

COUNTING IN GROUPS: FINE ASYMPTOTIC GEOMETRY

MOON DUCHIN

1. GROWTH: HOW FAST? HOW REGULAR?

Suppose we want to study a sequence of integers $(a_n)_{n \in \mathbb{N}}$ and characterize *how* it grows. A motivating example is the Fibonacci sequence $1, 1, 2, 3, 5, \dots$, which satisfies the famous recursion $a_n = a_{n-1} + a_{n-2}$. We can apply an 18th-century idea (attributed to de Moivre, and put to excellent effect by Euler) and form the associated *generating function* $\mathbb{A}(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}[[x]]$, with the values of the sequence as coefficients in a formal power series. From the recursion, we find that $\mathbb{A}(x) - x\mathbb{A}(x) - x^2\mathbb{A}(x) = 1$, obtaining the nice form $\mathbb{A}(x) = \frac{1}{1-x-x^2} \in \mathbb{Q}(x)$ as a *rational function* (a ratio of polynomials). Some of this generalizes readily. Let's say that a *Fibonacci-style recursion* is one with integer coefficients and finite depth: $a_n = \alpha_1 a_{n-1} + \dots + \alpha_k a_{n-k}$. We once again get $\mathbb{A}(x)$ as a rational function, with denominator $1 - \alpha_1 x - \dots - \alpha_k x^k$. We'll say that sequences whose generating functions are rational functions have *rational growth*. Let's consider what this tells us about the sequence...

Polynomials have rational growth. We can next observe that $\frac{1}{1-x} = \sum_n 1 \cdot x^n$, and that $\frac{x^k}{(1-x)^{k+1}} = \sum_n \binom{n}{k} x^n$, so the sequence $a_n = \binom{n}{k}$ has rational growth for each k . Furthermore, since $\binom{n}{k}$ is a degree- k polynomial in n , and these form a basis for $\mathbb{Q}[n]$, we have all sequences $a_n = f(n)$ for $f \in \mathbb{Q}[n]$ in the rational growth class.

Actually a very small generalization is in order: a function $g(n)$ is (*eventually*) *quasi-polynomial* with period N if there is a threshold $T > 0$ and a list of polynomials g_1, \dots, g_N such that $g(n) = g_k(n)$ for $k \equiv n \pmod N$ and $n \geq T$. We may think of this behavior as cycling through finitely many polynomials, or as being polynomial with oscillating coefficients if we prefer. It's easy to see that eventually quasi-polynomial functions have rational growth—just sum the $x^k \cdot \mathbb{A}_k(x^N)$, and add a polynomial to adjust the low values of n . There is a nice converse as well: if an integer sequence in the polynomial range (that is, $a_n \leq An^d$ for some A, d) satisfies a Fibonacci-style recursion, then it records the values of an eventually quasi-polynomial function. (To see this, convince yourself that the poles of $\mathbb{A}(x)$ must be roots of unity, so that each makes a periodic contribution to the expression.)

And so do exponentials. On the other hand, $\frac{1}{1-2x} = \sum_n 2^n x^n$ has $a_n = 2^n$, and indeed whenever a rational function $\mathbb{A}(x)$ has a pole inside the unit circle in \mathbb{C} , its associated sequence grows exponentially.

But lots of things don't! Any function growing at a rate faster than polynomials but slower than exponentials (like say $e^{\sqrt{n}}$) has no chance at rational growth; a rational function either has a pole inside the unit circle (forcing exponential growth) or not (forcing growth in the polynomial range—this is fun to check if you're so inclined).

Likewise, you can easily form a sequence that's very close—even bounded distance—to one with rational growth, but which fails badly in its own right. For instance, consider the digits-of-pi power series

$$\mathbb{P}(x) = 3 + 1x + 4x^2 + 1x^3 + 5x^4 + \dots$$

The transcendental nature of π itself tells us that this sequence will satisfy no recursion, and in fact we can go a bit further. If $\mathbb{A}(x) = \frac{p(x)}{q(x)}$ is rational, we have $q\mathbb{A} - p = 0$, which suggests that we can generalize rational growth to *algebraic growth* if \mathbb{A} satisfies any polynomial with polynomial coefficients; otherwise we'll say the growth is *transcendental*. This $\mathbb{P}(x)$ is transcendental in that sense, even though its coefficients are within globally bounded distance from those of the rational function $\frac{1}{1-x}$ (and indeed of the rational function 0).

