Tensor norms and the classical communication complexity of nonlocal quantum measurement[1] [2]

Yaoyun Shi
Department of Electrical Engineering and Computer Science
The University of Michigan
Ann Arbor, MI 48109-2122, USA
E-mail: shiyy@eecs.umich.edu
March 2, 2005

Abstract

Nonlocality is at the heart of quantum information processing. In this paper we investigate the minimum amount of classical communication required in order to simulate a nonlocal quantum measurement. We derive general upper bounds, which in turn translate to systematic classical simulations of quantum communication protocols.

As a concrete application, we prove that any quantum communication protocol with shared entanglement for computing a Boolean function can be simulated by a classical protocol whose cost does *not* depend on the amount of the shared entanglement. This implies that if the cost of communication is a constant, quantum and classical protocols, with shared entanglement and shared coins, respectively, compute the same class of functions.

Furthermore, we describe a new class of efficient quantum communication protocols based on fast quantum algorithms. While some of them have efficient classical simulations by our method, others appear to be good candidates for separating quantum v.s. classical protocols, and quantum protocols with v.s. without shared entanglement.

Yet another application is in the context of simulating quantum correlations using local hidden variable models augmented with classical communications. We give a *constant cost*, *approximate* simulation of quantum correlations when the number of correlated variables is a constant, while the dimension of the entanglement and the number of possible measurements can be arbitrary.

Our upper bounds are expressed in terms of some *tensor norms* on the measurement operator. Those norms capture the nonlocality of bipartite operators in their own way and may be of independent interest and further applications.

Keywords: Quantum entanglement, classical simulation, communication complexity, tensor norms, Bell Inequality, Fourier Sampling Problem

[1]This research was supported in part by NSF Awards 0347078, 0323555 and 0341784.

1 Introduction and summary of results

Although Einstein himself made significant contributions to the development of quantum mechanics, he famously questioned the "completeness" of the theory based on a "paradox" that he suggested along with Podolsky and Rosen [19]. The essence of the paradox was formulated by Bohm [10] as follows: two "quantum coins" may be correlated in a state that can be schematically represented as

$$\frac{1}{\sqrt{2}}(|\texttt{Head}\rangle_A|\texttt{Tail}\rangle_B - |\texttt{Tail}\rangle_A|\texttt{Head}\rangle_B.$$

If each party measures his or her coin, with 1/2 probability, one of the two outcomes would be observed. However, once a measurement is made by one party, say, Alice, then Bob always observes the opposite outcome. Hence it appears that what Alice does locally would affect Bob's world without any communication.

The Einstein-Podolsky-Rosen (EPR) paradox did not reduce quantum mechanics to contradictions. Instead, it revealed the essence — quantum entanglement — that underlies the many counter-intuitive properties and marvelous capabilities of quantum information. For example, in his far reaching paper [6], John Bell formulated a set of inequalities, referred to as *Bell Inequalities* now, that the correlations produced by any so called *hidden variable* classical model would have to satisfy but would nevertheless be violated by some quantum correlations. The latter has been confirmed by many experiments (e.g., [39]). Another seminal example is the *quantum key distribution* protocol [7], which has been shown to be *information theoretically secure* [27, 28], as a consequence of properties of quantum entanglement.

Given its importance, quantum entanglement has been the subject of numerous studies (see, e.g., the books [31, 32]). The focus has been on understanding the inherent quantitative tradeoffs among various resources involved in the creation and conversion of entangled states. As entanglement is the result of nonlocal quantum interactions, understanding the nonlocality of quantum operations is also of fundamental importance. A natural measure of nonlocality of a quantum operation is its *generating capacity*, which is the maximum entanglement increase that it could cause (see e.g., [8]). Another approach, more from a computational point of view, is to consider the amount of resources, such as the time in the case of using elementary Hamiltonians, or the number of elementary gates, required to simulate the operator (e.g., [14, 15]).

Inspired by communication complexity, we take a completely different approach to quantify the nonlocality of quantum operators. Consider the following scenario. Alice and Bob, who live in the classical world, would like to simulate a quantum event, where a two-outcome quantum measurement P is applied to a bipartite system (A, B). Furthermore, Alice knows the *classical description* of System A and Bob knows that of System B, and they both know a *classical description* of P. Since they do not have enough information about the other's system, they have to communicate to simulate the measurement. We define the *classical communication complexity* of P, denoted by $\mathrm{Com}(P)$, to be the minimum number of bits that Alice and Bob needs to communicate to simulate the measurement outcome distribution with a small deviation. We allow Alice and Bob to share unlimited amount of randomness.

Our main result is to derive a general upper bound on $\mathrm{Com}(P)$ in terms of a certain operator norm.

Theorem 1.1 (Informally). *For any bipartite quantum measurement Q,* $\mathrm{Com}(Q) = O(\|Q\|_\diamond^2)$, *where $\|Q\|_\diamond$ is the* diamond norm *of Q.*

The diamond norm is originally defined on superoperators, and has been a powerful tool in the study of quantum interactive proof systems [22] and quantum circuits on mixed states [2]. We make use a natural mapping from bipartite operators to superoperators to define norms on the former based on norms on the latter.

The approach in proving Theorem 1.1 can be extended to obtain general upper bounds on $\mathrm{Com}(Q)$ in terms of other operators norms. Those norms belong to so called *tensor norms*, i.e., norms $\|\cdot\|_\alpha$ that satisfies $\|P\|_\alpha \leq \|A\| \cdot \|B\|$, whenever $P = A \otimes B$. Tensor norms have been studied for decades with a great deal of rich concepts and deep results (see, e.g., [18]). In recent years, they have been applied to quantum information theory to characterize and quantify nonlocality of quantum states [35, 36]. Those tensor norms appear in our upper bounds capture the nonlocality of bipartite operators in their own way, and may have further applications.

We then show that those upper bounds in turn have useful applications on quantum communication complexity. Recall that in the setting of communication complexity [41, 42], Alice and Bob would like to compute a function $f(x, y)$, where x is known to Alice only, and y to Bob. The communication complexity of f is the minimum amount of information that Alice and Bob need to exchange in order to compute f correctly for any input. Communication complexity has been a major research field (see, e.g., the book [26]), with many problems of rich structures and deep connections to other aspects of complexity theory.

