Growth of groups and algebras

Jason Bell

University of Waterloo,
joint with E. Zelmanov (arXiv:1907.01777)

jpbell@uwaterloo.ca

Abend Seminar, September 24, 2020

What do we mean by growth?

Let G be a finitely generated group and let S be a finite symmetric generating set. (Here symmetric just means that if $s \in S$ then $s^{-1} \in S$, so we write $S = S^{-1}$.)

Then we can create a function

$$d_S(n),$$

which is the number of distinct elements of G that can be expressed as a product of at most n elements of S.

Notice that $d_S(n)$ is a weakly increasing function.

Two examples

Let $G = \langle x \rangle$, the infinite cyclic group with generator x, and let $S = \{x, x^{-1}\}$. Then the words that can be written as a product of at most n elements of S are the words

$$x^{-n}, x^{-n+1}, \dots, x^{-1}, 1, x, \dots, x^n,$$

and so

$$d_S(n) = 2n + 1.$$

Let $H = \langle x, y, z \mid xyx^{-1}y^{-1} = z, zx = xz, yz = zy \rangle$, the Heisenberg group, and let $U = \{x, x^{-1}, y, y^{-1}, z, z^{-1}\}$. Then every element of H is of the form $x^i y^j z^k$.

It is a bit more work to give a closed form for the growth, but it actually grows like a polynomial in n of degree 4.

Notice that if we again take $G = \langle x \rangle$, the infinite cyclic group with generator x, and let $T = \{x^2, x, x^{-1}, x^{-2}\}$, then $d_T(n) = 4n + 1$. So $2n + 1 = d_S(n) \neq d_T(n)$.

But $d_S(n)$ and $d_T(n)$ are both linear functions of n.

asymptotic equivalence

The function $d_S(n)$ is called the *growth function* of G. We saw that it depends upon one's choice of generating set S, but if one works with a notion of asymptotic equivalence then one can speak unambiguously of the growth function.

We say that two weakly increasing functions $f(n)$ and $g(n)$ are *asymptotically equivalent* if

$$f(n) \leq g(Cn)$$

and

$$g(n) \leq f(Cn)$$

for some positive integer C.
In general, if T is another generating set for G then the functions $d_S(n)$ and $d_T(n)$ are asymptotically equivalent.

As we saw in the two examples, if $f(n)$ grows linearly and $g(n)$ is asymptotically equivalent to $f(n)$ then $g(n)$ is also bounded above and below by linear functions. Thus we can speak of groups of *linear growth*; i.e., groups with a generating set S such that $C_1 n \leq d_S(n) \leq C_2 n$ for all n sufficiently large.

Similarly, we can speak of polynomially bounded growth; i.e., $d_S(n) \leq n^D$ for all n sufficiently large, for some D.

and of exponential growth; i.e., $d_S(n) \geq C^n$ for some $C > 1$ for all n sufficiently large.

Why do we care about growth?

The original motivation for growth of groups came from work of Milnor and Wolf.

Theorem. (Milnor, 1968) Let X be a closed negatively curved Riemannian manifold. Then the fundamental group of X has exponential growth.

Since this work, growth has proven to be an important invariant and has relations to amenability and other important group theoretic properties.

Gromov's theorem

One of the most beautiful results on growth of groups is a theorem of Gromov.

Theorem. (Gromov) Let G be a finitely generated group. Then G has polynomially bounded growth if and only if G has a normal nilpotent subgroup N of finite index (virtually nilpotent or nilpotent-by-finite).

Intuitively, a nilpotent group is the next best thing after being abelian and the class of nilpotent groups is sandwiched between the class of abelian groups and the class of solvable groups.

How do you prove Gromov's theorem?

It's hard. One starts with a symmetric generating set S and then looks at the vector space V of maps $f : G \to \mathbb{R}$ that are Lipschitz harmonic.

Lipschitz means that there is some C such that $|f(sx) - f(x)| \leq C$ for all $s \in S$ and $x \in G$.

Harmonic means that

$$\frac{1}{|S|} \sum f(sx) = f(x)$$

for all $x \in G$.