2. COUNTING IN DILATES

Next, we can parlay these ideas to a study of some classical counting problems: for a region $\Omega \subset \mathbb{R}^d$, we'll define $G_\Omega : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ by $G_\Omega(n) := \#(\mathbb{Z}^d \cap n\Omega)$, the number of lattice points in the n -times dilate of Ω .

Moon Duchin is associate professor of mathematics at Tufts University. Her email address is Moon.Duchin@tufts.edu.

Round counting. In the case $\Omega = \mathbb{D}$, the unit disk in \mathbb{R}^2 , this is the famous *Gauss circle problem*. Gauss himself made the simple observation that $G_{\mathbb{D}}(n) = \pi n^2 + O(n)$, with the first-order term being given by the area of the disk (because there is roughly one lattice point per unit square), while the second-order term reflects the fact that the boundary touches $O(n)$ squares. From a modern point of view, we would say that the first-order term of $G_{\Omega}(n)$ must be Vn^d whenever Ω is Riemann-integrable with volume V , because its boundary has a lower-order contribution. About a hundred years later, Sierpinski improved on this somewhat with the estimate $G_{\mathbb{D}}(n) = \pi n^2 + O(n^{\frac{2}{3}})$, and today it is believed that the optimal power law looks like

$$G_{\mathbb{D}}(n) = \pi n^2 + O(n^{\frac{1}{2}+\epsilon})$$

for any $\epsilon > 0$. (This is best possible, by a theorem of Hardy and Landau.) This “feels” like it should have transcendental growth, and indeed it does: a theorem of Stoll [3] tells us that if $a_n \sim \alpha n^d$, then α irrational or transcendental implies the same for \mathbb{A} .

Pointy counting. By contrast, suppose we start with $\Omega = P$, a lattice polytope (integer vertices). In the plane ($d = 2$), we have the remarkable Pick’s theorem which relates the area (A), interior lattice points (i), and boundary lattice points (b) by $A = i + \frac{b}{2} - 1$, which we can rearrange to $i + b = A + \frac{b}{2} + 1$, then scale to obtain $G_P(n) = An^2 + \frac{b}{2}n + 1$ for $n \in \mathbb{N}$. This is a beautiful fact: the lattice point count in a dilated polygon grows exactly like values of a polynomial; *polygonal counting has rational growth*. Now it is well known that Pick’s theorem doesn’t generalize to higher dimensions (i.e., there is no formula for the volume of a lattice polyhedron based only on a count of the lattice points in its k -cells), but nonetheless in the 1970s, former high school teacher Eugène Ehrhart found that the polynomiality persists: $G_P(n) = a_d n^d + a_{d-1} n^{d-1} + \dots + a_0$, where the leading coefficient a_d is of course the volume; the next coefficient a_{d-1} is an appropriately normalized surface area; and the constant term a_0 is the Euler characteristic of the polytope. These *Ehrhart polynomials* are part of a thoroughly beautiful story, which you can read about in Beck–Robins [1], and some of the numerology of the other coefficients remains a mystery.

It’s worth noting that if we began with Q with rational coordinates for its vertices rather than integers, then we’d find G_Q to be quasi-polynomial! So counting functions for rational polyhedra have rational growth.

3. COUNTING IN GROUPS

Onward to group theory, where we will study some counting problems in finitely-generated groups given by *presentations* $G = \langle S | R \rangle$, with S a generating set and R a list of relations. Recalling that $[a, b] = aba^{-1}b^{-1}$ denotes the *commutator* of two group elements, we can present three basic 2-generated groups by





$$\langle a, b \mid [a, b] = 1 \rangle \qquad \langle a, b \mid \emptyset \rangle \qquad \langle a, b \mid [a, b] \text{ central} \rangle.$$

The first is the free abelian group \mathbb{Z}^2 , the second is the free group F_2 of rank two, and the third is the (discrete) *Heisenberg group* $H(\mathbb{Z}) = \begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{bmatrix}$ as generated by the elementary matrices $a = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. In terms of algebraic structure, $H(\mathbb{Z})$ belongs to a class of groups called *nilpotent* (of step s): in nilpotent groups, some commutators of generators might be nontrivial, but commutators with commutators, or commutators with commutators with commutators, and so on, eventually all die after a fixed number of steps, s . (The Heisenberg group is 2-step because $[a, b]$ commutes with everything, so all commutators with commutators are trivial.) One might wonder whether counting problems can detect algebraic structure like this, or other algorithmic and geometric structure in groups.

