CHICAGO JOURNAL OF THEORETICAL COMPUTER SCIENCE
http://cjtcs.cs.uchicago.edu/

Coherent state exchange in multi-prover quantum interactive proof systems

Debbie Leung* Ben Toner† John Watrous‡

August 7, 2013

Abstract: We show that any number of parties can coherently exchange any one pure quantum state for another, without communication, given prior shared entanglement. Two applications of this fact to the study of multi-prover quantum interactive proof systems are given. First, we prove that there exists a one-round two-prover quantum interactive proof system for which no finite amount of shared entanglement allows the provers to implement an optimal strategy. More specifically, for every fixed input string, there exists a sequence of strategies for the provers, with each strategy requiring more entanglement than the last, for which the probability for the provers to convince the verifier to accept approaches one. It is not possible, however, for the provers to convince the verifier to accept with certainty with a finite amount of shared entanglement. The second application is a simple proof that multi-prover quantum interactive proofs can be transformed to have near-perfect completeness by the addition of one round of communication.

1 Introduction

The idea that entanglement may be used as a resource is central to the theory of quantum communication and cryptography. Well-known examples include teleportation [7] and the super-dense coding of both classical and quantum data [9, 10, 24]. In cryptography, entanglement is used not only in some

*Supported by CRC, ORF, NSERC, NSERC DAS, and CIFAR.
†Supported by NWO, EU project QAP, and BSIK/BRICKS.
‡Supported by NSERC and CIFAR.

Key words and phrases: Quantum computation, interactive proof systems, entanglement

implementations of quantum key distribution [20], but also as a mathematical tool in security proofs [32, 34] of quantum key-distribution protocols not based on entanglement (such as [6]). In these settings it may be said that the relationship between entanglement and other resources (in particular quantum communication, classical communication, and private shared randomness) is reasonably well-understood [8, 19].

There are, on the other hand, settings of interest where the properties of entanglement as a resource are poorly understood. One example can be found in quantum communication complexity, wherein it is not known if prior shared entanglement ever provides for more than a constant factor decrease in the number of qubits of communication required to solve a communication problem of the most standard form [11, 38]. A second example, which is the main focus of this paper, concerns the power of entanglement in the multi-prover interactive proof system model, which has been studied in several papers [13, 14, 15, 25, 27, 29, 31, 37]. Bell inequalities [4, 12], and many of the open problems concerning them [23], have a close connection to this model (although not necessarily to our main results).

Multi-prover interactive proof systems, which were first defined by Ben-Or, Goldwasser, Kilian, and Wigderson [5], involve interactions between a *verifier* and two or more *provers*. The verifier is always assumed to be efficiently implementable, while the provers are typically permitted to have arbitrary complexity. The verifier and provers each receive a copy of some input string x, and then engage in an interaction based on this string. During this interaction the verifier communicates privately with each of the provers, possibly over the course of many rounds of communication, but the provers are forbidden from communicating directly with one another. The provers may, however, agree on a joint strategy before the interaction begins. The provers act in collaboration to convince the verifier that the input string x is a *yes-input* to some fixed problem, and therefore should be *accepted*. The provers are not, however, considered to be trustworthy, and so the verifier must be defined in such a way that it *rejects* strings that are *no-inputs* to the problem being considered. These two conditions—that the provers can convince the verifier to accept yes-inputs but cannot convince the verifier to accept no-inputs—are called the *completeness* and *soundness* conditions, respectively, and are analogous to the notions in mathematical logic that share these names. In contrast to the notion of a mathematical proof, however, one typically requires only that the completeness and soundness conditions for interactive proof systems hold with high probability (for every fixed yes or no input string).

In the quantum setting, the verifier and the provers are allowed to use quantum computers and exchange quantum messages. The provers may also share initial entanglement, to be used as part of their strategy during the interaction. In general, shared entanglement increases the provers' power: they can use it to potentially solve harder problems, but they also have greater power through which they might violate soundness conditions. Intermediate models have also been studied, where some but not all of the local processing, the interaction, and the correlation between the provers are quantum.

Many known facts and techniques about classical multi-prover interactive proof systems become invalid within the quantum model. The following points illustrate the effect of this change on our current state of knowledge.

- When the provers are not allowed to share prior entanglement, it is known that the class of promise problems that have multi-prover interactive proof systems is precisely NEXP, the class of problems that can be solved nondeterministically in exponential time. This holds for both quantum and classical verifiers and provers [2, 31].

- It is not known if every promise problem having a multi-prover interactive proof systems in which the provers initially share entanglement, including the cases of both classical and quantum verifiers, is computable; and it was only very recently shown by Ito and Vidick [25] that multi-prover quantum interactive proof systems are no less powerful than multi-prover classical interactive proofs.

One basic question about multi-prover interactive proofs with entangled provers has remained unanswered, and is closely related to the lack of good upper bounds on their power: *For a given verifier and input string, how much entanglement is needed for the provers to play optimally?* To obtain an upper bound on the expressive power of multi-prover interactive proofs with entangled provers, one approach is to seek a general bound: a limit on the amount of entanglement, as a function of the verifier's description and the given input, needed for the provers to play optimally.

Our first main result partially explains the difficulty in answering the above question: we prove that there exist two-prover quantum interactive proof systems for which no finite amount of entanglement allows for an optimal strategy on any fixed input. In other words, there are interactive proofs such that, no matter what entangled state the provers choose on a given input, it would always be possible for them to do strictly better with more entanglement. There is, therefore, no strict upper bound of the form discussed above. This fact has an obvious but important implication: to obtain upper bounds on the power of multi-prover quantum interactive proofs via an upper bound on the entanglement required, one must consider *close-to-optimal* strategies instead of optimal ones.

