

Title: Classical interaction cannot replace a quantum message

Date: Mar 21, 2007 04:00 PM

URL: <http://pirsa.org/07030026>

Abstract: We give a communication problem between two players, Alice and Bob, that can be solved by Alice sending a quantum message to Bob, for which any classical interactive protocol requires exponentially more communication.

# Communication complexity: the multi-round model



## Multi-Round Communication:

- ▶ Alice receives  $x$  and Bob receives  $y$
- ▶ Alice sends a message to Bob
- ▶ Bob sends a message to Alice

...

# Communication complexity: the multi-round model

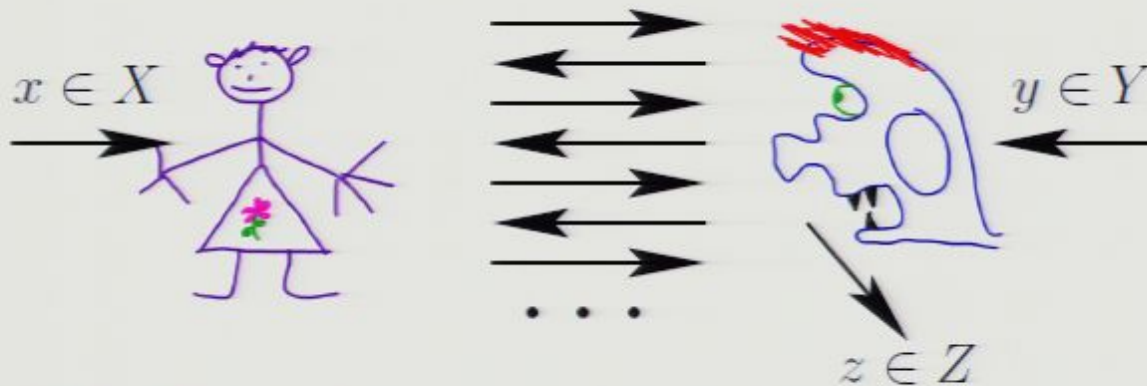


## Multi-Round Communication:

- ▶ Alice receives  $x$  and Bob receives  $y$
- ▶ Alice sends a message to Bob
- ▶ Bob sends a message to Alice

...

# Communication complexity: the multi-round model



## Multi-Round Communication:

- ▶ Alice receives  $x$  and Bob receives  $y$
- ▶ Alice sends a message to Bob
- ▶ Bob sends a message to Alice

...

# Communication complexity: the multi-round model



## 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

# Communication complexity: the multi-round model



## 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

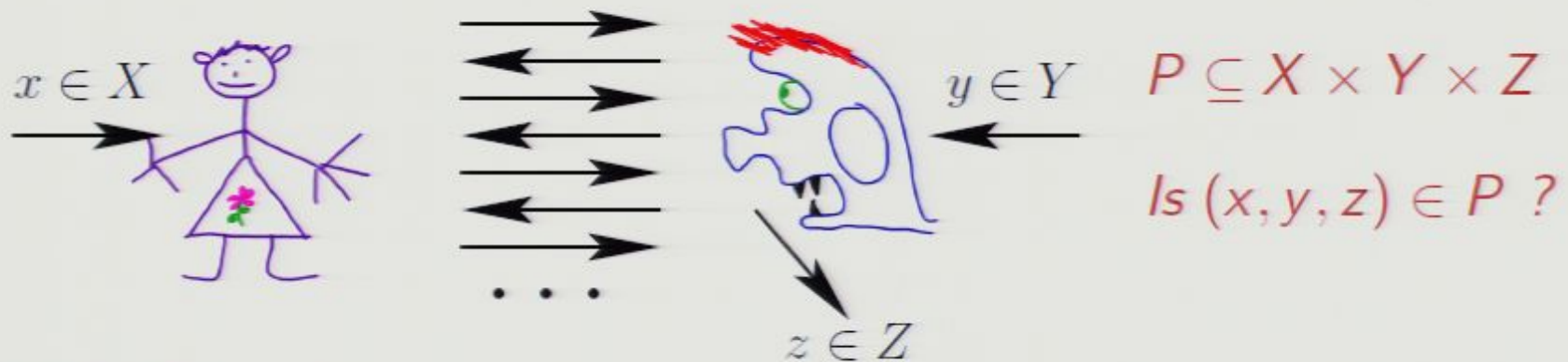
# Communication complexity: the multi-round model



## 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

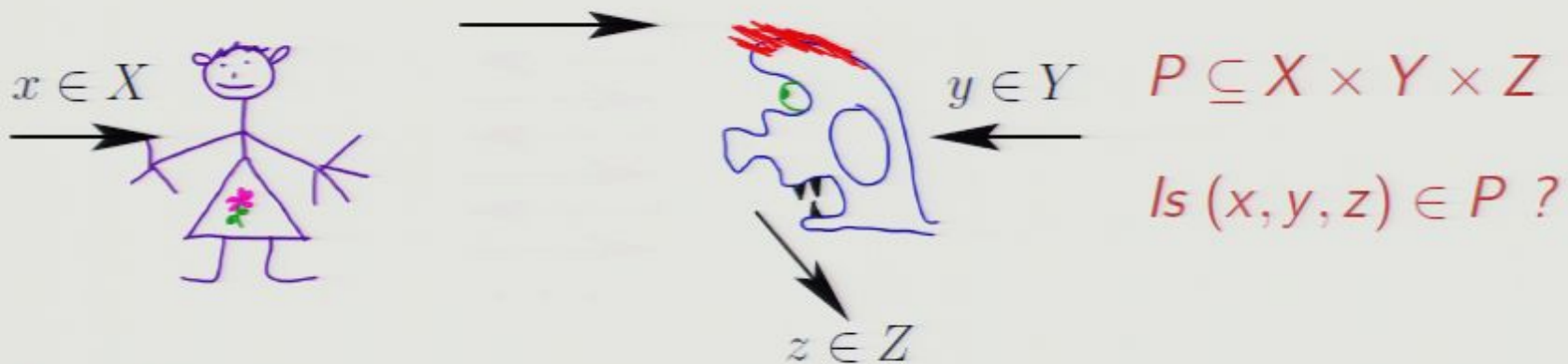
# Communication complexity: the multi-round model



## 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

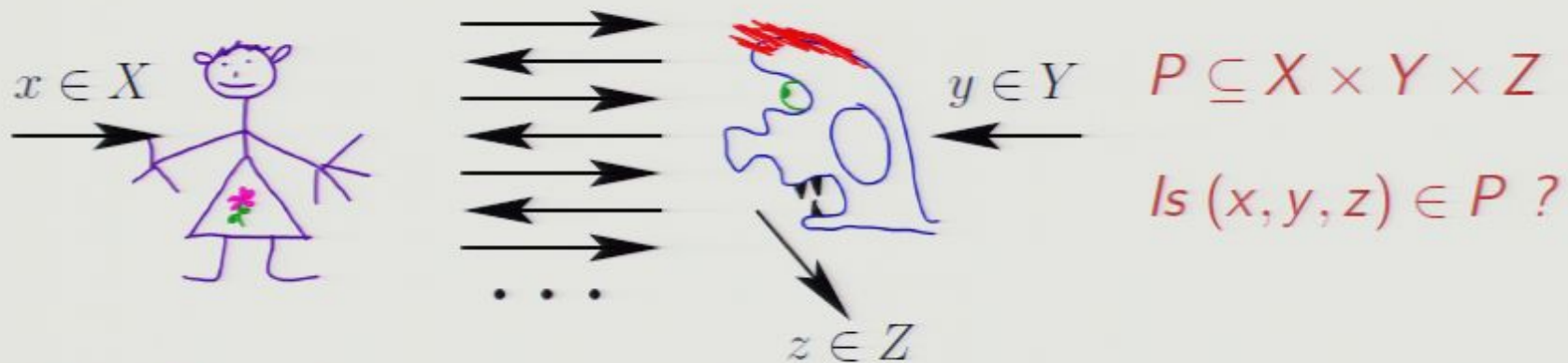
# Communication complexity: one-way communication



## One-Way Communication:

- ▶ Alice receives  $x$  and Bob receives  $y$
- ▶ Alice sends a message to Bob
- ▶ Bob sends a message to Alice
- ▶ ...
- ▶ Bob produces an answer

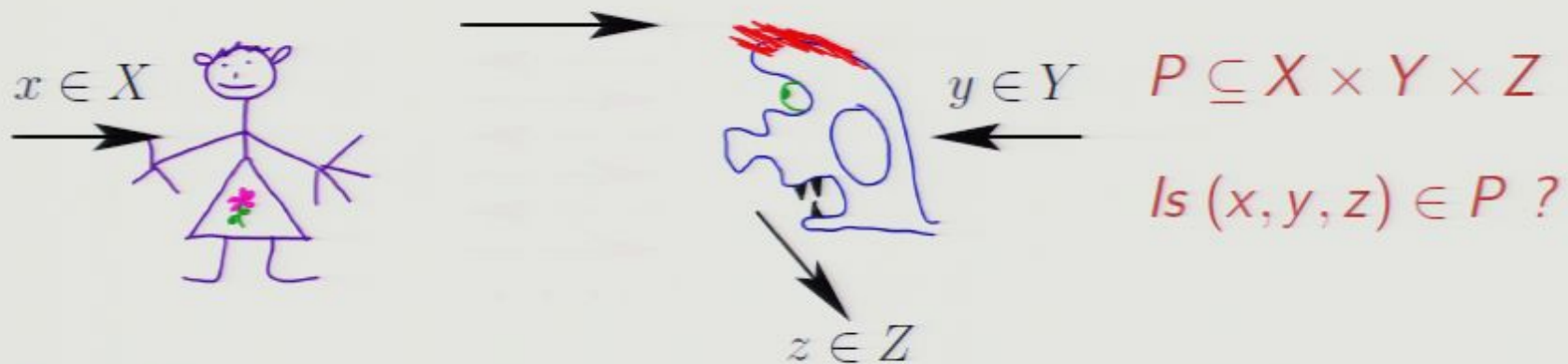
# Communication complexity: the multi-round model



## 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

# Communication complexity: one-way communication



## One-Way Communication:

- ▶ Alice receives  $x$  and Bob receives  $y$
- ▶ Alice sends a message to Bob
- ▶ Bob sends a message to Alice
- ...
- ▶ Bob produces an answer

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

$m_c \approx 170 \text{ GeV}$   $m_t = 170 \text{ GeV}$

$\frac{m_c^2 \lambda^2}{1} + \epsilon_c$   
 $0.04$



$p \rightarrow \pi^+ d\bar{d}$

$\frac{G_F^2 m_t^3}{(16\pi^2)}$

$m_c^2 \lambda^2$

$(0.2)^3 = 0.04$

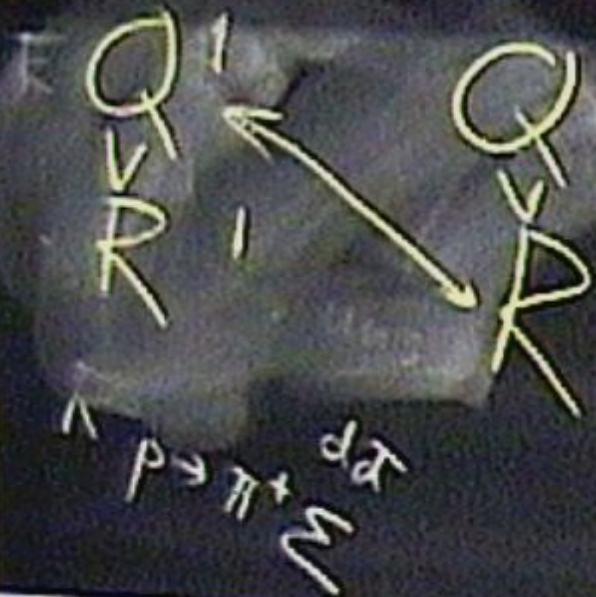


$\frac{(10^{-5} \text{ GeV})^2 (1 \text{ GeV})^3 (1 \text{ GeV})^2 (0.1)}{1000} \approx 10^{-5} \text{ GeV}$

$$\begin{array}{c|c|c|c} \lambda & 1 & \lambda & 1 \\ \hline 1 & 1 & 1 & 1 \end{array}$$

