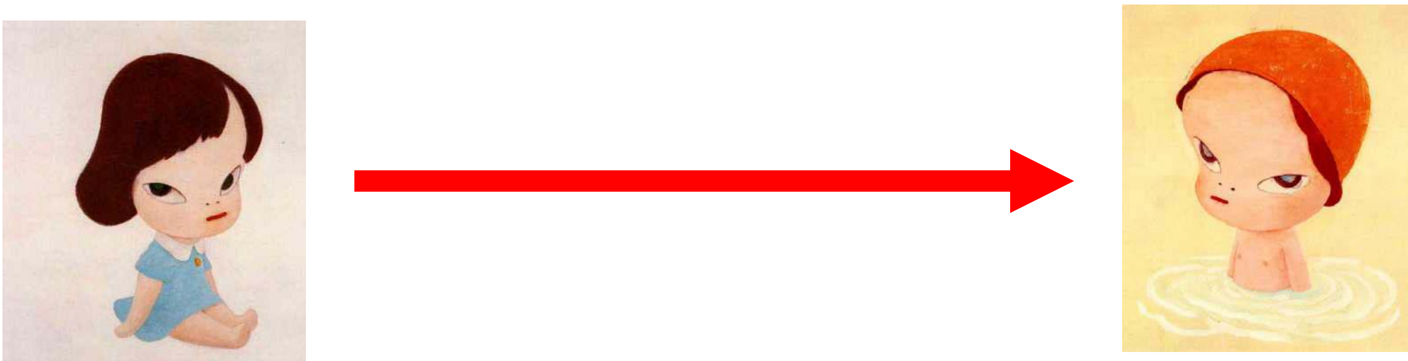
Exponential Separation of Quantum and Classical One-Way Communication Complexity

Iordanis Kerenidis
UC Berkeley

Joint work with: Ziv Bar-Yossef T. S. Jayram
IBM Almaden Research

One-Way Communication Complexity



One-Way Communication Complexity

Spot a difference!

One-Way Communication Complexity

Are the images the same?

One-Way Communication Complexity

00111010001101...

Input **x**

Input **y**

Goal: Output P(**x**,**y**)

(minimum communication)

- Applications of Communication Complexity

  VLSI design, Boolean circuits, Data structures, Automata, Formulae size, Data streams, …

- Encoding/Compression scheme C(x), such that P(x,y)=g(C(x),y)

Quantum one-way communication complexity

Input **x**

Input **y**

Goal: Output P(**x,y)**
(minimum communication)

Main question:

What is the relation between classical and quantum one-way communication?

Quantum one-way communication complexity

- Holevo's bound
  - We cannot compress information by using qubits.
    We need n qubits to transmit n classical bits.

- [Kremer95] defined a complete problem for boolean promise problems of logarithmic quantum communication complexity.

- [Raz 99] also considers the same problem. He gives an exponential separation for two-way communication.

Quantum one-way communication complexity

- Holevo's bound
  - We cannot compress information by using qubits.
    We need n qubits to transmit n classical bits.

- [Kremer95] defined a complete problem for boolean promise problems of logarithmic quantum communication complexity.

- [Raz 99] also considers the same problem. He gives an exponential separation for two-way communication.

Our result:

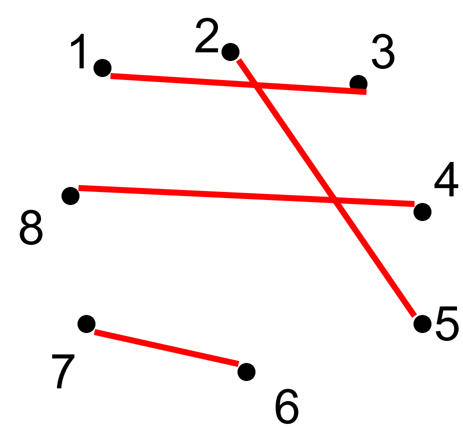
The first exponential separation of classical and quantum one-way communication complexity.