Hard questions about groups. Presentations seem deceptively simple but they are famously hard to work with. Given a presentation, the *word problem* seeks an algorithm to decide whether a string of generators represents the identity. One way to understand the structure of a group is to build a *Cayley graph* whose vertices are group elements, connected by an edge if they differ by a generating letter. Recognizing the identity word from a string of generators is the same as finding loops in the Cayley graph. These problems are in general undecidable, as we know since work of Boone and Novikov in the 1950s.

Cayley graphs are a key tool in geometric group theory; the large-scale geometry of the graphs carries fundamental information about the algebraic properties of the groups. For instance, if the graph has negative curvature in the large (i.e., is δ -hyperbolic), then we gain a great deal of information about the group, such as a fast solution to the word problem.

Growth. Consider the fundamental counting question *How many group elements can be spelled with $\leq n$ letters?* In terms of the Cayley graph from the generating set S , this asks for the count of group elements in the ball of radius n . Let's name this $\beta_n := \#B_n$, and we'll name the corresponding sphere count $\sigma_n := \beta_n - \beta_{n-1}$, noting that $\mathbb{B}(x) = \sum \beta_n x^n$ and $\mathbb{S}(x) = \sum \sigma_n x^n$ are related by $\mathbb{B}(x) = \frac{\mathbb{S}(x)}{1-x}$. In simple examples, we get simple recursions, and therefore rational growth, and in free abelian groups we can also find a suggestively parallel geometric counting problem. In the examples below, we'll write **std** for standard generators of a group, and we'll consider the dependence on generators in \mathbb{Z}^2 by additionally considering **hex** = $\pm\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}\}$ (the points of an integer hexagon in the plane) and **chess** = $\{\begin{bmatrix} \pm 2 \\ \pm 1 \end{bmatrix}, \begin{bmatrix} \pm 1 \\ \pm 2 \end{bmatrix}\}$ (the moves a chess knight makes).

(G, S)	$\beta_n \ (n \gg 1)$	$\sigma_n \ (n \gg 1)$	recursion $\sigma_n =$	$\mathbb{S}(x)$	Ω	$G_\Omega(n)$
(\mathbb{Z}, std)	$2n + 1$	2	σ_{n-1}	$\frac{1+x}{1-x}$	—	$2n + 1$
$(\mathbb{Z}^2, \text{std})$	$2n^2 + 2n + 1$	$4n$	$2\sigma_{n-1} - \sigma_{n-2}$	$\frac{(1+x)^2}{(1-x)^2}$		$2n^2 + 2n + 1$
$(\mathbb{Z}^2, \text{hex})$	$3n^2 + 3n + 1$	$6n$	$2\sigma_{n-1} - \sigma_{n-2}$	$\frac{1+4x+x^2}{(1-x)^2}$		$3n^2 + 3n + 1$
$(\mathbb{Z}^2, \text{chess})$	$14n^2 - 6n + 5$	$28n - 20$	$2\sigma_{n-1} - \sigma_{n-2}$	$\frac{(1+x)(1+5x+12x^2-8x^4+4x^5)}{(1-x)^2}$		$14n^2 + 6n + 1$
$(\mathbb{Z}^3, \text{std})$	$\frac{(2n+1)(2n^2+2n+3)}{3}$	$4n^2 + 2$	$3\sigma_{n-1} - 3\sigma_{n-2} + \sigma_{n-3}$	$\frac{(1+x)^3}{(1-x)^3}$		$\frac{(2n+1)(2n^2+2n+3)}{3}$
(F_2, std)	$2 \cdot 3^n - 1$	$4 \cdot 3^{n-1}$	$3\sigma_{n-1}$	$\frac{1+x}{1-3x}$		

