Groups Geom. Dyn. 1 (2007), 585–611 **Groups, Geometry, and Dynamics**

Complements of the socle in monolithic groups

Andrea Lucchini, Federico Menegazzo and Marta Morigi

To Avinoam Mann, in occasion of his 68th birthday, with gratitude

Abstract. We show that if H is a finite group with a unique minimal normal subgroup N, which is not abelian, then the number of conjugacy classes of complements of N in H is strictly smaller than $|N|$.

Mathematics Subject Classification (2000). 20E32, 20F28, 20J06.

Keywords. Monolithic groups, complements, finite simple groups.

Let G be a finite group and let K be a field. As one of the first applications of the classification of finite simple groups, Aschbacher and Guralnick [2] proved that if V is a faithful irreducible KG-module, then $\dim_K \mathrm{H}^1(G,V) < \dim_K V$. Clearly this result can be equivalently stated as follows: let H be a finite monolithic group, i.e. a group with a unique minimal normal subgroup $N = \operatorname{soc} H$; if N is abelian, then the number of conjugacy classes of complements of N is H is strictly smaller than $|N|$. One can ask whether the same result remains true without assuming that $N = \operatorname{soc} H$ is abelian; in other words the question is whether an analog of the theorem of Aschbacher and Guralnick holds in the non abelian context.

A first positive but partial answer has been given in [14], which considered the particular case when $N = \operatorname{soc} H$ is a simple group; in that paper, with a case by case analysis of the various possibilities, we proved that if the socle N of an almost simple group H is complemented, than there are less than $|N|$ conjugacy classes of complements of N in H. So in order to complete the discussion of this problem the case remains to be discussed when H is a monolithic group whose socle N is the direct product $S_1 \times \cdots \times S_k$ of k isomorphic non abelian simple groups and $k > 1$. Under these hypotheses, a useful tool is a result proved independently by Gross

The authors thank the anonymous referee for her/his helpful remarks and suggestions. The investigation is supported by MIUR (project Teoria dei gruppi e applicazioni) and the Universities of Bologna, Brescia and Padova.

and Kovács ([9], Corollary 4.4) and by Aschbacher and Scott ([3], Theorem 2): if $K = S_2 \times \cdots \times S_k$, then there is a bijection between the conjugacy classes of complements of N in H and the conjugacy classes of complements of N/K in $N_H(K)/K$. Using this result, it is not difficult to prove that there exists an absolute constant $c \leq 4$ such that the number of conjugacy classes of complements of N in H is smaller than $|N|^c$ (see, for example, [15], Lemma 2.8). The bound $c \leq 4$ can be obtained without a heavy use of the classification of finite simple groups: the only information which is needed is that any subgroup of the outer automorphism group of a finite simple group can be generated by three elements. But to establish our result we have to prove $c = 1$ and this requires a more detailed analysis, especially in the case of groups of Lie type. This is the work which is performed in the present paper and which leads to the following ultimate result:

Theorem. *Let H be a finite group with a unique minimal normal subgroup N, which is not abelian. Then the number of conjugacy classes of complements of N in H is strictly smaller than $|N|$.*

In Section 1 we prove that counting the conjugacy classes of complements of N/K in $N_H(K)/K$ is equivalent to counting up to conjugacy certain homomorphisms from $N_H(K)/K$ to $\mathrm{Aut}(S)$ and we give the general outline of the proof of the theorem. A short argument, depending on a result of P. Neumann, supplies the necessary bound when $|\mathrm{Out}(S)| \leq 2$. This holds for sporadic and alternating groups $\mathrm{Alt}(n)$ when $n \neq 6$. So we are left with simple groups S of Lie type, which are treated with a case-by-case analysis based on the isomorphism type of S. This discussion depends on the structure of $\mathrm{Out}(S)$, the most complicated cases being when $\mathrm{Out}(S)$ has subgroups requiring 3 generators. The cases $S = A_n(q)$, ${}^2A_n(q)$ and $D_l(q)$ are those that require a more careful analysis and are discussed in Section 3, 4 and 5 respectively. The remaining groups of Lie type are discussed in Section 6. Section 2 contains some technical results on generators and centralizers.

1. Preliminary results and outline of the proof

Let S be a finite simple nonabelian group, and assume that S is a normal subgroup of the group X. Consider the map $\iota\colon X \to \mathrm{Aut}(S)$ defined by $x \to \iota(x)$, where $\iota(x)$ is the automorphism induced by x on S by conjugation. We have the following:

Proposition 1. *Let X be a finite group and S a nonabelian simple normal subgroup of X. Let $\mathcal{C}$ be the set of complements to S in X and $\mathcal{H}$ the set of homomorphisms $\varphi\colon X/S \to \mathrm{Aut}(S)$ such that $\pi \circ \varphi = \rho$, where $\pi\colon \mathrm{Aut}(S) \to \mathrm{Out}(S)$ is the natural map and $\rho\colon X/S \to \mathrm{Out}(S)$ is defined by $\rho\colon Sx \mapsto \mathrm{Inn}(S)\iota(x)$. Then:*

(1) *The map $Y \mapsto \varphi_Y$ is a bijection of $\mathcal{C}$ with $\mathcal{H}$, where $\varphi_Y\colon Sy \mapsto \iota(y)$ for $y \in Y$.*

(2) *S acts on $\mathcal{H}$ on the left via $s\colon \varphi \mapsto c_{\iota(s)}\circ\varphi$, where for $\alpha \in \mathrm{Aut}(S)$, $c_\alpha\colon \mathrm{Aut}(S) \to \mathrm{Aut}(S)$ is defined to be conjugation by α.*

(3) *$Y, Z \in \mathcal{C}$ are conjugate in X if and only if φ_Y and φ_Z are in the same orbit of S on $\mathcal{H}$. Thus there is a bijection between the set $\mathcal{C}/S$ of conjugacy classes of complements to S in X with the set $\mathcal{H}/S$ of orbits of S on $\mathcal{H}$.*

Proof. (1) Let Y be a complement of S in X. The fact that the map φ_Y is a well-defined group homomorphism such that $(\pi \circ \varphi_Y)(Sx) = \mathrm{Inn}(S)\iota(x)$ is straightforward. Moreover, if $Z \neq Y$ is another complement of S in X then $\varphi_Y \neq \varphi_Z$. Namely, if $z \in Z \setminus Y$ then there exists a unique $y \in Y$ such that $Sz = Sy$ and $\iota(y) = \varphi_Y(Sy) = \varphi_Y(Sz) \neq \varphi_Z(Sz) = \iota(z)$, because $\iota(y) = \iota(z)$ implies that $zy^{-1} \in C_X(S) \cap S = 1$ and thus $z = y$, a contradiction. On the other side, if $\varphi\colon \frac{X}{S} \to \mathrm{Aut}(S)$ is such that $\pi \circ \varphi = \rho$, consider the subgroup of X defined by $Y = Y_\varphi = \{x \in X \mid \iota(x) = \varphi(Sx)\}$. Let now $x \in X$; as $\mathrm{Inn}(S)\iota(x) = \mathrm{Inn}(S)\varphi(Sx)$, there exists $s \in S$ such that $\varphi(Sx) = \iota(s)\iota(x)$. It follows that $\varphi(Ssx) = \varphi(Sx) = \iota(sx)$, so $sx \in Y$ and $x \in SY$, implying that $X = SY$. Moreover if $x \in S \cap Y$ we have that $\iota(x) = \varphi(S) = 1$ and so $x \in C_X(S) \cap S = 1$. This proves that Y is a complement of S in X. Moreover, for this Y and for any $y \in Y$ we have $\varphi_Y(y) = \iota(y) = \varphi(Sy)$, so that the maps $Y \mapsto \phi_Y$ and $\phi \mapsto Y_\phi$ are inverses to each other.

(2) This is clear since $c_{\iota(st)} = c_{\iota(s)\iota(t)} = c_{\iota(s)}c_{\iota(t)}$ for every $s, t \in S$.

(3) Let Y and Z be two complements of S. We have that $Y = Z^s$ for some $s \in S$ if and only if $\varphi_Y = c_{\iota(s)} \circ \varphi_Z$, as $c_{\iota(s)} \circ \varphi_Z\colon Sz = Sz^s \mapsto \iota(z)^{\iota(s)} = \iota(z^s)$. □

Outline of the proof of the theorem. As already mentioned in the introduction, we have that $N = S_1 \times \cdots \times S_k$, where S_i is isomorphic to some fixed nonabelian simple group S for every $i = 1, \ldots, k$. Let $K = S_2 \times \cdots \times S_k$; then by [9], Corollary 4.4 or [3], Theorem 2 there is a bijection between the conjugacy classes of complements of N in H and the conjugacy classes of complements of $N/K \cong S$ in $X := N_H(K)/K$.

We note that, as N is the unique minimal normal subgroup of H and it is nonabelian, $H \leq \mathrm{Aut}(N) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}(k)$ (see Proposition 3.3.20 of [17]), the permutational wreath product of the automorphism group of S by the symmetric group of degree k, and $N_H(K) = N_H(S_1) \leq N_{\mathrm{Aut}(N)}(S_1) \cong \mathrm{Aut}(S) \times (\mathrm{Aut}(S) \wr \mathrm{Sym}(k-1))$, so that, identifying N/K with S, we have that $\frac{X}{S} \leq \mathrm{Out}(S) \times (\mathrm{Out}(S) \wr \mathrm{Sym}(k-1))$.

By Proposition 1 we need to count $\mathrm{Inn}(S)$-classes of homomorphisms $\varphi\colon X/S \to \mathrm{Aut}(S)$ such that $\varphi(Sx) \in \mathrm{Inn}(S)\iota(x)$ for all $x \in X$. We will choose a suitable set $\mathcal{X} = \{y_1, \ldots, y_s\}$ of generators of X/S and use the fact that φ is determined by its effect on the elements of $\mathcal{X}$. So we will first bound the number of possible choices for $\varphi(y_1)$ (possibly up to $\mathrm{Inn}(S)$-conjugacy), then once $\varphi(y_1)$ is given we bound the number of possible choices for $\varphi(y_2)$ and so on.

The following observation will often be used in the sequel:

Lemma 2. *With the same notation as in Proposition* 1 *the following hold:*

i) *if* $T \leq X/S$ *is normalized by* $y \in X/S$ *and* $\varphi(T)$ *is given, then there are at most* $|C_S(\varphi(T))|$ *possible choices for* $\varphi(y)$*;*

ii) *if* $\varphi(y)$ *is subject to the further condition* $\varphi(y) \in P$ *for a fixed subgroup* $P \leq \mathrm{Aut}(S)$*, then there are at most* $|C_S(\varphi(T)) \cap P|$ *possible choices for* $\varphi(y)$.

Proof. For every $x \in T$ we have that $\varphi(x)^{\varphi(y)} = \varphi(x^y) = \varphi(x)\varphi([x,y]) \in \varphi(T)$ is given, so that if z_1, z_2 are two possible choices for $\varphi(y)$, then $z_1 z_2^{-1} \in C_{\mathrm{Aut}(S)}(\varphi(x))$. Moreover, the definition of $\mathcal{H}$ in Proposition 1 gives that $z_1 z_2^{-1} \in \mathrm{Inn}(S)$, so that $z_1 z_2^{-1} \in C_{\mathrm{Inn}(S)}(\varphi(x))$. This implies that $z_1 z_2^{-1} \in C_{\mathrm{Inn}(S)}(\varphi(T))$, i.e $z_1 C_{\mathrm{Inn}(S)}(\varphi(T)) = z_2 C_{\mathrm{Inn}(S)}(\varphi(T))$. As $|C_{\mathrm{Inn}(S)}(\varphi(T))| = |C_S(\varphi(T))|$ the result follows. The last statement is obvious. □

Lemma 3. *With the same notation as in Proposition* 1*, assume that* X *is* k*-generated. Then the number of conjugacy classes of complements of* S *in* X *is strictly smaller than* $|S|^k$.

Proof. We apply Proposition 1. The definition of $\mathcal{H}$ implies that if $\varphi \in \mathcal{H}$ then $\varphi(a)$ is determined modulo $\mathrm{Inn}(S)$ for each $a \in \mathcal{X}$, so that there are at most $|\mathrm{Inn}(S)|^k = |S|^k$ choices for φ. The S-orbit of φ has length greater than 1 unless φ is trivial; it follows that the number of S-orbits of $\mathcal{H}$ is indeed strictly smaller than $|S|^k$.

Lemma 1 and Lemma 2 indicate that information on the structure and generators of $\overline{X} = X/S$, as well as on centralizers of subgroups of $\mathrm{Aut}(S)$, will be crucial. We will come back to this point in the next section. For the moment, we recall a result of P. Neumann whose proof can be found in [4].

Let x be a real number; the notation $\lfloor x \rfloor$ indicates the greatest integer less or equal to x.

Lemma 4. *Let* $G \leq \mathrm{Sym}(k)$ *be a permutation group of degree* k*. Then* G *can be generated by at most* $\lfloor \frac{k}{2} \rfloor$ *elements if* $k \neq 3$*, and at most* 2 *elements if* $k = 3$.

When $S = \mathrm{Alt}(n)$ with $n \neq 6$ or S is a sporadic simple group, it is well known that $|\mathrm{Out}(S)| \leq 2$ so that $X \leq C_2 \times (C_2 \wr \mathrm{Sym}(k-1)) \leq \mathrm{Sym}(2k)$ and by Lemma 4 it is possible to choose a set $\mathcal{X}$ of generators of X/S of order k (here C_2 is the cyclic group of order 2). Then we apply Lemma 3 and we obtain that the number of conjugacy classes of complements of S in X is strictly smaller than $|S|^k = |N|$. By [9, Corollary 4.4] or [3, Theorem 2] this concludes the proof. □

As $\mathrm{Alt}(6)$ is isomorphic to $\mathrm{PSL}(2,9)$ we may now assume that S is a finite simple group of Lie type over a field $\mathrm{GF}(p^m)$ of order p^m, for some prime p. We will follow the definitions and notation of the book [8], unless otherwise stated. So S will be a group of the form $S = \Sigma_l(q)$ where l is the Lie rank of S and $q = p^m$, for some prime p. Also, ϕ denotes the Frobenius map.

The structure of $\mathrm{Aut}(S)$ and $\mathrm{Out}(S)$ is well known and is described *e.g.* in [8, Theorem 2.5.12].

2. Generators and centralizers

We present here some results on generators. We denote with $\mathrm{d}(G)$ the minimum number of generators of the (finite) group G.

