UNIVERSAL MINIMAL CONSTANTS FOR POLYNOMIAL GROWTH OF GROUPS

Russell Lyons and Avinoam Mann

Indiana University, Bloomington
Einstein Institute of Mathematics, Hebrew University, Jerusalem, Israel

Abstract. We study the minimal polynomial growth rate of finitely generated groups in the following sense. We prove that there exist positive numbers ϵ_d such that if G is a group either of polynomial growth of degree d, or of non-polynomial growth, then that growth is at least $\epsilon_d n^d$. If G is nilpotent, it suffices to assume that the degree is at least d. We indicate an application for random walks on groups.

The growth rate of finitely generated groups is one of the most basic topics in geometric group theory. There are three fundamental classifications of groups in this sense: those of polynomial growth, those of exponential growth, and the rest, called intermediate growth. These classes are all invariant under change of generators. It is known that there are groups of exponential growth whose rate of growth on the exponential scale is arbitrarily small for certain sets of generators, whereas some classes of groups are known to have uniformly exponential growth rate over all generating sets: for such a group, there is a constant $c > 1$ such that for every generating set, its ball of radius n has at least c^n elements; moreover, the same $c > 1$ sometimes exists for an entire class of groups. See, e.g., [BT] for results and history of exponential growth. There is much less knowledge for groups of intermediate growth: it is not even known whether there are such groups whose balls of radius n have asymptotically fewer than $e^{c\sqrt{n}}$ elements. We study polynomial growth. This class breaks up into further classes, because if balls grow like a polynomial in the radius, then the degree of the polynomial is invariant under change of generators. We prove that not only is there a lower bound on the growth rate when changing generators, but even when changing groups: there exist positive numbers ϵ_d such that if G is a group either of polynomial growth of degree d, or of non-polynomial growth, then that growth is at least $\epsilon_d n^d$. As far as we are aware, this question has not been treated in the literature before, although it is possible that some people may have known some version of our results. Because bounds on the growth of groups are often used in probability theory, we give an application of our results to random walks.

2010 *Mathematics Subject Classification.* 20F69, 20F05, 60B15.

Key words and phrases. Polynomial growth, nilpotent, random walks, superpolynomial growth, transition probabilities.

R.L. partially supported by NSF grant DMS-1954086.

We next establish some notation. All groups in this note are assumed to be finitely generated. Given such a group G and a finite system X of generators for it, we let $s_n(G) = s_n(G, X)$ be the number of elements of G that can be expressed as a product of at most n elements from $X \cup X^{-1}$. If there exist numbers C and d such that $s_n(G) \le Cn^d$ for all n, then G is said to be of *polynomial growth*. In that case, the *growth degree* $\deg(G)$ of G is the infimum of the numbers d for which another number C can be found such that the inequality above is satisfied. This degree is independent of the generator system X, and can be characterized equivalently by $\deg(G) := \limsup \frac{\log s_n(G)}{\log n}$. A celebrated theorem of Gromov states that a finitely generated group G has polynomial growth (if and) only if G is virtually nilpotent. If G does not have polynomial growth, then, given any numbers C and d, the inequality $s_n(G) > Cn^d$ holds for infinitely many n. In other words, the upper limit above is infinite. Unproven statements about growth that are made below can be found in [Ma]. However, we have given more details than customary for algebraists in order that our proofs be more easily understood by probabilists.

In particular, we recall that if G is nilpotent of *class* $\mathrm{cl}(G) = c$ with lower central series $G = \gamma_1(G) \rhd \gamma_2(G) \rhd \cdots \rhd \gamma_c(G) \rhd \gamma_{c+1}(G) = \{1\}$, then the growth degree can be expressed as $r := \sum_{i=1}^{c} i r(i)$, where $r(i)$ is the torsion-free rank of $\gamma_i(G)/\gamma_{i+1}(G)$, i.e., the number of infinite factors in the decomposition of this quotient as a direct sum of cyclic groups. A virtually nilpotent group has the same growth degree as its nilpotent, finite-index subgroups. The formula shows that the degree is an integer. Part of our proof mimics a part of the proof of that formula; see, e.g., [Ma], p. 48. We fix a finite set $X = \{x_1, \dots, x_i, \dots\}$ of generators of G, and all lengths are computed with respect to this set. Several times we will use the simple fact that if F is a normal subgroup of G, then $s_n(G, X) \ge s_n(G/F, XF)$.

