Uniform Exponential Growth in Linear Groups

Bogdan Grechuk · 13 Nov 2026

https://functor.network/user/3333/entry/2070

This post continues my series on favourite theorems of the twenty-first century. My choice for 2006 in Algebra is a theorem of Emmanuel Breuillard and Tsachik Gelander on the growth of linear groups (Breuillard and Gelander 2008). Their paper first appeared as a preprint in 2006 and was published in *Inventiones Mathematicae* in 2008.

The theorem provides a remarkably strong answer to the following question: *how quickly must the number of distinct products of generators of a group grow?*

Let us begin with some definitions.

A *group* is a set equipped with an associative multiplication operation, an identity element, and inverses. For example, the invertible $d \times d$ matrices with real entries form a group under matrix multiplication, denoted by $\mathrm{GL}_d(\mathbb{R})$.

A group G is called *finitely generated* if there exists a finite subset $S \subseteq G$ such that every element of G can be written as a product of elements of S and their inverses.

For example, the group $(\mathbb{Z}, +)$ of integers is generated by the single element 1, since every integer is a sum of copies of 1 or -1.

Given a finite generating set S, let $\gamma_S(n)$ denote the number of elements of G that can be expressed as products of at most n elements of $S \cup S^{-1}$. Here

$$S^{-1} = \{s^{-1} : s \in S\}.$$

The function $\gamma_S(n)$ is called the *growth function* of the group relative to S.

For example, if $G = \mathbb{Z}$ and $S = \{1\}$, then

$$\gamma_S(n) = 2n + 1,$$

because the integers that can be reached using at most n additions or subtractions of 1 are exactly $-n, -n+1, \ldots, n$.

Thus, the growth is linear.

Other groups may grow much faster.

Consider a group freely generated by two elements a and b. This means that distinct *reduced words* in the symbols

$$a, \quad a^{-1}, \quad b, \quad b^{-1}$$

represent distinct group elements, where a word is reduced if it has no adjacent pair of mutually inverse symbols.

For example,

$$ab, \qquad ba, \qquad a^2b, \qquad ab^{-1}a$$

are all different elements.

In particular, there are 2^n distinct products of length n using only a and b, without their inverses. Therefore,

$$\gamma_S(n) \geq 2^n$$

for $S = \{a, b\}$.

A group with such rapidly growing numbers of elements is said to have *exponential growth*.

More precisely, a finitely generated group G has exponential growth if, for some (and hence every) finite generating set S,

$$e_S(G) = \lim_{n\to\infty} \gamma_S(n)^{1/n} > 1.$$

The existence of this limit follows from the elementary inequality

$$\gamma_S(m+n) \leq \gamma_S(m)\gamma_S(n).$$

Although the qualitative distinction between exponential and subexponential growth does not depend on the choice of generators, the number $e_S(G)$ generally does.

This raises a natural question: *can we choose different generating sets for the same group so that its exponential growth rate becomes arbitrarily close to* 1*?*

A group is said to have *uniform exponential growth* if

$$\inf_S e_S(G) > 1,$$

where the infimum is taken over all finite generating sets S of G.

Thus, uniform exponential growth means that there is a single exponential lower bound valid for every choice of generators.

In 1981, Gromov (Gromov 1981) asked whether every finitely generated group of exponential growth necessarily has uniform exponential growth.

This seemed plausible, since many of the familiar mechanisms producing exponential growth also give a uniform lower bound.

However, in 2004, Wilson (Wilson 2004) constructed a finitely generated group of exponential growth that does not have uniform exponential growth.

I discussed Wilson's theorem in an earlier blog post.

Thus, Gromov's question has a negative answer for general groups. But perhaps the answer is positive for more structured groups?

An important example is the class of *linear groups*: groups that can be represented as groups of invertible matrices over some field K, that is, as subgroups of

$$\mathrm{GL}_d(K)$$

for some positive integer d.

Linear groups have a much more rigid algebraic structure than arbitrary groups, and their growth has been extensively studied.

A fundamental result is *Tits' alternative*, proved by Jacques Tits (Tits 1972) in 1972. It states that every finitely generated linear group either contains a nonabelian free subgroup or has a solvable subgroup of finite index.

The first possibility means that the group contains two elements a, b satisfying no nontrivial relation. In particular, all reduced words in $a^{\pm 1}$ and $b^{\pm 1}$ are distinct.

The second possibility means that the group is *virtually solvable*, a structural condition saying that it contains a subgroup of finite index that can be reduced to abelian groups by a finite sequence of normal-subgroup quotients.

Thus, Tits' alternative shows that linear groups which are not virtually solvable always contain a nonabelian free subgroup.

Consequently, they have exponential growth.

However, Tits' theorem by itself does not imply *uniform* exponential growth. The free generators a, b might require extremely long products of the elements of a chosen generating set S.

