Classifying finite 2-nilpotent p-groups, Lie algebras and graphs : equivalent and wild problems

Ruvim Lipyanski and Natalia Vanetik

Ben-Gurion University

International Conference on Algebras and Lattices

Prague, 2010

Featured results

Outline

1. We reduce the graph isomorphism problem to 2-nilpotent p-groups isomorphism problem and to 2-nilpotent Lie algebras over the ring $\mathbb{Z}/p^3\mathbb{Z}$.
2. We show that isomorphism problems in categories of graphs, finite 2-nilpotent p-groups, and 2-nilpotent Lie algebras over $\mathbb{Z}/p^3\mathbb{Z}$ are **polynomially equivalent**.
3. We show that classifying problems in categories graphs, finite 2-nilpotent p-groups, and 2-nilpotent Lie algebras are **wild**.

Groups on graphs

Graph isomorphism $\Rightarrow$ other isomorphisms

Kim and Roush '80, Kayal and Saxena '05:
Reducing graph isomorphism to isomorphism of rings and algebras in polynomial time.

Graph isomorphism $\Rightarrow$ infinite group isomorphism

C. Droms '87:

- For a graph $\Gamma = (V, E)$, group $G(\Gamma)$ is generated by vertices V with relations $x_i \cdot x_j = x_j \cdot x_i$ for every pair of adjacent vertices x_i and x_j of graph Γ.
- $G(\Gamma_1)$ and $G(\Gamma_2)$ are isomorphic if and only if the graphs Γ_1 and Γ_2 are isomorphic.

Graphs and finite groups isomorphism

Polynomial equivalence: an outline

- Graph isomorphism is reduced to isomorphism of 2-nilpotent Lie algebras over the ring $\mathbb{Z}/p^3\mathbb{Z}$.
- Isomorphism of 2-nilpotent Lie algebras over $\mathbb{Z}/p^3\mathbb{Z}$ is reduced to isomorphism of 2-nilpotent finite p-groups.
- Isomorphism of finite groups is reduced back to graphs.
- **Result**
  Problems of distinguishing graphs, finite 2-nilpotent *p*-groups and nilpotent of class 2 Lie algebras over the ring $\mathbb{Z}/p^3\mathbb{Z}$ up to isomorphism are polynomially equivalent.

Lie algebra of a graph (1)

Variables

Let $\Gamma = (V, E)$ be an undirected loopless graph with the vertex set $V = \{v_1, ..., v_n\}$ and the edge set E, where $|V| = n$ and $|E| = m$. We introduce following variables:

- $v_1, ..., v_n$
- $S = \{k = (i, j),\ \overline{k} = (j, i) \text{ where } 1 \leq i < j \leq n\}$ - a set of $l = n(n-1)$ variables indexed by k and $\overline{k}$.

Free Lie algebra

Let p be an odd prime. We construct a **free Lie algebra**

$$F = \mathbb{Z}/p^3\mathbb{Z}(\overrightarrow{v_i}, \overrightarrow{a_k}, \overrightarrow{a_{\overline{k}}})$$

Lie algebra of a graph (2)

Lie algebra of a graph

A 2-*step nilpotent Lie algebra* $L(\Gamma)$ corresponding to the graph Γ is defined as $L(\Gamma) := {}^{F}/_{I}$ where ideal I has following relations:

1. for all $1 \leq i < j \leq n$, $[v_i, v_j] = a_k - a_{\overline{k}}$ where $k = (i, j)$ and $\overline{k} = (j, i)$,
2. $[v_i, a_s] = [a_s, v_i] = [a_s, a_r] = 0$ for all $1 \leq i \leq n$ and $s, r \in S$,
3. for all $1 \leq i < j \leq n$, if $k = (i, j)$ and $\{v_i, v_j\} \in E$ then $pa_k = pa_{\overline{k}} = 0$, otherwise $p^2 a_k = p^2 a_{\overline{k}} = 0$.

Main theorem

For every two undirected simple graphs Γ_1 and Γ_2 it holds that

$$L(\Gamma_1) \approx L(\Gamma_2) \Longleftrightarrow \Gamma_1 \approx \Gamma_2$$

Lie algebra of a graph (3)

Let G be a Lie n-step nilpotent algebra over a ring K. A **universal enveloping n-nilpotent algebra** of G is a pair $(U'(G), i)$ composed of a n-nilpotent associative algebra $U'(G)$ together with the map i satisfying the following conditions:

1. i is a Lie algebra homomorphism from G into Lie algebra $U'(G)_L$.
2. Given any associative n-nilpotent algebra A and any Lie algebra homomorphism $f : G \to A_L$, there exists a unique algebra homomorphism $f' : U' \to A$ such that the following diagram commutes:

$$\begin{array}{ccccc} U'(G)_L = U'(G) & \longrightarrow & A = A_L \\ \uparrow & \nearrow & \\ G & & \end{array}$$

Lie algebra of a graph (4)

PBW theorem for nilpotent Lie algebras

If G is n-step nilpotent algebra over K and, in addition, it is a free K-module, then G admits an universal enveloping n-nilpotent algebra $(U'(G), i)$ and i is an isomorphism.

