The power word problem

Markus Lohrey[1] Armin Weiß[2]

[1]Universität Siegen, Germany

[2]Universität Stuttgart, Germany

Aachen, August 27, 2019

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

The word problem

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

- Word problem (WP): Given $w \in \Sigma^*$.
  Question: Is $w = 1$ in G?

The word problem

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

- Word problem (WP): Given $w \in \Sigma^*$.
  Question: Is $w = 1$ in G?

Is $b\,b^{-1}a\,a\,b^{-1}b\,a^{-1}a^{-1} = 1$ in $F(a, b)$?

The word problem

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

- Word problem (WP): Given $w \in \Sigma^*$.
  Question: Is $w = 1$ in G?

Is $b\,b^{-1}a\,a\,b^{-1}b\,a^{-1}a^{-1} = 1$ in $F(a,b)$?

- Compressed word problem: Given a straight-line program $\mathbb{G}$ which produces a word $w \in \Sigma^*$.
  Question: Is $w = 1$ in G?

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

- Word problem (WP): Given $w \in \Sigma^*$.
  Question: Is $w = 1$ in G?

$$\textit{Is} \qquad b\, b^{-1} a\, a\, b^{-1} b\, a^{-1} a^{-1} = 1 \text{ in } F(a,b) \qquad ?$$

- Compressed word problem: Given a straight-line program $\mathbb{G}$ which produces a word $w \in \Sigma^*$.
  Question: Is $w = 1$ in G?

- Power word problem (PowerWP):
  Given $p_1, \dots, p_k \in \Sigma^*$ and $x_1, \dots, x_k \in \mathbb{Z}$.
  Question: $p_1^{x_1} \cdots p_k^{x_k} = 1$ in G?

$$\textit{Is} \qquad b^{123} (b\, a\, a)^{123} a^{-246} b^{-123} (b\, a)^{-123} a^{123} = 1 \qquad ?$$

Why is the power word problem interesting?

- straightforward way of compression

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1 + 1 + \cdots + 1}_{\text{27 ones}}$

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1+1+\cdots+1}_{\text{27 ones}}$
- in nilpotent groups, every element can be expressed by a power word of logarithmic length

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1+1+\cdots+1}_{\text{27 ones}}$
- in nilpotent groups, every element can be expressed by a power word of logarithmic length
- binary encoded matrices in $\mathrm{SL}(2,\mathbb{Z})$ yield power words over the generators (Gurevich, Schupp 2007)

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1+1+\cdots+1}_{\text{27 ones}}$
- in nilpotent groups, every element can be expressed by a power word of logarithmic length
- binary encoded matrices in $\mathrm{SL}(2,\mathbb{Z})$ yield power words over the generators (Gurevich, Schupp 2007)

$$\begin{pmatrix} -499 & 5000 \\ -50 & 501 \end{pmatrix}$$

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1+1+\cdots+1}_{\text{27 ones}}$
- in nilpotent groups, every element can be expressed by a power word of logarithmic length
- binary encoded matrices in $\mathrm{SL}(2,\mathbb{Z})$ yield power words over the generators (Gurevich, Schupp 2007)

$$\begin{pmatrix} -499 & 5000 \\ -50 & 501 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{10} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{50} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-10}$$

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1+1+\cdots+1}_{\text{27 ones}}$
- in nilpotent groups, every element can be expressed by a power word of logarithmic length
- binary encoded matrices in $\mathrm{SL}(2,\mathbb{Z})$ yield power words over the generators (Gurevich, Schupp 2007)

$$\begin{pmatrix} -499 & 5000 \\ -50 & 501 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{10} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{50} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-10}$$

- tool for the knapsack problem in RAAGs (Lohrey, Zetsche, 2015) (Given $p_1, \ldots, p_k, w \in \Sigma^*$, $\exists\, x_1, \ldots, x_k \in \mathbb{N}$ with $p_1^{x_1} \cdots p_k^{x_k} = w$?)

Why is the power word problem interesting?

