Quantum Computing and Communication Complexity

Harry Buhrman*
Center for Mathematics and Computer Science
Quantum Computing and Advanced Systems Research
P.O. Box 94079, NL-1098 GB Amsterdam, The Netherlands.
buhrman@cwi.nl

January 18, 2000

Abstract

Quantum computing combines the framework of *quantum mechanics* with that of computer science. In this paper we give a short introduction to quantum computing and survey the results in the area of quantum *communication complexity*.

1 Introduction

One of the main areas of research in theoretical computer science is complexity theory. Complexity theory deals with questions like how much time or other resources are needed to perform a certain computational task. The P versus NP problem is probably the best known incarnation of this type of question. Its current research however ranges from lower bounds for circuits and related computational objects to for example investigations of logical proof systems and bounded arithmetic.

An important tool for attacking these questions is the concept of *Communication Complexity*, introduced by Abelson and Yao [Abe80, Yao79]. Communication complexity deals with the following scenario. There are two parties usually called Alice and Bob. Alice has as input an n bit string x and Bob an n bit string y. They can only see their own input but are allowed to send messages back and forth. Their goal is to compute some function $f(x, y) \mapsto \{0,1\}$ *minimizing* the amount of bits communicated. For example they have to figure out whether they both have the *same* input strings, i.e. whether $x = y$.

Quantum mechanics is currently the most accurate theory of nature. Although it sometimes is very counter intuitive there have been no violations of this theory and experiment has been in agreement with its predictions.

Quantum computing combines quantum mechanics and computation into one theory of computation. The field gained momentum when Peter Shor [Sho94, Sho97] discovered a polynomial time quantum algorithm for the factorization problem. In this paper we review part of this theory and survey some of the results that deal with Quantum Communication Complexity.

We will now first describe in a nutshell quantum mechanics and its relevance for computation.

2 Quantum Mechanics and Computing

One of the main, and very counterintuitive, features of quantum mechanics is the *superposition* principle. A physical system may be in a superposition of two or more *different* states at the same time. Quantum mechanics prescribes that when we observe such a system we will see one of these states with a certain probability resulting in a collapse of the system into the state that we observed.

*Partially supported by the EU through the 5th framework program FET.

2.1 Qubits, Superposition, and Measurement

Let us concentrate now to computation. Classically a bit can be in any of two states: 0 or 1. Quantum mechanically a quantum bit or qubit may be in a superposition of both 0 and 1. It is useful to describe such systems as vectors in a finite dimensional Hilbert space, in this case a two dimensional one. We will identify the vector $\begin{bmatrix}1\\0\end{bmatrix}$ with $|0\rangle$ to denote the classical bit 0 and vector $\begin{bmatrix}0\\1\end{bmatrix}$ with $|1\rangle$ denoting the classical bit 1. This notation is called Dirac or ket notation from bra-ket. The bra is $\langle|$ and $\langle a|b\rangle$ denotes the inner product between a and b. Quantum mechanics now allows for a superposition of these two classical states:

$$\alpha|0\rangle + \beta|1\rangle \tag{1}$$

Where α and β, called *amplitudes*, are complex numbers with the property that:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

Next *observing* or *measuring* a qubit $\alpha|0\rangle + \beta|1\rangle$ will yield outcome 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. Moreover after this measurement the qubit is either in the classical state $|0\rangle$ when we measured a 0, and in $|1\rangle$ when we measured a 1. Note that equation 2 guarantees that a qubit, when measured, indeed induces a probability distribution over 0 and 1.

Let's try to plug in some values for α and β:

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{3}$$

Observing this qubit will result with probability 0.5 in seeing a 0 and with probability 0.5 in a 1.

In general our system will consist of more than just one qubit. Equations 1 and 2 generalize in the obvious way. Suppose we want to model k qubits. Classically k *bits* can be in any of 2^k different configurations: $1 \ldots 2^k$. This means that k *qubits* can be in a superposition of all, or part, of these 2^k basis states:

$$\alpha_1 \overbrace{|00\ldots0\rangle}^{k} + \ldots + \alpha_{2^k} \overbrace{|11\ldots1\rangle}^{k} = \sum_{i\in\{0,1\}^k} \alpha_i|i\rangle \tag{4}$$

with the additional requirement that:

$$\sum_{i\in\{0,1\}^k} |\alpha_i|^2 = 1 \tag{5}$$

When observing these k qubits we will see i with probability $|\alpha_i|^2$.

