Conjugacy in Baumslag's group, generic case complexity, and division in power circuits

Volker Diekert[1], Alexei G. Myasnikov[2], **Armin Weiß**[1]

[1]FMI, Universität Stuttgart, Germany

[2]Department of Mathematics, Stevens Institute of Technology, Hoboken, NJ, USA

Montevideo, March 31, 2014

Dehn's fundamental problems

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

Dehn's fundamental problems

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

- Word problem. Is $w \in \Sigma^* = 1$ in G?

Dehn's fundamental problems

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

- Word problem. Is $w \in \Sigma^* = 1$ in G?
- Conjugacy problem. Given $v, w \in \Sigma^*$. Question: $v \sim w$? This means, is there some $z \in G$ such that $zvz^{-1} = w$?

Dehn's fundamental problems

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

- Word problem. Is $w \in \Sigma^* = 1$ in G?
- Conjugacy problem. Given $v, w \in \Sigma^*$. Question: $v \sim w$? This means, is there some $z \in G$ such that $zvz^{-1} = w$?

Here: conjugacy problem.

The Baumslag-Solitar group, a semi-direct product

Baumslag-Solitar group: $\mathbf{BS}_{1,2} = \mathbb{Z}[1/2] \rtimes \mathbb{Z}$
$$= \{ (r, m) \mid r \in \mathbb{Z}[1/2], m \in \mathbb{Z} \}$$

($\mathbb{Z}[1/2] = \{ p/2^q \in \mathbb{Q} \mid p, q \in \mathbb{Z} \}$), with multiplication

$$(r, m) \cdot (s, q) = (r + 2^m s, m + q).$$

The Baumslag-Solitar group, a semi-direct product

Baumslag-Solitar group: $\mathbf{BS}_{1,2} = \mathbb{Z}[1/2] \rtimes \mathbb{Z}$
$= \{\, (r, m) \;\mid\; r \in \mathbb{Z}[1/2], m \in \mathbb{Z} \,\}$

$(\mathbb{Z}[1/2] = \{\, p/2^q \in \mathbb{Q} \;\mid\; p, q \in \mathbb{Z} \,\})$, with multiplication

$$(r, m) \cdot (s, q) = (r + 2^m s, m + q).$$

Theorem (D., M., W.)

The conjugacy problem of $\mathbf{BS}_{1,2}$ *is* TC^0*-complete.*

Proof: see proceedings, uses DIVISION is in uniform TC^0 (Hesse, 2001).

The Baumslag(-Gersten) group

$$\text{Baumslag group:}\quad \mathbf{G}_{1,2} = \mathbf{BS}_{1,2} * \langle b \rangle \,/\, \{\, b\,(1,0)\,b^{-1} = (0,1) \,\}$$
$$= \left\langle a, b \mid (bab^{-1})\,a\,(bab^{-1})^{-1} = a^2 \right\rangle$$

The Baumslag group is an HNN extension of the Baumslag-Solitar group.

The Baumslag(-Gersten) group

Baumslag group: $$\mathbf{G}_{1,2} = \mathbf{BS}_{1,2} * \langle b \rangle \,/\, \{\, b\,(1,0)\,b^{-1} = (0,1)\,\} = \left\langle a, b \mid (bab^{-1})\,a\,(bab^{-1})^{-1} = a^2 \right\rangle$$

The Baumslag group is an HNN extension of the Baumslag-Solitar group.

Theorem (Myasnikov, Ushakov, Won, 2006)

The word problem of $\mathbf{G}_{1,2}$ is in P*.*

Theorem (D., M., W.)

There is an algorithm to decide the conjugacy problem of $\mathbf{G}_{1,2}$. It runs in polynomial time on a strongly generic subset of inputs.

Generic complexity

A set $S \subseteq \Sigma^*$ is called strongly generic if there is some $\varepsilon > 0$ such that

$$\frac{|\Sigma^n \setminus S|}{|\Sigma^n|} \leq 2^{-\varepsilon n}.$$

Generic complexity

A set $S \subseteq \Sigma^*$ is called strongly generic if there is some $\varepsilon > 0$ such that

$$\frac{|\Sigma^n \setminus S|}{|\Sigma^n|} \leq 2^{-\varepsilon n}.$$

Thus, from a practical viewpoint, "random inputs are always in S".

Difficulty of the word problem in $\mathbf{G}_{1,2}$

τ = tower function: $\tau(0) = 0$, $\tau(n+1) = 2^{\tau(n)}$.

