Subgroup growth: An introduction

Ashok Rajaraman
301121276
arajaram@sfu.ca

November 30, 2011

Abstract

A major topic in geometric group theory is the counting the number of subgroups of finite index in a group. This ties into the classification of finite simple groups, as well as classical geometric group theory, to culminate in a theorem similar in spirit to Gromov's theorem on polynomial growth of finitely generated groups. This short paper captures some of the elementary results in this field.

1 Introduction

Let us associate the following function with a group G:

$$n \mapsto a_n(G),$$

where $a_n(G)$ is a natural number which denotes the number of subgroups of index n in G. This is the *subgroup growth function* of G [1]. This function is well defined if the value of $a_n(G)$ is finite for all values of $n \in \mathbb{N}$.

The study of the behaviour of this function was motivated by the need to classify infinite groups by some invariant. Infinite groups with the same 'type' of subgroup growth are expected to show similar properties, as we shall see later on. In turn, subgroup growth has been the motivation for some major fields in group theory, such as strong approximation and linearity conditions for linear groups. The completion of the classification of finite simple groups proved a major turning point in the field, and a comprehensive theory of subgroup growth has been formulated by the works of Lubotzky, Segal, Mann [2], Larsen [3] and Ilani [4], to name a few. However, the tools used to analyze subgroup growth date much farther into the past. This paper is a short compilation of the approaches to the theory of subgroup growth.

Section 2 introduces some notation, and a few concepts and results that shall be used through the paper. After that, the sections are arranged roughly in order of decreasing rate of subgroup growth. Section 3 considers groups that have superexponential growth rate, and in particular, free groups. Section 4 then moves to characterize groups with exponential growth rates. Section 5 deals with one of the major theorems in subgroup growth and proves one direction of the same. Section 6 ties in generating functions with subgroup growth. Through the sections, we have a number of theorems and lemmas that are reused, and will be referred to according to their first occurrence.

2 Preliminaries

We first need some notation and a few definitions that will be reused liberally.

2.1 Definition and notation

We have already defined $a_n(G)$ as the number of subgroups of index n in G. We can also define $s_n(G)$, the total number of subgroups of index at most n in G. So, $s_n(G) = \sum_{i=1}^{n} a_i(G)$. If G is a finite group, we can define $s(G) = \sum_{i=1}^{\infty} a_i(G)$, the total number of subgroups in G.

Let us consider the simplest example, that of the group of integers under addition, $\mathbb{Z}$. It is clear that $a_n(\mathbb{Z}) = 1$ for all values of n, and $s_n(\mathbb{Z}) = n$. Of course, $s(\mathbb{Z})$ is not defined, since $\mathbb{Z}$ is an infinite group.

Let $R(G)$ be the intersection of all finite index subgroups of G. Then, we quotient out $R(G)$ from G, and this will not affect the number of subgroups of any index n, which we can see using the canonical map, i.e. $a_n(G) = a_n(G/R(G))$. This means that we need only study groups with $R(G) = \{1\}$. Such groups are called *residually finite* [1].

A class of groups $\mathcal{C}$ is considered 'good' if it is closed under taking normal subgroups, quotients and finite extensions (semidirect products). We can define an inverse system of surjective homomorphisms on this class, i.e. for $A_i, A_j \in \mathcal{C}$, we have $A_i \leq A_j$ (where $\leq$ denotes the poset order, not inclusion) if and only if there is a surjective homomorphism $\phi_{ij} : A_j \mapsto A_i$. The inverse limit of this system is a subgroup of the direct product of the groups in $\mathcal{C}$, and every group that can be described such an inverse system of surjective homomorphisms over $\mathcal{C}$ is called a pro-$\mathcal{C}$ group. If $\mathcal{C}$ is the set of all finite groups, then the inverse limit is called a *profinite group*. Related to this concept is the following definition.

Definition 2.1. *[5] The profinite completion of a group G, denoted by $\hat{G}$, is the inverse limit of the system G/N of all finite quotients of G by normal subgroups N of G.*

The profinite completion $\hat{G}$ of G has a natural topology inherited from the product topology on the system of quotient groups in the inverse system, which individually have a discrete topology. This means that there is a continuous homomorphism $i : G \mapsto \hat{G}$, which takes $g \in G$ to $gN \in \hat{G}$. The kernel of this homomorphism is the intersection of all finite index normal subgroups N in G. So, if this intersection is $\{1\}$, then the map is injective. This means that residually finite groups map as a dense subgroup into their profinite completion, and subgroups of G map to their closure in $\hat{G}$. So, the set of all finite index subgroups is in bijection with the open subgroups of the profinite completion, and their index in the respective groups (G and $\hat{G}$) is preserved.

We are interested in cases where $a_n(G)$ is finite. This is at least true for all finitely generated groups. Actually, this is true of all groups G which have a finitely generated profinite completion $\hat{G}$, since we can simply project via the homomorphism that we have discussed above, and work on the profinite completion instead.

We also define $a_n^{\lhd}(G)$ and $a_n^{\lhd\lhd}(G)$ (respectively $s_n^{\lhd}(G)$ and $s_n^{\lhd\lhd}(G)$) as the number of normal and subnormal subgroups of index n (respectively index at most n), and $m_n(G)$ as the number maximal subgroups of index n in G.

2.2 Preliminary results

Consider a group G, and a subgroup $H \leq G$, such that $[G : H] = n < \infty$. So, we have a set of n cosets of H, which we can label from 1 to n. Without loss of generality, let us label H as 1. Then, G can act on the set of cosets $\{H, g_1 H, g_2 H, \ldots, g_{n-1} H\}$ by the following action.

$$g \mapsto g\,\{H, g_1 H, g_2 H, \ldots, g_{n-1} H\} \qquad \text{for each } g \in G,$$

and this gives us a map ϕ from the elements of G to the symmetric group S_n. Note that this is a homomorphism, and G acts transitively on the cosets of H. Furthermore, the stabilizer of 1 under this action is the subgroup H itself, and this is the preimage of all the permutations that fix the first element of the permutation, and permute the rest freely. So, $\mathrm{Stab}_{G,\phi}(1) = \phi^{-1} S_{n-1}$, and for each such subgroup H of index n, we get $(n-1)!$ different transitive actions of G on $\{1, 2, \ldots, n\}$. Let $t_n(G)$ be the number of transitive actions. Then, we get our first principle to count subgroups.

