THE CHEBOTAREV INVARIANT OF A FINITE GROUP:
A CONJECTURE OF KOWALSKI AND ZYWINA

ANDREA LUCCHINI

ABSTRACT. A subset \{g_1, \ldots, g_d\} of a finite group \(G\) invariably generates \(G\) if \{\(g_1^{x_1}, \ldots, g_d^{x_d}\)\} generates \(G\) for every choice of \(x_i \in G\). The Chebotarev invariant \(C(G)\) of \(G\) is the expected value of the random variable \(n\) that is minimal subject to the requirement that \(n\) randomly chosen elements of \(G\) invariably generate \(G\). Confirming a conjecture of Kowalski and Zywina, we prove that there exists an absolute constant \(\beta\) such that \(C(G) \leq \beta \sqrt{|G|}\) for all finite groups \(G\).

1. Introduction

We say that a subset \{g_1, \ldots, g_d\} of a finite group \(G\) invariably generates \(G\) if \{\(g_1^{x_1}, \ldots, g_d^{x_d}\)\} generates \(G\) for every choice of \(x_i \in G\). The Chebotarev invariant \(C(G)\) of \(G\) is the expected value of the random variable \(n\) that is minimal subject to the requirement that \(n\) randomly chosen elements of \(G\) invariably generate \(G\). The main motivation for introducing the invariant \(C(G)\) is the relationship to Chebotarev’s Theorem and the calculation of Galois groups of polynomials with integer coefficients. Chebotarev’s Theorem provides elements of a suitable Galois group \(G\), where the elements are obtained only up to conjugacy in \(G\); the interest in the study of \(C(G)\) comes from computational group theory, where there is a need to know how long one should expect to wait in order to ensure that choices of representatives from the conjugacy classes provided by Chebotarev’s Theorem will generate \(G\). This is discussed more carefully in \([6]\) and \([22]\).

In response to a question of Kowalski and Zywina \([22]\), Kantor, Lubotzky and Shalev \([17]\) bounded the size of a randomly chosen set of elements of \(G\) that is likely to generate \(G\) invariably. As a corollary of their result, they proved that there exists an absolute constant \(c\) such that \(C(G) \leq c \sqrt{|G|} \log |G|\) for all finite groups \(G\) (\([17\) Theorem 1.2]). This bound is close to best possible: as it is noticed in \([17]\), sharply 2-transitive groups provide an infinite family of groups \(G\) for which \(C(G) \sim \sqrt{|G|}\). In particular, \(C(\text{AGL}(1, q)) \sim q\) as \(q \to \infty\) \([22\ Proposition 4.1]\). In fact \([22\ Section 9]\) asks whether \(C(G) = O(\sqrt{|G|})\) for all finite groups \(G\). In this paper we give an affirmative answer.

**Theorem 1.** There exists an absolute constant \(\beta\) such that \(C(G) \leq \beta \sqrt{|G|}\) for all finite groups \(G\).

For \(k \geq 1\), let \(P_t(G,k)\) be the probability that \(k\) randomly chosen elements of \(G\) generate \(G\) invariably. An easy argument in probability theory shows that if

---

Partially supported by Università di Padova (Progetto di Ricerca di Ateneo: “Invariable generation of groups”).
$P_1(G, k) \geq \epsilon$, then $C(G) \leq k/\epsilon$. Indeed we obtain Theorem 1 as a corollary of the following result.

**Theorem 2.** For any $\epsilon > 0$ there exists $\tau_\epsilon$ such that $P_1(G, k) \geq 1 - \epsilon$ for any finite group $G$ and any $k \geq \tau_\epsilon \sqrt{|G|}$.

One of the ingredients used in the proof of Theorem 2 is the notion of crown, introduced by Gaschütz in [7] in the case of finite solvable groups and generalized in [16] to arbitrary finite groups. The property of the crowns are enough to prove the theorem in the case of solvable groups, but in order to apply our arguments to arbitrary finite groups, we need some results relying on the classification of the finite simple groups. The first is a bound on the order of the first cohomology group of a finite group over a faithful irreducible module: if $V$ is an irreducible faithful $G$-module over a finite field, then $|H^1(G, V)| \leq \sqrt{|V|} < |V|$ (see [1] and [14]). This result is near to be sufficient for our purposes, but we need a more precise information in the particular case when $|V| \leq |G|$ and the proportion of elements of $G$ fixing no nontrivial vector of $V$ is small (see Proposition 9). Other two consequences of the classification of the finite simple groups are necessary to prove Lemma 13: there exists an absolute constant $c_1$ such that any finite group $G$ has at most $c_1|G|^{3/2}$ maximal subgroups [19, Theorem 1.3]; the proportion of fixed-point-free permutations in a non-affine primitive group of degree $n$ is at least $c_2/\log n$, for some absolute constant $c_2 > 0$ [8, Theorem 8.1]. This last result in turn relies on a conjecture made independently by Boston and Shalev, stating that there exists an absolute constant $\epsilon > 0$ such that the proportion of fixed-point-free elements in any finite simple transitive permutation group is at least $\epsilon$. This conjecture was proved for alternating groups by Luczak and L. Pyber in [20] and for the simple groups of Lie type by Fulman and Guralnick in a series of four papers ([8], [9], [10], [11]).

2. Crowns in finite groups

Let $L$ be a monolithic primitive group and let $A$ be its unique minimal normal subgroup. For each positive integer $k$, let $L^k$ be the $k$-fold direct product of $L$. The crown-based power of $L$ of size $k$ is the subgroup $L_k$ of $L^k$ defined by

$$L_k = \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \pmod{A}\}.$$

Equivalently, $L_k = A^k \text{diag } L^k$.

Following [16], we say that two irreducible $G$-groups $A$ and $B$ are $G$-equivalent and we put $A \sim_G B$, if there is an isomorphism $\Phi : A \times G \to B \times G$ such that the following diagram commutes:

$$\begin{array}{cccccc}
1 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\
\downarrow \phi & & \downarrow \Phi & & \Rightarrow & & \Rightarrow & & \downarrow \\
1 & \longrightarrow & B & \longrightarrow & B \rtimes G & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

Note that two $G$-isomorphic $G$-groups are $G$-equivalent. In the particular case where $A$ and $B$ are abelian the converse is true: if $A$ and $B$ are abelian and $G$-equivalent, then $A$ and $B$ are also $G$-isomorphic. It is proved (see for example [16, Proposition 1.4]) that two chief factors $A$ and $B$ of $G$ are $G$-equivalent if and only if either they are $G$-isomorphic between them or there exists a maximal
subgroup $M$ of $G$ such that $G/\Core_G(M)$ has two minimal normal subgroups $N_1$ and $N_2$ $G$-isomorphic to $A$ and $B$ respectively. For example, the minimal normal subgroups of a crown-based power $L_k$ are all $L_k$-equivalent.

