Classical Interaction Cannot Replace Quantum Nonlocality

Dmitry Gavinsky

NEC Labs, Princeton

Communication Complexity

$f : X \times Y \rightarrow \{0, 1\}$

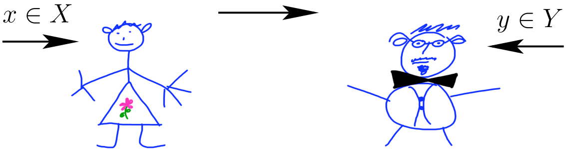
Communication Complexity

$f : X \times Y \rightarrow \{0,1\}$

- *Alice* receives x and *Bob* receives y

Communication Complexity

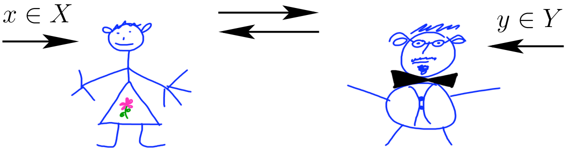
$f : X \times Y \to \{0,1\}$



- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*

Communication Complexity

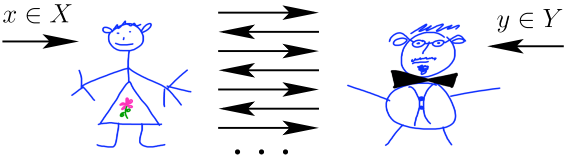
$f : X \times Y \to \{0,1\}$



- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*
- *Bob* sends a message to *Alice*

Communication Complexity

$f : X \times Y \to \{0,1\}$

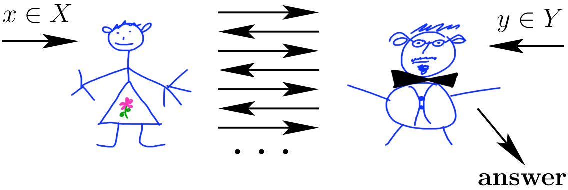


- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*
- *Bob* sends a message to *Alice*

• • •

Communication Complexity

$f : X \times Y \to \{0, 1\}$



- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*
- *Bob* sends a message to *Alice*

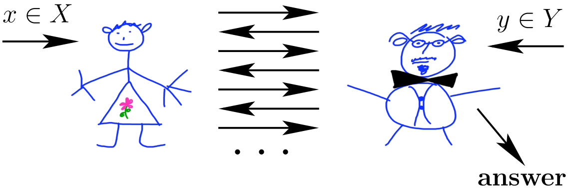
• • •

- *Bob* produces an answer

Communication Complexity

$f : X \times Y \to \{0,1\}$

Does the answer equal $f(x, y)$?



- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*
- *Bob* sends a message to *Alice*

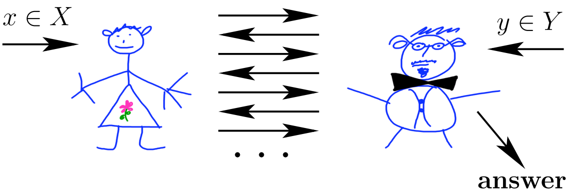
  • • •

- *Bob* produces an answer

Multi-Round vs. One-Way Communication

Does the answer equal $f(x, y)$?

Multi-Round Communication:



- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*
- *Bob* sends a message to *Alice*

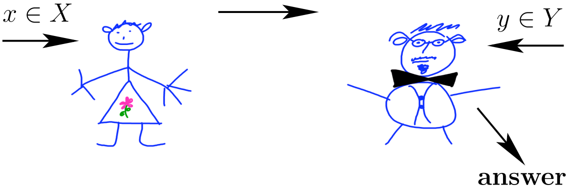
• • •

- *Bob* produces an answer

Multi-Round vs. One-Way Communication

Does the answer equal $f(x, y)$?

