Some More Quantum Communication Complexity

Quantum Computing Course, November 10, 2000

1 The EQ' problem

The EQ' problem is the following: Alice receives $x \in \{0,1\}^n$ (where n is a power of 2), Bob receives $y \in \{0,1\}^n$, with the promise that either $x = y$ or the Hamming distance between x and y is $\Delta(x,y) = n/2$. We call the first kind of (x,y) '1-inputs' and the second kind '0-inputs'. The aim of Alice and Bob is to determine whether $x = y$, using as little communication as possible.

Here's a quantum protocol for EQ' with only $\log n$ qubits of communication from [BCW98], based on the Deutsch-Jozsa algorithm:

1. Alice prepares the $\log n$-qubit state $H^{\otimes \log n}|0\ldots 0\rangle$, to which she applies the unitary transformation $|i\rangle \rightarrow (-1)^{x_i}|i\rangle$. She now has the state
$$\frac{1}{\sqrt{n}} \sum_{i \in \{0,1\}^{\log n}} (-1)^{x_i}|i\rangle,$$
which she sends to Bob.

2. Bob applies $|i\rangle \rightarrow (-1)^{y_i}|i\rangle$ and now has the state
$$\frac{1}{\sqrt{n}} \sum_{i \in \{0,1\}^{\log n}} (-1)^{x_i \oplus y_i}|i\rangle.$$
Bob then applies $H^{\otimes \log n}$, measures , and outputs 1 if he observes $|0\ldots 0\rangle$, and outputs 0 otherwise.

It is not hard to see that this algorithm will always output 1 on 1-inputs and 0 on 0-inputs. The protocol takes exactly $\log n$ qubits of communication.

Any classical protocol will require $\Omega(n)$ classical bits of communication to solve EQ' with certainty. This we prove as follows. Suppose there is a c-bit classical protocol for EQ'. Every conversation induces a rectangle $R = S \times T$, with $S, T \subseteq \{0,1\}^n$, such that the protocol gives the same output on every input that is in this rectangle (this was proven in the previous lecture). Since there are at most 2^c possible conversations, the protocol partitions $\{0,1\}^n \times \{0,1\}^n$ in at most 2^c different such "monochromatic" rectangles. Now consider all x of Hamming weight $n/2$, there are roughly $2^n/\sqrt{n}$ of those. Since every (x,x)-pair must occur in some rectangle and there are only 2^c rectangles, there is a rectangle $R = S \times T$ that contains at least $2^n/\sqrt{n}2^c$ different (x,x) pairs. Let A be the set of all such x in this R. Note that for all $x, y \in A$ it holds that $\Delta(x,y) \neq n/2$, since $(x,y) \in R$ and R is monochromatic so it cannot contain 0-inputs. Viewing those x as characteristic vectors of sets, it follows that the size of the intersection of $x, y \in A$ is never $n/4$. Thus we have a set system A of $2^n/\sqrt{n}2^c$ sets, such that the size of the intersection of any two sets in A is not $n/4$. However, by Corollary 1.2 of [FR87], such a set system can have at most 1.99^n elements, so we have
$$\frac{2^n}{\sqrt{n}2^c} \leq |A| \leq 1.99^n.$$
This implies $c \geq \log(2^n/\sqrt{n}1.99^n) \geq 0.007\, n$.

2 "Spooky" protocols without any communication

Here we give an example of something which you can do with entanglement and *no* communication, using a quantum computer and EPR-pairs, and which is impossible to do classically without a lot of communication [BCT99]. It gives what can be viewed as a quantitative version of Bell's theorem, which showed that quantum mechanics cannot be simulated by classical local hidden variable theories. Note that an EPR-pair can be used to simulate a joint random coin flip: if Alice and Bob each measure their part of the EPR-pair, they get the same random bit. However, an EPR-pair is "worth more" than just a random bit, because below we describe a no-communication situation where Alice and Bob can solve a certain problem if they share EPR-pairs but not if they only share random bits.

As before, Alice and Bob receive n-bit strings x and y, respectively, with the promise that either $x = y$ or $\Delta(x, y) = n/2$. They are not allowed to communicate, but they share $\log n$ EPR-pairs. Their goal is now to output $\log n$-bit strings a and b, respectively, such that $a = b$ iff $x = y$. They can do this as follows. Initially the $\log n$ EPR-pairs are in the following state:

$$\frac{1}{\sqrt{n}} \sum_{i \in \{0,1\}^{\log n}} |i\rangle|i\rangle.$$

This is a $2 \log n$-qubit state, where the first $\log n$ qubits belong to Alice and the last $\log n$ qubits belong to Bob. Alice applies $|i\rangle \to (-1)^{x_i}|i\rangle$ to her part and Bob applies $|i\rangle \to (-1)^{y_i}|i\rangle$, giving

$$\frac{1}{\sqrt{n}} \sum_{i \in \{0,1\}^{\log n}} (-1)^{x_i}|i\rangle(-1)^{y_i}|i\rangle.$$

They now each apply Hadamard transforms to their qubits, giving

$$\frac{1}{n^{3/2}} \sum_{i \in \{0,1\}^{\log n}} \left((-1)^{x_i} \sum_{k \in \{0,1\}^{\log n}} (-1)^{i \cdot k}|k\rangle \right) \left((-1)^{y_i} \sum_{\ell \in \{0,1\}^{\log n}} (-1)^{i \cdot \ell}|\ell\rangle \right).$$