Let $A = X/Y$ be a chief factor of $G$. A complement $U$ to $A$ in $G$ is a subgroup $U$ of $G$ such that $UX = G$ and $U \cap X = Y$. We say that $A = X/Y$ is a Frattini chief factor if $X/Y$ is contained in the Frattini subgroup of $G/Y$: this is equivalent to say that $A$ is abelian and there is no complement to $A$ in $G$. The number $\delta_G(A)$ of non-Frattini chief factors $G$-equivalent to $A$ in any chief series of $G$ does not depend on the series. Now, we denote by $L_A$ the monolithic primitive group associated to $A$, that is

$$L_A = \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian}, \\ G/C_G(A) & \text{otherwise}. \end{cases}$$

If $A$ is a non-Frattini chief factor of $G$, then $L_A$ is a homomorphic image of $G$. More precisely, there exists a normal subgroup $N$ of $G$ such that $G/N \cong L_A$ and $\soc(G/N) \sim_G A$. Consider now all the normal subgroups $N$ of $G$ with the property that $G/N \cong L_A$ and $\soc(G/N) \sim_G A$: the intersection $R_G(A)$ of all these subgroups has the property that $G/R_G(A)$ is isomorphic to the crown-based power $(L_A \delta_G(A))$. The socle $I_G(A)/R_G(A)$ of $G/R_G(A)$ is called the $A$-crown of $G$ and it is a direct product of $\delta_G(A)$ minimal normal subgroups $G$-equivalent to $A$.

Lemma 3. [2 Lemma 1.3.6] Let $G$ be a finite group with trivial Frattini subgroup. There exists a crown $I_G(A)/R_G(A)$ and a non trivial normal subgroup $U$ of $G$ such that $I_G(A) = R_G(A) \times U$.


3. Crown-based powers with abelian socle

In this section we will assume that $H$ is a finite group acting irreducibly and faithfully on an elementary abelian $p$-group $V$. The semidirect product $L = V \rtimes H$ is a monolithic primitive group. For a positive integer $u$ we consider the crown-based power $L_u$: we have that $L_u$ is isomorphic to the semidirect product $G = V^u \rtimes H$, where we assume that the action of $H$ is diagonal on $V^u$, that is, $H$ acts in the same way on each of the $u$ direct factors. We assume that $h_1, \ldots, h_d$ (invariably) generate $H$ and we look for conditions ensuring the existence of $d$-elements $w_1, \ldots, w_d \in V^u$ such that $h_1 w_1, \ldots, h_d w_d$ (invariably) generate $G$. The case when $H = 1$ is trivial: $V \cong C_p$ is a cyclic group of prime order and $G = C_p^u$ can be generated by $d$ elements $w_1, \ldots, w_d$ if and only if $u \leq d$. So for the remaining part of this section we will assume $H \neq 1$. We will denote by $\Der(H, V)$ the set of the derivations from $H$ to $V$ (i.e. the maps $\delta : H \to V$ with the property that $\delta(h_1 h_2) = \delta(h_1) h_2 + \delta(h_2)$ for every $h_1, h_2 \in H$). If $v \in V$ then the map $\delta_v : H \to V$ defined by $\delta_v(h) = [h, v]$ is a derivation. The set $\InnDer(H, V) = \{\delta_v \mid v \in V\}$ of the inner derivations from $H$ to $V$ is a subgroup of $\Der(V, H)$ and the factor group $H^1(H, V) = \Der(H, V)/\InnDer(H, V)$ is the first cohomology group of $H$ with coefficients in $V$.

The following is a generalization of a similar partial result ([3 Proposition 2.1]), proved in the particular case when $H$ is soluble, or, more in general, when $H^1(H, V) = 0$. 
Proposition 5. Suppose that \( H = \langle h_1, \ldots, h_d \rangle \). Let \( w_i = (w_{i,1}, \ldots, w_{i,n}) \in V^u \) with \( 1 \leq i \leq d \). The following are equivalent.

1. \( G \neq \langle h_1w_1, \ldots, h_dw_d \rangle \);
2. there exist \( \lambda_1, \ldots, \lambda_u \in F = \text{End}_F(V) \) and a derivation \( \delta \in \text{Der}(H,V) \) with \( (\lambda_1, \ldots, \lambda_u, \delta)^{-1} \neq (0, \ldots, 0, 0) \) such that \( \sum_{1 \leq j \leq u} \lambda_jw_{ij} = \delta(h_i) \) for each \( i \in \{1, \ldots, d\} \).

Proof. Let \( K = \langle h_1w_1, \ldots, h_dw_d \rangle \). First we prove, by induction on \( u \), that if \( K \neq G \) then (2) holds. Let \( z_i = h_i(w_{i,1} \ldots, w_{i,u-1},0) \) and let \( Z = \langle z_1, \ldots, z_d \rangle \). If \( Z \neq V^{u-1}H \), then, by induction, there exist \( \lambda_1, \ldots, \lambda_{u-1} \in F \) and \( \delta \in \text{Der}(H,V) \) with \( (\lambda_1, \ldots, \lambda_{u-1}, \delta)^{-1} \neq (0, \ldots, 0, 0) \) such that \( \sum_{1 \leq j \leq u-1} \lambda_jw_{ij} = \delta(h_i) \) for each \( i \in \{1, \ldots, d\} \). In this case \( \lambda_1, \ldots, \lambda_{u-1}, 0 \) and \( \delta \) are the requested elements.

So we may assume \( Z \cong V^{u-1}H \). Set \( V_u = \{ (0, \ldots, 0, v) \mid v \in V \} \). We have \( ZV_u = KV_u = G \) and \( Z \neq G \); this implies that \( Z \) is a complement of \( V_u \) in \( G \) and therefore there exists \( \delta^* \in \text{Der}(Z,V_u) \) such that \( \delta^*(z_i) = w_{i,u} \) for each \( i \in \{1, \ldots, d\} \). By Propositions 2.7 and 2.10 of [1], there exist \( \delta \in \text{Der}(H,V) \) and \( \lambda_1, \ldots, \lambda_{u-1} \in F \) such that for each \( h(v_1, \ldots, v_{u-1}, 0) \in Z \) we have

\[
\delta^*(h(v_1, \ldots, v_{u-1}, 0)) = \delta(h) + \lambda_1v_1 + \cdots + \lambda_{u-1}v_{u-1}.
\]

In particular \( -\sum_{1 \leq j \leq u-1} \lambda_jw_{ij} + w_{i,u} = \delta(h_i) \) for each \( i \in \{1, \ldots, d\} \), hence (2) holds.