Proposition 2.1. *[6, 7]*

$$a_n(G) = \frac{t_n(G)}{(n-1)!}. \tag{2.1}$$

If the actions are also primitive, i.e. if no single partition of $\{1, 2, \ldots, n\}$ is fixed, then the subgroups corresponding to these actions are maximal. So, if $p_n(G)$ is the number of primitive homomorphisms from G to S_n, then

Proposition 2.2. *[7, 1]*

$$m_n(G) = \frac{p_n(G)}{(n-1)!}. \tag{2.2}$$

Now, if G is finitely generated, with d generators, then the number of transitive homomorphism to S_n is determined by the images of each generator. So, we expect $a_n(G) \leq n.\,(n!)^{d-1}$.

Let us consider the whole set of homomorphisms from G to S_n. Denote the total number of such homomorphism by $h_n(G)$. We then get the following easy lemma.

Lemma 2.1. *[8] For any group G*

$$h_n(G) = \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G)\, h_{n-k}(G). \tag{2.3}$$

Proof. Let $h_{n,k}(G)$ be the number of homomorphisms from G to S_n in which the orbit of 1 under the action of G is exactly of length k. In order to choose this orbit, we need to choose $k-1$ other elements from n elements, with 1 already chosen. Once we have chosen this, we have t_k ways to act transitively on this orbit. As for the other $n-k$ elements, we can permute them randomly, so we have h_{n-k} ways of doing that. This gives us that

$$\begin{aligned} h_n(G) &= \sum_{k=1}^{n} h_{n,k}(G) \\ &= \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G)\, h_{n-k}(G), \end{aligned}$$

which finishes the proof. □

It would be nice to have a recursive formulation for $a_n(G)$. So, we have the following corollary.

Corollary 2.1. *[8, 4] For any group G,*

$$a_n(G) = \frac{h_n(G)}{(n-1)!} - \sum_{k=1}^{n-1} \frac{h_{n-k}(G)\, a_k(G)}{(n-k)!} \tag{2.4}$$

Proof. We use Proposition 2.1 and Lemma 2.1 and simply replace $t_k(G)$ with $a_k(G)(k-1)!$ to get the result after some rearrangement. □

We talked about finite quotients of groups while discussing the profinite completion. Often, it is possible to reduce the case of counting subgroups in infinite groups to counting subgroups in a finite quotient group. With this in mind, we also have the following two lemmas, which come in handy while discussing exponential subgroup growth.

Lemma 2.2. *[7, 1] If G is a finite group, and d is the number of generators needed to generate G, then*

$$s_n(G) \leq s(G) \leq |G|^d \tag{2.5}$$

$$d \leq \log|G|, \tag{2.6}$$

where $\log(x)$ *is the logarithm to the base* 2*.*

Proof. For the first part, the first inequality is trivial. The second follows from the fact that if we have d choices of elements, we can generate every subgroup of G. Now, if at least one subgroup of H needs d generators, then we have the following chain of finite groups, where each successive H_i is generated by i generators.

$$|H_1|\,[H_2 : H_1] \ldots [H : H_{d-1}] \leq |G|.$$

Since we cannot have index greater than 2 for each of these, we get $|G| \geq 2^d$, and the result follows. □

The second lemma is concerned with finite index subgroups.

Lemma 2.3. *[7, 1] Let K be a subgroup of G with index l. Then, for each k, the number of subgroups H of G, containing K, such that $[H : K] \leq k$, is bounded above by $l^{\lfloor \log k \rfloor}$.*

Proof. Since $K \leq H$, we should be able to find a chain of subgroups $H_1, H_2, \ldots H_s$ such that $K \leq H_1 \leq H_2 \leq \ldots \leq H$. Now,

$$[H : H_s]\,[H : H_{s-1}] \ldots [H_1 : K] \leq k.$$

This can be at most 2^k, and the chain, therefore, is of length at most $\lfloor \log k \rfloor$. To generate H, we can choose all the elements of K, and add in elements $x_1, x_2, \ldots, x_s$. Note that we could instead have multiplied those s elements by an element in K, and still generated a group in which K has rank k. This can be done in at most $l^{\lfloor \log k \rfloor}$ ways, proving our lemma. □

Now that we have some tools at our disposal, we can look at actual classes of groups.

3 Free groups

We mentioned as a footnote after proving Proposition 2.1 that if we can generate a group G with d generators, we can define maps from G to S_n by mapping the generators to the permutations. This gives us $(n!)^d$ such homomorphisms. Since the number of transitive homomorphism is definitely less than this, we know from the proposition that $a_n(G) \leq n.(n!)^{d-1}$.

3.1 Just subgroup growth

Where free groups on d generators are concerned, we can say more.

Theorem 3.1. *[9] For a free group G with $d \geq 2$ generators,*

$$a_n(G) \sim n.(n!)^{d-1} \tag{3.1}$$

$$m_n(G) \sim n.(n!)^{d-1}, \tag{3.2}$$

where we denote asymptotic equivalence by $\sim$, i.e. $f \sim g$ if $f/g \to 1$ as $n \to \infty$.

This means, in a sense, that almost all homomorphisms from the free group to the symmetric group of order $n!$ are transitive and primitive. This also means that the subgroup growth in free groups is superexponential, as we shall establish in a corollary of this result.

Proof. First of all, since we are dealing with a free group, every homomorphism can be described by the map of the generators. So, using the notation we have established, $h_n(G) = (n!)^d$. We already have a recursive formulation for $a_n(G)$, given in Corollary 2.1 [8]. So,

$$a_n(G) = n(n!)^{d-1} - \sum_{k=1}^{n-1} \binom{n-1}{k-1} (n-k)^{d-1} a_k(G).$$

Now, let us count the number of intransitive maps from G to S_n. So, we let the orbit of 1 vary in length from 1 to $n-1$, but never let it be n. Using the combinatorial argument given before in Lemma 2.1, and the known bounds for $t_n(G)$ and $h_n(G)$,

$$\begin{aligned}
\sum_{k=1}^{n-1} h_{n,k}(G) &= \sum_{k=1}^{n-1} \binom{n-1}{k-1} t_k(G)\, h_{n-k}(G) \\
&\leq \sum_{k=1}^{n-1} \binom{n-1}{k-1} (k!)^d ((n-k)!)^d \\
&= (n!)^d \sum_{k=1}^{n-1} \binom{n-1}{k-1} \frac{k}{n} \binom{n}{k}^{-(d-1)} \\
&\leq (n!)^d \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{k}^{-(d-1)}.
\end{aligned}$$