Note that the total amplitude of the state $|k\rangle|k\rangle$ is now

$$\frac{1}{n^{3/2}} \sum_{i \in \{0,1\}^{\log n}} (-1)^{x_i}(-1)^{i \cdot k}(-1)^{y_i}(-1)^{i \cdot k} = \frac{1}{n^{3/2}} \sum_{i \in \{0,1\}^{\log n}} (-1)^{x_i \oplus y_i}.$$

This amplitude will be $1/\sqrt{n}$ if $x = y$ and it will be 0 if $\Delta(x, y) = n/2$. Thus if Alice and Bob each measure their part of the state and output the resulting a, b (which are $\log n$-bit strings), then $a = b$ iff $x = y$ and they have achieved their goal.

Classically, Alice and Bob can only output $a, b \in \{0,1\}^{\log n}$ (satisfying $a = b$ iff $x = y$) if they communicate $\Omega(n)$ bits. This we prove as follows. Suppose they can solve the problem with c bits of communication. Then they can solve the EQ'-problem of the previous section using $c + \log n$ bits: they first obtain appropriate a, b (at the cost of c bits of communication) and then Alice sends a to Bob (another $\log n$ bits of communication), who compares it with his b in order to find out whether $x = y$. But then by the lower bound of the previous section we must have $c + \log n = \Omega(n)$, hence $c = \Omega(n)$. Accordingly, we have a problem which requires a lot of communication classically (this holds even if Alice and Bob share classical random bits), but requires *no* communication whatsoever if Alice and Bob have a quantum computer and share EPR-pairs — and this despite the fact that they cannot communicate using the EPR-pairs.

3 Raz's exponential separation

Note that the exponential separation for the EQ' problem (Section 1) only holds if we require the classical protocol to give the correct output always. Here we explain the first exponential separation between quantum and classical communication complexity which even holds if the classical protocol is allowed a bounded error probability, due to Raz [Raz99]. Consider the following promise problem **P**:

> Alice receives a unit vector $v \in R^m$ and a decomposition of the space R^m in two orthogonal subspaces $H^{(0)}$ and $H^{(1)}$. Bob receives an $m \times m$ unitary transformation U.
> Promise: Uv is either "close" to $H^{(0)}$ or to $H^{(1)}$.
> Question: which of the two?

As stated, this is a problem with continuous input, but it can be discretized in a natural way by approximating each real number by $O(\log m)$ bits. Alice and Bob's input is now $n = O(m^2 \log m)$ bits long. There is a simple yet efficient 2-round quantum protocol for this problem: Alice views v as a $\log m$-qubit vector and sends this to Bob. Bob applies U and sends back the result. Alice then measures in which subspace $H^{(i)}$ the vector Uv lies and outputs the resulting i. This takes only $2 \log m = O(\log n)$ qubits of communication.

The efficiency of this protocol comes from the fact that an m-dimensional vector can be "compressed" or "represented" as a $\log m$-qubit state. Similar compression is not possible with classical bits, which suggests that any classical protocol for **P** will have to send the vector v more or less literally and hence will require a lot of communication. This turns out to be true but the proof (given in [Raz99]) is surprisingly hard. It shows that any classical bounded-error protocol for **P** requires $\Omega(n^{1/4}/\log n)$ bits of communication.

4 Exercises

The *equality* function is defined as $EQ(x, y) = 1$ if $x = y$ and $EQ(x, y) = 0$ if $x \neq y$.
The *inner product* function is defined as $IP(x, y) = \sum_{i=1}^{n} x_i y_i \bmod 2$.

1. Show that if Alice and Bob share at least n random bits (coin flips), then there is a classical bounded-error protocol for the equality function, using only 1 bit of communication.
   Hint: Let r be a string of n random bits, shared by Alice and Bob. Alice sends the bit $IP(x, r)$ to Bob, who compares it with $IP(y, r)$.

2. For $n = 2$, the communication matrix of IP has x, y-entry equal to $IP(x, y)$ and looks like:

$$M_{IP} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

   Suppose we want to partition this matrix into monochromatic rectangles, how many such rectangles do we need for that?

3. Prove that a *quantum* protocol that computes IP needs $\Omega(n)$ qubits of communication.
   Hint: Consider a protocol which maps $|x\rangle|y\rangle \rightarrow (-1)^{IP(x,y)}|x\rangle|y\rangle$, and see what happens if we run this protocol when Alice has x and Bob has $\frac{1}{\sqrt{2^n}} \sum_y |y\rangle$, and afterwards Bob does a Hadamard transform on his qubits. Remember Holevo's theorem, which says that in order to communicate n classical bits, you need n qubits of communication. This solution comes from [CDNT98].

References

[BCT99] G. Brassard, R. Cleve, and A. Tapp. The cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999. quant-ph/9901035.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation (preliminary version). In *Proceedings of 30th STOC*, pages 63–68, 1998. quant-ph/9802040.

[CDNT98] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1998. quant-ph/9708019.

[FR87] P. Frankl and V. Rödl. Forbidden intersections. *Transactions of the American Mathematical Society*, 300(1):259–286, 1987.

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