Conversely, if (2) holds then \( \langle h(v_1, \ldots, v_u) \mid \delta(h) = \lambda_1v_1 + \cdots + \lambda_u v_u \rangle \) is a proper subgroup of \( G \) containing \( K \).

Notice that \( V, \text{Der}(H,V) \) and \( H^1(H,V) \) are vector spaces over \( F = \text{End}_F(V) \). Let \( n := \dim_F V = \dim_F \text{ImDer}(H,V) \) and \( m := \dim_F H^1(H,V) \). Clearly, we have \( \dim_F \text{Der}(H,V) = n + m \).

Let \( \pi_i : V^u \to V \) be the canonical projection on the \( i \)-th component:

\[
\pi_i(v_1, \ldots, v_u) = v_i.
\]

Let \( w_i = (w_{i,1}, \ldots, w_{i,u}) \in V^u \) for \( i \in \{1, \ldots, d\} \), and consider the vectors

\[
r_j = (\pi_j(w_1), \ldots, \pi_j(w_u)) = (w_{1,j}, \ldots, w_{u,j}) \in V^d \text{ for } j \in \{1, \ldots, u\}.
\]

Proposition [5] says that the elements \( h_1w_1, \ldots, h_dw_d \) generate a proper subgroup of \( G \) if and only if there exists a non-zero vector \( (\lambda_1, \ldots, \lambda_u, \delta) \) in \( F^u \times \text{Der}(H,V) \) such that

\[
\sum_{1 \leq j \leq u} \lambda_jr_j = (\delta(h_1), \ldots, \delta(h_d)).
\]

Equivalently, \( \langle h_1w_1, \ldots, h_dw_d \rangle = G \) if and only if \( r_1, \ldots, r_u \) in \( V^d \) are linearly independent modulo the vector space

\[
D = \{ (\delta(h_1), \ldots, \delta(h_d)) \in V^d \mid w \in V \}.
\]

Since \( G = \langle h_1, \ldots, h_d \rangle \), the map \( \text{Der}(H,V) \to D \) defined via \( \delta \mapsto (\delta(h_1) \cdots \delta(h_d)) \) is an \( F \)-isomorphism. In particular \( \dim_F(D) = \dim_F(\text{Der}(H,V)) = n + m \), and so we conclude that there exist elements \( w_1, \ldots, w_u \) in \( V^u \) such that \( \langle h_1w_1, \ldots, h_dw_d \rangle = G \) if and only if \( u \leq \dim_F(V^d) = \dim_F(D) = n(d-1) - m \).

We now discuss the same question in the case of invariable generation, generalizing to an arbitrary irreducible \( H \)-module \( V \) a partial result ([5, Proposition 8]) proved under the hypothesis \( H^1(H,V) = 0 \).
Proposition 6. Suppose that $h_1, \ldots, h_d$ invariably generate $H$. Let $w_1, \ldots, w_d \in V^u$ with $w_i = (w_{i,1}, \ldots, w_{i,u})$. For $j \in \{1, \ldots, u\}$, consider the vectors

$$r_j = (\pi_j(w_1), \ldots, \pi_j(w_d)) = (w_{1,j}, \ldots, w_{d,j}) \in V^d.$$

Then $h_1 w_1, h_2 w_2, \ldots, h_d w_d$ invariably generate $V^u \times H$ if and only if the vectors $r_1, \ldots, r_u$ are linearly independent modulo $D + W$ where

$$D = \{(\delta(h_1), \ldots, \delta(h_d)) \in V^d \mid \delta \in \text{Der}(H, V)\},$$

$$W = \{(u_1, \ldots, u_d) \in V^d \mid u_i \in [h_i, V], \ i = 1, \ldots, d\}.$$

In particular, there exist elements $w_1, \ldots, w_d \in V^u$ such that $h_1 w_1, h_2 w_2, \ldots, h_d w_d$ invariably generate $V^u \times H$ if and only if $u \leq nd - \dim_F(D + W)$.

Proof. Let $g_i = y_i x_i$ with $x_i \in H$ and $y_i = (y_{i,1}, \ldots, y_{i,u}) \in V^u$ for $i \in \{1, \ldots, d\}$ and let $X_{g_1, \ldots, g_d} = \langle (h_1 w_1)^{g_1}, \ldots, (h_d w_d)^{g_d} \rangle$. We have

$$(h_i w_i)^{g_i} = (h_i^{y_i} w_i^{x_i})^{y_i} = h_i^{x_i} (h_i, y_i) + w_i^{x_i} = h_i^{x_i} z_i$$

where $z_i = ([h_i, y_i] + w_i)^{x_i} \in V^u$. Then $X_{g_1, \ldots, g_d} = G$ if and only if the vectors

$$(\pi_j(z_1), \ldots, \pi_j(z_d)) = (([h_1, y_{1,j}] + w_{1,j})^{x_1}, \ldots, ([h_d, y_{d,j}] + w_{d,j})^{x_d}) \in V^d,$$

for $j \in \{1, \ldots, u\}$, are linearly independent modulo the subspace

$$D^* = \{\delta(h_1^{x_1}), \ldots, \delta(h_d^{x_d}) \in V^d \mid \delta \in \text{Der}(H, V)\}$$

$$= \left\{\left((\delta(h_1) - [h_1, \delta(x_1^{-1})])^{x_1}, \ldots, (\delta(h_d) - [h_d, \delta(x_d^{-1})])^{x_d}\right) \in V^d \mid \delta \in \text{Der}(H, V)\right\}$$

(we have indeed that $\delta(h^x) = \delta(x^{-1} h x) = \delta(x^{-1} h)x + \delta(x) = (\delta(x^{-1} h) + \delta(x)x^{-1})x = (\delta(x^{-1})^h + \delta(h) - \delta(x^{-1}))x$).

Note that the map $f(x_1, \ldots, x_d) : V^d \to V^d$ defined by

$$f(x_1, \ldots, x_d)(v_1, \ldots, v_d) = (v_1^{x_1}, \ldots, v_d^{x_d})$$

is an isomorphism. Therefore $X_{g_1, \ldots, g_d} = G$ if and only if the vectors

$$([h_1, y_{1,j}] + w_{1,j}, \ldots, [h_d, y_{d,j}] + w_{d,j}) = r_j + ([h_1, y_{1,j}], \ldots, [h_d, y_{d,j}]),$$

for $j = 1, \ldots, u$, are linearly independent modulo the subspace

$$\left\{\left((\delta(h_1) - [h_1, \delta(x_1^{-1})])\right), \ldots, (\delta(h_d) - [h_d, \delta(x_d^{-1})])\right\} \in V^d \mid \delta \in \text{Der}(H, V)\right\}.$$

Since this condition has to hold for every choice of $y_i \in V^u$ and $x_j \in H$, this means that the elements $r_1, \ldots, r_u$ have to be linearly independent modulo the subspace $D + W$, as required. \[\square\]

Lemma 7. In the situation described in Proposition 6 and using the same notations, we have that

$$nd - \dim_F(D + W) \geq \sum_{1 \leq i \leq d} \dim_F C_V(h_i) - m,$$

with $m = \dim_F H^1(H, V)$.