Lemma 5. *Let p be a prime, and P a Sylow p-subgroup of $\mathrm{Sym}(k)$. If $H \leq P$ then $\mathrm{d}(H) \leq \lfloor \frac{k}{p} \rfloor$. If $p \mid k$, $t = \frac{k}{p}$, $p \neq 2$ and $G \leq \mathrm{Sym}(k)$ has an abelian factor group of order p^t, then G is an elementary abelian p-group of rank t.*

Proof. This is a simple consequence of Theorem and Corollary in [12]. □

Lemma 6. *Let $H \in \{\mathrm{Sym}(3), C_6\}$. If G is a subgroup of $H \wr \mathrm{Sym}(k)$, then $\mathrm{d}(G) \leq k + 1$. Moreover the equality $\mathrm{d}(G) = k + 1$ holds only if $H = \mathrm{Sym}(3)$ and $G = \mathrm{Alt}(3)^k \langle g \rangle$ where g is an involution that inverts every element of $\mathrm{Alt}(3)^k$.*

Proof. The group G has a factor group G/N such that $\mathrm{d}(G/N) = \mathrm{d}(G)$, its socle M/N is the direct product of G-equivalent chief factors of G, and $C_G(M/N) \leq M$ (see for example [6, Corollary 15]). If M/N is abelian, then there exist an irreducible G-module A and an integer t such that M/N is G-isomorphic to A^t; the relation between $\mathrm{d}(G)$, t and the structure of A as a G-module can be deduced from a formula due to Gaschütz, as explained for example in [5]; in particular (as follows from Lemma 1.5 in [13]), $\mathrm{d}(G) \leq t + 1$ and if $\mathrm{d}(G) = t + 1$ then G does not centralize A. Now let $B = H^k$ be the base subgroup of $H \wr \mathrm{Sym}(k)$ and let $E = O_3(B \cap G)$. Then $E \leq M$. If $E \leq N$, then $\mathrm{d}(G) = \mathrm{d}(G/N) = \mathrm{d}(G/E) \leq k$, since G/N is isomorphic to a subgroup of $\mathrm{Sym}(2) \wr \mathrm{Sym}(k) \leq \mathrm{Sym}(2k)$. If $E \not\leq N$, then M/N is a 3-group, in particular $M/N \cong A^t$, with A an irreducible G-module. Note that $O_2(B \cap G) \leq N$ and G/N is a factor group of $\mathrm{Sym}(3) \wr \mathrm{Sym}(k) \leq \mathrm{Sym}(3k)$, hence, by Lemma 5, $\mathrm{d}(M/N) \leq k$. As $t\mathrm{d}(A) = \mathrm{d}(M/N)$, we have $\mathrm{d}(G) \leq t + 1 \leq k + 1$. Moreover if $\mathrm{d}(G) = k + 1$ then $t = k$, $A \cong C_3$ is non central and, again by Lemma 5, $N = O_2(B \cap G)$. This cannot occur if $H = C_6$, since no element of $C_6 \wr \mathrm{Sym}(k)$ acts as inversion on the Sylow 3-subgroup of the base subgroup of the wreath product. So $H = \mathrm{Sym}(3)$, $N = 1$, $M = \mathrm{Alt}(3)^k$, $|G/M| = 2$ and any element of order 2 in G acts on M as inversion. □

Lemma 7. *Let G be a finite group and let A be an abelian normal subgroup of G. We have $\mathrm{d}(G) \leq \mathrm{d}(A \rtimes (G/A))$.*

Proof. As we recalled in the proof of the previous lemma, G has a factor group G/N such that $\mathrm{d}(G/N) = \mathrm{d}(G)$, the socle $M/N \cong B^\delta$ of G/N is the direct

product of δ G-equivalent non-Frattini chief factors of G, and $C_G(M/N) \leq M$. Since A centralizes every chief factor of G, we have $A \leq M$. If $A \leq N$, then $\mathrm{d}(G) = \mathrm{d}(G/N) = \mathrm{d}(G/A) \leq \mathrm{d}(A \rtimes (G/A))$. Assume now $N < AN \leq M$. In this case M/N has a complement in G/N and $G/N \cong B^\delta \rtimes G/M$. There exists $\delta_1 \leq \delta$ with $M/AN \cong_G B^{\delta_1}$ and $A/A \cap N \cong_G AN/N \cong_G B^{\delta-\delta_1}$. This means that $G/N \cong (A/A \cap N) \rtimes G/AN$ is an epimorphic image of $A \rtimes G/A$. □

Lemma 8 ([10], Proposition 3.6). *If P is a Sylow subgroup of a non abelian simple group S, then $|P|^2 < |S|$.*

Most of the relevant information on centralizers in S of subgroups of $\mathrm{Aut}(S)$, where S is a simple group, is well known and can be found *e.g.* in [8] or [11]. We present here a few special results that we could not find in the literature.

If r is a prime and x is an integer, x_r will indicate the biggest power of r dividing x.

Lemma 9. *Let $S = \Sigma_l(q)$ be an untwisted simple group, where $q = p^m$ for some prime p, ϕ the Frobenius automorphism, and $d = |\mathrm{OutDiag}(S)|$. For every $a \in \mathrm{InnDiag}(S)$ we have that $|C_S(\phi^t a)| \leq (d\,|S|)^{\frac{1}{|\phi^t|}}$.*

Proof. By the Lang–Steinberg theorem (see [8, Theorem 2.1.1]) $\phi^t a$ is conjugate to ϕ^t in $\Sigma_l(\bar{F})$, where $\bar{F}$ is the algebraic closure of the field F with q elements. So we have $|C_S(\phi^t a)| \leq |C_{\Sigma_l(\bar{F})}(\phi^t a)| = |C_{\Sigma_l(\bar{F})}(\phi^t)| = \left|\mathrm{InnDiag}\left(\Sigma_l\left(q^{\frac{1}{|\phi^t|}}\right)\right)\right|$ $\leq (d\,|S|)^{\frac{1}{|\phi^t|}}$, where the last inequality follows by direct calculation. □

Lemma 10. *Let $S = \mathrm{PSL}(n,q)$, and $d = (n, q-1)$. For every $a \in \mathrm{InnDiag}(S)$ we have that $|C_S(a)| \leq \frac{1}{d}|\mathrm{GL}(n-1,q)|$ if $n \geq 3$ and $|C_S(a)| \leq q+1$ if $n = 2$.*

Proof. The structure of $C_{\mathrm{PGL}(n,q)}(a)$ is described in [8, Theorem 4.2.2], and then the result follows by comparing orders. □

Lemma 11. *Let $S = \mathrm{PSL}(n,q)$ where $q = p^m$ for some prime p, ϕ the Frobenius automorphism, and $d = (n, q-1)$. Assume that $a, b \in \mathrm{InnDiag}(S)$, $|a| = r$ where r is a prime which divides d, d is not a power of 2, m is even and $\phi^{\frac{m}{2}} b$ induces on $\langle a \rangle$ an automorphism of order at most 2. Then $|C_S(\langle \phi^{\frac{m}{2}} b, a\rangle)| \leq |\mathrm{GL}(n-1, q^{\frac{1}{2}})|$ and $|C_S(\langle \phi^{\frac{m}{2}} b, a\rangle)|_2 \leq |\mathrm{GL}(n-1, q^{\frac{1}{2}})|^{\frac{1}{2}}$.*

Proof. Let $C = C_S(\langle \phi^{\frac{m}{2}} b, a\rangle)$. From the fact that $d \neq d_2$ it follows that $n \geq 3$, $n \neq n_2, q \neq 9$ and $|q-1|_2 \leq \frac{q-1}{3}$. Moreover $a^{\phi^{\frac{m}{2}} b} \in \{a^{\pm 1}\}$. Let $\bar{F}$ be the algebraic closure of the field with q elements.

Assume that $a^{\phi^{\frac{m}{2}} b} = a$. Then by the Lang–Steinberg theorem (see [8, Theorem 2.1.1]) we have that $(\phi^{\frac{m}{2}} b)^y = \phi^{\frac{m}{2}}$ for some $y \in \mathrm{PSL}(n, \bar{F})$, so that $|C| \leq$

$|C_{\mathrm{PSL}(n,\bar{F})}(\langle \phi^{\frac{m}{2}}, a^y\rangle)|$. Now $C_{\mathrm{PSL}(n,\bar{F})}(\phi^{\frac{m}{2}}) = \mathrm{PGL}(n, q^{\frac{1}{2}})$, and the result follows by Lemma 10 because $a^y \in \mathrm{InnDiag}(\mathrm{PSL}(n, q^{\frac{1}{2}}))$.

So we may assume that $a^{\phi^{\frac{m}{2}} b} = a^{-1}$ and r is odd. Let $A, B \in \mathrm{GL}(n, \bar{F})$ be two pre-images of a and b, so that $(A^{\phi^{\frac{m}{2}} B})^{-1} = \xi A$ for some $\xi \in \bar{F}$. We may assume that A is a diagonal matrix, and let $W_1, \ldots, W_t$ be the eigenspaces of A, with eigenvalues $\lambda_1, \ldots, \lambda_t$. We have that $\phi^{\frac{m}{2}} B$ induces a permutation σ of the eigenspaces of A, because for every i the subspace $W_i^{\phi^{\frac{m}{2}} B}$ is an eigenspace of A of eigenvalue $\xi\lambda_i^{-1}$. We may assume that $\sigma = (1, 2, \ldots, e_1)(e_1 + 1, e_1 + 1, \ldots, e_2) \cdots (e_{k-1}, \ldots, e_k)$ is the product of disjoint cycles. Let us look at $W_1 + \cdots + W_{e_1}$. We choose a basis $w_{1,1}, \ldots, w_{h,1}$ of W_1, so that $w_{i,2} = w_{i,1}^{\phi^{\frac{m}{2}} B}$ is a basis of W_2 and in general $w_{i,j} = w_{i,j-1}^{\phi^{\frac{m}{2}} B}$ is a basis of W_j. We do the same for the other cycles of σ and with respect to this basis B is a block diagonal matrix in which every block corresponds to a cycle of σ and is of the form $\begin{pmatrix} & I & & \\ & & \ddots & \\ B_i & & & I \end{pmatrix}$.

Assume that $M \in \mathrm{GL}(n, \bar{F})$ centralizes A. Then M is a block diagonal matrix and its restriction to $W_1 + \cdots + W_{e_1}$ is of the form $\begin{pmatrix} M_1 & & & \\ & M_2 & & \\ & & \ddots & \\ & & & M_{e_1} \end{pmatrix}$. We have that

$$M^{\phi^{\frac{m}{2}} B} = \begin{pmatrix} M_{e_1}^{\phi^{\frac{m}{2}} B_1} & & & \\ & M_1^{\phi^{\frac{m}{2}}} & & \\ & & \ddots & \\ & & & M_{e_1-1}^{\phi^{\frac{m}{2}}} \end{pmatrix}.$$

If $M\bar{F}^\times$ centralizes $\phi^{\frac{m}{2}} b$ in $\mathrm{PGL}(n, \bar{F})$ we have that $\lambda M^{\phi^{\frac{m}{2}} B} = M$ for some λ. So $M_{i+1} = \lambda M_i^{\phi^{\frac{m}{2}}}$ for $i \geq 1$ and also

$$M_1 = \lambda M_{e_1}^{\phi^{\frac{m}{2}} B_1} = \cdots = \lambda^{1+p^{\frac{m}{2}}+\cdots+p^{(e_1-1)\frac{m}{2}}} M_1^{\phi^{e_1 \frac{m}{2}} B_1}.$$

So, once λ is fixed, the choices for M_1 are at most $|\mathrm{GL}(h, p^{e_1 \frac{m}{2}})|$, by the Lang–Steinberg Theorem applied to $\mathrm{GL}(h, \bar{F})$, and then all the matrices M_i are determined.

Let $T = \frac{C_{\mathrm{GL}(n,\bar{F})}(A)\bar{F}^\times}{\bar{F}^\times} \cap C_{\mathrm{PSL}(n,\bar{F})}(\phi^{\frac{m}{2}} b)$.

We have that $|\mathrm{GL}(\frac{h}{e}, p^{e\frac{m}{2}})| \leq |\mathrm{GL}(h, p^{\frac{m}{2}})|$. If σ consists of at least two different cycles or if $\sigma = 1$ then $|T| \leq |\mathrm{GL}(n-1, q^{\frac{1}{2}})|$ and $|T|_2 \leq |\mathrm{GL}(n-1, q^{\frac{1}{2}})|^{\frac{1}{2}}$, while if σ is a cycle then $|T| \leq |\mathrm{GL}(\frac{n}{e}, p^{e\frac{m}{2}})| \leq |\mathrm{GL}(n-1, p^{\frac{m}{2}})|$ and $|T|_2 \leq |\mathrm{GL}(\frac{n}{e}, p^{e\frac{m}{2}})|_2 \leq |\mathrm{GL}(n-1, p^{\frac{m}{2}})|^{\frac{1}{2}}$ (all these inequalities follow by easy calculations).

Now we note that $|C_{\mathrm{PSL}(n,\bar{F})}(\langle \phi^{\frac{m}{2}} b, a\rangle) : T| \in \{1, r\}$, and if that index is r then A has precisely r different eigenvalues and all the eigenspaces have the same dimension $\frac{n}{r}$. Moreover, as r is an odd prime which divides $q-1$, we have that $r \leq q^{\frac{1}{2}} + 1$. In this case, the inequality $r|\mathrm{GL}(\frac{n}{e}, p^{e\frac{m}{2}})| \leq |\mathrm{GL}(n-1, p^{\frac{m}{2}})|$ proves that $|C| \leq |\mathrm{GL}(n-1, q^{\frac{1}{2}})|$, and $|C|_2 \leq |\mathrm{GL}(n-1, q^{\frac{1}{2}})|^{\frac{1}{2}}$, as claimed. □

Lemma 12. *Let $S = \mathrm{PSU}(n, q^2)$, where $q = p^m$ for some prime p, ϕ the Frobenius automorphism and $d = (n, q+1)$. Let α be an automorphism of S of the form $\alpha = \phi^{\frac{2m}{r}} a$, where $1 < r$ divides $2m$ and $a \in \mathrm{InnDiag}(S)$, and assume that $|\alpha^r|$ divides d. If $r \geq 3$ then $|C_S(\alpha)| \leq (d|S|)^{\frac{1}{3}}$. If $r = 2$ and $n \geq 5$ then $|C_S(\alpha)| \leq (d|S|)^{\frac{2}{3}}$ and $|C_S(\alpha)|_2 \leq (d|S|)^{\frac{2}{7}}$.*

Proof. Let $\bar{F}$ be the algebraic closure of the field F with q elements and let $G = \mathrm{SL}(n, \bar{F})$, $\bar{G} = \mathrm{PSL}(n, \bar{F})$. We want to study $C_{\bar{G}}(\phi^m \tau) \cap C_{\bar{G}}(\phi^{\frac{2m}{r}} a)$, where $[\phi^m \tau, a] = 1$.