One-Way Communication:

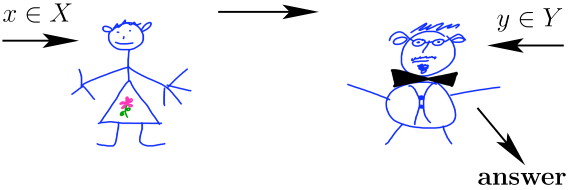


- *Alice* receives x and *Bob* receives y
- *Alice* sends a message to *Bob*
- *Bob* produces an answer

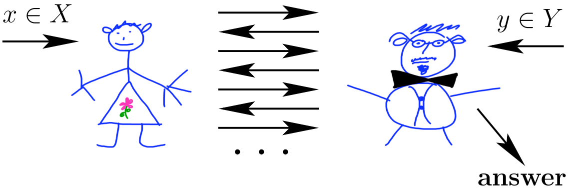
Multi-Round vs. One-Way Communication

Does the answer equal $f(x, y)$?

One-Way Communication:

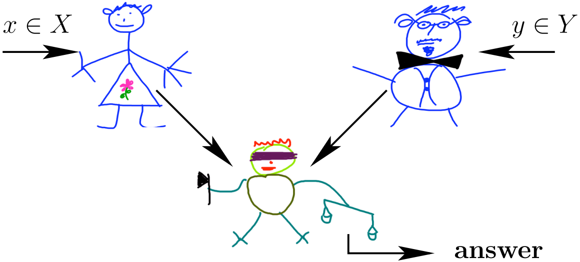


Multi-Round Communication:



Simultaneous Message Passing (SMP) Communication Model

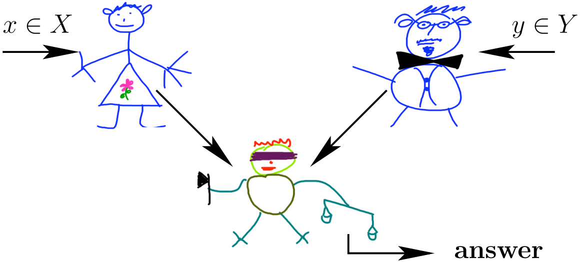
$f : X \times Y \to \{0,1\}$



- *Alice* receives x and sends a message to the *referee*
- (at the same time) *Bob* receives y and sends a message to the *referee*

Simultaneous Message Passing (SMP) Communication Model

$f : X \times Y \to \{0, 1\}$

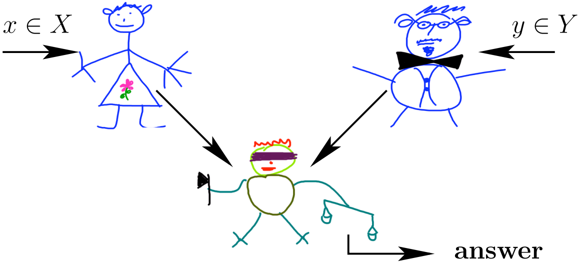


- *Alice* receives x and sends a message to the *referee*
- (at the same time) *Bob* receives y and sends a message to the *referee*
- the *referee* reads the messages and produces an answer

Simultaneous Message Passing (SMP) Communication Model

$f : X \times Y \rightarrow \{0, 1\}$

Does the answer equal $f(x, y)$?



- *Alice* receives x and sends a message to the *referee*
- (at the same time) *Bob* receives y and sends a message to the *referee*
- the *referee* reads the messages and produces an answer

How to Compare Models (One Classical Example)

How to Compare Models (One Classical Example)

- **Communication complexity** *of a problem is the minimum amount of bits that have to be sent by the players in order to solve the problem with good probability.*
  Usually, the communication complexity of a problem is expressed as a *function of the input length*.

How to Compare Models (One Classical Example)

- **Communication complexity** *of a problem is the minimum amount of bits that have to be sent by the players in order to solve the problem with good probability.*
  Usually, the communication complexity of a problem is expressed as a *function of the input length*.

- *Indexing function:* Alice receives $x \in \{0,1\}^n$, Bob receives $i \in \{1,\ldots,n\}$. Bob must output x_i.