Proof. Firstly, notice that

$$\dim_F W = \sum_{1 \leq i \leq d} \dim_F [h_i, V] = \sum_{1 \leq i \leq d} (n - \dim_F C_V(h_i)) = nd - \sum_{1 \leq i \leq d} \dim_F C_V(h_i).$$
Moreover $D \cap W$ contains $I = \{(\delta(h_1), \ldots, \delta(h_d)) \in V^d \mid \delta \in \text{InnDer}(H, V)\}$, which is $F$-isomorphic to $\text{InnDer}(H, V)$, and consequently
\[
\dim_F(D + W) - \dim_F(W) = \dim_F((D + W)/W) = \dim_F(D/(D \cap W)) \\
\leq \dim_F D/I = \dim_F(\text{Der}(H, V)/\text{InnDer}(H, V)) \\
= \dim_F H^1(H, V) = m.
\]
We conclude
\[
\dim_F(D + W) \leq \dim_F W + \dim_F H^1(H, V) \\
\leq nd - \sum_{1 \leq i \leq d} \dim_F C_V(h_i) + m. \quad \square
\]

4. FIRST COHOMOLOGY GROUPS FOR FINITE GROUPS

For all this section we will assume that $H$ is a finite group, $F$ is a field of finite characteristic and $V$ is a faithful and absolutely irreducible $FH$-module. Moreover let $n = \dim_F V$, $m = \dim_F H^1(H, V)$.

In the proof of our main result we will need a good bound upper bound for $m$. The following result is available (see [1] Theorem A, [14] Theorem 1):

**Proposition 8.** $m \leq n/2 \leq n - 1$.

Guralnick made a conjecture that there should be a universal bound on the dimension of the first cohomology groups $H^1(H, V)$, where $H$ is a finite group and $V$ is an absolutely irreducible faithful representation for $H$. The conjecture reduces to the case where $H$ is a finite simple group. Very recently, computer calculations of Frank Lübeck, complemented by those of Leonard Scott and Tim Sprowl, have provided strong evidence that the Guralnick conjecture may unfortunately be false. For our purpose it is not necessary that the Guralnick conjecture is true. A much weaker version, which will be discussed in this section, is enough. First we need a preliminary lemma.

**Lemma 9.** If $m \neq 0$, then:

1. $H$ has a unique minimal normal subgroup $N$ and $N$ is nonabelian.
2. If $S$ is a component of $N$ and $W$ is an irreducible $FN$-submodule of $V$ which is not centralized by $S$, then the other components of $N$ act trivially on $W$.
3. $m \leq \dim_F H^1(S, W)$ for any irreducible submodule of $V$ which is not centralized by $S$.
4. Every element of $C_H(S)$ fixes at least a nonzero vector of $V$.

**Proof.** It is well known that if $K$ is an extension field of $F$, then $H^1(H, V) \otimes_F K$ and $H^1(H, V \otimes_F K)$ are naturally isomorphic, so may assume that $F$ is algebraically closed. The first three statements are proved in [15] Lemma 5.2. Let $\Omega$ be the set of irreducible $FN$-submodules of $V$ which are not centralized by $S$ and let $U = \sum_{W \in \Omega} W$. Let $I$ be the stabilizer of $U$ in $H$. It follows from (2) that $I = N_H(S)$. Since $V$ is irreducible, $U$ is an irreducible $I$-module. Let $R = SC_H(S)$. By [15] Lemma 3.4, $H^1(H, V) = H^1(I, U)$ and, by [15] Lemma 3.11, $\dim H^1(I, U) \leq \dim H^1(R, U)$. Since $R = S \times C_H(S)$, $U$ is a direct sum of modules of the form $W \otimes X$ where $W \in \Omega$ and each $X$ is an irreducible $C_H(S)$-module. By [15] Lemma 3.10 if
all the $X$ are nontrivial $C_H(S)$-modules then $H^1(R,U) = 0$, and so $H^1(H,V) = 0$. So $C_H(S)$ acts trivially on some of the direct factors of $U$. \hfill \Box

**Proposition 10.** Denote by $p$ the probability that an element $h$ of $H$ centralizes a non-zero vector of $V$. There exists a constant $\alpha$ (independent on the choice of $H$ and $V$) with the property that if $|V| \leq |H|$, then either $m \leq \alpha$ or $p|H| \geq 2^m$.

**Proof.** We may assume $m \neq 0$. By Lemma 9, $H$ has a unique minimal normal subgroup $N$ where $S$ is a nonabelian simple group. First assume $t \neq 1$. We may identify $H$ with a subgroup of $\text{Aut} S \wr K$ being $K$ the transitive subgroup of $\Sym(t)$ induced by the conjugation action of $H$ on the components. It follows from Lemma 9(3), that

$$p|H| \geq |C_H(S)| \geq \frac{|H|}{t|\text{Out} S|} \geq \frac{|K||S|^{t-1}}{t|\text{Out} S|},$$

while, since $2^n \leq q^n \leq |H|$, we have

$$m < n \leq \log |H| \leq \log(|\text{Aut} S|^{t|K|}) \leq \log(|S|^{2^{t}}|K|)).$$

It follows that there exists $\tau$ such that $p|H| \geq m^2$ if $|S| \geq \tau$. On the other hand, there are only finitely many possible pairs $(S,W)$ where $S$ is a simple group of order at most $\tau$ and $W$ is an irreducible $FS$-module with $H^1(S,W) \neq 0$ (since $H^1(S,W) = 0$ if $S$ and $W$ have coprime orders) so it follows from Lemma 9(3) that there exists $m \leq \alpha$ whenever $|S| \leq \tau$.

So we may assume that $H$ is an almost simple group, and that $S = \text{soc } H$ is a finite group of Lie type or alternating group, since the number of possibilities for $H$ and $V$ when $H$ is sporadic and $H^1(H,V) \neq 0$ is finite. Let $r$ be the characteristic of $F$. The condition $m \neq 0$ implies that $r$ divides $|H|$. Moreover all the elements of a Sylow $r$-subgroup of $H$ centralize at least a non-zero vector of $V$, so $p|H| \geq |H|_r$, the largest power of $r$ dividing $|H|$. We have three possibilities:

a) $S = \text{Alt}(k)$. Since $2^n \leq q^n \leq |H| \leq k!$, we have $m \leq n \leq k \log k$. By [13] Corollary 3, we have $m \leq n/(f - 1)$ being $f$ the largest prime such that $f \leq k - 2$. Nagura [23] proved that for each $x \geq 25$, the interval $[x, 6x/5]$ contains a prime, hence if $k$ is large enough then $(f - 1) \geq k/2$ and consequently $m \leq k \log k/(f - 1) \leq 2 \log k$.

