

Title: Quantum Kolmogorov complexity

Date: Jan 10, 2007 04:00 PM

URL: <http://pirsa.org/07010005>

Abstract: Kolmogorov complexity is a measure of the information contained in a binary string. We investigate the notion of quantum Kolmogorov complexity, a measure of the information required to describe a quantum state. We show that for any definition of quantum Kolmogorov complexity measuring the number of classical bits required to describe a pure quantum state, there exists a pure  $n$ -qubit state which requires exponentially many bits of description. This is shown by relating the classical communication complexity to the quantum Kolmogorov complexity. Furthermore we give some examples of how quantum Kolmogorov complexity can be applied to prove results in different fields, such as quantum computation and communication.



Waterloo, 10<sup>th</sup> January 2007



# Quantum Kolmogorov complexity

Caterina-Eloisa Mora

arXiv: quant-ph/0610109

Joint work with Barbara Kraus and Hans J. Briegel

# Outline



## Kolmogorov complexity:

- What is it and why is it useful?
- Quantum complexity: why and how?



## Communication complexity:

- The SMP model and fingerprinting
- A condition for quantum Kolmogorov complexity



## Quantum Kolmogorov complexity:

- One definition in (some) detail
- Kolmogorov complexity and entanglement
- Applications for quantum Kolmogorov complexity



# Outline



## Kolmogorov complexity:

- What is it and why is it useful?
- Quantum complexity: why and how?



## Communication complexity:

- The SMP model and fingerprinting
- A condition for quantum Kolmogorov complexity



## Quantum Kolmogorov complexity:

- One definition in (some) detail
- Kolmogorov complexity and entanglement
- Applications for quantum Kolmogorov complexity



# Information and physics

Concepts from information theory have been successfully adopted in quantum physics

The modification of the basic unit:

Bits  $\longrightarrow$  Qubits

has changed the whole theory

# Information and physics

Concepts from information theory have been successfully adopted in quantum physics

The modification of the basic unit:

Bits  $\longrightarrow$  Qubits

has changed the whole theory

Shannon entropy  $H(X)$

Error correction,  
coding theorem,...

Von Neumann entropy  $S(\rho)$

Quantum error correction,  
coding theorem,...

Kolmogorov complexity

$K(x)$

Quantum Kolmogorov  
complexity  $K(|\varphi\rangle)$

# Shannon entropy

Random variable:  $X=\{x_i, p_i\}$  (source: output  $x_i$  with prob.  $p_i$ )

The **Shannon entropy**:  $H(x)=-\sum_i p_i \log p_i$  measures:

- The information we gain on average knowing  $X$
- The uncertainty we have before knowing  $X$

Related to information transmission over channels:

Shannon's noiseless (noisy) channel coding theorem



# Shannon entropy

Random variable:  $X=\{x_i, p_i\}$  (source: output  $x_i$  with prob.  $p_i$ )

The **Shannon entropy**:  $H(x)=-\sum_i p_i \log p_i$  measures:

- The information we gain on average knowing  $X$
- The uncertainty we have before knowing  $X$

Related to information transmission over channels:

Shannon's noiseless (noisy) channel coding theorem

Successfully generalized to quantum physics:

→ von Neumann entropy of quantum states:  $S(\rho)$

# Shannon entropy

Random variable:  $X=\{x_i, p_i\}$  (source: output  $x_i$  with prob.  $p_i$ )

The **Shannon entropy**:  $H(x)=-\sum_i p_i \log p_i$  measures:

- The information we gain on average knowing  $X$
- The uncertainty we have before knowing  $X$

Related to information transmission over channels:

Shannon's noiseless (noisy) channel coding theorem

Successfully generalized to quantum physics:

→ von Neumann entropy of quantum states:  $S(\rho)$



And what about the information contained in a single output of the source?



# Classical Kolmogorov complexity (the idea)

Consider 2 sequences of coin tosses:

a) T T T T T T T T T T

b) H T T H T H T T T H

They have the same probability, but very different structure: b) seems "more random"

Also the two descriptions are different:

a) 10 times tails

b) head, 2 tails, head...



# Classical Kolmogorov complexity (the idea)

Consider 2 sequences of coin tosses:

a) T T T T T T T T T T

b) H T T H T H T T T H

They have the same probability, but very different structure: b) seems "more random"

Also the two descriptions are different:

a) 10 times tails

b) head, 2 tails, head...



There is a relation between what we see as random and the complexity of its description

# Classical Kolmogorov complexity (definition)

**Def:** The complexity of a  $N$ -bit string  $\omega_N = \omega_{i_1}\omega_{i_2}\dots\omega_{i_N}$  is the length of the shortest program that has output  $\omega_N$  when running on a computer (universal Turing machine)  $U$ .

$$K_U(\omega_N) = \min_p \{l(p) \mid U(p) = \omega_N\}$$



# Classical Kolmogorov complexity (definition)

**Def:** The complexity of a N-bit string  $\omega_N = \omega_{i_1}\omega_{i_2}\dots\omega_{i_N}$  is the length of the shortest program that has output  $\omega_N$  when running on a computer (universal Turing machine)  $U$ .

$$K_U(\omega_N) = \min_p \{l(p) \mid U(p) = \omega_N\}$$

➔ Invariance: does not depend (up to a constant) on the machine  $\Rightarrow K(\omega_N)$



# Classical Kolmogorov complexity (definition)

**Def:** The complexity of a N-bit string  $\omega_N = \omega_{i_1}\omega_{i_2}\dots\omega_{i_N}$  is the length of the shortest program that has output  $\omega_N$  when running on a computer (universal Turing machine)  $U$ .

$$K_U(\omega_N) = \min_p \{l(p) \mid U(p) = \omega_N\}$$

➔ Invariance: does not depend (up to a constant) on the machine  $\Rightarrow K(\omega_N)$



The time needed by the computer is not important!  
Algorithmic complexity  $\neq$  Computation complexity

# Classical Kolmogorov complexity (properties)

- $K(\omega_N) \leq N$ : there always exists a program of the form  
"write  $\omega_N = \omega_{i_1} \omega_{i_2} \dots \omega_{i_N}$ "  
→  $\omega_N$  is complex if  $K(\omega_N) \sim N$



# Classical Kolmogorov complexity (properties)

- $K(\omega_N) \leq N$ : there always exists a program of the form "write  $\omega_N = \omega_{i_1} \omega_{i_2} \dots \omega_{i_N}$ "
  - $\omega_N$  is complex if  $K(\omega_N) \sim N$
- The Kolmogorov complexity of a string is **uncomputable**
  - Upper bounds are computable, though



# Classical Kolmogorov complexity (properties)

- $K(\omega_N) \leq N$ : there always exists a program of the form "write  $\omega_N = \omega_{i_1} \omega_{i_2} \dots \omega_{i_N}$ "
  - $\omega_N$  is complex if  $K(\omega_N) \sim N$
- The Kolmogorov complexity of a string is **uncomputable**
  - Upper bounds are computable, though
- At most  $2^k - 1$  strings have complexity lower than  $k$ 
  - There are  $2^N$   $N$ -bit strings
  - $\forall N$  there exists a complex string

# Classical Kolmogorov complexity (applications and relations)

👁 Application: general proof method (diverse fields)

Idea: want to prove a property  $P$

1) Choose  $\omega_N$  complex

2) Show:  $P \text{ false} \Rightarrow K(\omega_N) < N$



# Classical Kolmogorov complexity (applications and relations)

👁 Application: general proof method (diverse fields)

Idea: want to prove a property  $P$

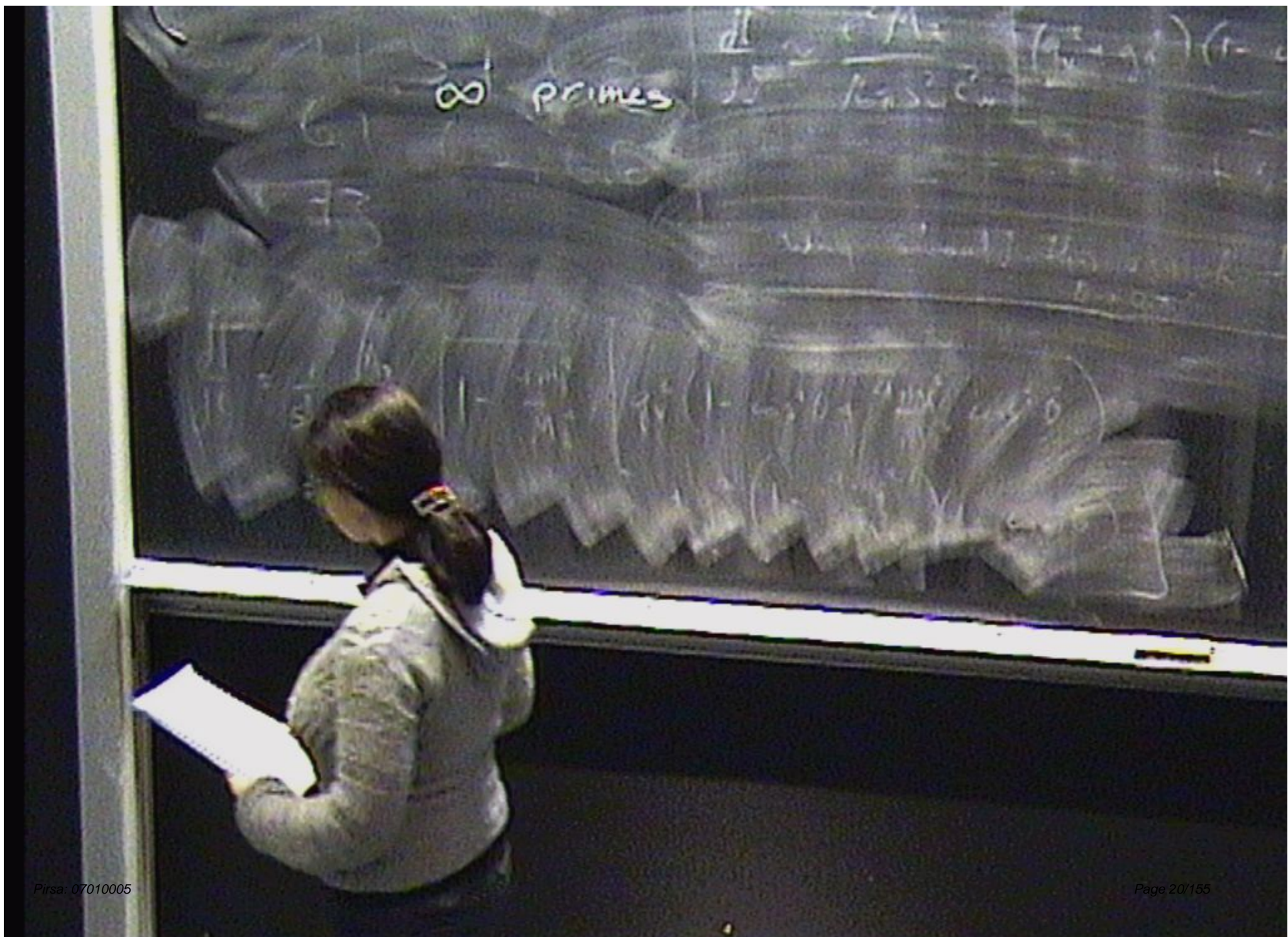
1) Choose  $\omega_N$  complex

2) Show:  $P \text{ false} \Rightarrow K(\omega_N) < N$

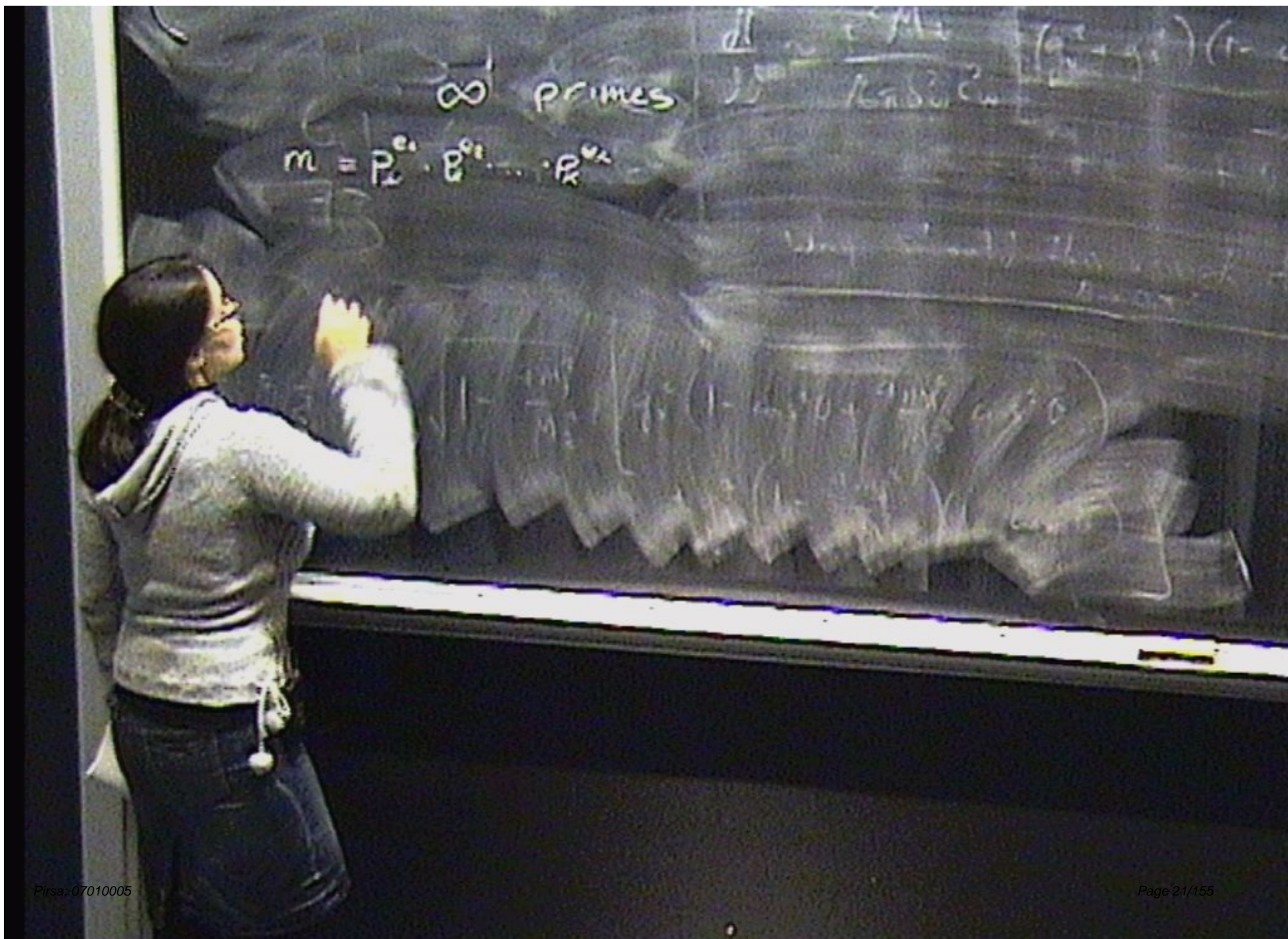
➡ Ex. Gödel's theorem (logic)

Regularity of languages (finite automata)











$\infty$  primes

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \quad e < \log m$$

$k$  primes

$$m \rightarrow e_1, e_2, \dots, e_k$$



$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k} \quad a_i \in \mathbb{N}$$

$K$  primes

$$m \rightarrow e_1, e_2, \dots, e_k$$

$$K(m) \leq \sum_{i=1}^k K(e_i) \leq K \log m$$



$\infty$  primes

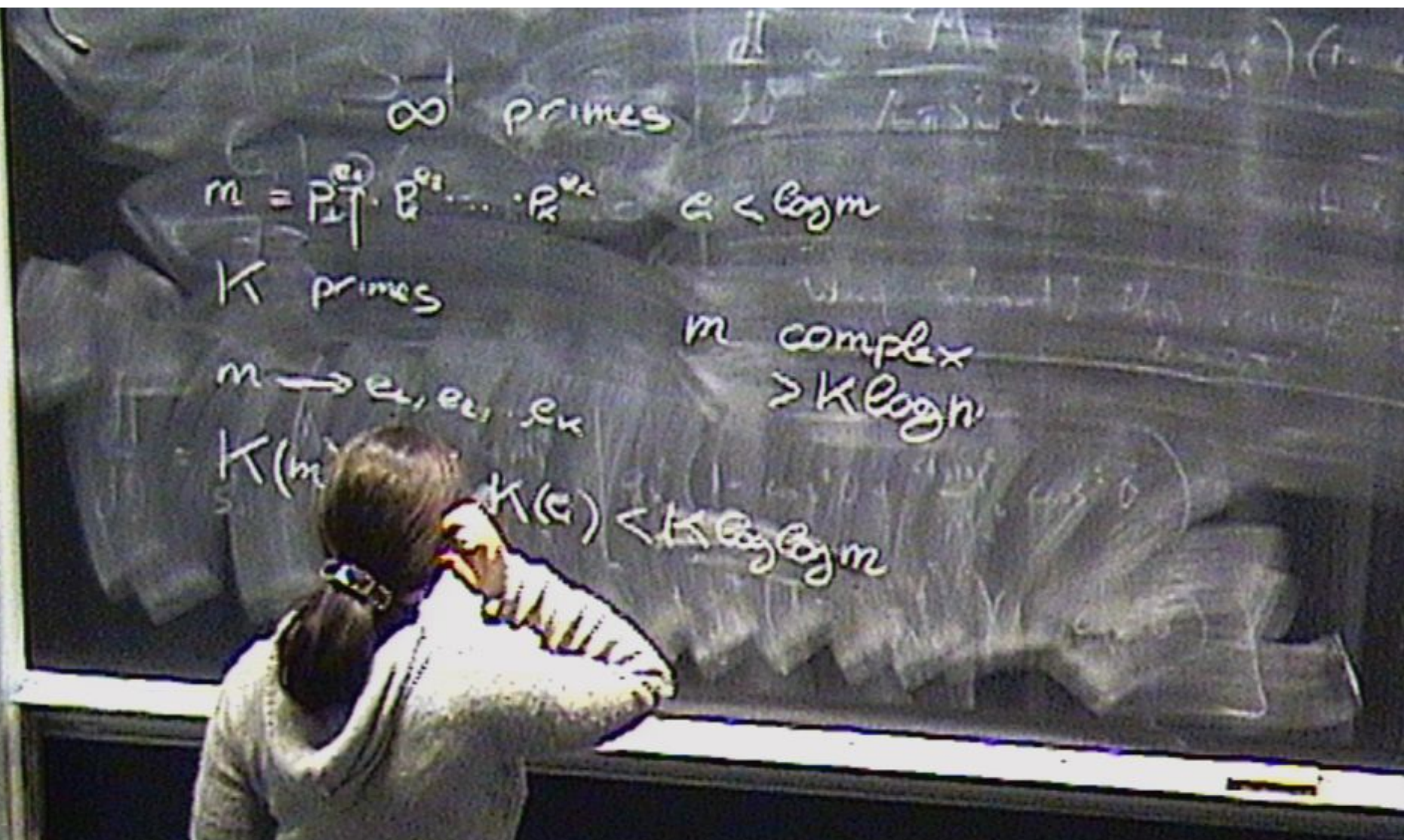
$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k} \quad e_i < \log m$$

