Factorizing a Finite Group into Conjugates of a Subgroup

Martino Garonzi
Department of Mathematics
University of Padova
Via Trieste 63
35121 Padova
Italy

Dan Levy
The School of Computer Sciences
The Academic College of Tel-Aviv-Yaffo
2 Rabenu Yeruham St.
Tel-Aviv 61083
Israel

July 1, 2014

Abstract

For every non-nilpotent finite group G, there exists at least one proper subgroup M such that G is the setwise product of a finite number of conjugates of M. We define $\gamma_{\mathrm{cp}}(G)$ to be the smallest number k such that G is a product, in some order, of k pairwise conjugated proper subgroups of G. We prove that if G is non-solvable then $\gamma_{\mathrm{cp}}(G) \leq 36$ while if G is solvable then $\gamma_{\mathrm{cp}}(G)$ can attain any integer value bigger than 2, while, on the other hand, $\gamma_{\mathrm{cp}}(G) \leq 4\log_2 |G|$.

1 Introduction

In this paper we consider representations of a finite group[1] as a product of conjugates of a single proper subgroup. This problem belongs to the broader class of covering problems. By a covering of a finite group G we mean a collection of proper subsets of G, whose union or setwise product is G. The covering operation (union or product) is fixed from the start, and in the case that the covering operation is setwise product there may be restrictions on the ordering of the subsets and their repetitions. Questions of interest besides the mere existence

[1] Unless otherwise stated, all our groups are assumed to be finite.

of coverings of a specified type, include the possible sizes of the coverings, and in particular, exact values or bounds on minimal sizes. Several problems of this type are considered in the literature: Union coverings by (conjugacy classes of) proper subgroups (for Union coverings see [22], [9], [13], for Normal Union coverings see [8], [7], [20]), product coverings by conjugacy classes ([1]), factorizing groups as a product of two subgroups ([18]), and other problems.

Definition 1 *Let G be a group. A conjugate product covering of G is a sequence $(A_1, ..., A_k)$ of $k \geq 2$ proper subgroups of G such that any two of the A_i are conjugate in G and $G = A_1 \cdots A_k$.*

Since a group G is nilpotent if and only if every maximal subgroup of G is normal, a conjugate product covering of G exists if and only if G is non-nilpotent.

Definition 2 *Let G be a finite group. Define $\gamma_{cp}(G)$ to be the minimal integer k such that G is a product of k conjugates of a proper subgroup of G if G is non-nilpotent, and $\gamma_{cp}(G) = \infty$ if G is nilpotent (as usual $n < \infty$ for any natural number n, and $\infty \leq \infty$).*

We remark that Liebeck, Nikolov and Shalev ([16],[17]) also consider conjugate product coverings, however, their discussion is limited from the outset to finite simple groups, and concentrates on bounding the size of specific coverings in terms of the orders of both the group and the covering subgroup.

Note (Lemma 6 below) that $\gamma_{\text{cp}}(G) > 2$ for any group G . For non-solvable groups our main result is the existence of a universal constant bound on γ_{cp}.

Theorem 3 *Let G be a non-solvable group. Then $\gamma_{cp}(G) \leq 36$.*

In fact, we believe that 36 is not the best possible bound (see Remark 18). On the other hand, for solvable groups we have:

Theorem 4 *For any integer $n \geq 3$ there exists a solvable group G such that $\gamma_{cp}(G) = n$.*

Theorem 5 *Let G be a finite solvable group. Then $\gamma_{cp}(G) \leq 4\log_2 |G|$.*

The rest of the paper is organized as follows. In Section 2 we collect some general results about γ_{cp}, and identify a class of groups which we term quotient minimal non-nilpotent groups, on which γ_{cp} is maximal in a sense to be made precise. In sections 3 and 4, we apply these general results to proving Theorem 3 and Theorems 4 and 5 respectively, as well as additional results and examples.

Notation. We use fairly standard notation. In particular, $\mathbb{N}$ and $\mathbb{N}_0$ denote the positive and the non-negative integers respectively, $\wr$ stands for wreath product, $\rtimes$ denotes semi-direct product, $\Phi(G)$ and $F(G)$ are the Frattini and Fitting subgroups of G, $T^m = \underbrace{T \times ... \times T}_{m \text{ direct factors}}$, and for x real, $\lceil x \rceil$ is the smallest integer satisfying $\lceil x \rceil \geq x$.

2 Quotient Minimal non-Nilpotent Groups

The following lemma is a basic well-known result.

Lemma 6 *Suppose that $G = AB$ for some subgroups A and B then $G = A^{g_1}B^{g_2}$ for any $g_1, g_2 \in G$. In particular $\gamma_{cp}(G) > 2$ for every group G.*

The next lemma is an immediate useful consequence of Lemma 6.

Lemma 7 *Let $H, A_1, ..., A_k \leq G$.*

1. If $HA_k = G$ and $H \subseteq A_1 \cdots A_k$ then $A_1 \cdots A_k = G$.

2. If each of $A_1, ..., A_k$ is conjugate to $A \leq G$, $HA = G$ and $H \subseteq A_1 \cdots A_k$ then $A_1 \cdots A_k = G$.

Proof. For (1) we have $G = HA_k \subseteq (A_1 \cdots A_k) A_k = A_1 \cdots A_k$, and (2) follows from (1) and Lemma 6. ■

The following is a key property for evaluating γ_{cp}.

