TC^0 circuits for algorithmic problems in nilpotent groups

Alexei Myasnikov[1] Armin Weiß[2]

[1]Stevens Institute of Technology, USA
[2]Universität Stuttgart, Germany

Aalborg, August 21, 2017

Dehn's algorithmic problems

Let G be a group generated by a finite set $\Sigma = \Sigma^{-1} \subseteq G$.

Word problem:	Given:	$w \in \Sigma^*$
	Question:	Is $w = 1$ in G?
Subgroup membership problem:	Given:	$v, w_1, \ldots, w_n \in \Sigma^*$.
	Question:	$v \in \langle w_1, \ldots, w_n \rangle$?

Dehn's algorithmic problems

Let G be a group generated by a finite set $\Sigma = \Sigma^{-1} \subseteq G$.

Word problem:	Given:	$w \in \Sigma^*$
	Question:	Is $w = 1$ in G?
Subgroup membership problem:	Given:	$v, w_1, \ldots, w_n \in \Sigma^*$.
	Question:	$v \in \langle w_1, \ldots, w_n \rangle$?

Theorem (Robinson, 1993)

The word problem of nilpotent groups is in TC^0.

Dehn's algorithmic problems

Let G be a group generated by a finite set $\Sigma = \Sigma^{-1} \subseteq G$.

Word problem:	Given:	$w \in \Sigma^*$
	Question:	Is $w = 1$ in G?
Subgroup membership problem:	Given:	$v, w_1, \ldots, w_n \in \Sigma^*$.
	Question:	$v \in \langle w_1, \ldots, w_n \rangle$?

Theorem (Robinson, 1993)

The word problem of nilpotent groups is in TC^0.

Theorem (Macdonald, Myasnikov, Nikolaev, Vassileva, 2015)

The subgroup membership problem of nilpotent groups is in LOGSPACE.

Circuit Complexity

TC^0 = solved by constant depth, polynomial size circuits with unbounded fan-in $\neg$, $\wedge$, $\vee$, and majority gates.

$$\mathrm{Maj}(w) = 1 \iff |w|_1 \geq |w|_0 \text{ for } w \in \{0, 1\}^*$$

Circuit Complexity

TC^0 = solved by constant depth, polynomial size circuits with unbounded fan-in $\neg$, $\wedge$, $\vee$, and majority gates.

$$\mathrm{Maj}(w) = 1 \iff |w|_1 \geq |w|_0 \text{ for } w \in \{0,1\}^*$$

$$\mathsf{AC}^0 \subsetneq \mathsf{TC}^0 \subseteq \mathsf{NC}^1 \subseteq \mathsf{LOGSPACE} \subseteq \mathsf{NC}^2 \subseteq \cdots \subseteq \mathsf{NC} \subseteq \mathsf{P}$$

Circuit Complexity

TC^0 = solved by constant depth, polynomial size circuits with unbounded fan-in $\neg$, $\wedge$, $\vee$, and majority gates.

$$\mathrm{Maj}(w) = 1 \iff |w|_1 \geq |w|_0 \text{ for } w \in \{0,1\}^*$$

$$\mathsf{AC}^0 \subsetneq \mathsf{TC}^0 \subseteq \mathsf{NC}^1 \subseteq \mathsf{LOGSPACE} \subseteq \mathsf{NC}^2 \subseteq \cdots \subseteq \mathsf{NC} \subseteq \mathsf{P}$$

Arithmetic problems in TC^0:

- Iterated Addition (input: n-bit numbers $r_1, \ldots, r_n$, compute $\sum_{i=1}^{n} r_i$)
- Iterated Multiplication
- Integer Division (Hesse 2001)

Word problem of $\mathbb{Z}$

The word problem of $\mathbb{Z}$ with generators $\{+1, -1\}$ is in TC^0.

Word problem of $\mathbb{Z}$

The word problem of $\mathbb{Z}$ with generators $\{+1, -1\}$ is in TC^0.

Encode -1 by 0 and 1 by 1.

Word problem of $\mathbb{Z}$

The word problem of $\mathbb{Z}$ with generators $\{+1, -1\}$ is in TC^0.

