# Separating Words Problem on Groups

Neha Kuntewar, Anoop S. K. M. & Jayalal Sarma

Indian Institute of Technology, Madras, India

DCFS 2023, Potsdam, Germany

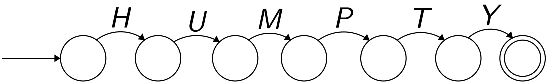
July 6, 2023

# Introduction

- Can we have a DFA that accepts HUMPTY and rejects DUMPTY?

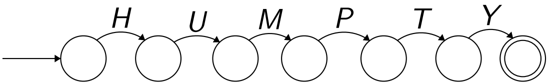
# Introduction

- Can we have a DFA that accepts HUMPTY and rejects DUMPTY?



# Introduction

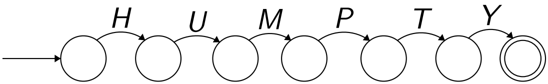
- Can we have a DFA that accepts HUMPTY and rejects DUMPTY?



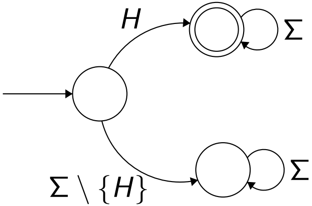

- Can we have a smaller DFA in terms of its number of states?

## Introduction

- Can we have a DFA that accepts HUMPTY and rejects DUMPTY?




- Can we have a smaller DFA in terms of its number of states?



# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0, 1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0, 1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$

# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0, 1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$
- Suppose $w$ and $x$ are words that differ in some symbol that occurs d positions from the start or end, then $sep(w, x) \leq d + 2$. [DESW11]

# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0, 1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$
- Suppose $w$ and $x$ are words that differ in some symbol that occurs d positions from the start or end, then $sep(w, x) \leq d + 2$. [DESW11]
- If $HammingDistance(w, x) \leq d$, $sep(w, x) = O(d \log n)$.[DESW11]

# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0, 1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$
- Suppose $w$ and $x$ are words that differ in some symbol that occurs d positions from the start or end, then $sep(w, x) \leq d + 2$. [DESW11]
- If $HammingDistance(w, x) \leq d$, $sep(w, x) = O(d \log n)$.[DESW11]
- When $|w| \neq |x|, \exists$ an automaton $O(\log n)$ that separates $w, x$.

# Separating Words Problem ($sep(w,x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0,1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$
- Suppose $w$ and $x$ are words that differ in some symbol that occurs d positions from the start or end, then $sep(w,x) \leq d+2$. [DESW11]
- If $HammingDistance(w,x) \leq d$, $sep(w,x) = O(d \log n)$.[DESW11]
- When $|w| \neq |x|, \exists$ an automaton $O(\log n)$ that separates $w, x$.
  If $0 \leq i \neq j \leq n$, $\exists p \leq O(\log n)$ such that $i \not\equiv j \mod p$.

# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0, 1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$
- Suppose $w$ and $x$ are words that differ in some symbol that occurs d positions from the start or end, then $sep(w, x) \leq d + 2$. [DESW11]
- If $HammingDistance(w, x) \leq d$, $sep(w, x) = O(d \log n)$.[DESW11]
- When $|w| \neq |x|, \exists$ an automaton $O(\log n)$ that separates $w, x$. If $0 \leq i \neq j \leq n$, $\exists p \leq O(\log n)$ such that $i \not\equiv j \mod p$. Hence, counting modulo $p$ separates $w, x$.

# Separating Words Problem ($sep(w, x)$)

**Separating Words Problem [GK86]**

Given two words $w, x \in \{0,1\}^*$, what is the size of the smallest automaton (in terms of number of states) which accepts one of them and rejects the other.

- Trivial Upper Bound : $O(n)$
- Suppose $w$ and $x$ are words that differ in some symbol that occurs d positions from the start or end, then $sep(w, x) \leq d + 2$. [DESW11]
- If $HammingDistance(w, x) \leq d$, $sep(w, x) = O(d \log n)$.[DESW11]
- When $|w| \neq |x|, \exists$ an automaton $O(\log n)$ that separates $w, x$. If $0 \leq i \neq j \leq n$, $\exists p \leq O(\log n)$ such that $i \not\equiv j \mod p$. Hence, counting modulo $p$ separates $w, x$.
- Separating Words Problem is NP-Complete [BKSS17]

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]

## Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w,x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]
- $O(n^{2/5} \log^{3/5} n)$ [Rob96]

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]
- $O(n^{2/5} \log^{3/5} n)$ [Rob96]
- $O(n^{1/3} \log^{7} n)$ [Cha21]

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]
- $O(n^{2/5} \log^{3/5} n)$ [Rob96]
- $O(n^{1/3} \log^{7} n)$ [Cha21]

**Lower Bound :** $\Omega(\log n)$ [DESW11]

$$w = 0^{m-1} 1^{m-1+\ell cm(1,2,\ldots,m)}, x = 0^{m-1+\ell cm(1,2,\ldots,m)} 1^{m-1}$$

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]
- $O(n^{2/5} \log^{3/5} n)$ [Rob96]
- $O(n^{1/3} \log^{7} n)$ [Cha21]

**Lower Bound :** $\Omega(\log n)$ [DESW11]

$$w = 0^{m-1} 1^{m-1+\ell cm(1,2,\ldots,m)}, x = 0^{m-1+\ell cm(1,2,\ldots,m)} 1^{m-1}$$

Exponential Gap between Lower and Upper bounds!