Proposition 8 *Let G be a finite group. Then $\gamma_{cp}(G) \leq \gamma_{cp}(G/N)$ for every $N \trianglelefteq G$. We shall call this "the lifting property".*

Proof. We can assume that G/N is non-nilpotent and hence $G/N = \overline{A}_1 \cdots \overline{A}_k$ where $k = \gamma_{\mathrm{cp}}(G/N)$ and the $\overline{A}_i < G/N$ are pairwise conjugated. Using the correspondence theorem one shows that $G = A_1 \cdots A_k$ where $A_i < G$ is the inverse image of $\overline{A}_i$, and the A_i are pairwise conjugated. ■

Definition 9 *A group G is called a quotient minimal non-nilpotent group (qmnn-group) if G is non-nilpotent but G/N is nilpotent whenever $\{1_G\} \neq N \trianglelefteq G$.*

Due to the lifting property $\gamma_{\mathrm{cp}}(G)$ attains maximal integer values on qmnn-groups, and hence we study their structure. Let $N(G)$ denote the nilpotent residual of G. By definition, this is the unique normal subgroup of G which satisfies: $G/N(G)$ is nilpotent and for every $N \trianglelefteq G$ such that G/N is nilpotent we have $N(G) \leq N$. Note that $N(G)$ is the intersection of all $N \trianglelefteq G$ such that G/N is nilpotent.

Lemma 10 *Let G be a qmnn-group. Then:*

a. $N(G)$ is the unique minimal normal subgroup of G. In particular, $N(G) \cong T^m$ where T is simple and $m \in \mathbb{N}$, and G is solvable if and only if $N(G)$ is elementary abelian.

b. $\Phi(G) = Z(G) = 1$.

c. G has a faithful primitive action.

Proof. a. Let N be a minimal normal subgroup of G. Then $N > 1$ and G/N is nilpotent. Hence $N(G) \leq N$. But $N(G) > 1$ since G is non-nilpotent, so $N(G) = N$.

b. First suppose that $\Phi(G) > 1$. Then $G/\Phi(G)$ is nilpotent, so ([14] Corollary 5.1.2) G is nilpotent - a contradiction. Hence $\Phi(G) = 1$. Next

Suppose that $Z(G) > 1$. Then $N(G) \leq Z(G)$. Since $N(G)$ is the lowest term in the lower central series, $[G, N(G)] = N(G)$. But $N(G) \leq Z(G)$ so this gives $[G, N(G)] = 1$ and therefore $N(G) = 1$ - a contradiction.

c. It is sufficient to prove that one of the maximal subgroups of G is core-free. Suppose not. Then by (a) $N(G) \leq Core_G(M)$ for every maximal subgroup M of G. It follows that $N(G) \leq \Phi(G)$ in contradiction to (b). ■

Now we exhibit a connection between $\gamma_{\text{cp}}(G)$ and the ranks of the permutation representations of G. Let G be a group and let M be a proper subgroup of G. Set $\Omega = \{Mg | g \in G\}$ (the set of right cosets of M in G). Then G acts transitively by right multiplication on Ω and the point stabilizer of $M1 \in \Omega$ is M. The action of G induces an action of M on Ω whose orbits are in bijection with double cosets of M, when we view a double coset of M as a collection of right cosets of M: $MxM = \{M(xm) | m \in M\}$ where $x \in G$. The number of M-orbits is denoted r (the rank of G). Note that $r \geq 2$ and that G acts 2-transitively on Ω if and only if $r = 2$.

Proposition 11 *Let G be a group and let M be any non-normal maximal subgroup of G. Then $\gamma_{cp}(G) \leq r + 1$. Moreover, if $r = 2$ then $\gamma_{cp}(G) = 3$.*

Proof. Since M is non-normal there exists a conjugate M_1 of M such that $M_1 \nsubseteq M$. Let $x \in M_1 - M$. Then $\{M\}$ and MxM are two distinct orbits of the action of M. Set $B := M \cup MxM$. We have:

$$B^{k+1} = B^k \cup (MxM)^{k+1}, \forall k \in \mathbb{N}. \tag{*}$$

and in particular, $B^k \subseteq B^{k+1}$. Equation (*) can be proven by induction on $k \geq 1$ using $M^2 = M$ and the fact that the setwise product of G subsets is distributive over union. By finiteness of G there exists a positive integer k_0 such that $B^{k_0} = B^{k_0+1}$. Choose k_0 which is minimal with respect to this property. Then for every $1 \leq i \leq k_0 - 1$ we have $B^i \subset B^{i+1}$. Observe that B^i is a union over a family of M-orbits, since each double coset of M is an M-orbit, and product of double cosets is a union of double cosets. We can thus conclude that if $B^i \subset B^{i+1}$, then B^{i+1} contains more orbits of the action of M than B^i. Since $B^i \subset B^{i+1}$ for all $1 \leq i \leq k_0 - 1$, and B contains two orbits, the number of orbits which are contained in B^{k_0} is at least $k_0 + 1$.

Next observe that $B^{k_0} = B^{k_0+1}$ implies $\left(B^{k_0}\right)^2 = B^{k_0}$. Thus B^{k_0} is a subgroup. Since $M < B$ and M is maximal, we get $B^{k_0} = G$. By our previous argument it follows that $k_0 + 1 \leq r$.