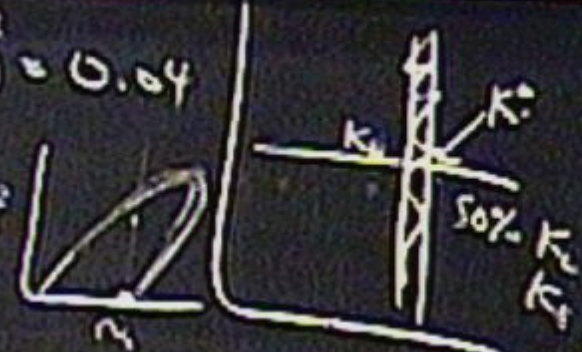
$$m_c \approx 170 \text{ GeV} \quad m_c / \Lambda \approx 0.04$$

$$\frac{m_c^2 \lambda^2}{1} + \epsilon_c \approx 0.04$$



$$\frac{g^2 m_c^3}{(16\pi^2)}$$

$$m_c^2 \lambda^2 \quad (0.2)^2 = 0.04$$



$$\frac{(10^{-5} \text{ GeV})^2 (1 \text{ GeV})^3 (1 \text{ GeV})^2 (0.1)}{1000} \approx 10^{-5} \text{ GeV}$$

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

## Our Communication Problem

<i>1</i>	<i>2</i>
1,5	3,8
4,7	2,6

- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem

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

- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem

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

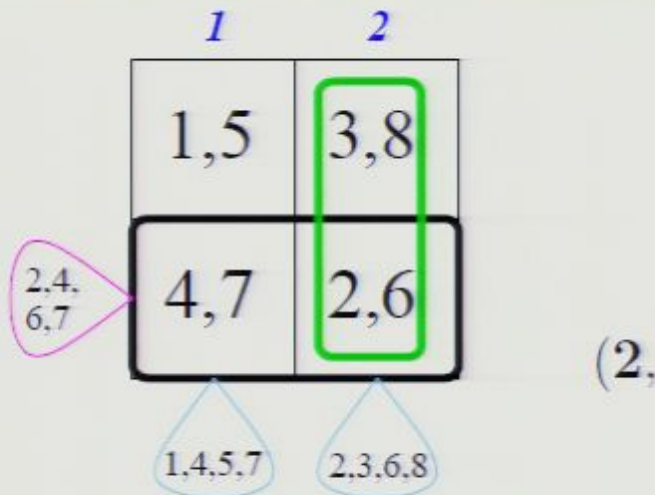
- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem

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

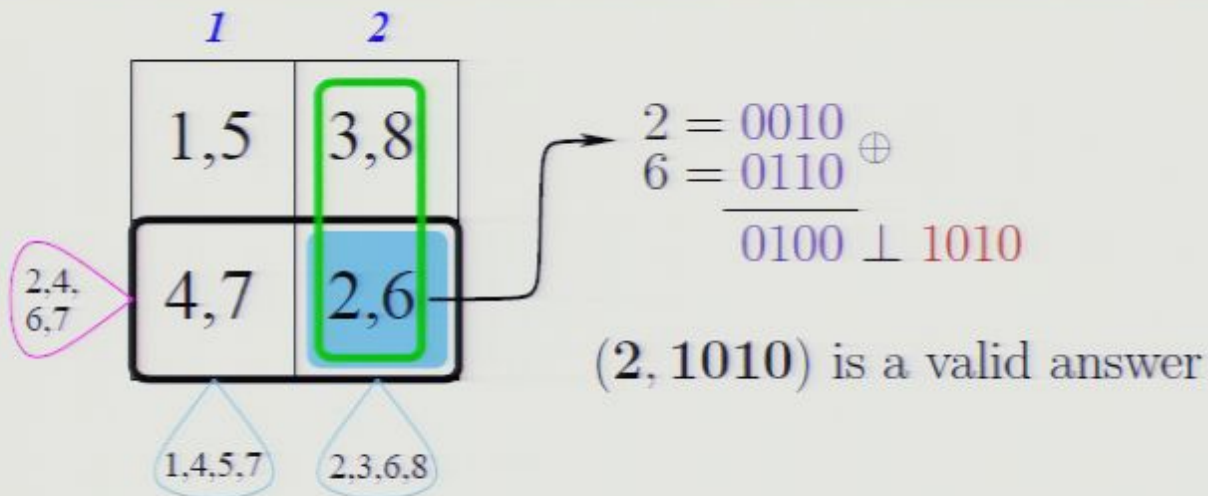
- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem



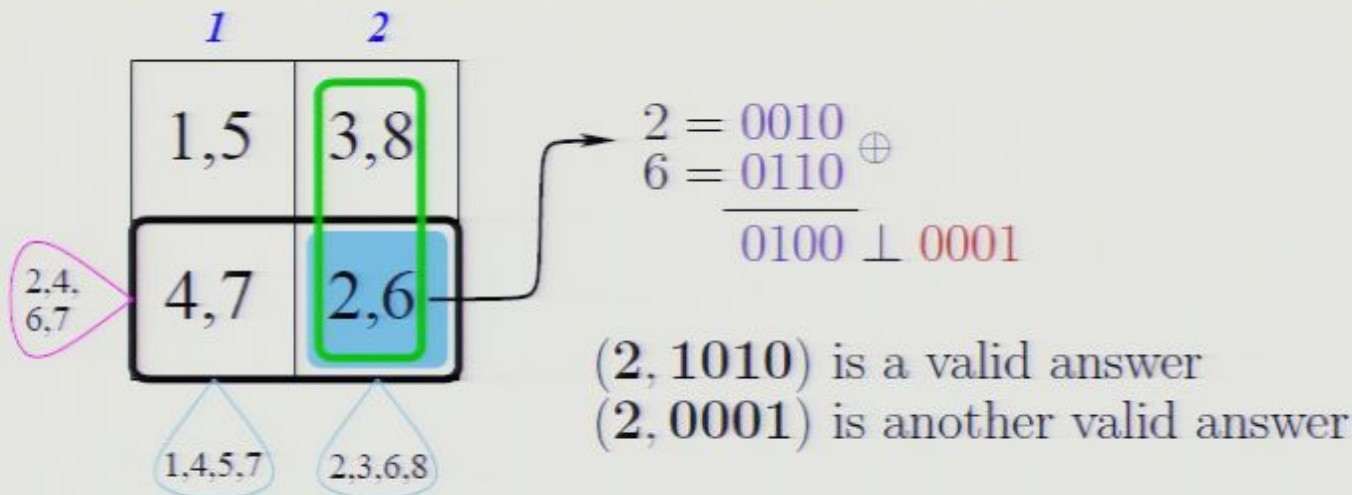
- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output **a column index**, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem



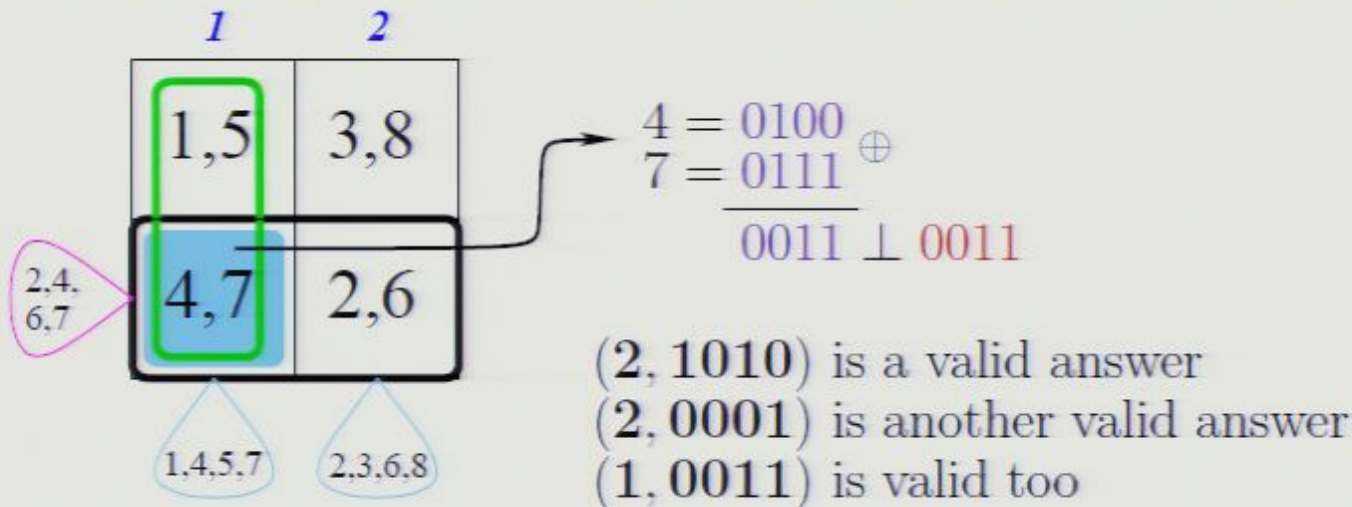
- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem



- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

## Our Communication Problem



- ▶ Integers  $1..2n^2$  are placed in an  $n \times n$  table, two numbers in every cell; the columns are indexed  $1..n$
- ▶ Alice's input consists of the elements of the last row
- ▶ Bob's input consists of the elements of each column
- ▶ Alice and Bob have to output a column index, and a number which is orthogonal to the bit-wise xor of the two elements in the corresponding cell of the last row

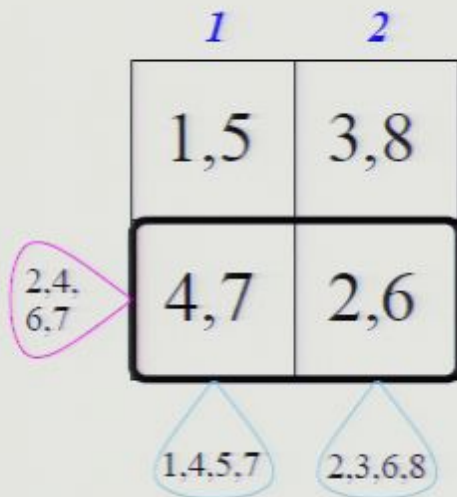
# Our Statement

- ▶ Our problem is solvable by a one-way quantum protocol of cost  $O(\log n)$
- ▶ The problem requires  $\tilde{\Omega}(n^{1/8})$  bits of communication in the classical multi-round model
- ▶ The gap is exponential

## Our Statement

- ▶ Our problem is solvable by a one-way quantum protocol of cost  $O(\log n)$
- ▶ The problem requires  $\tilde{\Omega}(n^{1/8})$  bits of communication in the classical multi-round model
- ▶ The gap is exponential

# Quantum One-Way Protocol



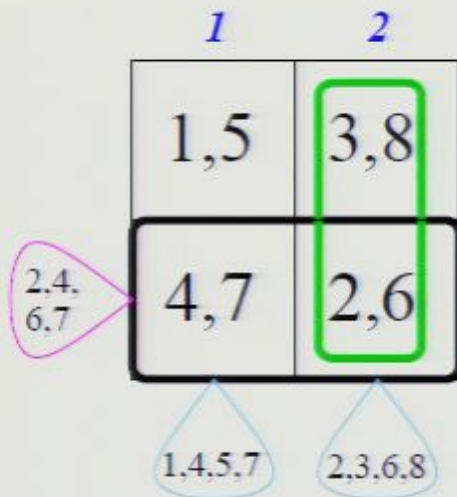
$$\blacktriangleright \frac{|2\rangle + |4\rangle + |6\rangle + |7\rangle}{2}$$

$$\blacktriangleright \frac{|2\rangle + |6\rangle}{\sqrt{2}} = \frac{|0010\rangle + |0110\rangle}{\sqrt{2}}$$

$$\frac{\sum_j |0100\rangle |j\rangle}{4}$$

- ▶ Alice sends to Bob the superposition of the indices in the last row
- ▶ Bob projects the state to the content of one of the columns, then applies the Hadamard transform and measures in the computational basis