Now, note that the number of intransitive homomorphism is the same as $h_n(G) - t_n(G)$. Using this, and the fact that $\binom{n}{k} \geq 2^{k-1}n/2$ as long as $1 \leq k \leq n/2$,

$$\begin{aligned}
h_n(G) - t_n(G) &= (n!)^d \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{k}^{-(d-1)} \\
&\leq (n!)^d \sum_{k=1}^{\lfloor n/2 \rfloor} \frac{2^{-(d-1)}}{n^{d-1}2^{(d-1)(k-1)}} \\
&< \frac{4}{n}(n!)^d = \frac{4}{n}h_n(G) \\
\Leftrightarrow 1 - \frac{t_n(G)}{h_n(G)} &< \frac{4}{n} \\
\Rightarrow \lim_{n\to\infty} \frac{t_n(G)}{h_n(G)} &= 1,
\end{aligned}$$

where the last limit follows from the fact that $t_n(G) \leq h_n(G)$. This proves that most homomorphisms from a free group to the symmetric group of order $n!$ are transitive. Of course, this also means that $a_n(G) \sim n(n!)^{d-1}$.

Analogously, let us now consider all the imprimitive actions of G on $\{1, 2, \ldots, n\}$, i.e. there is some non-trivial partition that is preserved. Let us consider such a preserved parition of this set, T, such that each part has equal size. The size of each part, r, is given by $n/|T|$, and we have the following usual conditions for partitions.

$$\begin{aligned}
\{1, 2, \ldots, n\} &= \bigcup_{P_t \in T} P_t \\
P_i \cap P_j &= \emptyset \qquad \forall\, P_i, P_j \in T.
\end{aligned}$$

An imprimitive homomorphism will act on this partition and preserve some partition P_k. Let us look at the automorphism group of these partitions. Since we are fixing them, the partition members can only be permuted within themselves, so they are acted on by S_r. On the other hand, we can map paritions transitively, by $S_{|T|}$. So, preserving the paritions is simply an automorphism from the group formed by the direct product of S_r's to itself, giving us $S_r \wr S_{|T|}$. The action of G is a homomorphism from G to this automorphism group. Now we do some basic counting. The number of partitions of the set into $|T|$ parts of size r is given by first selecting r elements, then r more elements from the rest, etc., and normalizing by $|T|!$, since we do not consider the order in which these parts are chosen.

$$\frac{1}{|T|!}\binom{|T|r}{r}\binom{(|T|-1)\,r}{r}\cdots\binom{r}{r} = \frac{n!}{(r!)^{|T|}\,|T|!}.$$

Also, the number of imprimitive homomorphisms is just $t_n(G) - p_n(G)$. Using the same type of argument as in the previous case,

$$\begin{aligned}
t_n(G) - p_n(G) &\leq \sum_{|T| | n} \frac{n!}{(r!)^{|T|}\,|T|!}\left((r!)^{|T|}\,|T|!\right)^d \\
&< k_n n!\left((r!)^{|T|}\,|T|!\right)^{d-1} \\
&< k_n \frac{(n!)^d}{n^{d-1}} \\
&= k_n \frac{h_n(G)}{n^{d-1}},
\end{aligned}$$

where k_n is the number of divisors of n. This quantity grows as $o(n)$ [10]. So, the number of imprimitive homomorphisms tends to 0 as $n \to \infty$, which proves that $m_n(G)$ is asymptotically equivalent to $n(n!)^{d-1}$, using Proposition 2.2. This completes the proof of the theorem. □

As stated before, there is an easy corollary to this result, which can be thought of as a characterization of groups that have 'fast' subgroup growth.

Corollary 3.1. *Every finitely generated free group has subgroup growth (and maximal subgroup growth) of type n^n.*

Proof. Just notice that $n! \leq n^n$ and $n! \geq n^{n/2}$. Since $a_n(G) \sim n.(n!)^{d-1}$ for any free group G with d generators, the result follows. □

Free groups are comparatively easy to deal with where subgroup growth is concerned, but it is probably illustrative to notice that these are some of the easier proofs in this field. In short, counting the number of subgroups is not as easy as in the example we did for $\mathbb{Z}$.

3.2 Growth of subnormal subgroups

Let H be a subgroup of G. Then, a subgroup $K \lhd H$ is said to be a *subnormal subgroup* of G. Our next theorem deals with the growth of finite index subnormal subgroups in a free group. Here, we shall see how Schreier's work on free groups as well as the classification of finite simple groups plays a crucial role in studying subgroup growth.

Theorem 3.2. *[11] Let G be a free group with d generators. Then, for all n,*

$$a_n^{\lhd\lhd}(G) \leq n^2 2^{(n-1)(d-1)}. \tag{3.3}$$

Proof. We assume that G is not cyclic. If it were, then the result is trivial (recall example 2.1). Let us now prove the following lemma.

Lemma 3.1. *A d-generator group has at most $2n^{d-1}$ maximal normal subgroups of index n.*

This is a consequence of the classification of finite simple groups.

Proof. The classification of finite simple groups leads to the conclusion that there are at most 2 finite simple groups of order n, and only 1 if n is prime. Now, let us take a finitely generated group G on d-generators, and consider surjective homomorphisms of the same into simple groups of order n. Since there are at most 2 such groups, and since the homomorphism is completely determined by the map of the generating elements, the number of such surjective homomorphisms is $2n^d$. The kernel of such a homomorphism is definitely a normal subgroup, and furthermore, this must be a maximal normal subgroup of index n, since the quotient is simple.

The second concept we need is the fact that if n is not prime, then a simple groups has at least n automorphisms. So, the actual number of homomorphisms, ruling out the automorphisms, is $2n^d/n = 2n^{d-1}$. In the case n is prime, then the group under consideration is the cyclic group of prime order, and there are $n-1$ automorphisms. This means that the number of maps is $n^d/(n-1)$, which is still less that $2n^{d-1}$. Since we know the kernel is a maximal normal subgroup of index n, we have bounded the number of such subgroups by $2n^{d-1}$. □

Now, we refer to a major theorem on free groups.

Theorem 3.3 (Nielsen-Schreier theorem). *[12] If H is a subgroup of a free group G, then H is a free group. Furthermore, if $[G : H] = n < \infty$, and G is generated by d elements, then H is generated by $nd - n + 1$ elements.*

In the interest of brevity, we shall not give a proof for this theorem, which is common in most textbooks.

