Local–global generation properties of commutators in finite groups

Evgeny Khukhro

University of Lincoln, UK

Seminar at SUSTech International Center for Mathematics

19 February 2025

Joint work with

Cristina Acciarri, Robert M. Guralnick, and Pavel Shumyatsky

Commutators and centralizers

Recall: a commutator $[g, h] = g^{-1}h^{-1}gh$; it is $= 1$ iff $gh = hg$.

In general, a small number of generators does not mean that the group is small.

But if a group G has finite number m of commutators, then the derived subgroup $[G, G]$ is finite of m-bounded order. The proof is an exercise, follows from Schur's theorem.

Need another piece of notation:

the centralizer $C_G(g) = \{x \in G \mid gx = xg\}$.

Easy to see: $|G : C_G(g)| = |\{[x, g] \mid x \in G\}|$.

Local–global generating property for order

Example (folklore)

Suppose that in a group G there are finitely many commutators, say, m. Then $[G, G]$ has m-bounded order.

Proof: Let $\{[a_1, a_2], \ldots, [a_{2m-1}, a_{2m}]\}$ be all the commutators. Note that $|G : C_G(a_i)| \leqslant m$ for every i.

Since the $[a_{2i-1}, a_{2i}]$ generate $[G, G]$, we can assume that $G = \langle a_1, \ldots, a_{2m} \rangle$.

Then $\bigcap_{i=1}^{2m} C_G(a_i)$ is a central subgroup of m-bounded index.

Then the derived subgroup $[G, G]$ has m-bounded order by Schur's theorem. □

Rank

Definition

A group G has **rank** at most r if every subgroup of G can be generated by r elements.

(also known as the Prüfer rank)

Having a bound for the rank is a good thing:

- finite p-group of rank r has a powerful (very good:-)) subgroup of (p, r)-bounded index;
- a profinite group of finite rank is virtually prosoluble;
- a residually finite group of finite rank is virtually locally soluble;
- a finite soluble group of rank r has r-bounded Fitting height;
- etc.

Local–global generating properties: rank

Analogues for rank: in general, a small number of generators does not mean that the group has small rank.

But for commutators we have the following corollary of one of our main results.

Corollary

Let G be a finite group. Suppose that, for a positive integer r, any subgroup generated by a subset of commutators can be generated by r elements. Then the derived subgroup $[G, G]$ has r-bounded rank.

(Actually, stronger results hold, details below.)

Thus the set of commutators has this 'local–global' property:

r-generation by subsets of this generating set of $[G, G]$

implies $f(r)$-generation of <u>all subgroups</u> of $[G, G]$.

Commutator set

Notation

For a subgroup S of a group G, let $I_G(S)$ denote the set of all commutators

$$I_G(S) = \{[g, s] = g^{-1}g^s \mid g \in G,\ \ s \in S\}.$$

Then the commutator subgroup $[G, S]$ is generated by $I_G(S)$.

In most cases, $[G, S] \neq I_G(S)$.

Local–global rank properties of commutators

One of our main results.

Theorem 1

Let p be a prime, r a positive integer, G a p-soluble finite group, and P a Sylow p-subgroup of G. Suppose that any subgroup generated by a subset of $I_G(P) = \{[g, h] \mid g \in G,\ h \in P\}$ can be generated by r elements.
Then $[G, P]$ has r-bounded rank.

Thus the corresponding set of commutators $I_G(P)$ has this 'local–global' property: r-generation by subsets of this generating set implies $f(r)$-generation of <u>all subgroups</u> of $[G, P]$.

p-Solubility essential

Recall that p-soluble means that there is a normal series with each factor either a p-group or a p'-group.

Examples show that the condition of p-solubility in Theorem 1 cannot be dropped.

Example

For every prime p we produce a series of finite groups G having a Sylow p-subgroup P such that any subgroup generated by a subset of $I_G(P)$ can be generated by 3 elements, while the rank of $[G, P]$ is unbounded.

Remark: In fact, the groups G in these examples are $SL_2(q)$ for certain prime-powers q. There is a hope (work in progress) that we could prove that these SL_2 are the only exceptions, and then the theorem could be extended to all finite groups, with additional dependence on the ranks of such obstructions.

Commutators in any finite groups

The following local–global result is proved for arbitrary finite groups.

Theorem 2

Let G be a finite group. Suppose that for every prime p dividing $|G|$ for any Sylow p-subgroup P, any subgroup generated by a subset of $I_G(P) = \{[g,h] \mid g \in G,\ h \in P\}$ can be generated by r elements. Then the derived subgroup $[G,G]$ has r-bounded rank.

(Stronger than that Corollary above, where the condition was on all commutators.)

Automorphisms

As an important tool in the proofs, we prove the following result about automorphisms, which is also of independent interest.