Our second main result concerns methods to achieve *perfect completeness* of quantum interactive proof systems while retaining small soundness error. In the single-prover case, an efficient transformation for doing this exists that is both simple and easy to analyze [30]. In the multi-prover setting, an analogous result was obtained by Kempe, Kobayashi, Matsumoto, and Vidick [28] based on a more complicated transformation and analysis. This more complicated transformation was designed to handle the locality constraints imposed on multiple provers. It turns out, however, that this complicated procedure is not needed after all, provided one is willing to make a small sacrifice. We prove that the simple single-prover technique can be applied in the multi-prover case to yield a proof system with *near-perfect* completeness: honest provers are able to convince the verifier to accept yes-inputs with any probability smaller than 1 that they desire—but they might never reach probability 1 using finite resources.

The two main results just discussed are connected by the notion of *coherent state exchange*. This notion, which is closely related to that of *quantum state embezzlement* [18], is the subject of the section following this one. The first main result is then proved in Section 3, while the second is proved in Section 4. The paper concludes with Section 5. Throughout the paper we assume the reader is familiar with quantum computing and with basic aspects of classical and quantum interactive proof systems. Our notation and terminology are consistent with other papers on these topics.

Remarks on recent related work

An initial version of this paper was posted to arXiv.org in April 2008, and the present version does not differ significantly from the initial version in content. Since the posting of this initial version, several interesting papers studying entanglement in two-player games have appeared. In addition to [25] that was already mentioned, along with a recent follow-up paper by Vidick [36], the papers [16] and [33] are

particularly relevant to this one. A class of games called *rank one quantum games*, which generalizes the main type of game we consider in this paper, is defined and studied in [16], and many interesting results about this class are proved. The main technique we use in this paper has found applications to a somewhat different class of games, called *quantum XOR games*, which are defined and studied in [33].

2 Coherent state exchange

Suppose that m players wish to transform a shared state $|\phi\rangle$ into a different state $|\psi\rangle$. Also suppose that we require this task to be completed *(1) without communication* and *(2) by a coherent process* (meaning that it can be applied in a way that preserves superpositions). We refer to this task as *coherent state exchange*.

In the absence of additional resources, it is not possible in general to perform this task when $m \geq 2$. In particular, given that the players cannot create entanglement out of thin air, the task is easily seen to be impossible when the target state $|\psi\rangle$ has more entanglement than the initial state $|\phi\rangle$. However, if we consider the situation in which the players initially share an auxiliary quantum state, and we allow this state to be perturbed slightly by the process, then the above impossibility argument based on entanglement is no longer valid—and, as we will show, the task indeed becomes possible. We note that the coherence condition requires that a process of this sort must leave the auxiliary quantum state nearly unchanged, in essence using it as a catalyst. The players cannot, for instance, simply swap the input state $|\phi\rangle$ with an initially shared copy of $|\psi\rangle$ without losing coherence. Note also that the coherence condition makes the exchange in both directions equally difficult, independent of whether entanglement is increased or decreased in the process.

Definition 2.1 (Coherent state exchange)**.** Consider m players $P_1, \ldots, P_m$, and suppose that player P_i holds a quantum system whose associated Hilbert space is denoted $\mathcal{R}_i$, for each $i \in \{1, \ldots, m\}$. Let $|\phi\rangle, |\psi\rangle \in \mathcal{R}_1 \otimes \cdots \otimes \mathcal{R}_m$ be two chosen pure states. Coherent state exchange of $|\phi\rangle$ to $|\psi\rangle$ with error ε is defined as a process that transforms any state of the form

$$\alpha |0^m\rangle |\gamma\rangle + \beta |1^m\rangle |\phi\rangle$$

into a state ρ whose fidelity with

$$\alpha |0^m\rangle |\gamma\rangle + \beta |1^m\rangle |\psi\rangle$$

is at least $1 - \varepsilon$. In the above states, the first m qubits represent control qubits, with one held by each player, and $|\gamma\rangle$ represents an arbitrary state in $\mathcal{R}_1 \otimes \cdots \otimes \mathcal{R}_m$. The players can share an initially entangled state, but cannot communicate.

In the above definition, the spaces $\mathcal{R}_i$ and $\mathcal{R}_j$ need not have equal dimension for $i \neq j$.

Lemma 2.2. *Let $P_1, \ldots, P_m$ and $|\phi\rangle, |\psi\rangle \in \mathcal{R}_1 \otimes \cdots \otimes \mathcal{R}_m$ be as in Definition 2.1. Suppose each player P_i holds an additional quantum system whose associated Hilbert space is denoted $\mathcal{X}_i$, and let $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$ be referred to as the* auxiliary space*. If there is a state $|E\rangle$ in the auxiliary space, along with m unitary operators $U_i \in \mathrm{L}(\mathcal{R}_i \otimes \mathcal{X}_i)$, such that*

$$|\langle\psi|\langle E| U_1 \otimes \cdots \otimes U_m |\phi\rangle |E\rangle| \geq 1 - \varepsilon,$$

then coherent state exchange with error ε is possible.

Proof. Starting from the initial state

$$\left(\alpha\left|0^m\right\rangle\left|\gamma\right\rangle+\beta\left|1^m\right\rangle\left|\phi\right\rangle\right)\left|E\right\rangle,$$

each party P_i performs the operation $|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes U_i$ on their control qubit, system, and portion of the auxiliary space. The parties now share the state

$$\left|\zeta\right\rangle=\alpha\left|0^m\right\rangle\left|\gamma\right\rangle\left|E\right\rangle+\beta\left|1^m\right\rangle\left(U_1\otimes\cdots\otimes U_m\right)\left|\phi\right\rangle\left|E\right\rangle.$$

