Some results and questions related to the generating graph of a finite group

Andrea Lucchini

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

Attila Maróti

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences,
Reáltanoda utca 13-15,
H-1053, Budapest, Hungary
E-mail: maroti@renyi.hu and
Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113, U.S.A.
E-mail: maroti@usc.edu

To the memory of Maria Silvia Lucido.

1. Introduction

For a finite group G a graph $\Gamma(G)$ is defined on the elements of G in such a way that two distinct vertices are connected by an edge if and only if they generate G. Some results and questions are given about $\Gamma(G)$. This article is much focused on the relationship between two invariants associated to the graph $\Gamma(G)$: the clique number (the size of a largest complete subgraph

2

in the graph) and the chromatic number (the least number of colors needed to color the vertices of the graph in such a way that the endpoints of every edge receive different colors). For G a non-cyclic 2-generated group a third invariant associated to G is also of importance: the least cardinality of a set of proper subgroups whose union is G.

Section 2 gives some background and motivation for the study of minimal covers of finite groups. The case of solvable groups is highlighted. Section 3 introduces the commuting graph of a finite group. Among other things a result of Pyber is mentioned in order to motivate our investigations of the above-mentioned three invariants associated to G (or $\Gamma(G)$). In Section 4 a recent result of Breuer, Guralnick, Kantor is stated about the structure of $\Gamma(G)$ for G a non-Abelian finite simple group. Also, a theorem of Lucchini and Maróti is mentioned about $\Gamma(G)$ where G is a finite group of Fitting height at most 2. Section 5 gives background and motivation for the study of the clique and chromatic numbers of $\Gamma(G)$ for G a finite solvable group. Questions and results are presented. Algebraic and combinatorial aspects of the general problem are revealed. Investigations in Section 5 lead to a graph $\Gamma(R)$ defined on the elements of an Artinian ring R in such a way that vertices r and s are connected by an edge if and only if $r - s$ is invertible. In Section 6 it is proved that the clique and chromatic numbers of $\Gamma(R)$ are equal. Section 7 concerns various kinds of arc transitive graphs which come up naturally in investigations of the graph $\Gamma(G)$. Turán graphs, Kneser graph, q-Kneser graphs and other arc transitive graphs are considered. Some questions are given. Section 8 is centered around the case of the symmetric group. A proof of Blackburn introduced the probabilistic method to this subject via the Lovász Local Lemma. Blackburn's proof is not sketched however motivation and background is presented along with two questions. In Section 9 further useful combinatorial tools (König's, Hall's, and Haxell's theorems) and group theoretic theorems are given. Section 10 is somewhat independent from other material in this article. However it is related to the general problem of Section 5 and it weakly relies on results in Section 9. In Section 10 the clique numbers of the graphs $\Gamma(G)$ are considered for various affine groups G.

2. Covering groups with proper subgroups

No group is the union of two proper subgroups. Scorza [37] showed that a group G is the union of three proper subgroups if and only if the Klein

four group is a factor group of G. By a result of Neumann [35], if G is the union of finitely many proper subgroups then the intersection of all these subgroups is a subgroup of finite index in G. This lead to the following definition. For a non-cyclic group G let $\sigma(G)$ be the least cardinality of proper subgroups whose union is G.

Cohn [9] was the first mathematician to study the invariant σ systematically. He described all groups G with $\sigma(G) = 4$, 5, and 6. By answering two of Cohn's questions, Tomkinson [39] showed that there is no group G with $\sigma(G) = 7$ and that for every finite solvable group G we have $\sigma(G) = q + 1$ where q is the minimal size of a chief factor of G that has more than one complement. Recently Bhargava [1] proved that for every positive integer n there exists a finite (possibly empty) set of finite groups $S(n)$ such that $\sigma(G) = n$ if and only if G has a factor group in $S(n)$ but does not have a factor group in $S(m)$ for $m < n$. Even more recently, answering a question of Tomkinson [39], Detomi and Lucchini [10] showed that there is no group G with $\sigma(G) = 11$.

The function $\sigma(G)$ was much investigated for various non-solvable groups G (see [7], [32], [33], [20], [4]) and even for infinite groups G (see [29]).

3. The non-commuting graph

Let Γ be the commuting graph of the finite group G. This is the simple graph defined on the elements of G in such a way that two distinct vertices are connected by an edge if and only if they commute. One reason why the commuting graph Γ is important is that bounds on the number of edges in Γ give restrictions on the structure of G (see [15]). Let $\bar{\Gamma}$ be the complement of Γ. (Two vertices of $\bar{\Gamma}$ are connected if and only if they do not commute.) Let $\alpha(G)$ be the clique number (size of a largest complete subgraph) of $\bar{\Gamma}$ and let $\beta(G)$ be the chromatic number (least number of colors needed to color the vertices of the graph in such a way that for each edge in the graph the endpoints receive different colors) of $\bar{\Gamma}$. Notice that $\alpha(G)$ is the maximal size of a set of pairwise non-commuting elements in G, while $\beta(G)$ is the minimal number of Abelian subgroups of G whose union is G. Clearly, $\alpha(G) \leq \beta(G)$ (since the clique number is at most the chromatic number for any finite graph). One of our motivations is the following result.

Theorem 3.1 (Pyber, [36]). *There exists an absolute constant $c > 0$*

4

such that $\beta(G) < c^{\alpha(G)}$ for any finite group G.

This result is best possible for certain p-groups G. For $G = \mathrm{Sym}(n)$ the symmetric group of degree n, Brown [5] showed that $\alpha(G)$ and $\beta(G)$ are surprisingly close to each other, though for $n \geq 15$, they are never equal [6].

4. The generating graph

Define a graph $\Gamma(G)$ on the elements of a finite group G by connecting two vertices by an edge if and only if they generate G. We say that $\Gamma(G)$ is the generating graph of G.

For a non-Abelian finite group G the set of edges $E(\Gamma(G))$ of the generating graph $\Gamma(G)$ is a subset of the set of edges $E(\bar{\Gamma})$ of the complement of the commuting graph $\bar{\Gamma}$ of G with $E(\Gamma(G)) = E(\bar{\Gamma})$ only if G is a minimally non-Abelian group. (For an Abelian group G we have $E(\Gamma(G)) = E(\bar{\Gamma})$ only when G is not 2-generated.)

Let us mention the following deep theorem from [3] which is equivalent to saying that for a non-Abelian finite simple group G the generating graph $\Gamma(G)$ consists of two connected components: an isolated vertex and a graph of diameter equal to 2.

Theorem 4.1 (Breuer, Guralnick, Kantor, [3]). *Let G be a non-Abelian finite simple group. For every pair of non-identity elements x_1 and x_2 in G there exists a y in G so that $\langle x_1, y \rangle = \langle x_2, y \rangle = G$.*

Not much else is known about $\Gamma(G)$ for a finite group G. An alternative statement of Conjecture 1.8 of [3] is

Conjecture 4.2 (Breuer, Guralnick, Kantor, [3]). *Let G be a finite group. Then $\Gamma(G)$ has exactly 1 isolated vertex if and only if G/N is cyclic for every nontrivial normal subgroup N of G.*

A trivial observation about $\Gamma(G)$ is that it is an empty graph in case G cannot be generated by 2 elements. If $\mathrm{Frat}(G)$ denotes the Frattini subgroup of G, then $\langle x\mathrm{Frat}(G), y\mathrm{Frat}(G) \rangle = G/\mathrm{Frat}(G)$ if and only if $\langle x, y \rangle = G$ for arbitrary elements x and y in G. From this one can describe the structure of $\Gamma(G)$ for G a finite nilpotent group.

In view of Theorem 3.1 and the above-mentioned papers of Brown it is perhaps justified to introduce the following definitions. Let the clique number of $\Gamma(G)$ be $\omega(G)$ and let the chromatic number of $\Gamma(G)$ be $\chi(G)$. It is clear that $\omega(G) \leq \chi(G)$. Notice also that $\chi(G) \leq \sigma(G)$ for a non-cyclic finite group G.

It can be checked that $\omega(G) = \chi(G)$ for a finite nilpotent group G. A natural question arises: does $\omega(G) = \chi(G)$ hold for a broader class of finite groups? A group G is said to have Fitting height at most 2 if there exists a nilpotent normal subgroup N in G such that G/N is nilpotent.

