An upper bound on the Chebotarev invariant of a finite group

Lucchini, Andrea; Tracey, Gareth

Citation for published version (Harvard):
Lucchini, A & Tracey, G 2017, 'An upper bound on the Chebotarev invariant of a finite group', *Israel Journal of Mathematics*, vol. 219, no. 1, pp. 449-467.

ISRAEL JOURNAL OF MATHEMATICS **00** (XXXX), 1–18
DOI: 10.1007/s000000000000000000000000

AN UPPER BOUND ON THE CHEBOTAREV INVARIANT OF A FINITE GROUP*

BY

ANDREA LUCCHINI

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

AND

GARETH TRACEY

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom

ABSTRACT

A subset $\{g_1, \dots, g_d\}$ of a finite group G invariably generates 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 first author recently showed that $C(G) \leq \beta\sqrt{|G|}$ for some absolute constant β. In this paper we show that, when G is soluble, then β is at most 5/3. We also show that this is best possible. Furthermore, we show that, in general, for each $\epsilon > 0$ there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$.

1. Introduction

Following [8] 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 every 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 variable n that is minimal subject to the requirement that n randomly chosen elements of G invariably generate G.

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

In [9], Kowalski and Zywina conjectured that $C(G) = O(\sqrt{|G|})$ for every finite group G. Progress on the conjecture was first made in [8], where it was shown that $C(G) = O(\sqrt{|G|}\log|G|)$ (here, and throughout this paper,"log" means log to base 2). The conjecture was confirmed by the first author in [10]; more precisely, [10, Theorem 1] states that *there exists an absolute constant β such that $C(G) \leq \beta\sqrt{|G|}$ whenever G is a finite group.*

In this paper, we use a different approach to the problem. In doing so, we show that one can take $\beta = 5/3$ when G is soluble, and that this is best possible. Furthermore, we show that for each $\epsilon > 0$, there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$. From [9, Proposition 4.1], one can see that this is also (asymptotically) best possible.

Our main result is as follows

Theorem 1: *Let G be a finite group.*

(i) For any $\epsilon > 0$, there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|}+c_\epsilon$;
(ii) If G is a finite soluble group, then $C(G) \leq \frac{5}{3}\sqrt{|G|}$, with equality if and only if $G = C_2 \times C_2$.

We also derive an upper bound on $C(G)$, for a finite soluble group G, in terms of the set of *crowns* for G. Before stating this result, we require the following notation: Let G be a finite soluble group. Given an irreducible G-module V which is G-isomorphic to a complemented chief factor of G, let $\delta_V(G)$ be the number of complemented factors in a chief series of G which are G-isomorphic to V. Then set $\theta_V(G) = 0$ if $\delta_V(G) = 1$, and $\theta_V(G) = 1$ otherwise. Also, let $q_V(G) := |\operatorname{End}_G(V)|$, let $n_V(G) := \dim_{\operatorname{End}_G(V)} V$, and let $H_V(G) := G/C_G(V)$ (we will suppress the G in this notation when the group is clear from the context). Also, let $\sigma := 2.118456563\ldots$ be the constant appearing in [11, Corollary 2]. The afore mentioned upper bound can now be stated as follows.

Theorem 2: *Let G be a finite soluble group, and let A [respectively B] be a set of representatives for the irreducible G-modules which are G-isomorphic to a non-central [resp. central] complemented chief factor of G. Then*

$$C(G) \leq \sum_{V\in A} \min\left\{(\delta_V\cdot\theta_V + c_V)|V|, \left(\left\lceil\frac{\delta_V\cdot\theta_V}{n_V}\right\rceil + \frac{q_V^{n_V}}{q_V^{n_V}-1}\right)|H_V|\right\} + \max_{V\in B}\delta_V + \sigma$$

where $c_V := q_V/(q_V-1) \leq 2$.

The layout of the paper is as follows. In Section 2 we recall the notion of a *crown* in a finite group. In Section 3 we prove Theorem 2 and deduce a number of consequences, while Section 4 is reserved for the proof of Theorem 1 Part (i). Finally, we prove Theorem 1 Part (ii) in Section 5.

2. Crowns in finite groups

In Section 2, we recall the notion and the main properties of 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

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

Equivalently, $L_k = A^k \operatorname{Diag} L^k$.

Following [7], 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:

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

Note that two G-isomorphic G-groups are G-equivalent. In the particular case where V_1 and V_2 are abelian 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 [7, 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 between them or there exists a maximal subgroup M of G such that $G/\operatorname{Core}_G(M)$ 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 $\delta_V(G)$ of non-Frattini chief factors G-equivalent to V in any chief series of G does not depend on the series. Now, we denote by L_V the monolithic primitive group associated to V, that is

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

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.

Lemma 3: [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 $I_G(V) = R_G(V) \times U$.*

Lemma 4: [4, Proposition 11] *Assume that G is a finite group with trivial Frattini subgroup and let $I_G(V), R_G(V), U$ be as in the statement of Lemma 3. If $KU = KR_G(V) = G$, then $K = G$.*

3. Crown-based powers with abelian socle

The aim of this section is to prove Theorem 2. For a finite group G and an irreducible G-group V, we write $\Omega_{G,V}$ for the set of maximal subgroups M of G such that either $\mathrm{soc}\,(G/\operatorname{Core}_G(M)) \sim_G V$ or $\mathrm{soc}\,(G/\operatorname{Core}_G(M)) \sim_G V \times V$. Also, for $M \in \Omega_{G,V}$, we write $\widetilde{M}$ for the union of the G-conjugates of M. We will also say that the elements $g_1, g_2, \ldots, g_k \in G$ *satisfy the V-property in* G if $g_1, g_2, \ldots, g_k \in \widetilde{M}$ for some $M \in \Omega_V$. Finally, let $P^*_{G,V}(k)$ denote the probability that k randomly chosen elements of G satisfy the V-property in G.