Hidden matching problem HM_n

Input: x 2 $\{0,1\}^n$

Input: a matching M on [n]

e.g. {(1,3),(2,5),(4,8),(6,7)}



Hidden matching problem HM_n

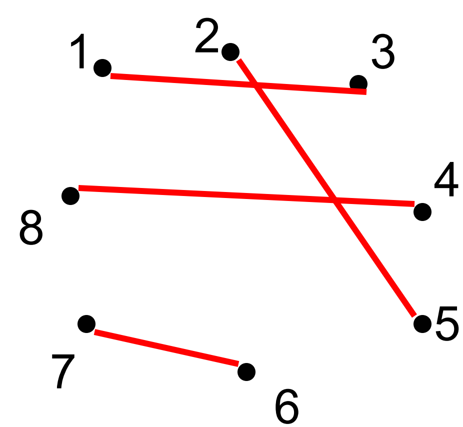
Input: x 2 $\{0,1\}^n$

Output:

$$((i,j), x_i \oplus x_j),$$
for $(i,j) \in M$

Input: a matching M on [n]

e.g. {(1,3),(2,5),(4,8),(6,7)}



Complexity of HM_n

Input: x 2 $\{0,1\}^n$

Input: a matching M on [n]

Output

$$((i,j), x_i \oplus x_j),$$
for $(i,j) \in M$

Theorem

- There exists a quantum algorithm with complexity $O(\log n)$
- Any randomized algorithm with public coins has complexity $\Omega(\sqrt{n})$

Quantum algorithm for HM_n

Let $M = \{(i_1, i_2), (i_3, i_4), \ldots, (i_{n-1}, i_n)\}$ be Bob's matching.

- Alice sends the state

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$$

- Bob measures in the basis

$$B = \{|i_1\rangle \pm |i_2\rangle, |i_3\rangle \pm |i_4\rangle, \ldots, |i_{n-1}\rangle \pm |i_n\rangle\}$$

and outputs
$$\begin{cases} ((j,k), 0) & \text{if he measures } |j\rangle + |k\rangle \\ ((j,k), 1) & \text{if he measures } |j\rangle - |k\rangle \end{cases}$$

Quantum algorithm for HM_n

- Alice sends the state

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i}|i\rangle = \frac{1}{\sqrt{n}}(((-1)^{x_{i_1}}|i_1\rangle+(-1)^{x_{i_2}}|i_2\rangle)+\ldots+((-1)^{x_{i_{n-1}}}|i_{n-1}\rangle+(-1)^{x_{i_n}}|i_n\rangle))$$

- Bob measures in the basis

$$B = \{|i_1\rangle \pm |i_2\rangle, |i_3\rangle \pm |i_4\rangle, \ldots, |i_{n-1}\rangle \pm |i_n\rangle\}$$

- $Prob[\text{outcome is } |j\rangle+|k\rangle] = \frac{1}{2n}((-1)^{x_j}+(-1)^{x_k})^2$

  $Prob[\text{outcome is } |j\rangle-|k\rangle] = \frac{1}{2n}((-1)^{x_j}-(-1)^{x_k})^2$

- Bob can compute the XOR of a pair of the matching with prob. 1

HM_n and Other problems

Locally Decodable Codes

- The quantum algorithm relies on the property that we can compute efficiently the XOR of a pair of a matching from a uniform superposition.
- Same property was used in [K., deWolf] to prove a lower bound for 2-query Locally Decodable Codes.

