Knapsack in Graph Groups, HNN-Extensions and Amalgamated Products

Markus Lohrey\textsuperscript{1} \hspace{1cm} Georg Zetzsche\textsuperscript{2}

\textsuperscript{1}Department für Elektrotechnik und Informatik
Universität Siegen

\textsuperscript{2}LSV, CNRS & ENS Cachan
Université Paris-Saclay

Equations and formal languages in algebra
Les Diablerets 2016
Theorem

For every virtually special group, compressed knapsack is in NP.

- virtually special: finite extension of a subgroup of a right-angled Artin group
- compressed knapsack: equation $g_1^{x_1} \cdots g_k^{x_k} = g$, where $g_1, \ldots, g_k, g$ are given by SLPs over $\Sigma \cup \Sigma^{-1}$. 
Theorem

For every virtually special group, compressed knapsack is in NP.

- virtually special: finite extension of a subgroup of a right-angled Artin group
- compressed knapsack: equation $g_1^{x_1} \cdots g_k^{x_k} = g$, where $g_1, \ldots, g_k, g$
  are given by SLPs over $\Sigma \cup \Sigma^{-1}$.

Definition

Let $A$ be an alphabet and $I \subseteq A \times A$ be irreflexive and symmetric.
Theorem

For every virtually special group, compressed knapsack is in NP.

- virtually special: finite extension of a subgroup of a right-angled Artin group
- compressed knapsack: equation \( g_1^{x_1} \cdots g_k^{x_k} = g \), where \( g_1, \ldots, g_k, g \) are given by SLPs over \( \Sigma \cup \Sigma^{-1} \).

Definition

Let \( A \) be an alphabet and \( I \subseteq A \times A \) be irreflexive and symmetric. The group \( \mathbb{G}(A, I) \) is defined as

\[
\mathbb{G}(A, I) = \langle A \mid ab = ba \ ((a, b) \in I) \rangle.
\]
**Theorem**

*For every virtually special group, compressed knapsack is in NP.*

- virtually special: finite extension of a subgroup of a right-angled Artin group
- compressed knapsack: equation $g_1^{x_1} \cdots g_k^{x_k} = g$, where $g_1, \ldots, g_k, g$ are given by SLPs over $\Sigma \cup \Sigma^{-1}$.

**Definition**

Let $A$ be an alphabet and $I \subseteq A \times A$ be irreflexive and symmetric. The group $G(A, I)$ is defined as

$$G(A, I) = \langle A \mid ab = ba \ ((a, b) \in I) \rangle.$$  

Groups of the form $G(A, I)$ are called *right-angled Artin group.*
Semilinear sets

- A subset of $\mathbb{N}^k$ of the form

$$L = \left\{ v_0 + \sum_{i=1}^{n} x_i v_i \middle| x_1, \ldots, x_n \in \mathbb{N} \right\}$$

with $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ is called linear.
Semilinear sets

A subset of $\mathbb{N}^k$ of the form

$$L = \left\{ v_0 + \sum_{i=1}^{n} x_i v_i \mid x_1, \ldots, x_n \in \mathbb{N} \right\}$$

with $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ is called **linear**.

A subset of $\mathbb{N}^k$ is **semilinear** if it is a finite union of linear sets.
Semilinear sets

- A subset of $\mathbb{N}^k$ of the form

$$L = \left\{ v_0 + \sum_{i=1}^{n} x_i v_i \mid x_1, \ldots, x_n \in \mathbb{N} \right\}$$

with $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ is called linear.

- A subset of $\mathbb{N}^k$ is semilinear if it is a finite union of linear sets.

Examples: non-negative solutions of linear diophantine equations
Semilinear sets

- A subset of $\mathbb{N}^k$ of the form

$$L = \left\{ v_0 + \sum_{i=1}^{n} x_i v_i \mid x_1, \ldots, x_n \in \mathbb{N} \right\}$$

with $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ is called linear.

- A subset of $\mathbb{N}^k$ is semilinear if it is a finite union of linear sets.

Examples: non-negative solutions of linear diophantine equations

Theorem (Ginsburg-Spanier 1966)

A set is semilinear if and only if it is first-order definable in $(\mathbb{N}, +, \geq, 0)$. 
Semilinear sets

- A subset of $\mathbb{N}^k$ of the form

$$L = \left\{ v_0 + \sum_{i=1}^{n} x_i v_i \;\mid\; x_1, \ldots, x_n \in \mathbb{N} \right\}$$

with $v_0, v_1, \ldots, v_n \in \mathbb{N}^k$ is called linear.

