DERANGEMENTS IN SIMPLE AND PRIMITIVE GROUPS

JASON FULMAN AND ROBERT GURALNICK

Abstract. We investigate the proportion of fixed point free permutations (derangements) in finite transitive permutation groups. This article is the first in a series where we prove a conjecture of Shalev that the proportion of such elements is bounded away from zero for a simple finite group. In fact, there are much stronger results. This article focuses on finite Chevalley groups of bounded rank. We also discuss derangements in algebraic groups and in more general primitive groups. These results have applications in questions about probabilistic generation of finite simple groups and maps between varieties over finite fields.

1. Introduction

Let G be a group and X a transitive G-set. An element of $g \in G$ is called a derangement on X if g has no fixed points on X. We are interested in showing that under certain hypotheses the set of derangements of G on X is large – in particular, we will mainly focus on the case where G is finite. We then define $\delta(G, X)$ to be the proportion of elements in G that are derangements acting on X. The rare situations when $\delta(G, X)$ is very small are also quite interesting and arise in the theory of permutation and exceptional polynomials, coverings of curves and graph theory.

The study of derangements goes back to the origins of permutation group theory. It is an elementary result of Jordan that if X is a finite transitive G-set of cardinality $n > 1$, then $\delta(G, X) > 0$. It is also one of the earliest problems in probability theory – the problem was considered by Montmort in 1708. Diaconis pointed out to us that Frobenius in 1904 showed that $G \leq S_n$ is k-fold transitive if and only if the first k moments of the number of fixed points is equal to the first k moments of a Poisson(1) random variable. He used this to determine character tables of Mathieu groups.

Jordan's result fails if G is infinite. There are various constructions for example where any two nontrivial elements of G are conjugate. Then G contains no derangements in any transitive action with a nontrivial point stabilizer. Another example is the case of $GL(V)$ where V is a finite dimensional vector space over an algebraically closed field and X is the set of subspaces of fixed dimension or more generally X is the set of flags of a given type (every matrix is similar to an upper triangular matrix is the equivalent formulation). The same holds for any connected algebraic group

Guralnick was partially supported by National Science Foundation grant DMS-9970305.
Originally submitted June 25, 2002, revised August 1, 2002.

over an algebraically closed field acting its on flag variety — every element is contained in a Borel subgroup and all Borel subgroups are conjugate.

Derangements have proved to be very useful. In particular, they have applications to images of rational points for maps between curves over finite fields (and more generally to higher dimensional varieties as well). See [GW] for more details. They also are useful in studying probabilistic generation (see [GLSS]). From Chapter 3D of [Dia], one sees that derangements are useful for bounding convergence rates of random walks on finite groups; page 43 gives applications to lower bounds and since character ratios are sometimes fixed point ratios, derangements are relevant to upper bounds as well. We will explore these ideas further in future articles.

Recall that G is called a Frobenius group of degree n if G acts transitively on a set of cardinality n such that no element in G fixes 2 points (and $|G| > n$). Surprisingly, it was only very recently that Cameron and Cohen proved:

Theorem 1.1. [CC] *If X is a transitive G-set of cardinality $n > 2$, then $\delta(G, X) \geq 1/n$ with equality if and only if G is a Frobenius group of cardinality $n(n-1)$ (and in particular, n is a prime power).*

The proof is quite elementary. Another proof of this is given in [GW] and the result is extended in various ways. In particular, it was shown that:

Theorem 1.2. [GW] *If X is a transitive G-set of cardinality $n > 6$, then $\delta(G, X) > 2/n$ unless G is a Frobenius group of cardinality $n(n-1)$ or $n(n-1)/2$ (and in particular, n is a prime power).*

The proof of this result seems to require the classification of almost simple 2-transitive groups (and so the classification of finite simple groups).

Note that when trying to produce lower bounds for the proportion of derangements, there is no loss in assuming that G acts faithfully on X. We will typically make that assumption.

We particularly want to focus on the case of primitive permutation groups and simple and almost simple groups. The Aschbacher-O'Nan-Scott theorem [AS] gives the structure of primitive permutation groups and reduces many questions about them to almost simple groups (groups which have a unique minimal normal subgroup which is nonabelian simple).

A primitive permutation group G of degree n is called affine if it preserves an affine structure on the set. This is equivalent to saying that G has a nontrivial normal elementary abelian p-subgroup N for some prime p. Necessarily, $|N| = n$ is a power of p. In particular, primitive Frobenius groups are always affine permutation groups.

The major part of this paper deals with $\delta(G, X)$ when G is a finite nonabelian simple group. In particular, we will discuss a recent result of the authors proving a conjecture that has been attributed to Shalev. This theorem is proved in a series of papers by the authors starting with this one – see also [FG1], [FG2] and [FG3].

Theorem 1.3. *There exists a positive number δ such that $\delta(G,X) > \delta$ for all finite nonabelian simple groups G and all nontrivial transitive G-sets X.*

Note that it suffices to prove the previous theorem when X is a primitive G-set (for if $f : Y \to X$ is a surjection of G-sets, then $\delta(G,Y) \geq \delta(G,X)$). We also note that as stated this is an asymptotic result – we only need to prove that there exists a $\delta > 0$ such that for any sequence G_i, X_i with $|X_i| \to \infty$ with $\delta(G_i, X_i) > \delta$ for all sufficiently large i. This result is known for G alternating essentially by [D] and [LuP] and for $G = PSL(d,q)$ for a fixed q [Sh] for many families of actions. Shalev's method used some difficult results about the order of a random matrix; we use simpler properties of random matrices.

We will prove much more specific theorems and obtain much better asymptotic results. Our proof shows that we can take δ to be roughly $1/25$ aside from finitely many exceptions (and it is likely that there are no exceptions).

This paper is a partially expository paper regarding variations on this theme in [FG1] and [FG2]. We will discuss in detail analogous results for algebraic groups and give the proof for finite Chevalley groups of bounded rank.

As in [LuP] and [Sh], we obtain results about families of subgroups as well. The following result is proved in [FG1], [FG2] and [FG3].

Theorem 1.4. *Let $X := X_n(q)$ be a classical group of dimension n over $\mathbb{F}_q$. Let $I(X)$ be the union of all proper irreducible subgroups of X except when $X = Sp_{2m}(q)$ we do not include the irreducible subgroups containing $\Omega^{\pm}_{2m}(q)$ with q even. Then $\lim_{n\to\infty} |I(X)|/|X| = 0$.*

In the theorem, we can take X to be a simple classical group or the full conformal subgroup or anything in between. Moreover, we can allow a center. Of course if X is not quasisimple, we only consider maximal subgroups which do not contain $F^*(X)$. In [FG4], we will use this result to obtain some new results about probabilistic generation.

One might think that Theorem 1.3 is valid for almost simple groups. However, examples constructed in [FGS] and [GMS] (coming from problems in coverings of curves) show that the result fails for almost simple groups. We give some examples of this phenomenon later in the paper. The presence of field automorphisms is critical in producing such examples.

However, we do prove that the result on simple groups does lead to a weaker bound for primitive groups which are not affine. See §8.

Theorem 1.5. *Let X be a primitive G-set with $|X| = n$. There exists a positive number δ such that either*

1. *$\delta(G,X) > \delta/\log(n)$; or*
2. *G preserves an affine structure on X.*

We will investigate the affine case in future work.

We will also consider a slight refinement of this problem:

Let G be a normal subgroup of A with A and G acting transitively on a finite A-set X. Assume that A/G is generated by the coset aG.

We wish to investigate the quantity $\delta(A, G, X)$, the proportion of derangements in the coset aG. We note the following easy facts:

(1) the quantity $\delta(A, G, X)$ does not depend on the choice of the generating coset aG; and
(2) $\delta(G, X) = \delta(G, G, X)$.

This quantity is important in studying maps of varieties over finite fields via a Cebotarev density theorem (see [GW] for more details). In contrast to the case $A = G$, there may be no derangements in a given coset. This turns out to be a very special and important case in the study of exceptional covers [FGS] and graph theory [GLPS]. See §6 and §7 for further discussion.

In [GW], the following was shown via an elementary proof:

Theorem 1.6. *Let G be a normal subgroup of A with A/G cyclic. Let X be a transitive A-set of cardinality $n > 2$. Either $\delta(A, G, X) = 0$ or $\delta(A, G, X) \geq 1/n$. Moreover, equality holds if and only if $A = G$ is a Frobenius group of order $n(n-1)$.*

One of the eventual goals of this project is to greatly improve this result.

We now give a brief sketch of the contents and ideas of the paper.

Let G be a group acting primitively and faithfully on the transitive G-set X and let H be the stabilizer of a point $x \in X$. Set

$$\mathcal{C}_G(H) := \cup_{u \in G} uHu^{-1}.$$

An element $g \in G$ is a derangement if and only if $g \notin \mathcal{C}_G(H)$.