Suppose now that V is abelian, and consider the faithful irreducible linear group $H := G/C_G(V)$. We will denote by $\mathrm{Der}(H,V)$ the set of the derivations from H to V (i.e. the maps $\zeta : H \to V$ with the property that $\zeta(h_1h_2) = \zeta(h_1)^{h_2} + \zeta(h_2)$ for every $h_1, h_2 \in H$). If $v \in V$ then the map $\zeta_v : H \to V$ defined by $\zeta_v(h) = [h, v]$ is a derivation, called an *inner derivation* from H to V. The set $\mathrm{InnDer}(H,V) = \{\zeta_v \mid v \in V\}$ of the inner derivations from H to V is a subgroup of $\mathrm{Der}(V,H)$ and the factor group $\mathrm{H}^1(H,V) = \mathrm{Der}(H,V)/\,\mathrm{InnDer}(H,V)$ is the first cohomology group of H with coefficients in V.

Proposition 5: *Let H be a group acting faithfully and irreducibly on an elementary abelian p-group V. For a positive integer u, we consider the semidirect product $G = V^u \rtimes H$ where the action of H is diagonal on V^u; that is, H acts in the same away on each of the u direct factors. Assume also that $u = \delta_V(G)$. View V as a vector space over the field $F = End_H(V)$. Let $h_1, \dots, h_k \in H$, and $w_1, \dots, w_k \in V^u$, and write $w_i = (w_{i,1}, w_{i,2}, \dots, w_{i,u})$. Assume that $h_1w_1, h_2w_2, \dots, h_kw_k$ satisfy the V-property in G. Then for $1 \le j \le u$, the vectors*

$$r_j := (w_{1,j}, w_{2,j}, \dots, w_{k,j})$$

of V^k are linearly dependent modulo the subspace $W + D$, where

$$W := \{(y_1, y_2, \dots, y_k) : y_i \in [h_i, V] \text{ for } 1 \le i \le k\}, \text{ and}$$
$$D := \left\{(\zeta(h_1), \zeta(h_2), \dots, \zeta(h_k)) \in V^k : \zeta \in \mathrm{Der}(H,V)\right\}.$$

Proof. Let M be a maximal subgroup of G such that $M \in \Omega_V$, and $h_1w_1, \dots, h_kw_k \in \widetilde{M}$. Since $u = \delta_V(G)$, M cannot contain V^u, and hence $MV^u = G$. Thus, $M/M \cap V^u \cong H$, and hence there exists an integer $t \ge 0$ and elements $h_{k+1}w_{k+1}, \dots, h_{k+t}w_{k+t} \in M$ such that $h_1, \dots, h_k, h_{k+1}, \dots, h_{k+t}$ invariably generate H. But then, [10, Proposition 6] implies, in particular, that $r_1, \dots, r_u \in V^k$ are linearly dependent modulo $W + D$, as needed. ∎

Before proceeding to the proof of Theorem 2, we require the following easy result from probability theory.

Proposition 6: *Write $B(k,p)$ for the binomial random variable with k trials and probability $0 < p \le 1$. Fix $l \ge 0$. Then*

$$\sum_{k=l}^{\infty} P(B(k,p) = l) \le \frac{1}{p}.$$

Proof. Note first that

$$\binom{k}{l} x^{k-l} = \frac{1}{l!}\frac{d^l}{dx^l}x^k$$

where $\frac{d^l}{dx^l}x^k$ denotes the l-th derivative of x^k. Let $x = 1 - p$. By definition, $P(B(k,p) = l) = \binom{k}{l}(1-x)^l x^{k-l}$. Thus

$$\begin{aligned}\sum_{k=l}^{\infty} P(B(k,p) = l) &= (1-x)^l \sum_{k=l}^{\infty} \binom{k}{l} x^{k-l} \\ &= \frac{(1-x)^l}{l!} \sum_{k=l}^{\infty} \frac{d^l}{dx^l} x^k \\ &= \frac{(1-x)^l}{l!} \frac{d^l}{dx^l} \sum_{k=l}^{\infty} x^k \\ &\leq \frac{(1-x)^l}{l!} \frac{d^l}{dx^l} \frac{1}{1-x} \\ &= \frac{(1-x)^l}{l!} \frac{l!}{(1-x)^{(l+1)}} = \frac{1}{1-x} = \frac{1}{p}\end{aligned}$$

as needed. (Note that the third equality above follows since the series $\sum_{k=l}^{\infty} x^k$ is convergent.) ∎

We shall also require the following. We remark that since $P^*_{G,V}(k) \leq \sum_{\widetilde{M}\in\Omega_V} \left(\frac{|\widetilde{M}|}{|G|}\right)^k$ and $\frac{|\widetilde{M}|}{|G|} < 1$, $\sum_{k=0}^{\infty} P^*_{G,V}(k)$ converges.

