Infinite Groups

Cornelia Druțu

University of Oxford

Part C course MT 2024, Oxford

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 $\neq 1$).*

Proof.

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 $|\lambda| > 2$.

Key Lemma

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:

$$\begin{array}{rcl} \Phi : \bigoplus_{k\in\mathbb{Z}_+} \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}^n \\ \Phi : (s_k)_k & \mapsto & s_0 v + s_1 M\mathbf{v} + \ldots + s_k M^k \mathbf{v} + \ldots . \end{array} \tag{1}$$

Proof of the Proposition

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

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

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 t and v. The word-length $|g_s|$ is at most $2K+1$, $\forall s \in \Sigma_K$. Thus, for every K we obtain 2^{K+1} distinct elements of G of length at most $2K+1$, 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. □

The general Wolf Theorem

Theorem (Wolf's Theorem)

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

Proof. It suffices to prove the statement for poly-C_∞ groups.

Let G be poly-C_∞, consider a subnormal descending series of minimal (Hirsch) length

$$G = N_0 \geqslant N_1 \geqslant \ldots \geqslant N_n \geqslant N_{n+1} = \{1\}$$

such that $N_i/N_{i+1} \simeq \mathbb{Z}$ for every $i \geqslant 0$.

We argue by induction on n. For $n = 0$, $G \simeq \mathbb{Z}$. Assume statement true for n, consider the case of $n+1$. The subgroup $N_1 \leqslant G$ is either virtually nilpotent or has exponential growth. In the second case the group G has exponential growth.

Proof of Wolf's Theorem, continued

Assume that N_1 is virtually nilpotent.

$G \simeq N_1 \rtimes_\theta \mathbb{Z}$, corresponding to $\Psi : \mathbb{Z} \to \mathrm{Aut}\,(N_1)$, $\theta = \Psi(1)$.
N_1 contains a nilpotent subgroup H of finite index.

N_1 f.g. $\Rightarrow$ we may assume that H is characteristic in N_1 $\Rightarrow$ H invariant under the automorphisms in $\Psi(\mathbb{Z})$.

Therefore, $H \rtimes_\theta \mathbb{Z}$ is a normal subgroup of G.

We retain the notation θ for the restriction $\theta|_H$. $H \rtimes_\theta \mathbb{Z}$ has finite index in G, since $G/(H \rtimes_\theta \mathbb{Z})$ is a quotient of N_1/H.

By the previous Proposition, $H \rtimes_\theta \mathbb{Z}$ is either virtually nilpotent or of exponential growth $\Rightarrow$ the same alternative for $N_1 \rtimes_\theta \mathbb{Z} = G$. $\square$

Milnor's theorem

Theorem (J. Milnor)

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

Lemma

If a finitely generated group G has sub-exponential growth then for all $\beta_1, \ldots, \beta_m, g \in G$, the set of conjugates

$$\{g^k \beta_i g^{-k} \mid k \in \mathbb{Z}, i = 1, \ldots, m\}$$

generates a finitely generated subgroup $N \leqslant G$.

Proof.

Exercise on Ex. Sheet 4. □

Proof of Milnor's theorem

Proof. By induction on the derived length d of G.
$d = 1$: G f. g. abelian, statement immediate.
Assume alternative true for f. g. solvable groups of derived length $\leqslant d$. Let G of derived length $d + 1$.

$H = G/G^{(d)}$ is f. g. solvable of derived length $d \Rightarrow$ (inductive assumption) either H has exponential growth or H polycyclic.

H has exponential growth $\Rightarrow$ G has exponential growth.

Assume H is polycyclic. Milnor's Theorem will follow from:

Lemma

Let G f.g. and a short exact sequence

$$1 \to A \to G \xrightarrow{\pi} H \to 1\,, \quad \textit{with } A \textit{ abelian and } H \textit{ polycyclic.} \tag{2}$$

Then G is either polycyclic or has exponential growth.

Proof of the final lemma

Proof. Assume G has sub-exponential growth. We will prove that G is polycyclic. The group G is polycyclic iff A is finitely generated.
Since H is polycyclic, it is finitely presented. This allows us to begin by proving that A is normally generated by a finite set.
An older set of ideas: We had proven that finite presentability is independent of the generating set.

Proposition

Assume $G = \langle S \mid R \rangle$ finite presentation, and $G = \langle X \mid T \rangle$ is such that X is finite. Then $\exists$ finite subset $T_0 \subset T$ such that $G = \langle X \mid T_0 \rangle$.

This can be reformulated as follows: If G is finitely presented, X is finite and

$$1 \to N \to F(X) \to G \to 1$$

is a short exact sequence, then N is normally generated by finitely many elements $n_1, \ldots, n_k$.

Generalization of 'independence of finite presentability from the generating set'

This can be generalized to an arbitrary short exact sequence:

Lemma

Consider a short exact sequence

$$1 \to N \to K \xrightarrow{\pi} G \to 1\,, \quad \textit{with } K \textit{ finitely generated.} \tag{3}$$

If G is finitely presented, then N is normally generated by finitely many elements $n_1, \ldots, n_k \in N$.

Proof Let S be a finite generating set of $K \Rightarrow \overline{S} = \pi(S)$ finite generating set for G. G finitely presented $\Rightarrow \exists$ words $r_1, \ldots, r_k$ in S s. t.

$$\langle \overline{S} \mid r_1(\overline{S}), \ldots, r_k(\overline{S}) \rangle$$

is a presentation of G.