The proofs of many of these results are heavily dependent upon the classification of finite simple groups – both in the fact that we are assuming the complete list of finite simple groups and in using information about subgroups of the finite simple groups. Since Theorem 1.3 is really an asymptotic result, we are considering the following situation – we have a sequence (G_i, X_i) where G_i is a finite nonabelian simple group and X_i is a primitive G_i-set of cardinality of n_i. We may assume that $|G_i|$ (or n_i) tends to infinity. We need to show that $\liminf \delta(G_i, X_i) \geq \delta$ for some positive δ (a single δ for all such sequences). This implies that $\delta(G, X) \geq \delta$ for all but finitely many simple G and primitive X, whence $\delta(G, X)$ is bounded away from 0 for all simple G and primitive X.

In [FG1], [FG2] and [FG3], we obtain much stronger results.

By passing to infinite subsequences, to prove Theorem 1.3, it suffices to assume that all the G_i are alternating groups (of increasing degree), are all Chevalley groups of a given type (and rank) over fields of size q_i with $q_i \to \infty$ or are classical groups of dimension d_i over fields of cardinality q_i with $d_i \to \infty$.

In the case of alternating (and symmetric groups), we can apply the work of Dixon [D] and Luczak-Pyber [LuP]. We improve some of these results in [FG1] and [FG2]. In the case of Chevalley groups of fixed type, we can use

the theory of algebraic groups and algebraic geometry to obtain the desired results. Here the dichotomy is between subgroups that contain maximal tori and those that do not. See §2, §3 and §4.

Now consider the case that the G_i are classical groups of dimension d_i over a field of size q_i. We subdivide this case further. First of all, either the $q_i \to \infty$ or we may assume that $q_i = q$ is constant. In the first situation, by [GL], it suffices to consider only semisimple regular elements. We subdivide each case further using the idea of Aschbacher's classification of maximal subgroups of classical groups [A2]. In particular, we consider subspace stabilizers and show that we can reduce certain questions to the study of the Weyl group (and so to symmetric groups). We prove in [FG1] the following result about subspace stabilizers. For the next theorem, in the case of a linear group, all subspaces are considered to be totally singular.

Theorem 1.7. *Let G_i be a sequence of classical groups with the natural module of dimension d_i. Let X_i be a G_i-orbit of either totally singular or nondegenerate subspaces (of the natural module) of dimension $k_i \leq d_i/2$. If $k_i \to \infty$, then $\lim \delta(G_i, X_i) = 1$. If k_i is a bounded sequence, then there exists $0 < \delta_1 < \delta_2 < 1$ so that $\delta_1 < \delta(G_i, X_i) < \delta_2$.*

One of the key ingredients in the proof of Theorem 1.3 for fixed q is getting estimates for the number of conjugacy classes for finite Chevalley groups of rank r over a field of size q. We show that there is an explicit universal constant C so that the number of conjugacy classes of such a group is at most Cq^r – see §9. See also Gluck [Gl] and Liebeck-Pyber [LiP] for weaker estimates. These results are of independent interest and should be useful (see the above mentioned references for some applications). Two other important ideas in the proof are an upper bound for the maximum size of a conjugacy class and a result that says that most elements in a classical group are nearly regular semisimple (i.e. they are regular semisimple on a subspace of small codimension). Another ingredient we use in the proof of Shalev's conjecture (for q fixed) is precise estimates on proportions of regular semisimple elements (proved via generating functions). See [FNP]. Finally, we require results on random permutations.

This article is organized as follows:

We first discuss derangements in algebraic groups (in algebraic actions) – see §2. We then prove Theorem 1.3 for groups of bounded rank in §§3, 4 – the second of which focuses on subgroups containing a maximal torus. As a corollary (§5), we solve for bounded rank groups a problem studied by Dixon [D] and McKay (unpublished) for symmetric groups. The case of classical groups with rank going to ∞ is treated in [FG4]. In §§6, 7, we give some examples and mention the connection with so called exceptional permutation actions and give a short proof of Theorem 1.6. In §8, we then show how Theorem 1.5 follows as a corollary to Theorem 1.3. In the final section, we tabulate some of our results about conjugacy classes for classical groups.

2. Algebraic Groups

In this section, we investigate the existence of derangements in (algebraic) permutation actions for connected algebraic groups. We refer to [H1] for the basic results about algebraic groups.

We first make a simple observation that holds for solvable groups (not just algebraic groups).

Lemma 2.1. *Let G be a solvable group and H a proper subgroup of G. Then $\cup_{g\in G} H^g \neq G$.*

Proof. Let A be the last term in the derived series of G. If $HA \neq G$, we can pass to G/A and the result follows by induction on the derived length (the case of abelian groups being obvious). So assume that $G = HA$ and in particular, H does not contain A. Then $H \cap A$ is normal in G (since $H \cap A$ is normal in H and in the abelian group A). It follows that the only elements in A which have fixed points are the elements of $A \cap H$, a proper subgroup of A. □

We now consider connected algebraic groups. We restrict attention to semisimple groups.

Let G be a connected semisimple algebraic group and X a nontrivial faithful algebraic G-set G/H. In particular, H is a proper closed subgroup of G. Let $J = \cup_{g\in G} H^g$. Let J' denote the complement of J – thus, J' is precisely the set of derangements.

Let T denote a maximal torus of G and N its normalizer. Note that T is self centralizing and N/T is a finite group (the Weyl group of G). Moreover, any two elements of T are conjugate in G if and only if they are conjugate in N. We recall that any two maximal tori of G are conjugate.

Lemma 2.2. *Let G be a connected semisimple algebraic group over an algebraically closed field. Let H be a closed subgroup of G and $J = \cup_{g\in G} H^g$. Then the closure $\bar{J}$ of J is all of G if and only if T has a fixed point on X.*

Proof. Since the set of semisimple elements of G contains an open subvariety of G, the reverse implication is clear.

Assume that J is dense in G. Let S be a maximal torus of the connected component H_0 of H. Let $d = |H : H_0|$.

Since J is the image of the morphism $f : H \times G \to G$ with $f(h, g) = h^g$, it follows that J contains a dense open subset of its closure and so under this hypothesis an open subset of G.

Note that if $g \in G$ is semisimple regular, then the there are at most d^r solutions to $x^d = g$ (where r is the rank of G) – for $x^d = g$ implies that $x \in C_G(g)$, a maximal torus of rank r. This implies that the dth power map on G is dominant and so the set of dth powers of elements in J also contains an open subvariety of G. This implies that the union of the conjugates of H_0 contains an open subvariety of G. Since the union of the conjugates of S

contains an open subvariety of H_0, we have that $\cup_{g\in G} S^g$ contains an open subvariety of G.

By conjugating, we may assume that $S \leq T$. We have the surjection from $G/T \times S \to \cup_{g\in G} S^g$ given by $(gT, s) \to s^g$, whence

$$\dim G = \dim \cup_{g\in G} S^g \leq \dim G + \dim S - \dim T,$$

and so $\dim S = \dim T$ and $S = T$. □

Of course, every element is contained in a Borel subgroup. So if H is a parabolic subgroup (i.e. an overgroup of a Borel subgroup), there are no derangements. We can give an easy proof that these are the only examples if H is connected.

Theorem 2.3. *Let G be a semisimple algebraic group over an algebraically closed field k of characteristic p. Let H be a closed proper subgroup of G. Assume that H is connected or that p does not divide the order of the Weyl group of G (this includes the case $p = 0$).*

(a) *If H contains a maximal torus of G and a regular unipotent element of G, then H is a parabolic subgroup of G.*
(b) *If $\cup_{g\in G} H^g = G$, then H is a parabolic subgroup.*

Proof. If $\cup_{g\in G} H^g = G$, the previous lemma implies that H contains a maximal torus. Clearly, it contains a regular unipotent element, whence (b) follows from (a).

We now prove (a). Let H_0 be the connected component of H. We will first show that H_0 contains a regular unipotent element. We can then reduce to the case that H is connected.

If $p = 0$, this is clear because all unipotent subgroups are connected. Let T be a maximal torus of H_0 (which is also a maximal torus of G). Since all maximal tori of H are H_0-conjugate, it follows that $H = N_H(T)H_0$, whence $|H : H_0| = |N_H(T) : N_{H_0}(T)|$ is a divisor of the order of the Weyl group of G. In particular, it has order prime to p and so H_0 contains all unipotent elements of H.

If H_0 is a parabolic subgroup, then so is H (and indeed $H = H_0$ as any overgroup of a Borel subgroup is a parabolic subgroup). So we may assume that H is connected.