- A subset of $\mathbb{N}^k$ is semilinear if it is a finite union of linear sets.

Examples: non-negative solutions of linear diophantine equations

**Theorem (Ginsburg-Spanier 1966)**

A set is semilinear if and only if it is first-order definable in $(\mathbb{N}, +, \geq, 0)$.

Equivalence is effective $\rightarrow$ decidability
Theorem

Let $u_1, u_2, \ldots, u_n \in \mathbb{G}(A, I) \setminus \{1\}$, $v_0, v_1, \ldots, v_n \in \mathbb{G}(A, I)$ and let $x_1, \ldots, x_n$ be variables ranging over $\mathbb{N}$. Then, the set of solutions of the exponent equation

$$v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_n^{x_n} v_n = 1$$

is semilinear.
Theorem

Let \( u_1, u_2, \ldots, u_n \in \mathbb{G}(A, l) \setminus \{1\} \), \( v_0, v_1, \ldots, v_n \in \mathbb{G}(A, l) \) and let \( x_1, \ldots, x_n \) be variables ranging over \( \mathbb{N} \). Then, the set of solutions of the exponent equation

\[
v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_n^{x_n} v_n = 1
\]

is semilinear. Moreover, if there is a solution, then there is a solution where the \( x_i \) are exponential in the size of SLPs for \( u_1, u_2, \ldots, u_n, v_0, v_1, \ldots, v_n \).
Theorem

Let $u_1, u_2, \ldots, u_n \in \mathbb{G}(A, I) \setminus \{1\}$, $\nu_0, \nu_1, \ldots, \nu_n \in \mathbb{G}(A, I)$ and let $x_1, \ldots, x_n$ be variables ranging over $\mathbb{N}$. Then, the set of solutions of the exponent equation

$$\nu_0 u_1^{x_1} \nu_1 u_2^{x_2} \nu_2 \cdots u_n^{x_n} \nu_n = 1$$

is semilinear. Moreover, if there is a solution, then there is a solution where the $x_i$ are exponential in the size of SLPs for $u_1, u_2, \ldots, u_n, \nu_0, \nu_1, \ldots, \nu_n$.

Algorithm for compressed knapsack

- Consider right-angled Artin groups
**Theorem**

Let $u_1, u_2, \ldots, u_n \in \mathbb{G}(A, I) \setminus \{1\}$, $v_0, v_1, \ldots, v_n \in \mathbb{G}(A, I)$ and let $x_1, \ldots, x_n$ be variables ranging over $\mathbb{N}$. Then, the set of solutions of the exponent equation

$$v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_n^{x_n} v_n = 1$$

is semilinear. Moreover, if there is a solution, then there is a solution where the $x_i$ are exponential in the size of SLPs for $u_1, u_2, \ldots, u_n, v_0, v_1, \ldots, v_n$.

**Algorithm for compressed knapsack**

- Consider right-angled Artin groups
- Guess binary representation of solution of $g_1^{x_1} \cdots g_k^{x_k} = g$
Theorem

Let $u_1, u_2, \ldots, u_n \in \mathbb{G}(A, I) \setminus \{1\}$, $v_0, v_1, \ldots, v_n \in \mathbb{G}(A, I)$ and let $x_1, \ldots, x_n$ be variables ranging over $\mathbb{N}$. Then, the set of solutions of the exponent equation

$$v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_n^{x_n} v_n = 1$$

is semilinear. Moreover, if there is a solution, then there is a solution where the $x_i$ are exponential in the size of SLPs for $u_1, u_2, \ldots, u_n, v_0, v_1, \ldots, v_n$.

Algorithm for compressed knapsack

- Consider right-angled Artin groups
- Guess binary representation of solution of $g_1^{x_1} \cdots g_k^{x_k} = g$
- Construct an SLP for $g_1^{x_1} \cdots g_k^{x_k} g^{-1}$
Theorem

Let \( u_1, u_2, \ldots, u_n \in \mathbb{G}(A, I) \setminus \{1\} \), \( \nu_0, \nu_1, \ldots, \nu_n \in \mathbb{G}(A, I) \) and let \( x_1, \ldots, x_n \) be variables ranging over \( \mathbb{N} \). Then, the set of solutions of the exponent equation

\[
\nu_0 u_1^{x_1} \nu_1 u_2^{x_2} \nu_2 \cdots u_n^{x_n} \nu_n = 1
\]

is semilinear. Moreover, if there is a solution, then there is a solution where the \( x_i \) are exponential in the size of SLPs for \( u_1, u_2, \ldots, u_n, \nu_0, \nu_1, \ldots, \nu_n \).

