TC^0 computations and the subgroup membership problem in nilpotent groups

Armin Weiß

Stevens Institute of Technology

Manhattan Algebra Day, December 9, 2016

Outline

- Why circuit complexity for groups?
- Computing gcds
- Subgroup membership for nilpotent groups

Dehn's fundamental problems (and others)

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

- Word problem: Given $w \in \Sigma^*$. Question: Is $w = 1$ in G?
- Conjugacy problem: Given $v, w \in \Sigma^*$.
  Question: $\exists\, z \in G$ such that $zvz^{-1} = w$?
- (Uniform) Subgroup membership problem:
  Given $v, w_1, \ldots, w_n \in \Sigma^*$. Question: $v \in \langle w_1, \ldots, w_n \rangle$?

Dehn's fundamental problems (and others)

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

- Word problem: Given $w \in \Sigma^*$. Question: Is $w = 1$ in G?
- Conjugacy problem: Given $v, w \in \Sigma^*$.
  Question: $\exists\, z \in G$ such that $zvz^{-1} = w$?
- (Uniform) Subgroup membership problem:
  Given $v, w_1, \ldots, w_n \in \Sigma^*$. Question: $v \in \langle w_1, \ldots, w_n \rangle$?

Classification:

- Decidable vs. undecidable.

Dehn's fundamental problems (and others)

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

- Word problem: Given $w \in \Sigma^*$. Question: Is $w = 1$ in G?
- Conjugacy problem: Given $v, w \in \Sigma^*$.
  Question: $\exists\, z \in G$ such that $zvz^{-1} = w$?
- (Uniform) Subgroup membership problem:
  Given $v, w_1, \ldots, w_n \in \Sigma^*$. Question: $v \in \langle w_1, \ldots, w_n \rangle$?

Classification:

- Decidable vs. undecidable.
- Complexity: e. g. primitive recursive, NP, polynomial time

Dehn's fundamental problems (and others)

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

- Word problem: Given $w \in \Sigma^*$. Question: Is $w = 1$ in G?
- Conjugacy problem: Given $v, w \in \Sigma^*$.
  Question: $\exists\, z \in G$ such that $zvz^{-1} = w$?
- (Uniform) Subgroup membership problem:
  Given $v, w_1, \ldots, w_n \in \Sigma^*$. Question: $v \in \langle w_1, \ldots, w_n \rangle$?

Classification:

- Decidable vs. undecidable.
- Complexity: e. g. primitive recursive, NP, polynomial time
  Inside polynomial time:
  - linear time (e. g. WP/CP of hyperbolic groups)

Dehn's fundamental problems (and others)

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

- Word problem: Given $w \in \Sigma^*$. Question: Is $w = 1$ in G?
- Conjugacy problem: Given $v, w \in \Sigma^*$.
  Question: $\exists\, z \in G$ such that $zvz^{-1} = w$?
- (Uniform) Subgroup membership problem:
  Given $v, w_1, \ldots, w_n \in \Sigma^*$. Question: $v \in \langle w_1, \ldots, w_n \rangle$?

Classification:

- Decidable vs. undecidable.
- Complexity: e. g. primitive recursive, NP, polynomial time
  Inside polynomial time:
  - linear time (e. g. WP/CP of hyperbolic groups)
  - LOGSPACE (e. g. WP of linear groups)

Dehn's fundamental problems (and others)

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

- Word problem: Given $w \in \Sigma^*$. Question: Is $w = 1$ in G?
- Conjugacy problem: Given $v, w \in \Sigma^*$.
  Question: $\exists\, z \in G$ such that $zvz^{-1} = w$?
- (Uniform) Subgroup membership problem:
  Given $v, w_1, \ldots, w_n \in \Sigma^*$. Question: $v \in \langle w_1, \ldots, w_n \rangle$?

Classification:

- Decidable vs. undecidable.
- Complexity: e. g. primitive recursive, NP, polynomial time
  Inside polynomial time:
  - linear time (e. g. WP/CP of hyperbolic groups)
  - LOGSPACE (e. g. WP of linear groups)
  - parallel complexity

Parallel Complexity

Why parallel complexity?

- Finer classification of problems inside polynomial time.

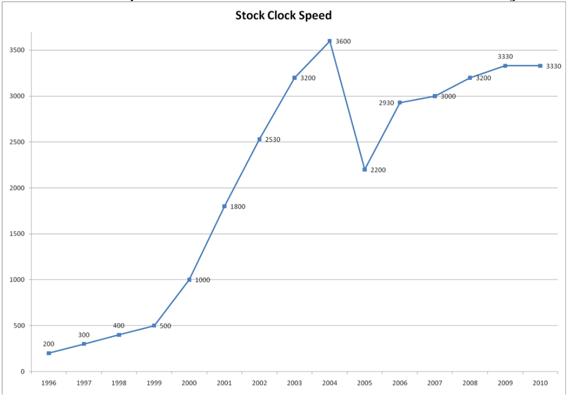
Parallel Complexity

Why parallel complexity?

- Finer classification of problems inside polynomial time.
- We cannot be faster than linear time on one processor,
  but we can on many processors.

Why parallel complexity?

- Finer classification of problems inside polynomial time.
- We cannot be faster than linear time on one processor, but we can on many processors.
- Parallel computing is more and more important in the "real world":
  - while clock frequencies almost do not increase anymore



Parallel Complexity

Why parallel complexity?

- Finer classification of problems inside polynomial time.
- We cannot be faster than linear time on one processor,
  but we can on many processors.
- Parallel computing is more and more important in the “real world”:
  - while clock frequencies almost do not increase anymore
  - 4 cores on most desktop processors

Parallel Complexity

Why parallel complexity?

