-12. For $G = {}^2\mathrm{B}_2(8)$ note that an element of order 13 in G is self-centralizing (see [8]). □

Theorem 6.1 and Theorems 6.2-6.8 give the proof of Theorem 1.2 (and hence of Theorem 1.1) for the group G, unless G is one of the following groups: $\mathrm{PSL}_2(q)$, $\mathrm{PSp}_4(4)$, $\mathrm{PSU}_3(8)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_3(5)$, $\mathrm{PSL}_3(8)$, A_7, and $A_8 \cong \mathrm{PSL}_4(2)$.

7. The groups $\mathrm{PSL}_2(q)$

Denote by $\Phi(m)$ the Euler function, i.e., the number of integers i such that $1 \leqslant i < m$ with $(i, m) = 1$.

Theorem 7.1. *Let $G = \mathrm{PSL}_2(q)$, with $q \geqslant 11$. Then*

$$d(G) \geqslant \frac{1}{3}\ \Phi\left(\frac{q+1}{(2,q-1)}\right)\ \left(q^2-q\right).$$

Proof. Fix $1 \neq g_1 \in G$. Let C be a conjugacy class of elements of order $m = \frac{q+1}{(2,q-1)}$ in $\mathrm{PSL}_2(q)$. By [2, Theorem 1.1] there are at least $(2/3)|C| = (2/3)(q^2-q)$ elements $g_2 \in C$ such that $\langle g_1, g_2\rangle = G$ (since $q \geq 11$). For each power g_2^i such that $(i, m) = 1$, we have $\langle g_2\rangle = \langle g_2^i\rangle$, hence $\langle g_1, g_2^i\rangle = G$. Under the assumption $q \geqslant 11$, two powers g_2^i, g_2^j (with $(i, m) = (j, m) = 1$ and $-m/2 \leqslant i, j \leqslant m/2$) are conjugate in G only if $j = \pm i$. This means that there are $\frac{1}{2}\ \Phi(m)$ conjugacy classes C_i in G, of elements of order m, to which we may apply [2, Theorem 1.1]. Our claim follows. □

Let $G = \mathrm{PSL}_2(q)$ with $q \geq 13$. In order to prove Theorem 1.2 (whence Theorem 1.1) for these groups, it is sufficient to deduce from Theorem 7.1 the inequality

$$\frac{|G|-1}{|G|} \cdot \Phi\left(\frac{q+1}{(2,q-1)}\right)\ \cdot \frac{q^2-q}{6f} > 2\sqrt{|G|}.$$

Using $f \leqslant \sqrt{q}$ and the well known fact $\Phi(m) \geqslant \sqrt{m}$ whenever $m > 6$, the previous inequality holds if

$$\frac{59}{60}\sqrt{q-1} > 60 \cdot 12.$$

This is true if $q \geqslant 151$. For the intermediate values of q we use direct calculation.

That leaves us with the groups $A_5 \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $A_6 \cong \mathrm{PSL}_2(9)$, and $\mathrm{PSL}_2(11)$.

By [8], one finds $h(A_5) = 19 > 2\sqrt{60}$ and $h(A_6) = 53 > 2\sqrt{360}$. This proves Theorem 1.1 for these groups.

By [8], one also finds $d(\mathrm{PSL}_2(7)) = 80$, $d(\mathrm{PSL}_2(8)) = 336$, and $d(\mathrm{PSL}_2(11)) = 384$. The statement of Theorem 1.2 can be checked directly for these groups.

8. The remaining groups

In this section we prove Theorem 1.2 (and hence Theorem 1.1) for the remaining groups $G = \mathrm{PSp}_4(4)$, $\mathrm{PSU}_3(8)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_3(5)$, $\mathrm{PSL}_3(8)$, A_7, and $A_8 \cong \mathrm{PSL}_4(2)$.

By [8], one finds $d(\mathrm{PSL}_3(3)) = 2784$, $d(\mathrm{PSL}_3(4)) = 8448$, $d(A_7) = 720$ and $d(A_8) = 4992$. The statement of Theorem 1.2 can be checked directly for these groups.