Assume that r is divisible by an odd prime. Then replacing $\phi^{\frac{2m}{r}} a$ with a suitable power we may assume that $r = 2s+1$ is an odd prime, so that by the Lang–Steinberg theorem $\phi^m \tau (\phi^{\frac{2m}{r}} a)^{-s} = \phi^{\frac{m}{r}} \tau c$ is conjugate to $\phi^{\frac{m}{r}} \tau$ and its centralizer in $\bar{G}$ is isomorphic to $\mathrm{PGU}(n, q^{\frac{2}{r}})$, so it has order at most $|\mathrm{PGU}(n, q^{\frac{2}{3}})| < (d|S|)^{\frac{1}{3}}$.

Let now r be a power of 2; replacing $\phi^{\frac{2m}{r}} a$ with a suitable power we may assume that r is either 2 or 4 and that $|\alpha^r| = 2^s$ as an element of $\mathrm{Aut}(S)$, i.e. $(\phi^{\frac{2m}{r}} a)^r = \phi^{2m} z$ where $z \in \mathrm{InnDiag}(S)$ has order 2^s, a divisor of d.

Let $\phi^m \tau (\phi^{\frac{2m}{r}} a)^{-\frac{r}{2}} = \tau y$. Then $[y, \phi^{2m}] = 1$ and $(\tau y)^2 = z^{-1}$ has order 2^s. We have that $C_{\bar{G}}(\phi^m \tau) \cap C_{\bar{G}}(\phi^{\frac{2m}{r}} a) = C_{\bar{G}}(\phi^{\frac{2m}{r}} a) \cap C_{\bar{G}}(\tau y)$. By the Lang–Steinberg theorem there exists $x \in \bar{G}$ such that $(\phi^{\frac{2m}{r}} a)^x = \phi^{\frac{2m}{r}}$ so that conjugating by x we may assume that $a = 1$. As $C_{\bar{G}}(\phi^{\frac{2m}{r}}) = \mathrm{PGL}(n, q^{\frac{2}{r}})$, we have that $C_S(\alpha)$ is isomorphic to a subgroup of $C_{\mathrm{PGL}(n, q^{\frac{2}{r}})}(\tau y)$, where $y \in \mathrm{PGL}(n, q^{\frac{2}{r}})$ and $(\tau y)^2$ has order 2^s.

We now study the structure of $C_{\mathrm{PGL}(n, q^{\frac{2}{r}})}(\tau y)$, with the aim of bounding its order. If $(\tau y)^2 = 1$ (this is certainly the case if $p = 2$), then τy is a graph automorphism of $\mathrm{PGL}(n, q^{\frac{2}{r}})$, its centralizer is well known and its order satisfies the required inequalities. So we assume that q is odd and $2^s > 1$. Let Y be a preimage of y in $\mathrm{GL}(n, q^{\frac{2}{r}})$ and $B = (\tau Y)^2$. The minimum polynomial of B has simple irreducible factors; it divides $x^{2^s} - \mu$ and μ is either 1 or -1, since if λ is an eigenvalue of B then also λ^{-1} is one. As the elements of $C_{\mathrm{GL}(n, q^{\frac{2}{r}})}(\tau Y)$ are exactly the isometries of the bilinear form on the natural module V over the field with $q^{\frac{2}{r}}$ elements given by the matrix Y^{-1} with respect to a suitable basis, the structure of $C_{\mathrm{GL}(n, q^{\frac{2}{r}})}(\tau Y)$ can be studied with the methods of [16]. We note that the asymmetry σ associated to the given bilinear form

is represented by the matrix $Y^{-1}Y^{\top} = B^{-1}$ and that if A is any matrix representing an element of $C_{\mathrm{PGL}(n,q^{\frac{2}{r}})}(\tau y)$ then A centralizes B. If f is an irreducible factor of the minimum polynomial of B^{-1} let V_f be the f-primary component of the natural module V, and let n_f be its dimension. Let $f^* = x^{\deg f} f(\frac{1}{x})$. The dimensions of V_f and V_{f^*} are the same and $V_f = V_{f^*}$ iff f^* and f are associates. Set $\widetilde{V}_f = V_f$ if $V_f = V_{f^*}$ and $\widetilde{V}_f = V_f \oplus V_{f^*}$ otherwise. Then $V = \oplus_f \widetilde{V}_f$ is the direct sum of orthogonal B-invariant, non isomorphic subspaces. It follows that our isometry group is the direct product of the isometry groups of the factors; upon conjugation by an element of $\mathrm{GL}(n, q^{\frac{2}{r}})$ we may assume that B is in block-diagonal form, with blocks $\widetilde{B}_f$ according to the decomposition $V = \oplus_f \widetilde{V}_f$; then also Y has a similar form, with blocks $\widetilde{Y}_f$.

We now have a number of possibilities to discuss.

First, if f is self-paired of degree 1, then $\tau\widetilde{Y}_f$ induces a graph automorphism of order 2 on $\mathrm{GL}(n_f, q^{\frac{2}{r}})$. Second, if f is self-paired of degree > 1, then $C_{\mathrm{GL}(n_f,q^{\frac{2}{r}})}(\widetilde{B}_f)$ is isomorphic to a subgroup of $\mathrm{GL}(\frac{n_f}{2}, q^{\frac{4}{r}})$, on which $\tau\widetilde{Y}_f$ acts as an automorphism of order 2 that is not inner-diagonal. To see this, we note that $\widetilde{B}_f$ is diagonalizable in $\mathrm{GL}(n, \bar{F})$, so if λ is an eigenvalue of $\widetilde{B}_f$, then $I + \widetilde{B}_f$ is centralized by $\tau\widetilde{Y}_f$ if and only if $1 + \lambda^{-1} = (1 + \lambda)^{-1}$. It follows that $\tau\widetilde{Y}_f$ cannot centralize both $I + \widetilde{B}_f$ and $I - \widetilde{B}_f$. Finally, in the remaining cases f and f^* are not associate, n_f is even and $\tau\widetilde{Y}_f$ induces an automorphism of order 2 on $\mathrm{GL}(n_f, q^{\frac{2}{r}})$. Moreover, if $\widetilde{M}_f = \begin{pmatrix} M_1 & \\ & M_2 \end{pmatrix}$ is a matrix centralized by $\tau\widetilde{Y}_f$ it follows easily that $M_2 = M_1^{-\top}$ so that the centralizer of $\tau\widetilde{Y}_f$ is isomorphic to a subgroup of $\mathrm{GL}(\frac{n_f}{2}, q^{\frac{2}{r}})$.

The bounds on $|C_{\mathrm{PGL}(n,q^{\frac{2}{r}})}(\tau y)|$ and on the order of a Sylow 2-subgroup can be deduced from these observations and some easy calculations. □

3. The special linear groups

Throughout this section we will have $S = \mathrm{PSL}(n, q)$, where $q = p^m$ for some prime p. If $n \geq 3$ we have that $\mathrm{Out}(S) = \mathrm{OutDiag}(S)\langle \mathrm{Inn}(S)\phi, \mathrm{Inn}(S)\tau \rangle$, where ϕ is the Frobenius automorphism and τ is the automorphism induced on S by the "inverse-transpose" automorphism of $\mathrm{GL}(n, q)$: $(a_{ij})^{\tau} = (a_{ji})^{-1}$, while if $n = 2$ then $\mathrm{Out}(S) = \mathrm{OutDiag}(S)\langle \mathrm{Inn}(S)\phi \rangle$. Moreover, $\mathrm{OutDiag}(S)$ is cyclic of order $d = (n, q-1)$, $|\langle\phi\rangle| = m$, $|\langle\tau\rangle| = 2$ and $[\phi, \tau] = 1$.

We will need the following technical results:

Proposition 13. *Let $G = P_1 \times P_2 \times \cdots \times P_s$ be an irreducible nilpotent subgroup of the general linear group* $\mathrm{GL}(V, F)$*, where* $\dim_F(V) = n$*, $|F| = q$, $P_i \in \mathrm{Syl}_{p_i}(G)$*

and $p_i \mid q-1$. *Then* G *is a subgroup of the tensor product* $Q_1 \otimes Q_2 \otimes \cdots \otimes Q_s$ *where* $Q_i \in \mathrm{Syl}_{p_i}(\mathrm{GL}(p_i^{r_i}, F))$ *and* $\dim_F(V) = p_1^{r_1} \cdots p_s^{r_s}$.

Proof. By induction on s. If $s = 1$ we have that $G = P_1$ is contained in a Sylow p_1-subgroup Q_1 of $\mathrm{GL}(n, F)$. If n were not a power of p_1 then Q_1 would be reducible (*cfr.* [18], Theorem 25.2) and so would P_1, contradicting our hypotheses.

Let now $s > 1$, and write $G = H \times P$ where $H = P_1 \times \cdots \times P_{s-1}$ and $P = P_s$. Let V_1 be an irreducible FH-submodule of V. Then $V = V_1 \oplus V_2 \oplus \cdots \oplus V_t$, a direct sum of isomorphic FH-modules, is a homogeneous FH-module.

Let $T = \mathrm{End}_{FH}(V_1)$. By induction H is a subgroup of the tensor product $Q_1 \otimes Q_2 \otimes \cdots \otimes Q_{s-1}$ where $Q_i \in \mathrm{Syl}_{p_i}(\mathrm{GL}(p_i^{r_i}, F))$ and $\dim_F(V_1) = p_1^{r_1} \cdots p_{s-1}^{r_{s-1}}$. So if $u = [T : F]$ from the fact that $\dim_F(V_1) = u \dim_T(V_1)$ it follows that also u is a $\{p_1, \ldots, p_{s-1}\}$-number. We have that $M = C_{\mathrm{GL}_T(V)}(H)$ is isomorphic to $\mathrm{GL}(t, T)$, $T = \mathrm{End}_{FHM}(V)$ and V may be regarded as a T-vector space. Moreover $P \leq M$. The maximal $\{p_1, \ldots, p_{s-1}\}$-subgroup S of the multiplicative group $T^\times$ of the field T commutes with H and P; replacing G with $\langle G, S\rangle$, we may assume that $S \leq H$. As $[T : F]$ is a $\{p_1, \ldots, p_{s-1}\}$-number the F-algebra generated by S is T, and so $FH = TH$.

Let $A = \mathrm{Hom}_{FH}(V_1, V) = \mathrm{Hom}_{TH}(V_1, V)$; A is a T-space of dimension t, with a T-base $\alpha_1, \ldots, \alpha_t$ such that $\alpha_1 = 1$ and $V_1\alpha_i = V_i$ ([1], Proposition (3.11)). The map $\beta \mapsto \beta x$ ($\beta \in A$, $x \in M$) gives a faithful T-representation of M on A, and moreover $M \cong \mathrm{GL}_T(A)$. In particular M contains a Sylow p_s-subgroup Q of $\mathrm{GL}_T(A)$ such that $P \leq Q$. By replacing G with $\langle G, Q\rangle$, we may assume that $P = Q$.

Now V, considered as a $T(HM)$-module, is isomorphic to $V_1 \otimes_T A$; if $v_1, \ldots, v_r$ is a T-base of V_1, then $\{v_i\alpha_j\}$ is a T-base of V and the action of HM is given by $(v_i\alpha_j)(gx) = v_i g\alpha_j x$ (here $g \in H$, $x \in M$).

As $|T| = q^u$ and u is a $\{p_1, \ldots, p_{s-1}\}$-number, for every $k > 0$ the p_s-part of $q^{uk} - 1$ equals the p_s-part of $q^k - 1$, and so a Sylow p_s-subgroup of $\mathrm{GL}(t, F)$ is also a Sylow p_s-subgroup of $\mathrm{GL}(t, T)$. It follows that there exists a T-base $\beta_1, \ldots, \beta_t$ of A such that the elements of P are matrices with entries in F. Moreover the set $\{v_i\beta_j\}$ is a T-base of V. Once we fix an F-base $c_1, \ldots, c_u$ of T, the set $\{c_k v_i\}$ is an F-base of V_1. Moreover the set $\{c_k v_i \beta_j\}$ is linearly independent over F and has $urt = [T : F]\dim_T(V_1 \otimes_T A) = \dim_F(V)$ elements, so it is an F-base.

Finally, let $B = \sum F\beta_j$: we have that B is an F-space and an absolutely irreducible FP-module and it turns out that V is isomorphic to $V_1 \otimes_F B$ as an $F(H \times P)$-module. □

Lemma 14. *Let* F *be a field of order* q *and* $G \leq \mathrm{GL}(n, F)$ *be a nilpotent group such that the primes dividing* $|G|$ *divide also* $q-1$. *Then* $|G| \leq 2^{\frac{5}{2}n-1}$ *if* $q = 3$, *otherwise* $|G| \leq (q-1)^n 2^{n-1}$ *unless* $n = 2$, q *is a Mersenne prime and* $|G| = 2(q^2-1)$.

Proof. If $q = 3$ then G is contained in a Sylow 2-subgroup of $\mathrm{GL}(n,3)$ which has order at most $2^{\frac{5n}{2}-1}$. So we may assume that $q \neq 3$.

G is completely reducible by Maschke's theorem, so let us first assume that G is irreducible. By Proposition 13 $n = p_1^{r_1} \cdots p_s^{r_s}$ where each p_i divides $q-1$ and G is isomorphic to a subgroup of the direct product $Q_1 \times \cdots \times Q_s$, where Q_i is a Sylow p_i-subgroup of $\mathrm{GL}(p_i^{r_i}, q)$ (note that it could be $r_i = 0$ for some i).