Now, we try to proceed by induction on n. If $n = 1$, then we have a degenerate case, and the theorem is obviously true. Assume that $n > 1$, and that the theorem holds for all indices less than n, and all finitely generated groups. Consider $H \lhd \lhd G$, $[G : H] = n$, and take a maximal normal subgroup $N \trianglelefteq G$ such that $H \lhd \lhd N$. Let $[G : N] = r$. Using Theorem 3.3, we know that N is a free group, and it is generated by $rd - r + 1$ elements. Also, chaining together the indices, we know that $[N : H] = n/r$. Now, if we consider N, and the subnormal group H of N, since $n/r < n$, we can apply the induction hypothesis, and we get that the number of subgroups which are subnormal to N and of index n/r are at most $(n/r)^2\, 2^{(d-1)(n/r-1)}$. We use Lemma 3.1 to bound the possibilities for N, and simply sum over all such N.

$$a_n^{\lhd\lhd}(G) \leq \sum_{r|n,r>1} 2r^{d-1} \frac{n^2 2^{(d-1)n}}{r^2 2^{r(d-1)}}.$$

Note that $d \geq 2$ and $r/2^{r-1} \leq 1/2$ for $r \geq 4$. This means that we can decompose the sum as follows:

$$\sum_{r|n,r>1} \frac{2.\,(2r)^{d-1}}{r^2 2^{r(d-1)}} \leq \frac{1}{2} + \frac{2 \times 6}{3^2 \times 8} + \sum_{r=4}^{\infty} \frac{1}{r^2}.$$

Using Euler's theorem for the convergence of $\sum_{r=1}^{\infty} r^{-2}$ to $\pi^2/6$, we can bound this sum from above by 1. So, $a_n^{\lhd\lhd}(G) < n^2 2^{(d-1)(n-1)}$, which concludes the proof. □

Notice that while the number of subgroups of index n was growing as n^n, the number of subnormal subgroups is at most exponential.

3.3 What about normal subgroups?

What about them indeed? This is not a result that we shall expand on, but we provide it here for the sake of completeness, and to sate the reader's curiosity. Assume that we have a free group G, finitely generated with d generators, and we want to find the number of normal subgroups of index n in the same. Let us define $\lambda(n) = \sum_{l_i}$, where l_i are the multiplicities of distinct primes in the prime factorization of n. Eg. for $n = 60 = 2^2.3.5$, $\lambda(60) = 2 + 1 + 1 = 4$. We then have the following theorem.

Theorem 3.4. *[13] Let G be a free group on d generators. Then, for all n,*

$$a_n^{\lhd}(G) < n^{2(d+2)(1+\lambda(n))}. \tag{3.4}$$

The proof involves classifying the isomorphisms of d-generator groups of order n, and again relies heavily on the classification of finite simple groups. Since $\lambda(n) \leq \log n$, this implies that $a_n^{\lhd}(G) \sim n^{\log n}$.

4 Exponential subgroup growth

Let us first introduce two invariants. For a group G, define the following.

$$\sigma(G) = \limsup \frac{\log s_n(G)}{n} \tag{4.1}$$

$$\sigma^-(G) = \liminf \frac{\log s_n(G)}{n}. \tag{4.2}$$

Notice that here we are considering $s_n(G)$ instead of $a_n(G)$. If the invariant $\sigma(G)$ is finite, then $s_n(G)$ is judged to be growing at most exponentially. If $\sigma(G) > 0$, then we have exponential subgroup growth, otherwise, i.e. when $\sigma(G) = 0$, we have subexponential subgroup growth. What role does $\sigma^-(G)$ play? If we can prove that $\sigma(G) = \sigma^-(G)$ for some G, then we can say that a group has some strict subgroup growth type, assuming the quantity is finite.

4.1 Characterizing groups with exponential subgroup growth

Let us also introduce a definition.

Definition 4.1. *An* upper section *of a group G is a quotient A/B, where $B \lhd A \leq G$, and $[G:B] < \infty$.*

Now, we consider a series of theorems, which are linked.

Theorem 4.1. *[14] Let G be a finitely generated group, which avoids a certain finite group H as an upper section, i.e. there is no upper section of G which is isomorphic to H. Then G has at most exponential subgroup growth.*

Note the direction of the theorem. It does not rule out the possibility of groups with exponential subgroup growth that have upper sections isomorphic to all finite groups. This theorem is 'raw', in the sense that it classifies a large number of groups having *at most* exponential growth.

We recall our definition of a 'good' class of groups closed under quotients, semidirect products and normal subgroups, given in Section 2. Assume that $\mathcal{C}$ is such a class of finite groups, which is a subset of the class of all finite groups. In the spirit of a profinite group, we can consider an inverse system and look at the free pro-$\mathcal{C}$ group on d generators, $\hat{F}_d(\mathcal{C})$. Now, if G is a d generator group which avoids some finite group H as an upper section, then we can look at its completion $\hat{G}$ in the profinite topology. This is just an image of $\hat{F}_d(\mathcal{C})$, where $\mathcal{C}$ is a class of finite groups that avoids H. The question now becomes, what sort of class is $\mathcal{C}$? Let $\mathcal{C}_k$ be the class of finite groups, $k \geq 4$, which does not contain the alternating group A_{k+1}. Clearly, $\mathcal{C}_4 \subset \mathcal{C}_5 \subset \ldots$. At the same time, note that solvable groups have abelian quotients, and so their quotients must avoid the alternating groups. If $\mathcal{S}$ is the class of all finite solvable groups, $\mathcal{S} \subset \mathcal{C}_4$.

We already established $\hat{G}$ as an image of $\hat{F}_d(\mathcal{C})$, G being generated by d generators. Now, G must lie somewhere in these 'good' classes of groups, i.e. it belongs to some $\mathcal{C}_k$. Then, its profinite completion $\hat{G}$ must be an image of $\hat{F}_d(\mathcal{C}_k)$. Conversely, if the profinite completion is an image of this free pro-$\mathcal{C}_k$ group on d generators, then d avoids the alternating group A_k as an upper section. Now, we can state the next two theorems.

Theorem 4.2. *[14] Let $\mathcal{C}$ be a good class of finite groups, does not contain all finite groups. Then, the free pro-$\mathcal{C}$ group on d generators $\hat{F}_d(\mathcal{C})$ has subgroup growth of strict type 2^n.*

But now, we already have a stratification of the class of all finite groups, by the inclusion chain described before. So, if we can prove that both the class of solvable groups, and any class of finite groups avoiding the alternating group A_k have a free pro-$\mathcal{C}$ group on d generators as an inverse limit, such that the subgroup growth rate for this group is bounded, we are done. So, the final form of the theorem, which is the form we shall work on, can be stated as follows.

