ON THE CLIQUE NUMBER OF THE GENERATING GRAPH OF A FINITE GROUP

ANDREA LUCCHINI AND ATTILA MARÓTI

(Communicated by Jonathan I. Hall)

Abstract. The generating graph $\Gamma(G)$ of a finite group $G$ is the graph defined on the elements of $G$ with an edge connecting two distinct vertices if and only if they generate $G$. The maximum size of a complete subgraph in $\Gamma(G)$ is denoted by $\omega(G)$. We prove that if $G$ is a non-cyclic finite group of Fitting height at most 2 that can be generated by 2 elements, then $\omega(G) = q + 1$, where $q$ is the size of a smallest chief factor of $G$ which has more than one complement. We also show that if $S$ is a non-abelian finite simple group and $G$ is the largest direct power of $S$ that can be generated by 2 elements, then $\omega(G) \leq (1 + o(1))m(S)$, where $m(S)$ denotes the minimal index of a proper subgroup in $S$.

1. Introduction

The generating graph $\Gamma(G)$ of a finite group $G$ is the graph defined on the elements of $G$ with an edge connecting two distinct vertices if and only if they generate $G$. By the solution of Dixon's conjecture, it is known that $\Gamma(S)$ has "many" edges for $S$ a non-abelian finite simple group. In particular, Liebeck and Shalev [9] proved that there exists a universal positive constant $c$ such that the maximal size of a complete subgraph in $\Gamma(S)$ is at least $c \cdot m(S)$ where $m(S)$ is the minimal index of a proper subgroup in $S$. This result, in general, is best possible. Indeed, by a result of Dye [6], the group $S = Sp_{2n}(2)$ is the union of all conjugates of the maximal subgroups $O^+_{2n}(2)$ and $O^-_{2n}(2)$, and so $\omega(S) \leq 2^{2n} = (2 + o(1))m(S)$.

This result of Liebeck and Shalev together with the above-mentioned remark on the symplectic group justifies the following definitions. For a finite group $G$ let the maximum size of a complete subgraph in $\Gamma(G)$ be denoted by $\omega(G)$. For a non-cyclic finite group $G$ let $\sigma(G)$ denote the least number of proper subgroups of $G$ whose union is $G$. Clearly, $\omega(G) \leq \sigma(G)$. Moreover, if $\chi(G)$ denotes the chromatic number of $\Gamma(G)$ (that is, the least number of colors needed to color the vertices of $\Gamma(G)$ in such a way that the endpoints of each edge receive different colors), then we also have $\omega(G) \leq \chi(G) \leq \sigma(G)$, where the second inequality follows from the fact that $\Gamma(G)$ is $\sigma(G)$-colorable since its vertex set is the union of $\sigma(G)$ empty subgraphs.

Received by the editors July 22, 2008.

2000 Mathematics Subject Classification. Primary 05C25, 20D10, 20P05.

The research of the second author was supported by OTKA NK72523, OTKA T049841, NSF Grant DMS 0140578, and by a fellowship of the Mathematical Sciences Research Institute.

©2009 American Mathematical Society
The function $\sigma$ has been much investigated. For example, for a finite solvable group $G$, Tomkinson [14] showed that $\sigma(G) = q + 1$, where $q$ is the minimal size of a chief factor of $G$ having more than one complement. Our first result is

**Theorem 1.1.** Let $G$ be a finite group with Fitting height at most 2. Then $\omega(G) = \chi(G)$. Moreover, if the minimal number of generators of $G$ is 2, then $\omega(G) = \sigma(G)$.

It is not known whether the conclusions of Theorem 1.1 are true for an arbitrary finite solvable group $G$. Blackburn [3] showed that $\omega(\text{Sym}(n)) = \sigma(\text{Sym}(n)) = 2^{n-1}$ for a sufficiently large odd positive integer, and also that $\omega(\text{Alt}(n)) = \sigma(\text{Alt}(n)) = 2^{n-2}$ for $n$ a sufficiently large even integer not divisible by 4. However, by [11], there are infinitely many non-abelian finite simple groups $S$ with $\omega(S) < \chi(S) < \sigma(S)$.

Still $\omega(S)$ and $\sigma(S)$ do not seem to be “far apart” for a non-abelian finite simple group $S$. In fact, Blackburn [3] asked whether $\omega(S)/\sigma(S)$ tends to 1 as the size of the non-abelian finite simple group $S$ tends to infinity. Our second result shows that there is an infinite sequence of 2-generated finite groups $G$ such that $\omega(G)/\sigma(G)$ tends to 0 as the size of $G$ tends to infinity.

**Theorem 1.2.** Let $S$ be a non-abelian finite simple group, let $m(S)$ be the minimal index of a proper subgroup in $S$ and let $G$ be the largest direct power of $S$ that can be generated by 2 elements. Then $\omega(G) \leq m(S) + O(m(S)^{14/15})$ if $S$ is a group of Lie type and $\omega(G) \leq m(S) + O(1)$ otherwise. In particular, if $S = \text{Alt}(n)$, then $\omega(G)/\sigma(G) \leq (n + O(1))/2^{n-2}$.

## 2. Groups of fitting height at most 2

In this section we prove Theorem 1.1.

Let $V$ be a finite dimensional vector space over a finite field of prime order. Let $H$ be a linear solvable group acting irreducibly and faithfully on $V$. Suppose that $H$ can be generated by 2 elements. For a positive integer $t$ consider the semidirect product $G = V^t \rtimes H$, where $H$ acts in the same way on each of the $t$ direct factors. We would like to derive some information about $\omega(G)$. Put $F = \text{End}_H(V)$.