- straightforward way of compression
- natural for abelian groups: we write 27 instead of $\underbrace{1+1+\cdots+1}_{\text{27 ones}}$
- in nilpotent groups, every element can be expressed by a power word of logarithmic length
- binary encoded matrices in $\mathrm{SL}(2,\mathbb{Z})$ yield power words over the generators (Gurevich, Schupp 2007)

$$\begin{pmatrix} -499 & 5000 \\ -50 & 501 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{10} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{50} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-10}$$

- tool for the knapsack problem in RAAGs (Lohrey, Zetsche, 2015) (Given $p_1, \ldots, p_k, w \in \Sigma^*$, $\exists\, x_1, \ldots, x_k \in \mathbb{N}$ with $p_1^{x_1} \cdots p_k^{x_k} = w$?)
- better understanding of the compressed word problem:
  - lower bounds
  - better upper bounds in the special case

Word problems of free groups

$$F(a,b) = \{a, b, \bar{a}, \bar{b}\}^* / \{a\bar{a} = \bar{a}a = b\bar{b} = \bar{b}b = 1\}$$

Word problems of free groups

$$F(a, b) = \{a, b, \overline{a}, \overline{b}\}^* / \{a\overline{a} = \overline{a}a = b\overline{b} = \overline{b}b = 1\}$$

- The word problem of free groups is in LOGSPACE (Lipton, Zalcstein, 1977).

Word problems of free groups

$$F(a,b) = \{a, b, \bar{a}, \bar{b}\}^* / \{a\bar{a} = \bar{a}a = b\bar{b} = \bar{b}b = 1\}$$

- The word problem of free groups is in LOGSPACE (Lipton, Zalcstein, 1977).
- $\mathrm{WP}(F_k)$ is NC^1-hard for $k \geq 2$ (Robinson, 1993).

Word problems of free groups

$$F(a,b) = \{a, b, \bar{a}, \bar{b}\}^* / \{a\bar{a} = \bar{a}a = b\bar{b} = \bar{b}b = 1\}$$

- The word problem of free groups is in LOGSPACE (Lipton, Zalcstein, 1977).
- $\mathrm{WP}(F_k)$ is NC^1-hard for $k \geq 2$ (Robinson, 1993).
- $\textsc{CompressedWP}(F_k)$ is P-complete for $k \geq 2$ (Lohrey, 2004).

Word problems of free groups

$$F(a, b) = \{a, b, \bar{a}, \bar{b}\}^* / \{a\bar{a} = \bar{a}a = b\bar{b} = \bar{b}b = 1\}$$

- The word problem of free groups is in LOGSPACE (Lipton, Zalcstein, 1977).
- $\mathrm{WP}(F_k)$ is NC^1-hard for $k \geq 2$ (Robinson, 1993).
- $\textsc{Compressed}\mathrm{WP}(F_k)$ is P-complete for $k \geq 2$ (Lohrey, 2004).

Theorem

The power word problem for free groups is in $\mathrm{AC}^0(\mathrm{WP}(F_2))$.

AC^0 = constant-depth, polynomial-size Boolean circuit
$\mathrm{AC}^0(L)$ = AC^0 + oracle gates for L

Word problems of free groups

$$F(a, b) = \{a, b, \bar{a}, \bar{b}\}^* / \{a\bar{a} = \bar{a}a = b\bar{b} = \bar{b}b = 1\}$$

- The word problem of free groups is in LOGSPACE (Lipton, Zalcstein, 1977).
- $\mathrm{WP}(F_k)$ is NC^1-hard for $k \geq 2$ (Robinson, 1993).
- $\textsc{CompressedWP}(F_k)$ is P-complete for $k \geq 2$ (Lohrey, 2004).

Theorem

The power word problem for free groups is in $\mathsf{AC}^0(\mathrm{WP}(F_2))$.