Let ρ be the state obtained by taking the partial trace over the auxiliary space. It holds that

$$\begin{aligned}F\left(\rho,\alpha\left|0^m\right\rangle\left|\gamma\right\rangle+\beta\left|1^m\right\rangle\left|\psi\right\rangle\right)&\geq F\left(\left|\zeta\right\rangle,\alpha\left|0^m\right\rangle\left|\gamma\right\rangle\left|E\right\rangle+\beta\left|1^m\right\rangle\left|\psi\right\rangle\left|E\right\rangle\right)\\&=\left|\alpha\right|^2+\left|\beta\right|^2\left|\langle\psi|\langle E|U_1\otimes\cdots\otimes U_m\left|\phi\right\rangle|E\rangle\right|\geq 1-\varepsilon,\end{aligned}$$

as required. □

For the bipartite case ($m=2$), one method for coherent state exchange with arbitrarily small error can be obtained through the use of van Dam and Hayden's *quantum state embezzlement* [18]. In quantum state embezzlement, two parties (Alice and Bob) transform a state $\left|\mu_N\right\rangle$ into one that approximates $\left|\mu_N\right\rangle\left|\phi\right\rangle$. Here, $\left|\phi\right\rangle$ is an arbitrary entangled state known to both Alice and Bob, and $\{\left|\mu_N\right\rangle\}$ is a special family of states defined so that the approximation can be made arbitrarily accurate as N increases. Thus, Alice and Bob "embezzle" $\left|\phi\right\rangle$ from $\left|\mu_N\right\rangle$, leaving little trace of their crime. The transformation described is coherent and requires no communication, and can therefore be done twice (once in reverse) to achieve coherent state exchange. It relies, however, on a representation of two-party pure quantum states that no longer exists for m-party states when $m\geq 3$. Here, we show that coherent state exchange of any two pure states with arbitrarily small error for any number of parties is always possible.

Coherent exchange of orthogonal states

For simplicity, we first describe a procedure for the coherent exchange of orthogonal states $\left|\phi\right\rangle$ and $\left|\psi\right\rangle$. Modifications that extend to any $\left|\phi\right\rangle$ and $\left|\psi\right\rangle$ are discussed in the subsection following this one.

Let N be a positive integer, which will determine the accuracy of the coherent exchange of $\left|\phi\right\rangle$ into $\left|\psi\right\rangle$. By Lemma 2.2, it suffices to find a state $\left|E_N\right\rangle$ on an auxiliary space $\mathcal{X}_1\otimes\cdots\otimes\mathcal{X}_m$ and unitary operators $U_i\in\mathrm{L}\left(\mathcal{R}_i\otimes\mathcal{X}_i\right)$ such that

$$\left|\langle\psi|\langle E_N|U_1\otimes\cdots\otimes U_m\left|\phi\right\rangle|E_N\rangle\right|\geq 1-\varepsilon_N,$$

where ε_N vanishes as N goes to infinity.

For each player P_i, the auxiliary space $\mathcal{X}_i$ will correspond to $N+1$ identical registers labeled $\mathsf{X}_i^1,\ldots,\mathsf{X}_i^{N+1}$, where each register has an associated Hilbert space that is isomorphic to $\mathcal{R}_i$. We take the initial state of the registers $(\mathsf{X}_1^1,\ldots,\mathsf{X}_m^1),\ldots,(\mathsf{X}_1^{N+1},\ldots,\mathsf{X}_m^{N+1})$ to be

$$\left|E_N\right\rangle=\frac{1}{\sqrt{N}}\sum_{k=1}^{N}\left|\phi\right\rangle^{\otimes k}\left|\psi\right\rangle^{\otimes(N-k+1)},\tag{2.1}$$

representing the entanglement initially shared by $P_1, \ldots, P_m$. The state to be exchanged resides in the registers $(\mathsf{X}_1^0, \ldots, \mathsf{X}_m^0)$.

The procedure that transforms $|\phi\rangle$ into $|\psi\rangle$ is simple: each player P_i cyclically shifts the contents of the registers $\mathsf{X}_i^0, \ldots, \mathsf{X}_i^{N+1}$ by applying a unitary operation U_i defined by the action

$$|x_0\rangle\,|x_1\rangle \cdots |x_{N+1}\rangle \mapsto |x_{N+1}\rangle\,|x_0\rangle \cdots |x_N\rangle$$

on standard basis states.

Let us now consider the properties of the above procedure. It is clear that after the cyclic shift, the registers $(\mathsf{X}_0^1, \ldots, \mathsf{X}_0^m)$ will contain a perfect copy of $|\psi\rangle$, and the remaining registers will contain the state

$$|E_N'\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} |\phi\rangle^{\otimes(k+1)}\,|\psi\rangle^{\otimes(N-k)}. \tag{2.2}$$

Thus, the procedure transforms $|\phi\rangle\,|E_N\rangle$ into $|\psi\rangle\,|E_N'\rangle$, and

$$|\langle\psi|\langle E_N|\,U_1 \otimes \cdots \otimes U_m\,|\phi\rangle|E_N\rangle| = \langle E_N|E_N'\rangle = 1 - \frac{1}{N}.$$

So, by Lemma 2.2, coherent state exchange is achieved with error $\varepsilon_N = 1/N$.

The fidelity between $|E_N\rangle$ and $|E_N'\rangle$ can be improved[1] if an alternative choice of the state $|E_N\rangle$ is made in (2.1). In particular, if the amplitude of the k-th term $|\phi\rangle^{\otimes k}\,|\psi\rangle^{\otimes(N-k+1)}$ is changed from $1/\sqrt{N}$ to

$$a_k = \sqrt{\frac{2}{N+1}}\,\sin\!\left(\frac{\pi k}{N+1}\right),$$

a lower bound of

$$\langle E_N|E_N'\rangle = \sum_{k=2}^{N} a_{k-1}a_k \geq 1 - \frac{\pi^2}{2N^2}$$

on the fidelity is obtained.

