Subset sum problem in polycyclic groups

Andrey Nikolaev
(Stevens Institute of Technology)

GAGTA-10, June 14, 2016

Based on joint work with A.Ushakov

Non-commutative discrete optimization

Basic idea:

Take a classic algorithmic problem from computer science (traveling salesman, Post correspondence, knapsack, ...) and translate it into group-theoretic setting.

Example: Post correspondence problem

Let A be an alphabet, $|A| \geq 2$.

The classic Post correspondence problem (**PCP**)

Given a finite set of pairs $(g_1, h_1), \ldots, (g_k, h_k)$ of elements of A^* determine if there is a non-empty word $w(x_1, \ldots, x_k) \in X^*$ such that $w(g_1, \ldots, g_k) = w(h_1, \ldots, h_k)$ in A^*.

Example: Post correspondence problem

Matching dominoes: top = bottom

g_{i_1}	g_{i_2}	g_{i_3}	$\ldots$	g_{i_n}
h_{i_1}	h_{i_2}	h_{i_3}	$\ldots$	h_{i_n}

Decidable if number of pairs is $k \leq 2$.
Undecidable if $k \geq 5$ (T.Neary 2015).
Unknown if $3 \leq k \leq 4$.

Example: Post correspondence problem

Matching dominoes: top = bottom

g_{i_1}	g_{i_2}	g_{i_3}	$\ldots$	g_{i_n}
h_{i_1}	h_{i_2}	h_{i_3}	$\ldots$	h_{i_n}

Decidable if number of pairs is $k \leq 2$.
Undecidable if $k \geq 5$ (T.Neary 2015).
Unknown if $3 \leq k \leq 4$.

Example: Post correspondence problem

Variations of **PCP** in groups turn out to be closely related to:

- double-endo-twisted conjugacy problem
  (find $w \in G$ s.t. $uw^{\varphi} = w^{\psi}v$),
- equalizer problem
  (find the subgroup of elements g s.t. $\varphi(g) = \psi(g)$),
- hereditary word problem
  (word problem in any quotient of G by a subgroup f.g. as a normal subgroup).

Example: Post correspondence problem

Variations of **PCP** in groups turn out to be closely related to:

- double-endo-twisted conjugacy problem
  (find $w \in G$ s.t. $uw^{\varphi} = w^{\psi}v$),
- equalizer problem
  (find the subgroup of elements g s.t. $\varphi(g) = \psi(g)$),
- hereditary word problem
  (word problem in any quotient of G by a subgroup f.g. as a normal subgroup).

Example: Post correspondence problem

Variations of **PCP** in groups turn out to be closely related to:

- double-endo-twisted conjugacy problem
  (find $w \in G$ s.t. $uw^{\varphi} = w^{\psi}v$),
- equalizer problem
  (find the subgroup of elements g s.t. $\varphi(g) = \psi(g)$),
- hereditary word problem
  (word problem in any quotient of G by a subgroup f.g. as a normal subgroup).

Example: Post correspondence problem

Variations of **PCP** in groups turn out to be closely related to:

- double-endo-twisted conjugacy problem
  (find $w \in G$ s.t. $uw^{\varphi} = w^{\psi}v$),
- equalizer problem
  (find the subgroup of elements g s.t. $\varphi(g) = \psi(g)$),
- hereditary word problem
  (word problem in any quotient of G by a subgroup f.g. as a normal subgroup).

Example: Post correspondence problem

Variations of **PCP** in groups turn out to be closely related to:

- double-endo-twisted conjugacy problem
  (find $w \in G$ s.t. $uw^{\varphi} = w^{\psi}v$),
- equalizer problem
  (find the subgroup of elements g s.t. $\varphi(g) = \psi(g)$),
- hereditary word problem
  (word problem in any quotient of G by a subgroup f.g. as a normal subgroup).

Example: Post correspondence problem

Variations of **PCP** in groups turn out to be closely related to:

- double-endo-twisted conjugacy problem
  (find $w \in G$ s.t. $uw^{\varphi} = w^{\psi}v$),
- equalizer problem
  (find the subgroup of elements g s.t. $\varphi(g) = \psi(g)$),
- hereditary word problem
  (word problem in any quotient of G by a subgroup f.g. as a normal subgroup).