If $q \equiv 1 \pmod 4$ or if $p_i \neq 2$ we have:

$$|Q_i| \leq |q-1|_{p_i}^{p_i^{r_i}} \, p_i^{p_i^{r_i}(\frac{1}{p_i}+\cdots+\frac{1}{p_i^{r_i}})} = |q-1|_{p_i}^{p_i^{r_i}} \, p_i^{\frac{p_i^{r_i}-1}{p_i-1}} \leq |q-1|_{p_i}^{p_i^{r_i}} \, 2^{p_i^{r_i}-1}.$$

If $p_i = 2$ and $q \equiv -1 \pmod 4$, then we have:

$$|Q_i| = (2|q+1|_2)^{2^{r_i-1}} 2^{2^{r_i}-1}.$$

Now assume that $n = p_1^{r_1}$ is a prime power. If $p_1 \neq 2$ or $q \equiv 1 \pmod 4$ then

$$|G| \leq |q-1|_{p_1}^{n} |q-1|_{p_1'} 2^{n-1} = |q-1|_{p_1}^{n-1} (q-1) 2^{n-1}.$$

If $p_1 = 2, q \equiv -1 \pmod 4, n \geq 2$ then

$$|G| \leq |q+1|_2 |q^2-1|_2^{\frac{n}{2}-1} 2^{n-1}(q-1),$$

so that $|G| \leq (q^2-1)^{\frac{n}{2}} 2^{n-1}$. But in fact if q is not a Mersenne prime or if $n > 2$ we have $|G| \leq (q-1)^n 2^{n-1}$. This is clear if q is not a Mersenne prime. If q is a Mersenne prime, it follows from the inequality $(2(q+1))^{\frac{n}{2}} \leq 2(q-1)^{n-1}$ that holds for $q \geq 7, n \geq 4$.

Now assume that n is not a prime power. If n is odd or $q \equiv 1 \pmod 4$ then

$$|G| \leq (q-1)^{\max(p_i^{r_i})} 2^{\sum(p_i^{r_i}-1)} \leq (q-1)^{n-1} 2^{n-2}.$$

If n is even and $q \equiv -1 \pmod 4$ ($p_1 = 2$) then (set $m = \max(2^{r_1-1}, p_2^{r_2}, \ldots, p_s^{r_s})$)

$$|G| \leq |q^2-1|_2^{2^{r_1-1}} 2^{2^{r_1}-1} \prod_{p_i>2} (|q-1|_{p_i}^{p_i^{r_i}} 2^{p_i^{r_i}-1})$$

$$\leq (q-1)^m |q+1|_2^{2^{r_1-1}} 2^{\sum(p_i^{r_i}-1)} \leq (q-1)^{\frac{n}{2}} |q+1|_2^{\frac{n}{6}} 2^{n-2} \leq (q-1)^{n-1} 2^{n-2}.$$

In all these cases $|G| \leq (q-1)^n 2^{n-1}$.

Now assume that V is not irreducible, so that $V = V_1 \oplus \cdots \oplus V_t$ where $t > 1$, $\dim V_j = n_j$ and the V_j's are irreducible G-spaces. We have that $G \leq \prod G_j$ where G_j is the restriction of G to V_j and $|G_j| \leq (q-1)^{n_j} 2^{n_j-1}$, unless $n_j = 2$, q is a Mersenne prime and $|G_j| = 2(q^2-1)$. If q is not a Mersenne prime or if $n_j \neq 2$ for all j then $|G| \leq (q-1)^n 2^{n-1}$.

Now assume that q is a Mersenne prime and that the number of 2-dimensional subspaces occurring in the decomposition of V in irreducible subspaces is $h \geq 1$, so that $|G| \leq 2^h(q^2-1)^h \prod_{n_j \neq 2}(q-1)^{n_j} 2^{n_j-1}$. If $h = 1$ then $\prod_{n_j \neq 2}(q-1)^{n_j} 2^{n_j-1} \leq (q-1)^{n-2}2^{n-3}$ so that $|G| \leq (q-1)^{n-2}2^{n-3}2(q^2-1) \leq (q-1)^n 2^{n-1}$. If $h \geq 2$ then $2^h(q^2-1)^h \leq (q-1)^{2h}2^{2h-1}$ and we get the same conclusion. □

Lemma 15. *If F is a field of order q and $G \leq \mathrm{GL}(n, F)$ is maximal with respect to the conditions that G is nilpotent and the primes dividing $|G|$ divide also $q-1$, then $|(GF^\times/F^\times) \cap \mathrm{PSL}(n,q)| = \frac{|G|}{d(q-1)}$.*

Proof. Maximality of G implies that G contains all the scalar matrices, so it remains to prove that if r is a prime, $r \,|\, q-1$, then G contains an element x_r such that $\det(x_r)$ generates the Sylow r-subgroup $F_r^\times$ of $F^\times$. G is completely reducible, and it is clearly enough if we prove the lemma when G is irreducible, so that Proposition 13 applies. Let $F_r^\times = \langle \lambda \rangle$ and assume that $r \nmid n$. Then $x_r = \lambda I \in G$ by maximality of G and has the required property. Otherwise, in the notation of Proposition 13, by maximality we have that $G = Q_1 \otimes Q_2 \otimes \cdots \otimes Q_s$, $r = p_j$ for some j and every Sylow r-subgroup of $\mathrm{GL}(p_j^{r_j}, q)$ contains an element y_r such that $\det(y_r) = \lambda_r$, so that $x_r = I_1 \otimes \cdots \otimes y_r \otimes \cdots \otimes I_s \in G$ has the desired property (here I_i is the identity matrix of $\mathrm{GL}(p_i^{r_i}, q)$). □

Lemma 16. *There are at most $\lambda(n)$ $\mathrm{PSL}(n,q)$-conjugacy classes of subgroups $\bar{G} \leq \mathrm{PGL}(n, F)$ which are maximal with respect to the conditions that $\bar{G}$ is nilpotent and the primes dividing $|\bar{G}|$ divide also $q-1$, where $\lambda(n)$ is the number of partitions of n.*

Proof. The preimage G of $\bar{G}$ in $\mathrm{GL}(n,q)$ is completely reducible by Maschke's theorem. Once we know the dimensions m_i of the G-irreducible subspaces V_i such that $V = V_1 \oplus \cdots \oplus V_t$ (there are at most $\lambda(n)$ possibilities), by Proposition 13 G is completely determined up to $\mathrm{GL}(n,q)$-conjugacy. By the proof of Lemma 15 we have that if r is a prime, $r \,|\, q-1$, then G contains an element x_r such that $\det(x_r)$ generates the Sylow r-subgroup $F_r^\times$ of $F^\times$, so G is actually unique up to $\mathrm{SL}(n,q)$-conjugacy. The result then follows easily. □

Lemma 17. *We have that $|\mathrm{PSL}(n,q)| \geq q^{\frac{n(2n-1)}{2}}$, with the following exceptions:*

(1) *$n = 2$. If q is even then $d = 1$ and $|S| = q(q^2-1) \geq \frac{1}{2}q^3$. If q is odd then $d = 2$ and $|S| = \frac{1}{2}q(q^2-1) \geq \frac{1}{3}q^3$;*

(2) *$n = 3$, $q = 2$: $d = 1$, $|S| \geq \frac{1}{2}q^{\frac{n(2n-1)}{2}}$;*

(3) *$n = 3$, $q = 4$: $d = 3$, $|S| \geq \frac{1}{2}q^{\frac{n(2n-1)}{2}}$;*

(4) *$n = 3$, $q = 7$: $d = 3$, $|S| \geq \frac{1}{2}q^{\frac{n(2n-1)}{2}}$.*

Proof. By direct calculation. □

3.1. Proof of the theorem when $S = \mathrm{PSL}(n,q)$. We have that $\bar{X} = \frac{X}{S} \leq \mathrm{Out}(S) \times (\mathrm{Out}(S) \wr \mathrm{Sym}(k-1)) = \mathrm{Out}(S)^k \rtimes \mathrm{Sym}(k-1)$, where $\mathrm{Sym}(k-1)$ acts trivially on the first component of $B = \mathrm{Out}(S)^k$. We shall prove that the number of S-orbits of homomorphisms $\bar{X} \to \mathrm{Aut}(S)$ as in Proposition 1 is smaller than $|S|^k$.

Let $D = \mathrm{OutDiag}(S)^k$, $\Phi = \langle \mathrm{Inn}(S)\phi \rangle^k$, $\Gamma = \langle \mathrm{Inn}(S)\tau \rangle^k$.

Case 1: $\bar{X} \cap \Phi D = 1$.

In this case $\bar{X} \hookrightarrow C_2 \wr \mathrm{Sym}(k)$ is k-generated by Lemma 4, so we conclude by Lemma 3.

Case 2: $\bar{X} \cap \Phi D \neq 1$, $\bar{X} \cap D = 1$.

In this case $\bar{X} \cap B$ is isomorphic to a subgroup of $B/D \cong \Phi \times \Gamma$, which is abelian, and $\bar{X}$ is isomorphic to a subgroup of $(\langle \phi \rangle \times \langle \tau \rangle) \wr \mathrm{Sym}(k)$.

We recall that $\bar{X} \leq (\mathrm{Out}(S_1) \times \cdots \times \mathrm{Out}(S_k)) \rtimes \mathrm{Sym}(k-1)$, so that every element of $\bar{X} \cap \Phi D$ is a k-tuple of elements of $\mathrm{Out}(S)$. Let $\mathrm{Inn}(S)\phi^t a \in \mathrm{Out}(S)$ such that $t < m$, $a \in \mathrm{InnDiag}(S)$ and $\mathrm{Inn}(S)\phi^t a$ is of maximal order among the entries of this form of the elements of $\bar{X} \cap \Phi D$. As H acts transitively on the components of N, we may assume that $\mathrm{Inn}(S)\phi^t a$ is the first entry of some $z_1 \in \bar{X} \cap \Phi D$. If $|\mathrm{Inn}(S)\phi^t a| > |\mathrm{Inn}(S)\phi^t|$ then $1 \neq z_1^{|\mathrm{Inn}(S)\phi^t|} \in \bar{X} \cap D$, a contradiction. It follows that $|z_1| = |\phi^t|$. By Proposition 1 we have that $\varphi(z_1) = \phi^t a s$ for some $s \in S$ (here we identify S with $\mathrm{Inn}(S)$) so $|\varphi(z_1)| = |\phi^t|$ and by Lemma 9 $|C_S(\varphi(z_1))| \leq (d|S|)^{\frac{1}{|\phi^t|}}$.

There exist elements $z_2, \ldots, z_{2k} \in \bar{X} \cap B$ such that the set $\mathcal{Z} = \{z_1, \ldots, z_{2k}\}$ generates $\bar{X} \cap B$, then by Lemma 4 we need to add to $\mathcal{Z}$ at most $\frac{k}{2}$ more elements to obtain a generating set $\mathcal{X}$ of $\bar{X}$. Let us now count the choices for $\varphi(z_1)$, up to S-conjugacy. If $\phi^t a s_1, \phi^t a s_2$ are two such choices, by the argument above $|\phi^t a s_1| = |\phi^t a s_2| = |\phi^t|$, so by [14, Proposition 1.1] they are $\mathrm{PGL}(n,q)$-conjugate, and as we are counting S-orbits the choices are at most $|\mathrm{PGL}(n,q) : S| = d$. As $[z_j, z_1] = 1$ for every $j = 2, \ldots, 2k$ by Lemma 2 with $T = \langle z_1 \rangle$ we have that the choices for each $\varphi(z_j)$ are at most $|C_S(\varphi(z_1))| \leq (d|S|)^{\frac{1}{|\phi^t|}}$. Again, all the remaining elements $x \in \mathcal{X}$ normalize $\bar{X} \cap B$ so by Lemma 9 with $T = \bar{X} \cap B$ the choices for $\varphi(x)$ are at most $|C_S(\varphi(\bar{X} \cap B))| \leq |C_S(\varphi(z_1))| \leq (d|S|)^{\frac{1}{|\phi^t|}}$. So the number of conjugacy classes of complements of N in H is at most $d(d|S|)^{\frac{1}{|\phi^t|}(\frac{5}{2}k-1)} < |S|^k = |N|$ if $|\phi^t| \geq 4$.

Assume now that $|\phi^t| = 3$. Then $\bar{X} \cap B$ is k-generated and as z_1 is fixed we may assume that $|\mathcal{Z}| = k+1$ and arguing as above we obtain that the number of conjugacy classes of complements of N in H is at most $d(d|S|)^{\frac{1}{3}(\frac{3}{2}k)} < |S|^{\frac{1}{2}+\frac{k}{4}+\frac{k}{2}} \leq |S|^k = |N|$, for $k \geq 2$.

Assume now that $|\phi^t| = 2$. Then $\bar{X} \cap B$ is a 2-group, so that $\varphi(\mathcal{Z})$ will be contained in a Sylow 2-subgroup P of $\mathrm{Inn}(S)\iota(\bar{X} \cap B)$, which is unique up to S-conjugacy. The choices for $\varphi(z_1)$ are at most $|P \cap S| < |S|^{\frac{1}{2}}$. We now use Lemma 2 and we have that the choices for the remaining $\varphi(z_i)$'s are at most $|C_S(\phi^t) \cap P|$.

We may also assume that $n > 2$, as otherwise $\bar{X} \cap B$ is elementary abelian of rank k and we argue as in case 1. So $d \leq |S|^{\frac{1}{7}}$ and $|C_S(\phi^t) \cap P| = |C_S(\phi^t)|_2 \leq |S|^{\frac{1}{4}}$; it follows that $|P \cap S||C_S(\phi^t) \cap P|^{2k-1}(d|S|)^{\frac{1}{2}\frac{k}{2}} \leq |S|^{\frac{1}{4}+\frac{k}{2}+\frac{k}{28}+\frac{k}{4}} < |S|^k$ for $k \geq 2$ and this concludes the proof for this case.

Case 3: $\bar{X} \cap B = \bar{X} \cap D \neq 1$.

If $q = 3$ or if $n = 2$ then $\bar{X} \hookrightarrow C_2 \wr \mathrm{Sym}(k)$ is k-generated and we conclude as in case 1.

Let $\mathcal{Z}$ be a set of k generators of $\bar{X} \cap D$. As $\bar{X} \cap D$ is abelian, $\varphi(\mathcal{Z})$ is contained in a maximal nilpotent subgroup $\bar{G}$ of $\mathrm{PGL}(n,q)$ (here we identify $\mathrm{PGL}(n,q)$ with $\iota(\mathrm{PGL}(n,q))$). As the primes dividing $|\bar{X} \cap D|$ are also divisors of $q-1$ by Lemma 16 there are at most $\lambda(n)$ choices for $\bar{G}$, up to $\mathrm{PSL}(n,q)$-conjugacy. The preimage G of $\bar{G}$ in $\mathrm{GL}(n,q)$ is a nilpotent subgroup of $\mathrm{GL}(n,q)$ satisfying the hypotheses of Lemma 15 so by Lemmas 14 and 15 it follows that $|\bar{G} \cap S| \leq (q-1)^{n-1}2^{n-1}$.

Thus there are at most $\lambda(n)(q-1)^{k(n-1)}2^{k(n-1)}$ choices for $\varphi(\mathcal{Z})$.