We cannot have $r > k/2$, otherwise a Sylow $r$-subgroup of $H$ would be cyclic and this would implies $m = 0$ (see [12] Proposition 3.4]). But then $k = ar + b$ with $a, b \in \mathbb{N}, a \geq 1$ and $b < r \leq k/2$. So $(k!)_r \geq r^a \geq r \cdot a \geq k/2$. We conclude that $|H|_r \geq k/2 \geq (2 \log k)^2 \geq m^2$ if $k$ is large enough, say $k \geq \tau$. Since there are only finitely many possibilities of $k \leq \tau$ and an absolutely irreducible $\text{Alt}(k)$-module $V$ such that $H^1(\text{Alt}(k), V) \neq 0$, we are done in this case.

b) $S$ is a group of Lie type defined over a field whose characteristic is different from the characteristic $r$ of $F$. Let us denote by $\delta(S)$ the smallest degree of a nontrivial irreducible representation of $S$ in cross characteristic. Lower bounds for the degree of irreducible representations of finite groups of Lie type in cross characteristic were found by Landazuri and Seitz [18] and improved later by Seitz and Zalesskii [25] and Tiep [26]. It turns out that $\delta(S)$ is quite large, and, apart from finitely many exceptions, we have $r^\delta(S) > |\text{Aut} S|$, in contradiction with $r^\delta(S) \leq |V| < |H| \leq |\text{Aut} S|$.

c) $S$ is a group of Lie type defined over a field whose characteristic coincides with the characteristic $r$ of $F$. We have $p|H| \geq |H|_r \geq |S|^{1/3}$ (see [21] Proposition
3.5). On the other hand $|V| \leq |H| \leq |S|^2$, hence $m \leq n/2 \leq \log |S|$ and again we can conclude that $p|H| \geq |S|^{1/3} \geq \log^2 |S| \geq m^2$ if $|S|$ is large enough. \hfill \Box

5. Auxiliary results

We begin this section with an elementary result in probability theory, which will play a crucial role in our considerations. Let us denote by $B(m, p)$ the binomial random variable of parameters $m$ and $p$.

**Proposition 11.** For every real number $0 < \epsilon < 1$, there exists an absolute constant $\gamma_\epsilon$ such that, for any positive integer $l$ and any positive real number $p < 1$, we have that $P(B(m, p) \geq l) \geq \epsilon$ if $m \geq \gamma_\epsilon l/p$.

**Proof.** Let $M(t)$ be the moment generating function of the random variable $X = B(m, p)$. We have $M(t) = (pe^t + (1 - p))^m$. By Chernoff’s bounds (see for example [24, Chapter 8, Proposition 5.2]), $P(X \leq e^{-t})M(t)$ for every real negative number $t$. Taking $t = -\epsilon$ and $a = l$, we deduce

$$P(X \leq l) \leq e^{\epsilon(1 - \alpha p)^m}$$

with $\alpha = (1 - 1/\epsilon)$. In particular $P(X \geq l) \geq 1 - e^{\epsilon(1 - \alpha p)^m}$, and we reduce to prove that there exists $\gamma_\epsilon$ such that $e^{\epsilon(1 - \alpha p)^m} \leq (1 - \epsilon)$ if $m \geq \gamma_\epsilon l/p$. It suffices to choose $\gamma_\epsilon$ such that $(1 - \alpha p)^{\gamma_\epsilon} \leq (1 - \epsilon)/\epsilon$. Since $(1 - \alpha p)^{\gamma_\epsilon} \leq (1 - \alpha p)^{\gamma_\epsilon p} \leq e^{-\gamma_\epsilon \alpha}$, it suffices to take $\gamma_\epsilon \geq (1 - \log(1 - \epsilon))/\alpha$. \hfill \Box

From now on we will use the notation $\langle x_1, \ldots, x_d \rangle_I = G$ to say that $x_1, \ldots, x_d$ invariably generate $G$.

**Lemma 12.** Assume that $G$ is a finite group with trivial Frattini subgroup and let $I = I_G(A), R = R_G(A), U$ be as in the statement of Lemma 3. Let $g_1, \ldots, g_l \in G$. If $\langle g_1U, \ldots, g_lU \rangle_I = G/U$ and $\langle g_1R, \ldots, g_lR \rangle_I = G/R$, then $\langle g_1, \ldots, g_l \rangle_I = G$.

**Proof.** Let $x_1, \ldots, x_l \in G$ and consider $K = \langle x_1^{x_1}, \ldots, x_l^{x_l} \rangle$. Since $\langle g_1U, \ldots, g_lU \rangle_I = G/U$ (and resp. $\langle g_1R, \ldots, g_lR \rangle_I = G/R$) we have $KU = G$ (and resp. $KR = G$). But then $K = G$ by Lemma 3. \hfill \Box

**Lemma 13.** [17] Proof of Theorem 4.1] Denote by $P_G^*(k)$ the probability that $k$ randomly chosen elements $g_1, \ldots, g_k \in G$ have the property that there exists a maximal subgroup $M$ of $G$ such that the primitive group $G/\text{Core}_G(M)$ is not of affine type and $g_1, \ldots, g_k \in \cup_{g \in G} M^g$. For any $\epsilon > 0$, there exists $c_\epsilon$ such that $P_G^*(k) \leq \epsilon$ for any finite group $G$ and any $k \geq c_\epsilon (\log |G|)^2$.

**Proof.** This result is part of the proof of [17, Theorem 4.1]. In the first part of that proof, the authors show that

$$P_G^*(k) \leq c_1 \sqrt{|G|^3} \left(1 - c_2/\log |G|^k\right)^k$$

for some absolute constants $c_1$ and $c_2$ and notice that there exists $c_3$ such that if $k \geq c_3 (\log |G|)^2$, then the right-hand tends to zero as $|G| \to \infty$. \hfill \Box

The authors of [17] notice that the proof of the previous result uses [8, Theorem 8.1], which in turn relies on the conjecture, due to Boston and Shalev, stating that there exists an absolute constant $\epsilon > 0$ such that the proportion of fixed-point-free elements in any finite simple transitive permutation group is at least $\epsilon$. However, in [17] it is noticed that a weaker version of [8, Theorem 8.1] allows to prove that for any $\epsilon > 0$ there exists $c_\epsilon$ such that $P_G^*(k) \leq \epsilon$ for any finite group $G$ and
any $k \geq c_1 (\log |G|)^3 |G|^{1/3}$. This weaker version of Lemma 13 still suffices for our purpose.

