Distributed Problems in Quantum Communication

Bhaskar Mookerji
6.896 Quantum Computational Complexity

9 December 2008

Abstract

Locality might prohibit Alice and Bob from using quantum entanglement to transmit information superluminally, but it does not prevent them from either reducing the communication required for some problems, or playing impossible games requiring no communication at all. Accordingly, we will review the polynomial method for determining quantum communication complexity lower bounds. We will also review quantum psuedo-telepathy, which permits certain distributed tasks amongst entangled parties to be completed without communication.

Communication complexity quantifies the communication requirements of two separated parties, Alice and Bob, living far-apart in a country where telephone calls and email are extremely expensive. Fortunately, Alice and Bob each have quantum supercomputers, an infinite supply of nuclear energy, and can communicate without fear of eavesdroppers, since Eve has recently been executed. They want to compute some function $f : R \to \{0, 1\}$ such that $R \subseteq X \times Y$. The function f is a *total function* if $R = X \times Y$, and a *promise function* if otherwise. Alice and Bob have two n-bit string inputs x and y from $X = Y = \{0, 1\}^n$, and want to compute the value of the function $f(x, y)$ on their inputs. However, because communication is so expensive, they want to minimize information transmitted between them, and accordingly define the *communicational complexity* of a total Boolean function $f : X \times Y \to \{0, 1\}$ as the minimum number of (qu)bits required for either of them to evaluate $f(x, y)$.

Our goal here is to quantify the limits of quantum communication between Alice and Bob. We will first provide a method for proving lower bounds for the quantum communicational complexity of a given Boolean function f and relate it to some other important results and conjectures in classical information theory. We will discuss Mermin-Peres magic square

game, the simplest example of a psuedo-telepathic game that Alice and Bob can play in the absence of communication and still win with absolute certainly.

1 Motivation and Notation

The history of communicational complexity and our current understanding of classical and quantum channel capacities motivates our intuition for complexity lower bounds. Yao first introduced the notion of quantum communicational complexity by replacing bits with qubits in communicational complexity, but failed to demonstrate that qubit communication channels actually provided an advantage [1]. Yao's suspicion was confirmed when Cleve and Buhrman showed that entanglement could be used to save on one bit of communication between two parties [2], a classical-quantum separation which was eventually generalized k parties [3]. Raz later gave a promise problem exhibiting an exponential separation between classical and quantum communication protocols[4].

In the context of these results, recall that if Alice and Bob share an EPR pair, Alice can use a single qubit teleportation to transmit two classical bits, a scheme known as *superdense coding*. The following result, generally referred to as *Holevo's Theorem*, quantifies this result [5].

Theorem 1 (Holevo, WDMA98) *If Alice wants to send n bits of information to Bob via a qubit channel, and they don't share prior entanglement, then they have to exchange at least n qubits. If they do share prior entanglement, then Alice has to send at least $n/2$ qubits to Bob, no matter how many qubits Bob sends to Alice.*

To extend this result to an arbitrary Boolean function f, we must first establish some notation for exact protocols [6]. In the following, we will denote $D(f)$ as the deterministic classical communication complexity and $Q(f)$ as the qubit complexity without shared EPR pairs. When shared entanglement is available, $Q^*(f)$ ($C^*(f)$) quantifies the qubit (bit) communicational complexity. There are known results for several total functions already. For example, the *equality* function $\mathrm{EQ}(x,y) = 1$ iff $x = y$, and the *disjointness* function $\mathrm{DISJ}(x,y) = \mathrm{NOR}(x \wedge y)$. This latter function evaluates to 1 iff there is no i such that $x_i = y_i = 1$, meaning that x and y are disjoint if they are characteristic sets of vectors. The remaining *inner product* function was used in the proof of the entanglement clause of

Holevo's Theorem above:

$$\mathrm{IP}(x,y) = \mathrm{PARITY}(x \wedge y) = \sum_i x_i y_i \,(\mathrm{mod}\ 2). \tag{1}$$

For each of these functions, it has been shown that $Q^*(f) \geq n/2$ and $C^*(f) \geq n$. The results for these functions, as well as the power of quantum channels suggested by Holevo's theorem, implies the rather obvious result for total Boolean functions f that $Q^*(f) \leq Q(f) \leq D(f)$.