HM_n and Other problems

Locally Decodable Codes

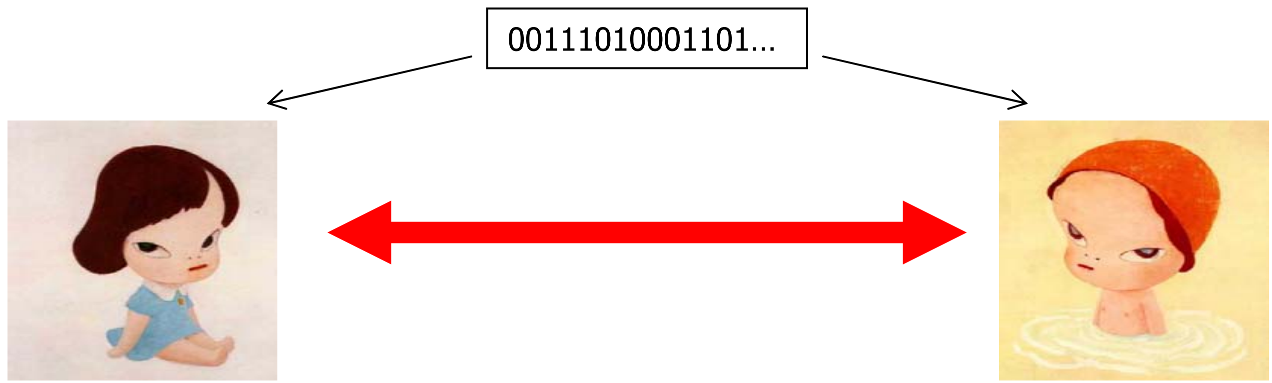
- The quantum algorithm relies on the property that we can compute efficiently the XOR of a pair of a matching from a uniform superposition.
- Same property was used in [K., deWolf] to prove a lower bound for 2-query Locally Decodable Codes.

Complete Problems

- We can define a variant of Kremer's problem which is complete for non-boolean promise problems of logarithmic on-way quantum communication complexity.
- Our bounds extend to this problem.

Other models of communication complexity

- Two-way communication



- [Raz99] proved an exponential separation.
- The quantum protocol needs two rounds.

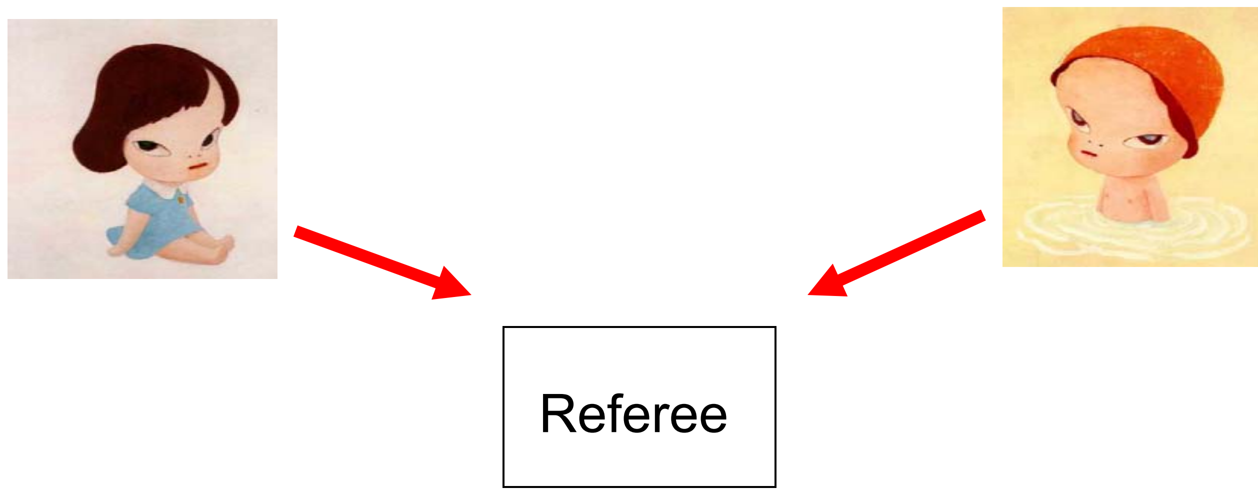
Other models of communication complexity

- Sampling model

- [ASTVW98] proved an exponential separation.
- The separation does not hold with public coins.