Let B_H be a Borel subgroup of H containing T and let B be a Borel subgroup of G containing B_H. Let U be the unipotent radical of B. Since H is connected, B_H contains a regular unipotent element u as well (because every unipotent element of H is conjugate to an element of U). We can write $u = v\prod U_\alpha(t_\alpha)$ where the α are the simple roots relative to T, $t_\alpha \neq 0$ and $v \in [U, U]$. It follows that $u^T[U, U]$ contains all elements in U which have a nonzero entry in U_α for each simple root α. Thus, $[u, T][U, U] = U$. Since U is nilpotent, this implies that $U = [u, T]$ and so $B = TU \leq H$. Thus, $B_H = B$ and $H \geq B$ as required. □

There are only a handful of examples of proper closed nonconnected subgroups containing a conjugate of every element of G. This requires a result of Saxl and Seitz. We note that the result of [SaSe] has the unneeded hypothesis that the characteristic is good (their proof never uses this fact). We will use the following fact in the next result – any positive dimension closed subgroup of a simple algebraic group is contained in a maximal closed subgroup.

Theorem 2.4. *Let G be a simple algebraic group over an algebraically closed field k of characteristic p. Let H be a closed proper subgroup of G. Assume that H is not contained in a parabolic subgroup. The following are equivalent:*

(a) *H contains a maximal torus of G and a conjugate of every unipotent element of G;*
(b) *H contains a conjugate of every element of G;*
(c) *The characteristic of k is 2 and $(G, H) = (Sp(2m, k), O(2m, k))$ or $(G, H) = (G_2(k), A_2(k).2)$.*

Proof. Clearly (b) implies (a).

We next show that (a) implies (c). So assume that H satisfies (a). If H is maximal (among closed subgroups), then Theorem C of [SaSe] shows that (c) holds.

Let M be a maximal closed subgroup of G containing H. Then (G, M) satisfies the conclusion of (a) as well and so as noted, (G, M) satisfies (c). In particular, k has characteristic 2. Moreover, H must have maximal rank and is not connected.

If $G = G_2(k)$ and H is a proper (disconnected) rank 2 subgroup of M, then the only possibility is that H is contained in the normalizer of a maximal torus, which does not contain a conjugate of every unipotent element.

So we may assume that $G = Sp(2m, k)$. If $m = 1$, then M is the normalizer of a maximal torus T and M/T has order 2 and so clearly $H = M$. So consider the case that $G = Sp(2m, k), m \geq 2$. If H acts reducibly on the natural module V for G, then H is contained in the stabilizer of a proper subspace W. Take W of minimal dimension. Since H is not contained in a parabolic subgroup, it follows that this subspace is nondegenerate. The stabilizer of such a subspace is not contained in a conjugate of M, a contradiction.

Suppose that the connected component H_0 does not act irreducibly on V. Then either H is contained in a maximal subgroup not contained in $O(2m, k)$, a contradiction or $V = W_1 \oplus W_2$, where H_0 is irreducible on each W_i and W_i is a maximal totally singular subspace of dimension m. Thus, H is contained in the stabilizer of a pair of complementary totally singular subspaces. We claim that H contains no transvections. A transvection in H cannot swap the two spaces and so would have to stabilize each W_i. The action on W_1 is dual to that on W_2 and so the element is not a transvection.

Thus, H_0 acts irreducibly on V, whence H_0 is semisimple. Since H has rank m, this forces H_0 to contain the connected component of $O(2m,k)$, whence $H = O(2m,k)$.

All that remains is to verify that (c) implies (b).

This is well known for the first family (see [SaSe], Lemma 4.1) The latter case is an easy consequence of the first case (since $G_2(k) \leq Sp(6,k)$, $Sp(6,k) = O(6,k)A_2.2$ and $A_2.2 = G_2(k) \cap O_6(k)$). □

3. Groups of Bounded Rank I

In this section and the next, we consider the case where the groups have bounded rank. We will prove Theorem 1.3 in this case. The next section deals with subgroups containing a maximal torus. We deal with the other cases in this section.

As we have observed, as stated it is an asymptotic result. We only need to produce a δ so that the proportion of derangements is at least δ for all but finitely many cases. If this fails, there would be a sequence with the proportion of derangements all less than δ. Thus, Theorem 1.3 is an asymptotic result (as noted, eventually we want a non-asymptotic version). Since the groups have bounded rank, we may assume that they have fixed type $X(q_i)$ with X a simple algebraic group and only the field size is varying. We can use methods of algebraic geometry and algebraic groups to study this situation.

We recall that $F^*(H)$ is the generalized Fitting subgroup of H. See [A1]. In particular, $F^*(H)$ simple just means that $F^*(H) \leq H \leq \mathrm{Aut}(H)$. There is no harm in considering covering groups of almost simple groups since all the maximal subgroups will contain the center.

Fix a type of simple algebraic group X of rank r. Let σ be an endomorphism of X with fixed point group X_σ of finite order. We will typically write $X(q) = X_\sigma$ if q is the absolute value of the eigenvalues of σ on the character group of the maximal torus T of X. In the case of the Suzuki or Ree groups q will not be an integer. This will cause no problems. Indeed, in those cases, one knows all the maximal subgroups and it is quite easy to obtain our results. We may take X simply connected or of adjoint type or anything in between – this allows us to obtain results for Chevalley groups generated by inner-diagonal automorphisms.

The maximal subgroups H of $X(q)$ (which do not contain $F^*(X(q))$) are of four types:

(1) $|H| < N$ for some fixed $N = N(X)$;
(2) $H = N_{X(q)}(X(q'))$ for some q' dividing q (this includes the twisted forms, e.g., ${}^2E_6(q) \leq E_6(q^2)$);
(3) $H = Y_\sigma$ where Y is a proper σ-invariant algebraic subgroup of X of rank $s < r$ and the connected component of Y is semisimple;
(4) $H = Y_\sigma$ where Y is a proper σ-invariant algebraic subgroup of X of maximal rank r.

This is well known for the case of classical groups (see [A2]). If H is of exceptional type, this follows in a very precise way from results of Liebeck and Seitz [LS1]. See the remarkable paper of Larsen and Pink [LaP] for a classification free proof of the previous result. Note that if Y is a maximal σ-invariant positive dimensional algebraic subgroup, then either Y has maximal rank or the connected component of Y is semisimple (for if the unipotent radical of Y is nontrivial, Y is a parabolic subgroup by the Borel-Tits theorem and if it contains a normal torus, then Y contains a maximal torus).

We also note the following result.

Lemma 3.1. *If X is a simple connected algebraic group and Y is a proper positive dimensional σ-invariant subgroup , then Y is contained in a maximal proper closed σ-invariant subgroup. Moreover, there is a bound $m = m(X)$ for the number of connected components for any maximal σ-invariant closed subgroup.*

Proof. Let Y_1 be a proper closed σ-invariant subgroup of X containing Y that has maximal dimension. Let Y_0 be the connected component of Y_1. Then $N_X(Y_0)$ is maximal among σ-invariant closed subgroups (for any such overgroup would have the same dimension as Y_0 whence would have connected component Y_0).

All that remains is to prove the statement about the number of components. So we may assume that Y is a maximal proper closed σ-invariant subgroup. If Y_0 has a unipotent radical, then Y is contained in a parabolic subgroup and in particular is connected.

So assume Y_0 is reductive. If Y_0 is not semisimple, then the connected component of $Z(Y_0)$ is a nontrivial torus and Y is contained in the normalizer of this torus, whence we may take Y to be the normalizer of this torus. Thus, Y_0 contains a maximal torus and so contains its centralizer (which is contained in the maximal torus). By the Frattini argument, any closed subgroup containing a maximal torus has at most $|W|$ components, where W is the Weyl group of X.

So we may assume that Y_0 is semisimple. Let $C = C_X(Y_0)$. Then C is finite (since $C \cap Y_0$ is finite). If X is classical and Y_0 is not simple acting irreducibly on the natural module, then the result follows by [A2] which gives all possibilities for Y (although the fields are assumed to be finite, the proofs go through without change for the algebraic closure – see [LS3] for a treatment of the algebraic group case). If Y_0 is simple acting irreducibly, then $C \leq Y_0$ and Y/Y_0 is bounded by the size of the (algebraic) outer automorphism group and so has order at most 6.

If X is exceptional, all such maximal subgroups are classified (see [LS2], Corollary 2 – we only need to handle the case where $F^*(Y)$ is not quasisimple, such maximal subgroups were classified much earlier) and the result follows by inspection. □

Let $\mathcal{M}_i$ denote the maximal subgroups in the corresponding families $i = 1, 2, 3$ or 4 above.

We will deal with each of these families separately. In this section, we deal with the first three cases. In the next section, we deal with the remaining case. The purpose of this section is to prove:

Theorem 3.2. $\lim_{q\to\infty} |\cup_{i=1}^{3} \cup_{M\in\mathcal{M}_i} M|/|X(q)| = 0$.

This is not true for $\mathcal{M}_4$ (compare with the result Lemma 2.2 for algebraic groups). We first start with some general known results.