Theorem 4.3 (Lucchini, Maróti, [30]). *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 $\omega(G) = \sigma(G)$.*

5. Solvable groups

We have mentioned in Section 1 that there is a formula for $\sigma(G)$ for G a finite solvable group (see [39]).

Question 5.1. Let G be a finite solvable group. Is it true that $\omega(G) = \chi(G)$? Moreover, is it true that $\omega(G) = \sigma(G)$ when the minimal number of generators of G is 2?

An affirmative answer to the second question would imply an affirmative answer to the first question of Question 5.1.

There is a serious obstacle in answering Question 5.1. Before we say what this is, we must fix some notations.

Throughout this section let us fix the following notations and assumptions. Let H be a solvable group that can be generated by 2 elements. Let K be a field of prime order and let V be an irreducible faithful KH-module. Let $F = \mathrm{End}_H(V)$ and let $n = \dim_F(V)$. We form the semidirect product $G = V^n \rtimes H$ where H acts in the same way on each of the n direct summands. (Note that G is 2-generated and in fact n is the largest positive integer t with $V^t \rtimes H$ 2-generated.)

The group G can be generated by 2 elements. One obstacle to answer Question 5.1 is to determine $\omega(G)$ provided that we know $\omega(H)$ (and maybe assume that $\omega(H) = \chi(H)$).

6

An observation in this direction is given by Proposition 5.1. Let X be an element of H. We can view X as an $n \times n$ matrix with coefficients from F.

Proposition 5.1 ([30]). *Assume that $X_1, \ldots, X_\omega$ pairwise generate H for some positive integer ω. Then there exist elements $\bar{X}_1, \ldots, \bar{X}_\omega$ pairwise generating G (so that for all i with $1 \leq i \leq \omega$ the element X_i is the projection of $\bar{X}_i$ 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*

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

For example, if H is cyclic then $n = 1$ and $G = V \rtimes H$. Since V is a chief factor in G with more than one complement, we have $\omega(G) \leq \sigma(G) \leq |V| + 1 = |F| + 1$. Let X be a generator of H and let $\omega = |F| + 1$. Put $X_1 = 1$ and $X_2 = \ldots = X_\omega = X$. Let $F = \{f_2, \ldots, f_\omega\}$. Set $A_1 = 1$ and $A_i = f_i$ for all i with $2 \leq i \leq \omega$. Then (1) holds for all i and j with $1 \leq i < j \leq \omega$. Hence, by Proposition 5.1, we have $|V| + 1 \leq \omega(G)$. This gives $\omega(G) = |V| + 1$.

In the previous example $G = V^n \rtimes H$ was a Frobenius group.

Proposition 5.2. *Suppose that H is non-cyclic. If $V \rtimes H$ is a Frobenius group, then $\omega(G) = \omega(H)$.*

Proof. Suppose that $X_1, \ldots, X_\omega$ pairwise generate H where $\omega = \omega(H)$. Let i and j be arbitrary indices with $1 \leq i \leq j \leq \omega$ and $i \neq j$. Since $V \rtimes H$ is a Frobenius group, we see that $1 - X_i$, $1 - X_j$, and $1 - X_i X_j^{-1}$ are invertible matrices. In particular, $X_j - X_i$ is invertible. Hence

$$\det \begin{pmatrix} 1 - X_i & 1 - X_j \\ 1 & 1 \end{pmatrix} \neq 0.$$

By Proposition 5.1, we conclude that $\omega \leq \omega(G) \leq \omega(H)$. $\square$

Let us continue with another example.

Theorem 5.3. *Suppose that $n > 1$. Let S be a Singer cycle acting on V and let C be a cyclic group of order n acting on V as a group of Frobenius*

automorphisms. Let H be the semidirect product of S by C. We view C as the group of automorphisms of the field extension $[V : F]$. Set $q = |F|$ and let G be as above. Then $\omega(G) = \sigma(G) = \sigma(H) = \omega(H) = p + 1$ where p denotes the smallest prime divisor of $(q^n - 1)/(q - 1)$.

Proof. Put $|F| = q$. Let a be a generator of S and b be a generator of C. Then $a^{q^n-1} = b^n = 1$ and (assume that) $b^{-1}ab = a^q$.

For each i such that $1 \leq i \leq p - 1$, let k_i be a positive integer satisfying the following two conditions: (1) $k_i \equiv i \pmod{r}$ for every prime factor r of $(q^n - 1)/(q - 1)$; (2) $k_i \equiv 1 \pmod{r}$ for every prime factor r of $q^n - 1$ with r not dividing $(q^n - 1)/(q - 1)$. (Note that the k_i's exist by the Chinese Remainder Theorem.) Define Δ to be the set $\{a, b^{-1}, a^{k_1}b^{-1}, a^{k_2}b^{-1}, \ldots, a^{k_{p-1}}b^{-1}\}$. We claim that every distinct pair of elements of Δ generates H. Let i and j be distinct integers at least 1 and at most $p - 1$. Since k_i is coprime to $q^n - 1$, the element a^{k_i} generates S and so $\langle a^{k_i}b^{-1}, a \rangle = \langle a^{k_i}b^{-1}, b^{-1} \rangle = H = \langle a, b^{-1} \rangle$. Put $M_{i,j} = \langle a^{k_i}b^{-1}, a^{k_j}b^{-1} \rangle$. To prove our claim, it is sufficient to see that $M_{i,j} = H$. Certainly, $a^{k_i - k_j} \in M_{i,j}$ and $a^{(k_i(q^n-1))/(q-1)} = (a^{k_i}b^{-1})^n \in M_{i,j}$. Hence $a^{((k_i(q^n-1))/(q-1))+(k_i-k_j)} \in M_{i,j}$. We claim that $((k_i(q^n - 1))/(q - 1)) + (k_i - k_j)$ is coprime to $q^n - 1$. Indeed, if r divides $(q^n - 1)/(q - 1)$, then r does not divide $i - j$ and so does not divide $k_i - k_j$. On the other hand, if r is a prime factor of $q^n - 1$ not dividing $(q^n - 1)/(q - 1)$, then r divides $k_i - k_j$ but does not divide k_i. Our claim implies that $a^{((k_i(q^n-1))/(q-1))+(k_i-k_j)}$ generates S, and so $S \leq M_{i,j}$. But then $\langle a, b^{-1} \rangle \leq M_{i,j}$, and so $M_{i,j} = H$. This proves $p + 1 \leq \omega(H)$.

There are two possibilities for p: the prime p divides or does not divide $q - 1$. Suppose that p divides $q - 1$. Then p must also divide n (since p divides $1 + q + \ldots + q^{n-1}$), and so $H/\langle a^p, b^p \rangle$ is an elementary Abelian p-group of order p^2. Hence $\sigma(H) \leq p + 1$. Now suppose that p does not divide $q - 1$. Then $\bar{F} = H/\langle a^p \rangle$ has a central subgroup Z of order dividing n such that $\bar{F}/Z$ is a (meta-cyclic) Frobenius group with Frobenius kernel a cyclic group of order p. In this case we also have $\sigma(H) \leq p + 1$.

So far we showed that $\omega(H) = \sigma(H) = p+1$. Since $\sigma(G) \leq \sigma(H) = p+1$, it is sufficient to show that $p + 1 \leq \omega(G)$.

Consider a matrix representation of H on V over the field F. Let the matrix associated to a be A and the matrix associated to b be B. Put $X_1 = A$, $X_2 = B^{-1}$, $X_3 = A^{k_1}B^{-1}$, $X_4 = A^{k_2}B^{-1}, \ldots, X_{p+1} = A^{k_{p-1}}B^{-1}$.

8

We must find $n \times n$ matrices $A_1, \ldots, A_{p+1}$ over F such that the matrices

$$\begin{pmatrix} 1 - X_i & 1 - X_j \\ A_i & A_j \end{pmatrix}$$

are non-singular for all i and j with $1 \leq i < j \leq p + 1$. Take $A_1 = 0$ and $A_j = X_j$ for all j with $2 \leq j \leq p + 1$. Then, for all i and j with $2 \leq i < j \leq p + 1$, the matrices

$$\begin{pmatrix} 1 - X_i & 1 - X_j \\ X_i & X_j \end{pmatrix}$$

are non-singular since the matrices $X_j - X_i$ are non-singular. Finally, for all j with $2 \leq j \leq p + 1$, the matrices

$$\begin{pmatrix} 1 - A & 1 - X_j \\ 0 & X_j \end{pmatrix}$$

are non-singular since $1 - A$ and X_j are non-singular. Hence Proposition 5.1 gives the desired conclusion. $\square$

For the rest of this section let G be a non-cyclic finite solvable group that can be generated by 2 elements. Let $m(G)$ denote the minimal index of a proper subgroup in G. If the answer to Question 5.1 is affirmative, then, by Tomkinson's theorem [39], $m(G) < \omega(G)$.