Encode -1 by 0 and 1 by 1. Let $w \in \{0, 1\}^*$,

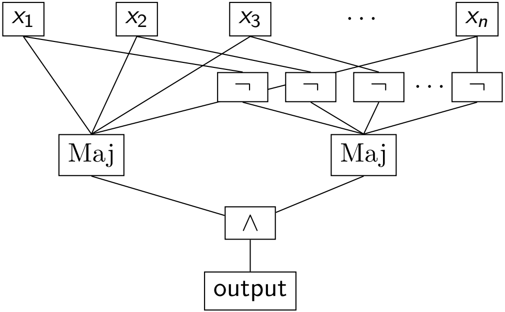
$$\begin{aligned} w \text{ represents } 0 \text{ in } \mathbb{Z} &\iff |w|_1 = |w|_0 \\ &\iff \mathrm{Maj}(w) \wedge \mathrm{Maj}(\neg w) \end{aligned}$$

Word problem of $\mathbb{Z}$

The word problem of $\mathbb{Z}$ with generators $\{+1, -1\}$ is in TC^0.

Encode -1 by 0 and 1 by 1. Let $w \in \{0,1\}^*$,

$$\begin{aligned} w \text{ represents } 0 \text{ in } \mathbb{Z} &\iff |w|_1 = |w|_0 \\ &\iff \mathrm{Maj}(w) \wedge \mathrm{Maj}(\neg w) \end{aligned}$$



Nilpotent groups

Definition

A group G is nilpotent of class c if

$$G = G_1 > G_2 > \cdots G_c > G_{c+1} = \{1\}$$

where $G_{i+1} = [G_i, G] = \left\langle x^{-1} g^{-1} x g \text{ for } x \in G_i, g \in G \right\rangle$.

Nilpotent groups

Definition

A group G is nilpotent of class c if

$$G = G_1 > G_2 > \cdots G_c > G_{c+1} = \{1\}$$

where $G_{i+1} = [G_i, G] = \langle x^{-1}g^{-1}xg \text{ for } x \in G_i, g \in G \rangle$.

Examples:

- abelian groups (nilpotent of class 1)

Nilpotent groups

Definition

A group G is nilpotent of class c if

$$G = G_1 > G_2 > \cdots G_c > G_{c+1} = \{1\}$$

where $G_{i+1} = [G_i, G] = \langle x^{-1}g^{-1}xg \text{ for } x \in G_i, g \in G \rangle$.

Examples:

- abelian groups (nilpotent of class 1)
- finite p-groups

Nilpotent groups

Definition

A group G is nilpotent of class c if

$$G = G_1 > G_2 > \cdots G_c > G_{c+1} = \{1\}$$

where $G_{i+1} = [G_i, G] = \langle x^{-1}g^{-1}xg \text{ for } x \in G_i, g \in G \rangle$.

Examples:

- abelian groups (nilpotent of class 1)
- finite p-groups
- unitriangular matrices $UT_n(\mathbb{Z})$
  (upper triangular and diagonal entries 1)

Nilpotent groups

Definition

A group G is nilpotent of class c if

$$G = G_1 > G_2 > \cdots G_c > G_{c+1} = \{1\}$$

where $G_{i+1} = [G_i, G] = \left\langle x^{-1}g^{-1}xg \text{ for } x \in G_i, g \in G \right\rangle$.

Examples:

- abelian groups (nilpotent of class 1)
- finite p-groups
- unitriangular matrices $UT_n(\mathbb{Z})$
  (upper triangular and diagonal entries 1)
- free nilpotent groups
  $F_{k,c} = \langle a_1, \ldots, a_k \mid [x_1, \ldots, x_{c+1}] = 1 \text{ for } x_1, \ldots, x_{c+1} \in F_{k,c} \rangle$
  where $([x_1, \ldots, x_{c+1}] = [[x_1, \ldots, x_c], x_{c+1}])$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

  with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x,y],z] = 1 \text{ for } x,y,z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \text{mod } \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle.$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 =$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \text{mod } \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle.$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x,y],z] = 1 \text{ for } x,y,z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 =$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1 a_2 [a_2, a_1] a_2 a_1$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \mod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle.$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x,y],z] = 1 \text{ for } x,y,z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1 a_2 a_2 a_1 [a_2, a_1]$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle.$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1 a_2 a_2 a_1 [a_2, a_1]$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle.$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x,y],z] = 1 \text{ for } x,y,z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1 a_2^2 a_1 [a_2, a_1]$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \mathrm{mod} \ \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x, y], z] = 1 \text{ for } x, y, z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1 a_1 a_2^2 [a_2, a_1]^2 [a_2, a_1]$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \qquad \bmod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x,y],z] = 1 \text{ for } x,y,z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1^2 a_2^2 [a_2, a_1]^3$$