AC^0 = constant-depth, polynomial-size Boolean circuit
$\mathsf{AC}^0(L) = \mathsf{AC}^0$ + oracle gates for L

The proof consists of three steps:

- Preprocessing
- Make exponents small
- Solve regular word problem

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$(a\, b)^{1000}\, a\, b^{-100}\, b^{100}\, a\, b^{-100}\, b^{100}\, \overline{a}\, \overline{a}\, (a\, b)^{-1000}$$

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$(a\,b)^{1000}\,a\,\cancel{b^{-100}}\,\cancel{b^{100}}\,a\,b^{-100}\,b^{100}\,\overline{a}\,\overline{a}\,(a\,b)^{-1000}$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$(a\,b)^{1000}a \qquad\qquad a\,b^{-100}\,b^{100}\overline{a}\;\overline{a}\,(a\,b)^{-1000}$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$(a\,b)^{1000}\,a \qquad\qquad a\,\cancel{b^{-100}}\,\cancel{b^{100}}\,\overline{a}\;\overline{a}\,(a\,b)^{-1000}$$

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$(a\,b)^{1000} a \qquad\qquad a \qquad\qquad \overline{a}\,\overline{a}\,(a\,b)^{-1000}$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$(a\,b)^{1000}\cancel{a} \qquad \cancel{a} \qquad \cancel{\overline{a}}\,\cancel{\overline{a}}(a\,b)^{-1000}$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$(a\,b)^{1000}$ $(a\,b)^{-1000}$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$\cancel{(a\,b)^{1000}}$ $\qquad\qquad$ $\cancel{(a\,b)^{-1000}}$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$\cancel{(a\,b)^{1000}} \qquad\qquad \cancel{(a\,b)^{-1000}} = 1$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$\cancel{(a\,b)^{1000}} \qquad \cancel{(a\,b)^{-1000}} = 1$$

Example 2

$$b^{123}(b\,a\,a)^{123}a^{-246}b^{-123}(\overline{b}\,\overline{a})^{123}a^{123}$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$\cancel{(a\,b)^{1000}} \qquad\qquad \cancel{(a\,b)^{-1000}} = 1$$

Example 2

$$b^{123}(b\,a\,a)^{123}a^{-246}b^{-123}(\overline{b}\,\overline{a})^{123}a^{123} \neq 1$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\bar{a}$ for a^{-1}.

Example 1

$$\cancel{(a\,b)^{1000}} \qquad \cancel{(a\,b)^{-1000}} = 1$$

Example 2

$$b^{123}(b\,a\,a)^{123}a^{-246}b^{-123}(\bar{b}\,\bar{a})^{123}a^{123} \neq 1$$

Example 3

$$(a\,a)^{500}\,(\bar{a})^{999}\,\bar{a}$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$\cancel{(a\,b)^{1000}} \qquad\qquad \cancel{(a\,b)^{-1000}} = 1$$

Example 2

$$b^{123}(b\,a\,a)^{123}a^{-246}b^{-123}(\overline{b}\,\overline{a})^{123}a^{123} \neq 1$$

Example 3

$$(a\,a)^{500}\,(\overline{a})^{999}\,\overline{a} = 1$$

Examples: Power word problem in free groups

Let $F = F(\{a, b\})$ be the free group. Write $\overline{a}$ for a^{-1}.

Example 1

$$\cancel{(a\,b)^{1000}} \qquad \cancel{(a\,b)^{-1000}} = 1$$

Example 2

$$b^{123}(b\,a\,a)^{123}a^{-246}b^{-123}(\overline{b}\,\overline{a})^{123}a^{123} \neq 1$$

Example 3

$$(a\,a)^{500}\,(\overline{a})^{999}\,\overline{a} = 1$$

Example 4

$$(b\,a\,a\,\overline{a}\,b\,a)^{500}\,(b)^{2}\,(\overline{b}\,\overline{b}\,\overline{a}b)^{999}\,(\overline{b}\,\overline{a}\,\overline{b}\,\overline{b}\,a\,b)^{1}(a\,b)^{-1}$$

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,
(2) p is primitive,
(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\left\{\, uv \;\middle|\; vu = p \text{ or } vu = p^{-1} \,\right\}$).

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

$$\Omega = \{ a, b, ab, a\overline{b}, aab, aa\overline{b}, \dots \}$$

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{\, uv \;\big|\; vu = p \text{ or } vu = p^{-1} \,\}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Proof.

- By (1), $v = w^{-1}$ as words.

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Proof.

- By (1), $v = w^{-1}$ as words. $\rightsquigarrow$ v has periods $|p|$ and $|q|$.

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\left\{ uv \;\middle|\; vu = p \text{ or } vu = p^{-1} \right\}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Proof.