Then G acts on the vector space V and this gives a representation $G \to \mathrm{GL}(V)$.

Remarkably if G is infinite and has polynomially bounded growth then V is finite-dimensional and has dimension at least 2!

Now you let N be the kernel of this homomorphism $\pi : G \to \mathrm{GL}(V)$. Then you can show N has strictly smaller growth and so by an induction you get that N is virtually nilpotent. For linear groups, Gromov's theorem was already known so we get that the image of π is virtually nilpotent.

So you have a short exact sequence

$$1 \to N \to G \to \pi(G) \to 1.$$

This gives that G is virtually solvable and now a result of Wolff gives that G is virtually nilpotent.

Growth and Burnside's question

One of the interesting consequences of Gromov's theorem is about torsion groups of polynomially bounded growth.

Burnside's question

One of the interesting consequences of Gromov's work has to do with torsion groups. Recall that a group G is torsion if every element of G has finite order.

Burnside's question (1902): Let G be a finitely generated torsion group. Is G finite?

Burnside/Schur proved this when G is a finitely generated torsion subgroup of $\mathrm{GL}_n(K)$. Burnside also showed this is true if every element of G has order 2 or if every element of G has order 3.

It wasn't until 1964 that Golod and Shafarevich produced a finitely generated infinite torsion group. This group has exponential growth. Later, Grigorchuk produced a finitely generated infinite torsion group of subexponential growth (but still superpolynomial).

Can we have a finitely generated infinite torsion group of polynomially bounded growth?

No! This follows immediately from Gromov's theorem. If we did, it would have an infinite nilpotent subgroup N of finite index. This group N would be finitely generated and torsion and you can show that a finitely generated nilpotent torsion group is finite.

Can we do the same thing with rings?

Let k be a field and let A be a finitely generated (unital) associative k-algebra. Then we say that a k-vector subspace $V \subseteq A$ is a *frame* if

$$1 \in V, \dim(V) < \infty,$$

and V generates A as a k-algebra.

Example. Let $A = k[x, y]$ and let $V = k + kx + ky = \mathrm{Span}\{1, x, y\}$. Then V is a frame for A. Frames for algebras play the role of symmetric generating sets for groups.

If V is a frame, then we have a chain of subspaces

$$V \subseteq V^2 \subseteq V^2 \cdots \subseteq \bigcup V^i = A,$$

where V^n is the span of all products of n elements of V.

Then we let $d_V(n) = \dim(V^n)$. We call this function the growth function of A.

If $A = k[x_1, \dots, x_d]$ and $V = k + kx_1 + \cdots + kx_d$, then

$$\dim(V^n) = \binom{n+d}{d} \cong n^d/d!.$$

Why?

Notice that V^n has a basis consisting of monomials $x_1^{i_1} \cdots x_d^{i_d}$ with $i_1 + \cdots + i_d \leq n$.

This is in bijection with the number of ways of placing d X's into $n + d$ slots.

$$\underbrace{\underbrace{- - -}_{i_1} X \underbrace{- - -}_{i_2} X - \cdots - X \underbrace{- - -}_{i_d} X - - -}_{n+d}$$

So we get $\binom{n+d}{d}$. As a function of n, this is just a polynomial of degree d in n and so the growth function of $k[x_1, \ldots, x_d]$ is asymptotically equivalent to n^d.

For those who are familiar with Krull dimension, you'll note that d is exactly the Krull dimension, so the degree of the polynomial $d_V(n)$ is the Krull dimension of this algebra.

Is this a coincidence?

In general if A is a finitely generated k-algebra and V is a frame for A then $d_V(n)$ grows like a polynomial in n of degree d, where d is the Krull dimension of A. The proof is not much harder than the polynomial ring case....

Connections to classical algebraic geometry

Krull dimension is of fundamental importance in algebraic geometry. We know there is an equivalence of categories

$$\text{finitely generated reduced } \mathbb{C}-\text{algebras} \leftrightarrow \text{complex affine varieties.}$$

Then under this correspondence, the Krull dimension of an algebra A is equal to the dimension of the corresponding variety X as a complex manifold (let's assume that the variety is smooth!).

