On p-singular Elements in Chevalley Groups in Characteristic p

Robert M. Guralnick and Frank Lübeck*

Abstract. We give upper bounds for the proportion of p-singular elements in finite Chevalley groups in characteristic p.

1991 Mathematics Subject Classification: primary 20G40; secondary 20D60.

1. Introduction

Let $\mathbf{G}$ be a reductive algebraic group over an algebraic closure of a prime field of characteristic p, defined over a finite field F_q with q elements. Let σ denote a (possibly twisted) Frobenius endomorphism of $\mathbf{G}$ with field of definition F_q. We denote $G = \mathbf{G}(q)$ the the corresponding finite group of F_q-rational points of $\mathbf{G}$, i.e., the fixed points of σ. Since we can take $\mathbf{G}$ to be simply connected or adjoint (or anything in between) and since (as we see below) a center will not change our computations, the finite groups we are considering are those with $J(q) \leq G \leq \mathrm{Inndiag} J(q)$ where $J(q)$ is a simple finite group of Lie type defined over F_q.

Kantor and Seress [**KS**] have asked for an upper bound on the proportion of p-singular elements (i.e., those elements whose order is divisible by p) in G. As far as we know, Kantor was the first to conjecture that a bound of c/q was likely. The motivation came from a specific need within computational group theory. See also [**NP**] where estimates for some of the classical groups are given (not necessarily simple).

Spaltenstein observed that one gets asymptotic results (at least for a fixed characteristic) by counting the number of components of codimension 1 in the hypersurface which is the complement of regular semisimple elements. Asymptotic results can also be obtained from results in [**FJK98,FJ93,FJ93b,FJ94**] which give formulae for the number of regular semisimple classes.

The issue of a lower bound was addressed in [**IKS95**]. See also [**NP**].

Let S denote the set of p-singular elements in $\mathbf{G}$ (i.e., the unipotent part is nontrivial). Let R denote the set of regular semisimple elements in $\mathbf{G}$ – i.e., the

*Partially supported by an NSF grant.

set of elements whose connected centralizer is a (necessarily maximal) torus or, equivalently, those elements which do not commute with any nontrivial unipotent element. Clearly, R and S do not intersect. It is well known that R is an open subset of $\mathbf{G}$ and so R', the complement of R contains the closure of S. In fact R' is the closure of S: R' consists of the elements which commute with a nontrivial unipotent element – this implies that any element x in R' commutes with a root subgroup U (see Theorem 4.1) – then xU is an irreducible variety and with at most one exception consists of p-singular elements; in particular, x is in the closure of S.

So we define $s(G)$ to be the proportion of p-singular elements in G and $r(G)$ to be the proportion of regular semisimple elements in G. Let $r'(G) = 1-r(G)$. So $r'(G)$ is the proportion of elements which commute with an element of order p. Clearly, $s(G) < r'(G)$ and it is $r'(G)$ that we will obtain estimates for.

So if c is the number of components of R' of codimension 1, it follows from the Lang-Weil estimates for the number of points on an absolutely irreducible variety that

$$r'(G) = |R'(q)|/|\mathbf{G}(q)| \leq c/q + O(q^{-3/2}).$$

As mentioned above, this approach was suggested by Spaltenstein. The weakness of this approach is that one does not obtain effective bounds, only asymptotic ones. In particular, the nature of the error term conceivably depends on the characteristic of the underlying field. In this note, we obtain effective bounds as follows.

Theorem 1.1. *If* $\mathbf{G}$ *is simple then* $s(\mathbf{G}(q)) < r'(\mathbf{G}(q)) < 3/(q-1)+2/(q-1)^2$.

As noted above, this theorem applies to all groups G with $J(q) \leq G \leq \mathrm{InnDiag}(J(q))$, where $J(q)$ is a simple finite group of Lie type defined over the field of q elements and $\mathrm{InnDiag}(J(q))$ is the full group generated by inner and diagonal automorphisms (see **[Car72]** for definitions). Note if we take $\mathbf{G}$ to be simply connected, then $G = \mathbf{G}(q)$ is almost always quasisimple. Since the center is a p'-group, there is no harm in passing to the quotient in computing either $r(q)$ or $s(q)$. Similarly, if we take $\mathbf{G}$ to be the adjoint group, then G will be the full group of inner and diagonal automorphisms of $J(q)$.

In the main body of the paper, we give more precise bounds for each type of group which are also asymptotically correct for growing q. One can modify our methods to obtain asymptotic lower bounds with the correct main term; see **[NP]**. In that paper, they also obtain results for fixed q as the rank tends to infinity.