Other models of communication complexity

- Simultaneous Messages



- Quantum fingerprints [BCWdW01]
  The separation does not hold with shared public coins

Our problem provides the first exponential separation in the model of Simultaneous Messages with public coins.

Neat application [Harry Buhrman]

Hidden matching Problem as a non-locality game

- Using EPR pairs and NO communication, we can create correlations for which we need exponential classical communication even to approximate them!

Hidden matching problem HM_n

Input: x 2 $\{0,1\}^n$

Input: a matching M on [n]

Output

$$((i,j), x_i \oplus x_j),$$
$$\text{for } (i,j) \in M$$

Theorem

- There exists a quantum algorithm with complexity $O(\log n)$
- Any randomized algorithm with public coins has complexity $\Omega(\sqrt{n})$

Lower bound for HM_n

- By Yao's Lemma we will construct a "hard" distribution over instances of HM_n and prove a distributional lower bound w.r.t. deterministic one-way protocols.

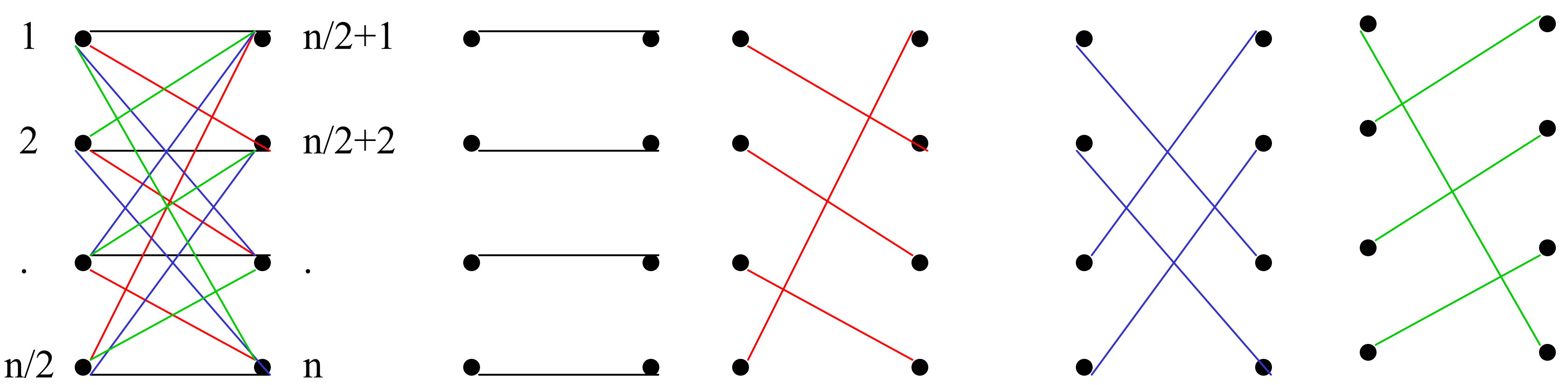
Lower bound for HM_n

- By Yao's Lemma we will construct a "hard" distribution over instances of HM_n and prove a distributional lower bound w.r.t. deterministic one-way protocols.

- Distribution of Alice's input: $x \; 2_R \; \{0,1\}^n$

- Distribution of Bob's input: $M \; 2_R \; M_n$

  M_n is any set of $\Omega(n)$ pairwise edge-disjoint matchings.



Lower bound for HM_n

Intuition :

Alice's message must contain information about at least one edge of each matching (Ω(n) edges).

(e.g. x_1© x_2 , x_2© x_3 , x_1© x_3 , …)

There are $\Omega(\sqrt{n})$ independent edges.

Hence, the message needs to be of length $\Omega(\sqrt{n})$

Lower bound for HM_n

Intuition :

Alice's message must contain information about at least one edge of each matching (Ω(n) edges).

(e.g. x_1© x_2 , x_3© x_4 , x_1© x_4 , x_2© x_3 …)

There are $\Omega(\sqrt{n})$ independent edges.

