Boundedly Generated Subgroups of Finite Groups

Andrea Lucchini

Università di Padova, Italy

2nd Biennial International Group Theory Conference
Istanbul, February 4-8, 2013

An (easy?) question

Assume that G is a finite group and let $\pi(G)$ be the set of prime divisors of the order of G. Does there exist a 2-generated subgroup H of G with $\pi(H) = \pi(G)$?

An (easy?) question

Assume that G is a finite group and let $\pi(G)$ be the set of prime divisors of the order of G. Does there exist a 2-generated subgroup H of G with $\pi(H) = \pi(G)$?

YES! and a stronger result can be proved:

An (easy?) question

Assume that G is a finite group and let $\pi(G)$ be the set of prime divisors of the order of G. Does there exist a 2-generated subgroup H of G with $\pi(H) = \pi(G)$?

YES! and a stronger result can be proved:

Theorem (AL, M. Morigi, P. Shumyatsky (2011))

Let $\mathcal{C}(G)$ be the set of isomorphism classes of composition factors of G, then there exists a 2-generated subgroup H of G such that $\mathcal{C}(H) = \mathcal{C}(G)$.

How a result like this can be proved?

Let L be a primitive monolithic group (L has a unique minimal normal subgroup A, and if A is abelian then A has a complement in G).

The crown-based power of L of size k is the subgroup L_k of L^k defined by: $L_k = \{(l_1, \ldots, l_k) \in L^k | l_1 \equiv \ldots \equiv l_k \bmod A\}$.

Let $d(G)$ denotes the minimal number of generators of the group G.

Theorem (F. Dalla Volta, AL (1998))

Let m be a natural number and let G be a finite group such that $d(G/N) \leq m$ for every non-trivial normal subgroup N, but $d(G) > m$. Then there exists a primitive monolithic group L such that $G \cong L_k$ for some k.

Let $H \leq G$, minimal with the property that $\mathcal{C}(H) = \mathcal{C}(G)$.

Let $H \leq G$, minimal with the property that $\mathcal{C}(H) = \mathcal{C}(G)$.

$$\Downarrow$$

There exists $N \trianglelefteq H$ such that: $d(H/N) = d(H)$ but $d(H/M) < d(H)$ whenever $N < M \trianglelefteq H$.

Let $H \leq G$, minimal with the property that $\mathcal{C}(H) = \mathcal{C}(G)$.

$$\Downarrow$$

There exists $N \trianglelefteq H$ such that: $d(H/N) = d(H)$ but $d(H/M) < d(H)$ whenever $N < M \trianglelefteq H$.

$$\Downarrow$$

There exist L and k with $H/N \cong L_k$.

Let $H \leq G$, minimal with the property that $\mathcal{C}(H) = \mathcal{C}(G)$.

$$\Downarrow$$

There exists $N \trianglelefteq H$ such that: $d(H/N) = d(H)$ but $d(H/M) < d(H)$ whenever $N < M \trianglelefteq H$.

$$\Downarrow$$

There exist L and k with $H/N \cong L_k$.

$$\Downarrow$$

There exists $N \leq H^* \leq H$ with $H^*/N \cong L$.
Since $\mathcal{C}(H) = \mathcal{C}(H^*)$, it must be $H = H^*$, hence $k = 1$.

Let $H \leq G$, minimal with the property that $\mathcal{C}(H) = \mathcal{C}(G)$.

$$\Downarrow$$

There exists $N \trianglelefteq H$ such that: $d(H/N) = d(H)$ but $d(H/M) < d(H)$ whenever $N < M \trianglelefteq H$.

$$\Downarrow$$

There exist L and k with $H/N \cong L_k$.

$$\Downarrow$$

There exists $N \leq H^* \leq H$ with $H^*/N \cong L$.
Since $\mathcal{C}(H) = \mathcal{C}(H^*)$, it must be $H = H^*$, hence $k = 1$.