Finally, using again Equation (*), we have:

$$(M \cup MxM)^{k_0} = M \cup MxM \cup (MxM)^2 \cup ... \cup (MxM)^{k_0}.$$

Since $(MxM)^i = MM^{x^{-1}}M^{x^{-2}} \cdots M^{x^{-i}}x^i$, we get:

$$\begin{gathered} G = (M \cup MxM)^{k_0} \\ = M \cup MM^{x^{-1}}x \cup MM^{x^{-1}}M^{x^{-2}}x^2 \cup ... \cup MM^{x^{-1}}M^{x^{-2}} \cdots M^{x^{-k_0}}x^{k_0}. \end{gathered}$$

Recall that $x \in M_1$, and hence $x^i M_1 = M_1$ for any integer i and we get :

$$\begin{aligned} G &= GM_1 \\ &= \left(M \cup MM^{x^{-1}} x \cup MM^{x^{-1}} M^{x^{-2}} x^2 \cup ... \cup MM^{x^{-1}} M^{x^{-2}} \cdots M^{x^{-k_0}} x^{k_0} \right) M_1 \\ &= MM_1 \cup MM^{x^{-1}} M_1 \cup MM^{x^{-1}} M^{x^{-2}} M_1 \cup ... \cup MM^{x^{-1}} M^{x^{-2}} \cdots M^{x^{-k_0}} M_1 \\ &= MM^{x^{-1}} M^{x^{-2}} \cdots M^{x^{-k_0}} M_1, \end{aligned}$$

where the last step follows from the fact that a product of a sequence of subgroups contains the product of every subsequence of the sequence. It follows that $\gamma_{\mathrm{cp}}(G) \leq k_0 + 2 \leq r + 1$. If $r = 2$ then $\gamma_{\mathrm{cp}}(G) > 2$ forces $\gamma_{\mathrm{cp}}(G) = 3$. ■

Remark 12 *The rank r of the action of G on Ω is given by $r = \sum_{\theta \in Irr(G)} m_\theta^2$, where m_θ is the multiplicity of the irreducible complex character θ in the permutation character associated with the action (see [15], Corollary (5.16)).*

3 $\gamma_{\mathbf{cp}}(G)$ for non-solvable G

As we shall see, if G is non-solvable then $\gamma_{\mathrm{cp}}(G)$ is controlled by γ_{cp} of non-solvable qmnn-groups. Hence we consider the following setting.

Minimal Non-Solvable Setting

1. G is a non-solvable group with a unique minimal normal subgroup $N = soc(G) = T^m$, where T is simple non-abelian and m a positive integer.

2. $X := N_G(T_1)/C_G(T_1)$ where T_1 is the first component of T^m.

Assuming the above setting, X is an almost simple group with $soc(X) \cong T$ (for convenience we will set $T := soc(X)$). Furthermore (see Remark 1.1.40.13 of [3]), there is an embedding of G into $X \wr K = X^m \rtimes K$ where the action of K as a transitive permutation group on the components of X^m, is determined by the permutation action of G on the components of $N = T^m$. The embedding of G into $X^m \rtimes K$ satisfies $GX^m = X^m \rtimes K$ and hence $K \cong GX^m/X^m \cong G/G \cap X^m$. Note that $N = T^m \trianglelefteq X^m \rtimes K$, but G needs not contain K.

Lemma 13 *Assume the minimal non-solvable setting. Let $V \leq X$ satisfy $VT = X$. Set $M = V \cap T$. Then $G = N_G(M^m)N$.*

Proof. Let $R = V \wr K \leq X \wr K$. Since V normalizes $V \cap T = M$, and K normalizes M^m, we have that R normalizes M^m, whence $G \cap R \leq N_G(M^m)$. Since $VT = X$ we get $RN = X \wr K$, and by Dedkind's law,

$$G = G \cap (RN) = (G \cap R)N \leq N_G(M^m)N.$$

Since both $N_G(M^m)$ and N are contained in G we get $G = N_G(M^m)N$. ■

Lemma 14 *Assume the minimal non-solvable setting. Suppose that $U \leq X$ satisfies $UT = X$ and $(U_1 \cap T) \cdots (U_h \cap T) = T$ where $U_1, ..., U_h$ are h conjugates of U in X. Then:*

$$G = N_G\left((U_1 \cap T)^m\right) \cdots N_G\left((U_h \cap T)^m\right).$$

In particular, if $1 < U \cap T < T$, then G is a product of h conjugates of a proper subgroup of G and $\gamma_{cp}(G) \leq h$.

Proof. Since $(U_i \cap T)^m \leq N_G\left((U_i \cap T)^m\right)$ for every $1 \leq i \leq m$, we have

$$\begin{aligned} T^m &= \left((U_1 \cap T) \cdots (U_h \cap T)\right)^m = (U_1 \cap T)^m \cdots (U_h \cap T)^m \\ &\leq N_G\left((U_1 \cap T)^m\right) \cdots N_G\left((U_h \cap T)^m\right). \end{aligned}$$

Taking $V = U_h$ in Lemma 13 (by Lemma 6, $U_h T = X$) we conclude that $G = T^m N_G\left((U_h \cap T)^m\right)$. Now, $G = N_G\left((U_1 \cap T)^m\right) \cdots N_G\left((U_h \cap T)^m\right)$ follows from Lemma 7(1), with $H = T^m \leq G$, $k = h$ and $A_i = N_G\left((U_i \cap T)^m\right) \leq G$ for all $1 \leq i \leq k$.

