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 $N = \text{soc} \ H$ is abelian, the conjugacy classes of complements of $N$ in $H$ are in bijective correspondence with the elements of the first cohomology group $H^1(H/N, N)$. Using the classification of finite simple groups, Aschbacher and Guralnick [1] proved that $|H^1(H/N, N)| < |N|$; therefore, when $\text{soc} \ H = N$ is abelian, there are at most $|N|$ conjugacy classes of complements of $N$ in $H$. To study the case when $N = \text{soc} \ H$ 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 $c \leq 4$ 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 $G \cong \text{Inn}(G)$, we may identify $G$ with $\text{Inn}(G)$. We will prove the following

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

When $G = \text{Alt}(n)$ with $n \neq 6$ or $G$ is a sporadic simple group, it is well known that $|H:G| \leq 2$; if $H \ncong G$, 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 $G = \text{Alt}(6) \cong \text{PSL}(2, 9)$ 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, $\phi$ denotes the Frobenius map and $\Gamma$ denotes the group of graph automorphisms of $G$.

If $G$ has no complement in $\text{Aut}(G)$ 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 $\text{Out}(G)$, 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 $xu_i, yu_i, zu_i$ 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 $\phi' a \in \text{Aut}(G)$, with $a \in \text{InnDiag}(G)\Gamma$, and assume that $|\phi' a| = m/r$. If $x \in \text{InnDiag}(G)$ is such that $|\phi' ax| = m/r$ then $\phi' a$ and $\phi' ax$ are $\text{InnDiag}(G)$-conjugate.

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

Let $r_x$ be the inner automorphism of $\mathcal{G}$ induced by $x$. There exists $a \in \text{Aut}(\mathcal{G})$ such that $a$ is the product of a graph automorphism and an inner automorphism, and $a$ induces $a$ on $G$. We note that $(\phi' a)^{m/r} = (\phi' a)^{m/r} = \phi^w$. So $\phi' a$ is a surjective homomorphism $\psi$ of $\mathcal{G}$ whose set of fixed points in $\mathcal{G}$ is finite. By the Lang-Steinberg theorem (see [Theorem 2.1.1] [4]) there exists $w \in \mathcal{G}$ such that $x = (w^{-1})^w \psi$.

Let $s = m/r$. We have that: $\phi^w = (\psi r_x)^w = \psi r_x r_x^{-1} r_x^{w-2} \cdots r_x^w r_x^{-1} = \phi^w r_x r_x^{-1} r_x^{w-2} \cdots r_x^w r_x = 1$. As $x = (w^{-1})^w \psi$ we obtain that $(r_x)^{w-1} r_x = 1$, so $r_x^{w-1} r_x^{-1} = 1$, that is $w \in \text{InnDiag}(G)$.

It follows that $(\phi' a)^w = w^{-1} \phi' a w = \phi' a(w^{-1})^w = \phi' a(w^{-1})^w = \phi' a$, 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 $a \in \text{Aut}(G)$ 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, $G \leq H \leq \text{Aut}(G)$ 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: $^3D_4(q), G_2(q), F_4(q), E_6(q), ^2F_4(q)$ or $^4G_2(q)$ and let $G \leq H \leq \text{Aut}(G)$. 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 $C = \langle \phi^*a, b \rangle$, with $a \in \text{InnDiag}(G)$, $b \in \text{InnDiag}(G) \backslash \text{Inn}(G)$ and $|\phi^*a| = |\phi^*|$. 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 $\phi^*ag$, with $g \in G$ and $|\phi^*ag| = |\phi^*a| = |\phi^*|$, so by proposition 1.1 we have at most $d = |\text{InnDiag}(G) : G|$ choices for it, up to G-conjugation. Moreover, again by proposition 1.1, we may assume that $\phi^*ag = (\phi^*)^x$ for some $x \in \text{InnDiag}(G)$. So $C' = \langle \phi^*, (bv)^{x^{-1}} \rangle$, 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 $\phi^*$ in G. If $G = \Sigma_1(q)$ then $\Sigma_1(p) \leq \text{Inn}(\phi^*)$. We have that $[yu, \Sigma_1(p)] \neq 1$ (see [Lemma 2.5.7] [4]), so that $C_{\Sigma_1(p)}(yu)$ is a proper subgroup of $\Sigma_1(p)$. As the index of a maximal subgroup of $\Sigma_1(p)$ is at least $d$ (see Table 5.2 A of [p. 175] [7]) each orbit of the set $\{yu | u \in G\}$ under the action of $\Sigma_1(p)$ 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 $C = \langle \phi^*a, b \rangle$, with $a, b \in \text{InnDiag}(G) \backslash \text{Inn}(G)$ and $|\phi^*a| = |\phi^*|$. 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 $(\phi^*)^x$, for some $x \in \text{InnDiag}(G)$. Let $C' = \langle (\phi^*)^x, bv \rangle$, where $u \in G$. As $\text{InnDiag}(G) \leq H = GC'$ we have that $x = yz$ for some $z \in G$ and some $y \in C'$, so that $C' = \langle (\phi^*)^z, (bv)^{y^{-1}} \rangle$ is G-conjugate to a complement of the form $C'' = \langle (\phi^*)^z, v \rangle$. 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).
Complements of the socle etc. 145

