Elimination Theory II: Elimnation Proceses

Alexei Miasnikov

Alagna
December 15, 2008

Diophantine problems in a groups

The Diophantine problem in a given algebraic structure G:

Is there an algorithm that for a given equation $S = 1$ with coefficients in G decides whether $S = 1$ has a solution in G or not.

Algebra was developed as a tool for solving equations (in classical number systems).

Solving equations in groups is an important algebraic problem.

One-variable equations

A one-variable equation $S(x) = 1$ over a group G:

$$g_0 x^{\varepsilon_0} g_1 x^{\varepsilon_1} \ldots g_{d-1} x^{\varepsilon_{d-1}} = 1, \quad g_i \in G.$$

Theorem [Appel, Lorents, Chiswell-Remeslennikov]

The solution set for a one variable equation $S(x) = 1$ in a free group F is either the whole group F, or the empty set, or a finite union of sets $\{uv^i \mid i \in \mathbb{Z}\}$, where $u, v \in F$.

Theorem [Bormotov, Gilman, Myasnikov]

There is a polynomial time algorithm that for a given one-variable equation $S(x) = 1$ over a free group F finds the solution set for $S(x) = 1$.

One-variable equations

A one-variable equation $S(x) = 1$ over a group G:

$$g_0 x^{\varepsilon_0} g_1 x^{\varepsilon_1} \ldots g_{d-1} x^{\varepsilon_{d-1}} = 1, \quad g_i \in G.$$

Theorem [Appel, Lorents, Chiswell-Remeslennikov]

The solution set for a one variable equation $S(x) = 1$ in a free group F is either the whole group F, or the empty set, or a finite union of sets $\{uv^i \mid i \in \mathbb{Z}\}$, where $u, v \in F$.

Theorem [Bormotov, Gilman, Myasnikov]

There is a polynomial time algorithm that for a given one-variable equation $S(x) = 1$ over a free group F finds the solution set for $S(x) = 1$.

Quadratic equations

For a long time quadratic equations were the focal point of the theory of equations in groups:

Free groups: **Malcev (1962), Wicks (1962,1971), Lyndon (1971), Comerford-Edmunds (1981), Culler (1981), Grigorchuk-Kurchanov (1989)**.

Hyperbolic groups: **Comerford (1981), Grigorchuk-Lysenok (1992)**.

Free products:
Comerford-Edmunds (1981).

Quadratic equations. Complexity

Theorem [Olshanskii, Grigorchuk-Kurchanov]

If the number $|X| = n$ of variables is fixed, then there is an algorithm $\mathcal{A}_n$ to decide if a quadratic equation $S(X) = 1$ has a solution or not, which works in polynomial time in the total length of coefficients in $S(X) = 1$.

Theorem [Kharlampovich, Lysenok, Myasnikov, Touikan (2008)]

The Diophantine problem for quadratic equations in free groups is NP-complete.

Quadratic equations. Complexity

Theorem [Olshanskii, Grigorchuk-Kurchanov]

If the number $|X| = n$ of variables is fixed, then there is an algorithm $\mathcal{A}_n$ to decide if a quadratic equation $S(X) = 1$ has a solution or not, which works in polynomial time in the total length of coefficients in $S(X) = 1$.

Theorem [Kharlampovich, Lysenok, Myasnikov, Touikan (2008)]

The Diophantine problem for quadratic equations in free groups is NP-complete.

Diophantine problem in free groups

The initial version of the Process appeared in the proof of the following result.

Theorem [Makanin, 1982]

There is an algorithm to verify whether a given system of equations has a solution in a free group (free semigroup) or not.

Makanin introduced several fundamental notions: generalized equations, elementary transformations and the entire transformation, transformation process, complexity of a generalized equation.

Diophantine problem in free groups

The initial version of the Process appeared in the proof of the following result.

Theorem [Makanin, 1982]

There is an algorithm to verify whether a given system of equations has a solution in a free group (free semigroup) or not.

Makanin introduced several fundamental notions: generalized equations, elementary transformations and the entire transformation, transformation process, complexity of a generalized equation.

Two parts of an elimination process

Every Elimination Process (EP) consists of two parts:

- **Reduction to "generalized equations**
- **The "Machine"**

Two parts of an elimination process

Every Elimination Process (EP) consists of two parts:

- **Reduction to "generalized equations**
- **The "Machine"**

Two parts of an elimination process

Every Elimination Process (EP) consists of two parts:

- **Reduction to "generalized equations**
- **The "Machine"**

Generalized equations

A Generalized Equation (GE) Ω is a finite system of equations

$$L_1(X) = R_1(X), \ldots, L_k(X) = R_k(X)$$

in a free monoid $M(A)$ with an involution $u \to u^{-1}$.

A reduced solution $\phi : x_1 \to g_1, \ldots x_n \to g_n$ of a GE Ω in $M(A)$ is a solution such that

- all words L_i^{ϕ} and R_i^{ψ} are reduced as written,
- equalities $L_i^{\phi} = R_i^{\psi}$ hold as written,
- $\phi(x_j) \neq 1$ for every j.

Generalized equations

A Generalized Equation (GE) Ω is a finite system of equations

$$L_1(X) = R_1(X), \ldots, L_k(X) = R_k(X)$$

in a free monoid $M(A)$ with an involution $u \to u^{-1}$.

A reduced solution $\phi : x_1 \to g_1, \ldots x_n \to g_n$ of a GE Ω in $M(A)$ is a solution such that

- all words L_i^{ϕ} and R_i^{ψ} are reduced as written,
- equalities $L_i^{\phi} = R_i^{\psi}$ hold as written,
- $\phi(x_j) \neq 1$ for every j.

Reduction to GE:

Given a system $S(X) = 1$ of equations in a free group $F(A)$ one can effectively construct a finite set of generalized equations

$$\Omega_1, \ldots, \Omega_k$$

in the free monoid $M(A)$ semigroup with involution (systems of equations of a particular type) such that:

- given a solution of $S(X) = 1$ in $F(A)$ one can effectively construct a reduced solution of one of Ω_i in the free semigroup with basis $A \cup A^{-1}$.
- given a solution of some Ω_i in the free semigroup with basis $A \cup A^{-1}$ one can effectively construct a solution of $S(X) = 1$ in $F(A)$.