2 Lower Bounds By Polynomials

With the intuition from the previous section, we can now relate lower bounds for quantum communicational complexity to the rank property of a total Boolean function f, denoted by $\mathrm{rank}(f)$. A total Boolean function $f : X \times Y \to \{0,1\}$, can be represented in two different ways: first, as a Boolean matrix $M_f[x,y] = f(x,y)$ over the $\mathbb{R}$; and second, as a unique multilinear polynomial $g(x \wedge y)$ over n variables. In the former, $\mathrm{rank}(f) = \mathrm{rank}(M_f)$. In the latter, $\mathrm{rank}(f)$ equals the number of monomials $\mathrm{mon}(g)$.

Theorem 2 (BW00) *$Q^*(f) \geq \frac{1}{2}\log rank(f)$ and $C^*(f) \geq \log rank(f)$ [6].*

Proof:

Let $f^{\wedge m}$ denote Boolean function which is the logical AND of m independent instances of f, given by $f^{\wedge m} : X^m \times Y^m \to \{0,1\}$. Also, let $Q_c(f)$ specify the qubit cost of a *clean* protocol for f that starts without prior entanglement. This type of protocol is simpler than the prior entanglement case, and it can be shown that $Q_c(f) \geq \log \mathrm{rank}(f) + 1$ without much difficulty.

Now suppose we have an exact protocol for f using l qubits for communication and k prior EPR-pairs. It can be shown that there exists a clean protocol that uses $2ml + 2k$ and no prior entanglement, giving

$$2ml + 2k \geq Q_c\left(f^{\wedge m}\right) \geq \log rank\left(f^{\wedge m}\right) + 1 = m \log rank(f) + 1, \tag{2}$$

which implies that

$$l \geq \frac{\log \mathrm{rank}(f)}{2} - \frac{2k-1}{2m}, \tag{3}$$

which is true for $m > 0$, implying the theorem. By Holevo's Theorem, a qubit protocol for $f \wedge f$ exists using $C^*(f)$ qubits, and by our first proof,

$$C^*(f) \geq Q^*(f \wedge f) \geq (\log \mathrm{rank}(f \wedge f))/2 = \log \mathrm{rank}(f). \tag{4}$$

Furthermore, because $\text{rank}(f) = \text{mon}(f)$, the lower bound cost for quantum communication can be determined from polynomial representations. $\square$

We can consider our previous Boolean function lower bounds in the context of this result. It has been shown that almost all total Boolean $2^n \times 2^n$ matrices $M_f[x, y]$ have full rank 2^n, which captures our previous statements regarding EQ, DISJ, and IP, as well as most other total Boolean functions:

Corollary 3 *$Q^*(EQ)$, $Q_E^*(DISJ)$, $Q^*(IP) \geq n/2$ and $C^*(EQ)$, $C^*(DISJ)$, $C^*(IP) \geq n$. For $X = Y = \{0,1\}^n$, almost all $f : X \times Y \to \{0,1\}$ have $Q^*(f) \geq n/2$ and $C^*(f) \geq n$.*

We can apply Theorem 2 to one remaining result, known as the 'log-rank conjecture,' which implies that $\text{rank}(f)$ specifies the deterministic classical communicational complexity $D(f)$ up to a polynomial factor. Combined with Theorem 2, this implies a polynomial equivalence between classical and exact quantum communicational complexities.

Corollary 4 *If $D(f) \in O\left((\log rank f)^k\right)$, then $Q^*(f) \leq Q(f) \leq D(f) \in O\left(Q^*(f)^k\right)$ for all f.*

3 Quantum Pseudo-Telepathy

In the previous section, we reviewed some strong lower bounds for quantum communicational complexity and can move on to an even more unusual extreme! The fiber lines connecting Alice and Bob live are extremely unreliable, and they soon find themselves being forced to demonstrate their mysterious telepathic powers to group of paraphysicists from MIT. Fortunately, Alice and Bob shared an infinite supply of EPR-entangled photons pairs before their fiber lines went down. More generally, their scheme is known as a 'psuedo-telepathy' game, a distributed problem where k-players can agree on a prior strategy and share unlimited entanglement [7]. Furthermore, the game must be such that the players can win with unitary probability when classical players cannot. How can we compaire the success of classical deterministic and probabilistic strategies against entanglement correlations?

