The isomorphism problem for finite extensions of free groups is in PSPACE

Géraud Sénizergues¹ <u>Armin Weiß</u>²

¹LaBRI, Bordeaux, France ²Universität Stuttgart, Germany

Prague, July 11, 2018

Let G be a group, generated by a finite set Σ and $p: \Sigma^* \to G$ the canonical projection. Write \overline{a} for the letter $a^{-1} \in \Sigma$.

- Word problem: Given $w \in \Sigma^*$. Question: Is w = 1 in G? WP(G) = $p^{-1}(1)$
- Conjugacy problem: Given v, w ∈ Σ*. Question: v ~ w?
 (∃ z ∈ G such that zvz⁻¹ = w?)
- Isomorphism problem: Are the groups $\langle \Sigma \mid R \rangle$ and $\langle \Sigma' \mid R' \rangle$ isomorphic?

Free groups

The free group with basis X (where $\Delta = X \cup \overline{X}$):

$$F(X) = \Delta^* / \{ a\overline{a} = \overline{a}a = 1 \mid a \in X \}$$

WP(F(X)) =two-sided Dyck language

Free groups

The free group with basis X (where $\Delta = X \cup \overline{X}$):

$$F(X) = \Delta^* / \{ a\overline{a} = \overline{a}a = 1 \mid a \in X \}$$

WP(F(X)) =two-sided Dyck language

PDA for WP(F(X)): when reading $a \in \Delta$:

```
if stack-top ≠ ā then
    push(a);
else
    pop;
```

endif

Virtually free = free subgroup of finite index

Virtually free = free subgroup of finite index

 \rightsquigarrow there are F free, Q finite, and a short exact sequence

 $1 \to F \to G \to Q \to 1.$

Virtually free = free subgroup of finite index

 \rightsquigarrow there are F free, Q finite, and a short exact sequence

 $1 \rightarrow F \rightarrow G \rightarrow Q \rightarrow 1.$

Virtually free presentation:

- generating set X of F,
- a system of representatives $R \subseteq G$ of Q ($\rightsquigarrow G = F \cdot R$)
- multiplication rules: for $q \in R$, $a \in R \cup X$ there are $f \in F$, $r \in R$ with

qa = fr.

Virtually free = free subgroup of finite index

 \rightsquigarrow there are F free, Q finite, and a short exact sequence

 $1 \rightarrow F \rightarrow G \rightarrow Q \rightarrow 1.$

Virtually free presentation:

- generating set X of F,
- a system of representatives $R \subseteq G$ of Q ($\rightsquigarrow G = F \cdot R$)
- multiplication rules: for $q \in R$, $a \in R \cup X$ there are $f \in F$, $r \in R$ with

qa = fr.

Example			
Let	$F = \mathbb{Z} = \langle x \rangle,$ ($Q=\mathbb{Z}/2\mathbb{Z},$	$R = \{1, a\}$
with rules	ax = x	a, aa = 1.	

Virtually free = free subgroup of finite index

 \rightsquigarrow there are F free, Q finite, and a short exact sequence

 $1 \rightarrow F \rightarrow G \rightarrow Q \rightarrow 1.$

Virtually free presentation:

Géraud Sénizergues, Armin Weiß

- generating set X of F,
- a system of representatives $R \subseteq G$ of Q ($\rightsquigarrow G = F \cdot R$)
- multiplication rules: for $q \in R$, $a \in R \cup X$ there are $f \in F$, $r \in R$ with

qa = fr.

Example	
Let	$F = \mathbb{Z} = \langle x \rangle, \qquad Q = \mathbb{Z}/2\mathbb{Z}, \qquad R = \{1, a\}$
with rules	ax = xa, $aa = 1$.
Every elem	ent can be written as $x^k a^{\varepsilon}$ with $k \in \mathbb{Z}$, $\varepsilon \in \{0, 1\}$.
_	

The isomorphism problem for finite extensions of free groups is in PSPACE

Example	
Let	$F = \mathbb{Z} = \langle x \rangle, \qquad Q = \mathbb{Z}/2\mathbb{Z}, \qquad R = \{1, a\}$
with rules	$ax = xa, \qquad aa = x.$