- Finer classification of problems inside polynomial time.
- We cannot be faster than linear time on one processor,
  but we can on many processors.
- Parallel computing is more and more important in the "real world":
  - while clock frequencies almost do not increase anymore
  - 4 cores on most desktop processors
  - $>$ 2000 cores on high-end graphics devices

Why parallel complexity?

- Finer classification of problems inside polynomial time.
- We cannot be faster than linear time on one processor, but we can on many processors.
- Parallel computing is more and more important in the "real world":
  - while clock frequencies almost do not increase anymore
  - 4 cores on most desktop processors
  - > 2000 cores on high-end graphics devices
  - $> 10^6$ cores on supercomputers

Why parallel complexity?

- Finer classification of problems inside polynomial time.
- We cannot be faster than linear time on one processor, but we can on many processors.
- Parallel computing is more and more important in the "real world":
  - while clock frequencies almost do not increase anymore
  - 4 cores on most desktop processors
  - > 2000 cores on high-end graphics devices
  - $> 10^6$ cores on supercomputers

Parallel Complexity

Machine models:

- parallel RAMs (random access machines)
- (Boolean) circuits

Parallel Complexity

Machine models:

- parallel RAMs (random access machines)
- (Boolean) circuits

Circuit = directed acyclic graph where each vertex is either:

- input gates (has only outgoing edges)
- Boolean gates (and $\wedge$, or $\vee$, not $\neg$ having incoming and outgoing edges)
- output gates (only incoming edges)

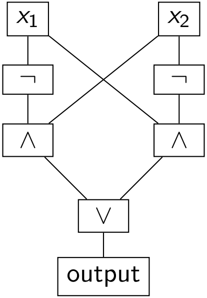
Parallel Complexity

Machine models:

- parallel RAMs (random access machines)
- (Boolean) circuits

Circuit = directed acyclic graph where each vertex is either:

- input gates (has only outgoing edges)
- Boolean gates (and $\wedge$, or $\vee$, not $\neg$ having incoming and outgoing edges)
- output gates (only incoming edges)



Parallel Complexity

Machine models:

- parallel RAMs (random access machines)
- (Boolean) circuits

Circuit = directed acyclic graph where each vertex is either:

- input gates (has only outgoing edges)
- Boolean gates (and $\wedge$, or $\vee$, not $\neg$ having incoming and outgoing edges)
- output gates (only incoming edges)

size = number of gates
depth = longest path from input to output gate

NC = problems which can be solved by a family of circuits of polynomial size and polylogarithmic depth

= problems which can be solved by a parallel RAM with a polynomial number of processors in polylogarithmic time.

Inside NC:

- NC^i = solved by a family of circuits of depth $\mathcal{O}(\log^i n)$ and polynomial size with bounded fan-in (= in-degree) $\neg$, $\wedge$, $\vee$ gates.

Parallel Complexity

Inside NC:

- NC^i = solved by a family of circuits of depth $\mathcal{O}(\log^i n)$ and polynomial size with bounded fan-in (= in-degree) $\neg$, $\wedge$, $\vee$ gates.

Infinite hierarchy:

$$\mathsf{NC}^1 \subseteq \mathsf{LOGSPACE} \subseteq \mathsf{NC}^2 \subseteq \mathsf{NC}^3 \subseteq \cdots \subseteq \mathsf{NC} \subseteq \mathsf{P}.$$

Inside NC:

- NC^i = solved by a family of circuits of depth $\mathcal{O}(\log^i n)$ and polynomial size with bounded fan-in (= in-degree) $\neg$, $\wedge$, $\vee$ gates.

Infinite hierarchy:

$$\mathsf{NC}^1 \subseteq \mathsf{LOGSPACE} \subseteq \mathsf{NC}^2 \subseteq \mathsf{NC}^3 \subseteq \cdots \subseteq \mathsf{NC} \subseteq \mathsf{P}.$$

Theorem (Lipton, Zalcstein, 1977 / Simon, 1979)

The word problem of linear groups is in LOGSPACE.

"Proof": Given matrices $A_1, \ldots, A_n$, compute

$$\prod A_i \mod p$$

for sufficiently many primes p.

Inside NC^1:

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

Parallel Complexity

Inside NC^1:

- AC^0 = solved by a family of circuits of constant depth and polynomial size with unbounded fan-in $\neg$, $\wedge$, $\vee$ gates.
- TC^0 allows additionally majority gates: $\mathrm{Maj}(w) = 1$ iff $|w|_1 \geq |w|_0$ for $w \in \{0,1\}^*$.

Theorem (Robinson, 1993)

The word problem of

- *Baumslag-Solitar groups* $\mathbf{BS}_{1,q}$ *and*
- *nilpotent groups*

are uniform TC^0*-complete.*

More problems in TC^0:

- conjugacy problem in $\mathbf{BS}_{1,q}$ (Diekert, Myasnikov, W., 2014)
- word problem in solvable linear groups (König, Lohrey, 2015)
- word and conjugacy problem in free solvable groups (Myasnikov, Vassileva, W., 2016)

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.

Use 0 to encode -1 and 1 for 1.