Mal'cev coordinates

Every (torsion-free) nilpotent group G has a Mal'cev basis $(a_1, \ldots, a_m)$.

- Each $g \in G$ has a unique normal form

$$g = a_1^{x_1} \cdots a_m^{x_m}$$

  with $(x_1, \ldots, x_m) \in \mathbb{Z}^m$ and

$$a_i a_j \equiv a_j a_i \mod \left\langle a_{\max\{i,j\}+1}, \ldots, a_m \right\rangle .$$

Example

$F_{2,2} = \langle a_1, a_2 \mid [[x,y],z] = 1 \text{ for } x,y,z \in F_{2,2} \rangle$

- (a_1, a_2) is not a Mal'cev basis since $a_2 a_1$ cannot be written as $a_1^x a_2^y$
- $(a_1, a_2, [a_2, a_1])$ is a Mal'cev basis:

$$a_2 a_1 a_2 a_1 = a_1^2 a_2^2 [a_2, a_1]^3$$

- $F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3, [a_3, a_1] = [a_3, a_2] = 1 \rangle = UT_3(\mathbb{Z})$

Mal'cev coordinates

The products of two elements can be written in the same way

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{p_1} \cdots a_m^{p_m}$$

Mal'cev coordinates

The products of two elements can be written in the same way

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{p_1} \cdots a_m^{p_m}$$

The exponents $p_1, \ldots, p_m$ are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$

Mal'cev coordinates

The products of two elements and powers can be written in the same way

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{p_1} \cdots a_m^{p_m}$$
$$(a_1^{x_1} \cdots a_m^{x_m})^z = a_1^{q_1} \cdots a_m^{q_m}.$$

The exponents $p_1, \ldots, p_m$ (resp. $q_1, \ldots, q_m$) are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ (resp. $x_1, \ldots, x_m$ and z).

Mal'cev coordinates

The products of two elements and powers can be written in the same way

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{p_1} \cdots a_m^{p_m}$$
$$(a_1^{x_1} \cdots a_m^{x_m})^z = a_1^{q_1} \cdots a_m^{q_m}.$$

The exponents $p_1, \ldots, p_m$ (resp. $q_1, \ldots, q_m$) are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ (resp. $x_1, \ldots, x_m$ and z).

Fact

$$p_1(x_1, \ldots, x_m, y_1, \ldots, y_m) = x_1 + y_1$$

Mal'cev coordinates

The products of two elements and powers can be written in the same way

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{p_1} \cdots a_m^{p_m}$$
$$(a_1^{x_1} \cdots a_m^{x_m})^z = a_1^{q_1} \cdots a_m^{q_m}.$$

The exponents $p_1, \ldots, p_m$ (resp. $q_1, \ldots, q_m$) are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ (resp. $x_1, \ldots, x_m$ and z).

Fact

$$p_1(x_1, \ldots, x_m, y_1, \ldots, y_m) = x_1 + y_1$$

Theorem (P. Hall, 1957)

If G is torsion-free, then

$$p_1, \ldots, p_m \in \mathbb{Q}[x_1, \ldots, x_m, y_1, \ldots, y_m],$$
$$q_1, \ldots, q_m \in \mathbb{Q}[x_1, \ldots, x_m, z].$$

Mal'cev coordinates

The products of two elements and powers can be written in the same way

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{p_1} \cdots a_m^{p_m}$$
$$(a_1^{x_1} \cdots a_m^{x_m})^z = a_1^{q_1} \cdots a_m^{q_m}.$$

The exponents $p_1, \ldots, p_m$ (resp. $q_1, \ldots, q_m$) are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ (resp. $x_1, \ldots, x_m$ and z).