Hence, the message needs to be of length $\Omega(\sqrt{n})$

Idea of Proof :

We prove that Alice cannot send the same message for too many inputs x.

Every matching imposes a linear constraint on x. (e.g. x_1© $x_2 = 0, \ldots$)

There are at least $\Omega(\sqrt{n})$ linearly independent constraints,

hence only $2^{n-\Omega(\sqrt{n})}$ x's can be mapped to the same message.

We need to take care of errors!!!

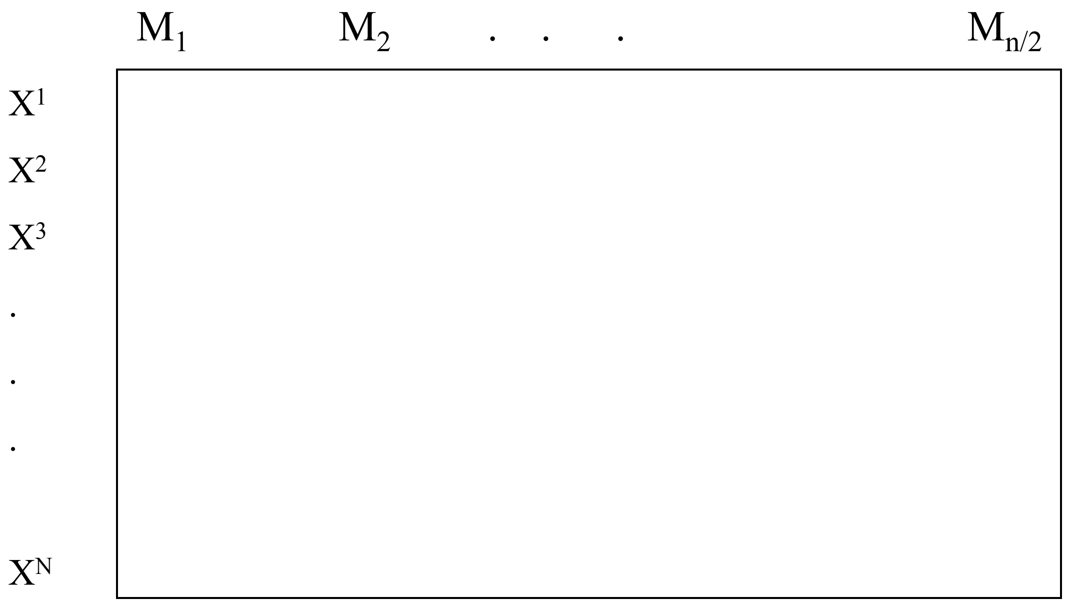
Lower bound for HM_n

$$
\begin{array}{c}
 \\
X^1 \\
X^2 \\
X^3 \\
. \\
. \\
. \\
X^N
\end{array}
\begin{array}{c}
M_1 \qquad M_2 \qquad . \quad . \quad . \qquad\qquad M_{n/2} \\
\boxed{\begin{array}{c} \\ \\ \\ ((i,j)\ ,\ x_i©x_j) \\ \\ \\ \\ \end{array}}
\end{array}
$$