- By (1), $v = w^{-1}$ as words. $\rightsquigarrow$ v has periods $|p|$ and $|q|$.
- By Fine and Wilf's theorem v has period $\gcd(|p|, |q|)$.

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y. If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Proof.

- By (1), $v = w^{-1}$ as words. $\rightsquigarrow$ v has periods $|p|$ and $|q|$.
- By Fine and Wilf's theorem v has period $\gcd(|p|, |q|)$.
  $\rightsquigarrow$ also p and q.

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Proof.

- By (1), $v = w^{-1}$ as words. $\rightsquigarrow$ v has periods $|p|$ and $|q|$.
- By Fine and Wilf's theorem v has period $\gcd(|p|, |q|)$.
  $\rightsquigarrow$ also p and q.
- By (2), $|p| = |q|$.

Preprocessing

$\Omega \subseteq \Sigma^+$ is set of non-empty words p with

(1) p is cyclically reduced,

(2) p is primitive,

(3) p is lexicographically minimal among all cyclic permutations of p and p^{-1} (i. e., in $\{ uv \mid vu = p \text{ or } vu = p^{-1} \}$).

Lemma

Let $p, q \in \Omega$ and v a factor of p^x and w a factor of q^y.
If $vw = 1$ in F and $|v| = |w| \geq |p| + |q| - 1$, then $p = q$.

Proof.

- By (1), $v = w^{-1}$ as words. $\rightsquigarrow$ v has periods $|p|$ and $|q|$.
- By Fine and Wilf's theorem v has period $\gcd(|p|, |q|)$.
  $\rightsquigarrow$ also p and q.
- By (2), $|p| = |q|$.
- By (3), since p is a factor of w^{-1}, we get $p = q$. $\square$

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Preprocessing

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

Preprocessing

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

- Freely reduce the q_i (in $\mathrm{AC}^0(\mathrm{WP}(F))$), W., 2016).

Preprocessing

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

- Freely reduce the q_i (in $\mathrm{AC}^0(\mathrm{WP}(F))$), W., 2016).
- Make each q_i cyclically reduced.

Preprocessing

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

- Freely reduce the q_i (in $\mathrm{AC}^0(\mathrm{WP}(F))$, W., 2016).
- Make each q_i cyclically reduced.
- Make each q_i primitive.

Preprocessing

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \qquad (1)$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

- Freely reduce the q_i (in $\mathrm{AC}^0(\mathrm{WP}(F))$), W., 2016).
- Make each q_i cyclically reduced.
- Make each q_i primitive.
- Make q_i lex. minimal in $\left\{ uv \;\middle|\; vu = q_i \text{ or } vu = q_i^{-1} \right\}$.

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

- Freely reduce the q_i (in $\mathrm{AC}^0(\mathrm{WP}(F))$, W., 2016).
- Make each q_i cyclically reduced.
- Make each q_i primitive.
- Make q_i lex. minimal in $\left\{ uv \;\middle|\; vu = q_i \text{ or } vu = q_i^{-1} \right\}$.

This yields $s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n$

Preprocessing

The first aim is to rewrite an input word $q_1^{y_1} \cdots q_n^{y_n}$ in the form

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.} \tag{1}$$

Lemma

Given a power word v, a power word w of the form (1) with $v =_F w$ can be computed in $\mathrm{AC}^0(\mathrm{WP}(F))$.

- Freely reduce the q_i (in $\mathrm{AC}^0(\mathrm{WP}(F))$), W., 2016).
- Make each q_i cyclically reduced.
- Make each q_i primitive.
- Make q_i lex. minimal in $\left\{ uv \;\middle|\; vu = q_i \text{ or } vu = q_i^{-1} \right\}$.

This yields $$s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n$$

- Freely reduce the s_i.

Make exponents small

Now we have a "nice" instance

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.}$$

We know that

- if a long factor of $p_i^{x_i}$ cancels with a factor of $p_j^{x_j}$, then $p_i = p_j$.

Make exponents small

Now we have a "nice" instance

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.}$$

We know that

- if a long factor of $p_i^{x_i}$ cancels with a factor of $p_j^{x_j}$, then $p_i = p_j$.

