REND. SEM. MAT. UNIV. PADOVA, Vol. 112 (2004)

Complements of the Socle in Almost Simple Groups.

A. LUCCHINI (*) - F. MENEGAZZO (**) - M. MORIGI (***)

Assume that a finite group H has a unique minimal normal subgroup, say N, and that N has a complement in H. We want to bound the number of conjugacy classes of complements of N in H; in particular we are looking for a bound which depends on the order of N. When $N = \operatorname{soc} H$ is abelian, the conjugacy classes of complements of N in H are in bijective correspondence with the elements of the first cohomology group $\mathrm{H}^1(H/N, N)$. Using the classification of finite simple groups, Aschbacher and Guralnick [1] proved that $|\mathrm{H}^1(H/N, N)| < |N|$; therefore, when $\operatorname{soc} H = N$ is abelian, there are at most $|N|$ conjugacy classes of complements of N in H. To study the case when $N = \operatorname{soc} H$ is nonabelian we can employ a result proved by Gross and Kovács ([6], Theorem 1): there exists a finite group K containing a (non necessarily unique) minimal normal subgroup S which is simple and nonabelian (indeed S is isomorphic to a composition factor of N) and there is a correspondence between conjugacy classes of complements of N in H and conjugacy classes of complements of S in K. Using this result it is not difficult to prove that there exists an absolute constant $c \leqslant 4$ such that the number of conjuga-

(*) Indirizzo dell'A.: Dipartimento di Matematica, Università degli Studi di Brescia, Via Valotti n. 9, 25123 Brescia, Italy. E-mail: lucchini@ing.unibs.it
(**) Indirizzo dell'A.: Dipartimento di Matematica, Pura ed Applicata, Università di Padova, Via Belzoni n. 7, 35131 Padova, Italy.
E-mail: federico@math.unipd.it
(***) Indirizzo dell'A.: Dipartimento di Matematica, Università di Bologna, Piazza di Porta S. Donato n. 5, 40126 Bologna, Italy.
E-mail: mmorigi@dm.unibo.it
Investigation supported by MIUR (project Teoria dei gruppi e applicazioni) and the Universities of Bologna (funds for selected research topics), Brescia and Padova.

cy classes of complements of N in H is at most $|N|^c$ (see, for example, [9] Lemma 2.8). We conjecture that one can take $c = 1$, as occurs when N is abelian.

In this paper we deal with this conjecture in the case of finite almost simple groups. Let G be a finite simple group. As $G \cong \mathrm{Inn}(G)$, we may identify G with $\mathrm{Inn}(G)$. We will prove the following

THEOREM. *Let G be a finite non-abelian simple group and assume that $H \leq \mathrm{Aut}(G)$ contains G. Then the number of conjugacy classes of complements of G in H is less than $|G|$.*

When $G = \mathrm{Alt}(n)$ with $n \neq 6$ or G is a sporadic simple group, it is well known that $|H : G| \leq 2$; if $H \neq G$, then the complements of G in H are in bijective correspondence with the involutions of H which are not contained in G; hence the number of complements for G in H is strictly smaller than $|G|$. The case $G = \mathrm{Alt}(6) \cong \mathrm{PSL}(2, 9)$ is dealt with as a group of Lie type.

We may now assume that G is a finite simple group of Lie type over a field $K = GF(p^m)$ of order p^m, for some prime p. We will follow the definitions and notations of the book [4], unless otherwise stated. So G will be a group of the form $G = \Sigma_l(q)$ where l is the Lie rank of G and $q = p^m$, for some prime p.

Also, ϕ denotes the Frobenius map and Γ denotes the group of graph automorphisms of G.

If G has no complement in $\mathrm{Aut}(G)$ there is nothing to prove, so we may assume that there exists $C \leq H$ such that $H = GC$ and $G \cap C = 1$.

Then we have that C is isomorphic to a subgroup of $\mathrm{Out}(G)$, whose structure is well known. In particular, C is at most 3-generated. Also, if x, y, z are generators of C and C' is any other complement for G in H, then C' is generated by three elements of the form xu_1, yu_2, zu_3 satisfying the same relations as x, y, z and with $u_i \in G$, for $i = 1, 2, 3$.

In the whole paper, C will be a fixed complement for G in H.

1. Preliminary results.

We collect in this section some results which will be very useful in the sequel. The first is actually a corollary of Lang's theorem, in the general form proved by Steinberg.

PROPOSITION 1.1. *Let G be an untwisted finite simple group of Lie type over the field K with p^m elements. Let $\phi^r a \in \mathrm{Aut}(G)$, with $a \in \in \mathrm{InnDiag}(G)\Gamma$, and assume that $|\phi^r a| = m/r$. If $x \in \mathrm{InnDiag}(G)$ is such that $|\phi^r ax| = m/r$ then $\phi^r a$ and $\phi^r ax$ are* $\mathrm{InnDiag}(G)$*-conjugate.*

PROOF. Let $G = \Sigma_l(p^m)$ and let $\overline{G}$ be the connected algebraic group over the algebraic closure $\overline{K}$ of K such that $\overline{G}$ is adjoint and $G = = O^{p'}(C_{\overline{G}}(\phi^m))$ (see [4, Theorem 2.2.6 (e)]). By Lemma 2.5.8. (a) of [4] we have that $\mathrm{InnDiag}(G) = C_{\overline{G}}(\phi^m)$.

Let τ_x be the inner automorphism of $\overline{G}$ induced by x. There exists $\overline{a} \in \mathrm{Aut}(\overline{G})$ such that $\overline{a}$ is the product of a graph automorphism and an inner automorphism, and $\overline{a}$ induces a on G. We note that $(\phi^r\overline{a})^{m/r} = = (\phi^r\overline{a}\tau_x)^{m/r} = \phi^m$. So $\phi^r\overline{a}$ is a surjective homomorphism ψ of $\overline{G}$ whose set of fixed points in $\overline{G}$ is finite. By the Lang-Steinberg theorem (see [Theorem 2.1.1] [4]) there exists $\overline{w} \in \overline{G}$ such that $x^{-1} = \overline{w}^{-1}\overline{w}^{\phi^r\overline{a}}$. Let $s = \dfrac{m}{r}$. We have that: $\phi^m = (\psi\tau_x)^s = \psi^s \tau_x^{\psi^{s-1}} \tau_x^{\psi^{s-2}} \ldots \tau_x^{\psi}\tau_x = = \phi^m \tau_x^{\psi^{s-1}} \tau_x^{\psi^{s-2}} \ldots \tau_x^{\psi}\tau_x$, so $\tau_x^{\psi^{s-1}} \tau_x^{\psi^{s-2}} \ldots \tau_x^{\psi}\tau_x = 1$. As $x = (\overline{w}^{-1})^{\psi}\overline{w}$ we obtain that $(\tau_{\overline{w}}^{-1})^{\psi^s}\tau_{\overline{w}} = 1$, so $\tau_{\overline{w}}^{\phi^m} = \tau_{\overline{w}}$, that is $\overline{w} \in \mathrm{InnDiag}(G)$.

It follows that $(\phi^r a)^{\overline{w}} = \overline{w}^{-1}\phi^r a\overline{w} = \phi^r a(\overline{w}^{-1})^{\phi^r a}\overline{w} = = \phi^r a(\overline{w}^{-1}\overline{w}^{\phi^r a})^{-1} = \phi^r ax$, as we wanted to prove.

We will also need a lemma proved in [8].

LEMMA 1.2. *Let G be a finite simple group of Lie type, and let $a \in \in \mathrm{Aut}(G)$ then there exists $g \in G$ such that $|a| \neq |ag|$.*

Our first results are easy consequences of the proposition and lemma above.

PROPOSITION 1.3. *Let G be a finite simple group of Lie type, $G \leqslant \leqslant H \leqslant \mathrm{Aut}(G)$ and assume that a complement C for G in H is cyclic. Then the number of complements for G in H is less than $|G|$.*

PROOF. If $C = \langle a \rangle$, then any other complement C' is generated by an element of the form ag, with $g \in G$ and $|ag| = |a|$, and lemma 1.2 applies.

COROLLARY 1.4. *Let G be a finite simple group of one of the following types: ${}^3D_4(q)$, $G_2(q)$, $F_4(q)$, $E_8(q)$, ${}^2F_4(q)$ or ${}^2G_2(q)$ and let $G \leqslant H \leqslant \leqslant \mathrm{Aut}(G)$. Then the number of complements for G in H is less than $|G|$.*

PROOF. By Theorem 2.5.12 of [4] the groups listed above have cyclic outer automorphism group, so proposition 1.3 applies.