Coherent exchange of non-orthogonal states

Here we briefly discuss two methods for performing coherent state exchange for non-orthogonal states $|\phi\rangle$ and $|\psi\rangle$. For the first method, one may take any state $|\eta\rangle \in \mathcal{R}_1 \otimes \cdots \otimes \mathcal{R}_m$ that is orthogonal to both $|\phi\rangle$ and $|\psi\rangle$, and perform two state exchanges: first from $|\phi\rangle$ and $|\eta\rangle$ and then from $|\eta\rangle$ to $|\psi\rangle$. The auxiliary state naturally takes the form $|E_N\rangle\,|F_N\rangle$, where $|E_N\rangle$ is used to transform $|\phi\rangle$ to $|\eta\rangle$ and $|F_N\rangle$ is used to transform $|\eta\rangle$ to $|\psi\rangle$. Aside from this change, no new analysis is required. This method works whenever $\dim(\mathcal{R}_1 \otimes \cdots \otimes \mathcal{R}_m) \geq 3$ which is immediate provided that $m \geq 2$ and that each $\mathcal{R}_i$ is non-trivial.

Another method is as follows. Suppose $\langle\phi|\psi\rangle = ae^{i\theta}$ for $a > 0$, and define $|\tilde{\psi}\rangle = e^{-i\theta}\,|\psi\rangle$. It is easy to coherently exchange $|\tilde{\psi}\rangle$ for $|\psi\rangle$ by letting one player induce a global phase (which translates into a phase shift on a control qubit if the process is performed in superposition). Thus, it remains to exchange

[1] This improvement was communicated to us by Aram Harrow, who attributes the idea to Peter Shor.

$|\phi\rangle$ for $|\tilde{\psi}\rangle$. If $a = 1$ there is nothing to do, while if $a < 1$ the procedure for orthogonal states can be applied with little modification. The players share the state

$$|E_N\rangle = \frac{1}{\sqrt{N_1}} \sum_{k=1}^{N} |\phi\rangle^{\otimes k} |\tilde{\psi}\rangle^{\otimes(N-k+1)},$$

which is identical to (2.1) except for a different normalization. It is easily verified that $N \leq N_1 \leq N^2$, and more explicitly we have

$$N_1 = \frac{1+a}{1-a} N - 2a \frac{1-a^N}{(1-a)^2}.$$

Now

$$|E'_N\rangle = \frac{1}{\sqrt{N_1}} \sum_{k=1}^{N} |\phi\rangle^{\otimes k+1} |\tilde{\psi}\rangle^{\otimes(N-k)}$$

and

$$\langle E_N | E'_N \rangle = 1 - \frac{1-a^N}{N_1} \leq 1 - \frac{1}{N}.$$

Thus the accuracy is no worse than in the orthogonal case.

Further connections to embezzlement and other work

As mentioned earlier, in the case $m = 2$ one may use quantum state embezzlement twice to implement coherent state exchange. The family of states $\{|\mu_N\rangle\}$ defined in [18] also has the added property of being *universal*, or independent of the state $|\phi\rangle$ to be embezzled. We note that it is possible to use our method to give universal embezzling families for all m. To define a universal embezzling family for any fixed m, we may consider an ε-net of states $\{|\psi\rangle\}$ in N^m dimensions (for $\varepsilon = 1/N$, say), take $|\phi\rangle = |0^m\rangle$, and define the embezzling state for each N to be the tensor product of all the states $|E_N\rangle$ ranging over the ε-net. The embezzlement of a particular state is then performed in the most straightforward way. Unlike the families of van Dam and Hayden for the case $m = 2$, our method is highly inefficient, but nevertheless establishes that universal embezzling families exist for all m.

A notion related to coherent state exchange, known as *catalytic transformation* of pure states, was considered by Jonathan and Plenio [26]. In particular, they considered the situation in which two parties transform one pure state to another (by local operations and classical communication) using a catalyst—or a state that assists but is left unchanged by the process. Coherent state exchange and embezzlement do almost exactly this, allowing approximations in the target state and the regenerated catalyst, and without the exchange of classical information and preserving coherence.

3 Finite entanglement is suboptimal

The purpose of this section is to prove the first main result of the paper, which is that there exist two-prover quantum interactive proof systems for which no finite amount of entanglement allows for an optimal strategy. It suffices to consider *cooperative quantum games*, defined as the class of two-prover quantum interactive proof systems having no dependence on the input x. In particular, we consider such games with only one round of communication.

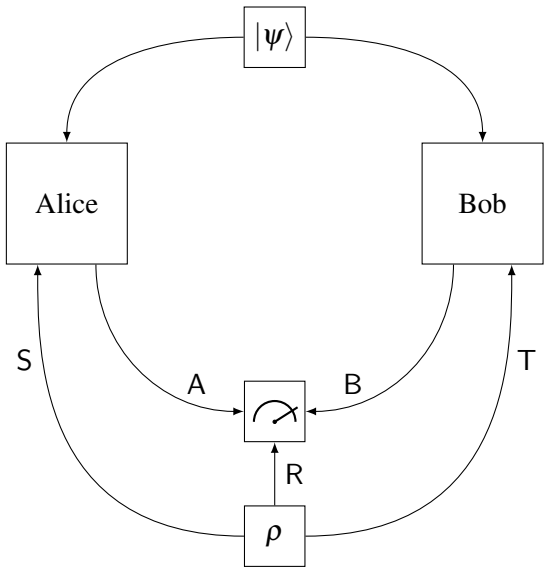

Figure 1: An illustration of a two-player, one-round cooperative quantum game.

Definition 3.1 (Two-player, one-round cooperative quantum game)**.** Let $\mathsf{R},\mathsf{S},\mathsf{T},\mathsf{A},\mathsf{B}$ be finite-dimensional quantum registers, let ρ be a quantum state of the registers $(\mathsf{R},\mathsf{S},\mathsf{T})$, and let $\mathcal{M}$ be a binary measurement on the registers $(\mathsf{R},\mathsf{A},\mathsf{B})$.

