

One-Way Quantum Communication Complexity

Dominic Moylett*

*Quantum Engineering Centre for Doctoral Training,
University of Bristol*

March 11, 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 advantages 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 [Yao79]. 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 [Yao93], 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 [CB97] 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 [BBC⁺93].

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

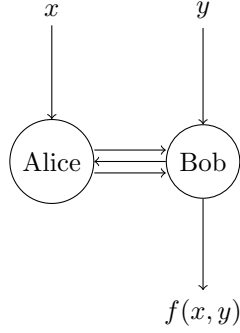


Figure 1: An example of communication complexity. Alice and Bob begin computation with bit strings x and y . They then exchange a series of messages based on a pre-determined protocol. Computation completes when Bob outputs $f(x, y)$.

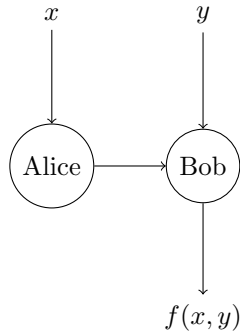


Figure 2: An example of one-way communication complexity. Alice receives input x and Bob receives input y . Alice then sends a single message to Bob. Using this additional information from Alice, Bob performs and outputs the computation $f(x, y)$.

$x, y \in \{0, 1\}^n$ 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 naively 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 [Hol73], 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 [Nay99] 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 [BW92]. Brassard [Bra01] 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 [BBC⁺93].

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 [BCW98], was the first example of an exponential separation between quantum and classical computation complexity. The problem, and its quantum protocol as described in Buhrman et al. [BCMdW10], 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 $x \in \{0, 1\}^n$:

Protocol DISTRIBUTED DEUTSCH-JOZSA

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: 0 iff $x = y$, 1 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 $|\psi\rangle$.
- 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.

The state Alice sends to Bob is $|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i} |i\rangle$. When Bob applies U_y to this state, they end up with the state $\frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i} (-1)^{y_i} |i\rangle$. We'll now consider this state for two situations: one where $x = y$ and one where they differ in $n/2$ places, denoted $|\psi_0\rangle$ and $|\psi_1\rangle$, respectively.

Note that if $x = y$ then $(-1)^{x_i} (-1)^{y_i} = 1$, so $|\psi_0\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle$. $|\psi_1\rangle$ on the other hand will have exactly $n/2$ amplitudes which are positive, and $n/2$ amplitudes which are negative. From this we can see that $\langle \psi_0 | \psi_1 \rangle = \frac{n/2 - n/2}{n} = 0$, so the states can be distinguished from one another upon measurement. Finally, Bob's application of $H^{\otimes \log n}$ converts their state to the computational basis. Note that $H|\psi_0\rangle = |0\rangle^{\otimes \log n}$, so measuring this state will indicate that $x = y$ and any other state will indicate that $\mathcal{D}(x, y) = n/2$.

So we have been able to deterministically solve this problem with $O(\log n)$ qubits of communication between Alice and Bob. How much classical communication is required to solve it? It was shown in Appendix 4 of Buhrman et al. [BCMdW10] that any deterministic protocol must send at least $0.007n$ bits from Alice to Bob, otherwise the protocol will fail for some input. However, this quantum advantage is lost when compared to randomised classical computation for some positive integer c :

Protocol DISTRIBUTED DEUTSCH-JOZSA

- 1 Alice picks c unique items $a \in \{0, 1\}^n$ uniformly at random.
- 2 Alice sends $(a_i, x_{a_i}) \forall i \in \{0, \dots, c-1\}$.
- 3 Bob returns 0 if $x_{a_i} = y_{a_i} \forall i \in \{0, \dots, c-1\}$, and 1 otherwise.

Bob always returns 0 if $x = y$, so our protocol has no true negative results. If $\mathcal{D}(x, y) = n/2$, then the protocol fails if $x_{a_i} = y_{a_i} \forall i \in \{0, \dots, c-1\}$, which happens with probability $1/2^c$. Finally, note that each a_i can be communicated in $\log n$ bits, so the overall communication required is $c(\log n + 1)$ bits.