Question 5.2. Does there exist a universal positive constant c so that $c \cdot m(G) < \omega(G)$?

A proper subgroup of G induces an empty subgraph in $\Gamma(G)$. On the other hand, an empty subgraph of $\Gamma(G)$ does not necessarily correspond to a proper subgroup of G. Let H be a subgroup of G of index $m(G)$.

Question 5.3. Does there exist a universal constant c so that whenever Δ is an empty subgraph of $\Gamma(G)$ we have $|\Delta| \leq c \cdot |H|$?

An affirmative answer to Question 5.3 would imply that there is a universal positive constant c so that $c \cdot m(G) \leq \chi(G)$.

6. Artinian rings

Markus Linckelmann [26] pointed out that, in view of the various applications of Question 5.1, the following graph may be of interest. Let R be a

ring. Define a graph $\Gamma(R)$ on the elements of R by connecting vertices a and b by an edge if and only if $a - b$ is invertible (in R). Let $\omega(R)$ be the largest cardinality of a complete subgraph in $\Gamma(R)$ and let $\chi(R)$ be the least cardinality of colors needed to color the vertices of $\Gamma(R)$ in such a way that the endpoints of each edge in $\Gamma(R)$ receive different colors.

Theorem 6.1. *If R is an Artinian ring, then $\omega(R) = \chi(R)$.*

Proof. If an element x in R is invertible, then so is $x + j$ for all j in the Jacobson radical $J(R)$ of R. A consequence of this observation is that $\Gamma(R)$ can be obtained from $\Gamma(R/J(R))$ just by replacing each vertex of $\Gamma(R/J(R))$ by an empty graph of cardinality $|J(R)|$ and by replacing each edge of $\Gamma(R/J(R))$ by a cardinality of $|J(R)|^2$ edges running between the relevant two empty graphs replacing the relevant two vertices of $\Gamma(R/J(R))$. Hence $\omega(R) = \omega(R/J(R))$. It also follows that in order to show $\omega(R) = \chi(R)$, it is sufficient to see that $\omega(R/J(R)) = \chi(R/J(R))$. Since $J(R/J(R)) = 0$, we may (and do) assume from now on that $J(R) = 0$.

By the Artin-Wedderburn Theorem, R is semisimple and so it is the direct product of finitely many, say k, matrix rings $M_{n_i}(D_i)$ where the n_i's are positive integers and the D_i's are division rings. Since $\omega(R) = \min_{1 \leq i \leq k} \omega(M_{n_i}(D_i))$, it is sufficient to show that $\Gamma(R)$ can be colored using $\min_{1 \leq i \leq k} \omega(M_{n_i}(D_i))$ colors. Without loss of generality, suppose that $\omega := \omega(M_{n_1}(D_1)) = \min_{1 \leq i \leq k} \omega(M_{n_i}(D_i))$. Notice that if $\Gamma(M_{n_1}(D_1))$ can be colored by ω colors, then $\Gamma(R)$ can also be colored by ω colors. Hence, from now on, we may (and do) assume that R is isomorphic to a simple ring $M_n(D)$ for some positive integer n and division ring D.

If D is an infinite division ring, then D has the same cardinality as $M_n(D)$. In this case R is clearly $|M_n(D)|$-colorable, D is isomorphic to the diagonal subgroup of $M_n(D)$, and so $|D| \leq \omega(R) \leq \chi(R) \leq |M_n(D)|$ which is exactly what we want.

From now on, assume that D is a finite division ring. Hence D is a finite field. Put $m = |D|^n$. Let s be a generator of a Singer cycle in $M_n(D)$. Then the elements $0, s^1, s^2, \ldots, s^{m-1} = 1$ determine a complete subgraph in $\Gamma(R)$ of size m. Hence $m \leq \omega(R)$. There are m row vectors over D of length n. Let these be $v_1, \ldots, v_m$. Color the vertices of $\Gamma(R)$ in the following way. Assign the color i to vertex A if and only if the first row of A is v_i. This is a good coloring of $\Gamma(R)$. Hence $m \leq \omega(R) \leq \chi(R) \leq m$ which is exactly what we wanted. $\qquad\square$

10

7. Arc transitive graphs

At this stage the reader may think that there is no group G with $\omega(G) \neq \chi(G)$. However, this is not true. It is not very hard to see that $\omega(\mathrm{Alt}(5)) = 8$, $\chi(\mathrm{Alt}(5)) = 9$, and $\omega(\mathrm{Alt}(5)) = 10$. By looking at generating graphs $\Gamma(G)$ for which the clique and chromatic numbers are (possibly) different, we were led to certain arc transitive graphs. A graph Γ is said to be arc transitive (or symmetric) if the automorphism group $\mathrm{Aut}(\Gamma)$ is transitive on both the set of vertices of Γ and also on the set of edges of Γ. This section concerns those arc transitive graphs which came up naturally in our investigations of the generating graph of a finite group.

Before we consider finite groups let us note that $\Gamma(R)$ is an arc transitive graph for an arbitrary ring R. (See the previous section for the definition of $\Gamma(R)$.) Indeed, $\varphi_r : R \longrightarrow R$ defined by $x \mapsto x + r$ can be viewed as an automorphism of $\Gamma(R)$ for any $r \in R$. Hence $\Gamma(R)$ is vertex transitive. Also, for an arbitrary invertible element s, the map $\psi_s : R \longrightarrow R$ defined by $x \mapsto x \cdot s$ can be viewed as an automorphism of $\Gamma(R)$. Let (x_1, y_1) and (x_2, y_2) be two arbitrary edges of $\Gamma(R)$. (Note that $\Gamma(R)$ may as well be an empty graph (for example if R has no identity element).) We must show that there exists a graph automorphism which maps x_1 to x_2 and y_1 to y_2. Since $\Gamma(R)$ is vertex transitive we may assume, without loss of generality, that $x_1 = 0$ and $x_2 = 0$. Then y_1 and y_2 are invertible elements and $\psi_{y_1^{-1}y_2}$ is the desired automorphism which maps $(0, y_1)$ to $(0, y_2)$.

Let r and n be positive integers with $r \leq n$. The Turán graph $T(n, r)$ is a graph formed by partitioning a set of n vertices into r subsets, with sizes as equal as possible, and connecting two vertices by an edge whenever they belong to different subsets. (If we write n in the form $n = r[n/r] + k$ for a non-negative integer k with $0 \leq k \leq r - 1$, then the vertex set of $T(n, r)$ consists of k subsets of size $[n/r] + 1$ and $r - k$ subsets of size $[n/r]$.) The graph $T(n, r)$ is extremal in the sense that whenever a graph on n vertices has more edges than that of $T(n, r)$ then this graph contains a complete subgraph on $r + 1$ vertices. The graph $T(n, r - 1)$ was introduced for the following reason.

Theorem 7.1 (Turán, [40]). *Let Γ be a graph on n vertices. If Γ does not have a complete subgraph of size r, then it has at most $((r-2)/(r-1)) \cdot n^2/2$ edges.*

For a 2-generated non-cyclic finite group G let $\Gamma(G)^*$ be the graph

obtained from $\Gamma(G)$ by removing all isolated vertices from $\Gamma(G)$.

Let G be a finite group with $G/\mathrm{Frat}(G)$ an elementary Abelian group of order p^2 where p is a prime. Then $\Gamma(G)^* \cong T(|G| - |\mathrm{Frat}(G)|, p + 1)$. Turán graphs appear naturally as induced subgraphs in $\Gamma(G)$ for any G. Indeed, let G be a finite group. Let S be a subset of G of size $r = \omega(G)$ with the property that every distinct pair of elements in S generate G. For any $s \in S$ let $t(s)$ be the number of generators of $\langle s \rangle$. Let t be the minimum of the $t(s)$'s as s runs through the elements of S. Then $T(tr, r)$ is an induced subgraph in $\Gamma(G)$.