How to Compare Models (One Classical Example)

- **Communication complexity** *of a problem is the minimum amount of bits that have to be sent by the players in order to solve the problem with good probability.*
  Usually, the communication complexity of a problem is expressed as a *function of the input length*.
- *Indexing function:* Alice receives $x \in \{0,1\}^n$, Bob receives $i \in \{1, \ldots, n\}$. Bob must output x_i.
- *Multi-round protocol:* Bob sends to Alice i, she responds with x_i; that costs $O(\log n)$ *bits*.

How to Compare Models (One Classical Example)

- **Communication complexity** *of a problem is the minimum amount of bits that have to be sent by the players in order to solve the problem with good probability.*
  Usually, the communication complexity of a problem is expressed as a *function of the input length*.
- *Indexing function:* Alice receives $x \in \{0,1\}^n$, Bob receives $i \in \{1,\ldots,n\}$. Bob must output x_i.
- *Multi-round protocol:* Bob sends to Alice i, she responds with x_i; that costs $O(\log n)$ *bits*.
- *One-way lower bound:* A single message which would let Bob know any of n mutually independent bits of x with probability $1/2 + \Omega(1)$ must contain $\Omega(n)$ *bits*.

How to Compare Models (One Classical Example)

- **Communication complexity** *of a problem is the minimum amount of bits that have to be sent by the players in order to solve the problem with good probability.*
  Usually, the communication complexity of a problem is expressed as a *function of the input length*.
- *Indexing function:* Alice receives $x \in \{0,1\}^n$, Bob receives $i \in \{1, \ldots, n\}$. Bob must output x_i.
- *Multi-round protocol:* Bob sends to Alice i, she responds with x_i; that costs $O(\log n)$ *bits*.
- *One-way lower bound:* A single message which would let Bob know any of n mutually independent bits of x with probability $1/2 + \Omega(1)$ must contain $\Omega(n)$ *bits*.

▶ Therefore, *multi-round communication can be exponentially more efficient than one-way communication*.

Quantum Communication Complexity

Quantum Communication Complexity

- Most classical communication models under investigation have natural quantum analogues.

Quantum Communication Complexity

- Most classical communication models under investigation have natural quantum analogues.
- In quantum models, both communication and local operations of the parties are governed by the *laws of quantum mechanics*.

Quantum Communication Complexity

- Most classical communication models under investigation have natural quantum analogues.
- In quantum models, both communication and local operations of the parties are governed by the *laws of quantum mechanics*.
- All (reasonable) quantum models are at least as strong as their classical analogues.

Quantum Communication Complexity

- Most classical communication models under investigation have natural quantum analogues.
- In quantum models, both communication and local operations of the parties are governed by the *laws of quantum mechanics*.
- All (reasonable) quantum models are at least as strong as their classical analogues.
- Both quantum and classical communication can be amplified by *shared entanglement*.

Previous and New Results

- An exponential separation between *multi-round* quantum and classical communication models was given by Raz [R99].

Previous and New Results

- An exponential separation between *multi-round* quantum and classical communication models was given by Raz [R99].
- An exponential separation between *one-way* quantum and classical models was given by Bar-Yossef, Jayram and Kerenidis [BJK04].

Previous and New Results

- An exponential separation between *multi-round* quantum and classical communication models was given by Raz [R99].
- An exponential separation between *one-way* quantum and classical models was given by Bar-Yossef, Jayram and Kerenidis [BJK04].
- In [G07] it was demonstrated that there existed a communication task that was *exponentially easier to solve in the one-way quantum model than in the multi-round classical model*.

Previous and New Results

- An exponential separation between *multi-round* quantum and classical communication models was given by Raz [R99].
- An exponential separation between *one-way* quantum and classical models was given by Bar-Yossef, Jayram and Kerenidis [BJK04].
- In [G07] it was demonstrated that there existed a communication task that was *exponentially easier to solve in the one-way quantum model than in the multi-round classical model*.

► *Our main result*: *There exists a communication task that is exponentially easier to solve in the SMP model with classical communication and shared entanglement than in the multi-round classical model*. In fact, our separation also subsumes that from [G07].