$K$  primes

$$m \rightarrow e_1, e_2, \dots, e_k$$

$$K(m) < \sum_{i=1}^k K(e_i) < K \log \log m$$





$\infty$  primes

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \quad e < \log m$$

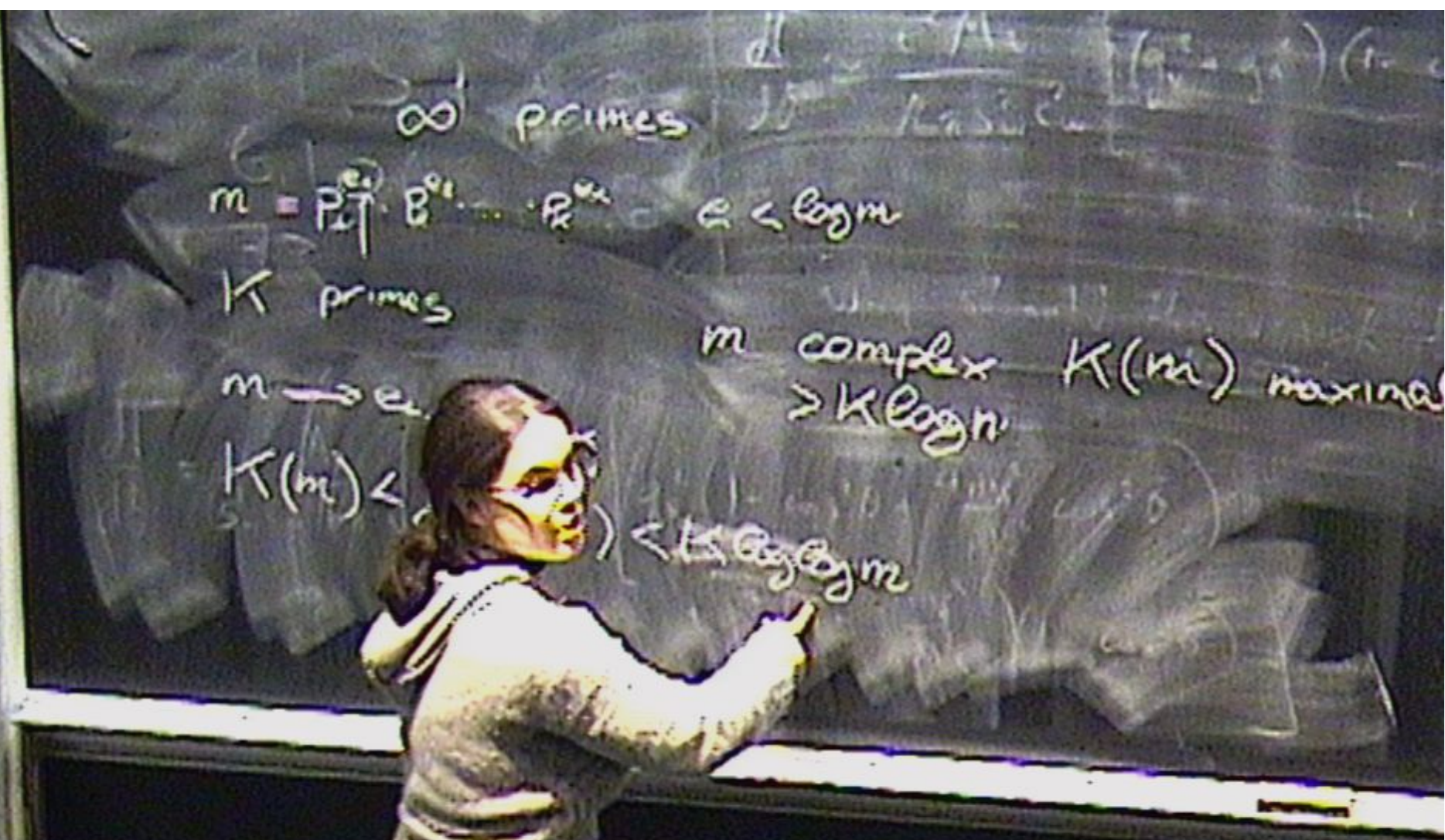
$K$  primes

$$m \rightarrow e_1, e_2, \dots, e_k$$

$m$  complex  
 $> K \log n$

$$K(m) \quad K(e) < K \log \log m$$





$\sum_{p \text{ primes}} \frac{1}{p}$

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \quad e_i \leq \log m$$

$K$  primes

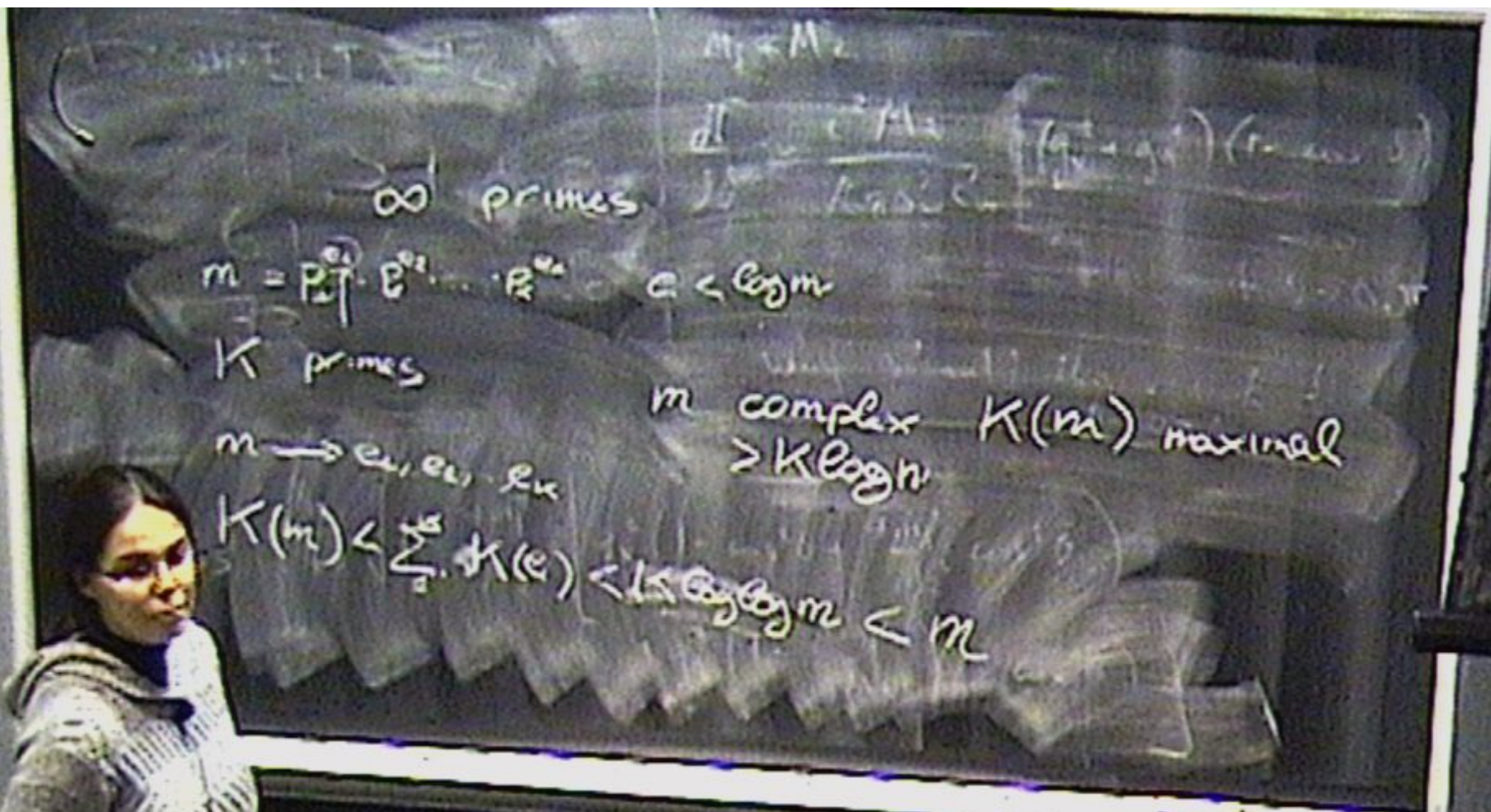
$$m \rightarrow e$$

$$K(m) <$$

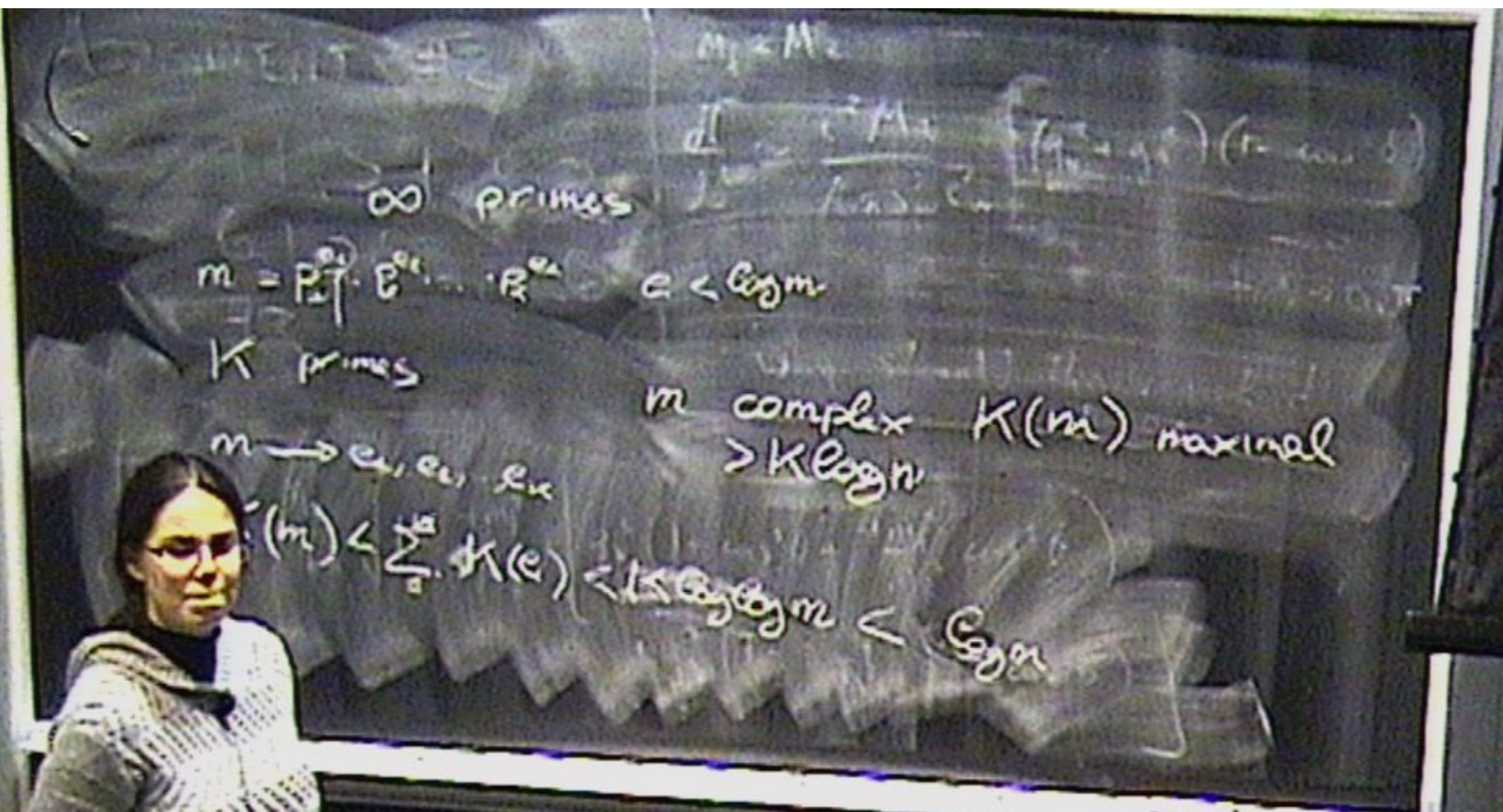
$m$  complex  $K(m)$  maximal  
 $> K \log n$

$$< K \log m$$

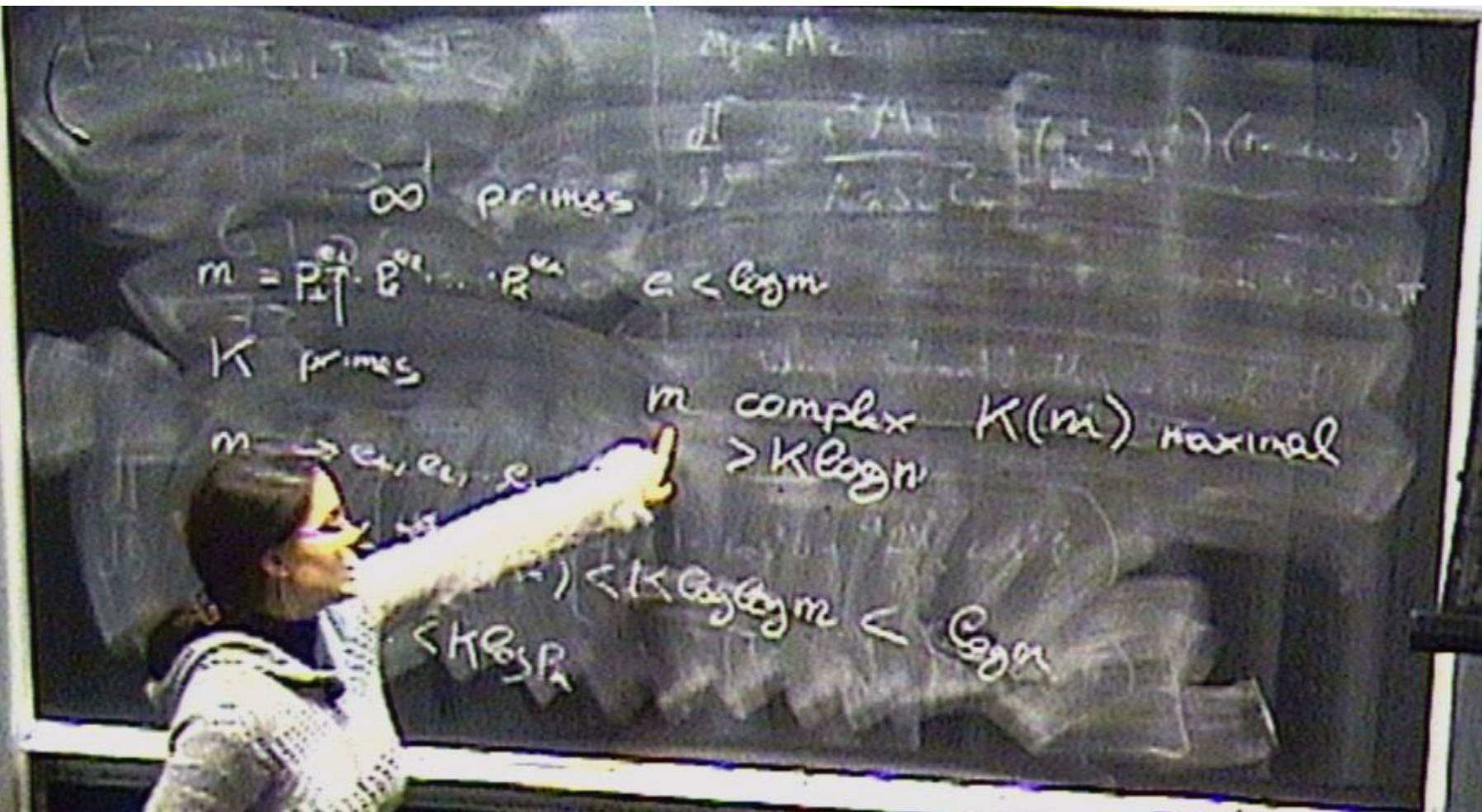














$\infty$  primes  
 $m = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k} \quad e_i < \log m$   
 $K$  primes  
 $m \rightarrow e_1, e_2, \dots, e_k$   
 $K(m) < \sum_{i=1}^k K(e_i) < k \log m < \log m$   
 $+ < K \log p_k$   
 $m$  complex  $K(m)$  maximal  
 $> K \log n$



$\infty$  primes

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} \quad e_i < \log m$$

$K$  primes

$$m \rightarrow e_1, e_2, \dots, e_k$$

$m$  complex  $K(m)$  maximal  
 $> K \log m$

$$\log m = K(m) < \sum_{p|m} K(p) < K \log \log m < \log \log m$$



# Classical Kolmogorov complexity (applications and relations)

👁 Application: general proof method (diverse fields)

Idea: want to prove a property  $P$

1) Choose  $\omega_N$  complex

2) Show:  $P \text{ false} \Rightarrow K(\omega_N) < N$

➡ Ex. Gödel's theorem (logic)

Regularity of languages (finite automata)

# Classical Kolmogorov complexity (applications and relations)

- 👁 Application: general proof method (diverse fields)

Idea: want to prove a property  $P$

1) Choose  $\omega_N$  complex

2) Show:  $P \text{ false} \Rightarrow K(\omega_N) < N$

➡ Ex. Gödel's theorem (logic)

Regularity of languages (finite automata)

- 👁 Relation: expected Kolmogorov complexity equals Shannon entropy rate (average entropy production) of the source



# Classical Kolmogorov complexity (applications and relations)

- 👁 Application: general proof method (diverse fields)

Idea: want to prove a property  $P$

1) Choose  $\omega_N$  complex

2) Show:  $P \text{ false} \Rightarrow K(\omega_N) < N$

➡ Ex. Gödel's theorem (logic)

Regularity of languages (finite automata)

- 👁 Relation: expected Kolmogorov complexity equals Shannon entropy rate (average entropy production) of the source

# Classical Kolmogorov complexity (applications and relations)

- Application: general proof method (diverse fields)

Idea: want to prove a property  $P$

1) Choose  $\omega_N$  complex

2) Show:  $P \text{ false} \Rightarrow K(\omega_N) < N$

→ Ex. Gödel's theorem (logic)

Regularity of languages (finite automata)

- Relation: expected Kolmogorov complexity equals Shannon entropy rate (average entropy production) of the source

- Relation: a complex string is incompressible



# Quantum Kolmogorov complexity (the idea)

What is Kolmogorov complexity in the context of **quantum information**?

1) Kolmogorov complexity of what?

Classical: bits  $\{0,1\} \longleftrightarrow \{0,1\}^N$  string of bits

Quantum: qubits  $\mathbb{C}^2 = \mathbb{Q}_N \longleftrightarrow (\mathbb{C}^2)^N$  string of qubits?

# Quantum Kolmogorov complexity (the idea)

What is Kolmogorov complexity in the context of **quantum information**?

1) Kolmogorov complexity of what?

Classical: bits  $\{0,1\} \longleftrightarrow \{0,1\}^N$  string of bits

Quantum: qubits  $\mathbb{C}^2 = \mathbb{Q}_N \longleftrightarrow (\mathbb{C}^2)^N$  **STATE**



# Quantum Kolmogorov complexity (the idea)

What is Kolmogorov complexity in the context of **quantum information**?

1) Kolmogorov complexity of what?

Classical: bits  $\{0,1\} \longleftrightarrow \{0,1\}^N$  string of bits

Quantum: qubits  $\mathbb{C}^2 = Q_N \longleftrightarrow (\mathbb{C}^2)^N$  **STATE**

2) What do we want? Classically we reproduce the sequence. Do we require to reproduce the state? How? And how should we measure it? Bits? Qubits?

# Quantum Kolmogorov complexity (the idea)

What is Kolmogorov complexity in the context of **quantum information**?

1) Kolmogorov complexity of what?

Classical: bits  $\{0,1\} \longleftrightarrow \{0,1\}^N$  string of bits

Quantum: qubits  $\mathbb{C}^2 = Q_N \longleftrightarrow (\mathbb{C}^2)^N$  **STATE**

2) What do we want? Classically we reproduce the sequence. Do we require to reproduce the state? How? And how should we measure it? Bits? Qubits?

3) How do we define it? – Quantum Turing machine?  
– Other models?