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 $a^k = a^t$ 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 $(au)^{bv'} = (au)^{bv''}$ 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 $PGL(n, q) = GL(n, q)/K^\times$, $PSL(n, q) = SL(n, q)K^\times/K^\times$ and if $g \in GL(n, q)$ its image in $PGL(n, q)$ will be denoted with $\overline{g}$. Also, as usual, $\det(g)$ will indicate the determinant of a matrix $g$ and $\text{diag}(a_1, \ldots, a_n)$ will denote a diagonal matrix, whose entries on the diagonal are those listed between the brackets.

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

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

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

We have that $C$ is isomorphic to a subgroup of $Out(G) = \langle \phi G, \tau G, aG \rangle$, where $a \in PGL(n, q)$, $(aG)^\phi = a^\phi G, (aG)^\tau = a^{-1}G$, $[\phi G, \tau G] = 1$ 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 $n \geq 4$ is even.

We may assume that $C = \langle \phi^{*}N_1, rM_1, U_1 \rangle$, where $M_1, N_1, U_1 \in GL(n, q)$ and $r|m$. Also we have that $U_1$ has order $d'$, with $2 | d' | d$ and we also have that $(\phi^{*}N_1)^{mir} \in \langle U_1 \rangle$.

Lemma 2.1. In the above setting, we may also assume that $[\phi^{*}N_1, rM_1] = 1$ and $rM_1$ has order 2.

Proof. As $C$ is isomorphic to a subgroup of Out($G$), it will be isomorphic to a subgroup $T$ of the group $X = \langle a, b, c | a^d = b^{2^r} = c^m = 1, a^k = = a^{-1}, a^r = a^r, b^r = b \rangle$ where $p$ is a prime and $p^m \equiv 1 \mod d$. 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 $b \not\in T$ and $ba \in T$. Note that $C_X(ba) = \langle a^{q_2}, ba, u \rangle$ 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 $T \cap \langle a, b \rangle$ if $p \not= 2, l, d, m/k$ are even, $\frac{p^m-1}{d}$ 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: $(\phi^{*}N_1)^{mir} = 1$

We may assume that another complement $C'$ for $G$ in $H$ is generated by $\phi^{*}N_1 X, rM_1 U$, with $X \in G, M_1, U \in PGL(n, q)$, satisfying the same relations as $\phi^{*}N_1, rM_1, U_1$. In particular $(\phi^{*}N_1 X)^{mir} = 1$, so by proposition 1.1 there are at most $d$ possibilities for the choice of $\phi^{*}N_1 X$, up to conjugation by elements of $G$. Moreover, again by proposition 1.1, we have that $\phi^{*}N_1 X = (\phi^{*})^S$, with $S \in PGL(n, q)$. Changing no-
tations for the last two generators, we may now assume that $C' = \langle \phi' \rangle^5$, $(\tau M)^5$, $(U)^5$.

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

From the fact that $[\phi', \tau M] = 1$ it follows that $M^{\phi'} = \beta M$, with $\beta \in K$. This implies that $m_{ij}^{\phi'} = \beta$ 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 $m_{ij} m_{hk}^{-1} \in \Gamma(p')$, i.e., $m_{ij} = m_{hk} m_{ij}'$ for some $m_{ij}' \in \Gamma(p')$. It follows that $M = \tau m_{bk} M'$, with $M' \in \Gamma(n, p')$. Choosing $M'$ instead of $M$ as a pre-image of $M$ we may assume that $M \in \Gamma(n, p')$.