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w,x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]
- $O(n^{2/5}\log^{3/5} n)$ [Rob96]
- $O(n^{1/3}\log^{7} n)$ [Cha21]

**Lower Bound :** $\Omega(\log n)$ [DESW11]

$$w = 0^{m-1}1^{m-1+\ell cm(1,2,\ldots,m)}, x = 0^{m-1+\ell cm(1,2,\ldots,m)}1^{m-1}$$

Exponential Gap between Lower and Upper bounds! still open !.

# Known Bounds

**Choffrut Conjecture [Chr86]**

Given distinct words of length $n$, for all $\epsilon > 0$, the value $sep(w, x) \in O(n^{\epsilon})$

**Upper Bound :**

- $o(n)$ [GK86]
- $O(n^{1/2})$ [Rob89]
- $O(n^{2/5} \log^{3/5} n)$ [Rob96]
- $O(n^{1/3} \log^{7} n)$ [Cha21]

**Lower Bound :** $\Omega(\log n)$ [DESW11]

$$w = 0^{m-1}1^{m-1+\ell cm(1,2,\ldots,m)}, x = 0^{m-1+\ell cm(1,2,\ldots,m)}1^{m-1}$$

Exponential Gap between Lower and Upper bounds! still open !.

**Question:** What if the automaton is restricted?

# Permuting Automaton

# Permuting Automaton

### Permuting Automaton

An Automaton such that for each $a \in \Sigma$, the transition function is a permutation of the set of states.

# Permuting Automaton

### Permuting Automaton

An Automaton such that for each $a \in \Sigma$, the transition function is a permutation of the set of states.

- Robson [Rob89] :For any two words of length $n$, we can construct a permuting automaton with $O(\sqrt{n})$ states that separates them.

# Permuting Automaton

**Permuting Automaton**

An Automaton such that for each $a \in \Sigma$, the transition function is a permutation of the set of states.

- Robson [Rob89] :For any two words of length $n$, we can construct a permuting automaton with $O(\sqrt{n})$ states that separates them.
- Each permuting automaton is associated with a subgroup of $S_n$.
- Motivated by this : we define the separating words problem over groups.

# Separating Words with Groups

- Let $G$ be a group.
- Let $\phi : \Sigma \to G$

# Separating Words with Groups

- Let $G$ be a group.
- Let $\phi : \Sigma \to G$
- $w = w_1 w_2 \dots w_n \in \Sigma^n$, is said to *yield* $g \in G$ if $\prod_{i=1}^{n} \phi(w_i) = g$

# Separating Words with Groups

- Let $G$ be a group.
- Let $\phi : \Sigma \to G$
- $w = w_1 w_2 \ldots w_n \in \Sigma^n$, is said to *yield* $g \in G$ if $\prod_{i=1}^{n} \phi(w_i) = g$
- Given $w, x \in \Sigma^*$, a group $G$ is said to *separate* $w$ and $x$ if there exists a function $\phi$ such that $\phi(w) \neq \phi(x)$.

# Separating Words with Groups

- Let $G$ be a group.
- Let $\phi : \Sigma \to G$
- $w = w_1 w_2 \dots w_n \in \Sigma^n$, is said to *yield* $g \in G$ if $\prod_{i=1}^{n} \phi(w_i) = g$
- Given $w, x \in \Sigma^*$, a group $G$ is said to *separate* $w$ and $x$ if there exists a function $\phi$ such that $\phi(w) \neq \phi(x)$.

**Example:** Consider $w, x \in \{0,1\}^*$ with $|w| \neq |x|$.

# Separating Words with Groups

- Let $G$ be a group.
- Let $\phi : \Sigma \to G$
- $w = w_1 w_2 \dots w_n \in \Sigma^n$, is said to *yield* $g \in G$ if $\prod_{i=1}^{n} \phi(w_i) = g$
- Given $w, x \in \Sigma^*$, a group $G$ is said to *separate* $w$ and $x$ if there exists a function $\phi$ such that $\phi(w) \neq \phi(x)$.

**Example:** Consider $w, x \in \{0,1\}^*$ with $|w| \neq |x|$.
the group $\mathbb{Z}_p$ with prime $p = O(\log n)$, with $\phi(1) = 1$, $\phi(0) = 0$ (or vice versa), will separate $w$ and $x$.

# Can we always find a separating group?

**Separating Group**

Given any $w$ and $x$, does there always exist a group $G$ that separates them?

# Can we always find a separating group?

**Separating Group**

Given any $w$ and $x$, does there always exist a group $G$ that separates them?

- Yes!

# Can we always find a separating group?

**Separating Group**

Given any $w$ and $x$, does there always exist a group $G$ that separates them?

- Yes! Group associated with Robson's Permuting Automaton.
- The group is a subgroup of $Sym\left(\sqrt{n}\right)$.