We now introduce some other definitions. Let $N$ be a normal subgroup of a finite group $G$ and let $\Lambda_{G,N}$ be the set of the ordered sequence $(x_1, \ldots, x_d) \in G^d$ (for any possible choice of $d$) having the property that $(Nx_1, \ldots, Nx_d)_I = G/N$. For $\xi = (x_1, \ldots, x_d) \in \Lambda_{G,N}$, denote by $P_I(G, N, \xi, k)$ the probability that $k$ randomly chosen elements $y_1, \ldots, y_k$ of $G$ have the property that $(x_1, \ldots, x_d, y_1, \ldots, y_k)_I = G$ and let

$$P_I(G, N, k) = \inf_{\xi \in \Lambda_{G,N}} P_I(G, N, \xi, k).$$

We have in particular

$$P_I(G, k_1 + k_2) \geq P_I(G/N, k_1)P_I(G, N, k_2)$$

for every $k_1, k_2 \in \mathbb{N}$.

**Lemma 14.** Assume that $G$ is a finite group with trivial Frattini subgroup and let $I = I_G(A)$, $R = R_G(A)$, $U$ be as in the statement of Lemma 3. There exists an absolute constant $c$, independent on the choice of $G$, such that if $k \geq c(\log |G|)^{1/3}$, then $P_I(G, U, k) \geq 3/4$.

**Proof.** It suffices to prove that there exists an absolute constant $c$, independent on the choice of $G$ and $\xi$, such that if $k \geq c(\log |G|)^{1/3}$, then $P_I(G, U, \xi, k) \geq 3/4$ for every $\xi \in \Lambda_{G,U}$. So we fix $\xi = (x_1, \ldots, x_d) \in \Lambda_{G,U}$ and we estimate $P_I(G, U, \xi, k)$.

Let $\bar{G} = G/R$ and $\bar{\xi} = (x_1R, \ldots, x_dR) \in \bar{G}^d$. By Lemma 12 given $(y_1, \ldots, y_k) \in H^k$, if $(x_1R, \ldots, x_dR, y_1R, \ldots, y_kR)_I = \bar{G}$ then $(x_1, \ldots, x_d, y_1, \ldots, y_k)_I = G$, hence

$$P_I(G, U, \xi, k) \geq P_I(\bar{G}, \bar{\xi}, k),$$

and so we may assume $R = 1$. We have $R = R_G(A)$ where $A$ is an irreducible $G$-group: in particular $G = L_\delta$ where $L$ is the monolithic primitive group associated to $A$ and $\delta = \delta_G(A)$.

First assume that $A$ is nonabelian. We want to count the $k$-tuples $(y_1, \ldots, y_k)$ such that $(x_1, \ldots, x_d, y_1, \ldots, y_k)_I = G$. If $(x_1, \ldots, x_d, y_1, \ldots, y_k)_I \neq G$, then there exists a maximal subgroup $M$ of $G$ such that

$$\{x_1, \ldots, x_d, y_1, \ldots, y_k\} \subset \cup_{g \in G} M^g.$$

This $M$ cannot contain $U$, otherwise $\{Ux_1, \ldots, Ux_d\} \subset \cup_{g \in G/U} (M/U)^gU$, against the property that $Ux_1, \ldots, Ux_d$ invariably generate $G/U$. Thus $MU = G$ and, consequently, being $U \cong A^d$ with $A$ nonabelian, the primitive group $G/C_G(M)$ is not of affine type and $\{y_1, \ldots, y_k\} \subset \cup_{g \in G} M^g$. Hence, by Lemma 13 $P_I(G, U, \xi, k) \geq 1 - P_G^\xi(k) \geq 3/4$ if $k \geq c_1(\log |G|)^{1/3}$. Clearly there exists an absolute constant $c^*$ such that $c_1/4(\log m)^2 \leq c^* \sqrt{m}$ for every $m \in \mathbb{N}$.

We assume now that $A$ is abelian. In this case $A$ is $G$-isomorphic to an irreducible $G$-module $V$. Moreover either $V \cong C_p$ is a trivial $G$-module and $G \cong (C_p)^\delta$ or $G \cong U \rtimes H$ where $H$ acts in the same say on each of the $\delta$ factors of $U \cong V^\delta$ and this action is faithful and irreducible.

In the first case, denoting by $P(C_p^\delta, k)$ the probability that $k$ elements of $C_p^\delta$ generate $C_p^\delta$, we have

$$P_I(G, U, \xi, k) \geq P_I(C_p^\delta, k) = P(C_p^\delta, k) = \prod_{k-\delta+1 \leq i \leq k} \left(1 - \frac{1}{p^i}\right) \geq 1 - \frac{p^\delta - 1}{p - 1} \frac{1}{p^k} \geq 1 - \frac{p^\delta}{p^k},$$
in particular $P_l(G, U, \xi, k) \geq 3/4$ if $k \geq \delta + 2$: it suffices to choose $c \geq 3/\sqrt{2}$, since in that case $c\sqrt{|G|} \geq 3p^{\delta/2}/\sqrt{2} \geq \delta + 2$.

In the second case, we have $G = V^\delta \rtimes H$ and we estimate $P_l(G, U, \xi, k)$ by applying Proposition \ref{prop:main}. Let $F = \text{End}_H V$, with $|F| = q$, and let $n = \dim_F V$ (so in particular $|V| = q^n$). For $i \in \{1, \ldots, d\}$, let $x_i = k_i w_i$ with $w_i \in V^\delta$ and $k_i \in H$.