# Quantum Kolmogorov complexity (...many definitions...)

## 👁 Qubits needed to describe a state

Length of the shortest **quantum program**  $|\pi\rangle$  that outputs the state with high fidelity when running on a **quantum Turing machine**

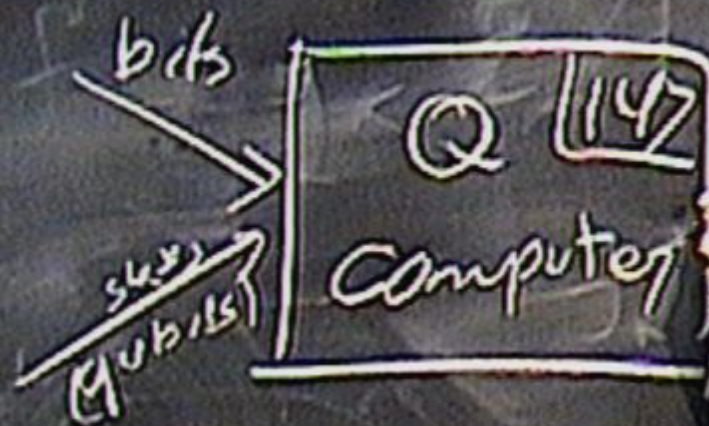
(Length of  $|\pi\rangle$  = number of qubits needed to span the smallest Hilbert space containing  $|\pi\rangle$ )

A. Berthiaume, W. van Dam and S. Laplante, J. of Computer and System Sciences **63**, 201 (2001)

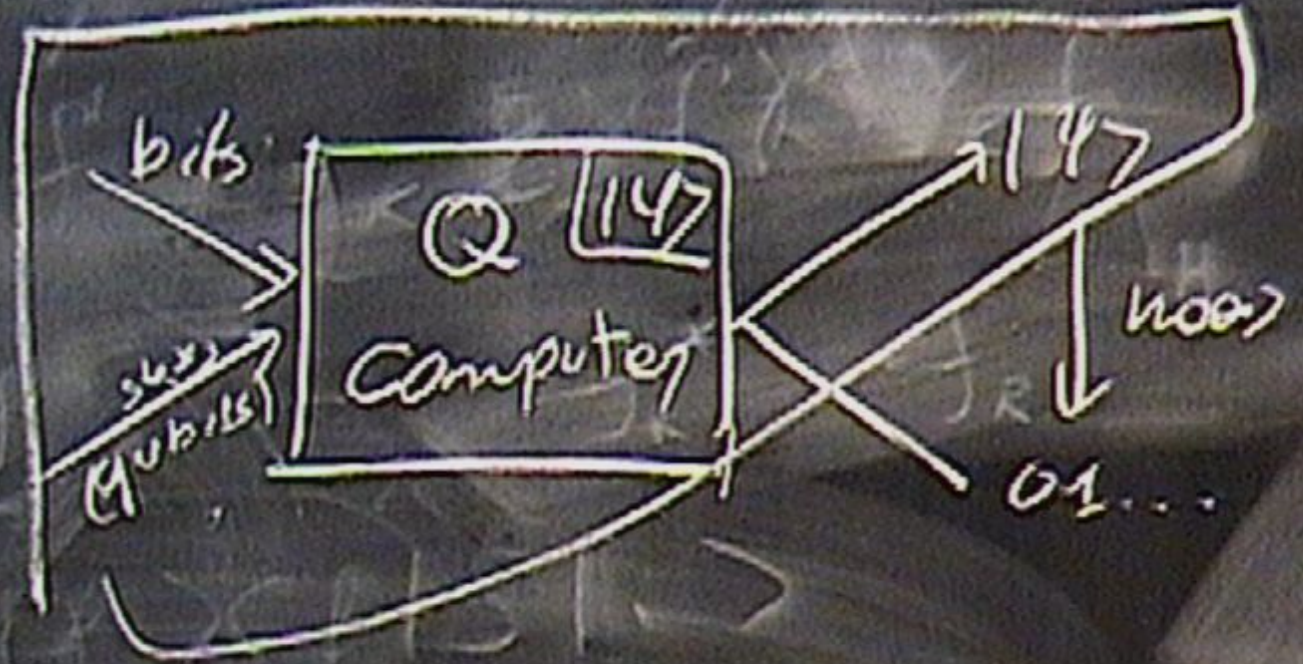


Q  
Computer











# Quantum Kolmogorov complexity (...many definitions...)

## 👁 Qubits needed to describe a state

Length of the shortest **quantum program**  $|\pi\rangle$  that outputs the state with high fidelity when running on a **quantum Turing machine**

(Length of  $|\pi\rangle$  = number of qubits needed to span the smallest Hilbert space containing  $|\pi\rangle$ )

A. Berthiaume, W. van Dam and S. Laplante, J. of Computer and System Sciences **63**, 201 (2001)

# Quantum Kolmogorov complexity (...many definitions...)

## 👁 Qubits needed to describe a state

Length of the shortest **quantum program**  $|\pi\rangle$  that outputs the state with high fidelity when running on a **quantum Turing machine**

(Length of  $|\pi\rangle$  = number of qubits needed to span the smallest Hilbert space containing  $|\pi\rangle$ )

A. Berthiaume, W. van Dam and S. Laplante, J. of Computer and System Sciences **63**, 201 (2001)

$$\rightarrow |\varphi\rangle \in Q_N \Rightarrow K(|\varphi\rangle) \lesssim N$$



# Quantum Kolmogorov complexity (...many definitions...)

## 🌀 Qubits needed to describe a state

Length of the shortest **quantum program**  $|\pi\rangle$  that outputs the state with high fidelity when running on a **quantum Turing machine**

(Length of  $|\pi\rangle$  = number of qubits needed to span the smallest Hilbert space containing  $|\pi\rangle$ )

A. Berthiaume, W. van Dam and S. Laplante, J. of Computer and System Sciences **63**, 201 (2001)

$$\rightarrow |\varphi\rangle \in Q_N \Rightarrow K(|\varphi\rangle) \lesssim N$$

# Quantum Kolmogorov complexity (...many definitions...)

## 🌀 Qubits needed to describe a state

Length of the shortest **quantum program**  $|\pi\rangle$  that outputs the state with high fidelity when running on a **quantum Turing machine**

(Length of  $|\pi\rangle$  = number of qubits needed to span the smallest Hilbert space containing  $|\pi\rangle$ )

A. Berthiaume, W. van Dam and S. Laplante, J. of Computer and System Sciences **63**, 201 (2001)

$$\rightarrow |\varphi\rangle \in Q_N \Rightarrow K(|\varphi\rangle) \lesssim N$$

$\rightarrow$  Related to von Neumann entropy rate

F. Benatti et al., Comm. Math. Phys. **265**, 2(2006)



# Quantum Kolmogorov complexity (...and more...)

## 👁 Bits needed to describe a state

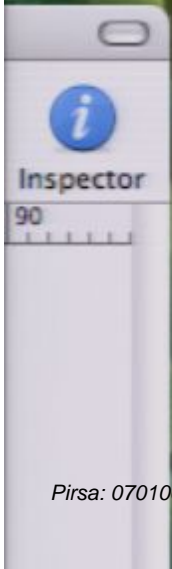
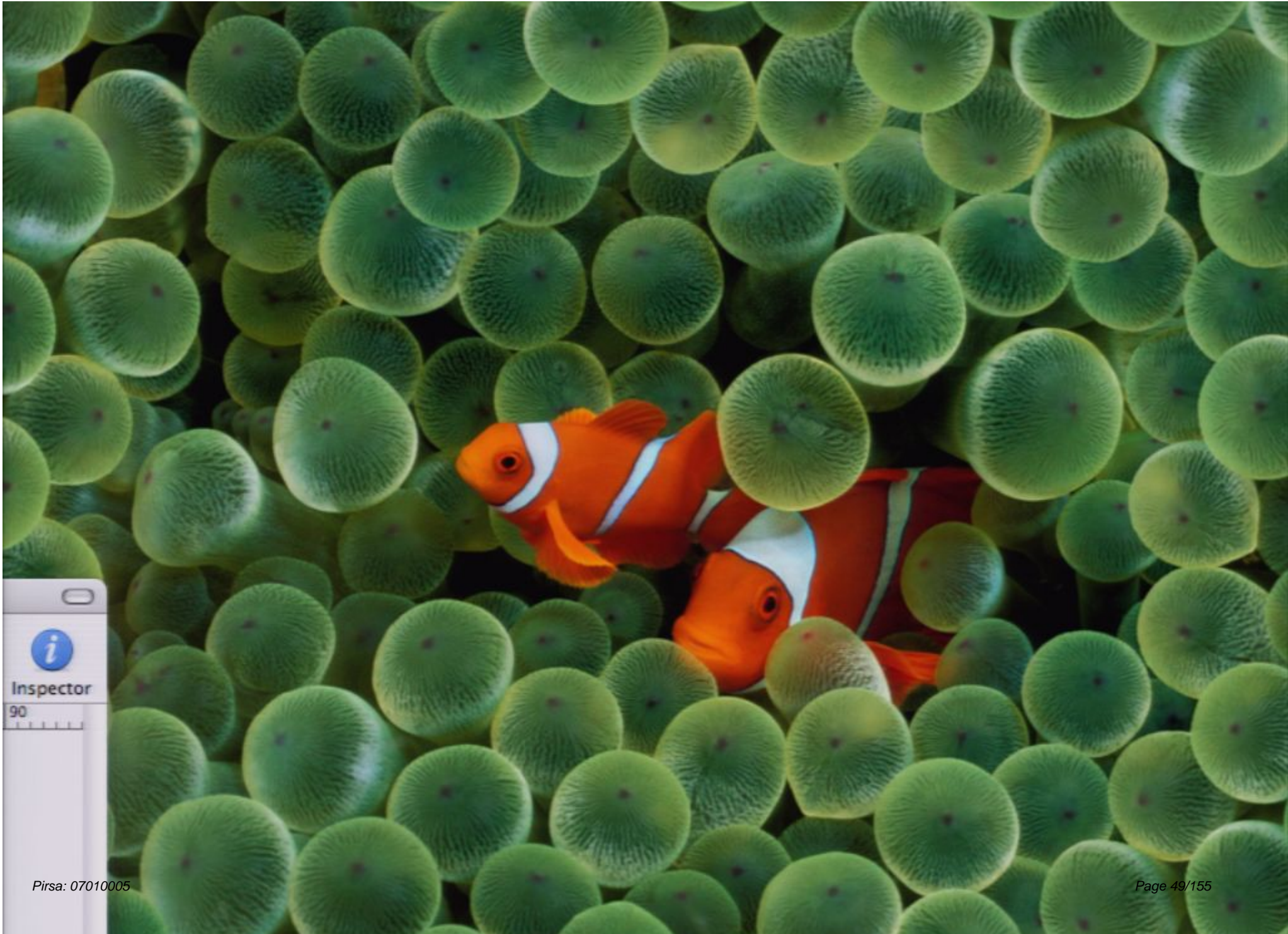
$$K(|\varphi\rangle |y) = \min_{\text{Classical program } p \text{ approximates } |\varphi\rangle} \{ l(p) + \lceil -\log(|\langle \varphi | z \rangle|^2) \rceil \mid U_p(p, y) = |z\rangle \}$$

Two parts:

–  $\lceil -\log(|\langle \varphi | z \rangle|^2) \rceil$  penalty for

approximation

P. Vitányi, IEEE Transactions on Information Theory 47, 2464 (2001)





# Quantum Kolmogorov complexity (...and more...)

## • Bits needed to describe a state

$$K(|\varphi\rangle |y) = \min_p \{ |p| + \lceil -\log(|\langle \varphi|z\rangle|^2) \rceil : U_p(p,y) = |z\rangle \}$$

Classical program  $p$  approximates  $|\varphi\rangle$

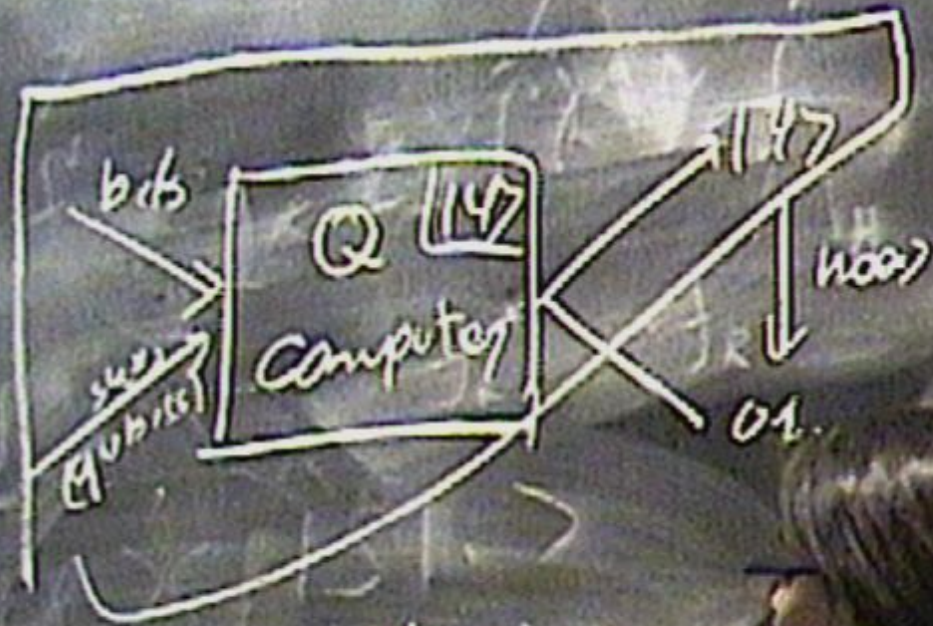
Two parts:

–  $\lceil -\log(|\langle \varphi|z\rangle|^2) \rceil$  penalty for

approximation

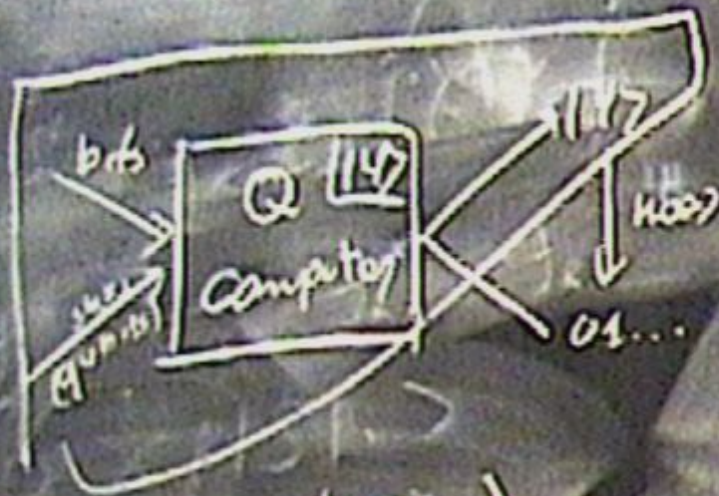
P. Vitanyi, IEEE Transactions on Information Theory 47, 2464 (2001)





$$K(|\psi\rangle) = \min_p \left\{ \right.$$

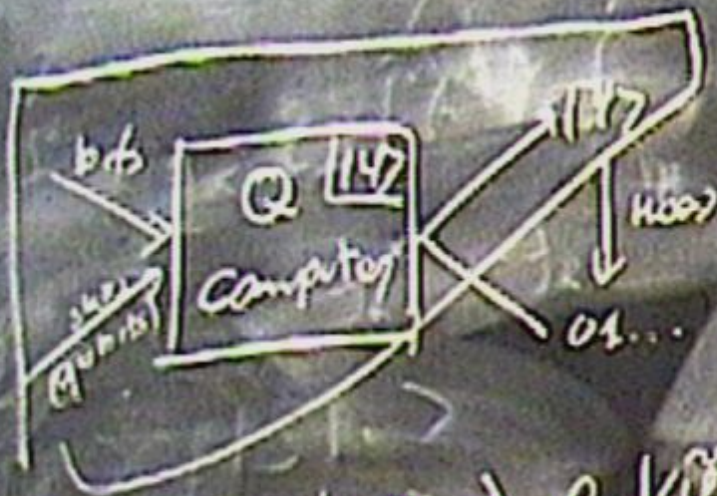




$$K(|\psi\rangle) = \min_p \{ \ell(p) \}$$

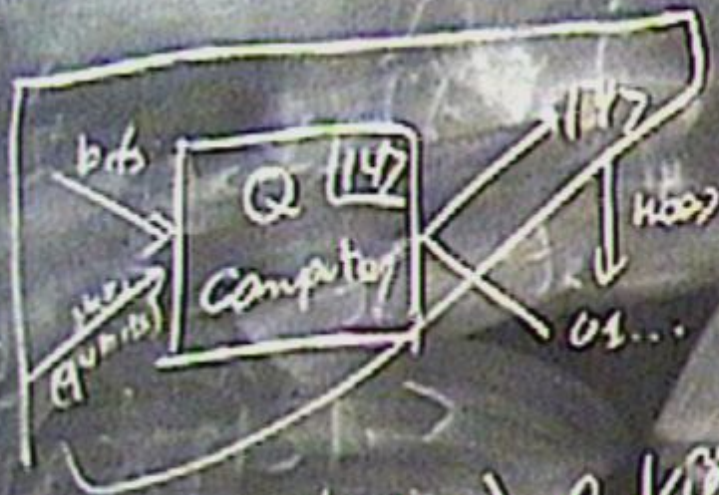
$$|Q(P|\psi)\rangle = 1$$





$$K(|\psi\rangle) = \min_p \left\{ \ell(p) - \ell_{\text{avg}} \langle Q | \psi \rangle / U(p | \psi) = 1 \right. \\ \left. = |\psi\rangle \right\}$$





$$K(|\psi\rangle) = \min_p \left\{ \ell(p) - \log |\langle \psi | \psi \rangle| U(p | \psi) = 1 \right. \\ \left. = |\psi\rangle \right\}$$



# Quantum Kolmogorov complexity

## (...and more...)

### Bits needed to describe a state

$$K(|\varphi\rangle |y) = \min_{\text{Classical program } p \text{ approximates } |\varphi\rangle} \{l(p) + \lceil -\log(|\langle \varphi|z\rangle|^2) \rceil : U_p(p,y) = |z\rangle \}$$

Two parts:

–  $\lceil -\log(|\langle \varphi|z\rangle|^2) \rceil$  penalty for

approximation

P. Vitanyi, IEEE Transactions on Information Theory 47, 2464 (2001)

### Bits needed to describe how to prepare a state

$K_{\text{set}}(|\varphi\rangle |y)$  = complexity of the simplest classical string describing a circuit that prepares  $|\varphi\rangle$

C.M. and H. J. Briegel, IJQI 4, 4 (2006)



# Communication complexity (I)

Typical scenario: Alice and Bob receive (binary) inputs  $x, y$  and want to compute a function  $f(x, y)$

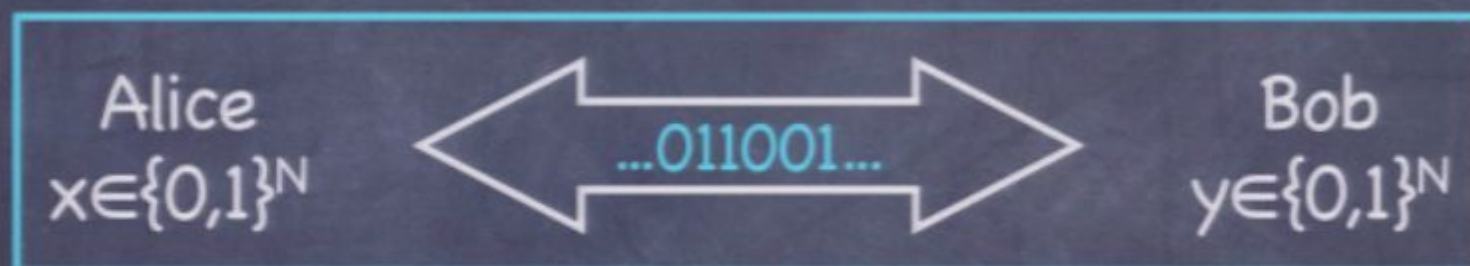
Alice  
 $x \in \{0, 1\}^N$

Bob  
 $y \in \{0, 1\}^N$

# Communication complexity (I)

Typical scenario: Alice and Bob receive (binary) inputs  $x, y$  and want to compute a function  $f(x, y)$

To do this they are allowed (need) to communicate



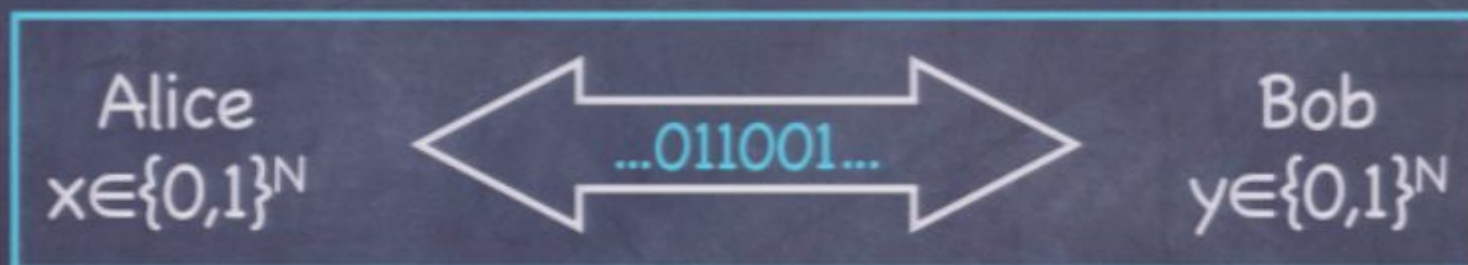
**Def:** The (classical) communication complexity  $C_c(f)$  is the minimum number of bits that A and B need to exchange



# Communication complexity (I)

Typical scenario: Alice and Bob receive (binary) inputs  $x, y$  and want to compute a function  $f(x, y)$

To do this they are allowed (need) to communicate

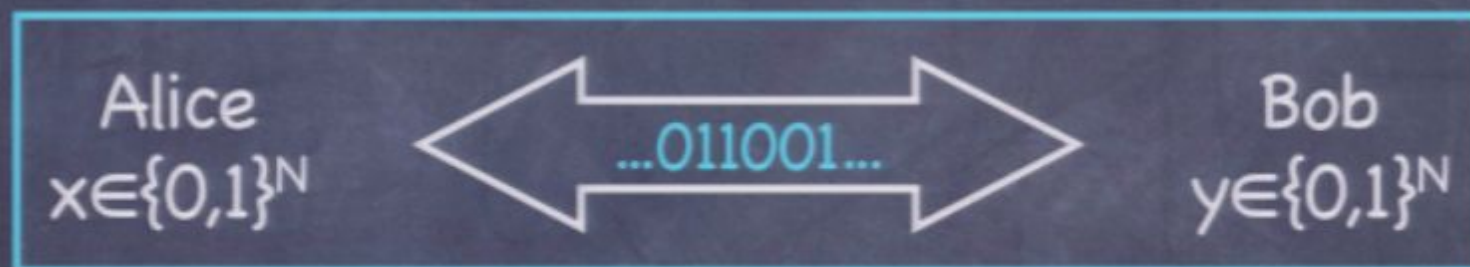


**Def:** The (classical) communication complexity  $C_c(f)$  is the minimum number of bits that A and B need to exchange

# Communication complexity (I)

Typical scenario: Alice and Bob receive (binary) inputs  $x, y$  and want to compute a function  $f(x, y)$