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $\dot{a} a x x a \overline{x} \overline{x} a \overline{x}$	
Stack:	
State: 1	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $\overrightarrow{a} x x a \overline{x} \overline{x} a \overline{x}$	
Stack:	
State: a	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $a {a} {x} x a \overline{x} \overline{x} a \overline{x}$	
Stack: x	
State: 1	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $a a \times x a \overline{x} \overline{x} a \overline{x}$	
Stack: xx	
State: 1	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $a a \times x \stackrel{*}{a} \overline{x} \overline{x} a \overline{x}$	
Stack: xxx	
State: 1	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $a a \times x a \overleftarrow{x} \overline{x} a \overline{x}$	
Stack: xxx	
State: a	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
nput: $a a x x a \overline{x} \overline{x} a \overline{x}$	
Stack: xx	
State: a	

Example	
Let	$F = \mathbb{Z} = \langle x \rangle, \qquad Q = \mathbb{Z}/2\mathbb{Z}, \qquad R = \{1, a\}$
with rules	$ax = xa, \qquad aa = x.$
PDA for the word problem:	
Input: a a x	$x \times a \overline{x} \overline{x}^* a \overline{x}$
Stack: 🗴	
State: a	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $a a x x a \overline{x} \overline{x} a \overline{\overline{x}}$	
Stack: xx	
State: 1	

Example	
Let $F = \mathbb{Z} = \langle x \rangle$,	$Q = \mathbb{Z}/2\mathbb{Z}, \qquad R = \{1, a\}$
with rules ax	$= xa, \qquad aa = x.$
PDA for the word problem:	
Input: $a a x x a \overline{x} \overline{x} a \overline{x}^{\dagger}$	
Stack: x	
State: 1	

PDA: given a word $w \in (X \cup \overline{X} \cup R)^*$, rewrite it as fr with $f \in F, r \in R$, keep f on the stack, r in the state.

Example	
Let $F = \mathbb{Z} = \langle x \rangle$, $Q = \mathbb{Z}/2\mathbb{Z}$, $R = \{1, a\}$	
with rules $ax = xa$, $aa = x$.	
PDA for the word problem:	
Input: $a a x x a \overline{x} \overline{x} a \overline{x}^*$	
Stack: x	
State: 1	

Theorem (Muller, Schupp, 1983)

A group is finitely generated virtually free iff it is context-free (the word problem is a context-free language).

$$1 \rightarrow F_i \rightarrow G_i \rightarrow Q_i \rightarrow 1$$



$$1 \rightarrow F_i \rightarrow G_i \rightarrow Q_i \rightarrow 1$$



$$1 \rightarrow F_i \rightarrow G_i \rightarrow Q_i \rightarrow 1$$



$$1 \rightarrow F_i \rightarrow G_i \rightarrow Q_i \rightarrow 1$$



Then $G_1 \cong G_3 \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (via $z \mapsto x$, $c \mapsto ax$) and $G_2 \cong \mathbb{Z}$.

Theorem (Krstić, 1989)

The isomorphism problem for virtually free groups is decidable (input: presentations with the promise to be virtually free).

Theorem (Krstić, 1989)

The isomorphism problem for virtually free groups is decidable (input: presentations with the promise to be virtually free).

Theorem (Sénizergues, 1993)

The isomorphism problem for virtually free groups is primitive recursive (input: virtually free presentation).

Theorem (Krstić, 1989)

The isomorphism problem for virtually free groups is decidable (input: presentations with the promise to be virtually free).

Theorem (Sénizergues, 1993)

The isomorphism problem for virtually free groups is primitive recursive (input: virtually free presentation).

Theorem (Sénizergues, 1996)

The isomorphism problem for context-free groups is primitive recursive (input: pda or c.f. grammar).

Theorem (Krstić, 1989)

The isomorphism problem for virtually free groups is decidable (input: presentations with the promise to be virtually free).

Theorem (Sénizergues, 1993)

The isomorphism problem for virtually free groups is primitive recursive (input: virtually free presentation).

Theorem (Sénizergues, 1996)

The isomorphism problem for context-free groups is primitive recursive (input: pda or c.f. grammar).

Theorem (S.,W.)