As demonstrated by Liebeck and Shalev [24], Theorem 7.1 is useful in bounding $\omega(G)$ when G is a finite simple group. Indeed, Dixon's [11] conjecture was to show that the probability that a random pair of elements of G generates G tends to 1 as $|G|$ tends to infinity. Loosely speaking this says that $\Gamma(G)$ has "many" edges for G a finite simple group. But if a graph has "many" edges, then, by Theorem [40], it should contain a "large" complete subgraph.

Theorem 7.2 (Liebeck, Shalev, [24]). *There exists a positive constant c_1 such that $c_1 \cdot m(G) \leq \omega(G)$ for any finite simple group G where $m(G)$ denotes the minimal index of a proper subgroup in G.*

If G is a non-Abelian finite simple group different from an alternating group, then $|G| < m(G)^{c_2 \cdot \ln(m(G))}$ for some universal constant c_2. This together with Theorem 7.2 implies the following result.

Proposition 7.3. *There exists an absolute constant $c > 0$ such that $\sigma(G) < \omega(G)^{c \cdot \ln(\omega(G))}$ for any non-Abelian finite simple group G different from an alternating group.*

Proposition 7.3 seems to be weak.

Question 7.1 (Blackburn, [2]). *Is it true that $\omega(G)/\sigma(G)$ tends to 1 as $|G|$ tends to infinity for a non-Abelian finite simple group G?*

In certain special cases it is known that the answer to Question 7.1 is affirmative.

Theorem 7.4. *There exists a constant $c \geq 1$ such that if G is a projective special linear group, a Suzuki group, a Ree group, an alternating group of*

degree not divisible by 4 *and not a prime of the form* $(q^k - 1)/(q - 1)$ *where* q *is a prime power and* k *is a positive integer, then* $(1 - c/m(G))\sigma(G) \leq \omega(G) \leq \sigma(G)$ *where* $m(G)$ *is the minimal index of a proper subgroup in* G.

The case of alternating groups in Theorem 7.4 is due to Linda Stringer. All other cases of Theorem 7.4 is due to Lucchini and Maróti [31].

A consequence of Theorem 7.2 and the proof of Theorem 7.4 is

Theorem 7.5 (Lucchini, Maróti, [31]). *Let* α *denote* ω, χ, *or* σ. *For a positive number* x *define* $\alpha(x)$ *to be the number of positive integers* n *at most* x *with the property that there exists a non-Abelian finite simple group* G *so that* $\alpha(G) = n$. *Then* $\alpha(x) = (2\sqrt{2} + o(1))(\sqrt{x}/\ln x)$.

The following class of graphs was kindly brought to our attention by Péter Hajnal [17]. Let r and n be positive integers with r no greater than n. The Kneser graph $K(n, r)$ is the graph whose vertices are the r-element subsets of a set of size n and there is an edge between two subsets if and only if they are disjoint. ($K(n, r)$ is an empty graph if $n < 2r$. If $n = 2r$, then every connected component of $K(n, r)$ consists of 2 vertices. $K(n, 1)$ is the complete graph on n vertices, and $K(5, 2)$ is the Petersen graph.) Kneser conjectured that the chromatic number of $K(n, r)$ is $n - 2r + 2$. This was proved by Lovász in [27]. Let F be a finite field of order q. The q-Kneser graph $qK(n, r)$ is the graph whose vertices are the r-dimensional subspaces of an n-dimensional vector space over F and two vertices are connected by an edge if and only if their intersection is trivial. (If $n < 2r$, then $qK(n, r)$ is an empty graph. $qK(n, 1)$ is a complete graph.) The chromatic number of the graph $qK(n, r)$ is investigated in [8].

For a positive integer m let G be the cyclic group of order m and let R be the ring $\mathbb{Z}/m\mathbb{Z}$ of integers modulo m. Then it is easy to see that $K(n, r)$ is an induced subgraph of both $\Gamma(G)$ and $\Gamma(R)$ for all positive integers r at most n where n is the number of distinct prime divisors of m. It is less obvious (but true) that $K(q + 1, 2)$ is an induced subgraph of $\Gamma(PSL(2, q))$ and that $K(q^2 + 1, 2)$ is an induced subgraph of $\Gamma(Suz(q))$ for q an even prime power at least 4 (see [31]). These latter observations play an ingredient role in computing $\chi(PSL(2, q))$ and $\chi(Suz(q))$ (see [31]). We end our treatment of Kneser graphs by stating the following question.

Question 7.2. Let r and n be positive integers with $r \leq n$ and $r \neq n/2$.

Let q be a prime power. Then, is it true that, for sufficiently large n, we have the following

(1) the Kneser graph $K(n, r)$ is an induced subgraph of $\Gamma(\mathrm{Sym}(n))$ for all even $n - r$;
(2) the Kneser graph $K(n, r)$ is an induced subgraph of $\Gamma(\mathrm{Alt}(n))$ for all odd $n - r$;
(3) the q-Kneser graph $qK(n, r)$ is an induced subgraph of $\Gamma(GL(n, q))$ for all r?

For a positive integer n and a non-Abelian finite simple group S, let S^n be the direct product of n copies of S. The maximal subgroups of S^n are of two types: product type and diagonal type. These can be described in the following way:

- 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 $\phi \in \mathrm{Aut}(S)$.

From this it can be deduced that $\sigma(S^n) = \sigma(S)$ (see [30]) and it also follows that there is a largest integer m for which S^m can be generated by 2 elements. (S is 2-generated, so $m \geq 1$.) In fact, this largest positive integer m is $\delta(S)$, the number of $\mathrm{Aut}(S)$-orbits on the set of (ordered) generating pairs whose entries are from S. Put $\delta = \delta(S)$ and, for the rest of this section, set $G = S^\delta$.

Consider $\mathrm{Aut}(G) \cong \mathrm{Aut}(S) \wr \mathrm{Sym}(\delta)$ and let (x, y) be a fixed pair of generators for G with $x = (x_1, \ldots, x_\delta)$ and $y = (y_1, \ldots, y_\delta)$ where the x_i's and y_i's are elements of S. Since $\langle x, y \rangle = G$, the elements $(x_1, y_1), \ldots, (x_\delta, y_\delta)$ form a set of representatives for the $\mathrm{Aut}(S)$-orbits of the set of generating pairs for S. From this it is easy to see that G has the following relevant property: $(\mathcal{P})$ if $G = \langle \bar{x}, \bar{y} \rangle$ then there exists $a \in \mathrm{Aut}(G)$ with $(\bar{x}, \bar{y}) = (x^a, y^a)$. By property $(\mathcal{P})$ it follows that the graph $\Gamma(G)^*$ is edge-transitive and vertex-transitive hence arc transitive. In [30] it is shown that the clique number of this arc transitive graph $\Gamma(G)^*$ is at most $(1 + o(1))m(S)$ where $m(S)$ is the minimal index of a proper subgroup in S. More precisely, we have

Theorem 7.6 (Lucchini, Maróti, [30]). *We have $\omega(G) \leq m(S) + O(m(S)^{14/15})$ if S is a group of Lie type and $\omega(G) \leq m(S) + O(1)$ oth-*

14

erwise. In particular, if $S = \mathrm{Alt}(n)$ then $\omega(G)/\sigma(G) \leq (n + O(1))/2^{n-2}$.

The meaning of the last statement of Theorem 7.6 is essentially that there is an infinite sequence of finite non-cyclic 2-generated groups X for which $\omega(X)/\sigma(X)$ tends to 0. (This statement uses the fact from [33] that $2^{n-2} \leq \sigma(\mathrm{Alt}(n))$ unless $n = 7$ or 9.) But Theorem 7.6 is also interesting from another point of view. In view of Question 5.2 and Theorem 7.2 one can ask whether there exists an absolute positive constant c so that $c \cdot m(X) \leq \omega(X)$ where X is an arbitrary 2-generated finite group. Unfortunately Theorem 7.6 does not give us an immediate counter-example to this question. However the following problem may be of interest.

Question 7.3. Is there a non-Abelian finite simple group S for which $\omega(G) > 3$?

Gábor Nagy [34] kindly pointed out that there is an invariant called the Lovász theta function $\vartheta(\Gamma)$ defined for a finite simple graph Γ. As shown in [28], this is at least the clique number and at most the chromatic number of the complementary graph of Γ. (For the exact definition of $\vartheta(\Gamma)$ the reader is referred to [28].) If n denotes the number of vertices in Γ, then the adjacency matrix A of Γ is an $n \times n$ matrix with $0 - 1$ coefficients with a 1 in the (i, j)-entry of A if and only if the i-th and j-th vertices of Γ are joined by an edge. Now suppose that Γ is a d-regular graph. Then d is an eigenvalue of A. In fact, by the Perron-Frobenius theorem for non-negative matrices, d is the largest eigenvalue of A. In Theorem 9 of [28] it is shown that if Γ is edge transitive, then $\vartheta(\Gamma) = n\lambda/(\lambda - d)$ where λ is the smallest eigenvalue of A.