A sketch of the proof of the Main theorem

Let $L = L(\Gamma)$ be a 2-step nilpotent Lie algebra associated with graph Γ. Let C be an ideal of $U'(L)$ generated by

$$v_1^2, ..., v_n^2, a_1, ..., a_l$$

Let $U''(L) = {}^{U'(L)}/_{C}$ be a quotient algebra of $U'(L)$ modulo C. The elements $v_i v_j, v_i, a_k, a_{\overline{k}}$, where $1 \leq i < j \leq n$ and $k, \overline{k} \in S$, **form a basis** of $U''(L)$ over ${}^{\mathbb{Z}}/_{p^3\mathbb{Z}}$.

Proof steps (2)

Let Γ_1 and Γ_2 be two graphs and L_1, L_2 be the two algebras associated with them. Suppose that $\phi : L_1 \to L_2$ is an isomorphism of Lie algebras. Then ϕ can be extended to an isomorphism $\phi'' : U''(L_1) \to U''(L_2)$ of 2-nilpotent associative algebras (PBW-argument). Let

$$\phi'(v_1) = c_{11}v_1' + ... + c_{1n}v_n' + (\text{l.c. of } a_i'\text{'s})$$

where $c_{1k} \in \mathbb{Z}/p^3\mathbb{Z}$ for all k. Since $\phi'(v_1^2) = 0$, we get

$$\sum_{1 \le i < j \le n} (2c_{1i}c_{1j}v_i'v_j' + c_{1i}c_{1j}(a_{ij}' - a_{ji}')) = 0$$

An analysis shows that exactly one of the c_{1i} is a unit, say c_{1i_0}. We can define a mapping $\pi : [1n] \to [1n]$ with $\pi(1) = i_0$. Thereby we may construct a permutation π on $[1n]$ so that $\pi : \Gamma_1 \to \Gamma_2$ is an isomorphism.

Finite 2-nilpotent group of a graph

Construction

- Let us observe 2-nilpotent Lie algebra $L = L(\Gamma)$ of graph Γ as $\mathbb{Z}/p^3\mathbb{Z}$-module and its submodule $V^0 = \bigoplus_{i=1}^{n}(\mathbb{Z}/p^3\mathbb{Z})v_i$ with an additive basis $B =< b_1, ..., b_n >$.
- $V^0 = Span_{\mathbb{Z}/p^3\mathbb{Z}} < b_1, ..., b_n >$.
- Denote by Z the center of $L(\Gamma)$.
- $G_n = \{g_1, ..., g_n\}$ denotes a set of n elements and $\chi : B \rightarrow G_n$ is a bijection.
- $G = G(\Gamma)$ denotes *the set of all formal expressions* of the form

$$G := \{g_1^{\alpha_1}...g_n^{\alpha_n}a_k \mid a_k \in Z, g_i \in G_n,\ 0 \leq \alpha_i \leq p^3 - 1\},$$

where $g_i = \chi(b_i)$ for $i \in [1, ..., n]$.

Multiplication in $G(\Gamma)$

We use the multiplicative notation $b_i^{\alpha_i} \cdot b_j^{\alpha_j}$ instead of the additive notation $\alpha_i b_i + \alpha_j b_j$ for the module operation on $L(\Gamma)$).

$$g_1^{\alpha_1} \dots g_n^{\alpha_n} a g_1^{\beta_1} \dots g_n^{\beta_n} b = g_1^{\overline{\alpha_1+\beta_1}} \dots g_n^{\overline{\alpha_n+\beta_n}} \cdot a \cdot$$
$$\cdot\, b \cdot \varphi(b_2^{\alpha_2} \dots b_n^{\alpha_n}, b_1^{\beta_1}) \varphi(b_3^{\alpha_3} \dots b_n^{\alpha_n}, b_2^{\beta_2}) \dots \varphi(b_n^{\alpha_n}, b_{n-1}^{\beta_{n-1}}),$$

where $\varphi(b_i, b_j) = b_i \times b_j$ is the multiplication on R^0 and $\overline{\alpha_i + \beta_i} = \alpha_i + \beta_i \bmod p^3$.

Example

For complete graph K_n and one lacking an edge $K_n - e$ groups $G(K_n)$ and $G(K_n - e)$ are generated by centers of different size.

Theorem (L. and V.)

$G(\Gamma)$ is a p-group of exponent p^3.

Proof. In the algebra $L(\Gamma))$ elements v_i have order p^3, elements a_i corresponding to the edges of Γ have order p and elements corresponding to the non-edges of Γ - order p^2.
Now assume that for $x, y \in G$ the condition $x^{p^3} = y^{p^3} = 1$ is fulfilled. Then:

$$(xy)^{p^3} = x^2y^2xy...xy[y,x] = x^{p^3}y^{p^3}[y,x][y^2,x]...[y^{p^3-1},x]$$
$$= [y,x]^{1+2+...+(p^3-1)} = [y,x]^{\frac{(p^3-1)p^3}{2}} = 1.$$

□

The main theorem

Theorem (L. and V.)