One central question in quantum communication complexity is how much quantum protocols outperform classical ones. Despite much success in finding efficient quantum protocols [13, 12, 21, 1, 33, 3, 5], many questions remain open. For example, is there any exponential gap between quantum and classical communication complexity for a *total* Boolean function? Our upper bounds on $\mathrm{Com}(P)$ provide a systematic approach for obtaining a classical simulation of a given quantum protocol.

A concrete application is on the question of the advantage of sharing entanglement in quantum protocols, a question that has puzzled many researchers [16, 11, 24, 29]. It is known that sharing entanglement could give a constant additive advantage [16, 11], or save half of the communication [17]. However, little is known on the limit of the advantage. This is in sharp contrast with the classical case of sharing randomness, where we know that it can only save at most a logarithmic additive term [30]. If there is a quantum protocol that exchanges q qubits with m qubits of prior entanglement, then the best classical simulation we know is $\exp(\Omega(q + m))$. This is rather embarrassing, especially when $q << m$. Using our upper bound on the classical communication complexity of nonlocal operators, we prove the following.

Theorem 1.2. *If a twoway quantum protocol uses q qubits of communication and m qubits of share entanglement, then it can be simulated by a classical protocol using* $\exp(O(q))$ *bits with shared randomness. The simulation does* not *depend on m. Furthermore, it can be done in the restricted* Simultaneous Message Passing (SMP) *model with shared randomness, where Alice and Bob each sends a single message to Charlie, who determines the outcome.*

Notice that the exponential dependence on q can not be improved, because of the existence of an exponential separation of quantum and classical communication complexities for some partial function, discovered by Raz [33]. As a consequence of the above theorem,

Corollary 1.3. *If a communication complexity problem has a constant cost quantum communication protocol with shared entanglement, it also has a constant cost classical protocol with shared randomness.*

It is interesting to contrast the above with a recent result by Yao [43], which is of a similar type but of the opposite direction.

Theorem 1.4 ([43]). *If a communication complexity problem of input size n has a constant cost classical SMP protocol with shared randomness, it has an $O(\log n)$ cost quantum SMP protocol* without *shared entanglement.*

Combining this result with ours, we have

Corollary 1.5. *If a communication complexity problem of input size n has a constant cost twoway quantum protocol with shared entanglement, it has an $O(\log n)$ cost quantum SMP protocol without shared entanglement.*

One more contribution of this paper is to establish a new connection between quantum algorithms and quantum communication complexity. An elegant connection discovered by Buhrman, Cleve and Wigderson [13] translates an efficient quantum *search algorithm* into an efficient quantum communication problem. In contrast, our connection translates a highly parallel quantum algorithm into an efficient communication protocol in the quantum SMP model with shared entanglement. The suitable quantum algorithms include that for Fourier Sample Problem [9] and Period Finding, a generalization of Simon's Algorithm [38] and the core of Shor's factoring algorithm [37].

Our classical simulations show that some of these problems have efficient classical protocols as well, while most of them appear to be hard to simulate. Hence potentially they may be examples that would separate quantum and classical communication complexities. As entanglement is critical in those protocols, they may also give separations among quantum protocols that do or do not share entanglement, another important open problem.

Yet another application of our classical simulation of quantum measurements is to give efficient simulations of quantum correlations by the hidden variable model assisted with classical communication. The scenario is as follows. Suppose Alice and Bob are given an entangled quantum state. Then each of them, without any communication, applies to their portion of the state some local measurement not known to the other party. The result is a correlated joint distribution on both measurement outcomes. There are such correlations that violate the Bell Inequalities, hence are impossible to generate by any reasonable classical procedure in which Alice and Bob do not communicate.

Decades after Bell's work, many researchers work on questions of the following type: what is the minimum amount of classical communication required to simulate a quantum correlation? Most of their works focus on the exact simulation and on measuring a constant number of qubits. We study the approximate and asymptotic simulation of quantum correlations, where the joint random variables take a constant number of possible values but are nevertheless produced from (the two party) sharing an entangled state of an arbitrary dimension and applying arbitrary local measurements.

Theorem 1.6 (Informally). *In the above scenario, a $O\left(\ln \frac{1}{\epsilon}/\epsilon^2\right)$ number of classical bits is sufficient to approximate the quantum correlation with a ϵ statistical distance.*

2 Simulation framework

Our classical simulation of quantum protocols falls into the following framework. Let p be the acceptance probability (i.e., the probability of outputting 1) of a given the quantum protocol. We express $p = \langle \psi_A | \psi_B \rangle$, for two vectors $|\psi_A\rangle$ and $|\psi_B\rangle$ that can be prepared by Alice and Bob by herself/himself. Note that the lengths of the two vectors may be very large, in general. Indeed the shorter their lengths are, the better our simulation is.

More precisely, if for some number C, $\||\psi_A\rangle\| \le C$ and $\||\psi_B\rangle\| \le C$, then the following simulation uses $O(C^4)$ bits. Alice and Bob send Charlie $\||\psi_A\rangle\|$ and $\||\psi_B\rangle\|$, respectively, up to $O(1/C)$ precision. This requires $O(\log C)$ bits. They then proceed to estimate $\cos\theta$, for the angle θ between $|\psi_A\rangle$ and $|\psi_B\rangle$ up to a precision of $O(1/C^2)$. The protocol in Kremer, Nisan and Ron[25], which is based on the following observation of Goemans and Williamson [20], gives a protocol that accomplishes the latter task using $O(C^4)$ bits.

Assume for simplicity that all vectors are real (the complex number case can be easily reduced to the real case). If $|\psi\rangle$ is a random unit vector in the same space of $|\phi_A\rangle$ and $|\phi_B\rangle$, then

$$\mathrm{Prob}\left[\mathrm{sign}(\langle\psi|\psi_A\rangle) \neq \mathrm{sign}(\langle\psi|\psi_B\rangle)\right] \;=\; \theta/\pi. \tag{1}$$

Hence, in order to estimate $\cos\theta$ with error term δ, it suffices to estimate θ/π to some error term $O(\delta)$ using the above equality checking of signs. Obviously this can be done by a SMP protocol, and by a simple application of Chernoff Bound, requires $O\left(\ln\frac{1}{\epsilon}/\delta^2\right)$ repetitions. With $\delta = O(\epsilon/C^2)$, this is $O\left(C^4 \ln\frac{1}{\epsilon}/\epsilon^2\right)$ bits.