If $1 < U \cap T < T$, then $1 < (U \cap T)^m < N = T^m$ and since N is minimal normal in G, $N_G\left((U \cap T)^m\right)$ is a proper subgroup of G. Moreover, observe that for all $1 \leq i \leq h$, there exists $t_i \in T$ such that $U_i = U^{t_i}$. This follows from the fact that U_i is conjugate to U in X. Hence there exists $x_i \in X$ such that $U_i = U^{x_i}$. However $X = UT$ so $x_i = u_i t_i$ with $u_i \in U$ and $t_i \in T$ and hence $U_i = U^{x_i} = U^{u_i t_i} = U^{t_i}$. Furthermore, for all $1 \leq i \leq h$, $U_i \cap T = U^{t_i} \cap T = (U \cap T)^{t_i}$. Since $T^m \leq G$, we can deduce that for all $1 \leq i, j \leq h$, $(U_i \cap T)^m$ and $(U_j \cap T)^m$ are conjugate in G. Finally, since normalizers of conjugate subgroups are conjugate to each other, $N_G\left((U_i \cap T)^m\right)$ and $N_G\left((U_j \cap T)^m\right)$ are conjugate in G, for every $i, j \in \{1, \ldots, h\}$. This proves that $\gamma_{\text{cp}}(G) \leq h$. ■

Corollary 15 *Assume the minimal non-solvable setting with $T \cong A_n$, $n \geq 5$. Then $\gamma_{cp}(G) = 3$.*

Proof. For $n \neq 6$, we have either $X \cong A_n$ or $X \cong S_n$. Now T acts 2-transitively on $\{1, ..., n\}$ with a point stabilizer which is isomorphic to A_{n-1}. By Proposition 11, A_n is a product of three suitable conjugates of A_{n-1}. For $X \cong A_n$ we can choose $U \cong A_{n-1}$ and for $X \cong S_n$ we can choose $U \cong S_{n-1}$ so that in both cases U satisfies all of the assumptions of Lemma 14 with $h = 3$, and hence $\gamma_{\text{cp}}(G) = 3$. For $n = 6$ we use the fact that $T \cong A_6$ has another 2-transitive action of degree 10, whose point stabilizer is a normalizer of a Sylow 3-subgroup P of T (see, for example, [24] permutation representations of A_6). Thus T is a product of three conjugates of $N_T(P)$. Since all of the normalizers of Sylow 3-subgroups of T are conjugate in T and $T \trianglelefteq X$, we have, by the Frattini argument, that $X = N_X(N_T(P))T$. Taking $U = N_X(N_T(P))$ one checks that U satisfies all of the assumptions of Lemma 14 with $h = 3$, and therefore $\gamma_{\text{cp}}(G) = 3$ also for $n = 6$. ■

Corollary 16 *Assume the minimal non-solvable setting with T a sporadic simple group, or the Tit's group ${}^2F_4(2)'$. Then $\gamma_{cp}(G) \leq 36$.*

Proof. Under our assumptions $|Aut\,(T) : T| \leq 2$ so X is either T or $Aut\,(T)$, where the second possibility arises if $|Aut\,(T) : T| = 2$. For each of the 27 possible T's, and for each of the possible X corresponding to a given T, we wish to choose U which satisfies the conditions of Lemma 14 such that $U \cap T$ has the smallest rank with respect to the action of T on the coset space $\{(U \cap T)\,x | x \in T\}$. By Proposition 11 and Lemma 14, $\gamma_{\mathrm{cp}}\,(G) \leq r + 1$. For $X = T$ we choose U to be a maximal subgroup of T with minimal rank. For $X = Aut\,(T)$ where $|Aut\,(T) : T| = 2$, we choose U to be a maximal subgroup of X which is not contained in T, such that $U \cap T$ is maximal in T and its rank with respect to T is minimal. Examining Table 1 in the appendix, which summarizes these choices, one finds that the largest bound, $r+1 = 36$, is realized for $Aut\,(O'N)$ with $U = J_1 \times 2$. ■

Theorem 17 *Assume the minimal non-solvable setting, then* $\gamma_{cp}\,(G) \leq 36$.

Proof. We use the classification of finite simple non-abelian groups and split the discussion according to the isomorphism type of T.

1. $T \cong A_n$, $n \geq 5$. By Corollary 15 $\gamma_{\mathrm{cp}}\,(G) = 3$.

2. T is a simple group of Lie type of characteristic p. By Theorem D of [19] we have that T is a product of at most 25 Sylow p-subgroups (which are of course conjugate to each other by Sylow's theorem). Let P be a Sylow p-subgroup of T. By Frattini's argument $X = N_X\,(P)\,T$. Now we can apply Lemma 14 with $U = N_X\,(P)$. Note that $U \cap T = N_X\,(P) \cap T = N_T\,(P) < T$ since T is simple and clearly $\{1_T\} < P \leq U \cap T$. In particular, we can assume that h in Lemma 14 satisfies $h \leq 25$. We deduce $\gamma_{\mathrm{cp}}\,(G) \leq 25$ whenever T is a simple group of Lie type.

3. T is one of the 26 sporadic simple groups or T is the Tit's group ${}^2F_4\,(2)'$. By Corollary 16 we have $\gamma_{\mathrm{cp}}\,(G) \leq 36$.

Thus $\gamma_{\mathrm{cp}}\,(G) \leq 36$. ■

Proof of Theorem 3. We proceed by induction on the length $l\,(G)$ of a chief series of G (G can be any non-solvable group). If $l\,(G) = 1$ then G is simple non-abelian and $\gamma_{\mathrm{cp}}\,(G) \leq 36$ by Theorem 17. If $l\,(G) > 1$ there are two possibilities to consider:

1. Either G has an abelian minimal normal subgroup N_0, or all minimal normal subgroups of G are non-abelian and G has at least two minimal normal subgroups. In the first case set $N := N_0$ and in the second case set N to any minimal normal subgroup of G. Then G/N is non-solvable and $l\,(G/N) < l\,(G)$, so, by induction, $\gamma_{\mathrm{cp}}\,(G/N) \leq 36$ and therefore, by the lifting property, $\gamma_{\mathrm{cp}}\,(G) \leq 36$.