Theorem (AL, F. Menegazzo (1997))

If L is a primitive monolithic group, then $d(L) = \max(2, d(L/\operatorname{soc} L))$.

Let $H \leq G$, minimal with the property that $\mathcal{C}(H) = \mathcal{C}(G)$.

$$\Downarrow$$

There exists $N \trianglelefteq H$ such that: $d(H/N) = d(H)$ but $d(H/M) < d(H)$ whenever $N < M \trianglelefteq H$.

$$\Downarrow$$

There exist L and k with $H/N \cong L_k$.

$$\Downarrow$$

There exists $N \leq H^* \leq H$ with $H^*/N \cong L$.
Since $\mathcal{C}(H) = \mathcal{C}(H^*)$, it must be $H = H^*$, hence $k = 1$.

Theorem (AL, F. Menegazzo (1997))

If L is a primitive monolithic group, then $d(L) = \max(2, d(L/\operatorname{soc} L))$.

Let $M/N = \operatorname{soc} H/N$: $d(H) = d(H/N) = \max\{2, d(H/M)\} = 2$.

The previous proof suggests a strategy to tackle other similar (more difficult) questions:

Question

Let $i(G)$ be a group invariant. Does there exist $d \in \mathbb{N}$ such that every finite group G contains a d-generated subgroup H with $i(H) = i(G)$?

Strategy

- Let $H \leq G$ minimal such that $i(H) = i(G)$ and let $d = d(H)$.
- There is $N \trianglelefteq H$ s.t. $d(H/N) = d$, $d(H/M) < d \ \forall N < M \trianglelefteq H$.
- $H/N \cong L_k$ for suitable L and k.
- Can we prove that $k \leq t$, where t depends on the invariant we are considering but not on H?
- If the previous question has a positive answer and we can prove that there exists an absolute constant τ such that $d(L_t) \leq \max(d(L), \tau)$ for any choice of L, then we can conclude that $d(H) \leq \tau$.

$d(L_k) \leq f(k)$

Let L be a primitive monolithic group, $A = \operatorname{soc} L$. Assume $d(L) \leq d$.

Assume that A is abelian

Let $q = |\operatorname{End}_{L/A}(A)|$, $q^r = |A|$, $q^s = |\mathrm{H}^1(L/A, A)|$, $\theta = 0$ or 1 according to whether A is a trivial L/A-module or not. Then

$$d(L_k) \leq d \Leftrightarrow k \leq r(d - \theta) - s.$$

Notice that $s < r$, as a consequence of a result of Aschbacher and Guralnick, indeed we have: $|\mathrm{H}^1(L/A, A)| < |A|$.

In particular $d(L_k) \leq \max(d(L), \lceil (k+s)/r \rceil + \theta) \leq \max(d(L), k+1)$.

$d(L_k) \leq f(k)$

Let L be a primitive monolithic group, $A = \operatorname{soc} L$. Assume $d(L) \leq d$.

Assume that A is non abelian

Let $P_{L,A}(d)$ be the conditional probability that d randomly chosen elements of L generate L given that they generate L modulo A. Then

$$d(L_k) \leq d \Leftrightarrow k \leq \frac{P_{L,A}(d)|A|^d}{|C_{\mathrm{Aut}(A)}(L/A)|}.$$

$A = S^n$ where n is a positive integer and S is a nonabelian simple group. It is not difficult to prove that $|C_{\mathrm{Aut}(A)}(L/A)| \leq n|S|^{n-1}|\mathrm{Aut}(S)|$.
We need an estimation of $P_{L,A}(d)$.

$d(L_k) \leq f(k)$

Let L be a primitive monolithic group with non-abelian socle $A \cong S^n$.

Theorem (E. Detomi, C. Roney-Dougal, AL (2013))

If $d \geq d(L)$ then there exists a 2-generated almost simple group Y with socle S such that $P_{L,A}(d) \geq P_{Y,S}(2)$.