Lemma 3.3. *Let U be a unipotent connected group of dimension r defined over the finite field F_q. Let $\tau = g\sigma$ where g is an algebraic automorphism of U and σ is the q-Frobenius map. Then $|U_\tau| = q^r$.*

Proof. Suppose that Y is a connected τ invariant subgroup of U. The result would follow by induction and Lang's theorem (since $|U_\tau| = |Y_\tau||(U/Y)_\tau|$). So we may assume this is not the case. It follows that U is abelian of exponent p (where p is the prime dividing q). Then X is just a product of copies of the field and another application of Lang's theorem (applied to $\mathrm{Aut}(X)$) gives that τ and σ are conjugate via an element of $\mathrm{Aut}(X)$ and the result follows. □

Lemma 3.4. *Let $x \in X(q)$. Let C be the centralizer of x in $X(q)$.*

1. *If x is unipotent, then $|C|$ is divisible by q^r.*
2. *$|C| \geq (q-1)^r$.*

Proof. If x is unipotent, the result follows since all unipotent classes are known as well as their centralizers. Aside from the cases of Suzuki and Ree groups, this also follows from the previous lemma. Let B be a σ invariant Borel subgroup with unipotent radical U containing x and consider the connected component of $C_U(x)$. Since regular unipotent elements are dense in B, it follows that $\dim C_B(x) \geq r$ and so C has order divisible by the cardinality of the subgroup of fixed points in $C_U(x)$. By the previous lemma (applied to σ acting on U), this cardinality is divisible by q^r. A variation of the previous lemma could be applied to the case of Suzuki and Ree groups.

We note that the result holds for semisimple groups as well.

We prove the second statement more generally for reductive groups of rank r. Write $x = su = us$ with u unipotent and s semisimple. Pass to the connected component of D of $C_X(s)$. This is still reductive of rank r. Write $D = AB$ with A a central torus in C and $B = [C, C]$ semisimple with A of rank a and B of rank b. Since a torus of rank a over the field of q elements has at least size $(q-1)^a$ and $C_{B(q)}(u)$ has order divisible by q^b, we see that $|C| \geq (q-1)^a q^b$, whence the second statement holds. □

The following was originally proved by Steinberg in the case of simply connected X. See [Ca] or [H2].

Lemma 3.5. *The number of conjugacy classes of semisimple elements in $X(q)$ is at most q^r with equality if X is simply connected.*

The next result follows from [GL].

Lemma 3.6. *The proportion of regular semisimple elements in $X(q)$ is greater than $1 - 5/(q-1)$.*

The previous result indicates that the proportion of elements which are not semisimple regular goes to 0 linearly with $1/q$. The same is thus true for the set of derangements which are not semisimple regular. Thus, it suffices to consider the set of derangements which are semisimple (and indeed regular). We will do so in the next two sections without further comment.

Lemma 3.7. $|\cup_{M\in\mathcal{M}_1} M|/|X(q)| \to 0$ *as* $q \to \infty$.

Proof. $\cup_{M\in\mathcal{M}_1} M$ is a union of at most N' conjugacy classes of elements for some N' (that depends only on N and so only on X). Thus the union has order at most $|X(q)|N'/(q-1)^r$ and the result follows. □

Lemma 3.8. $|\cup_{M\in\mathcal{M}_2} M|/|X(q)| \to 0$ *as* $q \to \infty$.

Proof. Consider $X(q')$. The number of semisimple conjugacy classes in $X(q')$ is at most $(q')^r$. Let $S(q', q)$ denote the union of the semisimple conjugacy classes of $X(q)$ intersecting $X(q')$. Thus,

$$|S(q', q)| \leq |X(q)|(q')^r/(q-1)^r.$$

In the case of the Suzuki or Ree groups, we write $X = X(p^{2a+1})$ (this conflicts slightly with our notation above). The number of possible classes of subfield groups is the number of distinct prime divisors of $2a+1$, whence the estimate above shows that the union of the semisimple elements in any subfield group is certainly at most $\sum_b |X(q)|q^{r/b}/(q-1)^r$, where b ranges over prime divisors of $2a+1$. This yields the result.

Consider the remaining cases. Write $q = p^a$. Note that for each choice of q' (corresponding essentially to a prime divisor of a), there are at most $2c$ choices for $S(q, q')$ where c is the order of the group of outer diagonal automorphisms ($6c$ in case $X = D_4$). This is because we may take $\sigma = \alpha\tau f_{q'}$ where τ is a graph automorphism, α is a diagonal automorphism and f_q is the standard Frobenius (any two such elements in the coset with the same order are conjugate up to diagonal automorphisms – see I.7.2 [GoLy]). In fact as noted above, we only need to consider semisimple elements, the diagonal outer automorphisms will not make a difference, but we do not need to use this. □

Lemma 3.9. $|\cup_{M\in\mathcal{M}_3} M|/|X(q)| \to 0$ *as* $q \to \infty$.

Proof. It follows by the theory of high weights if X is classical [GKS] and by [LS2] if X is exceptional that there are only finitely many conjugacy classes (with a bound depending only upon X) in $\mathcal{M}_3$. Thus, it suffices to show the result for a fixed type of subgroup $Y < X$. Then Y_σ has at most cq^s conjugacy classes of semisimple elements (where c is the number of connected components of Y – note that c is bounded in terms of X). It follows that $|\cup_{g\in X_\sigma} Y_\sigma^g| \leq |X_\sigma|cq^s/(q-1)^r$, whence the result. □

This completes the proof of Theorem 3.2. The next section deals with $\mathcal{M}_4$.

4. Maximal Rank Subgroups

In this section we consider $\mathcal{M}_4$. It follows from the results on algebraic groups that the proportion of derangements will be positive in this case. For the Suzuki and Ree groups, one just inspects the maximal rank subgroups and the result about derangements follows quite easily. We assume for the rest of the section that we are not in any of those cases. We remark again that it suffices to consider only regular semisimple elements (since as $q \to \infty$, the proportion of regular semisimple elements is $1 + O(1/q)$).

Keep notation as in the previous section. Let Y be a σ-stable subgroup of X of maximal rank and $H = Y_\sigma$. The possibilities are that Y is a parabolic subgroup (maximal with respect to being σ-stable) or is reductive. Let Y_0 denote the connected component of Y. Let $H_0 = (Y_0)_\sigma$. This is a normal subgroup of H.

There exists a σ-stable maximal torus T contained in a Borel subgroup B of X. A maximal torus of X_σ is S_σ where S is a σ-stable maximal torus of X. There is a notion of nondegenerate maximal tori (for example, if $X = SL(n)$, then over the field of 2-elements, a maximal torus might be trivial, see §3.6 in [Ca] for details). We will just note that if the maximal torus contains a regular semisimple element, then $N_{X_\sigma}(S_\sigma) = N_X(S)_\sigma$ – this follows since $S = C_X(S_\sigma)$. Moreover (for fixed X), if q is sufficiently large, all maximal tori contain regular semisimple elements (indeed almost all elements are regular semisimple).

Let W be the Weyl group of G (more precisely identify $W = N_X(T)/T$). Consider the semidirect product $W\langle\sigma\rangle$. There is a bijection between conjugacy classes of maximal tori in X_σ and W-classes of elements in the coset σW (see [SpSt] or [Ca]). In particular, if σ is a field automorphism, σ commutes with W and so the correspondence is with W-conjugacy classes (this latter fact is still true for all groups of type A and type D_n with n odd).

Let T_w denote a maximal torus of X_σ corresponding to σw. Let N_w be the normalizer in X_σ of T_w. Then $|N_w : T_w| = |C_W(\sigma w)|$. Let $f(w)$ be the size of W-class of σw. So $f(w) = |W : C_W(\sigma w)| = |W||T_w|/|N_w|$.

In particular, we see that

$$|\cup_{g\in X_\sigma} T_w^g|/|X_\sigma| < |T_w|/|N_w| = f(w)/|W|.$$

Since a semisimple regular element lies in a unique maximal torus, it follows that the union of all regular semisimple elements of X_σ that are conjugate to an element of T_w has cardinality at most $|X_\sigma|f(w)/|W|$.

Since the proportion of elements which are not semisimple regular tends to 0 as $q \to \infty$ and the same is true for each maximal torus, it follows that the inequality above becomes equality as $q \to \infty$.

We first show that the collection of elements which are conjugate to an element of H but not H_0 is small. We need the following result. A very easy

result (see Proposition 4.3 below) gives an upper bound (always at least 1/2) for the proportion of derangements contained in H_0 (assuming that $H \neq H_0$).

Lemma 4.1. *Let G be a connected reductive algebraic group with σ an endomorphism of G such that G_σ is finite. Assume that all eigenvalues of σ on the character group of T have absolute value q. Let S and T be distinct σ-stable maximal tori of G. Then $|T_\sigma : (S \cap T)_\sigma| \geq (q-1)/2$.*

Proof. Consider a counterexample with $\dim G$ minimal. Since G is reductive, G is the central product of Z and H where H is semisimple and Z is the connected component of the center of G. Since Z is contained in every maximal torus, there is no loss in taking $G = H$ to be semisimple. We can replace G by its universal central extension (since the center will be contained in every maximal torus) and so assume that G is a direct product of simply connected simple algebraic groups.