If we have two qubits $|x\rangle$ and $|y\rangle$ then $|x\rangle \otimes |y\rangle$ are the two qubits in a 4 dimensional Hilbert space. This construction is called the tensor or Kronecker product:

$$\begin{aligned} |x\rangle \otimes |y\rangle &= (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle - \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle. \end{aligned}$$

by convention $|0\rangle \otimes |0\rangle$, $|0\rangle|0\rangle$, and $|00\rangle$ will mean the same thing.

In general not all the 2 qubit states that satisfy equations 2 and 4 are obtained as the tensor of two qubits. We will see an important example, the EPR-pair, in subsection 2.3. Such states are called *entangled*.

2.2 Unitary Operations

Next we would like to model operations on qubits. Quantum mechanics tells us that these operation have to be modeled as *linear* operations with the additional constraint that these operations preserve the probability interpretation, that is the squares of the amplitudes sum up to 1 (see equations 2 and 5). Such transformations are called *unitary* and can be stated in purely mathematical terms:

$$UU^* = I \tag{6}$$

Where U^* is the complex conjugate transpose of U and I is the identity matrix. In terms of computation the unitary constraint implies that the computation is *reversible*.

The following transformation on a single qubit is important and very useful. It is called the Hadamard transform.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{7}$$

It is a unitary operation since:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Now let's do a Hadamard operation on a qubit that is in the classical state $|0\rangle$:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{8}$$

This is in ket notation: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ which is the random qubit from equation 3. When we apply the Hadamard transform again on this qubit:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} + \frac{1}{2} \\ \frac{1}{2} - \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{9}$$

We get the $|0\rangle$ again. The important thing to notice is the minus sign in the Hadamard transform. Its effect is illustrated in the above equation 9. The minus sign caused the $\frac{1}{2} - \frac{1}{2}$ in the lower half of the vector to cancel out, or destructively interfere, while both terms in the upper half constructively interfered. It is both the superposition principle together with this interference behavior that gives quantum computing its power.

The tensor product is also defined on linear operations. In general if we have an $m \times n$ matrix A and an $n' \times m'$ matrix B then $A \otimes B$ is a $(m \cdot m') \times (n \cdot n')$ matrix defined as:

$$\begin{bmatrix} a_{1,1} \cdot B & a_{1,2} \cdot B & \dots & a_{1,n} \cdot B \\ a_{2,1} \cdot B & a_{2,2} \cdot B & \dots & a_{2,n} \cdot B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} \cdot B & a_{m,2} \cdot B & \dots & a_{m,n} \cdot B \end{bmatrix}$$

2.3 Einstein-Podolsky-Rosen paradox

In the section 2.1 we have seen that any set of k qubits is admissible if it satisfies equations 4 and 5. Bearing this in mind let's examine the following state consisting out of 2 qubits:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{10}$$

Note that the first 0 and the first 1 form the first qubit and the second 0 and the second 1 form the second qubit. This state is called the EPR state after their inventors Einstein, Podolsky, and Rosen [EPR35]. The purpose of this state was to devise a thought experiment to show the incompleteness of quantum mechanics. Imagine that we have this EPR state and that Alice has the first qubit somewhere on Mars and that Bob has the second, say, here on earth. If Alice measures her qubit she will see a 0 or a 1 with equal probability and the state will have collapsed to either $|00\rangle$, if she saw a 0 or $|11\rangle$ in case it was a 1. The same is true for Bob. This leads to the following situation. Suppose that the first qubit, on Mars, was measured first and that Alice saw a 1. This now means that when Bob measures his qubit he will also measure a 1. It appears that information, i.e. the outcome of Alice's measurement, has somehow traveled to earth *instantaneously*. Since nothing can travel faster than the speed of light something must be wrong.

The EPR paradox has been, and still is, a subject of dispute. Much progress was made when Bell [Bel64] came up with a test that would, in case quantum mechanics was correct, show correlations that could not be explained with just classical reasoning. This test has been done in the lab [ADR82] and these non-classical correlations have been observed.

