

Quantum Communication Complexity

Yves Delley

April 21, 2008

Introduction

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

Conclusion

- Communication Complexity (CC) assesses the amount of communication resources needed to achieve distributed computation tasks
- In Quantum Communication Complexity (QCC) we are interested to see whether utilising quantum channels improves communication

Introduction

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

Conclusion

- Communication Complexity (CC) assesses the amount of communication resources needed to achieve distributed computation tasks
- In Quantum Communication Complexity (QCC) we are interested to see whether utilising quantum channels improves communication

What do we expect?

Introduction

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

Conclusion

- Communication Complexity (CC) assesses the amount of communication resources needed to achieve distributed computation tasks
- In Quantum Communication Complexity (QCC) we are interested to see whether utilising quantum channels improves communication

What do we expect?

- Holevo's theorem: One qbit does not contain more than one bit classical information
- Superdense coding: With one entangled qbit pair, two bits of classical information can be transferred at maximum
- Quantum teleportation: With one entangled qbit pair, two classical bits suffice to transmit one quantum bit

Outline

- Introduction
- **Outline**
- Introductory example

Definitions

Exponential separation

Conclusion

Introduction

Outline

Introductory example

Definitions

Distributed problem

Classification of protocols

Measuring the complexity

Summary

Entanglement

Exponential separation

Result

Definition

Quantum upper bound

Classical upper bound

Classical lower bound

Sketch of proof

Applications

Conclusion

Conclusion

Introductory example

- Introduction
- Outline
- **Introductory example**

Definitions

Exponential separation

Conclusion

Alice and Bob each have a big file stored on their computer. They want to find out if they are the same. What should they do?

- Send it to each other and compare byte per byte

Introductory example

- Introduction
- Outline
- **Introductory example**

Definitions

Exponential separation

Conclusion

Alice and Bob each have a big file stored on their computer. They want to find out if they are the same. What should they do?

- Send it to each other and compare byte per byte - **much communication needed**

Introductory example

- Introduction
- Outline
- **Introductory example**

Definitions

Exponential separation

Conclusion

Alice and Bob each have a big file stored on their computer. They want to find out if they are the same. What should they do?

- Send it to each other and compare byte per byte - **much communication needed**
- Send a checksum

Introductory example

- Introduction
- Outline
- **Introductory example**

Definitions

Exponential separation

Conclusion

Alice and Bob each have a big file stored on their computer. They want to find out if they are the same. What should they do?

- Send it to each other and compare byte per byte - **much communication needed**
- Send a checksum - **fails for some inputs**

Introductory example

- Introduction
- Outline
- **Introductory example**

Definitions

Exponential separation

Conclusion

Alice and Bob each have a big file stored on their computer. They want to find out if they are the same. What should they do?

- Send it to each other and compare byte per byte - **much communication needed**
- Send a checksum - **fails for some inputs**
- Send a randomized checksum

Introductory example

- Introduction
- Outline
- **Introductory example**

Definitions

Exponential separation

Conclusion

Alice and Bob each have a big file stored on their computer. They want to find out if they are the same. What should they do?

- Send it to each other and compare byte per byte - **much communication needed**
- Send a checksum - **fails for some inputs**
- Send a randomized checksum - **might still fail by bad luck**

Definition of a distributed problem

- Introduction
- Outline
- Introductory example

Definitions

- **Distributed problem**
- Classification of protocols
- Measuring the complexity
- Summary
- Entanglement

Exponential separation

Conclusion

- Alice and Bob are given some input $a \in A$ and $b \in B$ respective
- They are to produce some output $x \in X$
- Output has to fulfill:
 - Total function: $x = f(a, b)$
 - Partial or promise function:
 $x = f(a, b) \vee (a, b) \notin P \subset A \times B$
 - Relation problem: $(a, b, x) \in R \subset A \times B \times X$
- Size of input: $n := \log(|A| |B|)$

Definition of a distributed problem

- Introduction
- Outline
- Introductory example

Definitions

- **Distributed problem**
- Classification of protocols
- Measuring the complexity
- Summary
- Entanglement

Exponential separation

Conclusion

- Alice and Bob are given some input $a \in A$ and $b \in B$ respective
- They are to produce some output $x \in X$
- Output has to fulfill:
 - Total function: $x = f(a, b)$
 - Partial or promise function:
 $x = f(a, b) \vee (a, b) \notin P \subset A \times B$
 - Relation problem: $(a, b, x) \in R \subset A \times B \times X$
- Size of input: $n := \log(|A| |B|)$
- Usually $|X| \ll |A|, |B|$
- Often used special case: $X = \{0, 1\}$

Classification of protocols

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- **Classification of protocols**
- Measuring the complexity
- Summary
- Entanglement

Exponential separation

Conclusion

The protocol is for communication what the algorithm is for computation.