Theorem (N. Menezes, M. Quick, C. Roney-Dougal (2012))

If Y is a 2-generated almost simple group with non abelian socle S, then $P_{Y,S}(2) \geq 53/90$ with equality if and only if $Y = \mathrm{Alt}(6), \mathrm{Sym}(6)$.

It follows: if $d(L) \geq d$, then $P_{L,A}(d) \geq 53/90$.
Moreover $P_{L,A}(d) \to 1$ as $|A| \to \infty$.

Prime graph

Denote by $\Gamma(G)$ the prime graph of a finite group G. This is the graph whose set of vertices is $\pi(G)$ and $p, q \in \pi(G)$, with $p \neq q$, are connected by an edge if and only if G has an element of order pq.

Prime graph

Denote by $\Gamma(G)$ the prime graph of a finite group G. This is the graph whose set of vertices is $\pi(G)$ and $p, q \in \pi(G)$, with $p \neq q$, are connected by an edge if and only if G has an element of order pq.

Theorem (M. Morigi, P. Shumyatsky, AL (2011))

Let G be a finite group. Then there exists a 3-generated subgroup H of G such that $\Gamma(H) = \Gamma(G)$.

Prime graph

Denote by $\Gamma(G)$ the prime graph of a finite group G. This is the graph whose set of vertices is $\pi(G)$ and $p, q \in \pi(G)$, with $p \neq q$, are connected by an edge if and only if G has an element of order pq.

Theorem (M. Morigi, P. Shumyatsky, AL (2011))

Let G be a finite group. Then there exists a 3-generated subgroup H of G such that $\Gamma(H) = \Gamma(G)$.

The previous theorem cannon be improved.

$$V_1 = \mathbb{F}_5 \times \mathbb{F}_5, \quad V_2 = \mathbb{F}_7 \times \mathbb{F}_7.$$

$$\mathrm{Sym}(3) \cong \left\langle \alpha_1 := \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \beta_1 := \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \right\rangle \leq \mathrm{GL}(V_1).$$

$$\mathrm{Sym}(3) \cong \left\langle \alpha_2 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \beta_2 := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \right\rangle \leq \mathrm{GL}(V_2).$$

$$(\mathrm{Sym}(3))_2 \cong K = \langle (\beta_1, 1), (1, \beta_2), (\alpha_1, \alpha_2) \rangle \leq \mathrm{GL}(V_1) \times \mathrm{GL}(V_2).$$

$$G := (V_1 \times V_2) \rtimes K.$$

$$d(G) = 3, \text{ but } \Gamma(H) \neq \Gamma(G) \text{ for all } H < G.$$

$$V_1 = \mathbb{F}_5 \times \mathbb{F}_5, \quad V_2 = \mathbb{F}_7 \times \mathbb{F}_7.$$

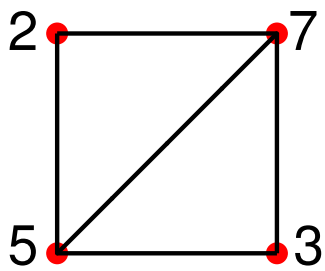
$$\mathrm{Sym}(3) \cong \left\langle \alpha_1 := \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \beta_1 := \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \right\rangle \leq \mathrm{GL}(V_1).$$

$$\mathrm{Sym}(3) \cong \left\langle \alpha_2 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \beta_2 := \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \right\rangle \leq \mathrm{GL}(V_2).$$

$$(\mathrm{Sym}(3))_2 \cong K = \langle (\beta_1, 1), (1, \beta_2), (\alpha_1, \alpha_2) \rangle \leq \mathrm{GL}(V_1) \times \mathrm{GL}(V_2).$$

$$G := (V_1 \times V_2) \rtimes K.$$

$d(G) = 3$, but $\Gamma(H) \neq \Gamma(G)$ for all $H < G$.



$$15 \| |g| \Rightarrow g \in V\langle \beta_2 \rangle$$
$$21 \| |g| \Rightarrow g \in V\langle \beta_1 \rangle$$

Spectrum

The spectrum of a group G is the set of orders of the elements of G.

