Hall polynomials for finitely generated torsion-free nilpotent groups ($\mathcal{T}$-groups)

Alexander Cant (joint with Bettina Eick)

Dehn (1911) published the following well known problems for finitely presented groups:

The word problem: Given a word in the generators of a finitely presented group, how can we decide if it's the identity element of the group?
The conjugacy problem: Given two elements of a finitely presented group, how can we decide if they are conjugate?
The isomorphism problem: Given two finitely presented groups, how can we decide if they are isomorphic?

These problems are known to be undecidable in general. We examine the word and the isomorphism problem in $\mathcal{T}$-groups.

Presentations and the word problem for $\mathcal{T}$-groups

Every $\mathcal{T}$-group G has a presentation of the form

$$G(t) \;=\; \langle g_1,\dots,g_n \mid g_j g_i = g_i g_j g_{j+1}^{t_{i,j,j+1}} \cdots g_n^{t_{i,j,n}} \text{ for } 1 \leqslant i < j \leqslant n \rangle,$$

where $t = (t_{i,j,k}) \in \mathbb{Z}^{\binom{n}{3}}$. The number n is known as the Hirsch length of G. For each $h \in G$ there is a unique $e = (e_1,\dots,e_n) \in \mathbb{Z}^n$ with

$$h \;=\; g^e \;:=\; g_1^{e_1} \cdots g_n^{e_n}.$$

This is called the normal form of h. The relations can be used to compute the normal form of any element and we can thus solve the word problem in $\mathcal{T}$-groups.

Examples of $\mathcal{T}$-groups

Basic examples are the free abelian groups $(\mathbb{Z}^n,+)$. More generally, $\mathcal{T}$-groups are up to isomorphism precisely the subgroups of the unitriangular matrix groups $U_s(\mathbb{Z})$. That are the groups of upper triangular matrices in $GL_s(\mathbb{Z})$ with 1's on their diagonals.

Hall polynomials

Since each element of a given $\mathcal{T}$-group $G(t)$ has a unique normal form, it is possible to express the multiplication and powering in $G(t)$ by functions m_i and p_i defined via

$$g^x \cdot g^y \;=\; g_1^{m_1(x,y)} \cdots g_n^{m_n(x,y)} \quad \text{and} \quad (g^x)^z \;=\; g_1^{p_1(x,z)} \cdots g_n^{p_n(x,z)}.$$

Theorem (Hall, 1957): m_i and p_i can be described by rational polynomials in x, y, z.

Examples of Hall polynomials

A $\mathcal{T}$-group of Hirsch length 1 or 2 is free abelian. Hence the Hall polynomials are

$$m_i(x,y) \;=\; x_i + y_i \quad \text{resp.} \quad p_i(x,z) \;=\; x_i z.$$

The Hall polynomials at g_1 and g_2 have this form in all $\mathcal{T}$-groups.
The remaining polynomials for Hirsch length 3 are

$$m_3(x,y) \;=\; x_3 + y_3 + t_{1,2,3}\, x_2 y_1 \quad \text{and} \quad p_3(x,z) \;=\; x_3 z + \tfrac{(z-1)z}{2} t_{1,2,3}\, x_1 x_2.$$

Result: An algorithm for the computation of Hall polynomials

We consider t as a set of indeterminates and compute parametrised Hall polynomials by induction on the Hirsch length. If $G(t)$ has Hirsch length n, the group $G(t)/\langle g_n\rangle$ has Hirsch length $n-1$. Hence it suffices to compute $m_n(x,y)$ and $p_n(x,z)$.

Step 1: Compute conjugation polynomials $r_{i,j,k}(a,b)$ so that for any $a, b \in \mathbb{Z}$

$$(g_j^a)^{g_i^b} \;=\; g_i^{-b} g_j^a g_i^b \;=\; g_j^a g_{j+1}^{r_{i,j,j+1}(a,b)} \cdots g_n^{r_{i,j,n}(a,b)}$$

holds. Use induction and the defining relations of $G(t)$ to compute the normal form of

$$g_2^{g_1^{b+1}} \;=\; (g_2^{g_1^b})^{g_1} \;=\; g_2^{g_1} (g_3^{g_1})^{r_{1,2,3}(1,b)} \cdots (g_n^{g_1})^{r_{1,2,n}(1,b)}.$$

This yields a recurrence relation which can be used to compute $r_{1,2,n}(1,b)$.
The polynomial $r_{1,2,n}(a,b)$ can be deduced using induction.