If $S \cap T = Z(G)$, the result is clear (pass to the simple case). Otherwise, we can consider $H = C_G(x)$ with $x \in S \cap T \setminus Z(G)$. Then H is connected and reductive and S, T are maximal tori in H. □

Note that if $G = SL(2)$, we do have equality in the previous result.

Proposition 4.2.

$$\lim_{q \to \infty} | \cup_{g \in X_\sigma} (Y \setminus Y_0)_\sigma^g | / |X_\sigma| = 0.$$

Proof. It suffices to consider a single coset yY_0 for some element $y \in Y_\sigma \setminus Y_0$.

We will obtain an upper bound on the number of conjugacy classes of semisimple regular elements of X_σ that intersect yY_0. We will do this by bounding the number of Y_σ classes in that coset.

Suppose that $u \in yY_0 \cap X_\sigma$ is a semisimple regular element. Then the centralizer of u in the algebraic group is a σ-stable maximal torus T. Let S be a σ stable maximal torus of Y_0 containing $T \cap Y_0$. The number of $(Y_0)_\sigma$ conjugates of u is

$$|(Y_0)_\sigma : (S \cap T)_\sigma| \geq |(Y_0)_\sigma|(q-1)/2|S_\sigma|.$$

Since $|S_\sigma| \leq (q+1)^r$, it follows that the number of conjugates of u in the coset $u(Y_0)_\sigma$ is at least $|(Y_0)_\sigma| q^{r-1}/2$ (up to a small error term). This implies that there are at most $2q^{r-1}$ classes of semisimple regular elements in this coset (again up to a term of smaller order). Since each class has size approximately $O(|X_\sigma|)/q^r$, the union of these classes has size $O(|X_\sigma|/q)$ as required. □

We now consider the connected component Y_0 and its fixed points H_0. We first note that if $H_0 \neq H$, then we have the following easy estimate for derangements.

Lemma 4.3. *If $H \neq H_0$, then $| \cup_{g \in X_\sigma} H_0^g | / |X_\sigma| < 1/|H : H_0| \leq 1/2$.*

Proof. Since H normalizes H_0, $\cup_{g\in X_\sigma} H_0^g$ is the union where g ranges over a transversal of X_σ/H, whence the cardinality of this union is less than $|X_\sigma : H||H_0| = |X_\sigma/|H : H_0|$. □

We just remark that Lang's theorem implies that $|H : H_0|$ is the number of σ-stable cosets of Y_0 in Y.

Let S be a σ stable maximal torus of Y_0. Then $S = xTx^{-1}$ where $x^{-1}\sigma(x) \in N(T)$. Note that $x^{-1}N(S)x = N(T)$. So we have subgroups $T \leq x^{-1}N_H(S)x \leq x^{-1}N_Y(S)x \leq N(T)$ and this gives rise to corresponding subgroups $1 \leq W_0 \leq W_1 \leq W$ in W the Weyl group of T.

The σ-stable maximal tori of H (up to H_σ-conjugacy) are of the form $ySy^{-1} = yxT(yx)^{-1}$ where $v := y^{-1}\sigma(y) \in N_H(S)$. Moreover, we see that S is conjugate to T_w where

$$w = (yx)^{-1}\sigma(yx)T = x^{-1}y^{-1}\sigma(y)\sigma(x) \in \tau W_0,$$

where $\tau = x^{-1}\sigma(x)T \in W$.

Thus, setting R to be the union of all X_σ conjugates of maximal tori of H_σ, we see that $|R|/|X_\sigma| \leq \sum f(w)/|W|$ where the sum is a set of representatives Γ of conjugacy classes in W that are represented by elements in τW_0.

We note that R is precisely the set of conjugacy classes of regular semisimple elements conjugate to an element of H_σ (since the centralizer of such an element will be a maximal torus in H). Thus, we have an upper bound for the proportion of regular semisimple elements in X_σ that are not derangements in X_σ/Y_σ. By Proposition 4.2, we can replace H_σ by Y_σ (up to an $O(1/q)$ term) and we can consider all elements (not just regular semisimple elements) by introducing another such term (by [GL]) and so we see that $\delta(X_\sigma, Y_\sigma) \geq 1 - \sum_{w\in\Gamma} f(w)/|W| + O(1/q)$. We just need to bound $\sum_{w\in\Gamma} f(w)/|W|$ away from 1.

There is one very easy case – if σ does not involve a graph automorphism and $W_1 \neq W$, then $1 - \sum_{w\in\Gamma} f(w)/|W| \leq \delta(W, W/W_1)$. Note in this case $f(w)$ is just the size of the W-conjugacy class of w. This can be computed for the exceptional Weyl groups. In any case, for bounded rank, we can even use the Jordan bound to see this is bounded away from 1. For classical groups, using [D], [LuP], [FG1], [FG2] we see that this quantity will typically be at most 2/3.

If σ does involve a graph automorphism, then we consider the group Z defined above. Since σ stabilizes both W_1 and W_0, we can define Z_1 and Z_0 in an obvious manner. Note that in this case $f(w)$ is the size of the W-class of σw. Thus, we still have a bound $1 - \sum_{w\in\Gamma} f(w)/|W| \leq \delta(Z, W, Z/Z_1)$.

We note by inspection that unless $W = W_1$, there are always derangements in the coset σW. Since except for type D_4, W can be thought as of a subgroup of index 2 in Z (only the graph automorphism makes a difference), exceptionality would force $|W : W_1|$ to have odd index.

There are only a few cases where $W = W_1$. In all cases, we see that whenever this happens $H \neq H_0$ and so the upper bound of $1/2 + O(1/q)$

holds. One possibility is that H is a maximal torus. In that case, we note directly that $f(w)/|W| \leq 1/2$. Another possibility is $X = G_2$ and $H = A_2$. Similarly, there is the possibility of $(X, Y) = (F_4, D_4)$.

The only other such possibility for X classical is in characteristic 2 with X of type B_n and Y of type D_n. Then W_0 has index 2 in $W = W_1$. In this case, one sees that there are two possible forms of Y_σ (i.e. two conjugacy classes corresponding the single X_σ class of σ stable conjugates of Y) – the two forms of orthogonal groups. One form of the orthogonal group has maximal tori T_w with $w \in W_0$ and the other the complement (note a maximal torus is contained in a unique orthogonal group in the symplectic group). Thus, $\delta(Sp(2m, 2^a), O^\epsilon(2m, 2^a)) = 1/2 + O(1/2^a)$.

We note that our analysis works for any form of the Chevalley group and for any fixed coset in the group of inner-diagonal automorphisms.

Thus, we have proved:

Theorem 4.4. *Let r be a positive integer. Let S be a simple Chevalley group of rank at most r over the field of q elements and $S \leq G$ with G contained in the group of inner-diagonal automorphisms of S. Let X be a transitive faithful G-set. Then there exists $\delta > 0$ such that $\delta(G, S, V) \geq \delta + O(1/q)$ for any transitive G-set V.*

We will give an explicit δ in the sequel. Note that the error term depends only on r (and we do remove that dependence in [FG1], [FG2] and [FG3]).

If X is classical, then the possibilities for Y are rather limited. There is the special case in characteristic 2 when X is symplectic and Y is an orthogonal group. The remaining cases are essentially when Y_σ is the group preserving a decomposition of the space or Y_σ is an extension field group (both forms of $Y \leq C \wr S_m$ where C is a classical group on a subspace). In the bounded rank case, we have seen that we could work with the connected piece.

If the rank increases, there are two added complications. If q is fixed, then we can no longer deal with only semisimple regular elements (the error term may be larger than the main term). Even if q increases, the error term associated with reducing to the connected component may be increasing with the rank. Thus, the analysis is much more difficult. See [FG1] and [FG2]. We also want to produce an explicit δ that is valid for either all cases or all but a specified finite set of cases.

We close this section by considering a few examples.

(1) Let $G = PSL(n, q)$ and let H be the stabilizer of a k-dimensional vector space. In this case H is the set of fixed points of a connected subgroup and so we see from the analysis above that for a fixed n, $\lim_{q\to\infty} \delta(G, H) = \delta(S_n, Y_k)$ where $Y_k = S_k \times S_{n-k}$ is a Young subgroup. By [D], $\delta(S_n, Y_k) \geq 1/3$ and by [LuP] (and also by [FG1]), $\delta(S_n, Y_k) \to 1$ as $k \to \infty$ (for $k \leq n/2$). This example holds more

generally for any parabolic subgroup – the limiting proportion of derangements is precisely the proportion of derangements of the Weyl group acting on the cosets of the corresponding parabolic subgroup.

(2) Let $G = Sp(2n, q)$ with q even. Let $H = O^\epsilon(2n, q)$. Then H is the set of σ fixed points on some σ invariant conjugate of $O(2n) < Sp(2n)$. The Weyl group of the connected component of $O(2n)$ has index 2 in the Weyl group of $Sp(2n)$ and so we see that $\lim_{q\to\infty} \delta(G, H) = 1/2$ (each type corresponds to maximal tori in one coset of the Weyl group of Ω). Note that a regular semisimple element is contained in precisely one orthogonal group.

