Bounded generation in linear groups and exponential parametrizations

(based on joint work with P. Corvaja, J. Demeio, A. Rapinchuk and J. Ren)

22 December 2022

Bounded Generation in an abstract group Γ may be seen as a strong form of **Finite Generation (FG)**. Indeed, we have:

DEFINITION: The group Γ is said to be **boundedly generated** (abbr. (BG)) if there exist $\gamma_1, \dots, \gamma_r \in \Gamma$ such that

$$\Gamma = \gamma_1^{\mathbb{Z}} \cdots \gamma_r^{\mathbb{Z}} := \{ \gamma_1^{m_1} \cdots \gamma_r^{m_r} : m_1, \dots, m_r \in \mathbb{Z} \}$$

- The "bounded generators" γ_i need not be distinct.
- (BG) is sometimes called **Finite cyclic width**.

Examples

- Every (virtually) abelian, or even (virtually) nilpotent group has (BG) as soon as it has (FG).

- An extension G: $1 \to N \to G \to H \to 1$ where N, H have (BG), has itself (BG).

  In particular, a solvable group has (BG) provided all pieces in a solvability filtration are (FG).

  However there are solvable groups (already in SL_2) having (FG) but not (BG) (an example appears in a paper at the basis of this talk).

Through a result by Mal'cev it follows that every solvable subgroup of $GL_n(\mathbb{Z})$ (is polycyclic hence) has (BG).

OUR CONTEXT

We shall be concerned with $\boxed{\text{linear groups}}$ Γ, i.e. subgroups of $G(k)$ for some linear algebraic group G and field k, here assumed of char. 0 (and usually a number field).

Typically, we also restrict the entries to lie in some subring of k, e.g. the ring $\mathcal{O}_K$ of algebraic integers in K. (Context of the so-called "arithmetic groups".)

RELEVANCE OF (BG)

In this setting the (BG) property has been found to have several relevant consequences toward many other known questions on linear groups.

For instance, we may recall the

following:

- As shown by Rapinchuk (1990) (BG) has strong implications toward finiteness of completely reducible complex representation in any given dimension. ("SS-rigidity")

- We mention e.g. work of Lubotzky 1992 and Platonov-Rapinchuk 1992: they proved the congruence subgroup property for certain arithmetic groups, provided (BG) holds.

- Also, Shalom-Willis 2013 used crucially (BG) for proving the Margulis-Zimmer conjecture for certain arithmetic subgroups of Chevalley groups.

- Further implications of (BG) appear in work by Avni, Lubotzky, Meiri.

SOME EXAMPLES AND REMARKS

- (BG) does NOT hold for $SL_2(\mathbb{Z})$.

In fact, this contains a non-cyclic free group of finite index (e.g., Γ_2) and it is not difficult to see that this excludes (BG)

- Carter - Keller 1983 proved (BG) for $SL_n(\mathcal{O})$ ($n \geq 3$, $\mathcal{O}$ = ring of integers in a number field) actually using only elementary matrices (hence unipotent) as generators.

- For $n=2$ this holds if and only if $\mathcal{O}$ has infinite unit group: Morgan, Rapinchuk, Sury 2018

PAUSE : (BG) and parametrizations

Bounded generation by UNIPOTENT matrices allows in particular to parametrize polynomially $SL_n(\mathcal{O})$, $n \geq 3$, in the sense that there is (for some N) a surjective polynomial map $P: \mathcal{O}^N \to SL_n(\mathcal{O})$.

This follows after observing that the entries of γ^m, for γ a unipotent matrix, are polynomials in m.

This is a kind of diophantine property

which can be of independent motivation and interest.

Remark: In fact, a polynomial parametrization exists also for $n=2$, after work by Vaserstein 2010 and Larsen-Nguyen 2021.
(Counterexamples to a question of Skolem.)

In particular, this shows that a polynomial parametrization does not imply (BG), which e.g. does not hold for $SL_2(\mathbb{Z})$, as noted above.

