Asymptotic Properties of Finite Groups

Efim Zelmanov  
School of Mathematics, KIAS

This is a short survey of recent results in asymptotic group theory. We are concerned with infinite families of finite groups as their size tends to infinity. Usually these families consist of finite homomorphic images of some infinite group. That’s why the subject is all about infinite groups.

Let $G$ be a group. If there exists a family of homomorphisms $\phi_i : G \rightarrow G_i$, such that all groups $G_i$ are finite and $\bigcap \ker \phi_i = (1)$, then the group $G$ is said to be residually finite.

The family of subgroups $\ker \phi_i$ of finite index can be taken for a basis of neighborhoods of 1 which makes $G$ a topological group. If this topology is complete then we say that $G$ is a profinite group. The other way to say it is that $G$ is an inverse limit of finite groups. If the topological group $G$ is not complete then we can consider its completion $\hat{G}$ which is a profinite group.

Finally, if $G$ is not even residually finite, we consider the intersection $\bigcap \{H \triangleleft G : |G : H| < \infty\}$ of all subgroups of finite index and factor it out. The factor group $G/\bigcap \{H \triangleleft G : |G : H| < \infty\}$ is residually finite. Its completion is called the profinite completion of the group $G$. Thus we can consider the profinite completion for an arbitrary group, but only residually finite groups are embeddable in their profinite completions.

Now fix a prime number $p$. A group $G$ is said to be residually-$p$ if there exists a family of homomorphisms $\phi_i : G \rightarrow G_i$ into finite $p$-groups $G_i$, such that $\bigcap \ker \phi_i = (1)$. As above this makes $G$ a topological group. If this topology is complete then we may say that $G$ is a pro-$p$ group (in other words: an inverse limit of finite $p$-groups). For an arbitrary group $G$ factoring out this intersection of all normal subgroups of $p$-power index we make it residually-$p$. The subsequent completion gives us a pro-$p$ group $G_p$, which is called the pro-$p$ completion of $G$.

**Example 1.** Let $F_n$ be the free group on $m$ generators $x_1, \ldots, x_m$. The group $F_n$ is residually-$p$ for an arbitrary prime number $p$. The pro-$p$ completion $(F_n)_p$ is called the free pro-$p$ group. It deserves this name because an arbitrary mapping of $x_1, \ldots, x_m$ into a pro-$p$ group $G$ uniquely extends to a homomorphism $(F_n)_p \rightarrow G$.
Example 2. Let $\Lambda$ be a commutative complex local Noetherian ring with a maximal ideal $M$ such that $\Lambda / M \cong GF(p^k)$. Then the congruence subgroup $SL^1(n, \Lambda) = \{ A \in SL(n, \Lambda) \mid A = I_n \mod M \}$ is a pro-$p$ group.

**Growth of groups and representations.**

Suppose that a group $G$ is generated by a finite set $X$, $|X| < \infty$, $1 \in X = X^{-1}$.

Consider the ascending chain of finite sets

$$X^n = \{ x_1 \ldots x_n, x_i \in X \}, \quad X^1 \subseteq X^2 \subseteq \ldots, \quad \cup X^n = G, \quad |X^1| \leq |X^2| \leq \ldots$$

It is clear that $X^n$ is the ball of radius $n$ with the center at 1 in the Cayley graph of $G$. The growth of the sequence $|X^1| \leq |X^2| \leq \ldots$ is referred to as the growth of the group $G$. It may look as though it depends on the choice of the generating system $X$. In fact, it does not. For any two generating systems the growth functions $f_X(n) = |X^n|$ are asymptotically equivalent, which leads to the same type of growth.

A group is said to be of polynomial growth if there exists a polynomial $p(n)$ such that $|X^n| \leq p(n)$ for all $n$. All nilpotent groups have this property. In 1968 J. Milnor formulated two problems:

1. is it true that a group $G$ has polynomial growth if and only if $G \triangleleft H$, $|G : H| < \infty$, and $H$ is nilpotent?
2. do there exist groups of intermediate growth (i.e. groups that grow faster than any polynomial, but slower than any exponential)?

The answers to both questions were published in 1980. M. Gromov proved that, indeed, a group is of polynomial growth if and only if it is virtually nilpotent. The proof had a tremendous impact on mathematics and heralded the arrival of Geometric Group Theory.

The same year R.I. Grigorchuck constructed the first groups of intermediate growth. It was the beginning of study of self-similar (or fractal) groups, which have deep connections to many areas of mathematics.