Theorem 1. *Given an integer $d > 0$, there exists a number $\epsilon_d > 0$ such that for all groups G with generating sets X, if the growth of G with respect to X is either polynomial of degree d or non-polynomial, then $s_n(G, X) \ge \epsilon_d n^d$ for all $n \ge 1$.*

An explicit expression for ϵ_d follows from our proof. We begin with two lemmas.

Write $l(z)$ for the length of z with respect to the generating system X, i.e., the smallest number of terms from $X \cup X^{-1}$ needed to write z as a product.

Lemma 2. *If G is nilpotent and torsion-free, then $r(i) \ge 1$ for $1 \le i \le c := \mathrm{cl}(G)$, and if G is not cyclic, then $r(1) \ge 2$.*

Proof. Suppose that $r(i) = 0$ for some i, and let i be the maximum such. If $i = c$, then $\gamma_c(G)$ is finite, hence trivial, contrary to the definition of c. Suppose that $i = c - 1$. Let $z_1, \dots, z_s \in G$ be a set of elements whose images generate $\gamma_{c-1}(G)/\gamma_c(G)$. They have finite order *modulo* $\gamma_c(G)$ by assumption. For any $x \in G$, $[x, z_t]$ is central, whence $[x, z_t]^k = [x, z_t^k] = [x^k, z_t]$ for all integers k and $t \le s$. Therefore, $\gamma_c(G)$ is generated by commutators $[x_i, z_j]$ of finite order. Thus also $r(c) = 0$, contrary to the choice of i. For a general $i < c-1$, dividing out $\gamma_{i+2}(G)$ and applying the same argument shows that if $r(i) = 0$, then also $r(i+1) = 0$, contrary to the choice of i.

Now assume that $r(1) = 1$. Then we can choose the set X such that only one of the x_i has infinite order *modulo* $\gamma_2(G)$. It follows that all the commutators $[x_i, x_j]$ have finite order in $\gamma_2(G)/\gamma_3(G)$. Since the images of these commutators generate that factor group, we find that $r(2) = 0$. By the previous part, that means that G is free abelian of rank $r(1)$, i.e., infinite cyclic. ∎

Lemma 3. *Let G be nilpotent of class c and degree d. Then there exists a set Z of generators of $\gamma_c(G)$ such that if $z \in Z$ has an infinite order, then $l(z^n) \le (3^d-1)n^{1/c}$ for all $n \ge 1$.*

Proof. For any set Z of generators, we have $l(z^n) \le n$. Hence, the abelian case ($c = 1$) is trivial, and we assume that $c > 1$. The proof is by induction on d. The case $d = 1$ is trivial. We may assume that $\gamma_c(G)$ is infinite, the conclusion being vacuous otherwise. Then $\deg\big(G/\gamma_c(G)\big) = d - cr(c)$ with $r(c) \ge 1$. By induction, there exists a set P of generators of $\gamma_{c-1}(G)/\gamma_c(G)$ that satisfies our requirements in $G/\gamma_c(G)$, and we can find a set Y of elements of G that map onto the set P and whose lengths in G equal the lengths of their images in $G/\gamma_c(G)$. Then $\gamma_c(G)$ is generated by the commutators of elements of Y by elements of X, and we take these commutators to constitute Z.