Now choose $y_1, \ldots, y_k \in G$, where $y_j = h_j w_j^\delta$ with $w_j^\delta \in V^\delta$ and $h_j \in H$. Given a subset $J = \{j_1, \ldots, j_f\}$ of $I = \{1, \ldots, k\}$, consider the projection $\pi_J : V^{d+k} \to V^f$ defined by setting $\pi_J(v_1, \ldots, v_d, v_1^*, \ldots, v_f^*) = (v_{j_1}^*, \ldots, v_{j_f}^*)$ and for $t \in \{1, \ldots, \delta\}$ let

$$r_t = (\pi_t(w_1), \ldots, \pi_t(w_d), \pi_t(w_1^*), \ldots, \pi_t(w_k^*)) \in V^{d+k},$$

$$r_{t,J} = \pi_J(r_t) = (\pi_t(w_{j_1}^*), \ldots, \pi_t(w_{j_f}^*)) \in V^f.$$ 

Moreover let

$$W = \{(u_1, \ldots, u_d, u_1^*, \ldots, u_k^*) | u_i \in [k_i, V] \text{ for } 1 \leq i \leq d, u_j^\delta \in [h_j, V] \text{ for } 1 \leq j \leq k\},$$

$$D = \{(\delta(k_1), \ldots, \delta(k_d), \delta(h_1), \ldots, \delta(h_k)) \in V^{d+k} | \delta \in \text{Der}(H, V)\},$$

$$W_J = \pi_J(W) = \{(u_{j_1}^*, \ldots, u_{j_f}^*) | u_{j_i} \in [h_{j_i}, V] \text{ for } 1 \leq i \leq f\},$$

$$D_J = \pi_J(D) = \{\pi(h_{j_1}, \ldots, h_{j_f}) \in V^f | \delta \in \text{Der}(H, V)\}.$$ 

Notice that if the vectors $r_{1,\ldots, \delta, J}$ are $F$-linearly independent modulo $W_J + D_J$ for some $J \subseteq I$, then $r_1, \ldots, r_{\delta}$ are linearly independent modulo $W + D$ and, by Proposition \ref{prop:main} \((x_1, \ldots, x_d, y_1, \ldots, y_k)_{1} = G\). Now let $m = \dim_F H^1(H, V)$ and distinguish the following cases:

1) $|H| \geq |V|^{m^2}$. Let $\Delta_l$ be the subset of $H^k$ consisting of the $k$-tuples $(h_1, \ldots, h_k)$ with the property that $C_V(h_i) \neq 0$ for at least $l$ different choices of $i \in \{1, \ldots, k\}$. If $(h_1, \ldots, h_k) \in \Delta_l$, then, by Lemma \ref{lem:main} \((x_1, \ldots, x_d, y_1, \ldots, y_k)_{1} = G\). Since $\delta$ is an element of $H$ of codimension at least $l - m$, so the probability that $r_{1,\ldots, \delta, I}$ are $F$-linearly independent modulo $W_I + D_I$ is at least

$$p_l = \left(\frac{q^{nk} - q^{nk-l+m}}{q^{nk}}\right) \cdots \left(\frac{q^{nk} - q^{nk-l+m+\delta-1}}{q^{nk}}\right) = \left(1 - \frac{1}{q^{l-m}}\right) \cdots \left(1 - \frac{q^{\delta-1}}{q^{l-m}}\right) \geq 1 - \left(\frac{q^{\delta-1}}{q-1}\right) \frac{1}{q^{l-m}}.$$ 

Notice in particular that $p_l \geq 7/8$ if $l \geq \delta + m + 3$ hence

$$P_l(G, U, \xi, k) \geq \frac{7\rho}{8}$$ 

where $\rho$ denotes the probability that $(h_1, \ldots, h_k) \in \Delta_{\delta+m+3}$. Therefore in order to conclude our proof it suffices to show that there exists a constant $c_1$ such that

$$\rho \geq 6/7 \text{ if } k \geq c_1 \sqrt{|G|}.$$ 

Let $p$ be the probability that a randomly chosen element $h$ of $H$ satisfies the condition $C_V(h) \neq 0$. We have

$$\rho = P(B(k, p) \geq \delta + m + 3).$$ 

Therefore, by Proposition \ref{prop:main} \(\rho \geq 6/7 \text{ if } k \geq \gamma(\delta + m + 3)/p\), being $\gamma = \gamma_{6/7}$. Let $v$ be a fixed nonzero vector of $V$ and let $H_v$ be the stabilizer of $v \in H$. Clearly $p \geq |H_v|/|H| \geq 1/|V| = 1/q^n$, hence $\rho \geq 6/7$ if $k \geq \gamma(\delta + m + 3)q^n$. Since we are assuming $|G| = |H||V|^\delta \geq q^{n^2}q^{n\delta} = q^{n(\delta+1)m^2}$, there exists an absolute constant $c_1$ such that

$$\gamma(\delta + m + 3)q^n \leq c_1 mq^{n(\delta+1)/2} \leq c_1 \sqrt{|G|}.$$ 

Hence $\rho \geq 6/7 \text{ if } k \geq c_1 \sqrt{|G|}$. 

b) $|H| \geq |V|$ and $m \leq \alpha$, where $\alpha$ is the constant with appears in the statement of Proposition 10. Arguing as before, we have that $P_l(G, U, \xi, k) \geq 3/4$ if

$$\gamma(\delta + m + 3)q^n \leq \gamma(\delta + \alpha + 3)q^n \leq k.$$ 

We are assuming $|G| = |H||V|^d \geq q^nq^d = q^{n(d+1)}$, so there exists a constant $c_2$ such that $\gamma(\delta + m + 3)q^n \leq \gamma(\delta + \alpha + 3)q^n \leq c_2q^{n(d+1)/2} \leq c_2\sqrt{|G|}$.

c) $|V| \leq |H| \leq |V|m^2$ and $m > \alpha$. We repeat the same argument as above, using the bound $p \geq |H|/m^2$, ensured by Proposition 10. We find that $P_l(G, U, \xi, k) \geq 3/4$ if $k \geq \gamma(\delta + m + 3)|H|/m^2$. Since $|H|^{1/2} \leq q^{n/2m}$, there exists a constant $c_3$ such that

$$\frac{\gamma(\delta + m + 3)|H|}{m^2} \leq \frac{\gamma(\delta + 4)|H|}{m} \leq \gamma(\delta + 4)|H|^{1/2}q^{1/2} \leq c_3|H|^{1/2}q^{\delta/2} \leq c_3\sqrt{|G|}.$$ 

d) $|H| \leq |V| = q^n$. Let $\Omega_l$ be the subset of $H^k$ consisting of the $k$-tuples $(h_1, \ldots, h_k)$ with the property that $h_i = 1$ for at least $l$ different choices of $i \in I = \{1, \ldots, k\}$. For a given $\omega \in \Omega_l$, let $J_\omega = \{i \in I \mid h_i = 1\}$ and let $l_\omega = |J_\omega| \geq l$. We have that $W_{J_\omega} + D_{J_\omega} = 0$, so the probability that $r_{1,J_\omega}, \ldots, r_{l,J_\omega}$ are $F$-linearly independent modulo $W_{J_\omega} + D_{J_\omega} = 0$ is at least

$$q_\omega = \frac{q^{|l_\omega|_\omega} - 1}{q^{|l_\omega|_\omega}} \cdot \frac{q^{|l_\omega|_\omega} - q^{|l_\omega|_\omega - 1}}{q^{|l_\omega|_\omega}} = \frac{1 - \frac{1}{q^{|l_\omega|_\omega}}}{1 - \frac{1}{q^{|l_\omega|_\omega}}} \cdot \frac{1 - \frac{q^{|l_\omega|_\omega - 1}}{q^{|l_\omega|_\omega}}}{1 - \frac{q^{|l_\omega|_\omega - 1}}{q^{|l_\omega|_\omega}}} \geq 1 - \frac{q^{|l_\omega|_\omega - 1}}{q^{|l_\omega|_\omega}} \geq 1 - \frac{q^{|l_\omega|_\omega - 1}}{q^{|l_\omega|_\omega}}.$$ 