Proposition 7: *Let G be a finite group, and let A [respectively B] be a set of representatives for the irreducible G-groups which are G-equivalent to a non-central [resp. central] non-Frattini chief factor of G. Then*

1. *$C(G) \leq \sum_{V\in A} \sum_{k=0}^{\infty} P^*_{G,V}(k) + \max_{V\in B} \delta_V + \sigma$, and;*
2. *If $\mathrm{Frat}(G) = 1$ and U and V are as in Lemma 3, then $C(G) \leq C(G/U) + \sum_{k=0}^{\infty} P^*_{G,V}(k)$.*

Proof. By definition, $C(G) = \sum_{k=0}^{\infty}(1 - P_I(G,k))$, where $P_I(G,k)$ denotes the probability that k randomly chosen elements of G invariably generate G. Let $P_{G,G/G'}(k)$ denote the probability that k randomly chosen elements $g_1, \ldots, g_k$ of G satisfy $\langle G'g_1, \ldots, G'g_k\rangle = G$. Then it is easy to see that

$$1 - P_I(G,k) \leq 1 - P_{G,G/G'}(k) + \sum_{V\in A} P^*_{G,V}(k). \tag{3.1}$$

Clearly $P_{G,G/G'}(k)$ is the probability that a random k-tuple of elements from G/G' generates G/G'. Hence, $C(G/G') = \sum_{k=0}^{\infty}(1 - P_{G,G/G'}(k))$ is at most $d(G/G') + \sigma$ by [11, Corollary 2] (here, for a group X, $d(X)$ denotes the minimal number of elements required to generate X). Since $d(G/G') \leq \max_{V\in B}\delta_V$, it follows from (3.1) that $C(G) \leq \max_{V\in B}\delta_V + \sigma + \sum_{V\in A}\sum_{k=0}^{\infty} P^*_{G,V}(k)$, and Part (i) follows.

Assume that $\mathrm{Frat}(G) = 1$, and let U and V be as in Lemma 3. Then

$$1 - P_I(G,k) \leq 1 - P_I(G/U,k) + \sum_W P^*_{G,W}(k) \tag{3.2}$$

where the sum in the second term goes over all complemented chief factors W of G not containing U. Now, if M is a maximal subgroup of G not containing U, then M contains $R_G(V)$, by Lemma 4. Hence, $\mathrm{Core}_G(M)$ contains $R_G(V)$, so $M \in \Omega_{G,V}$. Since $C(G) = \sum_{k=0}^{\infty}(1 - P_I(G,k))$, Part (ii) now follows immediately from (3.2), and this completes the proof. ∎

The proof of Theorem 2 will follow as a corollary of the proof of the next proposition. 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 $p = p_V = p_V(G)$ for the probability that a randomly chosen element h of H_V fixes a non zero vector in V. Also, let $\delta_V = \delta_V(G)$ be the number of complemented factors in a chief series of G which are G-isomorphic to V, 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 $n_V = n_V(G) := \dim_{\mathrm{End}_G(V)} V$.

Proposition 8: *Let G be a finite group with trivial Frattini subgroup, and let U, V and $R = R_G(V)$ be as in Lemma 3. If V is nonabelian, then set $\alpha_U := \sum_{k=0}^{\infty} P^*_{G,V}(k)$. If V is abelian, then write $q = q_V$, $n = n_V$ and $H = H_V$, $p = p_V$ and $m = m_V$. Also, set $\delta = \delta_V$ and define $\theta = 0$ if $\delta = 1$, $\theta = 1$ otherwise, and set*

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

Then

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

Proof. By Proposition 7 Part (ii), we have

$$C(G) \leq C(G/U) + \sum_{k=0}^{\infty} P^*_{G,V}(k). \tag{3.3}$$

Thus, we just need to prove that $\sum_{k=0}^{\infty} P^*_{G,V}(k) \leq \alpha_U$. Therefore, we may assume that V is abelian. Writing bars to denote reduction modulo $R_G(V)$, note that if M is a maximal subgroup of G with $M \in \Omega_{G,V}$, then $R_G(V) \leq M$ and $\overline{M} \in \Omega_{\overline{G},V}$. Hence, $P^*_{G,V}(k) \leq P^*_{\overline{G},V}(k)$, so we may assume that $R_G(V) = 1$. Thus, $G \cong V^\delta \rtimes H$, where H acts faithfully and irreducibly on V, and diagonally on V^δ.

Suppose first that $|H| = 1$. Then $G = V^\delta \cong (C_r)^\delta$, for some prime r, and $P^*_{G,V}(k)$ is the probability that k randomly chosen elements of G fail to generate G. Hence, $\sum_{k=0}^{\infty} P^*_{G,V}(k)$ is the expected number of random elements to generate $(C_r)^\delta$, which is well known to be

$$\sum_{i=0}^{\delta-1} \frac{r^\delta}{r^\delta - r^i}.$$

See, for instance, [11, top of page 193].

So we may assume that $|H| > 1$. Let $F = \mathrm{End}_H V$, so that $|F| = q$, $\dim_F V = n$, and $|V| = q^n$. Fix elements x_1, x_2 ,..., x_k in G, and for $i \in \{1, \ldots, k\}$, let $x_i = w_i h_i$ with $w_i \in V^\delta$ and $h_i \in H$. For $t \in \{1, \ldots, \delta\}$ let

$$r_t = (\pi_t(w_1), \ldots, \pi_t(w_k)) \in V^k.$$

where π_t denotes projection onto the t-th direct factor of V^δ. Moreover let

$$W := \{(u_1, u_2, \ldots, u_k) : u_i \in [h_i, V] \text{ for } 1 \leq i \leq k\}, \text{ and}$$
$$D := \left\{(\zeta(h_1), \zeta(h_2), \ldots, \zeta(h_k)) \in V^k : \zeta \in \mathrm{Der}(H, V)\right\}.$$

By Proposition 5, $P^*_{G,V}(k)$ is at most the probability that $r_1, \ldots, r_\delta$ are linearly dependent modulo $W + D$. Also, for an f-tuple $J := (j_1, j_2, \ldots, j_f)$ of distinct elements j_i of $\{1, \ldots, k\}$, set

$$r_{t,J} := (\pi_t(w_{j_1}), \pi_t(w_{j_2}), \ldots, \pi_t(w_{j_f})) \in V^f$$

for $t \in \{1, \ldots, \delta\}$, and set

$$W_J := \left\{(u_{j_1}, u_{j_2}, \ldots, u_{j_f}) \in V^f : u_i \in [h_{j_i}, V] \text{ for } 1 \leq i \leq f\right\}, \text{ and}$$
$$D_J := \left\{(\zeta(h_{j_1}), \zeta(h_{j_2}), \ldots, \zeta(h_{j_f})) \in V^f : \zeta \in \mathrm{Der}(H, V)\right\}.$$

Notice that: $(*)$ If J is fixed and $r_1, \ldots, r_\delta$ are F-linearly dependent modulo $W + D$, then the vectors $r_{1,J}, \ldots, r_{\delta,J}$ of V^f are F-linearly dependent modulo $W_J + D_J$.