1. The referee prepares $(\mathsf{R},\mathsf{S},\mathsf{T})$ in the state ρ, and then sends S to Alice and T to Bob.

2. Alice and Bob transform the registers S and T sent to them however they choose, resulting in registers A and B that are sent back to the referee.

3. The referee applies the binary measurement $\mathcal{M}$ on the registers $(\mathsf{R},\mathsf{A},\mathsf{B})$. The outcome 1 means that Alice and Bob win, while the outcome 0 means that they lose.

The usual restrictions for provers in a quantum interactive proof system apply to Alice and Bob: they are not permitted to communicate once the game begins, but may agree on a strategy beforehand. Such a strategy may include the sharing of an entangled state $|\psi\rangle$ of their own choosing, which they may use when transforming the registers sent to them via local quantum operations. Alice's most general strategy is to apply a quantum channel to S together with her share of the entangled state, outputting A. A general strategy for Bob may be described in a similar way. The complexity of the referee, which corresponds to the verifier in an interactive proof system, is ignored given that we no longer consider an input string.

We note that two-player, one-round cooperative quantum games represent a generalization of the *non-local games* model of [14], where now the referee can send, receive, and process quantum information.

Description of the game

We now specify the two-player one-round cooperative quantum game of interest, using the same notation as in Definition 3.1. Choose S and T to be qutrit registers, and R, A and B to be single-qubit registers. The referee initializes the registers $(\mathsf{R},\mathsf{S},\mathsf{T})$ to the state

$$\frac{1}{\sqrt{2}}|0\rangle|00\rangle+\frac{1}{\sqrt{2}}|1\rangle|\phi\rangle$$

where

$$|\phi\rangle=\frac{1}{\sqrt{2}}|11\rangle+\frac{1}{\sqrt{2}}|22\rangle,$$

and sends S and T to Alice and Bob, who return A and B to the referee. The triple $(\mathsf{R},\mathsf{A},\mathsf{B})$ is measured with respect to the projective measurement $\{\Pi_0,\Pi_1\}$, where $\Pi_0=I-|\gamma\rangle\langle\gamma|$ and $\Pi_1=|\gamma\rangle\langle\gamma|$, for $|\gamma\rangle=(|000\rangle+|111\rangle)/\sqrt{2}$.

The intuition behind this game is as follows. Alice and Bob are presented with two possibilities, in superposition: they receive either the unentangled state $|00\rangle$ or the entangled state $|\phi\rangle$. Their goal is essentially to do nothing to $|00\rangle$ and to convert $|\phi\rangle$ to $|11\rangle$, for they want the referee to hold the state $|\gamma\rangle$ when the final measurement is made. These transformations must be done coherently, without measurements or residual evidence of which of the two transformations $|00\rangle\mapsto|00\rangle$ or $|\phi\rangle\mapsto|11\rangle$ was performed, for otherwise the final state of the referee will not have a large overlap with $|\gamma\rangle$.

The required transformation will be possible using coherent state exchange, with a winning probability approaching 1. It will be shown, however, that it is never possible for Alice and Bob to win with certainty, provided they initially share a finite entangled state.

Strategies that win with probability approaching 1

We now present a family of strategies for Alice and Bob that win with probability approaching 1. In the above game, Alice receives S from the referee and returns A; and likewise for Bob with registers T and B. Alice will begin with the qubit A initialized to $|0\rangle$, and Bob begins with B initialized to $|0\rangle$ as well. Let U be a unitary operation, acting on a pair consisting of a qutrit and a qubit, with the following behavior:

$$U:|0\rangle|0\rangle\mapsto|0\rangle|0\rangle,\qquad U:|1\rangle|0\rangle\mapsto|1\rangle|1\rangle,\qquad\text{and}\qquad U:|2\rangle|0\rangle\mapsto|2\rangle|1\rangle.$$

Upon receiving S, Alice applies U to (S,A), and Bob does likewise to (T,B) after receiving T. This leaves the 5-tuple $(\mathsf{R},\mathsf{A},\mathsf{B},\mathsf{S},\mathsf{T})$ in the state

$$\frac{1}{\sqrt{2}}|000\rangle|00\rangle+\frac{1}{\sqrt{2}}|111\rangle|\phi\rangle.$$

The coherent state exchange of $|\phi\rangle$ to $|00\rangle$ with error $1/N$ can now be done as described in Section 2. Sending A and B to the referee gives Alice and Bob a winning probability at least $1-1/N$.

Impossibility to win with certainty

Now we will prove that Alice and Bob cannot win with certainty regardless of the strategy they employ. Without loss of generality, it may be assumed that Alice and Bob initially share a pure entangled state $|\psi\rangle \in \mathcal{X}_A \otimes \mathcal{X}_B$, where the spaces $\mathcal{X}_A$ and $\mathcal{X}_B$ have the same dimension d. When Alice and Bob receive S and T from the referee, the state of the entire system is given by

$$\frac{1}{\sqrt{2}}|0\rangle|00\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle|\phi\rangle|\psi\rangle.$$

General operations performed by Alice and Bob at this point can be described by linear isometries through the use of the usual Stinespring representation of quantum channels. These isometries take the form $A : \mathcal{S} \otimes \mathcal{X}_A \to \mathcal{A} \otimes \mathcal{Y}_A$ for Alice and $B : \mathcal{T} \otimes \mathcal{X}_B \to \mathcal{B} \otimes \mathcal{Y}_B$ for Bob, where $\mathcal{S}, \mathcal{T}, \mathcal{A}, \mathcal{B}$ are the spaces associated with the registers S, T, A, and B, and the spaces $\mathcal{Y}_A$ and $\mathcal{Y}_B$ are arbitrary. The state of the system immediately before the referee measures is therefore

$$\frac{1}{\sqrt{2}}|0\rangle(A\otimes B)|00\rangle|\psi\rangle + \frac{1}{\sqrt{2}}|1\rangle(A\otimes B)|\phi\rangle|\psi\rangle.$$