# Separating Words with Groups : Two Natural Questions

**Size of the group**

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

# Separating Words with Groups : Two Natural Questions

## Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $(\sqrt{n})! = 2^{O(\sqrt{n}\log n)}$ (directly from Robson's automaton).

# Separating Words with Groups : Two Natural Questions

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $(\sqrt{n})! = 2^{O(\sqrt{n}\log n)}$ (directly from Robson's automaton).
- **Lower bound :** $\Omega(\log n)$ (group of size $k \implies$ automaton of size $k$).

# Separating Words with Groups : Two Natural Questions

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $(\sqrt{n})! = 2^{O(\sqrt{n}\log n)}$ (directly from Robson's automaton).
- **Lower bound :** $\Omega(\log n)$ (group of size $k \implies$ automaton of size $k$).

Question : Still an exponential gap !

# Separating Words with Groups : Two Natural Questions

## Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $(\sqrt{n})! = 2^{O(\sqrt{n}\log n)}$ (directly from Robson's automaton).
- **Lower bound :** $\Omega(\log n)$ (group of size $k \implies$ automaton of size $k$).

Question : Still an exponential gap !

## Universality of restricted group classes

A class of groups $\mathcal{G}$ is said to be *universal* if for any two words $w, x \in \Sigma^*$, there exists a group $G \in \mathcal{G}$ for which a separating substitution map exists such that the yields of the words under the map are distinct.

# Separating Words with Groups : Two Natural Questions

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $(\sqrt{n})! = 2^{O(\sqrt{n}\log n)}$ (directly from Robson's automaton).
- **Lower bound :** $\Omega(\log n)$ (group of size $k \implies$ automaton of size $k$).

Question : Still an exponential gap !

### Universality of restricted group classes

A class of groups $\mathcal{G}$ is said to be *universal* if for any two words $w, x \in \Sigma^*$, there exists a group $G \in \mathcal{G}$ for which a separating substitution map exists such that the yields of the words under the map are distinct.

Question : Which classes of groups are *universal*?

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$.

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$.
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal.
  - Class of Abelian groups and dihedral groups are **not** universal.
  - Sufficiency conditions for non-universality of classes of groups.

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$.
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal.
  - Class of Abelian groups and dihedral groups are **not** universal.
  - Sufficiency conditions for non-universality of classes of groups.
- **Computational Version :** SepGroupWords Problem - Given two words $w, x \in \Sigma^*$, a set of permutations $S$ that generates a group $G \leq S_n$ and a function $\phi : \Sigma \to S$, with the guarantee that yield($w$)$\neq$ yield($x$) and an integer $k$, check if there is an automaton of size $k$ which separates $w$ and $x$.

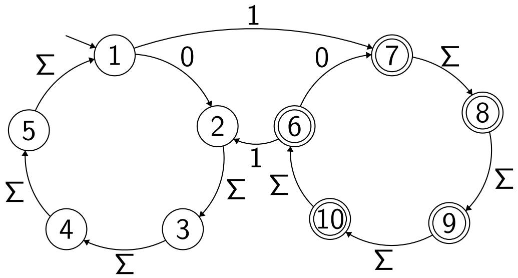
# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$.
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal.
  - Class of Abelian groups and dihedral groups are **not** universal.
  - Sufficiency conditions for non-universality of classes of groups.
- **Computational Version :** SepGroupWords Problem - Given two words $w, x \in \Sigma^*$, a set of permutations $S$ that generates a group $G \leq S_n$ and a function $\phi : \Sigma \to S$, with the guarantee that yield($w$)$\neq$ yield($x$) and an integer $k$, check if there is an automaton of size $k$ which separates $w$ and $x$.

  We show that SepGroupWords is NP-Complete

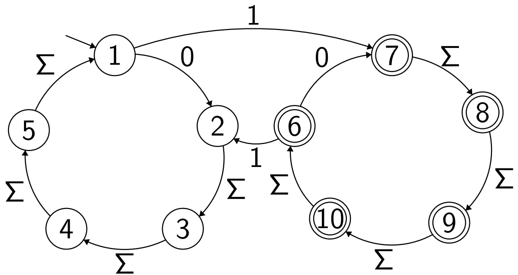
# Robson's Permuting Automaton

# Robson's Permuting Automaton




$M_{i,m} = (Q, \{0,1\}, q_0, \delta, F)$ accepts strings, where the parity of symbols at positions congruent to $i$ $(mod\ \ m)$ is odd (where $m \leq O\left(\sqrt{n}\right)$).

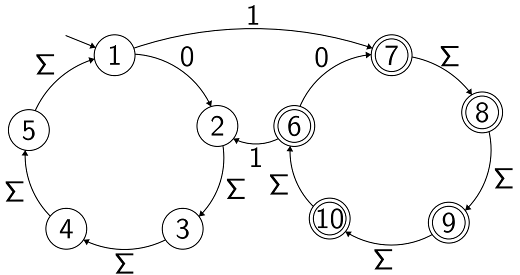
# Robson's Permuting Automaton




$M_{i,m} = (Q, \{0,1\}, q_0, \delta, F)$ accepts strings, where the parity of symbols at positions congruent to $i$ $(mod\ \ m)$ is odd (where $m \leq O\left(\sqrt{n}\right)$).