Example: Bounded submonoid membership problem

Bounded submonoid membership problem **BSMP**(G):

Given $g_1, \ldots, g_n, g \in G$ and $N \in \mathbb{N}$, decide if g can be expressed as

$$g = g_{i_1} \cdots g_{i_M}, \quad M \leq N.$$

There are hyperbolic groups where the membership problem is undecidable, but **BSMP**(G) is **P**-time for every hyperbolic G.

Example: Bounded submonoid membership problem

Bounded submonoid membership problem **BSMP**(G):

Given $g_1, \ldots, g_n, g \in G$ and $N \in \mathbb{N}$, decide if g can be expressed as

$$g = g_{i_1} \cdots g_{i_M}, \quad M \leq N.$$

There are hyperbolic groups where the membership problem is undecidable, but **BSMP**(G) is **P**-time for every hyperbolic G.

Example: Bounded submonoid membership problem

Bounded submonoid membership problem **BSMP**(G):

Given $g_1, \ldots, g_n, g \in G$ and $N \in \mathbb{N}$, decide if g can be expressed as

$$g = g_{i_1} \cdots g_{i_M}, \quad M \leq N.$$

There are hyperbolic groups where the membership problem is undecidable, but **BSMP**(G) is **P**-time for every hyperbolic G.

Subset sum problem

The classic subset sum problem (**SSP**):

Given $a_1, \ldots, a_k, a \in \mathbb{Z}$ decide if

$$\varepsilon_1 a_1 + \ldots + \varepsilon_k a_k = a$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

SSP for a group G:

Given $g_1, \ldots, g_k, g \in G$ decide if

$$g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

Elements in G are given as words in a fixed set of generators of G.

Subset sum problem

The classic subset sum problem (**SSP**):

Given $a_1, \ldots, a_k, a \in \mathbb{Z}$ decide if

$$\varepsilon_1 a_1 + \ldots + \varepsilon_k a_k = a$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

SSP for a group G:

Given $g_1, \ldots, g_k, g \in G$ decide if

$$g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

Elements in G are given as words in a fixed set of generators of G.

Subset sum problem

The classic subset sum problem (**SSP**):

Given $a_1, \ldots, a_k, a \in \mathbb{Z}$ decide if

$$\varepsilon_1 a_1 + \ldots + \varepsilon_k a_k = a$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

SSP for a group G:

Given $g_1, \ldots, g_k, g \in G$ decide if

$$g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k} = g$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

Elements in G are given as words in a fixed set of generators of G.

Algorithmic set-up

Classic **SSP** is pseudopolynomial

- If input is given in unary, **SSP** is in **P**,
- if input is given in binary, **SSP** is **NP**-complete.

The complexity of **SSP**(G) does not depend on a finite generating set, but may depend on a generating set if infinite ones are allowed.

For example:

SSP$(\mathbb{Z})$

- **SSP**$(\mathbb{Z}) \in$ **P** if $\mathbb{Z}$ is generated by $\{1\}$,
- **SSP**$(\mathbb{Z})$ is **NP**-complete if $\mathbb{Z}$ is generated by $\{2^n \mid n \in \mathbb{N}\}$.

Algorithmic set-up

Classic **SSP** is pseudopolynomial

- If input is given in unary, **SSP** is in **P**,
- if input is given in binary, **SSP** is **NP**-complete.

The complexity of **SSP**(G) does not depend on a finite generating set, but may depend on a generating set if infinite ones are allowed.

For example:

SSP$(\mathbb{Z})$

- **SSP**$(\mathbb{Z}) \in$ **P** if $\mathbb{Z}$ is generated by $\{1\}$,
- **SSP**$(\mathbb{Z})$ is **NP**-complete if $\mathbb{Z}$ is generated by $\{2^n \mid n \in \mathbb{N}\}$.

Algorithmic set-up

Classic **SSP** is pseudopolynomial

- If input is given in unary, **SSP** is in **P**,
- if input is given in binary, **SSP** is **NP**-complete.