3.2 Subgroup Membership

One disadvantage of the Distributed Deutsch-Jozsa problem that we saw above is that a quantum protocol has no advantage over a randomised classical protocol. Another disadvantage is that the problem is a

partial function, in that it requires a *promise* on the input: that either the two bit strings are identical or they differ in exactly $n/2$ places. This promise results in a very contrived problem with little practical application. This begs the question: Are there any functions which do not rely on promises that yield a quantum advantage under the communication complexity model – better known as *total functions*?

Sadly, no significant gap has been shown for total functions in the one-way model, even though two-way communication has shown polynomial gaps [BCW98], and other models such as Simultaneous Message Passing have shown exponential gaps [BCWdW01]. But there are some problems which have shown potential. Aaronson et al. [AGRT09] were the first to explore the problem of subgroup membership as potentially yielding a quantum advantage in the one-way communication complexity setting. Their protocol for solving subgroup membership, based on an earlier quantum algorithm by Watrous [Wat00], is described below, where G is a group, \mathcal{H}_G is the set of all subgroups of G , $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $U_{G,y} = \sum_{g \in G} |yg\rangle\langle g|$ for some $y \in G$:

Protocol SUBGROUP-MEMBERSHIP

ALICE'S INPUT: $H \in \mathcal{H}_G$.

BOB'S INPUT: $y \in G$.

BOB'S OUTPUT: 1 if $y \in H$, 0 otherwise.

- 1 Alice prepares the state $|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle$, which is then sent to Bob.
- 2 Bob prepends an ancilla qubit to get $|H\rangle|+\rangle$ and applies $U_{G,y}$ controlled on the final qubit.
- 3 Bob applies a Hadamard to the second qubit and measures in the computational basis.

Any element $h \in H$ can be described in $\lceil \log |G| \rceil$ bits, so Alice needs to send $O(\log |G|)$ qubits to Bob in order to perform this protocol.

After line 2, Bob has the state $\frac{1}{\sqrt{2}}(|H\rangle|0\rangle + |yH\rangle|1\rangle)$, where $|yH\rangle = \frac{1}{\sqrt{|H|}} \sum_{y h \in H} |h\rangle$. If $y \in H$ then $y h \in H \forall h \in H$, so $|yH\rangle = |H\rangle$. Therefore, if $y \in H$ then $U_{G,y}|H\rangle|+\rangle = |H\rangle|+\rangle$, so applying a Hadamard to the final qubit makes the final qubit $|0\rangle$. A measurement in the computational basis will thus always yield 0.

On the other hand, if $y \notin H$ then $\langle yH|H\rangle = 0$, so applying the Hadamard produces

$$\frac{1}{2}(|H\rangle|0\rangle + |H\rangle|1\rangle + |yH\rangle|0\rangle - |yH\rangle|1\rangle).$$

Measuring the final qubit will result in $|0\rangle$ – and thus a false positive – with probability $1/2$. We can repeat this protocol a constant number of times to get a negligible error probability.

Classically, it has been shown by Miltersen et al. [MNSW98] that any one-way randomised protocol with completeness probability of $1/2$ and perfect soundness must use $\Omega(\log |G|)$ bits of communication. Aaronson et al. [AGRT09] have conjectured that this bound still holds even if we relax soundness to $1/3$ and tighten completeness to $2/3$.

So, if we can find a total subgroup membership function that cannot classically be solved using $O(\log |G|)$ bits of communication, then we will have a polynomial gap between classical and quantum communication for a total function. The problem is that there are many subgroup membership problems which *can* be solved classically within these constraints. One example is that of normal subgroups. Aaronson et al. [AGRT09] showed that this problem can be solved with error probability of $1/2$ using only $O(\log |G|)$ bits of communication.

To explain this classical protocol, we first need to describe complex characters. For any complex field representation ρ of G , the complex character χ is the function $\chi(g) = \text{tr}(\rho(g)) \forall g \in G$. For any two elements $g, g' \in G$, we have the relation that $\chi(gg'g^{-1}) = \chi(g)$. $\chi(1)$ is the dimension of ρ , and the kernel of χ , denoted $\ker(\chi) = \{g \in G | \chi(g) = \chi(1)\}$. If ρ is irreducible then χ is an irreducible character, and the set of irreducible complex characters of G is denoted $\text{Char}(G)$. Finally, if H is a normal subgroup of G , then let

$$\Lambda_H = \{\chi \in \text{Char}(G) | H \subseteq \ker(\chi)\}.$$

Finally, given this definition we note that

$$\sum_{\chi \in \Lambda_H} [\chi(1)]^2 = \frac{|G|}{|H|}.$$

We now describe the protocol from Aaronson et al. [AGRT09]:

Protocol NORMAL-SUBGROUP-MEMBERSHIP

ALICE'S INPUT: $H \in \mathcal{H}_G$ such that H is normal.