(3) Let $G(q) = E_8(q)$ and $H(q) = D_8(q)$. Since the corresponding algebraic subgroup is connected, it follows that

$$\lim_{q\to\infty} \delta(G(q), G(q)/H(q)) = \delta(W(E_8), W(D_8)).$$

5. Generation and Derangements

In this section, we indicate how some generation results follow immediately from our results. See [FG4] for more results about probabilistic generation that follow from the results in this paper, [FG1], [FG2] and [FG3].

If G is a finite simple group, set $P_G(x)$ the probability that a random $y \in G$ satisfies $G = \langle x, y\rangle$. Let P_G be the minimum of $P_G(x)$ over all nontrivial x. It follows by [GK] that $P_G > 0$. One can easily deduce the following result (a special case of [GLSS]):

Theorem 5.1. *Let X be a type of simple algebraic group. Then one has that $\lim_{q\to\infty} P_{X(q)} = 1$.*

Recall that a group G is generated *invariably* by the elements $x_1, \cdots, x_m$ if the elements $y_1, \cdots, y_m$ generate G whenever y_i is conjugate to x_i for $i = 1, \cdots, m$. Luczak and Pyber [LuP] proved the following conjecture of McKay, useful in computational Galois theory. (We make the constants in Theorem 5.2 more explicit in forthcoming work).

Theorem 5.2. *(*[LuP]*) There exists N so that for all $n \geq N$ and all $\epsilon > 0$, there is a constant $C = C(\epsilon)$ so that C permutations, chosen from S_n uniformly and independently, generate S_n invariably with probability at least $1 - \epsilon$.*

For Chevalley groups of bounded rank, we have the following result.

Theorem 5.3. *Let X be a type of simple algebraic group. For any $\epsilon > 0$, there is a constant $C = C(\epsilon)$ (not depending upon q) so that C elements, chosen from $X(q)$ uniformly and independently, generate $X(q)$ invariably with probability at least $1 - \epsilon$.*

Proof. The probability that some $y_1, \ldots, y_m$ generate a maximal subgroup in $\mathcal{M}_i, i \leq 3$ tends to 0 as $q \to \infty$ by Theorem 3.2. Indeed our proof shows that this probability is $O(1/q^m)$. There are at most d (depending only on X) conjugacy classes of maximal subgroups in $\mathcal{M}_4$ and the probability that

some conjugate of a random element $x \in G$ is contained in one is at at most $1-\delta$ for some $\delta > 0$ (for some δ depending only on X). Thus, the probability that some collection of y_i are contained in one of these maximal subgroups is at most $d(1-\delta)^m$. So for q sufficiently large, we can choose an m so with probability greater than $1-\epsilon$, m random elements invariably generate $X(q)$. Note that we are ignoring the possibility that $X(q)$ may not be simple – however, this quotient is bounded in terms of X and so is not a problem. □

We will prove the analogous result for classical groups of unbounded rank in a future article.

6. Exceptionality and Derangements

In this section, we discuss the notion of exceptional permutation representations and its connection to curves. See [GMS] for a more elaborate discussion of these ideas.

Let G be a normal subgroup of A. Let X be a transitive A-set that is also transitive for G. We say that (A, G, X) is exceptional if A and G have no nontrivial common orbits on $X \times X$ (the trivial orbit being the diagonal). We note the following easy example. See [GMS] for more examples and some classification theorems.

Recall that a Hall subgroup H of a finite group G is a subgroup with $\gcd(|H|, |G:H|) = 1$.

Theorem 6.1. *Let A be a finite group and G a normal Hall subgroup. Then $A = GD$ for some complement D (by the Schur-Zassenhaus theorem). Let $H = N_A(D)$ and $X = A/H$. Then (A, G, X) is exceptional.*

Proof. Suppose not. We can identify X with the set of conjugates of D. Let $K = C_G(D) = G \cap H$. It is easy to see that exceptionality is equivalent to K and H having no common orbit (other than D itself). Suppose $D \neq E$ is in a common orbit. Then the length of this orbit divides $|K|$ and in particular has order prime to $|D|$. Thus, $|H : N_H(E)|$ has order prime to D, whence $N_H(E)$ contains a Hall π-subgroup D_1 of H (where π is the set of primes dividing $|D|$). Since D and D_1 are both Hall π-subgroups of H, they are conjugate in H (by the Schur-Zassenhaus theorem), whence D normalizes some K-conjugate of E. So we may assume that D normalizes E. Then DE is a π-subgroup, whence $D = E$, a contradiction. □

In particular, this result applies to the case G is a Chevalley group defined over the field of q^b elements, b is relatively prime to $|G|$ and we take D to be the cyclic group of order b of field automorphisms of G. Specifically, take $G = L(2, p^b)$ with b any prime not dividing $p(p^2-1)$. See [GMS]. In this family of examples, the degree of the permutation representation has size less than p^{3b} and the proportion of derangements is less than $1/b$ (since all derangements are contained in G and $|A : G| = b$). Thus, even for almost simple groups acting primitively, the proportion of derangements can be

less than any given $\epsilon > 0$. The best general result one could hope for is $\delta(A, X) > C/\log|X|$. See §8 for such a result.

Some easy facts about exceptional triples are (see [FGS], [GW], [GMS]):

(1) If A/G is generated by the coset aG, then (A, G, X) is exceptional if and only if every element in the coset aG has a unique fixed point or equivalently $\delta(A, G, X) = 0$.
(2) If A/G is cyclic and (A, G, X) is exceptional, then so is (A, G, Y) where Y is the image of a morphism of A-sets from X is an A-morphism.

In particular, if A/G has prime order and (A, G, X) is exceptional, then $\delta(A, X) < |G|/|A|$ (since all derangements are contained in G).

So the analog of Shalev's conjecture for almost simple groups fails. In future work, we hope to obtain a result that says that Shalev's conjecture holds except for certain primitive actions (mostly related to the case where the point stabilizer is the set of fixed points of some Lang-Steinberg endomorphism of an algebraic group).

As we have remarked, $\delta(A, G, X)$ is related to images of rational points for maps between curves and higher dimensional varieties over finite fields. The connection is through the following estimate that follows from the Cebotarev density theorem (see [GTZ] or [GW] for more details).

We make this more precise.

Let U, V be smooth projective curves defined over $F := F_q$ the field of q elements. Let $U(q^a)$ denote the F_{q^a} rational points of U. Let $f : U \to V$ be a separable rational map of degree n also defined over F. Let $F(U)$ and $F(V)$ be the function fields of U and V over F. Let A be the arithmetic monodromy group of this cover (i.e. A is the Galois group of the Galois closure of $F(U)/F(V)$) and G the geometric monodromy group of the cover (the subgroup of A which acts trivially on the algebraic closure of F). Let H be the subgroup of A trivial on $F(U)$ (so $|A : H| = n$). Note that A/G is cyclic. Let xG be a generator for A/G. It follows from the Cebotarev density theorem (cf. [GTZ]) that:

Theorem 6.2.

$$|f(U(q_a))| = 1 - \delta(\langle x^a, G\rangle, G, H) + O(q^{a/2}).$$

The special case where $\delta(\langle x^a, G\rangle, G, H) = 0$ gives rise to exceptional covers. In this case, it is not difficult to show that f is in fact bijective on rational points. Of course, this cannot be the case if $x^a \in G$. See [FGS], [GMS] and [GSa] for more about exceptional covers. By [GSt], any group theoretic solution does give rise to some cover of curves with the appropriate property.

7. Derangements in a Coset

In this section, we present a proof of the Guralnick-Wan result – Theorem 1.6 that is a bit different than the one given in [GW]. It is more in the spirit

of the proof in [CC] and an unpublished proof of Marty Isaacs (both for the case $A = G$).

Let G be a normal subgroup of A with A/G generated by aG. Suppose that A and G both act on the finite set X. Let $f(g)$ be the number of fixed points of g on X. We note the following well known easy result (cf. [GW]).

Lemma 7.1. *$\sum_{g\in G} f(ag) = |G|c$, where c is the number of common A, G-orbits on X.*

Now suppose that A and G are both transitive on X (and so in particular $c = 1$ in the previous result). Let H be the stabilizer of a point and set $K = H \cap G$.

Let Δ denote the derangements in the coset xG. There must be some element in the coset with a fixed point and so we may assume that $a \in H$.

We split xG into three disjoint sets, xK, Δ and Γ (the complement of the union of xK and Δ).

Breaking up the sum into the sum into two pieces, one over xK and the other the remaining terms, we see that

$$|G| = \sum_{g\in K} f(ag) + \sum_{xg\in\Gamma} f(ag) \geq c|K| + |G| - |K| - |\Delta|,$$

where d is the number of common H, K orbits on X (of course, $d \geq 1$).