In the following we will see that this EPR paradox cast in a quantum communication complexity setting sheds some more light on the matter. As we will see it turns out that EPR pairs can not be used to reduce communication but they can be used to reduce *communication complexity*.

In the next section we will see another feature of EPR pairs: teleportation.

3 No-Cloning and Teleportation

Classical bits can be copied. Qubits on the other hand can *not* be copied [WZ82].

Theorem 1 *[WZ82] Qubits can not be copied*

The reason for this is that the copy-qubit operation is not linear and hence not unitary. Suppose we had a linear operation U_c that would copy a qubit. That means on state $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle$ it would do the following:

$$\begin{aligned} U_c[(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle] &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) & (11) \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle & (12) \end{aligned}$$

On the other hand since U_c is linear and because $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle$:

$$U_c[\alpha|00\rangle + \beta|10\rangle] = \alpha|00\rangle + \beta|11\rangle \qquad (13)$$

It is clear that equation 12 and 13 are the same if and only if $\alpha = 1$ and $\beta = 0$ or $\alpha = 0$ and $\beta = 1$. Which is precisely the case if we have a classical 0 or 1. Hence there can not be a linear operation that copies an arbitrary unknown qubit.

Now imagine that Alice has an unknown qubit $x = \alpha|0\rangle + \beta|1\rangle$ that she wants to send to Bob and that she furthermore can only communicate using classical bits. Is it, in this case, possible for Alice to communicate x to Bob? In the light of the no-cloning Theorem 1 it certainly is impossible to do this since whenever she measures x she will destroy/collapse it to a classical bit and she can not copy it first. But suppose that Alice and Bob in addition each share one half of an EPR-pair (see equation 10). The surprising thing is that there is a scheme that allows Alice to send or teleport x to Bob using only 2 classical bits [BBC$^+$93].

In operational terms the scheme works as follows. Let ϕ^+ be the first part of an EPR-pair and ϕ^- the other half. That is ϕ^+ is the first bit of $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$ and ϕ^- the second bit.

Alice has ϕ^+ and Bob has ϕ^-. At some point Alice gets the unknown qubit $x = \alpha|0\rangle + \beta|1\rangle$. She now does a unitary operation[1] on the two qubits, ie ϕ^+ and x. Then she measures these two qubits obtaining two bits: 00, 01, 10, or 11. Next she send these two bits to Bob who depending on the two bits does one of four unitary operations on his ϕ^-. It turns out that this last unitary operation on ϕ^- has changed [2]into the unknown qubit x. After the protocol the EPR-pair is destroyed, so in order to repeat this procedure a fresh EPR-pair is needed.

The important point for communication complexity is that this teleportation scheme is a way to simulate a qubit channel between Alice and Bob with a classical channel, at the cost of two bits per qubit, whenever Alice and Bob share EPR-pairs.

Theorem 2 *[BBC$^+$93] When Alice and Bob share EPR-pairs, they can simulate a qubit channel with a classical bit channel at the cost of two classical bits per qubit.*

[1] The unitary operation is a controlled-not of x on ϕ^+, followed by a Hadamard on x.

[2] In fact after the controlled-not and the Hadamard transform of Alice, it follows that their joint state is: $|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)$. This means that after Alice does her measurement, the third bit ie ϕ^- is the unknown qubit x up to a possible bit flip and/or phase shift depending on the outcome of Alice's measurement.

4 Quantum Communication Complexity

One of the main themes in quantum information processing is to extend classical communication and communication schemes with quantum ones. Here we will consider three models of quantum communication and compare them with classical communication.

1. Communication is done with qubits.
2. Both parties share EPR-pairs but communication is done via a classical bit-channel.
3. Both parties share EPR-pairs and communication is done with qubits.

4.1 Communication

The most simple form of communication is that where Alice wants to send a message m of say k bits to Bob. We know that classically in general Alice needs to send k bits to Bob. Is this still true in the setting 1, 2, and 3? It follows from a theorem of Holevo [Hol73] that when only qubits are used for communication Alice still needs to send k qubits. Moreover Cleve et.al. [CvDNT98] show that the same is true when both parties share EPR-pairs and classical communication is used.

