Groups with bounded generation: old and new

Andrei S. Rapinchuk

U of Virginia

Definition 1

An abstract group Γ has *bounded generation* (BG) if there exist $\gamma_1, \ldots, \gamma_d \in \Gamma$ such that

$$\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_d \rangle,$$

where $\langle \gamma_i \rangle$ is cyclic subgroup generated by γ_i.

Profinite version:

Definition 2

A profinite group Γ has *bounded generation* $(\mathrm{BG})_{\mathrm{pr}}$ if there exist $\gamma_1, \ldots, \gamma_d \in \Gamma$ such that

$$\Gamma = \overline{\langle \gamma_1 \rangle} \cdots \overline{\langle \gamma_d \rangle},$$

where $\overline{\langle \gamma_i \rangle}$ is closure of cyclic subgroup generated by γ_i.

- (BG) for $\Gamma \Rightarrow$ $(\mathrm{BG})_{\mathrm{pr}}$ for $\widehat{\Gamma}$ (profinite completion).

- Question of whether the converse is true remained open for a long time.

- Our results show that $(\mathrm{BG})_{\mathrm{pr}} \not\Rightarrow$ (BG).

This indicates that in some situations $(\mathrm{BG})_{\mathrm{pr}}$ may be more useful (and maybe even more natural) than (BG) itself.

We will return to this in the end but for now will talk almost exclusively about (BG) for discrete groups.

Remarks and Examples

(BG) and $(\mathrm{BG})_{\mathrm{pr}}$ are *purely group-theoretic properties*, but both positive and negative results on (BG) have strong number-theoretic connections.

Let us begin with some remarks and examples.

- Every group with (BG) is finitely generated.

- Conversely, every finitely generated *abelian*, or more generally, *nilpotent* group has (BG).

- Every solvable subgroup of $GL_n(\mathbb{Z})$ is polycyclic (Mal′cev) hence has (BG).

In other known cases, verification of (BG) is nontrivial.

First "semi-simple" examples (viz., $\mathrm{SL}_n(\mathbb{Z})$, $n \geqslant 3$) came about from investigation of a linear algebra question.

Every $A \in \mathrm{SL}_n(F)$ (F a field) can be reduced to I_n by a sequence of elementary row/column operations:

$$A \longrightarrow A_1 \longrightarrow \cdots \longrightarrow I_n \qquad \Rightarrow$$

$$A = e_{i_1 j_1}(\alpha_1) \cdots e_{i_r j_r}(\alpha_r) \quad (\alpha_i \in F)$$

where $e_{ij}(\alpha) = \begin{pmatrix} 1 & & \alpha & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$. In fact,

$$\boxed{r \leqslant n^2 + (\mathrm{const}) \cdot n}$$

(<u>independent</u> of A).

Examples

Every $A \in \mathrm{SL}_n(\mathbb{Z})$ can also be reduced to I_n by integral elementary operations, resulting in a factorization

$$A = e_{i_1 j_1}(\alpha_1) \cdots e_{i_r j_r}(\alpha_r) \quad \text{with} \quad \alpha_i \in \mathbb{Z}.$$

Question. Can r be *bounded* by $c(n)$ *independent* of A?

"**No!**" for $n = 2$ b/c $\mathrm{SL}_2(\mathbb{Z})$ is v. free. What about $n \geqslant 3$?

This question was asked by Dennis and van der Kallen in 1979 over any ring $\mathcal{O}$ of algebraic integers.

Theorem (Carter, Keller, 1983)

Let $\mathcal{O} = \mathcal{O}_K$ be a ring of algebraic integers, and $n \geqslant 3$. Then every $A \in \mathrm{SL}_n(\mathcal{O})$ is a product of

$$\leqslant \frac{1}{2}(3n^2 - n) + 68 \cdot \Delta - 1$$

elementaries, $\Delta = \#$ of prime divisors of discriminant of K.

Examples

The theorem results in a factorization

$$\Gamma = \langle \gamma_1 \rangle \cdots \langle \gamma_d \rangle \qquad \text{(BG)}$$

of $\Gamma = \mathrm{SL}_n(\mathcal{O})$ with **all** γ_i unipotent.