- $Q = \{(p,q) \mid p \in \{0,1\}\ q \in \{0,..m-1\}\}$, $|Q| = 2m$

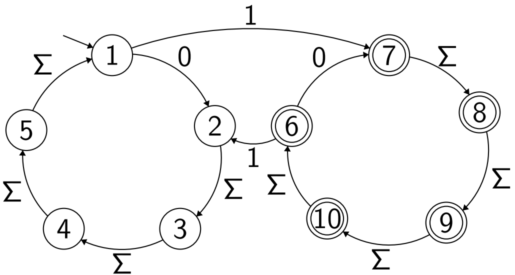
# Robson's Permuting Automaton




$M_{i,m} = (Q, \{0,1\}, q_0, \delta, F)$ accepts strings, where the parity of symbols at positions congruent to $i$ $(mod\ \ m)$ is odd (where $m \leq O\left(\sqrt{n}\right)$).

- $Q = \{(p,q) \mid p \in \{0,1\}\ q \in \{0,..m-1\}\}$, $|Q| = 2m$
- $\delta : Q \times \Sigma \longrightarrow Q$
  - $\delta((p,q),0) = (p,(q+1) \mod m)$
  - $\delta((p,q),1) = \begin{cases} (p,(q+1) \mod m), & \text{if } q \neq i \\ (1-p,(q+1) \mod m), & \text{otherwise} \end{cases}$

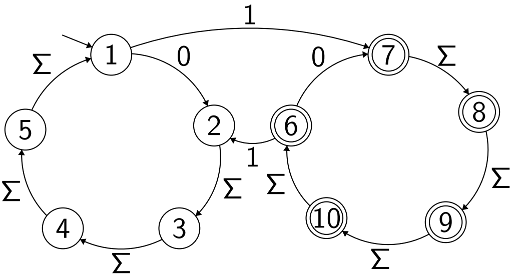
# Robson's Permuting Automaton




$M_{i,m} = (Q, \{0,1\}, q_0, \delta, F)$ accepts strings, where the parity of symbols at positions congruent to $i$ $(mod\ m)$ is odd (where $m \leq O\left(\sqrt{n}\right)$).

- $Q = \{(p,q) \mid p \in \{0,1\}\ q \in \{0,..m-1\}\}$, $|Q| = 2m$
- $\delta : Q \times \Sigma \longrightarrow Q$
  - $\delta((p,q),0) = (p,(q+1) \mod m)$
  - $\delta((p,q),1) = \begin{cases} (p,(q+1) \mod m), & \text{if } q \neq i \\ (1-p,(q+1) \mod m), & \text{otherwise} \end{cases}$

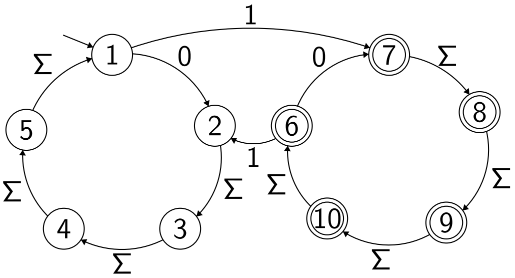
# Robson's Permuting Automaton to Group




Robson's group $G_m = \langle g, h \rangle$ where,

$g = (1, 2 \ldots m)(m+1, \ldots 2m)$ $\qquad$ $h = (1, m+2, m+3 \ldots 2m, m+1, 2 \ldots m)$

# Robson's Permuting Automaton to Group




Robson's group $G_m = \langle g, h \rangle$ where,

$g = (1, 2 \ldots m)(m+1, \ldots 2m)$ $\qquad$ $h = (1, m+2, m+3 \ldots 2m, m+1, 2 \ldots m)$

**Theorem :** For any $w, x \in \Sigma^*$, with $|w| = |x| = n$, there is a group of size $O\left(\sqrt{n}2^{\sqrt{n}}\right)$ that separates them.

# Estimating the Size of Robson's Group

Robson's group $G_m = \langle g, h \rangle$ where,

- $g = (1, 2 \ldots m)(m+1, \ldots 2m)$
- $h = (1, m+2, m+3 \ldots 2m, m+1, 2 \ldots m)$

**Theorem**

$|G_m| = m2^m$

# Estimating the Size of Robson's Group

Robson's group $G_m = \langle g, h \rangle$ where,

- $g = (1, 2 \ldots m)(m + 1, \ldots 2m)$
- $h = (1, m + 2, m + 3 \ldots 2m, m + 1, 2 \ldots m)$

**Theorem**

$|G_m| = m2^m$

We know $|G_m| = |H_m| * [G_m : H_m]$, $H_m$ is the commutator subgroup of $G_m$ and $[G_m : H_m]$ is the index (equal to the number of left cosets).

