Sets of Elements that Pairwise Generate a Group

Andrea Lucchini

University of Padova, Italy

Joint work with Attila Maroti

GLAUBERMAN CONFERENCE
Chicago, 25 March 2008

Outline

DEFINITIONS

G a finite (non cyclic) group that can be generated by two elements;

$\mu(G)$ the largest positive integer m so that there exists a subset X in G of order m, with the property that any distinct pair of elements of X generates G.

DEFINITIONS

G a finite (non cyclic) group that can be generated by two elements;

$\mu(G)$ the largest positive integer m so that there exists a subset X in G of order m, with the property that any distinct pair of elements of X generates G.

EXAMPLE

$\mu(\mathrm{Alt}(5)) = 8$. We can consider

$$X := \{(1,2,3),(3,4,5),(1,2,3,4,5),(1,2,3,5,4),(1,2,4,3,5),$$
$$(1,2,4,5,3),(1,2,5,3,4),(1,2,5,4,3)\}$$

IN GRAPH THEORETICAL NOTATIONS:

We define a graph $\Gamma(G)$ on the set of elements of G, connecting two vertices by an edge if they generate G.
$\mu(G)$ is the clique number of $\Gamma(G)$ (the maximum size of a complete subgraph).

REMARK

$\mu(G) \leq \chi(\Gamma(G))$, where $\chi(\Gamma(G))$ is the chromatic number of $\Gamma(G)$, i.e the smallest number of colors needed to color the vertices of $\Gamma(G)$ so that no two adjacent vertices share the same color.

REMARK

If G is a union of m proper subgroups, then $\chi(\Gamma(G)) \leq m$ (we assign different colors to the different subgroups and a vertex can receive any of the colors associated to the covering subgroups containing that vertex).

IN GRAPH THEORETICAL NOTATIONS:

We define a graph $\Gamma(G)$ on the set of elements of G, connecting two vertices by an edge if they generate G.
$\mu(G)$ is the clique number of $\Gamma(G)$ (the maximum size of a complete subgraph).

REMARK

$\mu(G) \leq \chi(\Gamma(G))$, where $\chi(\Gamma(G))$ is the chromatic number of $\Gamma(G)$, i.e the smallest number of colors needed to color the vertices of $\Gamma(G)$ so that no two adjacent vertices share the same color.

REMARK

If G is a union of m proper subgroups, then $\chi(\Gamma(G)) \leq m$. Hence $\chi(\Gamma(G)) \leq \sigma(G)$, where $\sigma(G)$ is the least integer k such that G is the union of k proper subgroups .

SUMMARIZING

$\Gamma(G)$	$\{x, y\} \in \mathsf{E}(\Gamma(G)) \iff \langle x, y \rangle = G$
$\mu(G)$	maximum size of a complete subgraph
$\chi(\Gamma(G))$	the smallest number of colors so that no two adjacent vertices share the same color
$\sigma(G)$	the least integer k such that G is the union of k proper subgroups

$$\mu(G) \leq \chi(\Gamma(G)) \leq \sigma(G)$$

KNOWN RESULTS FOR SIMPLE GROUPS

Let S be a finite nonbelian simple group and let $m(S)$ be the minimal index of a proper subgroup of S.

- (Liebeck and Shalev, 1995) There exists a constant c such that for any S we have $c \cdot m(S) \leq \mu(S)$ (Using probabilistic results on the generation of finite simple groups combined with Turán's Theorem of extremal graph theory).

KNOWN RESULTS FOR SIMPLE GROUPS

Let S be a finite nonbelian simple group and let $m(S)$ be the minimal index of a proper subgroup of S.

- (Liebeck and Shalev, 1995) There is a constant c such that $c \cdot m(S) \leq \mu(S)$ for any finite nonabelian simple group S.
- (Blackburn, 2006) If $S = \mathrm{Alt}(n)$, n is a sufficiently large integer and $n \equiv 2 \mod 4$, then $\mu(S) = \sigma(S) = 2^{n-2}$.