For the third variant, where both EPR-pairs and qubits are used, things are slightly different. Bennett and Wiesner [BW92] show that in this case there is a kind of a reverse of Theorem 2. This is a scheme, called super dense coding, that allows Alice to send *two* classical bits with one qubit to Bob provided they share an EPR-pair. It can be shown that like Holevo's theorem this is optimal.

We will next see that the situation is quite different in the setting of communication complexity.

4.2 Communication Complexity

Communication Complexity was introduced by Yao and Abelson [Abe80, Yao79]. Alice and Bob each have an n bit string x and y and their goal is to compute some function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ minimizing the number of bits they communicate to each other. The area of communication complexity is well studied see for example the book by Kushilevitz-Nisan [KN97]. The question we want to address here is how does the communication complexity of certain problems vary when different models of quantum communication are used. We will denote $C(f)$ to denote the classical communication complexity of f. That is the number of bits the optimal protocol uses on the worst-case input. The model where only qubits can be used for communication (model 1, Section 4.1) was introduced by Yao [Yao93]. We will use $Q(f)$ for the quantum communication complexity in the model where only qubits are used for communication. The first results in that model were lower bounds or impossibility results due to Yao and Kremer [Kre95] and we will discuss them in Section 4.3.

The model where the communication is classical but both parties share entanglement, model 2, was introduced by Cleve and Buhrman [CB97]. We will denote the communication complexity in this model with $C^*(f)$, the model which uses both EPR-pairs and qubits will be $Q^*(f)$. Cleve and Buhrman were the first to show that communication complexity can be reduced contrary to what one might believe considering Holevo's theorem. Their setting differed slightly from the models we discuss here. In this setting they exhibit an example of a *three party* communication problem where the three parties share an entangled state, like an EPR-pair but then for three parties. It is shown that when the parties share this entangled state the communication problem can be solved with two bits of communication whereas without such a prior shared state three bits are necessary. That is there is a function f such that $C^*(f) = 2$ whereas $C(f) \geq 3$. Better separations in the multiparty setting were found in [BCvD97] and [BvDHT99]. The latter paper exhibits a function f for k parties such that $C^*(f) = k$ and $C(f) = \Omega(k \log(k))$.

Next we will turn our attention to the qubit communication model $Q(f)$. However keep in mind that protocols for this model can be translated to the model where both parties share EPR-pairs and communicate classically, since via teleportation, Theorem 2 gives us: $2C^*(f) \leq Q(f)$.

The first gap for two-party qubit communication complexity was demonstrated by Buhrman, Cleve, and Wigderson [BCW98]. They showed for a promise version of the equality problem[3], EQ' see section 5.2 for a definition, that $Q(EQ') = O(\log(n))$ and that also $C(EQ') = \Omega(n)$. This exhibits an exponential gap between classical and quantum communication complexity. In section 5 we will show in more detail how the protocol works

4.2.1 Bounded Error Protocols

All the above (quantum) protocols don't make errors and compute the outcome exactly. When studying randomized versions of communication complexity however it is unavoidable to introduce errors. A classical randomized protocol for f, $R_2(f)$, is a protocol where both Alice and Bob can use random bits. They are required to compute the correct outcome with probability at least 2/3. The distinction between private and public random bits can be made, where in the public bit/coin model Alice and Bob see the same random bits and in the private they each have a different random source. Newman [New91] has shown that up to an additive logarithmic term the models are the same.

Rabin and Yao show for EQ that there exists a classical randomized protocol that only needs $O(\log(n))$ bits: $R_2(EQ) = O(\log(n))$. This implies that the promise problem EQ' also has a $O(\log(n))$ randomized classical bit protocol that is correct with probability at least 2/3. Note however that the quantum protocol never makes an error.

The disjointness problem $DISJ$ is defined as follows. Alice and Bob each have a subset A and B of $\{0,1\}^n$, they have to decide whether $A \cap B = \emptyset$. Kalyanasundaram and Schnitger [KS92] show that this problem also has high communication complexity in the randomized setting: $R_2(DISJ) = \Omega(n)$.

Buhrman, Cleve and Wigderson in the same paper show that when we allow the quantum protocol to compute the answer with probability at least 2/3, we denote this by $Q_2(f)$, that $Q_2(DISJ) = O(\sqrt{n}\log(n))$. Exhibiting an almost quadratic gap between classical randomized and quantum communication complexity. Moreover this is the only example of a gap known where the function f is not a promise problem.