By defining operators $A_0, A_1 \in \mathrm{L}(\mathcal{S}\otimes\mathcal{X}_A, \mathcal{Y}_A)$ and $B_0, B_1 \in \mathrm{L}(\mathcal{T}\otimes\mathcal{X}_B, \mathcal{Y}_B)$ as

$$A_0 = (\langle 0|\otimes I)A, \quad A_1 = (\langle 1|\otimes I)A, \quad B_0 = (\langle 0|\otimes I)B, \quad B_1 = (\langle 1|\otimes I)B,$$

we may express the probability that Alice and Bob win as

$$\left\| \frac{1}{2}(A_0\otimes B_0)|00\rangle|\psi\rangle + \frac{1}{2}(A_1\otimes B_1)|\phi\rangle|\psi\rangle \right\|^2 \leq \frac{1}{2} + \frac{1}{2}\left|\langle\phi|\langle\psi| A_1^* A_0 \otimes B_1^* B_0 |00\rangle|\psi\rangle\right|.$$

We have that $\|A_1^* A_0\| \leq 1$ and $\|B_1^* B_0\| \leq 1$, and therefore it is possible to express both $A_1^* A_0$ and $B_1^* B_0$ as convex combinations of unitary operators. By convexity, the winning probability p_{win} is upper-bounded as

$$p_{\mathrm{win}} \leq \frac{1}{2} + \frac{1}{2}\left|\langle\phi|\langle\psi| U\otimes V |00\rangle|\psi\rangle\right| \tag{3.1}$$

for some choice of unitary operators U and V. (As a side remark, we note that the optimal U, V in (3.1) can be derived from Lemma 1 of [35]. The inequality (3.1) can then be attained by choosing $A = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U$ and $B = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes V$.)

Notice that $|\phi\rangle|\psi\rangle$ has more entanglement than $(U\otimes V)|00\rangle|\psi\rangle$ so the states cannot be equal, and therefore the success probability cannot be 1. A quantitative bound may be proved as follows. Let ρ and ξ be the reduced density matrices on Alice's side for the above states,

$$\rho = \mathrm{Tr}_{\mathcal{B}\otimes\mathcal{Y}_B}\left(|\phi\rangle\langle\phi|\otimes|\psi\rangle\langle\psi|\right) \qquad \text{and} \qquad \xi = \mathrm{Tr}_{\mathcal{B}\otimes\mathcal{Y}_B} U\left(|00\rangle\langle 00|\otimes|\psi\rangle\langle\psi|\right)U^*.$$

If we first apply the monotonicity of the fidelity under partial tracing, and then the Fuchs-van de Graaf inequalities [22] relating the fidelity and the trace distance between two states, we obtain the bound

$$\left|\langle\phi|\langle\psi| U\otimes V |00\rangle|\psi\rangle\right| \leq \mathrm{F}(\rho,\xi) \leq \sqrt{1-\Delta^2},$$

where $\Delta = \frac{1}{2}\|\rho - \xi\|_1$ is the trace distance between ρ and ξ. Using (3.1),

$$1 - p_{\text{win}} \geq \frac{1}{2}(1 - |\langle\phi|\langle\psi| U \otimes V |00\rangle|\psi\rangle|) \geq \frac{1}{2}\left(1 - \sqrt{1-\Delta^2}\right) \geq \frac{\Delta^2}{4}.$$

The trace distance can be bounded along similar lines to what is done in [18]. The von Neumann entropies of ρ and ξ, denoted by $S(\rho)$ and $S(\xi)$, differ by 1. By the Fannes-Audenaert inequality [21, 1], it holds that

$$1 = S(\rho) - S(\xi) \leq \Delta \log(3d) + H(\Delta), \tag{3.2}$$

for $H(\cdot)$ denoting the binary entropy function. If it were the case that $\Delta < 1/(4\log(3d))$, then because the binary entropy function is increasing on the interval $(0, 1/2)$ it would follow that

$$\Delta \log(3d) + H(\Delta) < \frac{1}{4} + H\left(\frac{1}{4\log(3)}\right) \approx 0.88 < 1,$$

in contradiction with (3.2). It follows that

$$\Delta \geq \frac{1}{4\log(3d)},$$

and thus

$$p_{\text{win}} \leq 1 - \frac{1}{64\log^2(3d)}.$$

The error probability therefore decreases at most quadratically in the number of qubits that Alice and Bob initially share. (We note that the bound can be improved through a more fine-grained analysis. The bound is saturated, up to a change of constant factors, by the alternative choice of $|E_N\rangle$ described in Section 2.)

Consequences for entanglement assisted local quantum channels

For fixed spaces $\mathcal{S}$, $\mathcal{T}$, $\mathcal{A}$, and $\mathcal{B}$, a quantum channel $\Phi : \mathrm{L}(\mathcal{S} \otimes \mathcal{T}) \to \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$ is an *entanglement assisted local quantum channel* if it can be realized as illustrated in Figure 2; or more precisely, if there exists some choice of finite dimensional spaces $\mathcal{X}_A$ and $\mathcal{X}_B$, a density operator $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$, and quantum channels $\Psi_A : \mathrm{L}(\mathcal{S} \otimes \mathcal{X}_A) \to \mathrm{L}(\mathcal{A})$ and $\Psi_B : \mathrm{L}(\mathcal{T} \otimes \mathcal{X}_B) \to \mathrm{L}(\mathcal{B})$ such that $\Phi(\xi) = (\Psi_A \otimes \Psi_B)(\rho \otimes \xi)$ for all $\xi \in \mathrm{L}(\mathcal{S} \otimes \mathcal{T})$. Channels of this type are also known as *localizable* channels [3]. In addition to having an obvious relevance to two-prover quantum interactive proof systems, this is an interesting and fundamental class of quantum channels in its own right.