We note that [40] gives a procedure along the lines of checking equality of signs but it produces a random ± 1 variable whose expectation is precisely $\cos\theta$, though this is not asymptotically advantageous.

We summarize the above discussion as the basis for our future discussions.

Theorem 2.1 ([25, 20]). *Suppose the acceptance probability of a quantum protocol can be expressed as $\langle\psi_A|\psi_B\rangle$, where $|\psi_A\rangle$ and $|\psi_B\rangle$ can be prepared by each party individually. Furthermore, for some number C, $\||\psi_A\rangle\| \le C$, and $\||\psi_B\rangle\| \le C$. Then there is a classical SMP protocol with shared coins that uses $O\left(C^4 \ln\frac{1}{\epsilon}/\epsilon^2\right)$ bits and whose acceptance probability deviates from that of the protocol by at most ϵ.*

3 A general theorem

In this section, we formally define the classical communication complexity and the diamond norm of bipartite quantum operators, derive an upper bound of the former in terms of the latter. We shall focus on the following case: that the measurement gives two outcomes, and that the dimensions of the two systems are the same. Our results can be extended trivially to more general cases.

We use script letters $\mathcal{N}$, $\mathcal{M}$, $\mathcal{F}$, $\cdots$, to denote Hilbert spaces, and $\mathbf{L}(\mathcal{N})$ to denote the space of operators on $\mathcal{N}$. The identity operator on $\mathcal{N}$ is denoted by $I_{\mathcal{N}}$, and the identity superoperator on $\mathbf{L}(\mathcal{N})$ is denoted by $\mathbf{I}_{\mathcal{N}}$.

3.1 Quantum measurement scenarios

Let $\mathcal{N}_A$, $\mathcal{N}_B$, $\mathcal{M}_A$, and $\mathcal{M}_B$ be Hilbert spaces such that $\dim(\mathcal{N}_A) = \dim(\mathcal{N}_B)$ and $\dim(\mathcal{M}_A) = \dim(\mathcal{M}_B)$. Let $|E\rangle \in \mathcal{M}_A \otimes \mathcal{M}_B$, and $\{Q, I-Q\}$ be a binary-valued POVM on $\mathcal{N}_A \otimes \mathcal{N}_B$. That is, Q is a positive semidefinite operator on $\mathcal{N}_A \otimes \mathcal{N}_B$ with $\|Q\| \le 1$.

We define a *quantum measurement scenario* as a quadruple $(Q, |E\rangle, \mathcal{M}_A \otimes \mathcal{M}_B, \mathcal{N}_A \otimes \mathcal{N}_B)$ that parameterizes the following quantum event involving three parties Alice, Bob, and Charlie. Charlie sends Alice and Bob the bipartite quantum state $|E\rangle$, upon receiving which Alice and Bob each applies physically realizable operators $R_A : \mathbf{L}(\mathcal{M}_A) \to \mathbf{L}(\mathcal{N}_A)$ and $R_B : \mathbf{L}(\mathcal{M}_B) \to \mathbf{L}(\mathcal{N}_B)$, respectively, on their portion of $|E\rangle$. The choices of R_A and R_B are not known to the other party. They send the resulted systems to Charlie, who finally applies Q on the received state, observing outcome 1 with probability p.

Now suppose Alice and Bob loose their quantum power completely but nevertheless would like to simulate the above quantum event through classical communications. The classical descriptions of both Q and $|E\rangle$ are known to both of them, so is that of R_A to Alice and that of R_B to Bob. For a fixed precision parameter $\epsilon \in [0, 1/2)$, their goal is to output 1 with a probability $p' \in [p-\epsilon, p+\epsilon]$.

Definition 3.1. Let $\epsilon \in [0, 1/2)$. The *classical communication complexity* of Q with precision ϵ, denoted by $\mathrm{Com}_\epsilon(Q)$, is the minimum cost with which any quantum measurement scenario $(Q, |E\rangle, \mathcal{M}_A \otimes \mathcal{M}_B, \mathcal{N}_A \otimes \mathcal{N}_B)$ can be simulated with a precision ϵ by a two-way interactive, public-coin classical communication protocol. If the simulating protocols are restricted to be *Simultaneous Message Passing(SMP)* with shared-coins, then call the corresponding minimum cost the *classical SMP complexity* of Q, written as $\mathrm{Com}_\epsilon^{pub,\|}(Q)$. When ϵ is a universal constant, it may be omitted from the subscript.

Apparently $\mathrm{Com}_\epsilon(Q) \leq \mathrm{Com}_\epsilon^{pub,\|}(Q)$. All Our upper bounds on $\mathrm{Com}_\epsilon(Q)$ are proved as upper bounds on $\mathrm{Com}_\epsilon^{pub,\|}(Q)$.

3.2 The diamond norm on bipartite operators

Let $\mathcal{N}$ be a Hilbert space and $T : \mathbf{L}(\mathcal{N}) \to \mathbf{L}(\mathcal{N})$ be a superoperator. The *diamond norm* on super operators is defined as (c.f. [23])

$$\|T\|_\diamond \stackrel{\text{def}}{=} \inf\{\|A\|\|B\| : \mathrm{tr}_{\mathcal{F}}(A \cdot B^\dagger) = T,\ A,\ B \in \mathbf{L}(\mathcal{N}, \mathcal{N} \otimes \mathcal{F})\}.$$

For our application, the following alternative characterization of the diamond norm is more convenient.

Lemma 3.2. *For any superoperator T,*

$$\|T\|_\diamond = \min \left\{ \|\sum_t A_t^\dagger A_t\| \cdot \sqrt{\|\sum_t B_t^\dagger B_t\|}\ :\ A_t,\ B_t \in \mathbf{L}(\mathcal{N}),\ T = \sum_t A_t \cdot B_t^\dagger \right\}.$$

Let $\mathcal{N}_A$, $\mathcal{N}_B$, and $\mathcal{N}$ be Hilbert spaces of the same dimension. We fix an isomorphism between any two of them. For an operator in one space, we use the same notation for its images and preimages, under the isomorphisms, in the other spaces.