The complexity of **SSP**(G) does not depend on a finite generating set, but may depend on a generating set if infinite ones are allowed.

For example:

SSP$(\mathbb{Z})$

- **SSP**$(\mathbb{Z}) \in$ **P** if $\mathbb{Z}$ is generated by $\{1\}$,
- **SSP**$(\mathbb{Z})$ is **NP**-complete if $\mathbb{Z}$ is generated by $\{2^n \mid n \in \mathbb{N}\}$.

SSP in groups. Initial results

Complexity of **SSP**(G) (A.Myasnikov, A.N., A.Ushakov. Knapsack problems in groups):

Group	Complexity	Why
Virt. nilpotent	**P**	Poly growth
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-complete	$\mathbb{Z}^\omega$, **ZOE**
Free metabelian	**NP**-complete	$\mathbb{Z} \wr \mathbb{Z}$
Thompson's F	**NP**-complete	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1, p)$	**NP**-complete	Binary **SSP**($\mathbb{Z}$)
Hyperbolic	**P**	Log depth

Note that the **NP**-completeness is despite unary input.

SSP in groups. Initial results

Complexity of **SSP**(G) (A.Myasnikov, A.N., A.Ushakov. Knapsack problems in groups):

Group	Complexity	Why
Virt. nilpotent	**P**	Poly growth
$\mathbb{Z} \wr \mathbb{Z}$	**NP**-complete	$\mathbb{Z}^\omega$, **ZOE**
Free metabelian	**NP**-complete	$\mathbb{Z} \wr \mathbb{Z}$
Thompson's F	**NP**-complete	$\mathbb{Z} \wr \mathbb{Z}$
$BS(1, p)$	**NP**-complete	Binary **SSP**($\mathbb{Z}$)
Hyperbolic	**P**	Log depth

Note that the **NP**-completeness is despite unary input.

SSP in groups. Initial results

Polynomial time solution to **SSP** in virtually nilpotent groups.

Given input $g_1, \ldots, g_k, g$, build lists of elements that can be represented as

$$g_1^{\varepsilon_1},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3},$$
$$\ldots,$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_k^{\varepsilon_k}.$$

Each list is polynomial size by polynomial growth.

SSP in groups. Initial results

Polynomial time solution to **SSP** in virtually nilpotent groups.

Given input $g_1, \ldots, g_k, g$, build lists of elements that can be represented as

$$g_1^{\varepsilon_1},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3},$$
$$\ldots,$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_k^{\varepsilon_k}.$$

Each list is polynomial size by polynomial growth.

SSP in groups. Initial results

Polynomial time solution to **SSP** in virtually nilpotent groups.

Given input $g_1, \ldots, g_k, g$, build lists of elements that can be represented as

$$g_1^{\varepsilon_1},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3},$$
$$\ldots,$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_k^{\varepsilon_k}.$$

Each list is polynomial size by polynomial growth.

SSP in groups. Initial results

Polynomial time solution to **SSP** in virtually nilpotent groups.

Given input $g_1, \ldots, g_k, g$, build lists of elements that can be represented as

$$g_1^{\varepsilon_1},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2},$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3},$$
$$\ldots,$$
$$g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_k^{\varepsilon_k}.$$

Each list is polynomial size by polynomial growth.

SSP in groups. Initial results

Polynomial time solution to **SSP** in virtually nilpotent groups.

Given input $g_1, \ldots, g_k, g$, build lists of elements that can be represented as

$$
\begin{aligned}
& g_1^{\varepsilon_1}, \\
& g_1^{\varepsilon_1} g_2^{\varepsilon_2}, \\
& g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3}, \\
& \ldots, \\
& g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_k^{\varepsilon_k}.
\end{aligned}
$$

Each list is polynomial size by polynomial growth.

SSP in groups. Initial results

Polynomial time solution to **SSP** in virtually nilpotent groups.

Given input $g_1, \ldots, g_k, g$, build lists of elements that can be represented as

$$
\begin{aligned}
& g_1^{\varepsilon_1}, \\
& g_1^{\varepsilon_1} g_2^{\varepsilon_2}, \\
& g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3}, \\
& \ldots, \\
& g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \cdots g_k^{\varepsilon_k}.
\end{aligned}
$$

Each list is polynomial size by polynomial growth.