Instead, if we ALSO have SEMI SIMPLE matrices, we obtain parametrizations by semi-exponential polynomials.

At the other extreme, we have Purely Exponential Parametrizations (PEP) if only semisimple elements occur in a BG.
We shall meet this restriction below.

These facts follow easily: on diagonalizing a semi-simple matrix γ, we see that the entries of γ^m are linear forms in the m-th powers of the eigenvalues.

Back to Bounded Generation

- Further examples were found of linear groups with (BG). For instance,
  the result by Carter-Keller was extended by Tavgen 1991 to all 'Chevalley groups' of rank >1 and to most 'quasi-split' groups.

These (and some other) results raised the expectation that (BG) could hold in even rather greater generality

UNIPOTENT vs. SEMISIMPLE BOUNDED GENERATION

As remarked before:
In many of the quoted results, e.g. about $SL_n(\mathcal{O})$, bounded generation occurs with UNIPOTENT elements. However one would need also to allow SEMISIMPLE elements for other potential applications of the (BG) property.

From now on, with this in mind,

I shall call anisotropic any subgroup Γ of $GL_n(k)$ that contains only semisimple elements, and I shall for the moment think of (BG) for such a group.

Examples:

- Virtually abelian groups generated by semisimple matrices. (A trivial case.)

- Quaternions of norm 1 over certain rings of S-integers.

- More generally, replace quaternions with other division algebras.

- Orthogonal groups of quadratic forms not representing zero. (One gets many examples working over number fields or over rings $\mathbb{Z}[\frac{1}{n}]$.)

These examples motivate the above terminology "anisotropic".

Remark

We have already remarked that a group

Γ admitting (BG) by semisimple elements may be parametrized by purely exponential polynomials.

$$E(x_1,\dots,x_r)=\sum_{j=1}^{h} c_j\,\lambda_1^{\ell_{j1}(\underline{x})}\cdots\lambda_s^{\ell_{js}(\underline{x})}$$

with constants c_j, λ_i, and linear forms $\ell_{i\mu}$ in r variables $x_1,\dots,x_r$, supposed here to take integer values.

A DICHOTOMY

The dichotomy polynomials ⟺ exponential polynomials may remind of the Hilbert X problem, when Matijasevich reduced certain exponential diophantine equations to usual ones.

The same dichotomy appears with integral points on curves of genus 0, depending on the number, 1 or 2, of points at ∞.)

And we have just observed once more this dichotomy on considering (BG) for linear groups.

Despite the behaviour of polynomials

being quite different from exponential ones, there was expectation that some nontrivial (F.G) anisotropic groups over rings of S-integers would still satisfy (BG).

However, no such example was found.

Indeed, in joint work with

Corvaja, Rapinchuk, Ren 2021

we have instead realized strong limitations to (BG) in linear FG anisotropic groups.

In order to state some results, let as above

K be a field of char. 0

and let

$\Gamma \subset GL_n(K)$ be a linear group.

We have:

Theorem 1 (with Corvaja, Rapinchuk, Ren 2021)

If Γ is boundedly generated by semi-simple elements, then it is virtually solvable.

Remarks

One may even allow one non-semisimple generator, with the same conclusion.

This supplementary result costs some effort in the arguments. Indeed, we have:

Open question: Which is the maximum number of such elements that we can allow in order to keep the conclusion?

Examples show that we can't allow more than four. (Consider $SL_2(\mathbb{Z}[1/p])$.)

NOTE: Non-semi-simple elements lead to ordinary diophantine equations, so might even lead to undecidable issues.

There exist v. solvable (FG) linear groups without (BG), so a pure converse does not hold.

PROFINITE (BG)

There is a pro-finite version $(BG)_{pr}$ of the concept of (BG), and it may be proved that, if $\hat{\Gamma}$ denotes the profinite completion of Γ then

$$(BG) \text{ for } \Gamma \Longrightarrow (BG)_{pr} \text{ for } \hat{\Gamma}.$$

It was an open question whether the

converse implication holds.