Moreover, as $\varphi(\mathcal{Z})$ contains a non trivial diagonal automorphism of S and $n \geq 3$, by Lemma 10 we have that $|C_S(\varphi(\mathcal{Z}))| \leq \frac{q-1}{(q^n-1)q^{n-1}}|S|$.

By Lemma 4 we need to add to $\mathcal{Z}$ at most $\frac{k}{2}$ elements $x_1, \ldots, x_{\lfloor \frac{k}{2} \rfloor}$ to obtain a generating set for $\bar{X}$ and by Lemma 2 with $T = \bar{X} \cap B$ the choices for each $\varphi(x_i)$ are at most $|C_S(\varphi(\mathcal{Z}))| \leq \frac{q-1}{(q^n-1)q^{n-1}}|S|$.

Therefore the number of conjugacy classes of complements of N in H is at most $\lambda(n)((q-1)^{n-1}2^{n-1})^k \left(\frac{q-1}{(q^n-1)q^{n-1}}|S|\right)^{\frac{k}{2}} < |S|^k$, as $\lambda(n) \leq 2^{n-1}$.

Case 4: $\bar{X} \cap \Phi D = \bar{X} \cap D \neq 1$.

The abelian group $\bar{X} \cap D$ has exponent dividing d and is generated by a set $\mathcal{Z}$ of order at most k; as $\bar{X}/\bar{X} \cap D = \bar{X}/\bar{X} \cap \Phi D \hookrightarrow C_2 \wr \mathrm{Sym}(k)$ is k-generated, we may assume that a generating set for $\bar{X}$ is of the form $\mathcal{Z} \cup \{x_1, \ldots, x_k\}$.

Assume that $\bar{X} \cap D$ is an r-group for some prime r. Then $\varphi(\mathcal{Z})$ will be contained in a Sylow r-subgroup P of $\mathrm{Inn}(S)\iota(\bar{X} \cap D)$, which is unique up to $\mathrm{Inn}(S)$-conjugacy. By Lemma 2 ii) the choices for $\varphi(\mathcal{Z})$ are at most $|P \cap S|^k \leq \left(\frac{1}{d}(q-1)^{n-1}2^{n-1}\right)^k$ if $q \neq 3$ and $n \neq 2$ and at most $2^{\left(\frac{5}{2}n-3\right)k}$ if $q = 3$ (see Lemmas 14 and 15), while if $n = 2$ we have $|P \cap S|^k \leq (q+1)^k$.

Assume now that there are at least two different primes dividing $|\bar{X} \cap D|$. Then $d \geq 6$, $n \geq 6$, $q \geq 7$. We have that $\varphi(\mathcal{Z})$ is contained in a maximal nilpotent subgroup $\bar{G}$ of $\mathrm{PGL}(n,q)$ and by Lemma 16 there are at most $\lambda(n)$ choices for $\bar{G}$, up to $\mathrm{PSL}(n,q)$-conjugacy. Also, by Lemmas 14 and 15 it follows that $|\bar{G} \cap S| \leq (q-1)^{n-1}2^{n-1}$.

Again, by Lemma 2 with $T = \bar{X} \cap B$ and by Lemma 10 the choices for each $\varphi(x_i)$ are at most $|C_S(\varphi(\mathcal{Z}))| \leq \frac{q-1}{(q^n-1)q^{n-1}}|S|$ if $n \geq 3$ and at most $q+1$ if $n = 2$.

In all these cases an easy calculation shows that the number of conjugacy classes of complements of N in H is smaller than $|S|^k$, as required.

Case 5: $\bar{X} \cap \Phi D > \bar{X} \cap D \neq 1$.

Let $\mathcal{Z}$ be a generating set of $\bar{X} \cap D$ of order at most k; we may also assume that $1 \neq \iota(z_1) \in \mathrm{InnDiag}(S)$ for some $z_1 \in \mathcal{Z}$.

As before, we recall that $X/S \leq (\mathrm{Out}(S_1) \times \cdots \times \mathrm{Out}(S_k)) \rtimes \mathrm{Sym}(k-1)$, so that every element of $\bar{X} \cap \Phi D$ is a k-tuple of elements of $\mathrm{Out}(S)$ of the form $S\phi^s x$, with $x \in \mathrm{InnDiag}(S)$. Let $\mathrm{Inn}(S)\phi^t a$, with $a \in \mathrm{InnDiag}(S)$, be an entry of an element of $\bar{X} \cap \Phi D$ such that $|\phi^t|$ is maximal. As H acts transitively on the components of N, we may assume that $\mathrm{Inn}(S)\phi^t a$ is precisely the first entry of some $y_1 \in \bar{X} \cap \Phi D$.

There are suitable elements $y_2, \ldots, y_k \in \bar{X}$ such that the set $\mathcal{Y} = \{y_1, \ldots, y_k\}$ generates $\bar{X} \cap \Phi D$ modulo $\bar{X} \cap D$, and then as $\bar{X}/\bar{X} \cap \Phi D \hookrightarrow C_2 \times (C_2 \wr \mathrm{Sym}(k-1))$ is k-generated, a generating set of $\bar{X}$ will be of the form $\mathcal{X} = \mathcal{Z} \cup \mathcal{Y} \cup \{x_1, \ldots . x_k\}$, where x_1 generates $(\bar{X}/\bar{X} \cap \Phi D) \cap C_2$ (*i.e.* the intersection with the first component of the direct product).

Assume that $|\phi^t| \geq 4$. Given $\varphi(\bar{X} \cap D)$, by Lemma 2 with $T = \bar{X} \cap B$ and by Lemma 10 the choices for $\varphi(y_1)$ are at most $|C_S(\varphi(\mathcal{Z}))| \leq \frac{q-1}{(q^n-1)q^{n-1}}|S|$. Then again by Lemma 2 the choices for the images of the remaining elements of $\mathcal{X}$ are at most $|C_S(\varphi(y_1))|$; as $\varphi(y_1) = \phi^t a x$ for some $x \in S$, by Lemma 9 $|C_S(\varphi(y_1))| \leq (d|S|)^{\frac{1}{4}}$.

By Lemma 14, Lemma 15 and Lemma 16 we have that the number of conjugacy classes of complements of N in H is at most

$$\big(\lambda(n)\big)^{\varepsilon} \left(\frac{(q-1)^{n-1}2^{n-1}}{d}\right)^k \frac{q-1}{(q^n-1)q^{n-1}}|S|(d|S|)^{\frac{1}{4}(2k-1)}. \qquad (\star)$$

Here $\varepsilon = 1$ if there are at least two different primes dividing $|\bar{X} \cap D|$ and $\varepsilon = 0$ if $\bar{X} \cap D$ is an r-group for some prime r. The expression in $(\star)$ is strictly less than $|S|^k$. This is easily checked if $n = 2$. If $n > 2$ to reach the conclusion we use the inequality $q^{\frac{n(2n-1)}{2}} \leq |S|$ from Lemma 17 and, if $\varepsilon = 1$, the information that $d \geq 6$, $n \geq 6$, $q \geq 2^4$, $\lambda(n) \leq 2^{n-1}$.

If $|\phi^t| = 3$ then by Lemma 6 $\bar{X}/\bar{X} \cap D \hookrightarrow C_6 \wr \mathrm{Sym}(k)$ is k-generated and we argue as in case 4.

So from now on we will assume that $|\phi^t| = 2$ and that $\bar{X} \cap B > \bar{X} \cap \Phi D$, as otherwise $\bar{X}/\bar{X} \cap D \hookrightarrow C_2 \wr \mathrm{Sym}(k)$ and we could argue as in case 4. In particular $n > 2$.

First we assume that $\bar{X} \cap D$ is not a 2-group. As $\bar{X} \cap B$ is supersolvable, $\bar{X} \cap D$ contains a cyclic subgroup $\langle a_1 \rangle$ of order an odd prime r which is normal in $\bar{X} \cap B$, and we may also assume that $\iota(a_1) \notin \mathrm{Inn}(S)$ and that $a_1 \in \langle z_1 \rangle$, where $z_1 \in \mathcal{Z}$. Also, $\bar{X} \cap B = (\bar{X} \cap D)L$, where L is a Sylow 2-subgroup of $\bar{X} \cap B$, and we may also assume that $\mathcal{Y} \cup \{x_1\} \subseteq L$ and that $\iota(y_1) \in \phi^{\frac{m}{2}}\,\mathrm{InnDiag}(S)$, where $y_1 \in \mathcal{Y}$. By Lemmas 14,

15 and 16 the choices for $\varphi(\bar{X} \cap B)$ are at most $\big(\lambda(n)\big)^{\varepsilon}\big((q-1)^{n-1}2^{n-1}/d\big)^k$, where ε is as in $(\star)$.

Again, we have that $\varphi(L) \leq P$, where P is a Sylow 2-subgroup of $\iota(L)\,\mathrm{Inn}(S)$. The choices for P are at most $|\iota(L)\,\mathrm{Inn}(S)/P| = |S|/|S \cap P|$ and the choices for $\varphi(y_1)$ are at most $|P \cap C_S(\varphi(a_1))| \leq |S \cap P|$. Now we can apply Lemma 11, and we note that $|\,\mathrm{GL}(n-1, q^{\frac{1}{2}})| < \frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}}$. Moreover, by Lemmas 2 and 11 the choices for $\varphi(\{y_2, \ldots, y_k, x_1\})$ are at most $\left(\frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}}\right)^{\frac{1}{2}k}$ and the choices for the images of the remaining generators are at most $\left(\frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}}\right)^{k-1}$. First assume that $k \geq 4$ and $q \neq 4$, so that $2 \leq q^{\frac{1}{4}}$ – the missing cases will be dealt with using *ad hoc* arguments.

We obtain that the number of conjugacy classes of complements of N in H is at most

$$\big(\lambda(n)\big)^{\varepsilon}\big((q-1)^{n-1}2^{n-1}\big)^k |S| \left(\frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}}\right)^{\frac{3}{2}k-1}.$$

If $\bar{X} \cap D$ is an r-group we have that

$$\begin{aligned}\big((q-1)^{n-1}2^{n-1}\big)^k |S| \left(\frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}}\right)^{\frac{3}{2}k-1} &\leq q^{\frac{5}{4}k(n-1)} |S|^{\frac{3}{4}k+\frac{1}{2}} \frac{(q-1)^{\frac{3}{4}k-\frac{1}{2}} q^{n-1}}{q^{\frac{3}{2}k(n-1)}} \\ &\leq |S|^{\frac{3}{4}k+\frac{1}{2}} (q-1)^{\frac{3}{4}k} < |S|^{\frac{7}{8}k+\frac{1}{2}} < |S|^k,\end{aligned}$$

as $(q-1)^{\frac{3}{4}} < |S|^{\frac{1}{8}}$ for $n \geq 3$.

If there are at least two different primes dividing $|\bar{X} \cap D|$ the result follows because $d \geq 6, n \geq 6, \lambda(n) \leq 2^{n-1} \leq q^{\frac{1}{4}(n-1)} < |S|^{\frac{1}{24}}$ and $(q-1)^{\frac{3}{4}} < |S|^{\frac{1}{40}}$.

Here are the arguments for the exceptions:

If $k = 2$ then $\bar{X} \leq B$.

In case $\bar{X} \cap D$ is an r-group we have

$$(q-1)^{2(n-1)} 4^{n-1} |S| \left(\frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}}\right)^{\frac{3}{2}} < |S|^{\frac{7}{4}} (q-1)^{n-1} d^{\frac{3}{4}} < |S|^2,$$

as $d^{\frac{3}{4}}(q-1)^{n-1} < |S|^{\frac{1}{4}}$ for $n \geq 4$, while if $n = 3$ then we need the sharper bound $(q-1)^2$ for the order of a Sylow 3-subgroup of S.

If $k = 2$ and there are at least two different primes dividing $|\bar{X} \cap D|$ the result follows because $2^{n-1} d^{\frac{3}{4}} (q-1)^{n-1} < |S|^{\frac{1}{4}}$ for $n \geq 6$.

If $k = 3$ we assume that L is a Sylow 2-subgroup of $\bar{X}$ and that $x_1 \in L$, so the number of choices for $\varphi(\bar{X})$ is at most that of the case $k = 2$ multiplied by $(q-1)^{n-1} 2^{n-1} \frac{(d|S|)^{\frac{1}{2}}}{q^{n-1}} < (q-1)^{\frac{1}{4}(n-1)+\frac{1}{2}} |S|^{\frac{1}{2}} < |S|$.

If $q = 4$ then $3 < |S|^{\frac{1}{9}}$ and the choices for each generator of $\varphi(\bar{X} \cap B)$ are at most the order of a Sylow 3-subgroup P of $\mathrm{PSL}(n,4)$, which is at most $3^{\frac{3}{2}(n-1)}$, and the result follows in the same way (for $k = 2$ it is also necessary to take into account that $|P| = 9$ when $n = 3$).)

Now assume that $\bar{X} \cap D$ is a 2-group. Then $\bar{X} \cap B$ is a 2-group so that $\varphi(\bar{X} \cap B) \leq P$, where P is a Sylow 2-subgroup of $\iota(\bar{X} \cap B)\,\mathrm{Inn}(S)$, which is unique up to $\mathrm{Inn}(S)$-conjugacy. Moreover, as $\bar{X}/\bar{X} \cap \Phi D \hookrightarrow C_2 \times (C_2 \wr \mathrm{Sym}(k))$, we may assume that $x_1, \ldots, x_{\lceil \frac{k}{2} \rceil} \in \bar{X} \cap B$ (here $\lceil \frac{k}{2} \rceil$ denotes the least integer greater or equal to $\frac{k}{2}$). Then the choices for $\varphi(\mathcal{Z} \cup \{y_1\})$ are at most $|P \cap S|^{k+1} \leq \left(\frac{(q-1)^{n-1}2^{n-1}}{d}\right)^{k+1}$. Then by Lemma 2 for $i = 2, \ldots, k$ the choices for $\varphi(y_i)$ are at most $|P \cap C_S(\varphi(y_1))| \leq |\mathrm{GL}(n, q^{\frac{1}{2}})|_2 \leq (q^{\frac{1}{2}} - 1)^n 2^{n-1}$, and again by Lemma 2 with $T = \bar{X} \cap \Phi D$ for each of the remaining $\left\lceil \frac{k}{2} \right\rceil + 1$ generators the choices are at most $(d|S|)^{\frac{1}{2}}$ (see also Lemma 9). So the number of conjugacy classes

$$\begin{aligned}\left(\frac{(q-1)^{n-1}2^{n-1}}{d}\right)^{k+1} & \left((q^{\frac{1}{2}} - 1)^n 2^{n-1}\right)^{\frac{3}{2}k-1} (d|S|)^{\frac{1}{2}\frac{k}{2}} \\ &\leq \left((q-1)^{\frac{7}{4}n} 2^{\frac{5}{2}(n-1)}\right)^{k+1} |S|^{\frac{k}{4}} \\ &\leq (q-1)^{\frac{31}{12}n(k+1)} |S|^{\frac{k}{4}} \\ &\leq |S|^{\frac{1}{2}(k+1)+\frac{k}{4}} < |S|^k\end{aligned}$$

for $k \geq 2$.