The isomorphism problem for virtually free groups is in PSPACE, for context-free groups it is in DSPACE($2^{2^{O(n)}}$).

7/13

A graph of groups \mathcal{G} is a connected graph Y = (V(Y), E(Y)) and

- for each vertex $P \in V(Y)$, a vertex group G_P ,
- 2) for each edge $y \in E(Y)$, an edge group G_y such that $G_y = G_{\overline{y}}$.

3 for each $y \in E(Y)$, an injective hom. from G_y to $G_{s(y)}$.

A graph of groups G is a connected graph Y = (V(Y), E(Y)) and

- for each vertex $P \in V(Y)$, a vertex group G_P ,
- **2** for each edge $y \in E(Y)$, an edge group G_y such that $G_y = G_{\overline{y}}$.
- **3** for each $y \in E(Y)$, an injective hom. from G_y to $G_{s(y)}$.

Definition (Fundamental group)

The fundamental group $\pi_1(\mathcal{G}, P)$ of a graph of groups \mathcal{G} over Y is the fundamental group of Y + elements of the respective vertex groups.

A graph of groups \mathcal{G} is a connected graph Y = (V(Y), E(Y)) and

- for each vertex $P \in V(Y)$, a vertex group G_P ,
- 2) for each edge $y \in E(Y)$, an edge group G_y such that $G_y = G_{\overline{y}}$.

3 for each $y \in E(Y)$, an injective hom. from G_y to $G_{s(y)}$.

Definition (Fundamental group)

The fundamental group $\pi_1(\mathcal{G}, P)$ of a graph of groups \mathcal{G} over Y is the fundamental group of Y + elements of the respective vertex groups.

Example

 F_m

$$G_{y_1} = \{1\}$$

 $G_{y_2} = \{1\}$
 \vdots
 $G_{y_m} = \{1\}$

8/13

A graph of groups \mathcal{G} is a connected graph Y = (V(Y), E(Y)) and

- for each vertex $P \in V(Y)$, a vertex group G_P ,
- 2) for each edge $y \in E(Y)$, an edge group G_y such that $G_y = G_{\overline{y}}$.

3 for each $y \in E(Y)$, an injective hom. from G_y to $G_{s(y)}$.

Definition (Fundamental group)

The fundamental group $\pi_1(\mathcal{G}, P)$ of a graph of groups \mathcal{G} over Y is the fundamental group of Y + elements of the respective vertex groups.

Example



 $\mathrm{PSL}(2,\mathbb{Z})\cong \mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/3\mathbb{Z}$

8/13

A graph of groups \mathcal{G} is a connected graph Y = (V(Y), E(Y)) and

- for each vertex $P \in V(Y)$, a vertex group G_P ,
- **2** for each edge $y \in E(Y)$, an edge group G_y such that $G_y = G_{\overline{y}}$.

3 for each $y \in E(Y)$, an injective hom. from G_y to $G_{s(y)}$.

Definition (Fundamental group)

The fundamental group $\pi_1(\mathcal{G}, P)$ of a graph of groups \mathcal{G} over Y is the fundamental group of Y + elements of the respective vertex groups.

Example

$$\fbox{(a)} G_y = \langle b \rangle$$

 $\mathsf{BS}_{p,q} = \left\langle a, y \mid ya^p y^{-1} = a^q \right\rangle$ with embeddings $b \mapsto a^p$ and $b \mapsto a^q$

A f. g. group is virtually free iff it is the fundamental group of a finite graph of groups with finite vertex groups.

A f. g. group is virtually free iff it is the fundamental group of a finite graph of groups with finite vertex groups.

Theorem (Guirardel, Levitt 07; Clay, Forester 09)

Let \mathcal{G}_1 and \mathcal{G}_2 be reduced finite graph of groups with finite vertex groups. Then $\pi_1(\mathcal{G}_1, \mathcal{P}_1) \cong \pi_1(\mathcal{G}_2, \mathcal{P}_2)$ iff \mathcal{G}_1 can be transformed into \mathcal{G}_2 by a sequence of slide moves.

A f. g. group is virtually free iff it is the fundamental group of a finite graph of groups with finite vertex groups.

