Finite groups with large Chebotarev invariant

Lucchini, Andrea; Tracey, Gareth

Citation for published version (Harvard):
Lucchini, A & Tracey, G 2019, 'Finite groups with large Chebotarev invariant', *Israel Journal of Mathematics*, vol. 235, pp. 169-182.

ISRAEL JOURNAL OF MATHEMATICS **00** (XXXX), 1–13
DOI: 10.1007/s000000000000000000000000

FINITE GROUPS WITH LARGE CHEBOTAREV INVARIANT*

BY

ANDREA LUCCHINI

Università degli Studi di Padova, Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy

AND

GARETH TRACEY

Department of Mathematical Sciences, University of Bath, Bath BA2 7AY, United Kingdom

ABSTRACT

A subset $\{g_1, \dots, g_d\}$ of a finite group G is said to invariably generate G if the set $\{g_1^{x_1}, \dots, g_d^{x_d}\}$ 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 authors recently showed that for each $\epsilon > 0$, there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$. This bound is asymptotically best possible. In this paper we prove a partial converse: namely, for each $\alpha > 0$ there exists an absolute constant δ_α such that if G is a finite group and $C(G) > \alpha\sqrt{|G|}$, then G has a section X/Y such that $|X/Y| \geq \delta_\alpha\sqrt{|G|}$, and $X/Y \cong \mathbb{F}_q \rtimes H$ for some prime power q, with $H \leq \mathbb{F}_q^\times$.

1. Introduction

Following [10] and [5], we say that a subset $\{g_1, g_2, \dots, g_d\}$ of a group G *invariably generates* G if $\{g_1^{x_1}, g_2^{x_2}, \dots, g_d^{x_d}\}$ generates G for each d-tuple $(x_1, x_2 \dots, x_d) \in G^d$. The *Chebotarev invariant* $C(G)$ of G is the expected value of the random

* Partially supported by Università di Padova (Progetto di Ricerca di Ateneo: "Invariable generation of groups").

variable n which is minimal subject to the requirement that n randomly chosen elements of G invariably generate G.

Motivated by the problem of finding field extensions K/F such that a fixed finite group G occurs as the Galois group of K/F, E. Kowalski and D. Zywina carried out a detailed investigation of the invariant $C(G)$ in [12]. Amongst many interesting results, they show that $C(G)$ can be quite large in comparison to $|G|$. More precisely, it is shown that if $G \cong G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$, then

$$C(G) = q - \sum_{1 \neq d | q-1} \frac{\mu(d)}{q(1-d^{-1})(1-d^{-1}+q^{-1})}.$$

In particular, $C(G_q) \sim \sqrt{|G_q|}$ as $q \to \infty$. It was also conjectured in [12] that these are the "worst" cases: that is, that $C(G) = O(\sqrt{|G|})$ as $|G| \to \infty$. The conjecture was proved by the first author in [15], and was later improved in [17] where it is shown that for each $\epsilon > 0$, there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$. Furthermore, one has $C(G) \leq \frac{5}{3}\sqrt{|G|}$ when G is soluble.

In this paper, we prove a partial converse. Informally, we prove that the the only examples where $C(G)$ is a constant times $\sqrt{|G|}$ are those groups with a "large" section isomorphic to a subgroup of G_q, for some prime power q. Our main result reads as follows.

THEOREM 1: *Fix a constant $\alpha > 0$. There exists absolute constants β_α, γ_α, δ_α and k_α, depending only on α, such that whenever G is a finite group with the property that $C(G) > \alpha\sqrt{|G|}$, then G has a factor group $\overline{G}$ such that*

(i) $\overline{G} \cong V \rtimes H$, *with* $V \cong \mathbb{F}_q^k$, *and* $H \leq \Gamma L_1(q) \wr \mathrm{Sym}(k)$, *with q a prime power and $k \leq k_\alpha$;*
(ii) $|\overline{G}| \geq \delta_\alpha \sqrt{|G|}$; *and*
(iii) $\beta_\alpha |V| \leq |H| \leq \gamma_\alpha |V|$.

Our approach utilises the theory of crowns in finite groups, which we describe in Section 2. We also require a characterisation of those irreducible linear groups $H \leq GL(V)$ such that the set $H^*(V) := \{h \in H : v^h = v \text{ for some } v \in V \backslash \{0\}\}$ is bounded above by an absolute constant, and this is the content of Section 3. Finally, Section 4 is reserved for the proof of Theorem 1.

2. Crowns in finite groups

Before defining the notion of a crown in a finite group, we require some terminology. First, let L be a monolithic primitive group. That is, L is a finite group with a unique minimal normal subgroup $V \not\leq \mathrm{Frat}(L)$. For each positive integer k, write L^k for 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

$$L_k = \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \bmod V\}.$$

Equivalently, $L_k = V^k \,\mathrm{Diag}\, L^k$.

