ON THE COMMUTING PROBABILITY IN FINITE GROUPS

ROBERT M. GURALNICK AND GEOFFREY R. ROBINSON

For Bernd Fischer on the occasion of his 70th birthday

Introduction: When G is a finite group, we may endow $G \times G$ with the structure of a probability space by assigning the uniform distribution. As was pointed out by W.H. Gustafson [10], the probability that a randomly chosen pair of elements of G commute is then $\frac{k(G)}{|G|}$, where $k(G)$ is the number of conjugacy classes of G. We denote this probability by $\mathrm{cp}(G)$. It was also noted in [10] that $\mathrm{cp}(G) \leq \frac{5}{8}$ for any non-Abelian finite group G and equality holds precisely when $[G : Z(G)] = 4$.

Our work here has several objectives. One is to point out some general properties of $\mathrm{cp}(G)$ which may not have been observed before. Another is to give elementary (ie free of the classification of finite simple groups (CFSG)) proofs of numerical properties of $\mathrm{cp}(G)$ with explicit (but sometimes crude) bounds, though in one case we use CFSG to sharpen significantly an estimate obtained without it. We show that $\mathrm{cp}(G) \to 0$ as either the index or the derived length of the Fitting subgroup of G tends to infinity. Dihedral 2-groups illustrate that the same is not true for the nilpotence class. The third objective is to point out that the solution of the (coprime) $k(GV)$-problem can lead to some quite strong information about cp (we mostly use this for solvable groups in which case the results do not depend on CFSG. In fact, the case when G is nilpotent is important to us, and that case was proved by R. Knörr [12] in his early work on the $k(GV)$-problem). One general result in this direction which we prove is:

$$\mathrm{cp}(G) \leq \mathrm{cp}(F)^{1/2}[G : F]^{-1/2} \leq [G : F]^{-1/2},$$

where F is the Fitting subgroup of G. This result depends on CFSG for general G but only on [12] for solvable G. Note that this can be restated as

$$k(G) \leq (k(F)|G|)^{1/2} \leq (|F||G|)^{1/2}.$$

A related result of a similar nature, which makes full use of the solution of the $k(GV)$-problem for solvable groups is that for a non-trivial finite solvable group G, we always have $k(G) \leq \frac{|F|^2}{2}$, where F is as above.

J. Dixon observed that $\mathrm{cp}(G) \leq 1/12$ for any finite non-Abelian simple group G (this was submitted by Dixon as a problem in Canadian Math. Bulletin, 13, (1970), with his own solution appearing in 1973). Of course, this bound is attained for $G = A_5$. We extend this result to non-solvable groups (and determine precisely for which non-solvable groups equality is attained). This may be compared with the result [9] that if G is a finite non-solvable group, then the probability that two

Date: September 18, 2005.

The first author acknowledges support from the NSF grant DMS 0140578. The second author is grateful to the Centre Bernoulli, EPFL, Switzerland for its support and hospitality during the preparation of this work. Both authors thank Attila Maróti for his comments and the referee for careful reading of the paper and helpful suggestions.

random elements generate a solvable group is less than 19/30 (CFSG was used in this proof). Results of this type may be used in some Monte Carlo type algorithms for determining properties of finite groups.

There is an extensive literature about probabilistic questions in finite group theory. See, for example, [3] and [20] for some results and additional references.

Notation: Let X be a finite group. When X acts as a group of automorphisms of another finite group Y, we denote the number of X-orbits on Y by $k_X(Y)$. We let $\pi(X)$ denote the set of prime divisors of X.

We recall that a component of X is a subnormal quasi-simple subgroup of X. We denote the central product of all components of X by $E(X)$. The generalized Fitting subgroup of X, which is the product $F(X)E(X)$, is denoted by $F^*(X)$.

A section of a finite group X is a group of the form Y/Z, where $Z \lhd Y$ and Y is a subgroup of X. We denote the hypercenter of X (that is, the terminal member of the upper central series of X) by $Z_\infty(X)$, the terminal member of the derived series of X by $X^{(\infty)}$, and the solvable radical of X (that is, the (unique) maximal solvable normal subgroup of X) by $\mathrm{sol}(X)$. We let $F_i(X)$ denote the i-th term of the Fitting series of X (so that $F(X/F_i(X)) = F_{i+1}(X)/F_i(X)$ and $F_0(X) = 1_X$). We let $\Phi(X)$ denote the Frattini subgroup of X. For convenience, we will occasionally use $|Y : X|$ to denote $[X : Y]^{-1}$ when Y is a subgroup of a group X.

For a family of finite groups $\mathcal{X}$, we will interpret the statement $\mathrm{cp}(X) \to 0$ as $|X| \to \infty$ for $X \in \mathcal{X}$ to mean that for all $\varepsilon > 0$, there is an integer $N \in \mathbb{N}$ such that whenever $X \in \mathcal{X}$ with $|X| > N$, we have $\mathrm{cp}(X) < \varepsilon$. If the family is omitted, it is assumed to be the family of all finite groups. As usual, when π is a collection of primes, the complementary set of primes is denoted by π'.

We first record some refinements of results of Gallagher [7] and Nagao [16].

Lemma 1. *Let G be a finite group.*

(i) *For every proper subgroup H of G, we have*

$$[G : H]^{-1}k(H) < k(G) \leq [G : H]k(H).$$

Moreover, if $k(G) = [G : H]k(H)$, then H contains $[G, G]$ and every L-conjugacy class is G-stable for every subgroup L with $H \leq L \leq G$. In that case, setting $\pi = \pi(H)$, G is a direct product of a π-group with a (possibly trivial) Abelian π'-group.

If, conversely, H contains $[G, G]$ and every L-conjugacy class is G-stable for every subgroup L with $H \leq L \leq G$, then we have $k(G) = [G : H]k(H)$.

(ii) *For every normal subgroup N of G, $k(G) \leq k(N)k(G/N)$.*

(iii) *If N is a normal subgroup of G and c is an integer with the property that $k(H) \leq c$ for every subgroup H of G/N, then $k(G) \leq ck_G(N)$.*

Proof. (i) The proof of this part is given in [7], apart from the explicit statements about the strictness of the inequalities and the consequences of equality. Suppose that equality is attained in the rightmost inequality. Then whenever L is a subgroup of G containing H, we have $k(L) \leq [L : H]k(H)$ and $k(G) \leq [G : L]k(L)$, so both of these inequalities become equalities. The proof of the inequality in [7] then shows that equality implies that whenever μ is an irreducible character of H, the induced character $\mathrm{Ind}_H^G(\mu)$ is a direct sum of $[G : H]$ distinct irreducible characters of G. In particular, when μ is the trivial character of H, we see that $\mathrm{Ind}_H^G(\mu)$ is a sum of $[G : H]$ linear characters of G. Clearly the normal closure N of H is contained in the kernel of each of these characters. Thus, $[G : N] \geq [G : H]$ and so $H = N$ is normal in G. Moreover all irreducible characters of G/H are linear, so that G/H is Abelian. Returning to a general irreducible character, μ, of H, we note, in particular, that μ extends (in $[G : H]$ ways) to an irreducible character of G. Hence μ is G-stable.

The same argument applies to any subgroup L with $H \leq L \leq G$, so every irreducible character of L is G-stable for any such L. The statement about G-stability of L-conjugacy classes follows by Brauer's permutation lemma.