The biggest gap between the randomized and the quantum model was obtained by Ran Raz [Raz99]. He showed that there is a promise problem f such that $Q(f) = O(\log(n))$ but $R_2(f) = \Omega(\sqrt{n})$.

Theorem 3 *The best known gaps between Quantum and Classical communication complexity are:*

1. *There exists a promise problem EQ', such that $Q(EQ') = O(\log(n))$ but $C(EQ') = \Omega(n)$ [BCW98].*
2. *There exists a promise problem f, such that $Q(f) = O(\log(n))$ but $R_2(f) = \Omega(\sqrt{n}$ [Raz99].*
3. *$Q_2(DISJ) = O(\sqrt{n}\log(n))$ [BCW98] and $R_2(DISJ) = \Omega(n)$ [KS92].*

Ambainis et. al. [ASTS+98] also exhibit an exponential gap between quantum protocols and classical protocols for a different form of communication problem called sampling which we shall not discuss here further.

Summarizing for promise problems there exist exponential gaps between classical and quantum communication complexity. For total problems the best known gap is only nearly quadratic. In turn this sheds some light on the EPR-paradox. Holevo's theorem proves that EPR-pairs can not be used to reduce communication. Since all the protocols in this section work for the model where the parties share EPR-pairs and communicate classically it follows that EPR-pairs can reduce the communication complexity of certain problems. This situation seems contradictory but notice that the actual amount of information that needs to be communicated between Alice and Bob is only 1 bit, namely the outcome of f.

4.3 Lower Bounds

In the previous section we showed that quantum communication protocols are sometimes superior to classical protocols. In this section we examine the converse and turn our attention to lower bounds for quantum communication complexity.

[3] $EQ(x,y) = 1$ if $x = y$ and 0 otherwise. EQ requires n bits of communication. A promise version of a problem means that Alice and Bob are only required to compute the answer correctly on certain instances that fall within the promise and it doesn't matter what they compute on the other instances that don't satisfy the promise.

Classically for deterministic communication complexity there is a general technique for proving lower bounds. For any function $f : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}$ one can define the boolean $2^n \times 2^n$ communication matrix $M_f(x,y) = f(x,y)$. Mehlhorn and Schmidt [MS82] related the rank of this matrix to the communication complexity. They show that $\log(\text{rank}(M_f)) \leq C(f)$. This is a very useful tool. Take for example the equality problem. The communication complexity matrix for EQ is the $2^n \times 2^n$ identity matrix which has only 1's on the diagonal and is 0 on off-diagonal entries. Since this matrix has rank 2^n it follows that $C(f) \geq n$.

A similar statement is true in the quantum setting:

Theorem 4 *For any communication problem f:*

1. $\log(rank(M_f))/2 \leq Q(f)$ *[Kre95].*
2. $\log(rank(M_f)) \leq C^*(f)$ *[BdW99].*
3. $\log(rank(M_f))/2 \leq Q^*(f)$ *[BdW99].*

A natural and long standing open problem is whether the communication complexity is also a lower bound for the log-rank. That is whether the log-rank characterizes the communication complexity. The biggest known gap between the log-rank and the communication complexity is almost quadratic [NW95]. The log-rank conjecture states that for every total f, $\log(\text{rank}(f))$ and $C(f)$ are all polynomially related.

It follows from Theorem 4 that if the log-rank conjecture is true then for total f: $Q(f), C^*(f), Q^*(f)$, and $C(f)$ are polynomially related.

The log rank lower bound method only works well for errorless protocols. For bounded error models there is another bound called *discrepancy*. Kremer [Kre95] and Yao show that the discrepancy bound also works for the bounded error qubit communication model Q_2. This enables them to show a linear lower bound in this model for a problem called inner product modulo 2, IP. Here $IP(x,y) = x_1 \cdot y_1 + \cdots + x_n \cdot y_n \mod 2$. Ambainis et. al. [ASTS$^+$98] extend this bound to also yield a $\Omega(n)$ bound even when Alice and Bob are allowed to make an error which is very close to 1/2.