Theorem 3

Suppose that G is a finite group admitting a group of coprime automorphisms A such that, for a positive integer r, any subgroup generated by a subset of $I_G(A) = \{[g, a] = g^{-1}g^a \mid g \in G,\ a \in A\}$ can be generated by r elements.
Then $[G, A]$ has r-bounded rank.

Here, "coprime" means that $(|G|, |A|) = 1$.

In the proofs we use the Lubotzky–Mann theory of powerful p-groups.

(For example, an analogue of Schur's theorem holds for rank: if $G/Z(G)$ has rank r, then the rank of $[G, G]$ is r-bounded by Lubotzky–Mann.)

Other tools are provided by representation theory of Hall–Higman type.

Remarks on ‘duality’ for automorphisms

A lot of important results derive nice properties of a finite group G from various smallness conditions on $C_G(A)$ for groups of automorphisms A, many of these stemming from the works of J. G. Thompson and G. Higman on automorphisms with small $|C_G(A)|$.

In the same vein, Khukhro & Mazurov 2005–06 proved results on finite groups G with a group of automorphisms A such that $C_G(A)$ has small rank. For example, if A is cyclic of prime order p (in addition coprime to $|G|$ if G is insoluble), then there are normal subgroups $N \leqslant H \leqslant G$ with G/H and N of (p, r)-bounded rank and H/N nilpotent of p-bounded class.

The set $I_G(A) = \{[g, a] \mid g \in G,\ a \in A\}$ is in a sense dual to the set of fixed points $C_G(A)$. For example, for an automorphism α we have $|I_G(\alpha)| = |G : C_G(\alpha)|$.

Theorem 3 represents the ‘dual’ direction, where conditions on the set $I_G(A)$ strongly influence the structure of the subgroup $[G, A]$.

Carter subgroups

A nilpotent self-normalizing subgroup is called a Carter subgroup.

For example, if A is a nilpotent group of automorphisms of G such that $C_G(A) = 1$, then A is a Carter subgroup of the semidirect product $G \rtimes A$.

Carter proved that every finite soluble group has Carter subgroups, they are all conjugate, and the image of a Carter subgroup in a quotient is a Carter subgroup of this quotient. Vdovin recently used CFSG to prove the same for any finite group that has a Carter subgroup; he also determined which almost simple groups have Carter subgroups.

Carter subgroups often behave like coprime groups of automorphisms. For example, Thompson proved that the Fitting height of a finite soluble group G is bounded in terms of composition length of A and the Fitting height of $C_G(A)$ for a soluble group of coprime automorphisms $A \leqslant \mathrm{Aut}\, G$. Then Dade obtained a bound for the Fitting height of a soluble group G in terms of the composition length of a Carter subgroup C.

Commutators and Carter subgroups

Theorem 4

Let C be a Carter subgroup of a soluble finite group G. Suppose that any subgroup generated by a subset of $I_G(C) = \{[g, c] \mid g \in G,\ c \in C\}$ can be generated by r elements. Then $G' = [G, C]$ has r-bounded rank.

Theorem 4 does not hold without the assumption of solubility, as shown by examples. But such examples seem to exist only for a small class of almost simple groups, so it should be possible to obtain a bound for the rank of G' in terms of r and the ranks of these obstructions.

Theorem 5 (Work in progress)

Suppose that a finite group G contains a Carter subgroup C such that any subgroup generated by a subset of $I_G(C)$ can be generated by r elements. Let l be the maximum rank of compositions factors of G isomorphic to $PSL_2(q)$ for $q \equiv 7 \pmod 8$. Then $[G, G] = [G, C]$ has (r, l)-bounded rank.

Proofs depend on the classification

The proofs of Theorems 1, 2, 3, 5 depend on the classification of finite simple groups.

More on the proof for automorphisms

Recall: Theorem 3

$G = [G, A]$, coprime automorphisms A, any subgroup generated by a subset of $I_G(A)$ is r-generated. Then G has r-bounded rank.

First the result is proved for nilpotent G.

Then for semisimple G (direct product of simple groups).

Next the exponent of the automorphisms induced by A on $G/F^*(G)$ is r-bounded. Combined with AGS-TAMS: the Fitting height of soluble A-invariant sections with $H = [H, A]$ is r-bounded, as well as proof for cyclic A.

Next key proposition: can assume G is generated by r-boundedly many orbits of elements of $I_G(A)$ under the action of A.

All of above is used for reducing to the case where A is a p-group of r-bounded derived length, and finishing the proof by induction on this derived length.

Using theory of powerful p-groups

For G nilpotent, it is sufficient to consider a finite p-group $G = [G, A]$. (Showing here case $p \neq 2$, while for $p = 2$ similar.)

(1) If M is a normal A-invariant subgroup of G and $|I_M(A)| = p^m$, then $M \leqslant \zeta_{2m+1}(G)$.

Indeed, if $M \cap \zeta_2(G) \not\leqslant Z(G)$, then $M \cap \zeta_2(G)$ must have nontrivial elements of $I_G(A)$: if A centralized $M \cap \zeta_2$, then $G = [G, A]$ would centralize $M \cap \zeta_2$, a contradiction. Then induction applies.