Word problem of $\mathbb{Z}$

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

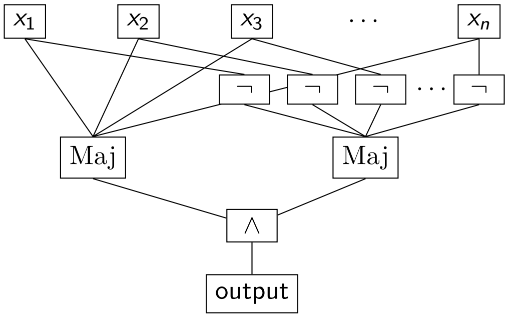
Use 0 to encode -1 and 1 for 1. Let $w \in \{0, 1\}^*$,

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

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

Use 0 to encode -1 and 1 for 1. Let $w \in \{0,1\}^*$,

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



Arithmetic problems in TC^0

Iterated Addition

- input: n-bit numbers $r_1, \ldots, r_n$,
- compute $\sum_{i=1}^{n} r_i$.

Iterated Addition

- input: n-bit numbers $r_1, \ldots, r_n$,
- compute $\sum_{i=1}^{n} r_i$.

Iterated Addition is in TC^0.

Arithmetic problems in TC^0

Iterated Addition

- input: n-bit numbers $r_1, \ldots, r_n$,
- compute $\sum_{i=1}^{n} r_i$.

Iterated Addition is in TC^0.

Iterated Multiplication

- input: n-bit numbers $r_1, \ldots, r_n$,
- compute $\prod_{i=1}^{n} r_i$.

Integer Division

- input: n-bit numbers a, b,
- compute $\left\lfloor \frac{a}{b} \right\rfloor$.

Arithmetic problems in TC^0

Iterated Addition

- input: n-bit numbers $r_1, \ldots, r_n$,
- compute $\sum_{i=1}^{n} r_i$.

Iterated Addition is in TC^0.

Iterated Multiplication

- input: n-bit numbers $r_1, \ldots, r_n$,
- compute $\prod_{i=1}^{n} r_i$.

Integer Division

- input: n-bit numbers a, b,
- compute $\left\lfloor \frac{a}{b} \right\rfloor$.

Theorem (Hesse, 2001)

Iterated Multiplication and Integer Division are in TC^0.

Reductions

- For a formal language $L \subseteq \{0,1\}^*$, $\mathsf{AC}^0(L)$ allows additionally oracle gates for L.
- $L' \in \mathsf{AC}^0(L)$ means L' is AC^0-reducible to L.
- Every problem in TC^0 is AC^0-reducible to Majority.

  $\rightsquigarrow$ Majority is TC^0-complete.

Reductions

- For a formal language $L \subseteq \{0,1\}^*$, $\mathsf{AC}^0(L)$ allows additionally oracle gates for L.
- $L' \in \mathsf{AC}^0(L)$ means L' is AC^0-reducible to L.
- Every problem in TC^0 is AC^0-reducible to Majority.
  $\rightsquigarrow$ Majority is TC^0-complete.

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

Again, 1 encodes 1 and 0 encodes -1. For $u \in \{0,1\}^*$:

$$\begin{aligned}
\mathrm{Maj}(u) &\iff |u|_1 \geq |u|_0 \\
&\iff \bigvee_{0 \leq i \leq |u|} \left|u0^i\right|_1 = \left|u0^i\right|_0 \\
&\iff \bigvee_{0 \leq i \leq |u|} (u0^i \text{ represents } 0 \text{ in } \mathbb{Z})
\end{aligned}$$

Reductions

- For a formal language $L \subseteq \{0,1\}^*$, $\mathsf{AC}^0(L)$ allows additionally oracle gates for L.
- $L' \in \mathsf{AC}^0(L)$ means L' is AC^0-reducible to L.
- Every problem in TC^0 is AC^0-reducible to Majority.

  $\rightsquigarrow$ Majority is TC^0-complete.

- $\mathsf{TC}^0 = \mathsf{AC}^0(\mathrm{WP}(\mathbb{Z})) \subseteq \mathsf{AC}^0(\mathrm{WP}(F_2))$
- $\mathsf{AC}^0(\mathrm{WP}(F_2)) \subseteq \mathsf{LOGSPACE}$

Overview: small circuit classes

AC^0	$= \mathsf{FO}(+,*)$	$\mathbb{Z}/n\mathbb{Z}$ with one monoid generator
ACC^0	$= \mathsf{FO}(+,*;\mathrm{Mod})$	finite solvable
TC^0	$= \mathsf{FO}(+,*;\mathrm{Maj})$	$\mathbb{Z}$, linear solvable (e. g. nilpotent), free solvable
$\mathsf{NC}^1 = \mathsf{AC}^0(\mathrm{WP}(A_5))$		finite non-solvable, regular languages
$\mathsf{AC}^0(\mathrm{WP}(F_2))$		virtually free, Baumslag-Solitar groups, RAAGs, free products
LOGSPACE		linear groups
NC		hyperbolic groups
P	polynomial time	compressed word problem of free groups, etc.

Aim: subgroup membership problem in nilpotent groups.

Greatest Common Divisors

Aim: subgroup membership problem in nilpotent groups.

Why compute greatest common divisors?

Aim: subgroup membership problem in nilpotent groups.

Why compute greatest common divisors?

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.

Why compute greatest common divisors?

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

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

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

Greatest Common Divisors

Observation

If $a_1, \ldots, a_n \in \mathbb{Z}$ are given in unary (a_i is represented by $\underbrace{11\cdots1}_{a_i \text{ many}}0\cdots0$), then the gcd can be computed in TC^0.

Greatest Common Divisors

Observation

If $a_1, \ldots, a_n \in \mathbb{Z}$ are given in unary (a_i is represented by $\underbrace{11\cdots1}_{a_i \text{ many}}0\cdots0$), then the gcd can be computed in TC^0.