Spectrum

The spectrum of a group G is the set of orders of the elements of G.

For every positive integer d there exists a group G such that $d(G) = d$ and no $(d-1)$-generated subgroup of G has the same spectrum.

Spectrum

The spectrum of a group G is the set of orders of the elements of G.

For every positive integer d there exists a group G such that $d(G) = d$ and no $(d-1)$-generated subgroup of G has the same spectrum.

- $X = \{p_1, \ldots, p_d\}$ a set of d different odd prime numbers
- $D_i = \langle b_i, a_i \mid b_i^{p_i} = a_i^2 = 1, b_i^{a_i} = b_i^{-1} \rangle \cong D_{2p_i}$, $\quad G = \prod_{i=1}^{d} D_i$
- if $d \geq 2$, then $d(G) = d$
- the spectrum of G is the set of the proper divisors of $m = 2p_1 \cdots p_d$
- the elements of order m/p_i are of the form $(b_1^{r_1}, \ldots, b_{i-1}^{r_{i-1}}, a_i b_i^{r_i}, b_{i+1}^{r_{i+1}}, \ldots, b_d^{r_d})$.

COMPLEX IRREDUCIBLE CHARACTER DEGREES

Let $\pi_{cd}(G)$ be the set of the prime divisors of the complex irreducible character degrees of G.

COMPLEX IRREDUCIBLE CHARACTER DEGREES

Let $\pi_{cd}(G)$ be the set of the prime divisors of the complex irreducible character degrees of G.

THEOREM

Let G be a finite group. There exists a 3-generated subgroup H of G such that $\pi_{cd}(H) = \pi_{cd}(G)$.

COMPLEX IRREDUCIBLE CHARACTER DEGREES

Let $\pi_{cd}(G)$ be the set of the prime divisors of the complex irreducible character degrees of G.

THEOREM

Let G be a finite group. There exists a 3-generated subgroup H of G such that $\pi_{cd}(H) = \pi_{cd}(G)$.

The previous theorem cannot be improved.

- The non abelian group P of order 27 and exponent 3 admits an automorphism α of order 2, acting on $P/\operatorname{Frat}(P)$ as the inverting automorphism.
- Let $G = P \rtimes \langle \alpha \rangle : d(G) = 3$ and $\pi_{cd}(G) = \{2, 3\}$.
- Let $H < G : \pi_{cd}(H) = \{3\}$ if $H \leq P$, $\pi_{cd}(H) = \{2\}$ otherwise.

CONJUGACY CLASS SIZES

Let $\pi_{cs}(G)$ be the set of the prime divisors of the conjugacy class sizes of G.

CONJUGACY CLASS SIZES

Let $\pi_{cs}(G)$ be the set of the prime divisors of the conjugacy class sizes of G.

For every positive integer d there exists a finite group G such that if $H \leq G$ and $\pi_{cs}(H) = \pi_{cs}(G)$ then $d(H) \geq d$.

CONJUGACY CLASS SIZES

Let $\pi_{cs}(G)$ be the set of the prime divisors of the conjugacy class sizes of G.

For every positive integer d there exists a finite group G such that if $H \leq G$ and $\pi_{cs}(H) = \pi_{cs}(G)$ then $d(H) \geq d$.

- To each $\sigma = \{i, j\} \subseteq \{1, \ldots, t\}$, with $i \neq j$, we associate a different prime p_σ.
- Let A_σ be a cyclic group of order p_σ and $A = \prod_\sigma A_\sigma$.
- For $1 \leq i \leq t$, let $C_i = \langle x_i \rangle$ be a cyclic group of order 2 and let $C = \prod_i C_i$.
- We define an action of C on A: x_i centralizes A_σ if $i \notin \sigma$, x_i acts of A_σ as the inverting automorphism otherwise.
- Let $G = A \rtimes C$; $\pi_{cs}(G) = \pi(G) = \{2\} \cup \{p_\sigma \mid \sigma\}$.
- $H \leq G$ and $\pi_{cs}(H) = \pi_{cs}(G) \Longrightarrow d(H) \geq \log_2 t$.