Idea:

- Decrease all exponents of p_i simultaneously.

Make exponents small

Now we have a "nice" instance

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.}$$

We know that

- if a long factor of $p_i^{x_i}$ cancels with a factor of $p_j^{x_j}$, then $p_i = p_j$.

Idea:

- Decrease all exponents of p_i simultaneously.

But: cannot delete them entirely:

$$a^{100} b\, a^{-100} \overline{b} \neq 1, \text{ but } a^{0} b\, a^{0} \overline{b} = 1$$

Make exponents small

Now we have a "nice" instance

$$w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n \qquad \text{with } p_i \in \Omega \text{ and } s_i \text{ freely reduced.}$$

We know that

- if a long factor of $p_i^{x_i}$ cancels with a factor of $p_j^{x_j}$, then $p_i = p_j$.

Idea:

- Decrease all exponents of p_i simultaneously.

But: cannot delete them entirely:

$$a^{100} b\, a^{-100} \overline{b} \neq 1, \text{ but } a^{0} b\, a^{0} \overline{b} = 1$$

Nor down to 1:

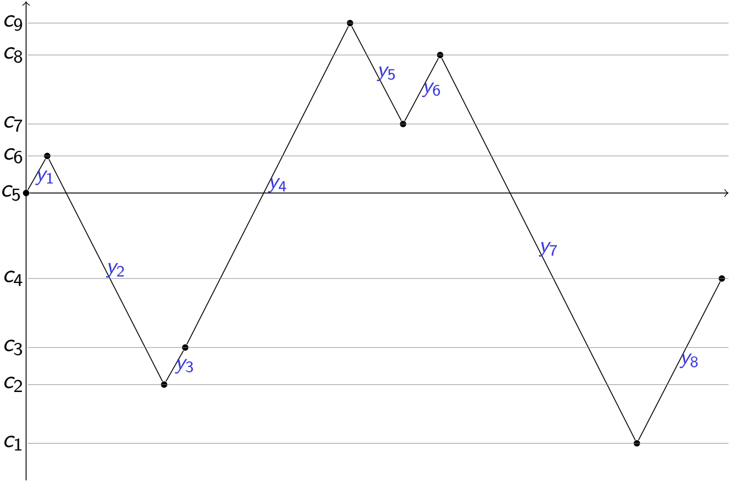
$$a^{100} (\overline{a}\, b\, a)^1 a^{-100} \overline{b} \neq 1 \text{ but } a^{1} (\overline{a}\, b\, a)^1 a^{-1} \overline{b} = 1$$

Make exponents small

For $p \in \Omega$ rite $w = u_0 p^{y_1} u_1 \cdots p^{y_m} u_m$ such that no u_i contains p^x.

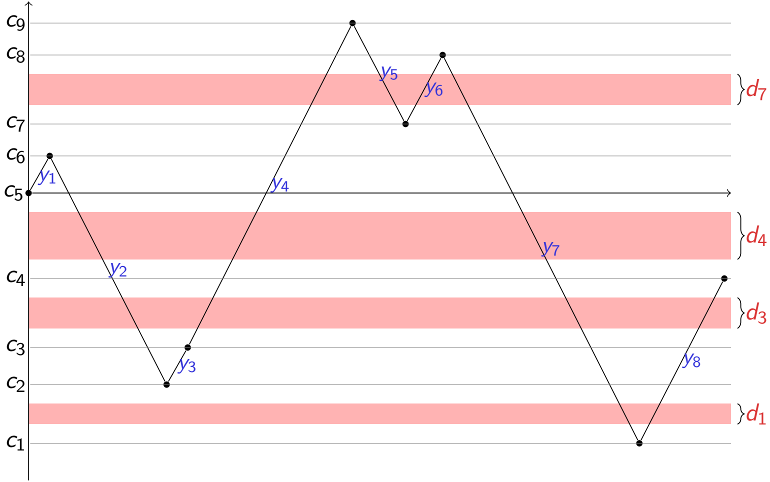
Make exponents small

For $p \in \Omega$ rite $w = u_0 p^{y_1} u_1 \cdots p^{y_m} u_m$ such that no u_i contains p^x.