Reduction to generalized equations: example

Equation $xyz = 1$ in a free group F.

Let

$$\phi : x \to x^{\phi}, y \to y^{\phi}, z \to z^{\phi}$$

be a solution in F, where $x^{\phi}, y^{\phi}, z^{\phi}$ are reduced words in $F(A)$.

When we read solutions in the Cayley graph of $F(A)$ we get a cancellation tree.

Then

$$x^{\phi} = \lambda_1 \circ \lambda_2, \; y^{\phi} = \lambda_2^{-1} \circ \lambda_3, z^{\phi} = \lambda_3^{-1} \circ \lambda_1^{-1}.$$

Reduction to generalized equations: example

Equation $xyz = 1$ in a free group F.

Let

$$\phi : x \to x^{\phi}, y \to y^{\phi}, z \to z^{\phi}$$

be a solution in F, where $x^{\phi}, y^{\phi}, z^{\phi}$ are reduced words in $F(A)$.

When we read solutions in the Cayley graph of $F(A)$ we get a cancellation tree.

Then

$$x^{\phi} = \lambda_1 \circ \lambda_2, \; y^{\phi} = \lambda_2^{-1} \circ \lambda_3, z^{\phi} = \lambda_3^{-1} \circ \lambda_1^{-1}.$$

Reduction to generalized equations: example

Equation $xyz = 1$ in a free group F.

Let

$$\phi : x \to x^{\phi}, y \to y^{\phi}, z \to z^{\phi}$$

be a solution in F, where $x^{\phi}, y^{\phi}, z^{\phi}$ are reduced words in $F(A)$.

When we read solutions in the Cayley graph of $F(A)$ we get a cancellation tree.

Then

$$x^{\phi} = \lambda_1 \circ \lambda_2, \; y^{\phi} = \lambda_2^{-1} \circ \lambda_3, z^{\phi} = \lambda_3^{-1} \circ \lambda_1^{-1}.$$

Reduction to generalized equations: example

Equation $xyz = 1$ in a free group F.

Let

$$\phi : x \to x^{\phi}, y \to y^{\phi}, z \to z^{\phi}$$

be a solution in F, where $x^{\phi}, y^{\phi}, z^{\phi}$ are reduced words in $F(A)$.

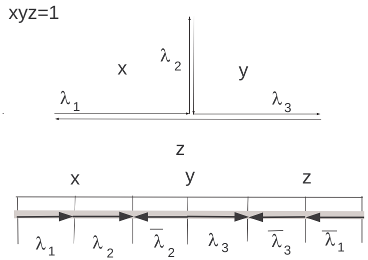
When we read solutions in the Cayley graph of $F(A)$ we get a cancellation tree.

Then

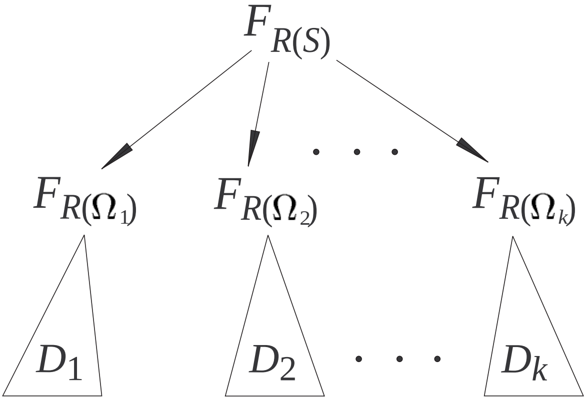
$$x^{\phi} = \lambda_1 \circ \lambda_2,\ \ y^{\phi} = \lambda_2^{-1} \circ \lambda_3, z^{\phi} = \lambda_3^{-1} \circ \lambda_1^{-1}.$$

Reduction to generalized equations: example

In the case when all the words $\lambda_1, \lambda_2, \lambda_3$ are non-empty, the generalized equation would be the interval in Fig. 2.



Reduction to GE: the beginning of the process



Makanin's Transformation Process

Given a generalized equation Ω with a solution σ one can apply an elementary transformation (there are only finitely many of them) and get a new generalized equation Ω' with a solution σ'.

$$(\Omega, \sigma) \to (\Omega', \sigma').$$

Transformation Process is a sequence of elementary transformations, applied according to some precise rules to an initial pair (Ω_0, σ_0):

$$(\Omega_0, \sigma_0) \to (\Omega_1, \sigma_1) \to \ldots \to (\Omega_k, \sigma_k).$$

Makanin's Transformation Process

Given a generalized equation Ω with a solution σ one can apply an elementary transformation (there are only finitely many of them) and get a new generalized equation Ω' with a solution σ'.

$$(\Omega, \sigma) \to (\Omega', \sigma').$$

Transformation Process is a sequence of elementary transformations, applied according to some precise rules to an initial pair (Ω_0, σ_0):

$$(\Omega_0, \sigma_0) \to (\Omega_1, \sigma_1) \to \ldots \to (\Omega_k, \sigma_k).$$

Makanin's Transformation Process

Given a generalized equation Ω with a solution σ one can apply an elementary transformation (there are only finitely many of them) and get a new generalized equation Ω' with a solution σ'.

$$(\Omega, \sigma) \to (\Omega', \sigma').$$

Transformation Process is a sequence of elementary transformations, applied according to some precise rules to an initial pair (Ω_0, σ_0):

$$(\Omega_0, \sigma_0) \to (\Omega_1, \sigma_1) \to \ldots \to (\Omega_k, \sigma_k).$$

Main idea

Transformation argument

Let Ω be a generalized equation and σ a solution with the minimal total length. Then there exists a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

such that:

- σ_k is an "obvious" solution of Ω_k and its length is bounded by the length of Ω;
- the number k is bounded above by a computable function $f(\Omega)$.

Decision algorithm

If Ω has a solution, it has a minimal solution σ.

By Transformation Argument there is a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

with $k \leq f(\Omega)$.

From properties of elementary transformations: $|\sigma_i| \leq 2|\sigma_{i+1}|$.