Conversely, we claim that if $[G, G] \leq H$ and every irreducible character of L is H-stable whenever $H \leq L \leq G$, then $k(G) = [G : H]k(H)$. We prove this by induction on $[G : H]$, so we may suppose that H is proper. Let M be a maximal subgroup of G containing H. Then $[G : M] = q$ for some prime q and $k(M) = [M : H]k(H)$ by induction. By hypothesis, every irreducible character of M is G-stable, so, since G/M is cyclic, every irreducible character of M extends in q distinct ways to an irreducible character of G. Thus $k(G) = qk(M) = [G : H]k(H)$, as required to complete the proof.

Let us now return to the case $k(G) = [G : H]k(H)$. Then, setting $\pi = \pi(H)$, and recalling that $H \lhd G$ with $[G, G] \leq H$, we have $G = LA$, where $L = O_\pi(G)$ and A is an Abelian Hall π'-subgroup of G. As above, we have $k(G) = [G : L]k(L)$, so we may suppose that $H = O_\pi(G)$ to establish the last claim of i). Now A is an Abelian group of coprime automorphisms of H and A fixes each conjugacy class of H. It is well-known that A centralizes H under these circumstances, but we outline the argument (the first part of which is due to G. Glauberman). For any element x of H, we have $G = HC_G(x)$, since A-stabilizes the conjugacy class of x. Thus $C_G(x)$ contains a conjugate of A (by the Schur-Zassenhaus theorem), and A centralizes an H-conjugate of x. Hence $C_H(A)$ meets every conjugacy class of H. In a finite group, no proper subgroup meets every conjugacy class, so $H = C_H(A)$.

The proof of the inequality $k(H) \leq [G : H]k(G)$ in [7] relies on the fact that whenever χ is an irreducible character of G, the restricted character $\mathrm{Res}^G_H(\chi)$ is a sum of at most $[G : H]$ irreducible characters of H. However, when H is proper, the trivial character of G shows that equality can never be attained.

(ii) is proved in [16].

(iii) is Remark A2$'$ in [13]. □

We note that the conditions in i) are necessary, but not generally sufficient for the rightmost inequality to become equality (consider, for example, the case when G is extra-special of order p^3 for some prime p, and $H = Z(G)$).

Next, an omnibus Lemma.

Lemma 2. *Let G be a finite group.*

(i) *For every proper subgroup, H, of G, we have*

$$[G : H]^{-2}\mathrm{cp}(H) < \mathrm{cp}(G) \leq \mathrm{cp}(H).$$

Hence $\mathrm{cp}(G) \geq [G : H]^{-2}$ whenever $H \leq G$ is Abelian. Furthermore, $\mathrm{cp}(H) = \mathrm{cp}(G)$ (for an arbitrary subgroup H) if and only if $[G, G] \leq H$ and all L-conjugacy classes are G-stable for every subgroup L with $H \leq L \leq G$. In that case, setting $\pi = \pi(H)$, we have $G = O_\pi(G) \times O_{\pi'}(G)$.

(ii) *Whenever* $N \lhd G$, *we have*

$$\mathrm{cp}(G) \leq \mathrm{cp}(N)\mathrm{cp}(G/N).$$

In particular, we always have $\mathrm{cp}(G) \leq \mathrm{cp}(G/N)$.

(iii) *For every section,* X, *of* G, *we have*

$$\mathrm{cp}(G) \leq \mathrm{cp}(X).$$

(iv) *We have*

$$\mathrm{cp}(G) \leq \prod_S \mathrm{cp}(S),$$

where S *runs through the non-Abelian composition factors of* G, *including repetitions.*

(v) *If* H *is another finite group, we have* $\mathrm{cp}(G \times H) = \mathrm{cp}(G)\mathrm{cp}(H)$.

(vi) *If* G *is non-Abelian, we have*

$$|[G,G]|^{-1} < \mathrm{cp}(G) \leq d^{-2} + (1 - d^{-2})|[G,G]|^{-1},$$

where d *is the smallest degree of a non-linear complex irreducible character of* G. *Furthermore, the rightmost inequality becomes equality if and only if all non-linear irreducible characters of* G *have degree* d, *in which case* $[G : G']$ *is divisible by* d.

(vii) *If* G *is non-Abelian, we have*

$$\mathrm{cp}(G) < \frac{3}{2}[G : C_G(x)]^{-1}$$

for some $x \in G \setminus Z(G)$, *and if* $Z(G) = 1$, *we have*

$$\mathrm{cp}(G) \leq [G : C_G(x)]^{-1}$$

for some $x \in G^{\#}$. *In this last case, if* G *is a direct product of several groups, the element* x *may be chosen to have non-trivial projection in each direct factor.*

(viii) *If* G *is a non-Abelian* p*-group for some prime* p, *we have*

$$\mathrm{cp}(G) < \frac{1}{p} + [G : Z(G)]^{-1} \leq \frac{1}{p} + \frac{1}{p^2}.$$

(ix) *If* G *is nilpotent with a non-Abelian Sylow* r*-subgroup for some prime* r, *then we have* $\mathrm{cp}(G) < \frac{1}{r}$, *except, perhaps, when* $|[G,G]| = r$ *(in which case the prime* r *is unique).*

(x) *If* p *is a prime such that* G *is not* p*-closed, then* $\mathrm{cp}(G) \leq \frac{1}{p}$.

(xi) *If* p *is a prime divisor of* $|G|$ *and* P *is a Sylow* p*-subgroup of* G, *then there is* $x \in G$ *of order* p *such that*

$$\mathrm{cp}(G) < |P|^{-2} + \frac{|Z(P)||C_G(x)|}{|G|(|Z(P)| - 1)}.$$

(xii) *If* G *is non-Abelian with* $\mathrm{cp}(G) > \frac{11}{27}$, *then the derived length of* G *is* 2 *and either* G *is nilpotent with* $|[G,G]| \in \{2,4\}$, *or else* $G/Z(G) \cong S_3$. *In particular,* $|G|$ *is even.*

(xiii) *If* π *is a set of primes such that* G *has an Abelian Sylow* p*-subgroup for each prime* $p \in \pi$ *and* Z *is a central* π*-subgroup of* G, *then we have* $\mathrm{cp}(G) = \mathrm{cp}(G/Z)$.