Let $x \in X$ and $y \in Y$, and put $z := [x, y] \in Z \subseteq \gamma_c(G)$. Now suppose that z has infinite order. Then so does the image p of y in $G/\gamma_c(G)$ (if $y^k \in \gamma_c(G)$, then $z^k = 1$). Given n, let the integer m satisfy $2n^{1/c} \ge m > n^{1/c}$, and write $n = qm^{c-1} + s$ with $q \ge 0$ and $0 \le s < m^{c-1}$. Then $0 \le q < m$. By induction applied to $p \in G/\gamma_c(G)$, there exist two elements u and v of lengths $\le Bm$, with $B \le 3^{d-cr(c)} - 1$, such that $y^{m^{c-1}} = ut$, $y^s = vw$, and $t, w \in \gamma_c(G)$. Then $z^n = (z^{m^{c-1}})^q z^s = [x^q, ut][x, vw] = [x^q, u][x, v]$ has length at most $4Bm + 2q + 2 \le (4B + 4)m \le (8B + 8)n^{1/c} \le (3^d - 1)n^{1/c}$ because $cr(c) \ge 2$. ∎

Write $\delta_d := 2^{-d^2}3^{-d^3}$.

Proof of Theorem 1. Since $d \ge 1$, the group G is infinite and satisfies $s_n(G) \ge 2n+1$: a path $1 = z_0, z_1, \ldots, z_{2n}$ from 1 to a point at distance $2n$ from 1 in the Cayley graph of G yields $2n + 1$ elements in the ball of radius n about z_n. Thus for $d = 1$ we may take $\epsilon_1 = 2$. We proceed by induction on d. If G is abelian, then $d = \deg(G) = r(1)$ and X contains d independent elements that generate a free abelian group H of rank d, hence $s_n(G) \ge s_n(H) > 2^d n^d/d!$. We now assume that G is not abelian, and at first we also assume that it is nilpotent, say of class $c > 1$. We claim that $s_n(G) \ge \delta_d n^d$.

Let F be the torsion subgroup of G. Then F is finite, G and G/F have the same growth degree, and $s_n(G) \ge s_n(G/F)$. Thus it suffices to consider G/F, i.e., we may assume that G is torsion-free. Choose a set Z as in Lemma 3, let $z \ne 1$ be in Z, and write $N := \langle z \rangle$. Then $\deg(G/N) = d - c \le d - 1$. By the lemma, the powers z^i ($1 \le i \le n^c$) produce n^c elements of length $\le (3^d - 1)n$, and the induction hypothesis supplies us with at least $\delta_{d-c}n^{d-c}$ elements of G of length $\le n$ that are all different *modulo* N. The products of these two sets of elements yield at least $\delta_{d-c}n^d \ge \delta_{d-1}n^d$ elements of length at most $3^d n$. That is, $s_{3^d n}(G) \ge \delta_{d-1}n^d$. It follows that $s_n(G) \ge \delta_{d-1}\big(\frac{n}{2\cdot 3^d}\big)^d \ge \delta_d n^d$, as claimed.

Next assume only that G is virtually nilpotent. By Theorem 9.8 of [Ma], G contains two normal subgroups, L and N, with $L \trianglelefteq N$, such that L is finite, N/L is nilpotent, and G/N is finite of index at most $g(d)$, where $g(d)$ is the maximal order of the finite subgroups of $\mathrm{GL}(n, \mathbb{Z})$, and depends only on d. An upper bound for $g(d)$ was given already by Minkowski in 1887 [Mi]. One such bound is $(2d)!$ (see equation (16) on p. 175 of [Ne]; see also [Fe] and the remarks about $g(d)$ on pp. 88–89 of [Ma]).

Again it suffices to prove the result for G/L, whence we assume that $L = 1$. Choose a set A of representatives for the cosets of N such that the length of each

$a \in A$ is at most $g(d) - 1$ (see the proof of Proposition 2.3 in [M]). Then N can be generated by elements of the form axb^{-1} ($a, b \in A$ and $x \in X$) of length at most $h_d := 2g(d) - 1$. By the previous part, N contains at least $\delta_d \cdot (\frac{n}{2h_d})^d$ elements of length at most n. Thus we can take $\zeta_d := \frac{\delta_d}{(2h_d)^d}$ to play the role of ϵ_d for virtually nilpotent groups.