Hence $|\sigma_0| \leq 2^{f(\Omega)}|\Omega|$.

So if Ω has a solution then it has a solution of length at most $2^{f(\Omega)}|\Omega|$ - brut force check.

Decision algorithm

If Ω has a solution, it has a minimal solution σ.

By Transformation Argument there is a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

with $k \leq f(\Omega)$.

From properties of elementary transformations: $|\sigma_i| \leq 2|\sigma_{i+1}|$.

Hence $|\sigma_0| \leq 2^{f(\Omega)}|\Omega|$.

So if Ω has a solution then it has a solution of length at most $2^{f(\Omega)}|\Omega|$ - brut force check.

Decision algorithm

If Ω has a solution, it has a minimal solution σ.

By Transformation Argument there is a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

with $k \leq f(\Omega)$.

From properties of elementary transformations: $|\sigma_i| \leq 2|\sigma_{i+1}|$.

Hence $|\sigma_0| \leq 2^{f(\Omega)}|\Omega|$.

So if Ω has a solution then it has a solution of length at most $2^{f(\Omega)}|\Omega|$ - brut force check.

Decision algorithm

If Ω has a solution, it has a minimal solution σ.

By Transformation Argument there is a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

with $k \leq f(\Omega)$.

From properties of elementary transformations: $|\sigma_i| \leq 2|\sigma_{i+1}|$.

Hence $|\sigma_0| \leq 2^{f(\Omega)}|\Omega|$.

So if Ω has a solution then it has a solution of length at most $2^{f(\Omega)}|\Omega|$ - brut force check.

Decision algorithm

If Ω has a solution, it has a minimal solution σ.

By Transformation Argument there is a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

with $k \leq f(\Omega)$.

From properties of elementary transformations: $|\sigma_i| \leq 2|\sigma_{i+1}|$.

Hence $|\sigma_0| \leq 2^{f(\Omega)}|\Omega|$.

So if Ω has a solution then it has a solution of length at most $2^{f(\Omega)}|\Omega|$ - brut force check.

Decision algorithm

If Ω has a solution, it has a minimal solution σ.

By Transformation Argument there is a transformation sequence

$$(\Omega, \sigma) = (\Omega_0, \sigma_0) \to \ldots \to (\Omega_k, \sigma_k)$$

with $k \leq f(\Omega)$.

From properties of elementary transformations: $|\sigma_i| \leq 2|\sigma_{i+1}|$.

Hence $|\sigma_0| \leq 2^{f(\Omega)}|\Omega|$.

So if Ω has a solution then it has a solution of length at most $2^{f(\Omega)}|\Omega|$ - brut force check.

Complexity

The original Makanin's algorithm is very inefficient - not even **primitive recursive**.

Plandowski gave a much improved version (for free semigroups): P-**space**.

Gutierrez devised a P-**space** algorithm for free groups.

Conjecture

The Diophantine problem in free semigroups is NP-complete.

If so - interesting consequences for algorithmic group theory, topology, and computer science.

Complexity

The original Makanin's algorithm is very inefficient - not even **primitive recursive**.

Plandowski gave a much improved version (for free semigroups): P-**space**.

Gutierrez devised a P-**space** algorithm for free groups.

Conjecture

The Diophantine problem in free semigroups is NP-complete.

If so - interesting consequences for algorithmic group theory, topology, and computer science.

Complexity

The original Makanin's algorithm is very inefficient - not even **primitive recursive**.

Plandowski gave a much improved version (for free semigroups): P-**space**.

Gutierrez devised a P-**space** algorithm for free groups.

Conjecture

The Diophantine problem in free semigroups is NP-complete.

If so - interesting consequences for algorithmic group theory, topology, and computer science.

Complexity

The original Makanin's algorithm is very inefficient - not even **primitive recursive**.

Plandowski gave a much improved version (for free semigroups): P-**space**.

Gutierrez devised a P-**space** algorithm for free groups.

Conjecture

The Diophantine problem in free semigroups is NP-complete.

If so - interesting consequences for algorithmic group theory, topology, and computer science.

Description of solution

Razborov (1987): described **all solutions** of a given system of equations in F.

Razborov introduced: infinite branches, periodic structures, the kernel, the excess.

He used: fully residually free groups, groups of automorphisms, and fundamental sequences to encode solutions.

Description of solution

Razborov (1987): described **all solutions** of a given system of equations in F.

Razborov introduced: infinite branches, periodic structures, the kernel, the excess.

He used: fully residually free groups, groups of automorphisms, and fundamental sequences to encode solutions.

Description of solution

Razborov (1987): described **all solutions** of a given system of equations in F.

Razborov introduced: infinite branches, periodic structures, the kernel, the excess.

He used: fully residually free groups, groups of automorphisms, and fundamental sequences to encode solutions.

Razborov's Transformation Process

Given a generalized equation Ω one can construct an infinite rooted **solution tree** T_Ω of bounded degree which describes all solutions of Ω.
Put Ω in the root.

Given a vertex v with an associated equation Ω_v apply to Ω all possible elementary transformations

$$\Omega_v \to \Omega_{v_1}, \ldots, \Omega_v \to \Omega_{v_{m_v}}$$

according to some precise rules (as if constructing the Transformation Sequence for each possible solutions of Ω_v).

Terminate at v if Ω_v is obviously inconsistent or trivial.

Razborov's Transformation Process

Given a generalized equation Ω one can construct an infinite rooted **solution tree** T_Ω of bounded degree which describes all solutions of Ω.
Put Ω in the root.

Given a vertex v with an associated equation Ω_v apply to Ω all possible elementary transformations

$$\Omega_v \to \Omega_{v_1}, \ldots, \Omega_v \to \Omega_{v_{m_v}}$$

according to some precise rules (as if constructing the Transformation Sequence for each possible solutions of Ω_v).

Terminate at v if Ω_v is obviously inconsistent or trivial.

Razborov's Transformation Process

Given a generalized equation Ω one can construct an infinite rooted **solution tree** T_Ω of bounded degree which describes all solutions of Ω.
Put Ω in the root.