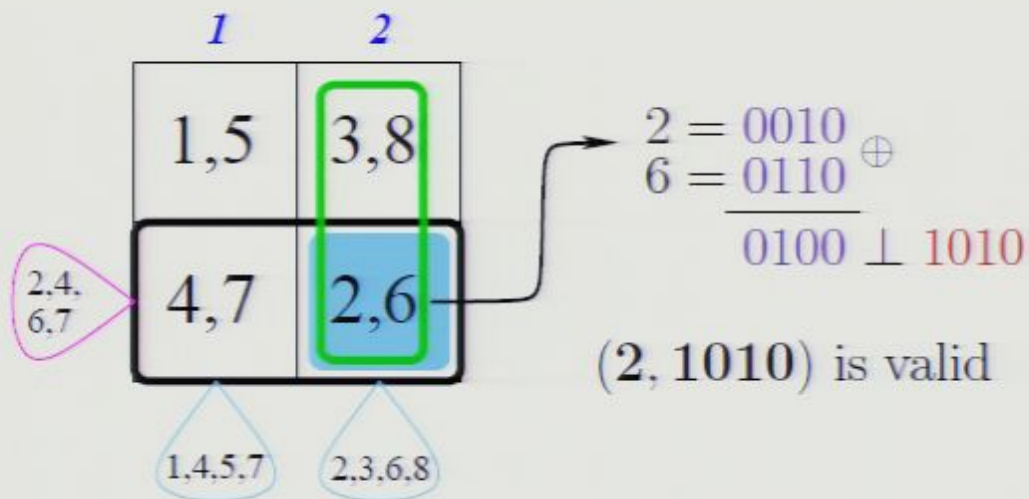
# Quantum One-Way Protocol



$$\begin{aligned} &\triangleright \frac{|2\rangle + |4\rangle + |6\rangle + |7\rangle}{2} \\ &\triangleright \frac{|2\rangle + |6\rangle}{\sqrt{2}} = \frac{|0010\rangle + |0110\rangle}{\sqrt{2}} \\ &\quad \frac{\sum_{j \perp 0100} |j\rangle}{4} \end{aligned}$$

- ▶ Alice sends to Bob the superposition of the indices in the last row
- ▶ Bob projects the state to the content of one of the columns, then applies the Hadamard transform and measures in the computational basis

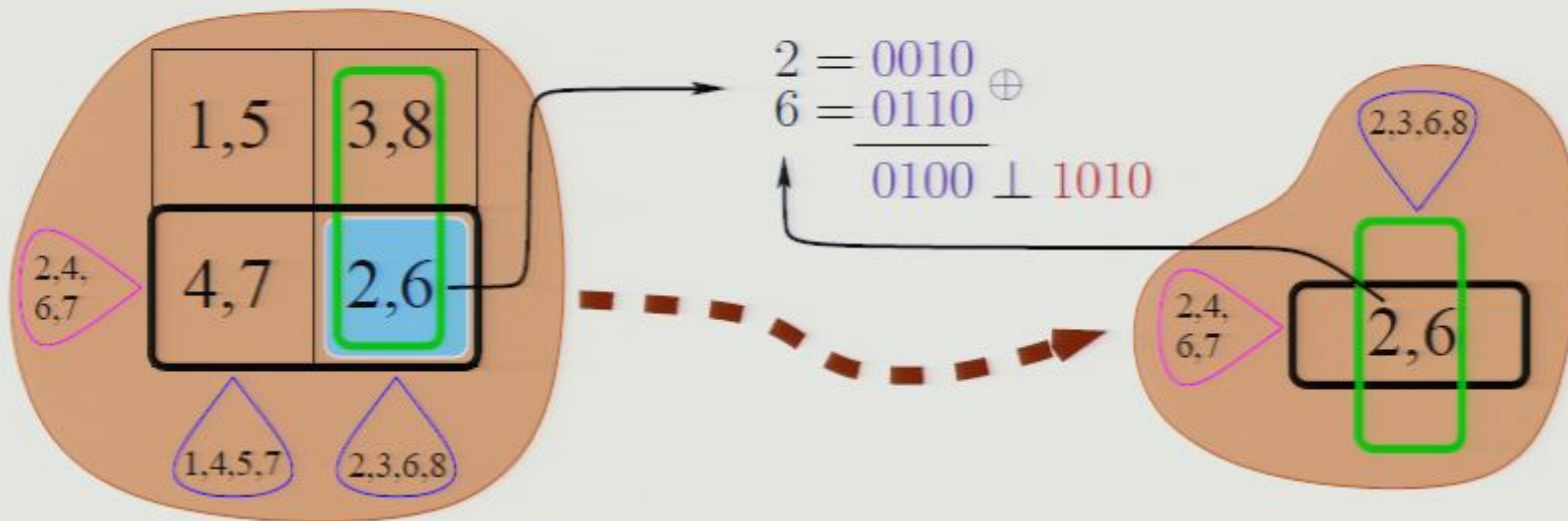
# Quantum One-Way Protocol



$$\begin{aligned} & \frac{|2\rangle + |4\rangle + |6\rangle + |7\rangle}{2} \\ & \frac{|2\rangle + |6\rangle}{\sqrt{2}} = \frac{|0010\rangle + |0110\rangle}{\sqrt{2}} \\ & \frac{\sum_{j \perp 0100} |j\rangle}{4} \end{aligned}$$

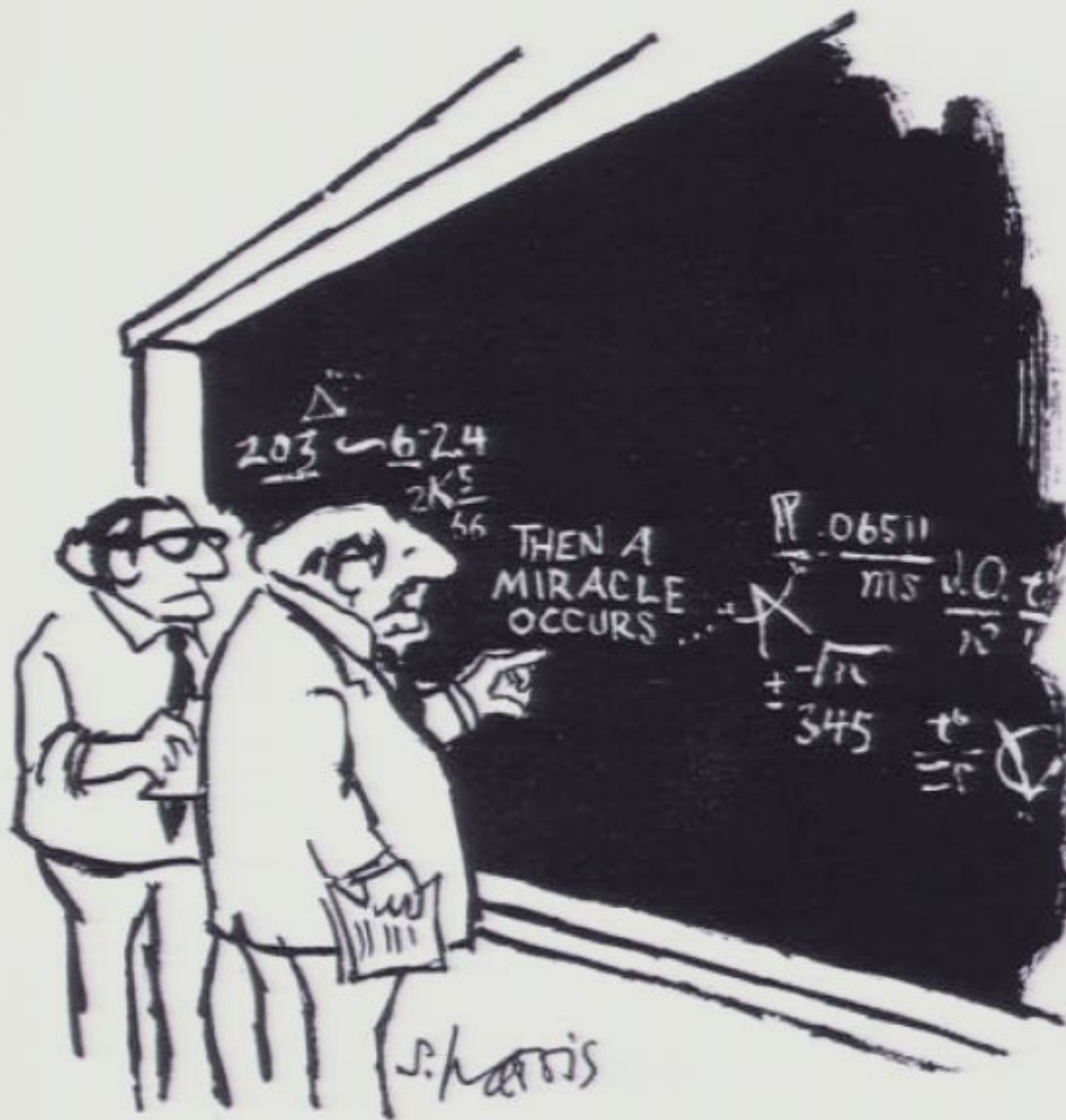
- ▶ Alice sends to Bob the superposition of the indices in the last row
- ▶ Bob projects the state to the content of one of the columns, then applies the Hadamard transform and measures in the computational basis

# Classical Solution is Expensive: The First Reduction

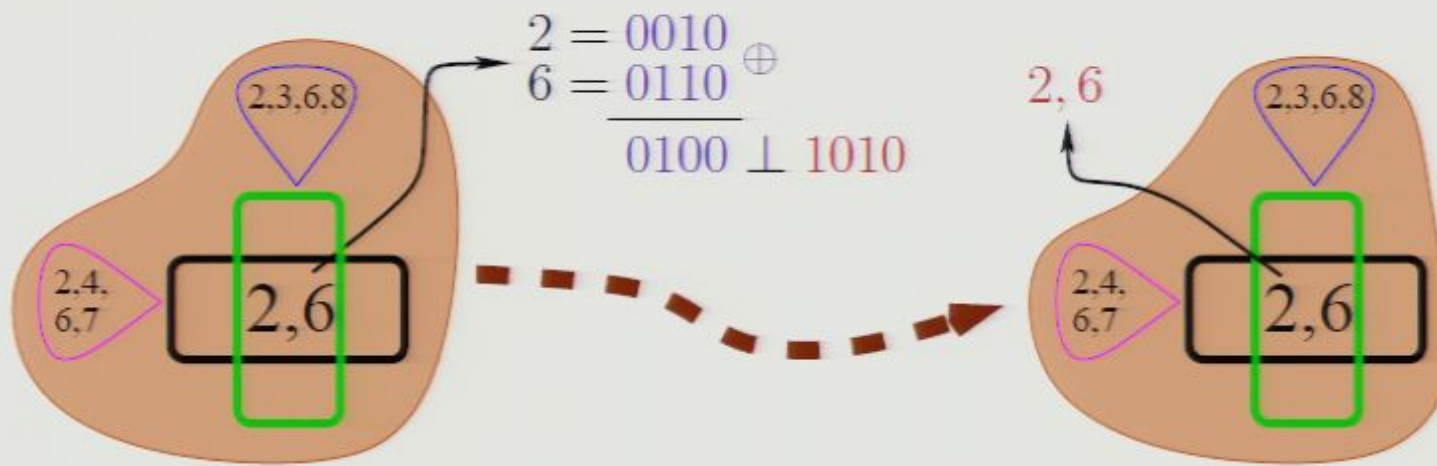


## Claim

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



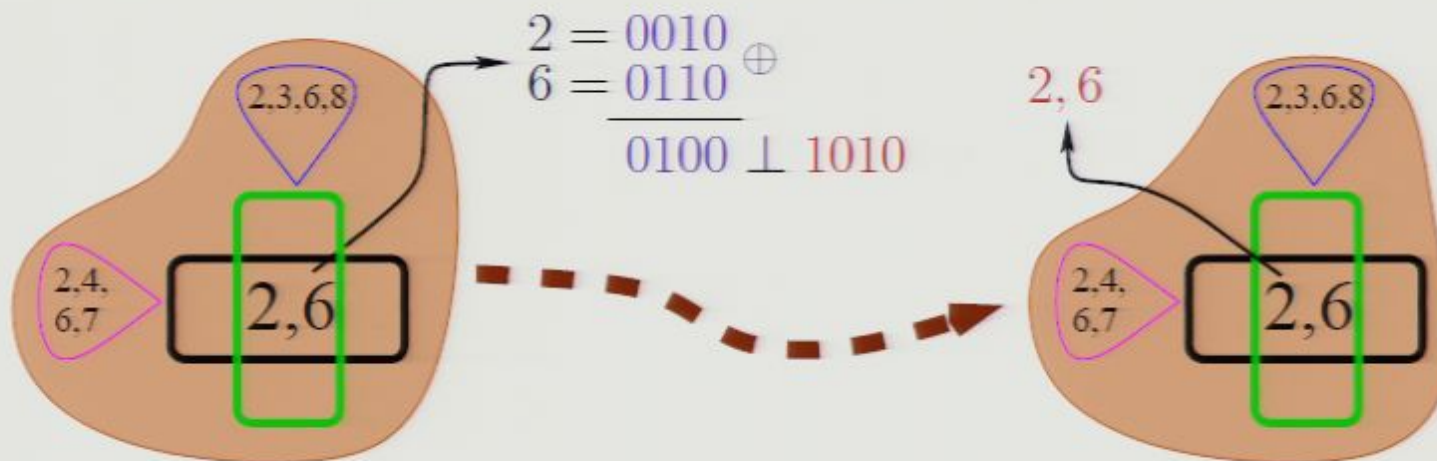
# Classical Solution is Expensive: The Second Reduction