A *classical* strategy is *deterministic* if there are two functions $f : X \to A$ and $g : Y \to B$ such that Alice and Bob systematically output $f(x)$ and $g(y)$ for their respective inputs x and y. We wish to quantify the proportion of legitimate questions for which the strategy provides a correct answer. For

a given game G, we formally define the maximum success proportion $\tilde{\omega}(G)$, over all deterministic strategies as

$$\tilde{\omega}(G) = \max_{f,g} \frac{\#\{(x,y) \in P | (x, y, f(x), g(x)) \in W\}}{\#P}. \tag{5}$$

The maximum success proportion for a deterministic strategy can be related easily to the maximum probability of success in a probabilistic game. These classical *probabilistic* strategies are considered successful with probability p if they produce a correct answer with minimal probability p on all legitimate questions. For a game G, $\omega(G)$ denotes the maximum success probability, over all classical probabilistic strategies, given formally by

$$\omega(G) = \max_{s} \min_{(x,y) \in P} \Pr_s(\text{win} | (x, y)). \tag{6}$$

With these definitions, we can relate correlations from classical probabilistic strategies to deterministic ones.

Theorem 5 (BBT04) *Let G be a game. Consider any probabilistic strategy s. If the questions are asked uniformly at random among all legitimate questions, the probability that the players win using s is $\tilde{\omega}(G)$ at best. Furthermore, for any game G, $\omega(G) \leq \tilde{\omega}(G)$.*

This theorem implies that correlations from probabilistic strategies succeed over classical ones. We know, however, that correlations from entanglement trump those of randomized strategies. Our following two examples demonstrates this idea explicitly.

3.1 Mermin-Peres Magic Square Game

Alice and Bob participate in a two-player coordination game where they must fill a 3×3 table with $+$ and $-$ signs, but are forbidden to communicate. Such a grid might look like this[1]:

+1	+1	+1
+1	-1	-1
-1	+1	?

[1]Figure from `http://en.wikipedia.org/wiki/File:Mermin-Peres_magic_square.png`

In each round, Alice selects a row and Bob selects a column: they must fill entry with the common row and column with the same sign. Furthermore, Alice must fill the remainder of the row such that there is an even number of $-$'s, and Bob must fill the remainder of the column such that there is an odd number of $+$'s. Prior agreement on a specific table is not possible, as such tables actually violate the rules of the game (see the square above). Because such agreed-upon squares are *magic*, a classical strategy for winning the game is absolutely impossible.

On the other hand, Alice and Bob *can* succeed at the game by sharing entangled state composed of two Bell states,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle_3 |0\rangle_4 + |1\rangle_3 |1\rangle_4\right), \tag{7}$$

and making measurements in the Pauli basis to give the table values. The observables for the outcomes of these measurements be given by tensor products of Pauli matrices,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{8}$$

which each have measurement eigenvalues of either $1\,(+)$ or $-1\,(-)$. They carry out the measurement following this table, where the product of the observables in any row or column is equal to $\pm I$, thereby allowing them to satisfy the rules of the game.

$1 \otimes \sigma_z$	$\sigma_z \otimes 1$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes 1$	$1 \otimes \sigma_x$	$\sigma_x \otimes \sigma_x$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$

(9)

3.2 The Mermin-GHZ Game

The magic square parity game can be extended to a more general game involving n players as follows [7].

Definition 1 (Mermin-GHZ) *For any $n \geq 3$, a game G_n involves n players, where each player receives an input x_i and must produce an output y_i. The players are promised that there is an even number of 1's amongst them and are asked to produce an output such that*

$$\sum_{i=1}^{n} y_i = \frac{1}{2}\sum_{i=1}^{n} x_i \,(mod\ 2)\,. \tag{10}$$

Using the definition of $\omega(G)$, it can be shown that there exists a classical strategy for game G_n that is successful with probability at most $\frac{1}{2}+2^{-\lceil n/2 \rceil}$. This implies that the best classical strategy can be no better than using a fair coin toss. Entanglement correlations, however, win this game with certainty.