For the model where both parties share EPR-pairs, Cleve et. al. [CvDNT98] were the first to show a linear lower bound for IP. They came up with a new technique that is essentially quantum mechanical in nature. It can be seen as a quantum adversary argument. This enabled them to show that any (quantum) protocol for IP can be (ab)used, when run in superposition, to communicate n bits from Alice to Bob. Let $Q_2^*(f)$ denote the communication complexity of f where Alice and Bob compute f correctly with probability 2/3, they share EPR-pairs and the communication is with qubits.

Theorem 5 *1.* $Q_2(IP) = \Omega(n)$ *[Kre95].*

2. $Q_2^*(IP) = \Omega(n)$ *[CvDNT98].*

Theorem 4 yields a lower bound of $\Omega(n)$ for $DISJ$ in the errorless models since the M_{DISJ} has rank 2^n. In the bounded error setting however the best known lower bound is $\Omega(\log(n))$ [BdW99].

5 Quantum Computation and Communication Complexity

In this section we will explain in more detail how to reduce the communication complexity of certain functions in the quantum model. The main idea is to use a quantum algorithm that outperforms any classical algorithm.

5.1 Quantum Black-Box Computation

perhaps the simplest form of a computational task is the following. Suppose we have n boolean variables $X_0, \ldots, X_{n-1}$, and we want to compute a property $P(X_0, \ldots, X_{n-1})$. The goal is to compute P with the minimum amount of variables we look at. For example suppose $P(X_0, \ldots, X_{n-1}) = 1$ iff there exists an i such that $X_i = 1$. That is we want to compute the $OR(X_0, \ldots, X_{n-1})$. How many variables do we have to query? It is not too hard to see that we have to look at all the variables. A similar kind of reasoning shows that also in the randomized setting the bound is $\Omega(n)$. It has been shown by Grover [Gro96] that a quantum algorithm can solve the OR with only $O(\sqrt{n})$ quantum queries.

Next we will turn our attention to another problem that allows even an exponential speed up. Define the following promise on the variables. We are guaranteed that they are either constant: all the X_i are either all 0 or all 1. Or they are balanced: exactly half the X_i are 0 and the other half is 1. The problem is to find out whether the variables are constant or balanced.

It is easy to see that classically this problem requires $n/2+1$ queries to the variables. One of the first quantum algorithms by Deutsch and Jozsa [Jos92] establishes that this problem can be solved with just a single quantum query! Before we demonstrate this algorithm we first have to explain how we model a quantum query.

5.1.1 Quantum Query

We have to model a quantum query in such a way that it is a unitary operation. We define a quantum query to variable X_i as follows. The query $|i,0\rangle$ becomes after the query $|i,X_i\rangle$, and $|i,1\rangle$ becomes $|i,1-X_i\rangle$. That is for $1 \leq i \leq n$ and $b \in \{0,1\}$:

$$|i,b\rangle \mapsto |i,b \oplus X_i\rangle \tag{14}$$

It can be easily checked that this operation is unitary. Since this describes what a query does on basis states, because of linearity it also works on states that are in superposition:

$$\sum_{i\in\{0,1\}^{\log(n)}} \alpha_i|i,b_i\rangle \mapsto \sum_{i\in\{0,1\}^{\log(n)}} \alpha_i|i,b_i \oplus X_i\rangle \tag{15}$$

for $b_i \in \{0,1\}$

5.1.2 The Deutsch-Jozsa Algorithm

Suppose n is a power of 2 and $l = \log(n)$. We start in a state with l 0's followed by a 1:

$$|0^l 1\rangle \tag{16}$$

Remember the Hadamard transform H on one qubit from equation 7. Next we do a Hadamard transform on all the qubits of the state. That is the following operation $\overbrace{H \otimes H \otimes \ldots \otimes H}^{l+1} = H^{\otimes l+1}$. This will result in the following state:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} |i\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{17}$$

Then we perform the only quantum query. This will effect our state according to equation 15 as follows:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} (-1)^{X_i}|i\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{18}$$