## 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

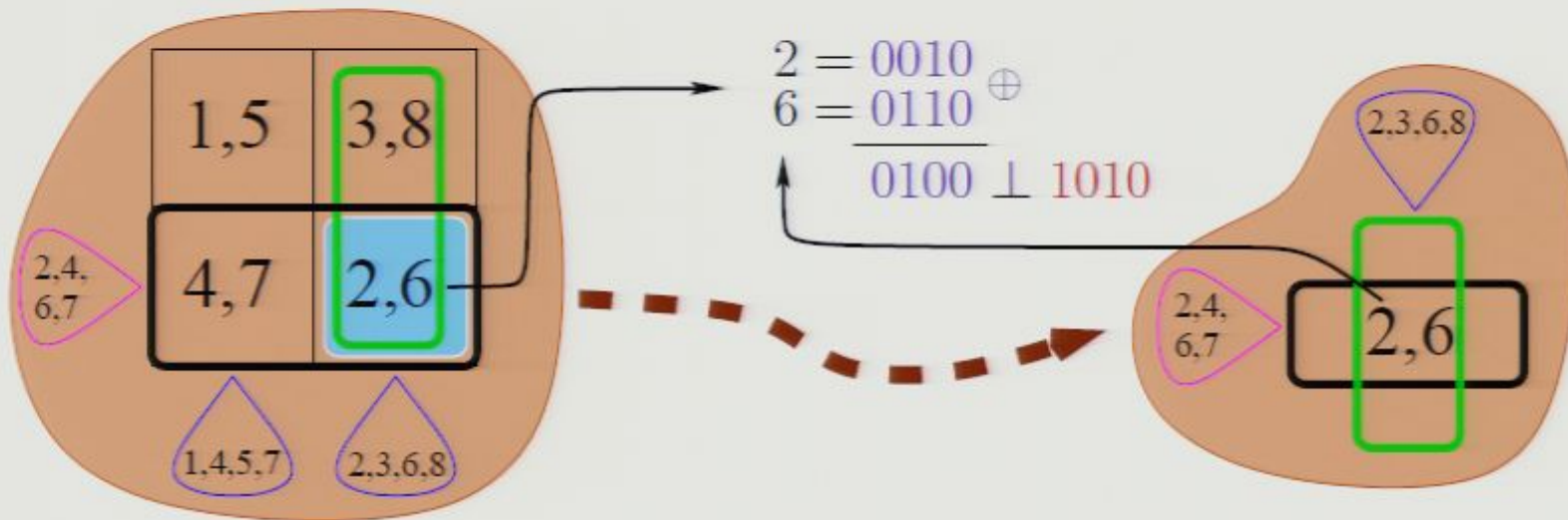


## Claim

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.

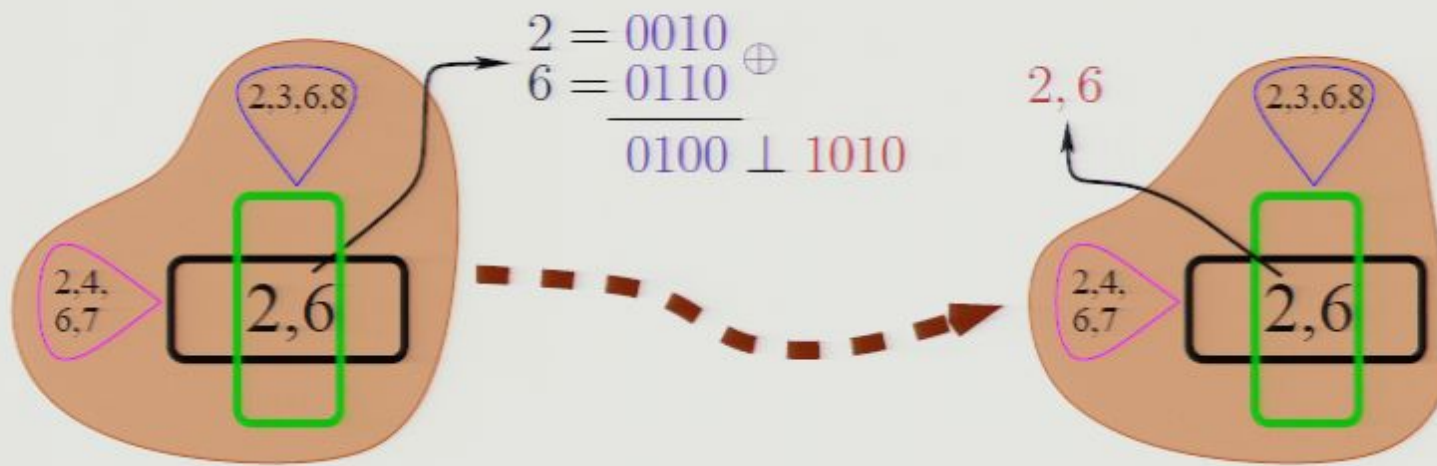
# Classical Solution is Expensive: The First Reduction



## Claim

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

# 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  $\frac{1}{nk^2 \log^2(n)}$ .

B-B t-quark because  $m_t^2$

$d, s, K$   $\Delta m \approx \frac{1}{2}$

$\rightarrow 0100$



$2$   
 $3$   
 $CF$   $ML$

B-B t-quark because  $m_t^2$

$\Delta m \approx \frac{1}{2}$



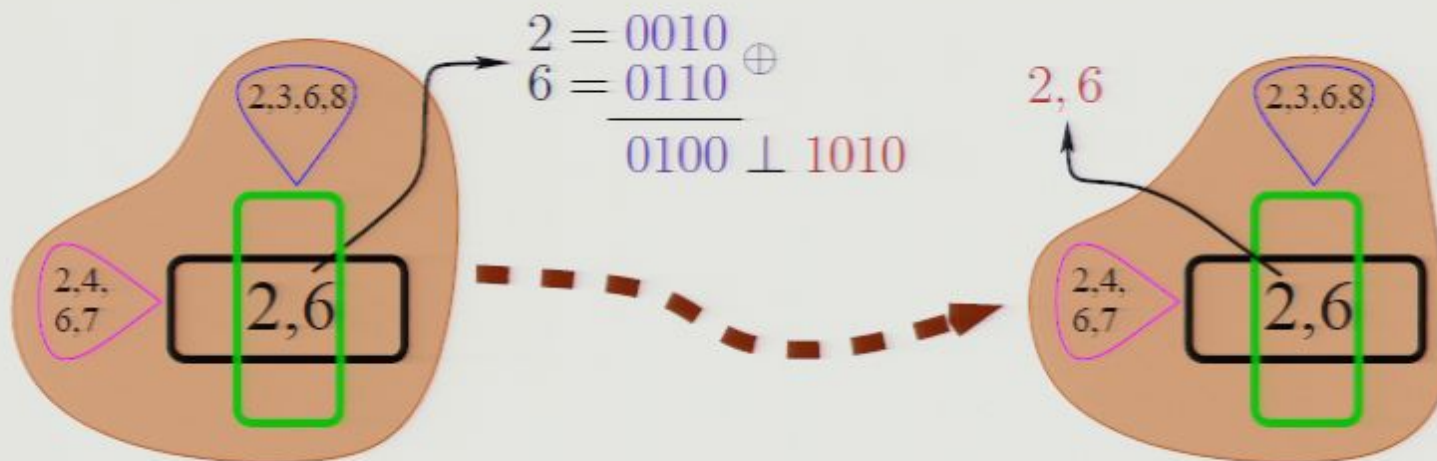
$\rightarrow 0100$

$\rightarrow (2, 7)$



$GF^2 ML^3$

# Classical Solution is Expensive: The Second Reduction

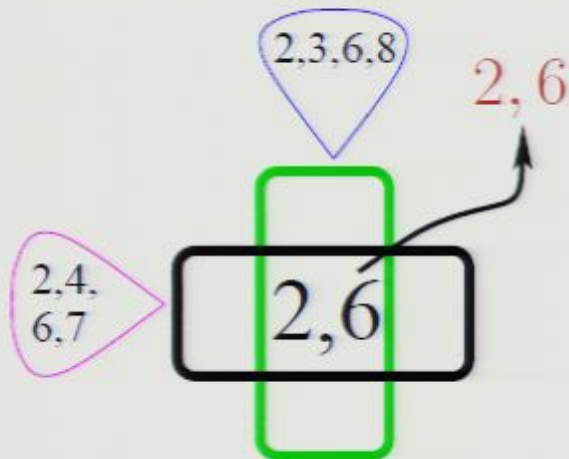


## Claim

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  $\frac{1}{nk^2 \log^2(n)}$ .

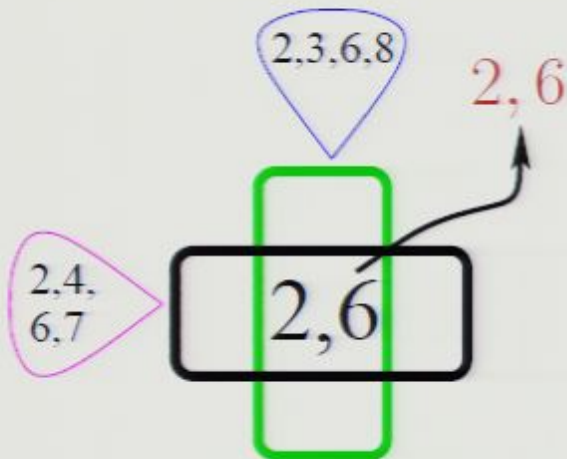
The proof is combinatorial, technical.