KNOWN RESULTS FOR SIMPLE GROUPS

Let S be a finite nonbelian simple group and let $m(S)$ be the minimal index of a proper subgroup of S.

- (Liebeck and Shalev, 1995) There is a constant c such that $c \cdot m(S) \leq \mu(S)$ for any finite nonabelian simple group S.
- (Blackburn, 2006) If $S = \mathrm{Alt}(n)$, n is a sufficiently large integer and $n \equiv 2 \mod 4$, then $\mu(S) = \sigma(S) = 2^{n-2}$.
- (Britnell, Evseev, Guralnick, Holmes and Maroti, 2007) Let $S = \mathrm{PSL}(n, q)$, $n \geq 12$. If q is odd or $n \not\equiv 2 \mod 4$, then $\mu(S) = \sigma(S)$. In any case $\frac{\mu(S)}{\sigma(S)} \geq 1 - \frac{q-1}{q^n-1} = 1 - \frac{1}{m(S)}$.

KNOWN RESULTS FOR SIMPLE GROUPS

Let S be a finite nonbelian simple group and let $m(S)$ be the minimal index of a proper subgroup of S.

- (Liebeck and Shalev, 1995) There is a constant c such that $c \cdot m(S) \leq \mu(S)$ for any finite nonabelian simple group S.
- (Blackburn, 2006) If $S = \mathrm{Alt}(n)$, n is a sufficiently large integer and $n \equiv 2 \mod 4$, then $\mu(S) = \sigma(S) = 2^{n-2}$.
- (Britnell, Evseev, Guralnick, Holmes and Maroti, 2007) Let $S = \mathrm{PSL}(n, q)$, $n \geq 12$. If q is odd or $n \not\equiv 2 \mod 4$, then $\mu(S) = \sigma(S)$. In any case $\frac{\mu(S)}{\sigma(S)} \geq 1 - \frac{q-1}{q^n-1} = 1 - \frac{1}{m(S)}$.
- If $S = \mathrm{Sz}(q)$, then $\mu(S)/\sigma(S) = 1 - 1/m(S)$.

In general, it seems interesting to investigate the quotient $\mu(S)/\sigma(S)$ for a finite nonabelian simple group.

QUESTION

- Is it true that
$$\frac{\mu(S)}{\sigma(S)} \to 1 \text{ as } |S| \to \infty \text{ ?}$$
- Does there exist a universal constant c such that
$$\frac{\mu(S)}{\sigma(S)} \geq 1 - \frac{c}{m(S)}$$
for all nonabelian finite simple groups S?

WHAT ABOUT ARBITRARY FINITE GROUPS?

No result is known about $\mu(G)$ when G is an arbitrary finite 2-generated group.

QUESTION

For simple groups the numbers $\mu(G)$, $\chi(\Gamma(G))$ and $\sigma(G)$ are not too different and coincide in many cases. Does something similar hold for any finite (non cyclic) 2-generated group?

The crowns of a group play a relevant role in the discussion of problems about generation.

DEFINITIONS

- Let $\mathcal{L}$ be the set of the monolithic primitive epimorphic images L of G.
- For $L \in \mathcal{L}$ and $t \in \mathbb{N}$ define the crown based power of size t:

$$L_t = \left\{ (l_1, \ldots, l_t) \in L^t \;\middle|\; l_1 \equiv \cdots \equiv l_t \bmod \operatorname{soc} L \right\}.$$

- Let $\mathcal{R}$ be the set of normal subgroups R of G, minimal with respect to the property $G/R \cong L_t$ for some $L \in \mathcal{L}$ and $t \in \mathbb{N}$.

PROPOSITION

$x_1, \ldots, x_\mu$ pairwise generate G if and only if $x_1 R, \ldots, x_\mu R$ pairwise generate G/R for each $R \in \mathcal{R}$.

QUESTION

Assume that L is a 2-generated monolithic primitive group and define $\tau = \tau(L)$ as the largest t with the property that L_t is 2-generated.