Previous and New Results

- An exponential separation between *multi-round* quantum and classical communication models was given by Raz [R99].
- An exponential separation between *one-way* quantum and classical models was given by Bar-Yossef, Jayram and Kerenidis [BJK04].
- In [G07] it was demonstrated that there existed a communication task that was *exponentially easier to solve in the one-way quantum model than in the multi-round classical model*.
- *Our main result*: *There exists a communication task that is exponentially easier to solve in the SMP model with classical communication and shared entanglement than in the multi-round classical model*. In fact, our separation also subsumes that from [G07].
- *Our second result*: *There exists a nonlocality game that is "robust" against $n^{\Omega(1)}$ communication between unentangled players*.

Previous and New Results

- An exponential separation between *multi-round* quantum and classical communication models was given by Raz [R99].
- An exponential separation between *one-way* quantum and classical models was given by Bar-Yossef, Jayram and Kerenidis [BJK04].
- In [G07] it was demonstrated that there existed a communication task that was *exponentially easier to solve in the one-way quantum model than in the multi-round classical model*.
- *Our main result*: *There exists a communication task that is exponentially easier to solve in the SMP model with classical communication and shared entanglement than in the multi-round classical model*. In fact, our separation also subsumes that from [G07].
- *Our second result*: *There exists a nonlocality game that is "robust" against $n^{\Omega(1)}$ communication between unentangled players*.

▶ These *two results* give almost the strongest possible (and the strongest known) indication of nonlocal properties of two-party entanglement.

Our Communication Task

Our Communication Task

	1	*2*	
	1,5	3,8	*1*
	4,7	2,6	*2*

- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.

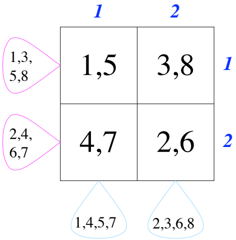
Our Communication Task

		1	*2*	
1,3, 5,8		1,5	3,8	*1*
2,4, 6,7		4,7	2,6	*2*

- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.

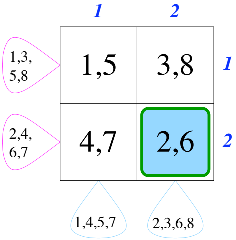
▶ Alice knows the elements of each row.

Our Communication Task



- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.
- Alice knows the elements of each row.
- Bob knows the elements of each column.

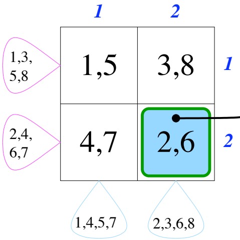
Our Communication Task



$\big((\mathbf{2},\mathbf{2}),$

- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.
- Alice knows the elements of each row.
- Bob knows the elements of each column.
- Bob has to *choose a cell*, and *to output a number orthogonal to the bit-wise xor of its two elements*.

Our Communication Task

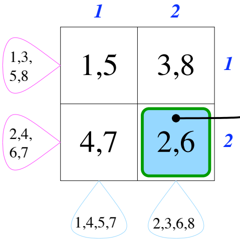


$$\begin{array}{r} 2 = 0010 \\ 6 = 0110 \\ \hline 0100 \end{array} \oplus \quad 0100 \perp 1010$$

$\big((\mathbf{2},\mathbf{2}),\mathbf{1010}\big)$ is a valid answer

- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.
- Alice knows the elements of each row.
- Bob knows the elements of each column.
- Bob has to *choose a cell*, and *to output a number orthogonal to the bit-wise xor of its two elements*.

Our Communication Task

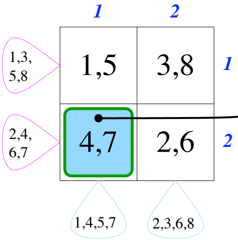


$$\begin{array}{r} 2 = 0010 \\ 6 = \underline{0110} \end{array} \oplus$$
$$0100 \perp 0001$$

$\big((\mathbf{2},\mathbf{2}),\mathbf{1010}\big)$ is a valid answer
$\big((\mathbf{2},\mathbf{2}),\mathbf{0001}\big)$ is another valid answer

- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.
- Alice knows the elements of each row.
- Bob knows the elements of each column.
- ▶ Bob has to *choose a cell*, and *to output a number orthogonal to the bit-wise xor of its two elements*.