We handle the classical groups first. The method we use is to show that any p-singular element commutes with a conjugate of one of a family of unipotent subgroups (for algebraic groups, this family can be taken to be the root subgroups). For the classical groups, we estimate how many elements are in

the union of the set of conjugates of these subgroups. For exceptional groups, one can compute exactly the number of p'-elements of $\mathbf{G}(q)$ and $|R'(q)|$.

In section 4, we discuss asymptotic results for the variety of p-singular elements and results for simple algebraic groups. In the final section, we make some brief remarks about the general case of almost simple groups.

2. Classical Groups

In the case of GL_n or SL_n, the subset R is the collection of elements with distinct eigenvalues – a condition that can be expressed by saying that the discriminant of the characteristic polynomial is nonzero. There are similar descriptions for the other classical groups.

Let $J = \mathbf{G}(q)$ denote a simple classical group (i.e., linear, unitary, symplectic or orthogonal) over F_q with $q = p^a$. Let $J \leq G \leq A$, where A is the full group of inner and diagonal automorphisms. We view J, G and A all acting on its natural module V (since whatever center is allowed has order prime to p, this has no effect on the proportion of p-singular elements or of elements which commute with a nontrivial p-element). So the groups we are considering for J are $PSL_n(q), n \geq 2$, $PSp_n(q), n \geq 4$ and even, $PSU_n(q), n \geq 3$ or $O_n^{\pm}(q), n \geq 7$ (where the latter group is the commutator subgroup of the orthogonal group). The natural module is defined over F_q except in the unitary case where it is defined over F_{q^2}.

If $x \in G$, we will let s_x and u_x denote the semisimple and unipotent parts of x (so x is the commuting product of s_x and u_x and these element are the p' and p-parts of x).

Our strategy is as follows. We first identify semisimple elements in R' in terms of their module structure on the natural module. We then choose a unipotent subgroup U which is contained in the center of a Sylow subgroup of the centralizer of this semisimple element. It follows that any element of R' with this given semisimple part commutes with a conjugate of U. Fortunately, the choice of U (up to conjugacy) will not depend very much on the semisimple element, but only on the homogeneous components of the semisimple element. It follows that R' is the union of the conjugates of the centralizers of these families of unipotent subgroups and this is the estimate we use.

In the case of algebraic groups (and not just the classical groups), it turns out that we need only consider U to be a root subgroup (so in case of one root length, only one subgroup and in general at most two).

In this section we will repeatedly use the following easy lemmas.

Lemma 2.1. *Let G be a finite group and U be a subgroup of G with $t = |N_G(U) : U|$. Then $|\cup_{g \in G} U^g| < |G|/t$.*

Proof. There are $|G|/|N_G(U)| = |G|/(t|U|)$ different subgroups U^g, all of order $|U|$. □

Lemma 2.2. *Let $q > 1$ a real number. Then*

$$\sum_{e=1}^{\infty} 1/(q^e - 1) < 1/(q-1) + 1/(q-1)^2.$$

Proof. This follows from

$$\sum_{e=2}^{\infty} 1/(q^e - 1) < \sum_{e=2}^{\infty} 1/(q^e - q) = 1/(q(q-1)) + (1/q)\sum_{e=2}^{\infty} 1/(q^e - 1).$$

□

Recall that $r'(G) = |R'(q)|/|\mathbf{G}(q)|$.

In the remaining part of this section, we prove the following:

Theorem 2.3. *If G is almost simple with socle J of classical type and G is contained in the group of inner-diagonal automorphisms of J, then $r'(G)$ is bounded above as given in the following table:*

J	$\lvert G : J\rvert$	*Upper Bound for* $r'(G)$
$PSL_2(q)$	*1*	$(2, q-1)/(q-1)$
$PSL_2(q)$	*2*	$1/(q-1)$
$PSL_n(q)$, $n \geq 3$		$1/(q-1) + 2/(q-1)^2$
$PSU_n(q)$, $n > 2$		$1/(q-1) + 4/(q-1)^2$
$Sp_n(q)$, $n = 2k > 2$, *q even*		$2/(q-1) + 1/(q-1)^2$
$PSp_n(q)$, $n = 2k > 2$, *q odd*	*1*	$3/(q-1) + 1/(q-1)^2$
$PSp_n(q)$, $n = 2k > 2$, *q odd*	*2*	$2/(q-1) + 1/(q-1)^2$
$O^{\pm}_{2n}(q)$, $n \geq 4$		$1/(q-1) + 2/(q-1)^2$
$O_{2n+1}(q)$, $n \geq 3$, *q odd*		$2/(q-1) + 2/(q-1)^2$

Proof. Let $x = su$ be the Jordan decomposition of $x \in R'$. Since s is not regular, it follows that s has a homogeneous component W on V which has multiplicity $m > 1$. Define e by $\mathrm{End}_{F_q}(W) = M_m(F_{q^e})$.