Next, let G be a finite group. We say that a group V is a *G-group* if G acts on V via automorphisms. Following [9], we say that two irreducible G-groups V_1 and V_2 are *G-equivalent* and we put $V_1 \sim_G V_2$, if there are isomorphisms $\phi : V_1 \to V_2$ and $\Phi : V_1 \rtimes G \to V_2 \rtimes G$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V_1 & \longrightarrow & V_1 \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \big\downarrow \phi & & \big\downarrow \Phi & & \Big\| & & \\ 1 & \longrightarrow & V_2 & \longrightarrow & V_2 \rtimes G & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Note that two G-isomorphic G-groups are G-equivalent. In the abelian case, the converse is true: if V_1 and V_2 are abelian and G-equivalent, then V_1 and V_2 are also G-isomorphic. It is proved (see for example [9, Proposition 1.4]) that two chief factors V_1 and V_2 of G are G-equivalent if and only if either they are G-isomorphic, or there exists a maximal subgroup M of G such that $G/\,\mathrm{Core}_G(M)$ has two minimal normal subgroups N_1 and N_2 G-isomorphic to V_1 and V_2 respectively. For example, the minimal normal subgroups of a crown-based power L_k are all L_k-equivalent.

Let $V = X/Y$ be a chief factor of G. A complement U to V in G is a subgroup U of G such that $UV = G$ and $U \cap X = Y$. We say that $V = X/Y$ is a Frattini chief factor if X/Y is contained in the Frattini subgroup of G/Y; this is equivalent to saying that V is abelian and there is no complement to V in G. The number of non-Frattini chief factors G-equivalent to V in any chief series of G does not depend on the series, and so this number is well-defined: we will write it as $\delta_V(G)$. We now define L_V, the monolithic primitive group associated to V, by

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

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

We now record a lemma and two propositions which will be crucial in our proof of Theorem 1. The lemma reads as follows.

Lemma 2: [1, Lemma 1.3.6] *Let G be a finite group with trivial Frattini subgroup. There exists a chief factor V of G and a non trivial normal subgroup U of G such that $I_G(V) = R_G(V) \times U$.*

To state the propositions, we need some additional notation. For a finite group G, and an abelian chief factor V of G, set $H_V = H_V(G) := G/C_G(V)$, $m = m_V = m_V(G) := \dim_{\mathrm{End}_G(V)} \mathrm{H}^1(H_V, V)$, and write $H^* = H^*(V) = H^*_G(V)$ for the set of elements h of H_V which fix a non-zero vector in V. Also, let $\delta_V = \delta_V(G)$, and set $\theta_V = \theta_V(G) = 0$ if $\delta_V = 1$, and $\theta_V = 1$ otherwise. Finally, let $q_V = q_V(G) := |\mathrm{End}_G(V)|$ and $n_V = n_V(G) := \dim_{\mathrm{End}_G(V)} V$. Note that $\mathrm{End}_G(V)$ is a finite field, since V is finite and irreducible.

Proposition 3: [17, Proposition 8 and the Proof of Theorem 1] *Let G be a finite group with trivial Frattini subgroup, and let U, V and $R = R_G(V)$ be as in Lemma 2. If U is non-abelian, then there exists absolute constants b_1, b_2 and b_3 such that*

$$C(G) \leq C(G/U) + \lceil b_3(\log|G|)^2\rceil + \frac{b_1}{b_2}\sqrt{|G|^3}\log|G|(1 - b_2/\log|G|)^{\lceil b_3(\log|G|)^2\rceil}.$$

Proposition 4: [17, Proposition 8 and the Proof of Theorem 1] *Let G be a finite group with trivial Frattini subgroup, and let U, V and $R = R_G(V)$ be as in Lemma 2. Suppose that V is abelian, and write $q = q_V$, $n = n_V$ and $H = H_V$, $H^* = H^*(V)$ and $m = m_V$. Also, set $\delta = \delta_V$ and $\theta = \theta_V$. Set*

$$\alpha_U := \begin{cases} \sum_{0\leq i\leq \delta-1} \frac{q^\delta}{q^\delta-q^i} \leq \delta + \frac{q}{(q-1)^2} & \text{if } H=1, \\ \min\left\{ \left(\delta\cdot\theta + m + \frac{q}{q-1}\right)\frac{|H|}{|H^*|}, \left(\lceil \frac{\delta\cdot\theta}{n}\rceil + \frac{q^n}{q^n-1}\right)|H| \right\} & \text{otherwise.} \end{cases}$$

Then

$$C(G) \leq C(G/U) + \alpha_U.$$

We conclude this section with the theorem of the first author mentioned in the introduction.

