One-Way Quantum Communication Complexity

Dominic Moylett[*]

Quantum Engineering Centre for Doctoral Training,
University of Bristol

March 7, 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 review article, 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 [5]. Under this model of computation, our computation is done between two parties, commonly referred to as Alice and Bob, with inputs x and y, respectively. Alice and Bob then exchange a series of messages between each other, with the aim of the two of them being able to output $f(x, y)$. 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.

In quantum communication complexity, first proposed in 1993 by Yao [4], we also have parties Alice and Bob given inputs x and y, respectively, and have to produce $f(x, y)$. 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 [2] 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 the report however will be on the former.

2.1 One-Way Communication Complexity

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 [3], 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: an n-bit string x.
BOB'S INPUT: none.
BOB'S OUTPUT: x.

[*] dominic.moylett@bristol.ac.uk

By Holevo's theorem, we know that the above problem requires Alice to send $\Omega(n)$ qubits to Bob. 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 [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

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

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

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

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

[5] 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.