Proof. Parts (i) and (ii) follow immediately from Lemma 1.
(iii) Follows on combining (i) and (ii).
(iv) Follows from repeated applications of (ii).
(v) This is clear since $k(G \times H) = k(G)k(H)$.
(vi) Since G is non-Abelian, we clearly have

$$[G : G'] < k(G) \leq [G : G'] + d^{-2}(|G| - [G : G']).$$

The rightmost inequality is an equality if and only if all non-linear irreducible characters of G have degree d, so part vi) follows.
(vii) Let c be the maximum order of $C_G(x)$ for $x \in G \backslash Z(G)$. Set $Z = Z(G)$ and $k = k(G)$. From the class equation for G, we have $|G| \geq |Z| + (k - |Z|)\frac{|G|}{c}$, from which it readily follows that $k \leq c + |Z| - 1$. The inequalities involving $\mathrm{cp}(G)$ follow easily from this. For the last statement, if $G = G_1 \times G_2 \times \ldots \times G_t$ and $Z(G) = 1$, then for each i, we may choose $x_i \in G_i^{\#}$ with $k(G_i) \leq |C_{G_i}(x_i)|$, and, setting $x = x_1 x_2 \ldots x_t$, we have $k(G) \leq |C_G(x)|$.
(viii) We have $k(G) \leq |C_G(x)| + |Z(G)| - 1$ for some non-central element x of G. Since $|C_G(x)| \leq \frac{|G|}{p}$, the result is clear.
(ix) If G is nilpotent, with a non-Abelian Sylow q-subgroup and a non-Abelian Sylow r-subgroup, where $q < r$ are primes, then

$$\mathrm{cp}(G) \leq \mathrm{cp}(O_q(G))\mathrm{cp}(O_r(G)) < (\frac{1}{q} + \frac{1}{q^2})(\frac{1}{r} + \frac{1}{r^2}) \leq \frac{1}{r},$$

since $q \geq 2$ and $r \geq 3$. Hence we may suppose that there is a unique prime r such that G has a non-Abelian Sylow r-subgroup. If $|[G, G]| \neq r$, then part (vi) above yields that $\mathrm{cp}(G) < \frac{2}{r^2} \leq \frac{1}{r}$ (since r divides d).
(x) By the earlier parts of this Lemma, we may suppose that every proper section of G is p-closed. Then certainly $G = O^{p'}(G)$ and $O_p(G) = 1$.

Suppose that $E(G) = 1$. Then $C_G(F(G)) \leq F(G)$. In that case, for an element x of order p in G, we see that $G = F(G)\langle x \rangle$. The hypotheses on G then imply that G is a Frobenius group with kernel $F(G)$, which is a minimal normal subgroup. Then

$$\mathrm{cp}(G) = \frac{p^2 + |F(G)| - 1}{p^2|F(G)|} \leq \frac{1}{p},$$

since $|F(G)| \geq p + 1$.

Hence G has a component, L say, and the hypotheses on G force $G = L$ and L simple. In particular, by [3], we have $\mathrm{cp}(G) \leq \frac{1}{12}$ so we may suppose that $p \geq 13$. Also, $|G| \geq 2p(p+1)$, since (for a Sylow p-subgroup, P of G) we have $[G : N_G(P)] \geq p + 1$ and $|N_G(P)| \geq 2p$ (the second inequality following from (for example), Burnside's normal p-complement theorem).

Let d be the smallest degree of a non-trivial complex irreducible character of G. Then $d \geq \frac{p-1}{2}$ by [5]. Now part vi) yields

$$\mathrm{cp}(G) < \frac{4}{(p-1)^2} + \frac{1}{|G|},$$

so certainly

$$\mathrm{cp}(G) < \frac{4}{(p-1)^2} + \frac{1}{2p(p+1)} < \frac{1}{p}$$

since $p > 5$ under current assumptions.

(xi) By Corollary 2 of [19], there is an element $x \in G$ of order p such that the number of irreducible characters of G which do not lie in p-blocks of defect 0 is less than $\frac{|C_G(x)||Z(P)|}{|Z(P)|-1}$. Since the unique irreducible character in any p-block of defect zero has degree divisible by $|P|$, we certainly have

$$k(G) < \frac{|C_G(x)||Z(P)|}{|Z(P)|-1} + \frac{|G|}{|P|^2},$$

so the claimed result follows.
(xii) If $|G|$ is odd, then part vi) yields the contradiction $\mathrm{cp}(G) \leq \frac{11}{27}$, since $|[G,G]| \geq 3$ and $d \geq 3$. Hence $|G|$ is even and every subgroup of G of odd order is Abelian, using part iii). By part x), G has a normal 2-complement, H say. Part vi) yields that $|[G,G]| < \frac{81}{17} < 5$ since $\mathrm{cp}(G) > \frac{11}{27}$ and $d \geq 2$. If $|[G,G]| \in \{2,4\}$, then G is nilpotent and we are done. If $|[G,G]| = 3$, then G has an Abelian Sylow 2-subgroup, S say. Now $H = [H,S] \times (H \cap Z(G))$ and $|[H,S]| = 3$, so that $[S : S \cap Z(G)] = 2$, and $G/Z(G) \cong S_3$.
(xiii) It suffices to prove that $k(G) = |Z|k(G/Z)$. By elementary transfer, we have $Z \cap G' \cap P = 1$ whenever $P \in \mathrm{Syl}_p(G)$ and $p \in \pi$. Hence $Z \cap G' = 1$, so Z certainly contains no non-identity commutator of G. By (for example), Lemma 4 of [18], we do have $k(G) = |Z|k(G/Z)$, as required.

□

Concerning part (vii) above, we remark that the groups $\mathrm{SL}(2, 2^n)$ show that $k(G) = \max_{x \in G^\#} |C_G(x)|$ for infinitely many non-Abelian simple groups G, since this maximum order is $2^n + 1 = k(G)$ in these cases.

The (coprime) $k(GV)$ problem is to show that whenever p is a prime and G is a finite p'-group acting faithfully on the $GF(p)$-module V, then $k(GV) \leq |V|$. This has recently been solved in full generality in [8].

Our next result uses the solution of a special case of the coprime $k(GV)$-problem (for nilpotent G) to yield a rather strong bound for $\mathrm{cp}(G)$ for solvable G.

Lemma 3. *Let G be a finite solvable group with Fitting subgroup F. Set $F_i = F_i(G)$. Assume that $G = F_{2r} = F_{2r+1}$. Then we have:*

(i) $\mathrm{cp}(F_2) \leq [F_2 : F_1]^{-1} = |F_1 : F_2|$;
(ii) $\mathrm{cp}(G) \leq \prod_{i=1}^{r} |F_{2i-1} : F_{2i}|$; *and*
(iii) $\mathrm{cp}(G) \leq \mathrm{cp}(F) \prod_{i=1}^{r} |F_{2i} : F_{2i+1}|$.

Proof. By induction and repeated use of part (ii) of Lemma 2, we see that (i) implies (ii). By Lemma 2, $\mathrm{cp}(G) \leq \mathrm{cp}(F)\mathrm{cp}(G/F)$. Now (ii) applied to G/F implies (iii).

So we only need prove (i), i.e. we need to prove that $k(G) \leq |F(G)|$ when $G/F(G)$ is nilpotent. We prove this by induction, so we assume, as we may, that $k(N) \leq |F(N)|$ whenever N is a proper section of G. Since $F(G/\Phi(G)) = F(G)/\Phi(G)$ and certainly $k(\Phi(G)) \leq |\Phi(G)|$, part ii) of Lemma 2 allows us to suppose that $\Phi(G) = 1$, and we do so.

Let M be a minimal normal subgroup of G, which is a p-group for some prime p. Notice that $M \leq Z(F)$. If $M = F$, then $O_p(G/M) = 1$, while G/M is nilpotent by assumption, so that G/M is a p'-group. Hence $k(G) \leq |M|$, as required, using the solution of the $k(HV)$-problem in the case that H is nilpotent, already proved in [12].

Hence we may suppose that $M \neq F$. Since $\Phi(G) = 1$, $G = ML$ for some maximal subgroup L of G and $M \cap L = 1$ as M is minimal normal. Set $C = C_L(M) \lhd G$.

