Representation Growth vs Subgroup Growth

David A. Craven

18th February 2009

The subgroup growth of finitely generated groups was seen last term, in a lecture of Dan Segal. This time, we see representation growth, and how it is similar to, and different from, subgroup growth.

1 Introduction

Let G be a group. If H is a subgroup of G, then let H_G denote the *core* of H in G; this is the largest normal subgroup of G contained in H, and can be seen to be $\bigcap_{g\in G} H^g$. If H has index n in G, then H_G has index at most $n!$, and in particular, every subgroup of finite index contains a normal subgroup of finite index.

We say that G is *residually finite* if the intersection of all of the (normal) subgroups of finite index is trivial. This is equivalent to saying that for every element $x \neq 1$, there is some normal subgroup N of finite index such that $x \notin N$, so that the image of x in G/N is non-trivial. If one wants to study a group via its finite images, then G has to be residually finite, since nothing can be said about the *finite residual* – the intersection of the subgroups of finite index.

Therefore one should study residually finite groups. The example of the Cartesian product $(C_2)^\infty$ – a residually finite group with infinitely many subgroups of index 2 – suggests that non-finitely generated groups could be bad. Since the free group on n generators has only finitely many subgroups of index m – a result of Marshall Hall Jr – we see that any finitely generated group has only finitely many subgroups of index n.

This restricts our attention to finitely generated, residually finite groups. This is good for subgroup growth (counting the subgroups of index n), but things are going to be bad for studying representation growth (counting the number of representations of degree n with kernel of finite index). For example, if $G = \mathbb{Z}$, then there are infinitely many representations of degree 1, and none of degree 2 or above; this is going to be true for any infinite abelian group. What we see here is that representation growth has difficulty dealing with abelian groups, and by extension so-called *virtually abelian* groups; that is, groups with an abelian subgroup of finite index. Indeed, if G has any virtually abelian, infinite quotient, then you are going to get an infinity in the number of representations of G for some degree.

In fact, this is a sufficient condition as well. Write $r_n(G)$ for the number of (inequivalent) complex representations of degree n, whose kernel has finite index.

Theorem 1.1 Let G be a finitely generated, residually finite group. Then $r_n(G)$ is finite for all n, if and only if for every subgroup H of finite index, $|H/H'|$ is finite.

I have proved this in a previous Kinderseminar, and so will not do so here. Broadly speaking, it is an application of Jordan's Theorem, which states that there is a function $f : \mathbb{N} \to \mathbb{N}$ such that a finite group G with an irreducible complex representation of degree n has an abelian normal subgroup of index at most $f(n)$. (A theorem of Michael Collins states that this function may be taken to be $(n+1)!$ for large n.)

Groups with the property that all finite-index subgroups have finite abelianizations are called *FAb*.

2 Representation Growth Grows

If $G = \mathbb{Z}$, then the number of subgroups of index n is 1, and so subgroup growth is really the wrong word here; such groups are said to have *constant (normal) subgroup growth.* The question is, does this happen for the numbers $r_n(G)$; that is, is there an infinite, residually finite group G such that $r_n(G) < N$ for all n?

Theorem 2.1 Let G be a finitely generated, residually finite group G. The numbers $r_n(G)$ are universally bounded by a number N if and only if G is finite.

I will not prove this theorem here, because its proof is far too complicated. Like many statements about residually finite groups, this translates to a theorem about finite groups. Let G be a finite group, and write

$$m(G) = \max_{n \in \mathbb{N}} r_n(G).$$

(Thus $m(G)$ is the maximal multiplicity of the irreducible character degrees of G.)

Theorem 2.2 There is a function $f : \mathbb{N} \to \mathbb{N}$ such that, if G is a finite group, then $m(G) \leqslant f(|G|)$.

Andrei Jaikin proved this theorem for p-groups, and then for soluble groups (using the Fitting subgroup). Moretó reduced the question for general groups to proving it for finite simple groups. For groups of Lie type, this is not particularly difficult (although more will be said about this later), and I proved it for alternating groups via combinatorics.