The above theorem leads to a negative answer to the question, providing examples of (FG) groups Γ without (BG) but such that the analogue property $(BG)_{pr}$ holds for the profinite completion $\widehat{\Gamma}$, moreover assumed Hausdorff.

To obtain this result, one combines some results by Platonov-Rapinchuk and uses the following necessary and sufficient condition for (BG) in anisotropic groups, a Corollary of the above theorem:

Corollary: If Γ is anisotropic then it has (BG) if and only if it has (FG) and it is virtually abelian.

This corollary is a quick consequence of the previous Theorem. Indeed, a (FG) v. abelian group clearly has (BG). Conversely, if we assume (BG), the theorem implies that Γ is v. solvable, and it may be proved through general theory that this, together with "anisotropic", implies v. abelian

NOTE

in positive characteristic, it was shown by Abért, Lubotzky, Pyber 2003 that

(BG) $\Longrightarrow$ virtually abelian

without further conditions.

Their methods are completely different from ours.
And conversely our methods do not apply, as they stand, to positive characteristic.

FURTHER RESULTS

More recently, in joint work also with Demeio, and by means of a partially different method, we obtained more precise conclusions, concerning moreover general Purely Exponential Parametrizations for a group Γ as above.

Namely: We consider (Exponential) parametrizations, without the assumption that they come from (BG).)

Theorem 2 (with Corvaja, Demeio, Rapinchuk, Ren, 2022)

The following are equivalent:

(a) Γ has a Purely Exponential Parametrization

(b) Γ is anisotropic and has (BG).

(c) Γ is finitely generated and the identity component of its Zariski closure is a torus.
in particular, Γ is virtually abelian

NOTE: Recall that a (usual) Polynomial Parametrization instead does NOT generally imply (BG).

In turn, this result is a consequence of "sparseness" of sets obtained from a PEP. This feature did not directly appear in the arguments for the former result.

ABOUT ESTIMATES FOR SPARSENESS

We omit detailed explicit statements for time reasons, and we only say that this sparseness is expressed by estimates related to Heights.

(Here we work with a Γ over a number field and we use Paula Cohen-Tretkoff notation: Height (resp. height) for the exponential (resp. logarithmic) Weil affine heights.)

The estimates have the shape

$$\ll (\log T)^r$$

for the number of elements in Γ of Height $\leq T$ and coming from a PEP.

Such estimate may be even turned into an asymptotic formula

$$\sim c(\log T)^{r'}, \quad \text{some } r' \leq r.$$

This more precise information in fact is not strictly needed for the present applications.

These estimates look natural. However consider that large integer values of the variables $x_1, \dots, x_r$ could a priori produce small values for the exponential polynomials $E(x_1, \dots, x_r)$ in question.

Similar estimates were produced by other authors, e.g. Everest ~ Shparlinski 1999, but worked under restrictions which would prevent our applications.)

The estimates are essentially derived from the following lower bound:

Let E be a purely exponential polynomial. We call $\underline{x} \in \mathbb{Z}^r$ minimal (for E) if $|\underline{x}|$ is minimal among all $\underline{x}' \in \mathbb{Z}^r$ with

$$E(\underline{x}') = E(\underline{x}).$$

There exists a $C = C_E > 0$ s.t.

$$h(E(\underline{x})) \geq C|\underline{x}|$$

for all $\underline{\text{minimal}}$ $\underline{x} \in \mathbb{Z}^r$, except for a FINITE set of values $E(\underline{x})$.

The condition on minimality is easily seen to be necessary.

In order to compare these UPPER estimates with LOWER BOUNDS, let us restrict for instance to S-arithmetic groups, of the shape

$$\Gamma = G(\mathcal{O}_S)$$

where G is an algebraic subgroup of some GL_n and $\mathcal{O}_S$ is the ring of S-integers of the number field K.