PROPOSITION 1.5. *Let G be an untwisted finite simple group of Lie type over the field K. Assume that $C = \langle \phi^r a, b \rangle$, with $a \in \mathrm{InnDiag}(G)$, $b \in \mathrm{InnDiag}(G)\Gamma \setminus \mathrm{Inn}(G)$ and $|\phi^r a| = |\phi^r|$. Then the number of G-conjugacy classes of complements for G in H is less than $|G|$.*

PROOF. If C' is another complement for G in H, then the first generator of C' is of the form $\phi^r ag$, with $g \in G$ and $|\phi^r ag| = |\phi^r a| = |\phi^r|$, so by proposition 1.1 we have at most $d = |\mathrm{InnDiag}(G) : G|$ choices for it, up to G-conjugation. Moreover, again by proposition 1.1, we may assume that $\phi^r ag = (\phi^r)^x$ for some $x \in \mathrm{InnDiag}(G)$. So $C' = \langle \phi^r, (bv)^{x^{-1}} \rangle^x$, for some $v \in G$. We now need to count the choices for the second generator, which is of the form $(yu)^x$, where $y = b^{x^{-1}}$ and $v = u^{x^{-1}}$. By lemma 1.2 we have less than $|G|$ choices for u, as $|yu| = |y|$. Moreover, as we are counting G-conjugacy classes of complements, we may count the elements of the form yu up to conjugation by elements of the centralizer of ϕ^r in G. If $G = \Sigma_l(q)$ then $\Sigma_l(p) \leq C_G(\phi^r)$. We have that $[yu, \Sigma_l(p)] \neq 1$ (see [Lemma 2.5.7] [4]), so that $C_{\Sigma_l(p)}(yu)$ is a proper subroup of $\Sigma_l(p)$. As the index of a maximal subgroup of $\Sigma_l(p)$ is at least d (see Table 5.2 A of [p. 175] [7]) each orbit of the set $\{yu \mid u \in G\}$ under the action of $\Sigma_l(p)$ by conjugation has at least d elements. This concludes the proof.

PROPOSITION 1.6. *Let G be an untwisted finite simple group of Lie type over the field K. Assume that $C = \langle \phi^r a, b \rangle$, with $a, b \in \mathrm{InnDiag}(G)\Gamma$, $\mathrm{InnDiag}(G) \leq H$ and $|\phi^r a| = |\phi^r|$. Then the number of G-conjugacy classes of complements for G in H is less than $|G|$.*

PROOF. If C' is another complement, by proposition 1.1 we may assume that the first generator of C' is $(\phi^r a)^x$, for some $x \in \mathrm{InnDiag}(G)$. Let $C' = \langle (\phi^r a)^x, bu \rangle$, where $u \in G$. As $\mathrm{InnDiag}(G) \leq H = GC'$ we have that $x = zy$ for some $z \in G$ and some $y \in C'$, so that $C' = \langle (\phi^r a)^z, (bu)^{y^{-1}} \rangle$ is G-conjugate to a complement of the form $C'' = \langle \phi^r a, v \rangle$. It follows that the first generator of C' is uniquely determined, up to G-conjugation. By lemma 1.2 the number of choices for the second generator of C' are less than $|G|$, and the conclusion follows.

We recall that if $a \in H$, then a is of one of the following types: inner, inner-diagonal, graph, field or graph-field (see [4], definition 2.5.13).

PROPOSITION 1.7. *Let G be a finite simple group of Lie type over the field K. Assume that $C = \langle a, b\rangle$, where the type of a is known and b normalizes $\langle a\rangle$. Then the number of conjugacy classes of complements for G in H is bounded by rs, where r is the number of G-conjugacy classes of elements of H of the same type and order as a and s is the order of a maximal subgroup of G.*

PROOF. If C' is another complement for G in H, we have that $C' = \langle au, bv\rangle$, for some $u, v \in G$, where $|au| = |a|$, $|bv| = |b|$ and if $a^b = a^t$ for some integer t, then $(au)^{bv} = (au)^t$. There are at most r choices for au, up to G-conjugacy. Moreover, any two elements bv' and bv'' such that $(au)^{bv'} = (au)^{bv''} = (au)^t$ satisfy $(bv')^{-1} bv'' \in C_G(au)$, so there are at most $|C_G(au)|$ choices for the second generator, and the conclusion follows.

2. The special linear groups.

Let K be the finite field with q elements, with $q = p^m$ for some prime number p. As usual $GL(n, q)$ (resp. $SL(n, q)$) will denote the general (resp. special) linear group of degree n over the field K. In the following we will identify the multiplicative group $K^\times$ of K with the subgroup of $GL(n, q)$ consisting of scalar matrices. Then $\mathrm{PGL}(n, q) = \mathrm{GL}(n, q)/K^\times$, $PSL(n, q) = SL(n, q)K^\times/K^\times$ and if $g \in \mathrm{GL}(n, q)$ its image in $\mathrm{PGL}(n, q)$ will be denoted with $\bar{g}$. Also, as usual, $\det(g)$ will indicate the determinant of a matrix g and $diag(a_1, \ldots, a_n)$ will denote a diagonal matrix, whose entries on the diagonal are those listed between the brackets.

In the whole section, we will consider $G = A_{n-1}(q) = \mathrm{PSL}(n, q)$, for n and q fixed. Let ϕ be the Frobenius automorphism of $\mathrm{GL}(n, q)$, given by: $(a_{ij})^\phi = (a_{ij}^p)$, for $i, j = 1, \ldots, n$.

Let $\tau : \mathrm{GL}(n, q) \to \mathrm{GL}(n, q)$ be the automorphism defined by $g^\tau = (g^\top)^{-1}$, where $g^\top$ denotes the transposed matrix of g.

Both ϕ and τ induce automorphisms of $\mathrm{PGL}(n, q)$, which we will still indicate by ϕ and τ. ϕ generates the group of field automorphisms, τ is a graph automorphism if $n \geqslant 3$, and it is an inner automorphism if $n = 2$. Also, $\mathrm{PGL}(n, q)/G$ is cyclic of order $d = (n, q-1)$.

We have that C is isomorphic to a subgroup of $\mathrm{Out}(G) = \langle \phi G, \tau G, aG\rangle$, where $a \in \mathrm{PGL}(n, q)$, $(aG)^{\phi G} = a^p G$, $(aG)^{\tau G} = a^{-1} G$, $[\phi G, \tau G] = 1$ and $|aG| = d$, $|\phi G| = m$, $|\tau G| = 2$.

Case A: C is 3-generated

In this case C has the group $Z_2 \times Z_2 \times Z_2$ as an epimorphic image and d is even, so that p is odd and $n \geqslant 4$ is even.

We may assume that $C = \langle \phi^r \overline{N}_1, \tau \overline{M}_1, \overline{U}_1 \rangle$, where $M_1, N_1, U_1 \in \in \mathrm{GL}(n, q)$ and $r | m$. Also we have that $\overline{U}_1$ has order d', with $2 | d' | d$ and we also have that $(\phi^r \overline{N}_1)^{m/r} \in \langle \overline{U}_1 \rangle$.

LEMMA 2.1. *In the above setting, we may also assume that* $[\phi^r \overline{N}_1, \tau \overline{M}_1] = 1$ *and* $\tau \overline{M}_1$ *has order* 2.

PROOF. As C is isomorphic to a subgroup of $\mathrm{Out}(G)$, it will be isomorphic to a subgroup T of the group $X = \langle a, b, c \,|\, a^d = b^2 = c^m = 1, \ a^b = = a^{-1}, a^c = a^p, b^c = b \rangle$ where p is a prime and $p^m \equiv 1 \bmod d$. Since T is not 2-generated, $T \cap \langle a, b \rangle$ and $T\langle a \rangle / \langle a \rangle$ are not cyclic; in particular m is even. Set $\langle a^l \rangle = T \cap \langle a \rangle$. If $b \in T$, easy calculations prove that $T = = \langle a^l, b, c^k \rangle$ where both a^l and c^k have even order. Assume that $b \notin T$ and $ba \in T$. Note that $C_X(ba) = \langle a^{d/2}, ba, u \rangle$ where $u = ca^{-\frac{p-1}{2}}$. Similar computations prove that $T = \langle a^l, ba, u^k \rangle$, where l is even, and the orders of a^l and of $u^k \langle a \rangle$ are even. As any subgroup of X which is not 2-generated is $\langle a \rangle$-conjugate to a subgroup containing either b or ba, the result follows.

OBSERVATION. With the notation of lemma 2.1 we note that it is possible that T does not split over $T \cap \langle a, b \rangle$. Namely, $T = \langle a^l, ba, u^k \rangle$ is not 2-generated and does not split over $T \cap \langle a, b \rangle$ iff $p \neq 2, l, d, m/k$ are even, $\dfrac{p^m - 1}{d}$ is odd, the order of a^l is divisible by 4, and finally $r_2 < < \max((p^k - 1)_2, (p^k + 1)_2)$ where we denote by x_2 the 2-part of the integer x. Also, if T does not split over $T \cap \langle a, b \rangle$ we have that u^m has order 2.

CASE I: $(\phi^r \overline{N}_1)^{m/r} = 1$

We may assume that another complement C' for G in H is generated by $\phi^r \overline{N}_1 \overline{X}$, $\tau \overline{M}$, $\overline{U}$, with $\overline{X} \in G$, $\overline{M}, \overline{U} \in \mathrm{PGL}(n, q)$, satisfying the same relations as $\phi^r \overline{N}_1, \tau \overline{M}_1, \overline{U}_1$. In particular $(\phi^r \overline{N}_1 \overline{X})^{m/r} = 1$, so by proposition 1.1 there are at most d possibilities for the choice of $\phi^r \overline{N}_1 \overline{X}$, up to conjugation by elements of G. Moreover, again by proposition 1.1, we have that $\phi^r \overline{N}_1 \overline{X} = (\phi^r)^{\overline{S}}$, with $\overline{S} \in \mathrm{PGL}(n, q)$. Changing notations for the last two generators, we may now assume that $C' = \langle (\phi^r)^{\overline{S}}, (\tau\overline{M})^{\overline{S}}, (\overline{U})^{\overline{S}} \rangle$.