Denote by $\Gamma_{cd}(G)$ the graph whose set of vertices is $\pi_{cd}(G)$ and $p, q \in \pi(G)$, with $p \neq q$, are connected by an edge if and only if $p \cdot q$ divides the degree of an irreducible complex character of G.

Denote by $\Gamma_{cd}(G)$ the graph whose set of vertices is $\pi_{cd}(G)$ and $p, q \in \pi(G)$, with $p \neq q$, are connected by an edge if and only if $p \cdot q$ divides the degree of an irreducible complex character of G.

Open question

Does there exist a positive integer c with the property that every finite group G contains a c-generated subgroup H with $\Gamma_{cd}(H) = \Gamma_{cd}(G)$?

EXPONENT

THEOREM (E. DETOMI, M. MORIGI, P. SHUMYATSKY, AL (2012))

Let G be a finite group. Then there exists a 3-generated subgroup H of G such that H has the same exponent of G.

EXPONENT

THEOREM (E. DETOMI, M. MORIGI, P. SHUMYATSKY, AL (2012))

Let G be a finite group. Then there exists a 3-generated subgroup H of G such that H has the same exponent of G.

A finite solvable group G contains a 2-generated subgroup H with the same exponent. We don't know whether this is true for arbitrary finite groups.

Proof in the solvable case

Assume that G is a finite solvable group without proper subgroups of the same exponent. There exist:

1. an elementary abelian p-group A
2. an irreducible subgroup H of $\mathrm{Aut}(A)$
3. a positive integer k such that $d(G) = d(A^k \rtimes H) > d(A^{k-1} \rtimes H)$
4. an epimorphism $\phi : G \to A^k \rtimes H$.

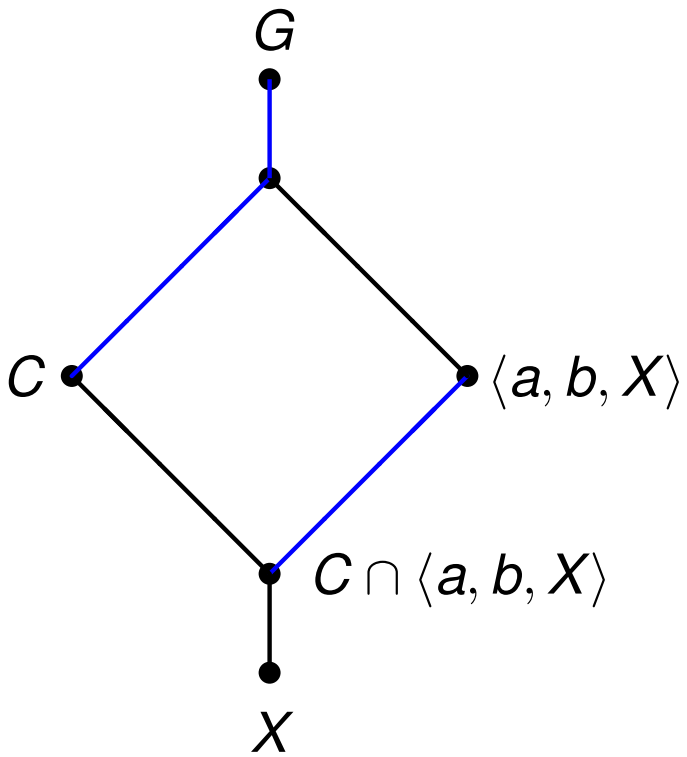
Let $\exp(G) = p^a m$ with $(p, m) = 1$. Choose $g \in G$ with $|g| = p^a$: there exist $a \in A^k$, $h \in H$ with $\phi(g) = ah$. Consider $K = \phi^{-1}(\langle a, H \rangle)$.