Theorem 4.3. *[15, 16] Let $d \geq 2$ and $k \geq 4$. Then*

$$\sigma\left(\hat{F}_d\left(\mathcal{C}_k\right)\right) = \sigma^-\left(\hat{F}_d\left(\mathcal{C}_k\right)\right) = (d-1)\frac{\log k!}{k-1} \tag{4.3}$$

$$\sigma\left(\hat{F}_d\left(\mathcal{S}\right)\right) = \sigma^-\left(\hat{F}_d\left(\mathcal{S}\right)\right) = (d-1)\frac{\log 24}{3}. \tag{4.4}$$

As a note before the proof, notice how free pro-$\mathcal{C}$ groups have an important role to play in this theorem. The take away message after a rather long discussion will be this: *if a group has superexponential subgroup growth rate, it is very close to a free group.* It needs also be said that this is only particularly rigorous proof in this paper, and the length gives an idea as to why we refrain from proving some of the results following this.

Proof. Let us first try to get an upper bound. Consider a 'good' class of finite groups, $\mathcal{C}$. Let $\mathcal{M}_{\mathcal{C}}^t(n)$ be the set of maximal subgroups of S_n which lie in $\mathcal{C}$ and act transitively on $\{1, 2, \ldots, n\}$. Each member of the conjugacy class of a maximal transitive subgroup will also be maximal transitive. This means that $\mathcal{M}_{\mathcal{C}}^t(n)$ is a union of subgroup conjugacy classes in S_n. Let us denote the number of conjugacy classes that we need to take a union of by $\mathfrak{c}_{\mathcal{C}}^t(n)$. Also, we denote the order of the largest subgroup in $\mathcal{M}_{\mathcal{C}}^t(n)$ by $\mathrm{Ord}_{\mathcal{C}}^t(n)$. Our next step is the following proposition.

Proposition 4.1. *[14] Let G be a pro-$\mathcal{C}$ group generated by d elements. Then, for all n,*

$$a_n(G) \leq n\mathfrak{c}_{\mathcal{C}}^t(n)\left[Ord_{\mathcal{C}}^t(n)\right]^{d-1}.$$

Proof. We know from Proposition 2.1 that $a_n(G) = t_n(G)/(n-1)!$. Since G is a pro-$\mathcal{C}$ group, if we consider a transitive map $\phi : G \mapsto S_n$, $\phi(G)$ will be a transitive $\mathcal{C}$ subgroup of S_n, and it will be a subgroup of some maximal subgroup H in $\mathcal{M}_{\mathcal{C}}^t(n)$. So, if we wanted to count $t_n(G)$,

$$\begin{aligned} t_n(G) &\leq \sum_{H \in \mathcal{M}_{\mathcal{C}}^t(n)} \text{Number of homomorphisms from G to H} \\ &\leq \sum_{H \in \mathcal{M}_{\mathcal{C}}^t(n)} |H|^d \\ &\leq \mathfrak{c}_{\mathcal{C}}^t(n) \max_{H \in \mathcal{M}_{\mathcal{C}}^t(n)} \left\{\frac{n!}{|H|}|H|^d\right\} \\ &\leq n!\mathfrak{c}_{\mathcal{C}}^t(n)\left[\mathrm{Ord}_{\mathcal{C}}^t(n)\right]^{d-1}. \end{aligned}$$

The last two steps follow from the fact that the size of the conjugacy class of a subgroup H of $S_n$is given by $[S_n : N_{S_n}(H)]$, which is less than $n!/|H|$. Then, we just use the formula for counting $a_n(G)$ given the number of transitive homomorphisms to complete the proof. □

After this, we need two results about the symmetric group and about permutation groups in general, which we shall state without proof.

Proposition 4.2. *[15] For a 'good' class of groups $\mathcal{C}$, $\mathcal{S} \subseteq \mathcal{C} \subseteq \mathcal{C}_k$, there exists a real number c which depends on $\mathcal{C}$, such that $\mathfrak{c}_{\mathcal{C}}^{t}(n) \leq n^c$ for all n.*

Proposition 4.3. *[11] Let $\mathcal{C}_k^{\lhd}$ be the class of finite groups such that, for each $G \in \mathcal{C}_k^{\lhd}$, and for all $n > k$, we can find a chain*

$$\{1\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_l = G,$$

such that each G_i is maximal in G_{i+1}, but no $G_{i+1}/G_i \cong A_n$ for any $n > k$. Take $\mathcal{C} \subseteq \mathcal{C}_k^{\lhd}$, $k \geq 4$, Then, $Ord_{\mathcal{C}}^{t}(n) \leq (k!)^{(n-1)/(k-1)}$.

Once we have these two results, combining with Proposition 4.1, we get

$$\begin{aligned}
a_n(G) &\leq n.n^c (k!)^{(n-1)(d-1)/(k-1)} \\
\Rightarrow \log s_n &= \log \sum_{i \leq n} a_i(G) \\
&\leq \log \sum_{i \leq n} n^{c+1} (k!)^{(n-1)(d-1)/(k-1)} \\
&\leq n(d-1) \log (k!)^{1/(k-1)} + (c+2) \log n \\
\Rightarrow \sigma(G) &\leq (d-1) \log (k!)^{1/(k-1)}.
\end{aligned}$$

Now, to get the upper bounds, we set $\mathcal{C}$ to be the class of solvable groups, $\mathcal{S}$, with $k = 4$, and $\mathcal{C} = \mathcal{C}_k$.

For the lower bound, consider the class $\mathcal{C}$ of finite groups such that $S_k \in \mathcal{C}$, $\mathcal{S} \subseteq \mathcal{C}$, and $k \geq 4$. We then try to prove by induction the following inequality for all $t \geq 0$.

Lemma 4.1. *For $t \geq 0$,*

$$\log a_{k^t}\left(\hat{F}_d(\mathcal{C})\right) \geq \kappa (d-1)\left(k^t - 1\right) - ct^2,$$

where $\kappa = \log k!/(k-1)$, and $c = (\log k)^2$.