Step 2: Compute $m_n(x,y)$ by determining the normal form of right hand side of

$$g_1^{x_1} \cdots g_n^{x_n} \cdot g_1^{y_1} \cdots g_n^{y_n} \;=\; g_1^{x_1+y_1} (g_2^{x_1})^{g_1^{y_1}} \cdots (g_n^{x_n})^{g_1^{y_1}} \cdot g_2^{y_2} \cdots g_n^{y_n}.$$

This can be done using the conjugation polynomials and induction.

Step 3: The normal form of the right hand side of

$$(g_1^{x_1} \cdots g_n^{x_n})^{z+1} \;=\; (g_1^{p_1(x,z)} \cdots g_{n-1}^{p_{n-1}(x,z)}) \cdot (g_1^{x_1} \cdots g_n^{x_n}) \cdot g_n^{p_n(x,z)}$$

can be computed using the multiplication polynomials of $G(t)$ and induction.
Finally we can compute $p_n(x,z)$ by solving another recurrence relation.

Application 1: Efficient solution to the word problem

We can use the Hall polynomials to solve the word problem in a given $\mathcal{T}$-group. Evaluating polynomials is more efficient than using the relations to obtain the normal form.

Application 2: Faithful representations for $\mathcal{T}$-groups

Let G be a $\mathcal{T}$-group. A faithful representation of G is an embedding $G \to U_s(\mathbb{Z})$. Nickel (2006) presented an algorithm that takes the multiplication polynomials of G and computes a faithful representation for G.

References

- M. Dehn: Über unendliche diskontinuierliche Gruppen. Math. Ann. **71**(1), 1911.
- P. Hall: The Edmonton notes on nilpotent groups. QMC Math. Notes, 1969.
- W. Nickel: Matrix representations for torsion-free nilpotent groups by Deep Thought. J. Algebra **300**, 2006.
- B. Eick and A.-K. Engel: The isomorphism problem for torsion free nilpotent groups of Hirsch length at most 5. Groups Complex. Cryptol. **9**, 2017.
- A. Cant and B. Eick: Polynomials describing the multiplication in finitely generated torsion-free nilpotent groups. J. Symb. Comp. **92**, 2019.

Application 3: The isomorphism problem

Let G be a $\mathcal{T}$-group of class c with lower central series $\gamma_1(G) > \ldots > \gamma_{c+1}(G)$. Consider the groups $I_i(G)$, where $I_i(G)/\gamma_i(G)$ is the torsion subgroup of $G/\gamma_i(G)$. Then $I_i(G)/I_{i+1}(G)$ is free abelian, say of rank d_i. $(d_1,\dots,d_c)$ is called the type of G.
Let $G(s) = \langle g_1,\dots,g_n\rangle$ and $G(t) = \langle h_1,\dots,h_n\rangle$ be $\mathcal{T}$-groups of the same type.
Any homomorphism $\varphi\colon G(s) \to G(t)$ is fully determined by $\varphi(g_1),\dots,\varphi(g_n)$, where $\varphi(g_i) = h_1^{m_{i1}} \cdots h_n^{m_{in}}$ with $m_{ij} \in \mathbb{Z}$. Thus φ corresponds to an $n \times n$ integral matrix.
We can choose presentations for $G(s)$ and $G(t)$ so that

$$(m_{ij})_{1\leqslant i,j\leqslant n} \;=\; \begin{pmatrix} M_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & M_c \end{pmatrix}$$

is in upper block triangular form. It follows that φ is an isomorphism if and only if all M_i are invertible and $\varphi(g_1),\dots,\varphi(g_n)$ satisfy the relations of $G(s)$.

(1) Use Hall polynomials to evaluate the relations of $G(s)$ in $\varphi(g_1),\dots,\varphi(g_n)$. Comparison of the exponents yields polynomial equations for m_{ij}.

(2) The condition that $M_1,\dots,M_c$ have to be invertible translates to further polynomial equations.

Now $G(s) \cong G(t)$ if and only if all polynomials from (1) and (2) have a common integral root (m_{ij}).
We can use this method to reduce the classification of $\mathcal{T}$-groups of a certain type to the investigation of some polynomial equations.

Technische Universität Braunschweig

Institut für Analysis und Algebra
Arbeitsgruppe Algebra