Algorithm for compressed knapsack

- Consider right-angled Artin groups
- Guess binary representation of solution of \( g_1^{x_1} \cdots g_k^{x_k} = g \)
- Construct an SLP for \( g_1^{x_1} \cdots g_k^{x_k} g^{-1} \)
- Lohrey and Schleimer (2007): compressed word problem for each right-angled Artin group in P.
Trace monoids

**Definition**

- Let $A$ be an alphabet and $I \subseteq A \times A$ irreflexive and symmetric.

- The trace monoid $M_p A, I_q$ is defined as $M_p A, I_q := A \hat{\sim} \{\}^I$.

- $I$ denotes the congruence class of $u \in A \hat{\sim} \{\}$.

- We consider $M_p A, I_q$, where $A = \{\alpha \, | \, \alpha \notin A\}$, $I = \{a \hat{=}_I b \, | \, a, b \in A \hat{\sim} \{\}$.
Trace monoids

Definition

- Let $A$ be an alphabet and $I \subseteq A \times A$ irreflexive and symmetric.
- Let $\equiv_I$ be the smallest congruence on $A^*$ with $ab \equiv_I ba$ for all $(a, b) \in I$. 

Lohrey, Zetzsche (Uni Siegen, LSV Cachan) 
Knapsack in Graph Groups 
Les Diablerets 2016 5 / 13
Trace monoids

Definition

- Let $A$ be an alphabet and $I \subseteq A \times A$ irreflexive and symmetric.
- Let $\equiv_I$ be the smallest congruence on $A^*$ with $ab \equiv_I ba$ for all $(a, b) \in I$.
- The *trace monoid* $\mathbb{M}(A, I)$ is defined as

$$\mathbb{M}(A, I) = A^*/\equiv_I.$$
Trace monoids

**Definition**

- Let $A$ be an alphabet and $I \subseteq A \times A$ irreflexive and symmetric.
- Let $\equiv_I$ be the smallest congruence on $A^*$ with $ab \equiv_I ba$ for all $(a, b) \in I$.
- The *trace monoid* $\mathbb{M}(A, I)$ is defined as
  \[ \mathbb{M}(A, I) = A^*/\equiv_I. \]
- $[u]_I$ denotes the congruence class of $u \in A^*$. 

Lohrey, Zetzsche (Uni Siegen, LSV Cachan)  
Knapsack in Graph Groups  
Les Diablerets 2016 5 / 13
Definition

- Let $A$ be an alphabet and $I \subseteq A \times A$ irreflexive and symmetric.
- Let $\equiv_I$ be the smallest congruence on $A^*$ with $ab \equiv_I ba$ for all $(a, b) \in I$.
- The trace monoid $\mathbb{M}(A, I)$ is defined as
  \[ \mathbb{M}(A, I) = A^*/\equiv_I. \]
- $[u]_I$ denotes the congruence class of $u \in A^*$.
- We consider $\mathbb{M}(A^{\pm 1}, I^{\pm 1})$, where
  \[ A^{\pm 1} = \{a^+, a^- | a \in A\}, \quad I^{\pm} = \{(a^{\pm 1}, b^{\pm 1}) | (a, b) \in I\}. \]
Trace monoids