Now $C_G(s)$ leaves W (and each homogeneous component) invariant. In particular, u does. If U is a central subgroup of a Sylow p-subgroup of $C_G(s)$, then we see that the union of all G-conjugates of $C_G(U)$ contains su. Thus, choosing one U for each s and taking all conjugates covers all of R'. We will see that in each case we can choose only a small number of U and that we can bound the union of all these conjugates.

Case 1. $J = PSL_2(q)$.

If $G = SL_2(q)$, we can get an exact formula. R' is precisely the union of elements of the form $\pm u$ with u unipotent. Thus, $r'(G) = (2, q-1)q/(q^2-1) < (2, q-1)/(q-1)$.

If q is odd and G/J has order 2, then R' does not change but $|G| = 2|J|$.

Case 2. $J = PSL_n(q), n > 2$

In this case, we choose $U = U_e$ to be a root subgroup of the centralizer acting on W (note this centralizer is $GL(m, q^e) \cap G$). Note that this conjugacy class does not depend on m, but only on e.

Thus R' is the union of the centralizers of the F_{q^e}-root subgroups. If $e < n/2$, then $|N_G(U)/C_G(U)| \geq (q^e - 1)$ (because all elements in the root subgroup are conjugate to a fixed one via some toral elements which normalize U – just consider the group over the extension field). If $e = n/2$, then similarly we see that $|N_G(U)/C_G(U)| \geq (q^e-1)/(2, q-1)$. Thus, by 2.1 and $U \subseteq C_G(U)$ we have $r'(G) < (2, q-1)/(q^{n/2} - 1) + \sum_{e=1}^{n/2-1} 1/(q^e - 1)$ if n is even and $r'(G) < \sum_{e=1}^{(n-1)/2} 1/(q^e - 1)$ if n is odd.

This yields easily that

$$r'(G) < 1/(q-1) + 1/(q-1)^2,$$

if q is even or $n \neq 4$. In the remaining case,

$$r'(G) < 1/(q-1) + 2/(q-1)^2.$$

Case 3. $J = PSU_n(q), n > 2$.

The first possibility is that W is nondegenerate. Then $C_G(s)$ (acting on W)is $U_m(q^{e/2})$ and we choose U to be the center of a root subgroup, so U consists of transvections (over the larger field) and has order $q^{e/2}$. Note that e is even, the class of U is independent of m and that $N_G(U)/C_G(U)$ has order at least $q^{e/2} - 1$ unless q is odd, n is even and $e = n$. In that case $|N_G(U)/C_G(U)| \geq (q^{e/2} - 1)/2$. Note that $1 \leq e/2 \leq n/2$.

The other possibility is that W is totally singular with $m \geq 2$. In this case, $C_G(s)'$ acts as $SL_m(q^e)$ on W – so $|U| = q^e$ and $|N_G(U)/C_G(U)| \geq (q^e - 1)$ or $(q^e - 1)/2$ if q is odd, n is even and $e = n$.

Summing over all possible e, we obtain the estimates

$$r'(G) < 1/(q-1) + 1/(q-1)^2 + 1/(q^2-1) + 1/(q^2-1)^2$$

for n odd or q even, and

$$r'(G) < 1/(q-1)+1/(q-1)^2+1/(q^2-1)+1/(q^2-1)^2+1/(q^n-1)+1/(q^{n/2}-1)$$

for n even and q odd.

In all cases, we obtain the inequality:

$$r'(G) < 1/(q-1) + 4/(q-1)^2.$$

Case 4. $J = PSp_n(q)$, $n = 2k > 2$.

There are various possibilities for the parameters in this case.

The first possibility is that W is nondegenerate and $C_G(s)$ leaves invariant an F_{q^e}-alternating form on W. Note in this case $s = \pm 1$ on W. So $e = 1$. In this case, we take U to be a long root subgroup of $Sp(m, q)$ which is a long root subgroup of G. So $|N_J(U)/C_J(U)| \geq (q-1)/(2, q-1)$. If $G \neq J$, then similarly we see that $|N_G(U)/C_G(U)| \geq (q-1)$.

The second possibility is that W is totally singular. Then W is paired with another totally singular homogeneous component, W^* and $C_G(s)$ acts as $GL(m, q^e)$ on W (and via the dual on W^*). In this case, we take U to be a root subgroup of $GL(m, q^e)$. Again, we note that the conjugacy class of U is independent of m. Note that $N_G(U)/C_G(U)$ has order at least $q^e - 1$.