The other point is, since there are only finitely many groups of a given order, the function f may simply be taken to be $f(n) = \min_{|G|=n} m(G)$. Moving to the infinite case, let $G = G_0 \geqslant G_1 \geqslant \cdots$ be a descending sequence of subgroups of finite index, whose intersection is trivial. Writing $m(G_i) = n_i$, we have that $r_{i_j}(G_i) \geqslant n_i$ for some $1 \leqslant i_j \leqslant \sqrt{G_i}$, and hence $r_{i_j}(G) \geqslant n_i$ for each i, a divergent subsequence. In particular, it grows faster than the function $f(n)$ in the theorem above. We see therefore the following theorem.

Theorem 2.3 There is a function $f : \mathbb{N} \to \mathbb{N}$ such that if G is a FAb group, then $r_n(G) \geqslant f(n)$ for infinitely many n. In particular, the growth in the partial sums of the $r_i(G)$ is bounded below by a the function f.

This is the disproof of the opposite of the theorem of Kassabov and Nikolov, which proves that the partial sums can grow arbitrarily fast, in some sense.

3 Growth of Finite Simple Groups

The representation growth of finite simple groups, along with the representation growth of p-groups, are the two areas that are of interest in understanding the results of the previous section. Unfortunately Jaikin's proof for p-groups, while amenable to deriving an explicit function, goes via a collection of different results. Because the proof is very indirect, there seems relatively little reason to calculate a lower bound for the representation growth from this proof.

Of more interest are the finite simple groups. The sporadic groups are of no interest for asymptotics, although the number $m(G)$ has been found for all twenty-six of them, using the Atlas.

For the alternating groups (or rather the symmetric groups) the representation growth has not been calculated. However, a lower bound is known, and must at least have been proved non-constructively for the proof of the main theorem.

Theorem 3.1 For all sufficiently large n, $m(S_n) > n^{0.15}$.

Thus $m(S_n)$ is at least a rational function in the *degree* of the symmetric group.

Conjecture 3.2 There are constants a and b such that, for all sufficiently large n,

$$n^a \leqslant m(S_n) \leqslant n^b.$$

The only way that this cannot be true is if there are super-polynomially (in n) many characters of the same degree for S_n. There are only $\mathrm{e}^{a\sqrt{n}}/bn$ characters of S_n to begin with, so this seems somehow unlikely. If this conjecture is true, when one moves from the degree of the symmetric groups to the order of the symmetric groups, the different constants in the power of n collapse to the same order. Hence this would say that $m(S_n) = \mathrm{O}(\log(n!)/\log\log(n!))$, giving the exact order of the growth of S_n.

Now let us move on to the finite groups of Lie type. If we fix the Lie rank L, then we can show that $m(L(q)) = \mathrm{O}(|L(q)|^{\varepsilon})$ for some ε depending on L. However, as the Lie rank r increases, this constant ε decreases so that, for example,

$$\lim_{n\to\infty} \frac{\log m(\mathrm{SL}_n(q))}{\log|\mathrm{SL}_n(q)|} = 0.$$

Of course, this is not important for the exceptional groups of Lie type, so one may explicitly calculate the constants ε in this case. I have done this, and they are in the following table.

Group	$\mathrm{O}(m(G))$	$\mathrm{O}(\|G\|)$	$\log(m(G))/\log(\|G\|)$
${}^2B_2$	q	q^5	1/5
G_2	q^2	q^{14}	1/7
${}^2G_2$	q	q^7	1/7
F_4	q^4	q^{52}	1/13
${}^2F_4$	q^2	q^{26}	1/13
${}^{\varepsilon}E_6$	q^6	q^{78}	1/13
E_7	q^7	q^{133}	1/19
E_8	q^8	q^{248}	1/31

The numbers in the second column should be familiar, since they are the Lie ranks of the groups! In fact, this is true for all of the groups, by a theorem of Liebeck and Shalev.

The problem with the classical groups is that, if you fix the prime and let the Lie rank vary, what happens to the orders, since the values in the table above are really only valid for large q. For the classical groups, in the table below we see lower bounds for $m(G)$.