# Estimating the Size of Robson's Group

Robson's group $G_m = \langle g, h \rangle$ where,

- $g = (1, 2 \dots m)(m+1, \dots 2m)$
- $h = (1, m+2, m+3 \dots 2m, m+1, 2 \dots m)$

**Theorem**

$|G_m| = m2^m$

We know $|G_m| = |H_m| * [G_m : H_m]$, $H_m$ is the commutator subgroup of $G_m$ and $[G_m : H_m]$ is the index (equal to the number of left cosets).
We prove

1. $|H_m| = 2^{m-1}$

# Estimating the Size of Robson's Group

Robson's group $G_m = \langle g, h \rangle$ where,

- $g = (1, 2 \ldots m)(m+1, \ldots 2m)$
- $h = (1, m+2, m+3 \ldots 2m, m+1, 2 \ldots m)$

**Theorem**

$|G_m| = m2^m$

We know $|G_m| = |H_m| * [G_m : H_m]$, $H_m$ is the commutator subgroup of $G_m$ and $[G_m : H_m]$ is the index (equal to the number of left cosets).
We prove

1. $|H_m| = 2^{m-1}$
2. $[G_m : H_m] = 2m$

# Estimating the size of the commutator subgroup: $|H_m|$

**Lemma**

*Consider a Robson's group $G_m$. Let $H_m$ be the commutator subgroup of $G_m$. Consider $S = \{(1, m+1)(m-i+1, 2m-i+1) | \forall i \in [m-1]\}$. Then $H_m = \langle S \rangle$*

# Estimating the size of the commutator subgroup: $|H_m|$

**Lemma**

*Consider a Robson's group $G_m$. Let $H_m$ be the commutator subgroup of $G_m$. Consider $S = \{(1, m+1)(m-i+1, 2m-i+1) | \forall i \in [m-1]\}$. Then $H_m = \langle S \rangle$*

Proof Idea

- We show that:(1) $S \subseteq H_m$ and (2) $H_m \subseteq \langle S \rangle$.

# Estimating the size of the commutator subgroup: $|H_m|$

**Lemma**

*Consider a Robson's group $G_m$. Let $H_m$ be the commutator subgroup of $G_m$. Consider $S = \{(1, m+1)(m-i+1, 2m-i+1) | \forall i \in [m-1]\}$. Then $H_m = \langle S \rangle$*

Proof Idea

- We show that:(1) $S \subseteq H_m$ and (2) $H_m \subseteq \langle S \rangle$.

**Lemma**

*Let $G = \langle S \rangle$ be an Abelian group such that every generator $g \in S$ is a transposition. Then, $|G| = 2^m$ where $m = |S|$.*

# Estimating the size of the commutator subgroup: $|H_m|$

**Lemma**

*Consider a Robson's group $G_m$. Let $H_m$ be the commutator subgroup of $G_m$. Consider $S = \{(1, m+1)(m-i+1, 2m-i+1) | \forall i \in [m-1]\}$. Then $H_m = \langle S \rangle$*

Proof Idea

- We show that:(1) $S \subseteq H_m$ and (2) $H_m \subseteq \langle S \rangle$.

**Lemma**

*Let $G = \langle S \rangle$ be an Abelian group such that every generator $g \in S$ is a transposition. Then, $|G| = 2^m$ where $m = |S|$.*

- Hence we prove $|H_m| = 2^{m-1}$

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*The Robson's group $G_m$ has a presentation*

$$\begin{cases} \langle g, h \mid \; g^m = h^{2m} = (gh^2)^{2m/3} = e \rangle \; when \; m = 3k \\ \langle g, h \mid \; g^m = h^{2m} = (gh^2)^m = e \rangle \; otherwise \end{cases}$$

*where $e$ is the identity element and $k \in \mathbb{N}$.*

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*The Robson's group $G_m$ has a presentation*

$$\begin{cases} \langle g, h \mid \; g^m = h^{2m} = (gh^2)^{2m/3} = e \rangle \; \textit{when } m = 3k \\ \langle g, h \mid \; g^m = h^{2m} = (gh^2)^m = e \rangle \; \textit{otherwise} \end{cases}$$

*where $e$ is the identity element and $k \in \mathbb{N}$.*

**Lemma (from group theory)**

*For any group $G$, $[G : H]$ where $H$ is a commutator subgroup of $G$ is number of group homomorphisms $\phi : G \longrightarrow \mathbb{C}^{\times}$.*

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*There are exactly $2m$ distinct homomorphisms $\phi : G_m \longrightarrow \mathbb{C}^{\times}$.*

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*There are exactly $2m$ distinct homomorphisms $\phi : G_m \longrightarrow \mathbb{C}^{\times}$.*

- $g^m = e$, we have $(\phi(g))^m = 1$. Hence, $\phi(g)$ must be an $m^{th}$ root of unity.

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*There are exactly $2m$ distinct homomorphisms $\phi : G_m \longrightarrow \mathbb{C}^\times$.*

- $g^m = e$, we have $(\phi(g))^m = 1$. Hence, $\phi(g)$ must be an $m^{th}$ root of unity.
- $h^{2m} = e$ that $\phi(h)$ must be a $2m^{th}$ root of unity.