Then $F = MF(C)$. Now $k(C) \leq |F(C)|$ by the inductive assumption. We claim that $k(G/C) \leq |M|$. Now $C_G(M) = MC$ and G/C acts irreducibly on M, so viewing M as a subgroup of G/C, we see that $F(G/C) = M$ is a self centralizing minimal normal subgroup of G/C. Moreover, $G/CM = G/C_G(M)$ is nilpotent, so by [12] again, $k(G/C) \leq |M|$ as required. □

The first part of the previous Lemma shows that if G is solvable of Fitting height 2, then $k(G) \leq |F(G))|$ (and indeed that this is equivalent to the coprime $k(GV)$ result for G nilpotent). This inequality does not hold in general for solvable groups. For example, when $G = VH$ with V elementary Abelian of order 9 and $H \cong GL(2,3)$ acting naturally on V, then $k(G) = 11$ and $|F(G)| = 9$. An even smaller counterexample is S_4, which may be viewed as the semi-direct product of $GL(2,2)$ and its natural module ($k(S_4) = 5$ and $|F(S_4)| = 4$).

The previous result can be used to provide a very good bound for $\mathrm{cp}(G)$ in the solvable case:

Theorem 4. *Let G be a finite solvable group with Fitting subgroup F. Then*

(i) $k(G) \leq (k(F)|G|)^{1/2} \leq (|F||G|)^{1/2} = |F|[G:F]^{1/2}$*; and*

(ii) $\mathrm{cp}(G) \leq \mathrm{cp}(F)^{1/2}[G:F]^{-1/2}$*; and*

(iii) $\mathrm{cp}(G) \to 0$ *as* $[G:F(G)] \to \infty$.

Proof. Note that (ii) is equivalent to the leftmost inequality of i), and ii) certainly implies iii). Parts (ii) and (iii) of the previous lemma, taken together, yield:

$$\mathrm{cp}(G)^2 \leq \mathrm{cp}(F)|F|/|G|,$$

and part ii) of this Theorem follows immediately □

Note that (i) of the previous result gives a weak variation on the $k(GV)$ question. Theorem 7 below will give more in this direction. First, we need to rectify an error in the paper [17] of the second author. In that paper, a function $f : \mathbb{N} \to \mathbb{N}$ was defined with the property that $f(1) = 1, f(ab) = f(a)f(b)$ whenever a and b are relatively prime. It is asserted there that whenever p^m is a prime power, $\frac{f(p^m)}{p^m}$ is the maximal order of a p-subgroup of a p-solvable subgroup G of $GL(m,p)$ with $O_p(G) = 1$. However, the value of $f(2^m)$ given in [17] is larger than the true value, due to an oversight about the field of realizability of the representations in question. In fact, the value of $\frac{f(2^m)}{2^m}$ given in [17] is the maximal possible order of a Sylow 2-subgroup of a finite solvable subgroup G of $GL(m,\mathbb{C})$ with $O_2(G) = 1$. This means that the statements that $k(G) \leq f(|F(G)|)$ and that a nilpotent injector, I, of G has order dividing $f(|F(G)|)$ are correct, but could be improved. However, the assertion that for every positive integer n, there is a finite solvable group H_n with $|F(H_n)| = n$ and with a nilpotent injector of order $f(n)$ is incorrect for even n with the function f given there, though the statement becomes correct with f amended as in the discussion below.

We recall from [17] that when p is an odd prime and m is a positive integer, we have

$$\frac{f(p^m)}{p^m} = (m!)_p,$$

except when p is a Fermat prime, in which case,

$$\frac{f(p^m)}{p^m} = [(p\lfloor \frac{m}{p-1} \rfloor)!]_p.$$

We amend f by defining $f(2^m) = 2^m(m!)_2$ for each positive integer m.

We remind the reader that for all primes p and positive integers n,

$$\log_p((n!)_p) = \frac{n - \sigma_p(n)}{p-1},$$

where $\sigma_p(n)$ is the sum of the digits in the p-adic expansion of n.

The following result is proved by Winter for p odd (see [11]) and another proof for all p was given by Wolf [21]. Wolf's proof used modular representation theory while Winter used the Fong-Swan theorem to lift to characteristic 0. Wolf's proof for p odd was for solvable groups. We point out a result of the two present authors that a coprime group of automorphisms of a finite group G acts faithfully on some nilpotent subgroup of G (this was used in [15] and the proof of the authors is given there). This easily reduces the general p-solvable case to that of solvable groups (although this reduction does require CFSG).

We note that it is easy to construct examples to show that the bounds below can be attained for every prime p and positive integer m.

Lemma 5. *Let p be a prime, m be a positive integer. Then the maximal order of a p-subgroup of a p-solvable subgroup H of $GL(m,p)$ with $O_p(H) = 1$ is $[n_p(m)!]_p$, where $n_p(m) = m$ if p is not a Fermat prime and $n_p(m) = p\lfloor \frac{m}{p-1} \rfloor$ if p is a Fermat prime.*

Combining this result with the solution of the coprime $k(GV)$ result leads to the following:

Theorem 6. *Let m be a positive integer, and let G be a p-solvable subgroup of $GL(V) \cong GL(m,p)$ with $O_p(G) = 1$. Then $k(G) < k(VG) \leq |V|^2/p$.*

Proof. Let P be a Sylow p-subgroup of G and H a Hall p'-subgroup of G. By the solution of the coprime $k(GV)$ problem, $k(VH) \leq |V|$. By part (i) of Lemma 1, $k(VG) \leq |V||P|$ and by the previous lemma, $|P| \leq |V|/p$. Clearly $k(G) < k(VG)$, since V is non-trivial. □

In fact, the exponent 2 can be made much smaller and it should be possible to remove the p-solvable hypothesis. In the next result, δ_{ab} is the usual Kronecker delta. We remind the reader that a nilpotent injector of a finite solvable group G is a maximal nilpotent subgroup of G containing $F(G)$.

Theorem 7. *Let G be a non-trivial finite solvable group and let I be a nilpotent injector of G. Let $\pi = \pi(F(G))$, $r = |\pi|$, let s be the number of prime factors of $|F(G)|$ (counting multiplicities) and let $|O_3(G)| = 3^t$. Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined prior to the previous lemma. Then*

$$\max\{k(G), |I|\} \leq f(|F(G)|) \leq 3^{\frac{3t-2+(2\delta_{t0}-\delta_{t1})}{4}} 2^{s-t-r+(1-\delta_{t0})}|F(G)| \leq \frac{|F(G)|^2}{\prod_{\{q\in\pi\}} q}.$$

Proof. For the (amended) function $f : \mathbb{N} \to \mathbb{N}$ defined as above, arguing as in [17], we obtain

$$k(G) \leq f(|F(G)|) = \prod_p f(|O_p(G)|)$$

(we have made use of the fact that the (coprime) $k(GV)$-problem is now known to have a positive answer for all primes p and for arbitrary G, though we only need the case that G is solvable here). We also have $|I| \leq f(|F(G)|)$.