SSP in groups. Initial results

NP-completeness of **SSP** in $BS(1,2)$.

$BS(1,2) = \langle a, t \mid a^t = a^2 \rangle$.

The subgroup $\langle a \rangle$ is exponentially distorted,

$$\underbrace{a^{t^n}}_{2n+1} = \underbrace{a^{2^n}}_{2^n}.$$

Encode classic binary **SSP** by elements of the form

$$g_i = a^{t^{n_1}} a^{t^{n_2}} \cdots a^{t^{n_m}}.$$

SSP in groups. Initial results

NP-completeness of **SSP** in $BS(1,2)$.

$BS(1,2) = \langle a, t \mid a^t = a^2 \rangle$.

The subgroup $\langle a \rangle$ is exponentially distorted,

$$\underbrace{a^{t^n}}_{2n+1} = \underbrace{a^{2^n}}_{2^n}.$$

Encode classic binary **SSP** by elements of the form

$$g_i = a^{t^{n_1}} a^{t^{n_2}} \cdots a^{t^{n_m}}.$$

SSP in groups. Recent results

E.Frenkel, A.N., A.Ushakov; M.Lohrey, G.Zetzshe.
Behavior of **SSP** under group-theoretic constructions.

A.Treyer, A.Mishchenko.
SSP in lamplighter groups is **NP**-complete.

D.König, M.Lohrey, G.Zetzsche.
SSP in virtually nilpotent groups is **NL**-complete.
There is a polycyclic group with **NP**-complete **SSP**.

SSP in groups. Recent results

E.Frenkel, A.N., A.Ushakov; M.Lohrey, G.Zetzshe.
Behavior of **SSP** under group-theoretic constructions.

A.Treyer, A.Mishchenko.
SSP in lamplighter groups is **NP**-complete.

D.König, M.Lohrey, G.Zetzsche.
SSP in virtually nilpotent groups is **NL**-complete.
There is a polycyclic group with **NP**-complete **SSP**.

SSP in groups. Recent results

E.Frenkel, A.N., A.Ushakov; M.Lohrey, G.Zetzshe.
Behavior of **SSP** under group-theoretic constructions.

A.Treyer, A.Mishchenko.
SSP in lamplighter groups is **NP**-complete.

D.König, M.Lohrey, G.Zetzsche.
SSP in virtually nilpotent groups is **NL**-complete.
There is a polycyclic group with **NP**-complete **SSP**.

SSP in groups. Recent results

E.Frenkel, A.N., A.Ushakov; M.Lohrey, G.Zetzshe.
Behavior of **SSP** under group-theoretic constructions.

A.Treyer, A.Mishchenko.
SSP in lamplighter groups is **NP**-complete.

D.König, M.Lohrey, G.Zetzsche.
SSP in virtually nilpotent groups is **NL**-complete.
There is a polycyclic group with **NP**-complete **SSP**.

Main result

What about other polycyclic groups?

Idea: a polycyclic group is either virtually nilpotent or has exponential distortion.

Theorem (A.N., A.Ushakov)

Let G be a polyclic group. Then **SSP**(G) *is* **NP***-complete if and only if G is not virtually nilpotent.*

Since polycyclic groups are linear, it suffices to prove **NP**-hardness.

Main result

What about other polycyclic groups?

Idea: a polycyclic group is either virtually nilpotent or has exponential distortion.

Theorem (A.N., A.Ushakov)

Let G be a polyclic group. Then **SSP**(G) *is* **NP***-complete if and only if G is not virtually nilpotent.*

Since polycyclic groups are linear, it suffices to prove **NP**-hardness.

Main result

What about other polycyclic groups?

Idea: a polycyclic group is either virtually nilpotent or has exponential distortion.

Theorem (A.N., A.Ushakov)

Let G be a polyclic group. Then $\mathbf{SSP}(G)$ *is* **NP***-complete if and only if G is not virtually nilpotent.*

Since polycyclic groups are linear, it suffices to prove **NP**-hardness.