Proof

Let $m = \max\{\,|a_i|\,\}$. For all $d \leq m$ do the following:

- check for all i whether there is some $c_i \leq m$ with $dc_i = a_i$ (by trying all possible values $-m \leq c_i \leq m$)

Greatest Common Divisors

Observation

If $a_1, \ldots, a_n \in \mathbb{Z}$ are given in unary (a_i is represented by $\underbrace{11\cdots1}_{a_i \text{ many}}0\cdots0$), then the gcd can be computed in TC^0.

Proof

Let $m = \max\{\,|a_i|\,\}$. For all $d \leq m$ do the following:

- check for all i whether there is some $c_i \leq m$ with $dc_i = a_i$ (by trying all possible values $-m \leq c_i \leq m$)

The largest d for which there are such c_i is the gcd.

Greatest Common Divisors

Observation

If $a_1, \ldots, a_n \in \mathbb{Z}$ are given in unary (a_i is represented by $\underbrace{11\cdots1}_{a_i \text{ many}}0\cdots0$), then the gcd can be computed in TC^0.

Proof

Let $m = \max\{\,|a_i|\,\}$. For all $d \leq m$ do the following:

- check for all i whether there is some $c_i \leq m$ with $dc_i = a_i$ (by trying all possible values $-m \leq c_i \leq m$)

The largest d for which there are such c_i is the gcd.

This requires $2nm^2$ multiplications – all of them can be done in parallel – and one computation of the maximum.

Greatest Common Divisors

Observation

If $a_1, \ldots, a_n \in \mathbb{Z}$ are given in unary (a_i is represented by $\underbrace{11\cdots1}_{a_i \text{ many}}0\cdots0$), then the gcd can be computed in TC^0.

Proof

Let $m = \max\{\,|a_i|\,\}$. For all $d \leq m$ do the following:

- check for all i whether there is some $c_i \leq m$ with $dc_i = a_i$ (by trying all possible values $-m \leq c_i \leq m$)

The largest d for which there are such c_i is the gcd.

This requires $2nm^2$ multiplications – all of them can be done in parallel – and one computation of the maximum.

Corollary

The subgroup membership problem of $\mathbb{Z}$ (where group elements are given as words over the generators) is in TC^0.

Greatest Common Divisors

Subgroup membership problem of $\mathbb{Z}^2$:

Given $a, b, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, is $(a, b) \in \langle (a_1, b_1), \ldots, (a_n, b_n) \rangle$?
With other words are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n \quad \text{and} \quad b = x_1 b_1 + \cdots + x_n b_n?$$

Greatest Common Divisors

Subgroup membership problem of $\mathbb{Z}^2$:

Given $a, b, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, is $(a, b) \in \langle (a_1, b_1), \ldots, (a_n, b_n) \rangle$?
With other words are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n \quad \text{and} \quad b = x_1 b_1 + \cdots + x_n b_n?$$

(1) Compute $d = \gcd(a_1, \ldots, a_n)$ and check whether $d \nmid a$.

Greatest Common Divisors

Subgroup membership problem of $\mathbb{Z}^2$:

Given $a, b, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, is $(a, b) \in \langle (a_1, b_1), \ldots, (a_n, b_n) \rangle$?
With other words are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n \quad \text{and} \quad b = x_1 b_1 + \cdots + x_n b_n?$$

(1) Compute $d = \gcd(a_1, \ldots, a_n)$ and check whether $d \nmid a$.
(2) Compute $y_1, \ldots, y_n \in \mathbb{Z}$ with $d = y_1 a_1 + \cdots + y_n a_n$

Subgroup membership problem of $\mathbb{Z}^2$:

Given $a, b, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, is $(a, b) \in \langle (a_1, b_1), \ldots, (a_n, b_n) \rangle$?
With other words are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n \quad \text{and} \quad b = x_1 b_1 + \cdots + x_n b_n?$$

(1) Compute $d = \gcd(a_1, \ldots, a_n)$ and check whether $d \nmid a$.
(2) Compute $y_1, \ldots, y_n \in \mathbb{Z}$ with $d = y_1 a_1 + \cdots + y_n a_n$
(3) Add a new pair (a_{n+1}, b_{n+1}) with $a_{n+1} = d$ and $b_{n+1} = y_1 b_1 + \cdots + y_n b_n$.

Greatest Common Divisors

Subgroup membership problem of $\mathbb{Z}^2$:

Given $a, b, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, is $(a, b) \in \langle (a_1, b_1), \ldots, (a_n, b_n) \rangle$?
With other words are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n \quad \text{and} \quad b = x_1 b_1 + \cdots + x_n b_n?$$

(1) Compute $d = \gcd(a_1, \ldots, a_n)$ and check whether $d \nmid a$.
(2) Compute $y_1, \ldots, y_n \in \mathbb{Z}$ with $d = y_1 a_1 + \cdots + y_n a_n$
(3) Add a new pair (a_{n+1}, b_{n+1}) with $a_{n+1} = d$ and $b_{n+1} = y_1 b_1 + \cdots + y_n b_n$.
(4) Subtract from all the other pairs multiples of (a_{n+1}, b_{n+1}), to make the first component zero:

$$(a_i', b_i') = (a_i, b_i) - \frac{a_i}{a_{n+1}} (a_{n+1}, b_{n+1})$$

Greatest Common Divisors

Subgroup membership problem of $\mathbb{Z}^2$:

Given $a, b, a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$, is $(a, b) \in \langle (a_1, b_1), \ldots, (a_n, b_n) \rangle$?
With other words are there $x_1, \ldots, x_n \in \mathbb{Z}$ with

$$a = x_1 a_1 + \cdots + x_n a_n \quad \text{and} \quad b = x_1 b_1 + \cdots + x_n b_n?$$