Definition

- Let $A$ be an alphabet and $I \subseteq A \times A$ irreflexive and symmetric.
- Let $\equiv_I$ be the smallest congruence on $A^*$ with $ab \equiv_I ba$ for all $(a, b) \in I$.
- The trace monoid $\mathbb{M}(A, I)$ is defined as
  \[
  \mathbb{M}(A, I) = A^*/\equiv_I.
  \]
- $[u]_I$ denotes the congruence class of $u \in A^*$.
- We consider $\mathbb{M}(A^{\pm1}, I^{\pm1})$, where
  \[
  A^{\pm1} = \{a^+, a^{-1} \mid a \in A\}, \quad I^{\pm} = \{(a^{\pm1}, b^{\pm1}) \mid (a, b) \in I\}.
  \]
- A trace $t$ is irreducible if there is no decomposition $t = [u a a^{-1} v]_I$ for $a \in A^{\pm1}, u, v \in (A^{\pm1})^*$. 
We call a trace $t$ connected if there is no factorization $t = uv$ with $u \neq 1 \neq v$ and $ulv$. 
We call a trace $t$ connected if there is no factorization $t = uv$ with $u \neq 1 \neq v$ and $ulv$. 
We call a trace $t$ connected if there is no factorization $t = uv$ with $u \neq 1 \neq v$ and $ulv$.

**Lemma**

Fix the alphabet $A$. Let $p, q, u, v, s, t \in \mathbb{M}(A, l)$ with $u \neq 1$ and $v \neq 1$ connected. Then the set

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pu^x s = qv^y t\}$$

is semilinear.
We call a trace $t$ connected if there is no factorization $t = uv$ with $u \neq 1 \neq v$ and $ulv$.

**Lemma**

*Fix the alphabet $A$. Let $p, q, u, v, s, t \in \mathbb{M}(A, I)$ with $u \neq 1$ and $v \neq 1$ connected. Then the set*

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pu^x s = qv^y t\}$$

*is semilinear.*

- Techniques from recognizable trace languages:
- Construct finite automaton for $[pu^*s]_I \cap [qv^*t]_I$. 

Lohrey, Zetzsche (Uni Siegen, LSV Cachan) 
Knapsack in Graph Groups 
Les Diablerets 2016
**Lemma**

Let \( u_1, \ldots, u_m, v_1, \ldots, v_n \in \mathbb{M}(A, l) \). Then \( u_1 u_2 \cdots u_m = v_1 v_2 \cdots v_n \) if and only if there exist \( w_{i,j} \in \mathbb{M}(A, l) \) \((1 \leq i \leq m, 1 \leq j \leq n)\) such that

- \( u_i = w_{i,1} w_{i,2} \cdots w_{i,n} \) for every \( 1 \leq i \leq m \),
- \( v_j = w_{1,j} w_{2,j} \cdots w_{m,j} \) for every \( 1 \leq j \leq n \), and
- \((w_{i,j}, w_{k,l}) \in l \) if \( 1 \leq i < k \leq m \) and \( n \geq j > l \geq 1 \).

<table>
<thead>
<tr>
<th>( v_n )</th>
<th>( w_{1,n} )</th>
<th>( w_{2,n} )</th>
<th>( w_{3,n} )</th>
<th>( \ldots )</th>
<th>( w_{m,n} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( v_3 )</td>
<td>( w_{1,3} )</td>
<td>( w_{2,3} )</td>
<td>( w_{3,3} )</td>
<td>( \ldots )</td>
<td>( w_{m,3} )</td>
</tr>
<tr>
<td>( v_2 )</td>
<td>( w_{1,2} )</td>
<td>( w_{2,2} )</td>
<td>( w_{3,2} )</td>
<td>( \ldots )</td>
<td>( w_{m,2} )</td>
</tr>
<tr>
<td>( v_1 )</td>
<td>( w_{1,1} )</td>
<td>( w_{2,1} )</td>
<td>( w_{3,1} )</td>
<td>( \ldots )</td>
<td>( w_{m,1} )</td>
</tr>
<tr>
<td></td>
<td>( u_1 )</td>
<td>( u_2 )</td>
<td>( u_3 )</td>
<td>( \ldots )</td>
<td>( u_m )</td>
</tr>
</tbody>
</table>
Levi’s Lemma

Lemma

Let \( u_1, \ldots, u_m, v_1, \ldots, v_n \in \mathbb{M}(A, I) \). Then \( u_1 u_2 \cdots u_m = v_1 v_2 \cdots v_n \) if and only if there exist \( w_{i,j} \in \mathbb{M}(A, I) \) (\( 1 \leq i \leq m, 1 \leq j \leq n \)) such that

- \( u_i = w_{i,1} w_{i,2} \cdots w_{i,n} \) for every \( 1 \leq i \leq m \),
- \( v_j = w_{1,j} w_{2,j} \cdots w_{m,j} \) for every \( 1 \leq j \leq n \), and
- \((w_{i,j}, w_{k,\ell}) \in I\) if \( 1 \leq i < k \leq m \) and \( n \geq j > \ell \geq 1 \).