## Complexity of the Search 1x1-Version



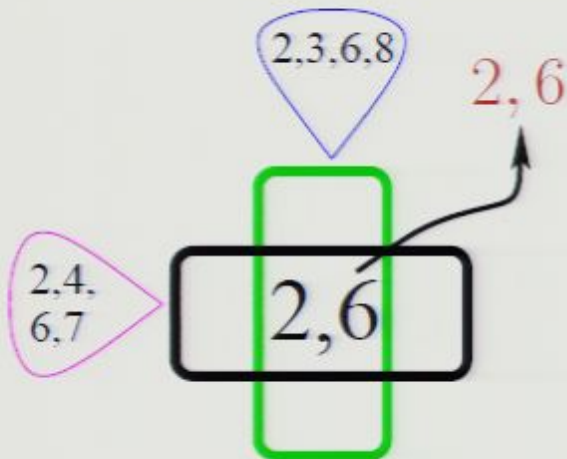
- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed only  $k$  bits of communication, we can find one element of the intersection with probability  $O\left(\frac{k}{n}\right)$ , our chances to find the both elements are  $O\left(\left(\frac{k}{n}\right)^2\right)$

## Complexity of the Search 1x1-Version



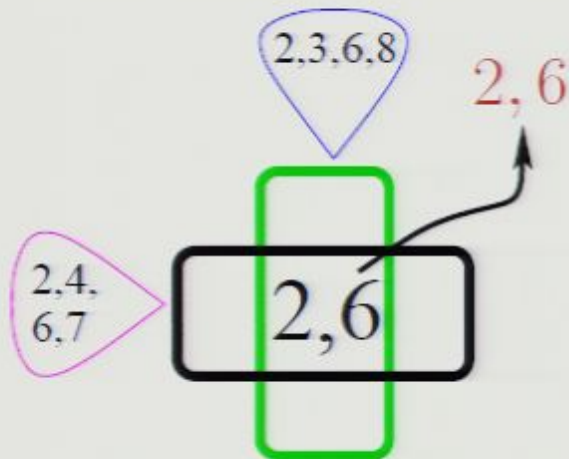
- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed only  $k$  bits of communication, we can find one element of the intersection with probability  $O\left(\frac{k}{n}\right)$ , our chances to find the both elements are  $O\left(\left(\frac{k}{n}\right)^2\right)$

## Complexity of the Search 1x1-Version

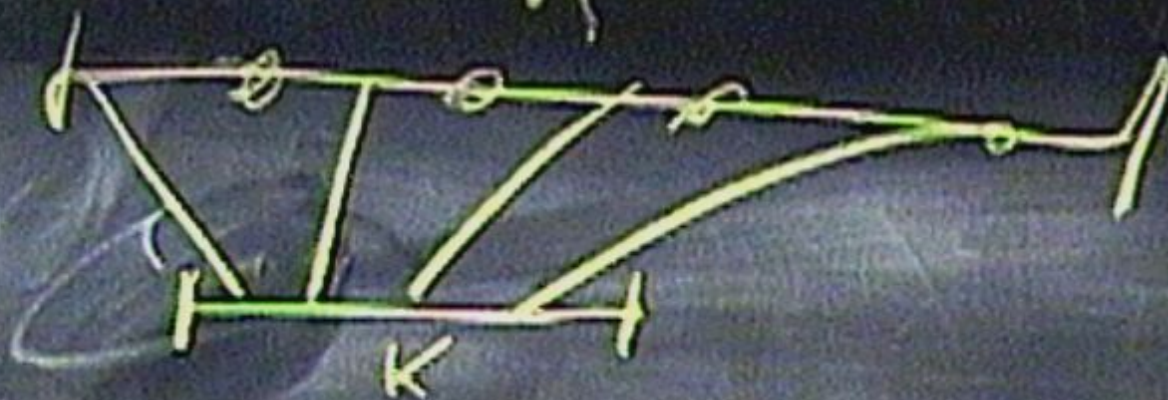


- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed **only  $k$  bits of communication**, we can find **one element** of the intersection with probability  $O\left(\frac{k}{n}\right)$ ,  
our chances to find the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$

## Complexity of the Search 1x1-Version



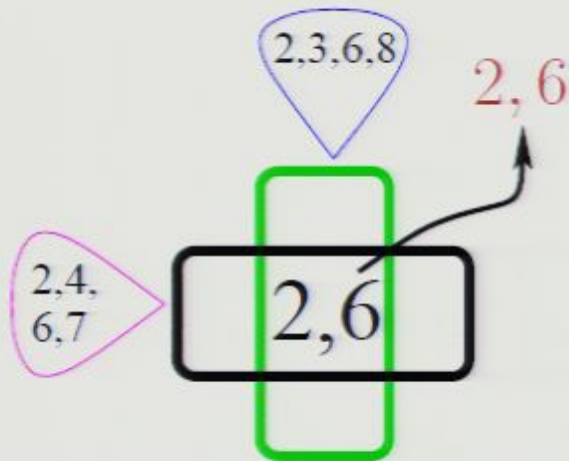
- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed **only  $k$  bits of communication**, we can find **one element** of the intersection with probability  $O\left(\frac{k}{n}\right)$ ,  
our chances to find the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$



$$(0.2)^2 = 0.04$$



## 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 the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$

Another combinatorial proof, uses a lemma by Razborov (1992)

## Lower Bound Summary

- ▶ If a protocol of cost  $k$  solves the **original problem** with small error then another protocol of similar cost solves the  **$1 \times 1$ -version** with probability  $\frac{1}{n}$  with small error
- ▶ If a protocol of cost  $k$  solves the  $1 \times 1$ -version of the problem with probability  $\frac{1}{n}$  with small error then another protocol of similar cost solves the **search  $1 \times 1$ -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  $1 \times 1$ -version are  $O\left(\left(\frac{k}{n}\right)^2\right)$
- ▶ This gives us the required  $k \in \tilde{\Omega}(n^{1/8})$

## Lower Bound Summary

- ▶ If a protocol of cost  $k$  solves the **original problem** with small error then another protocol of similar cost solves the  **$1 \times 1$ -version** with probability  $\frac{1}{n}$  with small error
- ▶ If a protocol of cost  $k$  solves the  $1 \times 1$ -version of the problem with probability  $\frac{1}{n}$  with small error then another protocol of similar cost solves the **search  $1 \times 1$ -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  $1 \times 1$ -version are  $O\left(\left(\frac{k}{n}\right)^2\right)$
- ▶ This gives us the required  $k \in \tilde{\Omega}(n^{1/3})$

## Lower Bound Summary

- ▶ If a protocol of cost  $k$  solves the **original problem** with small error then another protocol of similar cost solves the  **$1 \times 1$ -version** with probability  $\frac{1}{n}$  with small error
- ▶ If a protocol of cost  $k$  solves the  $1 \times 1$ -version of the problem with probability  $\frac{1}{n}$  with small error then another protocol of similar cost solves the **search  $1 \times 1$ -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  $1 \times 1$ -version are  $O\left(\left(\frac{k}{n}\right)^2\right)$
- ▶ This gives us the required  $k \in \tilde{\Omega}(n^{1/8})$

## Lower Bound Summary

- ▶ If a protocol of cost  $k$  solves the **original problem** with small error then another protocol of similar cost solves the  **$1 \times 1$ -version** with probability  $\frac{1}{n}$  with small error
- ▶ If a protocol of cost  $k$  solves the  $1 \times 1$ -version of the problem with probability  $\frac{1}{n}$  with small error then another protocol of similar cost solves the **search  $1 \times 1$ -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  $1 \times 1$ -version are  $O\left(\left(\frac{k}{n}\right)^2\right)$
- ▶ This gives us the required  $k \in \tilde{\Omega}(n^{1/8})$

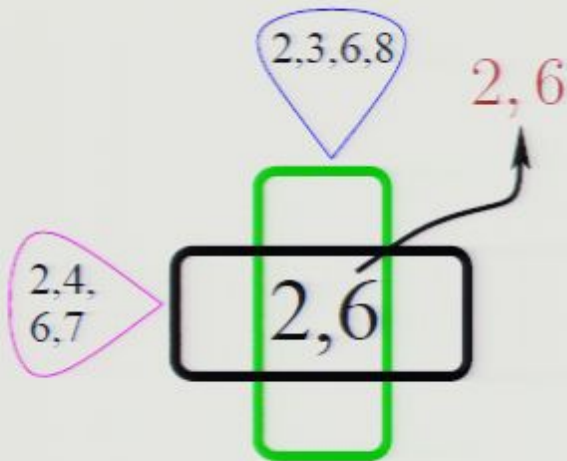
## Lower Bound Summary

- ▶ If a protocol of cost  $k$  solves the **original problem** with small error then another protocol of similar cost solves the  **$1 \times 1$ -version** with probability  $\frac{1}{n}$  with small error
- ▶ If a protocol of cost  $k$  solves the  $1 \times 1$ -version of the problem with probability  $\frac{1}{n}$  with small error then another protocol of similar cost solves the **search  $1 \times 1$ -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  $1 \times 1$ -version are  $O\left(\left(\frac{k}{n}\right)^2\right)$
- ▶ This gives us the required  $k \in \tilde{\Omega}(n^{1/8})$

## Open problems

- ▶ Is it possible to find a **functional** problem that requires exponentially more expensive protocol in  $R$  than in  $Q^1$ ?  
How about simultaneous protocols?
- ▶ Generally speaking, give a separation that would logically imply as many known results as possible.

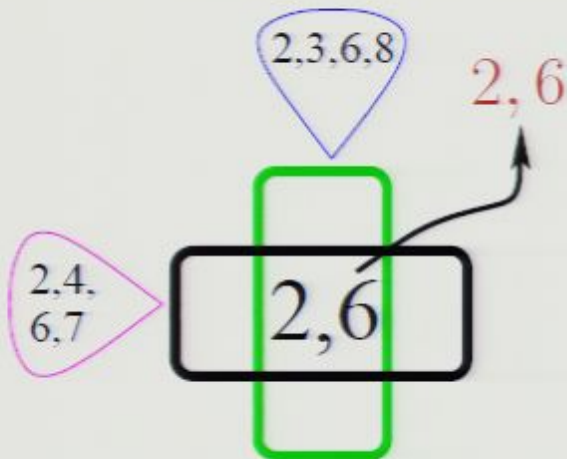
## Complexity of the Search 1x1-Version



- ▶ 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 the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$

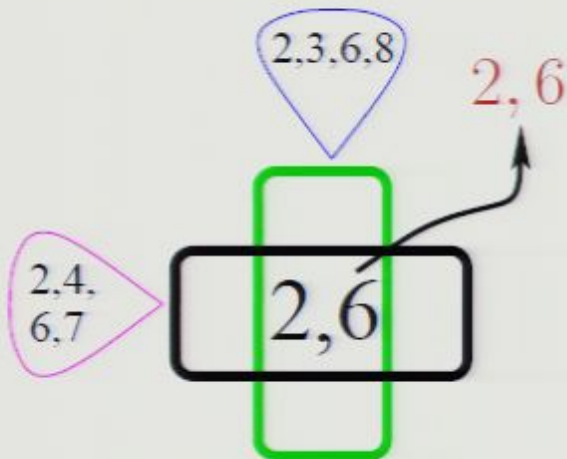
Another combinatorial proof, uses a lemma by Razborov (1992)

## Complexity of the Search 1x1-Version



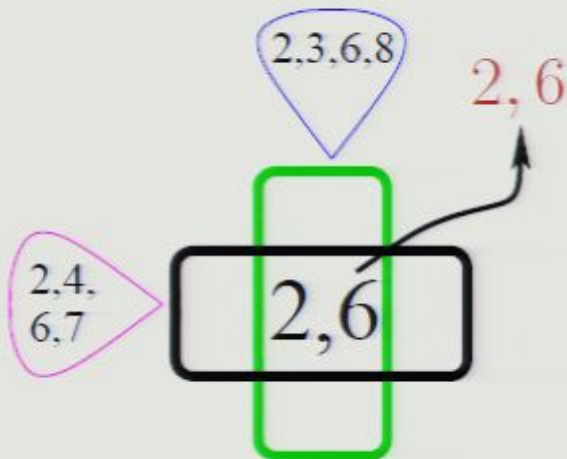
- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed **only  $k$  bits of communication**, we can find **one element** of the intersection with probability  $O\left(\frac{k}{n}\right)$ ,  
our chances to find the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$