When $p = 2$, we have $m!_2 \leq 2^{m-1}$, while if p is an odd prime which is not Fermat, we have $m!_p \leq p^{\frac{m-1}{p-1}} < 2^{m-1}$. If p is a Fermat prime, we obtain

$$\frac{f(p^m)}{p^m} \leq p^{\frac{m}{(p-1)} + \frac{\lfloor \frac{m}{p-1} \rfloor - 1}{p-1}} < p^{\frac{mp}{(p-1)^2}}.$$

This information suffices to prove the Theorem, after noting that $x^{\frac{x}{(x-1)^2}}$ decreases monotonically on (e, ∞), so that if $p > 3$ is a Fermat prime, we have

$$p^{\frac{mp}{(p-1)^2}} \leq 5^{\frac{5m}{16}} < 2^{\frac{3m}{4}}.$$

If this quantity is greater than 2^{m-1}, we must have $m < 4$. However, in that case, we have $\lfloor \frac{m}{p-1} \rfloor = 0$ and $f(p^m) = p^m$. □

A "correct" upper bound for $k(G)$ for solvable G should probably be something like $k(G) \leq |F(G)|^{1.2}$.

We next show that $\mathrm{cp}(G) \to 0$ as $[G : F(G)] \to \infty$ for all finite groups. As we will illustrate, the explicit bound given can be improved considerably using CFSG, but we first give an elementary proof.

Theorem 8. *Let G be a non-solvable finite group.*

(i) *We have* $\mathrm{cp}(G) < \log_2([G : \mathrm{sol}(G)])^{-1/3}$. *In particular,* $\mathrm{cp}(G) \to 0$ *as* $[G : \mathrm{sol}(G)] \to \infty$.

(ii) $\mathrm{cp}(G) \to 0$ *as* $[G : F(G)] \to \infty$.

Proof. i) By part (ii) of Lemma 2, we may, and do, suppose that $\mathrm{sol}(G) = 1$. Set $I = F^*(G)$. Then I is a direct product of non-Abelian simple groups. Now G is isomorphic to a subgroup of $\mathrm{Aut}(I)$ by standard properties of the generalized Fitting subgroup.

We note that a non-Abelian finite simple group H can be generated by $\log_p(|H|)$ or fewer elements, where p is the largest prime divisor of $|H|$. For let $x \in H$ be an element of order p. We inductively define a sequence of proper subgroups X_d of H such that X_d can be generated by d conjugates of x for each d and $|X_d| \geq p^d$. Since H is simple, H can't embed into the symmetric group S_n for any $n < p$, so we must have $|X_d| \leq \frac{|H|}{p}$ and $d \leq \log_p(|H|) - 1$ for each d. Once X_d has been constructed, and is proper, we choose a conjugate x_{d+1} of x which lies outside X_d (this is possible as H is generated by conjugates of x) and set $X_{d+1} = \langle X_d, x_{d+1} \rangle$. If this is proper, we continue the process, and we terminate the sequence at X_d otherwise. We notice that $|X_{d+1}| \geq p|X_d|$ as x_{d+1} has prime order p. Letting X_m be a maximal member of this sequence of proper subgroups, we see that $m \leq \log_p(|H|) - 1$, and that H can be generated by $m+1$ or fewer elements. We note also that $p \geq 5$ by Burnside's $p^a q^b$-theorem.

Hence I can certainly be generated by $\log_5(|I|)$ or fewer elements, and each of these generators can have at most $|I|$ images under an automorphism of I, so we obtain $|G| < |I|^{\log_5(|I|)}$ and

$$\log_2(|G|) < \log_2(|I|) \log_5(|I|).$$

We recall that $\mathrm{cp}(G) \leq \mathrm{cp}(I)$, so that $\mathrm{cp}(G)^{-1} \geq \mathrm{cp}(I)^{-1}$.

By part (vii) of Lemma 2, there is an element $x \in I$ with $k(I) \leq |C_I(x)|$ such that x has non-trivial projection onto every simple direct factor of I. Hence $C_I(x)$

is core-free in I. Setting $n = \lfloor \mathrm{cp}(I)^{-1} \rfloor$, we certainly have $|I| \le [I : C_I(x)]! \le n^n$. Thus

$$\log_2(|G|) < n^2 \log_2(n) \log_5(n) \le (\mathrm{cp}(G)^{-1})^2 \log_2(\mathrm{cp}(G)^{-1}) \log_5(\mathrm{cp}(G)^{-1}).$$

To prove part i), it remains to show that

$$\log_2(\mathrm{cp}(G)^{-1}) \log_5(\mathrm{cp}(G)^{-1}) \le \mathrm{cp}(G)^{-1}.$$

Now $\log(x)^2/x$ has a unique maximum on $(1, \infty)$ at $x = e^2 < 8$. Since

$$\log_2(e^2) \log_5(e^2) < e^2,$$

we deduce that $\log_2(x) \log_5(x) < x$ for all $x \ge 1$, and we have the desired inequality.

We note that ii) follows by i) together with part (iii) of Theorem 4 since

$$\mathrm{cp}(G) \le \min(\mathrm{cp}(G/\mathrm{sol}(G)), \mathrm{cp}(\mathrm{sol}(G))).$$

□

The previous result says that $k(G)/|G| < \log_2(|G|)^{-1/3}$ when $\mathrm{sol}(G) = 1$. The earlier remark also illustrates that the groups $\mathrm{SL}(2, 2^n)$ provide infinitely many non-isomorphic examples of finite groups G with $\mathrm{sol}(G) = 1$ and $k(G) > |G|^{1/3}$. If we take G to be a product of sufficiently many copies of S_5, we may produce an arbitrarily large finite group G with $\mathrm{sol}(G) = 1$ and $k(G) > |G|^{0.4}$.

In the next theorem, we use CFSG to show that $k(G) < \sqrt{|G|}$ for G with $\mathrm{sol}(G) = 1$.

Theorem 9. *Let G be a finite group. Then $\mathrm{cp}(G) \le [G : \mathrm{sol}(G)]^{-1/2}$ with equality if and only if G is Abelian.*

Proof. As in the previous proof, we may assume that $\mathrm{sol}(G) = 1$. Set $I = F^*(G)$ and suppose that I is a direct product of t simple groups. Let J be the kernel of the permutation action of G on the simple direct factors of I.

We first note that by [6] (using CFSG), it follows that $k(H) < |H|^{0.41}$ for H almost simple (and the example $H = S_5$ shows that this cannot be improved much). We claim that the same bound holds for J. We proceed by induction on the number of components contained in J. If there is one such component, then J is almost simple. Otherwise, let L be a simple component of J and set $C = C_J(L)$. Then G/C is almost simple (with socle L) and $F^*(C) = E(C)$ is a direct product of fewer components than $F^*(J)$. Since $k(J) \le k(C)k(J/C)$, the claim follows.

By a result of Maróti [14], it follows that $k(G/J) < 3^{t/2} < |J|^{0.14}$ (the latter inequality follows since $|J| \ge 60^t$). Thus $k(G) < |J|^{0.55}$ and this is less than $|G|^{1/2}$ when $|G/J| > |J|^{0.1}$.

If $|G/J| \le |J|^{0.1}$, then $|J|^{0.59} > |G|^{0.5}$. Since $\mathrm{cp}(G) \le \mathrm{cp}(J)$, we see that $k(G) < |J|^{0.41}|G/J| \le |G|/|J|^{0.59} < |G|^{0.5}$. □

We can combine the previous results to obtain:

Theorem 10. *Let G be a finite group with Fitting subgroup F. Then:*

(i) $k(G) \le k(F)^{1/2}|G|^{1/2} \le (|F||G|)^{1/2}$; *and*
(ii) $\mathrm{cp}(G) \le \mathrm{cp}(F)^{1/2}[G : F]^{-1/2} \le [G : F]^{-1/2}$.