Main result

What about other polycyclic groups?

Idea: a polycyclic group is either virtually nilpotent or has exponential distortion.

Theorem (A.N., A.Ushakov)

Let G be a polyclic group. Then $\mathbf{SSP}(G)$ *is* **NP***-complete if and only if G is not virtually nilpotent.*

Since polycyclic groups are linear, it suffices to prove **NP**-hardness.

Proof of main result. Case $\mathbb{Z} \ltimes \mathbb{Z}^n$

Consider $G = \mathbb{Z} \ltimes \mathbb{Z}^n = \langle h \rangle \ltimes \langle e_1, \ldots, e_n \rangle$.

Let h act by conjugation via matrix $M \in GL_n(\mathbb{Z})$.

Observation: G is not virtually nilpotent if and only if M has an eigenvalue $|\alpha| > 1$.

For any constant $\lambda > 0$, there is a power $\hat{h}$ of h and group elements $v_1, \ldots, v_k, \ldots \in \mathbb{Z}^n$,

$$v_k = \hat{h}^{-k} e_{i_k} \hat{h}^k,$$

such that $\|v_{k+1}\| > \lambda \|v_k\|$.

Proof of main result. Reduction of **ZOE**

Zero-one equation problem (exact set cover problem).

Given an $N \times N$ matrix A of 0 and 1, decide if there is a column X of 0 and 1 s.t. $AX = 1^N$, where $1^N = (1, \ldots, 1)$ is a column of 1s.

Reduce **ZOE** to **SSP**$(\langle g \rangle \ltimes \mathbb{Z}^n)$ as follows.

Given A and b, pick sufficiently large λ and encode each coordinate $1 \leq k \leq N$ by v_k. For example,

$$\text{column } 010011 \leftrightarrow v_2 v_5 v_6.$$

Proof of main result. Reduction of **ZOE**

Zero-one equation problem (exact set cover problem).

Given an $N \times N$ matrix A of 0 and 1, decide if there is a column X of 0 and 1 s.t. $AX = 1^N$, where $1^N = (1, \ldots, 1)$ is a column of 1s.

Reduce **ZOE** to **SSP**$(\langle g \rangle \ltimes \mathbb{Z}^n)$ as follows.

Given A and b, pick sufficiently large λ and encode each coordinate $1 \leq k \leq N$ by v_k. For example,

$$\text{column } 010011 \leftrightarrow v_2 v_5 v_6.$$

Proof of main result. Reduction of **ZOE**

More precisely, for

$$A = \begin{bmatrix} a_{11} & \dots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \dots & a_{NN} \end{bmatrix}$$

consider the instance $(g_1, \dots, g_N, g)$ of **SSP**(G), where:

$$g_i = v_1^{a_{1i}} \dots v_N^{a_{Ni}} \quad \text{and} \quad g = v_1 \dots v_N.$$

Since $\|v_{k+1}\| > \lambda \|v_k\|$, this instance of **SSP** is equivalent to the given instance of **ZOE**.

Proof of main result. Reduction of **ZOE**

More precisely, for

$$A = \begin{bmatrix} a_{11} & \dots & a_{1N} \\ \vdots & & \vdots \\ a_{N1} & \dots & a_{NN} \end{bmatrix}$$

consider the instance $(g_1, \dots, g_N, g)$ of $\mathbf{SSP}(G)$, where:

$$g_i = v_1^{a_{1i}} \dots v_N^{a_{Ni}} \quad \text{and} \quad g = v_1 \dots v_N.$$

Since $\|v_{k+1}\| > \lambda \|v_k\|$, this instance of **SSP** is equivalent to the given instance of **ZOE**.

Proof of main result. General case

Let G by polycyclic and F its Fitting (maximal nilpotent) subgroup. Suffices to assume $G = \langle h \rangle \ltimes F$.

Terms of lower central series for F are fully invariant, thus normal in G, so h acts by conjugation on abelian quotients F_j/F_{j+1}, say with matrix M_j.

Fact. G is not virtually nilpotent if and only if one of M_j has eigenvalue $|\alpha| > 1$.