2. G has a unique minimal normal subgroup N which is non-abelian. Then $\gamma_{\mathrm{cp}}\,(G) \leq 36$ by Theorem 17. ■

Remark 18 *We strongly suspect that the upper bound on* $\gamma_{cp}\,(G)$ *where* G *is non-solvable can be significantly lowered. The "worst case" in the proof of Theorem 17 is associated with* $Aut\,(O'N)$. *After submitting the paper we have discovered a new method to evaluate* $\gamma_{cp}\,(G)$, *where* G *is a sporadic almost simple* *group, which we believe ("work in progress") will eliminate this case. Furthermore, in case (2) of Theorem 17 (groups of Lie type) we have taken a conservative approach in choosing to rely on Theorem D of [19] which yields $\gamma_{cp}(G) \leq 25$. Since [19] was published there appeared in the literature claims for improving it. In [2] it was announced that every simple group of Lie type in characteristic p is a product of just five of its Sylow p-subgroups, although, as far as we know, no complete proof has yet been published. A sketch of a proof for exceptional Lie type groups appears in a survey by Pyber and Szabo ([21] Theorem 15). For classical Chevalley groups a better bound of four is claimed by Smolensky, Sury and Vavilov in [23].*

4 $\gamma_{\mathbf{cp}}(G)$ for solvable G

If G is solvable then it is clear that $\gamma_{\mathrm{cp}}(G)$ is controlled by γ_{cp} of solvable qmnn-groups. By Lemma 10(c), these groups are primitive. Using known properties of primitive solvable groups (Theorem (A15.6) of [11]) we can assume the following setting in our discussion.

Minimal Solvable Setting

1. $G = V \rtimes K$, where V is an elementary abelian group of order p^n, p a prime and n a positive integer, K is a non-trivial irreducible nilpotent subgroup of $GL(V) \cong GL_n(p)$, with $k := |K|$ not divisible by p, and $\rtimes$ is the semidirect product with respect to action of K on V obtained by restriction from the action of $GL(V)$ on V.

2. V is the unique minimal normal subgroup of G, and all complements to V in G are conjugate to K.

Note that the non-trivial action of K on V implies that G is non-nilpotent. When convenient we regard V as a vector space of dimension n over the field F_p of p elements and use additive notation for V and even a mixture of additive and multiplicative notation.

Lemma 19 *Assume the minimal solvable setting. If $M \leq G$ is maximal then either $M \cap V = 1$ in which case M is conjugate to K or $V \leq M$, in which case $M \trianglelefteq G$. In particular, G is the product of $\gamma_{cp}(G)$ conjugates of K.*

Proof. Suppose by contradiction that $1 < M \cap V < V$. Then $V \nleq M$ and hence $G = MV$. Now $M \cap V$ is normalized by V since V is abelian, and by M since M normalizes V and itself. Hence $M \cap V \trianglelefteq MV = G$, contradicting $1 < M \cap V < V$, and the fact that V is minimal normal in G. If $M \cap V = 1$ then M complements V in G and hence it is conjugate to K. If $M \cap V = V$ then $V \leq M$, and then, since G/V is nilpotent and M maximal in G, $M/V \trianglelefteq G/V$ and $M \trianglelefteq G$ by the correspondence theorem. ■

Lemma 20 *Assume the minimal solvable setting. For any $v \in V$ there exists $t \in V$ such that $v \in KK^t$.*

Proof. For any $x \in K$ set $C(x^{-1}, V) := \left\{x^{-1}vxv^{-1} = v^x - v | v \in V\right\} \subseteq V$. Note that $C(x^{-1}, V) \leq V$ because

$$v^x - v + u^x - u = (v+u)^x - (v+u) \in C(x^{-1}, V),\ \forall v, u \in V.$$

Since V is abelian it is clear that $C(x^{-1}, V)$ is normalized by V. We now prove that if $x \in Z(K)$ then $C(x^{-1}, V)$ is normalized by K as well:

$$(v^x - v)^y = v^{xy} - v^y = v^{yx} - v^y = (v^y)^x - v^y \in C(x^{-1}, V),\ \forall v \in V, \forall y \in K.$$

Therefore, assuming $x \in Z(K)$ we get that $C(x^{-1}, V) \trianglelefteq G$. Since $C(x^{-1}, V) \leq V$ and V is minimal normal this implies that either $C(x^{-1}, V) = \{0_V\}$ or $C(x^{-1}, V) = V$. Suppose, in addition, that $x \neq 1_G$ (since K is nilpotent such a choice of x exists). Now $C(x^{-1}, V) = \{0_V\}$ implies that V centralizes $\langle x \rangle$ and since $x \in Z(K)$ it follows that $x \in Z(G)$ in contradiction to Lemma 10(b). Thus, if $x \neq 1$ we can conclude $C(x^{-1}, V) = V$.

Let $v \in V$ be arbitrary. We wish to show that there exists $t \in V$ such that $v \in KK^t$. Choose $1 \neq x \in Z(K)$. Then $C(x^{-1}, V) = V$ and hence there exists $w \in V$ such that $v = w^x - w = x^{-1}wxw^{-1} = x^{-1}x^{w^{-1}} \in KK^{w^{-1}}$. Thus $t = w^{-1}$ satisfies the claim. ■

Theorem 21 *Assume the minimal solvable setting. Then:*

$$n\frac{\log_2 p}{\log_2 k} + 1 \leq \gamma_{cp}(G) \leq 2n(\log_2 p + 1).$$

Proof. 1. Suppose that $G = K_1 \cdots K_h$ where the K_i are pairwise conjugated subgroups of G. Then $p^n k = |G| \leq |K_1| \cdots |K_h| = k^h$ and the lower bound follows by taking logarithms.