We will prove first that

$$\sum_{k=0}^{\infty} P^*_{G,V}(k) \leq (\delta\cdot\theta + m + c_V)\frac{1}{p}, \tag{3.4}$$

where c_V is as in the statement of Theorem 2. To this end, let Δ_l be the subset of H^k consisting of the k-tuples $(h_1,\dots,h_k)$ with the property that $C_V(h_i)\neq 0$ for precisely l different choices of $i\in\{1,\dots,k\}$. If $(h_1,\dots,h_k)\in\Delta_l$, then, by [10, Lemma 7], $W+D$ is a subspace of $V^k\cong F^{nk}$ of codimension at least $l-m$: so the probability that $r_1,\dots,r_\delta$ are F-linearly dependent modulo $W+D$ is at most

$$\begin{aligned} p_l &= 1-\left(\frac{q^{nk}-q^{nk-l+m}}{q^{nk}}\right)\cdots\left(\frac{q^{nk}-q^{nk-l+m+\delta-1}}{q^{nk}}\right)\\ &= 1-\left(1-\frac{1}{q^{l-m}}\right)\cdots\left(1-\frac{q^{\delta-1}}{q^{l-m}}\right)\\ &\leq \min\left\{1,\left(\frac{q^\delta-1}{q-1}\right)\frac{1}{q^{l-m}}\right\}\leq \min\left\{1,1/q^{l-m-\delta\cdot\theta}\right\}. \end{aligned}$$

Hence, we have

$$\begin{aligned} \sum_{k=0}^{\infty} P^*_{G,V}(k) &\leq \sum_{k=0}^{\infty}\sum_{l=0}^{k} P(B(k,p)=l)\min\left\{1,q^{\delta\cdot\theta+m-l}\right\}\\ &\leq \sum_{k=0}^{\infty} P(B(k,p)<\delta\cdot\theta+m)+\sum_{k=0}^{\infty}\sum_{l=\delta\cdot\theta+m}^{k} P(B(k,p)=l)q^{\delta\cdot\theta+m-l}\\ &\leq \sum_{k=0}^{\infty} P(B(k,p)<\delta\cdot\theta+m)+\sum_{l=0}^{\infty}q^{-l}\sum_{k=l+\delta\cdot\theta+m}^{\infty} P(B(k,p)=l+\delta\cdot\theta+m)\\ &\leq \frac{\delta\cdot\theta+m+c_V}{p} \end{aligned}$$

where $c_V=\frac{q}{q-1}$. Note that the last step above follows from Proposition 6.

Thus, all that remains is to show that

$$\sum_{k=0}^{\infty} P^*_{G,V}(k) \leq \left(\left\lceil\frac{\delta\cdot\theta}{n}\right\rceil+\frac{q^n}{q^n-1}\right)|H|. \tag{3.5}$$

For this, we define Ω_l to be the subset of H^k consisting of the k-tuples $(h_1,\dots,h_k)$ with the property that $h_i=1$ for precisely l different choices of $i\in\{1,\dots,k\}$. Suppose that $(h_1,\dots,h_k)\in\Omega_l$, and set $J:=(j_1,j_2,\dots,j_l)$, where $j_1<j_2<\dots<j_l$ and $\{j_1,j_2,\dots,j_l\}=\{i\mid 1\leq i\leq k, h_i=1\}$. Then, by $(*)$, the probability p'_l that r_1, r_2, …, r_δ are F-linearly dependent modulo $W+D$ is at

most the probability that the vectors $r_{1,J}, r_{2,J}, \ldots, r_{\delta,J} \in V^l$ are F-linearly dependent modulo $W_J + D_J$. But $W_J + D_J = 0$, by the definition of J. Thus we have

$$\begin{aligned} p'_l &\leq 1 - \left(\frac{q^{nl}-1}{q^{nl}}\right)\cdots\left(\frac{q^{nl}-q^{nl-\delta-1}}{q^{nl}}\right) \\ &= 1 - \left(1-\frac{1}{q^{nl}}\right)\cdots\left(1-\frac{q^{\delta-1}}{q^{nl}}\right) \leq \min\left\{1, \left(\frac{q^{\delta}-1}{q-1}\right)\frac{1}{q^{nl}}\right\} \leq \min\left\{1, \frac{1}{q^{nl-\delta\cdot\theta}}\right\}. \end{aligned}$$

Hence, if $\alpha := \lceil \frac{\delta\cdot\theta}{n} \rceil$, and $p' = 1/|H|$ is the probability that a randomly chosen element of H is the identity, then we have

$$\begin{aligned} \sum_{k=0}^{\infty} P^*_{G,V}(k) &\leq \sum_{k=0}^{\infty} P(B(k,p') < \alpha) + \sum_{k=0}^{\infty}\sum_{l=\alpha}^{k} P(B(k,p') = l) q^{\delta\cdot\theta - nl} \\ &\leq \sum_{k=0}^{\infty} P(B(k,p') < \alpha) + \sum_{l=0}^{\infty} q^{-nl-n\alpha+\delta\cdot\theta} \sum_{k=l+\alpha}^{\infty} P(B(k,p') = l+\alpha) \\ &\leq \sum_{k=0}^{\infty} P(B(k,p') < \alpha) + \sum_{l=0}^{\infty} q^{-nl} \sum_{k=l+\alpha}^{\infty} P(B(k,p') = l+\alpha) \\ &\leq \frac{1}{p'}\left(\alpha + \frac{q^n}{q^n-1}\right) \end{aligned}$$

Note that the last step above again follows from Proposition 6. Since $p' = 1/|H|$, (3.5) follows, whence the result. ∎

We are now ready to prove Theorem 2.