## Complexity of the Search 1x1-Version

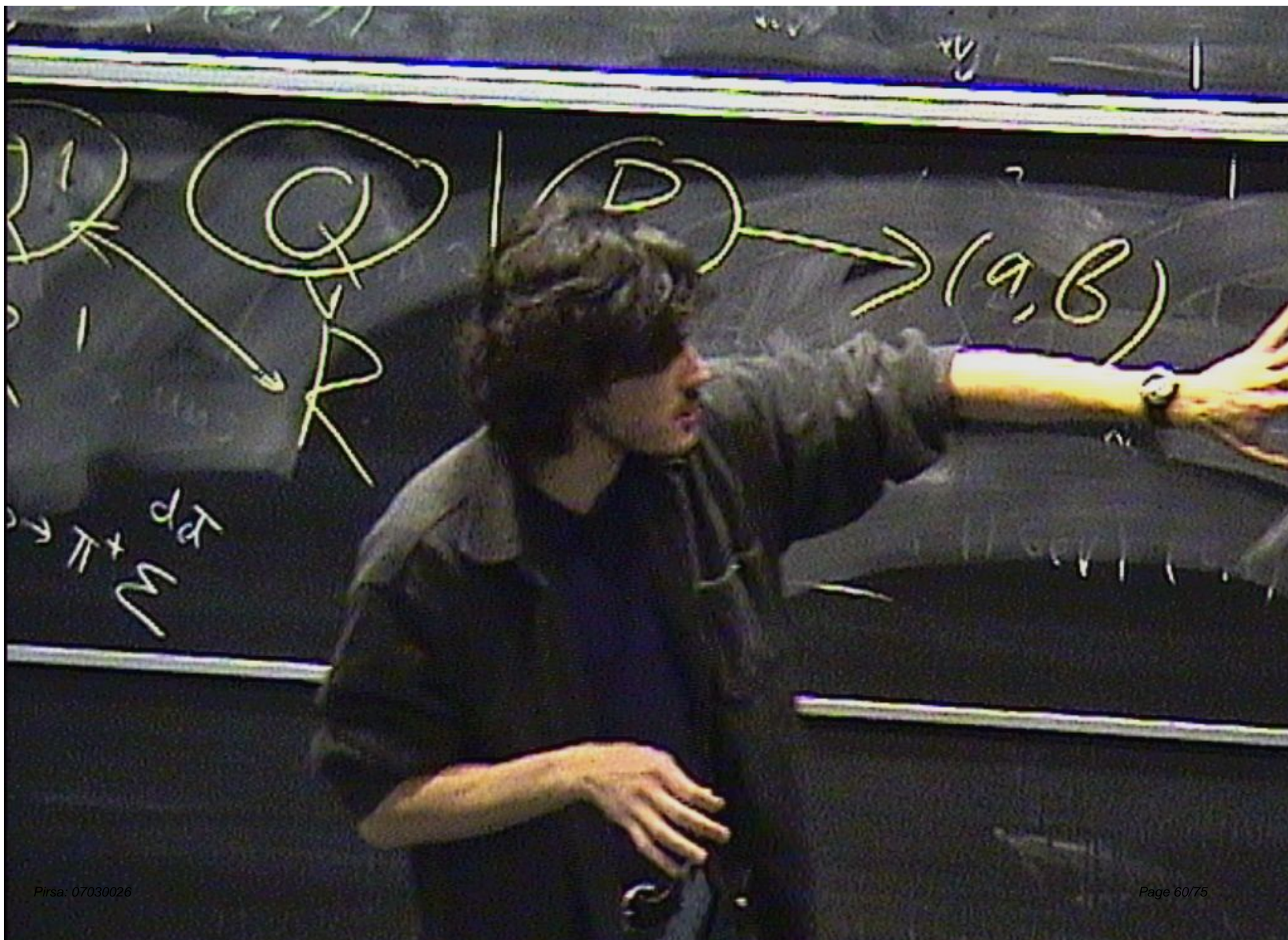


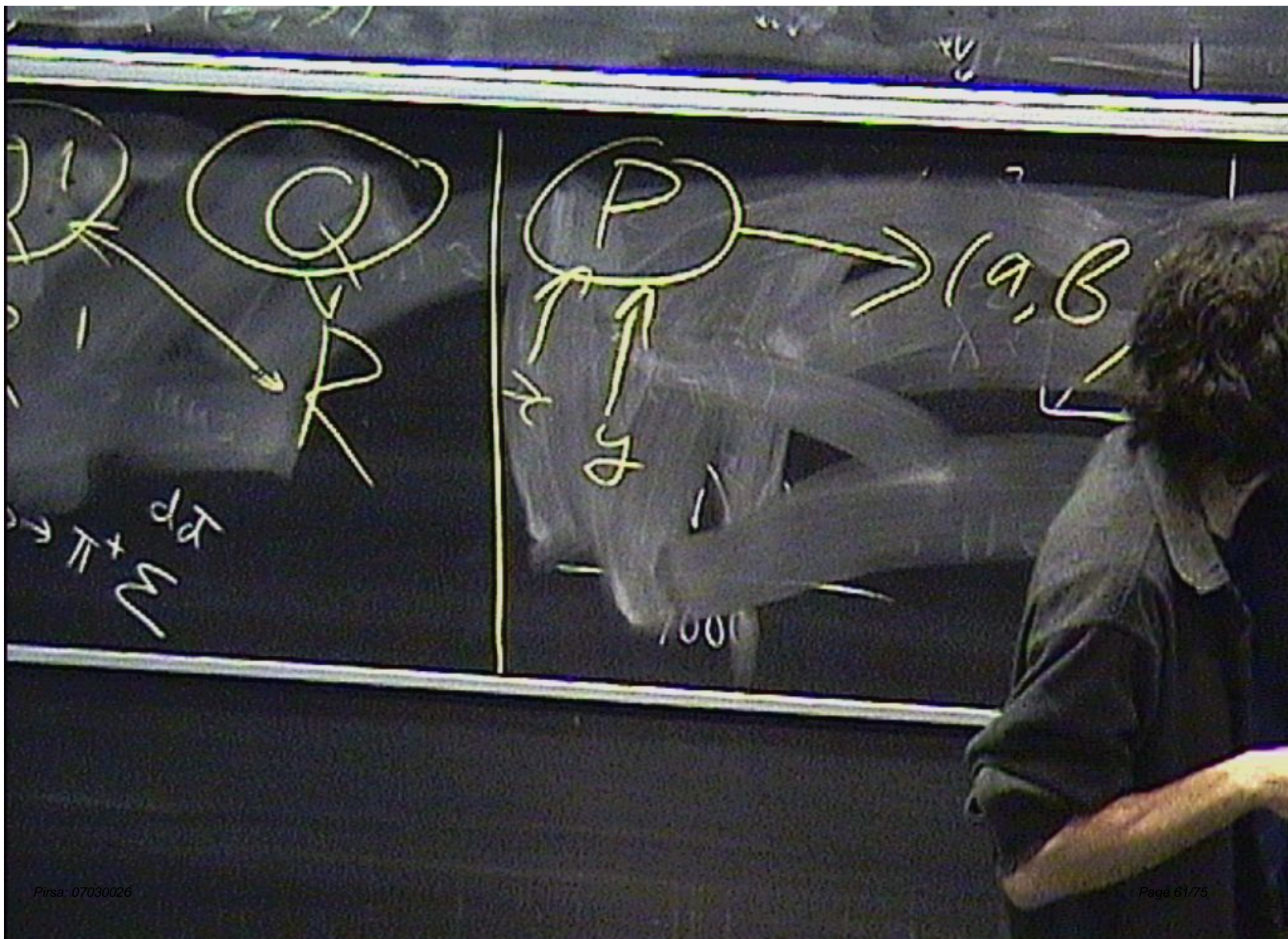
- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed **only  $k$  bits of communication**, we can find **one element** of the intersection with probability  $O\left(\frac{k}{n}\right)$ ,  
our chances to find the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$