Let $Q \in \mathbf{L}(\mathcal{N}_A \otimes \mathcal{N}_B)$ be a bipartite operator and $Q = \sum_t A_t \otimes B_t^\dagger$, for some $A_t \in \mathbf{L}(\mathcal{N}_A)$, and $B_t \in \mathbf{L}(\mathcal{N}_B)$. Define a mapping $\mathcal{T}$ from bipartite operators on $\mathcal{N}_A \otimes \mathcal{N}_B$ to superoperators $\mathbf{L}(\mathcal{N}) \to \mathbf{L}(\mathcal{N})$ by mapping $Q \mapsto \mathcal{T}(Q) \stackrel{\text{def}}{=} \sum_t A_t \cdot B_t^\dagger$. It can be easily verified that the mapping is independent of the choice of the decomposition of Q and is indeed an isomorphism.

Definition 3.3. Let $Q \in \mathbf{L}(\mathcal{N}_A \otimes \mathcal{N}_B)$ be a bipartite operator. The *diamond norm* of Q, denoted by $\|Q\|_\diamond$, is $\|Q\|_\diamond \stackrel{\text{def}}{=} \|\mathcal{T}(Q)\|_\diamond$.

By Lemma 3.2, for any Q,

$$\|Q\|_\diamond = \min \left\{ \sqrt{\|\sum_t A_t^\dagger A_t\|} \cdot \sqrt{\|\sum_t B_t^\dagger B_t\|}\ :\ A_t \in \mathbf{L}(\mathcal{N}_A),\ B_t \in \mathbf{L}(\mathcal{N}_B),\ Q = \sum_t A_t \otimes B_t^\dagger \right\}.$$

Note that if a superoperator $T = A \cdot B$ for some $A, B \in \mathbf{L}(\mathcal{N})$, $\|T\|_\diamond = \|A\| \cdot \|B\|$. Therefore the diamond norm on bipartite operators is a tensor norm:

Lemma 3.4. *If $K = A \otimes B$, $\|K\|_\diamond = \|A\| \cdot \|B\|$.*

A nice property of the superoperator diamond norm is that it is "stable", i.e., it remains unchanged when tensored with the identity operator on an additional space [23].

Lemma 3.5. *Let $\mathcal{N}$, $\mathcal{M}$, and $\mathcal{F}$ be Hilbert spaces, and $T : \mathbf{L}(\mathcal{N}) \to \mathbf{L}(\mathcal{M})$ be a superoperator. Then $\|\mathbf{I}_\mathcal{F} \otimes T\|_\diamond = \|T\|_\diamond$.*

This stability property is carried over to our diamond norm and is important for our applications. Let $\mathcal{F}_A$, $\mathcal{F}_B$, and $\mathcal{F}$ be Hilbert spaces of the same dimension, and $Q \in \mathbf{L}(\mathcal{N}_A \otimes \mathcal{N}_B)$. Denote by $Q_{\mathcal{F}_A,\mathcal{F}_B}$ the bipartite operator $Q \otimes I_{\mathcal{F}_A \otimes \mathcal{F}_B}$, where the two subsystems are $\mathcal{N}_A \otimes \mathcal{F}_A$ and $\mathcal{N}_B \otimes \mathcal{F}_B$.

Lemma 3.6. *For any Q, $\|Q_{\mathcal{F}_A,\mathcal{F}_B}\|_\diamond = \|Q\|_\diamond$.*

We now use the diamond norm to derive an upper bound on $\mathrm{Com}_\epsilon^{pub,\|}(Q)$. Recall that if $\mathcal{M}$ and $\mathcal{N}$ are two Hilbert spaces, an *isometric embedding* from $\mathcal{M}$ to $\mathcal{N}$ is a linear map from $\mathcal{M}$ to $\mathcal{N}$ with a unit operator norm.

Theorem 3.7. *For any quantum measurement scenario $(Q, |E\rangle, \mathcal{M}_A \otimes \mathcal{M}_B, \mathcal{N}_A \otimes \mathcal{N}_B)$,*

$$\mathrm{Com}_\epsilon^{pub,\|}(Q) = O\left(\|Q\|_\diamond^2 \cdot \ln\frac{1}{\epsilon}/\epsilon^2\right).$$

Proof. Without loss of generality, assume that on receiving their portions of $|E\rangle$, Alice and Bob apply an isometric embedding $U : \mathcal{M}_A \to \mathcal{N}_A \otimes \mathcal{F}_A$, and $V : \mathcal{M}_B \to \mathcal{N}_B \otimes \mathcal{F}_B$, respectively, for some Hilbert spaces $\mathcal{F}_A$ and $\mathcal{F}_B$ with an equal dimension. The distribution resulted from Charlie's measuring Q on $\mathrm{Tr}_{\mathcal{F}_A,\mathcal{F}_B}\left((U \otimes V)|E\rangle\langle E|(U \otimes V)^\dagger\right)$ is the same as that of Charlie applying $Q_{\mathcal{F}_A,\mathcal{F}_B}$ on the larger state $(U \otimes V)|E\rangle\langle E|(U \otimes V)^\dagger$. By Lemma 3.6, $\|Q_{\mathcal{F}_A,\mathcal{F}_B}\|_\diamond = \|Q\|_\diamond$. Therefore, to prove the theorem we need only to consider isometric embeddings $U : \mathcal{M}_A \to \mathcal{N}_A$ and $V : \mathcal{M}_A \to \mathcal{N}_B$.

Without loss of generality, we assume that Alice and Bob have agreed on a Schmidt decomposition $|E\rangle = \sum_i \sqrt{p_i}|i\rangle_A \otimes |i\rangle_B$, for some $p_i \geq 0$, $\sum_i p_i = 1$, and for an orthonormal basis $\{|i\rangle\}$. Denote by $|i_A\rangle \stackrel{\text{def}}{=} U|i\rangle$, and $|i_B\rangle \stackrel{\text{def}}{=} V|i\rangle$. Then the message that Charlie receives is $|\bar{E}\rangle \stackrel{\text{def}}{=} (U \otimes V)|E\rangle = \sum_i \sqrt{p_i}|i_A\rangle \otimes |i_B\rangle$.