Proof of Theorem 2. By Proposition 7 Part (i), we have

$$C(G) \leq \max_{V\in B} \delta_V + \sigma + \sum_{k=0}^{\infty}\sum_{V\in A} P^*_{G,V}(k)$$

Thus, it will suffice to prove that

$$\sum_{k=0}^{\infty} P^*_{G,V}(k) \leq \min\left\{(\delta_V + c_V) q_V^{n_V}, \left(\left\lceil\frac{\delta_V}{n_V}\right\rceil + \frac{q_V^{n_v}}{q_V^{n_V}-1}\right)|H_V|\right\} \tag{3.6}$$

for each non-central complemented chief factor V of G.

However, since $\mathrm{H}^1(H,V) = 0$ by [12, Lemma 1], and since $p_V \leq |H_v|/|H| \leq 1/|V|$ (for any non-zero vector $v \in V$), this follows immediately from the proof of Proposition 8. ∎

Corollary 9: *Let G be a finite soluble group, and let A and B be as in Theorem 2. Then*

$$C(G) \leq d(G) \sum_{V \in A} \left(1 + \frac{q_V^{n_V}|H_V|}{q_V^{n_V}-1}\right) + \sigma.$$

Proof. For $V \in A \cup B$, set $\gamma_V := \lceil \delta_V/n_V \rceil$, and $p'_V = 1/|H_V|$. Note also that $n_V = |H_V| = 1$ when $V \in B$. Arguing as in the last paragraph of the proof of Proposition 8, we have

$$\begin{aligned} C(G) &\leq \sum_{V \in A} \sum_{k=0}^{\infty} \sum_{l=0}^{k} \min\{q_V^{-n_V l+\delta_V}, 1\} P(B(k,p'_V)=l) + \max_{V \in B} \delta_V + \sigma \\ &\leq \sum_{V \in A} \sum_{k=0}^{\infty} P(B(k,p'_V) < \gamma_V) + \sum_{V \in A} \sum_{l=0}^{\infty} q_V^{-n_V l} \sum_{k=l+\gamma_V}^{\infty} P(B(k,p'_V) = l+\gamma_V) + \\ &\quad \max_{V \in B} \delta_V + \sigma \\ &\leq \sum_{V \in A} \gamma_V/p'_V + \sum_{V \in A} \frac{{q_V}^{n_V}}{p'_V({q_V}^{n_V}-1)} + \max_{V \in B} \delta_V + \sigma \\ &\leq \left(\max_{V \in A \cup B} \gamma_V\right) \sum_{V \in A} \left(1 + \frac{{q_V}^{n_V}}{{q_V}^{n_V-1}}\right) |H_V| + \sigma. \end{aligned}$$

We remark that the third inequality above follows from Proposition 6. Finally, [3, Theorem 1.4 and paragraph after the proof of Theorem 2.7] imply that $d(G) = \max_{V \in A \cup B} \left\{1 + a_V + \left\lfloor \frac{\delta_V - 1}{n_V} \right\rfloor \right\}$, where $a_V = 0$ if $V \in B$, and $a_V = 1$ otherwise. In particular, $d(G) \geq \max_{V \in A \cup B} \gamma_V$, and the result follows. ∎

4. Proof of Theorem 1 Part (i)

Before proceeding to the proof of Part (i) of Theorem 1, we require the following result, which follows immediately from the arguments used in [10, Proof of Proposition 10].

Proposition 10: [10, Proof of Proposition 10] *Let H be a finite group acting faithfully and irreducibly on an elementary abelian group V, and denote by p the probability that a randomly chosen element h of H centralises a non zero vector of V. Also, write $m := \dim_{\mathrm{End}_H(V)} \mathrm{H}^1(H,V)$. Assume that $\mathrm{H}^1(H,V)$ is nontrivial and that $|H| \geq |V|$. Then there exists an absolute constant C such that $p|H| \geq 2(m+1)^2$ if $|H| \geq C$.*

Proof of Theorem 1 Part (i). Since $C(G) = C(G/\operatorname{Frat}(G))$, we may assume that $\operatorname{Frat}(G) = 1$. Thus, Proposition 8 applies: adopting the same notation as used therein, we have

$$C(G) \leq C(G/U) + \alpha_U. \tag{4.1}$$

Using (4.1), the proof of the theorem reduces to proving that

$$\alpha_U \leq (1+\beta_U)\sqrt{|G|} \tag{4.2}$$

where $\beta_U \to 0$ as $|U| \to \infty$. Indeed, suppose that (4.2) holds, fix $\epsilon > 0$, and suppose that Theorem 1 holds for groups of order less than $|G|$. Then since $|U| > 1$, there exists a constant c_ϵ such that $C(G/U) \leq (1+\epsilon)\sqrt{|G/U|} + c_\epsilon$. Hence, by (4.1) and (4.2) we have $C(G) \leq (1+\beta_U + \frac{1+\epsilon}{\sqrt{|U|}})\sqrt{|G|} + c_\epsilon$. It is now clear that by choosing $|U|$ to be large enough, we have $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$, as needed.

