Infinite Groups

Cornelia Druțu

University of Oxford

Part C course MT 2023, Oxford

Bernt Øksendal: "We have not succeeded in answering all our problems. The answers we have found only serve to raise a whole set of new questions. In some ways we feel we are as confused as ever, but we believe we are confused on a higher level and about more important things."

William Shakespeare: "Once more unto the breach, dear friends, once more!" (from Henry V, Act III, Scene I, spoken by King Henry, who motivates his troops at the siege of Harfleur)

Growth function

Let $G = \langle S \rangle$, S finite, $S^{-1} = S$, $1 \notin S$, dist_S the word metric.

The growth function of G with respect to S is $\mathfrak{G}_{G,S}(R) := \mathrm{card}\, \bar{B}(1, R)$.

If S, S' finite generating sets of G then $\mathfrak{G}_S \asymp \mathfrak{G}_{S'}$.

Thus, one can speak of growth function $\mathfrak{G}_G$ of a group G, well defined up to $\asymp$.

1. For each finitely generated group G, $\mathfrak{G}_G(r) \preceq 2^r$.
2. If $F_k \leq G$ then $\mathfrak{G}_G(r) \asymp 2^r$.

Theorem (Bass–Guivarc'h Theorem)

The growth function of G f.g. nilpotent satisfies

$$\mathfrak{G}_G(n) \asymp n^d \,, \text{ where } d(G) = \sum_{i=1}^{k} i m_i, m_i \text{ free rank of } C^i G / C^{i+1} G. \quad (1)$$

Milnor's Conjecture

Question (J. Milnor)

Is it true that the growth of a finitely generated group is either polynomial (i.e. $\mathfrak{G}_G(t) \preceq t^d$ for some integer d) or exponential (i.e. $\gamma_{G,S} > 1$ for every S)?

R. Grigorchuk proved that Milnor's question has a negative answer, by constructing finitely generated groups of intermediate growth, i.e. their growth is superpolynomial but subexponential.

L. Bartholdi and A. Erschler provided the first explicit computations of growth functions for groups of intermediate growth: $\forall k \in \mathbb{N}$, they constructed torsion groups G_k and torsion-free groups H_k s.t.

$$\mathfrak{G}_{G_k}(x) \asymp \exp\left(x^{1-(1-\alpha)^k}\right), \mathfrak{G}_{H_k}(x) \asymp \exp\left(\log x \cdot x^{1-(1-\alpha)^k}\right).$$

Here $\alpha \in (0,1)$ is the number satisfying $2^{3-\frac{3}{\alpha}} + 2^{2-\frac{2}{\alpha}} + 2^{1-\frac{1}{\alpha}} = 2$.

The Milnor-Wolf Theorem

For the remainder of the course we will discuss the following result.

Theorem (Milnor–Wolf theorem)

Every finitely generated solvable group is either virtually nilpotent or it has exponential growth.

It is composed of two theorems:

Theorem (Wolf's Theorem)

A polycyclic group is either virtually nilpotent or has exponential growth.

Theorem (Milnor's theorem)

A finitely generated solvable group is either polycyclic or has exponential growth.

Notation and basic result

Notation

If G is a group, a semidirect product $G \rtimes_\Phi \mathbb{Z}$ is defined by a homomorphism $\Phi : \mathbb{Z} \to \mathrm{Aut}\,(G)$. The latter homomorphism is entirely determined by $\Phi(1) = \varphi$. We set

$$S = G \rtimes_\varphi \mathbb{Z} = G \rtimes_\Phi \mathbb{Z}.$$

Theorem

The group of automorphisms of $\mathbb{Z}^n$ is isomorphic to $GL(n, \mathbb{Z})$.

Notation

A semidirect product $\mathbb{Z}^n \rtimes_\Phi \mathbb{Z}$ is entirely determined by $\Phi(1) = \varphi$, automorphism of $\mathbb{Z}^n$, so a matrix M in $GL(n, \mathbb{Z})$. We write

$$\mathbb{Z}^n \rtimes_M \mathbb{Z}.$$

A particular case of Wolf's theorem

Proposition

A semidirect product $G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$ is

1. *either virtually nilpotent (when M has all eigenvalues of absolute value 1);*
2. *or of exponential growth (when M has at least one eigenvalue of absolute value $\neq 1$).*

1. The group $G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$ is nilpotent if M has all eigenvalues equal to 1 (see Case (1) of the proof of the proposition).
2. Not true if M has all eigenvalues of absolute value 1: the group $G = \mathbb{Z} \rtimes_M \mathbb{Z}$ with $M = (-1)$ is polycyclic, virtually nilpotent but not nilpotent: it admits as a quotient D_∞. In particular, the statement (1) in the Proposition above cannot be improved to '$G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$ is nilpotent'.

Proof of the Proposition

Lemma

$\mathbb{Z}^n \rtimes_{M^k} \mathbb{Z}$ is a finite index subgroup of $\mathbb{Z}^n \rtimes_M \mathbb{Z}$.

