Quantum Communication Complexity and Quantum Information Complexity

. . .

Muhammad Usman Farooq

https://usmanmunara.github.io/

Project Overview

- Working with [Professor Penghui Yao @ Nanjing University]
- The focus of this project is on the interaction between Quantum Information theory and Quantum Communication Complexity(QCC), can also be thought of as extension of information theoretic tools to study problems in QCC.
- This talk: overview of Quantum Communication Complexity and Quantum Information Complexity.

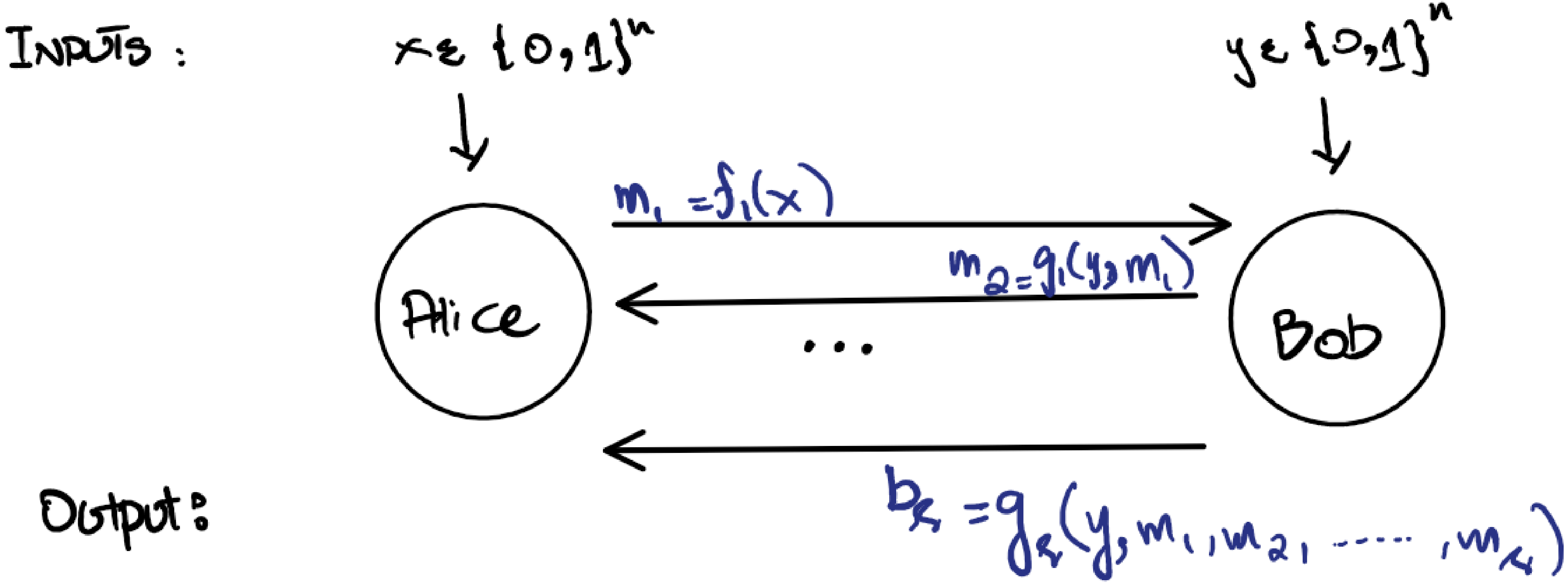
SUPPORTED BY UNITARY FUND

Communication Complexity

- Introduced by Andrew Yao(1979)
- Primary tool for unconditional bounds in various models of computation.
  - VLSI
  - Distributed Computing
  - Game theory
  - Differential privacy
- How much communication is necessary to solve a given problem?
- Communication Complexity is the amount of communication

Basic Communication Complexity Model

- In a two-party communication model, the goal is to compute a boolean function $f : \{0, 1\}^n \times \{0, 1\}^n \to 0, 1$
- Part of the input $x \in \{0, 1\}^n$ is held by Alice and the other input $y \in \{0, 1\}^n$ is held by Bob.
- During the communication, Alice and Bob will follow a predetermined protocol and send messages to each other. The communication complexity is defined as the minimum bits required in the protocol that computes f.


INPUTS :
Output:
x ∈ {0,1}^n
y ∈ {0,1}^n
Alice
Bob
m1 = f1(x)
m2 = g1(y, m1)
...
bk = gk(y, m1, m2, ..., mk)

For a communication protocol $\mathcal{P}$, with r rounds of communication, the Protocol transcript(Π) is given by

$$m_1 m_2 \cdots m_r$$

(A classical protocol is capable of memorizing the whole transcript Π, but this is a problem when it comes to a quantum protcol)

Communication Cost(CC) is the total number of bits communicated on the worst-case input (x, y).

$$|m_1| + |m_2| + \cdots + |m_r|$$

And Communication Complexity($C(f)$) for a problem is defined as $\mathcal{P} \in \mathcal{P}_{\mathcal{T}}$

$$\mathbf{C(f)} = min_{\mathcal{P} \in \mathcal{P}_{\mathcal{T}}} CC(\mathcal{P}) = min_{\Pi} CC(\Pi)$$

Quantum Communication Complexity (QCC)

- QCC is an extension of it's classical analogue.
- A quantum system divided into three parts A, B, and C
- Initial state $|x\rangle|0\rangle|y\rangle$
- A player can apply unitary transformation to their space and the channel.