Let G be any of the four remaining groups and let s be as in Section 4. Suppose that the generators of the cyclic group $\langle s\rangle$ fall into k conjugacy classes of G. Then we clearly have $d(G) \geq (2/3)k \cdot |C|$ by [2, Theorem 1.1] since G does not belong to $\mathcal{S}$. The value for k is 4 if $G = \mathrm{PSp}_4(4)$, is 6 if $G = \mathrm{PSU}_3(8)$, is 10 for $G = \mathrm{PSL}_3(5)$, and is 24 for $\mathrm{PSL}_3(8)$. Hence, to prove Theorem 1.2 for these groups, it remains to show the variation of the inequality (2) with α replaced by $0.1 \cdot k^2$. In all four cases the statement of Theorem 1.2 hold.

References

[1] M. Aschbacher and R. M. Guralnick, Some applications of the first cohomology group. *J. Algebra* **90** (1984), no. 2, 446-460.

[2] T. Breuer; R. M. Guralnick; W. M. Kantor, Probabilistic generation of finite simple groups, II. *J. Algebra* Vol. 320. **2**, (2008), 443-494.

[3] J. H. Conway; R. T. Curtis; S. P. Norton; R. A. Parker; R. A. Wilson, Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. *Oxford University Press*, Eynsham, (1985).

[4] L. E. Dickson, Linear groups: With an exposition of the Galois field theory. Dover Publications, Inc., New York, 1958.

[5] A. Erfanian, A note on growth sequences of $\mathrm{PSL}(m, q)$. *Southeast Asian Bull. Math.* **29** (2005), no. 4, 697-713.

[6] A. Erfanian and R. Rezaee, On the growth sequences of $\mathrm{PSp}(2m, q)$. *Int. J. Algebra* **1** (2007), no. 1-4, 51-62.

[7] A. Erfanian and J. Wiegold, A note on growth sequences of finite simple groups. *Bull. Austral. Math. Soc.* **51** (1995), no. 3, 495-499.

[8] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version 4.4*; 2005, (`http://www.gap-system.org`).

[9] J. Fulman and R. M. Guralnick, The probability of generating an irreducible subgroup, preprint.

[10] R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups. Special issue in honor of Helmut Wielandt. *J. Algebra* **234** (2000), no. 2, 743-792.

[11] R. M. Guralnick; M. W. Liebeck; J. Saxl; A. Shalev, Random generation of finite simple groups. *J. Algebra* **219** (1999), no. 1, 345355.

[12] P. Hall, The Eulerian function of a group. *Quart. J. Math. Oxford* **7** (1936) 134-151.

[13] B. Huppert, Singer-Zyklen in Klassischen Gruppen. *Math. Z.* **117** (1970), 141-150.

[14] N. Jacobson, Basic Algebra I, Second Edition, W.H. Freeman and Company, 1985.

[15] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group. *Geom. Dedicata* **36** (1990), no. 1, 67-87.

[16] The Kourovka Notebook. Unsolved problems in group theory. Seventeenth augmented edition, 2010. Edited by V. D. Mazurov and E. I. Khukhro.

[17] P. B. Kleidman and M. W. Liebeck, The subgoup structure of the finite classical groups. *London Math. Soc. Lecture Notes, Cambridge Univ. Press* **129**, (1990).

[18] M. W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* **184** (1996), no. 1, 31–57.

[19] A. Maróti and M. C. Tamburini, Bounds for the probability of generating the symmetric and alternating groups. *Arch. Math. (Basel)* **96** (2011), 115-121.

[20] T. S. Weigel, Generation of exceptional groups of Lie-type. *Geom. Dedicata* **41** (1992), no. 1, 63-87.

MTA Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: `maroti@renyi.hu`

Dipartimento di Matematica e Fisica, Università Cattolica del Sacro Cuore, Via Musei 41, 25121 Brescia, Italy

E-mail address: `c.tamburini@dmf.unicatt.it`