2. Set $m := \lceil \log_2 p \rceil$. Let $\{v_1, ..., v_n\}$ be a basis of the vector space V. If $i \in \{1, ..., n\}$ and $s \in \{1, ..., p-1\}$ then s is a sum of at most m distinct powers of 2 and hence sv_i is a sum of at most m vectors of the form $2^j v_i$ with $0 \leq j \leq m-1$ (just write s in base 2). By Lemma 20, for every $i \in \{1, ..., n\}$ and $j \in \{0, ..., m-1\}$ there exist $t_{ij} \in V$ such that $2^j v_i \in KK^{t_{ij}}$. Hence the product $\prod_{j=0}^{m-1} KK^{t_{ij}}$ contains all elements of V of the form sv_i, where sv_i, $0 \leq s \leq p-1$, is written in multiplicative notation: For each $j \in \{0, ..., m-1\}$ we either pick 1 from $KK^{t_{ij}}$ if the jth bit of s is zero or $2^j v_i$ if the jth bit of s is 1. Hence:

$$\prod_{i=1}^{n}\prod_{j=0}^{m-1} KK^{t_{ij}} = K\prod_{i=1}^{n}\prod_{j=0}^{m-1} KK^{t_{ij}} \supseteq K\prod_{i=1}^{n}\langle v_i \rangle = KV = G.$$

This proves that $\gamma_{\mathrm{cp}}(G) \leq 2nm = 2n(\lceil \log_2 p \rceil) \leq 2n(\log_2 p + 1)$. ■

Proof of Theorem 5. We can assume that G is a qmnn-group. Then, by Theorem 21 we have $\gamma_{\mathrm{cp}}(G) \leq 2n(\log_2 p + 1)$. Since $|G| = p^n k$, $4\log_2 |G| =$

$4n\log_2 p+4\log_2 k\geq 2n\left(\log_2 p+1\right)$ and the claim follows. ■

For the family of groups in the next example there is a true gap between the lower and the upper bounds of Theorem 21, and this may be taken as a hint that a tighter upper bound exists.

Example 22 *Assuming the minimal solvable setting take $n=1$ and $p>2$, which gives $V\cong C_p$. Choose $K=Aut\left(V\right)\cong C_{p-1}$. Then $G\cong AGL_1\left(F_p\right)$ which acts 2-transitively on F_p (See for instance [10] Exercise 2.8.1 p.52). Hence $\gamma_{cp}\left(G\right)=3$ and the lower bound is also $\left\lceil n\frac{\log_2 p}{\log_2 k}+1\right\rceil=\left\lceil\frac{\log_2 p}{\log_2 (p-1)}+1\right\rceil=3$.*

4.1 Proof of Theorem 4

Proposition 23 *Let p be an odd prime and let $G=D_{2p}$, the dihedral group of order $2p$. Then $\gamma_{cp}\left(G\right)=\lceil\log_2 p\rceil+1$.*

For proving Proposition 23 we need the following lemma.

Lemma 24 *Let $n\geq 1$ be an integer. Set*

$$X_n:=\left\{\sum_{i=0}^{h}\left(-1\right)^i 2^{a_i}|0\leq h\leq n-1,a_0<...<a_h\leq n-1,a_i\in\mathbb{N}_0\right\}.$$

Then $X_n=\left\{x\in\mathbb{Z}|-2^{n-1}+1\leq x\leq 2^{n-1}\right\}-\{0\}$, and:

$$\{1,...,k\}\subseteq X_n\operatorname{mod}\left(k+1\right):=\left\{x\operatorname{mod}\left(k+1\right)|x\in X_n\right\},\ \forall 1\leq k<2^n.$$

Proof. Set $Y_n:=\left\{\left(a_0,...,a_h\right)|0\leq h\leq n-1,a_0<...<a_h\leq n-1,a_i\in\mathbb{N}_0\right\}$. There is a bijection between Y_n and the set of non-empty subsets of $\{0,...,n-1\}$, and hence $|Y_n|=2^n-1$. We prove by induction on $n\geq 1$ that the natural mapping $Y_n\to X_n$ is injective (it is clearly surjective). For $n=1$ there is nothing to prove. Let $n>1$ and let $\left(a_0,a_1,...,a_h\right)\neq\left(b_0,b_1,...,b_{h'}\right)$ be two elements of Y_n. Assume by contradiction that

$$\sum_{i=0}^{h}\left(-1\right)^i 2^{a_i}=\sum_{i=0}^{h'}\left(-1\right)^i 2^{b_i}.$$

If $a_0=b_0$ then $\sum_{i=1}^{h}\left(-1\right)^i 2^{a_i}=\sum_{i=1}^{h'}\left(-1\right)^i 2^{b_i}$ and after canceling a common factor of 2 on both sides we can apply the induction assumption and obtain a contradiction. If $a_0>b_0$, then the left hand side is divisible by 2^{b_0+1} while the right hand side is not - a contradiction. The case $a_0<b_0$ is handled similarly. Thus $|X_n|=2^n-1$. In order to complete the proof of the first claim of the lemma it remains to check that $\min\left(X_n\right)=-2^{n-1}+1$ (take $h=1$, $a_0=1$ and $a_1=n-1$), that $\max\left(X_n\right)=2^{n-1}$ (take $h=0$, $a_0=n-1$), and that $0\notin X_n$ (Supposing $\sum_{i=0}^{h}\left(-1\right)^i 2^{a_i}=0$, where $0\leq a_0<...<a_h$, contradicts