The final possibility is that W is nondegenerate but that $C_G(s)$ does not preserve an alternating form over F_{q^e} on W. In this case, $C_G(s)$ acts on W as a unitary group over F_{q^e} and we take U to be the center of a Sylow p-subgroup of order q^e consisting of unitary transvections (over the bigger field). In particular, e is even. Again, this class is independent of m. Reducing to the case $m = 2$, we see that this subgroup is actually contained in $U_2(q^e)$ and that it is a short root subgroup of $Sp_4(q^e)$, a class of subgroups already allowed from the previous paragraph.

So as above, we obtain the estimates:

$$r'(G) < 3/(q-1) + 1/(q-1)^2$$

for q odd and $G = J$, and

$$r'(G) < 2/(q-1) + 1/(q-1)^2$$

for q even or G/J of order 2.

Case 5. Orthogonal Groups, $n \geq 7$.

We may assume that q is odd if n is odd (because otherwise the orthogonal group is the symplectic group, a case already dealt with).

We first note some elementary facts. If x is semisimple and a is an eigenvalue of x, let V_a denote the corresponding eigenspace (over the algebraic closure). Then V_a and V_b are orthogonal unless $ab = 1$. If $ab = 1$ and $a^2 \neq 1$, then $V_a \oplus V_b$ is nonsingular. In particular, a and a^{-1} have the same multiplicity.

These cases are all quite similar to the symplectic case. The possible components of centralizers of semisimple elements that we have to deal with correspond to the totally singular case where we get components of the form $GL(m, q^e)$ and the nondegenerate case where the components are either of the form $O^{\pm}(m, q)$ or $U(m, q^{e/2})$.

In the first case, the class of U depends only on e and $|N_G(U)/C_G(U)| \geq q^e - 1$ except that possibly if e is maximal, then only $|N_G(U)/C_G(U)| \geq (q^e-1)/(2, q-1)$. In the last case, we see that the conjugacy class of U depends only on e and not on m. Indeed, we see that we obtain the same conjugacy

classes of U as in the totally singular case (these are 'long root subgroups' over $F_{q^{e/2}}$). The usual argument shows that this gives a contribution bounded by $1/(q-1)+2/(q-1)^2$.

If the centralizer is an orthogonal group, then $e=1$ because the semisimple element must be ± 1 on W. If it acts as -1, then $m \geq 4$ is even (it is even because the determinant must be 1 and as noted above all eigenvalues are paired with their inverses and $m \geq 4$ because otherwise there is no unipotent element centralizing the semisimple element on that component). If $m > 4$, then the center of a Sylow p-subgroup of $C_G(s)$ is a long root subgroup and if $m = 4$, a long root subgroup of G embeds in O_4^+ and so is contained in the center of a Sylow p-subgroup of $C_G(s)$. So this class of subgroups is already accounted for.

If it acts as 1, then $n-m$ is even (because of the pairing of eigenvalues noted above). Thus, if n is even, we obtain nothing new. If n is odd (and so q is odd), we pick up the conjugacy class U of short root subgroups. In this case, $|N_G(U)/C_G(U)| = (q-1)$.

So we have shown that if $J = O_{2n}^{\pm}(q), n \geq 4$,

$$r'(G) < 1/(q-1) + 2/(q-1)^2,$$

and that if
$J = O_{2n+1}^{+}(q), n \geq 3$,

$$r'(G) < 2/(q-1) + 2/(q-1)^2.$$

This completes the proof of 2.3. □

3. Exceptional Groups

In principal we could handle the exceptional groups in a similar way as the classical ones. But it would become much more complicated to distinguish the possible types of centralizers of semisimple elements.

Instead we use that for exceptional groups we can compute exactly the number of semisimple and regular semisimple elements in $\mathbf{G}(q)$. We did this with the help of computer programs written by the second named author. They get as input a complete root datum which determines the algebraic group $\mathbf{G}$ up to isomorphism and a twisting type of a Frobenius morphism of $\mathbf{G}$. The numbers we are interested in are then computed completely automatically. They can be given in the form of polynomials in q, after distinguishing a finite number of congruence classes for q.