BOB'S INPUT: $y \in G$.

BOB'S OUTPUT: 1 if $y \in H$, 0 otherwise.

- 1 Alice chooses a random complex character μ such that $H \subseteq \ker(\mu)$ with probability $\frac{|H|}{|G|}[\mu(1)]^2$.
- 2 Alice sends μ to Bob.
- 3 Bob outputs 1 if $y \in \ker(\mu)$ and 0 otherwise.

If $y \in H$ then $y \in \ker(\mu)$, so $\mu(y) = \mu(1)$ and thus the protocol will always correctly report a member of H . So now we only need to consider the case where the $y \notin H$ yet the protocol accepts. This will occur if Alice picks a character μ such that $y \in \ker(\mu)$. We shall call the set of all characters that would cause an error B . Based on Alice's selection criteria, the probability of an error is thus

$$\frac{|H|}{|G|} \sum_{\chi \in B} [\chi(1)]^2.$$

To analyse this further, we will look at the smallest normal subgroup of G which contains both H and y . We will call this subgroup K , which can be stated formally as $K = \{gkg^{-1} | g \in G, k \in H \cup \{y\}\}$. Note that $|K| \geq 2|H|$, as $\forall h \in H, h \in K$ and $hyh^{-1} \in K$, but $hyh^{-1} \notin H$.

The final point we will need is that $B \subseteq \Lambda_K$. Consider a character $\chi \in B$. Because χ could be selected by Alice, we know that $H \subseteq \ker(\chi)$, and also that $y \in \ker(\chi)$ because $\chi \in B$. We can conclude from this that any other element in K must also be in $\ker(\chi)$, as $\chi(gkg^{-1}) = \chi(k) \forall g \in G, k \in H \cup \{y\}$. Thus $K \subseteq \ker(\chi)$ and we can conclude that $\chi \in \Lambda_K$.

Using the above points, we can show that

$$\frac{|H|}{|G|} \sum_{\chi \in B} [\chi(1)]^2 \leq \frac{|H|}{|G|} \sum_{\chi \in \Lambda_K} [\chi(1)]^2 = \frac{|H|}{|G|} \frac{|G|}{|K|} \leq \frac{|H|}{|G|} \frac{|G|}{2|K|} = \frac{1}{2}.$$

Thus this protocol fails with probability at most $1/2$. Finally, we note that it is possible to describe a character μ sent from Alice to Bob in $\lceil \log |G| \rceil$ bits, as $\mu \in \Lambda_H$ and $|\lambda_H| \leq |\text{Char}(G)| \leq |G|$, so this protocol only needs $O(\log |G|)$ classical bits of communication. So in order to find a subgroup membership problem which provides an exponential gap between random and quantum computation, we need to consider non-normal subgroups.

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

- [AGRT09] Scott Aaronson, François Le Gall, Alexander Russell, and Seiichiro Tani. The one-way communication complexity of group membership, 2009.
- [BBC⁺93] 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.
- [BCMdW10] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, Mar 2010.
- [BCW98] 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.
- [BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001.
- [Bra01] Gilles Brassard. Quantum communication complexity (a survey), 2001.
- [BW92] 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.
- [CB97] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication, 1997.
- [Hol73] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9:3–11, 1973.
- [MNSW98] Peter Bro Miltersen, Noam Nisan, Shmuel Safra, and Avi Wigderson. On data structures and asymmetric communication complexity. *Journal of Computer and System Sciences*, 57(1):37 – 49, 1998.
- [Nay99] 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.
- [Wat00] J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, FOCS '00, pages 537–, Washington, DC, USA, 2000. IEEE Computer Society.

- [Yao79] 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.
- [Yao93] A. Chi-Chih Yao. Quantum circuit complexity. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 352–361, Nov 1993.