Proof. $\mathbb{Z}^n \rtimes_{M^k} \mathbb{Z}$ is isomorphic to $\mathbb{Z}^n \rtimes_M (k\mathbb{Z})$, and the latter is a finite index subgroup of $\mathbb{Z}^n \rtimes_M \mathbb{Z}$. □

Proof of the Proposition.

Case 1. M has all eigenvalues of absolute value 1.

Case 1.a. M has all eigenvalues equal to 1. Then $\mathbb{Z} \rtimes_M \mathbb{Z}$ is nilpotent (Ex. Sheet 4).

Case 1.b. General case: apply Case 1, the above Lemma and

Theorem (L. Kronecker)

A matrix $M \in GL(n, \mathbb{Z})$ such that each eigenvalue of M has absolute value 1 has all the eigenvalues roots of unity.

Proof of the Proposition, 2

Case 2. M has an eigenvalue λ with $|\lambda| \neq 1 \Rightarrow M$ has an eigenvalue λ with $|\lambda| > 1$ ($\det M = \pm 1$) $\Rightarrow$ up to replacing G by a finite index subgroup, we may assume $|\lambda| > 2$.

Lemma

If a matrix M in $GL(n, \mathbb{Z})$ has one eigenvalue λ with $|\lambda| > 2$ then there exists a vector $\mathbf{v} \in \mathbb{Z}^n$ such that the following map is injective:

$$\begin{array}{rcl} \Phi : \bigoplus_{k \in \mathbb{Z}_+} \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}^n \\ \Phi : (s_k)_k & \mapsto & s_0 v + s_1 M\mathbf{v} + \ldots + s_k M^k \mathbf{v} + \ldots . \end{array} \tag{2}$$

Proof of the Lemma

Proof. M defines an automorphism $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$, $\varphi(\mathbf{v}) = M\mathbf{v}$.
The dual map φ^* has the matrix M^T in the dual canonical basis. Hence it also has the eigenvalue λ, hence there exists a linear form $f : \mathbb{C}^n \to \mathbb{C}$ such that $\varphi^*(f) = f \circ \varphi = \lambda f$.

Take $\mathbf{v} \in \mathbb{Z}^n \setminus \ker f$. Assume Φ is not injective: $\exists (t_n)_n$, $t_n \in \{-1, 0, 1\}$, such that

$$t_0\mathbf{v} + t_1 M\mathbf{v} + \ldots + t_n M^n\mathbf{v} + \ldots = 0.$$

Let N be the largest integer such that $t_N \neq 0$. Then

$$M^N\mathbf{v} = r_0\mathbf{v} + r_1 M\mathbf{v} + \ldots + r_{N-1} M^{N-1}\mathbf{v}$$

where $r_i \in \{-1, 0, 1\}$. By applying f to the equality we obtain

$$\left(r_0 + r_1\lambda + \cdots + r_{N-1}\lambda^{N-1}\right) f(\mathbf{v}) = \lambda^N f(\mathbf{v}),$$

whence $|\lambda|^N \leqslant \sum_{i=0}^{N-1} |\lambda|^i = \frac{|\lambda|^N - 1}{|\lambda| - 1} \leqslant |\lambda|^N - 1$, a contradiction. $\square$

Proof of the Proposition 2

Take $v \in \mathbb{Z}^n$ such that distinct elements $s = (s_k) \in \bigoplus_{k \geqslant 0} \mathbb{Z}_2$ define distinct vectors in $\mathbb{Z}^n$,

$$s_0 v + s_1 M v + \ldots + s_k M^k v + \ldots$$

With the multiplicative notation for the binary operation in $G = \mathbb{Z}^n \rtimes_M \mathbb{Z}$, and $\mathbb{Z} = \langle t \rangle$, the above vectors correspond to distinct elements

$$g_s = v^{s_0} (t v t^{-1})^{s_1} \cdots (t^k v t^{-k})^{s_k} \cdots \in G.$$

Consider the set Σ_K of sequences $s = (s_k)$ for which $s_k = 0\,, \forall k \geqslant K+1$. The map

$$\Sigma_K \to G, \quad s \mapsto g_s$$

is injective and its image consists of 2^{K+1} distinct elements g_s. Assume that the generating set of G contains the elements t and v. With respect to this generating set, the word-length $|g_s|$ is at most $3K+1$ for every $s \in \Sigma_K$. Thus, for every K we obtain 2^{K+1} distinct elements of G of length at most $3K+1$, whence G has exponential growth. □

Generalization

The main ingredient in the proof of Wolf's Theorem is the following generalization of the Proposition.

Proposition

Let G be a finitely generated nilpotent group and let $\varphi \in Aut(G)$. Then the polycyclic group $P = G \rtimes_{\varphi} \mathbb{Z}$ is

1. *either virtually nilpotent;*
2. *or has exponential growth.*

Proof.

See Ex. Sheet 4. □