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*There are exactly $2m$ distinct homomorphisms $\phi : G_m \longrightarrow \mathbb{C}^\times$.*

- $g^m = e$, we have $(\phi(g))^m = 1$. Hence, $\phi(g)$ must be an $m^{th}$ root of unity.
- $h^{2m} = e$ that $\phi(h)$ must be a $2m^{th}$ root of unity.
- $(\phi(g)\phi(h)^2)^p = 1$ where $p = 2m/3$ when $m = 3k$ and $p = m$ otherwise.

# Estimating Bounds on the Index: $[G_m : H_m]$

**Lemma**

*There are exactly $2m$ distinct homomorphisms $\phi : G_m \longrightarrow \mathbb{C}^{\times}$.*

- $g^m = e$, we have $(\phi(g))^m = 1$. Hence, $\phi(g)$ must be an $m^{th}$ root of unity.
- $h^{2m} = e$ that $\phi(h)$ must be a $2m^{th}$ root of unity.
- $(\phi(g)\phi(h)^2)^p = 1$ where $p = 2m/3$ when $m = 3k$ and $p = m$ otherwise.

# Estimating Bounds on the Index: $[G_m : H_m]$

Thus, we have the following constraints:

- $e^{\frac{2\pi ip}{m}}\left(e^{\frac{2\pi jp}{2m}}\right)^2 = 1$, $0 \leq i, p \leq m-1, 0 \leq j \leq 2m-1.$

# Estimating Bounds on the Index: $[G_m : H_m]$

Thus, we have the following constraints:

- $e^{\frac{2\pi ip}{m}}\left(e^{\frac{2\pi jp}{2m}}\right)^2 = 1$, $0 \leq i, p \leq m-1, 0 \leq j \leq 2m-1$.
- $e^{\frac{2\pi ip}{m}} e^{\frac{2\pi jp}{m}} = e^{2\pi\ell}$ where $\ell \in \mathbb{N}$.

# Estimating Bounds on the Index: $[G_m : H_m]$

Thus, we have the following constraints:

- $e^{\frac{2\pi ip}{m}}\left(e^{\frac{2\pi jp}{2m}}\right)^2 = 1$, $0 \le i, p \le m-1, 0 \le j \le 2m-1$.
- $e^{\frac{2\pi ip}{m}} e^{\frac{2\pi jp}{m}} = e^{2\pi\ell}$ where $\ell \in \mathbb{N}$.
- This gives, $i + j = \left(\frac{\ell}{p}\right) m$

# Estimating Bounds on the Index: $[G_m : H_m]$

Thus, we have the following constraints:

- $e^{\frac{2\pi ip}{m}}\left(e^{\frac{2\pi jp}{2m}}\right)^2 = 1$, $0 \le i, p \le m-1, 0 \le j \le 2m-1$.
- $e^{\frac{2\pi ip}{m}} e^{\frac{2\pi jp}{m}} = e^{2\pi\ell}$ where $\ell \in \mathbb{N}$.
- This gives, $i + j = \left(\frac{\ell}{p}\right) m$
- For a fixed value of $j$ there is a unique $0 \le i \le m-1$

# Estimating Bounds on the Index: $[G_m : H_m]$

Thus, we have the following constraints:

- $e^{\frac{2\pi ip}{m}}\left(e^{\frac{2\pi jp}{2m}}\right)^2 = 1$, $0 \leq i, p \leq m-1, 0 \leq j \leq 2m-1$.
- $e^{\frac{2\pi ip}{m}} e^{\frac{2\pi jp}{m}} = e^{2\pi\ell}$ where $\ell \in \mathbb{N}$.
- This gives, $i + j = \left(\frac{\ell}{p}\right) m$
- For a fixed value of $j$ there is a unique $0 \leq i \leq m-1$
- Number of distinct solutions to the equation is $2m$.
- There are $2m$ many one dimensional representations of $G_m$

# Estimating the Size of Robson's Group

Size of Robson's Group $G_m$ with commutator subgroup $H_m$ is

$$\begin{aligned}|G_m| &= |H_m| * [G_m : H_m] \\ &= 2^{m-1} * 2m \\ &= m2^m\end{aligned}$$

# Estimating the Size of Robson's Group

Size of Robson's Group $G_m$ with commutator subgroup $H_m$ is

$$\begin{aligned} |G_m| &= |H_m| * [G_m : H_m] \\ &= 2^{m-1} * 2m \\ &= m2^m \end{aligned}$$

**Theorem**

*For any $w, x \in \Sigma^*$, with $|w| = |x| = n$, there is a group of size $O\left(\sqrt{n}2^{\sqrt{n}}\right)$ that separates them.*

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$. ✓
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal.
  - Class of Abelian groups and dihedral groups are **not** universal.
  - Sufficiency conditions for non-universality of classes of groups.
- **Computational Version :** SepGroupWords Problem - Given two words $w, x \in \Sigma^*$, a set of permutations $S$ that generates a group $G \leq S_n$ and a function $\phi : \Sigma \to S$, with the guarantee that yield($w$)$\neq$ yield($x$) and an integer $k$, check if there is an automaton of size $k$ which separates $w$ and $x$.