- Compare $\mu(L)$ and $\mu(L_\tau)$. How much smaller is $\mu(L_\tau)$ than $\mu(L)$?

DIRECT POWER OF SIMPLE GROUPS

If L is a finite nonabelian simple group, then $L_\tau = L^\tau$ where τ is the number of the $\mathrm{Aut}(L)$-orbits on the set of the generating pairs of L.

QUESTION

It is easy to prove that $\sigma(L) = \sigma(L^\tau)$; what about $\mu(L^\tau)$?

REMARK

- Let $\{(x_i, y_i) \mid 1 \leq i \leq \tau\}$ be a set of representatives for the orbits of $\mathrm{Aut}(L)$ on the set of the generating pairs of L;
- define $x := (x_1, \ldots, x_\tau) \in L^\tau$, $y := (y_1, \ldots, y_\tau) \in L^\tau$.

$$L^\tau = \langle \bar{x}, \bar{y} \rangle \Leftrightarrow (\bar{x}, \bar{y}) = (x, y)^\gamma \ \exists \gamma \in \mathrm{Aut}(L^\tau).$$

The non isolated vertices of $\Gamma(L^\tau)$ are the elements of the set Ω of $\mathrm{Aut}(L^\tau)$-conjugates of x. The set Ω induces a subgraph $\bar{\Gamma}$ of $\Gamma(L^\tau)$ which is vertex-transitive and has the same clique-number as $\Gamma(L^\tau)$.

- $\mu(L^\tau)$ is the clique number of $\bar{\Gamma}$ and can be estimated using:

PROPOSITION

If X is a clique and Y a coclique in a vertex-transitive graph on m vertices, then $|X||Y| \leq m$.

- If M is a proper subgroup of L, then $\{(l_1, \ldots, l_\tau) \in \Omega \mid l_1 \in M\}$ is a coclique in $\bar{\Gamma}$.

THEOREM

Define P_M as the conditional probability that $(l_1, l_2) \in M \times L$, given that $\langle l_1, l_2 \rangle = L$. Then $\mu(L^\tau) \leq 1/P_M$.

COROLLARY

There exists a constant c such that for any nonabelian simple group L we have

$$\mu(L^\tau) \leq c \cdot m(L).$$

REMARK

If $n \equiv 2 \mod 4$ and n is large enough then

- $\sigma(\mathrm{Alt}(n)^\tau) = \sigma(\mathrm{Alt}(n)) = 2^{n-2}$;
- $\mu(\mathrm{Alt}(n)^\tau) \leq cn$.

Hence in general $\mu(L^\tau)$ is much smaller than $\sigma(L^\tau)$.

QUESTIONS

- How sharp is our upper bound for $\mu(L^\tau)$?
- $\mu(G) \geq 3$ for any 2-generated finite group. Does there exist a non abelian simple group L with $\mu(L^\tau) > 3$?
- What about the chromatic number of $\Gamma(L^\tau)$?

A SUDOKU GAME

- $\mu(\mathrm{Alt}(5)) = 8$ and $\sigma(\mathrm{Alt}(5)) = 10$.
- $G = \mathrm{Alt}(5)^{19}$ is the largest 2-generated direct power of Alt(5).

REMARK

If $\mu(\mathrm{Alt}(5)^{19}) \geq n$, then there exists a $n \times 19$ matrix, whose entries are elements of Alt(5), such that

- the n elements in each column pairwise generate Alt(5);
- if $\begin{pmatrix} l_1 & l_2 \\ m_1 & m_2 \end{pmatrix}$ is a 2×2 submatrix, then (l_1, m_1) and (l_2, m_2) are not Sym(5)-conjugate.

$$\begin{pmatrix} 5 & 3 & 5 & 5 & 5 & 3 & 3 & 2 & 5 & 5 & 5 & 2 & 2 & 3 & 5 & 5 & 5 & 3 & 3 \\ 5 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 2 & 5 & 2 & 5 & 5 & 2 & 3 & 5 & 3 & 5 & 5 \\ * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \end{pmatrix}$$