THEOREM 5: [15, Main Theorem] *There exists an absolute constant C such that $C(G) \leq C\sqrt{|G|}$ for any finite group G.*

3. Irreducible linear groups with few elements fixing a non-zero vector

Let V be a finite dimensional vector space over an arbitrary field. In this section, our aim is to characterise the groups $H \leq GL(V)$, such that the set of elements which fix at least one non-zero vector in V has cardinality bounded above by an absolute constant. For ease of notation, we will write

$$H^* = H^*(V) := \{h \in H : v^h = v \text{ for some } v \in V\backslash\{0\}\}$$

for such a subgroup H. Our main result reads as follows.

PROPOSITION 6: *Let V be a vector space of dimension n over a field F, and fix a constant $c > 0$. Suppose that H is an irreducible subgroup of $GL(V)$ with the property that $|H^*| \leq c$. Then there exists positive integers m and k such that $n = mk$, and $H \leq R \wr \mathrm{Sym}(k)$, where either $|R|$ has order bounded above by a function of $|H^*|$, or $R \cong \Gamma_1(F_m)$ for some extension field F_m of F of degree m.*

Proposition 6 will follows almost immediately from our next result. Recall that if F is a field, then an irreducible subgroup H of a linear group $GL_n(F)$ is called *weakly quasiprimitive* if every characteristic subgroup of G is homogeneous.

PROPOSITION 7: *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that if F is a field, n is a positive integer, and $H \leq GL_n(F)$ is finite and weakly quasiprimitive, then either $|H| \leq f(|H^*|)$, or H is a subgroup of $\Gamma L_1(F_n)$, for some extension field F_n of F of degree n.*

Proof. If $n = 1$, then $\Gamma L_n(F) = GL_n(F)$. Thus, we may assume that $n > 1$. Fix a subgroup H of $GL_n(F)$. We want to prove that if H is not a subgroup of $\Gamma L_1(F_n)$ for some extension field F_n of F of degree n, then $|H|$ is bounded in terms of $|H^*|$.

Suppose first that every characteristic abelian subgroup of H is contained in $Z(GL_n(F))$. Let L be the generalised Fitting subgroup of H. Our aim is to prove that $|L|$ is bounded above in terms of $|H^*|$. Since L is self-centralising, this will show that $|H|$ is bounded above in terms of $|H^*|$, which will give us what we need.

To this end, extend the field F so that F is a splitting field for all subgroups of L. Then L may longer be homogeneous, but its irreducible constituents are algebraic conjugates of each other, so L acts faithfully on them. Let W be such a constituent, and let r_i, m_i, s_i, t_i, S_i and T_i be as in [8, Lemma 2.14]. In particular, the r_i are prime numbers and L is a central product of the collection of groups $O_{r_i}(G)$, T_i, where T_i is a central product of t_i copies of a quasisimple group S_i. By [8, Lemmas 2.15, 2.16 and 2.17], W decomposes as a tensor product

$$W = W_Z \otimes W_{r_1} \otimes \ldots \otimes W_{r_a} \otimes W_{s_1} \otimes \ldots \otimes W_{s_b},$$

where W_Z is a 1-dimensional module for Z; W_{r_i} is an irreducible module for $O_{r_i}(G)$ of dimension $r_i^{m_i}$; and W_{s_i} is an irreducible module for T_i of dimension $s_i^{t_i}$. In particular, $[O_{r_i}(H), W_{r_j}] = [T_i, W_{s_j}] = 1$ for $i \neq j$, and $[O_{r_i}(H), W_{s_j}] = [T_i, W_{r_j}] = 1$, for all i, j. Hence, if $a + b > 1$, then $|L|$ is bounded above in terms of $|H^*|$, as needed. So we may assume that either $L = Z(G) \circ O_r(H)$, for some prime r, or $L = Z(G) \circ T$ is a central product of t copies of a quasisimple group S. If $Z(G) \not\leq O_r(H)$ in the first case, or $Z(G) \not\leq T$ in the second case, then the same argument as above gives that $|L|$ is bounded in terms of $|H^*|$.

So we may assume that either $L = O_r(H)$, for some prime r, or $L = T$ is a central product of t copies of a quasisimple group S. Hence, W is a tensor product of m [respectively t] copies of an irreducible module for an extraspecial group of order r^3 [resp. quasisimple group]. Thus, by arguing as in the paragraph above, we can immediately reduce to the case $m = 1$ [resp. $t = 1$].