To see that this is correct first observe that we perform the quantum query with the target qubit in superposition $(|0\rangle-|1\rangle)$ This means that state $|i\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ after the query becomes $|i\rangle\frac{1}{\sqrt{2}}(|0\oplus X_i\rangle-|1\oplus X_i\rangle)$. Furthermore if X_i is 0 then this is simply $|i\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, on the other hand if $X_i = 1$ then it becomes $|i\rangle\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$ which is the same as $(-1)|i\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Hence we get a factor of -1 iff $X_i = 1$. Next we apply again $H^{\otimes l+1}$ to the state and obtain the following messy looking expression:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} \frac{1}{\sqrt{n}} \sum_{j\in\{0,1\}^l} (-1)^{X_i \oplus (i,j)}|j\rangle|1\rangle \tag{19}$$

Where (i,j) is the inner-product between i and j modulo 2. Let's take a closer look at the part of this sum where $j = 0^l$:

$$\frac{1}{n} \sum_{i \in \{0,1\}^l} (-1)^{X_i} |0^l\rangle|1\rangle \tag{20}$$

Suppose that all the $X_i = 0$ and we are in the constant 0 case. Then equation 20 boils down to: $\frac{1}{n}\sum_{i\in\{0,1\}^l} |0^l\rangle|1\rangle = |0^l1\rangle$. For the constant 1 case we will end up in $(-1)|0^l1\rangle$. This means that when we observe the final state in equation 19 we will see 0^l1 with probability 1.

On the other hand if half of the $X_i = 1$ and the other half are 0 then half of the terms in equation 20 are 1 and the other half are -1 and cancel each other out. The result of this is that $|0^l1\rangle$ has amplitude 0 and will be seen with probability 0.

So by observing state 19 we can conclude that if we observe 0^l1 we are in the constant case and if we observe anything else we are in the balanced case.

5.2 The Communication Problem and Protocol

The idea for the communication complexity problem is to use the Deutsch-Jozsa algorithm from the previous section in a distributed manner.

This boils down to the following communication complexity problem EQ'. $EQ'(x,y) = 1$ iff $x = y$ but with the extra promise that it will always be the case that the Hamming distance $\Delta(x,y) = 0$ or $n/2$. The Hamming distance between two strings x and y, $\Delta(x,y)$, is the total number of bits where x and y are different. It can be shown [BCW98] that $C(EQ') = \Omega(n)$ using a deep and surprising combinatorial theorem from Frankl and Rödl [FR87].

Next we will see that EQ' can be solved with just $\log(n)+1$ qubits of communication from Bob to Alice. Note that under the Hamming distance promise, Alice and Bob have to figure out whether $x_1 \oplus y_1 \ldots x_n \oplus y_n$ is constant or balanced, since in the constant 0 case $x = y$ and in the balanced $x \neq y$. So if we set $X_i = x_i \oplus y_i$ then we have the Deutsch-Jozsa problem back.

If Alice could obtain the final state from equation 19:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} \frac{1}{\sqrt{n}} \sum_{j\in\{0,1\}^l} (-1)^{X_i \oplus (i,j)} |j\rangle|1\rangle \tag{21}$$

she would do a final measurement and know the answer. To this end Bob prepares the following state:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} |i\rangle \frac{1}{\sqrt{2}}(|0 \oplus y_i\rangle - |1 \oplus y_i\rangle) \tag{22}$$

and sends these $\log(n) + 1$ qubits to Alice. Alice then performs the unitary transformation that changes state $|i\rangle|b\rangle$ to $|i\rangle|b \oplus x_i\rangle$ resulting in state:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} |i\rangle \frac{1}{\sqrt{2}}(|0 \oplus y_i \oplus x_i\rangle - |1 \oplus y_i \oplus x_i\rangle) \tag{23}$$

which is after we rewrite it *precisely* the state from equation 18:

$$\frac{1}{\sqrt{n}} \sum_{i\in\{0,1\}^l} (-1)^{X_i} |i\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{24}$$

Next Alice proceeds as in the Deutsch-Josza algorithm and applies $H^{\otimes \log(n)+1}$ and measures the final state.

The general idea is to use a quantum black-box algorithm in a distributed setting. Whenever the black-box algorithm wants to make a query, Alice and Bob exchange a round of $\log(n) + 1$ qubits and Alice continues the black-box algorithm. This allows one in general to use any black-box algorithm as a communication protocol. In this way it can be shown that, by using Grover's algorithm [Gro96] the Disjointness problem can be solved with $O(\sqrt{n}\log(n))$ many qubits [BCW98].

