Various Faces of Fully Residually Free Groups and Algorithmic Problems

Alexei Myasnikov

(Based on joint results with O.Kharlampovich, V.Remeslennikov, D.Serbin)

In this talk I am going to discuss some recent developments in the area of algorithmic problems for fully residually free groups. These groups play a crucial role in the modern theory of equations in groups.

Plan:

1. Three approaches to fully residually free groups.

2. Coordinate groups of irreducible systems of equations.

3. Free constructible groups.

4. Presentations via infinite words.

5. Elimination process versus JSJ.

6. Applications.

Fully Residually Free Groups

Different names:

Fully residually free groups =
freely discriminated groups =
ω-residually free groups

The same definition:

Let $F = F(A)$ be a free group with basis A.

A group G is *fully residually free* if for any finite subset $K \subseteq G$ of non-trivial elements there exists a homomorphism $\phi : G \to F$ such that $g^{\phi} \neq 1$ for each $g \in K$.

$\mathcal{F}$ = class of finitely generated fully residually free groups.

Examples

Example 1: $F \times F \notin \mathcal{F}$ (residually free, but not fully).

Example 2: Surface groups

$$[x_1, y_1] \ldots [x_n, y_n] = 1$$

$$x_1^2 \ldots x_n^2 \quad (n \geq 4)$$

are in $\mathcal{F}$.

Elementary Properties:

- torsion-free
- commutative transitive (commutativity is transitive on non-trivial elements)
- CSA (maximal abelian subgroups are malnormal $A^g \cap A = 1$ for $g \notin A$)
- every 2-generated subgroup is free

Three ways to look at groups in $\mathcal{F}$:

1. Coordinate groups of irreducible systems of equations over free groups.

Tools: Algebraic geometry over groups, Makanin-Razborov's techniques.

2. Fundamental groups of graphs of groups of a very particular type.

Tools: Bass-Serre theory, JSJ decompositions.

3. Groups of infinite words over abelian ordered groups $\mathbb{Z}^n$.

Tools: cancellation techniques, Nielsen method, Stallings' foldings to study their finitely generated subgroups.

Other interesting characterizations:

For a finitely generated (non-abelian) G the following conditions are equivalent:

- $G \in \mathcal{F}$;
- $Th_{\forall}(G) = Th_{\forall}(F)$ (Remeslennikov);
- G is a limit group (Sela);
- G is a limit of free groups in a compact space of marked groups (Champetier and Guirardel).

1. Fully residually free groups as the coordinate groups of irreducible system of equations

Coordinate groups:

A set of *variables* $X = \{x_1, \ldots, x_n\}$

A finite system of *equations* over F:

$$S(X, A) = 1$$

in variables from X and constants from F.

The *algebraic set* defined by S:

$$V_F(S) = \{U \in F^n \mid S(U, A) = 1\}$$

$V_F(S)$ is uniquely defined by the *radical*:

$$R(S) = \{T \in F(A \cup X) \mid \forall U (S(U) = 1 \to T(U) = 1)\}$$

The *coordinate group* of $S = 1$:

$$F_{R(S)} = F(A \cup X)/R(S)$$

A k-tuple of words

$$P = (P_1(X), \ldots, P_k(X))$$

determines a *word mapping* or *morphism*

$$P : F^n \to F^m.$$

Two algebraic sets Y and Z are said to be *isomorphic* $Y \sim Z$ if there exist morphisms

$$\phi : Y \longrightarrow Z, \quad \theta : Z \longrightarrow Y$$

such that $\theta\phi = 1_Y$, $\phi\theta = 1_Z$.

(1999) **Baumslag, Myasnikov, Remeslennikov:**

1) $V_F(S_1) \sim V_F(S_2) \Longleftrightarrow F_{R(S_1)} \simeq_F F_{R(S_2)}$

2) Every f.g. residually free group is a coordinate group of some system $S = 1$ over F.

Irreducible components:

Zariski topology on F^m:
algebraic sets = closed subsets

R. Bryant (1977), V.Guba (1986): F is *equationally Noetherian*, i.e., every system $S(X, A) = 1$ is equivalent over F to a finite subsystem.

