Lower bounds on the simultaneous conjugacy problem in the symmetric group

Rok Požar

University of Primorska

Joint work with Andrej Brodnik and Aleksander Malnič

4th annual Mississippi Discrete Mathematics Workshop

University of Mississippi

November 14-15, 2015

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

The problem

The problem

The decision r-simultaneous conjugacy problem (DSCP)

Given two r-tuples $(a_1, a_2, \ldots, a_r)$ and $(b_1, b_2, \ldots, b_r)$ of elements of a group G has the following system over G

$$\begin{aligned} b_1 &= \tau^{-1} a_1 \tau \\ b_2 &= \tau^{-1} a_2 \tau \\ &\vdots \\ b_r &= \tau^{-1} a_r \tau \end{aligned}$$

a solution?

The problem

The decision r-simultaneous conjugacy problem (DSCP)

Given two r-tuples $(a_1, a_2, \ldots, a_r)$ and $(b_1, b_2, \ldots, b_r)$ of elements of a group G has the following system over G

$$\begin{aligned} b_1 &= \tau^{-1} a_1 \tau \\ b_2 &= \tau^{-1} a_2 \tau \\ &\vdots \\ b_r &= \tau^{-1} a_r \tau \end{aligned}$$

a solution?

The search r-simultaneous conjugacy problem (SSCP)

construct a solution of the above system

Applications

Applications

Cryptography

the security of cryptographic key exchange protocols
reduction to the SSCP in Artin's braid groups

Applications

Cryptography

the security of cryptographic key exchange protocols
reduction to the SSCP in Artin's braid groups

Computational Group theory

computing centralizers, testing semiregularity
reduction to the SSCP and DSCP in symetric groups

Applications

Cryptography

the security of cryptographic key exchange protocols
reduction to the SSCP in Artin's braid groups

Computational Group theory

computing centralizers, testing semiregularity
reduction to the SSCP and DSCP in symetric groups

Algebraic Graph theory

lifting automorphisms along coverings of graphs
reduction to the DSCP in symmetric groups

Related work

Related work

G is the symmetric group S_n on n letters $1, 2, \ldots, n$

$r = 1$: optimal algorithm which takes $\mathcal{O}(n)$ time and $\mathcal{O}(n)$ space
$r > 1$: the best-known algorithm which solves SSCP (and hence DSCP) takes $\mathcal{O}(rn^2)$ time and $\mathcal{O}(rn)$ space

Related work

G is the symmetric group S_n on n letters $1, 2, \ldots, n$

$r = 1$: optimal algorithm which takes $\mathcal{O}(n)$ time and $\mathcal{O}(n)$ space
$r > 1$: the best-known algorithm which solves SSCP (and hence DSCP) takes $\mathcal{O}(rn^2)$ time and $\mathcal{O}(rn)$ space

Note

an algorithm taking $\mathcal{O}(rn \log(n))$ time and $\mathcal{O}(rn)$ space published by Sridhar* is wrong

* Sridhar, M. A.: A Fast Algorithm for Testing Isomorphism of Permutation Networks. IEEE Trans. Computers (TC) 38(6), 903–909 (1989)

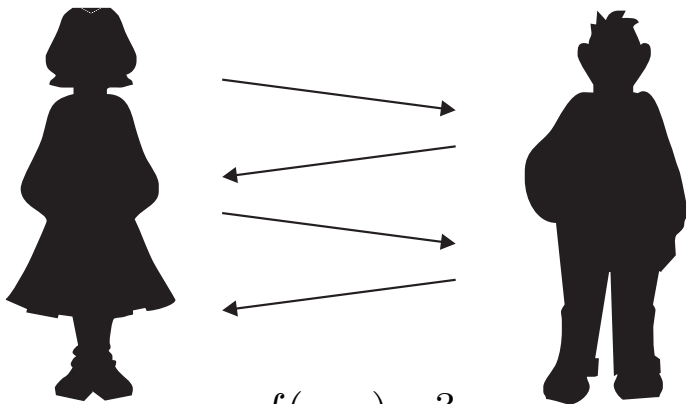
Communication model

Communication model

Decision problem

a Boolean-valued function $f : X \times Y \to \{0, 1\}$
two players Alice and Bob both knowing f
Alice holds $x \in X$, Bob holds $y \in Y$
goal is to evaluate f by exchanging bits according to some protocol