Our Communication Task

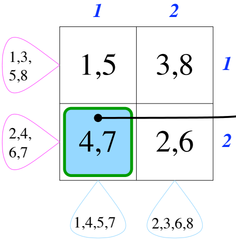


$$\begin{array}{r} 4 = 0100 \\ 7 = 0111 \\ \hline 0011 \end{array} \oplus \quad 0011 \perp 0011$$

$\big((\mathbf{2},\mathbf{2}),\mathbf{1010}\big)$ is a valid answer
$\big((\mathbf{2},\mathbf{2}),\mathbf{0001}\big)$ is another valid answer
$\big((\mathbf{2},\mathbf{1}),\mathbf{0011}\big)$ is valid too

- Integers $1..2n^2$ are placed in an $n \times n$ table, two numbers in every cell; the columns are indexed $1..n$.
- Alice knows the elements of each row.
- Bob knows the elements of each column.
- Bob has to *choose a cell*, and *to output a number orthogonal to the bit-wise xor of its two elements*.

Communication Complexity of Our Task

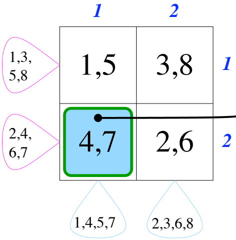


$$\begin{array}{r} 4 = 0100 \\ 7 = 0111 \\ \hline 0011 \end{array} \oplus \qquad 0011 \perp 0011$$

$\big((\mathbf{2},\mathbf{2}),\mathbf{1010}\big)$ is a valid answer
$\big((\mathbf{2},\mathbf{2}),\mathbf{0001}\big)$ is another valid answer
$\big((\mathbf{2},\mathbf{1}),\mathbf{0011}\big)$ is valid too

- It can be solved by a *SMP protocol of cost $O(\log n)$ with classical communication and shared entanglement*.

Communication Complexity of Our Task



$$\begin{array}{r} 4 = 0100 \\ 7 = \underline{0111} \end{array} \oplus$$
$$0011 \perp 0011$$

$\big((\mathbf{2},\mathbf{2}),\mathbf{1010}\big)$ is a valid answer
$\big((\mathbf{2},\mathbf{2}),\mathbf{0001}\big)$ is another valid answer
$\big((\mathbf{2},\mathbf{1}),\mathbf{0011}\big)$ is valid too

- It can be solved by a *SMP protocol of cost $O(\log n)$ with classical communication and shared entanglement.*
- It requires $\tilde{\Omega}\left(n^{1/4}\right)$ communication in the *classical multi-round model*. (Note that $n = \sqrt{[\textit{input size}]}$).

Efficient Protocol in SMP with Shared Entanglement

	1	*2*
1	1,5	3,8
2	4,7	2,6

$$|1,1\rangle + |2,2\rangle + |3,3\rangle + |4,4\rangle + |5,5\rangle + |6,6\rangle + |7,7\rangle + |8,8\rangle$$

- Alice and Bob share the state $\sum_{t\in[2n^2]} |t,t\rangle$.

Efficient Protocol in SMP with Shared Entanglement

	1	*2*
1	1,5	3,8
2	4,7	2,6

$|2,2\rangle + |4,4\rangle + |6,6\rangle + |7,7\rangle$

- Alice and Bob share the state $\sum_{t\in[2n^2]} |t,t\rangle$.
- Alice projects her part of the shared state to the subspace spanned by the elements of one of the rows.

Efficient Protocol in SMP with Shared Entanglement

1	*2*	
1,5	3,8	*1*
4,7	2,6	*2*

$|2,2\rangle + |6,6\rangle$

- Alice and Bob share the state $\sum_{t \in [2n^2]} |t, t\rangle$.
- Alice projects her part of the shared state to the subspace spanned by the elements of one of the rows.
- Bob does the same for columns.

