Notes on
Bell's Theorem and Communication Complexity

Richard Cleve*

For a discussion of Bell's Theorem from a data processing perspective, we refer the reader to [4, 3].[1] Also, an excellent survey of quantum communication complexity can be found in [2].[2] Both [4, 2] contain fairly extensive lists of references—more complete than those provided here. In what follows, we review some of the basics of classical and quantum communication complexity, limiting our attention to three fundamental communication complexity problems: equality, intersection, and inner product.

In the communication complexity model, there are two parties, traditionally referred to as Alice and Bob, who each receive an n-bit binary string as input ($x = x_0x_1 \ldots x_{n-1}$ for Alice and $y = y_0y_1 \ldots y_{n-1}$ for Bob) and the goal is for them to determine the value of some function of the of these $2n$ bits. The resource under consideration here is the *communication* between the two parties, and an algorithm is a *protocol*, where the parties send information to each other (possibly in both directions and over several rounds) until one of them (say, Bob) obtains the answer. This model was introduced by Yao [17] and has been widely studied in the classical context (see [15] for a survey).

An interesting example is the **equality problem**, where the function is EQ, defined as

$$EQ(x, y) \quad = \quad \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \neq y. \end{cases}$$

A simple n-bit protocol for EQ is for Alice to just send her bits $x_0, \ldots, x_{n-1}$ to Bob, after which Bob can evaluate the function by himself (in fact, there is a similar n-bit protocol for *any* function). The interesting question is whether or not the EQ function can be evaluated with fewer than n bits of communication—after all, the goal here is only for Bob to acquire one bit. The answer depends on whether or not any error probability is permitted.

*Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4. Email: cleve@cpsc.ucalgary.ca. Supported in part by Canada's NSERC.

[1] Both are available at http://www.cpsc.ucalgary.ca/~cleve/papers.html.

[2] Available at http://xxx.lanl.gov/archive/quant-ph.

If Bob must acquire the value of $EQ(x, y)$ with certainty then it turns out that n bits of communication are necessary. Note that Alice sending the first $n-1$ bits of x will clearly *not* work, since the answer could critically depend on whether or not $x_{n-1} = y_{n-1}$. The number of possible protocols to consider is quite large and an actual *proof* that n bits communication are necessary is nontrivial. The interested reader is referred to [15] for a proof.

On the other hand, for probabilistic protocols (where Alice and Bob can flip coins and base their behavior on the outcomes), if an error probability of $\varepsilon > 0$ is permitted then $O(\log(n/\varepsilon))$ bits of communication are sufficient. As usual, we are not assuming anything about a probability distribution on the input strings; the error probability is with respect to the random choices made by Alice and Bob, and it applies regardless of what x and y are.

We now describe an $O(\log(n/\varepsilon))$-bit protocol for EQ. First of all, Alice and Bob agree on a finite field whose size is between n/ε and $2n/\varepsilon$ (such a field always exists, and its elements can be represented as $O(\log(n/\varepsilon))$-bit strings). Now, consider the two polynomials

$$p_x(t) = x_0 + x_1 t + \cdots + x_{n-1} t^{n-1} \quad (1)$$

$$p_y(t) = y_0 + y_1 t + \cdots + y_{n-1} t^{n-1}. \quad (2)$$

For any value of t in the field, Alice can evaluate $p_x(t)$ and Bob can evaluate $p_y(t)$. If $x = y$ then the two polynomials are identical, so $p_x(t) = p_y(t)$ for every value of t. But, if $x \neq y$ then, since $p_x(t)$ and $p_y(t)$ are polynomials of degree $n-1$, there can be at most $n-1$ distinct values of t for which $p_x(t) = p_y(t)$. Therefore, if a value of t is chosen randomly from the field then the probability that $p_x(t) = p_y(t)$ is at most $\frac{n-1}{n}\varepsilon < \varepsilon$. Now, the protocol proceeds as follows. Alice chooses a random element of the field, t, and then sends t and $p_x(t)$ to Bob (this consists of $O(\log(n/\varepsilon))$ bits). Then Bob outputs 1 if and only if $p_x(t) = p_y(t)$. If $x = y$ then Bob always outputs 1 and if $x \neq y$ then the probability that Bob erroneously outputs 1 is less than ε.