$$X = \{x_1, x_2, x_3, x_4\} \qquad Y = \{y_1, y_2, y_3, y_4\}$$



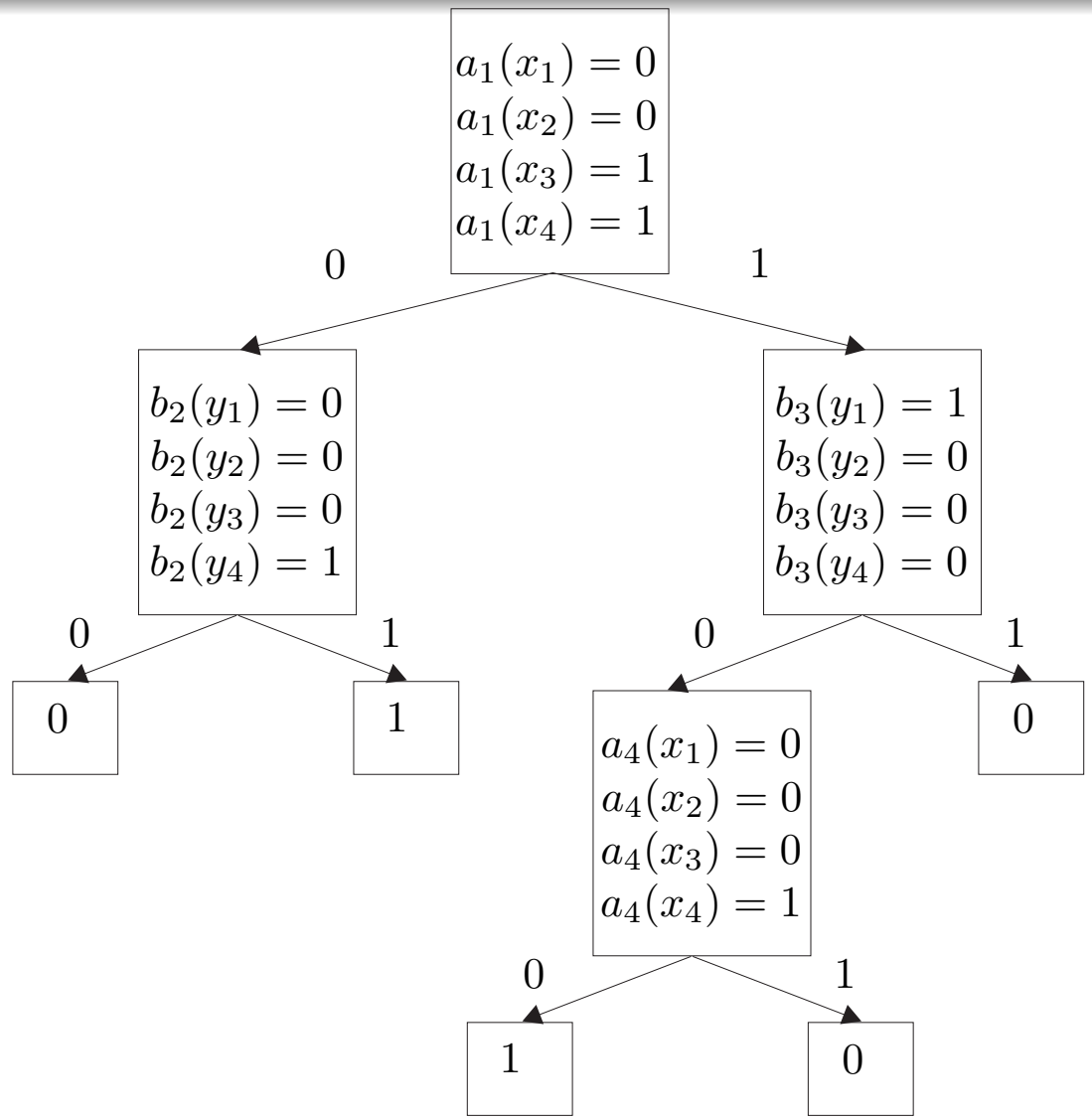
$$f(x, y) = ?$$

	y_1	y_2	y_3	y_4
x_1	0	0	0	1
x_2	0	0	0	1
x_3	0	1	1	1
x_4	0	0	0	0

Communication protocol

a binary tree
internal node v labeled
by $a_v : X \to \{0,1\}$ or
$b_v : Y \to \{0,1\}$
leaf labeled by 0 or 1