Finally, if G is not virtually nilpotent, then it does not have polynomial growth. By [ST], there exists a number N_d, depending only on d, such that $s_n(G) \geq n^d$ for all $n \geq N_d$. Take η_d to be the minimum of the numbers $\frac{s_k(G)}{k^d}$ for $k = 1, 2, \ldots, N_d$ and all such G; then $\eta_d \geq 2/N_d^{d-1}$ because $s_k(G) \geq 2k + 1$. Thus, we may take $\epsilon_d := \min\{\zeta_d, \eta_d\}$. Although [ST] do not give an explicit value for N_d, they say that one can be deduced from their proof and that they believe that $N_d = \lceil \exp\{\exp\{100d^{100}\}\} \rceil$ works. ∎

Sometimes we know that G is of polynomial growth, but have only a lower bound for the degree. For that case we can prove

Theorem 4. *For a positive integer d, if G is a finitely generated nilpotent group of growth degree at least d, then $s_n(G) \geq \delta_{\lfloor 7d/4 \rfloor} n^d$ for all $n \geq 1$.*

Proof. If $d = 1$, then G is infinite, so $s_n(G) \geq n$, and $\delta_1 < 1$, whence the desired inequality holds. Thus we assume that $d \geq 2$. Write $r := \deg(G)$. If $r = d$ or if G is abelian, the claim follows from the proof of Theorem 1. Let F be the torsion subgroup of G. Then $\deg(G/F) = \deg(G)$ and $s_n(G) \geq s_n(G/F)$, whence we may assume that G is non-abelian and torsion-free. Then for $c := \mathrm{cl}(G)$, the inequality $r \geq 1 + \sum_{i=1}^{c} i = 1 + c(c+1)/2$ holds by Lemma 2, implying that $c < \sqrt{2r - 2}$.

Since $r(1) \geq 2$ by Lemma 2, G has the free abelian group of rank 2 as a factor group, and the theorem holds if $d = 2$. Now let $d = 3$. If $r(1) \geq 3$, then G has a factor group isomorphic to the free abelian group of rank 3, implying $s_n(G) \geq \delta_3 n^3$. If $r(1) = 2$, then G can be generated by elements $x_1, x_2, \ldots, x_t$, of which only x_1 and x_2 have infinite order *modulo* $G' = \gamma_2(G)$. Then all commutators $[x_i, x_j]$, $i < j$, except possibly $[x_1, x_2]$, have finite order *modulo* $\gamma_3(G) \supseteq \gamma_2(G)'$. If that last commutator also has a finite order, then the finitely generated abelian group $G'/\gamma_3(G)$ is finite, contrary to Lemma 2. Thus that commutator has an infinite order, and $r(2) = 1$. Then $\deg(G/\gamma_3(G)) = 4$, and $s_n(G) \geq \delta_4 n^4 \geq \delta_5 n^3 = \delta_{\lfloor 7d/4 \rfloor} n^3$.

This takes care of the case $d = 3$, so assume that $d \geq 4$. Then our claim holds if $r \leq 7$, so we assume that $r \geq 8$. Let $1 \neq x \in \gamma_c(G)$, and $N = \langle x \rangle$. Then $\deg(G/N) = r - c$. Suppose that $r - c < d$. If r equals 8 or 9, the inequality $c < \sqrt{2r - 2}$ shows that $c \leq 3$, and in both cases $d > (4/7)r$. For $r \geq 10$, we have $c < \sqrt{2r - 2} < (3/7)r$. Then again $d > (4/7)r$, and $s_n(G) \geq \delta_r n^r \geq \delta_{\lfloor 7d/4 \rfloor} n^d$ in all cases. It remains to establish the cases where $r - c \geq d$. These cases follow from an immediate induction on r, namely, $s_n(G) \geq s_n(G/N) \geq \delta_{\lfloor 7d/4 \rfloor} n^d$. ∎

A similar proof establishes the following version of Theorem 4.