Two other interesting communication complexity problems are the **intersection problem**, where the function is IN, defined as

$$IN(x, y) = (x_0 \wedge y_0) \vee (x_1 \wedge y_1) \vee \cdots \vee (x_{n-1} \wedge y_{n-1}) \quad (3)$$

and the **inner product problem**, where the function is IP, defined as

$$IP(x, y) = (x_0 \wedge y_0) \oplus (x_1 \wedge y_1) \oplus \cdots \oplus (x_{n-1} \wedge y_{n-1}). \quad (4)$$

Intuitively, for IN, the inputs x and y can be thought as encodings of two subsets of $\{0, \ldots, n-1\}$ and the output is a bit indicating whether or not they intersect. Also, IP is the inner product of x and y as bit vectors in modulo two arithmetic. The deterministic communication complexity of each of these

problems is the same as that of EQ: any deterministic protocol requires n bits of communication. Also, it has been shown that both of these problems are more difficult than EQ when probabilistic protocols are considered: any probabilistic protocol with error probability up to (say) $\frac{1}{3}$ requires $\Omega(n)$ bits of communication (see [8] for IP, and [13] for IN; also [15]).

It is natural to ask whether any reduction in communication can be obtained by somehow using *quantum* information. Define a *quantum* communication protocol as one where Alice and Bob can exchange messages that consist of qubits. In a more formal definition of this model, there is an *a priori* system of m qubits, some of them in Alice's possession and some of them in Bob's possession. The initial state of all of these qubits can be assumed to be $|0\rangle$, and Alice and Bob can each perform unitary transformations on those qubits that are in their possession and they can also send qubits between themselves (thereby changing the ownership of qubits). The output is then taken as the outcome of some measurement of Bob's qubits. Various preliminary results about communication complexity with quantum information occurred in [4, 9, 7, 14, 18].

There are fundamental results in quantum information theory which imply that classical information cannot be "compressed" within quantum information [12]. For example, Alice cannot convey more than r classical bits of information to Bob by sending him an r-qubit message. Based on this, one might mistakenly think that there is no advantage to using quantum information in the communication complexity context. In fact, there exists a quantum communication protocol that solves IN whose qubit communication is approximately the square root of the bit communication of the best possible classical probabilistic protocol. The following result is from [5].

Theorem 1 ([5]) *There exists a quantum protocol for the intersection problem (IN) that uses $O(\sqrt{n \log(1/\varepsilon)} \log(n))$ qubits of communication and errs with probability at most ε.*

Moreover, the quantum protocol can be adapted to actually find a point in the intersection in the cases where $IN(x, y) = 1$. That is, to produce an $i \in \{0, \ldots, n-1\}$ such that $x_i \wedge y_i = 1$. This problem, like IN, has classical probabilistic communication complexity $\Omega(n)$.

The protocol in Theorem 1 can be viewed as a "distributed" version of Grover's quantum search algorithm [11] (see also [1]). To understand it, it is helpful to think of the inputs x and y as functions rather than strings, and we introduce some notation that makes this explicit. For convenience, assume that $n = 2^k$ for some k (if not then x and y can lengthened by padding them with zeroes), and define the functions $f_x, f_y : \{0,1\}^k \to \{0,1\}$ as

$$f_x(i) \quad = \quad x_i \tag{5}$$

$$f_y(i) \quad = \quad y_i \tag{6}$$

where $\{0,1\}^k$ and $\{0,1,\ldots,2^k-1\}$ are identified in the natural way. Alice and Bob's input data can be thought of as f_x and f_y, rather than x and y (respectively). In particular, given x, Alice can simulate an *f_x-query*, which is the unitary transformation that maps $|i\rangle\,|j\rangle$ to $|i\rangle\,|j \oplus f_x(i)\rangle$ (for all $i \in \{0,1\}^k$ and $j \in \{0,1\}$). Similarly Bob can simulate f_y-queries.