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3, [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$$a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{y_1} a_2^{y_2} a_3^{y_3} = a_1^{x_1+y_1} a_2^{x_2+y_2} a_3^{x_3+y_3+y_1 x_2}$$

Mal'cev coordinates

The products of two elements and powers can be written in the same way

$$\begin{aligned} a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} &= a_1^{p_1} \cdots a_m^{p_m} \\ (a_1^{x_1} \cdots a_m^{x_m})^z &= a_1^{q_1} \cdots a_m^{q_m}. \end{aligned}$$

The exponents $p_1, \ldots, p_m$ (resp. $q_1, \ldots, q_m$) are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ (resp. $x_1, \ldots, x_m$ and z).

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$$\begin{aligned} a_1^{x_1} a_2^{x_2} a_3^{x_3} \cdot a_1^{y_1} a_2^{y_2} a_3^{y_3} &= a_1^{x_1 + y_1} a_2^{x_2 + y_2} a_3^{x_3 + y_3 + y_1 x_2} \\ (a_1^{x_1} a_2^{x_2} a_3^{x_3})^z &= a_1^{z x_1} a_2^{z x_2} a_3^{z x_3 + \binom{z-1}{2} x_1 x_2}. \end{aligned}$$

Groups as inputs

$\mathcal{N}_{c,r} = \{$ r-generated nilpotent groups of class at most c $\}$.

$\mathcal{N}_{c,r} = \{\, r$-generated nilpotent groups of class at most $c\,\}$.

Every $G \in \mathcal{N}_{c,r}$ is a quotient of the free nilpotent group $F_{c,r}$:

$$G = F_{c,r}/N$$

for some normal subgroup $N \leq F_{c,r}$.

Groups as inputs

$\mathcal{N}_{c,r} = \{\, r\text{-generated nilpotent groups of class at most } c \,\}$.

Every $G \in \mathcal{N}_{c,r}$ is a quotient of the free nilpotent group $F_{c,r}$:

$$G = F_{c,r}/N$$

for some normal subgroup $N \leq F_{c,r}$.

Represent $G \in \mathcal{N}_{c,r}$ by a (nice) generating set of N.

Groups as inputs

$\mathcal{N}_{c,r} = \{\, r\text{-generated nilpotent groups of class at most } c \,\}$.

Every $G \in \mathcal{N}_{c,r}$ is a quotient of the free nilpotent group $F_{c,r}$:

$$G = F_{c,r}/N$$

for some normal subgroup $N \leq F_{c,r}$.

Represent $G \in \mathcal{N}_{c,r}$ by a (nice) generating set of N.

If $(a_1, \ldots, a_m)$ is a Mal'cev basis of $F_{c,r}$, it is also a Mal'cev basis of G.

Words with Binary Exponents

Usually: group elements represented as words

Words with Binary Exponents

Usually: group elements represented as words

Let Σ generate G. A word with binary exponents is

- a sequence $w_1, \ldots, w_n$ with $w_i \in \Sigma$
- together with $x_1, \ldots, x_n$ with $x_i \in \mathbb{Z}$ encoded in binary.

It represents $$w = w_1^{x_1} \cdots w_n^{x_n}.$$

Words with Binary Exponents

Usually: group elements represented as words

Let Σ generate G. A word with binary exponents is

- a sequence $w_1, \dots, w_n$ with $w_i \in \Sigma$
- together with $x_1, \dots, x_n$ with $x_i \in \mathbb{Z}$ encoded in binary.

It represents $$w = w_1^{x_1} \cdots w_n^{x_n}.$$

Example

Write $$a_1^{1000} a_3 a_2^{100} a_1^4$$

instead of $$\underbrace{a_1 \cdots a_1}_{1000 \text{ times}} a_3 \underbrace{a_2 \cdots a_2}_{100 \text{ times}} a_1 a_1 a_1 a_1.$$

Words with Binary Exponents

Usually: group elements represented as words

Let Σ generate G. A word with binary exponents is

- a sequence $w_1, \ldots, w_n$ with $w_i \in \Sigma$
- together with $x_1, \ldots, x_n$ with $x_i \in \mathbb{Z}$ encoded in binary.