Solving the word problem using Britton reductions:

$$b(k,0)b^{-1} \to (0,k) \qquad b^{-1}(k,0)b \to (0,k)$$

leads to non-elementary blow-up. Define words w_n inductively such that $w_n = (0, \tau(n))$ in $\mathbf{G}_{1,2}$ for $n \geq 0$. More precisely, $w_0 :=$ empty word. Then $w_0 = (0,0) = 1$ in $\mathbf{G}_{1,2}$ and:

$$\begin{aligned} w_{n+1} &:= b \cdot w_n \cdot (1,0) \cdot w_n^{-1} \cdot b^{-1} \\ &= b \cdot (0, \tau(n)) \cdot (1,0) \cdot (0, -\tau(n)) \cdot b^{-1} \\ &= b \cdot (\tau(n+1), 0) \cdot b^{-1} \\ &= (0, \tau(n+1)) \end{aligned}$$

Difficulty of the word problem in $\mathbf{G}_{1,2}$

τ = tower function: $\tau(0) = 0, \qquad \tau(n+1) = 2^{\tau(n)}.$

Solving the word problem using Britton reductions:

$$b(k,0)b^{-1} \to (0,k) \qquad\qquad b^{-1}(k,0)b \to (0,k)$$

leads to non-elementary blow-up. Define words w_n inductively such that $w_n = (0, \tau(n))$ in $\mathbf{G}_{1,2}$ for $n \geq 0$. More precisely, $w_0 :=$ empty word. Then $w_0 = (0,0) = 1$ in $\mathbf{G}_{1,2}$ and:

$$\begin{aligned} w_{n+1} &:= b \cdot w_n \cdot (1,0) \cdot w_n^{-1} \cdot b^{-1} \\ &= b \cdot (0, \tau(n)) \cdot (1,0) \cdot (0, -\tau(n)) \cdot b^{-1} \\ &= b \cdot (\tau(n+1), 0) \cdot b^{-1} \\ &= (0, \tau(n+1)) \end{aligned}$$

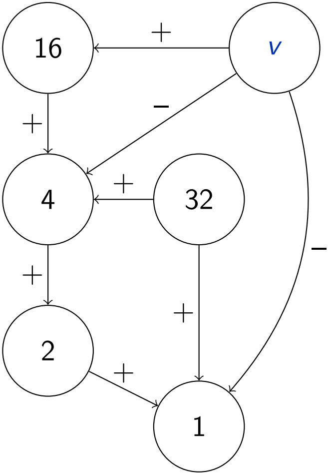
$|w_n| \in 2^{\Theta(n)}$, but w_n is a huge compression for the number $\tau(n)$.

Power circuits

- Write numbers as binary sums $\sum_{i \in I} \alpha_i \cdot 2^{p_i} \quad (\alpha_i \in \{-1, +1\})$
- Recursively repeat this for all p_i

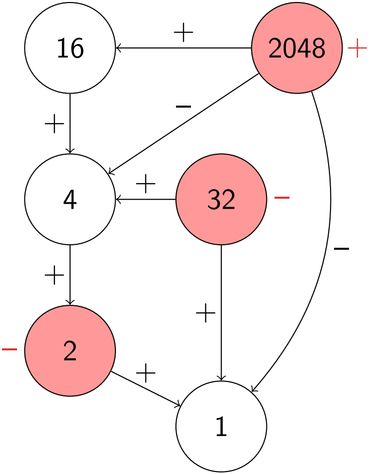
Myasnikov, Ushakov, Won (2006)
in IJAC 2011

$$\varepsilon(v) = 2^{+16-4-1} = 2048$$



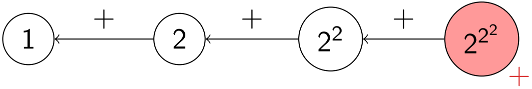
- Write numbers as binary sums $\sum_{i \in I} \alpha_i \cdot 2^{p_i} \quad (\alpha_i \in \{-1, +1\})$
- Recursively repeat this for all p_i

Myasnikov, Ushakov, Won (2006)
in IJAC 2011



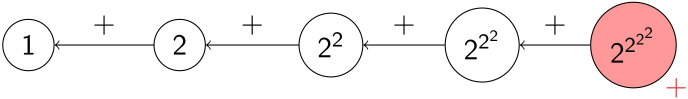
$$\varepsilon(M) = \sum_{v \in M} \pm \varepsilon(v)$$
$$= 2048 - 32 - 2$$
$$= 2014$$