Classification of protocols

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- **Classification of protocols**
- Measuring the complexity
- Summary
- Entanglement

Exponential separation

Conclusion

The protocol is for communication what the algorithm is for computation.

We can classify protocols into different categories:

- Classical:
 - Deterministic
 - Probabilistic
- Quantum:
 - Qbits
 - Entanglement
- One-way vs. k-round
- Simultaneous message

Measuring the complexity

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- **Measuring the complexity**
- Summary
- Entanglement

Exponential separation

Conclusion

The communication complexity for a problem P :

$$\mathcal{C}(P) = \min_{T \in \mathcal{T}_P} \left(\max_{(a,b) \in A \times B} \mathcal{C}_T(a,b) \right)$$

Measuring the complexity

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- **Measuring the complexity**
- Summary
- Entanglement

Exponential separation

Conclusion

The communication complexity for a problem P :

$$\mathcal{C}(P) = \min_{T \in \mathcal{T}_P} \left(\max_{(a,b) \in A \times B} \mathcal{C}_T(a,b) \right)$$

- $\mathcal{C}_T(a,b)$: **Communication cost needed for termination when inputs are (a,b)**

Measuring the complexity

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- **Measuring the complexity**
- Summary
- Entanglement

Exponential separation

Conclusion

The communication complexity for a problem P :

$$\mathcal{C}(P) = \min_{T \in \mathcal{T}_P} \left(\max_{(a,b) \in A \times B} \mathcal{C}_T(a,b) \right)$$

- $\mathcal{C}_T(a,b)$: Communication cost needed for termination when inputs are (a,b)
- \mathcal{T}_P : **Class of protocols**

Measuring the complexity

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- **Measuring the complexity**
- Summary
- Entanglement

Exponential separation

Conclusion

The communication complexity for a problem P :

$$\mathcal{C}(P) = \min_{T \in \mathcal{T}_P} \left(\max_{(a,b) \in A \times B} \mathcal{C}_T(a,b) \right)$$

- $\mathcal{C}_T(a,b)$: Communication cost needed for termination when inputs are (a,b)
- \mathcal{T}_P : Class of protocols

Communication cost for probabilistic protocols?
(Bit-count is a random variable)

- Worst case cost
- Expected cost

Measuring the complexity

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- **Measuring the complexity**
- Summary
- Entanglement

Exponential separation

Conclusion

The communication complexity for a problem P :

$$\mathcal{C}(P) = \min_{T \in \mathcal{T}_P} \left(\max_{(a,b) \in A \times B} \mathcal{C}_T(a,b) \right)$$

We call then

- **Deterministic CC:** Only deterministic protocols
- **Bounded error CC:** Measures worst case cost, protocols must not fail more than a ϵ -fraction of all coin tosses
- **Zero error CC:** Measures expected cost, protocols must never fail

Summary

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- Measuring the complexity
- **Summary**
- Entanglement

Exponential separation

Conclusion

- For a family of problems with varying input size, the CC is a function of n
- The CC is always $\in O(n)$ (obvious solution)
- $\text{QCC} \leq \text{CCC}$

Spooky communication

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- Measuring the complexity
- Summary
- **Entanglement**

Exponential separation

Conclusion

- Communication only with entanglement?

Spooky communication

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- Measuring the complexity
- Summary
- **Entanglement**

Exponential separation

Conclusion

- Communication only with entanglement? - **not possible, so no distributed functions can be evaluated**

Spooky communication

- Introduction
- Outline
- Introductory example

Definitions

- Distributed problem
- Classification of protocols
- Measuring the complexity
- Summary
- **Entanglement**

Exponential separation

Conclusion

- Communication only with entanglement? - **not possible, so no distributed functions can be evaluated**
- In probabilistic output relation requirements still a separation to the classical setting possible!
- Example: Bell's inequality
- Leads to question: How many bits needed to simulate entanglement?

Outline

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

Introduction

Outline

Introductory example

Definitions

Distributed problem

Classification of protocols

Measuring the complexity

Summary

Entanglement

Exponential separation

Result

Definition

Quantum upper bound

Classical upper bound

Classical lower bound

Sketch of proof

Applications

Conclusion

Conclusion

Result

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- **Result**
- Definition
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

I'm going to sketch an exponential separation between QCC and CCC in the following setting

- The problem is a variant of the *Boolean Hidden Matching Problem*
- Communication is *one-way*: Alice sends just one message to Bob
- We compare the *bounded error* complexity
- Quantum: Qbits are transmitted, entanglement is not used
- Classical: Public coins are tolerated

$$Q_{\epsilon}(\alpha\text{PM}) = O(\log n/\alpha) \text{ whereas } C_{\epsilon}(\alpha\text{PM}) = \Theta(\sqrt{n/\alpha})$$

Definition of the task

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

- Alice is given an n -bit string x
- Bob is given a α -matching M and a αn -bit string w
- The promise on w is that $w = b^{\alpha n} \oplus Mx$ where b is an arbitrary bit
- Bob is to produce b

Bob does a promise function evaluation.