Example

Let $A = \mathbb{C}[x, y]/(x^2 - y^3 - 1)$. Then A has Krull dimension one and corresponds to the (smooth) curve

$$\{(a, b) \in \mathbb{C}^2 \colon a^2 - b^3 - 1\},$$

which is a 1-dimensional complex manifold.

So the growth of the algebra is giving us a picture of its dimension, too.

What about noncommutative algebras?

Our definition of growth does not require that the algebra be commutative. We've seen that commutative algebras of linear growth correspond to curves and algebras of quadratic growth correspond to surfaces. By analogy, we can talk about noncommutative curves and noncommutative surfaces as being those algebras with linear and quadratic growth.

What can be said here?

Algebras of linear growth

There's an amazing result of Small-Stafford-Warfield-van den Bergh, which says the following. Let k be an algebraically closed field and let A be a finitely generated k-algebra that is a domain and suppose that A has linear growth. Then A is commutative!

Intuitively, this should make sense. Commutative algebras of linear growth correspond to curves, so a noncommutative algebra of linear growth should correspond to a "noncommutative curve". But we think of a curve as being parametrized by one variable and a variable always commutes with itself, so noncommutative curves should be commutative.

What about algebras of quadratic growth?

Here there is an incomplete picture, but there are a few examples which give a sense of what is going on.

The quantum plane. Let q be a nonzero, non root of unity in $\mathbb{C}$ and let $A = \mathbb{C}\langle x, y\rangle/(xy = qyx)$. Then A looks like a polynomial ring in two variables but we've deformed the multiplication rule using this q. This algebra is called the quantum plane.

The Weyl algebra This is the algebra $W = \mathbb{C}\langle x, y\rangle/(xy - yx = 1)$. This is capturing the fundamental relationship between the position and momentum operators.

The birational classification question

Michael Artin has given a proposed birational classification of domains of quadratic growth. Here "birational" is in analogy with the commutative case. His classification says that birationally every domain should either look close to being a polynomial ring in two variables or it should be close to being one of the two examples above. At the moment, the conjecture is wide open.

Noncommutative localization

We all know that a commutative domain has a field of fractions. As it turns out, there is a more general fact due to Alfred Goldie:

If S is a domain of polynomially bounded growth then S has a "noncommutative field of fractions," $\mathrm{Frac}(S)$, which we obtain by inverting the non-zero divisors in R. This ring is obviously not a field but it is the next best thing: it's a division ring, or a field but with the axiom of commutative multiplication removed.

When R is a domain of quadratic growth we can still form the "noncommutative field of fractions" and we get a division ring $\mathrm{Frac}(R)$.

A birational classification means understanding the division rings that can occur up to isomorphism.

In theory this is easier, because it is a coarser notion of equivalence compared to ordinary isomorphism.

For (commutative) surfaces, there is a birational classification due to Enriques and Castelnuovo, which birationally classifies surfaces in terms of geometric data: the Kodaira dimension, irregularity, various plurigenera, etc.

Unfortunately, noncommutative localization is much more pathological.

As an example, Makar-Limanov showed in 1983 that if W is the Weyl algebra $\mathbb{C}\langle x, y\rangle/(xy - yx = 1)$. then $\mathrm{Frac}(W)$ contains a copy of a free algebra on two generators.

In other words, W has quadratic growth but when we localize we get a huge algebra of exponential growth.

Theorem (B-Rogalski) Let A be a finitely generated domain of quadratic growth. Then $\mathrm{Frac}(A)$ is either finite-dimensional over its centre or it contains a copy of the free algebra on two generators.

In other words, noncommutative localization is either as nice as possible or it is as bad as possible: there's no in between!

The fact that these division rings are so big (i.e., they contain copies of a free algebra on two generators makes them very hard to study) and makes Artin's conjecture very hard. So far the biggest result towards it is work of Artin and Stafford who show that graded domains of quadratic growth can be completely described in terms of geometric data.

What about higher growth?

Not so fast! When we talk about Krull dimension, it takes values $0, 1, 2, \ldots$, so it makes sense to go from linear to quadratic, but with growth functions, there's no reason, a priori, that we can't have

$$\dim(V^n) \sim n^\alpha$$

with $\alpha \in (1, 2)$.