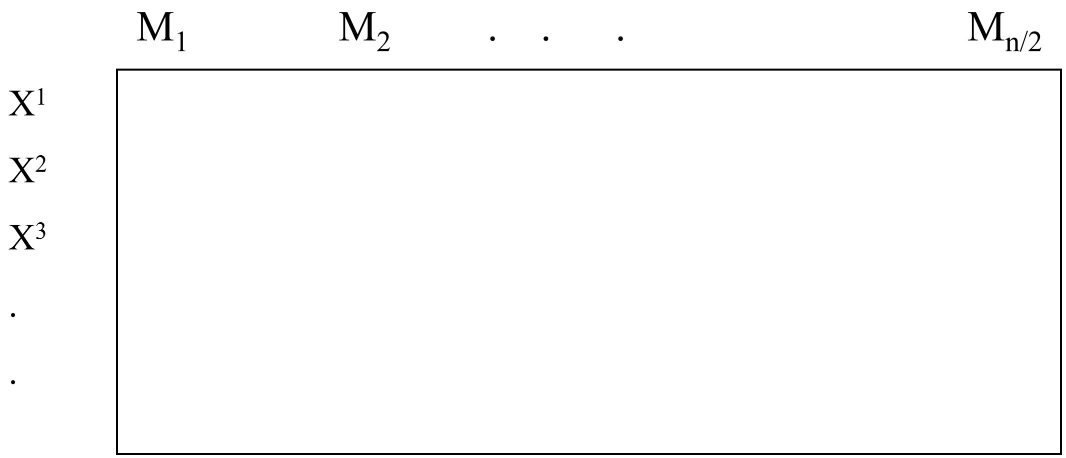
The Matrix

- At least a (1-δ) fraction of the entries are correct.
  - At least half the columns are (1-2δ)-"good".
  - At least half the rows are (1-2δ)-"good".

Step 1:Pick "good" rows corresponding to the same msg.

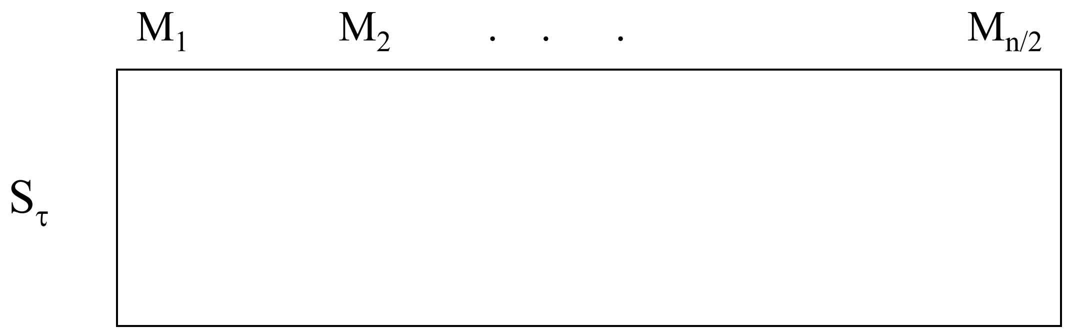


Step 1:Pick "good" rows corresponding to the same msg.



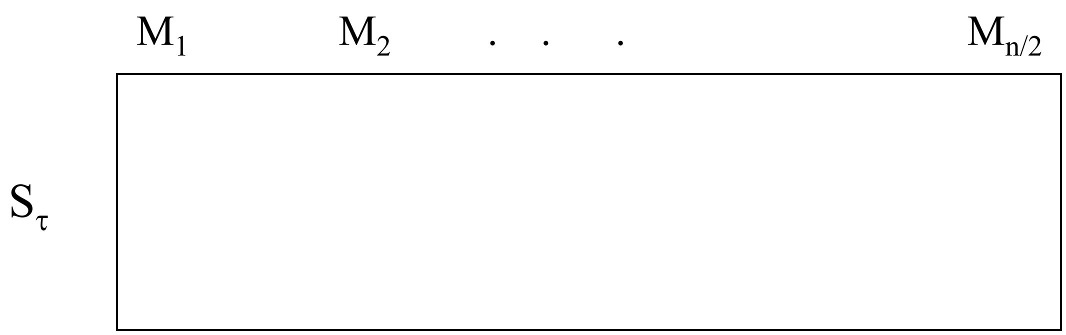
- Each row is $(1\text{-}2\delta)$-"good".

Step 1:Pick "good" rows corresponding to the same msg.