(1) Compute $d = \gcd(a_1, \ldots, a_n)$ and check whether $d \nmid a$.
(2) Compute $y_1, \ldots, y_n \in \mathbb{Z}$ with $d = y_1 a_1 + \cdots + y_n a_n$
(3) Add a new pair (a_{n+1}, b_{n+1}) with $a_{n+1} = d$ and $b_{n+1} = y_1 b_1 + \cdots + y_n b_n$.
(4) Subtract from all the other pairs multiples of (a_{n+1}, b_{n+1}), to make the first component zero:

$$(a_i', b_i') = (a_i, b_i) - \frac{a_i}{a_{n+1}}(a_{n+1}, b_{n+1})$$

(5) Set $b' = b - \frac{a}{a_{n+1}} b_{n+1}$ and check whether there are $x_1', \ldots, x_n' \in \mathbb{Z}$ such that $b' = x_1' b_1' + \cdots + x_n' b_n'$

Greatest Common Divisors as linear combinations

Question

Given $a_1, \dots, a_n \in \mathbb{Z}$ encoded in unary. Can $x_1, \dots, x_n \in \mathbb{Z}$ (in unary) with $d = x_1 a_1 + \cdots + x_n a_n$ be computed in TC^0?

Greatest Common Divisors as linear combinations

Question

Given $a_1, \ldots, a_n \in \mathbb{Z}$ encoded in unary. Can $x_1, \ldots, x_n \in \mathbb{Z}$ (in unary) with $d = x_1 a_1 + \cdots + x_n a_n$ be computed in TC^0?

If $a_1, \ldots, a_n \in \mathbb{Z}$ are encoded in binary,

- it is not known whether the gcd can be computed in NC.
- finding the smallest $x_1, \ldots, x_n \in \mathbb{Z}$ is NP-complete (Majewski, Havas, 1994).

Greatest Common Divisors as linear combinations

Question

Given $a_1, \dots, a_n \in \mathbb{Z}$ encoded in unary. Can $x_1, \dots, x_n \in \mathbb{Z}$ (in unary) with $d = x_1 a_1 + \dots + x_n a_n$ be computed in TC^0?

Straightforward solution (try all possible values) does not work because there are too many:

Greatest Common Divisors as linear combinations

Question

Given $a_1, \dots, a_n \in \mathbb{Z}$ encoded in unary. Can $x_1, \dots, x_n \in \mathbb{Z}$ (in unary) with $d = x_1 a_1 + \cdots + x_n a_n$ be computed in TC^0?

Straightforward solution (try all possible values) does not work because there are too many: Let $m = \max\{\,|a_i|\,\}$. There are $x_1, \dots, x_n \in \mathbb{Z}$ with $|x_i| \leq m/2$ – this is the best known upper bound (Majewski, Havas, 1994).

$\rightsquigarrow$ m^n possible choices for the x_i to try.

Question

Given $a_1, \ldots, a_n \in \mathbb{Z}$ encoded in unary. Can $x_1, \ldots, x_n \in \mathbb{Z}$ (in unary) with $d = x_1 a_1 + \cdots + x_n a_n$ be computed in TC^0?

Straightforward solution (try all possible values) does not work because there are too many: Let $m = \max\{\,|a_i|\,\}$. There are $x_1, \ldots, x_n \in \mathbb{Z}$ with $|x_i| \leq m/2$ – this is the best known upper bound (Majewski, Havas, 1994).

$\rightsquigarrow$ m^n possible choices for the x_i to try.

However, if $n = 2$, there are only m^2 many values to try $\rightsquigarrow$ TC^0.

We can use this idea to compute $x_1, \ldots, x_n$ in TC^0:

Greatest Common Divisors as linear combinations

First, set $d_0 = 0$ compute

$$d_i = \gcd(a_1, \ldots, a_i) \quad \text{for } i = 1, \ldots, n$$

$$\rightsquigarrow \qquad d_i = \gcd(d_{i-1}, a_i).$$

For each i, compute integers y_i and z_i such that $d_i = y_i d_{i-1} + z_i a_i$.
Next compute

$$x_i = z_i \cdot \prod_{j=i+1}^{n} y_j$$

in TC^0 using iterated multiplication. Now, we have

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

Greatest Common Divisors as linear combinations

First, set $d_0 = 0$ compute

$$d_i = \gcd(a_1, \ldots, a_i) \quad \text{for } i = 1, \ldots, n$$

$$\rightsquigarrow \qquad d_i = \gcd(d_{i-1}, a_i).$$

For each i, compute integers y_i and z_i such that $d_i = y_i d_{i-1} + z_i a_i$.
Next compute

$$x_i = z_i \cdot \prod_{j=i+1}^{n} y_j$$

in TC^0 using iterated multiplication. Now, we have

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

Problem: can compute the x_i only in binary in TC^0.

Greatest Common Divisors as linear combinations

First, set $d_0 = 0$ compute

$$d_i = \gcd(a_1, \ldots, a_i) \quad \text{for } i = 1, \ldots, n$$

$$\rightsquigarrow \qquad d_i = \gcd(d_{i-1}, a_i).$$

For each i, compute integers y_i and z_i such that $d_i = y_i d_{i-1} + z_i a_i$.
Next compute

$$x_i = z_i \cdot \prod_{j=i+1}^{n} y_j$$

in TC^0 using iterated multiplication. Now, we have

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

Problem: can compute the x_i only in binary in TC^0.