Suppose first that $L = O_r(H) = M \rtimes \langle x \rangle$ is extraspecial of order r^3, for a prime r, where M is cyclic of order r^2 if L has exponent r^2, and M is elementary abelian of order r^2 otherwise. Then, being an absolutely irreducible module for L of dimension r, W is isomorphic to $U \uparrow_M^L$, where U is a one dimensional module for M in which $Z(L)$ acts non-trivially. Hence, we may write $W = \bigoplus_{i=0}^{r-1} U \otimes x^i$. It follows that for each non-zero vector $u \in U$, x^j fixes the non-zero vector $u \otimes 1 + u \otimes x + \ldots + u \otimes x^{r-1}$. Thus, $r \leq |H^*|$, from which it follows that $|L| = r^3$ is bounded above in terms of $|H^*|$, as needed.

Finally, assume that L is quasisimple. Since L acts on L^* by conjugation, we may assume that $L^* \leq Z$ (otherwise $L \leq \mathrm{Sym}(L^*)$, which would imply that $|L|$ is bounded above in terms of $|H^*|$). However, since $Z = Z(H) \leq Z(GL_n(F))$, Z acts on V by scalar multiplication. Hence, $Z \cap H^* = 1$. It follows that $L^* = 1$, and hence that L is a Frobenius complement in the group $V \rtimes L$. Since L is perfect, it now follows from Zassenhaus' Theorem that $L \cong SL_2(5)$. Whence, $|L|$ is bounded, and this proves our claim.

Finally, assume that H has a characteristic abelian subgroup not contained in $Z(GL_n(F))$, and let $M \leq H$ be maximal with this property. Then by [16, Lemma 1.10], M is contained in $Z(GL_{\frac{n}{m}}(F_m))$ for some m dividing n, and some extension field F_m of F of degree m. Hence, $H_1 := C_H(M)$ is a subgroup of $GL_{\frac{n}{m}}(F_m)$ with the property that every characteristic abelian subgroup of H_1 is contained in $Z(GL_{\frac{n}{m}}(F_m))$. Furthermore, H_1 is weakly quasiprimitive, since it is characteristic in H. Also, the group H/H_1 is naturally embedded in $\mathrm{Gal}(F_m/F)$, its action induced by a vector space isomorphism $F_m^{\frac{n}{m}} \to F^n$. Since $H_1^*(F_m^{\frac{n}{m}}) = H_1^*(F^n)$, it follows from the arguments above that either $|H_1|$ is bounded in terms of $|H^*|$; or $n = 1$. If $|H_1|$ is bounded in terms of $|H^*|$, then so is $|H|$, since H_1 is self-centralising and normal in H. If $n = 1$, then $H_1 \leq GL_1(F_n)$, so $H \leq \Gamma L_1(F_n)$, since H/H_1 acts on $M = Z(H_1)$ via the Galois group, as described above. This completes the proof. ∎

Finally, we prove Proposition 6.

Proof of Proposition 6. If H is primitive, then the result follows immediately from Proposition 7. Thus, we may assume that H is not primitive. Then V may be decomposed into a system $V = W_1 \oplus W_2 \oplus \ldots \oplus W_k$ of imprimitivity for H. Let $\Gamma := \{W_1, \ldots, W_k\}$, let $S := H^\Gamma$ denote the induced (transitive) action of H on Γ, and let $R := \mathrm{Stab}_H(W_1)^{W_1}$ denote the induced action of $\mathrm{Stab}_H(W_1)$ on W_1. Then H is isomorphic to a subgroup of the wreath product $R \wr S$.

Finally, since $\mathrm{Stab}_H(W)$ induces R on W, we have $|R^*(W_1)| \leq |H^*(V)|$. Hence, Proposition 7 implies that either $R \leq \Gamma L_1(F_m)$, for some extension F_m of F of degree m, or $|R|$ is bounded above by a function of $|H^*|$. This completes the proof. ∎

4. The proof of Theorem 1

We begin our preparations towards the proof of Theorem 1 with a lemma concerning the cohomology of an irreducible linear group which has a bounded number of elements fixing a non-zero vector.

LEMMA 8: *There exists an absolute constant c such that if V is a vector space of dimension n over a field F of characteristic $p > 0$, and H is an irreducible subgroup of $GL(V)$ with the property that $|H| > \sqrt{|V|}$, then $2^m \leq c|H^*|^4$, where $m := \dim_F \mathrm{H}^1(H, V)$ and $F := \mathrm{End}_H V$.*

Proof. Clearly we may assume that $m > 0$. Then, it is proven in [15, Lemma 9] that

(1) H has a unique minimal normal subgroup N, which is non-abelian.
(2) If S is a component of H, then $C_H(S) \subseteq H^*$.
(3) If W is an irreducible N-submodule of V not centralised by S, then $m \leq \dim_F \mathrm{H}^1(S, W)$.