$\sum_{i=0}^{h}(-1)^{i}2^{a_i} \equiv 2^{a_0}\left(\operatorname{mod} 2^{a_0+1}\right)$). The second claim of the lemma is immediate if $k \leq 2^{n-1}$. If $2^{n-1} < k < 2^{n}$ then any $x \in \left\{2^{n-1}+1, ..., k\right\}$ is congruent, modulo $(k+1)$, to a number in $\left\{-2^{n-1}+1, -2^{n-1}+2, ..., -1\right\}$. ■

Proof of Proposition 23. We use the familiar presentation of dihedral groups, $D_{2p} = \left\langle v, b | v^{p} = b^{2} = 1, bvb = v^{-1}\right\rangle$. Note that G fits the minimal solvable setting with $V = \langle v\rangle$ and $K = \langle b\rangle$. Set $m := \lceil \log_2 p\rceil$. By Theorem 21 $\gamma_{\text{cp}}(G) \geq m+1$ so it remains to prove $\gamma_{\text{cp}}(G) \leq m+1$. For each $1 \leq j \leq m$ set $v_j := v^{2^{j-1}}$, and $B := \langle b\rangle^{v_1}\cdots\langle b\rangle^{v_m}\langle b\rangle$. We shall prove that $V \subseteq B$ and then, by Lemma 7, $B = G$ and $\gamma_{\text{cp}}(G) \leq m+1$ follows.

Observe that for any $1 \leq i \leq m$ the defining relations of the D_{2p} presentation imply $v_i^{-1}bv_i = v_i^{-2}b$. Consequently $b^{v_i}b^{v_j} = v_i^{-2}v_j^{2} = \left(v_i^{-1}v_j\right)^2$ for all $1 \leq i \neq j \leq m$. Thus, for any $1 \leq t \leq m$, and $1 \leq i_1 < i_2 < ... < i_t \leq m$ we have

$$\left(v_{i_1}^{-1}v_{i_2}v_{i_3}^{-1}v_{i_4}\cdots v_{i_{t-1}}^{-1}v_{i_t}\right)^2 \in \langle b\rangle^{v_1}\cdots\langle b\rangle^{v_m} \subseteq B, \text{ if } t \text{ is even}$$

$$\left(v_{i_1}^{-1}v_{i_2}v_{i_3}^{-1}v_{i_4}\cdots v_{i_{t-2}}^{-1}v_{i_{t-1}}v_{i_t}^{-1}\right)^2 \in \langle b\rangle^{v_1}\cdots\langle b\rangle^{v_m}b \subseteq B, \text{ if } t \text{ is odd.}$$

Substituting $v_j := v^{2^{j-1}}$, $1 \leq j \leq m$, we conclude that every element of V of the form $v^{-2x} = \left(v^{-2}\right)^{x}$ where $x \in X_m$ (X_m is defined in Lemma 24) is in B. Note that since p is odd v^{-2} is a generator of V. By definition of m we have $p-1 < 2^{m}$, and hence, by Lemma 24, $\{1, ..., p-1\} \subseteq X_m \operatorname{mod} p$. Since $v^{0} = 1_G \in B$ as well, we get $V \subseteq B$. ■

Proof of Theorem 4. By Bertrand's postulate, for every integer $n \geq 3$ there exists at least one odd prime p such that $2^{n-2} < p < 2^{n-1}$. Hence $\lceil \log_2 p\rceil = n-1$, and, by Proposition 23, $\gamma_{\text{cp}}(D_{2p}) = \lceil \log_2 p\rceil + 1 = n$. ■

Remark 25 *Here are two additional relevant results, stated without proofs.*

1. For a general dihedral group D_{2n} with $n \geq 2$ an arbitrary integer, $\gamma_{cp}(D_{2n}) = \infty$ if n is a power of 2 and otherwise $\gamma_{cp}(D_{2n}) = \lceil \log_2 p\rceil + 1$, where p is the smallest odd prime divisor of n.

2. One can generalize the ideas behind the proof of Proposition 23, for the case that G is a subgroup of $AGL_1(F_{p^n})$, p is an odd prime and n is a positive integer, with $V \cong (F_{p^n}, +, 0)$ and K acts irreducibly by multiplication on V as a subgroup of $\left(F_{p^n}^{*}, \cdot, 1\right)$. In particular, for $p = 13$, $n = 1$ and K the order 4 subgroup of F_{13}^{*}, one obtains $\gamma_{cp}(G) = 4$. Note that the lower bound of Theorem 21 for this case is 3 (compare to Example 22).

Appendix

Table 1 below presents a choice of $U \leq X$ for each almost simple sporadic group X, such that U satisfies the conditions of Lemma 14 with as minimal as possible value of r. The values of $h = r+1$ given here provide upper bounds on $\gamma_{\text{cp}}(G)$ in the proof of Corollary 16. The table is based on two sources:

1. Breuer and Lux ([6],[5]) have computed all multiplicity free permutation characters of almost simple sporadic groups. Note that $Aut(O'N)$ has no