**Proposition 2.1.** Assume $H = \langle x, y \rangle$ and let $(u_1, \ldots, u_t), (w_1, \ldots, w_t) \in V^t$. The following are equivalent:

1. $G \neq \langle x(u_1, \ldots, u_t), y(w_1, \ldots, w_t) \rangle$;
2. there exist $\lambda_1, \ldots, \lambda_t \in F$ and $w \in V$ with $(\lambda_1, \ldots, \lambda_t, w) \neq (0, \ldots, 0, 0)$ such that $\sum \lambda_iu_i = w - wx$ and $\sum \lambda_iw_i = w - wy$.

**Proof.** Let $a = x(u_1, \ldots, u_t)$, $b = y(w_1, \ldots, w_t)$, $K = \langle a, b \rangle$. First we prove, by induction on $t$, that if $K \neq G$, then (2) holds. Let $\tilde{a} = x(u_1, \ldots, u_{t-1}, 0)$, $\tilde{b} = y(w_1, \ldots, w_t, 0)$, $\tilde{K} = \langle \tilde{a}, \tilde{b} \rangle$. If $\tilde{K} \neq V^{t-1}H$, then, by induction, there exist $\lambda_1, \ldots, \lambda_{t-1} \in F$ and $w \in V$ with $(\lambda_1, \ldots, \lambda_{t-1}, w) \neq (0, \ldots, 0, 0)$ such that $\sum \lambda_iu_i = w - wx$ and $\sum \lambda_iw_i = w - wy$. In this case $\lambda_1, \ldots, \lambda_{t-1}, 0$ and $w$ are the requested elements. So we may assume $\tilde{K} \cong V^{t-1}H$. Set $V_t = \{ (0, \ldots, 0, v) \mid v \in V \}$. We have $K\langle V_t \rangle = KV_t = G$ and $K \neq G$; this implies that $K$ is a complement of $V_t$ in $G$ and therefore there exists $\delta \in \text{Der}(K, V_t)$ such that $\delta(a) = u_t$ and $\delta(b) = w_t$. However, by Propositions 2.7 and 2.10 of [2], we have $H^t(\tilde{K}, V_t) \cong F^{t-1}$. More precisely if $\delta \in \text{Der}(K, V_t)$, then there exist an inner derivation $\delta_w \in \text{Der}(H, V)$ and $\lambda_1, \ldots, \lambda_{t-1} \in F$ such that for each
$g(v_1, \ldots, v_{t-1}, 0) \in \tilde{K}$ we have $\delta(g(v_1, \ldots, v_{t-1}, 0)) = \delta_w(g) + \lambda_1 v_1 + \cdots + \lambda_{t-1} v_{t-1} = wq - w + \lambda_1 v_1 + \cdots + \lambda_{t-1} v_{t-1}$. In particular $u_t = w_x - w + \lambda_1 v_1 + \cdots + \lambda_{t-1} v_{t-1}$ and $w_t = w_x - w + \lambda_1 v_1 + \cdots + \lambda_{t-1} v_{t-1}$.

Conversely, if (2) holds, then $(b(v_1, \ldots, v_t) \mid w - wh = \lambda_1 v_1 + \cdots + \lambda_t v_t)$ is a proper subgroup of $G$ containing $K$.

Let $n$ be the dimension of $V$ over $F$. We may identify $H = \langle x, y \rangle$ with a subgroup of $GL(n, F)$. In this identification $x$ and $y$ become two $n \times n$ matrices $X$ and $Y$ with coefficients in $F$. Let $(u_1, \ldots, u_t), (w_1, \ldots, w_t) \in V^t$. Then every $u_i$ and $w_j$ can be viewed as a $1 \times n$ matrix. Denote the $t \times n$ matrix with rows $u_1, \ldots, u_t$ (resp. $w_1, \ldots, w_t$) by $A$ (resp. $B$). By Proposition 2.3.1 the elements $x(u_1, \ldots, u_t), y(w_1, \ldots, w_t)$ generate a proper subgroup of $G$ if and only if there exists a non-zero vector $(\lambda_1, \ldots, \lambda_t; \mu_1, \ldots, \mu_n)$ in $F^{t+n}$ such that

\[
\begin{pmatrix}
(\lambda_1, \ldots, \lambda_t)A = (\mu_1, \ldots, \mu_n)(1-X) \\
(\lambda_1, \ldots, \lambda_t)B = (\mu_1, \ldots, \mu_n)(1-Y)
\end{pmatrix}
\]

This is equivalent to saying that there exist elements $\tilde{X}$ and $\tilde{Y}$ in $G$ such that $\langle \tilde{X}, \tilde{Y} \rangle = G$ with the property that $\tilde{X}$ maps to $x$ and $\tilde{Y}$ maps to $y$ under the projection from $G$ to $H$ if and only if there exist $t \times n$ matrices $A$ and $B$ with

\[
\text{rank} \begin{pmatrix} 1-X & 1-Y \\ A & B \end{pmatrix} = n + t.
\]

From this it immediately follows that $G$ cannot be generated by 2 elements if $t > n$ (hence $\omega(G) = 1$ in this case). Notice also that if $X$ and $Y$ are two $n \times n$ matrices generating the matrix group $H$, then the linear map $\alpha : F^n \to F^n \times F^n, w \mapsto (w(1-X), w(1-Y))$ is injective (if $w \in \ker \alpha$, then $wx = wY = w$ against the fact that $X$ and $Y$ generate a non-trivial irreducible group); the matrix $(1-X \ 1-Y)$ has rank $n$, and so it is possible to find $A$ and $B$ satisfying (1) whenever $t \leq n$. Hence $3 \leq \omega(V^n \rtimes H) \leq \omega(G)$ whenever $t \leq n$. The case $t = n$ is of special importance. In this case our observations yield