Write $N = S_1 \times \ldots \times S_t \cong S^t$, and view H as a subgroup in the wreath product $\mathrm{Aut}(N) = \mathrm{Aut}(S) \wr K$, where K denote the induced action of H on the components in N. Suppose first that $t > 1$. Then (2) implies that $S_i \subseteq H^*$ for all i. Hence, $|H^*| \geq 1 + t(|S|-1)$. Also, $|H^*| \geq C_H(S_1) \geq |H \cap B||\,\mathrm{Stab}_K(1)| = |H \cap B|\frac{|K|}{t}$, where $B := \mathrm{Aut}(S_2) \times \ldots \times \mathrm{Aut}(S_t)$. Note that $|H| \leq |H \cap B||\,\mathrm{Aut}(S)||K|$. It follows that $|H| \leq |H^*|t|\,\mathrm{Aut}(S)| \leq |H^*|t(|S|-1)^2 \leq |H^*|^3$.

Next, it is shown by Guralnick and Hoffman in [7, Theorem 1] that $m \leq \frac{n}{2}$. Since we also have $|H| > \sqrt{|V|}$, it follows that

$$m \leq \frac{n}{2} \leq \log \sqrt{|V|} < \log |H| \leq \log |H^*|^3.$$

Thus, we may assume that $H \leq \mathrm{Aut}(S)$ is almost simple. Before distinguishing cases, we make some remarks. First, $p = \mathrm{char}\, F$ divides $|H|$, since $\mathrm{H}^1(H, V) \neq 0$. Furthermore, $|H^*| \geq |H|_p$, since every element of a Sylow p-subgroup of H fixes a non-zero vector in V. Finally, note that we may assume that S is not sporadic, since there are a bounded number of such groups having an irreducible module with non-zero cohomology.

Thus, we have two cases.

(a) $S \cong \mathrm{Alt}(k)$. In this case, we have $\frac{n}{2} \leq \log \sqrt{|V|} \leq \log |H| \leq k \log k$, as long as $k > 6$. Hence, by [15, Proof of Proposition 10], we have $m \leq 4 \log k$ and $|H|_p > \frac{k}{2}$, if k is large enough. Hence $2^m \leq k^4 \leq 16|H^*|^4$ in this case. If

k is bounded, then m is also bounded, since $m \leq \frac{n}{2} \leq \log |H|$. Hence, the result also follows in this case.

(b) $S \cong^{\epsilon} X_k(r)$ is a group of Lie type. Write $R_F(S)$ for the smallest degree of a non-trivial irreducible representation of S over the field F. If char F is different to the defining characteristic for S, then we have $p^{\frac{R_F(S)}{2}} > |\operatorname{Aut}(S)|$ for $|S|$ large enough (see [13, 18, 20]). Since $\sqrt{|V|} \leq |H|$, we conclude that either $|S|$ is bounded, or char F coincides with the defining characteristic of S. In the latter case, we have $|H|_p > |S|^{\frac{1}{3}}$ by [11, Proposition 3.5]. Also, $|S| \geq |\operatorname{Aut}(S)|^{\frac{4}{5}}$ by [14, Proposition 4.4]. Hence,

$$|H^*| > |S|^{\frac{1}{3}} \geq |\operatorname{Aut}(S)|^{\frac{4}{15}} > |H|^{\frac{1}{4}} \geq 2^{\frac{m}{4}}.$$

Thus, either $|S|$ is bounded, or $2^m \leq |H^*|^4$. This gives us what we need.

∎

Next, we prove a reduction lemma.

LEMMA 9: *Fix a constant $\alpha > 0$. There exists absolute constants $b = b(\alpha)$, $c = c(\alpha)$ and $c_i = c_i(\alpha)$, $1 \leq i \leq 4$, depending only on α, such that: If G is a finite group with trivial Frattini subgroup with the property that $C(G) > \alpha\sqrt{|G|}$, and U is as in Lemma 2, then one of the following holds.*

(i) U is non-abelian and $|G| \leq b$.
(ii) U is abelian and $|U| \leq c$.
(iii) U is abelian and G has a factor group $\overline{G}$ such that
   (a) $\overline{G} \cong V \rtimes H$, with $V \cong U$ an abelian chief factor of G, and $H \leq GL(V)$;
   (b) $|H^*(V)| \leq c_1$;
   (c) $\dim_{\operatorname{End}_H V} \mathrm{H}^1(H, V) \leq c_2$; and
   (d) $c_3|V| \leq |H| \leq c_4|V|$.