(2) The rank of A-inv. sections $S = [S, A]$ of exponent p is r-bounded:

Thompson's critical subgroup C has $|[Z(C), A]| \leqslant p^r$, so $Z(C) \leqslant \zeta_{2r+1}$ by (1). Since $[C, G] \leqslant Z(C)$, we obtain $C \leqslant \zeta_{2r+2}$. Hence $[C, \gamma_{2r+2}] = 1$, whence $\gamma_{2r+2} \leqslant Z(C) \leqslant \zeta_{2r+1}$, so $S = [S, A]$ has r-bounded nilp. class, and is r-generated, so its rank is r-bounded.

(3) $N = \gamma_{f(r)}(G)$ is powerful:

assuming $N^p = 1$ have $[N, A]$ small by (2), whence $N \leqslant \zeta_{f(r)}$ by (1), whence $[N, N] \leqslant [\zeta_{f(r)}, \gamma_{f(r)}] = 1$. (Meaning that $[N, N] \leqslant N^p$ in general.)

(4) $N = \gamma_{f(r)}(G)$ is generated by $g(r)$ elements:

in $G/\Phi(N)$ the order $|[\bar{N}, A]| \leqslant p^r$, whence $\bar{N} \leqslant \zeta_{2r+1}$ by (1), so $G/\Phi(N)$ has r-bounded class, plus r-generated $G = [G, A]$.

(5) The rank of G is r-bounded:

G/N has r-bounded class and r-generated, so has r-bounded rank; N is powerful and generated by $g(r)$ elements, so has rank at most $g(r)$.

Semisimple groups

First the classification is used to show that the rank is r-bounded when $G = [G, A]$ is a simple non-abelian group.

Now let $G = [G, A] = S_1 \times \cdots \times S_m$ be a direct product of non-abelian simple groups transitively permuted by A. Claim: then $m - 1 \leqslant r$.

Indeed, take an involution $t \in S_1$; then some $t^{-1}t^a$ with $a \in A$ will give an elementary abelian subgroup of rank $m - 1$ generated by elements of $I_G(A)$, so $m - 1 \leqslant r$ by hypothesis.

Further consideration and completion of the semisimple case
use a theorem from AGS-TAMS paper:
there are $g \in G$ and $a \in A$ such that $[g, a]$ has even order.

Applying Hall–Higman type results

Recall: $G = [G, A]$, coprime automorphisms A, any subgroup generated by a subset of $I_G(A)$ is r-generated. We wish to show that the exponent of the automorphisms induced by A on $G/F^*(G)$ is r-bounded.

Can assume $A = \langle \alpha \rangle$ of prime-power order p^m on $G/F^*(G)$.

By previous step for semisimple groups it is sufficient to consider Sylow s-subgroup S of $F(G/F^*(G))$ with SA acting on V, an elementary abelian q-subgroup of $F(G)$, where $q \neq s, p$.

This is a so-called 'non-modular' Hall–Higman–type situation:
the semidirect product $S\langle \alpha \rangle$ acts faithfully by linear transformations on V regarded as a vector space over $\mathbb{F}_q$.

The classical results of Dade–Shult–Gross would apply if $\langle \alpha \rangle$ also acted faithfully on S: the conclusion would be the minimum polynomial of α on V has degree at least $p^m - p^{m-1}$, which would work in our favour for the rank. But in general here we cannot assume faithful action of $\langle \alpha \rangle$ on S.

Khukhro–Moens variation and connection with rank

Recall: p-automorphism α acts on an s-group S, and the semidirect product $S\langle\alpha\rangle$ acts faithfully by linear transformations on V regarded as a vector space over $\mathbb{F}_q$ (but $\langle\alpha\rangle$ may not act faithfully on S). Goal: the order p^m of the automorphism of S induced by α is r-bounded.

Fortunately, this more general situation was considered in a recent paper of Khukhro and Moens 2022, where it was indeed proved that the minimum polynomial of α on V has degree at least $p^m - p^{m-1}$.

This degree
$= $ dimension of the span of the orbit of some $v \in V$ under $\langle\alpha\rangle$.

But elements $-v + v^\alpha$ belong to $I_G(\alpha)$, so $p^m - p^{m-1} - 1 \leqslant r$ by hypothesis, whence p^m is r-bounded, as required.

Completion of proof of automorphism result

Key proposition: can assume G is generated by r-boundedly many orbits of elements of $I_G(A)$ under the action of A.

All of above is used for reducing to the case where A is p-group of r-bounded derived length, and finishing the proof by induction on this derived length.

Theorem 3 and some of the lemmas in its proof are used in the proofs of Theorems 1, 2 and 4, 5.

Most recent development (last week:-))

Progress towards dropping the condition of coprimeness of automorphisms.

Thank you!