**Proposition 2.2.** Let $t = n$. Assume that $X_1, \ldots, X_\omega$ pairwise generate $H$. Then there exist elements $\tilde{X}_1, \ldots, \tilde{X}_\omega$ pairwise generating $G$ (so that for all $i$ with $1 \leq i \leq \omega$ the element $X_i$ is the projection of $\tilde{X}_i$ under the projection from $G$ to $H$) if and only if there exist $n \times n$ matrices $A_1, \ldots, A_\omega$ such that for all $i$ and $j$ with $1 \leq i < j \leq \omega$ we have

\[
\det \begin{pmatrix} 1-X_i & 1-X_j \\ A_i & A_j \end{pmatrix} \neq 0.
\]

From now on let $H$ be a nilpotent finite group that can be generated by 2 elements with an irreducible (but not necessarily faithful) action $\rho : H \to GL(V)$. Let $F = \text{End}_H(V)$ and let $n = \text{dim}_F(V)$. The Sylow subgroups of $H$ are either cyclic or non-cyclic and 2-generated. Let $\pi_1$ be the set consisting of those prime divisors of $|H|$ whose corresponding Sylow subgroups are not cyclic, and let $\pi_2$ be the set of all other prime divisors of $|H|$. Let $p$ be the smallest prime in $\pi_1$. (If $\pi_1 = \emptyset$, then set $p = \infty$.) We can find two generators $x$ and $y$ of $H$ such that $|x|$ is divisible only by primes in $\pi_1$ (if $\pi_1 = \emptyset$ we take $x = 1$. Let $X = x^u, Y = y^v$, and $u = \min(p, |V|)$. Clearly $\sigma(V^t \rtimes H^p) \leq u + 1$.

**Proposition 2.3.** With the notation and assumptions above we have $\omega(V^t \rtimes H^p) = u + 1$ if $t \leq n$ and $\omega(V^t \rtimes H^p) = 1$ otherwise.
Proof. By our observations above, to prove Proposition 2.3 it is sufficient to show that \( u + 1 \leq \omega(V^n \rtimes H^\rho) \). To see this it is sufficient to verify that there exist \( A, B_0, \ldots, B_{u-1} \in V^n \) such that the elements \( X, YB_0, XYB_1, X^2YB_2, \ldots, X^{u-1}YB_{u-1} \) pairwise generate \( V^n \rtimes H^\rho \).

We need to consider two different cases.

Case 1: \( X \neq 1 \).

Notice that \( Z(H^\rho) \leq (\text{End}_H(V))^* \); hence \( Z(H^\rho) \) is a subgroup of \( F^* \). This implies

- \( |X| \) divides \( |F| - 1 \) (in particular \( p \leq |F| - 1 \));
- for any \( h \in H \), \( V \) is a completely reducible \( \langle h \rangle \)-module (indeed any prime divisor of \( |H^\rho| \) divides \( |Z(H^\rho)| \), and hence it is coprime with \( |F| \)).

The second remark implies that we may write \( x \) in the form

\[
X = \begin{pmatrix} 1 & 0 \\ 0 & C \end{pmatrix},
\]

where 1 denotes the identity \( \ell \times \ell \) matrix for some non-negative integer \( \ell \) with \( \ell < n \) and \( C \) is an invertible \((n - \ell) \times (n - \ell)\) matrix which does not admit 1 as an eigenvalue. Decompose \( Y \) and \( 1 - Y \) as block matrices in the following way:

\[
Y = \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix}
\]

and

\[
1 - Y = \begin{pmatrix} T_1 - Y_1 \\ T_2 - Y_2 \end{pmatrix},
\]

where \( Y_1 \) and \( T_1 - Y_1 \) denote the matrices consisting of the first \( \ell \) rows of \( Y \) and \( 1 - Y \) respectively and \( Y_2 \) and \( T_2 - Y_2 \) denote the matrices consisting of the remaining rows of \( Y \) and \( 1 - Y \) respectively. Since

\[
\text{rank}(1 - X, 1 - Y) = \text{rank} \begin{pmatrix} 0 & T_1 - Y_1 \\ 1 - C & T_2 - Y_2 \end{pmatrix} = n
\]

we deduce that \( \text{rank}(T_1 - Y_1) = \ell \). Let \( D \) be an \((n - \ell) \times n\) matrix such that

\[
\det \begin{pmatrix} T_1 - Y_1 \\ D \end{pmatrix} \neq 0.
\]

By Theorem 2.2 we look for \( A, B_0, \ldots, B_{p-1} \) such that

\[
\det \begin{pmatrix} 1 - X & 1 - X^rY \\ A & B_r \end{pmatrix} \neq 0 \quad \text{and} \quad \det \begin{pmatrix} 1 - X^sY & 1 - X^sY \\ B_r & B_s \end{pmatrix} \neq 0
\]

for all \( r \) and \( s \) such that \( 0 \leq r \leq s \leq p - 1 \). Since \( p \) divides \( |F| - 1 \), there exist \( p \) pairwise distinct elements \( b_0, \ldots, b_{p-1} \in F^* \). Consider the following \( p \times p \) matrices:

\[
A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B_i = \begin{pmatrix} b_iY_1 \\ D \end{pmatrix}
\]

for all \( i \) with \( 0 \leq i \leq p - 1 \), where 1 in the definition of \( A \) denotes the \( \ell \times \ell \) identity matrix. We prove that \( A, B_0, \ldots, B_{p-1} \) are the matrices we are looking for. Notice that

\[
X^rY = \begin{pmatrix} Y_1 \\ C^rY_2 \end{pmatrix};
\]
hence
\[
\det \begin{pmatrix}
1 - X & 1 - X'Y \\
A & B_r
\end{pmatrix} = \det \begin{pmatrix}
0 & 0 & T_1 - Y_1 \\
0 & 1 - C & * \\
1 & 0 & * \\
0 & 0 & D
\end{pmatrix}
\]
\[
= \pm \det(1 - C) \det \begin{pmatrix}
T_1 - Y_1 \\
D
\end{pmatrix} \neq 0.
\]