Theorem 5. *Given a number $\alpha > 1$, there exists an (explicitly computable) number $K = K(\alpha)$ such that if G is a finitely generated nilpotent group of growth degree at least $d \geq K$, then $s_n(G) \geq \delta_{\lfloor \alpha d \rfloor} n^d$ for all $n \geq 1$.*

Proof. Choose $K = K(\alpha)$ such that if $r \geq K$, then $r - \sqrt{2r - 2} \geq r/\alpha$. We may assume that G is torsion-free. The theorem is clear for $r \leq \lfloor \alpha d \rfloor$. With the previous

notations, the inequality $c < \sqrt{2r-2}$ holds. If $r - c < d$, then $r \le \alpha d$, and our claim holds. Finally, by induction it holds, as above, for $r - c \ge d$. ∎

Unfortunately, we could not establish some natural extensions of our results. Does Theorem 4 hold without the assumption that G is nilpotent, i.e., assuming only that G has polynomial growth? For each n, what is the minimum of $s_n(G, X)$ over all groups G of growth degree d or of growth degree at least d? Which (G, X) attain that minimum? Do our results extend to vertex-transitive graphs?

We now give an application to probability of the above lower bounds. Given (G, X), define $\Delta := |X \cup X^{-1}|$. Assume that $1 \notin X$. Consider *lazy simple random walk* on G, the Markov chain whose transition probabilities from $y \in G$ to $z \in G$ are

$$p(y,z) = \begin{cases} 1/(2\Delta) & \text{if } z \in y(X \cup X^{-1}), \\ 1/2 & \text{if } y = z, \\ 0 & \text{otherwise.} \end{cases}$$

We write $p_t(y, z)$ for the t-step transition probabilities. The following is a special case of Corollary 6.6 of [LOG]:

Proposition 6. *If $C, d > 0$ are such that $s_n(G, X) \ge Cn^d$ for all $n \ge 1$, then for all $y, z \in G$ and $t \ge 1$,*

$$p_t(y,z) \le p_t(y,y) \le \frac{8d^{(d+5)/2}\Delta^{d/2}}{C\mathrm{e}^{d/2}} t^{-d/2}.$$

Combining this with our previous theorems above yields several corollaries, such as this:

Corollary 7. *Given an integer $d > 0$, there exists a number $\epsilon_d > 0$ such that for all groups G with generating sets X, if the growth of G with respect to X is either polynomial of degree d or non-polynomial, then for all $y, z \in G$ and $t \ge 1$,*

$$p_t(y,z) \le p_t(y,y) \le \frac{8d^{(d+5)/2}\Delta^{d/2}}{\epsilon_d \mathrm{e}^{d/2}} t^{-d/2},$$

where $\Delta := |X \cup X^{-1}|$. ∎

Because bounds on p_t are used extensively, such results can be used to give universal bounds for other quantities in probability.

Acknowledgments. We are grateful to Emmanuel Breuillard and David Fisher for discussions.

References

[**BT**]. M. Bucher and A. Talabutsa, Exponential growth rates of free and amalgamated products, *Israel J. Math.* **212** (2016), 521–546.

[**Fe**]. W. Feit, Finite linear groups and theorems of Minkowski and Schur, *Proc. Amer. Math. Soc.* **125** (1997), 1259–1262.

[**LOG**]. R. Lyons and S. Oveis Gharan, Sharp bounds on random walk eigenvalues via spectral embedding, *Int. Math. Res. Not. IMRN* **2018**, no. 24 (2018), 7555–7605.

[**Ma**]. A. Mann, *How Groups Grow*, LMS LNS 395, Cambridge University Press, 2012.

[**Mi**]. H. Minkowski, Zur Theorie der positiven quadratischen Formen, *J. Reine Angew. Math.* **101** (1887), 196–202.

[**Ne**]. M. Newman, *Integral Matrices*, Academic Press, New York, 1972.

[**ST**]. Y. Shalom and T. Tao, A finitary version of Gromov's polynomial growth theorem. *Geom. Funct. Anal.* **20**, no. 6 (2010), 1502–1547.

831 E 3rd St., Bloomington, IN 47405-7106 USA
E-mail address: rdlyons@indiana.edu

Givat Ram, Jerusalem 91904, Israel
E-mail address: avinoam.mann@mail.huji.ac.il