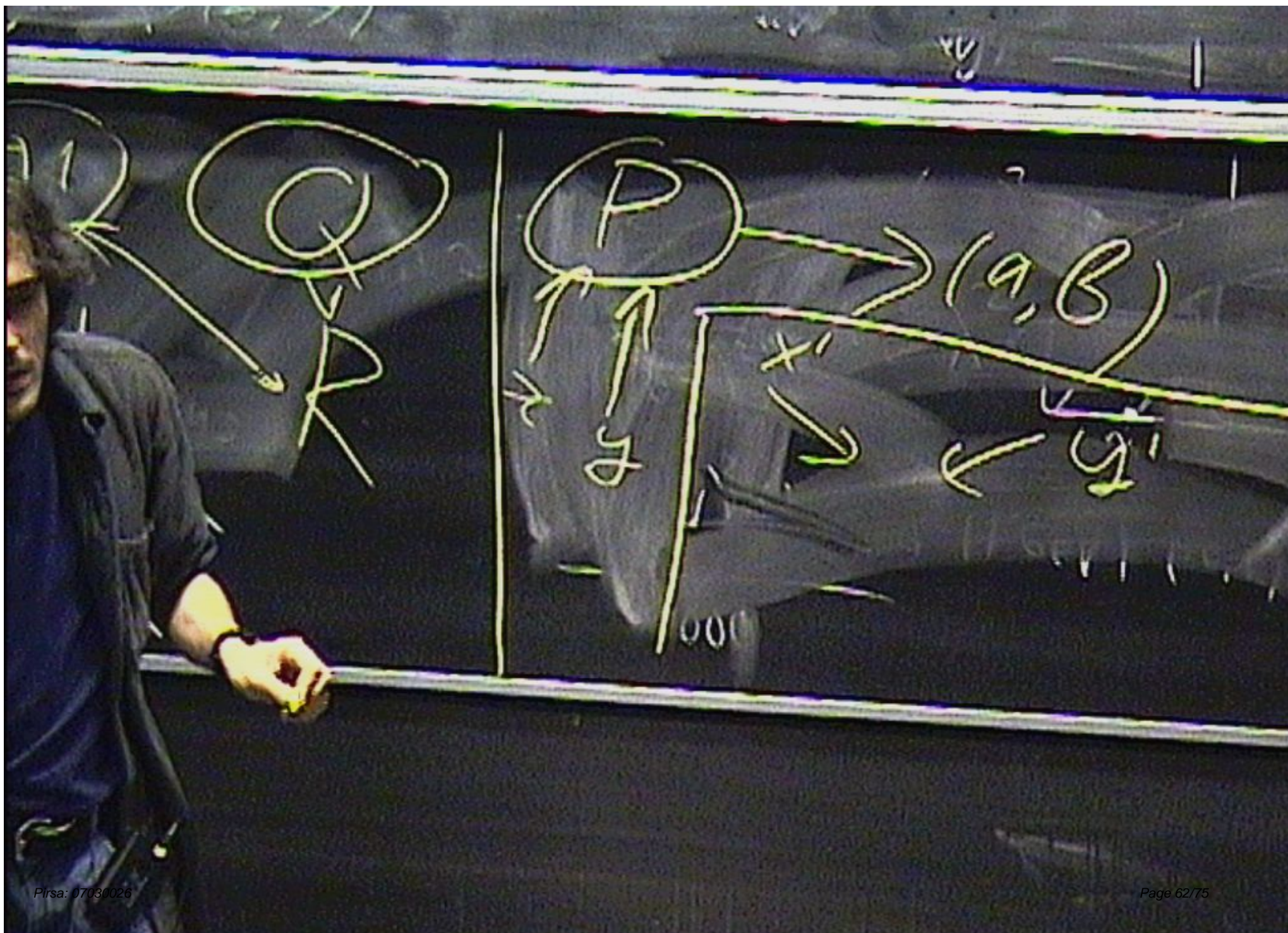
## Complexity of the Search 1x1-Version

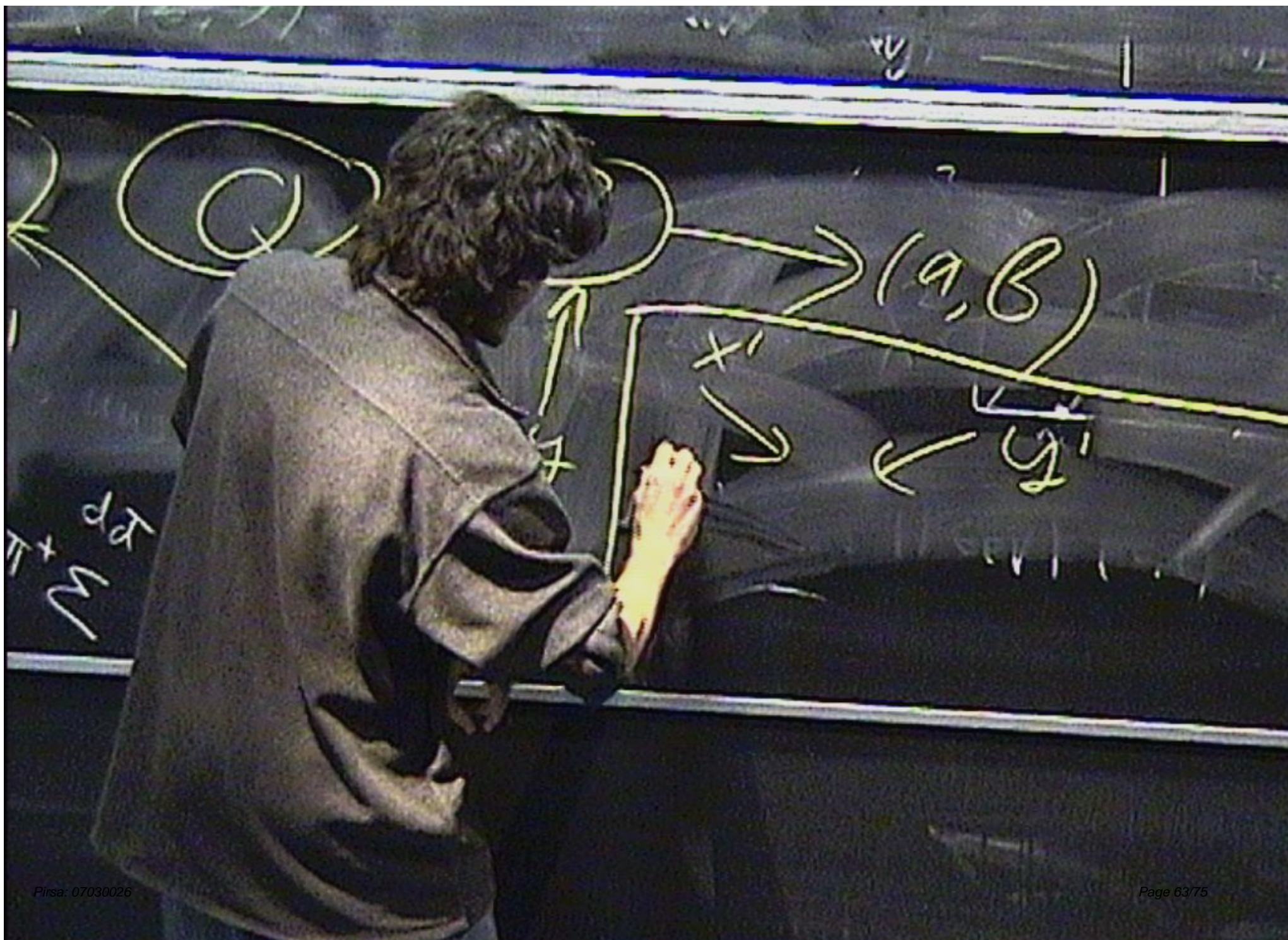


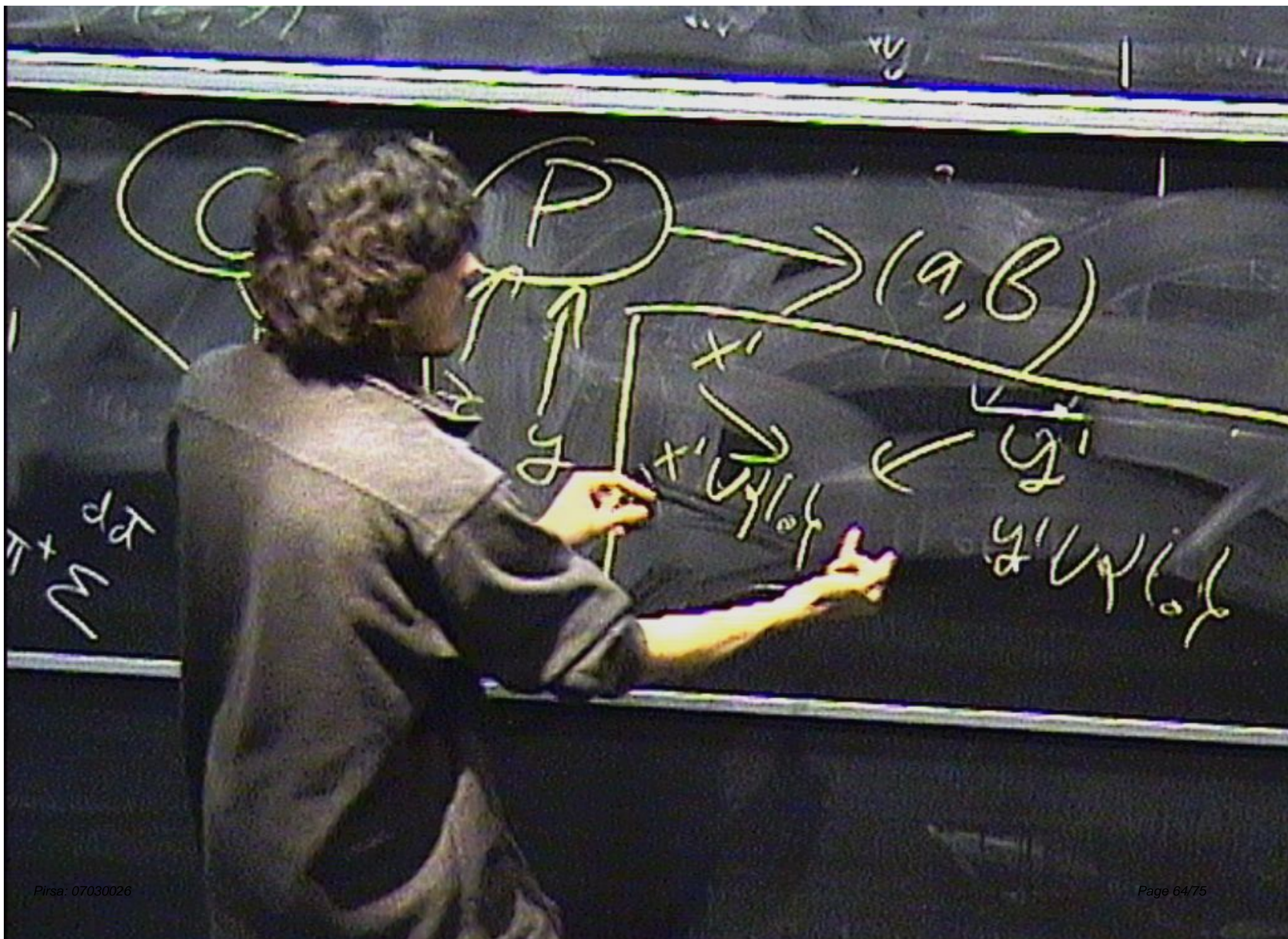
- ▶ To solve the problem with constant probability, we need  $\Omega(n)$  bits of communication
- ▶ If we are allowed **only  $k$  bits of communication**, we can find **one element** of the intersection with probability  $O\left(\frac{k}{n}\right)$ ,  
our chances to find the **both elements** are  $O\left(\left(\frac{k}{n}\right)^2\right)$