We now have to count how many possibilities there are for the other two generators. From the fact that $\tau\overline{M}$ has order 2 it follows that $\overline{M}^{\tau}\overline{M} = 1$, so $M^{\top} = \alpha M$, with $\alpha \in K$ and as $(M^{\top})^{\top} = M$ we have that $\alpha^2 = 1$, so that M is symmetric or skew-symmetric.

From the fact that $[\phi^r, \tau\overline{M}] = 1$ it follows that $M^{\phi^r} = \beta M$, with $\beta \in K^{\times}$. This implies that $m_{ij}^{p^r - 1} = \beta$ for each $i, j = 1, \ldots, n$ such that $m_{ij} \neq 0$. Choose h, k such that $m_{hk} \neq 0$. Thus, for each $i, j = 1, \ldots, n$ we have that $m_{ij} m_{hk}^{-1} \in \mathrm{GF}(p^r)$, that is $m_{ij} = m_{hk} m'_{ij}$ for some $m'_{ij} \in GF(p^r)$. It follows that $M = m_{hk} M'$, with $M' \in \mathrm{GL}(n, p^r)$. Choosing M' instead of M as a pre-image of $\overline{M}$ we may assume that $M \in \mathrm{GL}(n, p^r)$.

As we are counting conjugacy classes of complements, we note that to count the possibilities for the second generator of C' we are still free to conjugate it by an element $\overline{H}$ of G centralizing ϕ^r, that is $H \in \mathrm{SL}(n, p^r)$. Note that in that case we have that $(\tau\overline{M})^{\overline{H}} = \tau\overline{H}^{\top}\overline{M}\overline{H}$, and by [3] there exists $H \in \mathrm{GL}(n, p^r)$ such that $H^{\top} MH$ has one of the following forms: identity, $\mathrm{diag}(a, 1, \ldots, 1)$, where a is a non-square in $\mathrm{GF}(p^r)$, or a block-diagonal matrix whose blocks on the diagonal are all equal to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

As we are allowed to conjugate by matrices in $\mathrm{PSL}(n, q)$ and not in $\mathrm{PGL}(n, q)$, we have at most $3d$ possibilities for $\overline{M}$.

We now count the number of choices for $\overline{U}$. We have that $(\overline{U})^{\tau\overline{M}} = (\overline{U})^{-1}$, so $U^{\top M} = \gamma U$, with $\gamma^2 = 1$, and we have at most $q^{n(n+1)/2}$ possibilities for U for each choice of γ. So we have at most $2q^{n(n+1)/2}/(q-1)$ possibilities for $\overline{U}$, and thus at most $\frac{6d^3 q^{n(n+1)/2}}{(q-1)} < |G|$ possibilities for C', as $6q^{n+1} < (q^3 - 1)(q^n - 1)$ for $n \geqslant 4$ and $q \geqslant 9$.

Case II: $(\phi^r\overline{N}_1)^{m/r} \neq 1$

In this case $\frac{m}{r}$ is even. Actually, if $\frac{m}{r}$ is odd, putting $x = \tau\overline{M}_1$, $y = \phi^r\overline{N}_1$, if $m = 2^t s$, with $\frac{m}{r} \mid s$, then $C = \langle x, y^{2^t}, y^s, \overline{U} \rangle = \langle xy^{2^t}, \overline{U} \rangle$, as $y^s \in \langle y^{m/r} \rangle \in \langle \overline{U} \rangle$. So C is 2-generated, contradicting the assumptions.

Again, we may assume that another complement C' is generated by $\phi^r\overline{N}, \tau\overline{M}, \overline{U}$, satisfying the same relations as $\phi^r\overline{N}_1, \tau\overline{M}_1, \overline{U}_1$. In particular $(\tau\overline{M})^2 = 1$. As in Case I, it follows that M is symmetric or skew-symmetric, and conjugating by a suitable element of $\mathrm{PSL}(n, q)$ we have at most $3d$ possibilities for $\overline{M}$. Namely, we may assume that $\tau\overline{M}$ is of one of the following types:

i) $\tau^{\overline{S}}$,

ii) $(\tau\overline{A})^{\overline{S}}$, with $A = \operatorname{diag}(a, 1, \ldots, 1)$, where a is a non-square in K,

iii) $(\tau\overline{B})^{\overline{S}}$, where B is a block-diagonal matrix whose blocks on the diagonal are all equal to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Changing notations for the generators, we may assume that $C' = \langle (\phi^r\overline{N})^{\overline{S}}, (\tau\overline{M})^{\overline{S}}, (\overline{U})^{\overline{S}} \rangle$, with $\overline{M} \in \{\overline{I}, \overline{A}, \overline{B}\}$. Also, there is no loss in generality in assuming $\overline{S} = 1$, as this does not affect calculations.

We now consider the generator $\phi^r\overline{N}$. Let $\mu = \det(N)$ and $(\phi^r N)^{m/r} = L$.

In cases i) and iii) we have that $[\tau\overline{M}, \phi^r\overline{N}] = [\tau\overline{M}, \overline{N}] = 1$, so that $\overline{N}^{\tau\overline{M}} = \overline{N}$. It follows that $(N^{-1})^{\top M} = \gamma N$, with $\gamma \in K^\times$, and $\mu^2 \in K^n$ (here K^n is the set of elements of K which are n-th powers).

As $\dfrac{m}{r}$ is even and p is odd it follows that $2 \mid \dfrac{(p^r)^{m/r} - 1}{p^r - 1}$, so that $\det(L) = \mu^{\frac{(p^r)^{m/r}-1}{p^r-1}} \in K^n$, which implies that $(\phi^r\overline{N})^{m/r} \in C \cap G = 1$ and $(\phi^r\overline{N}_1)^{m/r} = (\phi^r\overline{N})^{m/r} = 1$, a contradiction.

We now deal with case ii). From $[(\tau\overline{A}), (\phi^r\overline{N})] = 1$ it follows that $\overline{N}^\tau\overline{A} = \overline{A}^{\phi^r}\overline{N}$, so $N^{-\top} = \gamma A^{\phi^r} N A^{-1}$, with $\gamma \in K^\times$ and $\mu^2 = a^{1-p^r}\gamma^{-n}$.

As before, $\det(L) = \mu^{\frac{(p^r)^{m/r}-1}{p^r-1}} \equiv a^{(1-p^r)\frac{p^m-1}{2(p^r-1)}} \equiv -1$ modulo K^n, so that $\overline{L}^2 = 1$ (note that $\dfrac{q-1}{d}$ is odd, as it is stated in the observation after lemma 2.1).

We distinguish two subcases:

a) $r \leqslant \dfrac{m}{4}$. We first bound the choices for the generator of the form $\phi^r\overline{N}$. By [p. 52] [5] $\phi^r\overline{B}$ and $\phi^r\overline{C}$ are conjugate in $\mathrm{GL}(n, q)$ if and only if $(\phi^r\overline{B})^{m/r}$ and $(\phi^r\overline{C})^{m/r}$ have the same property, so we need to count $\mathrm{PGL}(n, q)$-conjugacy classes of involutions $(\phi^r\overline{N})^{m/r} \in \mathrm{PGL}(n, q) \setminus \mathrm{PSL}(n, q)$. By Table 4.5.1 of [4] there are at most $n/2$ choices for $(\phi^r\overline{N})^{m/r}$, which means at most $\dfrac{n}{2}$ $\mathrm{PGL}(n, q)$-conjugacy classes of elements of the form $\phi^r\overline{N}$, that is at most $d\dfrac{n}{2}$ choices for $\phi^r\overline{N}$, up to $\mathrm{PSL}(n, q)$-conjugation.

Now once we have chosen an element $\tau\overline{V}$ as a second generator, from the fact that $(\phi^r\overline{N})^{\tau\overline{V}} = \phi^r\overline{N}$ it follows that all the other possible choices for the second generator are of the form $\tau\overline{V}\overline{U}$, where $\overline{U} \in C_G(\phi^r \overline{N})$.

Let $\overline{K}$ the algebraic closure of K. By the Lang-Steinberg theorem [p. 32] [2] we have that $\phi^r \overline{N}$ is conjugate to ϕ^r in $\mathrm{PGL}(n, \overline{K})$, so $|C_{\mathrm{PSL}(n,\overline{K})}(\phi^r \overline{N})| = |\mathrm{PGL}(n, p^r)|$. So we have at most $|\mathrm{PGL}(n, p^r)|$ choices for $\tau\overline{V}$.

By our hypothesis, there exists $\overline{R}$ such that $(\tau\overline{V})^{\overline{R}^{-1}}$ is of the form $\tau\overline{A}$, with $A = \mathrm{diag}(a, 1, \dots, 1)$, where a is a non-square in K.