Proof. Adopt in its entirety the notation of Proposition 4, so that U, V and $R = R_G(V)$ are as in Lemma 2. We first consider the case where V is non-abelian. Then by Proposition 3 we have

$$\alpha\sqrt{|G|} < C(G/U) + \lceil b_3(\log |G|)^2\rceil + \frac{b_1}{b_2}\sqrt{|G|^3}\log |G|(1 - b_2/\log |G|)^{\lceil b_3(\log |G|)^2\rceil},$$

where b_1, b_2 and b_3 are the absolute constants from Proposition 3. Since $C(G/U) \leq C\sqrt{|G/U|}$, it follows that $\sqrt{|G|} \leq \alpha'\lceil b_3(\log |G|)^2\rceil + \frac{b_1}{b_2}\sqrt{|G|^3}\log |G|(1 - b_2/\log |G|)^{\lceil b_3(\log |G|)^2\rceil}$, for some constant α' depending only on α. Hence, since the square root of $|G|$ divided by the right hand side of the above equation tends to ∞ as $|G|$ tends to infinity, we must have that $|G|$ is bounded above by a constant $b = b(\alpha)$ depending only on α.

Thus, we may assume that U is abelian. Then by Proposition 4 and Theorem 5, there exists an absolute constant C such that

$$\alpha\sqrt{|G|} \leq C(G) \leq C(G/U) + \alpha_U \leq c\sqrt{\frac{|G|}{|U|}} + \alpha_U.$$

In particular, using the definition of α_U from Proposition 4, we conclude that

$$\alpha \leq \frac{c}{\sqrt{|U|}} + (\delta \cdot \theta + m + 2)\,\frac{\sqrt{|H|}}{\sqrt{|V|^{\delta}|H^*|}}, \text{ and} \tag{4.1}$$

$$\alpha \leq \frac{c}{\sqrt{|U|}} + \left(\left\lceil \frac{\delta \cdot \theta}{n} \right\rceil + 2\right) \frac{\sqrt{|H|}}{\sqrt{|V|^{\delta}}}. \tag{4.2}$$

We claim first that $\delta = 1$. Indeed, assume otherwise, and note that $\frac{|H|}{|H^*|} \leq |H|/|H_v| \leq |V|$, for any non-zero $v \in V$. Hence, since $m \leq \frac{n}{2}$, we conclude from (4.1) that

$$|V|^{\frac{\delta-1}{2}} \leq C_1(n+\delta), \tag{4.3}$$

where $C_1 = C_1(\alpha)$ depending only on α. Now, since $|U| = |V|^{\delta} = q^{n\delta}$, we conclude that there exists a constant $c = c(\alpha)$ such that if $|U| > c$ and $\delta > 1$ then $|V|^{\frac{\delta-1}{2}} > C_1(n+\delta)$.

Hence, we may assume that $\delta = 1$. We will first prove that the properties (b) and (c) of Part (iii) of thge statement of the lemma hold in the factor group $\overline{G} := G/R_G(V)$. If $|H| \leq \frac{|V|}{n^2}$, then (4.1) [respectively (4.2)] implies that $|H^*|$ [resp. n] is bounded above by a constant depending only on α. Properties (b) and (c) then follow immediately.

So we may assume that $|H| > \frac{|V|}{n^2}$. We then use (4.1) and the fact that $|H|/|H_v| \leq |V|$ to deduce that $|H^*| \leq C_2(1+m^2)$, where $C_2 = C_2(\alpha)$ is a constant depending only on α. Since $|H| > \sqrt{|V|}$, if follows from Lemma 8 that $|H^*| \leq C_3(1+\log|H^*|^2)$, where $C_3 = C_3(\alpha)$ is a constant depending only on α. It follows that $|H^*|$, and hence m, are bounded above by constants depending only on α. This proves that Properties (b) and (c) hold.

Finally, the existence of c_3 follows immediately from (4.2), while the existence of c_4 follows from (4.1) and the bound $|H|/|H^*| \leq |V|$. This proves that Property (d) holds, and completes the proof. ∎

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let C be the constant from Theorem 5; let f be the function from Proposition 7; let b_1, b_2 and b_3 be the constants from Proposition 3; and let $b = b(\alpha)$ and $c = c(\alpha)$ be the constants from Lemma 9. Also, let c_i, $1 \leq i \leq 4$, be the functions of α from Lemma 9. Note that we may assume that f, c_1, c_2 and c_4 are increasing functions, while c_3 is decreasing. Hence, we may also assume that g satisfies $g(\alpha_1\alpha_2) \geq g(\alpha_1)\alpha_2$, for $g \in \{f, c_1\}$. For ease of notation, we will sometimes write c_i in place of $c_i(\alpha)$.