To do this they are allowed (need) to communicate



**Def:** The (classical) communication complexity  $C_c(f)$  is the minimum number of bits that A and B need to exchange

➡  $C_c(f) \leq N$ : Alice can always send her whole input  $x$



# Communication complexity (II)

Different models:

- Worst case scenario: interested in the communication needed for the “worst” choice of  $x$  and  $y$
- Expected communication: interested in the average (over  $x$  and  $y$ ) communication needed

# Communication complexity (II)

Different models:

- Worst case scenario: interested in the communication needed for the “worst” choice of  $x$  and  $y$
- Expected communication: interested in the average (over  $x$  and  $y$ ) communication needed
- Without error:  $f(x,y)$  must be evaluated exactly
- With error: an error probability  $\varepsilon$  allowed



# Communication complexity (II)

Different models:

- Worst case scenario: interested in the communication needed for the “worst” choice of  $x$  and  $y$
- Expected communication: interested in the average (over  $x$  and  $y$ ) communication needed
- Without error:  $f(x,y)$  must be evaluated exactly
- With error: an error probability  $\varepsilon$  allowed

Furthermore  $A$  and  $B$  might initially share a random key

# Communication complexity (II)

Different models:

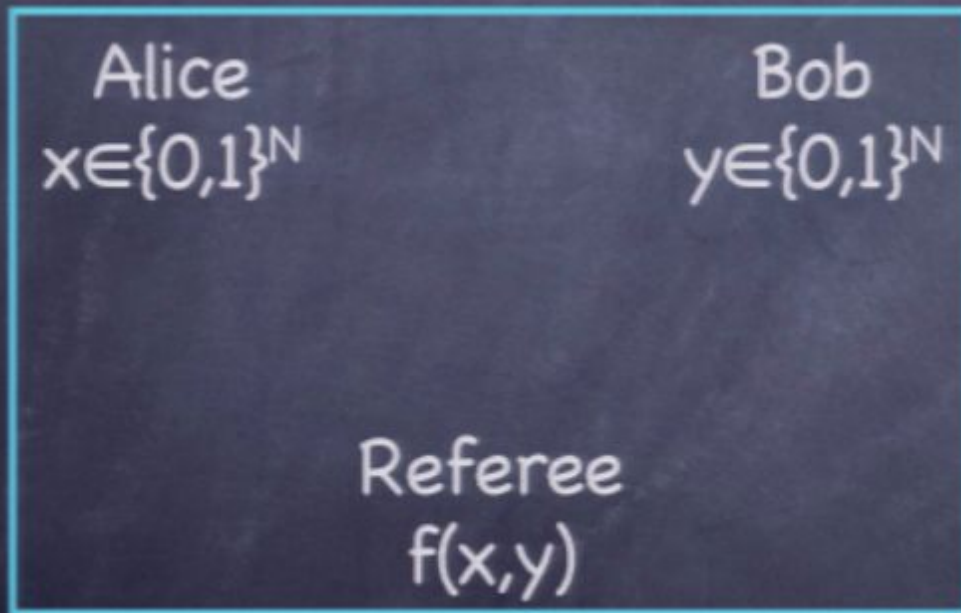
- Worst case scenario: interested in the communication needed for the “worst” choice of  $x$  and  $y$
- Expected communication: interested in the average (over  $x$  and  $y$ ) communication needed
- Without error:  $f(x,y)$  must be evaluated exactly
- With error: an error probability  $\varepsilon$  allowed

Furthermore  $A$  and  $B$  might initially share a random key



# Simultaneous message passing (SMP)

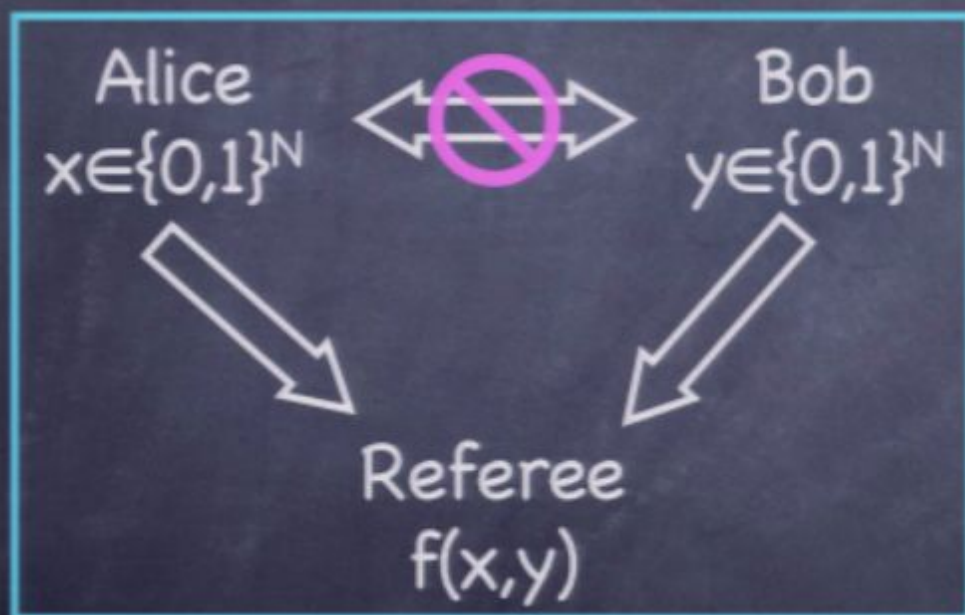
In addition to Alice and Bob there is a third party: Referee



# Simultaneous message passing (SMP)

In addition to Alice and Bob there is a third party: Referee

There is no communication between Alice and Bob, but only between each of them and the referee

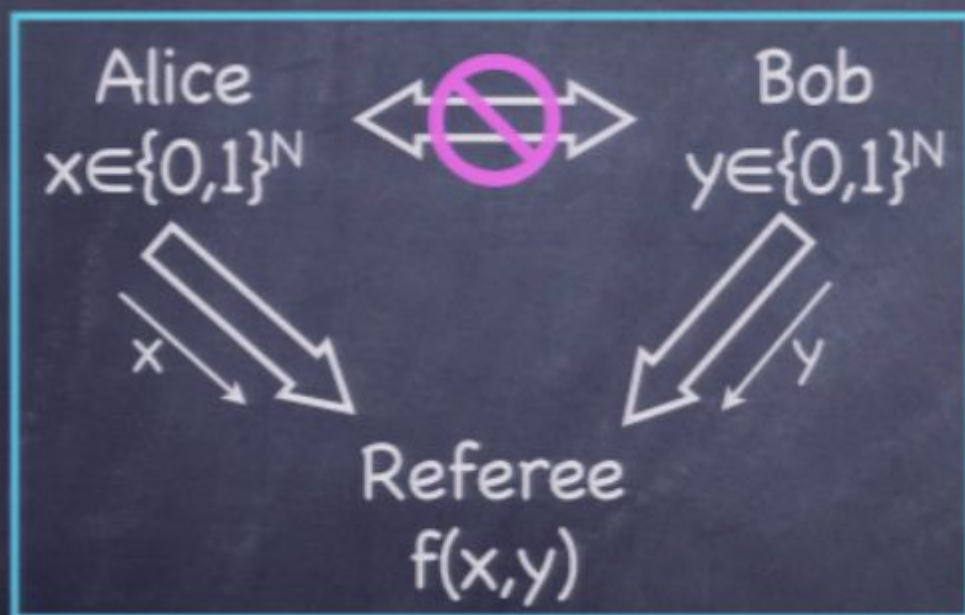




# Simultaneous message passing (SMP)

In addition to Alice and Bob there is a third party: Referee

There is no communication between Alice and Bob, but only between each of them and the referee



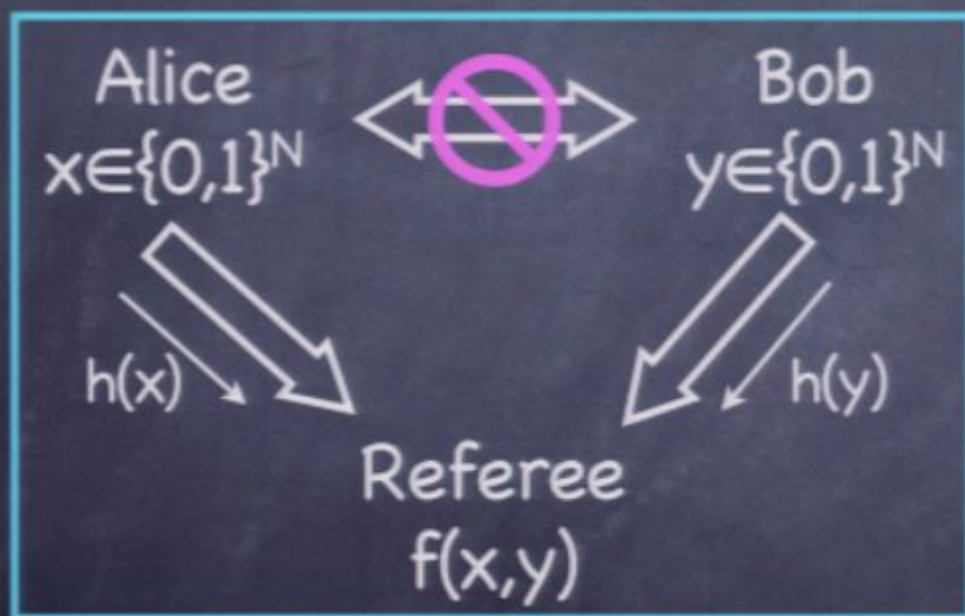
Trivial solution: Alice and Bob send  $x$  and  $y$  respectively

$$C_c(f) \leq 2N$$

# Simultaneous message passing (SMP)

In addition to Alice and Bob there is a third party: Referee

There is no communication between Alice and Bob, but only between each of them and the referee



Trivial solution: Alice and Bob send  $x$  and  $y$  respectively

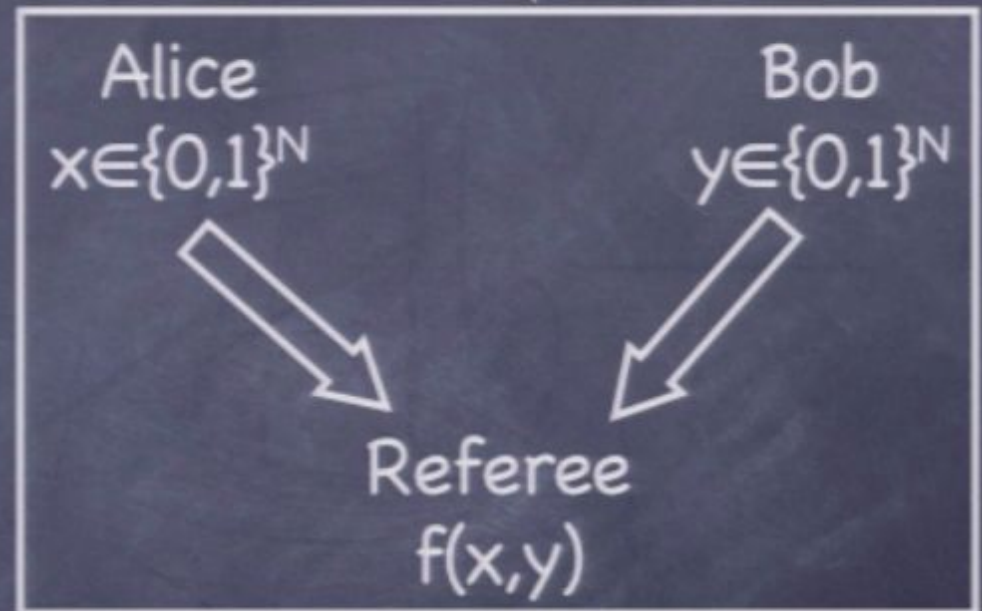
$$C_c(f) \leq 2N$$

Sometimes they can send only “fingerprints” of their inputs



# Equality: an example

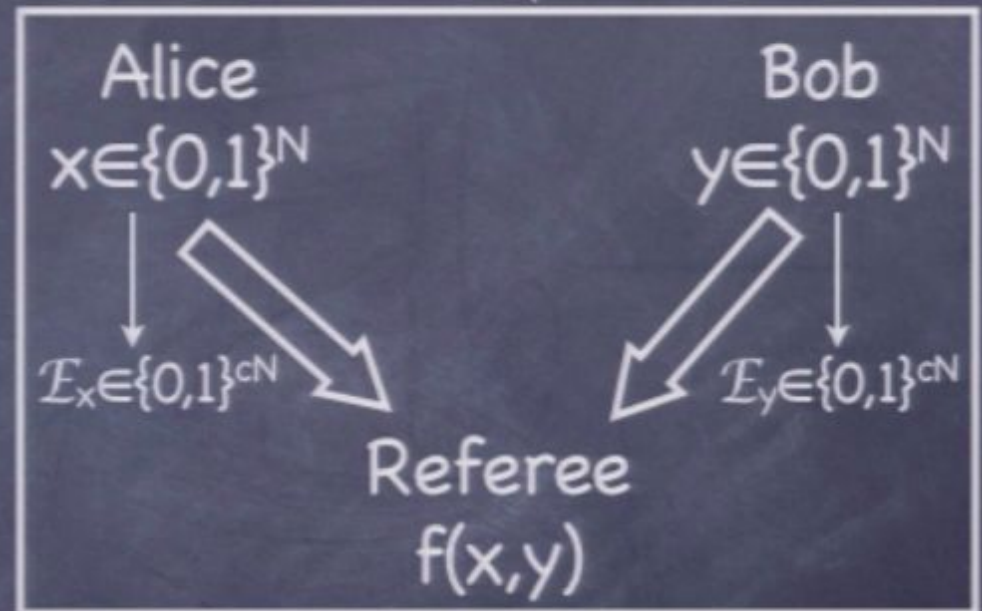
Consider SMP model and  $f(x,y)=EQ_N(x,y)=\begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x \neq y \end{cases}$



# Equality: an example

Consider SMP model and  $f(x,y)=EQ_N(x,y)=\begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x \neq y \end{cases}$

- 1) A and B encode the inputs (error correcting code) so that  $D_H[\mathcal{E}_x, \mathcal{E}_y] > (1-\delta)cN$



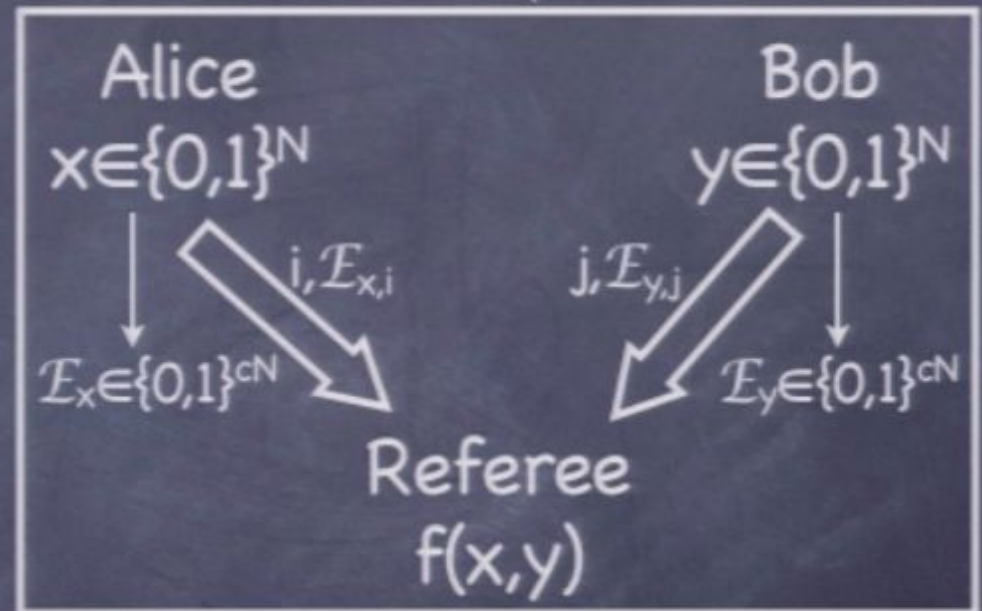


# Equality: an example

Consider SMP model and  $f(x,y)=EQ_N(x,y)=\begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x \neq y \end{cases}$

1) A and B encode the inputs (error correcting code) so that  $D_H[\mathcal{E}_x, \mathcal{E}_y] > (1-\delta)cN$

2) They send only a part of the encoded string

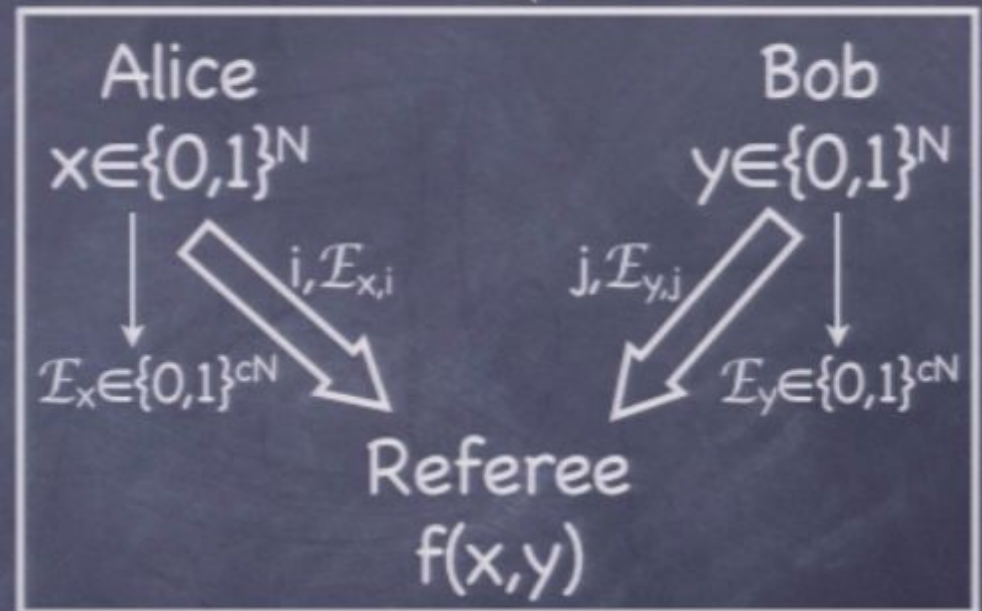


# Equality: an example

Consider SMP model and  $f(x,y)=EQ_N(x,y)=\begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x \neq y \end{cases}$

1) A and B encode the inputs (error correcting code) so that  $D_H[\mathcal{E}_x, \mathcal{E}_y] > (1-\delta)cN$

2) They send only a part of the encoded string



3) The Referee draws his conclusion by comparing the two strings he receives  $P_{\text{error}} = P(\mathcal{E}_{x,i}^{(j)} = \mathcal{E}_{y,j}^{(i)} \mid x \neq y) < \delta$

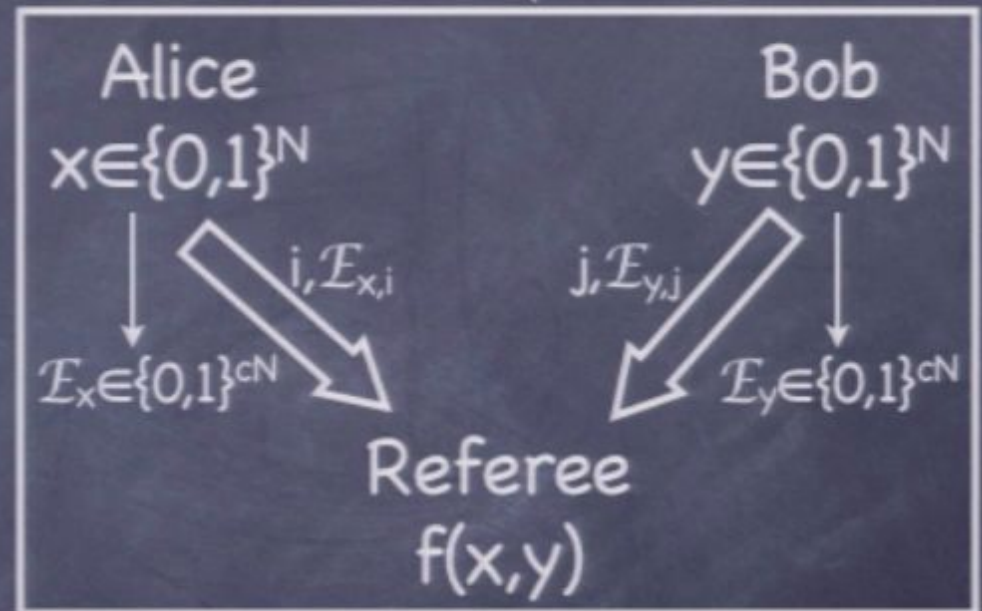


# Equality: an example

Consider SMP model and  $f(x,y)=EQ_N(x,y)=\begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x \neq y \end{cases}$

1) A and B encode the inputs (error correcting code) so that  $D_H[\mathcal{E}_x, \mathcal{E}_y] > (1-\delta)cN$