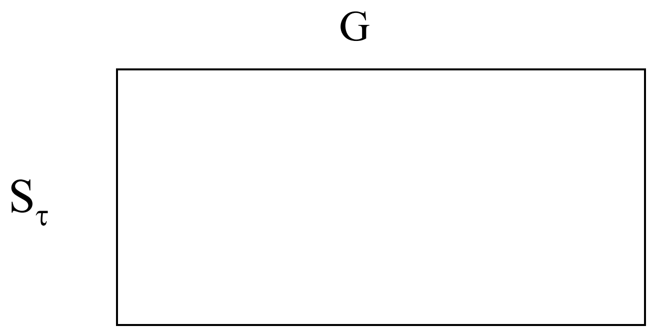


- Each row is $(1\text{-}2\delta)$-"good".
- Let S_τ be the set of x's that correspond to the most "popular" message τ.
- Number of Alice's distinct message ¸ $2^n / |S_\tau|$
- I need to bound the size of $|S_\tau|$!

Step 2: Pick "good" , independent columns

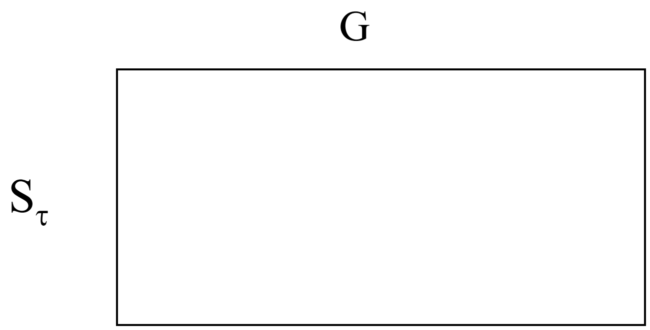


Step 2: Pick "good" , independent columns



- Each column is $(1-4\delta)$-"good". $|G| = \Omega(n)$

Step 2: Pick "good" , independent columns

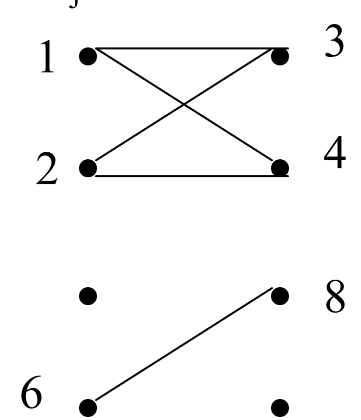


- Each column is (1-4δ)-"good". $|G| = \Omega(n)$
- All the rows of the matrix are the same.
- Each row contains $\Omega(n)$ entries of the form $((i,j),x_i$ © $x_j)$

Step 2: Pick "good" , independent columns

- Each column is (1-4δ)-"good". $|G| = \Omega(n)$
- All the rows of the matrix are the same.
- Each row contains $\Omega(n)$ entries of the form $((i,j), x_i$ © $x_j)$
- Define the Graph G.

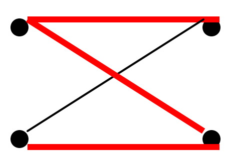
(e.g. x_1© x_3 , x_1© x_4 , x_2© x_4 , x_2© x_3 , x_6© x_8 …)



Step 2: Pick "good" , independent columns

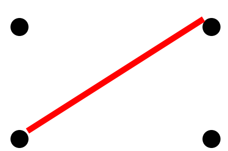
- Each column is (1-4δ)-"good". $|G| = \Omega(n)$
- All the rows of the matrix are the same.
- Each row contains $\Omega(n)$ entries of the form $((i,j), x_i \copyright x_j)$
- Define the Graph G.