Example: The number of semisimple elements of the exceptional groups of type $G_2(q)$ is given by:

c	number of semisimple elements if $q \equiv c \bmod 6$
1	$q^{14} - 2\,q^{13} + q^{12} + 3\,q^{11} - q^{10} - q^9 - q^8 + 2\,q^7 - 2\,q^6 - 3\,q^5 + q^4 + q^3 + 1$
2	$q^{14} - 2\,q^{13} + q^{11} + q^9 - q^8 + 2\,q^7 - q^6 - q^5 - q^3 + 1$
3	$q^{14} - 2\,q^{13} + q^{12} + 2\,q^{11} - q^{10} - q^8 + 2\,q^7 - 2\,q^6 - 2\,q^5 + q^4 + 1$
4	$q^{14} - 2\,q^{13} + 3\,q^{11} - q^9 - q^8 + 2\,q^7 - q^6 - 3\,q^5 + q^3 + 1$
5	$q^{14} - 2\,q^{13} + q^{12} + q^{11} - q^{10} + q^9 - q^8 + 2\,q^7 - 2\,q^6 - q^5 + q^4 - q^3 + 1$

Details of the programs and their mathematical background are described in [**Lüb**]. It is planned to publish a version of these programs for general use within the computer algebra package CHEVIE [**GHL$^+$96**].

We remark that these results in the case of simply connected $\mathbf{G}$ could in principal also be obtained from data which appear in the literature. This would involve simple but extremely lengthy and tedious computations by hand.

Of course the same computations could also be done for classical groups up to a certain rank (≤ 9, say) to improve the results of the last section.

Printing all the exact polynomials as in the example above would need a lot of space and is probably not very useful. They are available for interested readers from the authors. Instead we express for all types of simple exceptional groups the quotient $r'(q) = |R'(q)|/|\mathbf{G}(q)|$ in the form

$$r'(q) = \frac{c}{q-1} + \frac{d}{(q-1)^2}$$

(similar to the estimating expressions in section 2), taking for c the asymptotically correct value.

This leads to the following theorem.

Theorem 3.1. *Let $\mathbf{G}$ be simple and of exceptional type. The table below gives for each type constants c, x, y and $\tilde{d}$ such that for all q we have*

$$c/(q-1) + x/(q-1)^2 \leq r'(\mathbf{G}(q)) \leq c/(q-1) + y/(q-1)^2$$

and such that

$$\tilde{d} = \lim_{q\to\infty} (r'(\mathbf{G}(q)) - c/(q-1)) \cdot (q-1)^2.$$

In case of the Suzuki and Ree groups substitute q by q^2 in these expressions.

G	c	x	y	$\tilde{d}$
${}^2B_2(q^2)$, $q^2 = 2^{2m+1}$, $m \in \mathbb{N}$	*1*	*-1*	*0*	*0*
$G_2(q)$, q *even*	*2*	*-3*	*-1*	*-3*
$G_2(q)$, q *odd*	*2*	*-4*	*-2*	*-4*
${}^2G_2(q^2)$, $q^2 = 3^{2m+1}$, $m \in \mathbb{N}$	*2*	*-1*	*0*	*-1*
${}^3D_4(q)$	*1*	*-1*	*0*	*-1*
$F_4(q)$	*2*	*-4*	*-1*	*-4*
${}^2F_4(q^2)$, $q^2 = 2^{2m+1}$, $m \in \mathbb{N}$	*2*	*-2*	*-1*	*-2*
$E_6(q)$	*1*	*-1*	*0*	*-1*
${}^2E_6(q)$	*1*	*-1*	*0*	*-1*
$E_7(q)$	*1*	*-1*	*0*	*-1*
$E_8(q)$	*1*	*-1*	*0*	*-1*

Note that the estimates in the theorem are always the same for groups of simply connected and adjoint type (and hence they also hold for the corresponding finite simple groups) – although the exact numbers of semisimple elements do depend on the type of the group. Also, with the exception of $G_2(q)$, the estimates do not depend on the congruence classes of q. Finally, we remark that the lower bounds also estimate the complement of the set of all (not just regular) semisimple elements.

4. Algebraic Groups

In this section, we show how our approach in section 2 applies in the case of algebraic groups. As remarked in the introduction, these results will at least provide good asymptotic estimates for the finite groups and will also verify that the coefficient of $1/(q-1)$, as given in the table in Theorem 2.3, is correct. If we want the fixed points of the Frobenius endomorphism to be quasisimple, we must consider simply connected algebraic groups.

For this section, we refer to [**Car72**] and [**Bor91**] for general references about algebraic groups.

Let $\mathbf{G}$ be a reductive group over an algebraically closed field F as in the introduction. Recall that R' is the set of elements which commute with a unipotent element (i.e., R' is the complement of the set of regular semisimple elements in $\mathbf{G}$).