Suppose $\|Q\|_\diamond$ is achieved under the decomposition $Q = \sum_t A_t \otimes B_t^\dagger$, with which if $Q_A \stackrel{\text{def}}{=} \sum_t A_t^\dagger A_t$, and, $Q_B \stackrel{\text{def}}{=} \sum_t B_t^\dagger B_t$, we have $\|Q_A\| = \|Q_B\| = \|Q\|_\diamond$. With those definitions, we have

$$p = \langle\bar{E}|Q|\bar{E}\rangle = \sum_{i,j,t} \sqrt{p_i p_j}\ \langle i_A|A_t|j_A\rangle \cdot \langle i_B|B_t^\dagger|j_B\rangle.$$

Define two vectors

$$|\psi_A\rangle = \sum_{i,j,t} \sqrt{p_j}\ \langle j_A|A_t^\dagger|i_A\rangle\ |i,j,t\rangle, \quad \text{and,} \quad |\psi_B\rangle = \sum_{i,j,t} \sqrt{p_i}\ \langle i_B|B_t^\dagger|j_B\rangle\ |i,j,t\rangle. \tag{2}$$

Then $p = \langle\psi_A|\psi_B\rangle$. Further, with $\rho_A \stackrel{\text{def}}{=} \sum_j p_j |j_A\rangle\langle j_A|$,

$$\langle\psi_A|\psi_A\rangle = \sum_{i,j,t} p_j |\langle j_A|A_t^\dagger|i_A\rangle|^2 = \mathrm{tr}(\rho_A Q_A) \leq \|Q_A\| = \|Q\|_\diamond.$$

Similarly, $\langle\psi_B|\psi_B\rangle \leq \|Q_B\| = \|Q\|_\diamond$. Therefore, by Theorem 2.1, the measurement scenario can be approximated by a classical SMP with shared coins to be within an ϵ precision using $O\left(\|Q\|_\diamond^2 \ln\frac{1}{\epsilon}/\epsilon^2\right)$ bits. $\square$

Remark 3.8. One may improve the above upper bound on $\mathrm{Com}_\epsilon^{pub,\|}(Q)$ by a more carefully chosen $|\psi_A\rangle$ and $|\psi_B\rangle$ in Equation 2. More specifically, let $\alpha \in [0,1]$, define

$$|\psi_A^\alpha\rangle = \sum_{i,j,t} \sqrt{p_i^\alpha p_j^{1-\alpha}}\ \langle j_A|A_t^\dagger|i_A\rangle\ |i,j,t\rangle, \quad \text{and,} \quad |\psi_B^\alpha\rangle = \sum_{i,j,t} \sqrt{p_i^{1-\alpha} p_j^{\alpha}}\ \langle i_B|B_t^\dagger|j_B\rangle\ |i,j,t\rangle.$$

One can verify that minimizing $\||\psi_A\rangle\| \cdot \||\psi_B\rangle\|$ over all decompositions of Q gives rise to a tensor norm, which we do not know if is stable under tensoring with identity superoperators. Although we have not found any useful application of an $\alpha \neq 0$, we cannot rule out the possibility that a carefully chosen α may give a better bound.

Remark 3.9. In the case that $|E\rangle$ is not entangled, the same approach in Theorem 3.7 can be used to derive a systematic classical simulation. More specifically, in this context we would like to estimate $p = \langle \phi_A \otimes \phi_B|Q|\phi_A \otimes \phi_B\rangle$, for a state $|\phi_A\rangle$ known to Alice only and a state $|\phi_B\rangle$ known to Bob only. For a decomposition of $Q = \sum_t A_t \otimes B_t^\dagger$, we define

$$|\psi_A\rangle = \sum_t \langle \phi_A|A_t^\dagger|\phi_A\rangle|t\rangle, \quad \text{and,} \quad |\psi_B\rangle = \sum_t \langle \phi_B|B_t^\dagger|\phi_B\rangle|t\rangle.$$

Then $p = \langle \psi_A|\psi_B\rangle$. It can be verified that

$$\|Q\|_\otimes \stackrel{\text{def}}{=} \inf\{\|\psi_A\| \cdot \|\psi_B\| : Q = \sum_t A_t \otimes B_t^\dagger\}$$

defines a tensor norm and $\|Q\|_\otimes \leq \|Q\|_\diamond$. This approach gives a constant cost simulation of elegant quantum fingerprint protocol of Buhrman, Cleve, Watrous, and de Wolf [12].

4 Applications

We now apply the above to derive classical upper bounds on quantum communication complexity.

Quantum SMP with shared entanglement. If the quantum protocol is in the SMP model with shared entanglement, we immediately have,

Corollary 4.1 (of Theorem 3.7). *If in a quantum SMP protocol, Charlie applies the measurement P, then the protocol can be simulated by a classical SMP protocol with shared coins and using $O(\|P\|_\diamond^2)$ bits.*

Twoway interactive quantum communication with shared entanglement. Now consider the general twoway interactive quantum communication. We need the following lemma due to Yao [42], and the following formulation is from [34]:

Lemma 4.2 ([42, 34]). *Let $\mathcal{P}$ be a two-party interactive quantum communication protocol that uses q qubits. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be the state spaces of Alice and Bob, respectively. For an input (x,y), denote by $|\Phi_{x,y}\rangle_{AB}$ the joint state of Alice, Bob before the protocol starts. Then there exist linear operators $A_h \in \mathbf{L}(\mathcal{H}_A)$, and $B_h \in \mathbf{L}(\mathcal{H}_B)$, for each $h \in \{0,1\}^{q-1}$, such that*

(a) $\|A_h\| \leq 1$ *and* $\|B_h\| \leq 1$ *for all* $h \in \{0,1\}^{q-1}$*;*

(b) the acceptance probability of $\mathcal{P}$ on input x and y is $\|P|\Phi_{x,y}\rangle\|^2$, where $P \stackrel{\text{def}}{=} \sum_{h\in\{0,1\}^{q-1}} A_h \otimes B_h$.

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Let $|E\rangle$ be the shared entanglement. Fix an input (x, y). Let A_h and B_h be those in Lemma 4.2, and $A_h^x \stackrel{\text{def}}{=} A_h|x, 0\cdots 0\rangle$, $B_h^y \stackrel{\text{def}}{=} B_h|y, 0\cdots 0\rangle$. Then by Lemma 4.2, the final acceptance probability is $\langle E|P_{x,y}^\dagger P_{x,y}|E\rangle$, where $P_{x,y} \stackrel{\text{def}}{=} \sum_{h\in\{0,1\}^{q-1}} A_h^x \otimes B_h^y$. Let

$$Q_{x,y} \stackrel{\text{def}}{=} P_{x,y}^\dagger P_{x,y} = \sum_{h,h'} \left((A_{h'}^x)^\dagger A_h^x\right) \otimes \left((B_{h'}^y)^\dagger B_h^y\right).$$

Although we do not get precisely a measurement scenario with the parameters $Q_{x,y}$ and $|E\rangle$, following exactly the same proof of Theorem 3.7, the probability of observing 1, which is $\langle E|Q_{x,y}|E\rangle$, can be estimated with $O(\|Q_{x,y}\|_\diamond^2)$ bits of communication in the SMP model with shared randomness. Hence it suffices to prove that $\|Q_{x,y}\|_\diamond = \exp(O(q))$.