In principle, changing S could make the free subgroup increasingly difficult to reach.

In 2005, Eskin, Mozes, and Oh (Eskin et al. 2005) established uniform exponential growth for finitely generated linear groups over fields of characteristic zero.

Breuillard and Gelander's work provides a stronger quantitative result, allowing arbitrary fields and, importantly, generating sets that are not required to contain inverses.

To formulate their theorem, let S^n denote the set of all elements of G expressible as products of at most n elements of S, *without requiring that inverses belong to* S.

Theorem 1 (Breuillard–Gelander) *Let G be a finitely generated linear group containing a nonabelian free subgroup.*
Then there exists a constant $\lambda = \lambda(G) > 1$ such that for every finite generating set S of G and every positive integer n,

$$|S^n| \geq |S|\lambda^{n-1}.$$

The most important feature is that λ depends only on the group G, and *not* on the choice of generators S.

Thus, no matter how we generate G, the number of distinct products grows exponentially at a rate bounded away from 1.

The theorem is stronger than ordinary uniform exponential growth in two ways.

First, the set S need not be symmetric: we do not assume that $s^{-1} \in S$ whenever $s \in S$.

Second, the lower bound includes the factor $|S|$. Thus, choosing a larger generating set cannot make the guaranteed lower bound weaker.

Since

$$\gamma_S(n) \geq |S^n|,$$

the theorem immediately implies that G has uniform exponential growth.

Let us explain the main idea behind the proof.

The authors establish a remarkable strengthening of Tits' alternative.

They show that there exists an integer $m = m(G)$ such that, for *every* finite generating set S, one can find two elements $a, b \in G$, each expressible as a product of at most m elements of $S \cup S^{-1}$, which freely generate a nonabelian free subgroup.

This is called *uniform independence*.

The distinction from Tits' original theorem is crucial. Tits proved that such a pair a, b exists somewhere in the group. Breuillard and Gelander show that it can always be found within a bounded distance of the identity, where the bound does not depend on the generating set.

Once such a pair is available, exponential growth follows immediately.

Indeed, the 2^k positive words of length k in a and b are all distinct. Each is a product of at most mk elements of $S \cup S^{-1}$. Therefore,

$$\gamma_S(mk) \geq 2^k,$$

which gives the uniform exponential lower bound

$$e_S(G) \geq 2^{1/m} > 1.$$

This simple argument explains the connection between uniform independence and uniform exponential growth.

The sharper inequality in the theorem, including the factor $|S|$ and allowing nonsymmetric generating sets, follows from additional expansion estimates established in the paper.

But how do the authors find these two free generators at uniformly bounded distance?

Their proof uses the classical *ping-pong method*.

The idea is to make group elements act on a geometric space so that different transformations move points into disjoint regions.

For example, matrices act naturally on *projective space*, whose points correspond to one-dimensional subspaces of a vector space.

If two transformations have sufficiently strong attracting behaviour in appropriately separated regions, then different reduced words in these transformations have different effects on points. This allows one to prove that the transformations generate a free group.

The difficulty is not merely to find such transformations, but to find them as *short products of an arbitrary generating set*.

Breuillard and Gelander combine the ping-pong method with estimates on eigenvalues, matrix norms, and the geometry of linear groups over different fields. These estimates ensure that the required attracting transformations can always be constructed using a bounded number of generators.

Thus, a question about the number of group elements that can be reached in a given number of steps is reduced to a problem about the geometric action of matrices.

The theorem is a beautiful example of how algebraic structure can enforce a strong quantitative conclusion.

Wilson’s example shows that exponential growth need not be uniform for general finitely generated groups. Breuillard and Gelander show that, for linear groups containing a nonabelian free subgroup, such behaviour is impossible.

No matter how we change the generators, free behaviour appears within a bounded number of steps, and the group is forced to grow exponentially at a uniform rate.

References

Breuillard, Emmanuel, and Tsachik Gelander. 2008. “Uniform Independence in Linear Groups.” *Inventiones Mathematicae* 173 (2): 225–63. https://doi.org/10.1007/s00222-007-0101-y.

Eskin, Alex, Shahar Mozes, and Hee Oh. 2005. “On Uniform Exponential Growth for Linear Groups.” *Inventiones Mathematicae* 160 (1): 1–30. https://doi.org/10.1007/s00222-004-0373-0.

Gromov, Mikhael. 1981. *Structures métriques Pour Les Variétés Riemanniennes*. Vol. 1. Textes Mathématiques. Cedic.

Tits, Jacques. 1972. “Free Subgroups in Linear Groups.” *Journal of Algebra* 20: 250–70.

Wilson, John S. 2004. “On Exponential Growth and Uniformly Exponential Growth for Groups.” *Inventiones Mathematicae* 155 (2): 287–303. https://doi.org/10.1007/s00222-003-0327-0.