The case $\Gamma = \mathrm{SL}_2(\mathcal{O})$, where $\mathcal{O} = \mathcal{O}_{K,S}$ is ring of S-integers in a number field K, was completely resolved only recently.

When $\mathcal{O}$ is $\mathbb{Z}$ or ring of integers of imaginary quadratic field, Γ fails to have (BG). All other cases are covered in

Theorem (Morgan, R., Sury, 2018)

Assume that $\mathcal{O}^\times$ is infinite. Then every $A \in \mathrm{SL}_2(\mathcal{O})$ is a product of $\leqslant 9$ elementaries.

- Cooke and Weinberger (1975): assertion can be derived from GRH (still unproven!)

- Morris (Witte) reworked (2007) preprint of Carter, Keller and Paige to prove existence of a bound using model theory – no explicit bound can be obtained!

- Vsemirnov (2014) proved assertion for $\mathcal{O} = \mathbb{Z}[1/p]$ using results of Heath-Brown.

Our proof relies only on traditional ANT.

Note that theorem yields a factorization (BG) for $\Gamma = \mathrm{SL}_2(\mathcal{O})$ where generally *some* γ_i are unipotent and *some* semi-simple (with unipotents necessarily present!).

Examples (cont.)

(BG) is known for many other S-arithmetic subgroups of isotropic simple algebraic groups over number fields:

- Tavgen (1990) proved (BG) for all Chevalley groups of rank > 1 and many quasi-split groups.

- Erovenko, R. (2006) considered isotropic, but not necessarily split or quasi-split, orthogonal groups.

- Heald (2013) considered some isotropic unitary groups.

Why are we interested in groups with (BG)?

• **SS-rigidity** A group Γ is *SS-rigid* if it has finitely many equivalence classes of completely reducible representations $\rho\colon \Gamma \longrightarrow GL_n(\mathbb{C})$ in each dimension n.

If Γ is finitely generated, one defines *character variety* $X_n(\Gamma)$. Then Γ is SS-rigid $\Leftrightarrow$ $\dim X_n(\Gamma) = 0$ for all n.

Theorem (R., 1990)

If Γ has (BG) and satisfies

(F^{ab}) *every finite index subgroup $\Gamma_1 \subset \Gamma$ has finite abelianization $\Gamma_1^{ab} = \Gamma_1/[\Gamma_1, \Gamma_1]$,*

then *Γ is SS-rigid.*

Remarks. 1. Without (F^{ab}), Γ cannot be SS-rigid.

2. Assertion remains true if (BG) for Γ is replaced by $(\mathrm{BG})_{\mathrm{pr}}$ for $\widehat{\Gamma}$.

• **Congruence subgroup problem** Let $G \subset \mathrm{GL}_n$ be an algebraic group over a number field K, S be a set of places of K containing all archimedean ones, $\mathcal{O}_S$ be ring of S-integers, $\Gamma = G(\mathcal{O}_S)$.

$\widehat{\Gamma}$ - completion of Γ for topology defined by *all* finite index (normal) subgroups $N \subset \Gamma$

$\overline{\Gamma}$ - completion of Γ for topology defined by congruence subgroups $\Gamma(\mathfrak{a})$ for nonzero ideals $\mathfrak{a} \subset \mathcal{O}_S$

Then $\ker\left(\widehat{\Gamma} \to \overline{\Gamma}\right)$ is *congruence kernel* $C = C(G, S)$.

$C = \{1\} \iff$ every (normal) subgroup $N \subset \Gamma$ of finite index contains some $\Gamma(\mathfrak{a})$

Congruence subgroup problem is to compute C, in particular, to determine when C is finite.

Theorem (Lubotzky, Platonov - R., 1992)

Let G be absolutely almost simple and simply connected.

Assume that S does not contain any nonarchimedean v such that G is K_v-anisotropic and G/K satisfies Margulis-Platonov conjecture.