Proof of main result. General case

Let G by polycyclic and F its Fitting (maximal nilpotent) subgroup. Suffices to assume $G = \langle h \rangle \ltimes F$.

Terms of lower central series for F are fully invariant, thus normal in G, so h acts by conjugation on abelian quotients F_j/F_{j+1}, say with matrix M_j.

Fact. G is not virtually nilpotent if and only if one of M_j has eigenvalue $|\alpha| > 1$.

Proof of main result. General case

Let G by polycyclic and F its Fitting (maximal nilpotent) subgroup. Suffices to assume $G = \langle h \rangle \ltimes F$.

Terms of lower central series for F are fully invariant, thus normal in G, so h acts by conjugation on abelian quotients F_j/F_{j+1}, say with matrix M_j.

Fact. G is not virtually nilpotent if and only if one of M_j has eigenvalue $|\alpha| > 1$.

Proof of main result. General case

Have: reduction of **ZOE** to **SSP**($\langle h \rangle \ltimes F_j/F_{j+1}$).
Want: reduction of **ZOE** to **SSP**($\langle h \rangle \ltimes F_j$).

In terms of a specific instance:
Have:

$$g_{i_1}^{\varepsilon_{i_1}} \cdots g_{i_N}^{\varepsilon_{i_N}} = g.$$

Want:

$$g_1^{\varepsilon_1} \cdots g_N^{\varepsilon_N} = g.$$

Proof of main result. General case

Have: reduction of **ZOE** to **SSP**$(\langle h \rangle \ltimes F_j/F_{j+1})$.
Want: reduction of **ZOE** to **SSP**$(\langle h \rangle \ltimes F_j)$.

In terms of a specific instance:

Have:

$$g_{i_1}^{\varepsilon_{i_1}} \cdots g_{i_N}^{\varepsilon_{i_N}} = g.$$

Want:

$$g_1^{\varepsilon_1} \cdots g_N^{\varepsilon_N} = g.$$

Proof of main result. General case

Have: reduction of **ZOE** to **SSP**$(\langle h \rangle \ltimes F_j/F_{j+1})$.
Want: reduction of **ZOE** to **SSP**$(\langle h \rangle \ltimes F_j)$.

In terms of a specific instance:
Have:

$$g_{i_1}^{\varepsilon_{i_1}} \cdots g_{i_N}^{\varepsilon_{i_N}} = g.$$

Want:

$$g_1^{\varepsilon_1} \cdots g_N^{\varepsilon_N} = g.$$

Proof of main result. General case

Luckily, g_i are in *nilpotent* F, so we can rearrange

$$g = g_{i_1}^{\varepsilon_{i_1}} \cdots g_{i_N}^{\varepsilon_{i_N}} = g_1^{\varepsilon_1} \cdots g_N^{\varepsilon_N} \cdot [g_1, g_2]^{n_1} \cdots [g_{N-1}, g_N, \ldots, g_N]^{n_\ell}$$

at the cost of adding iterated commutators. By properties of nilpotent groups, ℓ and all n_i are only polynomially large.

Proof of main result. General case

Ultimately, for a given instance of **ZOE**, an equivalent instance of **SSP**(G) is

$$g_1, \ldots, g_N, \underbrace{f_1, \ldots, f_1}_{P(N)}, \underbrace{f_1^{-1}, \ldots, f_1^{-1}}_{P(N)}, \ldots, \underbrace{f_\ell, \ldots, f_\ell}_{P(N)}, \underbrace{f_\ell^{-1}, \ldots, f_\ell^{-1}}_{P(N)}, g,$$

where g_i, g are as described above, f_i are iterated commutators of g_i, and $P(N)$ is a polynomial in N.

What's next

- **SSP**(Metabelian),
- **SSP**(Solvable),
- **SSP**(Grigorchuk′s).

What's next

- **SSP**(Metabelian),
- **SSP**(Solvable),
- **SSP**(Grigorchuk's).

What's next

- **SSP**(Metabelian),
- **SSP**(Solvable),
- **SSP**(Grigorchuk′s).