Set $b_4 := \max\{b, \lceil b_3(\log b)^2\rceil + \frac{b_1}{b_2}\sqrt{b^3}\log b(1 - b_2/\log b)^{\lceil b_3(\log b)^2\rceil}\}$; $\alpha' := \max\{\alpha, C\}$; $c_5 := \max\{c, \frac{1}{c_3(\alpha')} f(\lfloor c_1(\alpha')\rfloor)^{\frac{c_1(\alpha')}{c_3(\alpha')}} \lfloor \frac{c_1(\alpha')}{c_3(\alpha')}\rfloor!\}$; and $c_6 := (2 + c_2)c_5$. Then define

$$\delta(\alpha) := \min\{f(\lfloor c_1(\beta)\rfloor) : 0 < \beta \leq \alpha'\} \text{ and}$$

$$k(\alpha) := \frac{c_1(\alpha')}{c_3(\alpha')}.$$

Finally, set $\beta := c_3$ and $\gamma := c_4$. Note that by construction k is an increasing function of α, and that

$$\delta(\beta\sqrt{u}) \geq \delta(\beta)\sqrt{u} \geq \delta(\alpha)\sqrt{u}, \tag{4.4}$$

whenever $\beta \leq \alpha$.

We will now prove by induction on $|G|$ that G has a factor group $\overline{G}$ such that

(i) $\overline{G} \cong V \rtimes H$, with $V \cong \mathbb{F}_q^k$, and $H \leq \Gamma L_1(q) \wr \mathrm{Sym}(k)$, with q a prime power and $k \leq k(\alpha)$;

(ii) $|\overline{G}| \geq \delta(\alpha)\sqrt{|G|}$; and

(iii) $\beta(\alpha)|V| \leq |H| \leq \gamma(\alpha)|V|$.

Suppose first that $\mathrm{Frat}(G) = 1$, and let U, V and $R = R_V(G)$ be as in Lemma 2. We would like to reduce to the case where $|G| > b$ if V is non-abelian, and $|U| > c_5$ if V is abelian. We first deal with the non-abelian case. So assume that V is non-abelian and that $|G| \leq b$. In this case, we have

$$\alpha\sqrt{|G|} < C(G/U) + b_4 \leq (1 + b_4)C(G/U),$$

by Proposition 3. In particular, it follows that $C(G/U) > \alpha_1\sqrt{|G/U|}$, where

$$\alpha_1 := \frac{\alpha\sqrt{|U|}}{1 + b_4}.$$

Note that $\gamma(\alpha_1) \leq \gamma(\alpha)$, since $\alpha_1 \leq \alpha$, and γ is an increasing function. Similarly, $k(\alpha_1) \leq k(\alpha)$ and $\beta(\alpha) \leq \beta(\alpha_1)$. Furthermore, $\delta(\alpha_1) \geq \delta(\alpha)\sqrt{|U|}$ by (4.4). The inductive hypothesis now implies that G, and hence G/U, has a factor group $\overline{G}$ with the desired properties.

Next, assume that V is abelian, and that $|U| \leq c$. Then since $\alpha_U \leq c_6$, Proposition 4 yields $C(G/U) > \alpha_2\sqrt{|G/U|}$, where

$$\alpha_2 := \frac{\alpha\sqrt{|U|}}{1+c_6}.$$

As above, it now follows from the inductive hypothesis and the definitions of $\delta(\alpha)$ and $k(\alpha)$ that G has a factor group $\overline{G}$ with the desired properties.

Thus, we may assume that $|G| > b$ if U is non-abelian, and $|U| > c_5 \geq c$ otherwise. However, Lemma 9 then implies that U must be abelian, and that G has a factor group $\overline{G}$ such that

(a) $\overline{G} \cong V \rtimes H$, with $V \cong U$ an abelian chief factor of G, and $H \leq GL(V)$;
(b) $|H^*(V)| \leq c_1(\alpha)$;
(c) $\dim_{\mathrm{End}_H V} \mathrm{H}^1(H,V) \leq c_2(\alpha)$; and
(d) $c_3(\alpha)|V| \leq |H| \leq c_4(\alpha)|V|$.

Furthermore, Lemma 6 guarantees the existence of positive integers m and k, and a transitive permutation group S of degree k, such that $n = mk$ and $H \leq R \wr S$, with either $|R| \leq f(c_1)$, or $R \leq \Gamma L_1(p^m)$. Hence, we just need to prove that $k \leq k(\alpha)$. Indeed, if this is true then we must have $R \leq \Gamma L_1(p^m)$, since otherwise $|V| \leq \frac{1}{c_3(\alpha)}|H| \leq \frac{1}{c_3(\alpha)} f(c_1(\alpha))^{\frac{c_1(\alpha)}{c_3(\alpha)}} \lfloor \frac{c_1(\alpha)}{c_3(\alpha)} \rfloor!$, contradicting $|U| > c_5$.