Proof. By part (ii) of Lemma 2, $\mathrm{cp}(G) \le \mathrm{cp}(G/\mathrm{sol}(G))\mathrm{cp}(\mathrm{sol}(G))$. By part (ii) of Theorem 4 and Theorem 9, $\mathrm{cp}(\mathrm{sol}(G)) \le k(F)^{1/2}|\mathrm{sol}(G)|^{-0.5}$ and $\mathrm{cp}(G/\mathrm{sol}(G)) \le [G : \mathrm{sol}(G)]^{-0.5}$. This proves (ii). Multiplying both sides of (ii) by $|G|$ yields (i). □

This gives a much better result on how quickly $\mathrm{cp}(G) \to 0$ as $[G : F(G)] \to \infty$ than that implied by Theorem 8.

The next result further highlights the distinguished role of the alternating group A_5.

Theorem 11. *Let G be a finite group such that $\mathrm{cp}(G) > \frac{3}{40} = 0.075$. Then either G is solvable, or else $G \cong A_5 \times T$ for some Abelian group T, in which case $\mathrm{cp}(G) = \frac{1}{12}$.*

Proof. Suppose that the Theorem is false, and let G be a minimal counterexample. We note that $\mathrm{cp}(SL(2,5)) = \frac{3}{40}$ and $\mathrm{cp}(S_5) = \frac{7}{120}$, so neither $SL(2,5)$ nor S_5 can occur as a section of G by part (iii) of Lemma 2.

Since G is not solvable, G has a non-Abelian composition factor S with $\mathrm{cp}(S) > \frac{3}{40}$ by part (iv) of Lemma 2. By part (vi) of Lemma 2, we have

$$\mathrm{cp}(S) \leq d^{-2} + |S|^{-1}(1 - d^{-2}),$$

where d is the smallest degree of a complex irreducible character of S. Suppose that $d > 3$. Then we obtain $|S| < 75$. However, $S \not\cong A_5$ since we are assuming that $d > 3$, while A_5 has an irreducible character of degree 3.

Hence $d \leq 3$. Since S is simple, we have $d > 2$. Hence $S \cong A_5$ or $PSL(2,7)$ from the classification of the finite irreducible subgroups of $GL(3, \mathbb{C})$. Since $\mathrm{cp}(PSL(2,7)) = \frac{1}{28}$, we have $S \cong A_5$.

Suppose that G has a component, L say. Then $L \cong A_5$ (since $L \cong SL(2,5)$ has already been excluded) and L is unique (otherwise $\mathrm{cp}(G) \leq \mathrm{cp}(E(G)) \leq \frac{1}{144}$). If there is some $x \in G \backslash LC_G(L)$, then $L\langle x \rangle$ has S_5 as a homomorphic image, a contradiction. Thus $G = L \times C_G(L)$. By the assumptions on G, the group $C_G(L)$ is Abelian, otherwise $\mathrm{cp}(G) \leq \frac{5}{8} \cdot \frac{1}{12} < \frac{3}{40}$. Thus $F^*(G) = F(G)$.

Let M be a maximal normal subgroup of G. Then M is solvable, since otherwise $E(M) \neq 1$ by the minimality of G, and then $E(G) \neq 1$. Let N be a minimal normal subgroup of G. Then $E(G/N) \cong A_5$ by the minimality of G, since G/N is not solvable. It follows that $G/N \cong A_5$, since every proper normal subgroup of G is solvable.

Now N is an elementary Abelian p-group for some prime p, and N is an irreducible $GF(p)G/N$-module. If N is trivial, then the fact that G has no component is contradicted. Hence $|N| \geq 16$. Now every subgroup of G/N has 5 or fewer conjugacy classes, so by part (iii) of Lemma 1, we have $k(G) \leq 5k_G(N)$. Now $k_G(N) \leq \frac{|N|+4}{5}$, since every orbit of G/N on non-identity elements of N has length at least 5. Hence

$$\mathrm{cp}(G) \leq \frac{|N| + 4}{60|N|} \leq \frac{1}{48},$$

contrary to the hypotheses on G. □

It is possible to avoid the classification of three dimensional linear groups. As above, we may reduce to the case that G is simple. By Lemma 2, there is $x \in G^{\#}$ with $[G : C_G(x)] < 14$. Moreover, by a result of Burnside, $[G : C_G(x)]$ is not a prime power, so $[G : C_G(x)] \in \{6, 10, 12\}$. Furthermore, either G embeds into A_6 or else $C_G(x)$ is a maximal subgroup of G. By inspection (or by elementary arguments), we see that only $G = A_5$ can occur.

Theorem 8 tells us that $\mathrm{cp}(G) \to 0$ as $[G : F(G)]$ tends to infinity. On the other hand, if we have $[G : F(G)] \leq b$ for an explicit bound b, then part (i) of Lemma 2 tells us that $b^{-2}\mathrm{cp}(F(G)) \leq \mathrm{cp}(G) \leq \mathrm{cp}(F(G))$. This motivates us to concentrate attention on $\mathrm{cp}(G)$ when G is solvable or nilpotent.

We next demonstrate that when the finite group G is solvable or nilpotent, then $\mathrm{cp}(G) \to 0$ as the derived length of G grows. The estimate in part (i) of Theorem 12 is rather crude, but sufficient for our immediate purpose. In fact, careful examination of the proof shows that equality is never attained in part (i) of the Theorem.

Theorem 12.

i) *Let G be a finite solvable group of derived length $d \geq 4$. Then*

$$\mathrm{cp}(G) \leq \frac{4d-7}{2^{d+1}}.$$

ii) *Let p be a prime and let G be a finite p-group of derived length $d \geq 2$. Then*

$$\mathrm{cp}(G) \leq \frac{p^d + p^{d-1} - 1}{p^{2d-1}}.$$

Proof. i) We first establish the case $d = 4$. It is easy to check that no group of order less than 24 has derived length greater than 2. Let H be a finite solvable group of derived length 4. Then $|[H,H]| \geq 24$, so part (vi) of Lemma 2 yields that

$$\mathrm{cp}(H) \leq \frac{1}{4} + \frac{3}{4|[H,H]|} \leq \frac{9}{32},$$

which establishes the desired inequality for $d = 4$. Suppose then that G has derived length $d > 4$, and that the result has been established for $d - 1$.

By part (ii) of Lemma 2, we may replace G by any homomorphic image of the same derived length. Hence we may suppose that no proper homomorphic image of G has derived length d. In that case, it follows that G has a unique minimal normal subgroup, M say, for if G has two distinct minimal normal subgroups M_1 and M_2, then G embeds in the direct product $G/M_1 \times G/M_2$ and hence has derived length less than d, a contradiction. Also, G/M has derived length $d - 1$.