On the other hand, if \( r \neq s \), then
\[
\det \begin{pmatrix}
1 - X'Y & 1 - X^sY \\
B_r & B_s
\end{pmatrix} = \det \begin{pmatrix}
1 - X'Y & X^sY - X^sY \\
B_r & B_s - B_r
\end{pmatrix}
\]
\[
= \det \begin{pmatrix}
T_1 - Y_1 & * \\
(b_s - b_r)Y_1 & D
\end{pmatrix} \det \begin{pmatrix}
(C^r - C^s)Y_2 \\
(b_s - b_r)Y_1
\end{pmatrix}
\]
\[
= (b_s - b_r) \det(C^r - C^s) \det(T_1 - Y_1) \det(Y_2, Y_1),
\]

which is non-zero if and only if \( \det(C^r - C^s) = \det(C^r(1 - C^s-r)) \neq 0 \). To show that the matrix \( 1 - C^s-r \) is non-singular it is sufficient to see that 1 is not an eigenvalue of \( C^s-r \). Since \( V \) is a completely reducible \( F(X) \)-module, \( C \) can be diagonalised over a suitable field extension of \( F \). Let \( \beta \) be an arbitrary eigenvalue of \( C^s-r \). Then \( \beta = \gamma^s-r \) for some eigenvalue \( \gamma \) of \( C \). Now \( \gamma \) is different from 1 by our choice of \( C \). Finally since \( 0 < s - r < p \) and since no prime smaller than \( p \) divides \( |X| \) we see that \( \gamma^s-r \) cannot be 1. This settles Case 1.

Case 2: \( X = 1 \).

In this case \( H^p = \langle X \rangle \) is a cyclic group and \( V \) is an absolutely irreducible \( FH \)-module. Hence \( V = F \) and \( n = 1 \). We have \( u \leq |F| \) and if \( 0 \neq A \in V \) and \( B_0, B_1, \ldots, B_{u-1} \) are distinct elements of \( V \), then, by Proposition 2.1, \( A, YB_0, YB_1, \ldots, YB_{u-1} \) pairwise generate \( V \triangleleft H^p \). This proves Proposition 2.3. \( \square \)

Let \( G \) be a finite solvable group, and let \( A \) be a set of representatives for the irreducible \( G \)-groups that are \( G \)-isomorphic to a complemented chief factor of \( G \). For \( A \in A \), let \( R_G(A) \) be the smallest normal subgroup contained in \( C_G(A) \) with the property that \( C_G(A)/R_G(A) \) is \( G \)-isomorphic to a direct product of copies of \( A \) and it has a complement in \( G/R_G(A) \). The factor group \( C_G(A)/R_G(A) \) is called the \( A \)-crown of \( G \). The non-negative integer \( \delta_G(A) \) defined by \( C_G(A)/R_G(A) \cong_G A^{\delta_G(A)} \) is called the \( A \)-rank of \( G \) and it coincides with the number of complemented factors in any chief series of \( G \) that are \( G \)-isomorphic to \( A \). If \( \delta_G(A) \neq 0 \), then the \( A \)-crown is the socle of \( G/R_G(A) \). The notion of crown was introduced by Gaschütz in [7].

**Proposition 2.4.** Let \( G \) and \( A \) be as above. Let \( x_1, \ldots, x_u \) be elements of \( G \) such that \( \langle x, \ldots, x, R_G(A) \rangle = G \) for any \( A \in A \). Then \( \langle x_1, \ldots, x_u \rangle = G \).

**Proof.** Let \( H = \langle x_1, \ldots, x_u \rangle \) and suppose that \( HR_G(A) = G \) for any \( A \in A \). There exists a normal subgroup \( N \) of \( G \) of minimum order with respect to the property \( HN = G \). Assume by contradiction that \( N \neq 1 \) and choose \( M \) such that \( A = N/M \) is a chief factor of \( G \). Since \( HM \neq G \), we have that \( A \) is a complemented chief factor and \( (HM/M)(R_G(A)M/M) = G/M = (HM/M)(N/M) \). By Proposition 11
of [5] and the fact that $R_{G/M}(A) = R_G(A)M/M$, we deduce $HM = G$, against the choice of $N$.\[\]

Let $d(X)$ denote the minimal number of generators of the finite group $X$.

**Proposition 2.5.** Let $G$ be a finite group of Fitting height equal to 2. If $d(G) = 2$, then $\omega(G) = \sigma(G)$.