Then in general, with "mild" assumptions, we have estimates

$$\gg T^{\delta} \quad , \text{ some } \delta > 0$$

for the number of elements of Height $\leq T$ in the whole Γ.

(These go back to Siegel, Weil, ..., in some important cases; in our paper we put together a number of separate results in this direction obtained until recently.

Again, these lower bounds are not strictly needed for the above theorem. However of course they illustrate the "sparseness" alluded to above.

In the sequel for time reasons we shall not be able to mention any real detail and shall only give rough descriptions.

SOME STEPS OF OUR PROOFS

1 REDUCTION TO LINEAR GROUPS OVER NUMBER FIELDS.

Let us think of Theorem 1 above:

(BG) by semisimple $\Longrightarrow$ virtually solvable

For this we consider first the $\mathbb{Q}$ algebra of regular functions on the Zariski closure G our group Γ.

We assume by contradiction that

- Γ is NOT virtually solvable but
- Γ has (BG) with semisimple elements

One argues now by specialization to points of GL_n defined over $\overline{\mathbb{Q}}$.

- It is easy to find specializations which maintain the SECOND property
- Arguing with the derived series

(and using uniform boundedness of its length for v. solvable groups inside GL_n) one also proves the existence of "good specializations", i.e., preserving the FIRST property.

Remark: This kind of reduction has alternatives and can be avoided in some arguments, but it is useful and practical for the whole context, especially for the statements depending on estimates.

---

(2) EXISTENCE OF MULTIPLICATIVELY INDEPENDENT EIGENVALUES

- We let $\gamma_1, \dots, \gamma_r \in GL_n(K)$ be Bounded Generators for Γ, where now K is a number field.

- We are also assuming that Γ is NOT virtually solvable.

Then, by taking the quotient

$$G' := G/R$$

where R is the radical of G^0 (= component of 1) and working in G in place of G, it is not difficult to see that we may further assume that

$$\boxed{G^\circ \text{ is a non-trivial semi-simple group}}$$

At this point, using Prasad-Rapinchuk theory of generic elements one deduces the

Existence of $\gamma \in \Gamma$ such that its eigenvalues are multiplicatively independent from those of $\gamma_1, \dots, \gamma_r$.

By this we mean that the respective eigenvalues generate subgroups of $\overline{\mathbb{Q}}^*$ with trivial intersection.

Remark: Multiplicative independence of values of rational functions on algebraic varieties falls within the topic usually called Unlikely Intersections. The present case is an instance, viewing the eigenvalues as functions on a suitable cover of G. In this view, the said result is not unrelated to theorems obtained jointly with Bombieri and Masser, later refined by Maurin.

SUMMARY OF THE PRESENT SETTING.

We have obtained a matrix $\gamma \in \Gamma$ having an eigenvalue λ, not a root of unity, and such that, denoting $\mu_1, \dots, \mu_s$ the eigenvalues of the hypothetical bounded semisimple generators $\gamma_1, \dots, \gamma_r$ of Γ, we have

$$\lambda^{\mathbb{Z}} \cap \mu_1^{\mathbb{Z}} \cdots \mu_s^{\mathbb{Z}} = \{1\}.$$

We may assume that $\lambda, \mu_1, \dots, \mu_s \in K$.

---

3 APPLICATION OF THE THEORY OF INTEGRAL POINTS ON SUBVARIETIES OF TORI $\mathbb{G}_m^r$.

We prove that not all powers of the matrix γ constructed above lie in the set $\gamma_1^{\mathbb{Z}} \cdots \gamma_r^{\mathbb{Z}}$.