<table>
<thead>
<tr>
<th>( v_n )</th>
<th>( w_{1,n} )</th>
<th>( w_{2,n} )</th>
<th>( w_{3,n} )</th>
<th>( \ldots )</th>
<th>( w_{m,n} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( v_3 )</td>
<td>( w_{1,3} )</td>
<td>( w_{2,3} )</td>
<td>( w_{3,3} )</td>
<td>( \ldots )</td>
<td>( w_{m,3} )</td>
</tr>
<tr>
<td>( v_2 )</td>
<td>( w_{1,2} )</td>
<td>( w_{2,2} )</td>
<td>( w_{3,2} )</td>
<td>( \ldots )</td>
<td>( w_{m,2} )</td>
</tr>
<tr>
<td>( v_1 )</td>
<td>( w_{1,1} )</td>
<td>( \textcolor{red}{w_{2,1}} )</td>
<td>( w_{3,1} )</td>
<td>( \ldots )</td>
<td>( w_{m,1} )</td>
</tr>
<tr>
<td>( u_1 )</td>
<td>( u_2 )</td>
<td>( u_3 )</td>
<td>( \ldots )</td>
<td>( u_m )</td>
<td></td>
</tr>
</tbody>
</table>
Let $u_1, u_2, \ldots, u_n \in \text{IRR}(A^{\pm 1}, I)$ be irreducible traces. The sequence $u_1, u_2, \ldots, u_n$ is $I$-freely reducible if it can be reduced to the empty sequence $\varepsilon$ by the following rules:

- $u_i, u_j \rightarrow u_j, u_i$ if $u_i I u_j$
- $u_i, u_j \rightarrow \varepsilon$ if $u_i = u_j^{-1}$ in $\mathbb{G}(A, I)$
- $u_i \rightarrow \varepsilon$ if $u_i = \varepsilon$. 

Let $u_1, u_2, \ldots, u_n \in \text{IRR}(A^{\pm1}, I)$ be irreducible traces. The sequence $u_1, u_2, \ldots, u_n$ is $I$-freely reducible if it can be reduced to the empty sequence $\varepsilon$ by the following rules:

- $u_i, u_j \rightarrow u_j, u_i$ if $u_i I u_j$
- $u_i, u_j \rightarrow \varepsilon$ if $u_i = u_j^{-1}$ in $\mathbb{G}(A, I)$
- $u_i \rightarrow \varepsilon$ if $u_i = \varepsilon$.

**Lemma**

Let $n \geq 2$ and $u_1, u_2, \ldots, u_n \in \text{IRR}(A^{\pm1}, I)$. If $u_1 u_2 \cdots u_n = 1$ in $\mathbb{G}(A, I)$, then there exist factorizations $u_i = u_{i,1} \cdots u_{i,k_i}$ such that the sequence

$$u_{1,1}, \ldots, u_{1,k_1}, u_{2,1}, \ldots, u_{2,k_2}, \ldots, u_{n,1}, \ldots, u_{n,k_n}$$

is $I$-freely reducible. Moreover, $\sum_{i=1}^{n} k_i \leq 2^n - 2$. 
Lemma

Let $u^x = y_1 \cdots y_m$ be an equation where $u$ is a concrete connected trace. It is equivalent to a disjunction of statements

$$\exists x_1, \ldots, x_m \geq 0: \quad x = \sum_{i=1}^{m} x_i + c \quad \land \quad \bigwedge_{i=1}^{m} y_i = p_i u^{x_i} s_i,$$

where

- $p_i, s_i$ are concrete traces of length polynomial in $m$ and $|u|
- c$ is a concrete number, polynomial in $m$
Theorem

Let \( u_1, u_2, \ldots, u_n \in G(A, I) \setminus \{1\} \), \( \nu_0, \nu_1, \ldots, \nu_n \in G(A, I) \) and let \( x_1, \ldots, x_n \) be variables ranging over \( \mathbb{N} \). Then, the set of solutions of the exponent equation

\[
\nu_0 u_1^{x_1} \nu_1 u_2^{x_2} \nu_2 \cdots u_n^{x_n} \nu_n = 1
\]

is semilinear. Moreover, if there is a solution, then there is a solution where the \( x_i \) are exponential in the size of SLPs for \( u_1, u_2, \ldots, u_n, \nu_0, \nu_1, \ldots, \nu_n \).
Consider \( v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1 \)

By preprocessing, all factors \( u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n \) are irreducible, connected
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected

Apply exponential refinement to obtain $I$-freely reducible sequence.
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected.