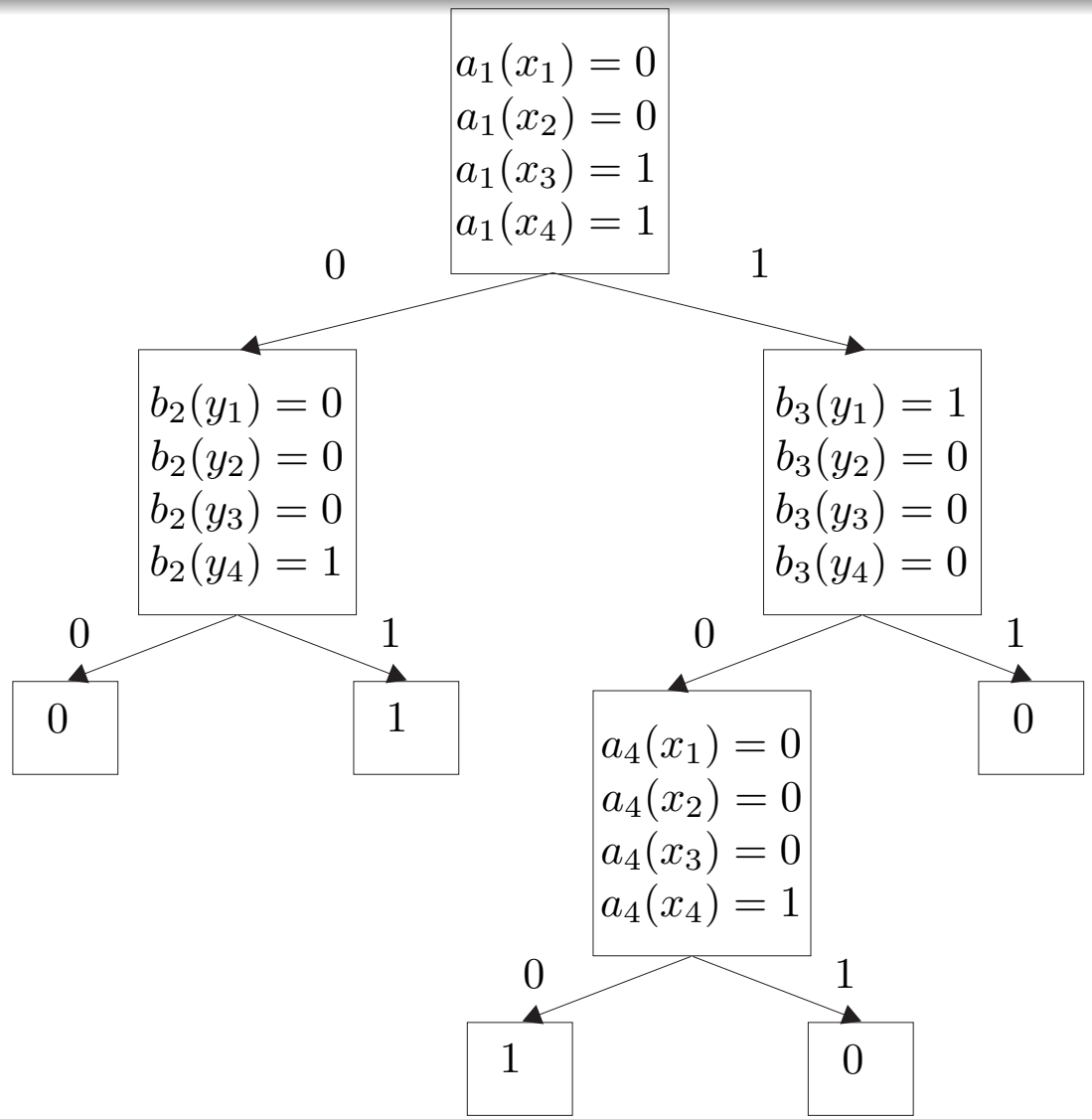
	y_1	y_2	y_3	y_4
x_1	0	0	0	1
x_2	0	0	0	1
x_3	0	1	1	1
x_4	0	0	0	0