**The strongest form of fast growth: property $\tau$.**

Let $\Gamma$ be a finite connected graph with set of vertices $V$ and set of edges $E$. For a set of vertices $W \subseteq V$ its boundary is defined as

$$\partial W = \{ v \in V \mid \dist(v, W) = 1 \}.$$
A vertex lies in $\partial W$ if it does not lie in $W$ but is connected to some element from $W$ by an edge.

The following definition is due to Pinsker.

**Definition 1.** Let $\epsilon > 0$. A finite connected graph $\Gamma$ is said to be an $\epsilon$-expander if for any subset $W \subset V$ such that $|W| < \frac{1}{2}|V|$ we have

$$|W \cup \partial W| \geq (1 + \epsilon)|W|.$$ 

Clearly, every finite connected graph becomes an $\epsilon$-expander if we choose a sufficiently small $\epsilon$. That’s why we are interested not in individual graphs but in infinite families of $K$-regular $\epsilon$-expanders $\Gamma$ with $K$ and $\epsilon$ fixed and size $|\Gamma|$ going to infinity. Such families have important applications in network design as they provide relatively sparse ($K$ is fixed!) and therefore inexpensive networks with uniformly good expansion properties ($\epsilon$ is also fixed!).

Pinsker and Erdős proved that families of random $K$-regular graphs are expander families. However, it would be nice to have an explicit construction. The first such construction was found by G. A. Margulis in 1973 and is based on Kazhdan’s property (T).

In 1967 D. Kazhdan made an observation that for some finitely generated groups $G = \langle X \rangle$, $|X| < \infty$, there exists $\epsilon > 0$ such that for any unitary representation $G \to U(H)$ without non-zero fixed points in a Hilbert space $H$, for an arbitrary element $0 \neq h \in H$ there exists a generator $x \in X$ which moves $h$ significantly:

$$||hx - xh|| \geq \epsilon \cdot ||h||$$

This property became known as Kazhdan’s property (T). The special integer groups of matrices $SL(n, \mathbb{Z})$, $n \geq 3$, have it.

G. Margulis noticed that if $G = \langle X \rangle$, $|X| < \infty$, is a residually finite group with property (T) then it provides a needed expander family. Indeed, consider a family of homomorphisms $\phi_i : G \to G_i, |G_i| < \infty, \cap_i \ker \phi_i = \langle 1 \rangle$. The generating set $X$ is mapped into a generating set $X_i$ of $G_i$. Then the family of Cayley graphs $\{Cay(G_i, X_i)\}$ is an expander family. A. Lubotzky and R. Zimmer called this property of finite homomorphic images property ($\tau$) as it is weaker than the property (T).

**Golod-Shafarevich groups**

Let $R$ be a subset of the free pro-$p$ group $(F_m)_p$, $N(R) =$ the closed normal subgroup of $(F_m)_p$ generated by $R$. We say that the factor group

$$(F_m)_p/N(R) = \langle x_1, \ldots, x_m | R = 1 \rangle$$

...
A vertex lies in if it does not lie in \( W \) but is connected to some element from \( W \) by an edge.

The following definition is due to Pinsker.

**Definition 1.** Let \( \epsilon > 0 \).

A finite connected graph is said to be an \( \epsilon \)-expander if for any subset \( W \subset V \) such that we have

\[
|W| \leq \frac{|V|}{2}
\]

Clearly, every finite connected graph becomes an \( \epsilon \)-expander if we choose a sufficiently small \( \epsilon \). That's why we are interested not in individual graphs but in infinite families of \( \epsilon \)-regular \( \epsilon \)-expanders with \( \epsilon \) and fixed and size \( |V| \) going to infinity. Such families have important applications in network design as they provide relatively sparse (\( \epsilon \) fixed!) and therefore inexpensive networks with uniformly good expansion properties (\( \epsilon \) also fixed!).

Pinsker and Erdos proved that families of random \( \epsilon \)-regular graphs are expander families. However, it would be nice to have an explicit construction. The first such construction was found by G. A. Margulis in 1973 and is based on Kazhdan's property (\( T \)).

In 1967 D. Kazhdan made an observation that for some finitely generated groups \( G = \langle X \rangle \), there exists \( \epsilon > 0 \) such that for any unitary representation \( G \to U(H) \) without non-zero fixed points in a Hilbert space \( H \), for an arbitrary element \( h \) there exists a generator which moves \( h \) significantly:

This property became known as Kazhdan's property (\( T \)). The special integer groups of matrices \( SL(n, \mathbb{Z}) \), have it.