Theorem 4.1. *Let $x \in \mathbf{G}$, then $x \in R'$ if and only if x centralizes a root subgroup of $\mathbf{G}$.*

Proof. Let $x = s_x u_x$ the Jordan decomposition of x, let B a Borel subgroup of $\mathbf{G}$ containing x and T a maximal torus in B containing s_x. Let R^+ denote the set of positive roots with respect to $T \subset B$. Order the positive set of roots. Then $u_x = \prod_{R^+} u_\alpha(t_\alpha)$ where $t_\alpha \in F$ and the product is taken in the given ordering. This expression is unique. Since s_x centralizes u_x and normalizes each root subgroup, it follows that s_x centralizes each root subgroup U_α with $t_\alpha \neq 0$. Let X denote the subgroup generated by these root subgroups. Then X is a product of root subgroups and moreover its center contains a root subgroup. So s_x and u_x centralize this root subgroup as desired. □

Now assume that $\mathbf{G}$ is a simply connected algebraic group. Let $Z = Z_\alpha$ be a root subgroup of $\mathbf{G}$. There are 1 or 2 conjugacy classes of such subgroups (depending upon the number of root lengths). Let X be the variety of elements in $\mathbf{G}$ which commute with some conjugate of Z. Fix a maximal torus T in $N := N(Z)$.

First observe that X has codimension 1 in $\mathbf{G}$ (to see this, note that a generic element in the centralizer of a root subgroup U has centralizer SU where the connected component of S is a maximal torus in the centralizer of U – so S has codimension 1 in a maximal torus and the map from $\mathbf{G} \times S^0U \to R'$ given by $(g, su) \mapsto (su)^g$ has generic fiber of dimension $1 + \mathrm{rank}(\mathbf{G})$).

First suppose that Z is a long root subgroup. Then $N := N(Z)$ contains a Borel subgroup and so is parabolic and in particular is connected. Moreover, $N = N'T$. Note that N' centralizes Z and so must be the connected component of $C(Z)$. Thus, the number of connected components of $C(Z)$ is precisely the number of connected components of $C := C_T(Z)$. The number of connected components of C is precisely the largest positive integer e relatively prime to p such that $\alpha = e\beta$ for some β in the weight lattice of $\mathbf{G}$. It is straightforward (using the description of the root and weight lattices in [**Car72**]) to see that $e = 1$ unless $e = 2, p \neq 2$ and one of the following holds:

$\mathbf{G}$ is of type A_1 or

$\mathbf{G}$ is of type C_l, $l \geq 2$.

Thus, the number of irreducible components in the variety X of elements which commute with a conjugate of Z is at most the number of components in C. So except in the cases above, X is an irreducible variety of codimension 1 in G.

In the two remaining cases one can check that the variety has 2 components. In fact, if X_1 is one component, then the other component is $\{A\} \times X_1$ where A is a generator of the center of G (and has order 2). Thus, both components have codimension 1.

Now assume that Z is a short root subgroup. Using estimates for the number of F_q-rational points in R' for exceptional groups, we see that the number of components of R' of codimension 1 in G is 1 for $G = G_2$ or F_4.

If $\mathbf{G} = B_\ell$ (or C_ℓ) with $p = 2$, we can argue as in the long root case (because short roots and long roots are interchanged when considering $\mathbf{G}$ as

B_ℓ or C_ℓ). So $C(Z)$ is connected and so X is irreducible. Finally, assume that $p \neq 2$ and $G = C_\ell$ or B_ℓ. A straightforward computation shows that there are 2 connected components in $C(Z)$ and so X has at most 2 connected components. Indeed, we see that in fact there are two connected components for X. The one corresponding to the identity component of $C(Z)$ has codimension 1 in $\mathbf{G}$.

Suppose that $G = C_\ell, \ell \geq 2$. A short root subgroup Z has a 2-dimensional commutator space with the natural module which is a totally singular 2-space. Thus, the normalizer of Z must stabilize this subspace and so $N(Z) \leq P$, the corresponding parabolic subgroup which is the full stabilizer of the totally singular 2-space. Since the radical Q of P is Abelian and contains the short root subgroup, we see that $C(Z)$ contains Q. The Levi complement of P is $GL(2) \times C_{\ell-2}$ where the second factor acts trivially on Q and so also on Q. The centralizer of Z in $GL(2)$ is precisely the two dimensional orthogonal group which has connected a 1-dimensional torus of index 2. Thus, we see the two components and we see that any element not in the connected component centralizes a long root element and so these elements are already accounted for.