  (e.g. $x_1 \copyright x_3$, $x_1 \copyright x_4$, $x_2 \copyright x_4$, $x_2 \copyright x_3$, $x_6 \copyright x_8$ …)

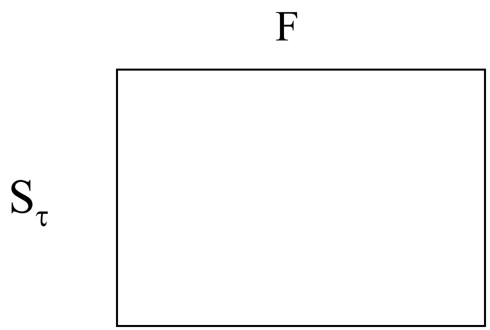


- There are Ω(n) edges)

  There exists a forest of size $\Omega(\sqrt{n})$

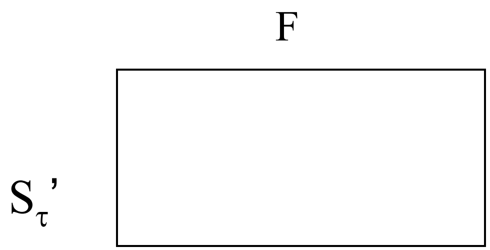


Step 2: Pick "good" , independent columns



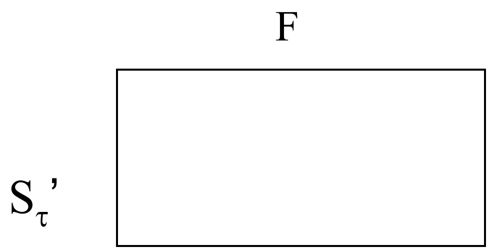
- The columns in F are independent and $|F| = \Omega(\sqrt{n})$

Pick "good" rows again!



- The columns in F are independent and |F|= $\Omega(\sqrt{n})$
- Each row is (1-8δ)-"good"

Lower bound for HM_n



- The rows correspond to inputs mapped to the same message.
- The columns correspond to independent edges, $|F|=\Omega(\sqrt{n})$
- In each row, (1- 8δ) fraction of the entries are correct.

Lower bound for HM_n

- How many x's can be mapped to the same message?
- n variables and a set F of $\Omega(\sqrt{n})$ independent linear constraints.
  - There are $2^{n-\Omega(\sqrt{n})}$ solutions.
- We also need to count all x's that satisfy a set of constraints which agrees with F on at least a (1-8δ) fraction.
  - There are $2^{H_2(8\delta)\Omega(\sqrt{n})}$ such sets of constraints.
- Total number of x's mapped to the same message:

$$|S_\tau| \cdot 2^{n-(1-H_2(8\delta))\Omega(\sqrt{n})}$$

Lower bound for HM_n

- Total number of x's mapped to the same message:

$$|S_\tau| \cdot \; 2^{n-(1-H_2(8\delta))\Omega(\sqrt{n})}$$

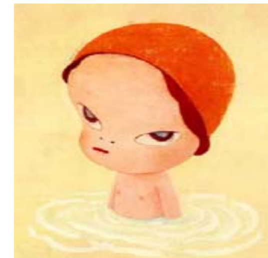
- Size of Alice's message = $\log(2^n / |S_\tau|) = \Omega(\sqrt{n})$

<u>Theorem:</u>

The one-way randomized communication complexity of HM_n is $\Theta(\sqrt{n})$

<u>Upper bound:</u> It's sufficient for Alice to send $O(\sqrt{n})$ random bits of x.

Boolean Hidden Matching Problem



Input: x 2 $\{0,1\}^n$

Output:

$\begin{cases} 0 \text{ if } w \text{ is correct} \\ 1 \text{ if } w \text{ is wrong} \end{cases}$

Input: a matching M on [n],

w 2 $\{0,1\}^{n/2}$

Theorem

- There exists a quantum algorithm with complexity $O(\log n)$
- Any linear randomized algorithm with public coins has complexity $\Omega(n^{1/3})$

Open problems

- Work in progress
  - Boolean HM_n : extend the lower bound to general randomised protocols.
  - Provide a separation between quantum one-way and classical two-way communication.

- Open problems
  - One-way communication complexity of total functions
  - Simultaneous Messages

  - Quantum advice: BQP/poly vs. BQP/qpoly
  - Quantum proofs: QMA vs. QCMA