Power circuits can represent huge numbers



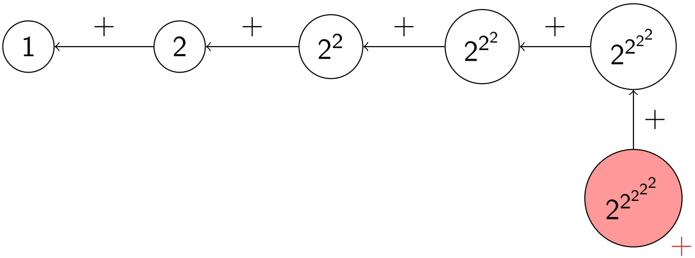
$\varepsilon(M) = 65536$

Power circuits can represent huge numbers



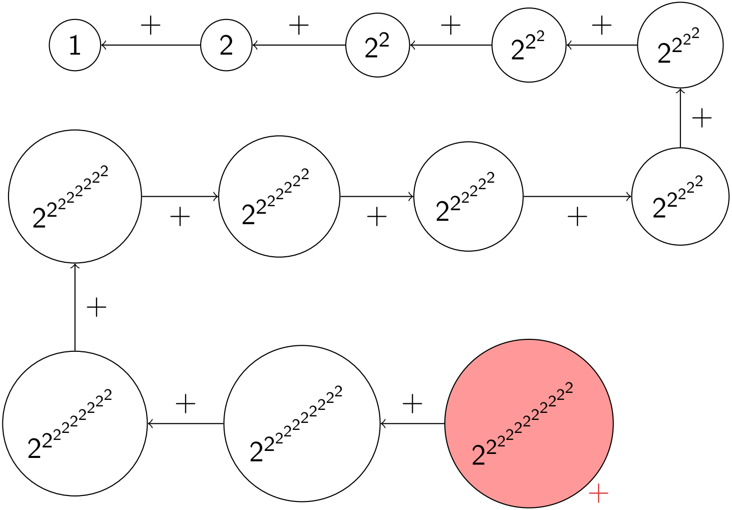
$\varepsilon(M) = 2^{65536} >$ number of atoms in the universe

Power circuits can represent huge numbers



$\varepsilon(M) = 2^{2^{65536}}$ impossible to write down in binary

Power circuits can represent huge numbers



$\varepsilon(M) =$ huuuge number

Solving the word problem in $\mathbf{G}_{1,2}$

Proposition (Myasnikov, Ushakov, Won, 2006)

Basic arithmetic operations (comparison, addition, $(x, y) \mapsto x \cdot 2^y$) in power circuits can be performed in polynomial time and with only a "small" blow-up.

Theorem (Myasnikov, Ushakov, Won, 2006)

The word problem of $\mathbf{G}_{1,2}$ is in P.

Theorem (Diekert, Laun, Ushakov, STACS 2012)

The word problem of $\mathbf{G}_{1,2}$ is can be solved in $\mathcal{O}(n^3)$.

Difficulty of the conjugacy problem in $\mathbf{G}_{1,2}$

In $\mathbf{BS}_{1,2} \leq \mathbf{G}_{1,2}$ we have (for $m \geq 2$)

$$(r, m) \sim_{\mathbf{BS}_{1,2}} (s, q) \iff m = q \text{ and } \exists k \in \mathbb{N} : 0 \leq k < m \text{ such that } (2^m - 1) \mid (r \cdot 2^k - s)$$

$\rightsquigarrow$ need to check divisibility in power circuits.

Difficulty of the conjugacy problem in $\mathbf{G}_{1,2}$

In $\mathbf{BS}_{1,2} \leq \mathbf{G}_{1,2}$ we have (for $m \geq 2$)

$$(r, m) \sim_{\mathbf{BS}_{1,2}} (s, q) \iff m = q \text{ and } \exists k \in \mathbb{N} : 0 \leq k < m \text{ such that } (2^m - 1) \mid (r \cdot 2^k - s)$$

$\rightsquigarrow$ need to check divisibility in power circuits.

Proposition

There is an exponential time reduction from the divisibility problem in power circuits to the conjugacy problem in $\mathbf{G}_{1,2}$.