Theorem (Guirardel, Levitt 07; Clay, Forester 09)

Let \mathcal{G}_1 and \mathcal{G}_2 be reduced finite graph of groups with finite vertex groups. Then $\pi_1(\mathcal{G}_1, \mathcal{P}_1) \cong \pi_1(\mathcal{G}_2, \mathcal{P}_2)$ iff \mathcal{G}_1 can be transformed into \mathcal{G}_2 by a sequence of slide moves.



Géraud Sénizergues, Armin Weiß The isomorphism problem for finite extensions of free groups is in PSPACE

A f. g. group is virtually free iff it is the fundamental group of a finite graph of groups with finite vertex groups.

Theorem (Guirardel, Levitt 07; Clay, Forester 09)

Let \mathcal{G}_1 and \mathcal{G}_2 be reduced finite graph of groups with finite vertex groups. Then $\pi_1(\mathcal{G}_1, \mathcal{P}_1) \cong \pi_1(\mathcal{G}_2, \mathcal{P}_2)$ iff \mathcal{G}_1 can be transformed into \mathcal{G}_2 by a sequence of slide moves.

Corollary

It can be decided in NSPACE(n) whether $\pi_1(\mathcal{G}_1, P_1) \cong \pi_1(\mathcal{G}_2, P_2)$ given two graph of groups \mathcal{G}_1 and \mathcal{G}_2 with finite vertex groups.

A f. g. group is virtually free iff it is the fundamental group of a finite graph of groups with finite vertex groups.

Theorem (Guirardel, Levitt 07; Clay, Forester 09)

Let \mathcal{G}_1 and \mathcal{G}_2 be reduced finite graph of groups with finite vertex groups. Then $\pi_1(\mathcal{G}_1, \mathcal{P}_1) \cong \pi_1(\mathcal{G}_2, \mathcal{P}_2)$ iff \mathcal{G}_1 can be transformed into \mathcal{G}_2 by a sequence of slide moves.

Corollary

It can be decided in NSPACE(n) whether $\pi_1(\mathcal{G}_1, P_1) \cong \pi_1(\mathcal{G}_2, P_2)$ given two graph of groups \mathcal{G}_1 and \mathcal{G}_2 with finite vertex groups.

Krstić's proof.

- For both input groups guess a gog + an isomorphism
- verify that the guesses are correct
- check the two gogs for isomorphism

New approach

Show that the gog and the isomorphism are "small".

- Guess a gog + an isomorphism.
- Check that the guess is correct.

New approach

Show that the gog and the isomorphism are "small".

- Guess a gog + an isomorphism.
- Check that the guess is correct.

Theorem (S.,W.)

The following problem is in NTIME($2^{2^{\mathcal{O}(n)}}$): Input: a c.f grammar for the word problem of a group G, Compute a gog \mathcal{G} with finite vertex groups and $\pi_1(\mathcal{G}, P) \cong G$

New approach

Show that the gog and the isomorphism are "small".

- Guess a gog + an isomorphism.
- Check that the guess is correct.

Theorem (S.,W.)

The following problem is in NTIME($2^{2^{\mathcal{O}(n)}}$): Input: a c.f grammar for the word problem of a group G, Compute a gog \mathcal{G} with finite vertex groups and $\pi_1(\mathcal{G}, P) \cong G$

Theorem (S.,W.)

The following problem is in NP: Input: a group G given as virtually free presentation, Compute a gog \mathcal{G} with finite vertex groups and $\pi_1(\mathcal{G}, P) \cong G$.

Main Lemma

Let G be given as context-free grammar of size $N \ge 4$ for its word problem. There is a graph of groups \mathcal{G} over Y and an isomorphism $\varphi : \pi_1(\mathcal{G}, T) \to G$ with

- $|V(Y)| \leq N^{50 \cdot 2^N},$
- $|G_P| \le N^{50 \cdot 2^N} \text{ for all } P \in V(Y),$
- $|\varphi(a)| \leq 24 \cdot N^{175 \cdot 2^N}$ for every $a \in \Delta =$ generating set of $\pi_1(\mathcal{G}, T)$.