We may assume that the third generator is of the form $(\overline{U})^{\overline{R}}$.

We have that $\overline{U}^{\overline{R}(\tau\overline{V})} = (\overline{U})^{\overline{R}(\tau\overline{A})^{\overline{R}}} = (\overline{U}^{\tau\overline{A}})^{\overline{R}}$, and as $(\overline{U}^{\overline{R}})^{(\tau\overline{V})} = (\overline{U}^{-1})^{\overline{R}}$, it follows that $\overline{U}^{\top\overline{A}} = \overline{U}$, that is $U^{\top A} = \gamma U$, with $\gamma \in \{\pm 1\}$.

This means that, fixed γ, U is determined by its entries along and above the diagonal, so we have at most $2q^{\frac{n(n+1)}{2}}$ choices for U, and at most $\frac{2}{q-1}q^{\frac{n(n+1)}{2}}$ choices for $\overline{U}$.

Putting all together, the number of conjugacy classes of complements for G in H is at most $\leqslant d\frac{n}{2}\,|\mathrm{PGL}(n, p^{m/4})|\,\frac{2}{q-1}q^{\frac{n(n+1)}{2}} < |\mathrm{PSL}(n, q)|$. (Here we have used that $8\,|\,n$, because m is even, so that $8\,|\,q-1$ and $\frac{q-1}{d}$ is odd).

b) $r = \frac{m}{2}$. We first bound the choices for the generator of the form $\phi^r \overline{N}$.

As $(\phi^{m/2}\overline{N})^2 = \overline{L}$ has order 2, the canonical form of L is either a diagonal matrix whose entries on the diagonal are in the set $\{\pm\gamma\}$, for some $\gamma \in K^\times$ (first type), or it is a block-diagonal matrix, whose blocks on the diagonal are all equal to $\begin{pmatrix} & \gamma \\ 1 & \end{pmatrix}$, with $\gamma \in K^\times$ (second type). By [p. 50] [5], by conjugating by a suitable element of $GL(n, q)$ we may assume that N is block-diagonal matrix, whose blocks N_i on the diagonal are of the form

$$N_i = \begin{bmatrix} 0 & \cdots & \cdots & 0 & a_{i,1} \\ 1 & \ddots & & \vdots & a_{i,2} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & a_{i,m_i} \end{bmatrix}.$$

So we may assume that also L is a block-diagonal matrix, whose blocks L_i on the diagonal have dimension m_i.

We now want to prove that the canonical form of L is diagonal.

If $m_j \geq 5$ for some j it is easy to see that $\overline{L}_j$ cannot have order 2. Also, if the canonical form of L is of the second type, then $2 \mid m_j$ for each j. Now assume that $m_j = 2$ for some j. As L_j^2 is a scalar matrix, L_j is of the form $L_j = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$. Moreover L_j is diagonalizable if and only if $x^2 + yz$ is a square. Let $N_j = \begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$. Then $L_j = \begin{pmatrix} b^{p^{m/2}} & ab^{p^{m/2}} \\ a^{p^{m/2}} & b + a^{p^{m/2}+1} \end{pmatrix}$, $-\det(L_j) = -b^{p^{m/2}+1}$ is a square (note that -1 is a square) and it follows that L_j is diagonalizable.

To conclude, assume that $m_j = 4$ for each j. We have that L_j is of the form

$$\begin{pmatrix} & & & a^{p^{m/2}} \\ 1 & & & b^{p^{m/2}} \\ & 1 & & c^{p^{m/2}} \\ & & 1 & d^{p^{m/2}} \end{pmatrix} \begin{pmatrix} & & & a \\ 1 & & & b \\ & 1 & & c \\ & & 1 & d \end{pmatrix} = \begin{pmatrix} & & a^{p^{m/2}} & \star \\ & & b^{p^{m/2}} & \star \\ 1 & & c^{p^{m/2}} & \star \\ & 1 & d^{p^{m/2}} & \star \end{pmatrix}.$$

So the first column of L_j^2 is $\begin{pmatrix} a^{p^{m/2}} \\ b^{p^{m/2}} \\ c^{p^{m/2}} \\ d^{p^{m/2}} \end{pmatrix}$, which implies that $b = c = d = 0$. So $L_j = \begin{pmatrix} & & a^{p^{m/2}} & \\ & & & a \\ 1 & & & \\ & 1 & & \end{pmatrix}$ and $L_j^2 = \mathrm{diag}\,(a^{p^{m/2}}, a, a^{p^{m/2}}, a)$.

As L^2 is a scalar matrix it follows that $a^{p^{m/2}} = a$ and a is the same for all blocks L_j. We have $a = \lambda^{u(p^{m/2}+1)}$, for some integer number u, and $\det L = (a^2)^{n/4} = \lambda^{u(n/2)(p^{m/2}+1)}$, which leads to a contradiction because $d \mid \frac{n}{2}(p^{m/2}+1)$.

It follows that L is diagonal.

So we have at most $\frac{n}{2}$ choices for $\overline{L}$ and thus at most $\frac{n}{2}$ choices for $\phi^{m/2}\overline{N}$, up to PGL(n, q)-conjugation. As we are counting PSL(n, q)-conjugacy classes we have to multiply this number by d.

We may also assume that $L = (L_1, L_2)$ is a block diagonal matrix with 2 blocks on the diagonal of the form $L_1 = \gamma I_{r_1}$ and $L_2 = -\gamma I_{r_2}$, for some γ

in $K^{\times}$, where $r_1 + r_2 = n$. We note that r_1 and r_2 are both odd, otherwise $\det(L) = \gamma^n$ contradicting the fact that $\overline{L} \notin \mathrm{PSL}(n, q)$. Moreover, as $8 \mid n$, we have that $r_1 \neq \frac{n}{2} \neq r_2$.

We have that $\overline{M}$, $\overline{N}$ and $\overline{U}$ centralize $\overline{L}$, so we may assume that they are all block-diagonal matrices, with $M = (M_1, M_2)$, $N = (N_1, N_2)$ and $U = (U_1, U_2)$. (Note that if $\overline{L}^{\overline{S}} = \overline{L}$ then $L^S = \alpha L$ for some $\alpha \in K^{\times}$, but looking at the eigenvalues of L and keeping in mind that $r_i \neq \frac{n}{2}$, it follows that $\alpha = 1$, that is S centralizes L).

By proposition 1.1, we have that $\phi^{m/2}\overline{N}_i$ is conjugate to ϕ in $\mathrm{PGL}(r_i, q)$, and so $\phi^{m/2}\overline{N}$ is conjugate to $\phi\overline{D}$ in $\mathrm{PGL}(n, q)$, with $D = (I_1, \beta I_2)$ for some $\beta \in K^{\times}$.

We now work separately on the two blocks, using exactly the same strategy as in case I.

We may assume that $M_1 = \xi M_1'$, with $\xi \in K^{\times}$ and $M_1' \in \mathrm{GL}(r_1, p^{m/2})$. Moreover M_1 is symmetric (note that r_1 is odd). By conjugating with elements of $\mathrm{GL}(r_1, p^{m/2})$ we find that there are at most 2 choices for M_1', and at most $2(q-1)$ choices up to $SL(r_1, p^{m/2})$-conjugation. So there are at most $2(q-1)^2$ choices for $M_1'\xi$. Arguing in the same way for M_2 and taking images in $\mathrm{PGL}(n, q)$ we obtain that there are at most $4(q-1)^3$ choices for $\overline{M}$.

The number of choices for U_i is now at most $q^{r_i(r_i+1)/2}$ (note that the element γ appearing in case I is now forced to be 1, as r_i is odd). So there are at most $q^{r_1(r_1+1)/2}q^{r_2(r_2+1)/2}/(q-1)$ possibilities for $\overline{U}$.

So we have at most $\frac{n}{2}d4(q^{r_1(r_1+1)/2}q^{r_2(r_2+1)/2})(q-1)^2 < |\mathrm{PSL}(n, q)|$ choices for C.

Case B: C is 2-generated

We may assume that $C = \langle \phi^r\overline{N}_1, \tau^{\varepsilon}\phi^s\overline{M}_1 \rangle$, where $M_1, N_1 \in \mathrm{GL}(n, q)$ and $\varepsilon \in \{0, 1\}$. We may also assume that any other complement C' is generated by $\phi^r\overline{N}, \tau^{\varepsilon}\phi^s\overline{M}$, satisfying the same relations as $\phi^r\overline{N}_1, \tau^{\varepsilon}\phi^s\overline{M}_1$.

Case I: $C \nleq \mathrm{InnDiag}(G)\Gamma, (\phi^r\overline{N}_1)^{m/r} = 1$
In this case we apply proposition 1.5.