- The first two rows of the matrix are known (their columns are a set of representatives for the 19 Sym(5)-conjugate classes of generating pairs). The other rows must contain elements of a given order in the same proportion: 10 element of order 5, 6 elements of order 3, 3 elements of order 2.
- A column contains at most two entries of order 3, and the elements of order 3 must be positioned in such a way that no 2×2 submatrix contains only elements of order 3. This implies

$$3 \leq \mu(\mathrm{Alt}(5)^{19}) \leq 4.$$

QUESTION

Decide whether $\mu(\mathrm{Alt}(5)^{19}) = 3$ or $\mu(\mathrm{Alt}(5)^{19}) = 4$.

$\mu(\mathrm{Alt}(5)^{19} = 4$ if and only if we can construct a matrix with the requested properties and where the orders of the elements are distributed in one of the two following way:

$$\begin{pmatrix} 5 & 3 & 5 & 5 & 5 & 3 & 3 & 2 & 5 & 5 & 5 & 2 & 2 & 3 & 5 & 5 & 5 & 3 & 3 \\ 5 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 2 & 5 & 2 & 5 & 5 & 2 & 3 & 5 & 3 & 5 & 5 \\ 5 & 5 & 5 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 3 & 5 & 3 & 5 & 5 & 2 & 2 & 5 & 2 \\ 5 & 5 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 2 & 5 & 3 & 5 & 5 & 2 & 3 & 5 & 2 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 3 & 5 & 5 & 5 & 3 & 3 & 2 & 5 & 5 & 5 & 2 & 2 & 3 & 5 & 5 & 5 & 3 & 3 \\ 5 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 2 & 5 & 2 & 5 & 5 & 2 & 3 & 5 & 3 & 5 & 5 \\ 5 & 5 & 5 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 3 & 5 & 3 & 5 & 5 & 2 & 2 & 5 & 2 \\ 2 & 2 & 3 & 3 & 5 & 3 & 5 & 5 & 3 & 2 & 5 & 3 & 5 & 5 & 5 & 3 & 5 & 5 & 5 \end{pmatrix}$$

SOLVABLE GROUPS

In the case of solvable groups the precise value of $\sigma(G)$ is known:

THEOREM (TOMKINSON 1997)

Let G be a finite non-cyclic solvable group and let H/K be the smallest chief factor of G having more than one complement in G. Then $\sigma(G) = |H/K| + 1$.

We want to study the relationship between $\mu(G)$ and $\sigma(G)$ when G is a 2-generated solvable group. We start by considering the crown based power.

DEFINITIONS AND USEFUL REMARKS

- Assume that L is a 2-generated solvable primitive group: $L = V \rtimes H$, with H an irreducible subgroup of $\mathrm{GL}(V)$.
- Let $F = \mathrm{End}_H(V)$, $r = |\mathrm{End}_H(V)|$: $L_t = V^t \rtimes H$ is 2-generated if and only if $t \leq r$.
- $L_r = V^r \rtimes H$ is the largest 2-generated crown based power of L.
- We may identify H with a subgroup of $GL(r, F)$.
- $H = \langle X_1, X_2 \rangle \Rightarrow \mathrm{rank} \begin{pmatrix} I_r - X_1 & I_r - X_2 \end{pmatrix} = r$.
- $W \in V^r$ can be viewed as a $r \times r$ matrix with coefficients over F.

PROPOSITION

Assume $W_1, W_2 \in V^r$ and $H = \langle X_1, X_2 \rangle$:

$$L_r = V^r \rtimes H = \langle W_1 X_1, W_2 X_2 \rangle \Leftrightarrow \det \begin{pmatrix} I_r - X_1 & I_r - X_2 \\ W_1 & W_2 \end{pmatrix} \neq 0.$$

The study of the behavior of the crown based power is reduced to the following:

A LINEAR ALGEBRA QUESTION

Assume that $Z_1, \ldots, Z_\mu$ are matrices in $M_{r\times r}(F)$ with the property that

$$\operatorname{rank}\begin{pmatrix} Z_i & Z_j \end{pmatrix} = r \quad \forall i \neq j.$$