Coarse counting. At first glance, the precise coefficients β_n or σ_n might seem like a poor tool to use in the study of groups, because they depend a great deal on the choice of generators! However, using the fundamental fact that changing generating sets can only modify the Cayley graph metric in an essentially linear way, we can observe that having growth in the polynomial range (indeed even polynomial of a certain degree) or the exponential range is coarse enough to be a well-defined group property. The possible growth *rates* of groups has been a major open question at least since Milnor wondered about it in the 1960s, and there was a breakthrough in the 1980s when Grigorchuk found groups of intermediate growth (on the order of $e^{\sqrt{n}}$). Work of Bass and Guivarc'h had demonstrated that nilpotent groups would all have growth in the polynomial range, and they had computed the degree. (So for instance the Heisenberg group $H(\mathbb{Z})$ has growth $\beta_n \asymp n^4$, $\sigma_n \asymp n^3$ with any generators.) And one of the fundamental theorems of geometric group theory remains Gromov's beautiful result from 1981 [2]. To state it, we'll use the terminology that a group is *virtually nilpotent* if it is nilpotent up to finite index, and similarly for abelian and other group properties.

Theorem 1 (Gromov). *The groups with growth in the polynomial range are precisely the virtually nilpotent groups.*

One way of narrating some of the math that goes into Gromov's theorem goes like this: on one hand, nilpotent groups admit "counting in dilates" in an appropriate ambient space, which implies polynomial growth; on the other hand, the presence of an appropriate kind of dilation characterizes nilpotency.

Fine counting. Rational growth in groups would pay off handsomely; we'd have a recursion giving us the growth values, and if we know how many group elements there are of each length, we can devise algorithms to solve the word problem and build the Cayley graph from only finitely much initial data.

However, rationality is extremely delicate—remember that it can be destroyed by adding a bounded function—so it may in principle depend on the choice of generating set. And a stunning theorem of Stoll from 1996 [3] shows that it may in fact: the higher Heisenberg group $\begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & 0 & \mathbb{Z} \\ 0 & 0 & 1 & \mathbb{Z} \\ 0 & 0 & 0 & 1 \end{bmatrix}$, which is nilpotent of step two, has rational growth with one generating set, but transcendental with another! So while growth rate is a coarse asymptotic invariant, you might say that rationality of growth has the paradoxical status of being a fine asymptotic property.

At this point, rationality across generating sets might seem to be asking too much. But amazingly, there are geometric regimes that are so well-behaved you don't need to be a slave to the generators.

Theorem 2 (Cannon, Thurston, Gromov, Benson 1980–1984). *No matter the generators, if the group is flat (virtually abelian) or hyperbolic, then the growth is rational.*

Per Stoll, nilpotent geometry is not such a regime. Nonetheless, for $H(\mathbb{Z})$ itself, a curious blend of sub-Finsler geometry, convex geometry, and combinatorial group theory turns out to be enough.

Theorem 3 (Duchin–Shapiro 2014). *Same for the Heisenberg group!*

That's the good news. On the other hand, even in standard generators, we get $\sigma_n = \frac{31n^3 - 57n^2 + 105n + c_n}{18}$, where $c_n = -7, -14, 9, -16, -23, 18, -7, 32, 9, 2, -23, 0$, repeating with period 12, for $n \geq 1$. In the next simplest choice of generators, the quasi-polynomial period is already sixty! I will leave you with that hopefully vivid illustration that you don't want to wrangle with Heisenberg's growth by hand.

REFERENCES

- [1] Matthias Beck and Sinai Robins. *Computing the continuous discretely. Integer-point enumeration in polyhedra*. Undergraduate Texts in Mathematics. Springer, New York, 2015.
- [2] Mikhael Gromov, *Groups of polynomial growth and expanding maps*. Inst. Hautes Études Sci. Publ. Math. No. 53 (1981), 53–73.
- [3] Michael Stoll, *Rational and transcendental growth series for the higher Heisenberg groups*. Invent. Math. 126 (1996), no. 1, 85–109.