What is a α -matching?

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

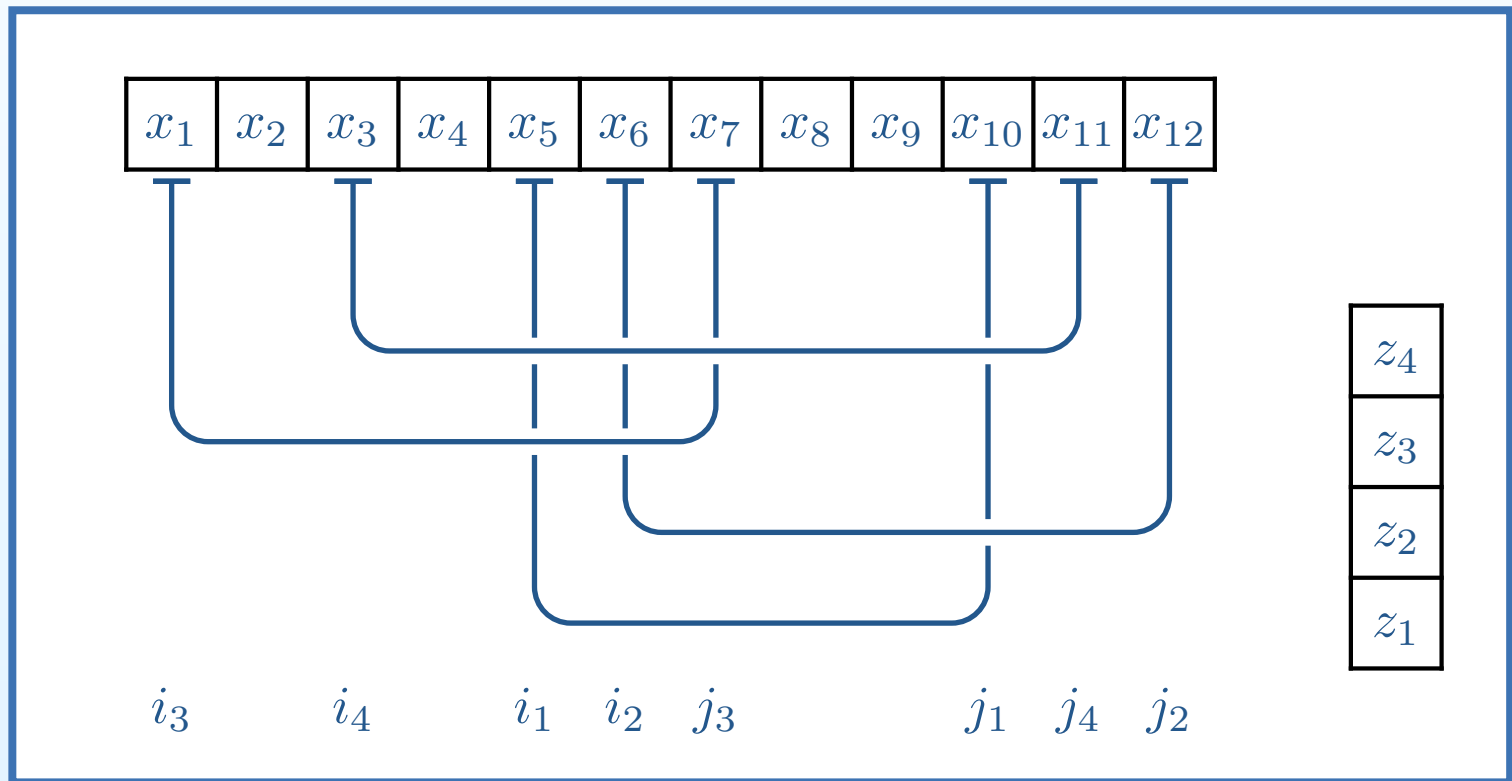
- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

A α -matching M is a sequence of αn pairs (i_l, j_l) of indices in the range $1 \dots n$, where no two indices are the same. If $\alpha = 1/2$ then we call this a *total* matching, else a *partial* matching. A matching M and a n -bit string x induce a αn bit string $z = z(M, x) = Mx$ via $z_l := x_{i_l} \oplus x_{j_l}$.

What is a α -matching?

A α -matching M is a sequence of αn pairs (i_l, j_l) of indices in the range $1 \dots n$, where no two indices are the same. If $\alpha = 1/2$ then we call this a *total* matching, else a *partial* matching. A matching M and a n -bit string x induce a αn bit string $z = z(M, x) = Mx$ via $z_l := x_{i_l} \oplus x_{j_l}$.