It represents
$$w = w_1^{x_1} \cdots w_n^{x_n}.$$

Example

Write
$$a_1^{1000} a_3 a_2^{100} a_1^4$$
instead of
$$\underbrace{a_1 \cdots a_1}_{1000 \text{ times}} a_3 \underbrace{a_2 \cdots a_2}_{100 \text{ times}} a_1 a_1 a_1 a_1.$$

Fact

In $\mathcal{N}_{c,r}$ groups every word of length n can be written as a word with binary exponents using $\mathcal{O}(\log n)$ bits.

Word Problem

Theorem

Let $c, r \geq 1$ be fixed. Let $(a_1, \ldots, a_m)$ be the standard Mal'cev basis of $F_{c,r}$. The following problem is in TC^0:

Input: $G \in \mathcal{N}_{c,r}$ *and* $w = w_1^{x_1} \cdots w_n^{x_n}$ *(with binary exponents),*

Find: $y_1, \ldots, y_m \in \mathbb{Z}$ *(in binary) such that* $w = a_1^{y_1} \cdots a_m^{y_m}$.

Word Problem

Theorem

Let $c, r \geq 1$ be fixed. Let $(a_1, \ldots, a_m)$ be the standard Mal'cev basis of $F_{c,r}$. The following problem is in TC^0:

Input: $G \in \mathcal{N}_{c,r}$ *and* $w = w_1^{x_1} \cdots w_n^{x_n}$ *(with binary exponents),*

Find: $y_1, \ldots, y_m \in \mathbb{Z}$ *(in binary) such that* $w = a_1^{y_1} \cdots a_m^{y_m}$.

For unary inputs and fixed G this is due to Robinson 1993.

Word Problem

Theorem

Let $c, r \geq 1$ be fixed. Let $(a_1, \ldots, a_m)$ be the standard Mal'cev basis of $F_{c,r}$. The following problem is in TC^0:

Input: $G \in \mathcal{N}_{c,r}$ *and* $w = w_1^{x_1} \cdots w_n^{x_n}$ *(with binary exponents),*

Find: $y_1, \ldots, y_m \in \mathbb{Z}$ *(in binary) such that* $w = a_1^{y_1} \cdots a_m^{y_m}$.

For unary inputs and fixed G this is due to Robinson 1993.

Corollary

Let $c, r \geq 1$ be fixed. The uniform, binary word problem for groups in $\mathcal{N}_{c,r}$ is TC^0-complete (input as in Theorem 1).

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x \ a_3^{xy}$ $\qquad a_3^x a_1^y \to a_1^y a_3^x$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\, a_3^{xy}$ $\qquad a_3^x a_1^y \to a_1^y a_3^x$

$$w = \quad a_3 \quad a_1^{13} \quad a_2^{10} \quad a_1^{5} \quad a_2 \quad a_1^{10} \quad a_1^{-20}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\ a_3^{xy}$ $\qquad a_3^x a_1^y \to a_1^y a_3^x$

$$w = \quad a_3 \quad a_1^{13} \quad a_2^{10} \quad a_1^{5} \quad a_2 \quad a_1^{10} \quad a_1^{-20}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\ a_3^{xy}$ $\qquad$ $a_3^x a_1^y \to a_1^y a_3^x$

$$w = a_3 \quad a_1^{13} \quad a_2^{10} \quad a_1^{5} \quad a_2 \quad a_1^{10} \quad a_1^{-20}$$

$$= a_1^{8}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\ a_3^{xy}$ $\qquad a_3^x a_1^y \to a_1^y a_3^x$

$$w = \underbrace{a_3}_{a_1^{8}} \quad a_1^{13} \quad \underbrace{a_2^{10}}_{a_1^{-5}} \quad a_1^{5} \quad \underbrace{a_2}_{a_1^{-10}} \quad a_1^{10} \quad a_1^{-20}$$

$$= a_1^{8}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x a_3^{xy}$ $\quad$ $a_3^x a_1^y \to a_1^y a_3^x$

$$w = \underbrace{a_3}_{a_1^{8}} \; a_1^{13} \; \underbrace{a_2^{10}}_{a_1^{-5}} \; a_1^{5} \; \underbrace{a_2}_{a_1^{-10}} \; a_1^{10} \; a_1^{-20}$$