$\rightsquigarrow$ we have to make them smaller.

Greatest Common Divisors as linear combinations

How to make them small?

Greatest Common Divisors as linear combinations

How to make them small?

If $n = 2$, this is easy:
Assume $a, b > 0$ and $ax + by = \gcd(a, b)$ with $x \geq b$. Set $p = \left\lfloor \frac{x}{b} \right\rfloor$ and replace

- x by $x - bp$ and
- y by $y + ap$.

How to make them small?

If $n = 2$, this is easy:
Assume $a, b > 0$ and $ax + by = \gcd(a, b)$ with $x \geq b$. Set $p = \left\lfloor \frac{x}{b} \right\rfloor$ and replace

- x by $x - bp$ and
- y by $y + ap$.

If $n > 2$, we can apply this method for selected pairs in parallel.

Greatest Common Divisors as linear combinations

How to make them small?

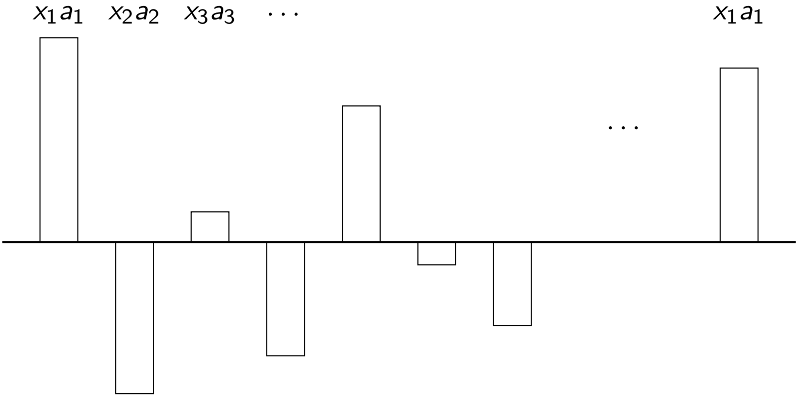
If $n = 2$, this is easy:
Assume $a, b > 0$ and $ax + by = \gcd(a, b)$ with $x \geq b$. Set $p = \left\lfloor \frac{x}{b} \right\rfloor$ and replace

- x by $x - bp$ and
- y by $y + ap$.

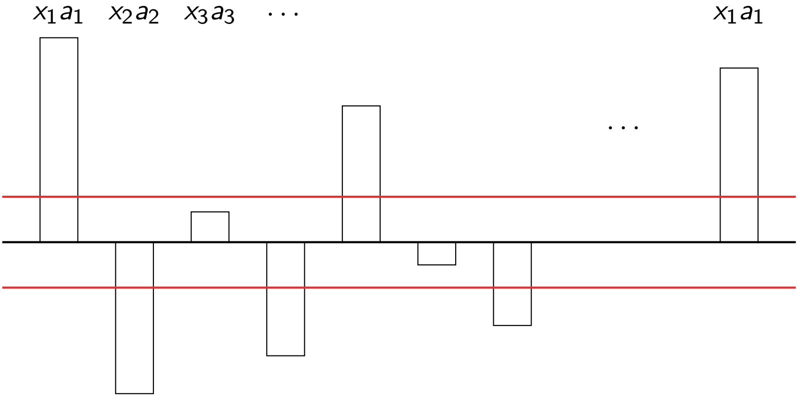
If $n > 2$, we can apply this method for selected pairs in parallel.

For which pairs?

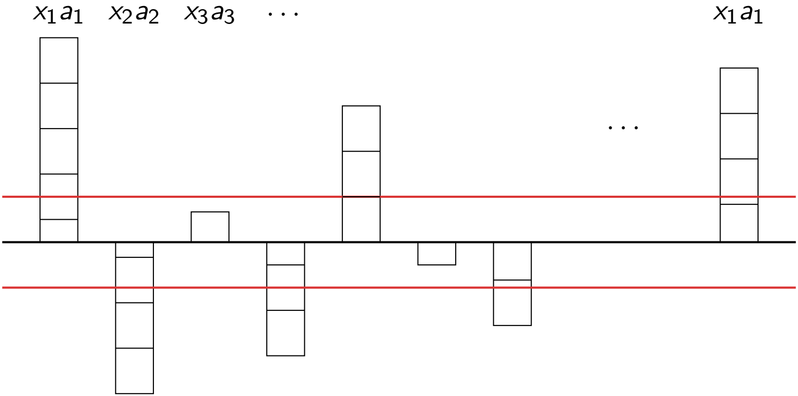
Greatest Common Divisors as linear combinations