Apply exponential refinement to obtain $l$-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected.

Apply exponential refinement to obtain $l$-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected.

Apply exponential refinement to obtain $l$-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

- $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$
- $v_i = z_{i,1} \cdots z_{i,l_i}$
- $y_{i,j} = y_{k,l}^{-1}$
- $y_{i,j} = z_{k,l}^{-1}$
- $z_{i,j} = z_{k,l}^{-1}$
- (h) commutation relations
Consider \( v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1 \)

By preprocessing, all factors \( u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n \) are irreducible, connected

Apply exponential refinement to obtain \( l \)-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

(a) \( u_i^{x_i} = y_{i,1} \cdots y_{i,k_i} \)  
(b) \( v_i = z_{i,1} \cdots z_{i,l_i} \)  
(c) \( y_{i,j} = y_{k,l}^{-1} \)

Replace \( z_{k,l} \) by concrete traces.

(f) \( y_{i,j} = z_{k,l}^{-1} \)
(g) \( z_{i,j} = z_{k,l}^{-1} \)
(h) commutation relations
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected.

Apply exponential refinement to obtain $I$-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

(a) $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$

(b) $v_i = z_{i,1}$

(c) $y_{i,j} = y_{k,l}^{-1}$

(h) commutation relations

Replace $z_{k,l}$ by concrete traces.
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected.

Apply exponential refinement to obtain $l$-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

(a) $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$

(b) $v_i = z_{i,1} \cdots z_{i,l_i}$

(c) $y_{i,j} = y_{k,l}^{-1}$

(h) commutation relations

Replace $z_{k,l}$ by concrete traces.

Replace $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$

\[
\sum_{j=1}^{k_i} x_{i,j} = c_i + \sum_{j=1}^{k_i} x_{i,j} \quad \land \quad y_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}
\]
Consider \( v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1 \)

By preprocessing, all factors \( u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n \) are irreducible, connected.

Apply exponential refinement to obtain \( l \)-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

\[
y_{i,j} = y_{k,l}^{-1}
\]

(h) commutation relations

Replace \( z_{k,l} \) by concrete traces.

Replace \( u_i^{x_i} = y_{i,1} \cdots y_{i,k_i} \)

\[
x_i = c_i + \sum_{j=1}^{k_i} x_{i,j} \quad \land \quad y_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}
\]
Consider \( v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1 \)

By preprocessing, all factors \( u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n \) are irreducible, connected

Apply exponential refinement to obtain \( l \)-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

\[ y_{i,j} = y_{k,l}^{-1} \] (h) commutation relations

Replace \( z_{k,l} \) by concrete traces.

Replace \( u_i^{x_i} = y_{i,1} \cdots y_{i,k_i} \)

\[ x_i = c_i + \sum_{j=1}^{k_i} x_{i,j} \quad \land \quad y_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j} \]

Guess which \( x_i \) are positive \( \rightarrow \) eliminate commutation relations
Consider $v_0 \cdot u_1^{x_1} \cdot v_1 \cdot u_2^{x_2} \cdot v_2 \cdots u_n^{x_n} \cdot v_n = 1$

By preprocessing, all factors $u_1^{x_1}, u_2^{x_2}, \ldots, u_n^{x_n}, v_0, \ldots, v_n$ are irreducible, connected.

Apply exponential refinement to obtain $I$-freely reducible sequence.

Consider all possible refinements and all possible reduction sequences.