X	U	h	X	U	h	X	U	h
M_{11}	$A_6.2_3$	3	M_{24}	M_{23}	3	$HN.2$	$4.HS.2$	10
M_{12}	M_{11}	3	M^cL	$U_4\left(3\right)$	4	Ly	$G_2\left(5\right)$	6
$M_{12}.2$	$L_2(11).2$	6	$M^cL.2$	$U_4\left(3\right).2_3$	4	Th	${}^3D_4(2).3$	12
J_1	$L_2(11)$	6	He	$S_4(4).2$	6	Fi_{23}	$2.Fi_{22}$	4
M_{22}	$L_3(4)$	3	$He.2$	$S_4(4).4$	6	Co_1	Co_2	5
$M_{22}.2$	$L_3(4).2_2$	3	Ru	${}^2F_4\left(2\right)'.2$	4	J_4	$2^{11}:M_{24}$	8
J_2	$U_3(3)$	4	Suz	$G_2(4)$	4	Fi'_{24}	Fi_{23}	4
$J_2.2$	$U_3(3).2$	4	$Suz.2$	$G_2(4).2$	4	$Fi'_{24}.2$	$Fi_{23}\times 2$	4
M_{23}	M_{22}	3	$O'N$	$L_3(7).2$	6	B	$2.{}^2E_6(2).2$	6
${}^2F_4\left(2\right)'$	$L_3(3).2$	5	$O'N.2$	$J_1\times 2$	36	M	$2.B$	10
${}^2F_4\left(2\right)'.2$	$2.[2^9]:5:4$	6	Co_3	$M^cL.2$	3			
HS	$U_3\left(5\right).2$	3	Co_2	$U_6(2).2$	4			
$HS.2$	$M_{22}.2$	4	Fi_{22}	$2.U_6(2)$	4			
J_3	$L_2(16).2$	9	$Fi_{22}.2$	$2.U_6(2).2$	4			
$J_3.2$	$L_2(16).4$	9	HN	$2.HS.2$	10			

Table 1: Subgroups of Almost Simple Sporadic Groups which provide the best upper bounds on γ_{cp} via the rank argument

suitable multiplicity free permutation characters.

2. Using GAP's character library ([12],[4]) we have been able to compute the permutation characters associated with maximal subgroups of all almost simple sporadic groups beside the groups B and M, and ${}^2F_4\left(2\right)'$. In particular one can estimate h for $Aut\left(O'N\right)$ in this way.

References

[1] Z. Arad and M. Herzog (ed.), "Products of Conjugacy Classes in Groups", Lecture Notes in Mathematics 1112, Springer-Verlag Berlin Heidelberg (1985).

[2] L. Babai, N. Nikolov and L. Pyber, "Product Growth and Mixing in Finite Groups", Proceeding SODA '08 Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms p. 248-257

[3] A. Ballester-Bolinches, L. M. Ezquerro, Classes of Finite Groups; Springer, 2006.

[4] T. Breuer, CTblLib, - GAP's Character Table Library package, version 1.2.1, (2012), http://www.math.rwth-aachen.de/\~Thomas.Breuer/ctbllib

[5] T. Breuer, Data provided by the GAP package mfer, http://www.math.rwth-aachen.de/~mfer/data/index.html

[6] T. Breuer, K. Lux, "The multiplicity-free permutation characters of the sporadic simple groups and their automorphism groups", Communications in Algebra, vol 24, number 7, (1996), 2293-2316

[7] J. R. Britnell and A. Maróti, Normal Coverings of Linear Groups, Algebra Number Theory, to appear.

[8] D. Bubboloni, C. E. Praeger, P. Spiga, Normal coverings and pairwise generation of finite alternating and symmetric groups, Journal of Algebra 390 (2013), 199–215.

[9] E. Detomi, A. Lucchini, On the Structure of Primitive n-Sum Groups; CUBO A Mathematical Journal Vol.10 n. 03 (195–210), 2008.

[10] J.D.Dixon and B. Mortimer, Permutation Groups, Graduate Texts in Mathematics, Springer (1996).

[11] K. Doerk and T. Hawkes, Finite Soluble Groups, de Gruyter Expositions in Mathematics 4, de Gruyter (1992).

[12] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.5; 2013. (http://www.gap-system.org)

[13] M. Garonzi and A. Lucchini, Direct products of finite groups as unions of proper subgroups, Arch. Math. 95 (2010), no. 3, 201—206.

[14] D. Gorenstein, Finite Groups, AMS Chelsea Publishing, second edition, (1980).

[15] I.M. Isaacs, Character Theory of Finite Groups, Dover Publications, 1994.

[16] M.W. Liebeck, N. Nikolov and A. Shalev, "A conjecture on product decompositions in simple groups", Groups Geom. Dyn. 4 (2010), 799–812.

[17] M.W. Liebeck, N. Nikolov and A. Shalev, "Product decompositions in finite simple groups", Bull. London Math. Soc. (2012) 44 (3): 469-472.

[18] M.W. Liebeck , C.E. Praeger, J. Saxl, "The maximal factorizations of the finite simple groups and their automorphism groups", Memoirs of the American Mathematical Society, (1990), vol 86, 1-151.

[19] M.W. Liebeck, L. Pyber: "Finite linear groups and bounded generation", Duke Math. J. 107, (2001), 159-171.

[20] A. Lucchini and M. Garonzi, Covers and Normal Covers of Finite Groups, preprint (http://arxiv.org/abs/1310.1775).

[21] L. Pyber, E. Szabo, "Growth in Linear Groups", (2012), http://arxiv.org/pdf/1208.2538v1.pdf

[22] M. J. Tomkinson, Groups as the union of proper subgroups, Math. Scand. 81 (2) (1997) 191–198.

[23] N. A. Vavilov, A. V. Smolensky, B. Sury, "Unitriangular Factorizations of Chevalley Groups", (2011), http://arxiv.org/pdf/1107.5414v1.pdf

[24] R. Wilson, P. Walsh, J. Tripp, I. Suleiman, S. Rogers, R. Parker, S. Norton, S. Nickerson, S. Linton, J. Bray and R. Abbott, ATLAS of Finite Group Representations, http://brauer.maths.qmul.ac.uk/Atlas/ (version 2) or http://brauer.maths.qmul.ac.uk/Atlas/v3/ (experimental version 3).