For the base case, consider $t = 1$. Consider all homomorphisms from the free group on d generators, F_d to S_k. The total number of homomorphisms is given by $(k!)^d$, and if we consider k large enough, we know that $a_k(F_d) \sim k(k!)^{d-1}$, from Theorem 3.1. Now, the kernels of all homomorphisms from F_d to S_k must intersect in some subgroup X. This means that every k-index subgroup in F_d must contain X. If we consider the quotient group F_d/X, this must be a finite group in $\mathcal{C}$, since $S_k \in \mathcal{C}$, and so we can find a surjective homomorphism from $\hat{F}_d(\mathcal{C})$ to F_d/X. This gives us

$$\begin{aligned}
a_k\left(\hat{F}_d(\mathcal{C})\right) &\geq a_k(F_d) \geq (k!)^{d-1} \\
\Rightarrow \log a_k\left(\hat{F}_d(\mathcal{C})\right) &\geq (d-1) \log k! \\
&= (d-1)\kappa(k-1),
\end{aligned}$$

proving the case for $t = 1$. Now assume the following is true.

$$\log a_{k^{t-1}}\left(\hat{F}_d(\mathcal{C})\right) \geq \kappa(d-1)\left(k^{t-1} - 1\right) - c(t-1)^2.$$

At this point we again turn our eyes to Schreier's work on free groups, and in particular, to his formula for pro-$\mathcal{C}$ groups.

Theorem 4.4 (Schreier's formula for pro-$\mathcal{C}$ groups)**.** *If $H \leq \hat{F}_d(\mathcal{C})$ is an open subgroup of index l in $\hat{F}_d(\mathcal{C})$, which is the pro-$\mathcal{C}$ completion of the free group F_d on d generators, then H is a free pro-$\mathcal{C}$ group on $l(d-1)+1$ generators.*

This means that each open subgroup of index k^{t-1} in $\hat{F}_d(\mathcal{C})$ is isomorphic to $\hat{F}_m(\mathcal{C})$, where $m = k^{t-1}(d-1)+1$. Such a subgroup will contain at least $(k!)^{m-1}$ subgroups of index k, using the base case. Also, we know, through Lemma 2.3, that the number of subgroups of $\hat{F}_d(\mathcal{C})$ of index k^{t-1} which contain a given subgroup of index k^t is at most $k^{t\log k}$. So,

$$a_{k^t}\left(\hat{F}_d(\mathcal{C})\right) \geq \frac{2^n (k!)^{m-1}}{k^{t\log k}},$$

where $n = \kappa(d-1)\left(k^{t-1}-1\right) - c(t-1)^2$. Simple manipulations now give us

$$\log a_{k^t}\left(\hat{F}_d(\mathcal{C})\right) \geq \kappa(d-1)\left(k^t-1\right) - ct^2,$$

which finishes the induction.

Now, for arbitrary $n > 1$, choose t and r carefully, to satisfy $k^{2t} \leq n < k^{2(t+1)}$ and $rk^t \leq n < (r+1)k^t$. If we map $\hat{F}_d(\mathcal{C})$ onto a finite cyclic group, of order n/r, we can see that an open subgroup of index r exists. So, $H \cong \hat{F}_{r(d-1)+1}(\mathcal{C})$ by Schreier's theorem again, and from the previous result,

$$\begin{aligned}\log a_{k^t}(H) &\geq \kappa(r(d-1)+1)\left(k^t-1\right) - ct^2\\ &\geq \kappa(d-1)\left(n-r-k^t\right) - ct^2.\end{aligned}$$

Note that $ct^2 \leq c(\log n)^2/(2\log k)^2$, and $r \leq k^{t+2} \leq k^2 n^{1/2}$. Using these inequalities, and also knowing that $s_n\left(\hat{F}_d(\mathcal{C})\right) \geq a_n(H)$, we get

$$\begin{aligned}&\log s_n\left(\hat{F}_d(\mathcal{C})\right) \geq n\kappa(d-1) - O(n)\\ \Rightarrow\ &\sigma^-\left(\hat{F}_d(\mathcal{C})\right) \geq (d-1)\frac{\log k!}{k-1},\end{aligned}$$

where we get the last part by substitution the value of κ. Then, we apply the same trick of choosing $\mathcal{C}$ to be $\mathcal{C}_k$ and $\mathcal{S}$ to get the bounds and finish the proof. □

4.2 An example for exponential subgroup growth

Having done all this work, let us look at an example to illustrate exponential subgroup growth. For some prime p, and some positive integer t, consider the group $G_t = C_p \wr C_{p^t}$, where C_k denotes the cyclic group of order k. We can instead look at this group as the semidirect product $A \rtimes C_{p^t}$. Now, if we consider $C_{p^t} \cong \langle x\rangle$ and $A \cong \mathbb{F}_p[\langle x\rangle]$, then A is a group algebra considered as an $\langle x\rangle$ module, or a $\mathbb{F}_p$ vector space of dimension p^t. Using q-binomial coefficients, it is easy to note that the number of subspaces in this vector space which have dimension p^t-1 is $\left(p^{p^t}-1\right)/(p-1)$, and these are just subgroups of index p^{t+1}. We can form an inverse system by mapping G_{t+1} to G_t for all t, and take the inverse limit to get a pro-p group on two generators, isomorphic to $C_p \wr \mathbb{Z}/p\mathbb{Z}$.

Now, if we consider the infinite group $G = C_p \wr C_\infty$, we can map this onto G_t for all t by adding a cyclic relation. The pro-p completion of this group is the same as the inverse limit that we got in the previous case. If we fix some c such that $1 < c < p^{1/p^2}$, and if we want to count the number of subgroups of index n such that $p^{t+1} \leq n < p^{t+2}$, then $a_{p^{t+1}}(G_t)$ is, as counted before, greater than p^{p^t-1}, which, by the inequalities, exceeds c^n.

The reason we are interested in this example is that this is a lower bound in the growth rate of a large class of groups which are not free.

5 Polynomial subgroup growth

Here, let us review what is probably the most famous theorem in geometric group theory.

Theorem 5.1 (Gromov's theorem). *[17] A finitely generated group has polynomial growth if and only if it is virtually nilpotent, i.e. it contains a finite index nilpotent subgroup.*

Here, the term 'growth' refers to growth of words using a finite set of generators. The question is, how can we extend this to subgroup growth? For one thing, groups do not need to be finitely generated to make sense of their subgroup growth. However, if we do restrict ourselves to finitely generated groups, what can we say about groups with 'slow' subgroup growth? Here, we have another remarkable theorem.