Case II: $C \nleq \mathrm{InnDiag}(G)\,\Gamma, (\phi^r\overline{N}_1)^{m/r} = \overline{L}_1 \neq 1,\ n \geqslant 3$

Let $u = |\overline{L}_1|$. We now want to count $\mathrm{PSL}(n, q)$-conjugacy classes of elements of the form $\phi^r \overline{N}$. By [p. 52] [5] $\phi^r \overline{A}$ and $\phi^r \overline{B}$ are conjugate if and only if $(\phi^r \overline{A})^{m/r}$ and $(\phi^r \overline{B})^{m/r}$ are conjugate, so we need to bound the number of $\mathrm{PGL}(n, q)$-conjugacy classes of elements $\overline{L}$ of order u, and then to multiply this bound by $|\mathrm{PGL}(n, q) : \mathrm{PSL}(n, q)| = d$. As L^u is a scalar matrix, L is conjugate to a block-diagonal matrix X whose blocks X_i have all the same dimension k and are of the form:

$$X_i = \begin{bmatrix} & & & c_i \\ 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \quad \end{bmatrix}, \tag{1}$$

where $c_i = c\varepsilon_i$ and $\varepsilon_i^d = 1$. We may also assume $c_1 = c$.

If $k = 1$ then there are at most $(q-1)\, d^{n-1}$ choices for X and thus at most d^{n-1} choices for $\overline{L}$, up to $\mathrm{PGL}(n, q)$-conjugacy.

If $k > 1$ there are at most $(q-1)\, d^{\frac{n}{k}-1}$ choices for X.

So, summing over all k's, the choices for $\overline{L}$ are at most

$$d^{n-1} + \sum_{1 < k \mid d} (q-1)\, d^{\frac{n}{k}-1}. \tag{2}$$

Note that $d^{n-1} + \sum_{1 < k \mid d} (q-1)\, d^{\frac{n}{k}-1} \leqslant (q-1)\dfrac{d^{n-1}-1}{d-1}$.

We now have that $\overline{L}^{\tau^\varepsilon \phi^s \overline{M}} = \overline{L}^t$. Once we have fixed one element $\overline{M}$ with that property, all the others can be obtained by multiplying $\overline{M}$ by an element of the centralizer $\overline{Z}$ of $\overline{L}^{\tau^\varepsilon \phi^s}$ in $\mathrm{PSL}(n, q)$, and we may assume without loss of generality that $\overline{L}^{\tau^\varepsilon \phi^s}$ has prime order u.

Using theorems 4.8.1, 4.8.2 and 4.8.4 of [4] for u odd and Table 4.5.1 of [4] for $u = 2$ and some easy calculations it is possible to see that an upper bound for the order of $\overline{Z}$ is $|\mathrm{GL}(n-1, q)|$. We now have to check that $d(q-1)\dfrac{d^{n-1}-1}{d-1}|\mathrm{GL}(n-1, q)| < |\mathrm{PSL}(n, q)|$, which is true for $n \geqslant 4$ because $d^2(q-1)^2\dfrac{d^{n-1}-1}{d-1} < (q^n - 1)\, q^{n-1}$. For $n = 3$ we use the more accurate bound (2).

Case III: $C \leqslant \mathrm{InnDiag}(G)\,\Gamma$, $n \geqslant 3$.

If C is cyclic we conclude by proposition 1.3. Otherwise we first choose a generator for $C' \cap \mathrm{InnDiag}(G)$, so that the number of possibilities is bounded by (2.6), then we argue as in case II.

Case IV: $n = 2$

If C is cyclic we conclude by proposition 1.3, otherwise we first choose a generator for $C' \cap \mathrm{InnDiag}(G)$, for which there is at most one possibility, by Table 4.5.1 of [4], and by lemma 1.2 there are less than $|G|$ choices for the second generator.

3. The unitary linear groups.

In this section, we will consider the group $G = {}^2A_{n-1}(q) = \mathrm{PSU}(n, q)$, for n and q fixed.

Let $K = \mathrm{GF}(q^2)$ be the finite field with q^2 elements, with $q = p^m$ for some prime number p. We fix a generator λ of the multiplicative group of the field $K^\times$. Then $\mathrm{GU}(n, q)$ (resp. $\mathrm{SU}(n, q)$) will denote the general (resp. special) unitary group of degree n, that is $\mathrm{GU}(n, q) = \{g \in \mathrm{GL}(n, q^2) \,|\, g(g^\top)^\sigma = 1\}$ where $\sigma = \phi^m \in \mathrm{Aut}(\mathrm{GL}(n, q^2))$, and $\mathrm{SU}(n, q) = \{g \in \mathrm{GU}(n, q) \,|\, \det(g) = 1\}$. All other notations, unless otherwise specified, are as in the previous section.

We may assume that C is non-cyclic, otherwise we conclude by proposition 1.

Let $C = \langle \phi^r \overline{N}_1, \overline{U}_1 \rangle$, with $\overline{U}_1, \overline{N}_1 \in P\mathrm{GU}(n, q)$. We argue as in case B II of the special linear group.

We have that U is $\mathrm{GL}(n, q^2)$-conjugate to a block-diagonal matrix X whose blocks X_i have all the same dimension k and are of the form (1), where $c_i = c\varepsilon_i$, $\varepsilon_i^d = 1$ and we may also assume that $c_1 = c$.

By [10, p. 34] the matrix X as above is conjugate to an element of $\mathrm{GU}(n, q)$ if and only if it is similar to the matrix $((X^\top)^\sigma)^{-1}$.

So $c\varepsilon_i = (c\varepsilon_j)^{-q}$, for some j, which implies that $c^{q+1} = (\varepsilon_i \varepsilon_j^q)^{-1}$ and $c^{(q+1)^2} = 1$. Let $c = \lambda^u$. We have that $q^2 - 1 \,|\, u(q+1)^2$, so $q - 1 \,|\, u(q+1)$. As $(q+1, q-1) \leqslant 2$, it follows that $\frac{q-1}{2} \,|\, u$ and there are at most $2(q+1)$ choices for c. Moreover, again by [10, p. 34] two matrices are conjugate in $\mathrm{GU}(n, q)$ if and only if they are conjugate in $\mathrm{GL}(n, q^2)$, so it is enough to count the number of choices for the matrix $\overline{X}$ as above, and then to multiply by $d = |\mathrm{PGU}(n, q) : \mathrm{PSU}(n, q)|$.

As in case B II of the special linear group, the choices for $\overline{X}$ are at most

$$d^{n-1} + \sum_{1<k|d} 2(q+1)d^{\frac{n}{k}-1}. \tag{3}$$

Note that $d^{n-1} + \sum_{1<k|d} 2(q+1)d^{\frac{n}{k}-1} \leqslant 2(q+1)\dfrac{d^{n-1}-1}{d-1}$.

To bound the number of choices for the second generator, we look for an upper bound for the order of the centralizer $\overline{Z}$ of $\overline{U}$ in $\mathrm{PGU}(n, q)$. We may assume that $\overline{U}$ has prime order u.

We first assume that $(n, q) \notin \{(3, 2), (3, 5), (4, 3), (8, 3)\}$.

Using theorems 4.8.1, 4.8.2 and 4.8.4 of [4] for u odd and Table 4.5.1 of [4] for $u = 2$ and some easy calculations it is possible to see that an upper bound for the order of $\overline{Z}$ is $|\mathrm{GU}(n-1, q)|$.

So we have to prove that $2d(q+1)\dfrac{d^{n-1}-1}{d-1}|\mathrm{GU}(n-1, q)| < < |\mathrm{PSU}(n, q)|$.

As $\dfrac{d}{d-1} \leqslant 2$, this is true because $4(q+1)^2 d^n < (q^n - 1)q^{n-1}$.

If $(n, q) = (8, 3)$ we use the more accurate bound (3) and the fact that $|\overline{Z}| \leqslant |\mathrm{GU}(n-1, q)|$.

We now study the remaining cases.

I: Case $(n, q) = (3, 2)$, $d = 3$ is divided into 2 subcases according as $\overline{U}$ is diagonalizable or not. For each case, we have to consider the possible canonical forms for $\overline{U}$ and the order of their centralizers, and the result follows just by counting the possible choices.

II: Case $(n, q) = (3, 5)$, $d = 3$.

There are at most 15 possibilities for the choice of X and $15\cdot \cdot 3|\mathrm{GU}(2, 5)| < |\mathrm{PSU}(3, 5)|$.

III: Case $(n, q) = (4, 3)$, $d = 4$ is divided into 2 subcases according as $|\overline{U}|$ is equal to 2 or 4. For each case, we have to consider the possible canonical forms for $\overline{U}$ and the order of their centralizers, and the result follows just by counting the possible choices.

4. $B_l(q)$, $C_l(q)$ and $E_7(q)$.

Let $G \in \{B_l(q), C_l(q), E_7(q)\}$. We have that C is isomorphic to a subgroup $\overline{C}$ of $Z_2 \times Z_m$, with $Z_m = \langle \phi G \rangle$ and $\mathrm{Out\,Diag}(G) \leqslant Z_2$.

Then either C is cyclic, and we may apply proposition 1.3, or it is 2-generated, and it is possible to choose one generator of the form $\phi^r z$, with $z \in G$ and $(\phi^r z)^{\frac{m}{r}} = 1$, so proposition 1.5 applies.

5. $D_l(q)$, $l \neq 4$.

Case $p = 2$

In this case we have that C is isomorphic to a subgroup $\overline{C}$ of $Z_2 \times Z_m$, with $Z_m = \langle \phi G \rangle$ and $\mathrm{Out\,Diag}(G)\,\Gamma = Z_2$, and we argue as for the case $G = B_l(q)$ or $C_l(q)$.