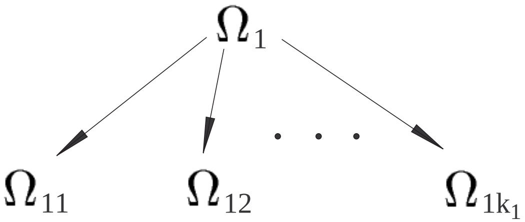
Given a vertex v with an associated equation Ω_v apply to Ω all possible elementary transformations

$$\Omega_v \to \Omega_{v_1}, \ldots, \Omega_v \to \Omega_{v_{m_v}}$$

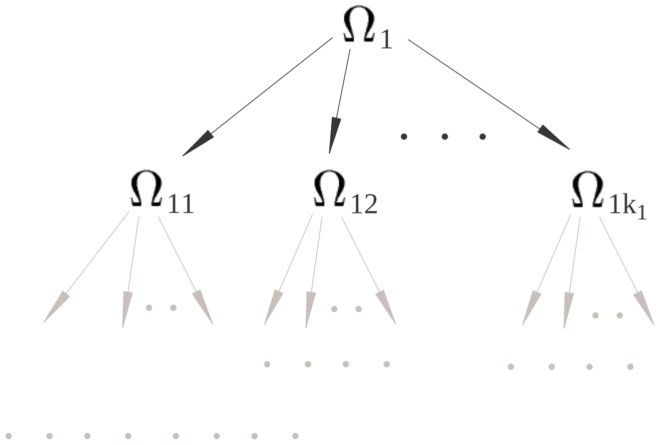
according to some precise rules (as if constructing the Transformation Sequence for each possible solutions of Ω_v).

Terminate at v if Ω_v is obviously inconsistent or trivial.

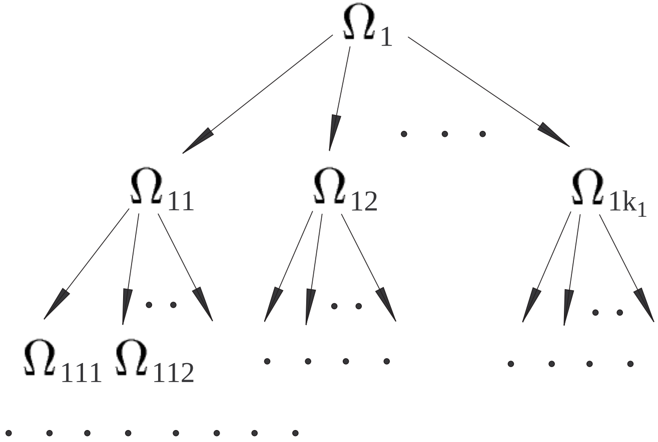
Razborov's Transformation Process



Razborov's Transformation Process



Razborov's Transformation Process



Transformation Argument

First Transformation Argument

There exists a computable function $f(\Omega)$ such that for every branch

$$\Omega_{v_0} \to \Omega_{v_1} \to \ldots \to \Omega_{v_k}$$

if $k \geq f(\Omega_{v_0})$ then $\Omega_{v_i} = \Omega_{v_j}$ for some $1 \leq i < j \leq k$.

Observation: an elementary transformation $\Omega \to \Omega'$ gives rise to an epimorphism of the coordinate groups $F_{R(\Omega)} \to F_{R(\Omega')}$.

Hence if $\Omega_{v_i} = \Omega_{v_j}$ then the sequence $\Omega_{v_i} \to \Omega_{v_{i+1}} \to \ldots \to \Omega_{v_j}$ gives an automorphism ϕ_{ij} of the coordinate group $F_{R(\Omega_{v_i})}$.

Transformation Argument

First Transformation Argument

There exists a computable function $f(\Omega)$ such that for every branch

$$\Omega_{v_0} \to \Omega_{v_1} \to \ldots \to \Omega_{v_k}$$

if $k \geq f(\Omega_{v_0})$ then $\Omega_{v_i} = \Omega_{v_j}$ for some $1 \leq i < j \leq k$.

Observation: an elementary transformation $\Omega \to \Omega'$ gives rise to an epimorphism of the coordinate groups $F_{R(\Omega)} \to F_{R(\Omega')}$.

Hence if $\Omega_{v_i} = \Omega_{v_j}$ then the sequence $\Omega_{v_i} \to \Omega_{v_{i+1}} \to \ldots \to \Omega_{v_j}$ gives an automorphism ϕ_{ij} of the coordinate group $F_{R(\Omega_{v_i})}$.

Transformation Argument

First Transformation Argument

There exists a computable function $f(\Omega)$ such that for every branch

$$\Omega_{v_0} \to \Omega_{v_1} \to \ldots \to \Omega_{v_k}$$

if $k \geq f(\Omega_{v_0})$ then $\Omega_{v_i} = \Omega_{v_j}$ for some $1 \leq i < j \leq k$.

Observation: an elementary transformation $\Omega \to \Omega'$ gives rise to an epimorphism of the coordinate groups $F_{R(\Omega)} \to F_{R(\Omega')}$.

Hence if $\Omega_{v_i} = \Omega_{v_j}$ then the sequence $\Omega_{v_i} \to \Omega_{v_{i+1}} \to \ldots \to \Omega_{v_j}$ gives an automorphism ϕ_{ij} of the coordinate group $F_{R(\Omega_{v_i})}$.

Reconstruction

New idea: rebuild graph T_Ω:

replace edges $\Omega_v \to \Omega_{v'}$ with the edges $F_{R(\Omega)} \to F_{R(\Omega')}$

if $\Omega_{v_i} = \Omega_{v_j}$ then delete the path

$$F_{R(\Omega_{v_i})} \to F_{R(\Omega_{v_{i+1}})} \to \ldots \to F_{R(\Omega_{v_j})}$$

and add the automorphism ϕ_{ij} to the vertex v_i.

Generate a group of automorphisms $A_{v_i} \leq AutF_{R(\Omega_{v_i})}$ by all the automorphism assigned to the vertex v_i.

Add an edges $v_i \to v_i$ labeled by A_{v_i}.

Transformation Argument

The resulting decorated graph (**Solution Diagram**) describes solutions of Ω as the compositions of edge homomorphisms along the paths from the root Ω to the leaves. But it might be infinite.