Divisibility cannot be reduced to modulo

Modulo is impossible in elementary time: $x = 2^{65536}$, $\lambda = 2^x$

$$\left(2^\lambda\right)^x \mod 2^\lambda - \lambda - 1 =$$

Divisibility cannot be reduced to modulo

Modulo is impossible in elementary time: $x = 2^{65536}$, $\lambda = 2^x$

$$\left(2^{\lambda}\right)^x \mod 2^{\lambda} - \lambda - 1 = (\lambda + 1)^x =$$

Divisibility cannot be reduced to modulo

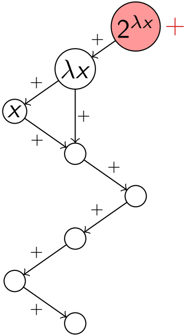
Modulo is impossible in elementary time: $x = 2^{65536}$, $\lambda = 2^x$

$$\left(2^\lambda\right)^x \mod 2^\lambda - \lambda - 1 \;=\; (\lambda+1)^x \;=\; \sum_{i=0}^{x} \binom{x}{i} \lambda^i \;=:\; X$$

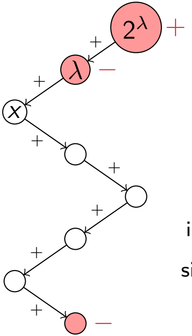
Divisibility cannot be reduced to modulo

Modulo is impossible in elementary time: $x = 2^{65536}$, $\lambda = 2^x$

$$\left(2^\lambda\right)^x \mod 2^\lambda - \lambda - 1 = (\lambda + 1)^x = \sum_{i=0}^{x} \binom{x}{i} \lambda^i =: X$$



mod



$= \underbrace{X}$

impossible to write down
in binary or as power circuit

since compact representation
contains too many 1s

Divisibility in power circuits

- Divisibility test cannot be done in elementary time by calculating modulo.

Divisibility in power circuits

- Divisibility test cannot be done in elementary time by calculating modulo.
- The trivial algorithm (convert to binary) needs non-elementary time.

Divisibility in power circuits

- Divisibility test cannot be done in elementary time by calculating modulo.
- The trivial algorithm (convert to binary) needs non-elementary time.
- There might be another way to check divisibility.

Divisibility in power circuits

- Divisibility test cannot be done in elementary time by calculating modulo.
- The trivial algorithm (convert to binary) needs non-elementary time.
- There might be another way to check divisibility.
- As markings are sums of vertices, it seems unlikely that divisibility can be tested without knowing the modulo value of the vertices.

Divisibility in power circuits

- Divisibility test cannot be done in elementary time by calculating modulo.
- The trivial algorithm (convert to binary) needs non-elementary time.
- There might be another way to check divisibility.
- As markings are sums of vertices, it seems unlikely that divisibility can be tested without knowing the modulo value of the vertices.

Good news: the conjugacy problem in $\mathbf{G}_{1,2}$ is only difficult for elements in $\mathbf{BS}_{1,2}$.

Solving the conjugacy problem in $\mathbf{G}_{1,2}$

Lemma (Collin's Lemma for HNN extensions)

Let $v, w \in \{(0,1),(1,0),(0,-1),(-1,0),b,b^{-1}\}^*$ be cyclically reduced words (no factor $b(k,0)b^{-1}$ or $b^{-1}(0,k)b$ in vv and ww) such that in v and w occurs at least one letter b or b^{-1}. Then $v \sim w$ if and only if there is a cyclic permutation w' of w and some $x \in \mathbf{BS}_{1,2}$ such that $v = xw'x^{-1}$.

Solving the conjugacy problem in $\mathbf{G}_{1,2}$

Lemma (Collin's Lemma for HNN extensions)

Let $v, w \in \left\{(0,1),(1,0),(0,-1),(-1,0),b,b^{-1}\right\}^*$ be cyclically reduced words (no factor $b(k,0)b^{-1}$ or $b^{-1}(0,k)b$ in vv and ww) such that in v and w occurs at least one letter b or b^{-1}. Then $v \sim w$ if and only if there is a cyclic permutation w' of w and some $x \in \mathbf{BS}_{1,2}$ such that $v = xw'x^{-1}$.

- There are only linearly many candidates for w'.