Theorem 5.2 (Polynomial Subgroup Growth theorem). *[2, 18] Let G be a finitely generated residually finite group. Then G has polynomial subgroup growth if and only if it is virtually solvable of finite rank, i.e. it contains a finite index solvable subgroup which is finitely generated.*

The theorem is very similar in spirit to Gromov's theorem. However, there are a few major differences. Most importantly, this is not a classification of *all groups with polynomial subgroup growth*. Indeed, there are classes of finitely generated profinite groups which have polynomial subgroup growth, and these may be the completion of non-finitely generated groups. The theorem, though, is quite powerful in its own right.

The proof of this theorem is quite involved, and we prove here only one direction, that virtually solvable groups of finite rank have polynomial subgroup growth. The proof of the other direction proceeds by first showing that a finitely generated linear group over a field of characteristic zero which is not virtually solvable does not have polynomial subgroup growth. Then, groups with a weak form of polynomial subgroup growth are classified as groups that have minimal upper sections of some finite rank, i.e. there is an upper bound on the size of their generating set. This result depends crucially on the classification of finite simple groups. It is this weak form of polynomial subgroup growth which is then extended to imply polynomial subgroup growth.

Proof. We begin with a definition.

Definition 5.1. *A* derivation *from a group G to a G-group H is a map $\delta : G \mapsto H$ such that*

$$\delta(x.y) = y\delta(x)\,y^{-1}\delta(y)\,.$$

The set of all derivations from G to H forms an abelian group if H is a G-module. We are interested in the largest size of the set of derivations, $\mathrm{der}(G, H)$. As long as we are dealing with finitely generated groups, and finitely generated quotients, if we want to get an upper bound on the size of the set of derivations from a finite quotient G/N to the normal subgroup N,

$$\mathrm{der}(G/N, N) \leq |N|^d,$$

where d is the size of the generating set of G/N. This result comes from simply mapping the generators. The second thing we note about derivations is that a derivation from G/N to N defines a semidirect product complement for N in G. Now, we have the following proposition.

Proposition 5.1. *[1] For a group G, and a normal subgroup N of finite rank in G,*

$$a_n(G) \leq \sum_{t|n} a_{n/t}(G/N)\, a_t(N)\, t^d,$$

where d is the size of the generating set of G/N. If G/N is a finite quotient, then

$$s_n(G) \leq s_n(N)\, n^{|G/N|}$$

Here, we prove only the first part of the proposition.

Proof. Consider $H \leq G$, such that $[G : H] = n$. Then, we can use the second isomorphism theorem to say that $NH/N \cong H/(H \cap N)$. Assume $[N : H \cap N] = t$, and let us look at the normalizer of the group $H \cap N$ (call it A) in NH. We can use the second isomorphism theorem again, to say $A/(A \cap N) \cong NH/N$, and this must be a subgroup of G/N.

If we want to count H now, we are looking at complements to N in G. At the same time, $H/(H \cap N)$ is a complement to $(A \cap N)/(H \cap N)$ in $A/(H \cap N)$. Using the previous results on derivations, the maximum number of derivations from $A/(A \cap N)$ to $(A \cap N)/(N \cap H)$ can be estimated. First, $(A \cap N)/(N \cap H)$ has size at most t. The number of generators of $A/(A \cap N)$ is less than the number of generators needed for G/N, since it is isomorphic to $NH/N \leq G/N$. So, the number of derivations is bounded by t^d, where d is the number of generators of G/N. Since the size of $(A \cap N)/(N \cap H)$ is at most t which means that the choices for $H \cap N$ is at most $a_t(N)$. On the other side, NH has $a_{n/t}(G/N)$ choices. Now, we just sum over all possibilities for t. This proves the first result. □

The next result we need concerns nilpotent groups, and gives us an automatic bound on the growth rate of subgroups in nilpotent groups.

Lemma 5.1. *[1] If G is a finitely generated nilpotent group with d generators, then*

$$a_n(G) < n^d$$
$$s_n(G) < n^{1+d}.$$

Proof. We prove the result for finite quotients, and it extends to the whole group. So let G be a finite group. Let p be a prime. If H is a subgroup of G with index p, then it is normal, and we can find a surjective homomorphism $\phi : G \mapsto C_p$ with kernel H. These homomorphisms can be completely defined by the image of the generators, and so we can find $p^d - 1$ such homomorphisms. So, $a_p(G) < p^d$. For any other subgroup of index $n = kp$, every such subgroup must be contained in a subgroup K of index p. Assume that $a_k(G) \leq k^d$ as our induction hypothesis. Then, $a_{kp}(G) \leq a_p(G) \,. \max_{[G:K]=p} a_k(K)$. So, $a_n(G) < n^d$. To get the bound on $s_n(G)$, just sum $a_n(G)$ over all n. □

Now, we use the previous lemma and Proposition 5.1 to prove the next result.

Proposition 5.2. *[1] If a group G has a chain $\{1\} = G_k \lhd G_{k-1} \lhd \ldots \lhd G_0 \lhd G$ where each G_i/G_{i+1} is nilpotent, finitely generated by d_i elements, and G/G_0 has finite order l, then*

$$s_n(G) \leq n^{l+k+\sum_i d_i}$$

Proof. Since G_i/G_{i+1} is nilpotent of finite rank, we get $a_n(G_{k-1}) < n^{d_{k-1}}$. Assume that $a_n(G_i) < n^{k-i-1+d_k+d_{k-1}+\ldots+d_{i+1}}$. Using Proposition 5.1, we get

$$\begin{aligned}
a_n(G_{i-1}) &\leq \sum_{t|n} a_{n/t}(G_{i-1}/G_i)\, a_t(G_i)\, t^{d_i} \\
&\leq \sum_{t|n} (n/t)^{d_i}\, t^{d_{i+1}+d_{i+2}+\ldots+d_k+k-1-i} t^{d_i} \\
&\leq n^{d_i} \sum_{t|n} t^{d_i} t^{-d_i} t^{d_{i+1}+d_{i+2}+\ldots+d_k+k-1-i} \\
&< n^{d_i+d_{i+1}+\ldots+d_k+k-i} \\
\Rightarrow a_n(G_0) &< n^{k-1+\sum_i d_i} \\
\Rightarrow s_n(G_0) &< n^{k+\sum_i d_i}.
\end{aligned}$$

Now, using the condition that $s_n(G) \leq s_n(N)\, n^{|G/N|}$ to prove the proposition. □

And finally, we just note that such a chain exists for every virtually solvable group with the solvable subgroup being finitely generated, which concludes the proof. □

In Section 4, we discussed an invariant $\sigma(G)$. There is a corresponding invariant that one may wish to study for polynomial subgroup growth. This invariant, denoted by $\alpha(G)$, can be defined as

$$\alpha(G) = \limsup \frac{\log s_n(G)}{\log n}.$$

For some simple abelian groups, such as $\mathbb{Z}^d$, finding this is comparatively straightforward. We use Proposition 5.1 to prove that $s_n(G) \leq n.s_n(N)$ for a normal subgroup N of G. This means that, for $\mathbb{Z}^d$, we get a subgroup growth rate of n^d, and the invariant is just d. The natural way to look at this is to look at all the subspaces of $\mathbb{Z}^d$ of index 1, and recursively compute the subgroup growth rate.