Group	O(|G|)	Multiplicity
$\mathrm{PSL}_n(q)$	$\frac{q^{n^2-1}}{\gcd(q-1,n)}$	$\dfrac{\phi(q^n-1)}{n^2(q-1)}$
$\mathrm{PSU}_{2n}(q)$	$\frac{q^{4n^2-1}}{\gcd(q+1,2n)}$	$\dfrac{\phi(q^n-1)}{4n^2}$
$\mathrm{PSU}_{2n+1}(q)$	$\frac{q^{4n(n+1)}}{\gcd(q+1,2n+1)}$	$\dfrac{\phi(q^n-1)}{(2n+1)^2}$
$\mathrm{PSp}_{2n}(q)$	$\frac{q^{2n^2+n}}{\gcd(2,q-1)}$	$\dfrac{\phi(q^n-1)}{4n}$
$\mathrm{P\Omega}_{2n+1}(q)$	$\frac{q^{2n^2+n}}{\gcd(2,q-1)}$	$\dfrac{\phi(q^n-1)}{4n+2}$
$\mathrm{P\Omega}^+_{2n}(q)$	$\frac{q^{2n^2-n}}{\gcd(4,q^n-1)}$	$\dfrac{\phi(q^n-1)}{4n}$
$\mathrm{P\Omega}^-_{2n+2}(q)$	$\frac{q^{2n^2+n+1}}{\gcd(4,q^{n+1}+1)}$	$\dfrac{\phi(q^n-1)}{4n+4}$

Each of these tends to infinity as $|G|$ tends to infinity. The question is, how quickly? It should be just slower than a rational function, but at the moment, I'm being stupid and cannot prove this. In particular, it should be relatively easy to prove that the alternating groups are definitely the slowest-growing simple groups.

4 From Representation Growth to Zeta Functions

One technique of authors (although not me) is to encode the numbers $r_n(G)$ into a zeta function:

$$\zeta_G(s) = \sum_{n=1}^{\infty} r_n(G) n^{-s}.$$

Some important results in this branch of the subject have been made by a number of authors, particularly in the case where G is a pro-p group. In this case, G has FAb if and only if all terms of the derived series are of finite index. In particular, if G is non-soluble but just infinite, then G has FAb. Thus examples of groups that have finite abelianizations are the Nottingham groups, the Grigorchuk group, the various index-subgroups of the Nottingham group, and so on.

Andrei Jaikin proved the following theorem about pro-p groups with FAb, in 2005.

Theorem 4.1 (Jaikin) Let G be a compact p-adic analytic group with FAb, and suppose that p is odd. There are natural numbers $n_1, \ldots, n_k$ and rational functions $f_1(p^{-s}), \ldots, f_k(p^{-s})$ such that

$$\zeta_G(s) = \sum_{i=1}^{n} n_i^{-s} f_i(p^{-s});$$

in particular, $\zeta_G(s)$ is a rational function of p^{-s}.

Actually computing this zeta function is not easy, however, and very few calculations have been done. Jaikin has done the case where $G = \mathrm{SL}_2(\mathbb{Z}_p)$, and Klopsch and Voll have attacked the case where $G = \mathrm{SL}_3^1(\mathbb{Z}_p)$, the first congruence subgroup of $\mathrm{SL}_3(\mathbb{Z}_p)$.

Let $R_n(G)$ be the partial sum $\sum_{i=1}^n r_i(G)$. Then the *abscissa of convergence* is

$$\rho(G) = \limsup_{n\to\infty} \frac{\log R_n(G)}{\log n}.$$

If G has the congruence subgroup property, then $\rho(G)$ is finite. The number $\rho(G)$ may be finite, zero, or infinity.

Theorem 4.2 (Larsen, Lubotzky) Let G be a complex, semisimple algebraic group. Let r denote its Lie rank, and κ denote the number of positive roots, which is $(\dim G - r)/2$. Then

$$\rho(G) = \frac{r}{\kappa} = \frac{2}{h},$$

where h is the Coxeter number of G.

However, if K is non-Archimedean and local, G is a simple algebraic group over K, and U is a compact open subgroup (think $\mathrm{SL}_n(\mathbb{Z})$), then $\rho(U) \geqslant 1/15$. This seems to contradict the facts for $\mathbb{C}$, and suggests that something weird is going on for non-Archimedean fields.