If χ is a complex irreducible character of G which does not contain M in its kernel, then χ must be faithful by the uniqueness of M. Furthermore, [2] certainly gives $d \leq 2 + 2\log_2(\chi(1))$. Hence $\chi(1)^2 \geq 2^{d-2}$. It follows that

$$k(G) \leq k(G/M) + \frac{|G| - [G : M]}{2^{d-2}}.$$

Thus we have

$$\mathrm{cp}(G) \leq \frac{\mathrm{cp}(G/M)}{|M|} + \frac{1 - |M|^{-1}}{2^{d-2}}.$$

The inductive assumption tells us that

$$\mathrm{cp}(G/M) \leq \frac{4d-11}{2^d},$$

so that

$$\mathrm{cp}(G/M) - \frac{1}{2^{d-2}} \leq \frac{4d-15}{2^d}$$

and

$$\frac{\mathrm{cp}(G/M) - 2^{2-d}}{|M|} \leq \frac{4d-15}{2^{d+1}}.$$

Hence

$$\mathrm{cp}(G) \leq \frac{8}{2^{d+1}} + \frac{4d-15}{2^{d+1}},$$

so the result follows by induction.

ii) We proceed by induction on d. If $d = 2$, then part vi) of Lemma 2 yields $\mathrm{cp}(G) \leq \frac{p^2+p-1}{p^3}$, since $|[G,G]| \geq p$ and each non-linear irreducible character of G has degree a power of p. Suppose then that $d > 2$, and that the result has been established for $d-1$.

As in part i), we may suppose that every proper homomorphic image of G has derived length less than d, so that G has a unique minimal normal subgroup, M say, which is now central of order p. Also, G/M has derived length $d-1$. Every irreducible character of G which does not contain M in its kernel is faithful, and has degree at least p^{d-1} since G is a p-group of derived length d.

This time,

$$\mathrm{cp}(G) \leq \frac{\mathrm{cp}(G/M)}{p} + \frac{p-1}{p^{2d-1}}.$$

Since

$$\mathrm{cp}(G/M) \leq \frac{p^d + p^{d-1} - p}{p^{2d-2}}$$

by the inductive hypothesis, the result follows easily. □

We continue by mentioning further links with the (coprime) $k(GV)$ problem, and some consequences for solvable groups.

Theorem 13. *Let G be a finite solvable group and π be a set of primes. Then:*

i)

$$\mathrm{cp}(G) \leq \frac{k_G(O_{\pi'}(G))}{|G|_{\pi'}}.$$

ii) *If $O_{\pi'}(G) = 1$, we have $\mathrm{cp}(G) \leq \frac{1}{|G|_{\pi'}}$.*

iii) *If $O_{\pi'}(G) = 1$ and $\mathrm{cp}(G) = \frac{1}{|G|_{\pi'}}$, we may write $G = Z(G) \times M$, where either M is trivial, or else*

$$M = V_1G_1 \times \ldots \times V_sG_s,$$

where for each i, V_i is an elementary Abelian q_i-subgroup for some prime $q_i \in \pi$, and G_i is a π'-group which acts faithfully and irreducibly on V_i with $k(G_iV_i) = |V_i|$.

Proof. In each case, we will prove the corresponding statements about $k(G)$.
i) We may suppose that $\pi \subseteq \pi(G)$. We prove by induction on $|\pi|$ that if G is a solvable group with $O_{\pi'}(G) = 1$, then every subgroup of G has at most $|G|_\pi$ conjugacy classes, the case $|\pi| = 1$ having been dealt with in [18]. Suppose then that $|\pi| > 1$ and that the result has been established for smaller sets of primes. Choose a prime $p \in \pi$ and an arbitrary subgroup, X, of G. Set $\sigma = \pi \backslash \{p\}$. By induction, $k(X \cap O_{p'}(G)) \leq |O_{p'}(G)|_\sigma$. Furthermore, we have

$$k(X/X \cap O_{p'}(G)) \leq |G|_p$$

by the $|\pi| = 1$ case. Hence we certainly have $k(X) \leq |G|_\pi$ by part (ii) of Lemma 1. Now i) follows from part iii) of Lemma 1.
ii) Is just the special case of i) when $O_{\pi'}(G) = 1$.
iii) We first prove, again by induction on $|\pi|$, that if G is solvable with $O_{\pi'}(G) = 1$, and $k(G) = |G|_\pi$, then G has an Abelian normal Hall π-subgroup, the case $|\pi| = 1$ having been dealt with in [18]. Again we may suppose that $\pi \subseteq \pi(G)$, that $|\pi| > 1$, and that the result has been established for smaller sets of primes. Choose a prime $p \in \pi$, set $\sigma = \pi \backslash \{p\}$, and set $H = O_{p'}(G)$. Then every subgroup of G/H has at most $|G|_p$ conjugacy classes, so that $k(G) \leq |G|_p k_G(H)$, again by part (iii) of Lemma 1. Also, $k_G(H) \leq k(H) \leq |H|_\sigma$ by part (ii). Since $k(G) = |G|_\pi$, we must conclude that $|H|_\sigma = |G|_\sigma$, that $k(H) = |H|_\sigma$ and that every conjugacy class of H is G-stable. Furthermore, we must also have $k(G/H) = |P|$ for $P \in \mathrm{Syl}_p(G)$. Hence by the case $|\pi| = 1$, P must be Abelian (with its image normal in G/H) and by the inductive assumptions, H has an Abelian normal Hall σ-subgroup. However, since P is a p-group stabilizing every conjugacy class of $H = O_{p'}(G)$, we must have $[P, H] = 1$. Hence $P \lhd G$ since $G = HN_G(P)$ by a Frattini argument. Thus G has an Abelian normal Hall π-subgroup.

Next, we prove that $\Phi(G) \leq Z(G)$. Let $K = \Phi(G)$, which is certainly a π-group. Then $O_{\pi'}(G/K) = 1$. For otherwise, we may take T to be a pre-image of $O_{\pi'}(G/K)$ and, letting L be a Hall π'-subgroup of T, we have $G = KN_G(L)$ by a Frattini-type argument, a contradiction. Hence every subgroup of G/K has at most $[G : K]_\pi$ conjugacy classes, and we have

$$k(G) \leq k_G(K)[G : K]_\pi$$

by part iii) of Lemma 1. By hypothesis, we must have $k_G(K) = |K|$, so that $K \leq Z(G)$.

The conclusion of the proof follows the pattern of that in [18], so we only sketch the beginning of the argument. Let A be the Abelian normal Hall π-subgroup of G, and let T be a Hall π'-subgroup of G. Then $G = C_A(T) \times (T[A, T])$, so we may, and do, suppose that $A = [A, T]$ as $C_A(T) = Z(G)$. Hence we now have $Z(G) = \Phi(G) = 1$, as we have already established that $\Phi(G) \leq Z(G)$. Now A is a direct product of minimal normal subgroups of G, and if $A = V_1 \times \ldots \times V_s$ where each V_i is minimal normal in G, we set $G_i = C_T(\prod_{j \neq i} V_j)$, and we find as in [18] that

$$G = V_1 G_1 \times \ldots \times V_s G_s$$

under current assumptions. □

We mention a very elementary proof of a result of Brauer-Fowler type which is related to the themes of this paper.

Theorem 14. (i) *For any finite group G, we have*

$$\mathrm{cp}(G) \geq \left(\frac{\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)}{|G|} \right)^2.$$

(ii) *Let G be a finite group of even order with $Z(G) = 1$. Then we have*

$$|G| < |C_G(x)|^3$$

for some $x \in G^\#$.