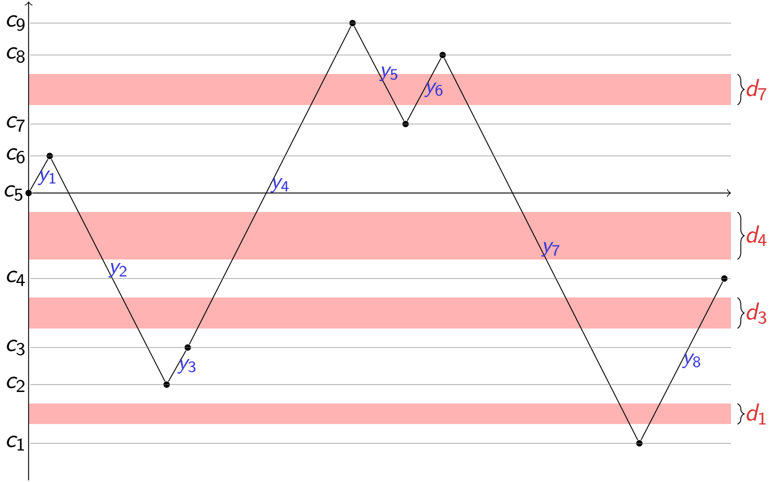
Make exponents small

For $p \in \Omega$ rite $w = u_0 p^{y_1} u_1 \cdots p^{y_m} u_m$ such that no u_i contains p^x.



Make exponents small

For $p \in \Omega$ rite $w = u_0 p^{y_1} u_1 \cdots p^{y_m} u_m$ such that no u_i contains p^x.



Define $\mathcal{S}(w) = u_0 p^{z_1} u_1 \cdots p^{z_m} u_m$ where $z_i = y_i - \operatorname{sign}(y_i) \cdot \sum_{j \in C_i} d_j$

Make exponents small

Proposition

$w =_F 1 \iff \mathcal{S}(w) =_F 1.$

Make exponents small

Proposition

$w =_F 1 \iff \mathcal{S}(w) =_F 1.$

Proof of the main theorem.

- Preprocessing gives a "nice word" $w = s_0 p_1^{x_1} s_1 \cdots p_n^{x_n} s_n$.
- For all $p \in \Omega$ which appear in w, compute $\mathcal{S}(w)$ in parallel (iterated addition $\rightsquigarrow$ in TC^0).
- Yields a word of polynomial length $\rightsquigarrow$ ordinary word problem.

Further results on the power word problem

Theorem

Let G be f.g. and $H \leq G$ of finite index. Then

$$\textsc{PowerWP}(G) \leq_{\mathrm{m}}^{\mathsf{NC}^1} \textsc{PowerWP}(H).$$

Further results on the power word problem

Theorem

Let G be f.g. and $H \leq G$ of finite index. Then

$$\textsc{PowerWP}(G) \leq_{\mathrm{m}}^{\mathsf{NC}^1} \textsc{PowerWP}(H).$$

Corollary

The power word problem of f.g. virtually free groups is in LOGSPACE.

Further results on the power word problem

Theorem

Let G be f.g. and $H \leq G$ of finite index. Then

$$\textsc{PowerWP}(G) \leq_{\mathrm{m}}^{\mathsf{NC}^1} \textsc{PowerWP}(H).$$

Corollary

The power word problem of f.g. virtually free groups is in LOGSPACE.

Theorem

If G is f.g. nilpotent, then $\textsc{PowerWP}(G)$ *is in* TC^0.

Further results on the power word problem

Theorem

Let G be f.g. and $H \leq G$ of finite index. Then

$$\textsc{PowerWP}(G) \leq_{\mathrm{m}}^{\mathsf{NC}^1} \textsc{PowerWP}(H).$$

Corollary

The power word problem of f.g. virtually free groups is in LOGSPACE.

Theorem

If G is f.g. nilpotent, then $\textsc{PowerWP}(G)$ is in TC^0.

Theorem

The power word problem of the Grigorchuk group is in LOGSPACE.

Theorem

For every f.g. abelian group G, $\textsc{PowerWP}(G \wr \mathbb{Z})$ is in TC^0.