- At the end of the protocol Alice or Bob makes a measurement to determine the output of the protocol.
- The cost of a protocol is the total number of qubits communicated on the worst-case input.
- We are interested in the minimal amount of communication they need.
- Cleve and Buhrman with pre-shared entanglement and communication via a classical channel.

A primer on Information Theory

- A message X is distributed according to some prior distribution μ
- Entropy $H(X)$ is the measure of uncertainty in a message.

$$H(X) = -\sum_{x \in \mathcal{X}} p_X(x) log(p_X(x))$$

w.r.t a random variable X with a probability mass function $p(x)$ is defined by

- Conditional Entropy: The uncertainity Alice has about Y when she already possess X.

$$H(Y|X) = \sum_{x \in \mathcal{X}} p(x) H(Y|X = x)$$

- Mutual Information $I(X;Y)$ can be defined as the reduction in uncertainty due to another random variable.

$$I(X;Y) = H(X) - H(X|Y)$$

- Conditional mutual information (CMI) is the reduction in the uncertainty of X due to knowledge of Y when Z is given:

$$I(X;Y|Z) = H(X|Z) + H(X|Y,Z)$$

- The quantum analogues can be defined similarly. However, Shannon's entropy is replaced by Von Neumann entropy, where given a state ρ

$$H(A)_\rho = -\mathrm{Tr}(\rho log \rho)$$

Information Complexity

- **Remember** Communication complexity studies the question "How many bits does Alice and Bob need to transmit to each other in order to solve a given problem?"
- Information complexity on the other hand studies the question, "How much information does Alice and Bob need to reveal to each other in order to solve a given problem?"

Given a distribution μ on a two-player input space $\mathcal{X} \times \mathcal{Y}$, a function $f : C \times Y \to 0, 1$, and an error parameter ϵ

- The information cost of a protocol π over inputs from $\mathcal{X} \times \mathcal{Y}$ is given by

$$IC_\mu(\pi) = I(\Pi; X|Y) + I(\Pi; Y|X)$$

- And the Information complexity is given by

$$IC(f) = inf_\pi max_\mu IC_\mu(\pi)$$

$IC_\mu(f, \epsilon)$ is defined to be the infimum of the information cost over all protocols π.

- **Why do we need Information Complexity?**
  - Discrete/Combinatorial vs Analytical
  - IC has some other properties that make it a really good extension into the CC realm.
  - However the most important result is: $\mathbf{IC}(\pi) \leq \mathbf{CC}(\pi)$
  - $IC(AND, 0) \approx 1.4923$

Quantum Information Complexity (QIC)

- In quantum communication protocols, there is no clear notion of a transcript.

- Hence by using a work around we have a new definition that counts how much information is exchanged in each round, which is given by

$$QIC(\Pi, \rho) = \sum_{i \geq 1, odd} I(C_i; R|B_i) + \sum_{i \geq 1, even} I(C_i; R|A_i)$$

- $QIC \leq QCC$

Alternative Characterization of QIC

- The above charachterization of QIC is for for quantum communication with quantum inputs.
- For quantum communication with classical inputs an alternative characterization is as the sum of the cost of transmitting information about the classical inputs and the cost of forgetting information about these inputs.

$$QIC(\pi, \mu) = CIC(\pi, \mu) + CRIC(\pi, \mu)$$

Our project focuses on **CRIC**

References

- I. Kremer. Quantum Communication. Master’s thesis (Hebrew University), 1995.
- A.C. Yao. Some Complexity Questions Related to Distributed Computing. Proc. 11th ACM Symp. on Theory of Computing, pp. 209–213, 1979.
- A.C. Yao. Quantum Circuit Complexity. 34th Symp. Foundations of Computer Science, pp. 352–361, 1993.
- Dave Touchette. Quantum information complexity. In Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, pages 317–326. ACM, 2015.

- Mark M. Wilde. Quantum Information Theory. Cambridge University Press, New York, 2013.
- Mathieu Lauri`ere and Dave Touchette. “The Flow of Information in Interactive Quantum Protocols: the Cost of Forgetting”.
- Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. Nearoptimal bounds on bounded-round quantum communication complexity of disjointness.
  In Proc. FOCS’15, 2015.
- R. Cleve and H. Buhrman, Phys. Rev. A 56, 1201 (1997).

- John Watrous. Theory of Quantum Information. 2015. Manuscript of a book, available at https://cs.uwaterloo.ca/˜watrous/.
- Ronald de Wolf. Quantum communication and complexity. Theoret. Comput. Sci.,
  287(1):337–353, 2002. Natural computing.
- Ronald de Wolf. Quantum Communication Complexity. 2001. Available at https://homepages.cwi.nl/~rdewolf/qcommcompl.pdf
- E. Kushilevitz and N. Nisan, Communication Complexity (Cambridge University Press, 1997).

Thank You

Slides: https://usmanmunara.github.io/NYCQuantum