  We show that SepGroupWords is NP-Complete

# Structure of the Separating Groups : Universal Groups

Theorem

*The class of solvable groups and the class of $p$-groups are universal.*

# Structure of the Separating Groups : Universal Groups

**Theorem**

*The class of solvable groups and the class of p-groups are universal.*

- Commutator subgroup of Robson's permutation group is Abelian.
- Robson's group is thus solvable.

# Structure of the Separating Groups : Universal Groups

**Theorem**

*The class of solvable groups and the class of $p$-groups are universal.*

- Commutator subgroup of Robson's permutation group is Abelian.
- Robson's group is thus solvable.

**Lemma**

*Given a pair of distinct words $w, x \in \{0,1\}^n$ there exists $0 \leq i < m \leq [2n]$ and $m = 2^k$ for some $k \in \mathbb{N}$ such that this 2-group separates $w, x$.*

- $p$-groups are universal.
- Nilpotent groups are universal.

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$. ✓
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal. ✓
  - Class of Abelian groups and dihedral groups are **not** universal.
  - Sufficiency conditions for non-universality of classes of groups.
- **Computational Version :** SepGroupWords Problem - Given two words $w, x \in \Sigma^*$, a set of permutations $S$ that generates a group $G \leq S_n$ and a function $\phi : \Sigma \to S$, with the guarantee that yield($w$)$\neq$ yield($x$) and an integer $k$, check if there is an automaton of size $k$ which separates $w$ and $x$.

  We show that SepGroupWords is NP-Complete

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of groups $\mathcal{G}$ is not universal where $\mathcal{G}$ is an Abelian group.*

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of groups $\mathcal{G}$ is not universal where $\mathcal{G}$ is an Abelian group.*

- Consider $w, x \in \Sigma^n$ such that $\forall a \in \Sigma$, the number of occurrences of $a$ is same in both $w$ and $x$.

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of groups $\mathcal{G}$ is not universal where $\mathcal{G}$ is an Abelian group.*

- Consider $w, x \in \Sigma^n$ such that $\forall a \in \Sigma$, the number of occurrences of $a$ is same in both $w$ and $x$.
- $\phi(w) = g_1^{n_1} g_2^{n_2} \ldots g_k^{n_k} = \phi(x)$, $g_i$ generator and $\forall i, n_i \geq 0$.

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of groups $\mathcal{G}$ is not universal where $\mathcal{G}$ is an Abelian group.*

- Consider $w, x \in \Sigma^n$ such that $\forall a \in \Sigma$, the number of occurrences of $a$ is same in both $w$ and $x$.
- $\phi(w) = g_1^{n_1} g_2^{n_2} \ldots g_k^{n_k} = \phi(x)$, $g_i$ generator and $\forall i, n_i \geq 0$.
- For any Abelian group $G$ & $\phi : \Sigma \to G$, $yield(\phi(w)) = yield(\phi(x))$.

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of dihedral groups is not universal.*

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of dihedral groups is not universal.*

- Dihedral Group: Group of symmetries of regular polygon

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of dihedral groups is not universal.*

- Dihedral Group: Group of symmetries of regular polygon
- Consider any Dihedral group $G = \{r_0, r_1, \dots r_{m-1}, s_0, s_1 \dots s_{m-1}\}$.
- We know that $r_i r_j = r_{i+j}$ and $s_i s_j = r_{i-j}$.

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of dihedral groups is not universal.*

- Dihedral Group: Group of symmetries of regular polygon
- Consider any Dihedral group $G = \{r_0, r_1, \ldots r_{m-1}, s_0, s_1 \ldots s_{m-1}\}$.
- We know that $r_i r_j = r_{i+j}$ and $s_i s_j = r_{i-j}$.
- Consider $w = 0^{2k}1^{2k}$, $x = 1^{2k}0^{2k}$ where $k \in \mathbb{N}$.
  Consider the following cases:

  Case 1: The elements in the group that get mapped are $\{r_i, r_j\}$.
  Then $yield(w) = (r_i)^{2k}(r_j)^{2k} = (r_j)^{2k}(r_i)^{2k} = yield(x)$.

# Structure of the Separating Groups : Non-Universal Groups

**Theorem**

*The class of dihedral groups is not universal.*

- Dihedral Group: Group of symmetries of regular polygon
- Consider any Dihedral group $G = \{r_0, r_1, \dots r_{m-1}, s_0, s_1 \dots s_{m-1}\}$.
- We know that $r_i r_j = r_{i+j}$ and $s_i s_j = r_{i-j}$.
- Consider $w = 0^{2k}1^{2k}$, $x = 1^{2k}0^{2k}$ where $k \in \mathbb{N}$.
  Consider the following cases:

  Case 1: The elements in the group that get mapped are $\{r_i, r_j\}$. Then $yield(w) = (r_i)^{2k}(r_j)^{2k} = (r_j)^{2k}(r_i)^{2k} = yield(x)$.

  Case 2: Suppose at least one of the elements gets mapped to some $s_j$. Then $(s_j)^{2k} = (s_j s_j)^k = (r_0)^k = r_0$. Then $yield(w) = h^{2k} r_0 = r_0 h^{2k} = yield(x)$, $h \in G \setminus \{s_j\}$.