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 $H$ of $G$ centralizing $\phi'$, that is $H \in \Gamma(n, p')$. Note that in that case we have that $(\tau M)^H = \tau H^T \tau M H$, and by [3] there exists $H \in \Gamma(n, p')$ such that $H^T M H$ has one of the following forms: identity, diag($a, 1, \ldots, 1$), where $a$ is a non-square in $\Gamma(p')$, 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 $\Gamma(n, q)$ and not in $\Gamma(n, q)$, we have at most $3d$ possibilities for $M$.

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

Case II: $(\phi' N_1)^{\phi'} \neq 1$

In this case $\frac{m}{r}$ is even. Actually, if $\frac{m}{r}$ is odd, putting $x = \tau M_1$, $y = \phi' N_1$, if $m = 2s$, with $\frac{m}{r} | s$, then $C = \langle x, x^{\phi'}, y, U \rangle = \langle x^{\phi'}, U \rangle$, as $y^{\phi'} \in \langle y^{\phi'} \rangle \in (U)$. So $C$ is 2-generated, contradicting the assumptions.

Again, we may assume that another complement $C'$ is generated by $\phi' N$, $\tau M$, $U$, satisfying the same relations as $\phi' N_1$, $\tau M_1$, $U_1$. In particular $(\tau M)^2 = 1$. As in Case I, it follows that $M$ is symmetric or skew-symmetric, and conjugating by a suitable element of $\Gamma(n, q)$ we have at
most 3d possibilities for $\mathcal{M}$. Namely, we may assume that $\tau \mathcal{M}$ is of one of the following types:

i) $\tau ^3$,

ii) $(\tau A)^3$, with $A = \text{diag}(a, 1, \ldots, 1)$, where $a$ is a non-square in $K$,

iii) $(\tau B)^3$, 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 $C' = = \langle (\phi ' N)^3, (\tau \mathcal{M})^3, (U)^3 \rangle$, with $\mathcal{M} \in \{T, A, B\}$. Also, there is no loss in generality in assuming $S = 1$, as this does not affect calculations.

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

In cases i) and iii) we have that $(\tau M, \phi ' N) = [\tau \mathcal{M}, N] = 1$, so that $N^2 = \mathcal{M} = N$. It follows that $(N^{-1})^T = \gamma N$, 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 $\frac{m}{r}$ is even and $p$ is odd it follows that $2 \mid \frac{p^r - 1}{p^r - 1}$, so that $\det(L) = \mu^{p^r - 1} \in K^n$, which implies that $(\phi ' N)^{\mu/r} \in C \cap G = 1$ and $(\phi ' N)^{\mu/r} = (\phi ' N)^{\mu/r} = 1$, a contradiction.

We now deal with case ii). From $[(\tau A), (\phi ' N)] = 1$ it follows that $N^2 = \bar{A}^T \bar{N}$, so that $N^{-1} = \gamma A^\phi N^{-1}$, with $\gamma \in K^\times$ and $\mu^2 = a^r - a^r \gamma^{-n}$.

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

We distinguish two subcases:

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

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

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

By our hypothesis, there exists $R$ such that $(rV)^{R^{-1}}$ is of the form $rA$, with $A = \text{diag}(a, 1, \ldots, 1)$, where $a$ is a non-square in $K$.

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

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

This means that, fixed $\gamma$, $U$ 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 $\frac{2}{q-1} q^{n-1}$ choices for $U$.

Putting all together, the number of conjugacy classes of complements for $G$ in $H$ is at most $d \frac{n}{2} |\text{PGL}(n, p^{m/2})| \frac{2}{q-1} q^{\frac{n(n+1)}{2}} < |\text{PSL}(n, q)|$.

(Here we have used that $8 | n$, because $m$ is even, so that $8 | q - 1$ and $\frac{q-1}{d}$ is odd).

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

As $(\phi'^{m/2}N)\phi' = L$ 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 $\begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}$, with $\gamma \in K^\times$ (second type). By [p. 50] [5], by conjugating by a suitable element of $\text{GL}(n, q)$ we may assume that $N$ is block-diagonal matrix, whose blocks $N_i$ on the diagonal are of the form

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

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

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 $L_j$ 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 $L_j = \begin{pmatrix} b^{p^{\frac{n}{2}}} & ab^{p^{\frac{n}{2}}} \\ a^{p^{\frac{n}{2}}} & b + a^{p^{\frac{n}{2} + 1}} \end{pmatrix}$, $-\det(L_j) = -b^{p^{\frac{n}{2} + 1}}$ 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

\[
L_j = \begin{pmatrix} 1 & a^{p^{\frac{n}{2}}} \\ 1 & b^{p^{\frac{n}{2}}} \\ 1 & c^{p^{\frac{n}{2}}} \\ 1 & d^{p^{\frac{n}{2}}} \end{pmatrix} = \begin{pmatrix} a^{p^{\frac{n}{2}}} & \star \\ b^{p^{\frac{n}{2}}} & \star \\ c^{p^{\frac{n}{2}}} & \star \\ d^{p^{\frac{n}{2}}} & \star \end{pmatrix}.
\]

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

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

It follows that $L$ is diagonal.