Case $p \neq 2$

We have that C and its image $\overline{C}$ in $\mathrm{Out}(G)$ are isomorphic to a subgroup of $D_8 \rtimes Z_m$, with the following notation: $Z_m = \langle \phi G \rangle$ and $\mathrm{Out\,Diag}(G)\,\Gamma \leqslant D_8$. More precisely, if l is odd and $4 \mid q-1$ or if l is even then $\mathrm{Out\,Diag}(G)\,\Gamma = D_8 = \langle wG, \tau G \rangle$, where τ is the graph automorphism of order 2, $\overline{w} = wG$ has order 4, $\overline{w}^\tau = \overline{w}^{-1}$, $[\tau, \phi] = 1$, and $\overline{w}^\phi = \overline{w}$ unless l is odd and $4 \nmid p-1$, in which case $\overline{w}^\phi = \overline{w}^{-1}$.

If l is odd and $4 \nmid q-1$ then $\mathrm{Out\,Diag}(G)\,\Gamma = \langle xG, \tau G \rangle$ is elementary abelian, τ is the graph automorphism of order 2, $x \in \mathrm{InnDiag}(G)$. Also ϕ centralizes $\mathrm{Out\,Diag}(G)$.

Let $T = C \cap \mathrm{InnDiag}(G)\,\Gamma$, and let $\overline{T}$ be its image in $\mathrm{Out}\,G$. By proposition 1 we may assume that C is not cyclic, and it is easy to check that C splits over T.

Let $\overline{C} \nleqslant \mathrm{Out\,Diag}(G)\,\Gamma$.

I) Assume that it is possible to choose a generator of C modulo T of the form $\phi^r a$, with $a \in \mathrm{InnDiag}(G)$ and $(\phi^r a)^{\frac{m}{r}} = 1$.

If T is cyclic proposition 1.5 applies, so we may assume that T is not cyclic.

If C' is another complement, by proposition 1.1 we may assume that, up to $\mathrm{InnDiag}(G)$-conjugacy, a generator of C' modulo $C' \cap \mathrm{InnDiag}(G)\,\Gamma$ is $(\phi^r)^x$, for some $x \in \mathrm{InnDiag}(G)$, and we have at most $|\mathrm{InnDiag}(G) : G| \leqslant 4$ choices for it, up to G-conjugacy.

T is generated by two involutions u^x and v^x, that are of graph type or of inner-diagonal type, depending on which case we are considering. Moreover we may assume that u is of the form $\tau^\varepsilon y$, with $y \in G$ and $\varepsilon \in \{0, 1\}$, and such that $[\tau^\varepsilon y, \phi^r] = 1$, so $y \in D_l(p^r)$. We note that we may conjugate $\tau^\varepsilon y$ by elements of $D_l(p^r)$, which centralize ϕ^r.

From table 4.5.1 of [4] we deduce that both the number of $D_l(p^r)$-conjugacy classes of involutions of graph type and the number of $D_l(p^r)$-conjugacy classes of involutions of inner-diagonal type are bounded by $2(l+3)$. So there are at most $2(l+3)$ choices for u. Then we have to count the involutions v of a fixed type. There are at most $2(l+3)$ conjugacy classes, and each class contains at most $|\mathrm{InnDiag}(G)\,\Gamma : C_{\mathrm{InnDiag}(G)\,\Gamma}(g)| \leqslant 8\,|G\colon C_G(g)|$ elements, where g is any involution in the class considered. We choose g such that the index of $H = C_G(g)$ in G is maximum. So there are at most $2(l+3)\,|G:H|$ possibilities for the choice of v. So we just have to check that $4\cdot 32(l+3)^2\,|G:H| < |G|$, which is true because $128(l+3)^2 < |H|$ (the structure of H is also described in table 4.5.1 of [4]).

II) Assume that we are not in the previous case, so that $\overline{C}$ does not contain $\mathrm{OutDiag}(G)\,\Gamma$; in particular $|T| < 8$. Let $\phi^r z$ be a generator of C modulo T of order $\dfrac{m}{r}$, with $z \in \mathrm{InnDiag}(G)\,\Gamma \setminus \mathrm{InnDiag}(G)$. We have that $\dfrac{m}{r}$ is even, otherwise we replace $\phi^r z$ with $(\phi^r z)^4$, which is a generator of C modulo T of order $\dfrac{m}{r}$ and of the form $\phi^r x$ with $x \in G$.

If $T = \langle u \rangle$ has order 2 then we apply proposition 1. By table 4.5.1 of [4] we have at most $2(l+3)$ conjugacy classes of involutions of the same type as u; moreover, by Table 5.2 A of [p. 175] [7] the index of a maximal subroup of G is less than $2(l+3)$, so in this case the conclusion follows.

If T is cyclic of order 4, from the fact that we are not in case I it follows that $\overline{T} = \mathrm{OutDiag}(G)$ and we can conclude by proposition 1.6.

So we may assume that T is elementary abelian of order 4.

If l is even then $\overline{T} = \mathrm{OutDiag}(G)$ and as we are not in case I it follows that $\phi^r z$ does not centralize T, so we conclude by proposition 1.6.

Let l be odd. Note that we also have that $8 \mid q-1$, because m is even. As we are not in case I, one of the following occurs:

- $\bar{z} = \tau$ and $\overline{T} = \langle \overline{w}^2, \overline{w}\tau \rangle$, or
- $\bar{z} = \overline{w}\tau$ and $\overline{T} = \langle \overline{w}^2, \tau \rangle$.

To deal with these cases we always adopt the same strategy. We first count the number of choices for a generator of $T \cap \mathrm{InnDiag}(G)$, then we count the number of choices for a generator of T modulo $T \cap \cap\, \mathrm{InnDiag}(G)$, and finally we count the number of choices for a generator of C modulo T.

We describe the calculations in detail only for the first case.

Let C' be another complement of of G in H; then we may assume that it is of the form $C' = \langle \phi^r \tau u, w^2 v, w\tau x \rangle$, with $u, v, x \in G$.

By Table 4.5.1 of [4] we have at most $l-1$ choices for $w^2 v$, up to G-conjugacy. Moreover let $C^* = C_{\mathrm{InnDiag}(G)}(w^2 v)$ and $L^* = O^p(C^*)$. From table 4.5.1 of [4] it follows that

i) either $L^* = {}^2D_{l-1}(q)$ and $Z = C_{C^*}(L^*) = C_{\mathrm{InnDiag}(G)\,\Gamma_k}(L^*)$ has order $q+1$ or

ii) $L^* = D_i(q) \times D_{l-i}(q)$ or $L^* = {}^2D_i(q) \times 2D_{l-1}(q)$, where $2 \leqslant i < \frac{l}{2}$ and $Z = C_{C^*}(L^*) = C_{\mathrm{InnDiag}(G)\,\Gamma_k}(L^*)$ has order 2.

We first deal with case ii). Note that $w\tau x$ centralizes $w^2 v$, so it normalizes L^*. Let $(y_1, y_2) \in \mathrm{Aut}({}^\varepsilon D_i(q)) \times \mathrm{Aut}({}^\varepsilon D_{l-i}(q))$ be the image of $w\tau x$ in $\mathrm{Aut}(L^*)$. The number of choices for $w\tau x$, up to G-conjugacy, is bounded by $|Z| r_1 r_2$, where $r_1 - 1$ is the number of ${}^\varepsilon D_i(q)$-conjugacy classes of involutions in $\mathrm{InnDiag}({}^\varepsilon D_i(q))\,\Gamma$ (we have to add one because y_1 might be the identity) and $r_2 - 1$ is the number of ${}^\varepsilon D_{l-i}(q)$-conjugacy classes of involutions in $\mathrm{InnDiag}({}^\varepsilon D_{l-i}(q))\,\Gamma$. Again by table 4.5.1 of [4] we have that $r_1, r_2 \leqslant 6l + 25$.

Note: For $i = 2, 3$ it is easy to check that $r_1, r_2 \leqslant 6l + 25$ is still true (see [p. 11] [4] and [p. 43] [7] for the description of D_i in these cases).

So there are at most $2(6l+25)^2$ choices for $w\tau x$.

We now have to choose $\phi^r \tau u$. Note that once we have fixed $\phi^r \tau u$ with the required properties, any other element of the form $\phi^r \tau u'$ is such that $(\phi^r \tau u)^{-1} \phi^r \tau u' \in C_G(w^2 v)$, so we have at most $|C_G(w^2 v)|$ choices for the third generator.

A similar argument applies to case i).

To conclude, we have that the number of complements for G in H is at most $(l-1)\,2(6l+25)^2\,|U|$, where U is a maximal subgroup of G, and this number is less than $|G|$, as by Table 5.2 A of [p.175] [7] the index of a maximal subgroup of G is at least $\dfrac{(q^l-1)(q^{l-1}+1)}{q-1}$ and $2(l-1)(6l+25)^2 < \dfrac{(q^l-1)(q^{l-1}+1)}{q-1}$ (here $l \geqslant 5$ and $q \geqslant 9$).

Let $\overline{C} \leqslant \mathrm{OutDiag}(G)\,\Gamma$.