Assuming the contrary, for all $m \in \mathbb{Z}$ there would exist $a_1 = a_1(m), \ldots, a_r = a_r(m) \in \mathbb{Z}$ such that

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

We may further assume that γ is in diagonal form. Also, writing

$$\gamma_i = \beta_i \delta_i \beta_i^{-1}, \quad i = 1, \ldots, r,$$

where δ_i are diagonal matrices, we derive in particular equations

$$\boxed{\lambda^m = Q(\nu_1^{b_1}, \ldots, \nu_t^{b_t}),} \quad (*_m)$$

for each $m \in \mathbb{Z}$, where

- Q is a fixed polynomial
- ν_i are fixed monomials in $\mu_1, \ldots, \mu_s$ (the eigenvalues of the γ_j)
- b_i are integers depending on m (actually certain linear forms in the a_i).

We view $(*_m)$ as a point P_m in the

variety X defined in $\mathbb{G}_m^{t+1}$ by

$$y = Q(x_1, \dots, x_t)$$

where p_m belongs to the (FG) subgroup Ω of $\mathbb{G}_m^{t+1}$ generated by the points

$(\lambda, 1, \dots, 1)$ and

$(1, \gamma_1, 1, \dots, 1)$, $\dots$, $(1, 1, \dots, \gamma_t)$.

Now, we have the following strong structure theorem, due to Laurent

Theorem: Let Ω be a (FG) subgroup of $\mathbb{G}_m^N(\bar{\mathbb{Q}})$, and let Σ be any subset of Ω. The Zariski closure of Σ is a finite union of translates of algebraic subgroups of $\mathbb{G}_m^N$.

Remarks • This result in practice describes the structure of S-integral points on subvarieties of $\mathbb{G}_m^N$.

It represents the "toric case" of what

was commonly called Mordell-Lang Conjecture.

- Laurent's results are even more general. It should be remarked however that this case relies on previous results by Evertse and (independently) van der Poorten - Schlickewei. In turn, all these theorems heavily use the deep Subspace Theorem of Wolfgang Schmidt, a far-reaching extension to higher dimensions of the Theorem of Roth in Diophantine Approximation.

- Recall that every algebraic subgroup of $\mathbb{G}_m^N$ can be defined by finitely many equations of the shape $x_1^{a_1} \cdots x_N^{a_N} = 1$ with integers $a_1, \dots, a_N$. This yields very explicit applications of the theorem.

CONCLUSION OF THE PROOF

With this result it is not difficult to conclude:

- Roughly: Suppose that we

have infinitely many points in $\Omega \cap X$; then infinitely many would fall in a same coset of algebraic subgroup entirely contained in X.

- The ratios between any two such elements would then belong to the subgroup, and it is easy to contradict then the multiplicative independence of λ and the μ_i.

Remark

A somewhat more delicate argument is needed in the case that one of the γ_i is not semisimple: indeed, in this case one of the variables in the equations appears polynomially (not as an exponent).

FINAL REMARKS

- It was asked to us what happens on replacing (BG) with the weaker condition that Γ may be factored as a product $\Gamma = A_1 \cdots A_r$ of

(rather than cyclic)

abelian (rather than cyclic)
subgroups A_i.

Keeping the other assumptions (i.e., Γ fin. gen. + anisotropic) the conclusion does not change: indeed, it may be proved that the A_i must be (FG), so in fact (BG) holds.

ABOUT THE ESTIMATES

For the estimates one replaces the QUALITATIVE theorem of Laurent with QUANTITATIVE results, due mainly to Evertse.

They concern equations

$$x_1 + x_2 + \dots + x_r = 0$$

where the x_i are "almost S-units".

This generality is crucial in our setting, where there is no S-unit assumption on one of the unknowns. In this case the Theorems imply that such unknown must have large height under appropriate circumstances.

APPLICATION OF ESTIMATES

The estimates may be applied through comparison with lower bounds, as mentioned earlier

However for our purposes a simple argument suffices:

On writing a matrix γ as a product $\gamma = \xi \eta$ with ξ semisimple and η unipotent commuting matrices, it is not difficult to see that

If sparseness holds for subsets in the group which are boundedly generated, then not all the powers of γ can lie in such a subset unless $\eta = 1$.

This reduces our issues to semisimple matrices.