So we have at most $\frac{n}{2}$ choices for $L$ and thus at most $\frac{n}{2}$ choices for $\phi^{p^{\frac{n}{2}}N}$, up to $\text{PGL}(n, q)$-conjugation. As we are counting $\text{PSL}(n, q)$-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 $L_1 = \gamma I_n$ and $L_2 = -\gamma I_n$, for some $\gamma$.
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 $L \notin \text{PSL}(n, q)$. Moreover, as $8 \mid n$, we have that $r_1 \neq \frac{n}{2} \neq r_2$.

We have that $M, N$ and $U$ centralize $L$, 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 $S \subseteq \text{PSL}(n, q)$, then $S \subseteq \text{PSL}(n, q)$.

Moreover, as $8 \mid n$, we have that $r_1 = c_2 c_3 c_4 n$. We have that $M, N$ and $U$ centralize $L$, 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 $L \subseteq \text{PSL}(n, q)$, then $L \subseteq \text{PSL}(n, q)$.

By proposition 1.1, we have that $f_{\frac{n}{2}}^{-1}(N_i)$ is conjugate to $f$ in $\text{PGL}(r, q)$, and so $f_{\frac{n}{2}}^{-1}(N_i)$ is conjugate to $\phi \overrightarrow{D}$ in $\text{PGL}(n, q)$, 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 $M'_1 \in \text{GL}(r_1, p^{m_2})$. Moreover $M'_1$ is symmetric (note that $r_1$ is odd). By conjugating with elements of $\text{GL}(r_1, p^{m_2})$ we find that there are at most 2 choices for $M'_1$, and at most $2(q - 1)^2$ choices up to $\text{SL}(r_1, p^{m_2})$-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 $\text{PGL}(n, q)$ we obtain that there are at most $4(q - 1)^3$ choices for $M$.

The number of choices for $U_i$ is now at most $q^{r_1(r_1 + 1)/2}$ (note that the element $\gamma$ appearing in case I is now forced to be 1, as $r_1$ 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 $U$.

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

Case B: $C$ is 2-generated

We may assume that $C = \langle \phi \overrightarrow{N_i}, \tau^\epsilon \phi \overrightarrow{M_i} \rangle$, where $M_i, N_i \in \text{GL}(n, q)$ and $\epsilon \in \{0, 1\}$. We may also assume that any other complement $C'$ is generated by $\phi \overrightarrow{N_i}, \tau^\epsilon \phi \overrightarrow{M_i}$, satisfying the same relations as $\phi \overrightarrow{N_i}, \tau^\epsilon \phi \overrightarrow{M_i}$.

Case I: $C \notin \text{InnDiag}(G) \Gamma, (\phi \overrightarrow{N_i})^{m/n} = 1$

In this case we apply proposition 1.5.

Case II: $C \notin \text{InnDiag}(G) \Gamma, (\phi \overrightarrow{N_i})^{m/n} = L_i \neq 1, n \geq 3$
Let \( u = |L| \). We now want to count \( \text{PSL}(n, q) \)-conjugacy classes of elements of the form \( \phi \cdot L \). By [p. 52] [5] \( f \) for \( A \) and \( f \) for \( B \) are conjugate if and only if \( (\phi \cdot A)^{m/r} \) and \( (\phi \cdot B)^{m/r} \) are conjugate, so we need to bound the number of \( \text{PGL}(n, q) \)-conjugacy classes of elements \( L \) of order \( u \), and then to multiply this bound by \( |\text{PGL}(n, q) : \text{PSL}(n, q)| = d \). As \( L \) 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:

\[
X_i = \begin{pmatrix}
1 & c_i \\
1 & \\
. & . \\
1 &
\end{pmatrix},
\]

where \( c_i = ce_i \) and \( e_i \) is a unit vector. 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 \( L \), up to \( \text{PGL}(n, q) \)-conjugacy.