If $G = B_\ell, \ell \geq 2$, then again a short root subgroup Z has a 2-dimensional commutator space with the natural module. However, in this case, the radical W of these space is 1-dimensional and is invariant under $N(Z)$. Thus, $N(Z)$ is the contained in P, the parabolic subgroup stabilizing a 1-dimensional totally singular subspace. One sees that the two components of $C(Z)$ correspond to whether the eigenvalue on W is ± 1. This implies that any element in $C(Z)$ has a triple eigenvalue either ± 1. The component corresponding to the case of eigenvalue -1 must have -1 occurring with multiplicity at least 4 (because the multiplicity of -1 is even). Restricting to the nonsingular subspace of dimension at least 4 which is the -1 eigenspace of the semisimple part of an element in $C(Z)$ shows that any element in the non-identity component of $C(Z)$ already centralizes a long root element (as in the C_ℓ case).

So in all cases, we obtain a single component of codimension 1 of elements centralizing a short root subgroup which is not contained in the centralizer of a long root subgroup.

Putting these results together we get the following theorem.

Theorem 4.2. *Let* $\mathbf{G}$ *be simple simply connected. Then the number of components of* R' *of codimension* 1 *is as given in the following table.*

In particular the asymptotic results agree with the asymptotic estimates obtained in sections 2 and 3 (since we are dealing with simply connected groups, we must compare these estimates with the simple groups) – i.e., the first term in our estimates for upper bounds for $r'(G)$ *cannot be improved.*

Group	*Number of Root Lengths*	*Number of Components*
A_1	*1*	*(2,p-1)*
$A_l, l \geq 2$	*1*	*1*
$B_l, l \geq 3$	*2*	*2*
$C_l, l \geq 2$	*2*	*1 + (2,p-1)*
$D_l, l \geq 4$	*1*	*1*
$E_l, l = 6, 7, 8$	*1*	*1*
F_4	*2*	*2*
G_2	*2*	*2*

We also note the following result which we assume is known to the experts in the field.

Theorem 4.3. *If* $\mathbf{G}$ *is simple then the subset of nonregular semisimple elements has codimension* 3 *in* $\mathbf{G}$ *and the number of components of this variety is at most* 3*.*

Proof. Let Y denote the set of semisimple elements which are not regular. As in 4.1, we see that $Y = Y_1 \cup Y_2$ where Y_i are those semisimple elements which centralize a long root subgroup (for $i = 1$) and or a short root subgroup (for $i = 2$). Arguing as above we see that Y_1 is irreducible unless $p \neq 2$ and $\mathbf{G} = A_1$ or C_ℓ. In those cases, there are two components. A generic element (in either component in the latter cases) has centralizer TA_1 where T is a maximal torus and A_1 is the subgroup generated by a pair of long root subgroups. Computing the dimension of the generic fiber of the conjugation map shows that each component of Y_1 has codimension 3.

Similarly, we see that Y_2 is irreducible of codimension 3. This completes the proof. □

We remark that in the case of $\mathbf{G} = SL$ or Sp, the closure of this variety is precisely the set of noncyclic matrices in each group.

5. Centers and Outer Automorphisms

In this section, we make some preliminary remarks about handling covering groups and other extensions of simple groups. We hope to return to this topic in a future article.

Fix a prime p. Let $S(G)$ denote the set of p-singular elements of G. Let $s(G) = |S(G)|/|G|$.

First consider the case that G has a center Z. If Z has order prime to p, then $s(G) = s(G/Z)$ (indeed, this is true for any normal subgroup with order prime to p). Furthermore, we note that:

Lemma 5.1. *Suppose that the center Z of G is a p-group. Then*

$$s(G) = s(G/Z)/|Z| + 1 - 1/|Z|.$$

Proof. Let $\pi : G \to G/Z$ be the natural map. Note that the inverse image of $S(G/Z)$ is contained in $S(G)$ and has cardinality $|Z||S(G/Z)$. Suppose that $x \in G$ is not p-singular in G/Z. If $z \in Z$, then $xz \in S(G)$ if and only if $z \neq 1$. Thus

$$|S(G)| = |Z||S(G/Z)| + |S'(G/Z)|(|Z| - 1) = |S(G/Z)| + |G/Z|(|Z| - 1).$$

Dividing by $|G|$ yields:

$$s(G) = s(G/Z)/|Z| + 1 - 1/|Z|.$$

□

Next we consider outer automorphisms. So let J be a finite simple group and G almost simple with socle J. We will consider the proportion of p-singular elements in a given coset xJ. So there is no harm in assuming that G/J is cyclic and generated by xJ. If p divides $|G/J|$, then every element in the coset xJ is p-singular.

So we shall assume that G/J is a p'-group. We restrict our attention to the case that J is a finite group of Lie type over the field F_q with q a power of p.