$$= a_1^{8} \; a_3 \; a_2^{10} a_3^{-50} \; a_2 a_3^{-10}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\, a_3^{xy}$ $\quad$ $a_3^x a_1^y \to a_1^y a_3^x$

$$w = a_3 \quad a_1^{13} \quad a_2^{10} \quad a_1^{5} \quad a_2 \quad a_1^{10} \quad a_1^{-20}$$

$$= a_1^{8} \quad a_3 \quad a_2^{10}\, a_3^{-50} \quad a_2\, a_3^{-10}$$

$$= a_1^{8}\, a_2^{11}\, a_3^{-59}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\, a_3^{xy}$ $\qquad a_3^x a_1^y \to a_1^y a_3^x$

$$w = \quad a_3 \quad a_1^{13} \quad a_2^{10} \quad a_1^{5} \quad a_2 \quad a_1^{10} \quad a_1^{-20}$$

$$= a_1^{8} \quad a_3 \quad a_2^{10}\, a_3^{-50} \quad a_2\, a_3^{-10}$$

$$= a_1^{8}\, a_2^{11}\, a_3^{-59}$$

Proof

Example

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_2, a_1] = a_3,\ [a_3, a_1] = [a_3, a_2] = 1 \rangle$

$w = a_3 a_1^{13} a_2^{10} a_1^{5} a_2 a_1^{10} a_1^{-20}$

Aim move a_1 to the left.

Substitution rules: $a_2^x a_1^y \to a_1^y a_2^x\ a_3^{xy}$ $\qquad a_3^x a_1^y \to a_1^y a_3^x$

$$w = \quad a_3 \quad a_1^{13} \quad a_2^{10} \quad a_1^{5} \quad a_2 \quad a_1^{10} \ a_1^{-20}$$

$$= a_1^{8} \quad a_3 \qquad\qquad a_2^{10}\ a_3^{-50} \qquad a_2\ a_3^{-10}$$

$$= a_1^{8}\ a_2^{11}\ a_3^{-59}$$

Greatest Common Divisors

Aim: subgroup membership problem in nilpotent groups.

Greatest Common Divisors

Aim: subgroup membership problem in nilpotent groups.

Subgroup membership problem of $\mathbb{Z}$:

Given $a, a_1, \ldots, a_n \in \mathbb{Z}$, is $a \in \langle a_1, \ldots, a_n \rangle$?
With other words: are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n?$$

Greatest Common Divisors

Aim: subgroup membership problem in nilpotent groups.

Subgroup membership problem of $\mathbb{Z}$:

Given $a, a_1, \ldots, a_n \in \mathbb{Z}$, is $a \in \langle a_1, \ldots, a_n \rangle$?
With other words: are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n?$$

Extended gcd problem ($\textsc{ExtGCD}$)

On input of $a_1, \ldots, a_n \in \mathbb{Z}$ in binary, compute $x_1, \ldots, x_n \in \mathbb{Z}$ such that

$$\gcd(a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n.$$

Greatest Common Divisors

Aim: subgroup membership problem in nilpotent groups.

Subgroup membership problem of $\mathbb{Z}$:

Given $a, a_1, \ldots, a_n \in \mathbb{Z}$, is $a \in \langle a_1, \ldots, a_n \rangle$?
With other words: are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n?$$

Extended gcd problem ($\textsc{ExtGCD}$)

On input of $a_1, \ldots, a_n \in \mathbb{Z}$ in binary, compute $x_1, \ldots, x_n \in \mathbb{Z}$ such that

$$\gcd(a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n.$$

$\rightsquigarrow$ $a \in \langle a_1, \ldots, a_n \rangle$ iff $\gcd(a_1, \ldots, a_n) \mid a$.

Greatest Common Divisors

Aim: subgroup membership problem in nilpotent groups.

Subgroup membership problem of $\mathbb{Z}$:

Given $a, a_1, \ldots, a_n \in \mathbb{Z}$, is $a \in \langle a_1, \ldots, a_n \rangle$?
With other words: are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n?$$

Extended gcd problem ($\textsc{ExtGCD}$)

On input of $a_1, \ldots, a_n \in \mathbb{Z}$ in binary, compute $x_1, \ldots, x_n \in \mathbb{Z}$ such that

$$\gcd(a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n.$$

$\rightsquigarrow a \in \langle a_1, \ldots, a_n \rangle$ iff $\gcd(a_1, \ldots, a_n) \mid a$.