Assume first that U is nonabelian. By [10, Proof of Lemma 13], there exist absolute constants c_1 and c_2 such that

$$P^*_{G,V}(k) \leq \min\left\{1, c_1\sqrt{|G|^3}(1-c_2/\log|G|)^k\right\}.$$

Also, there exists a constant c_3 such that if $k \geq c_3(\log|G|)^2$, then $c_1\sqrt{|G|^3}(1-c_2/\log|G|)^k$ tends to 0 as $|G|$ tends to ∞. It follows that

$$\begin{aligned}
\alpha_U &= \sum_{k=0}^{\infty} P^*_{G,V}(k)\\
&\leq \lceil c_3(\log|G|)^2\rceil + c_1\sqrt{|G|^3}(1-c_2/\log|G|)^{\lceil c_3(\log|G|)^2\rceil}\sum_{k=0}^{\infty}(1-c_2/\log|G|)^k\\
&= \lceil c_3(\log|G|)^2\rceil + \frac{c_1}{c_2}\sqrt{|G|^3}\log|G|(1-c_2/\log|G|)^{\lceil c_3(\log|G|)^2\rceil}
\end{aligned}$$

and (4.2) holds.

So we may assume that U is abelian, and hence $|G| \geq |V|^\delta|H|$. The inequality (4.2) then follows easily from the definition of α_U, except when $\delta = 1$ and $|H| \geq |V|$. Indeed, if $|H| \leq |V|$ and $\delta = 1$, then $\frac{q^n}{q^n-1} \to 1$ as $|U| = q^n \to \infty$; if $|H| \leq |V|$ and $\delta > 1$, then

$$\left(\left\lceil\frac{\delta}{n}\right\rceil + \frac{q^n}{q^n-1}\right)|H| \leq \frac{\left\lceil\frac{\delta}{n}\right\rceil + \frac{q^n}{q^n-1}}{|V|^{\frac{\delta-1}{2}}}\sqrt{|G|}$$

which clearly gives us what we need, since $|U| = |V|^\delta$ is tending to ∞. The other cases are similar.

So assume that $\delta = 1$ and $|H| \geq |V|$. We distinguish two cases:

(1) $m \neq 0$ and $|V| \leq |H| \leq (m+1)^2|V|$. Denote by p the probability that a randomly chosen element h of H centralizes a non-zero vector of V: By Proposition 10, there exists an absolute constant C such that $p|H| \geq 2(m+1)^2$ if $|H| \geq C$. Thus,

$$\alpha_U \leq \left(m + \frac{q}{q-1}\right)\frac{1}{p} \leq (m+2)\frac{|H|}{2(m+1)^2} \leq \frac{|H|}{m+1} \leq \sqrt{|H||V|}$$

if $|H| \geq C$, from which (4.2) follows.

(2) $|H| \geq |V|(m+1)^2$. We remark first that, for any fixed nonzero vector v in V, we have $p \geq \frac{|H_v|}{|H|}$, where H_v denotes the stabiliser of v in H. If H is not a transitive linear group, then there is an orbit Ω for the action of H on $V\setminus\{0\}$ with $|\Omega| \leq q^n/2$. Choose $v \in \Omega$: we have

$$\frac{1}{p} \leq \frac{|H|}{|H_v|} \leq \frac{q^n}{2},$$

hence

$$\alpha_U \leq \frac{m+2}{p} \leq (m+1)q^n \leq \sqrt{|H||V|}.$$

We remain with the case when H is a transitive linear group. There are four infinite families:

(a) $H \leq \Gamma L(1, q^n)$;
(b) $SL(a, r) \trianglelefteq H$, where $r^a = q^n$;
(c) $Sp(2a, r) \trianglelefteq H$, where $a \geq 2$ and $r^{2a} = q^n$;
(d) $G_2(r) \trianglelefteq H$, where q is even, and $q^n = r^6$.

Furthermore, H and m are exhibited in [2, Table 7.3]: in each case, we have $m \leq 1$. Furthermore, we have $|H| = (q^n - 1)\rho$, where ρ is the order of a point stabiliser. Hence, if $\rho \geq 9$, then

$$\alpha_U \leq \frac{m+2}{p} \leq \frac{3}{p} \leq 3|V| \leq \sqrt{|H||V|}.$$

So we may assume that $\rho \leq 8$. Suppose first that (a) holds. Then H is soluble, so $m = 0$. Also, $\rho = |H_v| \leq 8$ implies that $n \leq 8$. Hence, as $q^n \leq q^8$ approaches ∞, $\frac{q}{q-1}$ approaches 1, and (4.2) follows since

$$\alpha_U \leq \frac{q}{q-1}|V| \leq \frac{q}{q-1}\sqrt{|H||V|}.$$

So we may assume that (a) does not hold. In particular, if (b) or (c) holds then $a \geq 2$. It follows (in either of the cases (b), (c) or (d)) that if q^n is large enough, then $|H| \geq 9q^n$, and so

$$\alpha_U \leq \frac{(m+2)}{p} \leq 3q^n \leq \sqrt{|H||V|}.$$

This gives us what we need, and completes the proof. ∎

5. Proof of Theorem 1 Part (ii)

In this section, we prove Part (ii) of Theorem 1 in a number of steps. The first is as follows:

Lemma 11: *Let G be a finite soluble group with trivial Frattini subgroup, and let U and V be as in Lemma 3. Assume that V is abelian and non-central in G, and let $H = H_V$. Then*

$$\frac{\alpha_U}{|G|^{1/2}} < \frac{5}{3}\left(\frac{|U|^{1/2}-1}{|U|^{1/2}}\right)$$

except when $|H| < |V|$ and one of the following cases occur:

(1) $\delta = 2$, $q^n = 4$ and $|R_G(V)| = 1$.
(2) $\delta = 2$, $q^n = 3$ and $|R_G(V)| \leq 2$.
(3) $\delta = 1$, $4 \leq q^n \leq 7$ and $|R_G(V)| = 1$.
(4) $\delta = 1$, $q^n = 3$ and $|R_G(V)| \leq 3$.