2) They send only a part of the encoded string



3) The Referee draws his conclusion by comparing the two strings he receives  $P_{\text{error}} = P(\mathcal{E}_{x,i}^{(j)} = \mathcal{E}_{y,j}^{(i)} \mid x \neq y) < \delta$

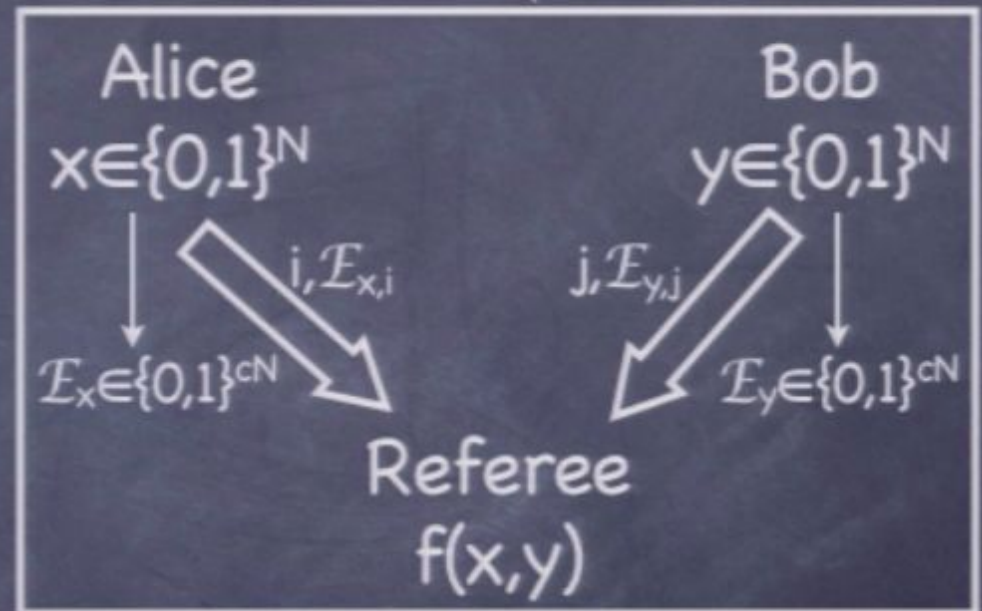
Can be reduced  
as necessary

# Equality: an example

Consider SMP model and  $f(x,y)=EQ_N(x,y)=\begin{cases} 1 & \text{if } x=y \\ 0 & \text{if } x \neq y \end{cases}$

1) A and B encode the inputs (error correcting code) so that  $D_H[\mathcal{E}_x, \mathcal{E}_y] > (1-\delta)cN$

2) They send only a part of the encoded string



3) The Referee draws his conclusion by comparing the two strings he receives  $P_{\text{error}} = P(\mathcal{E}_{x,i}^{(j)} = \mathcal{E}_{y,j}^{(i)} \mid x \neq y) < \delta$

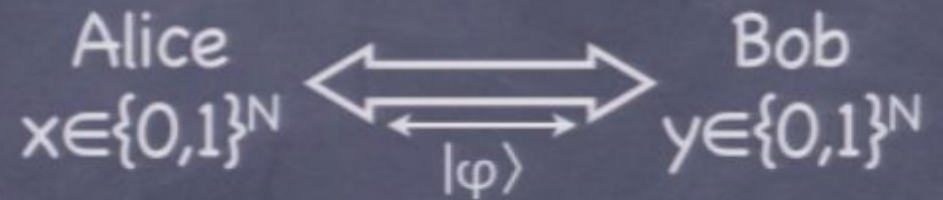
→  $C_C(EQ_N) = O(\sqrt{N})$  Proven to be optimal

Can be reduced  
as necessary



# Quantum communication complexity

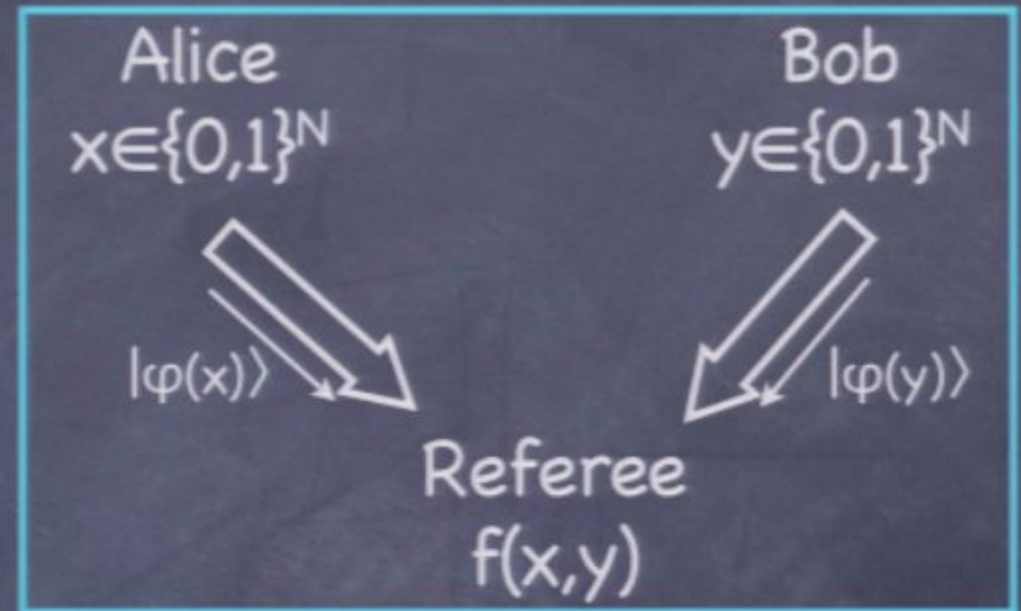
As in the classical case,  
but Alice and Bob share  
a quantum channel



# Quantum communication complexity

As in the classical case,  
but Alice and Bob share  
a quantum channel

And so do the two of  
them and the referee  
in the SMP model

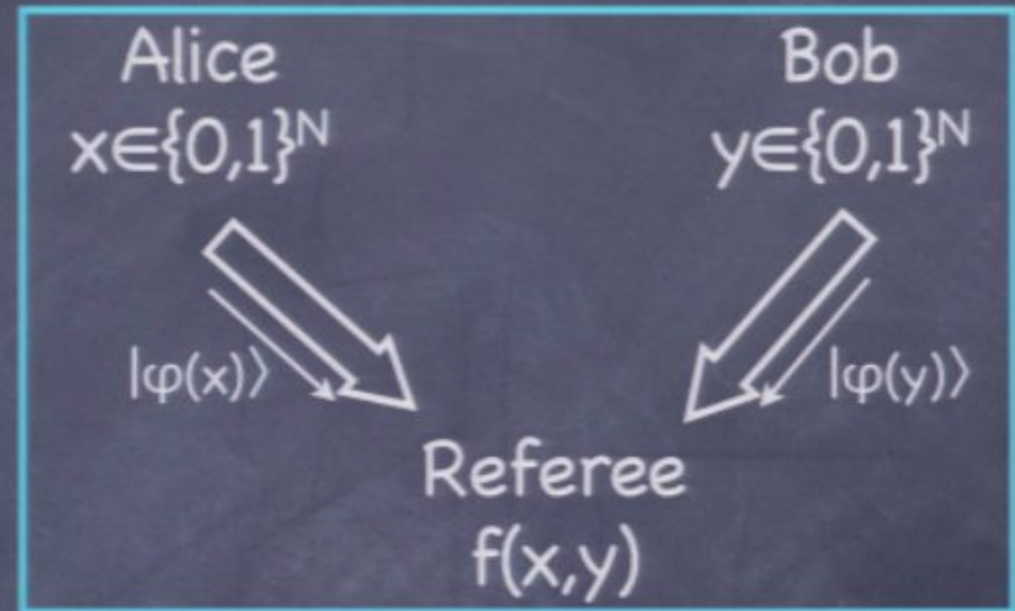




# Quantum communication complexity

As in the classical case,  
but Alice and Bob share  
a quantum channel

And so do the two of  
them and the referee  
in the SMP model

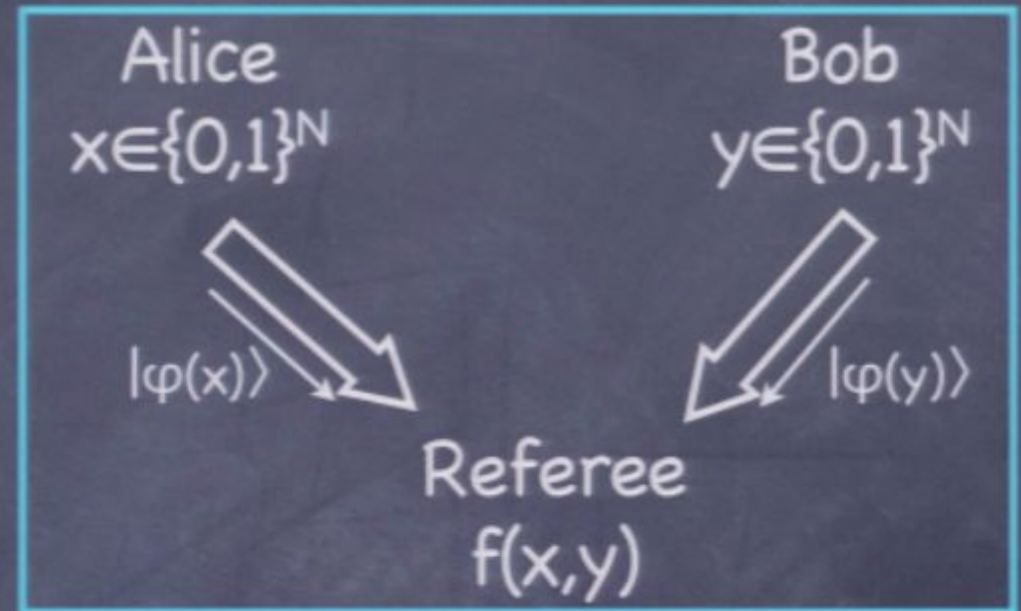


**Holevo:** one qubit cannot be used to transmit more than  
a single bit of (retrievable) information

# Quantum communication complexity

As in the classical case,  
but Alice and Bob share  
a quantum channel

And so do the two of  
them and the referee  
in the SMP model



**Holevo:** one qubit cannot be used to transmit more than  
a single bit of (retrievable) information



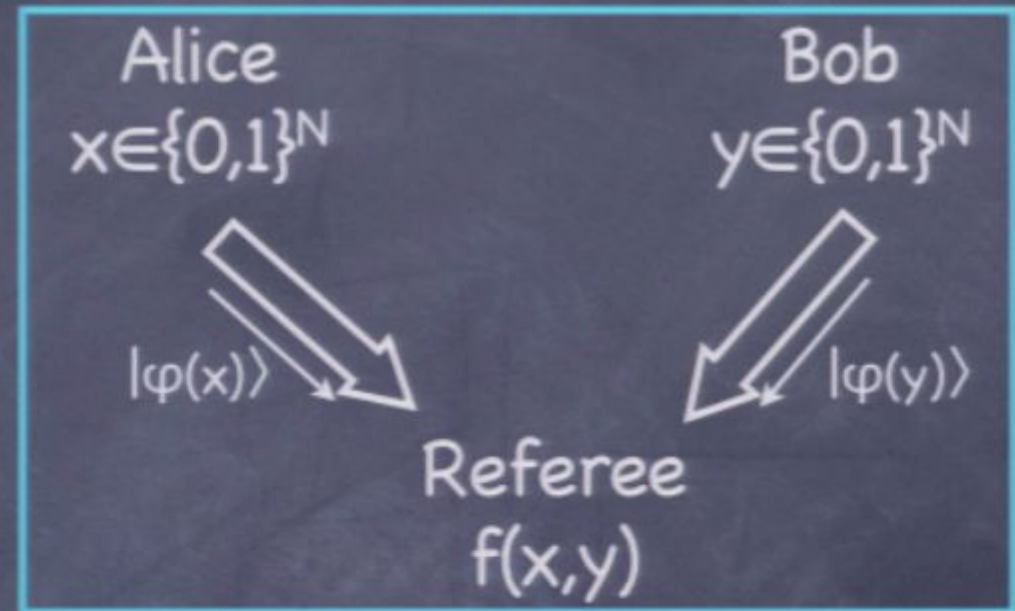
Can we expect any difference between classical  
and quantum communication scenarios?



# Quantum communication complexity

As in the classical case,  
but Alice and Bob share  
a quantum channel

And so do the two of  
them and the referee  
in the SMP model



**Holevo:** one qubit cannot be used to transmit more than  
a single bit of (retrievable) information



Can we expect any difference between classical  
and quantum communication scenarios?

**ATTENTION!** we are interested in  $f(x,y)$  : **single bit!**

# Quantum fingerprinting (and $EQ_N$ )

As in classical case: SMP model and  $f(x,y)=EQ_N(x,y)$

Main idea: Classical procedure

Alice:  $x \xrightarrow{\mathcal{E}} \mathcal{E}_x$

The diagram shows the word "Alice:" followed by the expression  $x \xrightarrow{\mathcal{E}} \mathcal{E}_x$ . The entire expression is enclosed in a white oval. The word "Classical" is written in a curved path above the oval.

Bob:  $y \xrightarrow{\mathcal{E}} \mathcal{E}_y$



# Quantum fingerprinting (and $EQ_N$ )

As in classical case: SMP model and  $f(x,y)=EQ_N(x,y)$

Main idea: Classical procedure + Quantum parallelism

Alice:  $\overset{\text{Classical}}{x} \xrightarrow{\mathcal{E}} \mathcal{E}_x \longrightarrow |\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_x^{(k)}\rangle$

Bob:  $y \xrightarrow{\mathcal{E}} \mathcal{E}_y \longrightarrow |\varphi_y\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_y^{(k)}\rangle$

# Quantum fingerprinting (and $EQ_N$ )

As in classical case: SMP model and  $f(x,y)=EQ_N(x,y)$

Main idea: Classical procedure + Quantum parallelism

Alice:  $\overset{\text{Classical}}{x} \xrightarrow{\mathcal{E}} \mathcal{E}_x \longrightarrow |\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} \underbrace{|k\rangle}_{\log(cN) \text{ qubits}} \underbrace{|E_x^{(k)}\rangle}_{1 \text{ qubit}} \left. \vphantom{\sum_{k=1}^{cN}} \right\} \begin{array}{l} \text{Send} \\ O(\log cN) \\ \text{qubits} \end{array}$

Bob:  $y \xrightarrow{\mathcal{E}} \mathcal{E}_y \longrightarrow |\varphi_y\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_y^{(k)}\rangle$

Referee:  $|\varphi_x\rangle |\varphi_y\rangle |0\rangle$



# Quantum fingerprinting (and $EQ_N$ )

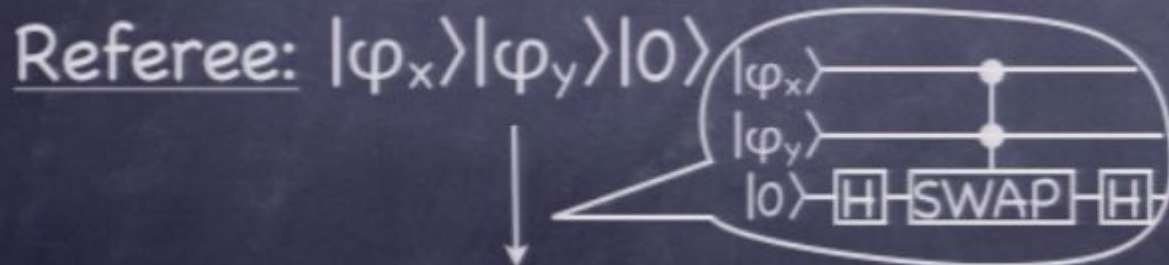
As in classical case: SMP model and  $f(x,y)=EQ_N(x,y)$

Main idea: Classical procedure + Quantum parallelism

Alice:  $\overset{\text{Classical}}{x} \xrightarrow{\mathcal{E}} \mathcal{E}_x \longrightarrow |\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} \overset{\log(cN) \text{ qubits}}{|k\rangle} \overset{1 \text{ qubit}}{|E_x^{(k)}\rangle}$

Bob:  $y \xrightarrow{\mathcal{E}} \mathcal{E}_y \longrightarrow |\varphi_y\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_y^{(k)}\rangle$

} Send  $O(\log cN)$  qubits



# Quantum fingerprinting (and $EQ_N$ )

As in classical case: SMP model and  $f(x,y)=EQ_N(x,y)$

Main idea: Classical procedure + Quantum parallelism

Alice:  $x \xrightarrow{\mathcal{E}} \mathcal{E}_x \longrightarrow |\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_x^{(k)}\rangle$

Bob:  $y \xrightarrow{\mathcal{E}} \mathcal{E}_y \longrightarrow |\varphi_y\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_y^{(k)}\rangle$

Send  $O(\log cN)$  qubits

*Annotations: "Classical" above x; "log(cN) qubits" above the sum index k; "1 qubit" above the state |E\_x^{(k)}\rangle*

Referee:  $|\varphi_x\rangle |\varphi_y\rangle |0\rangle$

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$



# Quantum fingerprinting and $EQ_N$

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

# Quantum fingerprinting and EQ<sub>N</sub>

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

Can measure 1 only if  
 $x \neq y$   
(no error here)



# Quantum fingerprinting and EQ<sub>N</sub>

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

If he measures 0  
he concludes  $x=y$

Can measure 1 only if  
 $x \neq y$   
(no error here)

↓

$$P_{\text{error}} = P(0 | x \neq y)$$

# Quantum fingerprinting and EQ<sub>N</sub>

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

If he measures 0  
he concludes  $x=y$

Can measure 1 only if  
 $x \neq y$   
(no error here)

$$P_{\text{error}} = P(0 | x \neq y) \leq \frac{1}{2(1+\delta^2)} \Rightarrow \text{Error can be reduced to any } \varepsilon > 0 \text{ sending } O(\log(1/\varepsilon))$$



# Quantum fingerprinting and EQ<sub>N</sub>

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

If he measures 0  
he concludes  $x=y$

Can measure 1 only if  
 $x \neq y$   
(no error here)

$$P_{\text{error}} = P(0 | x \neq y) \leq \frac{1}{2(1+\delta^2)} \Rightarrow \text{Error can be reduced to any } \varepsilon > 0 \text{ sending } O(\log(1/\varepsilon))$$

Communication

$$|\varphi_x\rangle \text{ and } |\varphi_y\rangle \rightarrow C_Q(\text{EQ}_N) = O(\log N)$$

# Quantum fingerprinting and EQ<sub>N</sub>

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

If he measures 0  
he concludes  $x=y$

Can measure 1 only if  
 $x \neq y$   
(no error here)

$$P_{\text{error}} = P(0 | x \neq y) \leq \frac{1}{2(1+\delta^2)} \Rightarrow \text{Error can be reduced to any } \varepsilon > 0 \text{ sending } O(\log(1/\varepsilon))$$

## Communication

$|\varphi_x\rangle$  and  $|\varphi_y\rangle \rightarrow C_Q(\text{EQ}_N) = O(\log N)$

Remember:  $C_C(\text{EQ}_N) = O(\sqrt{N})$  (optimal)



# Quantum fingerprinting and $EQ_N$

Referee measures the first qubit of

$$[|0\rangle(|\varphi_x\rangle|\varphi_y\rangle + |\varphi_y\rangle|\varphi_x\rangle) + |1\rangle(|\varphi_x\rangle|\varphi_y\rangle - |\varphi_y\rangle|\varphi_x\rangle)]/2$$

If he measures 0  
he concludes  $x=y$

Can measure 1 only if  
 $x \neq y$   
(no error here)

$$P_{\text{error}} = P(0 | x \neq y) \leq \frac{1}{2(1+\delta^2)} \Rightarrow \text{Error can be reduced to any } \varepsilon > 0 \text{ sending } O(\log(1/\varepsilon))$$

Communication

$|\varphi_x\rangle$  and  $|\varphi_y\rangle \rightarrow C_Q(EQ_N) = O(\log N)$

Remember:  $C_C(EQ_N) = O(\sqrt{N})$  (optimal)

EXPONENTIAL  
GAP

# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- 1) A
  - applies  $\mathcal{E}$  to  $x$
  - describes state  $|\varphi_x\rangle$
  - sends the description  
( $K(|\varphi_x\rangle)$  bits)



# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- |  |  |
|--|--|
| <p>1) A • applies <math>\mathcal{E}</math> to <math>x</math></p> <ul style="list-style-type: none"><li>• describes state <math> \varphi_x\rangle</math></li><li>• sends the description<br/>(<math>K( \varphi_x\rangle)</math> bits)</li></ul> | <p>2) B • applies <math>\mathcal{E}</math> to <math>y</math></p> <ul style="list-style-type: none"><li>• describes state <math> \varphi_y\rangle</math></li><li>• sends the description<br/>(<math>K( \varphi_y\rangle)</math> bits)</li></ul> |
|--|--|

# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- 1) A • applies  $\mathcal{E}$  to  $x$ 
  - describes state  $|\varphi_x\rangle$
  - sends the description  $(K(|\varphi_x\rangle))$  bits
- 2) B • applies  $\mathcal{E}$  to  $y$ 
  - describes state  $|\varphi_y\rangle$
  - sends the description  $(K(|\varphi_y\rangle))$  bits
- 3) Referee classically simulates the quantum circuit



# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- |   |   |
|---|---|
| 1) A • applies $\mathcal{E}$ to $x$                       | 2) B • applies $\mathcal{E}$ to $y$                       |
| • describes state $ \varphi_x\rangle$                     | • describes state $ \varphi_y\rangle$                     |
| • sends the description<br>( $K( \varphi_x\rangle)$ bits) | • sends the description<br>( $K( \varphi_y\rangle)$ bits) |

3) Referee classically simulates the quantum circuit

Communication (classical):

$K(|\varphi_x\rangle) + K(|\varphi_y\rangle)$  bits

# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- |   |   |
|---|---|
| 1) A • applies $\mathcal{E}$ to $x$ <ul style="list-style-type: none"><li>• describes state <math> \varphi_x\rangle</math></li><li>• sends the description<br/>(<math>K( \varphi_x\rangle)</math> bits)</li></ul> | 2) B • applies $\mathcal{E}$ to $y$ <ul style="list-style-type: none"><li>• describes state <math> \varphi_y\rangle</math></li><li>• sends the description<br/>(<math>K( \varphi_y\rangle)</math> bits)</li></ul> |
|---|---|

3) Referee classically simulates the quantum circuit

Communication (classical):

$K(|\varphi_x\rangle) + K(|\varphi_y\rangle)$  bits

Classical optimal:

$$C_C(EQ_N) = O(\sqrt{N})$$



# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- |   |   |
|---|---|
| 1) A • applies $\mathcal{E}$ to $x$ <ul style="list-style-type: none"><li>• describes state <math> \varphi_x\rangle</math></li><li>• sends the description<br/>(<math>K( \varphi_x\rangle)</math> bits)</li></ul> | 2) B • applies $\mathcal{E}$ to $y$ <ul style="list-style-type: none"><li>• describes state <math> \varphi_y\rangle</math></li><li>• sends the description<br/>(<math>K( \varphi_y\rangle)</math> bits)</li></ul> |
|---|---|

3) Referee classically simulates the quantum circuit

Communication (classical):

$K(|\varphi_x\rangle) + K(|\varphi_y\rangle)$  bits

Classical optimal:

$C_C(EQ_N) = O(\sqrt{N})$

$$K(|\varphi_x\rangle) + K(|\varphi_y\rangle) \geq O(\sqrt{N})$$

# An insight on Kolmogorov complexity

Classical implementation of the quantum protocol for  $EQ_N$

- 1) A • applies  $\mathcal{E}$  to  $x$ 
  - describes state  $|\varphi_x\rangle$
  - sends the description ( $K(|\varphi_x\rangle)$  bits)
- 2) B • applies  $\mathcal{E}$  to  $y$ 
  - describes state  $|\varphi_y\rangle$
  - sends the description ( $K(|\varphi_y\rangle)$  bits)

3) Referee classically simulates the quantum circuit

Communication (classical):

$K(|\varphi_x\rangle) + K(|\varphi_y\rangle)$  bits

Classical optimal:

$C_C(EQ_N) = O(\sqrt{N})$

$O(\log N \text{ qubits})$

$$K(|\varphi_x\rangle) + K(|\varphi_y\rangle) \geq O(\sqrt{N})$$



Exponential growth



# Condition on Kolmogorov complexity

If quantum Kolmogorov complexity measure the number of bits needed to classically describe a state in such a way that it can be reproduced



It must grow exponentially with the number of qubits

# Condition on Kolmogorov complexity

If quantum Kolmogorov complexity measure the number of bits needed to classically describe a state in such a way that it can be reproduced



It must grow exponentially with the number of qubits

→ Recall: two definitions for complexity based on classical information(bits):

Quantum Turing machine:  $K_Q(|\varphi\rangle)$

Quantum circuit:  $K_{Net}^\epsilon(|\varphi\rangle)$



# Condition on Kolmogorov complexity

If quantum Kolmogorov complexity measure the number of bits needed to classically describe a state in such a way that it can be reproduced



It must grow exponentially with the number of qubits

→ Recall: two definitions for complexity based on classical information(bits):

Quantum Turing machine:  $K_Q(|\varphi\rangle) \lesssim 2N$

Quantum circuit:  $K_{\text{Net}}^\epsilon(|\varphi\rangle) \lesssim 2^N \log(1/\epsilon)$

# Condition on Kolmogorov complexity

If quantum Kolmogorov complexity measure the number of bits needed to classically describe a state in such a way that it can be reproduced



It must grow exponentially with the number of qubits

→ Recall: two definitions for complexity based on classical information(bits):

Quantum Turing machine:  $K_Q(|\varphi\rangle) \lesssim 2^N$

Quantum circuit:  $K_{\text{Net}}^\epsilon(|\varphi\rangle) \lesssim 2^N \log(1/\epsilon)$



# Condition on Kolmogorov complexity

If quantum Kolmogorov complexity measure the number of bits needed to classically describe a state in such a way that it can be reproduced



It must grow exponentially with the number of qubits

→ Recall: two definitions for complexity based on classical information(bits):

Quantum Turing machine:  $K_Q(|\varphi\rangle) \lesssim 2^N$

Quantum circuit:  $K_{Net}^\epsilon(|\varphi\rangle) \lesssim 2^N \log(1/\epsilon)$

Note: one should include error ( $\epsilon$ ) in previous protocol!  
Does not change the result ( $\epsilon$  independent of  $N$ )

# "Network" complexity: the idea

Alice wants to send a state to Bob, but has only a classical channel  $\Rightarrow$  she can explain how to prepare it!

They had previously agreed

1) to use the same "toolbox" to prepare their states;

2) to use the same words when referring to the same elements in the toolbox




# "Network" complexity: the idea

Alice wants to send a state to Bob, but has only a classical channel  $\Rightarrow$  she can explain how to prepare it!

They had previously agreed

1) to use the same "toolbox" to prepare their states;

 A complete and finite gate basis

2) to use the same words when referring to the same elements in the toolbox




A code: i.e. a "law" that associates a letter to each gate (or set of gates)

# "Network" complexity: the idea

Alice wants to send a state to Bob, but has only a classical channel  $\Rightarrow$  she can explain how to prepare it!

They had previously agreed


1) to use the same "toolbox" to prepare their states;

 A complete and finite gate basis

2) to use the same words when referring to the same elements in the toolbox



A code: i.e. a "law" that associates a letter to each gate (or set of gates)

 Alice only has to send to Bob the (classical) word that codes the circuit

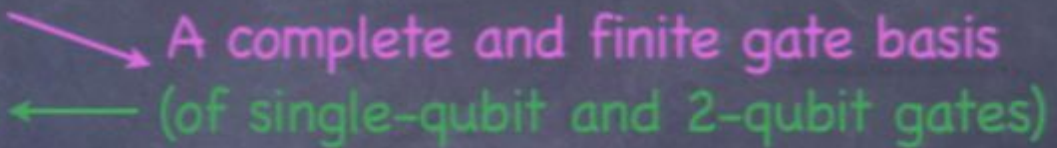


# "Network" complexity: the idea


Alice wants to send a state to Bob, but has only a classical channel  $\Rightarrow$  she can explain how to prepare it!

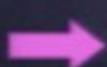
They had previously agreed

1) to use the same "toolbox" to prepare their states;

  
Invariance under basis change  $\leftarrow$  (of single-qubit and 2-qubit gates)

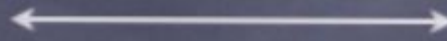
2) to use the same words when referring to the same elements in the toolbox

  
A code: i.e. a "law" that associates a letter to each gate (or set of gates)

 Alice only has to send to Bob the (classical) word that codes the circuit

# Network complexity: construction

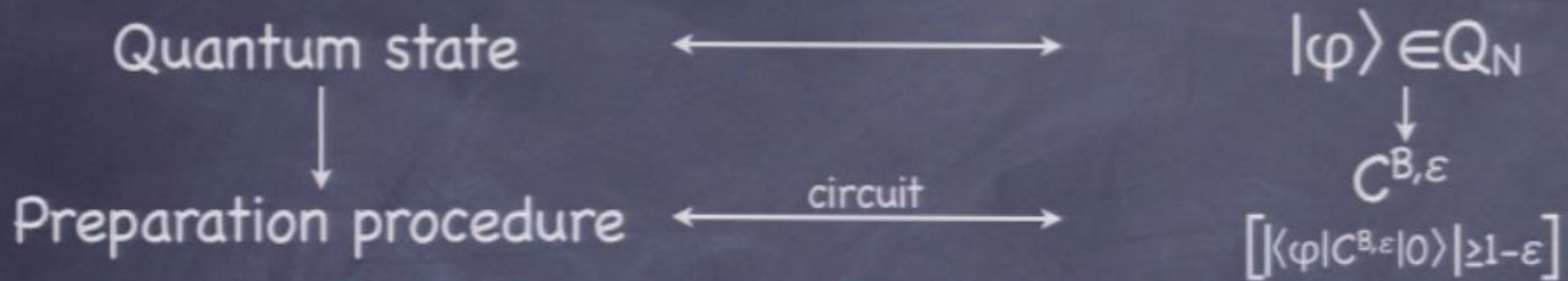
Quantum state



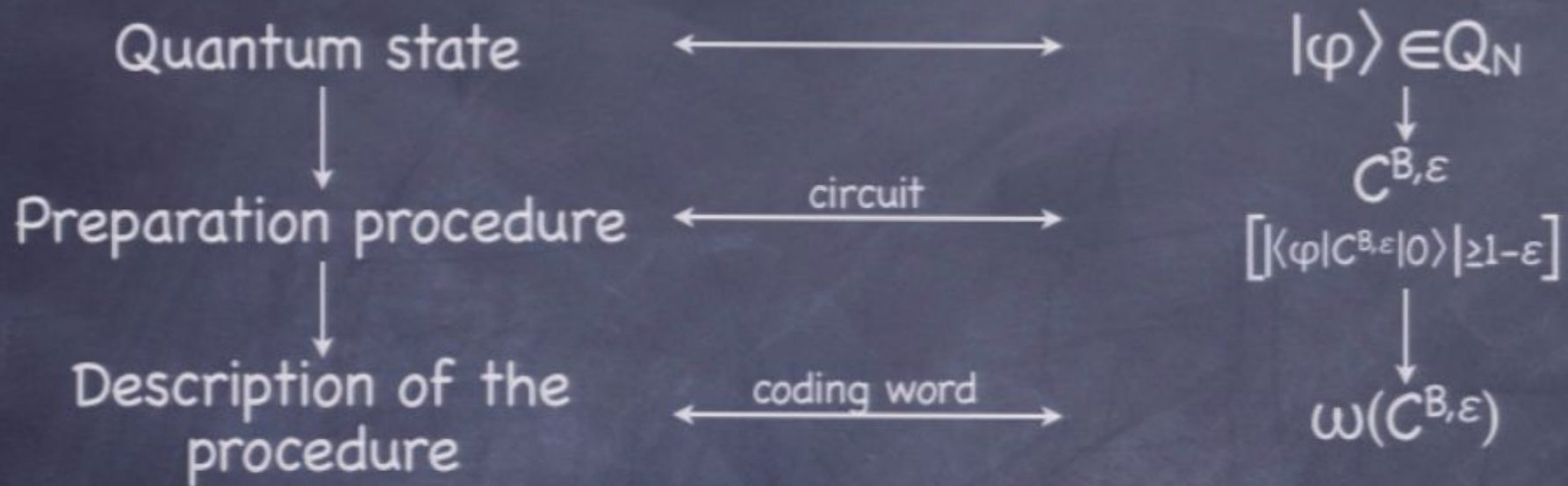
$|\varphi\rangle \in Q_N$



# Network complexity: construction

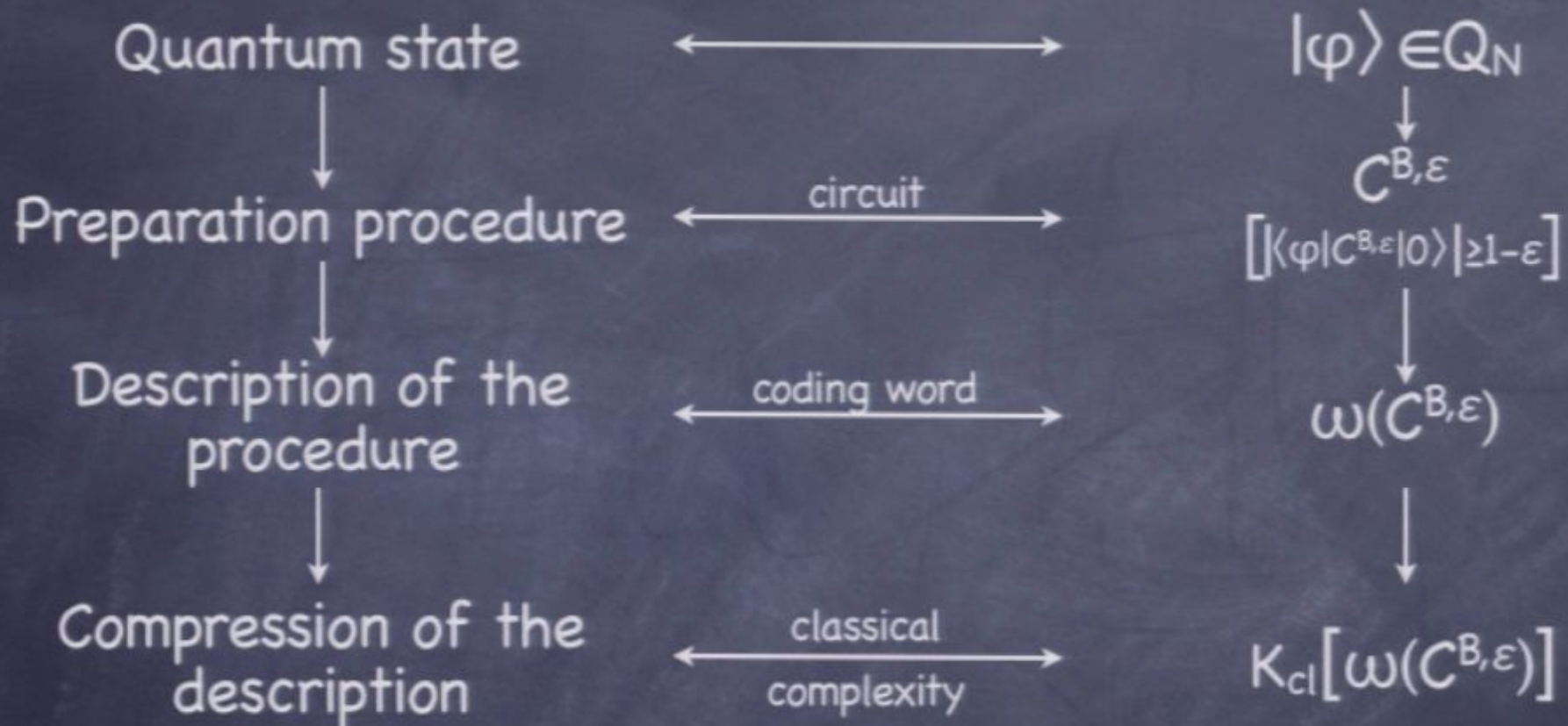


# Network complexity: construction

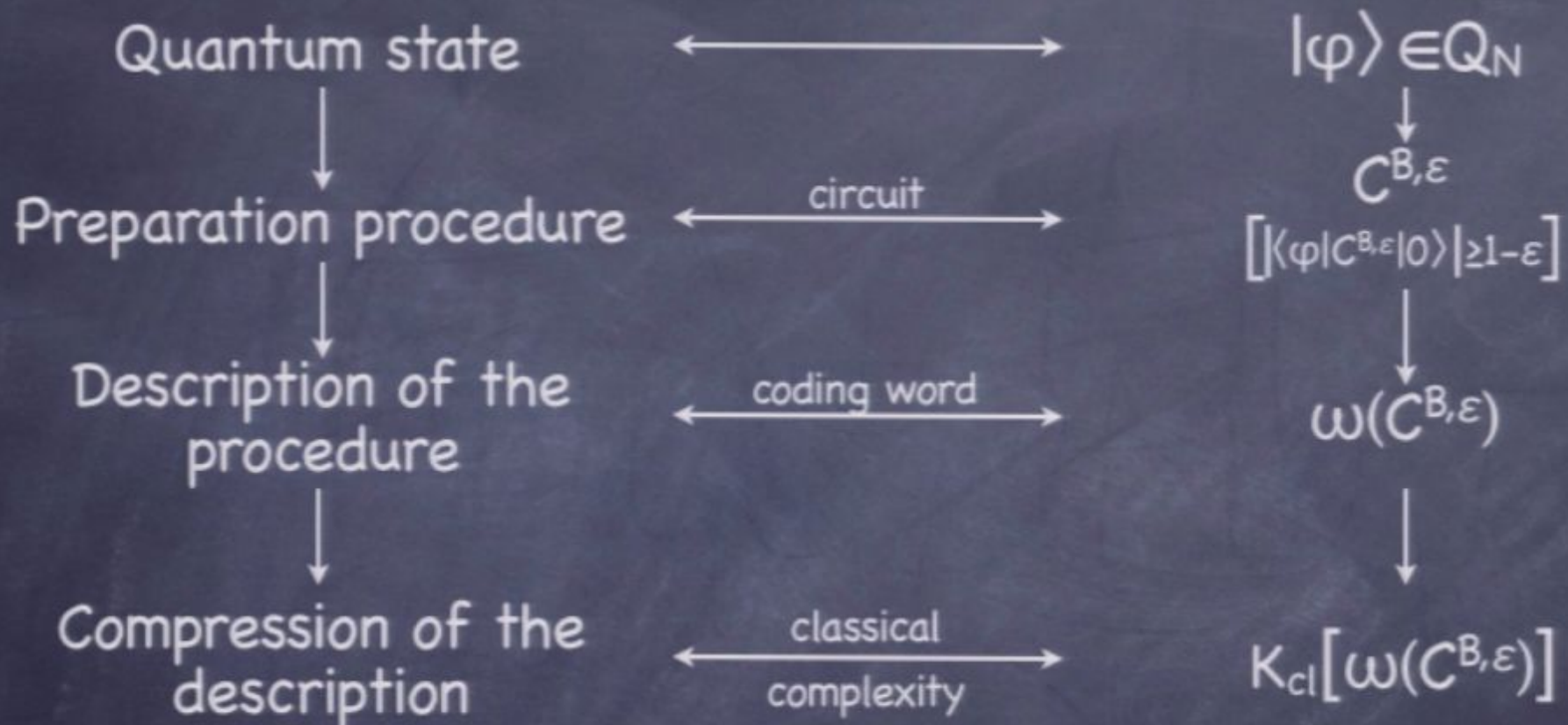




# Network complexity: construction



# Network complexity: construction



There could be more circuits that prepare the state with the required precision:  $K_{Net}^{B,\varepsilon}(|\varphi\rangle) = \min K_{cl}[\omega(C^{B,\varepsilon})]$



# Network complexity and precision

How do we explain the dependence of  $K_{\text{Net}}^{B,\varepsilon}$  on  $N$  and  $\varepsilon$ ?

# Network complexity and precision

How do we explain the dependence of  $K_{\text{Net}}^{B,\varepsilon}$  on  $N$  and  $\varepsilon$ ?

- The action of any unitary on  $|0\rangle$  can be implemented with precision  $\varepsilon$  using  $O(2^N \log(1/\varepsilon))$  gates from a fixed basis\*



# Network complexity and precision

How do we explain the dependence of  $K_{\text{Net}}^{B,\varepsilon}$  on  $N$  and  $\varepsilon$ ?

- The action of any unitary on  $|0\rangle$  can be implemented with precision  $\varepsilon$  using  $O(2^N \log(1/\varepsilon))$  gates from a fixed basis\*
- Length of the coding word  $\sim$  number of gates

$$|\varphi\rangle \in Q_N \Rightarrow K_{\text{Net}}^{B,\varepsilon}(|\varphi\rangle) \lesssim 2^N \log(1/\varepsilon)$$

Very different from the classical case, but not so strange

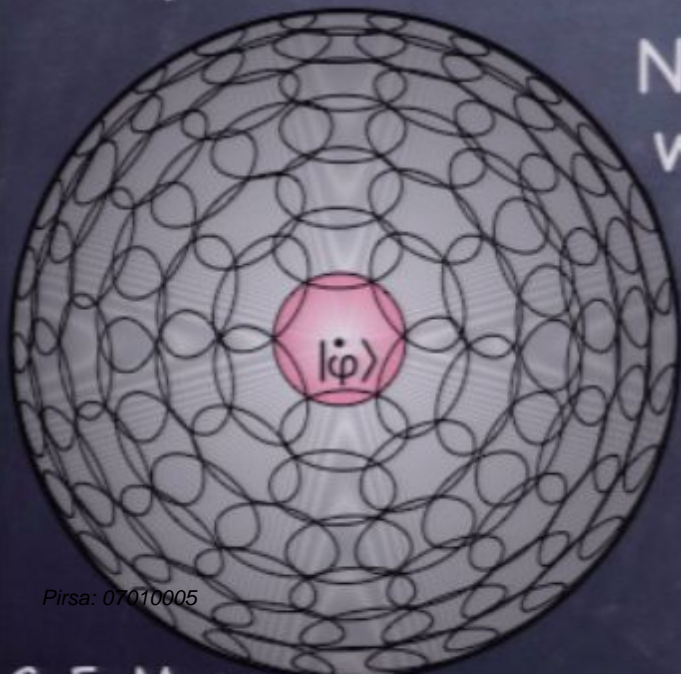
# Network complexity and precision

How do we explain the dependence of  $K_{\text{Net}}^{B,\varepsilon}$  on  $N$  and  $\varepsilon$ ?