4. The unitary groups

Throughout this section we will have $S = \mathrm{PSU}(n, q^2)$, where $q = p^m$ for some prime p and $n \geq 3$ ($n = 2$ is covered by the previous section). Then $\mathrm{Out}(S) = \mathrm{OutDiag}(S)\langle \mathrm{Inn}(S)\phi \rangle$, where ϕ is the Frobenius automorphism. Furthermore, $\mathrm{OutDiag}(S)$ is cyclic of order $d = (n, q+1)$ and $|\langle \phi \rangle| = 2m$. As usual, we have that $\bar{X} = \frac{X}{S} \leq \mathrm{Out}(S)^k \rtimes \mathrm{Sym}(k-1)$, where $\mathrm{Sym}(k-1)$ acts trivially on the first component of $B = \mathrm{Out}(S)^k$. Let $D = \mathrm{OutDiag}(S)^k$ and $\Phi = \langle \mathrm{Inn}(S)\phi \rangle^k$.

To prove our theorem for unitary groups we imitate as closely as possible the argument of the previous section.

If $\bar{X} \cap B = 1$, then $\bar{X}$ embeds in $\mathrm{Sym}(k-1)$, it is $\frac{k}{2}$-generated and the conclusion follows from Lemma 3.

If $\bar{X} \cap D = 1 \neq \bar{X} \cap B$, then $\bar{X}$ is isomorphic to a subgroup of $\langle \phi \rangle \wr \mathrm{Sym}(k)$. If the exponent of $\bar{X} \cap B$ is 2, then $\bar{X}$ is k-generated and again Lemma 3 applies. So we can assume that the exponent of $\bar{X} \cap B$ is at least 3. We choose – as in case 2

of the proof for PSL – an element $z_1 \in \bar{X} \cap B$ with the property that the order of its first coordinate is maximum among the orders of coordinates of elements of $\bar{X} \cap B$. We then choose $z_2, \ldots, z_k$ so that $\langle z_1, z_2, \ldots, z_k \rangle = \bar{X} \cap B$ and $w_1, \ldots, w_{\frac{k}{2}}$ such that $w_1(\bar{X} \cap B), \ldots, w_{\frac{k}{2}}(\bar{X} \cap B)$ generate $\bar{X}/(\bar{X} \cap B)$. A homomorphism φ as in Proposition 1 is determined by the images of z_1 (certainly less than $|S|$ possible choices), of $z_2, \ldots, z_k$ which by Lemma 2 are determined modulo $C_S(\varphi(z_1))$, and of $w_1, \ldots, w_{\frac{k}{2}}$ that are also determined modulo $C_S(\varphi(z_1))$. By Lemma 12 $|C_S(\varphi(z_1))| \leq (d|S|)^{\frac{1}{3}}$. It follows that we have less than $|S|(d|S|)^{\frac{1}{3}(k-1+\frac{k}{2})} < |S|^k$ possibilities for φ, up to S-conjugation.

So assume that $\bar{X} \cap D \neq 1$. We want to estimate the number of S-classes of homomorphisms φ as described in Proposition 1; we first discuss their restriction to $\bar{X} \cap D$ that is abelian of exponent dividing d and generated by some set $\mathcal{Y}$ of at most k elements. If the order of $\bar{X} \cap D$ is a prime power, then $\varphi(\bar{X} \cap D)$ will be contained in a Sylow subgroup R of $\mathrm{Aut}(S)$ and the image of any $y \in \mathcal{Y}$ is determined modulo $R \cap S$: at most $|R \cap S|^k$ possibilities. Lemma 8 gives the bound $|R \cap S| < |S|^{\frac{1}{2}}$, and better estimates are available for some specific cases that we need consider. In the general case $\varphi(\bar{X} \cap D)$ will be contained in a nilpotent subgroup $\bar{N}$ of $\mathrm{PGU}(n, q^2)$ of order coprime to p. From [19, Lemma 2.4] it follows easily that $\bar{N} \leq N_{\mathrm{PGU}(n,q^2)}(\bar{T})$ for some maximal torus $\bar{T}$ of $\mathrm{PGU}(n, q^2)$. The number of S-conjugacy classes of maximal tori of $\mathrm{PGU}(n, q^2)$ is $\lambda(n)$, so we have at most $\lambda(n)$ choices for $\bar{N}$, up to S-conjugation, and then the choices for $\varphi(y)$ for every $y \in \mathcal{Y}$ are at most $|\bar{N} \cap S| \leq n! \frac{(q+1)^{n-1}}{d}$.

This is enough to conclude in the case $\bar{X} \cap B = \bar{X} \cap D$. Namely, choose a set $\mathcal{W}$ of minimum cardinality s generating $\bar{X}$ modulo $\bar{X} \cap B$; as $\bar{X}/(\bar{X} \cap B)$ is isomorphic to a subgroup of $\mathrm{Sym}(k-1)$, $s \leq \lfloor \frac{k-1}{2} \rfloor$ if $k \neq 4$, $s \leq 2$ if $k = 4$. The image of any $w \in \mathcal{W}$ will be determined modulo the centralizer in S of a non trivial diagonal automorphism, whose order is at most $\frac{|S|d}{q^{n-1}(q^n-1)}$. It follows that the number of S-classes of φ's is smaller than $|S|^{\frac{k}{2}} \left(\frac{|S|d}{q^{n-1}(q^n-1)} \right)^{\frac{k}{2}} < |S|^k$ if $\bar{X} \cap D$ has prime power order; and that

$$\lambda(n)(n! \frac{(q+1)^{n-1}}{d})^k \left(\frac{|S|d}{q^{n-1}(q^n-1)} \right)^{\frac{k}{2}} \leq ((q+1)^{n-1} n!)^k |S|^{\frac{k}{2}}$$

otherwise. Since now $n > 4$ this last number is $< |S|^k$.

Let us now assume that $1 \neq \bar{X} \cap D < \bar{X} \cap B$. Let $z_1, \ldots, z_k$ be generators of $\bar{X} \cap B$ modulo $\bar{X} \cap D$, where z_1 has been chosen such that $z_1(\bar{X} \cap D)$ has maximum order in $(\bar{X} \cap B)/(\bar{X} \cap D)$, and that this is the order of its first coordinate.

For the moment we will also assume that the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is at least 3 (so that q is not a prime), and that $n \geq 6$. If φ is already defined on

$\bar{X} \cap D$, then $\varphi(z_1)$ is determined modulo the centralizer in S of a non trivial diagonal automorphism, whose order is at most $\frac{|S|d}{q^{n-1}(q^n-1)}$. And then the images of $z_2, \ldots, z_k$, as well as the images of the generators in $\mathcal{W}$ as described above, will be determined modulo $C_S(\varphi(z_1))$. As $\varphi(z_1) = \phi^t a$ for some $a \in \mathrm{InnDiag}(S)$ and $|\phi^t| > 2$, we know from Lemma 12 that $|C_S(\varphi(z_1))| < (d|S|)^{\frac{1}{3}}$. It follows that the number of S-classes of φ's is smaller than

$$\lambda(n)\left(\frac{(q+1)^{n-1}}{d}n!\right)^k \frac{|S|d}{q^{n-1}(q^n-1)}(d|S|)^{\frac{1}{3}(k-1+s)}.$$

As $\lambda(n) \leq 2^{n-1}$, $s \leq \lfloor \frac{k-1}{2} \rfloor$ if $k \neq 4$ and $s \leq 2$ if $k = 4$, and $(q+1)^{n-1}n! < |S|^{\frac{1}{3}}$ when $n \geq 6$ and $q \geq 4$, this number is smaller than $|S|^k$.

Assume now that the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is 2 and that $n \geq 6$ and $q \geq 5$. Suppose that φ is already defined on $\bar{X} \cap D$. Supersolvability of $\bar{X} \cap B$ implies that some non identity cyclic subgroup $\langle u \rangle$ of $\bar{X} \cap D$ is normal in $\bar{X} \cap B$ and we may also assume that the first coordinate of u is non trivial. We choose generators $z_1, \ldots, z_k$ of $\bar{X} \cap B$ modulo $\bar{X} \cap D$ in some Sylow 2-subgroup of $\bar{X} \cap B$, and we may assume that the first coordinate of z_1 has the form $\mathrm{Inn}(S)\alpha$ where $\alpha = \phi^m a$, $a \in \mathrm{InnDiag}(S)$, while the first coordinates of $z_2, \ldots, z_k$ are in $\mathrm{OutDiag}(S)$. The images of $z_1, \ldots, z_k$ will lie in a Sylow 2-subgroup P of the normalizer in $\langle \alpha, \mathrm{InnDiag}(S) \rangle$ of $\langle \varphi(u) \rangle$; such Sylow subgroups are all conjugate under $C_{\mathrm{InnDiag}\,S}(\varphi(u))$, so their number is at most $d|C_S(\varphi(u))|/|C_S(\varphi(u))|_2$. Then the image $\varphi(z_1)$ is determined modulo $P \cap C_{\mathrm{Inn}\,S}(\varphi(u))$, while $\varphi(z_2), \ldots, \varphi(z_k)$ are determined modulo $P \cap C_{\mathrm{Inn}\,S}(\varphi(z_1))$, and finally the images of generators in $\mathcal{W}$ as described above, will be determined modulo $C_S(\varphi(z_1))$. From Lemma 12 we obtain the bounds $|C_S(\varphi(z_1))| \leq (d|S|)^{\frac{2}{3}}$ and $|C_S(\varphi(z_1))|_2 \leq (d|S|)^{\frac{2}{7}}$.

It follows that the number of S-classes of φ's is smaller than

$$\lambda(n)\left(\frac{(q+1)^{n-1}}{d}n!\right)^k \frac{|S|d^2}{q^{n-1}(q^n-1)}(d|S|)^{\frac{2}{7}(k-1)+\frac{2}{3}s}.$$

As $\lambda(n) \leq 2^{n-1}$, $s \leq \lfloor \frac{k-1}{2} \rfloor$ if $k \neq 4$, and $(q+1)^{n-1}n! < |S|^{\frac{29}{100}}$ when $n \geq 6$ and $q \geq 5$, this number is smaller than $|S|^k$ unless $k = 3$, $s = 1$ or $k = 4$, $s = 2$. A small modification of the argument allows to reach the same conclusion also in the two remaining cases: we need one generator w_1 (respectively, two generators w_1, w_2) for $\bar{X}/\bar{X} \cap B$ which is isomorphic to $\mathrm{Sym}(2)$ (respectively, $\mathrm{Sym}(3)$), but the difficulty is overcome by choosing $z_1, \ldots, z_k, w_1$ to lie in the same Sylow 2-subgroup of $\langle \bar{X} \cap B, w_1 \rangle$.

At this point we are left with a list of small cases in which the 'generic' argument breaks down: $n < 6$ when $\bar{X} \cap D \neq 1$ and the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is greater than 2; $n < 6$ or $q < 5$ when $\bar{X} \cap D \neq 1$ and the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is 2. The additional arguments required to deal with these cases are sketched below.

When n is one of 3, 4, 5, $\bar{X} \cap D \neq 1$ and the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is greater than 2 we have that $\bar{X} \cap D$ is a 3-group (a 2-group, a 5-group, respectively), so that $\varphi(\bar{X} \cap D)$ is contained in a Sylow subgroup R (for the relevant prime) of Aut S and there are at most $|R \cap S|^k$ possible choices . The conclusion follows, since the orders of these Sylow subgroups are strictly smaller than $|S|^{\frac{1}{3}}$.

Similar considerations apply if $\bar{X} \cap D \neq 1$ and the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is 2, for almost all the remaining cases. Namely, if either $n = 5$ or $q = 4$ then $d = 5$ and a Sylow 5-subgroup of S has order smaller than $|S|^{\frac{1}{4}}$. If $n = 4$ or $q = 3$ then $\bar{X} \cap B$ is a $2k$-generated 2-group and $\varphi(\bar{X} \cap B)$ is contained in a Sylow 2-subgroup R of Aut S, so that its contribution is at most $|R \cap S|^{2k} < |S|^{\frac{2}{3}k}$ (since $|S|_2 < |S|^{\frac{1}{3}}$); then we have $\frac{k}{2}$ more generators, whose images are determined modulo $C_S(\varphi(z_1))$ that has order at most $|S|^{\frac{2}{3}}$. If $q = 2$ or $n = 3$ and the exponent of $(\bar{X} \cap B)/(\bar{X} \cap D)$ is 2, then $\bar{X}$ is isomorphic to a subgroup of $\mathrm{Sym}(3) \wr \mathrm{Sym}(k)$. In fact, $3 = d \mid q + 1$ implies that $q = p^m$ with m odd, $\mathrm{Out}(S) = \mathrm{OutDiag}(S)\langle \mathrm{Inn}(S)\phi^m \rangle \times \langle \mathrm{Inn}(S)\phi^2 \rangle$, $\mathrm{OutDiag}\, S\langle \mathrm{Inn}(S)\phi^m \rangle \cong \mathrm{Sym}(3)$, $\bar{X} \cap Z(B) = 1$ and $\bar{X}$ is isomorphic to a subgroup of $(\mathrm{Out}(S)/Z(\mathrm{Out}(S)) \wr \mathrm{Sym}(k) \cong \mathrm{Sym}(3) \wr \mathrm{Sym}(k)$. It follows that $\bar{X}$ is either k-generated or $k + 1$-generated with k generators mapping into a Sylow 3-subgroup whose order is strictly smaller than $|S|^{\frac{1}{3}}$.