We end this section with an example related to Question 7.3.

Let $S = \mathrm{Alt}(5)$. Then $\mathrm{Aut}(S) = \mathrm{Sym}(5)$. For positive integers r and s let us say that an element (x, y) of $\mathrm{Alt}(5)^2$ is of type (r, s) if x has order r and y has order s. A set of representatives of the orbits of the conjugacy action of $\mathrm{Sym}(5)$ on the set of (ordered) generating pairs for $\mathrm{Alt}(5)$ consists of 19 elements: 4 elements of type $(5, 5)$, 4 elements of type $(5, 3)$, 4 elements of type $(3, 5)$, 2 elements of type $(5, 2)$, 2 elements of type $(2, 5)$, 1 element of type $(2, 3)$, 1 element of type $(3, 2)$, and 1 element of type $(3, 3)$. Hence $\delta = \delta(S) = 19$ and $G = \mathrm{Alt}(5)^{19}$.

It was mentioned in the beginning of this section that $\omega(\mathrm{Alt}(5)) = 8$ and $\sigma(\mathrm{Alt}(5)) = 10$. We also have $\sigma(\mathrm{Alt}(5)^{19}) = 10$.

Proposition 7.7. $\omega(\mathrm{Alt}(5)^{19}) \leq 4$.

Proof. Since $\mathrm{Alt}(5)^{19}$ is 2-generated, we have $3 \leq \omega(\mathrm{Alt}(5)^{19})$. For a contradiction assume that $4 < \omega(\mathrm{Alt}(5)^{19})$. There exists 5 elements $y_1 = (x_{1,1}, \ldots, x_{19,1})$, $y_2 = (x_{1,2}, \ldots, x_{19,2})$, $y_3 = (x_{1,3}, \ldots, x_{19,3})$, $y_4 = (x_{1,4}, \ldots, x_{19,4})$, $y_5 = (x_{1,5}, \ldots, x_{19,5})$ which pairwise generate $\mathrm{Alt}(5)^{19}$. Consider the matrix $X = (x_{ij})$ with 19 rows and 5 columns. This matrix X has the following properties:

(1) the five elements in each row of X pairwise generate $\mathrm{Alt}(5)$ (in particular this implies that any row of X contains at most 2 element of order 3);
(2) any two columns of X correspond to two elements of $\mathrm{Alt}(5)^{19}$ which together generate $\mathrm{Alt}(5)^{19}$ (this implies that the 19 rows of X give a set of representatives for the orbits of the conjugacy action of $\mathrm{Sym}(5)$ on the set of pairs of elements generating $\mathrm{Alt}(5)$).

By property (2), each column of X contains 6 elements of order 3 and so X contains a total of 30 elements of order 3.

On the other hand, each row contains at most 2 elements of order 3 and there are at most $10 = \binom{5}{2}$ rows containing exactly 2 elements of order 3 (this latter statement follows from property (2): there is no 2×2 minor of X with all entries of order 3). This implies that there are at most $9 + 20 = 29 < 30$ elements of order 3 in X. A contradiction. $\square$

Unfortunately we were unable to decide whether $\omega(\mathrm{Alt}(5)^{19})$ is 3 or 4. Some computational evidence from Pablo Spiga [38] together with the fact that we were unable to construct a 19×4 matrix X with entries from $\mathrm{Alt}(5)$ with the property that the 4 elements of $\mathrm{Alt}(5)^{19}$ determined by the 4 columns of X pairwise generate $\mathrm{Alt}(5)^{19}$ suggest that $\omega(\mathrm{Alt}(5)^{19})$ is 3 rather than 4.

Finally, perhaps it is worth mentioning that $4 \leq \omega(\mathrm{Alt}(5)^{18})$. Indeed, consider the 18×4 matrix $\bar{X}$ as shown below.

16

$$\bar{X} = \begin{pmatrix} (145) & (12345) & (12354) & (13)(25) \\ (15423) & (12345) & (13425) & (15324) \\ (142) & (12345) & (14532) & (354) \\ (23)(45) & (12345) & (15243) & (142) \\ (154) & (12345) & (123) & (13452) \\ (13254) & (12345) & (132) & (345) \\ (13)(25) & (12345) & (124) & (14523) \\ (14523) & (12345) & (142) & (23)(45) \\ (12435) & (12345) & (12)(34) & (245) \\ (235) & (12345) & (13)(24) & (14532) \\ (13254) & (132) & (12345) & (145) \\ (23)(45) & (124) & (12345) & (13425) \\ (14523) & (142) & (12345) & (15)(34) \\ (14253) & (13)(25) & (13425) & (142) \\ (135) & (14)(25) & (15432) & (13245) \\ (12435) & (12)(34) & (135) & (12345) \\ (15432) & (135) & (12)(34) & (14352) \\ (15432) & (123) & (345) & (12453) \end{pmatrix}.$$

The entries of $\bar{X}$ are even permutations of $\{1, \ldots, 5\}$. The 4 columns of $\bar{X}$ correspond to 4 elements of $\mathrm{Alt}(5)^{18}$. One may check that these 4 elements pairwise generate $\mathrm{Alt}(5)^{18}$.

8. A probabilistic method

The symmetric group $\mathrm{Sym}(n)$ is a highly combinatorial structure. By working on this group we hope to be able to develop some algebraic and combinatorial methods useful in dealing with other finite groups. The special case of the symmetric group also seems to be of interest in view of Brown's work and Proposition 7.3.

The "easiest" case is when n is odd. For if n is odd, then $\mathrm{Sym}(n)$ is the union of $\mathrm{Alt}(n)$ and all maximal intransitive subgroups of $\mathrm{Sym}(n)$. This gives $\sigma(\mathrm{Sym}(n)) \leq 2^{n-1}$. To prove a lower bound for $\sigma(\mathrm{Sym}(n))$ we need a combinatorial observation from [33]. Let Π be a set of permutations of $\mathrm{Sym}(n)$. Define $\sigma(\Pi)$ to be the least integer m such that Π is the subset of the set-theoretic union of m proper subgroups of $\mathrm{Sym}(n)$. It is straightforward that $\sigma(\Pi) \leq \sigma(\mathrm{Sym}(n))$. We will say that a set $\mathcal{H} = \{H_1, \ldots, H_m\}$ of

m proper subgroups of $\mathrm{Sym}(n)$ is definitely unbeatable on Π if $\Pi \subseteq \bigcup_{i=1}^{m} H_i$; if $\Pi \cap H_i \cap H_j = \emptyset$ for all $i \neq j$; and if $|S \cap \Pi| \leq |H_i \cap \Pi|$ holds whenever $1 \leq i \leq m$ and when $S \notin \mathcal{H}$ is a proper subgroup of $\mathrm{Sym}(n)$. If $\mathcal{H}$ is definitely unbeatable on Π, then $|\mathcal{H}| = \sigma(\Pi) \leq \sigma(\mathrm{Sym}(n))$. Now if $\mathcal{H}$ is the set consisting of $\mathrm{Alt}(n)$ together with all maximal intransitive subgroups of $\mathrm{Sym}(n)$, then, for sufficiently large n, there exists a subset Π of $\mathrm{Sym}(n)$ such that $\mathcal{H}$ is definitely unbeatable on Π. This was used in [33] where it was shown that $\sigma(\mathrm{Sym}(n)) = 2^{n-1}$ whenever n is odd and different from 9. Interestingly, 9 was found to be "too small" in a certain sense and "too large" in another sense. The exact value of $\sigma(\mathrm{Sym}(9))$ is unknown.

Question 8.1. Is it true that $\sigma(\mathrm{Sym}(9)) = 256$?

We have seen that it is relatively easy to show that $\sigma(\mathrm{Sym}(n)) = 2^{n-1}$ for n odd excluding the case when $n = 9$. However, it is much more difficult to find the other two invariants $\omega(\mathrm{Sym}(n))$ and $\chi(\mathrm{Sym}(n))$.