We obtain a disjunction of statements:

1. $y_{i,j} = y_{k,l}^{-1}$
2. Replace $z_{k,l}$ by concrete traces.
3. Replace $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$

$$x_i = c_i + \sum_{j=1}^{k_i} x_{i,j} \land y_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}$$

Guess which $x_i$ are positive $\rightarrow$ eliminate commutation relations
The only remaining statements are of the form:

- \( x_i = c_i + \sum_{j=1}^{k_i} x_{i,j} \)

- \( p_{i,j} u_i^{x_{i,j}} s_{i,j} = s_{k,l}^{-1} (u_k^{-1})^{x_{k,l}} p_{k,l}^{-1} \)
- The only remaining statements are of the form:
  - $a') \quad x_i = c_i + \sum_{j=1}^{k_i} x_{i,j}$
  - $b') \quad p_{i,j} u_i^{x_{i,j}} s_{i,j} = s_{k,l}^{-1}(u_k^{-1})^{x_{k,l}} p_{k,l}$

- Now we apply the fact that sets

\[ \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pu^x s = qv^y t\} \]

are semilinear.
The only remaining statements are of the form:

- \( (a') \)
  \[ x_i = c_i + \sum_{j=1}^{k_i} x_{i,j} \]

- \( (b') \)
  \[ p_{i,j} u_i^{x_{i,j}} s_{i,j} = s_{k,l}^{-1} (u_k^{-1})^{x_{k,l}} p_{k,l}^{-1} \]

Now we apply the fact that sets

\[ \{(x, y) \in \mathbb{N} \times \mathbb{N} | \ pu^x s = qv^y t\} \]

are semilinear.

Replace \((a')\) and \((b')\) by linear diophantine equations.
The only remaining statements are of the form:

\[ a') \quad x_i = c_i + \sum_{j=1}^{k_i} x_{i,j} \]

\[ b') \quad p_{i,j} u_{i}^{x_{i,j}} s_{i,j} = s_{k,l}^{-1} (u_{k}^{-1})^{x_{k,l}} p_{k,l}^{-1} \]

Now we apply the fact that sets

\[ \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pu^x s = qv^y t\} \]

are semilinear.

- Replace (a') and (b') by linear diophantine equations.
- Result of von zur Gathen and Sieveking (1978) yields a small solution.
Theorem

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups
Transfer results

**Theorem**

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: \( v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1 \)
Transfer results

Theorem

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: \( v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1 \)
- Guess coset of \( v_0 u_1^{x_1} v_1 \cdots u_i^{x_i} v_i \) for \( 1 \leq i \leq n \)
Transfer results

Theorem

*The class of groups with knapsack in NP is closed under*

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: \( v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1 \)
- Guess coset of \( v_0 u_1^{x_1} v_1 \cdots u_i^{x_i} v_i \) for \( 1 \leq i \leq n \)
- Set of \( x_i \) that comply with this choice is ultimately periodic
Transfer results

Theorem

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: \( v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1 \)
- Guess coset of \( v_0 u_1^{x_1} v_1 \cdots u_i^{x_i} v_i \) for \( 1 \leq i \leq n \)
- Set of \( x_i \) that comply with this choice is ultimately periodic

For free products:

Adapt algorithm of Benois (1969) for rational subsets
Saturation procedure that successively adds transitions to automaton
Choose suitable class of automata such that adding transitions still leads to knapsack instances: knapsack automata.
Transfer results

Theorem

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: \( v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1 \)
- Guess coset of \( v_0 u_1^{x_1} v_1 \cdots u_i^{x_i} v_i \) for \( 1 \leq i \leq n \)
- Set of \( x_i \) that comply with this choice is ultimately periodic

For free products:

- Adapt algorithm of Benois (1969) for rational subsets
Transfer results

Theorem

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: $v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1$
- Guess coset of $v_0 u_1^{x_1} v_1 \cdots u_i^{x_i} v_i$ for $1 \leq i \leq n$
- Set of $x_i$ that comply with this choice is ultimately periodic

For free products:

- Adapt algorithm of Benois (1969) for rational subsets
- Saturation procedure that successively adds transitions to automaton
Transfer results

**Theorem**

The class of groups with knapsack in NP is closed under

- Taking finite extensions
- HNN-extensions over finite associated subgroups
- Amalgamated products with finite identified groups

For finite extensions:

- Generalize problem: \( v_0 u_1^{x_1} v_1 \cdots u_k^{x_k} v_k = 1 \)
- Guess coset of \( v_0 u_1^{x_1} v_1 \cdots u_i^{x_i} v_i \) for \( 1 \leq i \leq n \)
- Set of \( x_i \) that comply with this choice is ultimately periodic

For free products:

- Adapt algorithm of Benois (1969) for rational subsets
- Saturation procedure that successively adds transitions to automaton
- Choose suitable class of automata such that adding transitions still leads to knapsack instances: knapsack automata.