- Introduction
- Outline
- Introductory example

Definitions

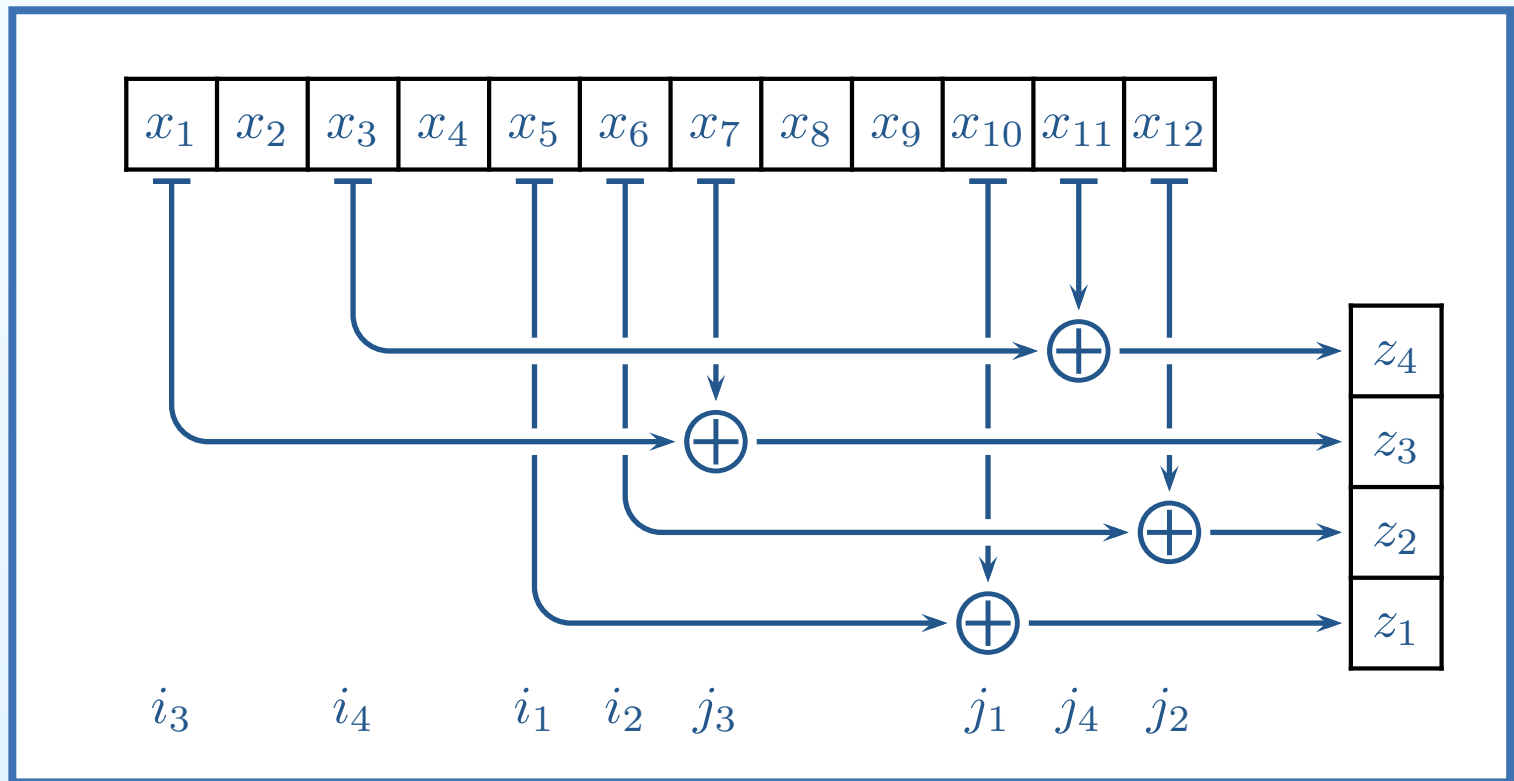
Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

What is a α -matching?

A α -matching M is a sequence of αn pairs (i_l, j_l) of indices in the range $1 \dots n$, where no two indices are the same. If $\alpha = 1/2$ then we call this a *total* matching, else a *partial* matching. A matching M and a n -bit string x induce a αn bit string $z = z(M, x) = Mx$ via $z_l := x_{i_l} \oplus x_{j_l}$.



- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

What is a α -matching?