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

So, summing over all \( k \)'s, the choices for \( L \) are at most

\[
d^{n-1} + \sum_{1 \leq k | d} (q - 1) d^{n-1}.
\]

Note that \( d^{n-1} + \sum_{1 \leq k | d} (q - 1) d^{n-1} \leq (q - 1) \frac{d^{n-1} - 1}{d - 1} \).

We now have that \( L^{\phi \cdot M} = L \). Once we have fixed one element \( M \) with that property, all the others can be obtained by multiplying \( M \) by an element of the centralizer \( Z \) of \( L \) in \( \text{PSL}(n, q) \), and we may assume without loss of generality that \( L \) 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 \( Z \) is \( |\text{GL}(n - 1, q)| \). We now have to check that

\[
d(q - 1) \frac{d^{n-1} - 1}{d - 1} |\text{GL}(n - 1, q)| < |\text{PSL}(n, q)|,
\]

which is true for \( n \geq 4 \) because \( d(q - 1)^2 \frac{d^{n-1} - 1}{d - 1} < (q^n - 1) q^{n-1} \). For \( n = 3 \) we use the more accurate bound (2).
Case III: $C \leq \text{InnDiag}(G) \Gamma$, $n \geq 3$.

If $C$ is cyclic we conclude by proposition 1.3. Otherwise we first choose a generator for $C' \cap \text{InnDiag}(G)$, 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 $C' \cap \text{InnDiag}(G)$, 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 $G = {^2A}_{n-1}(q) = \text{PSU}(n, q)$, for $n$ and $q$ fixed.

Let $K = GF(q^2)$ be the finite field with $q^2$ elements, with $q = p^m$ for some prime number $p$. We fix a generator $\lambda$ of the multiplicative group of the field $K^\times$. Then $\text{GU}(n, q)$ (resp. $\text{SU}(n, q)$) will denote the general (resp. special) unitary group of degree $n$, that is $\text{GU}(n, q) = \{ g \in \text{GL}(n, q^2) | g(g^{-1})^\sigma = 1 \}$ where $\sigma = \phi^m \in \text{Aut}(\text{GL}(n, q^2))$, and $\text{SU}(n, q) = \{ g \in \text{GU}(n, q) | \det(g) = 1 \}$. 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 $C = \langle \phi^* \overline{N}_1, \overline{U}_1 \rangle$, with $\overline{U}_1, \overline{N}_1 \in \text{PGU}(n, q)$. We argue as in case B II of the special linear group.

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

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

So $c_i(\epsilon_i^q)^{-j}$ for some $j$, which implies that $c^{q+1} = (\epsilon_1 \epsilon_2^q)^{-1}$ and $c^{(q+1)^2} = 1$. Let $c = \lambda^u$. We have that $q^2 - 1 \mid u(q+1)^2$, so $q - 1 \mid u(q+1)$.

As $(q+1, q-1) \leq 2$, it follows that $\frac{q-1}{2} \mid u$ and there are at most $2(q+1)$ choices for $c$. Moreover, again by [10, p. 34] two matrices are conjugate in $\text{GU}(n, q)$ if and only if they are conjugate in $\text{GL}(n, q^2)$, so it
is enough to count the number of choices for the matrix $X$ as above, and then to multiply by $d = |\operatorname{PGU}(n, q) : \operatorname{PSU}(n, q)|$.

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

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

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

To bound the number of choices for the second generator, we look for an upper bound for the order of the centralizer $\mathcal{Z}$ of $\mathcal{U}$ in $\operatorname{PGU}(n, q)$. We may assume that $\mathcal{U}$ 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 $\mathcal{Z}$ is $|\operatorname{GU}(n - 1, q)|$.

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

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

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

We now study the remaining cases.

I: Case $(n, q) = (3, 2), d = 3$ is divided into 2 subcases according as $\mathcal{U}$ is diagonalizable or not. For each case, we have to consider the possible canonical forms for $\mathcal{U}$ 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 $15 \cdot 3 |\operatorname{GU}(2, 5)| < |\operatorname{PSU}(2, 5)|$.

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

4. $B_3(q), C_3(q)$ and $E_7(q)$.

Let $G \in \{B_3(q), C_3(q), E_7(q)\}$. We have that $C$ is isomorphic to a subgroup $\mathcal{U}$ of $Z_2 \times Z_m$, with $Z_m = \langle \phi G \rangle$ and $\operatorname{Out} \operatorname{Diag}(G) \leq Z_2$. 