If n is a prime not of a certain kind, then, by Guralnick [14], it can be shown that $2^{n-1} \leq \omega(\mathrm{Sym}(n))$, hence all three invariants are equal to 2^{n-1} (see [33]). However, surprisingly, much more is true.

Theorem 8.1 (Blackburn, [2]). *If n is sufficiently large and odd, then $\omega(\mathrm{Sym}(n)) = 2^{n-1}$.*

The proof of Theorem 8.1 uses the classification of finite simple groups and a probabilistic method relying on

Theorem 8.2 (Lovász Local Lemma, [12]). *Let Γ be a finite graph with maximum valency d. Suppose that we associate an event E_v to every vertex $v \in \Gamma$, and suppose that E_v is independent of any subset of the events $\{E_v : u \nsim v\}$. Let p be such that $Pr(\cap_{v \in \Gamma} \bar{E}_v) > 0$ whenever $ep(d+1) < 1$ where e denotes the base of the natural logarithm.*

Unfortunately it seems more difficult to determine $\omega(\mathrm{Sym}(n))$ when n is even. In this case the following question may be of importance.

Question 8.2. For n an even positive integer let Γ denote the graph whose vertices are the permutations which are products of three disjoint cycles such that at least one cycle is of odd length with an edge between two

18

vertices if and only if they generate an intransitive subgroup in $\mathrm{Sym}(n)$. What can be said about the clique and chromatic numbers of Γ?

Alternating groups are dealt with similarly as symmetric groups. Blackburn [2] showed that if n is a sufficiently large even integer not divisible by 4 then $\omega(\mathrm{Alt}(n)) = \sigma(\mathrm{Alt}(n)) = 2^{n-2}$. This proof also uses Theorem 8.2.

9. Systems of distinct representatives

Given a conjugacy class $\mathcal{C}$ of a finite group G. We introduce two (sets of) conditions ((A) and (B)) on $\mathcal{C}$.

(A) There is exactly one conjugacy class of maximal subgroups of G whose members contain elements from $\mathcal{C}$ and whose members have "large" orders. Let this conjugacy class of subgroups be $\mathcal{H}$. Every member of $\mathcal{C}$ is contained in exactly two members of $\mathcal{H}$.

(B) For any conjugacy class $\mathcal{H}$ of maximal subgroups in G any member of $\mathcal{C}$ is contained in at most one member of $\mathcal{H}$.

Given (A) (and (B)), find the largest value of $|S|$ where S is a subset of $\mathcal{C}$ with the property that every distinct pair of elements of S generate G. Let us call this problem Problem A (and Problem (B)).

In this section we consider (but do not solve) Problems A and B.

A matching in an arbitrary unoriented graph Γ is a set of edges such that no pair of edges meet at a common vertex. A maximum matching is a matching of largest possible size. The number of edges in a maximum matching of Γ is called the maximal matching number of Γ and it is denoted by $\nu(\Gamma)$.

Suppose that Condition (A) holds. We may define an unoriented graph Γ with vertex-set $\mathcal{H}$ with an edge between distinct vertices H_1 and H_2 if and only if $H_1 \cap H_2 \cap \mathcal{C} \neq \emptyset$. Problem A is equivalent to finding $\nu(\Gamma)$.

Suppose that Condition (B) holds. In this case we introduce more notations. Let $\mathcal{H}_1, \ldots, \mathcal{H}_k$ be those conjugacy classes of maximal subgroups of G which have members containing elements of $\mathcal{C}$. We may define a k-uniform hypergraph Γ in the following way. The vertices of Γ are the maximal subgroups H such that $H \cap \mathcal{C} \neq \emptyset$ and the edges are in bijective correspondence with the elements of $\mathcal{C}$ in such a way that for each element c in $\mathcal{C}$ the set consisting of all maximal subgroups containing c is an edge in Γ. Problem

A is equivalent to finding the maximum size of a set of edges in Γ satisfying the condition that no two edges have a common vertex.

Perhaps it is worth noting that Problem B can be put in a much more general setting. Let G be a finite group. For any g in G define S_g to be the set consisting of those maximal subgroups of G which contain g. Let n be the order of G. If Wall's conjecture [25] is true, then $|S_g| \leq |S_1| \leq n$ for any $g \in G$. Let m be the maximal size of a proper subgroup in G. Clearly, there are at most m subsets S_g containing a fixed element (or maximal subgroup). Very broadly speaking we are given n subsets of a set of size n so that no element is contained in more than m of the subsets. We may consider this system of subsets.

Condition (A) occurred in one instance in the paper [4]. Let $G = GL(n, q)$ where n is congruent to 2 modulo 4. Let $\mathcal{C}$ be a conjugacy class consisting of such linear transformations of an n-dimensional vector space V over the field of q elements which act "almost as" Singer cycles on exactly two, complementary, $n/2$-dimensional subspaces of V. Then $\mathcal{H}$ is taken to be a certain conjugacy class of maximal parabolic subgroups of G. The above-mentioned equivalent form of Problem A is considered and solved in [4] for $\Gamma \cong qK(n, n/2)$ where $qK(n, n/2)$ is the q-Kneser graph defined in Section 6 where n is an even integer. For an arbitrary (undirected) graph Δ with N vertices, define $\text{def}(\Delta) = N - 2\nu(\Delta)$ to be the deficiency of Δ. Then we have

Theorem 9.1 (Britnell, Evseev, Guralnick, Holmes, Maróti, [4]).
Let $qK(n, n/2)$ be a q-Kneser graph for some even integer n. If q is odd, then $\text{def}(qK(n, n/2)) = 0$. If q is even, then $\text{def}(qK(n, n/2)) = 1$.

One of the ingredients of the proof of Theorem 9.1 is that if $q > 3$ then every vertex of $qK(n, n/2)$ has degree larger than the number of vertices of $qK(n, n/2)$ divided by 2. By Dirac's theorem, this implies that $qK(n, n/2)$ is Hamiltonian whenever $q > 3$. This raises the following question.

Question 9.1. Is the q-Kneser graph $qK(n, n/2)$ Hamiltonian?

From now on we assume that Condition (B) holds, adapt all relevant notations and consider Problem B.

Problem B is trivial if $k = 1$ hence this case is omitted. We distinguish two more cases, namely $k = 2$ and $k > 2$.

20

Unless otherwise stated assume that $k = 2$. In this case König's theorem [23] and Hall's Marriage Theorem [18] are of special importance. Indeed, in this case, $\Gamma = (X, Y, E)$ is a bipartite graph, that is, a graph with vertex set $X \cup Y$, edge set E with the property that every edge connects a vertex of X with a vertex of Y. A covering K is a set of vertices of Γ so that every edge in Γ has an endpoint in K. A minimum covering is a covering of least possible size. It can be seen that the size of a minimum covering in Γ is $\min\{|\mathcal{H}_1|, |\mathcal{H}_2|\}$. Hence Theorem 9.2 gives the desired solution.

Theorem 9.2 (König, [23]). *Suppose that Δ is a bipartite graph. Then $\nu(\Delta)$ is equal to the number of vertices in a minimum covering of Δ.*

For a positive integer m let $\mathcal{S}$ be an m-tuple $(S_1, \ldots, S_m)$ whose entries are subsets of a finite set Ω. We say that $(s_1, \ldots, s_m) \in \Omega^m$ is a system of distinct representatives for $\mathcal{S}$ if the s_i's are all distinct and $s_i \in S_i$ for all i with $1 \le i \le m$.

Theorem 9.2 is logically equivalent to

Theorem 9.3 (Hall, [18]). *$\mathcal{S}$ has a system of distinct representatives if and only if for each index set $I \subseteq \{1, \ldots, m\}$ we have $|I| \le |\cup_{i \in I} S_i|$.*

Theorems 9.2 and 9.3 can be used to consider Problem B in various situations, for example to find $\omega(G)$ for certain sporadic simple groups G.

Proposition 9.4 (Holmes, Maróti, Pálfy, [21]). *We have $\omega(M_{23}) = \sigma(M_{23}) = 41079$.*

We note that the exact value of $\sigma(M_{23})$ is computed in [20].