The power word problem in wreath products

Theorem

For every f.g. abelian group G, $\textsc{PowerWP}(G \wr \mathbb{Z})$ is in TC^0.

Theorem

Let G be either

- *finite non-solvable*
- *f.g. free of rank ≥ 2.*

Then $\textsc{PowerWP}(G \wr \mathbb{Z})$ is coNP-complete.

The power word problem in wreath products

Theorem

For every f.g. abelian group G, $\textsc{PowerWP}(G \wr \mathbb{Z})$ is in TC^0.

Theorem

Let G be either

- *finite non-solvable*
- *f.g. free of rank ≥ 2.*

Then $\textsc{PowerWP}(G \wr \mathbb{Z})$ is coNP*-complete.*

For comparison:

- $\mathrm{WP}(G \wr \mathbb{Z})$ is in LOGSPACE (resp. NC^1)
- $\textsc{CompressedWP}(G \wr \mathbb{Z})$ is PSPACE-complete (Lohrey 2019, unpublished)

The power word problem in wreath products

Theorem

For every f.g. abelian group G, $\textsc{PowerWP}(G \wr \mathbb{Z})$ *is in* TC^0*.*

Theorem

Let G be either

- *finite non-solvable*
- *f.g. free of rank ≥ 2.*

Then $\textsc{PowerWP}(G \wr \mathbb{Z})$ *is* coNP*-complete.*

Proof idea.

Show $\text{CNF-}\textsc{UnSAT} \leq \textsc{PowerWP}(G \wr \mathbb{Z})$:

- Every formula can be "simulated" in G (Barrington 89)
- Test all valuations "in parallel" in $G^{(\mathbb{Z})} \leq F_2 \wr \mathbb{Z}$

Open Questions

- What if we allow nested exponents:

$$\left(b^{13}\overline{a}\;\left((b\,a^{8}a)^{13}a^{-26}b^{-13}\right)^{12}\right)^{16}\left((\overline{b}\,\overline{a})^{13}a^{13}\right)^{20}$$

  - Conjecture: for constant nesting depth in $\mathsf{AC}^0(\mathrm{WP}(F_2))$.
  - Not clear what happens for unbounded nesting depth:
    ... is it P-complete? ... or in $\mathsf{AC}^0(\mathrm{WP}(F_2))$?

Open Questions

- What if we allow nested exponents:

$$\left(b^{13}\overline{a}\ \left((b\,a^{8}a)^{13}a^{-26}b^{-13}\right)^{12}\right)^{16}\left((\overline{b}\,\overline{a})^{13}a^{13}\right)^{20}$$

  - Conjecture: for constant nesting depth in $\mathsf{AC}^0(\mathrm{WP}(F_2))$.
  - Not clear what happens for unbounded nesting depth:
    ... is it P-complete? ... or in $\mathsf{AC}^0(\mathrm{WP}(F_2))$?
- Complexity of $\textsc{PowerWP}$ in other groups:
  - $(G \wr \mathbb{Z})$ for G non-abelian, but not free nor finite, non-solvable (e. g. G nilpotent)?
  - hyperbolic groups?
  - RAAGs (= graph groups)?
  - HNN extensions and amalgamated products over finite subgroups?
  - Baumslag-Solitar groups?

- What if we allow nested exponents:

$$\left(b^{13}\bar{a}\ \left((b\,a^{8}a)^{13}a^{-26}b^{-13}\right)^{12}\right)^{16}\ \left((\bar{b}\,\bar{a})^{13}a^{13}\right)^{20}$$

  - Conjecture: for constant nesting depth in $\mathsf{AC}^0(\mathrm{WP}(F_2))$.
  - Not clear what happens for unbounded nesting depth:
    ... is it P-complete? ... or in $\mathsf{AC}^0(\mathrm{WP}(F_2))$?
- Complexity of $\mathrm{P{\scriptsize OWER}WP}$ in other groups:
  - $(G \wr \mathbb{Z})$ for G non-abelian, but not free nor finite, non-solvable (e. g. G nilpotent)?
  - hyperbolic groups?
  - RAAGs (= graph groups)?
  - HNN extensions and amalgamated products over finite subgroups?
  - Baumslag-Solitar groups?

Thank you!