Main Lemma

Let G be given as context-free grammar of size $N \ge 4$ for its word problem. There is a graph of groups \mathcal{G} over Y and an isomorphism $\varphi : \pi_1(\mathcal{G}, T) \to G$ with $|V(Y)| \le N^{50 \cdot 2^N}$, $|G_P| \le N^{50 \cdot 2^N}$ for all $P \in V(Y)$, $|\varphi(a)| \le 24 \cdot N^{175 \cdot 2^N}$ for every $a \in \Delta$ = generating set of $\pi_1(\mathcal{G}, T)$. $\rightsquigarrow 2^{2^{\mathcal{O}(N)}}$

Main Lemma

Let *G* be given as context-free grammar of size $N \ge 4$ for its word problem. There is a graph of groups *G* over *Y* and an isomorphism $\varphi : \pi_1(\mathcal{G}, T) \to G$ with $|V(Y)| \le N^{50 \cdot 2^N}$, $|G_P| \le N^{50 \cdot 2^N}$ for all $P \in V(Y)$, $|\varphi(a)| \le 24 \cdot N^{175 \cdot 2^N}$ for every $a \in \Delta$ = generating set of $\pi_1(\mathcal{G}, T)$. $\rightsquigarrow 2^{2^{\mathcal{O}(N)}}$

If G is given as virtually free presentation of size $M \ge 4$, then

- $|V(Y)| \leq M+1,$
- $|G_P| \leq M \text{ for all } P \in V(Y),$
- $|\varphi(a)| \leq 12(M+1)^6 \text{ for every } a \in \Delta.$

Main Lemma

Let *G* be given as context-free grammar of size $N \ge 4$ for its word problem. There is a graph of groups \mathcal{G} over *Y* and an isomorphism $\varphi : \pi_1(\mathcal{G}, T) \to G$ with $\bullet |V(Y)| \le N^{50 \cdot 2^N}$, $\bullet |G_P| \le N^{50 \cdot 2^N}$ for all $P \in V(Y)$, $\bullet |\varphi(a)| \le 24 \cdot N^{175 \cdot 2^N}$ for every $a \in \Delta$ = generating set of $\pi_1(\mathcal{G}, T)$. $\sim 2^{2^{\mathcal{O}(N)}}$

If G is given as virtually free presentation of size $M \ge 4$, then

$$|V(Y)| \leq M+1,$$

$$|G_P| \leq M \text{ for all } P \in V(Y),$$

•
$$|\varphi(a)| \leq 12(M+1)^6$$
 for every $a \in \Delta$

 $\rightsquigarrow M^{\mathcal{O}(1)}$

Virtually free groups are "tree-like"

Let $\Gamma(G)$ be the Cayley graph of a c.f. group G. Then:

• $\Gamma(G)$ is quasi-isometric to a tree



The Cayley graph of $\mathrm{PSL}(2,\mathbb{Z})\cong\mathbb{Z}/2\mathbb{Z}*\mathbb{Z}/3\mathbb{Z}$ has finite tree-width.

Virtually free groups are "tree-like"

Let $\Gamma(G)$ be the Cayley graph of a c.f. group G. Then:

- $\Gamma(G)$ is quasi-isometric to a tree
- $\Gamma(G)$ has finite tree width



Cuts = edges of the structure tree.

Virtually free groups are "tree-like"

Let $\Gamma(G)$ be the Cayley graph of a c.f. group G. Then:

- $\Gamma(G)$ is quasi-isometric to a tree
- $\Gamma(G)$ has finite tree width



Cuts = edges of the structure tree.

Key point for the main Lemma: bound size of cuts and "vertices"

- Bound the number of slide moves.
- Precise complexity of isomorphism of gogs (e.g. PSPACE complete)?

- Bound the number of slide moves.
- Precise complexity of isomorphism of gogs (e.g. PSPACE complete)?
- Isomorphism problem for context-free groups in EXPSPACE?
- Upper/lower bound for the size of finite subgroups of c.f. groups?

- Bound the number of slide moves.
- Precise complexity of isomorphism of gogs (e.g. PSPACE complete)?
- Isomorphism problem for context-free groups in EXPSPACE?
- Upper/lower bound for the size of finite subgroups of c.f. groups?

Thank you!