6 The Zeta function

Since we are counting the number of subgroups of finite index, and we already have a recursive formulation (Corollary 2.1), one might be tempted to encode the counting sequence as a generating function. The obvious choice may be an ordinary generating function,

$$A_G(x) = \sum_{n\geq 1} a_n(G)\, x^n.$$

However, for groups with polynomial subgroup growth, we have a different choice. Consider the following Dirichlet series:

$$\zeta_G(s) = \sum_{n\geq 1} \frac{a_n(G)}{n^s}. \tag{6.1}$$

Hark back to the old example on $\mathbb{Z}$. In that case, $a_n(\mathbb{Z}) = 1$ for all n. So, we get

$$\zeta_{\mathbb{Z}}(s) = \sum_{n\geq 1} \frac{1}{n^s},$$

which is just the Reimann-Zeta function. This in itself is no surprise, since we have formulated it by definition. Similarly, we can do the same for other groups. What information can we extract from this, though? Suppose we have a group with polynomial growth, $\alpha(G) = c$. Then, the Dirichlet series given above converges for $\Re(s) > c$, and it is analytic on the half-plane where this condition is satisfied.

Our next result looks at nilpotent groups in light of their zeta functions.

Proposition 6.1. *[1] The zeta function of a nilpotent group G can be given by*

$$\zeta_G(s) = \prod_{p\ prime} \sum_{i\geq 0} \frac{a_{p^i}(G)}{p^{is}}. \tag{6.2}$$

Proof. Note that a finite nilpotent group isomorphic to the direct product of its Sylow subgroups. We replace any infinite nilpotent group by a finite quotient of the same. Choosing a subgroup H of G, we see that this subgroup must be isomorphic to the direct product of the intersection of H with each Sylow subgroup of G. So, we first get that, for $n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$,

$$a_n(G) = \prod_{p_i | n} a_{p_i^{l_i}}(G).$$

Now, since we are dealing with generating functions, we can encode the number of subgroups of some index in a p-group of order p^t by

$$\zeta_G(s) = \sum_{t\geq 0} \frac{a_{p^t}(G)}{p^{ts}},$$

and multiplying all these together just counts the total number of subgroups. □

Finally, another motivation for studying the properties of these zeta functions, the proof of which is not given here.

Theorem 6.1. *[19] For $\mathbb{Z}^d$,*

$$\zeta_{\mathbb{Z}^d}(s) = \zeta(s)\zeta(s-1)\dots\zeta(s-d+1). \tag{6.3}$$

7 Conclusion

The methods discussed above are by no means the only ones used to analyze subgroup growth. Of particular interest are probabilistic methods that are used to study profinite groups. Any topic on groups is essentially incomplete unless one has studied the implications of the same on p-groups, and a large body of work has been done on subgroup growth in these, as well as on pro-p groups, a flavour of which we saw in the example on exponential subgroup growth in Section 4.2.

Subgroup growth is a comparatively unwieldly topic to cover in just a few pages, mostly because of the sheer number of concepts used. In that sense, this is not a complete or comprehensive review of the subject, and instead aims to be a somewhat gentler introduction than the papers and books listed in the reference, mostly to provide a taste of the work that has been done. The field is still strewn with a variety of open problems, and as shown in the last section, it is also of interest from a combinatorial and number theoretic perspective.

References

[1] A. Lubotzky and D. Segal. *Subgroup growth*, volume 212. Birkhauser, 2003.

[2] A. Lubotzky, A. Mann, and D. Segal. Finitely generated groups of polynomial subgroup growth. *Israel journal of mathematics*, 82(1):363–371, 1993.

[3] M. Larsen and A. Lubotzky. Normal subgroup growth of linear groups: the (g2; f4; e8)-theorem. *Arxiv preprint arXiv:1108.1044*, 2011.

[4] I. Ilani. Counting finite index subgroups and the p. hall enumeration principle. *Israel Journal of Mathematics*, 68(1):18–26, 1989.

[5] J.S. Wilson. *Profinite groups*. Number 19. Oxford University Press, USA, 1998.

[6] P. de La Harpe. *Topics in geometric group theory*. University of Chicago Press, 2000.

[7] IMS Dey. Schreier systems in free products. *Proc. Glasgow Math. Soc*, 7:61–79, 1965.

[8] M. Hall. Subgroups of finite index in free groups. *Canad. J. Math*, 1(1):187–190, 1949.

[9] M. Newman. Asymptotic formulas related to free products of cyclic groups. *Mathematics of Computation*, pages 838–846, 1976.

[10] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers*. Clarendon press, 1984.

[11] A.V. Borovik, L. Pyber, and A. Shalev. Maximal subgroups in finite and profinite groups. *TRANSACTIONS-AMERICAN MATHEMATICAL SOCIETY*, 348:3745–3762, 1996.

[12] D.J.S. Robinson. *A Course in the Theory of Groups*, volume 80. Springer, 1996.

[13] A. Lubotzky. Enumerating boundedly generated finite groups. *Journal of Algebra*, 238(1):194–199, 2001.

[14] L. Pyber and A. Shalev. Groups with super-exponential subgroup growth. *Combinatorica*, 16(4):527–533, 1996.

[15] A. Maróti. On the orders of primitive groups. *Journal of Algebra*, 258(2):631–640, 2002.

[16] A. Mann. Enumerating finite groups and their defining relations. *Journal of Group Theory*, 1(1):59–64, 1998.

[17] M. Gromov. Groups of polynomial growth and expanding maps. *Publications Mathématiques de l'IHÉS*, 53(1):53–78, 1981.

[18] J.S. Wilson. Finite presentations of pro-p groups and discrete groups. *Inventiones Mathematicae*, 105(1):177–183, 1991.

[19] F.J. Grunewald, D. Segal, and G.C. Smith. Subgroups of finite index in nilpotent groups. *Inventiones Mathematicae*, 93(1):185–223, 1988.