5. The groups $D_l(q)$

In this section S will be a simple group of the form $D_l(q)$ with $q = p^m$ and $l \geq 4$. In this case $\mathrm{Out}(S) = H \times C$ where C is a cyclic group of order m and H is isomorphic to a subgroup of Sym(4). More precisely $C = \langle \mathrm{Inn}(S)\psi \rangle$ where ψ is a product $\phi\tau$ with ϕ a field automorphism and τ a graph automorphism if $p \equiv 3 \mod 4$, l is odd and m is even, ψ is a field automorphism in all the other cases. Finally $\mathrm{Out}(S)/\mathrm{OutDiag}(S)C \cong \mathrm{Sym}(3)$ if $l = 4$, $|\mathrm{Out}(S)/\mathrm{OutDiag}(S)C| = 2$ otherwise. Our first task is to estimate $|C_S(\alpha)|$ for $\alpha \in \langle \psi, \mathrm{Inn}(S) \rangle$.

Lemma 18. *Let $\alpha \in \langle \psi, \mathrm{Inn}(S) \rangle$ be an automorphism of order e. Then $|C_S(\alpha)| \leq |S|^{\frac{21e-3}{e(21e-4)}}$.*

Proof. By direct calculation. □

We also need information on generators for permutation groups of a very special form:

Lemma 19. *Let G be a subgroup of* $\mathrm{Sym}(4) \wr \mathrm{Sym}(k)$ *with transitive projection on* $\mathrm{Sym}(k)$*, and let H be the stabilizer of* 1 *in the action of G on the blocks. Denote by B the base subgroup of* $\mathrm{Sym}(4) \wr \mathrm{Sym}(k)$*, by A its subgroup* $\mathrm{Alt}(4)^k$*, by D the subgroup*

$O_2(B)$. *Assume that* $H \cap B$ *is neither a* 2*-group nor a* 3*-group and that* $H \cap D \neq 1$. *If* H *is not* k*-generated, then* $\mathrm{d}(H) = k + 1$, *and* H *is one of* $D \cdot \mathrm{diag}\,\mathrm{Sym}(3)$, $D \cdot \mathrm{diag}\,\mathrm{Alt}(3)$, $A \cdot \mathrm{diag}(C_2)$.

Proof. We note that no non trivial element of $H \cap D$ is central in $H \cap A$: if $d = (d_1, \ldots, d_k) \in H \cap D$ with $d_j \neq 1$ and $c = (c_1, \ldots, c_k) \in H \cap A$ is an element of order 3, we can find a G-conjugate c' of c whose j-coordinate $c'_j \neq 1$, and $[c', d] \neq 1$.

Assume that $\mathrm{d}(H) = l > k$. H has a factor group H/N such that $\mathrm{d}(H/N) = l$, its socle M/N is a direct product of H-equivalent chief factors of H and $C_H(M/N) \leq M$. We first discuss the case when $\mathrm{d}(H/(H \cap D)) \leq k$. M/N is a 2-group: otherwise $H \cap D \leq C_H(M/N)$, hence $H \cap D \leq N$ and H/N would be k-generated, a contradiction. Similarly we exclude the possibility that a 2-chief factor of H above $H \cap D$ is isomorphic to one of the chief factors contained in M/N: we would get $H \cap A \leq C_H(M/N)$, so that $H \cap A \leq N$ and $\mathrm{d}(H/N) \leq k$, a contradiction.

We are left with: M/N is the direct product of k non central chief factors H-isomorphic to chief factors contained in D. As D is self-centralizing in $\mathrm{Sym}(4) \wr \mathrm{Sym}(k)$, we get $D \leq H$ and H/D isomorphic to a subgroup of $\mathrm{Sym}(3)$, so that H is one of $D \cdot \mathrm{diag}\,\mathrm{Sym}(3)$, $D \cdot \mathrm{diag}\,\mathrm{Alt}(3)$.

Suppose now that $\mathrm{d}(HD/D) > k$. By Lemma 6 $HD/D \geq A/D$; more precisely, $HD/D = (A/D)\langle Dg \rangle$ where Dg is an involution inverting A/D. But $HD \geq A$ and $H \cap D \neq 1$ imply that $H \cap D$ contains one of the factors of D, and transitivity of G then gives $D \leq H$ so that finally $H = A \cdot \mathrm{diag}(C_2)$. □

After these preliminaries, we move to the proof of our theorem. We have $\bar{X} \leq \mathrm{Out}(S) \wr \mathrm{Sym}(k)$; more precisely, we have a subgroup $\bar{H}$ of $\mathrm{Out}(S) \wr \mathrm{Sym}(k)$ with transitive projection on $\mathrm{Sym}(k)$, and $\bar{X}$ is the stabilizer of the first coordinate. In the base subgroup B of $\mathrm{Out}(S) \wr \mathrm{Sym}(k)$ we single out the subgroups $\Psi = C^k$ and $D = (\mathrm{OutDiag}(S))^k$. We will show that the number h of S-orbits of homomorphisms $\bar{X} \to \mathrm{Aut}(S)$ as in Proposition 1 is smaller than $|S|^k$.

Case 1. $\bar{X} \cap \Psi \neq 1$.

Let e be the exponent of $\bar{X} \cap \Psi$. We take generators $f_1, \ldots, f_k$ of $\bar{X} \cap \Psi$ with the property that f_1 has first coordinate of order e. By [14, Proposition 1.1], the image of f_1 is S-conjugate to an element α of $\langle \psi, \mathrm{Inn}(S) \rangle$ or order e. We select the images of $f_2, \ldots, f_k$ in $C_S(\alpha)$. As $\bar{X}/\bar{X} \cap \Psi \hookrightarrow \mathrm{Sym}(4) \wr \mathrm{Sym}(k)$, to generate $\bar{X}$ we need at most $2k$ more elements; their images are determined modulo $C_S(\alpha)$. The number h is then at most $|C_S(\alpha)|^{3k-1}$.

If $e \geq 4$ we have $\frac{21e-3}{e(21e-4)}(3k-1) < k$.

If $e = 3$ we choose the images of the f_i's in a fixed Sylow 3-subgroup T of $C_S(\alpha)$, and we have $|C_S(\alpha) : T|$ choices for it. By Lemma 8, $|T| \leq |C_S(\alpha)|^{1/2}$. Hence h is at most $|S|^{\frac{60}{3 \cdot 59}(\frac{k-2}{2}+2k+1)} < |S|^k$.

If $e = 2$, then $\bar{X}/\bar{X} \cap \Psi$ is $2k$-generated (it is isomorphic to a subgroup of $\mathrm{Sym}(4) \wr \mathrm{Sym}(k)$), and its quotient $\bar{X}/\bar{X} \cap \Psi D$ isomorphic to a subgroup of

$\mathrm{Sym}(3) \wr \mathrm{Sym}(k)$, is $k+1$-generated. We choose generators for $\bar{X}$: f_i's as above, $k-1$ more elements in ΨD, $k+1$ more to generate $\bar{X}$ modulo $\bar{X} \cap \Psi D$. The image of f_1 is given; we choose a Sylow 2-subgroup T of $C_S(\alpha)$ (among $\leq |C_S(\alpha) : T|$ possibilities); $f_2, \ldots, f_k$ will be mapped into T, the images of the remaining $k-1$ generators from ΨD are determined modulo T; and finally, we have to choose images for $k+1$ more generators, that are determined modulo $C_S(\alpha)$. If q is odd, we check that $|T| \leq |S|^{\frac{1}{6}}$, hence h is at most $|S|^{\frac{39}{2\cdot 38}+\frac{1}{6}(2k-3)}|S|^{\frac{39}{2\cdot 38}(k+1)} < |S|^k$ for $k \geq 2$. If q is even, by Lemmas 8 and 9 we have a weaker bound, $|T| \leq |S|^{\frac{1}{4}}$, but in that case $D = 1$ so we do not need the $k-1$ generators in $\Psi D \setminus D$ and the number h is at most $|S|^{\frac{39}{2\cdot 38}+\frac{1}{4}(k-2)}|S|^{\frac{39}{2\cdot 38}(k+1)} < |S|^k$ for $k \geq 2$.

Case 2. $\bar{X} \cap \Psi = 1$.

As an abstract group $\bar{X} \hookrightarrow \mathrm{Sym}(4) \wr \mathrm{Sym}(k)$ is $2k$-generated.

2.1. $\bar{X} \cap B$ *is a* 2- *or a* 3-*group.*

Let $\bar{X} \cap B$ be a 2-group. If q is even, then $\mathrm{OutDiag}(S) = 1$ and $\bar{X} \cap B$ is a 2-subgroup of $\mathrm{Sym}(3)^k$; hence $\bar{X}$ is isomorphic to a subgroup of $\mathrm{Sym}(2) \wr \mathrm{Sym}(k)$ and can be generated by k elements. So we may assume q odd. We can generate $\bar{X}$ with s generators in $\bar{X} \cap B$ and t more elements coming from generators of $\bar{X}/\bar{X} \cap B$, $t \leq \frac{k}{2}$, $s+t \leq 2k$. The generators in $\bar{X} \cap B$ will be mapped into a Sylow 2-subgroup P of $\mathrm{Aut}(S)$, which is uniquely determined up to conjugacy by inner automorphisms of S. Once P is fixed, the image of each generator in $\bar{X} \cap B$ can be chosen in at most $|P \cap S| < |S|^{\frac{1}{3}}$ different ways. So the S-orbits on the set $\mathcal{H}$ of Proposition 1 are fewer than $|S|^{\frac{s}{3}}|S|^t$; the worst case is $t = \frac{k}{2}$, $s = \frac{3k}{2}$ so in any case $|S|^{\frac{s}{3}}|S|^t \leq |S|^k$.

Let now $\bar{X} \cap B$ be a 3-group. $\bar{X}$ can be generated with k elements of $\bar{X} \cap B$ and $\frac{k}{2}$ coming from generators of $\bar{X}/(\bar{X} \cap B)$. It is enough to note that the k elements of $\bar{X} \cap B$ will be mapped into a Sylow 3-subgroup P of $\mathrm{Aut}(S)$ and that $|P \cap S| < |S|^{\frac{1}{2}}$ by Lemma 8.

From now on we will assume that $\bar{X} \cap B$ has both 2- and 3-elements. This is possible only if $l = 4$.

2.2. $\bar{X} \cap D\Psi = 1$.

As an abstract group $\bar{X} \hookrightarrow \mathrm{Sym}(3) \wr \mathrm{Sym}(k)$, and we can assume that $\bar{X}$ is not k-generated. By Lemma 6 $\bar{X} \cong \mathrm{Alt}(3)^k \cdot \langle g \rangle$ where g is an involution inverting $\mathrm{Alt}(3)^k$. Hence $\bar{X}$ can be generated by $k+1$ elements $a_1, \ldots, a_k, b$ with the property that $\langle a_1, \ldots, a_k \rangle$ is a Sylow 3-subgroup of $\bar{X}$. This implies that $a_1, \ldots, a_k$ will be mapped into a Sylow 3-subgroup P of $\mathrm{Aut}\, S$. Once P is fixed, the image of each a_i can be chosen in at most $|P \cap S| < |S|^{\frac{1}{2}}$ different ways (here we use again Lemma 8). So the S-orbits of homomorphisms are at most $|S|^{\frac{k}{2}}|S| < |S|^k$.

2.3. $\bar{X} \cap D\Psi \neq 1$.

It easily follows that $\bar{X} \cap D \neq 1$ (which implies that q is odd): if $df \in \bar{X}$ with $d \in D$, $f \in \Psi$, $f \neq 1$, in $\bar{X} \cap B$ there is a 3-element g that does not commute

with d and $[g, df] = [g, d] \in \bar{X} \cap D$.

Assuming that $\bar{X}$ is not k-generated, its structure is described by Lemma 19. We take generators of $\bar{X}$ in the following way: $d_{11} \in D$ acting on S as a non inner automorphism, we split D into $\bar{X}$-modules $D_1 \times \cdots \times D_k$ with $d_{11} \in D_1$, we take a second generator d_{12} of D_1, $d_2, \ldots, d_k$ module generators of the other D_i's, c_1 of order 3 not centralizing $d_{11}, c_2, \ldots, c_k$ such that $\langle c_1, \ldots, c_k \rangle$ is a Sylow 3-subgroup of $\bar{X}$, z a 2-element.

We first choose $\varphi(d_{11})$: 2 choices, up to conjugation. We then fix a Sylow 2-subgroup T of $C(\varphi(d_{11}))$ (this is the centralizer in InnDiag(S)) and choose the images of the remaining d_i's in T. We fix a Sylow 3-subgroup R of the normalizer of $\varphi(D_1)$ in Aut(S): the images of the c_j's are determined modulo $R \cap C(\varphi(d_{11})) \cap S$; the image of z is also determined modulo $T \cap S$. As the possibilities for T are at most $|C(\varphi(d_{11}))|/|C(\varphi(d_{11}))|_2$ and the possibilities for R are at most $|C(\varphi(d_{11}))|/|C(\varphi(d_{11}))|_3$, the number h of S-orbits of homomorphisms will be at most

$$2 \cdot |C(\varphi(d_{11}))|^2 \cdot |C(\varphi(d_{11}))|_2^k \cdot |C(\varphi(d_{11}))|_3^{k-1}.$$

The possibilities for $\varphi(d_{11})$, *i.e.* representatives of the conjugacy classes of non inner diagonal involutions, are listed in the Table 4.5.1 of [8] together with their centralizers. We can check that in all cases $2 \cdot |C(\varphi(d_{11}))|^2 \leq |S|^{\frac{5}{4}}$, $|C(\varphi(d_{11}))|_2 \leq |S|^{\frac{1}{5}}$ and $|C(\varphi(d_{11}))|_3 \leq |S|^{\frac{1}{4}}$. It follows that h is at most

$$|S|^{\frac{5}{4}+\frac{1}{5}k+\frac{1}{4}(k-1)} < |S|^k.$$

6. The remaining simple groups

As in the previous cases, $\bar{X} \leq \text{Out}(S)^k \rtimes \text{Sym}(k-1)$; let $D = \text{OutDiag}(S)^k$ and $B = \text{Out}(S)^k$. In all the cases OutDiag(S) is a cyclic r-group (with $r = 3$ if $S \in \{E_6(q), {}^2E_6(q)\}$ and $r = 2$ otherwise). We will show that the number of orbits of S on the set $\mathcal{H}$ of homomorphisms $\bar{X} \to \text{Aut}(S)$ as in Proposition 1 is smaller than $|S|^k$.

Case 1. $\bar{X} \cap D = \bar{X} \cap B$.

We can generate $\bar{X}$ with k generators in $\bar{X} \cap B$ and $\frac{k}{2}$ more elements coming from generators of $\bar{X}/\bar{X} \cap B$. The generators in $\bar{X} \cap B$ will be mapped into a Sylow r-subgroup P of InnDiag S, which is uniquely determined up to conjugacy by inner automorphisms of S. Once P is fixed, the image of each generator in $\bar{X} \cap B$ can be chosen in at most $|P \cap S| < |S|^{\frac{1}{2}}$ different ways. So the S-orbits of homomorphisms are fewer than $|S|^k$.