Communication protocol

a binary tree
internal node v labeled
by $a_v : X \to \{0,1\}$ or
$b_v : Y \to \{0,1\}$
leaf labeled by 0 or 1

	y_1	y_2	y_3	y_4
x_1	0	0	0	1
x_2	0	0	0	1
x_3	0	1	1	1
x_4	0	0	0	0



A protocol solves f

$\forall (x, y) \in X \times Y$ walking down the tree leads to a leaf labeled by $f(x, y)$

Lower and upper bounds

Lower and upper bounds

Communication complexity $C(f)$

the minimum depth of the protocol tree among all protocols solving f

Lower and upper bounds

Communication complexity $C(f)$

the minimum depth of the protocol tree among all protocols solving f

Trivial protocol

suppose $|X| \leq |Y|$
Alice sends all her input to Bob – requiring $\log(|X|)$ bits
Upper bound: $C(f) \leq \log(|X|) + 1$

Lower and upper bounds

Communication complexity $C(f)$

the minimum depth of the protocol tree among all protocols solving f

Trivial protocol

suppose $|X| \leq |Y|$
Alice sends all her input to Bob – requiring $\log(|X|)$ bits
Upper bound: $C(f) \leq \log(|X|) + 1$

Communication matrix M_f

0-1 matrix M_f of dimension $|X| \times |Y|$
where (i, j) entry of M_f is $f(x_i, y_j)$

Lower and upper bounds

Communication complexity $C(f)$

the minimum depth of the protocol tree among all protocols solving f

Trivial protocol

suppose $|X| \leq |Y|$
Alice sends all her input to Bob – requiring $\log(|X|)$ bits
Upper bound: $C(f) \leq \log(|X|) + 1$

Communication matrix M_f

0-1 matrix M_f of dimension $|X| \times |Y|$
where (i, j) entry of M_f is $f(x_i, y_j)$

Lower bound

Mehlhorn and Schmidt: $C(f) \geq \log(\mathrm{rank}(M_f))$

Communication complexity of DSCP

Communication complexity of DSCP

Problem

Alice gets x, an r-tuple of elements of S_n
Bob gets y, an r-tuple of elements of S_n
they must decide whether x and y are simultaneously conjugated in S_n

Communication complexity of DSCP

Problem

Alice gets x, an r-tuple of elements of S_n
Bob gets y, an r-tuple of elements of S_n
they must decide whether x and y are simultaneously conjugated in S_n

Communication matrix M_f of dimension $(n!)^r \times (n!)^r$

$$M_f = \begin{bmatrix} E_1 & & 0 \\ & \ddots & \\ 0 & & E_m \end{bmatrix}$$

E_i matrix of ones and of dimension at most $n! \times n!$
$m \geq (n!)^{r-1}$ and hence $\mathrm{rank}(M_f) \geq (n!)^{r-1}$
$\log(\mathrm{rank}(M_f)) \geq (r-1)n\log(n)$

Communication complexity of DSCP

Problem

Alice gets x, an r-tuple of elements of S_n
Bob gets y, an r-tuple of elements of S_n
they must decide whether x and y are simultaneously conjugated in S_n

Communication matrix M_f of dimension $(n!)^r \times (n!)^r$

$$M_f = \begin{bmatrix} E_1 & & 0 \\ & \ddots & \\ 0 & & E_m \end{bmatrix}$$

E_i matrix of ones and of dimension at most $n! \times n!$
$m \geq (n!)^{r-1}$ and hence $\mathrm{rank}(M_f) \geq (n!)^{r-1}$
$\log(\mathrm{rank}(M_f)) \geq (r-1)n\log(n)$

For $r > 1$, the communication complexity of DSCP in S_n is $\Theta(rn\log(n))$.

Generalized communication model

Generalized communication model

Search problem

a relation $\mathcal{R} \subseteq X \times Y \times Z$
two players Alice and Bob both knowing $\mathcal{R}$
Alice holds $x \in X$, Bob holds $y \in Y$
goal is to find $z \in Z$ such that $(x, y, z) \in \mathcal{R}$ by exchanging bits according to some protocol

Generalized communication model

Search problem

a relation $\mathcal{R} \subseteq X \times Y \times Z$
two players Alice and Bob both knowing $\mathcal{R}$
Alice holds $x \in X$, Bob holds $y \in Y$
goal is to find $z \in Z$ such that $(x, y, z) \in \mathcal{R}$ by exchanging bits according to some protocol