Greatest Common Divisors as linear combinations

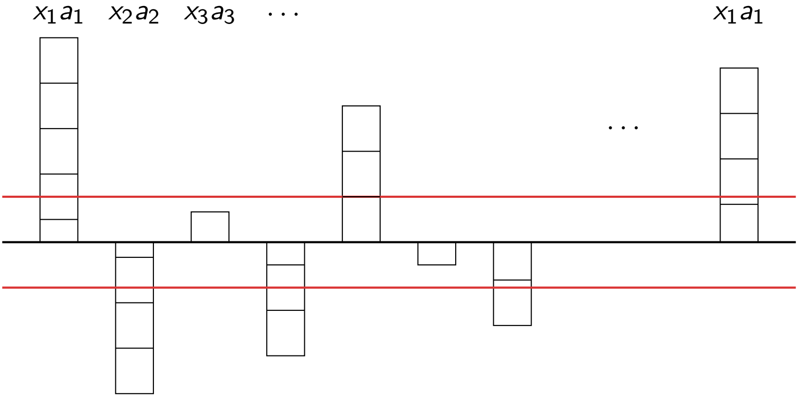


Greatest Common Divisors as linear combinations



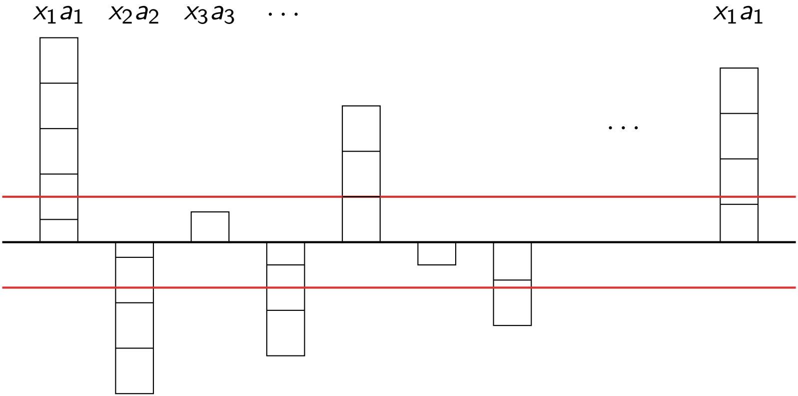
- Blocks of size $\max \{ a_i^2 \}$

Greatest Common Divisors as linear combinations



- Blocks of size $\max \{ a_i^2 \}$
- Using iterated addition, we can compute how many blocks from column i should go to column j in TC^0.

Greatest Common Divisors as linear combinations



- Blocks of size $\max\{ a_i^2 \}$
- Using iterated addition, we can compute how many blocks from column i should go to column j in TC^0.
- Use idea for $n = 2$ to approximate blocks moved from column i to column j.

Greatest common divisors in TC^0

Theorem (Myasnikov, W., 2016)

There is a family of TC^0 circuits for the following problem: given $a_1, \ldots, a_n \in \mathbb{Z}$ encoded in unary, compute $x_1, \ldots, x_n \in \mathbb{Z}$ in unary with $d = x_1 a_1 + \cdots + x_n a_n$.

Greatest common divisors in TC^0

Theorem (Myasnikov, W., 2016)

There is a family of TC^0 *circuits for the following problem: given* $a_1, \ldots, a_n \in \mathbb{Z}$ *encoded in unary, compute* $x_1, \ldots, x_n \in \mathbb{Z}$ *in unary with* $d = x_1 a_1 + \cdots + x_n a_n$.

Corollary

Let G *be a free abelian group. Then the subgroup membership problem for* G *is in* TC^0.

Definition

A group G is nilpotent of class c if

$$G = \Gamma_1(G) \geq \Gamma_2(G) \geq \cdots \Gamma_c(G) > \Gamma_{c+1}(G) = \{1\}$$

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

Definition

A group G is nilpotent of class c if

$$G = \Gamma_1(G) \geq \Gamma_2(G) \geq \cdots \Gamma_c(G) > \Gamma_{c+1}(G) = \{1\}$$

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

Definition

A group G is nilpotent of class c if

$$G = \Gamma_1(G) \geq \Gamma_2(G) \geq \cdots \Gamma_c(G) > \Gamma_{c+1}(G) = \{1\}$$

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

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

Let G be a nilpotent group. The (uniform) subgroup membership problem for G is in LOGSPACE.

The proof is based on so-called matrix reduction (Sims, 1994).

Mal'cev coordinates

Let G be a nilpotent group with Mal'cev basis $(a_1, \ldots, a_m) = \vec{a}$.

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

$$g = a_1^{x_1} \cdots a_m^{x_m} =: \vec{a}^{\vec{x}}$$

with $\vec{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^n$ (if there is torsion some of them are restricted $0 \leq x_i < e_i$) and such that

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

Mal'cev coordinates

Let G be a nilpotent group with Mal'cev basis $(a_1, \ldots, a_m) = \vec{a}$.

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

$$g = a_1^{x_1} \cdots a_m^{x_m} =: \vec{a}^{\vec{x}}$$

  with $\vec{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^n$ (if there is torsion some of them are restricted $0 \leq x_i < e_i$) and such that

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

- The product of two elements can be written in the same fashion

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{q_1} \cdots a_m^{q_m} .$$

  The exponents $q_1, \ldots, q_m$ are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ – if G is torsion-free they are polynomials.

Mal'cev coordinates

Let G be a nilpotent group with Mal'cev basis $(a_1, \ldots, a_m) = \vec{a}$.

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

$$g = a_1^{x_1} \cdots a_m^{x_m} =: \vec{a}^{\vec{x}}$$

with $\vec{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^n$ (if there is torsion some of them are restricted $0 \le x_i < e_i$) and such that

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

- The product of two elements can be written in the same fashion

$$a_1^{x_1} \cdots a_m^{x_m} \cdot a_1^{y_1} \cdots a_m^{y_m} = a_1^{q_1} \cdots a_m^{q_m} .$$

The exponents $q_1, \ldots, q_m$ are functions of $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$ – if G is torsion-free they are polynomials.

Fact

$$q_i(0, \ldots, 0, x_i, \ldots, x_m, y_1, \ldots, y_m) = x_i + y_i \pmod{e_i}$$

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 coordinate 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 coordinate of h_i.