**Proof.** Clearly we may assume that the Frattini subgroup Frat$(G)$ of $G$ is trivial. Then the Fitting subgroup Fit$(G)$ coincides with the direct product of the minimal normal subgroups of $G$ (see [13, 5.2.13]). So we have that $V$ be the subgroup of Fit$(G)$ generated by the non-central minimal normal subgroups of $G$. Now $V$ is an abelian normal subgroup of a finite group with trivial Frattini subgroup, so $V$ is complemented in $G$ (see [13, 5.2.13]). So we have that $G = V \times H$ for some nilpotent group $H$ with $d(H) \leq 2$. Let $Z$ be the set of $G$-irreducible modules $G$-isomorphic to some factor of $V$. We have that $V = \prod_{M \in Z} V_M$, where $V_M$ is the product of the minimal normal subgroups $G$-isomorphic to $M$. If $M \in Z$ and $\rho_M : H \to GL(M)$ is the action of $H$ on $M$, then $R_G(M) = C_H(M) \times \prod_{M \notin Z, L \neq M} V_L$ and $G/R_G(M) \cong V_M \times H^{\rho_M} = M^{t_M} \rtimes H^{\rho_M}$ for some positive integer $t_M$. Notice that $d(M^{t_M} \rtimes H^{\rho_M}) \leq 2$ for all $M \in Z$.

For the finite nilpotent group $H$ choose $p$, $x$, and $y$ as in the preceding paragraph of the statement of Proposition 2.3. Put $\tau = \min_{M \in Z} \{|M|\}$. (Note that $Z \neq \emptyset$, for otherwise $V = 1$ and $G = H$ is nilpotent.) Then $\sigma(G) = 1 + \min\{\tau, p\}$. Put $\sigma = \sigma(G)$. By Proposition 2.3, for any $M \in Z$ there exist $A_M$, $B_{0,M}, \ldots, B_{\sigma - 2,M}$ such that the $\sigma$ elements $x^{\rho_M}A_M, y^{\rho_M}B_{0,M}, \ldots, (x^{\sigma - 2}y)^{\rho_M}B_{\sigma - 2,M}$ pairwise generate $M^{t_M} \rtimes H^{\rho_M}$. Put

$$a = \prod_{M \in Z} A_M, \text{ and } b_i = \prod_{M \in Z} B_{i,M}$$

for all $i$ such that $0 \leq i \leq \sigma - 2$. Finally consider the set

$$\Omega = \{xa, yb_0, xyb_1, \ldots, x^{\sigma - 2}yb_{\sigma - 2}\}.$$ 

We claim that two distinct elements $\omega_1, \omega_2$ of $\Omega$ generate $G$. Indeed, take $M \in \mathcal{A}$. If $G$ centralizes $M$, then $V \leq R_G(M)$; otherwise $M \in Z$. In both cases $\langle \omega_1, \omega_2, R_G(M) \rangle = G$; hence, by Proposition 2.4, we have $\langle \omega_1, \omega_2 \rangle = G$. This proves Proposition 2.5. \[\]

We are now in the position to prove Theorem 1.1. Let $G$ be as in the statement of Theorem 1.1. If $d(G) > 2$, then $\Gamma(G)$ is the empty graph and so $\omega(G) = \chi(G) = 1$. So assume that $d(G) \leq 2$. If the Frattini subgroup of $G$ is denoted by Frat$(G)$, then $\omega(G) = \omega(G/\text{Frat}(G))$ and $\chi(G) = \chi(G/\text{Frat}(G))$. Moreover, if $G$ is non-cyclic, then $\sigma(G) = \sigma(G/\text{Frat}(G))$. Hence we may assume that Frat$(G) = 1$.

Let $G$ be cyclic. Since Frat$(G) = 1$, the cyclic group $G$ is the direct product of say $t$ cyclic groups of distinct prime orders. Let $S$ be the set of generators of $G$. In the graph $\Gamma(G)$ every vertex in $S$ is connected to every other vertex in $\Gamma(G)$. Thus, if $\Gamma(G) \setminus S$ denotes the graph obtained from $\Gamma(G)$ by removing all vertices from $S$ together with all edges having an endpoint in $S$, then $\omega(G)$ equals the maximum size of a complete subgraph in the graph $\Gamma(G) \setminus S$ plus $|S|$, and $\chi(G)$ equals the
chromatic number of the graph \( \Gamma(G) \setminus S \) plus \(|S|\). Now \( G \) has \( t \) maximal subgroups each of which is cyclic. We may choose a generator from each of these maximal subgroups. Since any distinct pair of these elements generate \( G \), we have a complete subgraph of size \( t \) in the graph \( \Gamma(G) \setminus S \). On the other hand, the graph \( \Gamma(G) \setminus S \) can be expressed as the union of \( t \) empty subgraphs (coming from the \( t \) maximal subgroups of \( G \)); hence it is \( t \)-colorable and so the chromatic number of \( \Gamma(G) \setminus S \) is at most \( t \). These observations yield \( t + |S| \leq \omega(G) \leq \chi(G) \leq t + |S| \); hence \( \omega(G) = \chi(G) \).

We may now also assume that \( d(G) = 2 \). Also, by Proposition 2.5 we assume that \( G \) is nilpotent. Then, since Frat\((G) = 1\), we have \( G = C \times N_{p_1} \times \ldots \times N_{p_t} \), for some positive integer \( t \), where \( p_1 < \ldots < p_t \) are distinct primes, \( N_{p_j} = C_{p_j} \times C_{p_j} \), for all \( j \) with \( 1 \leq j \leq t \), and \( C \) is a cyclic group that is a direct product of cyclic groups of prime orders different from \( p_j \) for \( j \) with \( 1 \leq j \leq t \). Let \( N \) be the normal subgroup of \( G \) for which \( G/N \cong N_{p_1} = C_{p_1} \times C_{p_1} \). Then \( \sigma(G) \leq \sigma(G/N) \leq p_1 + 1 \).