G. Margulis noticed that if \( G = \langle X \rangle \), \( |X| < \) is a residually finite group with property (\( T \)) then it provides a needed expander family. Indeed, consider a family of homomorphisms

The generating set \( X \) is mapped into a generating set \( X_i \) of \( G_i \). Then the family of Cayley graphs \( \{Cay(G_i, X_i)\} \) is an expander family.

A. Lubotzky and R. Zimmer called this property of finite homomorphic images property (\( T \)) as it is weaker than the property (\( T \)).

**Golod-Shafarevich groups**

Let \( R \) be a subset of the free pro-\( p \) group \( \mathbb{F}_p \) generated by \( R \). We say that the factor group \( G = \langle X \rangle / R \) is presented by the set of generators \( x_1, \ldots, x_m \) and the set of relators \( R \) in the category of pro-\( p \) groups. In 1964 E. Golod and I. Shafarevich found a sufficient condition for a pro-\( p \) group presented by generators and relators to be infinite. We will formulate only a special case of this criterion, which deals with finitely presented groups.

**Theorem 2. (Golod-Shafarevich)** If \( R \) lies in the Frattini subgroup

\[
R \subseteq F^p[F, F], \quad F = (F_m)^p
\]

and \( |R| < \frac{m^2}{4} \), then \( G \) is infinite.

We say that a pro-\( p \) group is a Golod-Shafarevich (GS) group if it satisfies the assumptions of the Golod-Shafarevich theorem. A discrete group is GS if its pro-\( p \) completion is GS. In 2000 I proved that a GS pro-\( p \) group contains \( (F_m)^p \) for all \( m \). Initially GS groups were viewed just as a source of counterexamples. Later it became clear that there are better reasons to be interested in them.

**Example 1.** Let \( S \) be a finite set of primes, \( |S| = m, p \notin S \). Let \( K / \mathbb{Q} \) be the maximal pro-\( p \) extension of the field of rational numbers, which is unramified outside of \( S \). Then the Galois group \( Gal(K/\mathbb{Q}) \) has a presentation

\[
Gal(K/\mathbb{Q}) = \langle x_1, \ldots, x_m | x_i^{p^{a_i}} = [x_i, a_i], 1 \leq i \leq m \rangle
\]

(I. Shafarevich, 1970). If \( m > 4 \) then it makes \( Gal(K/\mathbb{Q}) \) a GS group.

**Example 2.** Let \( X \) be a compact hyperbolic 3-manifold, \( \Gamma = \pi_1(X) \). Then for all but finitely many primes \( p \) the group \( \Gamma \) contains a subgroup \( H \) of finite index, such that \( H \) is GS (A. Lubotzky, 1983).

**Gal(K/Q)**

Let’s talk about the example 1 above.

**Fontaine-Mazur Conjecture:** an arbitrary (continuous) homomorphism \( Gal(K/Q) \to SL^1(n, \mathbb{Q}_p) \) has finite image (here \( \mathbb{Q}_p \) is the field of \( p \)-adic numbers).

However, even a weaker version of it is open:

Is \( Gal(K/Q) \) embeddable in a pro-\( p \) group \( SL^1(n, \Lambda) \), where \( \Lambda \) is a commutative complete local Noetherian ring?

If it were embeddable the Fontaine-Mazur Conjecture would be false.
Since $\text{Gal}(K/Q)$ is a GS group (except in small cases) and all GS groups contain free pro-$p$ groups (see the theorem in the previous section) we get a link to a well known problem in Algebra:

Can a nonabelian free pro-$p$ group $(F_m)_p$, $m \geq 2$ be embedded in a group of the type $SL^1(n, \Lambda)$?

Nonlinearity of $(F_m)_p$ implies nonlinearity of $\text{Gal}(K/Q)$. A partial answer is given by the following theorem.

**Theorem 3.** For $p \gg n$ the groups $\text{Gal}(K/Q), (F_m)_p$ are not embeddable in $SL^1(n, \Lambda)$.

This result is equivalent to existence of pro-$p$ identities in $p$-adic analytic groups.

**Theorem 4.** For $p \gg n$ there exists a nonidentical element $w(x_1, \ldots, x_m) \in (F_m)_p$ with the following property: for an arbitrary commutative complete local Noetherian ring $\Lambda$, and arbitrary elements $a_1, \ldots, a_m \in SL^1(n, \Lambda)$, $w(a_1, \ldots, a_m) = 1$.