Solving the conjugacy problem in $\mathbf{G}_{1,2}$

Lemma (Collin's Lemma for HNN extensions)

Let $v, w \in \left\{(0,1),(1,0),(0,-1),(-1,0),b,b^{-1}\right\}^*$ be cyclically reduced words (no factor $b(k,0)b^{-1}$ or $b^{-1}(0,k)b$ in vv and ww) such that in v and w occurs at least one letter b or b^{-1}. Then $v \sim w$ if and only if there is a cyclic permutation w' of w and some $x \in \mathbf{BS}_{1,2}$ such that $v = xw'x^{-1}$.

- There are only linearly many candidates for w'.
- If $v, w \notin \mathbf{BS}_{1,2}$, then some $x \in \mathbf{BS}_{1,2}$ with $v = xw'x^{-1}$ can be determined using only division by powers of 2.
  $\rightsquigarrow$ such x can be determined in polynomial time.

Solving the conjugacy problem in $\mathbf{G}_{1,2}$

Lemma (Collin's Lemma for HNN extensions)

Let $v, w \in \{(0,1), (1,0), (0,-1), (-1,0), b, b^{-1}\}^*$ be cyclically reduced words (no factor $b(k,0)b^{-1}$ or $b^{-1}(0,k)b$ in vv and ww) such that in v and w occurs at least one letter b or b^{-1}. Then $v \sim w$ if and only if there is a cyclic permutation w' of w and some $x \in \mathbf{BS}_{1,2}$ such that $v = xw'x^{-1}$.

- There are only linearly many candidates for w'.
- If $v, w \notin \mathbf{BS}_{1,2}$, then some $x \in \mathbf{BS}_{1,2}$ with $v = xw'x^{-1}$ can be determined using only division by powers of 2.
  $\rightsquigarrow$ such x can be determined in polynomial time.

Proposition

The conjugacy problem of $\mathbf{G}_{1,2}$ for elements $v, w \notin \mathbf{BS}_{1,2}$ is in P.

Solving the conjugacy problem in $\mathbf{G}_{1,2}$

Theorem

The set $\{a, a^{-1}, b, b^{-1}\}^* \setminus \mathbf{BS}_{1,2}$ *is strongly generic in* $\{ a, a^{-1}, b, b^{-1} \}^*$.

Proof.

- By random walk techniques.
- Uses the fact that Britton reductions can be described by Dyck words.

$\square$

Corollary

There is an algorithm to decide the conjugacy problem of $\mathbf{G}_{1,2}$. *It runs in polynomial time on a strongly generic subset of inputs.*

Conclusion

- The conjugacy problem of $\mathbf{G}_{1,2}$ is strongly generically in P.
- Our algorithm has non-elementary average case complexity.

Conclusion

- The conjugacy problem of $\mathbf{G}_{1,2}$ is strongly generically in P.
- Our algorithm has non-elementary average case complexity.

Conjecture

The conjugacy problem in $\mathbf{G}_{1,2}$ is not solvable in elementary time on average.

Conclusion

- The conjugacy problem of $\mathbf{G}_{1,2}$ is strongly generically in P.
- Our algorithm has non-elementary average case complexity.

Conjecture

The conjugacy problem in $\mathbf{G}_{1,2}$ is not solvable in elementary time on average.

- Lower bounds for the divisibility problem in power circuits?

Conclusion

- The conjugacy problem of $\mathbf{G}_{1,2}$ is strongly generically in P.
- Our algorithm has non-elementary average case complexity.

Conjecture

The conjugacy problem in $\mathbf{G}_{1,2}$ is not solvable in elementary time on average.

- Lower bounds for the divisibility problem in power circuits?
- Complexity of the conjugacy problem of $\mathbf{BS}_{p,q} = \left\langle a, t \mid ta^p t^{-1} = a^q \right\rangle$ for $|p|, |q| > 1$?

Conjecture

The conjugacy problem in $\mathbf{BS}_{p,q}$ is in LOGSPACE.

Conclusion

- The conjugacy problem of $\mathbf{G}_{1,2}$ is strongly generically in P.
- Our algorithm has non-elementary average case complexity.

Conjecture

The conjugacy problem in $\mathbf{G}_{1,2}$ is not solvable in elementary time on average.

- Lower bounds for the divisibility problem in power circuits?
- Complexity of the conjugacy problem of $\mathbf{BS}_{p,q} = \left\langle a, t \mid ta^p t^{-1} = a^q \right\rangle$ for $|p|, |q| > 1$?

Conjecture

The conjugacy problem in $\mathbf{BS}_{p,q}$ is in LOGSPACE.

Thank you!