For each \( j \) with \( 1 \leq j \leq t \) let \( a_{1,j}, a_{2,j}, \ldots, a_{p_{j+1},j} \) be non-identity elements from \( N_{p_j} \) generating distinct cyclic subgroups in \( N_{p_j} \). Let \( c \) be a generator from \( C \). For any \( i \) with \( 1 \leq i \leq p_1 + 1 \) let \( a_i \) be the element \((c, a_{i,1}, \ldots, a_{i,t})\) from \( G \). Clearly, \( \{a_1, \ldots, a_{p_1+1}\} \) spans a complete subgraph in \( \Gamma(G) \). Hence \( p_1 + 1 \leq \omega(G) \leq \sigma(G) \leq p_1 + 1 \), that is, \( \omega(G) = \sigma(G) \).

3. DIRECT PRODUCTS OF NON-ABELIAN SIMPLE GROUPS

In this section we prove Theorem 1.2.

Our first result (Proposition 3.1) was also proved (independently) by Abdollahi and Jafarian Amiri in [1].

**Proposition 3.1.** Let \( S \) be a non-abelian finite simple group. Then for any positive integer \( n \) we have \( \sigma(S^n) = \sigma(S) \), where \( S^n \) denotes the direct product of \( n \) copies of \( S \).

**Proof.** The inequality \( \sigma(S^n) \leq \sigma(S) \) follows at once from the observation that if \( \{M_i\} \) is a set of proper subgroups of \( S \) with \( S = \bigcup_i M_i \), then \( \{M_i \times S^{n-1}\} \) is a set of proper subgroups of \( S^n \) with \( S^n = \bigcup_i (M_i \times S^{n-1}) \).

Let \( \{Y_1, \ldots, Y_t\} \) be a set of proper subgroups of \( S^n \) such that \( S^n = \bigcup_{i=1}^t Y_i \). Suppose also that \( \tau \) is as small as possible (that is, \( \tau = \sigma(S^n) \)). Put \( \sigma = \sigma(S) \). We need to show that \( \sigma \leq \tau \).

We may assume that the \( Y_i \)'s are maximal subgroups of \( S^n \). What are the maximal subgroups of \( S^n \)? They are of the following two kinds:

- Product type: \( P_{M,i} = \{(x_1, \ldots, x_n) \in S^n \mid x_i \in M\} \), where \( M \) is a maximal subgroup of \( S \);
- Diagonal type: \( D_{i,j,\phi} = \{(x_1, \ldots, x_n) \mid x_j = x_i^\phi \} \), where \( \phi \in \text{Aut}(S) \).

 Without loss of generality assume that \( Y_i \) is of product type if \( i \leq a \) and \( Y_i \) is of diagonal type if \( a < i \leq \tau \) for some non-negative integer \( a \) at most \( \tau \). We may assume that \( a < \sigma \) for otherwise \( \sigma \leq a \leq \tau \) in which case we are done.

Let \( I \) be the set of those indices \( i \) with \( 1 \leq i \leq n \) for which there exists a maximal subgroup \( M \) of \( S \) and an index \( j \) with \( 1 \leq j \leq a \) such that \( Y_j = P_{M,i} \). For every \( i \in I \) let \( \mathcal{M}_i \) be the set of those maximal subgroups \( M \) of \( S \) for which there exists an index \( j \) with \( 1 \leq j \leq a \) such that \( Y_j = P_{M,i} \). Define \( \Omega_i = S \setminus \bigcup_{M \in \mathcal{M}_i} M \). Note that \( \Omega_i \) has cardinality at least \( \sigma - a \). Now for each index \( j \) with \( 1 \leq j \leq n \), let \( \Delta_j \) be a subset of \( S \) of cardinality \( \sigma - a \) with the property that \( \Delta_i \subseteq \Omega_i \) whenever
Let $S$ be a non-abelian finite simple group. Define $\delta = \delta(S)$ to be the largest positive integer $r$ such that $S^r$, the direct product of $r$ copies of $S$, can be generated by 2 elements. (The positive integer $\delta$ is well-defined. To see this, first note that it is known that every non-abelian finite simple group can be generated by 2 elements. Also, for any positive integer $d$, the group $S^d$ cannot be generated by $d$ elements whenever $r$ is larger than the number of $\text{Aut}(S)$-orbits on the set of $d$-tuples generating $S$. This latter claim follows from the combination of the definition of a maximal subgroup of product type and the Pigeonhole Principle.)

Let us denote $S^d$ by $G$. (Actually, $\delta$ is equal to the number of $\text{Aut}(S)$-orbits on ordered pairs of generators for $S$, and for arbitrary elements $x = (x_1, \ldots, x_6)$ and $y = (y_1, \ldots, y_6)$ of $G$ we have that $G = \langle x, y \rangle$ if and only if the pairs $(x_i, y_i)$ are distinct representatives for these orbits for $i$ with $1 \leq i \leq \delta$.)

Consider $A = \text{Aut}(G) \cong \text{Aut}(S) \rtimes \text{Sym}(\delta)$ and let $(x, y)$ be a fixed pair of generators for $G$ with $x = (x_1, \ldots, x_6)$ and $y = (y_1, \ldots, y_6)$, where the $x_i$'s and $y_i$'s are elements of $S$. Since $(x, y) = G$, the elements $(x_1, y_1), \ldots, (x_6, y_6)$ form a set of representatives for the $\text{Aut}(S)$-orbits of the set of generating pairs for $S$. From this it is easy to see that $G$ has the following relevant property: $(P)$ if $G = \langle x, y \rangle$, then there exists $a \in A$ with $(x, y) = (x^a, y^a)$.