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 $\phi^\gamma z$, with $z \in G$ and $(\phi^\gamma z)^\tau = 1$, 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 $\text{Out Diag}(G) \Gamma = Z_2$, 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 $\text{Out}(G)$ are isomorphic to a subgroup of $D_8 \rtimes Z_m$, with the following notation: $Z_m = \langle \phi G \rangle$ and $\text{Out Diag}(G) \Gamma \leq D_8$. More precisely, if $l$ is odd and $4 | q - 1$ or if $l$ is even then $\text{Out Diag}(G) \Gamma = D_8 = \langle xG, rG \rangle$, where $r$ is the graph automorphism of order 2, $\overline{w} = wG$ has order 4, $\overline{w}^r = \overline{w}^{-1}$, $[r, \phi] = 1$, 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 $\text{Out Diag}(G) \Gamma = \langle xG, rG \rangle$ is elementary abelian, $r$ is the graph automorphism of order 2, $x \in \text{InnDiag}(G)$. Also $\phi$ centralizes $\text{Out Diag}(G)$.

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

Let $\overline{C} \neq \text{Out Diag}(G) \Gamma$.

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

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 $\text{InnDiag}(G)$-conjugacy, a generator of $C'$ modulo $C' \cap \text{InnDiag}(G) \Gamma$ is $\langle \phi^\gamma \rangle$, for some $x \in \text{InnDiag}(G)$, and we have at most $|\text{InnDiag}(G) : G| \leq 4$ choices for it, up to $G$-conjugacy.

$T$ is generated by two involutions $u^\varepsilon$ and $v^\varepsilon$, 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 $[\tau^\varepsilon y, \phi^\gamma] = 1$, so $y \in D_l(p^\varepsilon)$. We note that we may conjugate $\tau^\varepsilon y$ by elements of $D_l(p^\varepsilon)$, which centralize $\phi^\gamma$. 
From Table 4.5.1 of [4] we deduce that both the number of $D_l(p')$-conjugacy classes of involutions of graph type and the number of $D_l(p')$-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 $|\text{InnDiag}(G)\cap G| \leq 8 |G: C_G(g)|$ 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 $2(l+3)^2 |G: H|$ 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 $C$ does not contain $\text{OutDiag}(G)$; in particular $|T| < 8$. Let $\phi'z$ be a generator of $C$ modulo $T$ of order $\frac{m}{r}$, with $z \in \text{InnDiag}(G) \cap \text{InnDiag}(G)$. We have that $\frac{m}{r}$ is even, otherwise we replace $\phi'z$ with $(\phi'z)^4$, which is a generator of $C$ modulo $T$ of order $\frac{m}{r}$ and of the form $\phi'x$ 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 subgroup 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 $T = \text{OutDiag}(G)$ 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 $T = \text{OutDiag}(G)$ and as we are not in case I it follows that $\phi'z$ does not centralize $T$, so we conclude by Proposition 1.6.

Let $l$ be odd. Note that we also have that $8 |q - 1$, because $m$ is even.

As we are not in case I, one of the following occurs:

- $\xi = \tau$ and $T = \langle \sigma^2, \sigma \tau \rangle$, or
- $\xi = \sigma \tau$ and $T = \langle \sigma^2, \tau \rangle$.

To deal with these cases we always adopt the same strategy. We first count the number of choices for a generator of $T \cap \text{InnDiag}(G)$, then we count the number of choices for a generator of $T$ modulo $T \cap \text{InnDiag}(G)$, 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 $C' = \langle \phi' x u, w^2 v, w x v \rangle$, 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 $C^* = C_{\text{InnDiag}(G)}(w^2 v)$ and $L^* = O^*(C^*)$. From table 4.5.1 of [4] it follows that

i) either $L^* = 2D_{i-1}(q)$ and $Z = C_{C^*}(L^*) = C_{\text{InnDiag}(G)}(r_1(L^*))$ has order $q + 1$ or

ii) $L^* = D_i(q) \times D_{i-1}(q)$ or $L^* = 2D_i(q) \times 2D_{i-1}(q)$, where $2 \leq i < \frac{l}{2}$ and $Z = C_{C^*}(L^*) = C_{\text{InnDiag}(G)}(r_1(L^*))$ has order $2$.

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

Note: For $i = 2, 3$ it is easy to check that $r_1, r_2 \leq 6 l + 25$ 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 $2(6 l + 25)^2$ choices for $w x v$.

We now have to choose $\phi' x u$ with the required properties, any other element of the form $\phi' x u$ is such that $(\phi' x u)^{-1} \phi' x u' \in C_G(w^2 v)$, 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 $(l - 1) 2(6 l + 25)^2 |U|$, 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 $q^2 (q^2 - 1)(q^{l-1} + 1)$ and $2(l - 1)(6 l + 25)^2 < (q^l - 1)(q^{l-1} + 1)$ (here $l \geq 5$ and $q \geq 9$).