Now let $k > 2$. We consider Problem B in the following special case (see [4]). Let G be $GL(n, q)$ where n is a positive integer with exactly k distinct prime divisors. Let the distinct prime divisors of n be $p_1 < p_2 < \ldots < p_k$. Let $\mathcal{C}$ be a conjugacy class of generators of Singer cycles in $GL(n, q)$. Then, by a result of Kantor [22], the possible maximal overgroups of elements of $\mathcal{C}$ are of the form $GL(n/p_i, q^{p_i}).p_i$ where i is so that $1 \le i \le k$. Moreover, for each i with $1 \le i \le k$ and for each $c \in \mathcal{C}$ there is exactly one copy of $GL(n/p_i, q^{p_i}).p_i$ containing c. Hence Condition (B) is indeed satisfied. In this situation the following generalization of Theorems 9.2 and 9.3 was used in [4] to solve Problem B.

Theorem 9.5 (Haxell, [19]). *Let Γ be a (simple) graph so that every vertex of Γ has degree at most d for some positive integer d. Let $V(\Gamma) = V_0 \cup \ldots \cup V_t$ be a partition of the vertex set of Γ. Suppose that $2d \leq |V_i|$ for each i. Then Γ has an independent set $\{v_0, \ldots, v_t\}$ where $v_i \in V_i$ for each i.*

Throughout the rest of this section let us fix the following notations. Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$ where n is a positive integer and q is a prime power. Let V be the n-dimensional vector space over the field of q elements. Let $[x]$ denote the integer part of the real number x. Let b be the smallest prime factor of n and let $N(b)$ be the number of proper subspaces of V of dimensions not divisible by b. Finally, let $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_q$ be the number of k-dimensional subspaces of the n-dimensional vector space V.

Theorem 9.5 together with deep group-theoretic results [16] relying on the classification of finite simple groups gave

Theorem 9.6 (Britnell, Evseev, Guralnick, Holmes, Maróti, [4]). *If $n \geq 12$, then*

$$\omega(G) = \frac{1}{b} \prod_{\substack{i=1 \\ b \nmid i}}^{n-1} (q^n - q^i) + [N(b)/2].$$

It turned out that in many cases $\sigma(G)$ is different from $\omega(G)$.

Theorem 9.7 (Britnell, Evseev, Guralnick, Holmes, Maróti, [4]). *Suppose that $n \geq 12$. Then if $n \not\equiv 2 \pmod 4$, or if $n \equiv 2 \pmod 4$, q odd and $G = (P)SL(n,q)$, then*

$$\sigma(G) = \mu(G) = \frac{1}{b} \prod_{\substack{i=1 \\ b \nmid i}}^{n-1} (q^n - q^i) + [N(b)/2].$$

Otherwise $\sigma(G) \neq \mu(G)$ and

$$\sigma(G) = \frac{1}{2} \prod_{\substack{i=1 \\ 2 \nmid i}}^{n-1} (q^n - q^i) + \sum_{\substack{k=1 \\ 2 \nmid k}}^{(n/2)-1} \begin{bmatrix} n \\ k \end{bmatrix}_q + \frac{q^{n/2}}{q^{n/2}+1} \begin{bmatrix} n \\ n/2 \end{bmatrix}_q + \epsilon$$

where $\epsilon = 0$ if q is even and $\epsilon = 1$ if q is odd.

22

Finally, the following question concerns the invariant $\chi(G)$.

Question 9.2. Suppose that $n \geq 12$. Is it true that $\chi(G) = \sigma(G)$?

10. Affine groups

Throughout this section V is a vector space of dimension n defined over a field of order q, the group G denotes a subgroup of $GL(n, q)$, and GV stands for the semidirect product with a normal subgroup V and a subgroup G acting on V in the natural way.

Theorem 10.1. *We have the following.*

(1) $\sigma(GV) \leq (q^{n+1} - 1)/(q - 1)$.
(2) $\omega(GV) = (q^{n+1} - 1)/(q - 1)$ if (but not necessarily only if) $G = GL(n, q)$ provided that $n \geq 12$.
(3) Suppose that G is solvable and irreducible on V. Suppose also that $(|G|, |V|) = 1$ and the minimal number of generators of G is 2. Then $\omega(GV) = \omega(G)$. In particular, if $\omega(G) = \sigma(G)$, then $\omega(GV) = \chi(GV) = \sigma(GV)$.

Proof. For a 1-dimensional subspace W of V denote the subspace stabilizer of W in G by G_W. Let Σ be the set consisting of all q^n conjugates of G in GV and all subgroups of GV of the form $G_W V$. The size of Σ is $(q^{n+1} - 1)/(q - 1)$. To prove (1) of Theorem 10.1 it is sufficient to see that Σ is a covering for GV. For any $g \in G$ and $v \in V$ the element $x \mapsto gx + (1 - g)v$ is in the union of all q^n conjugates of G in GV. If $g \in G$ has no non-zero fixed point on V, then $(1 - g)v$ runs through all vectors of V as v runs through all vectors of v. On the other hand, if g fixes a non-zero vector w of V, then the element $x \mapsto gx + v$ lies in $G_W V$ for any $v \in V$ where W is the subspace generated by w. Hence Σ is indeed a covering for GV.

For this and the next paragraph (only) let $G = GL(n, q)$ and $n \geq 12$. Let $\widetilde{Y}$ be a subset of G consisting of elements $\widetilde{y_1}, \ldots, \widetilde{y_{q^n}}$ and elements $\widetilde{y_W}$ (for all 1-dimensional subspaces W of V) such that the $\widetilde{y_i}$'s are generators of Singer cycles and each $\widetilde{y_W}$ fixes every vector of W and acts as a Singer cycle on some complementary subspace of V of dimension $n - 1$ such that $\widetilde{Y}$ induces a clique in $\Gamma(G)$. We need to show the existence of such a set $\widetilde{Y}$. In the proof of Theorem 1.1 of [4] it was shown that there exists a

subset X of G of size $\omega(G)$ such that X induced a clique in $\Gamma(G)$ with the property that X contains $|GL(n,q)|/|GL(n/b,q^b).b|$ generators of (the same number of) Singer cycles where b is the smallest prime divisor of n, and X contains $(q^n - 1)/(q - 1)$ elements fixing exactly q vectors and acting as Singer cycles on $n - 1$-dimensional subspaces of V. Finally, note that $|GL(n,q)|/|GL(n/b,q^b).b| > q^n$ (since $n \geq 12$).

Now, using elements of the normal subgroup V of GV, conjugate the $\widetilde{y_i}$'s so that they all lie in different (and unique) conjugates of G (in GV). Let a resulting list of elements be $y_1, \ldots y_{q^n}$. (For example, one can do the following. Let the distinct elements of V be $v_1, \ldots, v_{q^n}$ (in any order). For each i such that $1 \leq i \leq q^n$, set y_i to be the element $x \mapsto \widetilde{y_i}x + (1 - \widetilde{y_i})v_i$. The construction works since $1 - \widetilde{y_i}$ is invertible for each i with $1 \leq i \leq q^n$.) Similarly, for each 1-dimensional subspace W of V, choose an element y_W from $G_W V$ that has no fixed point on V and which maps onto the element $\widetilde{y_W}$ via the natural homomorphism ϕ_W from $G_W V$ to $G_W V/V \cong G_W$. (For example, y_W can be taken to be an element $x \mapsto \widetilde{y_W}x + w$ where $w \in V \setminus \operatorname{im}(1 - \widetilde{y_W})$.) Let Y be the set consisting of all the y_i's and all the y_W's. We claim that Y induces a clique in $\Gamma(GV)$. Consider the natural homomorphism ϕ from GV to $GV/V \cong G$, and pick arbitrary, distinct elements a and b from Y. For a contradiction, suppose that $\langle a, b \rangle$ is contained in a maximal subgroup H of GV. If H is not core free in GV, then $V \leq H$, since, as above, GV may be viewed as an affine primitive permutation group with unique minimal normal subgroup V. Moreover, since $\phi(a)$ and $\phi(b)$ generate G, we must have $H = GV$. A contradiction. Now suppose that H is core free. Then GV is an affine primitive permutation group with point stabilizer H, and so $H \cong G$. Since $H^1(G,V) = 0$, we see that H is conjugate to G. It follows that neither a nor b can be an element of the form y_W since the y_W's do not fix any vector of V. Hence a and b are two of the y_i's. But this is again a contradiction, since the y_i's were chosen to lie in different conjugates of G in GV. This proves that Y induces a clique in $\Gamma(GV)$. Part (1) of Theorem 10.1 together with the fact that $|Y| = (q^n - 1)/(q - 1)$ gives part (2) of Theorem 10.1.