Now we can define a graph $\Gamma$ in which the set of vertices $V$ is the set of all $A$-conjugates of $x$ and two vertices $\bar{x}_1$, $\bar{x}_2$ are connected by an edge if and only if $G = \langle \bar{x}_1, \bar{x}_2 \rangle$. Note that $\Gamma$ is obtained from $\Gamma(G)$ just by removing all isolated vertices. By property $(P)$, the graph $\Gamma$ is vertex-transitive and edge-transitive. Let $\alpha = |A|$, $C = C_A(x)$, and $\gamma = |C|$. The number of vertices in $V$ is $\alpha/\gamma$, and the number of edges in $\Gamma$ is $\alpha/2$ (since the action of $A$ on the pairs of generators is regular and 2 in the denominator comes from the fact that the edges of $\Gamma$ are unoriented).

In the remainder of this section we wish to give an upper bound for $\omega(G)$ which is precisely the clique number of $\Gamma$.

We will use Corollary 4 of [4] which states that if $X$ is a clique and $Y$ a coclique (an empty subgraph) in a vertex-transitive graph on $m$ vertices, then $|X||Y| \leq m$.

We also need a definition. Let $s$ be an element of $S$ and let $\omega(s)$ be the number of indices $i$ with $1 \leq i \leq \delta$ such that $x_i$ and $s$ are $\text{Aut}(S)$-conjugate. We have $\omega(s) = \rho(s)/|C_{\text{Aut}(S)}(s)|$, where $\rho(s)$ is the number of elements $t$ in $S$ such that $\langle s, t \rangle = S$ (this is because for any $t$ with $\langle s, t \rangle = S$ there exists a unique index $i$ with $1 \leq i \leq \delta$ and a unique automorphism $a \in \text{Aut}(S)$ such that $(s^a, t^a) = (x_i, y_i)$).

Now take $M$ to be a maximal subgroup of $S$ and put

$$Y_M = \{ v = (z_1, \ldots, z_6) \in V \mid \pi_1(v) = z_1 \in M \},$$

where $\pi_1$ is the natural projection from $G$ to the first direct factor. Since $Y_M$ is a coclique in $\Gamma$ we have $\omega(G) \leq |V|/|Y_M|$.

For any $z \in M$ with $z \neq 1$ there exists a vertex $v_z$ in $V$ such that $\pi_1(v_z) = z$. (This follows from the corollary on page 745 of [5], which states that any non-trivial element of a finite almost simple group $G$ belongs to a pair of elements
generating at least the socle of $G$.) Other vertices $v$ with the property that $\pi_1(v) = z$ can be obtained by conjugating $v_z$ by automorphisms from the subgroup $\overline{A} \cong \operatorname{Aut}(S) \wr \operatorname{Sym}(\delta - 1)$ of $A$. So if we define $C_z$ to be $C_{\overline{A}}(v_z)$, then we obtain

$$\sum_{z \in M, z \neq 1} \frac{|\overline{A}|}{|C_z|} \leq |Y_M|.$$ 

This implies

$$\omega(G) \leq \frac{|V|}{\sum_{z \in M, z \neq 1} \frac{|A|}{|C_z|}} = \left( \sum_{z \in M, z \neq 1} \frac{|\overline{A}||C|}{|A||C_z|} \right)^{-1}.$$ 

Clearly $|A|/|\overline{A}| = \delta|\operatorname{Aut}(S)|$. Now assume that $\{u_1, \ldots, u_l\}$ is a set of representatives for the orbits of the action of $\operatorname{Aut}(S)$ on $S \setminus \{1\}$. For $C = C_{\overline{A}}(x)$ we have

$$C \cong \prod_{i=1}^l C_{\operatorname{Aut}(S)}(u_i) \wr \operatorname{Sym}(\omega(u_i)).$$

On the other hand, if $z \in u_j^{\operatorname{Aut}(S)}$, we have

$$C_z \cong \left( \prod_{i \neq j} C_{\operatorname{Aut}(S)}(u_i) \wr \operatorname{Sym}(\omega(u_i)) \right) \times \left( C_{\operatorname{Aut}(S)}(u_i) \wr \operatorname{Sym}(\omega(u_i) - 1) \right).$$

It follows that $|C|/|C_z| = |C_{\operatorname{Aut}(S)}(z) : \omega(z)| = \rho(z)$ and

$$\omega(G) \leq \left( \sum_{z \in M, z \neq 1} \frac{\rho(z)}{|\operatorname{Aut}(S)|\delta} \right)^{-1}.$$ 

Note that $|\operatorname{Aut}(S)|\delta$ is the number of ordered pairs $(s, t)$ generating $S$, while $\sum_{z \in M, z \neq 1} \rho(z)$ is the number of ordered pairs $(s, t)$ generating $S$ such that $s \in M$. So if we define $P_M$ to be the conditional probability that $(s, t) \in M \times S$ given that $(s, t) = S$, then $\omega(G) \leq 1/P_M$. We may also write $P_M$ in the form

$$P_M = \frac{P(x, y) = S \mid x \in M \cdot P(x \in M)}{P(x, y) = S} \geq P(x, y) = S \mid x \in M \cdot \frac{|M|}{|S|},$$

where $Q_M = P(x, y) = S \mid x \in M$ is the conditional probability that the ordered pair $(x, y)$ generates $S$ given that $x \in M$, where $P(x \in M) = |M|/|S|$ is the probability that $x \in M$ and where $P((x, y) = S)$ is the probability that the ordered pair $(x, y)$ generates $S$. Clearly, $\omega(G) \leq 1/P_M \leq |S : M|/Q_M$. We need a lower bound for $Q_M$. In what follows $m(S)$ denotes the minimal index of a proper subgroup in $S$.