Proof of generalization of 'independence of finite presentability from the generating set'

Define $n_j = r_j(S)$, an element of N by the assumption. We prove that the finite set $\{n_1, \ldots, n_k\}$ normally generates N.
Let n be an arbitrary element in N and $w(S)$ a word in S such that $n = w(S)$ in K. Then $w(\overline{S}) = \pi(n) = 1$, whence in $F(S)$ the word $w(S)$ is a product of finitely many conjugates of $r_1, \ldots, r_k$. When projecting such a relation *via* $F(S) \to K$ we obtain that n is a product of finitely many conjugates of $n_1, \ldots, n_k$. □

Back to our final Lemma: we have a short exact sequence

$$1 \to A \to G \xrightarrow{\pi} H \to 1\,, \quad \text{with } A \text{ abelian, } G \text{ fin. gen., } H \text{ polycyclic.} \quad (4)$$

We assume G has sub-exponential growth, and deduce that G is polycyclic by proving that A is finitely generated.
H is polycyclic, hence finitely presented. Hence there exist finitely many elements $a_1, \ldots, a_k$ in A such that every element in A is a product of G-conjugates of $a_1, \ldots, a_k$.

H is polycyclic $\Rightarrow$ it has the bounded generation property: there exist finitely many elements $h_1, \ldots, h_q$ in H such that every element $h \in H$ can be written as

$$h = h_1^{m_1} h_2^{m_2} \cdots h_q^{m_q}, \text{ with } m_1, m_2, \ldots, m_q \in \mathbb{Z}.$$

Choose $g_i \in G$ such that $\pi(g_i) = h_i$ for every $i \in \{1, 2, \ldots, q\}$. Then every element $g \in G$ can be written as

$$g = g_1^{m_1} g_2^{m_2} \cdots g_q^{m_q} a, \text{ with } m_1, m_2, \ldots, m_q \in \mathbb{Z} \text{ and } a \in A. \quad (5)$$

We have that $A = \langle\langle a_1, \ldots, a_k \rangle\rangle$, and all the conjugates of a_j are of the form

$$g_1^{m_1} g_2^{m_2} \cdots g_q^{m_q} a_j \left(g_1^{m_1} g_2^{m_2} \cdots g_q^{m_q} \right)^{-1}. \quad (6)$$

The subgroup A_q generated by the conjugates $g_q^m a_j g_q^{-m}$ with $m \in \mathbb{Z}$ and $j \in \{1, \ldots, k\}$ is finitely generated. Let S_q be its finite generating set.

Proof of final Lemma, continued

The conjugates $g_{q-1}^n g_q^m a_j g_q^{-m} g_{q-1}^{-n}$ with $m, n \in \mathbb{Z}$ and $j \in \{1, \dots, k\}$ are in the subgroup A_{q-1} of A generated by $g_{q-1}^n s g_{q-1}^{-n}$ with $n \in \mathbb{Z}$ and $s \in S_q$. The subgroup A_{q-1} is finitely generated. Continuing inductively, we conclude that the group A is finitely generated. Hence G is polycyclic. □

This also concludes the proof of Milnor's Theorem. □

By combining the theorems of Milnor and Wolf we obtain:

Theorem

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

Milnor's conjecture is true for linear groups.

Theorem (The Alternative Theorem of Jacques Tits)

Let F be a field of zero characteristic and let G be a f. g. subgroup of $GL(n, F)$. Then either G is virtually nilpotent or it has exponential growth.

In fact, what J. Tits proved is that G as above is either virtually solvable or it contains a free non-abelian subgroup.

This combined with Milnor-Wolf yields the result.

Milnor formulated a second conjecture: is a group with polynomial growth virtually nilpotent?

Theorem (Gromov's Polynomial Growth Theorem)

Every finitely generated group of growth at most polynomial is virtually nilpotent.

This is a typical example of an algebraic property that may be recognized *via* a, seemingly, weak geometric information.

Gromov's proof uses the Alternative Theorem.

Later, Y. Shalom and T. Tao proved the following effective version of Gromov's Theorem:

Theorem (Shalom–Tao Effective Polynomial Growth Theorem)

There exists a constant C such that for any finitely generated group G and $d > 0$, if for some $R \geqslant \exp\left(\exp\left(Cd^C\right)\right)$, the ball of radius R in G has at most R^d elements, then G has a finite index nilpotent subgroup of class less than C^d.

The following questions related to growth remain open.

Question

What is the set Growth(groups) of the equivalence classes of growth functions of finitely generated groups?

Question

Does there exist a finitely presented group of intermediate growth (that is, subexponential and superpolynomial) ?

Question

What are the equivalence classes of growth functions for finitely presented groups?

Clearly, $Growth(f.p.groups) \subset Growth(groups)$.
This inclusion is proper since R. Grigorchuk proved that there exist uncountably many nonequivalent growth functions of finitely generated groups, while there are only countably many finitely presented groups, up to isomorphism.

Theorem (Grigorchuk's Subexponential Growth theorem)

Let $f(n)$ be an arbitrary sub-exponential function larger than $2^{\sqrt{n}}$. Then there exists a finitely generated group G with subexponential growth function $\mathfrak{G}(n)$ such that:

$$f(n) \leqslant \mathfrak{G}(n)$$

for infinitely many $n \in \mathbb{N}$.

Question (R. Grigorchuk)

Is it true that if the growth of a finitely generated group is below $e^{\sqrt{n}}$ then it is polynomial?