Can we find $Y_1, \ldots, Y_\mu \in M_{r\times r}(F)$ such that

$$\det\begin{pmatrix} Z_i & Z_j \\ Y_i & Y_j \end{pmatrix} \neq 0 \quad \forall i \neq j \quad ?$$

AN EASY EXAMPLE

Assume that $X_1, \ldots, X_\mu$ pairwise generate H and that $X_i - X_j$ is a non-singular matrix whenever $i \neq j$. Then

$$\det \begin{pmatrix} 1 - X_i & 1 - X_j \\ I_r & I_r \end{pmatrix} = \det \begin{pmatrix} 1 - X_i & X_i - X_j \\ I_r & 0 \end{pmatrix} \neq 0;$$

we may take $Y_1 = \cdots = Y_m = I_r$ and deduce that $\mu(L_r) \geq \mu$.

LEMMA

Assume that H is a 2-generated irreducible nilpotent subgroup of $\mathrm{GL}(V)$. *If* $L = V \rtimes H$ *and* $r = \dim_{\mathrm{End}_H(V)} V$, *then* $\mu(L_r) = \mu(L)$.

THEOREM

If G is a non cyclic 2-generated solvable group of Fitting length at most 2, then $\mu(G) = \chi(\Gamma(G)) = \sigma(G)$.

QUESTION

Does there exist a 2-generated solvable group with $\mu(G) \neq \sigma(G)$?

GENERALIZATIONS TO PROFINITE GROUPS

DEFINITIONS

- Let G be a profinite group that can be (topologically) generated by $d \geq 2$ elements:
- we denote by $\mu_d(G)$ the largest integer m with the property that there exists an m-tuple of elements of G such that any d distinct entries together (topologically) generate G.

LEMMA

If the non-cyclic group G can be generated by 2 elements, then

$$(d-1)\mu_2(G) \leq \mu_d(G) \leq (d-1)\sigma(G).$$

LEMMA

- $\mu_2(SL(2,\mathbb{Z})) = \sigma(SL(2,\mathbb{Z})) = 4$;
- $\mu_d(SL(2,\mathbb{Z})) = 4(d-1) = \mu_d(SL(2,\mathbb{Z}/2\mathbb{Z}))$.

QUESTION

Is it true that $\mu_d(SL(n,\mathbb{Z})) = \mu_d(SL(n,\mathbb{Z}/2\mathbb{Z}))$ for all integers n and d greater than or equal to 2?

THEOREM

If $n \geq 12$, then the following three statements are true.

1. $\mu_d(\widehat{SL(n,\mathbb{Z})}) = \mu_d(SL(n,\mathbb{Z}/2\mathbb{Z}))$.
2. $\sigma(SL(n,\mathbb{Z})) = \sigma(\widehat{SL(n,\mathbb{Z})}) = \sigma(SL(n,\mathbb{Z}/2\mathbb{Z}))$.
3. *If $n \not\equiv 2 \mod 4$, then* $\mu_d(\widehat{SL(n,\mathbb{Z})}) = (d-1)\mu_2(SL(n,\mathbb{Z}/2\mathbb{Z}))$.

REMARK

Let $G = \widehat{SL(n,\mathbb{Z})}$. Whenever $n \geq 3$, $d \geq 2$ and $d \leq k \leq \mu_d(G)$, the probability is positive that a randomly chosen k-tuple with entries from G has the property that any d entries will together generate G.

- Let G be a profinite group that can be generated by d elements;
- let ν be the normalized Haar measure on G (or on some direct power G^t);
- for any $k \geq d$, let $\Omega(G,k,d)$ be the set of k-tuples of elements of G with the property that every d distinct entries generate G;
- let $P(G,k,d) = \nu(\Omega(G,k,d))$ and $P(G,d) = P(G,d,d)$.

THEOREM

$$P(G,d) > 0 \Leftrightarrow P(G,k,d) > 0 \text{ for all } d \leq k \leq \mu_d(G).$$