Corollary:

1. Zariski topology is Noetherian;

2. Every closed set is a finite union of *irreducible components*.

Theorem [BMR]:

1) $V(S)$ *is irreducible* $\iff F_{R(S)} \in \mathcal{F}$

2) $G \in \mathcal{F} \iff G \simeq F_{R(S)}$ *for an irreducible* $V(S)$

Main Tool:

From the group theoretic view-point the elimination process (variation of Makanin-Razborov's method) tells something about the coordinate groups of the systems involved.

This allows one to *translate pure combinatorial and algorithmic results obtained in the process into statements about fully residually free groups*.

First applications:

Theorem [Kharlampovich, Myasnikov]: *There is an algorithm which for a given finite system of equations $S(X) = 1$ over F finds its irreducible components.*

It is known that groups in $\mathcal{F}$ are finitely presented [KM (1998), Sela (2001)].

Theorem [KM]: *For every finite irreducible system of equations $S = 1$ one can effectively find the radical $R(S)$ by specifying a finite set of generators of $R(S)$ as a normal subgroup.*

This gives an *"effective" Nullstellensatz*.

Description of radicals (generalized Nulsstellensatz) is one of the major problems in commutative algebra.

2. Fully residually free groups as fundamental groups of graphs of groups.

Lyndon: introduced *free exponential groups* $F^{\mathbb{Z}[t]}$ over polynomials $\mathbb{Z}[t]$ (to describe solution sets of one-variable equations).

He showed also: $F^{\mathbb{Z}[t]}$ *is discriminated by* F.

Myasnikov and Remeslennikov: $F^{Z[t]}$ can be obtained as union of an infinite chain of extensions of centralizers:

$$F = G_0 < G_1 < \ldots < \cup_{i=0}^{\infty} G_i = F^{Z[t]}$$

where

$$G_{i+1} = \langle G_i, t_i \mid [C_{G_i}(u_i), t_i] = 1 \rangle.$$

Bass-Serre Theory implies:

Finitely generated subgroups of $F^{Z[t]}$ are fundamental groups of very particular graphs of groups (essential splittings, etc.).

Theorem [KM]: *Given an irreducible system $S = 1$ (a group $G \in \mathcal{F}$) one can effectively embed $F_{R(S)}$ (the group G) into $F^{Z[t]}$. Namely, one can find n and an embedding $G \to G_n$.*

Theorem [KM]: *There is an algorithm which for a given group $G \in \mathcal{F}$ and a finitely generated subgroup $H \leq G$ (given by a finite generating set Y), finds a finite presentation for H in the generators Y.*

Idea of the proof:

Let $G = \langle X \mid S \rangle$ be a finite presentation of G.

Then $G = F_{R(S)}$ is irreducible.

Effectively embed $F_{R(S)}$ into $F^{Z[t]}$.

Use "effective version" of Bass-Serre theory to find the induced presentation of the subgroup.

"Effective version" of B-S theory requires algorithmic solution of various problems for finitely generated subgroups.

3. Fully residually free groups via infinite words

Lyndon: introduced abstract length functions on groups $L : G \to A$ with values in an ordered abelian group A to *axiomatize Nielsen cancellation argument*.

He showed: if a length function $L : G \to \mathbb{Z}$ is free ($x \neq 1 \Longrightarrow l(x^2) > l(x)$) then G is embeddable into a free group and the embedding preserves the length.

Main idea:

1. Generalize this to arbitrary free length functions $l : G \to \Lambda$ presenting elements of G by *infinite* words over Λ.

2. Present groups $G \in \mathcal{F}$ by *infinite words* over $\mathbb{Z}^n$ and prove results as in free groups (as for finite words).

Infinite words over $\mathbb{Z}[t]$:

Myasnikov, Remeslennikov, Serbin:

A (*infinite*) *word* over $\mathbb{Z}[t]$ is a function of the type

$$w : [1, \alpha_w] \rightarrow A^{\pm 1},$$

where

$$[1, \alpha_w] = \{g \in \mathbb{Z}[t] \mid 1 \leq g \leq \alpha_w\}$$

is a closed interval in $\mathbb{Z}[t]$ (in *lex* order).