- The action of any unitary on  $|0\rangle$  can be implemented with precision  $\varepsilon$  using  $O(2^N \log(1/\varepsilon))$  gates from a fixed basis\*
- Length of the coding word  $\sim$  number of gates

$$|\varphi\rangle \in Q_N \Rightarrow K_{\text{Net}}^{B,\varepsilon}(|\varphi\rangle) \lesssim 2^N \log(1/\varepsilon)$$

Very different from the classical case, but not so strange



Normalized state  
with precision  $\varepsilon$

↔ "Patch" on a  $2^N$ -dim  
hypersphere



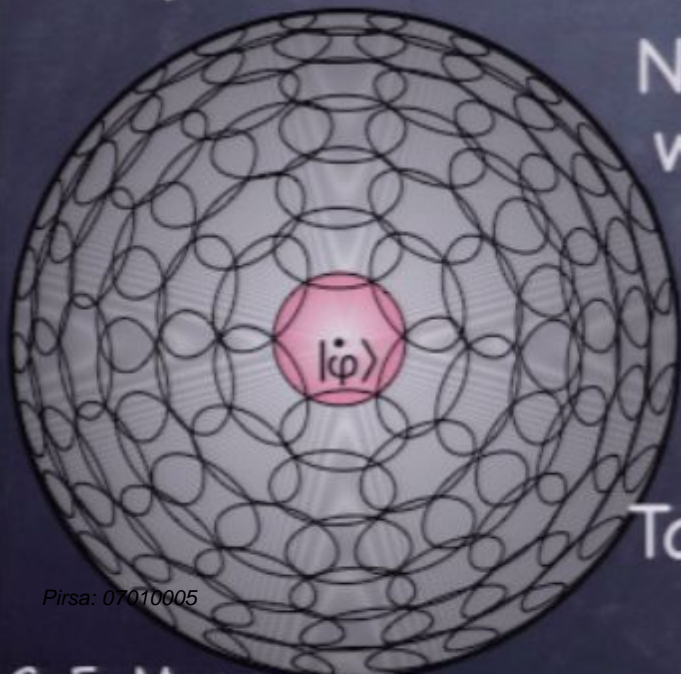
# Network complexity and precision

How do we explain the dependence of  $K_{\text{Net}}^{B,\varepsilon}$  on  $N$  and  $\varepsilon$ ?

- The action of any unitary on  $|0\rangle$  can be implemented with precision  $\varepsilon$  using  $O(2^N \log(1/\varepsilon))$  gates from a fixed basis\*
- Length of the coding word  $\sim$  number of gates

$$|\varphi\rangle \in Q_N \Rightarrow K_{\text{Net}}^{B,\varepsilon}(|\varphi\rangle) \lesssim 2^N \log(1/\varepsilon)$$

Very different from the classical case, but not so strange



Normalized state with precision  $\varepsilon$   $\longleftrightarrow$  "Patch" on a  $2^N$ -dim hypersphere

There are  $V^{-1} \sim 2^N \varepsilon^{2N+1}$  such patches



To specify one we need  $\log V^{-1} \sim 2^N \log(1/\varepsilon)$

# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$



# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$

$$|0\rangle \text{---} [U_1] \text{---} |\varphi_1\rangle$$

$$|0\rangle \text{---} [U_2] \text{---} |\varphi_2\rangle$$

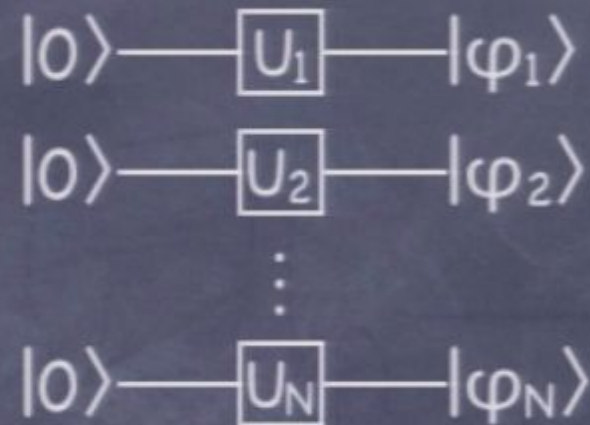
$$\vdots$$

$$|0\rangle \text{---} [U_N] \text{---} |\varphi_N\rangle$$

# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim N \log(1/\varepsilon)$$





# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim N \log(1/\varepsilon)$$

The absence of entanglement  
re-establishes the classical  
bound!

# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim N \log(1/\varepsilon)$$

The absence of entanglement  
re-establishes the classical  
bound!

More general:  $|\phi\rangle$  separable with respect to some partition

$$|\phi\rangle = |\varphi_1\rangle \otimes \cdots \otimes |\varphi_N\rangle; |\varphi_j\rangle \in Q_{N_j}; \sum_j N_j = N$$



# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim N \log(1/\varepsilon)$$

The absence of entanglement  
re-establishes the classical  
bound!

More general:  $|\phi\rangle$  separable with respect to some partition

$$|\phi\rangle = |\varphi_1\rangle \otimes \cdots \otimes |\varphi_N\rangle; |\varphi_j\rangle \in Q_{N_j}; \sum_j N_j = N$$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim \sum_j 2^{N_j} \log(J/\varepsilon)$$

# Entanglement and complexity

Consider a fully separable state:  $|\phi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_N\rangle$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim N \log(1/\varepsilon)$$

The absence of entanglement  
re-establishes the classical  
bound!

More general:  $|\phi\rangle$  separable with respect to some partition

$$|\phi\rangle = |\varphi_1\rangle \otimes \cdots \otimes |\varphi_N\rangle; |\varphi_j\rangle \in Q_{N_j}; \sum_j N_j = N$$

$$K_{\text{Net}}^{B,\varepsilon}(|\phi\rangle) \lesssim \sum_j 2^{N_j} \log(J/\varepsilon)$$

Only a truly N-party  
entangled state can have  
maximal complexity



# Schmidt measure of entanglement

Consider an  $n$ -partite quantum system with parties  $A_1, \dots, A_n$

Any state  $|\phi\rangle$  in such space can be written as:

$$|\phi\rangle = \sum_j \alpha_j |\varphi_1^{(j)}\rangle \otimes |\varphi_2^{(j)}\rangle \otimes \dots \otimes |\varphi_n^{(j)}\rangle$$

# Schmidt measure of entanglement

Consider an  $n$ -partite quantum system with parties  $A_1, \dots, A_n$

Any state  $|\phi\rangle$  in such space can be written as:

$$|\phi\rangle = \sum_1^R \alpha_j |\varphi_1^{(j)}\rangle \otimes |\varphi_2^{(j)}\rangle \otimes \dots \otimes |\varphi_n^{(j)}\rangle$$

Let  $r$  be the minimum number of terms  $R$  needed to write such a decomposition for  $|\phi\rangle$ , then

**Def:** The Schmidt measure\* of  $|\phi\rangle$  is  $E_s(|\phi\rangle) = \log r$



# Schmidt measure of entanglement

Consider an  $n$ -partite quantum system with parties  $A_1, \dots, A_n$

Any state  $|\phi\rangle$  in such space can be written as:

$$|\phi\rangle = \sum_1^R \alpha_j |\varphi_1^{(j)}\rangle \otimes |\varphi_2^{(j)}\rangle \otimes \dots \otimes |\varphi_n^{(j)}\rangle$$

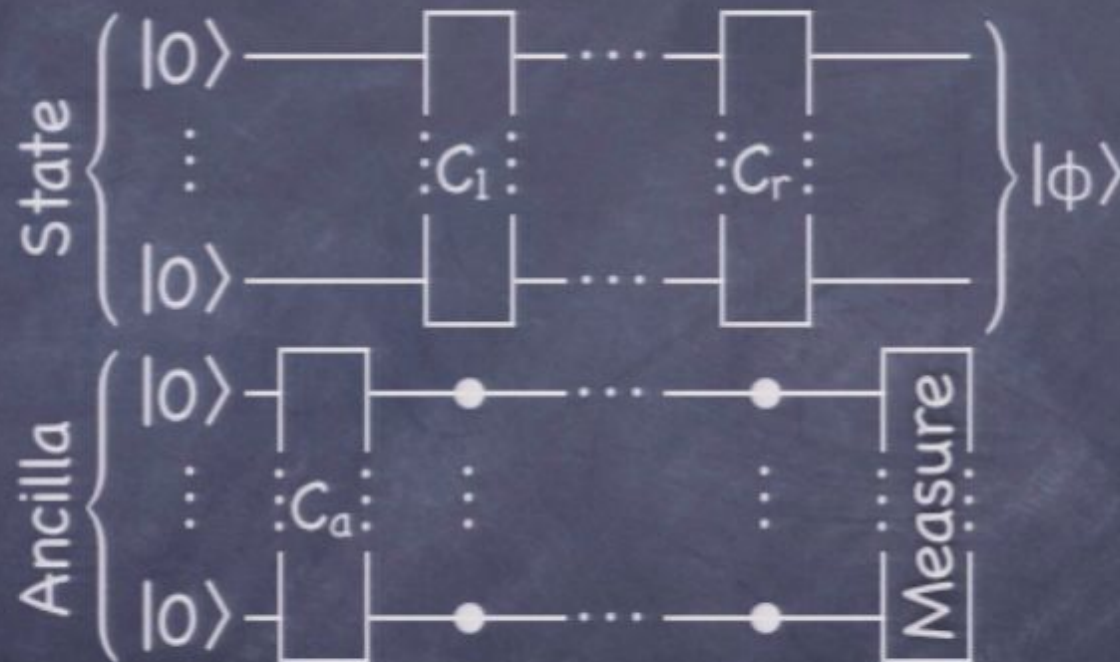
Let  $r$  be the minimum number of terms  $R$  needed to write such a decomposition for  $|\phi\rangle$ , then

**Def:** The Schmidt measure\* of  $|\phi\rangle$  is  $E_S(|\phi\rangle) = \log r$

Considering the minimal partition (each party has one qubit) there is a relation between  $E_S(|\phi\rangle)$  and  $K_{\text{Net}}^{B,\epsilon}(|\phi\rangle)$

# Complexity and Schmidt measure

And we have:

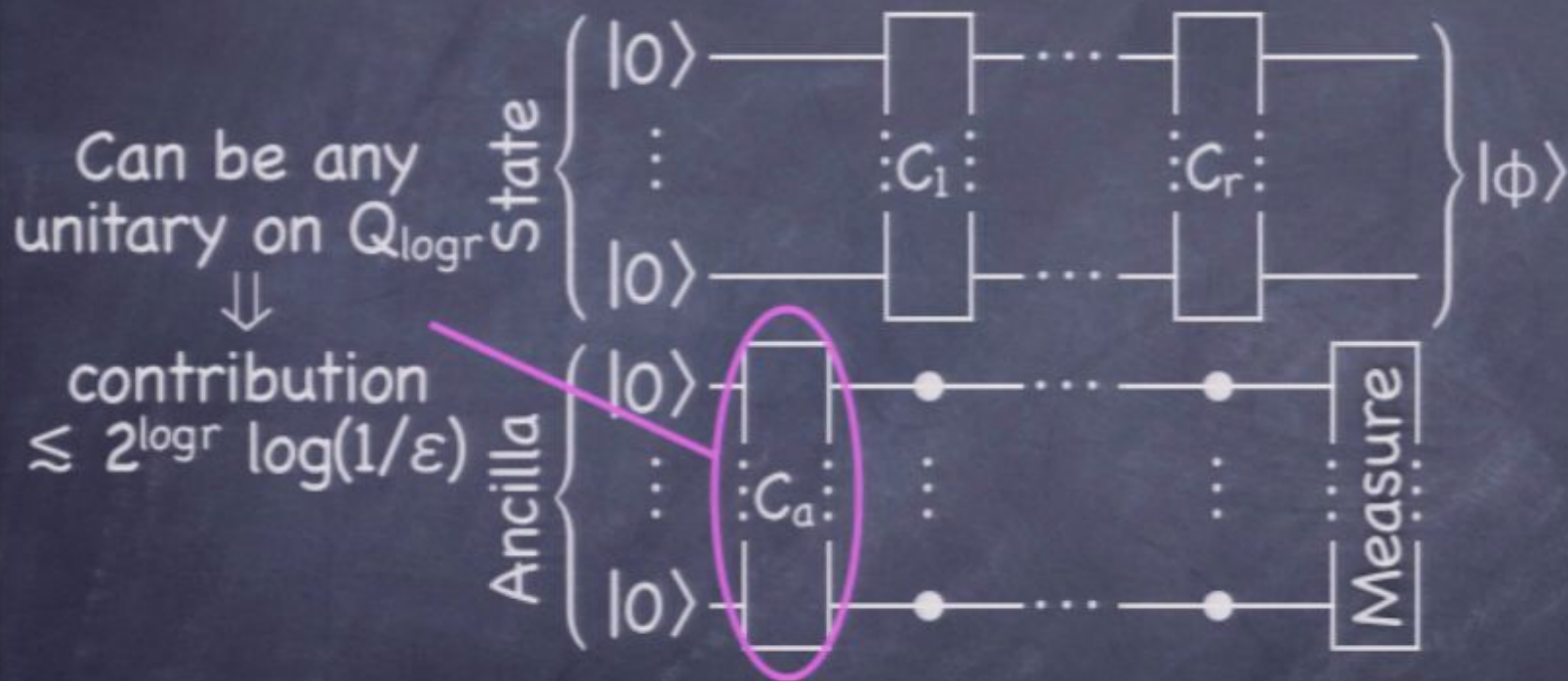


$$K_{\text{Net}}^{B, \epsilon} \lesssim$$



# Complexity and Schmidt measure

And we have:

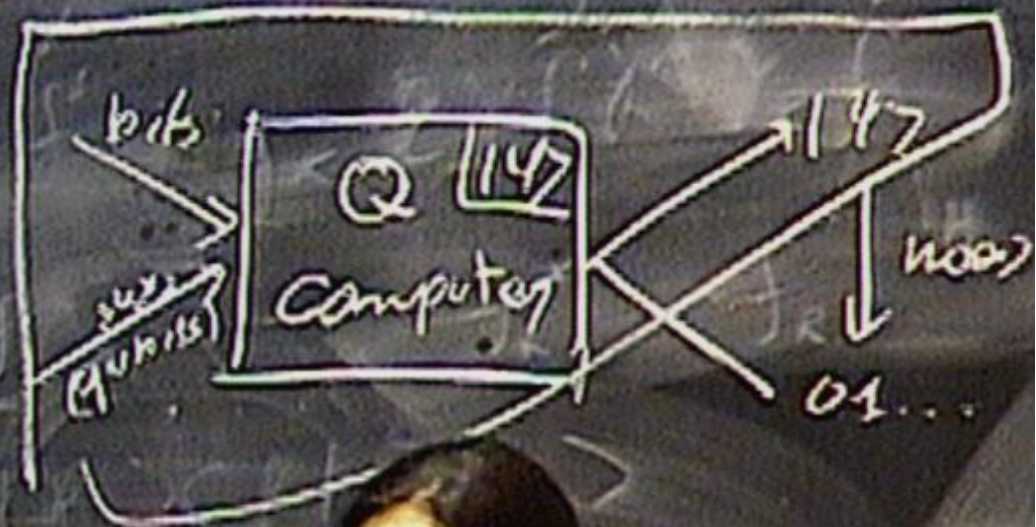


$$K_{\text{Net}}^{B, \epsilon} \lesssim$$



$$|\Phi\rangle = \sum_i \alpha_i |\varphi_i\rangle$$

$$|a\rangle = \sum_i \alpha_i |i\rangle$$

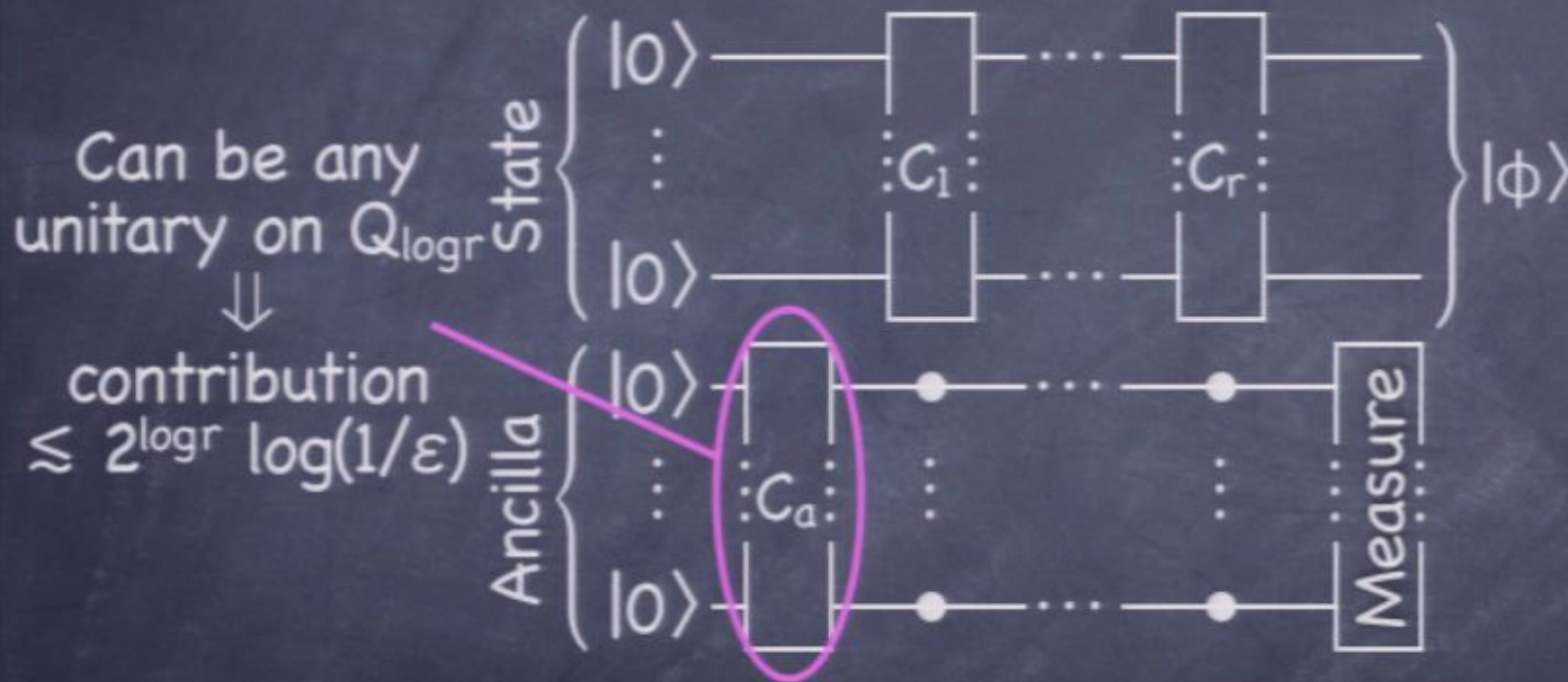


$$K(|\varphi\rangle) = \min_p (p) - \log |\langle \varphi |$$



# Complexity and Schmidt measure

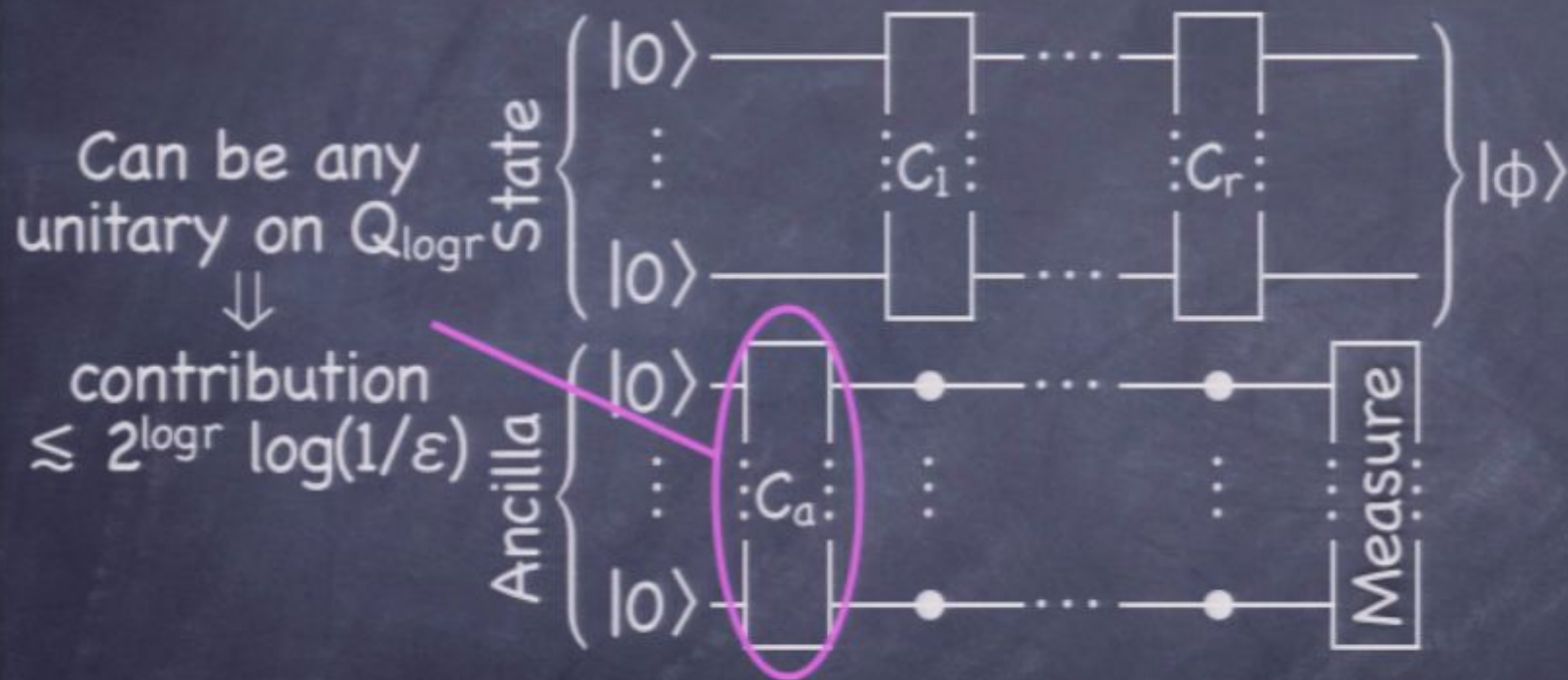
And we have:



$$K_{\text{Net}}^{B, \epsilon} \lesssim$$

# Complexity and Schmidt measure

And we have:

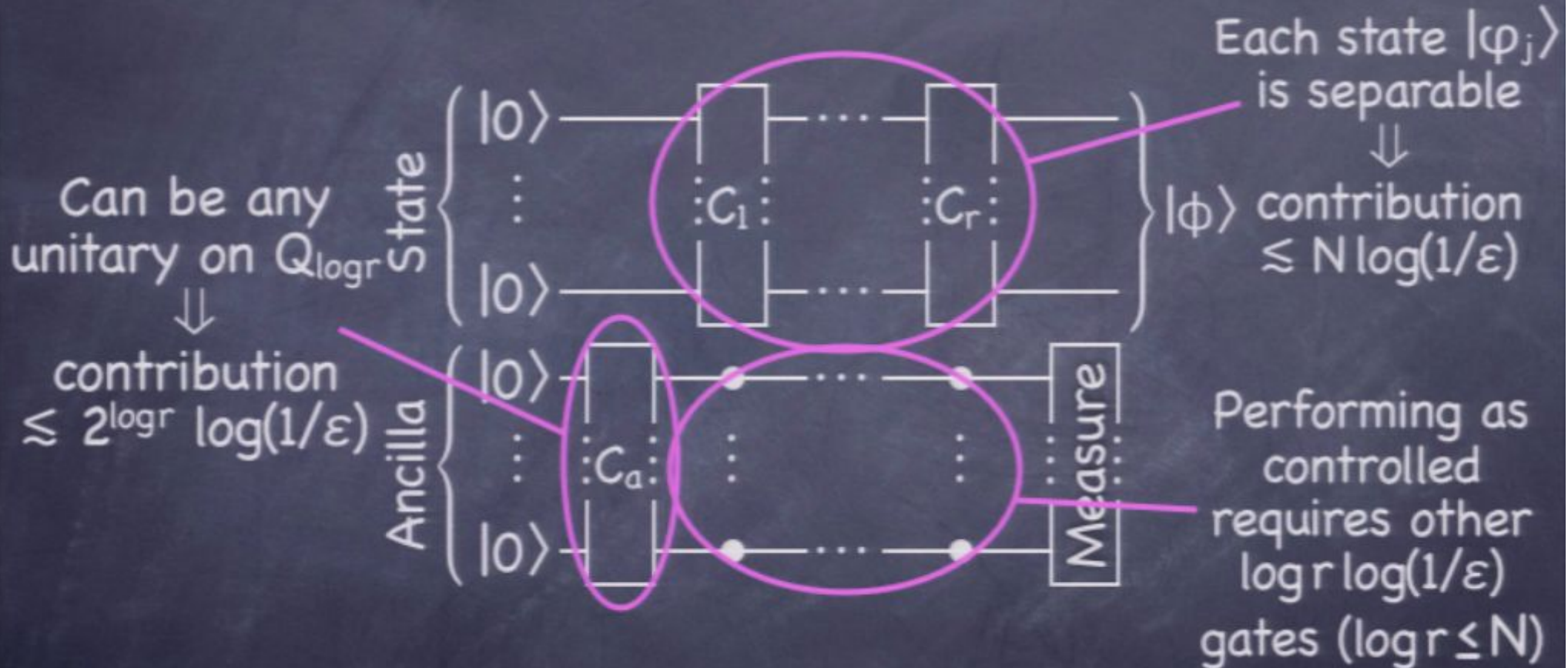


$$K_{\text{Net}}^{B, \epsilon} \lesssim r \log(1/\epsilon)$$



# Complexity and Schmidt measure

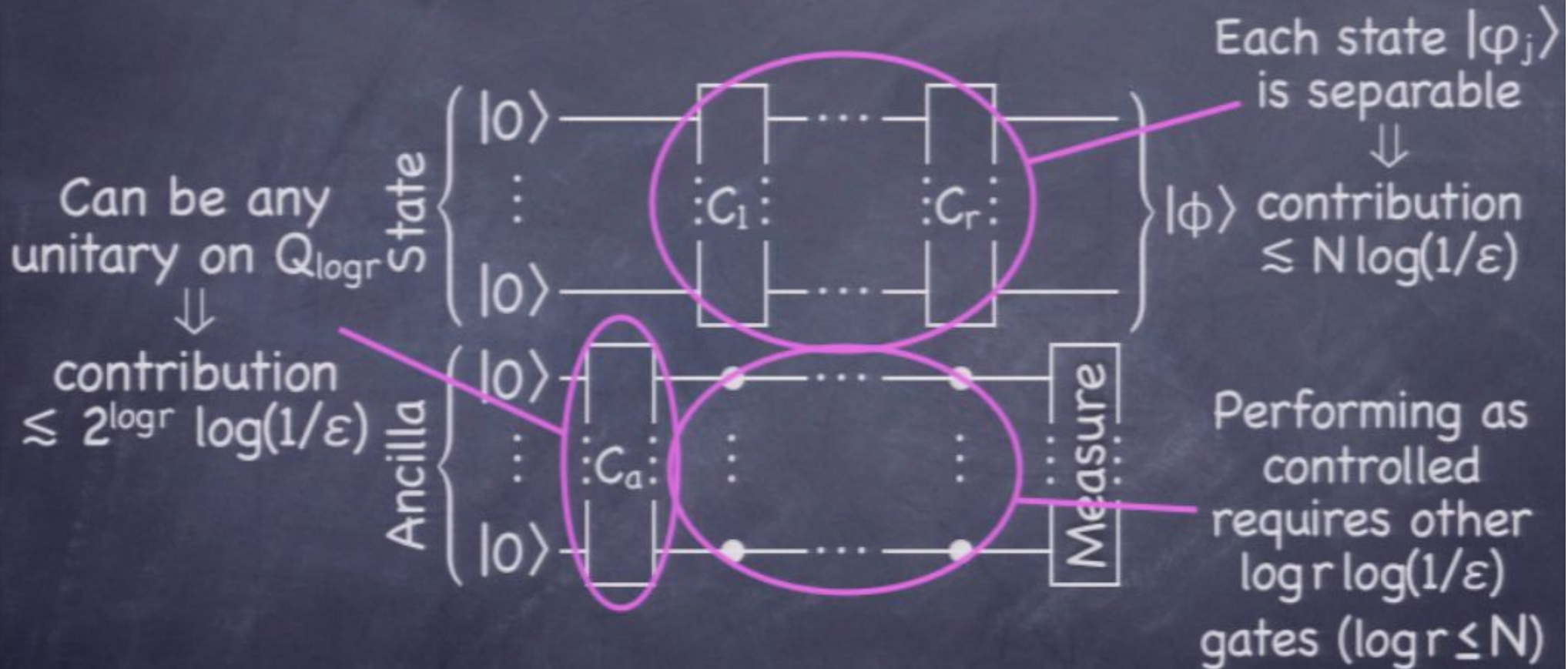
And we have:



$$K_{\text{Net}}^{B, \epsilon} \lesssim r \log(1/\epsilon) + N r \log(1/\epsilon) + N r \log(1/\epsilon) \approx 2Nr \log(1/\epsilon)$$

# Complexity and Schmidt measure

And we have:



$$K_{\text{Net}}^{B, \epsilon} \lesssim r \log(1/\epsilon) + N r \log(1/\epsilon) + N r \log(1/\epsilon) \approx 2Nr \log(1/\epsilon)$$



$$|\Phi\rangle = \sum_i \alpha_i |\varphi_i\rangle$$

$$|a\rangle = \sum_i \beta_i |i\rangle$$

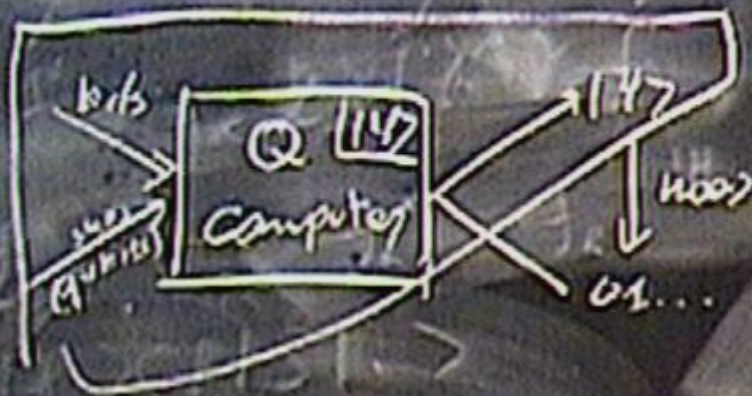


$$K(|\varphi\rangle) = \min_P \left\{ -\log |\langle \varphi | \varphi \rangle| U(P|\varphi) = 1 \right. \\ \left. = |\varphi\rangle \right\}$$



$$|\Phi\rangle = \sum_i \alpha_i |\varphi_i\rangle$$

$$|a\rangle = \sum_i \beta_i |i\rangle$$

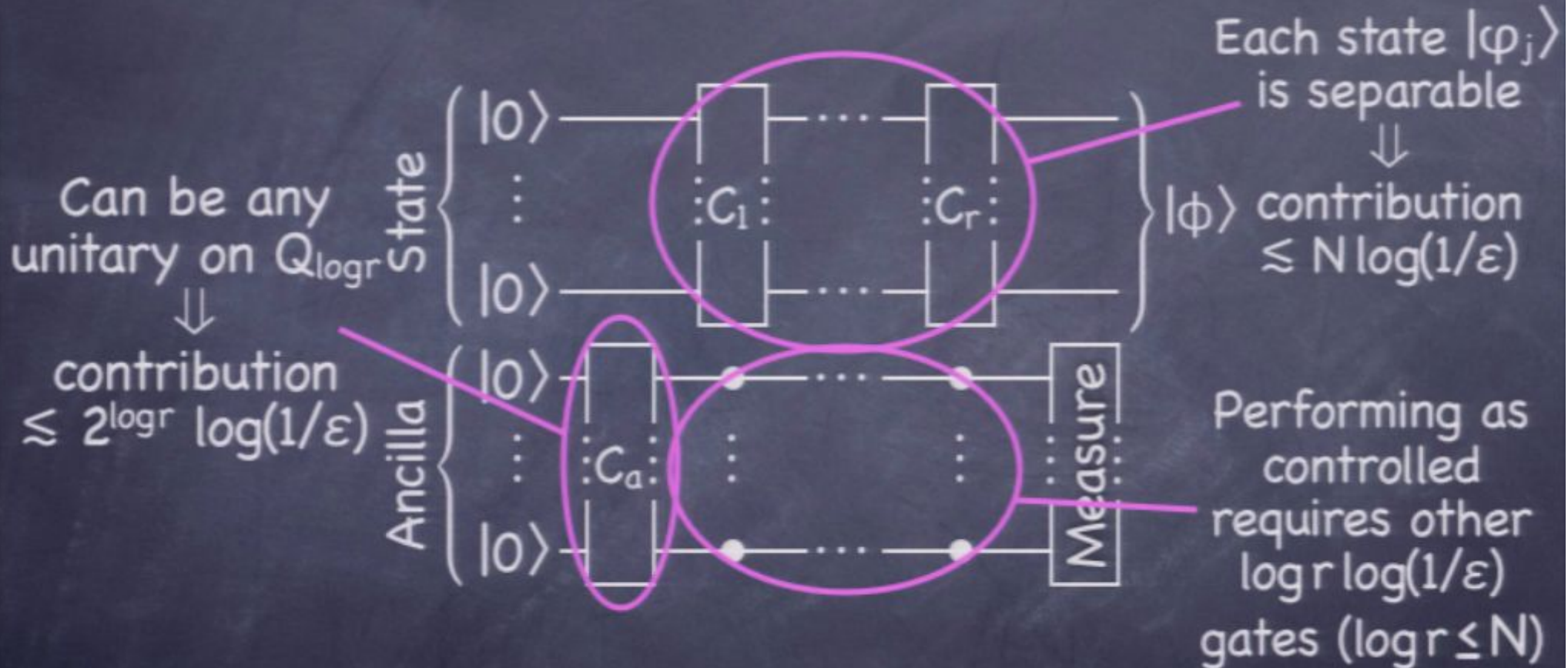


$$K(|\varphi\rangle) = \min_p \left\{ \ell(p) - \log |\langle \varphi | \varphi \rangle| \mathcal{U}(p | \langle \varphi | \varphi \rangle) = 1 \right\}$$



# Complexity and Schmidt measure

And we have:



$$K_{\text{Net}}^{B, \epsilon} \lesssim r \log(1/\epsilon) + N r \log(1/\epsilon) + N r \log(1/\epsilon) \approx 2Nr \log(1/\epsilon)$$

# Relation between complexities

## (...Kolmogorov and communication I...)

...quantum Kolmogorov complexity properties lead to results in communication complexity theory...



$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$$

$$|a\rangle = \sum_i |i\rangle$$

$$K(|\psi\rangle) = \min_p \left\{ \ell(p) - \log |\langle \psi | \psi \rangle| U(p | \psi) \right\}$$

$$= |\psi\rangle$$



# Relation between complexities

## (...Kolmogorov and communication I...)

...quantum Kolmogorov complexity properties lead to results in communication complexity theory...



# Relation between complexities

## (...Kolmogorov and communication I...)

...quantum Kolmogorov complexity properties lead to results in communication complexity theory...

- The Kolmogorov complexity of a state is at most exponential in the number of qubits
  - ➔ Gap between quantum and classical communication complexity is at most exponential  
(Recall: classical simulation)

# Relation between complexities

## (...Kolmogorov and communication I...)

...quantum Kolmogorov complexity properties lead to results in communication complexity theory...

- The Kolmogorov complexity of a state is at most exponential in the number of qubits
  - ➔ Gap between quantum and classical communication complexity is at most exponential  
(Recall: classical simulation)
- Only a highly entangled state can be maximally complex



# Relation between complexities (...Kolmogorov and communication II...)

...and results from communication complexity theory give insight on Kolmogorov complexity...

Recall: Exponential gap between  $C_C$  and  $C_Q$  due to the fact that complex states are sent (else the quantum protocol could be easily implemented classically)

# Relation between complexities

## (...Kolmogorov and communication II...)

...and results from communication complexity theory give insight on Kolmogorov complexity...

Recall: Exponential gap between  $C_C$  and  $C_Q$  due to the fact that complex states are sent (else the quantum protocol could be easily implemented classically)

EQ<sub>N</sub>: exponential quantum/classical gap

states of the form:  $|\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_x^{(k)}\rangle$



# Relation between complexities

## (...Kolmogorov and communication II...)

...and results from communication complexity theory give insight on Kolmogorov complexity...

Recall: Exponential gap between  $C_C$  and  $C_Q$  due to the fact that complex states are sent (else the quantum protocol could be easily implemented classically)

EQ<sub>N</sub>: exponential quantum/classical gap

states of the form:  $|\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_x^{(k)}\rangle$

→  
 $\exists$  complex state  
of this form  
(first example)

# Relation between complexities

## (...Kolmogorov and communication II...)

...and results from communication complexity theory give insight on Kolmogorov complexity...

Recall: Exponential gap between  $C_C$  and  $C_Q$  due to the fact that complex states are sent (else the quantum protocol could be easily implemented classically)

EQ<sub>N</sub>: exponential quantum/classical gap

states of the form:  $|\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_x^{(k)}\rangle$

→  
 $\exists$  complex state  
of this form  
(first example)



# Relation between complexities

## (...Kolmogorov and communication II...)

...and results from communication complexity theory give insight on Kolmogorov complexity...

Recall: Exponential gap between  $C_C$  and  $C_Q$  due to the fact that complex states are sent (else the quantum protocol could be easily implemented classically)

EQ<sub>N</sub>: exponential quantum/classical gap

states of the form:  $|\varphi_x\rangle = \frac{1}{\sqrt{cN}} \sum_{k=1}^{cN} |k\rangle |E_x^{(k)}\rangle$

Note: Same idea (classical simulation of quantum protocol) can be used to prove:  $K_{Net}^{B,\epsilon}(|\varphi_x\rangle) \sim K(x)$

$\exists$  complex state of this form (first example)

# Relation between complexities

## (...Kolmogorov and computation...)

Computation complexity measures the time needed by a computer to find the solution to a problem with input of size  $n$

**Big question:** how much faster are quantum computers?



# Relation between complexities

## (...Kolmogorov and computation...)

Computation complexity measures the time needed by a computer to find the solution to a problem with input of size  $n$

**Big question:** how much faster are quantum computers?  
What we knew (in 12 words): only using entanglement a quantum computer has a chance to be exponentially faster\*!

# Relation between complexities

## (...Kolmogorov and computation...)

Computation complexity measures the time needed by a computer to find the solution to a problem with input of size  $n$

**Big question:** how much faster are quantum computers?  
What we knew (in 12 words): only using entanglement a quantum computer has a chance to be exponentially faster\*!

We can contribute too! all states that appear in the computation must have complexity that grows at most polynomially with  $n$  (and no less than  $\log$ )!



# Conclusions and Outlook

- Found necessary property for any definition of quantum Kolmogorov complexity (that allows to prepare a state): **exponential growth in  $N$**

# Conclusions and Outlook

- Found necessary property for any definition of quantum Kolmogorov complexity (that allows to prepare a state): **exponential growth in  $N$**
- Given a definition of quantum Kolmogorov complexity that satisfies said condition and studied some properties: relation to **entanglement** and **classical complexity**



# Conclusions and Outlook

- Found necessary property for any definition of quantum Kolmogorov complexity (that allows to prepare a state): **exponential growth in  $N$**
- Given a definition of quantum Kolmogorov complexity that satisfies said condition and studied some properties: relation to **entanglement** and **classical complexity**
- Shown how this quantity can be used to **prove statements** in communication and computation complexity theory

# Conclusions and Outlook

- Found necessary property for any definition of quantum Kolmogorov complexity (that allows to prepare a state): **exponential growth in  $N$**
- Given a definition of quantum Kolmogorov complexity that satisfies said condition and studied some properties: relation to **entanglement** and **classical complexity**
- Shown how this quantity can be used to **prove statements** in communication and computation complexity theory

To do: Are there other applications?  
What is the relation between the various definitions that scale exponentially?



Thank you for your attention!

# Relation between complexities

## (...Kolmogorov and computation...)

Computation complexity measures the time needed by a computer to find the solution to a problem with input of size  $n$

**Big question:** how much faster are quantum computers?  
What we knew (in 12 words): only using entanglement a quantum computer has a chance to be exponentially faster\*!

We can contribute too! all states that appear in the computation must have complexity that grows at most polynomially with  $n$  (and no less than  $\log$ )!

➔ only **few special states** (if any) can do the trick!  
(Proof holds only for network complexity)