We now turn to the proof of part (3) of Theorem 10.1. Let G be a solvable group acting irreducibly on V. Suppose that G is not cyclic and that G can be generated by two elements. Suppose also that $(|G|,|V|) = 1$. Since G is solvable and is a point stabilizer of a primitive permutation group with minimal normal subgroup V, Gaschütz's theorem [13] says that every chief factor of G, apart from V, has size less than $|V|$. Hence, by

24

Tomkinson's theorem [39], we have $\omega(G) \leq \sigma(G) \leq |V|$. Take a subset $\widetilde{Y}$ of G of size $\omega(G)$ which induces a clique in $\Gamma(G)$. For each $\widetilde{y} \in \widetilde{Y}$ we will define an element y in GV in the following way. If $\widetilde{y}$ fixes some non-zero vector of V, then set y to be an element $x \mapsto \widetilde{y}x + w$ where $w \in V \setminus \mathrm{im}(1 - \widetilde{y})$. Notice that y does not lie in any conjugate of G in GV. Assume that there exist $m \geq 0$ elements in $\widetilde{Y}$ which fixes no non-zero vector in V. Without loss of generality suppose that these are $\widetilde{y_1}, \ldots, \widetilde{y_m}$. Clearly, $m \leq |V|$. Let $v_1, \ldots, v_m$ be distinct elements of V. For each i such that $1 \leq i \leq m$, set y_i to be the element $x \mapsto \widetilde{y_i}x + (1 - \widetilde{y_i})v_i$. Notice that each y_i lies in a unique conjugate of G in GV, and that every conjugate of G contains at most one of the y_i's. Let Y be the set consisting of all the above-described y's together with all the y_i's. The size of Y is $\omega(G)$. We claim that Y induces a clique in $\Gamma(GV)$. Pick two distinct elements a and b from Y. Let ϕ be the natural homomorphism from GV to $GV/V \cong G$ (with kernel V). Suppose that $\langle a, b \rangle$ is contained in a maximal subgroup H of GV. We will obtain a contradiction. If H is not core free in GV, then $V \leq H$ (since GV can be viewed as an affine primitive permutation group with a unique minimal normal subgroup V), and so $H = GV$. A contradiction. If H is a core free maximal subgroup in GV, then GV has a primitive permutation representation with point stabilizer H. But GV contains a unique (Abelian) minimal normal subgroup, namely V, which has to be regular in this permutation representation. Hence $|H| = |GV|/|V| = |G|$ and $H \cap V = \{1\}$ (latter because $(|H|, |V|) = 1$). By the Schur-Zassenhaus theorem, H is conjugate to G in GV. However this is a contradiction, since, by construction, a and b cannot lie in the same conjugate of G. This proves $\omega(G) \leq \omega(GV) \leq \omega(G)$. Finally, if $\omega(G) = \sigma(G)$, then $\sigma(G) = \omega(G) = \omega(GV) \leq \chi(GV) \leq \sigma(GV) \leq \sigma(G)$. $\square$

References

1. Bhargava, M. Finiteness criteria for coverings of groups by finitely many subgroups or cosets. *Int. Electronic J. of Alg.* Vol. **2** (2007) 83-89.
2. Blackburn, S. Sets of permutations that generate the symmetric group pairwise. *J. Combin. Theory Ser. A* **113** (2006), no. 7, 1572-1581.
3. Breuer, T.; Guralnick, R. M.; Kantor, W. M. Probabilistic generation of finite simple groups, II. To appear in *J. Algebra*.
4. Britnell, J. R.; Evseev, A; Guralnick, R. M.; Holmes, P. E.; Maróti, A. Sets of elements that pairwise generate a linear group. *J. Combin. Theory Ser. A.* **115** (2008), no. 3, 442-465.
5. Brown, R. Minimal covers of S_n by abelian subgroups and maximal subsets

25

of pairwise noncommuting elements. *J. Combin. Theory Ser. A* **49**, (1988), no. 2, 294-307.

6. Brown, R. Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. II. *J. Combin. Theory Ser. A* **56**, (1991), no. 2, 285-289.

7. Bryce, R. A; Fedri, V; Serena, L. Subgroup coverings of some linear groups. *Bull. Austral Math. Soc.* **60**, (1999), no. 2, 227-238.

8. Chowdhury, A.; Godsil, C.; Royle, G. Colouring lines in projective spaces.

9. Cohn, J. H. E. On n-sum groups. *Math. Scand.* **75**, (1994), no. 1, 44-58.

10. Detomi, E.; Lucchini, A. On the structure of primitive n-sum groups, submitted for publication.

11. Dixon, J. D. The probability of generating the symmetric group. *Math. Z.* **110** (1969), 199–205.

12. Erdős, P.; Lovász L. Problems and results on 3-chromatic hypergraphs and some related questions. A. Hajnal, R. Rado, and V. T. Sós, eds. Infinite and finite sets (to Paul Erdős on his 60th birthday) II. 609-627, North-Holland.

13. Gaschütz, W. Existenz und Konjugiertsein von Untergruppen, die in endlichen auflösbaren Gruppen durch gewisse Indexschranken definiert sind, *J. Algebra* **53** (1978), 1-20.

14. Guralnick, R. M. Subgroups of prime power index in a simple group. *J. Algebra* **81**, (1983), 304-311.

15. Guralnick, R. M.; Robinson, G. R. On the commuting probability of finite groups.

16. Guralnick, R.; Penttila, T.; Praeger, C. E.; Saxl, J. Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc.* (3) **78** (1999), no. 1, 167-214.

17. Hajnal, P. Personal communication.

18. Hall, P. On representatives of subsets. *J. London Math. Soc.*, **10** (1935) 26–30.

19. Haxell, P. E. A condition for matchability in hypergraphs. *Graphs and Combinatorics* **11** (1995) 245-248.

20. Holmes, P. E. Subgroup coverings of some sporadic groups. *J. Combin. Theory, Ser. A* **13** (2006), no. 6, 1204-1213.

21. Holmes, P. E.; Maróti, A.; Pálfy, P. P. Pairwise generation of sporadic groups, in preparation.

22. Kantor, W. M. Linear groups containing a Singer cycle. *J. Algebra* **62** (1980), no. 1, 232–234.

23. Kőnig, D. Graphen und Matrizen. *Mat. Fiz. Lapok* **38** (1931), 116-119.

24. Liebeck, M. W.; Shalev, A. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* **184** (1996), no. 1, 31–57.

25. Liebeck, M.; Pyber, L.; Shalev, A. On a conjecture of G. E. Wall. *J. Algebra* **317**, (2007), 184-197.

26. Linckelmann, M. Personal communication.

27. Lovász, L. Kneser's conjecture, chromatic number, and homotopy. *J. Combin. Theory, Ser. A* **25** (1978), 319–324.

28. Lovász, L. On the Shannon capacity of a graph. *IEEE Transactions on In-*

26

formation Theory, Vol. IT-25, no. 1, January 1979.

29. Lucchini, A.; Maróti, A.; Semmen, D. *d*-wise generation of some infinite groups, to appear.
30. Lucchini, A.; Maróti, A. On the clique number of the generating graph of a finite group, submitted for publication.
31. Lucchini, A.; Maróti, A. On the chromatic number of the generating graph of a finite group, in preparation.
32. Lucido, M. S. On the covers of finite groups. *Groups St. Andrews 2001* Vol. II, 395-399, London Math. Soc. Lecture Note Ser., **305**, Cambridge Univ. Press, Cambridge, 2003.
33. Maróti, A. Covering the symmetric groups with proper subgroups. *J. Combin. Theory Ser. A* **110** (2005), no. 1, 97–111.
34. Nagy, G. Personal communication.
35. Neumann, B. H. Groups covered by permutable subsets. *J. London Math. Soc.* **29**, (1954), 236–248.
36. Pyber, L. The number of pairwise noncommuting elements and the index of the centre in a finite group. *J. London Math. Soc. (2)* **35**, (1987), no. 2, 287-295.
37. Scorza, G. I gruppi che possono pensarsi come somma di tre loro sottogruppi. *Boll. Un. Mat. Ital.* **5**, (1926), 216-218.
38. Spiga, P. Personal communication.
39. Tomkinson, M. J. Groups as the union of proper subgroups. *Math. Scand.* **81**, (1997), 191-198.
40. Turán, P. An extremal problem in graph theory. *Mat. Fiz. Lapok* **48**, (1941), 436-452.