- Introduction
- Outline
- Introductory example

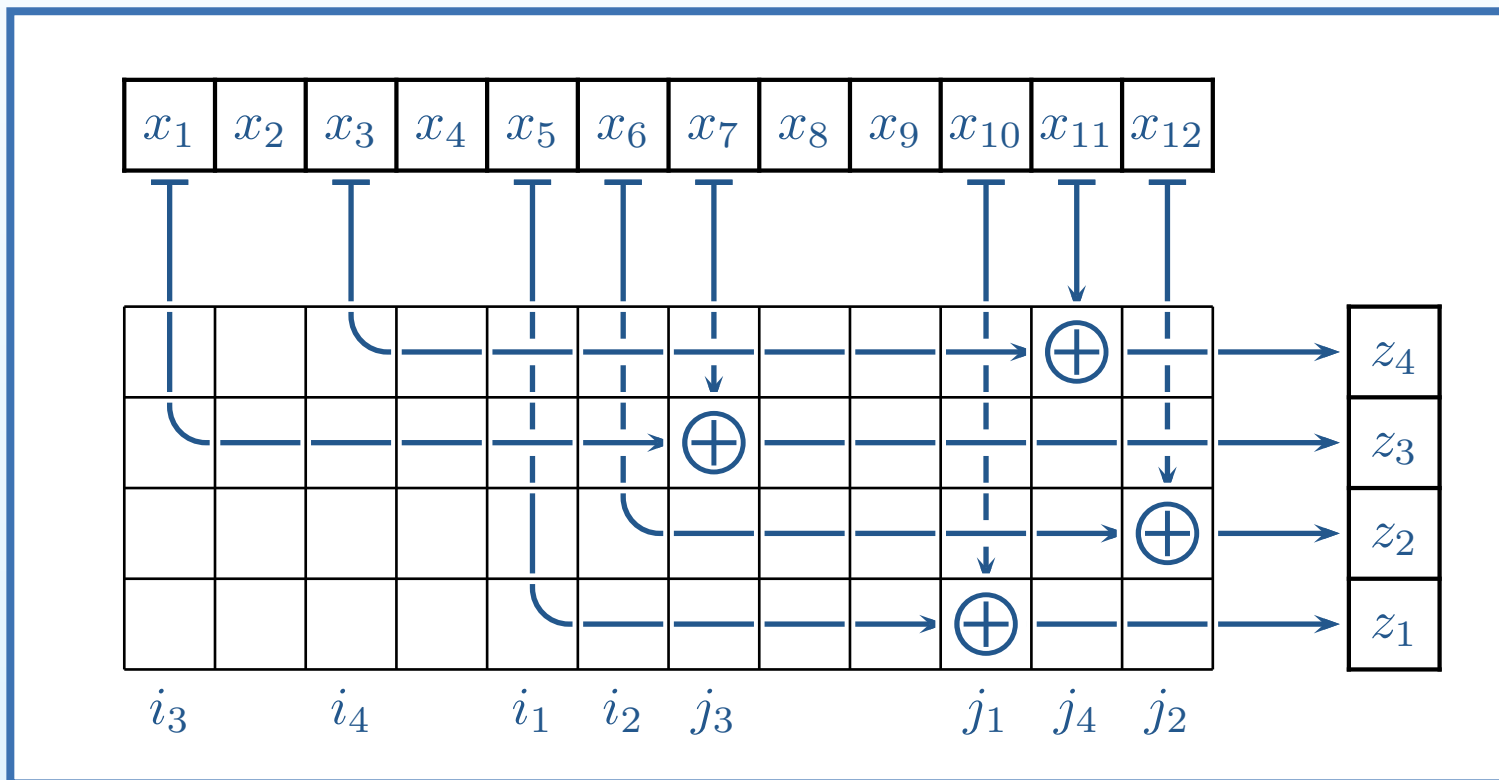
Definitions

Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

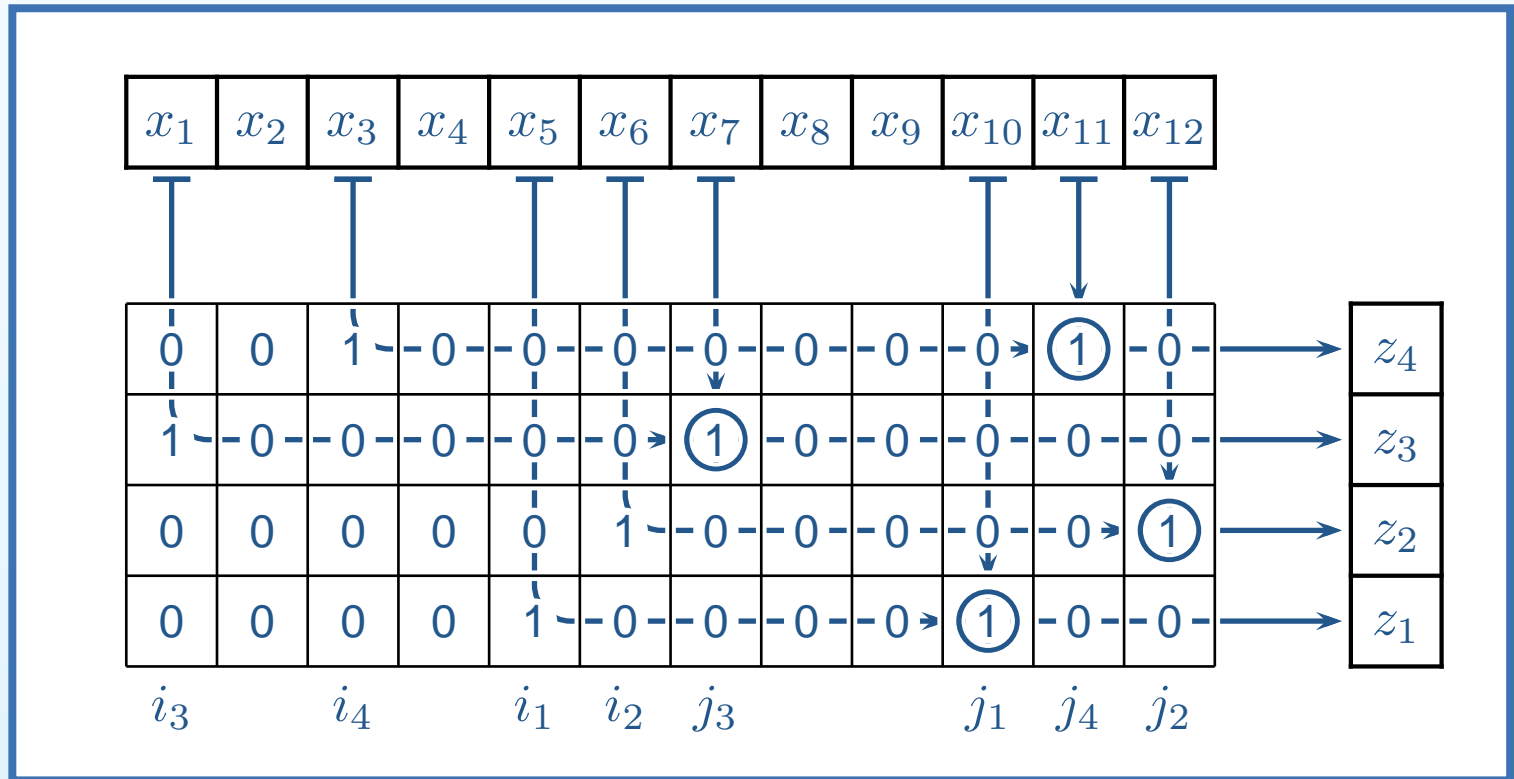
Conclusion

A α -matching M is a sequence of αn pairs (i_l, j_l) of indices in the range $1 \dots n$, where no two indices are the same. If $\alpha = 1/2$ then we call this a *total* matching, else a *partial* matching. A matching M and a n -bit string x induce a αn bit string $z = z(M, x) = Mx$ via $z_l := x_{i_l} \oplus x_{j_l}$.



What is a α -matching?

A α -matching M is a sequence of αn pairs (i_l, j_l) of indices in the range $1 \dots n$, where no two indices are the same. If $\alpha = 1/2$ then we call this a *total* matching, else a *partial* matching. A matching M and a n -bit string x induce a αn bit string $z = z(M, x) = Mx$ via $z_l := x_{i_l} \oplus x_{j_l}$.



- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

What is a α -matching?