Since $\|\cdot\|_\diamond$ is a tensor norm, we have

$$\|Q_{x,y}\|_\diamond \leq \sum_{h,h'} \|\left((A_{h'}^x)^\dagger A_h^x\right) \otimes \left((B_{h'}^y)^\dagger B_h^y\right)\|_\diamond = \sum_{h,h'} \|A_h^x\|\|A_{h'}^x\|\|B_h^y\|\|B_{h'}^y\| \leq 2^{2(q-1)}.$$

The last inequality is because $\|A_h^x\| \leq 1$ and $\|B_h^y\| \leq 1$ for all h. Hence p can be estimated by a classical SMP protocol using $\exp(O(q))$ bits. □

Corollary 1.3 follows trivially from the above by setting q to be a constant. Corollary 1.5 follows immediately from Theorem 1.4 and Corollary 1.3 together with the following observation.

Lemma 4.3. *If a communication complexity problem has a classical twoway protocol with shared randomness and b bits of cost, it has a classical SMP protocol with shared randomness and $O(b2^{b/2})$ bits of communication.*

Proof. Fix a twoway protocol for the problem in which Alice sends b_A bits and bob sends b_B bits. To simulate this protocol in the SMP model with shared randomness, Alice sends the referee 2^{b_B} strings each of which has b_A bits and is consistent with her input and a string of b_B bits interpreted as Bob's messages. Bob applies the same strategy to sends 2^{b_A} strings of b_B bits. The referee is then able to reconstruct a string of b bits, which is precisely the transcript of communication in the original protocol with the same input and random string. Hence by outputting the last bit of the reconstructed message, this SMP protocol achieves the same error probability of the original protocol. The cost of the simulating protocol is $2^{b_A}b_B + 2^{b_B}b_A = O(b2^{b/2})$ bits. □

Simulating quantum correlations. We now sketch a proof for Theorem 1.6. More details will be provided in the final paper.

Proof of Theorem 1.6. Let V be the set of possible measurement outcomes. For each local measurement (a POVM) P, and each $v \in V$, denote by P^v the positive operator corresponding to the outcome v. Fix a pair of measurements (P_A, P_B), and for each pairs of possible outcome (v, v'), let $P^{v,v'} \stackrel{\text{def}}{=} P_A^v \otimes P_B^{v'}$. Then by Lemma 3.4, $\|P^{v,v'}\|_\diamond = \|P_A^v\| \cdot \|P_A^{v'}\| \leq 1$. Hence by Corollary 4.1, the probability of observing outcome (v, v') can be calculated to be within $O(\epsilon/|V|^2)$ precision by by a classical SMP protocol using $O\left(|V|^4 \ln(|V|^2/\epsilon)/\epsilon^2\right)$ bits. Hence applying the simulation for all pairs of (v, v'), we can calculate the distribution to be within ϵ statistical distance using $O\left(|V|^6 \ln(|V|^2/\epsilon)/\epsilon^2\right)$ bits, which is $O\left(\ln\frac{1}{\epsilon}/\epsilon^2\right)$ when $|V|$ is a constant. □

5 New quantum protocols and their simulations

Let $N \geq 1$ and $M \geq 1$ be integers. Suppose the goal of a quantum black-box algorithm (c.f. [4]) is to determine a property $\mathcal{P}(f)$ of an oracle function $f : \mathbb{Z}_N \to \mathbb{Z}_M$, using as few as possible number of black-box queries. One black-box query is the application of the *query operator* $O_f : |x, a\rangle \to |x, f(x) + a\rangle$, where $x \in \mathbb{Z}_N$ and $a \in \mathbb{Z}_M$, and the summation here, and for the rest of this section, is modulo M. In the communication version of $\mathcal{P}$, denoted by $\mathcal{P}^c$ (and referred to as the *Distributed $\mathcal{P}$ Problem*), Alice and Bob each has an oracle function $f_A,\ f_B : \mathbb{Z}_N \to \mathbb{Z}_M$, and they would like to compute $\mathcal{P}(f_A + f_B)$. For technical clarity, we do not normalize vectors in this section.

Theorem 5.1. *If a quantum black-box problem $\mathcal{P}$ can be computed by r parallel queries, each of which involved $\leq k$ qubits, then the communication problem $\mathcal{P}^c$ can be solved using $O(rk)$ qubits of communication in the quantum SMP model with $O(rk)$ qubits of shared entanglement.*

Proof. We need only to show that one query in the black-box algorithm can be simulated by Alice and Bob using $O(k)$ qubits of entanglement.

Let $f : \mathbb{Z}_N \to \mathbb{Z}_M$ be the oracle function. Let $|\phi\rangle \stackrel{\text{def}}{=} \sum_{x \in \mathbb{Z}_N, a \in \mathbb{Z}_M} |x, a\rangle \otimes |\psi_{x,a}\rangle$ be the state that the algorithm presents to the oracle. We would like to have Alice and Bob send a single message to Charlie, who is then able to generate $O_f|\phi\rangle$. To start with, Alice and Bob share the entanglement

$$\sum_{x \in \mathbb{Z}_N, y, a \in \mathbb{Z}_M} e^{2\pi i a y / M}\ |x, y, \psi_{x,a}\rangle_A \otimes |x, y\rangle_B.$$

Alice applies $|x, y\rangle \to e^{2\pi i f_A(x) \cdot y / M}|x, y\rangle$, and Bob applies $|x, y\rangle \to e^{2\pi i f_B(x) \cdot y / M}|x, y\rangle$. Then they send everything to Charlie, who now has

$$\sum_{x,y,a} e^{2\pi i (f_A(x) + f_B(x) + a) \cdot y / M}|x, x, y, y, \psi_{x,a}\rangle \ = \ \sum_{x,y,a} e^{2\pi i (f(x) + a) \cdot y / M}|x, x, y, y, \psi_{x,a}\rangle.$$

After removing redundancies of x and y and a Fourier transform, he has $\sum_{x,a} |x, a + f(x), \psi_{x,a}\rangle = O_f|\phi\rangle$, as required. □

It turns out that a lot of known quantum algorithms fall within the framework of quantum black-box algorithms and use parallel queries. These include Period Finding, which is a generalization of Simon's Problem [38] and is the core of Shor's factoring algorithm [37]. Hence the efficient quantum algorithms for those problems give efficient quantum communication complexity for the corresponding communication problems.