Proof. By the Cauchy-Schwarz inequality and the orthogonality relations, we have

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \leq \sqrt{k(G)|G|}$$

and i) quickly follows.
ii) Suppose that G has even order and that $Z(G) = 1$. The number of solutions of $g^2 = 1$ in G is given by

$$\sum_{\chi \in \mathrm{Irr}(G)} \nu(\chi)\chi(1),$$

where $\nu(\chi)$ is the Frobenius-Schur indicator of χ (in particular, $\nu(\chi)$ always lies in $\{0, 1, -1\}$). The number of such solutions is strictly greater than $[G : C_G(t)]$ for any involution t of G. From part i), we see that for any involution $t \in G$, we have

$$[G : C_G(t)]^2 < k(G)|G|,$$

which leads to $|G| < k(G)|C_G(t)|^2$. From part (vii) of Lemma 2, we know that

$$k(G) \leq \max_{y \in G^\#} |C_G(y)|,$$

so it follows that $|G| < |C_G(x)|^3$ for some $x \in G^\#$. □

We remark that the groups $\mathrm{SL}(2, 2^n)$ again show that the bound of part (ii) of Theorem 14 is close to best possible. We point out that this bound is also strong enough to recover one of the usual forms of the Theorem of Brauer and Fowler ([1]). See Isaacs [11] for a similar proof.

Corollary 15. *Let G be a finite group of even order greater than 2. Then G has a proper subgroup H with $|G| < |H|^3$.*

Proof. We may, and do, suppose that G is not a 2-group. Set $G^* = G/Z_\infty(G)$. Then $Z(G^*) = 1$. If G^* has even order, then there is a non-identity element x^* of G^* with $|G^*| < |C_{G^*}(x^*)|^3$. Let H be the full pre-image in G of $C_{G^*}(x^*)$. Then $H < G$ and $|G| < |H|^3$. Hence we may suppose that G^* has odd order. Then G has a normal Sylow 2-subgroup, and (by the Schur-Zassenhaus theorem), G has a Hall $2'$-subgroup. One of these last two subgroups has order greater than $\sqrt{|G|}$. □

We conclude with some restrictions on the structure of solvable groups G for which $\mathrm{cp}(G) \geq \frac{1}{n}$ for a positive integer n.

Theorem 16. *Let n be a positive integer, and let G be a finite solvable group with $\mathrm{cp}(G) \geq \frac{1}{n}$. Let π denote the set of primes which do not exceed n. Then G has a nilpotent normal π-complement, there is at most one prime $p \in \pi'$ for which G has a non-Abelian Sylow p-subgroup, and any such prime is less than $n + \sqrt{n}$. If, furthermore, there is such a prime p, then $G/O_p(G)$ is Abelian and $[O_{\pi'}(G), O_{\pi'}(G)]$ has order p. Finally (in all cases), if T is a Hall π-subgroup of G, we have $|T| \leq n \cdot k_G(O_\pi(G))$, so certainly $[T : O_\pi(G)] \leq n$.*

Proof. We may, and do, suppose that $n > 1$. By part x) of Lemma 2, G has a nilpotent normal π-complement, say K. By parts (i) and (ix) of Lemma 2, there is at most one prime p for which K has a non-Abelian Sylow p-subgroup, and if there is such a prime, then we have $|[K, K]| = p$.

Suppose that there is such a prime p. By parts (i) and (viii) Lemma 2,

$$\frac{1}{p}+\frac{1}{p^2} > \mathrm{cp}(O_p(K)) \geq \mathrm{cp}(K) \geq \mathrm{cp}(G) \geq \frac{1}{n}.$$

Hence

$$\frac{1}{p}+\frac{1}{2} > \frac{1}{2}\sqrt{1+\frac{4}{n}},$$

which easily leads to $p < n+\sqrt{n}$. If, furthermore, $G/O_p(K)$ is non-Abelian, then by part (ii) of Lemma 2 and [10], we have

$$\frac{1}{n} \leq \mathrm{cp}(G) \leq \frac{5}{8}\left(\frac{1}{n}+\frac{1}{n^2}\right),$$

a contradiction.

Finally, in all cases, Theorem 13 yields

$$\frac{1}{n} \leq \mathrm{cp}(G) \leq \frac{k_G(O_\pi(G))}{|T|}.$$

□

References

[1] R. Brauer and K. Fowler, On groups of even order, Annals of Mathematics (2) 62,(1955), 565-583.

[2] J. Dixon, The solvable length of a solvable linear group, Math.Z., 107 (1968), 151-158.

[3] J. Dixon, Probabilistic group theory, C.R. Math. Rep. Acad. Sci. Canada 24 (2002), 1-15.

[4] L. Dornhoff, Group Representation Theory, Parts A and B, Dekker, New York, 1972.

[5] W. Feit and J.G. Thompson, On groups which have a faithful representation of degree less than $\frac{p-1}{2}$, Pacific J. Math. 4 (1961), 1257-1262.

[6] J. Fulman and R. Guralnick, Bounds on the numbers and sizes of conjugacy classes in finite Chevalley groups, preprint.

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

[8] D. Gluck, K. Magaard, U. Riese and P. Schmid, The solution of the $k(GV)$-problem, J. Algebra 279 (2004), 694–719.

[9] R. Guralnick and J. Wilson, The probability of generating a finite soluble group, Proc. London Math. Soc. (3) 81 (2000), 405–427.

[10] W. H. Gustafson, What is the probability that two group elements commute?, Amer. Math. Monthly 80 (1973), 1031–1034.

[11] I. Martin Isaacs, Character theory of finite groups, Dover Publications, Inc., New York, 1994.

[12] R. Knörr, On the number of characters in a p-block of a p-solvable group, Illinois J. Math. 28 (1984), 181-210.

[13] L. Kovács and G. Robinson, On the number of conjugacy classes of a finite group, J. Algebra, 160 (1993), 441–460.

[14] A. Maróti, Bounding the number of conjugacy classes of a permutation group, J. Group Theory, to appear.

[15] A. Moretó and G. Navarro, Heights of characters in blocks of p-solvable groups, Bull. London Math. Soc. 37 (2005), 373-389.

[16] H.Nagao, On a conjecture of Brauer for p-solvable groups J.Math. Osaka City University, 13, (1962), 35–38.

[17] G. Robinson, Nilpotent injectors and conjugacy classes in solvable groups, J. Australian Math. Soc., 71,(2001),3, (2001),349-352.

[18] G. Robinson, On Brauer's k(B)-problem for p-blocks of p-solvable groups with non-Abelian defect groups, J. Algebra, 280, (2004), 738–742.

[19] G. Robinson, More bounds on norms of generalized characters with applications to p-local bounds and blocks, Bull. London Math. Soc.,37,4,(2005),555-565.

[20] A. Shalev, Simple groups, permutation groups, and probability, Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), Doc. Math. 1998, Extra Vol. II, 129–137.

[21] T.R. Wolf, Sylow p-subgroups of p-solvable subgroups of $GL(n, p)$, Arch. Math. (Basel) 43 (1984), 1–10.

Department of Mathematics, University of Southern California, 3620 S. Vermont Ave, Los Angeles CA 90089-2532, USA

E-mail address: `guralnic@usc.edu`

Department of Mathematical Sciences, University of Aberdeen, Aberdeen AB24 3UE, Scotland

E-mail address: `grr@maths.abdn.ac.uk`