Second Transformation Argument

All the edge epimorphisms are *proper* epimorphisms (with non-trivial kernels)

Transformation Argument

The resulting decorated graph (**Solution Diagram**) describes solutions of Ω as the compositions of edge homomorphisms along the paths from the root Ω to the leaves. But it might be infinite.

Second Transformation Argument

All the edge epimorphisms are *proper* epimorphisms (with non-trivial kernels)

Transformation Argument

The resulting Solution Diagram still looks like an infinite tree.

Third Transformation Argument

If in the sequence

$$F_{R(\Omega_1)} \to F_{R(\Omega_2)} \to \ldots \to F_{R(\Omega_k)} \to \ldots$$

all epimorphisms are proper (not isomorphisms), then the sequence is finite.

Now Konig's Lemma gives a finite diagram.

Transformation Argument

The resulting Solution Diagram still looks like an infinite tree.

Third Transformation Argument

If in the sequence

$$F_{R(\Omega_1)} \to F_{R(\Omega_2)} \to \ldots \to F_{R(\Omega_k)} \to \ldots$$

all epimorphisms are proper (not isomorphisms), then the sequence is finite.

Now Konig's Lemma gives a finite diagram.

Transformation Argument

The resulting Solution Diagram still looks like an infinite tree.

Third Transformation Argument

If in the sequence

$$F_{R(\Omega_1)} \to F_{R(\Omega_2)} \to \ldots \to F_{R(\Omega_k)} \to \ldots$$

all epimorphisms are proper (not isomorphisms), then the sequence is finite.

Now Konig's Lemma gives a finite diagram.

Description of solutions

Theorem [Razborov]

Given a generalized equation Ω one can effectively construct a finite Solution Diagram D_Ω that describes all solutions of Ω

The reduction from a group equation $S(X) = 1$ to the generalized equations $\Omega_1, \ldots, \Omega_k$ is also effective, hence

Theorem [Razborov]

Given a finite system of equations $S(X) = 1$ in $F(A)$ one can effectively construct a finite Solution Diagram D_S that describes all solutions of $S(X) = 1$ in F.

Description of solutions

Theorem [Razborov]

Given a generalized equation Ω one can effectively construct a finite Solution Diagram D_Ω that describes all solutions of Ω

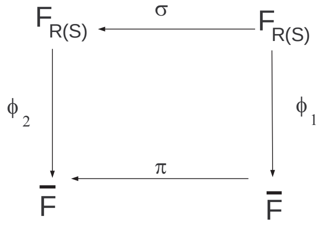
The reduction from a group equation $S(X) = 1$ to the generalized equations $\Omega_1, \ldots, \Omega_k$ is also effective, hence

Theorem [Razborov]

Given a finite system of equations $S(X) = 1$ in $F(A)$ one can effectively construct a finite Solution Diagram D_S that describes all solutions of $S(X) = 1$ in F.

Second Transformation Argument (Principal Quotients)

Let G and K be H-groups and $\mathcal{A} \leq Aut_H(G)$ a group of H-automorphisms of G.
Two H-homomorphisms ϕ and ψ from G into K are called *A-equivalent* (symbolically, $\phi \sim_{\mathcal{A}} \psi$) if there exists $\sigma \in \mathcal{A}$ such that $\phi = \sigma\psi$.
Obviously, $\sim_{\mathcal{A}}$ is an equivalence relation on $Hom_H(G, K)$.



Second Transformation Argument (Minimal solutions)

Let $G = F_{R(S)}$ be the coordinate group of an irreducible system of equation $S(X) = 1$ over F.
Let $\mathcal{A}$ be the group of canonical F-automorphisms of G.
We write $\phi_1 < \phi_2$ if there exists an automorphism $\sigma \in \mathcal{A}$ such that $\phi_2 = \sigma^{-1}\phi_1$ and

$$\sum_{x \in X} |x^{\phi_1}| < \sum_{x \in X} |x^{\phi_2}|.$$

An F-homomorphism $\phi : G \to F$ is called *minimal* if ϕ is $<$-minimal in its $\sim_{\mathcal{A}}$-equivalence class.

Second Transformation Argument (Principal Quotients)

Definition

Let $R_{\mathcal{A}}$ be the intersection of the kernels of all minimal (with respect to $\mathcal{A}$) F-homomorphisms from $Hom_F(G, F)$. Then $G/R_{\mathcal{A}}$ is called the *maximal standard quotient* of G and the canonical epimorphism $\eta : G \to G/R_{\mathcal{A}}$ is the *canonical projection*.

Theorem [KM (1998)]

The maximal standard quotient of a finitely generated fully residually free group is a proper quotient. The maximal standard quotient and the canonical projection can be effectively constructed.

In Sela's work this result (without effectiveness) appears as a *shortening quotient*.

Second Transformation Argument (Principal Quotients)

Definition

Let $R_{\mathcal{A}}$ be the intersection of the kernels of all minimal (with respect to $\mathcal{A}$) F-homomorphisms from $Hom_F(G, F)$. Then $G/R_{\mathcal{A}}$ is called the *maximal standard quotient* of G and the canonical epimorphism $\eta : G \to G/R_{\mathcal{A}}$ is the *canonical projection*.

Theorem [KM (1998)]

The maximal standard quotient of a finitely generated fully residually free group is a proper quotient. The maximal standard quotient and the canonical projection can be effectively constructed.

In Sela's work this result (without effectiveness) appears as a *shortening quotient*.

Second Transformation Argument (Principal Quotients)

Definition

Let $R_{\mathcal{A}}$ be the intersection of the kernels of all minimal (with respect to $\mathcal{A}$) F-homomorphisms from $Hom_F(G, F)$. Then $G/R_{\mathcal{A}}$ is called the *maximal standard quotient* of G and the canonical epimorphism $\eta : G \to G/R_{\mathcal{A}}$ is the *canonical projection*.

Theorem [KM (1998)]

The maximal standard quotient of a finitely generated fully residually free group is a proper quotient. The maximal standard quotient and the canonical projection can be effectively constructed.

In Sela's work this result (without effectiveness) appears as a *shortening quotient*.