Proof. Note that $m = 0$ since H is soluble. We distinguish the following cases: Case 1) $|H| < |V|$ and $\delta \neq 1$. Since, $|G| = \lambda|H||V|^\delta$ for some positive integer λ it suffices to prove

$$\frac{3\left(\delta+\frac{q^n}{q^n-1}\right)\left(\frac{q^{n\delta/2}}{q^{n\delta/2}-1}\right)|H|}{5\lambda^{1/2}|H|^{1/2}q^{n\delta/2}} \leq \frac{3}{5\lambda^{1/2}}\left(\delta+\frac{q^n}{q^n-1}\right)\left(\frac{(q^n-1)^{1/2}}{q^{n\delta/2}-1}\right) < 1. \tag{5.1}$$

If $\delta \geq 3$ then

$$\frac{3}{5\lambda^{1/2}}\left(\delta+\frac{q^n}{q^n-1}\right)\left(\frac{(q^n-1)^{1/2}}{q^{n\delta/2}-1}\right) \leq \frac{3}{5\lambda^{1/2}}\left(3+\frac{q^n}{q^n-1}\right)\left(\frac{(q^n-1)^{1/2}}{q^{3n/2}-1}\right) < 1.$$

Suppose $\delta = 2$. If $q^n \geq 5$, then

$$\frac{3}{5\lambda^{1/2}}\left(\delta+\frac{q^n}{q^n-1}\right)\left(\frac{(q^n-1)^{1/2}}{q^{n\delta/2}-1}\right) \leq \frac{3}{5\lambda^{1/2}}\left(2+\frac{q^n}{q^n-1}\right)\left(\frac{(q^n-1)^{1/2}}{q^{n}-1}\right) < 1.$$

Suppose $\delta = 2$ and $q^n = 4$. We have $|H| = 3$ so if $\lambda \neq 1$, then

$$\frac{3\left(\delta+\frac{q^n}{q^n-1}\right)\left(\frac{q^{n\delta/2}}{q^{n\delta/2}-1}\right)|H|}{5\lambda^{1/2}|H|^{1/2}q^{n\delta/2}} \leq \frac{2\cdot 3^{1/2}}{3\cdot\lambda^{1/2}} < 1$$

Suppose $\delta = 2$ and $q^n = 3$. We have $|H| = 2$ so if $\lambda > 2$, then

$$\frac{3\left(\delta+\frac{q^n}{q^n-1}\right)\left(\frac{q^{n\delta/2}}{q^{n\delta/2}-1}\right)|H|}{5\lambda^{1/2}|H|^{1/2}q^{n\delta/2}} \leq \frac{21\cdot 2^{1/2}}{20\cdot\lambda^{1/2}} < 1.$$

Case 2) $|H| \geq |V|$ (and consequently $n \neq 1$) and $\delta \neq 1$. It suffices to prove that

$$\frac{3\left(\delta+\frac{q}{q-1}\right)\left(\frac{q^{n\delta/2}}{q^{n\delta/2}-1}\right)q^n}{5|H|^{1/2}q^{n\delta/2}} < 1. \tag{5.2}$$

Suppose $q^n \neq 4$.

$$\frac{3\left(\delta+\frac{q}{q-1}\right)\left(\frac{q^{n\delta/2}}{q^{n\delta/2}-1}\right)q^n}{5|H|^{1/2}q^{n\delta/2}} \leq \frac{3\left(2+\frac{q}{q-1}\right)\left(\frac{q^n}{q^n-1}\right)}{5q^{n/2}} < 1.$$

Suppose $q^n = 4$. We have $H = \mathrm{GL}(2,2) \cong \mathrm{Sym}(3)$, and consequently $|H| = 6$ and $p = 2/3$. Hence

$$\frac{\alpha_U}{|G|^{1/2}}\frac{5}{3}\left(\frac{|U|^{1/2}}{|U|^{1/2}-1}\right) \leq \frac{(\delta+2)\cdot\frac{1}{p}\cdot\frac{3}{5}\cdot\frac{4}{3}}{|H|^{1/2}\cdot 2^\delta} \leq \frac{6}{5\sqrt{6}} < 1.$$

Case 3) $|H| < |V|$ and $\delta = 1$. Since, $|G| = \lambda|H||V|^\delta$ for some positive integer λ it suffices to prove

$$\frac{3\left(\frac{q^n}{q^n-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)|H|^{1/2}}{5\lambda^{1/2}q^{n/2}} < 1. \tag{5.3}$$

If $q^n \geq 8$, or $7 \geq q^n \geq 4$ and $\lambda \neq 1$, or $q^n = 3$ and $\lambda > 3$, then

$$\frac{3\left(\frac{q^n}{q^n-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)|H|^{1/2}}{5\cdot\lambda^{1/2}\cdot q^{n/2}} \leq \frac{3\left(\frac{q^n}{q^n-1}\right)\left(\frac{(q^n-1)^{1/2}}{q^{n/2}-1}\right)}{5\cdot\lambda^{1/2}} = \frac{3\left(\frac{q^n}{(q^n-1)^{1/2}(q^{n/2}-1)}\right)}{5\cdot\lambda^{1/2}} < 1.$$

Case 4) $|H| \geq |V|$ (and consequently $n \neq 1$) and $\delta = 1$. It suffices to prove that

$$\frac{3\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)}{5|H|^{1/2}q^{n/2}p} < 1. \tag{5.4}$$

If H is not a transitive linear group, then $|H|^{1/2}q^{n/2}p \geq 2$, so it suffices to have

$$\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right) \leq \frac{10}{3},$$

which is true if $(q,n) \neq (2,2)$. On the other hand, we may exclude the case $(q,n) = (2,2)$: indeed the only soluble irreducible subgroup of $\mathrm{GL}(2,2)$ with order ≥ 4 is $\mathrm{GL}(2,2)$, which is transitive on the nonzero vectors.