Here we focus on the distributed version of the Fourier Sampling Problem [9], for which the diamond norm in our classical simulation has a simple upper bound.

Let $n \in \mathbb{N}$ and $N \stackrel{\text{def}}{=} 2^n$. For any integer $k \geq 1$, we identify the sets $\{0,1\}^k$ with $\mathbb{Z}_{2^k}$ under the natural mapping. For a function $h : \{0,1\}^n \to \mathbb{R}$, define its Fourier transform $\hat{h} : \{0,1\}^n \to \mathbb{R}$ as follows:

$$\hat{h}(s) \stackrel{\text{def}}{=} \frac{1}{N} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} h(x), \qquad \forall s \in \{0,1\}^n.$$

Let $f : \{0,1\}^n \to \{0,1\}$ be Boolean function. Denote $f' \stackrel{\text{def}}{=} 1 - 2f$.

Definition 5.2. Let $S \subseteq \{0,1\}^n$, and $\epsilon = \epsilon(n) \in (0, 1/2)$. The *Noisy Fourier Sampling Problem* with the parameter S is the following partial function $\omega_S(f)$:

$$\omega_S(f) = \begin{cases} 1 & \text{if } \sum_{s \in S} \hat{f}'(s)^2 \geq \frac{2}{3}, \\ 0 & \text{if } \sum_{s \in S} \hat{f}'(s)^2 \leq \frac{1}{3}, \\ \text{not defined} & \text{otherwise.} \end{cases}$$

Let $P_S \stackrel{\text{def}}{=} \sum_{s\in S} |s\rangle\langle s|$, and $F \stackrel{\text{def}}{=} \sum_x \left(\frac{1}{\sqrt{N}} \sum_{x'} (-1)^{x\cdot x'} |x'\rangle\right) \langle x|$. The following straightforward generalization of the algorithm of Bernstein and Vazirani [9] for Fourier Sampling computes $\omega_S(f)$ using only one query and the probability of outputting 1 is precisely $\sum_{s\in S} \hat{f}'(s)^2$. Hence the error probability is $\leq 1/3$ for an oracle f that satisfies the promise.

Algorithm 1. (Noisy Fourier Sampling Problem). On oracle $f : \{0,1\}^n \to \{0,1\}$,

1. Query using $\sum_{x\in\{0,1\}^n} |x\rangle \otimes (|0\rangle - |1\rangle)$, resulting in $\sum_x f'(x)|x\rangle \otimes (|0\rangle - |1\rangle)$.

2. Apply the projective measure $F^\dagger P_S F$ On the first register.

Proposition 5.3. *The communication problem ω_S^c on with input $f_A, f_B : \{0,1\}^n \to \{0,1\}$ can be solved in the quantum SMP model with $O(n)$ qubits and sharing the same amount of entanglement.*

Proof. This follows from Theorem 5.1 and Algorithm 1. A simpler alternative is for Alice and Bob to start with sharing $\sum_x |x\rangle_A \otimes |x\rangle_B$, then each applies $|x\rangle \to (-1)^{f_A(x)}|x\rangle$ and $|x\rangle \to (-1)^{f_B(x)}|x\rangle$, respectively. They then send everything to Charlie, who has $\sum_x (-1)^{f(x)}|x, x\rangle$. He then applies the projective measurement

$$Q \stackrel{\text{def}}{=} \tilde{D}\tilde{F}^\dagger \tilde{P}_S \tilde{F}\tilde{D}, \tag{3}$$

where $D \stackrel{\text{def}}{=} \sum_x |x,x\rangle\langle x,x|$, $F \stackrel{\text{def}}{=} \sum_x \left(\frac{1}{\sqrt{N}} \sum_s (-1)^{x\cdot s} |s,s\rangle\right) \langle x,x|$, and $P_S \stackrel{\text{def}}{=} \sum_{s\in S} |s,s\rangle\langle s,s|$.

This results in the same distribution as in Algorithm 1 for the oracle $f_A + f_B$. The total number of qubits communicated and shared is both $2n$. □

Let $\chi_S : \{0,1\}^n \to \{0,1\}$ be the characteristic function for S, i.e., $f(x) = 1$ iff $x \in S$. Define $\|\hat{\chi}\|_1 \stackrel{\text{def}}{=} \sum_s |\hat{\chi}(s)|$.

Theorem 5.4. *For any set $S \subseteq \{0,1\}^n$, the Distributed Noisy Fourier Sampling Problem has a classical SMP protocol with shared randomness and $O(\|\hat{\chi}\|_1^2)$ bits of communication.*

Proof. By Proposition 5.3 and Corollary 4.1, it suffices to prove that $\|Q\|_\diamond \leq \|\hat{\chi}\|_1$, where Q, define in Equation 3, is the measurement that Charlie applies in the quantum SMP protocol. For each s, denote $Q_s \stackrel{\text{def}}{=} \sum_x |x\rangle\langle x+s| \otimes |x\rangle\langle x+s|$. By a straightforward calculation, $Q = \sum_s \hat{\chi}_S(s) Q_s$, hence

$$\|Q\|_\diamond \leq \sum_s |\hat{\chi}_S(s)| \|Q_s\|_\diamond \leq \|\hat{\chi}_S\|_1.$$

The last inequality is due to the simple fact that $\|Q_s\|_\diamond = 1$ for all s. □

We remark that in the above analysis, the operator $\tilde{F}$ can be replaced by using the Fourier transformation over $\mathbb{Z}_N$, and the result still holds. We also remark that while some χ_S has small $\|\hat{\chi}_S\|_1$, most have a large ℓ_1 norm. Hence there may be much room to improve on our upper bounds on $\mathrm{Com}(Q)$ and $\|Q\|_\diamond$.

6 Open Problems

Many new open problems emerge from this study.

PROBLEM 1. Can one improve our upper bounds on $\mathrm{Com}(P)$ and $\mathrm{Com}^{pub,\|}(P)$, or characterize them completely?