Third Transformation Argument

Stabilization of the sequence

$$F_{R(\Omega_1)} \to F_{R(\Omega_2)} \to \ldots \to F_{R(\Omega_k)} \to \ldots$$

comes from the result that F is equationally Noetherian.

Equationally Noetherian groups: problems

Open Problem

Is the class of equationally Noetherian groups closed under free products?

Open Problem

Are free Lie algebras equationally Noetherian?

Equationally Noetherian groups: problems

Open Problem

Is the class of equationally Noetherian groups closed under free products?

Open Problem

Are free Lie algebras equationally Noetherian?

Elimination Process

Kharlampovich - Myasnikov (1998): introduced a modification of Razborov's process, called an Elimination Process (EP) to describe solutions of systems of equations in free groups in terms of **triangular quadratic systems** of equations.

This solves (in the strongest possible form) an open problem posed by Razborov.

This process resembles the classical elimination theory for polynomials.

Elimination Process

Kharlampovich - Myasnikov (1998): introduced a modification of Razborov's process, called an Elimination Process (EP) to describe solutions of systems of equations in free groups in terms of **triangular quadratic systems** of equations.

This solves (in the strongest possible form) an open problem posed by Razborov.

This process resembles the classical elimination theory for polynomials.

Elimination Process

Kharlampovich - Myasnikov (1998): introduced a modification of Razborov's process, called an Elimination Process (EP) to describe solutions of systems of equations in free groups in terms of **triangular quadratic systems** of equations.

This solves (in the strongest possible form) an open problem posed by Razborov.

This process resembles the classical elimination theory for polynomials.

A triangular quasi-quadratic (TQ) system has the following form

$$S_1(X_1, X_2, \ldots, X_n, A) = 1,$$
$$S_2(X_2, \ldots, X_n, A) = 1,$$
$$\ldots$$
$$S_n(X_n, A) = 1$$

where S_i is either quadratic in variables X_i, or corresponds to an extension of a centralizer, or to an abelian extension.

Extension Theorem

A TQ system

$$S_1(X_1, X_2, \ldots, X_n, A) = 1,$$

$$S_2(X_2, \ldots, X_n, A) = 1,$$

$$\ldots$$

$$S_n(X_n, A) = 1$$

is **non-degenerate (NTQ)** if for every i the equation $S_i(X_i, \ldots, X_n, A) = 1$ has a solution in the coordinate group $F_{R(S_{i+1}, \ldots, S_n)}$, where $X_{i+1}, \ldots, X_n, A$ are viewed as constants.

Equivalently, in an NTQ system every equation $S_i(X_i) = 1$ has a solution in the generic point of the system $S_{i+1} = 1, \ldots, S_n = 1$.

Extension Theorem

A TQ system

$$S_1(X_1, X_2, \ldots, X_n, A) = 1,$$

$$S_2(X_2, \ldots, X_n, A) = 1,$$

$$\ldots$$

$$S_n(X_n, A) = 1$$

is **non-degenerate (NTQ)** if for every i the equation $S_i(X_i, \ldots, X_n, A) = 1$ has a solution in the coordinate group $F_{R(S_{i+1},\ldots,S_n)}$, where $X_{i+1}, \ldots, X_n, A$ are viewed as constants.

Equivalently, in an NTQ system every equation $S_i(X_i) = 1$ has a solution in the generic point of the system $S_{i+1} = 1, \ldots, S_n = 1$.

Description of solutions

Theorem [KM]

Given an arbitrary system $S(X, A) = 1$ EP starts on $S(X, A)$ and outputs finitely many NTQ systems

$$U_1(Y) = 1, \ldots, U_m(Y) = 1$$

such that

$$V_F(S) = P_1(V(U_1)) \cup \ldots \cup P_m((U_m))$$

for some word mappings $P_1, \ldots, P_m$.

Corollary

Up to the rational equivalence algebraic sets over F are finite unions of sets defined by NTQ systems.

Analogies with the classical case

Elimination Process can be viewed as a non-commutative analog of the classical **elimination process** in algebraic geometry. Indeed, going "down" it brings the system to the triangular form - eliminating variables:

$$S_1(X_1, X_2, \ldots, X_n, A) = 1,$$
$$S_2(X_2, \ldots, X_n, A) = 1,$$
$$\ldots$$
$$S_n(X_n, A) = 1$$

Analogies with the classical case

$$S_1(X_1, X_2, \dots, X_n, A) = 1,$$
$$S_2(X_2, \dots, X_n, A) = 1,$$
$$\dots$$
$$S_n(X_n, A) = 1$$

Going back from the "bottom to the top" every solution of the subsystem $S_{i+1} = 1, \dots S_n = 1$ can be extended to a solution of the next equation $S_i = 1$.

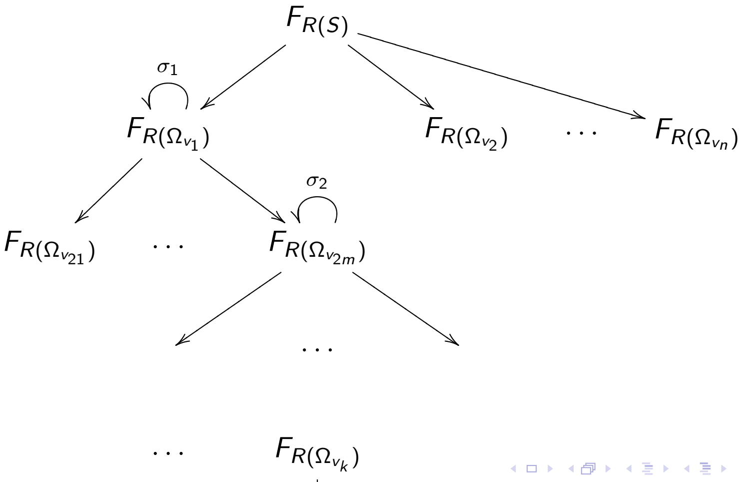
This is a non-commutative analog of the **extension theorems** in the classical elimination theory for polynomials.