This yields $|\Delta| \geq (d-1)|K|$ or $\delta(A, G, X) \geq (d-1)/n$.

If $d = 1$, then it is easy to see that Δ is empty (using the fact that the average number of fixed points is 1). So we obtain:

Theorem 7.2. *If (A, G, X) is not exceptional, then $\delta(A, G, X) \geq 1/n$.*

If $d \geq 3$, we see that $\delta(A, G, X) \geq 2/n$. It would be interesting to characterize those groups where $d = 2$ (this includes the case where G is 2-transitive) and classify the actions where $\delta(A, G, X) \leq 2/n$ (presumably only Frobenius groups and exceptional actions).

8. Primitive Groups

As we have seen in the previous section, we cannot hope to extend Shalev's conjecture to the almost simple case. There are many more examples in case of affine primitive groups and also diagonal actions (again related to exceptionality – see [GMS] for examples).

In this section we show how one can obtain a weaker result for primitive groups with no normal abelian subgroup (so in particular as long as the degree is not a prime power). The example in the previous section shows that one can do no better than this theorem. We do hope to classify which primitive representations have few derangements.

Theorem 8.1. *Let G be a primitive group of degree n and assume that G has no normal abelian subgroup. Then there exists a positive constant δ such that $\delta(G, X) > \delta/\log n$.*

We prove this by reducing to the almost simple case and then to the simple case.

We first need some auxiliary lemmas.

We will use the following result (which depends on the classification of finite simple groups – see [GMS] for a proof).

Lemma 8.2. *If h is an automorphism of a finite nonsolvable group J, then $C_J(h) \neq 1$.*

Lemma 8.3. *Let G be a transitive permutation group with a regular nonsolvable normal subgroup N acting on X. Then $\delta(G, X) \geq 1/2$.*

Proof. We can identify N with X. A point stabilizer H is a complement to N and the action on X is equivalent to the conjugation action of H. If $h \in H$, then the number of fixed points is just $|C_N(h)| > 1$ (by the previous result). Thus every element either has zero or at least 2 fixed points. Since the average number of fixed points is 1, this implies that $\delta(G, X) \geq 1/2$. □

We say that G preserves a product structure on X if X can be identified with $Y \times \ldots \times Y$ ($t > 1$ copies) and G embeds in $S_Y \wr S_t$ in its natural action (S_Y is the symmetric group on Y and each of the t copies acts on one copy of Y, the S_t permutes the coordinates). In particular, there is a homomorphism π from G into S_t. We assume that this image is transitive (which is always the case if G is primitive on X). Let G_1 denote the preimage of the stabilizer of 1 in $\pi(G)$. So G_1 acts on Y. If G is primitive, it follows that G_1 is as well [AS].

Lemma 8.4. $\delta(G, X) \geq \delta(G_1, Y)/t$.

Proof. The proportion of elements in G_1 is $1/t$. If $g \in G_1$, then g a derangement on Y implies that g is a derangement on X. □

Note in particular that $\log |X| = t \log |Y|$.

By examining the possibilities of primitive permutation groups (see [AS]) and using the two previous lemmas, there are only two cases remaining – G is almost simple or X is of full diagonal type (we explain this more fully below). Let H be a point stabilizer. In particular, G has a unique minimal normal subgroup N a direct product of t copies of a nonabelian simple L and either $t = 1$ or we may view $H \cap N \cong L$ as the diagonal subgroup of N (note that all diagonal subgroups are conjugate in $\mathrm{Aut}(N)$ so there is no loss of generality in assuming that $H \cap N$ is the canonical diagonal subgroup – alternatively, the arguments below are valid with $H \cap N$ any diagonal subgroup).

We next handle the diagonal case.

Lemma 8.5. *Let G be a finite group with a unique minimal normal subgroup $N = L^t$ with L a nonabelian finite simple group and $t > 1$. Let D be a diagonal subgroup of N and assume that $G = NH$ with $H = N_G(D)$. Then $\delta(G, G/H) > 1/\log_2 |G/H|$.*

Proof. Suppose that $g \in G$ has a unique fixed point on G/H. We claim that g is transitive on the t conjugates of L. Conjugating by an element of the transitive subgroup N allows us to assume that $g \in H$. Since g has a unique fixed point, it is invariant under $C_G(g)$ and so $C_G(g) \leq H$. In particular, $C_N(g) \leq D$. This implies the claim – for if g leaves invariant some proper factor N_1 of N, then $C_{N_1}(g) \neq 1$ (by Lemma 8.2) but $N_1 \cap D = 1$.

Now the proportion of elements in G that induce at t-cycle on the t conjugates of L is at most $1 - 1/t$ ($1/t$ of the elements normalize L). Thus, the proportion of elements with a unique fixed point is at most $1 - 1/t$, whence at least half the remaining elements must be derangements. Thus, the proportion of derangements is at least $1/2t$. Since $|G : H| = |L|^{t-1} \geq 60^{t-1}$, we have $2t < (t-1)\log_2 60 \leq \log_2 |G/H|$.

□

One can show that in most cases above, one can obtain an estimate not involving the log term. However, if the action of G on the t-conjugates of L is cyclic of order t and t does not divide the order of L, then in fact one can do no better than the previous result (this is another example of exceptionality).

If G is almost simple, then we can apply Theorem 1.3. Note that this implies the same result for almost simple groups as long as the socle of G has bounded index (with perhaps a different constant). Indeed, in the sequel we actually prove the result for all Chevalley groups contained in the group of inner diagonal automorphisms. Since the group of graph automorphisms always has order at most 6, we only need worry about field automorphisms. A simple inspection shows that the group of the field automorphisms has order at most $\log_2 n$ where n is the degree of the permutation representation. Thus, we have proved our result follows from Theorem 1.3. We have proved Theorem 1.3 in the bounded rank case. As we noted in the introduction, the complete proof of Theorem 1.3 is contained in [FG1], [FG2] and [FG3].

9. Numbers of conjugacy classes in finite classical groups

To conclude this paper we record some upper bounds on the number of conjugacy classes in the finite classical groups. These are treated fully in [FG2] where the results are used as a key ingredient in proving Theorem 1.3 and more. We mention that upper bounds on numbers of conjugacy classes are also of interest in random walks [Gl], [LiSh] and for computation of Fourier transforms on finite groups [MR].

The bounds we present are of the form cq^r where r is the rank and c is a small explicit constant. The paper [LiP] had previously established the bound $(6q)^r$ and the paper [Gl] had established bounds such as cq^{3r}. Thus our bounds in Theorem 9.1 are sharper for classical groups. For exceptional groups, one can compute precisely the number of classes as a monic polynomial in q (see [H2] for some discussion of this and references). In even characteristic $O(2n+1, q)$ is isomorphic to $Sp(2n, q)$ so we omit this case.

Here we only state the results for a specific form of each group. This gives bounds for the simple groups using the fact that the number of conjugacy classes decreases when one takes homomorphic images and also using the lemma below to pass to a subgroup or overgroup of bounded index. In [FG2], we actually prove results for more forms of the groups.

Theorem 9.1. *Let $k(G)$ denote the number of conjugacy classes of a finite group G.*

(1) $k(SL(2,q)) \leq q+4$.
(2) $k(SL(3,q)) \leq q^2+q+8$.
(3) $k(SU(3,q)) \leq q^2+q+10$.
(4) *For $n \geq 4$,* $k(SL(n,q)) \leq \frac{q^n}{q-1} + q^{1+\frac{n}{2}}$.
(5) *For $n \geq 4$,* $k(SU(n,q)) \leq 11.5\left(\frac{q^n}{q+1} + \frac{q+1}{q-1}q^{n/2+1}\right)$.
(6) $k(Sp(2n,q)) \leq 12q^n$ *if q is odd.*
(7) $k(Sp(2n,q)) \leq 21.4q^n$ *if q is even.*
(8) $k(O^{\pm}(2n,q)) \leq 29q^n$ *if q is odd.*
(9) $k(O^{\pm}(2n,q)) \leq 19.5q^n$ *if q is even.*
(10) $k(SO(2n+1,q)) \leq 7.38q^n$ *if q is odd.*

Our proof of Theorem 9.1 uses generating functions for numbers of conjugacy classes in finite classical groups [Lu], [M], [MR], [W] and is largely inspired by the proof in [MR] that $GL(n,q)$ has at most q^n classes and that $GU(n,q)$ has at most $8.26q^n$ conjugacy classes. However some new ingredients (combinatorial identities) are required.

Let $k_p(G)$ denote the number of conjugacy classes of p'-elements of G. This is also the number of absolutely irreducible representations of G in characteristic p. If p does not divide G, then $k_p(G) = k(G)$ the number of conjugacy classes of G (and also the number of irreducible complex representations). We also employ the following useful lemma, which allows us to move between various forms of the finite classical groups–at least when $|G/H|$ is bounded. This is proved in [Ga] for $k(G)$. The modification for p'-classes is straightforward and we omit the proof.