To construct an efficient quantum protocol for *IN*, define the function $(f_x \wedge f_y) : \{0,1\}^k \to \{0,1\}$ as $(f_x \wedge f_y)(i) = f_x(i) \wedge f_y(i)$ (for $i \in \{0,1\}^k$), and note that

$$IN(x,y) = \begin{cases} 1 & \text{if } (f_x \wedge f_y) \text{ is satisfiable} \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

(A $\{0,1\}$-valued function is *satisfiable* if it assumes the value 1 at at least one point in its domain.) Grover's search algorithm [11] can be used to determine if $(f_x \wedge f_y)$ is satisfiable by making $O(\sqrt{2^k \log(1/\varepsilon)}) = O(\sqrt{n \log(1/\varepsilon)})$ $(f_x \wedge f_y)$-queries, where ε is the error probability permitted [6]. The problem is that neither Alice nor Bob individually have enough information to perform an $(f_x \wedge f_y)$-query (since this depends on both x and y). If Alice were to begin by sending x to Bob then Bob could make $(f_x \wedge f_y)$-queries on his own, but note that this entails n bits of communication to begin with. Another, more efficient, approach is for Alice and Bob to collectively simulate $(f_x \wedge f_y)$-queries by combining f_x-queries (which Alice can perform) with f_y-queries (which Bob can perform), and a small amount of communication. To see how this is accomplished, consider the circuit in Fig. 1. First, ignoring the broken

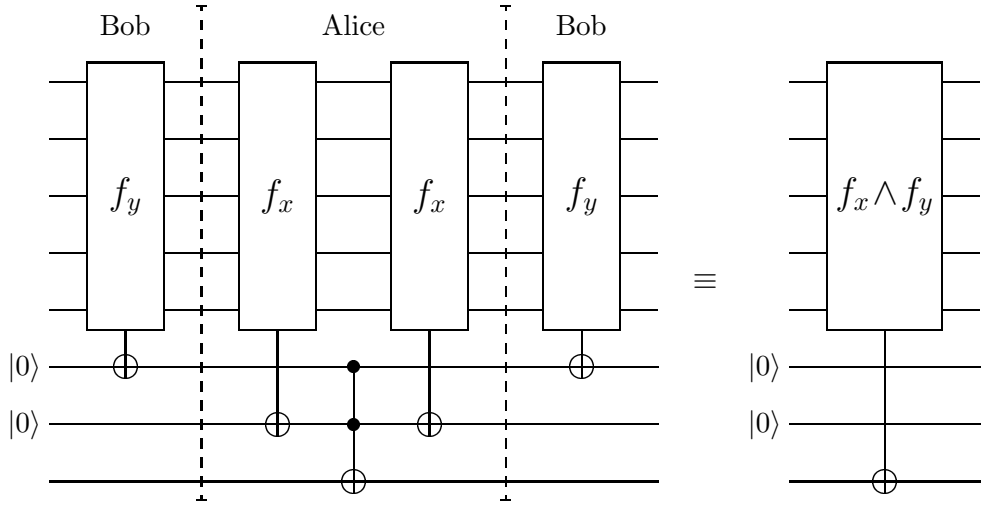

Figure 1: Simulation of an $(f_x \wedge f_y)$-query in terms of f_x-queries and f_y-queries.

vertical lines, note that the quantum circuit (composed of two f_x-queries, two f_y-queries, and one Toffoli gate) is equivalent to an $(f_x \wedge f_y)$-query. That is, it implements the unitary transformation that maps the state $|i\rangle\,|0\rangle\,|0\rangle\,|j\rangle$ to the state $|i\rangle\,|0\rangle\,|0\rangle\,|j \oplus (f_x \wedge f_y)(i)\rangle$ (for all $i \in \{0,1\}^k$, $j \in \{0,1\}$). This circuit uses two extra qubits that are each initialized in state $|0\rangle$ and which incur no net change.

Now, the protocol for *IN* can be thought of as Bob executing Grover's search algorithm to determine if $(f_x \wedge f_y)$ is satisfiable, except that, whenever an $(f_x \wedge f_y)$-query arises, Bob interacts with Alice to simulate the circuit in Fig. 1: first Bob performs an f_y-query gate, then he sends the $k+3$ qubits to Alice who performs some actions involving f_x-queries and a Toffoli gate (shown between the two broken lines) and sends the qubits back to Bob, who performs another f_y-query. Note that the total amount of communication that this entails is $2(k+3) \in O(\log n)$ qubits. Therefore, the total communication for Bob's simulation of the $O(\sqrt{n \log(1/\varepsilon)})$ queries to $(f_x \wedge f_y)$ is $O(\sqrt{n \log(1/\varepsilon)} \log(n))$, as claimed in Theorem 1.