**Proposition 3.2.** Let $M \leq S$ with $|S : M| = m(S)$. Then $1 - O(m(S)^{-1/15}) \leq Q_M$. Moreover if $S = \operatorname{Alt}(n)$, then $1 - O(n^{-1}) \leq Q_M$.

**Proof.** If $(m, s) \in M \times S$, then $(m, s) \neq S$ if and only if $(m, s) \in (K \cap M) \times K$ for some maximal subgroup $K$ of $S$. This allows us to deduce

$$1 - \sum_K \frac{1}{|S : K||M : K \cap M|} \leq Q_M,$$

where $K$ runs through the set of maximal subgroups of $S$. 
Now use the notation of Section 6 of [9]. There exist positive real numbers \( \delta \) and \( b \) with \( \delta > 1 \) such that the set \( \mathcal{A} \) of maximal subgroups whose index is smaller than \( b \cdot m(S)^{\delta} \) is known (and \( |\mathcal{A}| \) is “small”). The values of \( \delta \) and \( b \) together with the description of \( \mathcal{A} \) are given in [9] when \( S = \text{Alt}(n) \) and \( n \) is large enough, then any subgroup of \( \text{Alt}(n) \) different from a point-stabilizer has index at least \( n(n-1)/2 \), so for any \( \delta \) with \( 1 < \delta \leq 2 \) there exists \( b > 0 \) with the property that any maximal subgroup of \( \text{Alt}(n) \) with index smaller than \( b \cdot n^{\delta} \) is a point-stabilizer. By [9], we may take \( \delta = 16/15 \) if \( S \) is a group of Lie type, and, by the remarks above, we may take \( \delta = 2 \) if \( S \) is an alternating group. Let \( \mathcal{B} \) be the set of those maximal subgroups of \( S \) which do not belong to \( \mathcal{A} \). Note that

\[
\frac{1}{|S : K||M : K \cap M|} \leq \frac{m(S)}{|S : K|^2}.
\]

We will make use of the identity

\[
\sum_{K \in \mathcal{B}} |S : K|^{-2} = O(m(S)^{-\delta}),
\]

which, for exceptional groups \( S \) of Lie type, is found in line 2 of the proof of Lemma 6.7 in [9], and which, for classical groups \( S \), follows from Theorem 3.1 of [10] by noting that we may replace 2 by \( \delta \) since \( \delta \leq 2 \). This implies

\[
\sum_{K \in \mathcal{B}} |S : K|^{-1} |M : K \cap M|^{-1} = O(m(S)^{-\delta+1}).
\]

Hence

\[
1 - \sum_{K \in \mathcal{A}} \frac{1}{|S : K||M : K \cap M|} - O(m(S)^{-\delta+1}) \leq Q_M.
\]

Now let \( \{K_1, \ldots, K_t\} \) be a set of representatives for the \( S \)-conjugacy classes of all members of \( \mathcal{A} \). For every \( i \) with \( 1 \leq i \leq t \) let \( s_i \) be the number of \( M \)-orbits on the coset space \( (S : K_i) \). Note (see the proof of Lemma 6.10 in [9]) that for every \( i \) with \( 1 \leq i \leq t \) we have

\[
\sum_{K \in K_i^\p} \frac{1}{|S : K||M : K \cap M|} = \frac{s_i}{|S : K_i|} \leq \frac{s_i}{m(S)}.
\]

We conclude that

\[
1 - \sum_{i=1}^{t} \frac{s_i}{m(S)} - O(m(S)^{-\delta+1}) \leq Q_M.
\]

We now have to show that \( \sum_{i=1}^{t} s_i \) is “small”. If \( S \) is a group of Lie type, then, by [9], \( t \leq 3 \) and either \( s_i \leq 3 \) for all \( i \) with \( 1 \leq i \leq t \) or \( S = \text{PO}_{2m}^{+}(q) \) in which case there exists a constant \( c_1 \) such that \( s_i \leq c_1 q \) for all \( i \) with \( 1 \leq i \leq t \) (see the last part of the proof of Lemma 6.7 in [9]). Finally, if \( S = \text{Alt}(n) \) and \( n \neq 6 \), then \( t = 1 \) and \( s_1 \) is the number of orbits of the point-stabilizer \( M \) on the coset space \( (S : K_1) \) where \( K_1 \) is another point-stabilizer. In this case \( s_1 = 2 \) since \( \text{Alt}(n) \) is 2-transitive. By these remarks and by inequality (2), we get

\[
1 - O(m(S)^{-\delta+1}) \leq Q_M,
\]

which is exactly what we wanted. \( \square \)
By the inequality $\omega(G) \leq |S : M|/Q_M$ and by Proposition 3.2, we conclude that $\omega(G) \leq m(S) + O(m(S)^{14/15})$ if $S$ is a finite simple group of Lie type and $\omega(G) \leq m(S) + O(1)$ otherwise. Now let $S = \text{Alt}(n)$. Then, by Proposition 3.1, we have $2^{n-2} \leq \sigma(S)$ unless $n = 7$ or $9$. Hence, by Proposition 3.2, $2^{n-2} \leq \sigma(G)$ unless $n = 7$ or $9$. From this it follows that $\omega(G)/\sigma(G) \leq (n + O(1))/2^{n-2}$. The proof of Theorem 1.2 is now complete.

REFERENCES


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

Institute of Mathematics, Hungarian Academy of Sciences, Réaltanoda utca 13-15, H-1053, Budapest, Hungary
E-mail address: maroti@renyi.hu

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use