6 Open Problems

We have surveyed some of the results in quantum communication complexity. Many problems however remain. What is the relationship between the various models, Q, C^*, Q^* both in the errorless and in the bounded error setting? For the errorless models, a positive answer to the log-rank conjecture shows that they are all polynomially related but also this is at the moment still wide open.

We have seen that exponential gaps between classical and quantum communication complexity problems are possible, however all of these examples entailed promise problems. Can there also be exponential gaps for total problems in the bounded error setting?

What is the quantum lower bound for the $DISJ$ problem? The best known lower bound is $\Omega(\log(n))$ whereas the upper bound is $O(\sqrt{n}\log(n))$.

References

[Abe80] H. Abelson. Lower bounds on information transfer in distributed computations. *J. Assoc. Comput. Mach.*, 27(2):384–392, 1980. Earlier version in FOCS'78.

[ADR82] A. Aspect, J. Dalibard, and G. Roger. . *Phys. Rev. Lett.*, (49):1804, 1982.

[ASTS$^+$98] A. Ambainis, L. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson. The quantum communication complexity of sampling. In *39th IEEE Symposium on Foundations of Computer Science*, pages 342–351, 1998.

[BBC$^+$93] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physiscal Review Letters*, 70:1895–1899, 1993.

[BCvD97] H. Buhrman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. accepted for SIAM journal on Computing, see http://xxx.lanl.gov/abs/quant-ph/9705033, may 1997.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *The Thirtieth Annual ACM Symposium on Theory of Computing*, to appear in 1998 1998.

[BdW99] H. Buhrman and R. de Wolf. Communication complexity lower bounds by polynomials, 1999. See http://xxx.lanl.gov/abs/cs.CC/9910010.

[Bel64] J.S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1, 1964.

[BvDHT99] Harry Buhrman, Wim van Dam, Peter Høyer, and Alain Tapp. Multiparty quantum communication complexity. *Physical Review A*, 60(4):2737–2741, October 1999.

[BW92] C. Bennett and S. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physiscal Review Letters*, 69:2881–2884, 1992.

[CB97] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication complexity. *Physical Review A*, 56(2):1201–1204, august 1997.

[CvDNT98] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. In Springer-Verlag, editor, *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, 1998.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. *Phys. Rev.*, 47:777, 1935.

[FR87] P. Frankl and V. Rödl. Forbidden intersections. *Trans. Amer. Math. Soc.*, 300(1):259–286, 1987.

[Gro96] L. Grover. A fast quantum mechenical algorithm for database search. In *28th ACM Symposium on Theory of Computing*, pages 212–218, 1996.

[Hol73] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. English translation in *Problems of Information Transmission*, 9:177–183, 1973.

[Jos92] D. Deutsch R. Josza. Rapid solutions of problems by quantum computation. *Proc. Roy. Soc. London Se. A*, 439:553–558, 1992.

[KN97] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[Kre95] I. Kremer. Quantum communication. Master's thesis, Computer Science Department, The Hebrew University, 1995.

[KS92] Bala Kalyanasundaram and Georg Schnitger. The probabilistic communication complexity of set intersection. *SIAM J. Discrete Mathematics*, 5(4):545–557, 1992.

[MS82] Kurt Mehlhorn and Erik M. Schmidt. Las Vegas is better than determinism in VLSI and distributed computing (extended abstract). In *Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing*, pages 330–337, San Francisco, California, 5–7 May 1982.

[New91] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, July 1991.

[NW95] N. Nisan and A. Wigderson. On rank vs. communication complexity. *Combinatorica*, 15:557–566, 1995. Earlier version in FOCS'94.

[Raz99] R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of 31th STOC*, pages 358–367, 1999.

[Sho94] P.W. Shor. Algorithms for quantum computation: Discrete log and factoring. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, pages 20 – 22, 1994.

[Sho97] P. Shor. Polynomial-time algorithms of prime factorization and discrete logarithms. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[WZ82] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, (299):802, 1982.

[Yao79] A. C-C. Yao. Some complexity questions related to distributive computing. In *Proceedings of 11th STOC*, pages 209–213, 1979.

[Yao93] A. C-C. Yao. Quantum circuit complexity. In *Proceedings of 34th FOCS*, pages 352–360, 1993.