Notice in particular that $q_\omega \geq 7/8$ if $nl \geq \delta + 3$ hence

$$P_l(G, U, \xi, k) \geq \frac{7p}{8}$$

where $\rho$ denotes the probability that the number of trivial entries in $(h_1, \ldots, h_k)$ is larger than $\lfloor (\delta + 3)/n \rfloor \leq \delta + 3$. Therefore in order to conclude our proof it suffices to show that there exist a constant $c_4$ such that $\rho \geq 6/7$ if $k \geq c_4\sqrt{|G|}$. By Proposition 11 $\rho \geq 6/7$ if $k \geq \gamma(\delta + 3)|H|$, being $\gamma = \sqrt{G}$. Since $|G| = |H||V|^d$ and $|H| \leq |V|$, there exists an absolute constant $c_4$ such that

$$\gamma(\delta + 3)|H| \leq c_4|H|q^{n/2(\delta - 1)} \leq c_4|H|^{1/2}q^{\delta/2} \leq c_4\sqrt{|G|}.$$ 

Hence $\rho \geq 6/7$ if $k \geq c_4\sqrt{|G|}$.

If we take $c = \max\{c^*, \sqrt{3}/2, c_1, c_2, c_3, c_4\}$, we have $P_l(G, U, k) \geq 3/4$. \hfill $\square$

6. Proof of Theorem 2

An easy argument (see the end of this section) shows that in order to prove Theorem 2 it suffices to prove the statement for a particular choice of the positive real number $\epsilon$. So the proof of Theorem 2 will be a corollary of the following result:

Theorem 15. Let $\bar{c} = 15c$ where $c$ is constant introduced in the statement of Lemma 14. If $G$ is a finite group and $k \geq \bar{c}\sqrt{|G|}$, then $P_l(G, k) \geq 2/9$.

Proof. Let $F_1 = \text{Frat}(G)$. By Lemma 8 there exists a crown $I_1/R_1$ of $G$ and a nontrivial normal subgroup $U_1/F_1$ of $G/F_1$ such that $I_1/F_1 = R_1/F_1 \times U_1/F_1$. If $U_1 = G$, then, since $k \geq \bar{c}\sqrt{|G|} \geq c\sqrt{|G|}$, $P_l(G, k) = P_l(G/F_1, k) \geq 3/4$ by Lemma 14. Otherwise let $F_2/U_1 = \text{Frat}(G/U_1)$ : again by Lemma 8 there exists a crown $I_2/R_2$ of $G$ and a nontrivial normal subgroup $U_2/F_2$ of $G/F_2$ such that
$I_2/F_2 = R_2/F_2 \times U_2/F_2$. If $U_2 = G$ then there exists two integers $k_1$ and $k_2$, both larger than $c\sqrt{|G|}$ and such that $k_1 + k_2 \leq \bar{c}\sqrt{|G|}$. By Lemma 14 we have
\[
P_I(G, k) \geq P_I(G, k_1 + k_2) \geq P_I(G/U_1, k_1) P(G, U_1, k_2)
\]
\[
= P_I(G/F_2, k_1) P(G, U_1, k_2) \geq \left(\frac{3}{4}\right)^2.
\]
Finally assume $G \neq U_2$. We have that $U_2/F_2 \sim G$, $A_2^{s_2}$ and $U_1/F_1 \sim G$, $A_1^{s_1}$, where $A_1$ and $A_2$ are non $G$-equivalent chief factors of $G$: in particular $|A_1||A_2| \geq 6$ and consequently $|G|/|U_2| \leq |G|/6$. But then
\[
k \geq \bar{c}\sqrt{|G|} = 15c\sqrt{|G|} \geq 30 \cdot c\sqrt{|G|/6} + c\sqrt{|G|/2} + c\sqrt{|G|} + 4
\]
and there exist three integers $k_1$, $k_2$ and $k_3$ such that
\[
k_1 + k_2 + k_3 \leq k, \quad k_1 \geq 2 \left[\bar{c}\sqrt{|G/U_2|}\right], \quad k_2 \geq c\sqrt{|G/U_1|}, \quad k_3 \geq c\sqrt{|G|}.
\]
By induction, if $t \geq \bar{c}\sqrt{|G/U_2|}$, then $p = P_I(G/U_2, t) \geq 2/9$ and consequently
\[
P_I(G/U_2, 2t) \geq 1 - (1 - p)^2 = 2p - p^2 \geq 32/81.
\]
Hence the probability that $(x_1, \ldots, x_{k_1}) \in G^{k_1}$ satisfies the condition
\[
\langle x_1 U_2, \ldots, x_{k_1} U_2 \rangle_I = G/U_2
\]
is at least $32/81$. Applying twice Lemma 14 we conclude that
\[
P_I(G, k_1 + k_2 + k_3) \geq \frac{32}{81} \cdot \frac{3}{4} \cdot \frac{3}{4} = \frac{2}{9}. \quad \square
\]

Proof of Theorem 2. Given $0 < \epsilon < 1$, there exists a positive integer $t$ such that
\[
\epsilon \geq (7/9)^t.
\]
Let $\tau = t(1 + \bar{c})$ where $\bar{c}$ is the constant introduced in the statement of Theorem 15. Let $k$ be an integer larger than $\tau\sqrt{|G|}$. We have
\[
t \left[\bar{c}\sqrt{|G|}\right] \leq t\bar{c}\sqrt{|G|} + t = \tau\epsilon\sqrt{G} \leq k
\]
hence there exist $t$ integers $k_1, \ldots, k_t$ such that $k_1 + \cdots + k_t \leq k$ and $k_i \geq \epsilon\sqrt{|G|}$ for all $i \in \{1, \ldots, t\}$. It follows
\[
P_I(G, k) \geq P_I(G, k_1 + \cdots + k_t) \geq 1 - \prod_{1 \leq i \leq t} (1 - P_I(G, k_i)) \geq 1 - (7/9)^t \geq 1 - \epsilon
\]
since $P_I(G, k_i) \geq 2/9$ by Theorem 15. \quad \square

References

11. J. Fulman and R.M. Guralnick, Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture, arXiv:1508.00039

Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy.
E-mail address: lucchini@math.unipd.it