Lemma 9.2. *Let H be a subgroup of G with G/H of order d. Fix a prime p. Then $k_p(G) \leq dk_p(H)$ and $k_p(H) \leq dk_p(G)$. If H is normal in G, then $k_p(G) \leq k_p(H)k_p(G/H)$.*

In fact using generating functions it is possible to understand the asymptotic behavior of the constant c in the bound cq^n of Theorem 9.1. More precisely, we establish in [FG2] the following result.

Theorem 9.3.
(1) $lim_{n\to\infty}\frac{k(GL(n,q))}{q^n} = 1$
(2) $lim_{n\to\infty}\frac{k(GU(n,q))}{q^n} = \prod_{i\geq 1}\frac{1+1/q^i}{1-1/q^i}$
(3) $lim_{n\to\infty}\frac{k(Sp(2n,q))}{q^n} = \prod_{i=1}^{\infty}\frac{(1+\frac{1}{q^i})^4}{(1-\frac{1}{q^i})}$ *if q is odd.*
(4) $lim_{n\to\infty}\frac{k(Sp(2n,q))}{q^n} = \prod_{i=1}^{\infty}\frac{1-1/q^{4i}}{(1-1/q^{4i-2})(1-1/q^i)^2}$ *if q is even.*

(5) $lim_{n\to\infty}\frac{k(O^{\pm}(2n,q))}{q^n} = \frac{1}{4\prod_{i=1}^{\infty}(1-1/q^i)}(\prod_{i=1}^{\infty}(1+1/q^{i-1/2})^4 + \prod_{i=1}^{\infty}(1-1/q^{i-1/2})^4)$ *if* q *is odd.*

(6) $lim_{n\to\infty}\frac{k(O^{\pm}(2n,q))}{q^n} = \frac{1}{2}\frac{\prod_{i=0}^{\infty}(1-1/q^{2i+2})(1+1/q^{2i+1})^2}{\prod_{i=1}^{\infty}(1-1/q^i)^2}$ *if* q *is even.*

(7) $lim_{n\to\infty}\frac{k(SO(2n+1,q))}{q^n} = \prod_{i=1}^{\infty}\frac{(1-1/q^{4i})^2}{(1-1/q^i)^3(1-1/q^{4i-2})^2}$ *if* q *is odd.*

References

[A1] Aschbacher, M., Finite Group Theory, Cambridge University Press, Cambridge, 1986.

[A2] Aschbacher, M., On the maximal subgroups of the finite classical groups, Invent. Math. 76 (1984), 469–514.

[AS] Aschbacher, M. and Scott, L., Maximal subgroups of finite groups, J. Algebra 92 (1985), 44–80.

[CC] Cameron, P. and Cohen, A., On the number of fixed point free elements in a permutation group, Discrete Math. 106/107 (1992), 135–138.

[Ca] Carter, R., Finite groups of Lie type. Conjugacy classes and complex characters. Reprint of the 1985 original. John Wiley and Sons, Chichester, 1993.

[Co] Cohen, S., Permutation group theory and permutation polynomials, Algebras and combinatorics (Hong Kong, 1997), 133–146, Springer, Singapore, 1999.

[Dia] Diaconis, P., Group representations in probability and statistics, Lecture Notes Monograph Series 11, Institute of Mathematical Statistics, Hayward, CA 1988.

[D] Dixon, J., Random sets which invariably generate the symmetric group, *Discrete Math.* **105** (1992), 25-39.

[FGS] Fried, M., Guralnick, R., and Saxl, J., Schur covers and Carlitz's conjecture, Israel J. Math. 82 (1993), 157–225.

[FG1] Fulman, J. and Guralnick, R., Derangements in subspace actions of classical groups, preprint.

[FG2] Fulman, J. and Guralnick, R., Derangements in classical groups for nonsubspace actions, preprint.

[FG3] Fulman, J. and Guralnick, R., Derangements in simple and primitive groups II, in preparation.

[FG4] Fulman, J. and Guralnick, R., The probability of generating an irreducible subgroup, preprint.

[FNP] Fulman, J., Neumann, P.M. and Praeger, C.E., A generating function approach to the enumeration of matrices in finite classical groups, preprint.

[Ga] Gallagher, P., The number of conjugacy classes in a finite group, Math. Z. 118 (1970), 175–179.

[Gl] Gluck, D., Characters and random walks on finite classical groups, Adv. Math. 129 (1997), 46–72.

[GoLy] Gorenstein, D. and Lyons, R., The local structure of finite groups of characteristic 2 type. Mem. Amer. Math. Soc. 42 (1983), no. 276.

[GK] Guralnick, R. and Kantor, W., Probabilistic generation of finite simple groups, J. Algebra 234 (2000), 743–792.

[GKS] Guralnick, R., Kantor, W. and Saxl, J., The probability of generating a classical group, Comm. Algebra 22 (1994), 1395–1402.

[GLPS] Guralnick, R., Li, P., Praeger, C., and Saxl, J., Exceptional primitive group actions and partitions of orbitals, preprint.

[GLSS] Guralnick, R., Liebeck, M., Saxl, J, and Shalev, A., Random generation of finite simple groups, J. Algebra 219 (1999), 345–355.

[GL] Guralnick, R., Lübeck, F., On p-singular elements in Chevalley groups in characteristic p. Groups and computation, III (Columbus, OH, 1999), 169–182, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.

[GMS] Guralnick, R., Müller, P., and Saxl, J., The rational function analogue of a question of Schur and exceptionality of permutation representations, Memoirs of the Amer. Math. Soc., to appear.

[GSa] Guralnick, R. and Saxl, J., Exceptional polynomials over arbitrary fields, Proceedings of a Conference in honor of Abhyankar, to appear.

[GSt] Guralnick, R. and Stevenson, K., Prescribing ramification, 387–406 in Arithmetic fundamental groups and noncommutative algebra, Proceedings of Symposia in Pure Mathematics, 70 (2002) editors M. Fried and Y. Ihara, 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16-27, 1999 MSRI.

[GTZ] Guralnick, R. Tucker, T. and Zieve, M., Exceptional covers and bijections of rational points, preprint.

[GW] Guralnick, R., and Wan, D., Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, Israel J. Math. 101 (1997), 255–287.

[H1] Humphreys, J., Linear algebraic groups. Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975

[H2] Humphreys, J., Conjugacy classes in semisimple algebraic groups, Mathematical Surveys and Monographs, 43, American Mathematical Society, Providence, RI, 1995.

[LaP] Larsen, M. and Pink, R., Finite subgroups of algebraic groups, preprint.

[LiP] Liebeck, M. and Pyber, L., Upper bounds for the number of conjugacy classes of a finite group, J. Algebra 198 (1997), 538–562.

[LS1] Liebeck, M. and Seitz, G., On the subgroup structure of exceptional groups of Lie type, Trans. Amer. Math. Soc. 350 (1998), 3409–3482.

[LS2] Liebeck, M. and Seitz, G., The maximal subgroups of positive dimension in exceptional algebraic groups, Memoirs of the Amer. Math. Soc., to appear.

[LS3] Liebeck, M. and Seitz, G., On the subgroup structure of classical groups, Invent. Math. 134 (1998), 427–453.

[LiSh] Liebeck, M. and Shalev, Diameters of finite simple groups: sharp bounds and applications, Annals of Math. 154 (2001), 383-406.

[LuP] Luczak, T. and Pyber, L., On random generation of the symmetric group, Combin. Probab. Comput. 2 (1993), 505–512.

[Lu] Lusztig, G., Irreducible representations of the finite classical groups, *Invent. Math* **43** (1977), 125-176.

[M] Macdonald, I., Numbers of conjugacy classes in some finite classical groups, Bull. Austral. Math. Soc. 23 (1981), 23-48.

[MR] Maslen, D. and Rockmore, D., Separation of variables and the computation of Fourier transforms on finite groups, I., J. Amer. Math. Soc. 10 (1997), 169-214.

[No] Nori, M., On subgroups of $\mathrm{GL}_n(F_p)$, Invent. Math. 88 (1987), 257–275.

[SaSe] Saxl, J. and Seitz, G., Subgroups of algebraic groups containing regular unipotent elements, J. London Math. Soc. (2) 55 (1997), 370–386.

[Sh] Shalev, A., A theorem on random matrices and some applications, J. Algebra 199 (1998), 124–141.

[SpSt] Springer, T. and Steinberg, R., Conjugacy classes. 1970 Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69) pp. 167–266, Lecture Notes in Mathematics, Vol. 131, Springer, Berlin.

[W] Wall, G. E., On the conjugacy classes in the unitary, symplectic, and orthogonal groups, *J. Aust. Math. Soc.* **3** (1963), 1-63.

Department of Mathematics, University of Pittsburgh, Pittsburgh, PA 15260
E-mail address: fulman@math.pitt.edu

University of Southern California, Los Angeles, CA
E-mail address: guralnic@math.usc.edu