$|w| = \alpha_w$ is the *length* of w.

w is *reduced* if $\forall f \in [1, \alpha_w]$:

$$w(f) \neq w(f+1)$$

(no subwords aa^{-1} or $a^{-1}a$ in w).

$R(\mathbb{Z}[t], A)$ - the set of all reduced infinite words with *partial multiplication*.

Multiplication = concatenation + reduction (*if possible !*).

Product uv is defined if the maximal common initial segment of u^{-1} and v is *closed*.

MRS:

$$L : w \to |w|$$

is a free *Lyndon's length function* on $R(\mathbb{Z}[t], A)$ with values in $\mathbb{Z}[t]$.

If G is a finitely generated subgroup of $R(\mathbb{Z}[t], A)$ then

$$L|_G : G \to \mathbb{Z}^n$$

Chiswell:

$l : G \to \Lambda$ is free Lyndon's length function $\iff$ G acts freely on a Λ-tree.

Theorem [Myasnikov, Remeslennikov, Serbin]. *One can effectively embed $F^{\mathbb{Z}[t]}$ into $R(\mathbb{Z}[t], A)$.*

Corollary. $F^{\mathbb{Z}[t]}$ *acts freely on a* $\mathbb{Z}[t] - tree.$

Corollary [KM and MRS]. *Every group $G \in \mathcal{F}$ acts freely on a $\mathbb{Z}^n$-tree.*

Hint on how to embed $F^{\mathbb{Z}[t]}$ into $R(\mathbb{Z}[t], A)$

H.Bass: extension of a centralizer

$$G = \langle F, t \mid [u, t] = 1 \rangle$$

acts freely on a $\mathbb{Z} \times \mathbb{Z}$-tree.

Idea of a proof:

May assume u is cyclically reduced.

Define $\phi : G \to R(\mathbb{Z} \times \mathbb{Z}, A)$:

$$f^{\phi} = f, \quad t^{\phi} = u^{\infty} = u \circ u \circ \ldots \circ u$$

Then

$$(tu)^{\phi} = u^{\infty} \circ u = u \circ u^{\infty} = (ut)^{\phi}$$

So ϕ is a homomorphism. Easy to check ϕ is injective.

More generally (Bass):

$$G = \langle F, t \mid u^t = v \rangle$$

with $|u| = |v|$. Here $ut = tv$, so put $t = u^{\infty} v^{\infty}$.

Once a presentation of elements of $F^{\mathbb{Z}[t]}$ by infinite words is established, a host of problems about $F^{\mathbb{Z}[t]}$ can be solved precisely in the same way as in the standard free group F.

1. The *Word Problem* is decidable in groups from $\mathcal{F}$.

Compute the reduced form of a word!
[Original proof is due to **Makanin**]

2. The *Conjugacy Problem* is decidable in groups from $\mathcal{F}$.

The cyclic reduced words of conjugated elements are equal!
[Original proof is due to **Bumagin**]

3. The *Membership Problem* is decidable in groups from $\mathcal{F}$

Stallings' folding procedure!

For a given

$$H = \langle h_1, \dots, h_m \rangle \leq F^{\mathbb{Z}[t]}$$

construct effectively a finite labelled graph Γ_H which accepts precisely elements of H (given by their canonical forms in $F^{\mathbb{Z}[t]}$.

4. The *Intersection Problem* is decidable in groups from $\mathcal{F}$:

Let $G \in \mathcal{F}$ and H and K finitely generated subgroups of G given by finite generating sets. Then $H \cap K$ is finitely generated, and one can effectively find a finite set of generators of $H \cap K$.

5. The *Intersection of Conjugates Problem* is decidable in groups from $\mathcal{F}$:

Let $H, K \leq_{f.g.} G \in \mathcal{F}$. Then one can effectively find a finite family $\mathcal{J}(H, K)$ of non-trivial f.g. subgroups of G, such that for any non-trivial intersection $H^g \cap K$ there exists $J \in \mathcal{J}(H, K)$ and $f \in K$ such that

$$H^g \cap K = J^f,$$

moreover J and f can be found effectively.