Theorem 6 *If the n players are allowed to share prior entanglement, then they can always win game G_n*

Proof: Consider two n-qubit entangled quantum states

$$\left|\psi_n^+\right\rangle = \frac{1}{\sqrt{2}}\left(|0^n\rangle + |1^n\rangle\right) \qquad \left|\psi_n^-\right\rangle = \frac{1}{\sqrt{2}}\left(|0^n\rangle - |1^n\rangle\right) \tag{11}$$

and the Hadamard H and phase gates P specified by

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{12}$$

Applying the Hadamard gates to each qubit in $|\psi_n^+\rangle$ and $|\psi_n^-\rangle$ yields an equal superposition of all even and odd n-bit strings, respectively:

$$\left(H^{\otimes n}\right)\left|\psi_n^+\right\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{\text{y even}}|y\rangle \qquad \left(H^{\otimes n}\right)\left|\psi_n^-\right\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{\text{y odd}}|y\rangle \tag{13}$$

. Furthermore, applying P to any two qubits in $|\psi_n^+\rangle$ yields $|\psi_n^-\rangle$ (and vice versa); applying P to any four qubits of $|\psi_n^\pm\rangle$ leaves the global state undisturbed. Therefore, if n players have qubits $|\psi_n^+\rangle$, and exactly m of them apply P to their state, the global state is $|\psi_n^+\rangle$ if $m \equiv 0 \,(\text{mod } 4)$, and $|\psi_n^-\rangle$ if $m \equiv 2 \,(\text{mod } 4)$. The players then follow the strategy to win with certainty:

1. If $x_i = 1$, apply P to qubit.
2. Apply H to qubit.
3. Measure qubit in the $\{|0\rangle, |1\rangle\}$-basis in order to obtain x_i.
4. Produce y_i.

The first step implies that an even number of players will apply P to their qubit. If that number is divisible by 4 (i.e., $\frac{1}{2}\sum_i x_i$ is even), then the global state is $|\psi_n^+\rangle$ after step 1 and an even superposition of $|y\rangle$ after step 2. Therefore, the number $\sum_i y_i$ of players who measure and output 1 is even.

If the number of players is only even and not divisible by 4 (i.e., $\frac{1}{2}\sum_i x_i$ is odd), then the resulting state is $|\psi_n^-\rangle$ after step 1, and the superposition over $|y\rangle$ following the Hadamard step is odd. In this case, $\sum_i y_i$ is odd and the condition is satisfied.

□

3.3 Conclusion

In the preceding, we have given an overview of the complexity costs, limitations, and capabilities of quantum communication between parties sharing entanglement. Our two cases, lower bounds for total Boolean functions and the quantum psuedo-telepathy games leave a lot of low-hanging fruit for potential research problems. For example, it is not generally known if there exists a total function f for which a quantum communication protocol would be more efficient than a classical one. The latter is particularly interesting, as (far as I can tell) there is currently no criterion for determining if a particular game pseudo-telepathic or not.

References

[1] A. C. chih Yao, Quantum circuit complexity 1.

[2] R. Cleve and H. Buhrman, Substituting quantum entanglement for communication, 1997.

[3] H. Buhrman, W. van Dam, P. Hoyer, and A. Tapp, Physical Review A **60**, 2737 (1999).

[4] R. Raz, Exponential separation of quantum and classical communication complexity, in *STOC '99: Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pp. 358–367, New York, NY, USA, 1999, ACM.

[5] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, Lecture Notes in Computer Science **1509**, 61 (1999).

[6] H. Buhrman and R. D. Wolf, Communication complexity lower bounds by polynomials, in *in Proceedings of the 16th Annual IEEE Conference on Computational Complexity*, pp. 120–130, 2001.

[7] G. Brassard, A. Broadbent, and A. Tapp, FOUNDATIONS OF PHYSICS **11**, 1877 (2004).