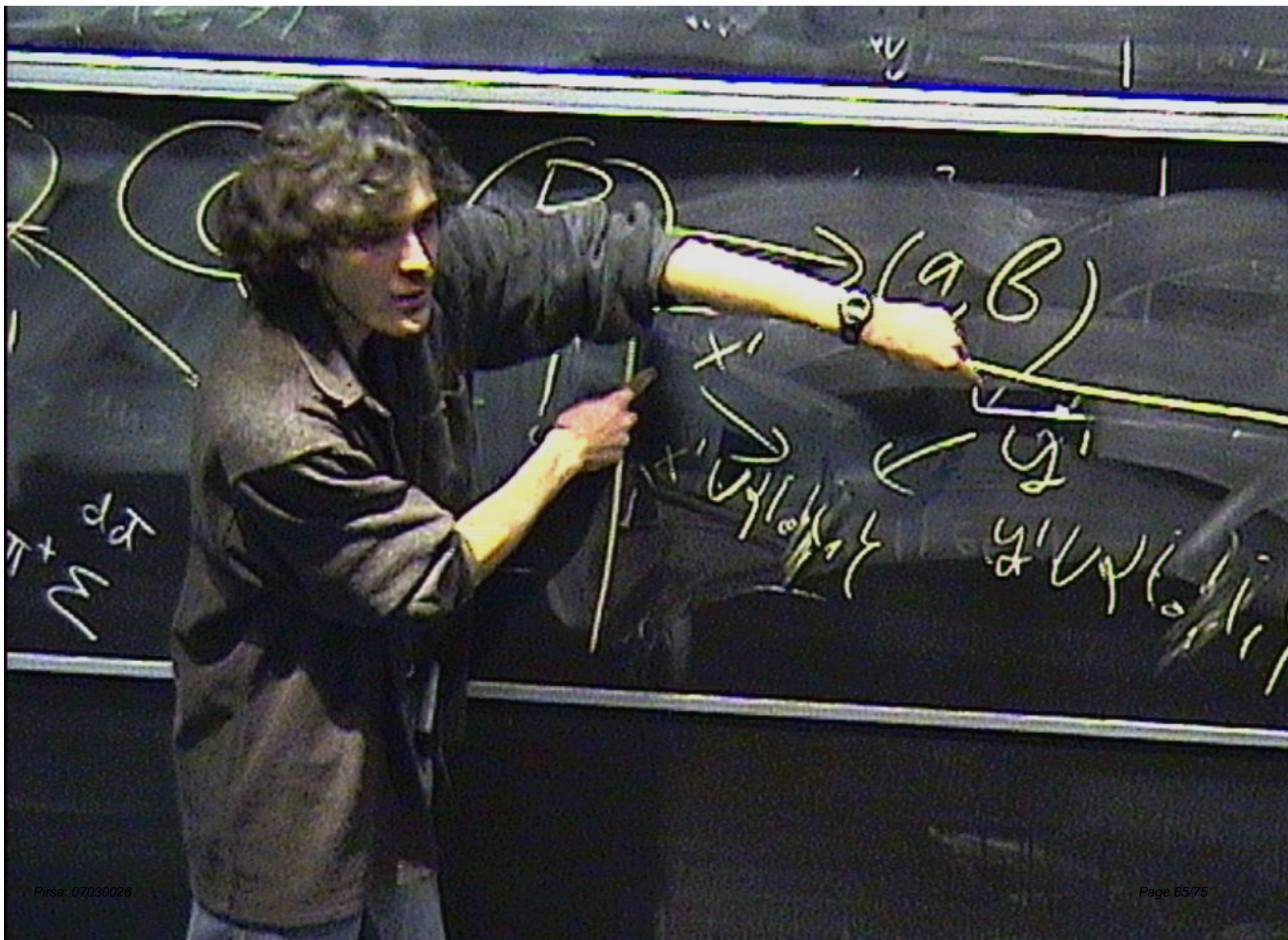


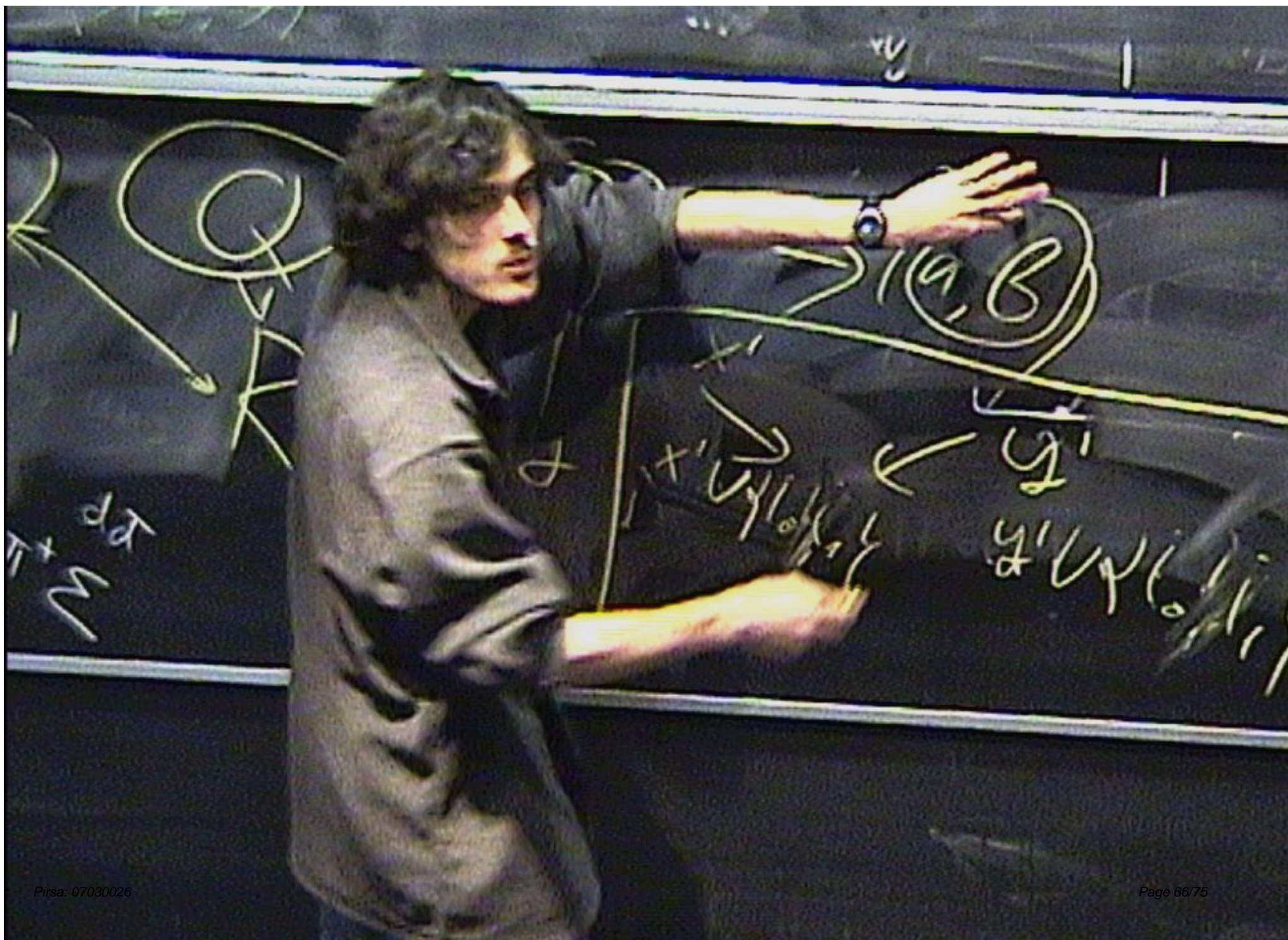


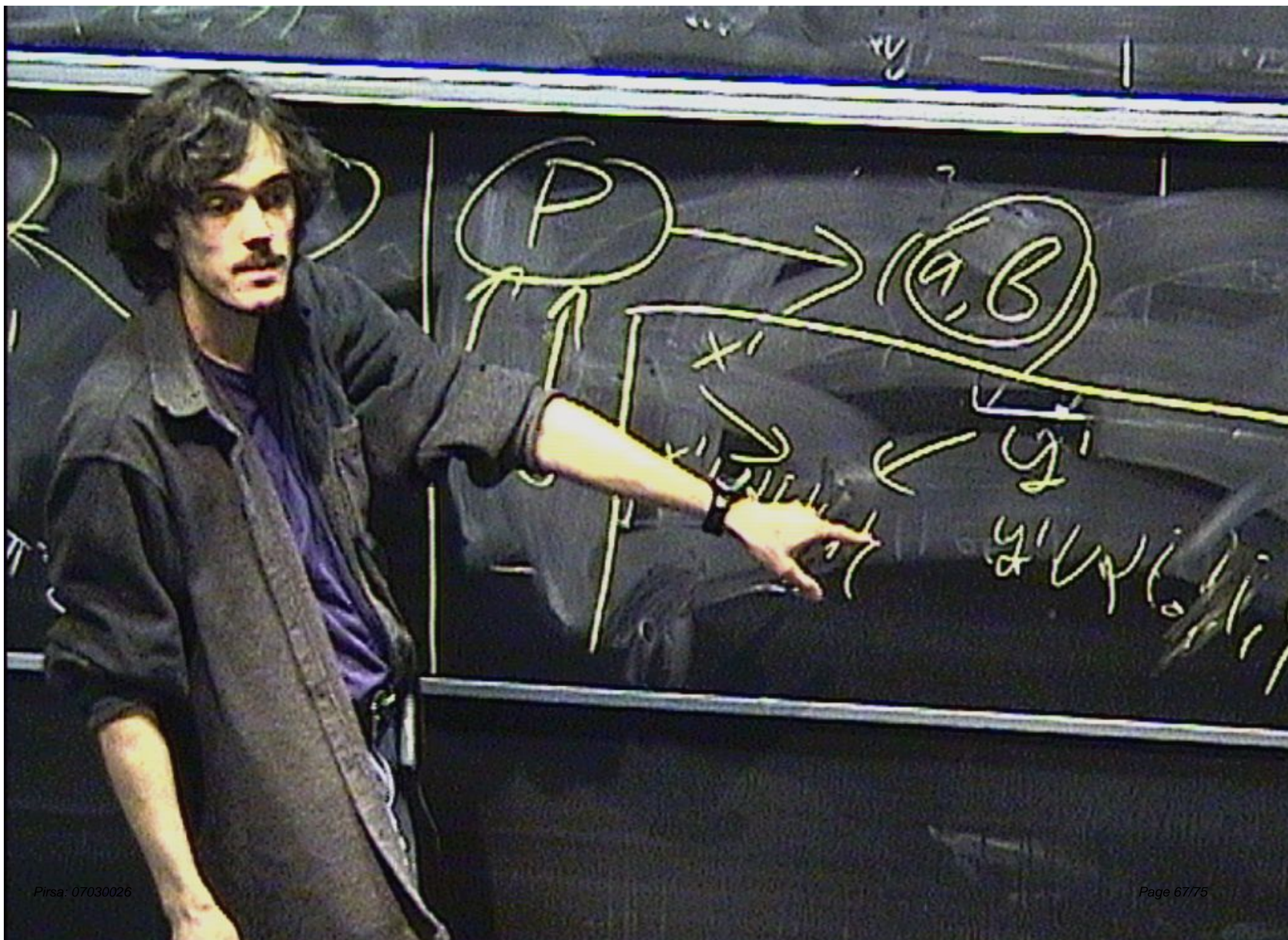












## Open problems

- ▶ Is it possible to find a **functional** problem that requires exponentially more expensive protocol in  $R$  than in  $Q^1$ ?  
How about simultaneous protocols?
- ▶ Generally speaking, give a separation that would logically imply as many known results as possible.

## Open problems

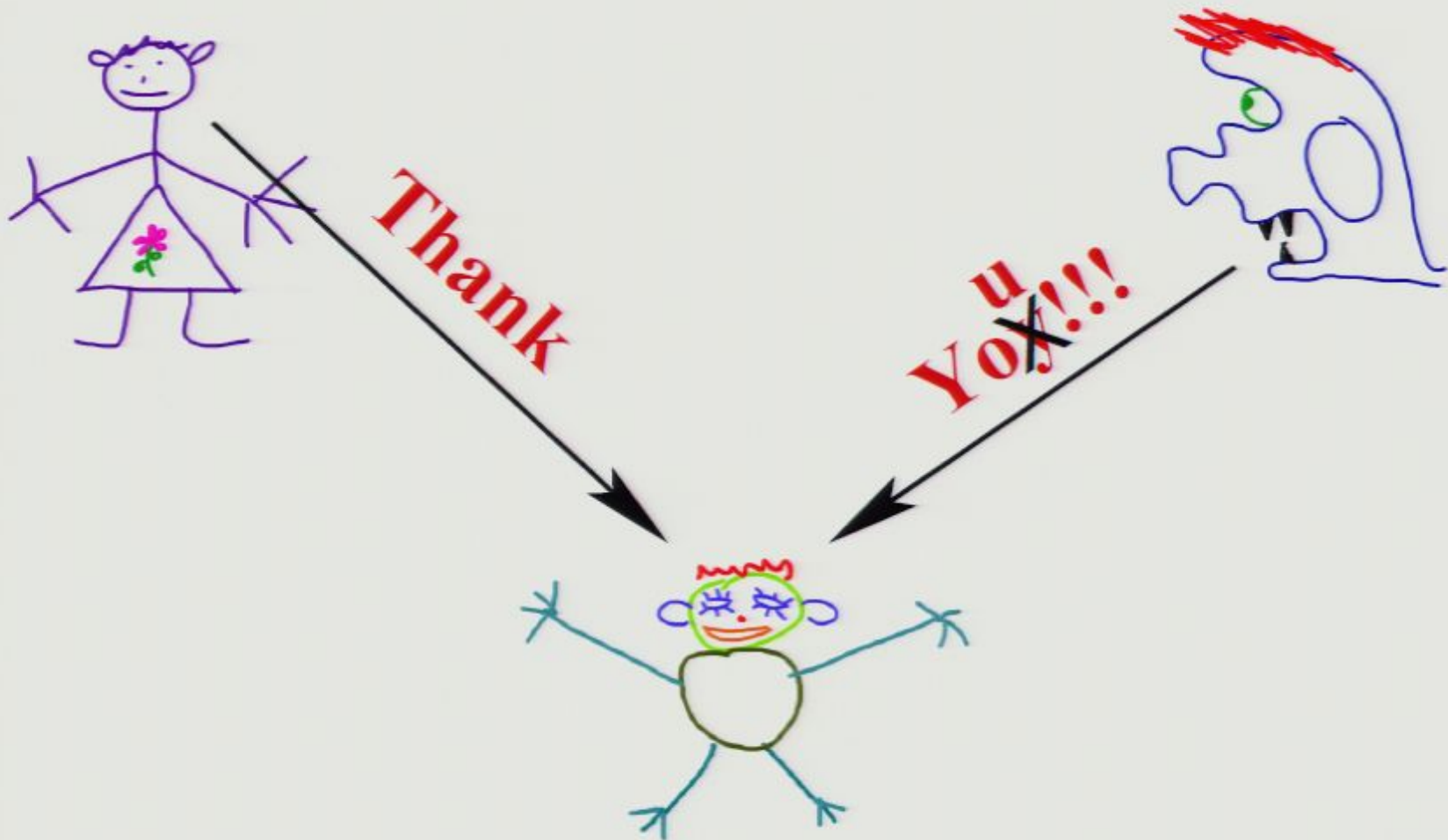
- ▶ Is it possible to find a **functional** problem that requires exponentially more expensive protocol in  $R$  than in  $Q^1$ ?  
How about simultaneous protocols?
- ▶ Generally speaking, give a separation that would logically imply as many known results as possible.

## Open problems

- ▶ Is it possible to find a **functional** problem that requires exponentially more expensive protocol in  $R$  than in  $Q^1$ ?  
How about simultaneous protocols?
- ▶ Generally speaking, give a separation that would logically imply as many known results as possible.

## Open problems

- ▶ Is it possible to find a **functional** problem that requires exponentially more expensive protocol in  $R$  than in  $Q^1$ ?  
How about simultaneous protocols?
- ▶ Generally speaking, give a separation that would logically imply as many known results as possible.



# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

# Exponential Savings from Quantum Communication

- ▶ Zero-error protocols,  $Q$  vs.  $R$  and  $Q^1$  vs.  $R^1$  (Buhrman, Cleve, and Wigderson, 1998)
- ▶ Bounded-error protocols,  $Q$  vs.  $R$  (Raz, 1999)
- ▶ Bounded-error protocols, simultaneous protocols (Buhrman, Cleve, Watrous, and de Wolf, 2001)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a relation (Bar-Yossef, Jayram, and Kerenidis, 2004)
- ▶ Bounded-error protocols,  $Q^1$  vs.  $R^1$ , for a function (Gavinsky, Kempe, Kerenidis, Raz, and de Wolf, 2007)
- ▶ We show a relation that can be solved with bounded error by a  $Q^1$ -protocol that is exponentially more efficient than any  $R$ -protocol