Then C is generated by two involutions u and v, that are of graph type or of inner-diagonal type, depending on which case we are considering, and we argue as in Case I above.

6. $D_4(q)$.

In this case we have that $\mathrm{OutDiag}(G) = 1$ if $p = 2$, otherwise $\mathrm{OutDiag}(G) = \langle \bar{z} \rangle \times \langle \bar{w} \rangle$ is elementary abelian of order 4 and it is centralized by ϕ. Also, $\Gamma = \langle \tau, \gamma \rangle$ is isomorphic to S_3 with $|\tau| = 2$, $|\gamma| = 3$, $\bar{w}^\tau = \bar{w}\bar{z}$, $\bar{z}^\tau = \bar{z}$, while $(\mathrm{InnDiag}(G)\,\Gamma)/G$ is isomorphic to S_4 and is centralized by ϕ.

Let $T = C \cap \mathrm{InnDiag}(G)\,\Gamma$, and let $\bar{T}$ be its image in $\mathrm{Out}\,G$. By proposition 1.3 we may assume that C is not cyclic, and it is easy to check that C splits over T.

Case: $C \nleq \mathrm{InnDiag}(G)\,\Gamma$

I) Assume that it is possible to choose a generator $\phi^r u$ of C modulo T of order $\dfrac{m}{r}$ and with $u \in \mathrm{InnDiag}(G)$.

If T is cyclic we conclude by proposition 1.5, so we may assume that T is not cyclic.

Assume that p is odd. By proposition 1.1 we have at most 4 possibilities for the choice of $\phi^r u$, up to G-conjugacy, and we may assume that it is of the form $(\phi^r)^x$ for some $x \in \mathrm{InnDiag}(G)$.

We may also assume that one generator of T is an involution y^x such that y centralizes ϕ^r. As we may conjugate y^x by elements of the form $w^x \in G$, where w centralizes ϕ^r, the choices for y are bounded by the number of G-conjugacy classes of non-inner involutions of fixed type in $\mathrm{InnDiag}(D_4(p^r))\,\Gamma$, which by table 4.5.1 of [4] is at most 24. The second generator of T is an element of $\mathrm{InnDiag}(D_4(p^r))\,\Gamma$ and we have that $96\,|\mathrm{InnDiag}(D_4(p^r))\,\Gamma| < |G|$, as we wanted.

If $p = 2$ then by proposition 1.1 we have at most one possibility for the choice of $\phi^r u$, up to conjugacy; we therefore take $x = 1$. Moreover, T is generated by a graph automorphism y of order 3, and a graph type involution v, which both centralize ϕ^r. Arguing as above and using table 4.7.3A of [4] we find that there are at most $16\,|\mathrm{InnDiag}(D_4(2^r))\,\Gamma| < |G|$ choices, as we wanted.

II) Assume that we are not in the previous case and let $\phi^r a$ be a generator of C modulo T of order $\dfrac{m}{r}$ with $a \in \mathrm{InnDiag}(G)\,\Gamma$, $a \notin \mathrm{InnDiag}(G)$.

If T is cyclic, as we are not in case I it is easy to see that T has order 2 or 3.

If $T = \langle y \rangle$ has order 3 then y is of graph type. We now apply proposition 1.7. By table 4.7.3A of [4] if $p \neq 3$ and by proposition 4.9.2 (b5) and (g) of [4] if $p = 3$ we have at most 16 G-conjugacy classes of type graph elements of order 3. Moreover, by Table 5.2 A of [p. 175] [7] the index of a maximal sbgroup of G is at least $\dfrac{(q^l - 1)(q^{l-1} + 1)}{q - 1} > 16$, so we have what we wanted.

If T has order 2 we argue as follows. By proposition 1.1 we have at most 4 possibilities for the choice of the first generator, up to G-conjugacy. Once we have fixed the first generator, say $\phi^r au$, the second generator b has the property that $[\phi^r au, b] = 1$. Thus the possible choices for the second generator are given by elements of the type bv, with $v \in G$, such that $[\phi^r au, bv] = 1$, so that $v \in C_G(\phi^r au)$. It follows that we have at most $4\,|C_G(\phi^r au)| < |G|$ choices, as we wanted (note that $C_G(\phi^r au)$ is a proper subgroup of G, so that its index is greater than 4).

Now we may assume that T is not cyclic. As we are not in case I it follows that $\mathrm{OutDiag}(G) \leqslant \overline{T}$ and that $T = \langle y, y^{\phi^r a}\rangle$ for some y in T, where y has order 2 or 3, so that $C = \langle \phi^r a, y\rangle$. Now proposition 1.6 allows us to conclude.

Case: $C \leqslant \mathrm{InnDiag}(G)\,\Gamma$

We first assume that $p = 2$. Then $C = \langle x, y\rangle \cong \Gamma$, where x and y are both of graph type, $|x| = 3$, $|y| = 2$ and $x^y = x^{-1}$. By table 4.7.3A of [4] there are at most 4 G-conjugacy classes of type graph elements of order 3. By proposition 1.7 there are at most $4\,|Z|$ conjugacy classes of complements for G in H, where Z is a maximal subgroup of G. To conclude, we note that by Table 5.2A of [p. 175] [7] we have that $4 < |G : Z|$.

We now assume that p is odd.

I) If $C \cong \mathrm{OutDiag}(G)\,\Gamma$ then C is isomorphic to either S_4 or S_3 and it is generated by 2 elements x and y of graph type, with $|x| = 3$ and $|y| = 2$.

By table 4.7.3A of [4] if $p \neq 3$ and by proposition 4.9.2 (b5) and (g) of [4] if $p = 3$ there are at most 16 G-conjugacy classes of type graph elements of order 3. Also, there are at most 6 $\mathrm{InnDiag}(G)$-conjugacy classes of involutions of graph type, and if g is a graph type involution such that $H = C_{\mathrm{InnDiag}(G)}(g)$ has minimum order, there are at most $6\,|\mathrm{InnDiag}(G) : H| \leqslant 24\,|G : G \cap H|$ choices for y. As $|H \cap G| > 16 \cdot 24$, it follows tht $16 \cdot 24\,|G : G \cap H| < |G|$. (The structure of $G \cap H$ is given in table 4.5.1 of [4].)

II) In the remaining cases, we have that $C = \langle x, y \rangle$ where $|x| = 2$, $x \in \mathrm{InnDiag}(G) \backslash G$ and $|y| \in \{2, 3\}$ and the type of y is known (either $y \in \mathrm{InnDiag}(G) \backslash G$ or y is of graph type). Arguing as in case I, by tables 4.5.1 and 4.7.3A and proposition 4.9.2 of [4], there are at most 6 choices for x, up to G-conjugacy, and at most $24\,|G : G \cap H|$ choices for y, where $H = C_{\mathrm{InnDiag}(G)}(g)$ for some g such that g has the same order and type of y. As $|H \cap G| > 6 \cdot 24$, it follows that $6 \cdot 24\,|G : G \cap H| < |G|$. (The structure of $G \cap H$ is given in table 4.5.1 of [4].)

7. ${}^2D_l(q)$.

If $p = 2$ we have that C is cyclic, so we may assume that p is odd.

Cases: l even or l odd and $4 \nmid q + 1$

We have that C is isomorphic to a subgroup $\overline{C}$ of $Z_2 \times Z_{2m}$, with $Z_2 = \langle aG \rangle$ and $Z_{2m} = \langle \phi \rangle$, where $a \in \mathrm{InnDiag}(G)$.

We have that $C = \langle y, \phi^r u \rangle$ where $y \in \mathrm{InnDiag}(G) \setminus \mathrm{Inn}(G)$ has order 2 and is centralized by $\phi^r u$, so we may apply proposition 1.7. By Table 4.5.1 of [4] there are at most $l - 1$ conjugacy classes of non-inner inner-diagonal involutions, and by Table 5.2A of [p. 175] [7], the index of a maximal subgroup of G is bigger than $l - 1$. This allows us to conclude.

l odd, $4 \,|\, q + 1$

In this case $4 \,|\, p + 1$ and m is odd. We have that C is isomorphic to a subgroup of $Z_4 \rtimes Z_{2m}$, with $Z_4 = \langle aG \rangle$ and $Z_{2m} = \langle \phi \rangle$, where $a \in \mathrm{InnDiag}(G)$. Moreover $(aG)^{\phi} = (aG)^{-1}$.

If $C \cap \mathrm{InnDiag}(G)$ has order 2 we argue exactly as in the previous case.

So we may assume that $C \cap \mathrm{InnDiag}(G)$ has order 4, and that any other complement C' is of the form $C' = \langle x, \phi^r y \rangle$, where $x \in \mathrm{InnDiag}(G)$ has order 4, $x^2 \in \mathrm{InnDiag}(G) \setminus \mathrm{Inn}(G)$ and $x\,\phi^r y = x^{(-1)^r}$.

We argue in a similar way as for a subcase of $D_l(q)$.