Efficient Protocol in SMP with Shared Entanglement

$$\begin{array}{cc|l} \mathit{1} & \mathit{2} & \\ \hline 1,5 & 3,8 & \mathit{1} \\ 4,7 & \boxed{2,6} & \mathit{2} \end{array} \qquad |2,2\rangle + |6,6\rangle$$

- Alice and Bob share the state $\sum_{t\in[2n^2]} |t,t\rangle$.
- Alice projects her part of the shared state to the subspace spanned by the elements of one of the rows.
- Bob does the same for columns.
- They end up with $|a,a\rangle + |b,b\rangle$, where $\{a,b\}$ is the content of a cell (i_0, j_0).

Efficient Protocol in SMP with Shared Entanglement

1	*2*	
1,5	3,8	*1*
4,7	2,6	*2*

$|2,2\rangle + |6,6\rangle$

- Alice and Bob share the state $\sum_{t\in[2n^2]} |t,t\rangle$.
- Alice projects her part of the shared state to the subspace spanned by the elements of one of the rows.
- Bob does the same for columns.
- They end up with $|a,a\rangle + |b,b\rangle$, where $\{a,b\}$ is the content of a cell (i_0, j_0).
- ▶ Both Alice and Bob locally *apply the Hadamard transform, measure the result in the computational basis and send the outcome, together with* (i_0, j_0)*, to the referee*.

Efficient Protocol in SMP with Shared Entanglement

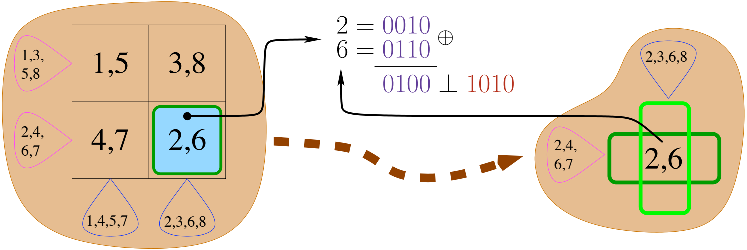
1	*2*	
1,5	3,8	*1*
4,7	$\boxed{2,6}$	*2*

$|2,2\rangle + |6,6\rangle$

- Alice and Bob share the state $\sum_{t\in[2n^2]} |t,t\rangle$.
- Alice projects her part of the shared state to the subspace spanned by the elements of one of the rows.
- Bob does the same for columns.
- They end up with $|a,a\rangle + |b,b\rangle$, where $\{a,b\}$ is the content of a cell (i_0, j_0).
- Both Alice and Bob locally *apply the Hadamard transform, measure the result in the computational basis and send the outcome, together with* (i_0, j_0)*, to the referee*.

▶ That information is *sufficient to produce a correct answer*.

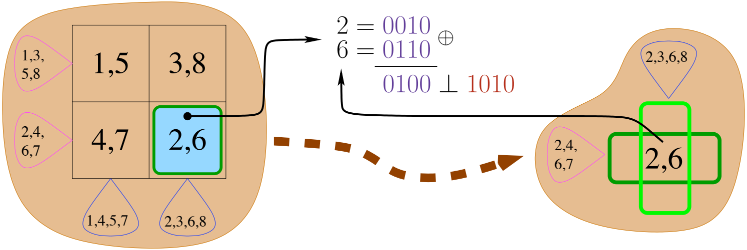
Classical Solution is Expensive: The First Reduction



Claim

Assume that a protocol of cost k solves the original problem with small error. Then another protocol of similar cost solves the 1×1-version with probability $\frac{1}{n}$ with small error.

Classical Solution is Expensive: The First Reduction

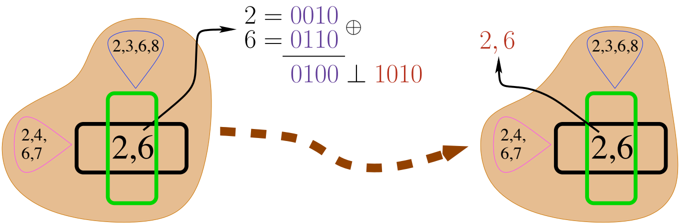


Claim

Assume that a protocol of cost k solves the original problem with small error. Then another protocol of similar cost solves the 1×1-version with probability $\frac{1}{n}$ with small error.