We have already handled the case of diagonal automorphisms. We do not answer the question completely but show that the answer can change in certain situations. Let p be a prime and let $\mathbf{G}$ be a simple algebraic group in characteristic p. Let q_0 be a power of p and e a positive integer with $q = q_0^e$. In a special case, we show that we can reduce the computation of the number of p-singular elements in a given coset to the same question for a group over the fixed field of a Frobenius map.

Theorem 5.2. *Let $G = \mathbf{G}(q)$. Assume that e is relatively prime to $|\mathbf{G}(q_0)|$. Let σ be the Frobenius automorphism of order e on $G(q)$. Set $H = \langle G, \sigma \rangle$ and $C = C_G(\sigma)$. Note that C is a group of the same type as $\mathbf{G}$ defined over the field of q_0 elements. The proportion of p-singular elements in the coset σG is equal to $s(C)$.*

Proof. Our hypotheses imply that $(e, |C|) = 1$ (since $C/\mathbf{G}(q_0)$ just involves diagonal automorphisms).

Let $y = \sigma g$ with $g \in G$. It is easy to see ([**GMS**] using (7.2) in [**GL83**]) that y lies in a unique conjugate of $D := \langle C, \sigma \rangle$.

Now assume that $y \in D$ (and so $g \in C$). Thus, y is p-singular if and only if g is. Thus, the number of p-singular elements in the coset σG is precisely $|S(C)||G : C|$ and so the proportion of p-singular elements in the coset is $s(C)$. □

Thus, since $s(C)$ is asymptotically of the form c/q_0 for $c = 1, 2$ or 3 (depending upon the type of $\mathbf{G}$), we see that the probability that a random element in the given coset is p-singular is much higher than for the simple group.

If e is not relatively prime to the order of $\mathbf{G}(q_0)$, the analysis becomes more difficult.

For graph automorphisms, the main case is when $\mathbf{G}$ has type A (for groups of type D, the involutory graph automorphism acts on the natural orthogonal module and an analysis as in section 2 suffices). A modification of the methods of section 2 show that the correct answer is still of the form c/q.

References

[Bor91] A. Borel. *Linear algebraic groups.* Number 126 in Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1991.

[Car72] R.W. Carter. *Simple Groups of Lie Type.* A Wiley-Interscience publication, London, 1972.

[FJ93a] P. Fleischmann and I. Janiszczak. The number of regular semisimple elements for Chevalley groups of classical type. *J. Algebra*, 155:482–528, 1993.

[FJ93b] P. Fleischmann and I. Janiszczak. The semisimple conjugacy classes of finite groups of Lie type E_6 and E_7. *Comm. in Alg.*, 21(1):93–161, 1993.

[FJ94] P. Fleischmann and I. Janiszczak. The semisimple conjugacy classes and the generic class numbers of Chevalley groups of type E_8. *Comm. in Alg.*, 22(6):2221–2303, 1994.

[FJK98] P. Fleischmann, I. Janiszczak, and R. Knörr. The number of regular semisimple classes of special linear and unitary groups. *Linear Algebra Appl.*, 274:17–26, 1998.

[GHL+96] M. Geck, G. Hiss, F. Lübeck, G. Malle, and G. Pfeiffer. CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras. *AAECC*, 7:175–210, 1996.

[GL83] D. Gorenstein and R. Lyons. The local structure of finite groups of characteristic 2-type. *Memoirs, Amer. Math. Soc.* 42, vol. 27, 1983.

[GMS] R. Guralnick, P. Müller, and J. Saxl. The rational function analogue of a question of Schur and exceptionality of permutation representations. *preprint.*

[IKS95] I. M. Isaacs, W. M. Kantor, and N. Spaltenstein. On the probability that a group element is p-singular. *J. Algebra*, 176:139–181, 1995.

[KS] W. M. Kantor and A. Seress. Probabilistic algorithms for finite groups. *preprint.*

[Lüb] F. Lübeck. Parameterization of semisimple conjugacy classes of finite groups of Lie type. *(in preparation).*

[NP] P. Neumann and C. Praeger. Cyclic matrices in classical groups over finite fields. *preprint.*

Prof. Robert Guralnick, Department of Mathematics, University of Southern California, 1042 West 36th Place, DRB 155, Los Angeles, California 90089-1113, USA
Email: guralnic@math.usc.edu

Dr. Frank Lübeck, RWTH Aachen, Lehrstuhl D für Mathematik, Templergraben 64, D-52062 Aachen, Germany
Email: Frank.Luebeck@Math.RWTH-Aachen.De