Now, note that (b) and (d) above imply that the number of orbits of H in its action on V is bounded above by $1 + \frac{c_1}{c_3}$. Hence, the number of orbits of $X := GL_m(p) \wr \mathrm{Sym}(k)$ is bounded above by $1 + \frac{c_1}{c_3}$. Then since $GL_m(p)$ has 2 orbits in its action on the natural module $(\mathbb{F}_p)^m$, it follows that the number of orbits of X on V is precisely the number of orbits of $\mathrm{Sym}(k)$ in its action on the k-fold cartesian power $\{0,1\}^k$ by permutation of coordinates. This number is precisely $k+1$. Hence, we have $k + 1 \leq 1 + \frac{c_1}{c_3}$, and this completes the proof in the case $\mathrm{Frat}(G) = 1$.

Finally, assume that $\mathrm{Frat}(G) > 1$. Then $C(G/\mathrm{Frat}(G)) = C(G) > \beta\sqrt{|G/\mathrm{Frat}(G)|}$, where $\beta := \alpha\sqrt{|\mathrm{Frat}(G)|}$. Now, since $\alpha\sqrt{|G|} < C(G/\mathrm{Frat}(G)) \leq C\sqrt{|G/\mathrm{Frat}(G)|}$, we have $|\mathrm{Frat}(G)| \leq (\frac{C}{\alpha})^2$. Hence, $\beta \leq C$. The result now follows from the inductive hypothesis and the definitions of $\delta(\alpha)$ and $k(\alpha)$. ∎

References

1. A. Ballester-Bolinches and L. M. Ezquerro, Classes of finite groups, Mathematics and Its Applications (Springer), vol. 584, Springer, Dordrecht, 2006.
2. P. J. Cameron, Permutation groups, London Math. Soc. (Student Texts), vol. 45, CUP, Cambridge, 1999.
3. F. Dalla Volta and A. Lucchini, Finite groups that need more generators than any proper quotient, J. Austral. Math. Soc., Series A, 64, (1998) 82–91.
4. E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, J. Algebra, 265 (2003), no. 2, 651–668.
5. J. D. Dixon, Random sets which invariably generate the symmetric group, Discrete Math 105 (1992) 25-39.
6. W. Gaschütz, Praefrattinigruppen, Arch. Mat. 13 (1962) 418–426.
7. R. Guralnick and C. Hoffman, The first cohomology group and generation of simple groups, Proceedings of the Conference on Groups and Geometries, Siena, September 1996 (eds. L. Di Martino, W.M. Kantor, G. Lunardon, A. Pasini and M.C. Tamburini, Birkhäuser, Basel) (1998), 149–153.
8. D.F. Holt and C.M. Roney-Dougal, Minimal and random generation of permutation and matrix groups, J. Algebra 387 (2013), 195–223.
9. P. Jiménez-Seral and J. Lafuente, On complemented nonabelian chief factors of a finite group, Israel J. Math. 106 (1998), 177–188.
10. W. M. Kantor, A. Lubotzky and A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, J. Algebra 348 (2011), 302–314.
11. W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague, Composition factors from the group ring and Artins theorem on orders of simple groups, Proc. London Math. Soc. (3) 60 (1990), no. 1, 89–122.
12. E. Kowalski and D. Zywina, The Chebotarev invariant of a finite group, Exp. Math. 21 (2012), no. 1, 38–56.
13. V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, J. Algebra 32 (1974), 418–443.
14. M. Liebeck, L. Pyber and A. Shalev, On a conjecture of G.E. Wall. J. Algebra 317 (2007), 184–197.
15. A. Lucchini, The Chebotarev invariant of a finite group: A conjecture of Kowalski and Zywina, Proc. Amer. Math. Soc. 146 (11) (2018), 4549–4962.
16. A. Lucchini, F. Menegazzo and M. Morigi, On the number of generators and composition length of finite linear groups, J. Algebra 243 (2001), 427–447.
17. A. Lucchini and G. Tracey, An upper bound on the Chebotarev invariant of a finite group, Israel J. Math. 219 (1) (2017), 449–467.
18. G. Seitz and A. Zalesskii, On the minimal degrees of projective representations of the finite Chevalley groups II, J. Algebra 158 (1993), no. 1, 233–243.
19. U. Stammbach, Cohomological characterisations of finite solvable and nilpotent groups, J. Pure Appl. Algebra 11 (1977/78), no. 1–3, 293–301.
20. P. H. Tiep, Low dimensional representations of finite quasisimple groups, Groups, combinatorics and geometry (Durham, 2001), 277–294, World Sci. Publ., River Edge, NJ, 2003.