Proposition

$\textsc{ExtGCD}$ *with unary inputs and outputs is in* TC^0.

Matrix reduction

Let $(h_1, \ldots, h_n)$ be generators of a subgroup H. We associate a matrix of coordinates

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix},$$

where $(\alpha_{i1}, \ldots \alpha_{im})$ are the Mal'cev coordinates of h_i.

Matrix reduction

Let $(h_1, \ldots, h_n)$ be generators of a subgroup H. We associate a matrix of coordinates

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix},$$

where $(\alpha_{i1}, \ldots \alpha_{im})$ are the Mal'cev coordinates of h_i.

Modify matrix without changing the subgroup generated by its rows:

Matrix reduction

Let $(h_1, \ldots, h_n)$ be generators of a subgroup H. We associate a matrix of coordinates

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix},$$

where $(\alpha_{i1}, \ldots \alpha_{im})$ are the Mal'cev coordinates of h_i.

Modify matrix without changing the subgroup generated by its rows:

- triangular shape ("Gaussian elimination")

Matrix reduction

Let $(h_1, \ldots, h_n)$ be generators of a subgroup H. We associate a matrix of coordinates

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix},$$

where $(\alpha_{i1}, \ldots \alpha_{im})$ are the Mal'cev coordinates of h_i.

Modify matrix without changing the subgroup generated by its rows:

- triangular shape ("Gaussian elimination")
- $H \cap \langle a_i, a_{i+1}, \ldots, a_m \rangle$ is generated by rows with 0 in first $i-1$ columns.

Matrix reduction

Let $(h_1, \ldots, h_n)$ be generators of a subgroup H. We associate a matrix of coordinates

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nm} \end{pmatrix},$$

where $(\alpha_{i1}, \ldots \alpha_{im})$ are the Mal'cev coordinates of h_i.

Modify matrix without changing the subgroup generated by its rows:

- triangular shape ("Gaussian elimination")
- $H \cap \langle a_i, a_{i+1}, \ldots, a_m \rangle$ is generated by rows with 0 in first $i-1$ columns.

Theorem

Matrix reduction is in TC^0.

Subgroup membership problem

Corollary

The subgroup membership problem is in TC^0 *for nilpotent groups.*

Proof.

Question is $a_1^{k_1} \ldots a_m^{k_m} \in H$? Forward substitution:

$$(X_1, \ldots, X_m) \circ \begin{pmatrix} * & * & * & * & * \\ & * & * & * & * \\ & & * & * & * \\ & 0 & & * & * \\ & & & & * \end{pmatrix} = (k_1, \ldots, k_m)$$

□

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $\qquad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $\qquad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6, 4) = 2 = 6 - 4$.

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$.

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2$.

The associated matrix is $\qquad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}$.

- Compute $\gcd(6, 4) = 2 = 6 - 4$.
- Add a new row corresponding to $h_3 = h_1 h_2^{-1}$.

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\quad h_1 = a_1^6 a_2^2 a_3, \quad h_2 = a_1^4 a_2^2.$

The associated matrix is $\quad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6,4) = 2 = 6 - 4$.
- Add a new row corresponding to $h_3 = h_1 h_2^{-1} = a_1^6 a_2^2 a_3 \, (a_1^4 a_2^2)^{-1}$.