Recall that by $X$ we denote a compact hyperbolic 3-manifold, $\Gamma = \pi_1(X)$.

**Conjecture (A. Lubotzky, P. Sarnak)** $\Gamma$ does not have property $(\tau)$.

This conjecture was motivated by the longstanding conjecture on the nonvanishing of the virtual first Betti number of hyperbolic 3-manifolds.

**Virtual Positive Betti Number Conjecture (Thurston, Waldhausen):** $\Gamma$ has a subgroup $H$ of finite index, which can be epimorphically mapped onto $\mathbb{Z}$.

Indeed, property $(\tau)$ is inherited by subgroups of finite index and homomorphic images. If we believe the Virtual Positive Betti Number Conjecture above and $\Gamma$ still has property $(\tau)$ then so do $H$ and $\mathbb{Z}$. But the latter is obviously false. Hence the Lubotzky-Sarnak Conjecture follows from the Virtual Positive Betti Number Conjecture.

M. Lackenby showed that you can walk in the other direction too. He showed that the positive solution of the Lubotzky-Sarnak Conjecture with the so called “gradient Heegaard conjecture” imply that every hyperbolic 3-manifold has a finite sheeted cover which is Haken.

Since $\Gamma$ is virtually GS for almost all $p$ (see Ex. 2 above) we hoped that an arbitrary GS - group does not have property $(\tau)$. These hopes were dashed by M. Ershov who showed that the
positive part of a certain Kac-Moody group over GF(p) is GS and has property (τ).

Which groups have properties (T) and (τ)?

In 2007 M. Kassabov found generating subsets $X_i$ in symmetric groups $S_n$, such that their orders are uniformly bounded from above $|X_n| \leq N$, and the family of graphs $\{\text{Cay}(S_n, X_n)\}_n$ is an expander family. Obviously, instead of the groups $S_n$ it is sufficient to consider alternating groups $A_n$. All infinite systems of finite simple groups are closely related to each other. So Kassabov started with another infinite system: $\{\text{SL}(n, F)\}_n$, where $F$ is a fixed finite field and $n \to \infty$. Let us consider only those $n$ that are divisible by 3. Then $\text{SL}(3n, F) = \text{SL}(3, M_n(F))$, where $M_n(F)$ is the full matrix ring. Kassabov’s idea was that one has to generalize the well known result about $\text{SL}(n, \mathbb{Z})$, $n \geq 3$, having property (τ) to $\text{SL}(n, R)$ where $R$ is a noncommutative ring. Since it is not clear what $\text{SL}(n, R)$ is we will choose another construction.

Let $R$ be an arbitrary associative ring and let $e_{ij}(a)$ be an $n \times n$ matrix having the element $a \in R$ at the intersection of the $i$-th row and $j$-th column and zeros elsewhere. Let $E(n, R)$ be the group generated by all matrices

$$I_n + e_{ij}(a), \ 1 \leq i \neq j \leq n, a \in R.$$  

Kassabov proved that $E(n, R), n \geq 3$ has property (τ) with respect to all homomorphisms that factor through $R \to R/I$, $|R/I| < \infty$.

Recently, building on the work of Kassabov, Ershov and Jaikin proved that for all associative rings $R$, for all $n \geq 3$ the groups $E(n, R)$ and some of their generalizations have property (T). This enabled Ershov to show that an arbitrary GS-group has an infinite homomorphic image with property (T). In particular, a GS-group can not be amenable as conjectured by A. Vershik and P. de la Harpe.

References


E. Zelmanov, Infinite algebras and pro-p groups, in Infinite groups: geometric, combinatorial and dynamical aspects, 403-413, Progr. Math. 248, Birkhäuser, Basel, 2005

Efim Isaakovich Zelmanov is one of the most distinguished mathematicians alive and a 1994 Fields Medalist. Born in former Soviet Union, he is known for his work on combinatorial problems in nonassociative algebra and group theory, including his solution of the restricted Burnside problem in recognition of which he was awarded the Fields Medal. He obtained his doctoral degree at Novosibirsk State University in 1980. Since 2002, he has held a position as a professor at the University of California, San Diego. And, he has been a Distinguished Professor of Mathematics at Korea Institute of Advanced Study since 1996. He was elected to the American Academy of Arts and Sciences in 1996 and to The National Academy of Sciences in 2001, the world’s highest scientific honors.

Contact information: Department of Mathematics, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0112 USA, E-mail: ezelmano@math.ucsd.edu