Let $C \subseteq \text{OutDiag}(G) G$.

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 $\text{OutDiag}(G) = 1$ if $p = 2$, otherwise $\text{OutDiag}(G) = (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z})$ is elementary abelian of order 4 and it is centralized by $\phi$. Also, $\Gamma = \langle \tau, \gamma \rangle$ is isomorphic to $S_3$ with $|\tau| = 2$, $|\gamma| = 3$, $\overline{\omega} = \overline{\tau}$, $\overline{\tau} = \tau$, while $\langle \text{InnDiag}(G) \Gamma \rangle / G$ is isomorphic to $S_4$ and is centralized by $\phi$.

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

Case: $C \not\in \text{InnDiag}(G) \Gamma$

I) Assume that it is possible to choose a generator $\phi' u$ of $C$ modulo $T$ of order $\frac{m}{r}$ and with $u \in \text{InnDiag}(G)$.

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 $\phi' u$, up to $G$-conjugacy, and we may assume that it is of the form $(\phi')^x$ for some $x \in \text{InnDiag}(G)$.

We may also assume that one generator of $T$ is an involution $y$ such that $y$ centralizes $\phi'$. As we may conjugate $y$ by elements of the form $w \in G$, where $w$ centralizes $\phi'$, the choices for $y$ are bounded by the number of $G$-conjugacy classes of non-inner involutions of fixed type in $\text{InnDiag}(D_4(p^r)) \Gamma$, which by table 4.5.1 of [4] is at most 24. The second generator of $T$ is an element of $\text{InnDiag}(D_4(p^r)) \Gamma$ and we have that $96 | \text{InnDiag}(D_4(p^r)) \Gamma | < |G|$, as we wanted.

If $p = 2$ then by proposition 1.1 we have at most one possibility for the choice of $\phi' u$, 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 $\phi'$. Arguing as above and using table 4.7.3A of [4] we find that there are at most 16 $\text{InnDiag}(D_4(2^r)) \Gamma | < |G|$, as we wanted.

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

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 proposi-
Complements of the socle etc. 159

tion 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 5.2A of [p. 175] [7] the index of a maximal sbsgroup of \( G \) is at least \( \frac{(q^2 - 1)(q^2 - 1 + 1)}{q - 1} \) > 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 \( \phi' au \), the second generator \( b \) has the property that \([\phi' au, b] = 1\). Thus the possible choices for the second generator are given by elements of the type \( bv \), with \( v \in G \), such that \([\phi' au, bv] = 1\), so that \( v \in C_G(\phi' au) \). It follows that we have at most \( 4 |C_G(\phi' au)| < |G| \) choices, as we wanted (note that \( C_G(\phi' au) \) 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 \( \text{OutDiag} (G) \leq T \) and that \( T = \langle y, y' \rangle \) for some \( y \) in \( T \), where \( y \) has order 2 or 3, so that \( C = \langle \phi' a, y \rangle \). Now proposition 1.6 allows us to conclude.

Case: \( C \leq \text{InnDiag} (G) \Gamma \)

We first assume that \( p = 2 \). Then \( C = \langle x, y \rangle \equiv \Gamma \), 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.

1) If \( C \equiv \text{OutDiag} (G) \Gamma \) 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 \( \text{InnDiag} (G) \)-conjugacy classes of involutions of graph type, and if \( g \) is a graph type involution such that \( H = C_{\text{InnDiag} (G)} (g) \) has minimum order, there are at most 6 \( |\text{InnDiag} (G) : H| \leq 24 |G : G \cap H| \) choices for \( g \). As \(|H \cap G| > 16\cdot 24\), it follows that 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 \( |x| = 2 \), \( x \in \text{InnDiag}(G) \backslash G \) and \( |y| \in \{2, 3\} \) and the type of \( y \) is known (either \( y \in \text{InnDiag}(G) \backslash G \) 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 \( N_G \) choices for \( y \), where \( H = C_{\text{InnDiag}(G)}(g) \) 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 \( 4 \mid q + 1 \)

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 \( a \in \text{InnDiag}(G) \).

We have that \( C = \langle y, \phi^u \rangle \) where \( y \in \text{InnDiag}(G) \backslash \text{Inn}(G) \) has order 2 and is centralized by \( \phi^u \), 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 [7], the index of a maximal subgroup of \( G \) is bigger than \( l - 1 \). This allows us to conclude.