Solution diagrams

Theorem [KM]

All solutions of the system of equations $S = 1$ in $F(A)$ can be effectively represented as homomorphisms from $F_{R(S)}$ into $F(A)$ encoded into the following canonical Hom-diagram. Here all groups, except, maybe, the one in the root, are fully residually free, (given by a finite presentation) arrows pointing down correspond to epimorphisms (defined effectively in terms of generators) with non-trivial kernels, and loops correspond to automorphisms of the coordinate groups. Moreover, for every branch in the diagram (from the root to a leaf) one can read off an NTQ system.

Solution diagrams



Zariski topology

The following conditions are equivalent:

- G is equationally Noetherian, i.e., every system $S(X) = 1$ over G is equivalent to some finite part of itself.
- the **Zariski topology** (formed by algebraic sets as a sub-basis of closed sets) over G^n is **Noetherian** for every n, i.e., every proper descending chain of closed sets in G^n is finite.
- Every **chain of proper epimorphisms** of coordinate groups over G is **finite**.

Zariski topology

The following conditions are equivalent:

- G is equationally Noetherian, i.e., every system $S(X) = 1$ over G is equivalent to some finite part of itself.
- the **Zariski topology** (formed by algebraic sets as a sub-basis of closed sets) over G^n is **Noetherian** for every n, i.e., every proper descending chain of closed sets in G^n is finite.
- Every **chain of proper epimorphisms** of coordinate groups over G is **finite**.

Zariski topology

The following conditions are equivalent:

- G is equationally Noetherian, i.e., every system $S(X) = 1$ over G is equivalent to some finite part of itself.
- the **Zariski topology** (formed by algebraic sets as a sub-basis of closed sets) over G^n is **Noetherian** for every n, i.e., every proper descending chain of closed sets in G^n is finite.
- Every **chain of proper epimorphisms** of coordinate groups over G is **finite**.

Irreducible components

If the Zariski topology is Noetherian then every algebraic set can be uniquely presented as a finite union of its **irreducible components**:

$$V = V_1 \cup \ldots V_k.$$

Recall, that a closed subset V is **irreducible** if it is not a union of two proper closed (in the induced topology) subsets.

Irreducible components

If the Zariski topology is Noetherian then every algebraic set can be uniquely presented as a finite union of its **irreducible components**:

$$V = V_1 \cup \ldots V_k.$$

Recall, that a closed subset V is **irreducible** if it is not a union of two proper closed (in the induced topology) subsets.

NTQ decompositions of algebraic sets

Let $V = V_F(S)$ be an algebraic set defined by a system $S = 1$ and

$$V = P_1(V(U_1)) \cup \ldots \cup P_m((U_m))$$

its NTQ decomposition as finite union of sets rationally equivalent to the NTQ systems $U_1 = 1, \ldots, U_m = 1$.

Theorem [KM]

Zariski closures of $P_1(V(U_1)), \ldots, P_m((U_m))$ are precisely the irreducible components of V.

Theorem [KM]

Given a system $S = 1$ one can effectively find systems $S_1 = 1, \ldots, S_m = 1$ that define the irreducible components of $V_F(S)$.

NTQ decompositions of algebraic sets

Let $V = V_F(S)$ be an algebraic set defined by a system $S = 1$ and

$$V = P_1(V(U_1)) \cup \ldots \cup P_m((U_m))$$

its NTQ decomposition as finite union of sets rationally equivalent to the NTQ systems $U_1 = 1, \ldots, U_m = 1$.

Theorem [KM]

Zariski closures of $P_1(V(U_1)), \ldots, P_m((U_m))$ are precisely the irreducible components of V.

Theorem [KM]

Given a system $S = 1$ one can effectively find systems $S_1 = 1, \ldots, S_m = 1$ that define the irreducible components of $V_F(S)$.

NTQ decompositions of algebraic sets

Let $V = V_F(S)$ be an algebraic set defined by a system $S = 1$ and

$$V = P_1(V(U_1)) \cup \ldots \cup P_m((U_m))$$

its NTQ decomposition as finite union of sets rationally equivalent to the NTQ systems $U_1 = 1, \ldots, U_m = 1$.

Theorem [KM]

Zariski closures of $P_1(V(U_1)), \ldots, P_m((U_m))$ are precisely the irreducible components of V.

Theorem [KM]

Given a system $S = 1$ one can effectively find systems $S_1 = 1, \ldots, S_m = 1$ that define the irreducible components of $V_F(S)$.

Philosophy

From the group theoretic view-point Elimination Process, when applied to a system $S = 1$, tells something about the coordinate group $F_{R(S)}$.

The Main Idea: Use Elimination Process to get results on the coordinate groups.

But, before that, why these coordinate groups are interesting?

Philosophy

From the group theoretic view-point Elimination Process, when applied to a system $S = 1$, tells something about the coordinate group $F_{R(S)}$.

The Main Idea: Use Elimination Process to get results on the coordinate groups.

But, before that, why these coordinate groups are interesting?

Philosophy

From the group theoretic view-point Elimination Process, when applied to a system $S = 1$, tells something about the coordinate group $F_{R(S)}$.

The Main Idea: Use Elimination Process to get results on the coordinate groups.

But, before that, why these coordinate groups are interesting?

The coordinate groups over F

Unification Theorems

Let G be a finitely generated group and $F \leq G$. Then the following conditions are equivalent:

1) [BKMR] G is the coordinate group of an irreducible variety over F.
2) [Newmann] G is **discriminated** by F, i.e. for any finite subset $M \subseteq G$ there exists an H-homomorphism injective on M.
3) [Remeslennikov] G is **universally equivalent** to F;
4) [Champetier, Guirardel] G is a limit of free groups in **Gromov-Hausdorff** metric.

The coordinate groups over F

Unification Theorems

Let G be a finitely generated group and $F \leq G$. Then the following conditions are equivalent:

1) [BKMR] G is the coordinate group of an irreducible variety over F.
2) [Newmann] G is **discriminated** by F, i.e. for any finite subset $M \subseteq G$ there exists an H-homomorphism injective on M.
3) [Remeslennikov] G is **universally equivalent** to F;
4) [Champetier, Guirardel] G is a limit of free groups in **Gromov-Hausdorff** metric.

The coordinate groups over F

Unification Theorems

Let G be a finitely generated group and $F \leq G$. Then the following conditions are equivalent:

1) [BKMR] G is the coordinate group of an irreducible variety over F.