Thankfully, a result of Bergman says these cannot occur.

Bergman's gap theorem

Let A be a finitely generated k-algebra and let V be a frame for A. Then either there is a constant $C > 0$ such that

$$\dim(V^n) \leq Cn$$

OR

$$\dim(V^n) \geq \binom{n+2}{2}.$$

Warfield shows that these gaps do not exist once one goes above quadratic growth.

Theorem. (Warfield) Let $\alpha \in [2, \infty]$. Then there is an algebra A with frame V such that

$$\log(\dim(V^n))/\log(n) \to \alpha.$$

What types of growth functions are possible?

Warfield's constructions showed that there is a continuum of possible growth functions for algebras, but it leaves open the question: can one classify the weakly increasing functions $F : \mathbb{N} \to \mathbb{N}$ that are asymptotically equivalent to the growth function of a group or an algebra?

For groups

For groups not much is known. Gromov's theorem along with work of Bass and Guivarch shows that if $F(n)$ is polynomially bounded and F is asymptotically equivalent to the growth function of an algebra then $F(n)$ is asymptotically equivalent to n^d for some nonnegative integer d.

Grigorchuk constructed an example of a group whose growth function grows superpolynomially but subexponentially. Its exact growth is unknown.

It is conjectured that the growth function of a group that is superpolynomial should grow at least as fast as $\exp(\sqrt{n})$,

Why this gap?

Why should there be nothing in between polynomial growth and $\exp(\sqrt{n})$? Grigorchuk has proven that this gap holds for a large class of groups. The idea behind Grigorchuk's proof is that for many groups one can create an associated Lie algebra and from the Lie algebra one can take the enveloping algebra and the growth of the group is related to the growth of the enveloping algebra.

Remarkably: for enveloping algebras it is known that there is a gap: if an enveloping algebra has superpolynomial growth then it grows at least as fast as the partition function $p(n)$, which up to asymptotic equivalence grows like $\exp(\sqrt{n})$.

Constraints!

Let $F : \mathbb{N} \to \mathbb{N}$ be a weakly increasing function and let $F'(n) = F(n) - F(n-1)$. If F is a growth function, we have the following:

- (Bergman) Either $F(n) \cong 1$, or $F(n) \cong n$, or $F(n) \succ n^2$. Moreover, if $F(n) \succ n^2$ then $F'(n) \geq n+1$.
- (Submultiplicativity) $F'(n+m) \leq F'(n)F'(m)$.

Are there any others?

In joint work with Zelmanov, we found one extra constraint that is required:
If $F(n) \geq n^2$ then

$$F'(m) \leq F'(n)^2$$

for

$$m \in \{n, n+1, n+2, \ldots, 2n\}.$$

Do we have all of the constraints?

Yes!

Theorem. (B-Zelmanov, 2019) Let $F : \mathbb{N} \to \mathbb{N}$ be a weakly increasing function and let $F'(n) = F(n) - F(n-1)$. If:

- $F'(n)$ is submultiplicative,
- $F'(m) \leq F'(n)^2$ for $m \in \{n, n+1, n+2, \ldots, 2n\}$,
- $F'(n) \geq n+1$ for all n,

then $F(n)$ is asymptotically equivalent to the growth function of an algebra.

In particular, this characterizes all possible growth functions for finitely generated algebras of superlinear growth. The conditions that $F'(n)$ is submultiplicative and that $F'(m) \leq F'(n)^2$ for $m \in \{n, n+1, n+2, \ldots, 2n\}$ always hold for any growth function that grows at least quadratically with n.

Bergman's theorem says that if $F'(n) < n+1$ for some n then $F(n)$ is either asymptotically equivalent to the function n or to the constant function 1. Both of these growth types can occur, so we have all of them.

In fact, we are able to show that the same conditions characterize the possible growth of finitely generated semigroups. So somehow the growth behaviour for semigroups is radically different from that of groups. The reason for this appears to be the failure of the cancellative property that holds for groups.

Thanks!