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$. ✓
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal. ✓
  - Class of Abelian groups and dihedral groups are **not** universal. ✓
  - Sufficiency conditions for non-universality of classes of groups.
- **Computational Version :** SepGroupWords Problem - Given two words $w, x \in \Sigma^*$, a set of permutations $S$ that generates a group $G \leq S_n$ and a function $\phi : \Sigma \to S$, with the guarantee that yield($w$)$\neq$ yield($x$) and an integer $k$, check if there is an automaton of size $k$ which separates $w$ and $x$.

  We show that SepGroupWords is NP-Complete

# Sufficiency Conditions for Non-Universality

**Lemma**

*Let $\mathcal{G}$ be a family of groups such that $\forall G \in \mathcal{G}, \forall g \in G$ order of $g \leq k$ for some finite $k \in \mathbb{N}$. Then $\mathcal{G}$ is not universal.*

**Lemma**

*If $\exists c\ \forall m$ such that $H_m \leq G_m$ is a maximal Abelian subgroup of $G_m$ and $\mathrm{lcm}(G_m \setminus H_m) \leq c$ then $\{G_m\}_{m \geq 0}$ is not universal*

# Our Results

- **Size Bounds :** $\forall w, x \in \{0,1\}^n$, a group of size $O(\sqrt{n}2^{\sqrt{n}})$ separating $w$ and $x$. ✓
- **Universality :**
  - Class of solvable groups, nilpotent groups, in particular, p-groups, are universal. ✓
  - Class of Abelian groups and dihedral groups are **not** universal. ✓
  - Sufficiency conditions for non-universality of classes of groups. ✓
- **Computational Version :** SepGroupWords Problem - Given two words $w, x \in \Sigma^*$, a set of permutations $S$ that generates a group $G \leq S_n$ and a function $\phi : \Sigma \to S$, with the guarantee that yield($w$)$\neq$ yield($x$) and an integer $k$, check if there is an automaton of size $k$ which separates $w$ and $x$.

  We show that SepGroupWords is NP-Complete

# Separating Group Words Problem

**Theorem**

$\textsc{SepGroupWords}$ *is* NP*-complete.*

- By reducing Separating Words Problem to $\textsc{SepGroupWords}$.
- $\textsc{SepWordProblem}(w, x, k) \iff \textsc{SepGroupWords}(w, x, S, \phi, k)$
  - $\exists$ Robson's permuting automaton $O(\sqrt{n})$.
  - $S$ is the set generators of Robson's group.
  - Given $w, x \in \{0, 1\}^n$, computing $S$ can be done in poly($n$) time.

# Open Problems

**Size of the group**

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

# Open Problems

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $\sqrt{n}2^{O\left(\sqrt{n}\right)}$

# Open Problems

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $\sqrt{n}2^{O\left(\sqrt{n}\right)}$
- **Lower bound :** $\Omega(\log n)$.

# Open Problems

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $\sqrt{n}2^{O\left(\sqrt{n}\right)}$
- **Lower bound :** $\Omega(\log n)$.

Question : Still an exponential gap !

- Characterization of Universality and Non-universality among classes of Groups.

# Open Problems

### Size of the group

Given $w$ and $x$ of length $n$, what is the size of the smallest group which separates them?

- **Upper bound :** $\sqrt{n}2^{O(\sqrt{n})}$
- **Lower bound :** $\Omega(\log n)$.

Question : Still an exponential gap !

- Characterization of Universality and Non-universality among classes of Groups.
- Bound on the size of $p$-groups used in Group Separation.

# Thank You!

# References I

Andrei A. Bulatov, Olga Karpova, Arseny M. Shur, and Konstantin Startsev.
Lower bounds on words separation: Are there short identities in transformation semigroups?
*Electron. J. Comb.*, 24(3):3, 2017.

Zachary Chase.
Separating words and trace reconstruction.
STOC 2021, page 21–31. Association for Computing Machinery, 2021.

Marek Chrobak.
Finite Automata and Unary Languages.
*Theoretical Computer Science*, 47:149 – 158, 1986.

# References II


Erik D. Demaine, Sarah Eisenstat, Jeffrey Shallit, and David A. Wilson.
Remarks on Separating Words.
In Markus Holzer, Martin Kutrib, and Giovanni Pighizzini, editors, *Descriptional Complexity of Formal Systems*, pages 147–157, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

William Fulton and Joe Harris.
*Representation theory: a first course.*
Springer, New York, 1st ed. edition, 2004.

P. Goralčík and V. Koubek.
On Discerning Words by Automata.
In Laurent Kott, editor, *Automata, Languages and Programming*, pages 116–122, Berlin, Heidelberg, 1986. Springer Berlin Heidelberg.

# References III

J.M. Robson.
Separating strings with small automata.
*Information Processing Letters*, 30(4):209 – 214, 1989.

J. M. Robson.
Separating words with machines and groups.
*RAIRO - Theoretical Informatics and Applications - Informatique Théorique et Appl.*, 30(1):81–86, 1996.

J Wiedermann.
Discerning Two Words by a Minimum Size Automaton.
Technical report, Institute of Computer Science, The Czech Academy of Sciences, 2015.