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $h_1 = a_1^6 a_2^2 a_3,\qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6, 4) = 2 = 6 - 4$.
- Add a new row corresponding to $h_3 = h_1 h_2^{-1} = a_1^2 a_3^1$.

$$\begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $\qquad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6, 4) = 2 = 6 - 4.$
- Add a new row corresponding to $h_3 = h_1 h_2^{-1} = a_1^2 a_3^1.$
- Replace h_1 by $h_1' = h_1 h_3^{-3}$ and h_2 by $h_2' = h_2 h_3^{-2}$

$$\begin{pmatrix} 0 & 2 & -6 \\ 0 & 2 & -6 \\ 2 & 0 & 1 \end{pmatrix}$$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\quad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $\quad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6, 4) = 2 = 6 - 4.$
- Add a new row corresponding to $h_3 = h_1 h_2^{-1} = a_1^2 a_3^1.$
- Replace h_1 by $h_1' = h_1 h_3^{-3}$ and h_2 by $h_2' = h_2 h_3^{-2}$
- Exchange first and last row and eliminate unnecessary row

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & -6 \end{pmatrix}$$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $\qquad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6, 4) = 2 = 6 - 4.$
- Add a new row corresponding to $h_3 = h_1 h_2^{-1} = a_1^2 a_3^1.$
- Replace h_1 by $h_1' = h_1 h_3^{-3}$ and h_2 by $h_2' = h_2 h_3^{-2}$
- Exchange first and last row and eliminate unnecessary row
- Add commutators

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & -6 \\ 0 & 0 & 4 \end{pmatrix}$$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1, \ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\quad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

The associated matrix is $\quad A = \begin{pmatrix} 6 & 2 & 1 \\ 4 & 2 & 0 \end{pmatrix}.$

- Compute $\gcd(6, 4) = 2 = 6 - 4.$
- Add a new row corresponding to $h_3 = h_1 h_2^{-1} = a_1^2 a_3^1.$
- Replace h_1 by $h_1' = h_1 h_3^{-3}$ and h_2 by $h_2' = h_2 h_3^{-2}$
- Exchange first and last row and eliminate unnecessary row
- Add commutators

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix}$$

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix}$$

- Is $a_1 a_2 a_3 \in H$?

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix}$$

- Is $a_1 a_2 a_3 \in H$? No!

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix}$$

- Is $a_1 a_2 a_3 \in H$? No!
- Is $a_1^4 a_3^6 \in H$?

Example: Matrix reduction

$G = F_{2,2} = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle.$

Let $H = \langle h_1, h_2 \rangle$ with $\qquad h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$

$$\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix}$$

- Is $a_1 a_2 a_3 \in H$? No!
- Is $a_1^4 a_3^6 \in H$? Yes: $a_1^4 a_3^6 \cdot (a_1^2 a_3)^{-2} = a_3^4 \in H.$

More Problems

Theorem

The following problems are in TC^0 *(resp.* $\mathsf{TC}^0(\textsc{ExtGCD})$ *for binary inputs):*

- *conjugacy problem,*
- *compute presentations of subgroups,*
- *compute kernels and preimages of homomorphisms,*
- *compute the centralizers,*
- *compute quotient presentations.*

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.
- Extended gcd problem with unary inputs and outputs is in TC^0.

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.
- Extended gcd problem with unary inputs and outputs is in TC^0.
- Binary versions in $\mathsf{TC}^0(\textsc{ExtGCD})$

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.
- Extended gcd problem with unary inputs and outputs is in TC^0.
- Binary versions in $\mathsf{TC}^0(\textsc{ExtGCD})$

Open Questions

- Complexity of the uniform word problem for fixed nilpotency class but an arbitrary number of generators?

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.
- Extended gcd problem with unary inputs and outputs is in TC^0.
- Binary versions in $\mathsf{TC}^0(\textsc{ExtGCD})$

Open Questions

- Complexity of the uniform word problem for fixed nilpotency class but an arbitrary number of generators?
- What if the nilpotency class is not fixed?

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.
- Extended gcd problem with unary inputs and outputs is in TC^0.
- Binary versions in $\mathsf{TC}^0(\textsc{ExtGCD})$

Open Questions

- Complexity of the uniform word problem for fixed nilpotency class but an arbitrary number of generators?
- What if the nilpotency class is not fixed?
- Same question for conjugacy...

Conclusion and Open Questions

- Most problems by Macdonald et. al. 2015 are in TC^0.
- Extended gcd problem with unary inputs and outputs is in TC^0.
- Binary versions in $\mathsf{TC}^0(\textsc{ExtGCD})$

Open Questions

- Complexity of the uniform word problem for fixed nilpotency class but an arbitrary number of generators?
- What if the nilpotency class is not fixed?
- Same question for conjugacy...

Thank you!