- Introduction
- Outline
- Introductory example

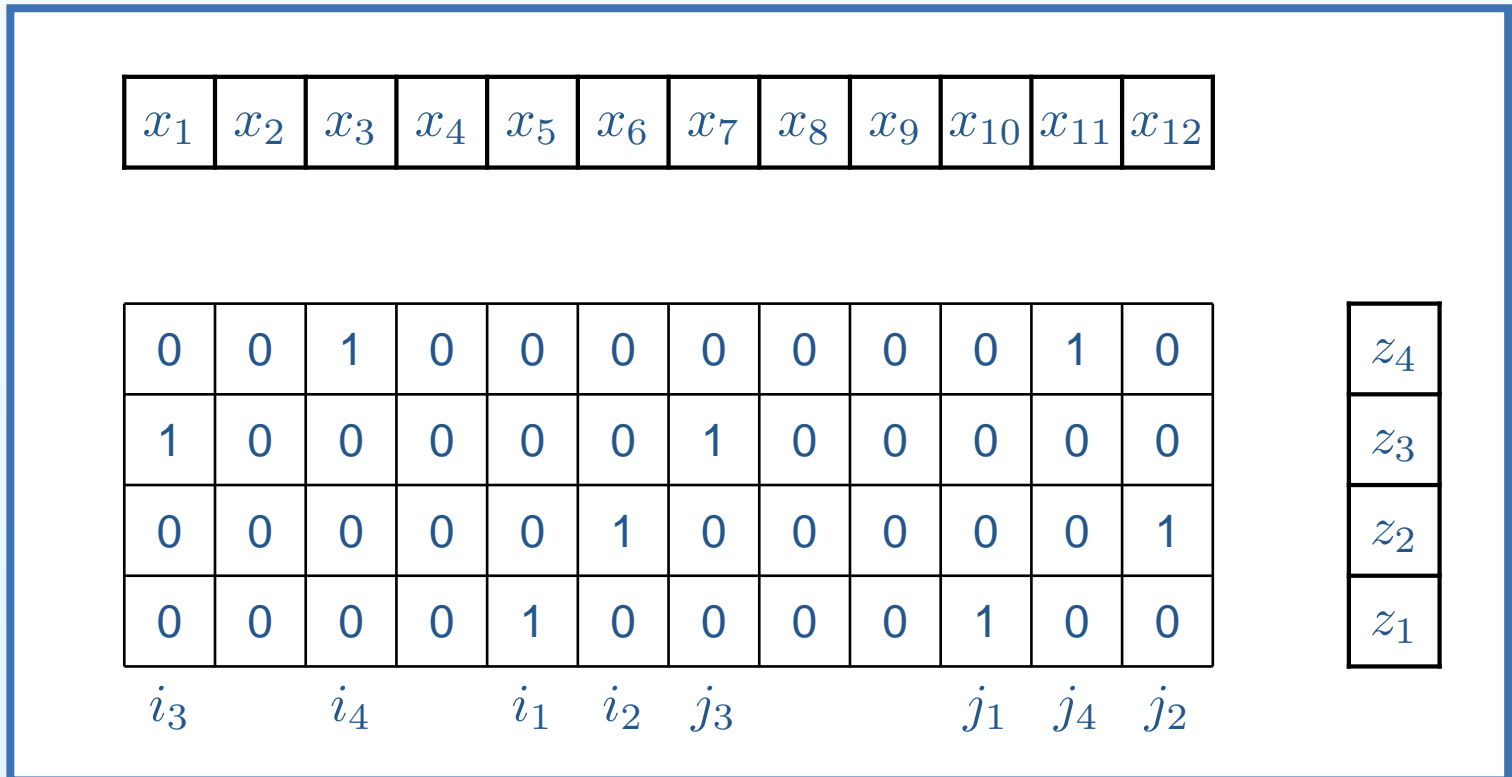
Definitions

Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

A α -matching M is a sequence of αn pairs (i_l, j_l) of indices in the range $1 \dots n$, where no two indices are the same. If $\alpha = 1/2$ then we call this a *total* matching, else a *partial* matching. A matching M and a n -bit string x induce a αn bit string $z = z(M, x) = Mx$ via $z_l := x_{i_l} \oplus x_{j_l}$.



The essence of it

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- **Definition**
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

- Bob needs to learn just one bit of $z = Mx$ to find b
- Any bit x_i on its own does not reveal any information on z
- As Alice does not know Bob's matching, she cannot decide which bits to send

The quantum upper bound

$$Q_{\epsilon}(\alpha\text{PM}) = O(\log n)$$

The quantum upper bound

$$Q_{\epsilon}(\alpha\text{PM}) = O(\log n)$$

Alice sends a uniform superposition of her bits in a $\log n$ qbit register:

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

The quantum upper bound

$$Q_{\epsilon}(\alpha\text{PM}) = O(\log n)$$

Alice sends a uniform superposition of her bits in a $\log n$ qbit register:

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

Bob measures using the following operator

$$\sum_{l=1}^{\alpha n} l |i_l\rangle \langle i_l| + l |j_l\rangle \langle j_l|$$

The quantum upper bound

$$Q_\epsilon(\alpha\text{PM}) = O(\log n)$$

Alice sends a uniform superposition of her bits in a $\log n$ qbit register:

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

Bob measures using the following operator

$$\sum_{l=1}^{\alpha n} l |i_l\rangle \langle i_l| + l |j_l\rangle \langle j_l|$$

With luck he measures k and the register collapses to the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} ((-1)^{x_{i_k}} |i_k\rangle + (-1)^{x_{j_k}} |j_k\rangle)$$

The quantum upper bound

$$Q_\epsilon(\alpha\text{PM}) = O(\log n)$$

Alice sends a uniform superposition of her bits in a $\log n$ qbit register:

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

Bob measures using the following operator

$$\sum_{l=1}^{\alpha n} l |i_l\rangle \langle i_l| + l |j_l\rangle \langle j_l|$$