A protocol solves $\mathcal{R}$

$\forall (x, y) \in X \times Y$ protocol reaches a leaf labeled by z such that $(x, y, z) \in \mathcal{R}$

Generalized communication model

Search problem

a relation $\mathcal{R} \subseteq X \times Y \times Z$
two players Alice and Bob both knowing $\mathcal{R}$
Alice holds $x \in X$, Bob holds $y \in Y$
goal is to find $z \in Z$ such that $(x, y, z) \in \mathcal{R}$ by exchanging bits according to some protocol

A protocol solves $\mathcal{R}$

$\forall (x, y) \in X \times Y$ protocol reaches a leaf labeled by z such that $(x, y, z) \in \mathcal{R}$

Communication complexity $C(\mathcal{R})$

the minimum depth among all communication protocols solving $\mathcal{R}$

Communication complexity of DSCP

Communication complexity of DSCP

Problem

Alice gets x, an r-tuple of elements of S_n
Bob gets y, an r-tuple of elements of S_n
they must find $\tau \in S_n$ which simultaneously conjugates x and y or return 'No'

Communication complexity of DSCP

Problem

Alice gets x, an r-tuple of elements of S_n
Bob gets y, an r-tuple of elements of S_n
they must find $\tau \in S_n$ which simultaneously conjugates x and y or return 'No'

SSCP at least as hard as DSCP

for $r > 1$, the communication complexity of SSCP in S_n is $\Theta(rn \log(n))$.

Decision tree model

Decision tree model

Binary tree

each interior vertex represents a decision
leaves represent the desired output

Decision tree model

Binary tree

each interior vertex represents a decision
leaves represent the desired output

Time complexity of a decision tree

height of the tree, as the function of the size of the problem

Decision tree model

Binary tree

each interior vertex represents a decision
leaves represent the desired output

Time complexity of a decision tree

height of the tree, as the function of the size of the problem

The number of leaves in a decision tree to search a solution $\tau \in S_n$

for $r > 1$, $\forall \tau \in S_n \ \exists$ r-tuples x and y s.t. τ is a unique solution
at least $n!$ leaves in a decision tree
height of the tree at least $\mathcal{O}(n \log(n))$

Decision tree model

Binary tree

each interior vertex represents a decision
leaves represent the desired output

Time complexity of a decision tree

height of the tree, as the function of the size of the problem

The number of leaves in a decision tree to search a solution $\tau \in S_n$

for $r > 1$, $\forall \tau \in S_n$ $\exists$ r-tuples x and y s.t. τ is a unique solution
at least $n!$ leaves in a decision tree
height of the tree at least $\mathcal{O}(n \log(n))$

Under the decision tree model

for $r > 1$, SSCP in S_n has lower bound of $\Omega(n \log(n))$

Tu sum up

Tu sum up

RAM model

Upper bound: $\mathcal{O}(rn^2)$ time ($\mathcal{O}(rn)$ space memory) for SSCP/DSCP
Trivial lower bound: $\Omega(rn)$ time ($\theta(n)/\theta(1)$ space memory) for SSCP/DSCP

Tu sum up

RAM model

Upper bound: $\mathcal{O}(rn^2)$ time ($\mathcal{O}(rn)$ space memory) for SSCP/DSCP
Trivial lower bound: $\Omega(rn)$ time ($\theta(n)/\theta(1)$ space memory) for SSCP/DSCP

Communication model

Upper bound: $\mathcal{O}(rn\log(n))$ (unbounded space memory) for SSCP/DSCP
Lower bound: $\Omega(rn\log(n))$ (unbounded space memory) for SSCP/DSCP

Tu sum up

RAM model

Upper bound: $\mathcal{O}(rn^2)$ time ($\mathcal{O}(rn)$ space memory) for SSCP/DSCP
Trivial lower bound: $\Omega(rn)$ time ($\theta(n)/\theta(1)$ space memory) for SSCP/DSCP

Communication model

Upper bound: $\mathcal{O}(rn\log(n))$ (unbounded space memory) for SSCP/DSCP
Lower bound: $\Omega(rn\log(n))$ (unbounded space memory) for SSCP/DSCP

Decision tree model

Lower bound: $\Omega(n\log(n))$ (unbounded space memory) for SSCP

Thank you!