An unfortunate fact that follows from the analysis of the game presented above is the following. When $\mathcal{S}$ and $\mathcal{T}$ have dimension at least 3 and $\mathcal{A}$ and $\mathcal{B}$ have dimension at least 2, the set of entanglement-assisted local quantum channels $\Phi : \mathrm{L}(\mathcal{S} \otimes \mathcal{T}) \to \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$ is not a closed set: the sequence of entanglement-assisted local quantum channels induced by the strategies described above converges to a valid quantum channel that is not an entanglement-assisted local quantum channel. It remains open whether the set of entanglement-assisted local quantum channels $\Phi : \mathrm{L}(\mathcal{S} \otimes \mathcal{T}) \to \mathrm{L}(\mathcal{A} \otimes \mathcal{B})$ is a closed set when $\mathcal{S}$ and $\mathcal{T}$ are 2-dimensional.

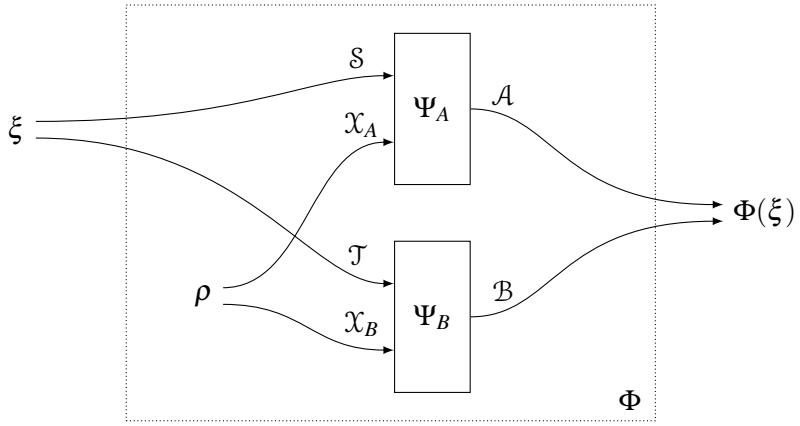

Figure 2: An entanglement-assisted local quantum channel Φ. An input state $\xi \in \mathrm{D}(\mathcal{S} \otimes \mathcal{T})$ is transformed into the output state $\Phi(\xi)$ by means of local quantum channels Ψ_A and Ψ_B, along with a shared entangled state $\rho \in \mathrm{D}(\mathcal{X}_A \otimes \mathcal{X}_B)$.

Another connection with prior work

We wish to point out one further connection between the above result and some existing work. In the exact catalytic transformation setting of Jonathan and Plenio [26], Daftuar and Klimesh [17] proved the following fact: the dimension of the catalyst required to transform one state to another, when this is possible, cannot be bounded by any function of the dimension of those states. Although this fact does not have a direct implication to the cooperative quantum games model, and is incomparable to our result as far as we can see, there is a similarity in spirit between the results that is worthy of note.

4 Near-perfect completeness

Kempe, Kobayashi, Matsumoto, and Vidick [28] proved that multi-prover quantum interactive proof systems can be efficiently transformed to have *perfect completeness*, while retaining small soundness error. An analogous fact was previously shown to hold for single-prover quantum interactive proof systems [30], but the two proofs are quite different. The proof in [30] for the single-prover case is very simple while the proof in [28] for the multi-prover case is rather complicated. In this section we show that the use of coherent state exchange allows the simple proof for the single-prover setting to be applied in the multi-prover setting.

There is, however, one small caveat: whereas Kempe, Kobayashi, Matsumoto, and Vidick achieve truly perfect completeness (in as far as quantum operations can ever be implemented perfectly), we must settle for *near-perfect* completeness: similar to the game from the previous section, honest provers will be able to convince the verifier to accept yes-inputs with any probability smaller than 1 that they desire, but the probability may not in actuality be 1. For most intents and purposes, though, we believe that this behavior can reasonably be viewed as representing perfect completeness.

Suppose that a verifier V interacts with m provers $P_1,\ldots,P_m$ for r rounds, and suppose the completeness and soundness probabilities for this verifier are given by c and s, respectively (which may be functions of the input length). Specifically, for the promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ of interest, the following conditions hold:

1. Completeness. The verifier is convinced to accept every yes-input $x \in A_{\text{yes}}$ with probability at least $c(|x|)$ by the provers' strategy.
2. Soundness. The verifier cannot be convinced to accept any no-input $x \in A_{\text{no}}$ with probability exceeding $s(|x|)$, regardless of the provers' strategy.

As usual and without loss of generality, we may "purify" a given proof system so that the verifier V and provers $P_1,\ldots,P_m$ are described by unitary operations and the provers' initial shared entanglement is pure. We also make two simple assumptions on the proof system and the completeness probability $c(|x|)$. First, we assume that it is possible for the provers to convince the verifier to accept every string $x \in A_{\text{yes}}$ with probability exactly $c(|x|)$. This can be achieved, for example, by appending an extra bit to the last message of the first prover and having the verifier reject when this bit is 1. Second, we assume that the value $c(|x|)$ is such that the verifier can efficiently implement the rotation

$$|0\rangle \mapsto \sqrt{1-c(|x|)}\,|0\rangle - \sqrt{c(|x|)}\,|1\rangle\,, \qquad |1\rangle \mapsto \sqrt{c(|x|)}\,|0\rangle + \sqrt{1-c(|x|)}\,|1\rangle$$

without error. (We also assume reversible computations incur no error.)