$$\begin{aligned} \exp(G) = \exp(K) &\Rightarrow G = K \Rightarrow A^k \rtimes H = \langle a, H \rangle \\ &\Rightarrow A^k \text{ is a cyclic } H\text{-module} \\ &\Rightarrow d(G) = d(A^k \rtimes H) \leq 2 \end{aligned}$$

PRIME DIVISORS OF INDICES

THEOREM

Let G be a finite group and let X, C be subgroups of G with $X \leq C$. Then there exist $a, b \in G$ s.t. $\pi(|G : C|) \subseteq \pi(|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|)$.



When $X = C$ we obtain:

COROLLARY

Let G be a finite group and let C be a subgroup of G. Then there exist $a, b \in G$ such that $\pi(|G : C|) = \pi(|\langle a, b, C\rangle : C|)$.

When X is the identity subgroup we obtain:

COROLLARY

Let G be a finite group and let C be a subgroup of G. Then there exist $a, b \in G$ such that $\pi(|G : C|) \subseteq \pi(|\langle a, b\rangle : C \cap \langle a, b\rangle|)$.

An application

Let $\mathrm{Ind}_G(x)$ be the index in G of the centralizer $C_G(x)$ of x in G.

Theorem (A.R Camina, P. Shumyatsky, C. Sica (2010))

If $\mathrm{Ind}_{\langle a,b,x\rangle}(x)$ is a prime-power for every $a, b \in G$, then $\mathrm{Ind}_G(x)$ is a prime-power.

An application

Let $\mathrm{Ind}_G(x)$ be the index in G of the centralizer $C_G(x)$ of x in G.

Theorem (A.R Camina, P. Shumyatsky, C. Sica (2010))

If $\mathrm{Ind}_{\langle a,b,x\rangle}(x)$ is a prime-power for every $a, b \in G$, then $\mathrm{Ind}_G(x)$ is a prime-power.

This theorem can be restated: let $C = C_G(x)$ and $X = \langle x \rangle$; if there is more than one prime dividing $|G : C|$, then there exist $a, b \in G$ such that $|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|$ is divisible by more than one prime.

From our previous result we have a stronger result: there exist $a, b \in G$ with $\pi(|G : C|) \subseteq \pi(|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|)$. In other words:

An application

Let $\mathrm{Ind}_G(x)$ be the index in G of the centralizer $C_G(x)$ of x in G.

Theorem (A.R Camina, P. Shumyatsky, C. Sica (2010))

If $\mathrm{Ind}_{\langle a,b,x\rangle}(x)$ is a prime-power for every $a, b \in G$, then $\mathrm{Ind}_G(x)$ is a prime-power.

This theorem can be restated: let $C = C_G(x)$ and $X = \langle x \rangle$; if there is more than one prime dividing $|G : C|$, then there exist $a, b \in G$ such that $|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|$ is divisible by more than one prime.

From our previous result we have a stronger result: there exist $a, b \in G$ with $\pi(|G : C|) \subseteq \pi(|\langle a, b, X\rangle : C \cap \langle a, b, X\rangle|)$. In other words:

Theorem

For each $x \in G$ there exists a and b in G such that

$$\pi(\mathrm{Ind}_G(x)) \subseteq \pi(\mathrm{Ind}_{\langle x,a,b\rangle}(x)).$$

Given a subset X of G, let $d_X(G)$ denote the minimum integer d such that there exist d elements $g_1, \ldots, g_d \in G$ with the property that $G = \langle X, g_1, \ldots, g_d \rangle$.

THEOREM

Let X be a subset of a finite group G and let N be a normal subgroup of G such that N is maximal with the property that $d_{XN}(G) = d_X(G)$. Then there exist a monolithic primitive group L and an isomorphism $\varphi : G/N \to L_k$ such that $\varphi(X) \leq \{(l, \ldots, l) \in L^k \mid l \in L\}$.