Elimination process

Elimination Process (EP) is a symbolic rewriting process of a certain type that transforms formal systems of equations in groups or semigroups.

Makanin (1982): Initial version of (EP).

Makanin's (EP) gives a decision algorithm to verify consistency of a given system (*decidability of Diophantine problem* over free groups).

Estimates on the length of the minimal solution (if it exists).

Razborov (1987): developed (EP) much further.

Razborov's (EP) produces *all solutions* of a given system in F.

KM (1998): refined Razborov's (EP).

Description of solutions in terms of *non-degenerate triangular quasi-quadratic (NTQ) systems*.

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.

Our (EP) starts on an arbitrary system

$$S(X, A) = 1$$

and results in finitely many TQ 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 $P_1, \ldots, P_m$.

This (EP) can be viewed as a *non-commutative analog* of the *classical elimination process* in algebraic geometry.

Extension Theorem

Moreover, TQ systems

$$U_1 = 1, \ldots, U_m = 1$$

are *"non-degenerate" (NTQ)*

$\Longleftrightarrow$

$S_i(X_i, \ldots, X_n, A) = 1$ has a solution over the coordinate group $F_{R(S_{i+1},\ldots,S_n)}$

$\Longleftrightarrow$

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

This corresponds to the *extension theorems* in the classical theory of elimination for polynomials.

Fundamental properties of various (EP)

This (EP) is not unique, every time it can be easily adjusted to some particular needs.

However, there exist fundamental common features that unify all recent variations of (EP):

1) only *three* precisely defined *infinite branches (subprocesses)* can occur in the process:

linear case (Cases 7-10),

quadratic case (Cases 11-12),

general JSJ case (Cases 13-15) which includes *periodic structures* and *abelian* vertex groups (Case 2).

2) Groups of *automorphisms* of the coordinate groups are used in *encoding the infinite branches* of the process.

Makanin's process and Rip's machines

Makanin's process: there are no infinite branches corresponding to the periodic structures, no linear case, no coordinate groups, no groups of automorphisms.

But there are: elementary and entire transformations, complexity.

These were used to prove the classification theorem for f.g. acting freely on $\mathbb{R}$-trees and to describe stable actions on $\mathbb{R}$-trees, via so-called Rip's machine **[Rips, Gaboriau, Levitt, Paulin, Bestvina, Feighn]**.

Later, these results played a key part in the proof of existence of JSJ decompositions of finitely presented groups with a single end **[Sela, Rips]**.

Elimination process and JSJ

Motto: JSJ is an algebraic counterpart of (EP).

Infinite branches of an elimination process $\Longleftrightarrow$ *splittings* of the coordinate group of the systems:

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

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

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

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

Effectiveness of 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 decomposition are essentially unique.

Theorem [KM] *There is an algorithm which for every $G \in \mathcal{F}$ finds its Grushko's decomposition (by giving finite generating sets of the factors).*

Effectiveness of JSJ decompositions

Theorem [KM] *There exists an algorithm to obtain a cyclic [abelian] JSJ decomposition of a freely indecomposable group $G \in \mathcal{F}$. The algorithm constructs a presentation of this group as the fundamental group of a JSJ graph of groups.*

Hint of the proof

$G \in \mathcal{F}$ *given as* $F_{R(S)}$.

Solutions of $S(X, A) = 1$ *in* $F \Longleftrightarrow$ *homomorphisms* $\phi : G \to F$.

Composition of ϕ *with* $\sigma \in Aut(G) \Longrightarrow$ *a new solution of* $S(X, A) = 1$ *in* F.

Different canonical automorphisms associated with a JSJ decomposition of $G \Longleftrightarrow$ *solutions of the system* $S(X, A) = 1$ *of a particular type.*

One can recognize these solutions in (EP) as infinite branches.

Infinite branches $\Longleftrightarrow$ *splittings of* G.

Bass-Serre Theory + length functions techniques $\Longrightarrow$ *JSJ decompositions of* G.