The proof is not "completely trivial".

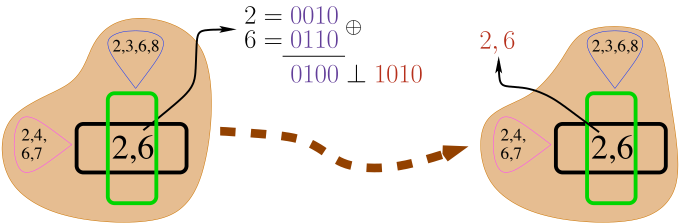
Classical Solution is Expensive: The Second Reduction



Claim

Assume that a protocol of cost k solves the 1x1-version of the problem with probability $\frac{1}{n}$ with small error. Then another protocol of similar cost solves the search 1x1-version of the problem with probability $\frac{1}{nk^2 \log^2(n)}$.

Classical Solution is Expensive: The Second Reduction

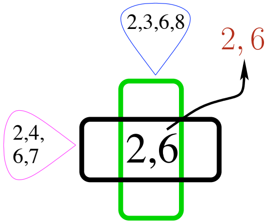


Claim

Assume that a protocol of cost k solves the 1x1-version of the problem with probability $\frac{1}{n}$ with small error. Then another protocol of similar cost solves the search 1x1-version of the problem with probability $\frac{1}{nk^2 \log^2(n)}$.

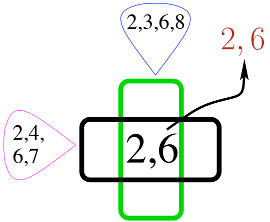
The proof is combinatorial, technical.

Complexity of the Search 1x1-Version



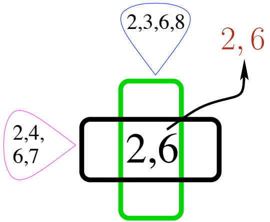
- To solve the problem with constant probability, we need $\Omega(n)$ bits of communication.

Complexity of the Search 1x1-Version



- To solve the problem with constant probability, we need $\Omega(n)$ bits of communication.
- If we are allowed *only k bits of communication*, we can find *one element* of the intersection with probability $O\left(\frac{k}{n}\right)$;

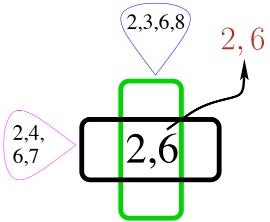
Complexity of the Search 1x1-Version



- To solve the problem with constant probability, we need $\Omega(n)$ bits of communication.
- If we are allowed *only k bits of communication*, we can find *one element* of the intersection with probability $O\left(\frac{k}{n}\right)$;

  our chances to find *both elements* are $O\left(\left(\frac{k}{n}\right)^2\right)$.

Complexity of the Search 1x1-Version



- To solve the problem with constant probability, we need $\Omega(n)$ bits of communication.
- If we are allowed *only k bits of communication*, we can find *one element* of the intersection with probability $O\left(\frac{k}{n}\right)$;

  our chances to find *both elements* are $O\left(\left(\frac{k}{n}\right)^2\right)$.

Another combinatorial proof.

Classical Solution is Expensive: Lower Bound Summary

- If a protocol of cost k solves the *original problem* with small error, then another protocol of similar cost solves the 1×1-*version* with probability $\frac{1}{n}$ with small error.

Classical Solution is Expensive: Lower Bound Summary

- If a protocol of cost k solves the *original problem* with small error, then another protocol of similar cost solves the 1×1-*version* with probability $\frac{1}{n}$ with small error.
- If a protocol of cost k solves the 1x1-version of the problem with probability $\frac{1}{n}$ with small error, then another protocol of similar cost solves the *search 1x1-version* of the problem with probability $\frac{1}{nk^2 \log^2(n)}$.