Then *C is finite iff $\widehat{\Gamma}$ has* $(\mathrm{BG})_{\mathrm{pr}}$. *Thus, if Γ has* (BG) *then C is finite.*

Shalom, Willis (2013) used (BG) to prove Margulis-Zimmer conjecture in some cases.

(BG) was also used to estimate Kazhdan constants (Kassabov)

and to study first-order rigidity (Avni, Lubotzky, Meiri).

$(\mathrm{BG})_{\mathrm{pr}}$ for pro-p groups is equivalent to *analyticity*.

Available results created expectation that higher rank lattices should have (BG).

(Fujiwara (2005) noted that rank-one lattices do not have (BG))

While borderline between *rank-one* and *higher rank* lattices is always expected, as far as (BG), there is also borderline between *non-uniform* and *uniform* cases.

Over more than 30 years no examples of S-arithmetic subgroups of simple anisotropic groups over number fields with (BG) have been found. (Recall: G is anisotropic over a field K of char 0 if $G(K)$ does not contain unipotents $\neq e$.)

Question A. *Can* (BG) *possibly hold for an infinite S-arithmetic subgroup of an anisotropic simple algebraic group?*

In all known examples of S-arithmetic subgroups with (BG), the corresponding factorizations (BG) always involve unipotent elements.

Question B. *Which linear groups are boundedly generated by semi-simple elements?*

Main Theorem (Corvaja, R., Ren, Zannier, 2020)

Let $\Gamma \subset \mathrm{GL}_n(K)$ *be a linear group,* $\mathrm{char}\, K = 0$, *which is* **not** *virtually solvable. Then any possible presentation* (BG) *for* Γ *involves at least* **two** *non-semi-simple elements. In particular, a linear group boundedly generated by semi-simple elements is virtually solvable.*

(There are solvable finitely generated linear groups without (BG).)

We say that $\Gamma \subset \mathrm{GL}_n(K)$ is *anisotropic* if it consists only of semi-simple elements.

Corollary 1

An anisotropic linear group $\Gamma \subset \mathrm{GL}_n(K)$, $\mathrm{char}\, K = 0$, *has* (BG) *iff it is finitely generated and virtually abelian.*

Corollary 2

Infinite S-arithmetic subgroups of simple anisotropic algebraic groups do not have (BG).

- Any $A \in \mathrm{SL}_n(\mathbb{Z})$ can be reduced to $\begin{pmatrix} a & b & \\ c & d & \\ & & I_{n-2} \end{pmatrix}$ by $\leqslant 1/2 \cdot (3n^2 - n)$ elementary operations.

So, it is enough to show that any $\begin{pmatrix} a & b & \\ * & * & \\ & & 1 \end{pmatrix}$ can be reduced to I_3 inside $\mathrm{SL}_3(\mathbb{Z})$ by a bounded number of elementary operations.

- Bounded multiplicativity of Mennicke symbols: for $\ell > 0$

$$\begin{pmatrix} a & b & \\ * & * & \\ & & 1 \end{pmatrix}^{\ell} \Rightarrow \begin{pmatrix} a^{\ell} & b & \\ * & * & \\ & & 1 \end{pmatrix}$$ by 16 elementary operations.

One elementary operation: $\begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} a & b+ta & \\ c & d+tc & \\ & & 1 \end{pmatrix}$

So, using Dirichlet's Prime Number Theorem, we can assume that $b = p$ a prime.

Applying Dirichlet's Theorem twice, we can assume that

$A = \begin{pmatrix} u & p & \\ q & v & \\ & & 1 \end{pmatrix}$ with p, q odd primes and $\gcd(\frac{p-1}{2}, \frac{q-1}{2}) = 1$

Find $m, n > 0$ such that $m \cdot \frac{p-1}{2} - n \cdot \frac{q-1}{2} = \pm 1$ and set

$$s = m \cdot \frac{p-1}{2} \quad \text{and} \quad t = n \cdot \frac{q-1}{2}$$

.