By Table 4.5.1 of [4] we have at most $\dfrac{l+1}{2}$ choices for x^2, up to G-conjugacy. Moreover let $C^* = C_{\mathrm{InnDiag}(G)}(x^2)$ and $L^* = O^p(C^*)$. From table 4.5.1 of [4] it follows that L^* is one of the following:

i) $L^* = {}^2D_{l-1}(q)$ and $Z = C_{C^*}(L^*) = C_{\mathrm{InnDiag}(G)}(L^*)$ has order $q-1$;

ii) $L^* = {}^2D_i(q) \times D_{l-i}(q)$, where i is even, $i \in \{2, \ldots, l-3\}$, and $Z = C_{C^*}(L^*) = C_{\mathrm{InnDiag}(G)}(L^*)$ has order 2;

iii) $L^* = \mathrm{SU}(l, q)$, $C^* = \mathrm{GU}(l, q)$ and $Z = C_{C^*}(L^*) = C_{\mathrm{InnDiag}(G)}(L^*)$ has order $q+1$.

We note that the case $L^* = {}^2D_i(q) \times D_{l-i}(q)$, where i is odd occurs only if x^2 is inner, which is not our case. To see this, note that $G \cong P\Omega^-(2l, q)$, and we may assume that the matrix associated to the symmetric bilinear form is the identity. We then have that in this case x^2 is the image in $P\Omega^-(2l, q)$ of the matrix $diag(-1, \ldots, -1, 1, \ldots, 1)$, where the number of entries equal to -1 is $2i$, and then by proposition 2.5.13 of [7] x^2 is inner.

We first deal with case ii). Note that x centralizes x^2, so it normalizes L^*. Let $(y_1, y_2) \in \mathrm{Aut}({}^2D_i(q)) \times \mathrm{Aut}(D_{l-i}(q))$ be the image of x in $\mathrm{Aut}(L^*)$. We note that (y_1, y_2) has order 2, so the number of choices for x, up to G-conjugacy, is bounded by $|Z| r_1 r_2$, where $r_1 - 1$ is the number of ${}^2D_i(q)$-conjugacy classes of involutions in $\mathrm{InnDiag}({}^2D_i(q))\,\Gamma$ (we have to add one because y_1 might be the identity) and $r_2 - 1$ is the number of $D_{l-i}(q)$-conjugacy classes of involutions in $\mathrm{InnDiag}(D_{l-i}(q))\,\Gamma$. Again by table 4.5.1 of [4] we have that $r_1 \leqslant 3i+1$, $r_2 \leqslant 3(l-i)+9$.

Note: it is easy to check that for $i = l-3$ it is still true that $r_2 \leqslant 3(l-i)+9$, and the same holds for $i=2$ and $r_1 \leqslant 3i+1$ (see [p. 11] [4] and [p. 43] [7] for the description of D_i in these cases).

As the maximum of the function $f(z) = (3z+1)(3l-3z+9)$ is $\frac{9}{4}l^2 + 15l + 25$, once we have fixed x^2 in case ii) there are at most $\frac{9}{2}l^2 + 30l + 50$ choices for x.

A similar argument applies to case i), and we get at most $4(3l+6) < \frac{9}{2}l^2 + 30l + 50$ choices for x.

We are left with case iii). In this case x is a unitary matrix of order 4. Arguing as in section 3, as l is odd we have that x is conjugate in $\mathrm{GU}(l, q)$ to a diagonal matrix whose entries on the diagonal are of the form ε^i, where ε is a primitive 4-th root of 1. Moreover, if $GF(q^2)^\times = \langle \lambda \rangle$, we have that $\mathrm{diag}(\lambda^{q-1}, 1, \ldots, 1)$ is a unitary matrix centralizing x, so that the number of $\mathrm{SU}(l, q)$ conjugacy classes for x is at most $4^l - 2^l$.

Now we apply proposition 1.7. By table 5.2 A of [p. 175] [7] the index of a maximal subgroup of G is at least $\dfrac{(q^l+1)(q^{l-1}-1)}{q-1}$, which is greater than $\dfrac{l+1}{2}\max\left\{\dfrac{9}{2}l^2+30l+50,\ 2^l(2^l-1)\right\}$.

8. $E_6(q)$.

We have that C is isomorphic to a subgroup $\overline{C}$ of $\mathrm{Out}(G) \leqslant S_3 \rtimes Z_m$, with $Z_m = \langle \phi G\rangle$, $S_3 = \langle aG, \tau G\rangle$, $|aG| = 3$, $|\tau| = 2$, $(aG)^{\tau G} = (aG)^{-1}$, $\mathrm{OutDiag}(G) \leqslant \langle aG\rangle$ and $\Gamma(G) = \langle \tau\rangle$. Also, ϕ centralizes τ and either inverts or centralizes aG.

By proposition 1.3 we may assume that C is not cyclic.

Let $\overline{C} \not\leqslant \mathrm{Out\,Diag}(G)\,\Gamma$, $T = C \cap \mathrm{InnDiag}(G)\,\Gamma$.

I) Assume that it is possible to choose a generator $\phi^r x$ of C modulo T of order $\dfrac{m}{r}$ and with $x \in \mathrm{InnDiag}(G)$.

By proposition 1.1 we have at most 3 possibilities for the choice of $\phi^r x$, up to conjugacy. Moreover, by proposition 1.5 we may assume that $\overline{T} = \mathrm{OutDiag}(G))\,\Gamma$.

We have that T is generated by a graph-type involution u centralizing a suitable conjugate of ϕ^r and an element $v \in \mathrm{InnDiag}(G)\setminus \mathrm{Inn}(G)$ of order 3. We now argue as in the analogue of this case for $D_l(q)$.

By Table 4.5.1 and proposition 4.9.2 (b)(4) and (f) of [4] there are at most 2 choices for u, up to G-conjugacy. By table 4.7.3A of [4] there are at most 8 G-conjugacy classes of elements of order 3 in $\mathrm{InnDiag}(G)\setminus \mathrm{Inn}(G)$, and each of them has at most $|\,\mathrm{InnDiag}(G) : C_{\mathrm{InnDiag}(G)}(g)\,|$ elements, where g is an element of one of those classes such that $C_G(g)$ has minimum order. To conclude, it is enough to note that $|C_G(g)\,| > 48$.

II) It is easy to see that if we are not in the previous case then it is possible to choose a generator $\phi^r z$ of C modulo T of order $\dfrac{m}{r}$ and with $z \in \mathrm{InnDiag}(G)\,\Gamma$. Moreover, T is cyclic of order 3, so proposition 1.7 applies. By Table 4.7.3A of [4] the number of G-conjugacy classes of elements of order 3 in $\mathrm{InnDiag}(G)\setminus \mathrm{Inn}(G)$ is at most 8, which is less than the index of a maximal subgroup of G.

Let $C \leqslant \mathrm{InnDiag}(G)\,\Gamma$.

We have that C is generated by a graph-type involution u and an element $v \in \mathrm{InnDiag}(G) \setminus \mathrm{Inn}(G)$ of order 3 and we argue as in case I.

9. $^2E_6(q)$.

We have that C is isomorphic to a subgroup $\overline{C}$ of $\mathrm{Out}(G) \leqslant Z_3 \rtimes Z_m$, with $Z_m = \langle \phi G \rangle$ and $Z_3 = \langle aG, \tau G \rangle$ and $a \in \mathrm{InnDiag}(G)$.

By proposition 1.3 we may assume that C is not cyclic, so that $C = \langle y, \phi^r z \rangle$, where $z \in \mathrm{InnDiag}(G)$; also $y \in \mathrm{InnDiag}(G) \setminus \mathrm{Inn}(G)$ has order 3 and it is normalized by $\phi^r z$.

By table 4.7.3A of [4] there are at most 8 G-conjugacy classes of type graph elements of order 3. By proposition 1.7 there are at most $8|Z|$ conjugacy classes of complements for G in H, where Z is a maximal subgroup of G. To conclude, we note that by Table 5.2A of [p. 175] [7] we have that $8 < |G : Z|$.

REFERENCES

[1] M. Aschbacher - R. Guralnick, *Some applications of the first cohomology group*, J. Algebra, **90** (1984), pp. 446-460.

[2] R. W. Carter, *Finite groups of Lie type. Conjugacy classes and complex characters*. Pure and Applied Mathematics. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1985.

[3] J. Dieudonné, *La géométrie des groupes classiques*, Seconde édition, revue et corrigée. Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[4] D. Gorenstein - R. Lyons - R. Solomon, *The Classification of the finite simple groups.* Number 3. Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.

[5] N. Jacobson, *The Theory of Rings.* American Mathematical Society Mathematical Surveys, vol. I. American Mathematical Society, New York, 1943.

[6] F. Gross - L. G. Kovács, *On normal subgroups which are direct products*, J. Algebra, **90** (1984), pp. 133-168.

[7] P. Kleidman - M. Liebeck, *The subgroup structure of the finite classical groups.* London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

[8] A. Lucchini - F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Sem. Mat. Univ. Padova, **98** (1997), pp. 173-191.

[9] A. Lucchini - F. Morini, *On the probability of generating finite groups with a unique minimal normal subgroup*, Pacific J. Math., **203** (2002), pp. 429-440.

[10] G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Australian Math. Soc., **3** (1965), pp. 1-62.

Manoscritto pervenuto in redazione l'8 gennaio 2004.