One-Way Quantum Communication Complexity

Dominic Moylett*

Quantum Engineering Centre for Doctoral Training,
University of Bristol

March 8, 2016

Abstract

Communication complexity is the study of how much information two or more parties need to share with each other in order to perform joint computation of a problem. There are many benefits to this model of computation, from many lower bound proofs to applications in cryptography and data streaming. In this report, we will summarise the most exciting recent trends in the one-way form of quantum communication complexity, look at what quantum speedups already exist and what problems are still open.

1 Introduction

2 Communication Complexity

Communication complexity was developed by Yao in 1979 as an analysis of distributed computing [9]. Under this model of computation, our computation is done between two parties, commonly referred to as Alice and Bob, with inputs $x, y \in \{0,1\}^n$, respectively. The two parties do not know each other's inputs; Alice does not know y and Bob does not know x. Alice and Bob then exchange a series of messages between each other through a protocol established before computation, with their aim being to jointly compute $f(x, y)$. The question communication complexity asks is how many bits of information do Alice and Bob need to communicate in order for the two of them to compute a solution. We offer a sketch of a typical communication complexity problem in Figure 1.

A naïve solution to any communication complexity problem can be completed using n bits of communication: Alice sends x to Bob and Bob then does all of the computation for $f(x, y)$. So the question then becomes if it is possible to compute $f(x, y)$ with $o(n)$ bits of communication.

In quantum communication complexity, first proposed in 1993 by Yao [8], we also have parties Alice and Bob given inputs x and y, respectively, and have to produce $f(x, y)$ for some function f. But now our two parties can send quantum messages between each other, and the complexity is measured in the number of qubits that are communicated.

Another model by Burhman and Cleve [5] does not use the physical sending of data between the parties, but instead uses the measurement of entangled particles for remote computation. Our focus for this report however will be on the former. Note that it is possible to simulate this model by the ability to communicate quantum states: Alice generates entangled pairs of qubits and sends one of the pair to Bob. Likewise, it is possible to simulate communicating l qubits by use of l entangled pairs and $2l$ classical bits of communication, via quantum teleportation [1].

2.1 One-Way Communication Complexity

A specific subset of communication complexity, which we will focus on throughout this report, is one-way communication complexity. In this model of computation, Alice and Bob again receive respective inputs

*dominic.moylett@bristol.ac.uk

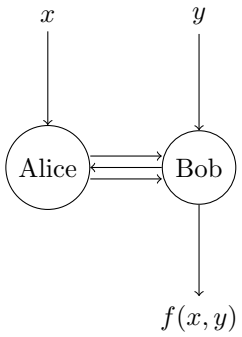

Figure 1: An example of communication complexity. Alice and Bob begin computation with bit strings x and y. They then exchange a series of messages based on a pre-determined protocol. Computation completes when Bob outputs $f(x, y)$.

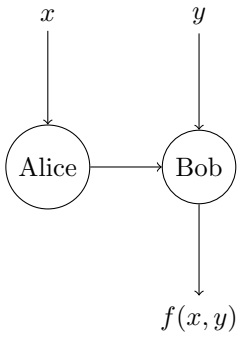

Figure 2: An example of one-way communication complexity. Alice receives input x and Bob receives input y. Alice then sends a single message to Bob. Using this additional information from Alice, Bob performs and outputs the computation $f(x, y)$.

$x, y \in \{0, 1\}^n$ with the aim of Bob being able to output $f(x, y)$ for some function f. The difference now is that only one message is allowed to be sent, from Alice to Bob. This is illustrated in 2.

Like general communication complexity, one-way communication complexity can also be solved naïvely in n bits of communication by Alice sending x to Bob. So once again, our question is if we can do better with less communication.

2.2 Holevo's Theorem

Even before Yao's work on the formalisation of Communication Complexity, it was clear that quantum communication would not be able to speed up some problems. In particular, a consequence of Holevo's theorem [6], meant that while a message of n bits could be compressed into a message of at most $n - 1$ qubits, the same message could not be retrieved from said qubits. We phrase this as a one-way communication complexity problem below.

Problem COMMUNICATION
ALICE'S INPUT: $x \in \{0, 1\}^n$.
BOB'S INPUT: none.
BOB'S OUTPUT: x.

By Holevo's theorem, we know that the above problem requires Alice to send $\Omega(n)$ qubits to Bob. A later proof by Nayak [7] shows that if we compress a message of n bits into a message of $m < n$ qubits, the probability that we can successfully retrieve all n bits again is at most 2^{m-n}. The only exception to this is when Alice and Bob have shared entangled qubits between each other prior to computation, in which case superdense coding can be used to send two bits by sending one qubit [2]. Brassard [3] explains that if we have unlimited entanglement between Alice and Bob then we can only at most reduce

the amount of communication by a factor of 1/2, as quantum teleportation can be used to send qubits from one party to the other using entangled pairs and communicating with classical bits [1].

While we cannot do communication of n bits with fewer than n qubits, we will in the next two sections look at more specific problems which we can solve by communication of fewer qubits.

3 Functions

3.1 Distributed Deutsch-Jozsa

The Distributed Deutsch-Jozsa problem, first introduced by Buhrman, Cleve and Wigderson [4], was the first example of an exponential separation between quantum and classical computation complexity. The problem, and its quantum protocol, are stated as follows, where $\mathcal{D}(x, y)$ is the Hamming distance between x and y and $U_x = \sum_{i=0}^{n-1}(-1)^{x_i}|i\rangle\langle i|$ for some parameter x:

Problem COMMUNICATION

ALICE'S INPUT: $x \in \{0,1\}^n$.
BOB'S INPUT: $y \in \{0,1\}^n$.
PROMISE: $x = y$ or $\mathcal{D}(x, y) = n/2$.
BOB'S OUTPUT: 1 iff $x = y$, 0 otherwise.

1 Alice starts computation in the $|0\rangle^{\otimes \log n}$ state and applies $U_x H^{\otimes \log n}$ to get the state $|\psi\rangle = \sum_{i=0}^{n-1}(-1)^{x_i}|i\rangle$.
2 Alice sends $|\psi\rangle$ to Bob.
3 Bob applies $H^{\otimes \log n}U_y$ and measures in the computational basis.
4 Bob outputs 0 if they measure $|0\rangle^{\otimes \log n}$ and 1 otherwise.

3.2 Subgroup Membership

3.3 Permutation Invariance

4 Relations

4.1 Hidden Matching

4.2 α-matching

5 Applications

6 Implementations

7 Conclusion

7.1 Open Problems

7.2 Other Areas

References

[1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[2] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992.

[3] Gilles Brassard. Quantum communication complexity (a survey), 2001.

[4] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 63–68, New York, NY, USA, 1998. ACM.

[5] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication, 1997.

[6] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9:3–11, 1973.

[7] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 369–376, 1999.

[8] A. Chi-Chih Yao. Quantum circuit complexity. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 352–361, Nov 1993.

[9] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing(preliminary report). In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 209–213, New York, NY, USA, 1979. ACM.