With luck he measures k and the register collapses to the state

$$|\psi\rangle = \frac{1}{\sqrt{2}} ((-1)^{x_{i_k}} |i_k\rangle + (-1)^{x_{j_k}} |j_k\rangle)$$

Bob measures this state in the $|\pm\rangle$ base to find z_k :

$$\langle\psi| \frac{1}{\sqrt{2}} (|i_k\rangle - |j_k\rangle) \frac{1}{\sqrt{2}} (\langle i_k| - \langle j_k|) |\psi\rangle = \frac{1}{4} ((-1)^{x_{i_k}} - (-1)^{x_{j_k}})^2 = x_{i_k} \oplus x_{j_k} = z_k$$

The classical upper bound

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- **Classical upper bound**
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

$$C_{\epsilon}(\alpha\text{PM}) = O(\sqrt{n/\alpha})$$

The classical upper bound

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- **Classical upper bound**
- Classical lower bound
- Sketch of proof
- Applications

Conclusion

$$C_{\epsilon}(\alpha\text{PM}) = O(\sqrt{n/\alpha})$$

- Alice sends $d \approx \sqrt{n/\alpha}$ random bits of her string to Bob
- By the Birthday Paradox he then with high probability has both bits of one of his pairs

The classical lower bound

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- Classical upper bound
- **Classical lower bound**
- Sketch of proof
- Applications

Conclusion

$$C_{\epsilon}(\alpha\text{PM}) = \Omega(\sqrt{n/\alpha})$$

The proof of this lower bound is very long and tedious. I will only sketch the proof in this talk. For a more complete version see the report. Notation:

- Number of transmitted bits: c
- Bob's knowledge on x : $x \in A$

$$|A| \approx 2^{n-c}$$

The classical lower bound

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- Classical upper bound
- **Classical lower bound**
- Sketch of proof
- Applications

Conclusion

$$C_\epsilon(\alpha\text{PM}) = \Omega(\sqrt{n/\alpha})$$

The proof of this lower bound is very long and tedious. I will only sketch the proof in this talk. For a more complete version see the report. Notation:

- Number of transmitted bits: c
- Bob's knowledge on x : $x \in A$
- Bob's induced distribution on z : Probability distribution $p_M(z)$

$$p_M(z) = \frac{|\{x \in A \mid Mx = z\}|}{|A|}$$

The central theorem

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- Classical upper bound
- **Classical lower bound**
- Sketch of proof
- Applications

Conclusion

Theorem Let x be uniformly distributed over a set $A \subseteq \{0, 1\}^n$ of size $|A| \geq 2^{n-c}$ for some $c \geq 1$ and let M be uniformly distributed over the set $\mathcal{M}_{\alpha n}$ of all α -matchings, for some $\alpha \in (0, 1/4]$. There exists a universal constant $\gamma > 0$ such that for all $\epsilon > 0$: if $c \leq \gamma \epsilon \sqrt{n/\alpha}$ then

$$\mathbf{E}_M [\|p_M - U\|_{\text{tvd}}] \leq \epsilon$$

Total variational distance:

$$\|a - b\|_{\text{tvd}} := \sum_{x \in S} |a(x) - b(x)|$$

where a and b are probability distributions over S .

Sketch of the proof of the classical lower bound

- Principle by Yao: Suffices to analyze deterministic protocols under some "hard" input distributions
- Consider any classical protocol with $C = c - \log(1/\epsilon)$
- Depending on output Bob's distribution of x is any one out of: A_1, \dots, A_{2^C}
- Only a small fraction in small sets: 2^{-l} of all x in sets of size $|A| \leq 2^{n-C-l}$
- Hence most of the time Bob's view on x is large where the theorem can be applied
- Markov inequality: The expectation of Bob's information about z is small, therefore most of the time he actually knows not much
- In these cases Bob can still find the function value:
 - The protocol leaves Bob with a small distribution A on x
 - The big distribution A nevertheless produces a uneven distribution on z
 - The almost uniform distribution still exhibits some tendency

Applications of the result for the α PM

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

- Result
- Definition
- Quantum upper bound
- Classical upper bound
- Classical lower bound
- Sketch of proof
- **Applications**

Conclusion

- Cryptography: Privacy amplification
- Computation: Streaming model

Conclusion

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

Conclusion

- **Conclusion**

We have seen:

- Several models of classical and quantum communication complexity
- An example of a communication complexity problem, where quantum communication is exponentially better than classical communication - and the separation is provable!
- QCC has applications in computation and cryptography

Conclusion

- Introduction
- Outline
- Introductory example

Definitions

Exponential separation

Conclusion

- Conclusion

We have seen:

- Several models of classical and quantum communication complexity
- An example of a communication complexity problem, where quantum communication is exponentially better than classical communication - and the separation is provable!
- QCC has applications in computation and cryptography

Questions?