Case 2. $\bar{X} \cap D < \bar{X} \cap B$.

2.1. $S \notin \{E_6(q), {}^2E_6(q)\}$.

We choose $x_1, \dots, x_a$ generating $\bar{X} \cap D$, $y_1, \dots, y_b$ generating $\bar{X} \cap B$ modulo $\bar{X} \cap D$ and $z_1, \dots, z_c$ generating $\bar{X}$ modulo $\bar{X} \cap B$. Since $\mathrm{OutDiag}(S)$ and $\mathrm{Out}(S)/\mathrm{OutDiag}(S)$ are cyclic groups, $a \leq k$, $b \leq k$ and $c \leq \frac{k}{2}$. The generators in $\bar{X} \cap D$ will be mapped into a Sylow 2-subgroup P of $\mathrm{InnDiag}(S)$, which is uniquely determined up to conjugacy by inner automorphisms of S. Once P is fixed, the image of each generator in $\bar{X} \cap B$ can be chosen in at most $|P \cap S|$ different ways. Let e be the exponent of $\bar{X} \cap B/\bar{X} \cap D$. We can choose y_1 with the property that $|y_1(\bar{X} \cap D)| = e$, and that e is also the order of its first coordinate. The image α of y_1 is an automorphism of S of order e modulo $\mathrm{InnDiag}(S)$. The images of $y_2, \dots, y_b, z_1, \dots, z_c$ are determined modulo $C_S(\alpha)$. So the S-orbits of homomorphisms are at most $\mu = |P \cap S|^{\eta k}|S||C_S(\alpha)|^{\frac{3k}{2}-1}$, with $\eta = 1$ if q is odd, $\eta = 0$ if q is even.

If $S \in \{B_l(q), C_l(q), E_7(q)\}$, then it can be easily checked that $2|P \cap S| < |S|^{\frac{1}{3}}$ if q is odd (if q is even $|P \cap S| < |S|^{\frac{1}{2}}$ by Lemma 8) and $|C_S(\alpha)| \leq (2|S|)^{\frac{1}{e}}$. If $e \geq 3$, then $\mu < |S|^k$; if $e = 2$, then $\bar{X} \cap B$ is a 2-group so we have at most $|P \cap S|^{k(\eta+1)}|C_S(\alpha)|^{\frac{k}{2}} < |S|^k$ possibilities for the images of our generators.

If $S = {}^2D_l(q)$, then $4|P \cap S| \leq |S|^{\frac{1}{3}}$ if q is odd, $|C_S(\alpha)| \leq (4|S|)^{\frac{1}{3}}$ if $e \notin \{2, 4\}$, $|C_S(\alpha)| \leq (4|S|)^{\frac{1}{4}}$ if $e = 4$. If $e \neq 2$ we conclude as in the previous case; if $e = 2$ then, by Lemma 6 and Lemma 7, $\bar{X}$ can be generated by $k(1 + \eta)$ elements and at least $k(\frac{1}{2} + \eta)$ are mapped into a Sylow 2-subgroup, so we have at most $|P \cap S|^{\frac{k}{2}+\eta}|S|^{\frac{k}{2}} < |S|^k$ possibilities.

If $S \in \{G_2(q), F_4(q), E_8(q), {}^2B_2(q), {}^2G_2(q), {}^2F_4(q), {}^3D_4(q)\}$, then we have $\mathrm{OutDiag}(S) = 1$, so $a = 0$, the choices for α are fewer than $|S|$ and the image of each of the remaining $\frac{3k}{2} - 1$ elements is determined in at most $|C_S(\alpha)|$ different ways. If e is not a prime power, then $|C_S(\alpha)| < |S|^{\frac{1}{2}}$ and the choices for our homomorphism are fewer than $|S||S|^{\frac{1}{2}(\frac{3k}{2}-1)} \leq |S|^k$. If e is power of a prime r, then the generators $y_1, \dots, y_b$ are mapped into a Sylow r-subgroup so we have at most $|S|_r^k|S|^{\frac{k}{2}} < |S|^k$ possibilities.

2.2. $S = E_6(q)$.

In this case $|\mathrm{OutDiag}(S)| = (3, q-1)$ and $\mathrm{Aut}(S) = \langle \phi, \tau, \mathrm{InnDiag}(S) \rangle$ with ϕ a field automorphism of order m and τ a graph automorphism of order 2. Let $\Phi = \langle \mathrm{Inn}(S)\phi \rangle^k$. We choose $x_1, \dots, x_a$ generating $\bar{X} \cap D$, $y_1, \dots, y_b$ generating $\bar{X} \cap D\Phi$ modulo $\bar{X} \cap D$ and $z_1, \dots, z_c$ generating $\bar{X}$ modulo $\bar{X} \cap D\Phi$. Clearly $a \leq k$, $b \leq k$ and $c \leq k$ since $\bar{X}/(\bar{X} \cap D\Phi) \leq C_2 \wr \mathrm{Sym}(k)$. The generators in $\bar{X} \cap D$ will be mapped into a Sylow 3-subgroup P of $\mathrm{Aut}(S)$, which is uniquely determined up to conjugacy by inner automorphisms of S. Once P is fixed, the image of each generator in $\bar{X} \cap B$ can be chosen in at most $|P \cap S|$ different ways. Let e be the exponent of $\bar{X} \cap \Phi D/\bar{X} \cap D$. We can choose y_1 with the property that $|y_1(\bar{X} \cap D)| = e$, and that e is also the order of its first coordinate. The image α

of y_1 is an element of $\langle \mathrm{InnDiag}(S), \phi\rangle$ with order e modulo $\mathrm{InnDiag}(S)$. The images of $y_2, \ldots, y_b, z_1, \ldots, z_c$ are determined modulo $C_S(\alpha)$. So the S-orbits of homomorphisms are at most $\mu = |P \cap S|^{\eta k}|S||C_S(\alpha)|^{2k-1}$, with $\eta = 1$ if 3 divides $q-1$, $\eta = 0$ otherwise. It can be easily checked that $3|P \cap S| < |S|^{\frac{1}{8}}$ if $p \neq 3$ and $|C_S(\alpha)| \leq (3|S|)^{\frac{1}{e}}$. If $e \geq 4$, then $\mu < |S|^k$. If $e = 3$ it suffices to notice that also the images of $y_1, \ldots, y_b$ can be chosen in P. Now assume $e \in \{1, 2\}$; in this case $\bar{X}/\bar{X} \cap D \leq (C_2 \times C_2) \rtimes \mathrm{Sym}(k-1)$, so we may choose our generators with the following further property: there exists $d \leq c$ such that $c - d \leq (k-1)/2$ if $k \neq 4$, $c - d \leq 2$ if $k = 4$ and $\langle y_1, \ldots, y_b, z_1, \ldots, z_d\rangle$ is contained in a Sylow 2-subgroup of $\bar{X} \cap B$. If $e = 2$, then the elements $y_1, \ldots, y_b, z_1, \ldots, z_d$ are mapped into a Sylow 2-subgroup Q of $\langle \mathrm{InnDiag}(S), \phi^{\frac{m}{2}}, \tau\rangle$ (and we have at most $|S|/|S|_2$ possibilities for Q), α belongs to Q and can be chosen in at most $|S|_2$ different ways, the elements $y_2, \ldots, y_b, z_1, \ldots, z_d$ are mapped into $C_Q(\alpha)$ and the images of each of these elements can be chosen it at most $|C_Q(\alpha) \cap \mathrm{Inn}\, S| \leq |S|^{\frac{1}{4}}$ different ways, the image of z_i with $i > d$ can be chosen in $|C_S(\alpha) \leq (3|S|)^{1/2}$ different ways, so we have at most $\left(\frac{|S|^{\frac{1}{8}}}{3}\right)^a |S||S|^{\frac{b+d-1}{4}}(3|S|)^{\frac{c-d}{2}} < |S|^k$ possibilities. If $e = 1$, then $b = 0$, the elements $z_1, \ldots, z_d$ are mapped into a Sylow 2-subgroup, so the possibilities are at most $\left(\frac{|S|^{\frac{1}{8}}}{3}\right)^a |S||S|^{\frac{d-1}{2}}(|S|)^{c-d} < |S|^k$.

2.3. $S = {}^2E_6(q)$.

In this case $|\mathrm{OutDiag}(S)| = (3, q+1)$ and $\mathrm{Aut}(S) = \langle \phi, \mathrm{InnDiag}(S)\rangle$ where ϕ is a field automorphism of order $2m$. We choose $x_1, \ldots, x_a$ generating $\bar{X} \cap D$, $y_1, \ldots, y_b$ generating $\bar{X} \cap B$ modulo $\bar{X} \cap D$ and $z_1, \ldots, z_c$ generating $\bar{X}$ modulo $\bar{X} \cap B$; $a \leq k$, $b \leq k$ and $c \leq \frac{k-1}{2}$ if $k \neq 4$, $c \leq 2$ if $k = 4$. The generators in $\bar{X} \cap D$ will be mapped into a Sylow 3-subgroup P of $\mathrm{InnDiag}\, S$. Let e be the exponent of $\bar{X} \cap \Phi D/\bar{X} \cap D$. As in the discussion of the previous cases, there exists $\alpha \in \mathrm{Aut}\, S$ with order e modulo $\mathrm{InnDiag}(S)$ and the S-orbits of homomorphisms are at most $\mu = |P \cap S|^{\eta a}|S||C_S(\alpha)|^{b+c-1}$, with $\eta = 1$ if 3 divides $q+1$, $\eta = 0$ otherwise. It can be easily checked that $3|P \cap S| < |S|^{\frac{1}{8}}$ if $\eta = 1$ and $|C_S(\alpha)| \leq (3|S|)^{\frac{1}{2}}$ if $e \neq 2$. Hence $\mu < |S|^k$ if $e \neq 2$. If $e = 2$ and $d = 1$, then we can use Lemma 7 to deduce that $\mathrm{d}(\bar{X}) \leq k$. If $e = 2$ and $d \neq 1$, then it can be shown that $\bar{X}$ is isomorphic to a subgroup of $\mathrm{Sym}(3) \wr \mathrm{Sym}(k)$, so by Lemma 6 either it is k-generated, or it can be generated by $k+1$ elements $a_1, \ldots, a_k, b$ with the property that $\langle a_1, \ldots, a_k\rangle$ is a Sylow 3-subgroup of $\bar{X}$. This implies that $a_1, \ldots, a_k$ will be mapped into a Sylow 3-subgroup P of $\mathrm{Aut}\, S$ and the S-orbits of homomorphisms are at most $|S|^{\frac{k}{2}}|S| < |S|^k$.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups. *Invent. Math.* **76** (1984), 469–514. Zbl 0537.20023 MR 746539

[2] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group. *J. Algebra* **90** (1984), 446–460. Zbl 0554.20017 MR 760022

[3] M. Aschbacher and L. Scott, Maximal subgroups of finite groups. *J. Algebra* **92** (1985), 44–80. Zbl 0549.20011 MR 772471

[4] P. J. Cameron, R. Solomon, and A. Turull, Chains of subgroups in symmetric groups. *J. Algebra* **127** (1989), 340–352. Zbl 0683.20004 MR 1028457

[5] F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc. Ser. A* **64** (1998), 82–91. Zbl 0902.20013 MR 1490148

[6] E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* **265** (2003), 651–668. Zbl 1072.20031 MR 1987022

[7] W. Gaschütz, Zu einem von B. H. und H. Neumann gestellten Problem. *Math. Nachr.* **14** (1955), 249–252 (1956). Zbl 0071.25202 MR 0083993

[8] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups*, Number 3, Almost simple K-groups. Math. Surveys Monogr. 40.3, Amer. Math. Soc., Providence, RI, 1998. Zbl 0890.20012 MR 1490581

[9] F. Gross and L. G. Kovács, On normal subgroups which are direct products. *J. Algebra* **90** (1984), 133–168. Zbl 0594.20018 MR 757086

[10] W. Kimmerle, R. Lyons, R. Sandling, and D. N. Teague, Composition factors from the group ring and Artin's theorem on orders of simple groups. *Proc. London Math. Soc.* (3) **60** (1990), 89–122. Zbl 0668.20009 MR 1023806

[11] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*. London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, Cambridge 1990. Zbl 0697.20004 MR 1057341

[12] L. G. Kovács and C. E. Praeger, Finite permutation groups with large abelian quotients. *Pacific J. Math.* **136** (1989), 283–292. Zbl 0679.20002 MR 978615

[13] A. Lucchini, Some questions on the number of generators of a finite group. *Rend. Sem. Mat. Univ. Padova* **83** (1990), 201–222. Zbl 0734.20012 MR 1066442

[14] A. Lucchini, F. Menegazzo, and M. Morigi, Complements of the socle in almost simple groups. *Rend. Sem. Mat. Univ. Padova* **112** (2004), 141–163. Zbl 1106.20014 MR 2109958

[15] A. Lucchini and F. Morini, On the probability of generating finite groups with a unique minimal normal subgroup. *Pacific J. Math.* **203** (2002), 429–440. Zbl 1064.20072 MR 1897908

[16] C. Riehm, The equivalence of bilinear forms. *J. Algebra* **31** (1974), 45–66. Zbl 0283.15016 MR 0347867

[17] D. J. S. Robinson, *A course in the theory of groups*. 2nd ed., Grad. Texts in Math. 80, Springer-Verlag, New York 1996. Zbl 0836.20001 MR 1357169

[18] D. A. Suprunenko, *Matrix groups*. Transl. Math. Monogr. 45, Amer. Math. Soc., Providence, RI, 1976. Zbl 0317.20028 MR 0390025

[19] E. P. Vdovin, The number of subgroups with trivial unipotent radicals in finite groups of Lie type. *J. Group Theory* **7** (2004), 99–112. Zbl 1041.20012 MR 2030232

Received December 22, 2006; revised May 7, 2007

A. Lucchini, Dipartimento di Matematica, Università degli Studi di Brescia, Via Valotti 9, 25123 Brescia, Italy

E-mail: lucchini@ing.unibs.it

F. Menegazzo, Dipartimento di Matematica Pura ed Applicata, Università di Padova, Via Trieste 63, 35121 Padova, Italy

E-mail: federico@math.unipd.it

M. Morigi, Dipartimento di Matematica, Università di Bologna, Piazza di Porta S. Donato 5, 40126 Bologna, Italy

E-mail: mmorigi@dm.unibo.it