We have $u^s \equiv \pm 1 (\mathrm{mod}\, p)$, so

$$A^s \overset{16}{\Rightarrow} \begin{pmatrix} u^s & p & \\ * & * & \\ & & 1 \end{pmatrix} \overset{1}{\Rightarrow} \begin{pmatrix} \pm 1 & p & \\ * & * & \\ & & 1 \end{pmatrix},$$

which is a bounded product of elementaries. So, A^s is a bounded product of elementaries.

Applying transpose and using same argument, we find that A^t is also a bounded product of elementaries.

Then $A^{\pm 1} = (A^s) \cdot (A^t)^{-1}$ is a bounded product of elementaries.

Van der Kallen (1980) showed that there is no bound N such that every matrix in $SL_3(\mathbb{C}[x])$ is a product of $\leqslant N$ elementaries.

Question of whether there is such a bound for $SL_3(\mathbb{Q}[x])$ or $SL_3(\mathbb{Z}[x])$ is open.

Main Theorem

Let $\Gamma \subset \mathrm{GL}_n(K)$ *be a linear group,* $\mathrm{char}\, K = 0$*, which is* **not** *virtually solvable. Then any possible presentation* (BG) *for* Γ *involves at least* **two** *non-semi-simple elements. In particular, a linear group boundedly generated by semi-simple elements is virtually solvable.*

First, we make two reductions:

1. By a specialization argument, we show that it is enough to prove Main Theorem when K is a number field, i.e. $\Gamma \subset \mathrm{GL}_n(\overline{\mathbb{Q}})$.

2. Assuming that Γ is not virtually solvable, one reduces to case where connected component G° of Zariski-closure G of Γ is *nontrivial* semi-simple group.

For $\gamma \in \mathrm{GL}_n(\overline{\mathbb{Q}})$, let $\Lambda(\gamma)$ denote subgroup of $\overline{\mathbb{Q}}^\times$ generated by eigenvalues of γ. Key statement is the following.

Theorem

Let $\gamma_1, \ldots, \gamma_r \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ be semi-simple with one possible exception, and let $\gamma \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ be another semi-simple matrix.

Assume that γ has an eigenvalue λ which is not a root of unity and which satisfies

$$\langle \lambda \rangle \bigcap [\Lambda(\gamma_1) \cdots \Lambda(\gamma_r)] = \{1\}.$$

Then $\langle \gamma \rangle \bigcap \langle \gamma_1 \rangle \cdots \langle \gamma_r \rangle$ is finite. In particular,

$$\langle \gamma \rangle \not\subset \langle \gamma_1 \rangle \cdots \langle \gamma_r \rangle.$$

To complete proof of Main Theorem we need to show that given $\gamma_1, \ldots, \gamma_r \in \Gamma$, there exists a semi-simple $\gamma \in \Gamma$ of infinite order such that

$$\Lambda(\gamma) \bigcap [\Lambda(\gamma_1) \cdots \Lambda(\gamma_r)] = \{1\}.$$

This follows from existence of *generic elements* in Zariski-dense subgroups of semi-simple groups (Prasad, R., 2003).

Proof of key statement critically depends on

Laurent's Theorem

Let Ω be a finitely generated subgroup of $(\overline{\mathbb{Q}}^{\times})^N$, and let $\Sigma \subset \Omega$. Then Zariski-closure of Σ in $T = (\mathbb{G}_m)^N$ is a finite union of translates of algebraic subgroups of T.

We consider case where all γ_i are semi-simple.

We can find $g, g_1, \ldots, g_r \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ so that

$$\begin{aligned} g^{-1}\gamma g &= \mathrm{diag}(\lambda_1, \ldots, \lambda_n), \quad \lambda_1 = \lambda, \\ g_i^{-1}\gamma_i g_i &= \mathrm{diag}(\lambda_{i1}, \ldots, \lambda_{in}), \quad i = 1, \ldots, r. \end{aligned}$$

Let $p(x_{11}, \ldots, x_{rn}) \in \overline{\mathbb{Q}}[x_{11}, \ldots, x_{rn}]$ be (11)-entry of

$$g^{-1} \cdot \left[\prod_{i=1}^{r} (g_i \cdot \mathrm{diag}(x_{i1}, \ldots, x_{in}) \cdot g_i^{-1}) \right] \cdot g.$$

Let $J = \{ m \in \mathbb{Z} \mid \gamma^m \in \langle \gamma_1 \rangle \cdots \langle \gamma_r \rangle \}$.