2) [Newmann] G is **discriminated** by F, i.e. for any finite subset $M \subseteq G$ there exists an H-homomorphism injective on M.

3) [Remeslennikov] G is **universally equivalent** to F;

4) [Champetier, Guirardel] G is a limit of free groups in **Gromov-Hausdorff** metric.

The coordinate groups over F

Unification Theorems

Let G be a finitely generated group and $F \leq G$. Then the following conditions are equivalent:

1) [BKMR] G is the coordinate group of an irreducible variety over F.
2) [Newmann] G is **discriminated** by F, i.e. for any finite subset $M \subseteq G$ there exists an H-homomorphism injective on M.
3) [Remeslennikov] G is **universally equivalent** to F;
4) [Champetier, Guirardel] G is a limit of free groups in **Gromov-Hausdorff** metric.

The coordinate groups over F

Unification Theorems

Let G be a finitely generated group and $F \leq G$. Then the following conditions are equivalent:

1) [BKMR] G is the coordinate group of an irreducible variety over F.
2) [Newmann] G is **discriminated** by F, i.e. for any finite subset $M \subseteq G$ there exists an H-homomorphism injective on M.
3) [Remeslennikov] G is **universally equivalent** to F;
4) [Champetier, Guirardel] G is a limit of free groups in **Gromov-Hausdorff** metric.

Elimination process and JSJ

A **splitting** of G is a representation of G as the fundamental groups of a graph of groups.

A splitting is **cyclic (abelian)** if all the edge groups are cyclic (abelian).

Elementary splittings:
$G = A *_C B, \quad G = A*_C = \langle A, t \mid t^{-1}Ct = C' \rangle,$

Free splittings:
$G = A * B$

Elimination process and JSJ

A **splitting** of G is a representation of G as the fundamental groups of a graph of groups.

A splitting is **cyclic (abelian)** if all the edge groups are cyclic (abelian).

Elementary splittings:
$G = A *_C B, \quad G = A*_C = \langle A, t \mid t^{-1}Ct = C' \rangle,$

Free splittings:
$G = A * B$

Elimination process and JSJ

A **splitting** of G is a representation of G as the fundamental groups of a graph of groups.

A splitting is **cyclic (abelian)** if all the edge groups are cyclic (abelian).

Elementary splittings:
$G = A *_C B, \quad G = A*_C = \langle A, t \mid t^{-1}Ct = C' \rangle,$

Free splittings:
$G = A * B$

Grushko's decompositions

All free splittings of G are encoded in **Grushko's decompositions**.
A free decomposition

$$G = G_1 * \ldots * G_k * F_r$$

is a Grushko's decomposition of G if $G_1, \ldots, G_k$ are freely indecomposable non-cyclic groups and F_r is a free group of rank r.
Grushko's decompositions are **essentially unique**.

JSJ decompositions

All cyclic (abelian) splittings of G are encoded in **JSJ decompositions** of G.

JSJ decompositions are universal decompositions with vertices of the following types: **QH-vertices, abelian, rigid**.

JSJ decompositions are **essentially unique**.

Infinite branches and JSJ

Motto: JSJ is an algebraic counterpart of EP.

infinite branches of EP $\Longleftrightarrow$ **abelian splittings** of the coordinate groups of the systems.

Moreover, the automorphisms associated with infinite branches of the process are precisely the canonical automorphisms of the JSJ decomposition associated with the splittings.

Effectiveness of Grushko's and JSJ decompositions

Theorem [KM]

There is an algorithm which for every finitely generated fully residually free group finds its Grushko's decomposition (by giving finite generating sets of the factors).

Theorem [KM]

There exists an algorithm to obtain a cyclic [abelian] JSJ decomposition of a freely indecomposable fully residually free group. The algorithm constructs a presentation of this group as the fundamental group of a JSJ graph of groups.

Effectiveness of Grushko's and JSJ decompositions

Theorem [KM]

There is an algorithm which for every finitely generated fully residually free group finds its Grushko's decomposition (by giving finite generating sets of the factors).

Theorem [KM]

There exists an algorithm to obtain a cyclic [abelian] JSJ decomposition of a freely indecomposable fully residually free group. The algorithm constructs a presentation of this group as the fundamental group of a JSJ graph of groups.

Isomorphism problem

Theorem [Bumagin, Kharlampovich, M.]

The isomorphism problem is decidable in the class of all finitely generated fully residually free groups.

Recently, **Dahmani and Groves** generalized this result to torsion-free groups which are hyperbolic relative to abelian subgroups.

Isomorphism problem

Theorem [Bumagin, Kharlampovich, M.]

The isomorphism problem is decidable in the class of all finitely generated fully residually free groups.

Recently, **Dahmani and Groves** generalized this result to torsion-free groups which are hyperbolic relative to abelian subgroups.

Elimination processes and free actions

Infinite branches of an elimination process correspond precisely to the standard types of free actions:

linear case $\Longleftrightarrow$ **thin (or Levitt)** type

the quadratic case $\Longleftrightarrow$ **surface type (or interval exchange)**,

periodic structures $\Longleftrightarrow$ **toral (or axial)** type.

Elimination processes and free actions

Infinite branches of an elimination process correspond precisely to the standard types of free actions:

linear case $\Longleftrightarrow$ **thin (or Levitt)** type

the quadratic case $\Longleftrightarrow$ **surface type (or interval exchange)**,

periodic structures $\Longleftrightarrow$ **toral (or axial)** type.

Elimination processes and free actions

Infinite branches of an elimination process correspond precisely to the standard types of free actions:

linear case $\Longleftrightarrow$ **thin (or Levitt)** type

the quadratic case $\Longleftrightarrow$ **surface type (or interval exchange)**,

periodic structures $\Longleftrightarrow$ **toral (or axial)** type.

Elimination processes and free actions

Infinite branches of an elimination process correspond precisely to the standard types of free actions:

linear case $\Longleftrightarrow$ **thin (or Levitt)** type

the quadratic case $\Longleftrightarrow$ **surface type (or interval exchange)**,

periodic structures $\Longleftrightarrow$ **toral (or axial)** type.