If H is a transitive linear group, then $|H| = (q^n - 1)\rho$, with ρ the order of the stabilizer in H of a nonzero vector and

$$\frac{3\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)}{5|H|^{1/2}q^{n/2}p} \leq \frac{3\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)}{5\sqrt{\rho}},$$

so it suffices to have

$$\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right) \leq \frac{5\sqrt{\rho}}{3},$$

which is true if $q \geq 3$ and if $(q,n,\rho) \notin \{(2,4,2),(2,3,2),(2,3,3),(2,2,2))\}$. We may exclude the case $(q,n,\rho) = (2,3,2)$ (there is no transitive linear subgroup of $\mathrm{GL}(3,2)$ of order 14). If $(q,n,\rho) = (2,4,2)$, then $H = \mathrm{GL}(1,16) \rtimes C_2$, hence $p = 6/30$ so $|H|^{1/2}q^{n/2}p \geq 2$ and (5.4) is true. If $(q,n,\rho) = (2,3,3)$ then $H = \Gamma\mathrm{L}(1,8)$ and consequently $p = 15/21$ and

$$\frac{3\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)}{5|H|^{1/2}q^{n/2}p} = \frac{3\cdot 2\cdot\sqrt{8}\cdot 21}{5\cdot(\sqrt{8}-1)\cdot 15\cdot\sqrt{21}\sqrt{8}} < 1.$$

If $(q,n,\rho) = (2,2,2)$ then $H = \mathrm{GL}(2,2)$ and consequently $p = 2/3$ and

$$\frac{3\left(\frac{q}{q-1}\right)\left(\frac{q^{n/2}}{q^{n/2}-1}\right)}{5|H|^{1/2}q^{n/2}p} = \frac{3\cdot 2\cdot 2\cdot 3}{5\cdot 2\cdot 2\cdot\sqrt{6}} < 1. \qquad \blacksquare$$

Lemma 12: *If G is one of the exceptional cases in the statement of Lemma 11, then $C(G) < \frac{5}{3}\sqrt{|G|}$.*

Proof. This follows easily by direct computation. We use MAGMA, and the code from [9, Appendix, page 36] to compute $C(G)$ explicitly whenever G is a group satisfying the conditions of one of the exceptional cases of Lemma 11. $\blacksquare$

The next step is to deal with the case of a central chief factor.

Lemma 13: *If $G \cong C_p^\delta$, then $C(G) \leq \frac{5}{3}\sqrt{|G|}$, with equality if and only if $G = C_2 \times C_2$.*

Proof. If $p \neq 3$ or $p = 2$ and $\delta > 3$, then

$$C(G) = \sum_{0 \leq i \leq \delta-1} \frac{p^\delta}{p^\delta - p^i} \leq \delta + \frac{p}{(p-1)^2} < \frac{5 \cdot p^{\delta/2}}{3} = \frac{5 \cdot \sqrt{|G|}}{3}.$$

If $(p, \delta) = (2, 1)$ then

$$\frac{C(G)}{\sqrt{G}} = \frac{2}{\sqrt{2}} = \sqrt{2};$$

if $(p, \delta) = (2, 2)$ then

$$\frac{C(G)}{\sqrt{G}} = \frac{\frac{4}{2} + \frac{4}{3}}{2} = \frac{5}{3};$$

if $(p, \delta) = (2, 3)$ then

$$\frac{C(G)}{\sqrt{G}} = \frac{\frac{8}{4} + \frac{8}{6} + \frac{8}{7}}{\sqrt{8}} \sim 1.5826. \qquad \blacksquare$$

Proof of Part (ii) of Theorem 1. We prove the claim by induction on the order of $|G|$. If $\operatorname{Frat}(G) \neq 1$, then the conclusion follows immediately since $C(G) = C(G/\operatorname{Frat}(G))$. Otherwise G contains a normal subgroup U as in Lemma 4. If $G = U \cong C_p^\delta$, then the conclusion follows from Lemma 13. Otherwise, Lemma 11, together with the inductive hypothesis gives

$$C(G) \leq C(G/U) + \alpha_U < \frac{5\sqrt{|G|}}{3\sqrt{|U|}} + \frac{5(\sqrt{|U|}-1)\sqrt{|G|}}{3\sqrt{|U|}} = \frac{5}{3}\sqrt{|G|}$$

as claimed. $\blacksquare$

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. P. Jiménez-Seral and J. Lafuente, On complemented nonabelian chief factors of a finite group, Israel J. Math. 106 (1998), 177–188.
8. W. M. Kantor, A. Lubotzky and A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, J. Algebra 348 (2011), 302–314.

9. E. Kowalski and D. Zywina, The Chebotarev invariant of a finite group, Exp. Math. 21 (2012), no. 1, 38–56.
10. A. Lucchini, The Chebotarev invariant of a finite group: A conjecture of Kowalski and Zywina, arXiv:1509.05859v2.
11. C. Pomerance, The expected number of random elements to generate a finite abelian group, Per. Math. Hungaria Vol. 43, 1-2, (2001), 191–198
12. U. Stammbach, Cohomological characterisations of finite solvable and nilpotent groups, J. Pure Appl. Algebra 11 (1977/78), no. 1–3, 293–301.