Then for each $m \in J$ there exist $a_1(m), \ldots, a_r(m) \in \mathbb{Z}$ so that

$$\gamma^m = \gamma_1^{a_1(m)} \cdots \gamma_r^{a_r(m)}.$$

By our choice of p we have

$$\lambda^m = p\left(\lambda_{11}^{a_1(m)}, \ldots, \lambda_{rn}^{a_r(m)}\right).$$

This polynomial identity holds on

$$\Sigma = \{ (\lambda^m, \lambda_{11}^{a_1(m)}, \ldots, \lambda_{rm}^{a_r(m)}) \mid m \in J\} \subset$$

$$\subset \Omega = \langle \lambda \rangle \times \langle \lambda_{11} \rangle \times \cdots \times \langle \lambda_{rn} \rangle \subset \overline{\mathbb{Q}}^{\times\,(1+rn)}.$$

Assuming that J is infinite and using description of Zariski-closure $\overline{\Sigma}$ provided by Laurent's Theorem, we obtain

$$\lambda^{\ell} \in \Lambda(\gamma_1) \cdots \Lambda(\gamma_r) \quad \text{for some} \quad \ell \neq 0.$$

A contradiction.

Many (infinite) S-arithmetic subgroups Γ of anisotropic simple groups are known to have *congruence subgroup property*, i. e. congruence kernel C is finite.

Then $\widehat{\Gamma}$ satisfies $(\mathrm{BG})_{\mathrm{pr}}$ **but** Γ itself fails to satisfy (BG).

Other conditions. SS-rigidity and CSP follow from *weaker* conditions.

Let $\Gamma^{(n)}$ be (normal) subgroup generated by nth powers.

(PG) there exist c, k such that $|\Gamma/\Gamma^{(n)}| \leqslant cn^k$ for all n,

or even weaker condition

(PG)′ for any m and a prime p there exist c, k such that $|\Gamma/\Gamma^{(mp^{\alpha})}| \leqslant cp^{k\alpha}$ for all α.

For $\mathrm{SL}_n(\mathbb{Z})$, $n \geqslant 3$, condition (PG)′ can be verified by purely algebraic computations w/o using any number-theoretic results.

(PG)′ can also be analyzed by computer-based experiments.

Problem 1

Let Γ be an S-arithmetic subgroup of a simple algebraic group G over a number field K. Prove that if $\sum_{v \in S} \mathrm{rk}_{K_v} G \geqslant 2$ then Γ satisfies (PG)′.

Amalgams. $\Gamma = \mathrm{SL}_2(\mathbb{Z}[1/p])$ is an amalgamated product

$$\Gamma = \Gamma_1 *_{\Gamma_0} \Gamma_2, \qquad [\Gamma_1 : \Gamma_0] = [\Gamma_2 : \Gamma_0] = p + 1,$$

$\Gamma_1 \simeq \Gamma_2 \simeq \mathrm{SL}_2(\mathbb{Z})$ (v. free). Γ has (BG).

Consider $\Gamma = G(\mathbb{Z}[1/p, 1/q])$ where $G = \mathrm{SL}(1, \mathbb{H})$, $\mathbb{H}$ algebra of Hamiltonian quaternions over $\mathbb{Q}$, p, q odd primes.

It has a similar presentation as an amalgamated product **but** does not have (BG).

Problem 2

Give a verifiable condition for amalgamated products $\Gamma = \Gamma_1 *_{\Gamma_0} \Gamma_2$ to have (BG) or to satisfy (PG)′.

Grigorchuk and Fujiwara gave necessary conditions for amalgamated products to have (BG) but these do not apply to above examples.

General question. Do all examples of "semi-simple" linear groups with (BG) involve S-arithmetic groups in an essential way?

Is this true for those linear groups that are nontrivial amalgamated products?