More recently, Raz has given an example of a communication complexity problem which a quantum protocol can solve with *exponentially* less communication than the best classical probabilistic protocol. The description of the problem is more complicated than *EQ*, *IN*, and *IP*, and the reader is referred to [16] for the details.

We conclude by noting that, for the inner product function *IP*, it has been shown [14, 10] that even quantum protocols require communication $\Omega(n)$ for this problem, even when the error probability is permitted to be as large as (say) $\frac{1}{3}$.

References

[1] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching", *Fortschritte der Physik*, Vol. 46, pp. 493–505, 1998. (An earlier version appeared in *Physcomp '96.*)

[2] G. Brassard, "Quantum Communication Complexity (A Survey)", Preprint quant-ph/0101005, 2001.

[3] G. Brassard, R. Cleve, and A. Tapp, "Cost of exactly simulation quantum entanglement with classical communication", *Phys. Rev. Lett.*, Vol. 83, No. 9, pp. 1874–1877, 1999.

[4] H. Buhrman, R. Cleve, and W. van Dam, "Quantum entanglement and communication complexity", to appear in *SIAM J. Comput.*. Vol. 30, No. 8, pp. 1829–1841, 2001. Preprint quant-ph/9705033, 1997.

[5] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation", *Proc. 30th Ann. ACM Symp. on Theory of Computing (STOC '98)*, pp. 63-68, 1998.

[6] H. Buhrman, R. Cleve, R. de Wolf, and C. Zalka, "Bounds for small-error and zero-error quantum algorithms", *Proc. 40th Ann. IEEE Symp. on Foundations of Computer Science (FOCS '99)*, pp. 358–368, 1999.

[7] H. Buhrman, W. van Dam, P. Høyer, A. Tapp, "Multiparty quantum communication complexity", *Phys. Rev. A*, Vol. 60, No. 4, pp. 2737–2741, 1999.

[8] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity", *SIAM J. Comput.*, Vol. 17, No. 2, pp. 230–261, 1988.

[9] R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication", *Phys. Rev. A*, Vol. 56, No. 2, pp. 1201–1204, 1997.

[10] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, "Quantum entanglement and the communication complexity of the inner product function", *Proc. 1st NASA Intl. Conf. on Quantum Computing and Quantum Communications*, C.P. Williams (Ed.), Lecture Notes in Computer Science, Vol. 1509 (Springer-Verlag), pp. 61-74, 1998.

[11] L.K. Grover, "A fast quantum mechanical algorithm for database search", *Proc. 28th Ann. ACM Symp. on Theory of Computing (STOC '96)*, pp. 212–219, 1996.

[12] A.S. Holevo, "Some estimates of the information transmitted by quantum communication channels", *Problemy Peredachi Informatsii*, Vol. 9, pp. 3–11, 1973. English translation in *Problems of Information Transmission (USSR)*, Vol. 9, pp. 177–183, 1973.

[13] B. Kalyanasundaram and G. Schnitger, "The probabilistic communication complexity of set intersection", *Proc. 2nd Conf. on Structure in Complexity Theory*, pp. 41–49, 1987.

[14] I. Kremer, *Quantum Communication*, MSc Thesis, Computer Science Department, The Hebrew University, 1995.

[15] E. Kushilevitz and N. Nisan, *Communication Complexity*, (Cambridge University Press), 1998.

[16] R. Raz, "Exponential separation of quantum and classical communication complexity", *Proc. 31st Ann. ACM Symp. on Theory of Computing (STOC '99)*, pp. 358–367, 1999.

[17] A. C.-C. Yao, "Some complexity questions related to distributive computing", *Proc. 11th Ann. ACM Symp. on Theory of Computing (STOC '79)*, pp. 209-213, 1979.

[18] A. C.-C. Yao, "Quantum circuit complexity", *Proc. 34th Ann. IEEE Symp. on Foundations of Computer Science (FOCS '93)*, pp. 352–361, 1993.