We do "Gaussian elimination" until we reach a matrix satisfying (here, π_i is the position of the i-th pivot = first non-zero entry in row i):

(i) $\pi_1 < \pi_2 < \ldots < \pi_s$ (where s is the number of pivots),

(ii) $\alpha_{i\pi_i} > 0$, for all $i = 1, \ldots, n$,

(iii) $0 \leq \alpha_{k\pi_i} < \alpha_{i\pi_i}$, for all $1 \leq k < i \leq s$

(iv) if $e_{\pi_i} < \infty$, then $\alpha_{i\pi_i}$ divides e_{π_i}, for $i = 1, \ldots, s$.

(v) $H \cap \langle a_i, a_{i+1}, \ldots, a_m \rangle$ is generated by $\{h_j \mid \pi_j \geq i\}$, for all $1 \leq i \leq m$.

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 coordinate of h_i.

We do "Gaussian elimination" until we reach a matrix satisfying (here, π_i is the position of the i-th pivot = first non-zero entry in row i):

(i) $\pi_1 < \pi_2 < \ldots < \pi_s$ (where s is the number of pivots),

(ii) $\alpha_{i\pi_i} > 0$, for all $i = 1, \ldots, n$,

(iii) $0 \leq \alpha_{k\pi_i} < \alpha_{i\pi_i}$, for all $1 \leq k < i \leq s$

(iv) if $e_{\pi_i} < \infty$, then $\alpha_{i\pi_i}$ divides e_{π_i}, for $i = 1, \ldots, s$.

(v) $H \cap \langle a_i, a_{i+1}, \ldots, a_m \rangle$ is generated by $\{h_j \mid \pi_j \geq i\}$, for all $1 \leq i \leq m$.

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
Let $H = \langle h_1, h_2 \rangle$ with

$$h_1 = a_1^6 a_2^2 a_3, \qquad h_2 = a_1^4 a_2^2.$$

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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

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

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $\gcd(6, 4) = 2 = 6 - 4$.

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1}$.

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1} = a_1^6 a_2^2 a_3 \, (a_1^4 a_2^2)^{-1}$.

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1} = a_1^6 a_2^2 a_3\, a_1^{-4} a_2^{-2} a_3^{-8}$.

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
Let $H = \langle h_1, h_2 \rangle$ with

$$h_1 = a_1^6 a_2^2 a_3, \qquad\qquad h_2 = a_1^4 a_2^2.$$

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 $h_4 = h_1 h_2^{-1} = a_1^2 a_2^{-2} a_3^1$.

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

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1} = a_1^2 a_2^{-2} a_3^1$.
- Replace h_1 by $h_1' = h_1 h_4^{-3}$ and h_2 by $h_2' = h_2 h_4^{-2}$

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

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
Let $H = \langle h_1, h_2 \rangle$ with

$$h_1 = a_1^6 a_2^2 a_3, \qquad\qquad h_2 = a_1^4 a_2^2.$$

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 $h_4 = h_1 h_2^{-1} = a_1^2 a_2^{-2} a_3^1$.
- Replace h_1 by $h_1' = h_1 h_4^{-3}$ and h_2 by $h_2' = h_2 h_4^{-2}$

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

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1} = a_1^2 a_2^{-2} a_3^1$.
- Replace h_1 by $h_1' = h_1 h_4^{-3}$ and h_2 by $h_2' = h_2 h_4^{-2}$
- Exchange first and last row and eliminate unnecessary row

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

Example: Matrix reduction

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1} = a_1^2 a_2^{-2} a_3^1$.
- Replace h_1 by $h_1' = h_1 h_4^{-3}$ and h_2 by $h_2' = h_2 h_4^{-2}$
- 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

Let $G = \langle a_1, a_2, a_3 \mid [a_1, a_3] = [a_2, a_3] = 1,\ [a_1, a_2] = a_3 \rangle$ be the 3-dimensional Heisenberg group with Mal'cev basis (a_1, a_2, a_3).
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 $h_4 = h_1 h_2^{-1} = a_1^2 a_2^{-2} a_3^1$.
- Replace h_1 by $h_1' = h_1 h_4^{-3}$ and h_2 by $h_2' = h_2 h_4^{-2}$
- Exchange first and last row and eliminate unnecessary row
- Add commutators

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

Matrix reduction

There are only a constant number of columns $\rightsquigarrow$ only a constant number of step and each can be done in TC^0.

Theorem (Myasnikov, W.)

Given $h_1, \ldots, h_n \in G$ (either as unary encoded Mal'cev coordinates or as words over the generators), Matrix reduction for the subgroup $\langle h_1, \ldots, h_n \rangle$ is in TC^0.

Matrix reduction

There are only a constant number of columns $\rightsquigarrow$ only a constant number of step and each can be done in TC^0.

Theorem (Myasnikov, W.)

Given $h_1, \ldots, h_n \in G$ (either as unary encoded Mal'cev coordinates or as words over the generators), Matrix reduction for the subgroup $\langle h_1, \ldots, h_n \rangle$ is in TC^0.

Corollary (Myasnikov, W.)

Let G be a nilpotent group. The (uniform) subgroup membership problem for G is in TC^0.

More problems in TC^0

Uniform algorithms/circuits for r-generated class c nilpotent groups where r and c are fixed (Macdonald, Ovchinnikov, Myasnikov, W. – work in progress).

- Conjugacy problem
- Compute kernels and images of homomorphisms
- Compute centralizers
- Compute coset intersection
- Compute torsion subgroup

More problems in TC^0

Uniform algorithms/circuits for r-generated class c nilpotent groups where r and c are fixed (Macdonald, Ovchinnikov, Myasnikov, W. – work in progress).

- Conjugacy problem
- Compute kernels and images of homomorphisms
- Compute centralizers
- Compute coset intersection
- Compute torsion subgroup

Thank you!