Classical Solution is Expensive: Lower Bound Summary

- If a protocol of cost k solves the *original problem* with small error, then another protocol of similar cost solves the 1×1-*version* with probability $\frac{1}{n}$ with small error.
- If a protocol of cost k solves the $1x1$-version of the problem with probability $\frac{1}{n}$ with small error, then another protocol of similar cost solves the *search* $1x1$-*version* of the problem with probability $\frac{1}{nk^2 \log^2(n)}$.
- The chances of a protocol of cost k to solve the search $1x1$-version are $O\left(\left(\frac{k}{n}\right)^2\right)$.

Classical Solution is Expensive: Lower Bound Summary

- If a protocol of cost k solves the *original problem* with small error, then another protocol of similar cost solves the 1×1-*version* with probability $\frac{1}{n}$ with small error.
- If a protocol of cost k solves the $1x1$-version of the problem with probability $\frac{1}{n}$ with small error, then another protocol of similar cost solves the *search* $1x1$-*version* of the problem with probability $\frac{1}{nk^2 \log^2(n)}$.
- The chances of a protocol of cost k to solve the search $1x1$-version are $O\left(\left(\frac{k}{n}\right)^2\right)$.

▶ This gives us the required $k \in \tilde{\Omega}\left(n^{1/4}\right)$.

Open Problems

Open Problems

- Is it possible to find a *functional* problem that requires exponentially more expensive protocol in $\mathcal{R}$ than in $\mathcal{Q}^1$?

Open Problems

- Is it possible to find a *functional* problem that requires exponentially more expensive protocol in $\mathcal{R}$ than in $\mathcal{Q}^1$?

  N.B. The question is open both for *complete* and for *partial* functions.

Open Problems

- Is it possible to find a *functional* problem that requires exponentially more expensive protocol in $\mathcal{R}$ than in $\mathcal{Q}^{1}$?

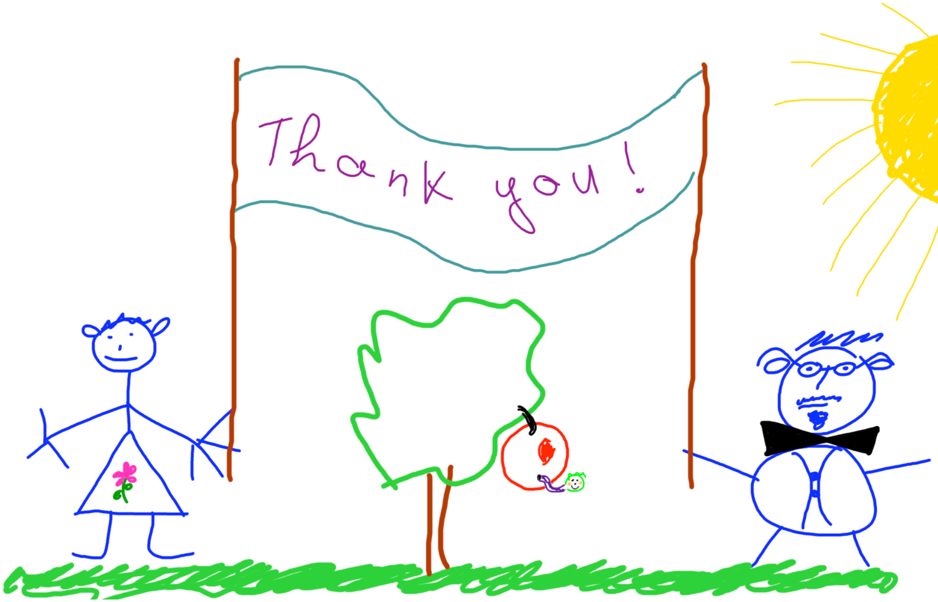
  N.B. The question is open both for *complete* and for *partial* functions.

- Can *SMP with quantum communication but without entanglement* be (exponentially) stronger than classical interactive protocols?

Open Problems

- Is it possible to find a *functional* problem that requires exponentially more expensive protocol in $\mathcal{R}$ than in $\mathcal{Q}^1$?

  N.B. The question is open both for *complete* and for *partial* functions.
- Can *SMP with quantum communication but without entanglement* be (exponentially) stronger than classical interactive protocols?
- Can shared entanglement have any advantages over *quantum* interactive (or even one-way) communication?


Thank you!