Problem 2. What is the connection of $\mathrm{Com}(P)$ to other measures of nonlocality, such as the entanglement capacity, and the minimum number of elementary gates, or the amount of time for evolving some elementary Hamiltonian, needed to approximate P?

Problem 3. The diamond norm of a superoperator is in essence its operator norm with respect to the trace norm on operators. This dual characterization is nontrivial yet makes it much more intuitive. Is there any more intuitive interpretation of our diamond norm on bipartite operators?

Problem 4. Although the upper bounds by the diamond norm and the other two tensor norms in Remark 3.8 and Remark 3.9 do not seem to be tight in general, they may be useful for individual problems. Furthermore, they capture nonlocality in their own way. Hence a better understanding of them would be of interest.

Problem 5. Can our result on removing the entanglement be strengthened to that one can always use an amount of entanglement linear in size of the messages, with at most a logarithmic additive term?

Problem 6. Can one prove strong lower bounds in any classical model on any of the distributed communication problems? Can one prove quantum lower bounds on the SMP complexity without entanglement on those problems?

Problem 7. Can one extend our simulation of quantum correlations to the case of large number of measurement outcomes, or prove that no good simulation exists?

7 Acknowledgments

I am indebted to Yufan Zhu for stimulating discussions, and to the anonymous reviewers for their valuable suggestions on improving the presentation of this paper.

References

[1] Aaronson and Ambainis. Quantum search of spatial regions (extended abstract). In *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 200–209, 2003.

[2] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the 31th Annual ACM Symposium on the Theory of Computation (STOC)*, pages 20–30, 1998.

[3] Ambainis, Schulman, Ta-Shma, Vazirani, and Wigderson. The quantum communication complexity of sampling. *SIAM Journal on Computing*, 32, 2003.

[4] A. Ambainis. Quantum query algorithms and lower bounds. In *Proceedings of Foundations of the Formal Sciences III*, September 2001.

[5] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In L. Babai, editor, *STOC*, pages 128–137. ACM, 2004.

[6] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964.

[7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India*, page 175, New York, 1984. IEEE Press.

[8] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin. On the capacities of bipartite Hamiltonians and unitary gates, 2002.

[9] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, Oct. 1997.

[10] D. Bohm. The paradox of Einstein, Rosen, and Podolsky. In *Quantum Theory and Measurement*, pages 611–623. Prentice-Hall, 1951.

[11] H. Buhrman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. *SIAM J. Comp.*, 30(6):1829–1841, March 2001.

[12] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, October 2001.

[13] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the thirtieth annual ACM Symposium on Theory of Computing (STOC)*, pages 63–68, New York, NY, USA, 1998. ACM Press.

[14] A. M. Childs, H. L. Haselgrove, and M. A. Nielsen. Lower bounds on the complexity of simulating quantum gates. *Phys. Rev. A*, 68:052311–052316, 2003.

[15] A. M. Childs, D. W. Leung, F. Verstraete, and G. Vidal. Asymptotic entanglement capacity of the Ising and anisotropic Heisenberg interactions. *Quantum Information and Computation*, 3:97, 2003.

[16] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication. *Phys. Rev. A*, 56:1201, 1997.

[17] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. *Lecture Notes in Computer Science*, 1509:61–74, 1999.

[18] A. Defant and K. Floret. *Tensor norms and operator ideals*, volume 176 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, 1993.

[19] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[20] M. X. Goemans and D. P. Williamson. .879-approximation algorithms for max cut and max 2sat. In *STOC*, pages 422–431, 1994.

[21] P. Høyer and R. de Wolf. Improved quantum communication complexity bounds for disjointness and equality. *Lecture Notes in Computer Science*, 2285:299–310, 2002.

[22] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 608–617. ACM Press, 2000.

[23] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002. Translated from the 1999 Russian original by Lester J. Senechal.

[24] H. Klauck. Lower bounds for quantum communication complexity. In B. Werner, editor, *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS-01)*, pages 288–297, Los Alamitos, CA, Oct. 14–17 2001. IEEE Computer Society.

[25] I. Kremer, N. Nisan, and D. Ron. On randomized one-round communication complexity. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pages 596–605. ACM Press, 1995.

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

[27] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, March 1999.

[28] D. Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48, 2001.

[29] A. Nayak and J. Salzman. On communication over an entanglement-assisted quantum channel. In *Proceedings of the thirty-fourth annual ACM symposium on Theory of computing*, pages 698–704. ACM Press, 2002.

[30] I. Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 31 July 1991.

[31] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[32] J. Preskill. Lecture notes for physics 229: Quantum information and computation.

[33] R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing (STOC'99)*, pages 358–367, New York, May 1999. Association for Computing Machinery.

[34] A. A. Razborov. Quantum communication complexity of symmetric predicates (Russian). *Izvestiya of the Russian Academy of Science, Mathematics*, 6, 2002. English translation available at http://genesis.mi.ras.ru/˜razborov/qcc_eng.ps.

[35] O. Rudolph. A separability criterion for density operators. *J. Phys. A-Math. Gen.*, 33(21):3951–3955, June 2000.

[36] O. Rudolph. Further results on the cross norm criterion for separability. Preprint available at quant-ph/0202143, February 2002.

[37] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, Oct. 1997.

[38] D. R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, Oct. 1997.

[39] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of Bell Inequalities by photons more than 10 km apart. *Phys. Rev. Lett.*, 81(17):3563, Oct 1998.

[40] B. Toner and D. Bacon. Communication cost of simulating Bell correlations. *Phys Rev Lett.*, 91(18):187904, Oct 2003.

[41] A. C.-C. Yao. Some complexity questions related to distributive computing. In *Eleventh Annual ACM Symposium on Theory of Computing (STOC '79)*, pages 209–213, New York, Apr. 1979. ACM.

[42] A. C.-C. Yao. Quantum circuit complexity. In *34th Annual Symposium on Foundations of Computer Science: November 3–5, 1993, Palo Alto, California: proceedings [papers]*, pages 352–361. IEEE Computer Society Press, 1993.

[43] A. C.-C. Yao. On the power of quantum fingerprinting. In ACM, editor, *Proceedings of the Thirty-Fifth ACM Symposium on Theory of Computing, San Diego, CA, USA, June 9–11, 2003*, pages 77–81, New York, NY, USA, 2003. ACM Press.