Let $L(\Gamma_1)$ and $L(\Gamma_2)$ be two 2-nilpotent Lie algebras and $G(\Gamma_1)$ and $G(\Gamma_2)$ two groups corresponding to them. Then

$$L(\Gamma_1) \approx L(\Gamma_2) \iff G(\Gamma_1) \approx G(\Gamma_2)$$

Graphs on finite groups (1)

Finite group

Finite group G on n elements $V = \{v_1, ..., v_n\}$ with binary operation $\cdot$ is assumed to be defined by specifying mapping $\mu : V \times V \rightarrow V$.

Hypergraph

Hypergraph $H(G)$ corresponding to finite group G has nodes V and directed hyperedges $(v, u, \mu(v, u))$ for all $v, u \in V$.

Graphs on finite groups (2)

Directed colored graph

Graph $\Gamma(G)$ corresponding to a hypergraph $H(G)$ has nodes $V \cup (V \times V \times V)$. Every directed hyperedge $(v, u, \mu(v, u))$ of color is represented by three colored directed edges of $\Gamma(G)$:

1. edge $(v, (v, u, \mu(v, u)))$ of color 1,
2. edge $(u, (v, u, \mu(v, u)))$ of color 2,
3. edge $(\mu(v, u), (v, u, \mu(v, u)))$ of color 3.

$\Gamma(G)$ has $n^3 + n$ nodes and $3n^2$ edges of 3 colors.

Note

Isomorphism problems for colored graphs, directed graphs, undirected graphs, simple graphs, multigraphs and every combination of the above are polynomially equivalent.

Graphs on other algebraic structures

Note

Similar graph construction can be done for other finite algebraic structures.

Example

Graphs on finite semigroups Graph $\Gamma(S)$ of finite semigroup S of order n also has $n^3 + n$ nodes and $3n^2$ edges. Edges of $\Gamma(S)$ have 3 colors.

Example

Graphs on finite rings Graph $\Gamma(R)$ of finite ring R of order n has $n^3 + n$ nodes and $6n^2$ edges. Edges of $\Gamma(R)$ have 6 colors.

Klein group and a part of the corresponding graph

Preserving isomorphisms and homomorphisms

Isomorphisms

Theorem

Let G_1 and G_2 be two finite groups. Then $G_1 \approx G_2$ if and only if $\Gamma(G_1) \approx \Gamma(G_2)$.

Homomorphisms

Theorem

Let G_1 and G_2 be two finite groups. Then for each homomorphism $\phi : G_1 \longrightarrow G_2$ there exists a homomorphism $\phi' : \Gamma(G_1) \longrightarrow \Gamma(G_2)$

Wildness

Definition

A **pair of matrices** matrix problem $\mathcal{W}$ is the problem of classifying pairs of square matrices over a field up to simultaneous similarity. A classification problem is called **wild** if it contains $\mathcal{W}$, and **tame** otherwise.

Theorem (V. Sergeichuk '75)

Let G be a 2-nilpotent finite p-group which is an extension of an abelian group A by an abelian group B:

$$1 \to A \to G \to B \to 1.$$

Problem of classifying of such groups G with group A of the order p is tame. However, if the order of A is more than p, the above problem is wild.

Our results (1)

Theorem (L. and V.)

The problems of classification of graphs, finite 2-nilpotent Lie algebras over $\mathbb{Z}/p^3\mathbb{Z}$ and finite 2-nilpotent groups up to isomorphism are wild.

Assumptions for complexity estimates

- finite associative graph algebras are given by specifying the product of its basis elements over $\mathbb{Z}/p^3\mathbb{Z}$;
- finite graph groups are given by systems of generators and defining relations;
- graphs are given by their adjacency matrices.

Our results (2)

Theorem (L. and V.)

The problems of classification of graphs, finite 2-nilpotent Lie algebras over $\mathbb{Z}/p^3\mathbb{Z}$ and finite 2-nilpotent groups up to isomorphism are polynomially equivalent.

Complexity

Let G be a group of order n. Size of $\Gamma(G)$ is $O(n^3)$.
The size of a basis of the Lie algebra $L(\Gamma)$ is $O(|\Gamma|^2)$.
Therefore

$$\Gamma\mathbf{I} \leq^P_T \mathbf{LI} \leq^P_T \mathbf{GI} \leq^P_T \Gamma\mathbf{I}$$

where Γ**I**, **LI**, and **GI** denote the isomorphism problems for graphs, 2-nilpotent Lie algebras over $\mathbb{Z}/p^3\mathbb{Z}$ of graphs, and 2-nilpotent p-groups of graphs.

Thank you!

Questions?