\( l \) odd, \( 4 \mid q + 1 \)

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

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

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

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 \( \frac{l + 1}{2} \) choices for \( x^2 \), up to \( G \)-conjugacy. Moreover let \( C^* = C_{\text{InnDiag}(G)}(x^2) \) and \( L^* = O^*(C^*) \). From table 4.5.1 of [4] it follows that \( L^* \) is one of the following:
i) \( L^* = D_{l-1}(q) \) and \( Z = C_{C^*}(L^*) = C_{\text{InnDiag}(G)}(L^*) \) has order \( q-1 \);

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

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

We note that the case \( L^* = D_i(q) \times D_{l-i}(q) \), where \( i \) is odd occurs only if \( x^2 \) is inner, which is not our case. To see this, note that \( G = P\Omega^-(2l, q) \), 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 \( \text{diag}(\mathbf{2}^1, R, \mathbf{2}^1, 1, R, 1) \), 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 \( (y_1, y_2) \in \text{Aut}(D_i(q)) \times \text{Aut}(D_{l-i}(q)) \) be the image of \( x \) in \( \text{Aut}(L^*) \). 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 \( D_i(q) \)-conjugacy classes of involutions in \( \text{InnDiag}(D_i(q)) \) \( \Gamma \) (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 \( \text{InnDiag}(D_{l-i}(q)) \) \( \Gamma \). Again by table 4.5.1 of \[4\] we have that \( r_1 \leq 3i + 1, r_2 \leq 3(l - i) + 9 \).

Note: it is easy to check that for \( i = l - 3 \) it is still true that \( r_2 \leq 3(l - i) + 9 \), and the same holds for \( i = 2 \) and \( r_1 \leq 3i + 1 \) (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 \( l^2 + 15l + 25 \), 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 \( GU(l, q) \) to a diagonal matrix whose entries on the diagonal are of the form \( e^i \), where \( e \) is a primitive 4-th root of 1. Moreover, if \( GF(q^2)^x = (\lambda) \), we have that \( \text{diag}(\lambda^{l-1}, 1, \ldots, 1) \) is a unitary matrix centralizing \( x \), so that the number of \( SU(l, q) \) 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 \( \frac{(q^l + 1)(q^{l-1})}{q - 1} \), which is greater than \( \frac{l + 1}{2} \max \left\{ \frac{9}{2}l^2 + 30l + 50, 2^l(2^l - 1) \right\} \).

8. $E_6(q)$. We have that $C$ is isomorphic to a subgroup $\overline{C}$ of $\text{Out}(G) \leq S_3 \rtimes Z_m$, with $Z_m = \langle \phi G \rangle$, $S_3 = \langle aG, \tau G \rangle$, $|aG| = 3$, $|\tau| = 2$, $(aG)^{\phi} = (aG)^{-1}$, $\text{OutDiag}(G) \leq \langle aG \rangle$ and $I(G) = \langle \tau \rangle$. Also, $\phi$ centralizes $\tau$ and either inverts or centralizes $aG$.

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

Let $\overline{C} \neq \text{Out Diag}(G) \Gamma$, $T = C \cap \text{InnDiag}(G) \Gamma$.

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

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

We have that $T$ is generated by a graph-type involution $u$ centralizing a suitable conjugate of $\phi \cdot x$ and an element $v \in \text{InnDiag}(G) \setminus \text{Inn}(G)$ 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 $\text{InnDiag}(G) \setminus \text{Inn}(G)$, and each of them has at most $|\text{InnDiag}(G)/\text{Inn}(G)|$ 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 $\phi \cdot z$ of $C$ modulo $T$ of order $\frac{m}{r}$ and with $z \in \text{InnDiag}(G) \Gamma$. 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 $\text{InnDiag}(G) \setminus \text{Inn}(G)$ is at most 8, which is less than the index of a maximal subgroup of $G$.

Let $C \leq \text{InnDiag}(G) \Gamma$. 
We have that $C$ is generated by a graph-type involution $u$ and an element $v \in \text{InnDiag}(G) \setminus \text{Inn}(G)$ 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 $\text{Out}(G) \leq Z_3 \times Z_m$, with $Z_m = \langle \phi(G) \rangle$ and $Z_3 = \langle uG, rG \rangle$ and $\alpha \in \text{InnDiag}(G)$.

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

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


Manoscritto pervenuto in redazione l'8 gennaio 2004.