Now, assume that an input string $x \in A_{\text{yes}} \cup A_{\text{no}}$ has been fixed. (As x is now fixed, we will not explicitly refer to x or $|x|$ when discussing quantities depending on x.) Let p denote the probability that the verifier accepts. Given the purity assumption of the proof system, this means that the final state of the entire system at the end of the interaction may be expressed as

$$\sqrt{1-p}\,|0\rangle\,|\phi_0\rangle + \sqrt{p}\,|1\rangle\,|\phi_1\rangle\,,$$

where the first qubit in this expression represents the verifier's output qubit. The remaining part of the state, represented by $|\phi_0\rangle$ and $|\phi_1\rangle$, corresponds to the state of every other register in the proof system, shared in some arbitrary way among the verifier and provers. For simplicity we will assume that $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthogonal, which at most requires that the verifier makes a pseudo-copy of the output qubit (meaning that it XORs the output qubit onto a new qubit initialized to the $|0\rangle$ state) as its last action.

To transform the proof system to one with near-perfect completeness, one additional round of communication is added to the end of the protocol. To describe what happens in this additional round of communication, let us write A to denote the verifier's output qubit, V to denote the register comprising all of the verifier's memory aside from the output qubit, and $\mathsf{P}_1,\ldots,\mathsf{P}_m$ to denote registers representing the provers' memories, all corresponding to the final state of the original protocol.

To start the additional round of communication, the verifier prepares m additional single-qubit registers $\mathsf{A}_1,\ldots,\mathsf{A}_m$ as pseudo-copies of A, so that the state of the system becomes

$$\sqrt{1-p}\,|0\rangle\,|0^m\rangle\,|\phi_0\rangle + \sqrt{p}\,|1\rangle\,|1^m\rangle\,|\phi_1\rangle\,.$$

The verifier then sends V to the first prover P_1 (which is an arbitrary choice, but one that all provers are aware of), and sends each register A_i to prover P_i.

Upon receiving these registers from the verifier, the provers perform the following actions. First, using the registers $(\mathsf{A}_1,\ldots,\mathsf{A}_m)$ as control qubits, the provers perform coherent state exchange: when each register A_i contains 0, nothing happens; and when each register A_i contains 1, the state $|\phi_1\rangle$ is exchanged for $|\phi_0\rangle$. The resulting state of the entire system is

$$\sqrt{1-p}\,|0\rangle\,|0^m\rangle\,|\phi_0\rangle\,|E_N\rangle + \sqrt{p}\,|1\rangle\,|1^m\rangle\,|\phi_0\rangle\,|E'_N\rangle\,,$$

where

$$|E_N\rangle = \frac{1}{\sqrt{N}}\sum_{k=1}^{N} |\phi_0\rangle^{\otimes k}\,|\phi_1\rangle^{\otimes(N-k+1)}$$

is an additional shared entangled state the provers use for this purpose, and $|E'_N\rangle$ is defined in the same way as in Section 2. The number N is the provers' choice for an accuracy parameter, which we assume to be as large as they wish. Once this is done, the provers return the registers $\mathsf{A}_1,\ldots,\mathsf{A}_m$ to the verifier.

The final step is that the verifier measures the registers $(\mathsf{A},\mathsf{A}_1,\ldots,\mathsf{A}_m)$ with respect to a basis containing the state $\sqrt{1-c}\,|0\rangle\,|0^m\rangle + \sqrt{c}\,|1\rangle\,|1^m\rangle$, accepting if the output matches this state. (This is possible given our assumptions on c.) In the case that $x \in A_{\text{yes}}$ the provers may take $p = c$, and so the acceptance probability is

$$\Big\|(1-c)\,|E_N\rangle + c\,|E'_N\rangle\Big\|^2 \geq 1 - \frac{2}{N}.$$

This is arbitrarily close to 1, given that the provers may take any value for N. In the case that $x \in A_{\text{no}}$ we have $p \leq s$, from which it is routine to show that the acceptance probability is at most

$$\left(\sqrt{s}\sqrt{c} + \sqrt{1-s}\sqrt{1-c}\right)^2 \leq 1 - (c-s)^2$$

(where the inequality follows from the arithmetic-geometric mean inequality).

5 Conclusion

We have discussed two applications of coherent state exchange to the study of multi-prover quantum interactive proof systems.

The first application demonstrates that provers in a multi-prover quantum interactive proof system may not always have an optimal strategy when limited to finite entanglement. We view that the primary importance of this fact is that it will serve to better focus efforts on proving bounds on the amount of entanglement needed for *close-to-optimal* provers in multi-prover quantum interactive proofs—for such bounds can only exist in general for close-to-optimal and not optimal success probability.

The second application is a simple proof that multi-prover quantum interactive proof systems can be efficiently transformed to have near-perfect completeness by adding one round of communication. There is a trade-off between this proof and the proof of Kempe, Kobayashi, Matsumoto, and Vidick [28], which is that it is considerably simpler but cannot be said to achieve absolutely perfect completeness.

Two other applications of coherent state exchange have also been mentioned. First, we have proved that the collection of entanglement-assisted local quantum channels on systems of dimension 3 and higher is not a closed set. Second, we have proved that universal embezzling families exist for any number of parties.

We will conclude with a couple of open problems. First, our universal embezzling families for three or more parties appear to be highly inefficient. Do there exist constructions that offer a significant improvement in efficiency? Second, as alluded to above, it is interesting to consider near-optimal strategies for multiple provers, and it is unclear how much entanglement is needed in such cases. More specifically, consider all possible two-player cooperative quantum games of the type defined in Section 3 with fixed dimensions for R, S, T, A, and B, and fix a constant $\varepsilon > 0$. It would be interesting to find a uniform upper bound of the size of the auxiliary entangled state such that, for each game, an approximate strategy exists whose winning probability is ε-close to the optimal value.

Acknowledgments

We thank Aram Harrow and Peter Shor for the discussion how a modification to (2.1) improves the error in the coherent state exchange procedure. We also note that a shared state similar to the one in (2.1) was considered independently by Aram Harrow and Peter Show in the context of improving the performance of nonuniversal quantum state embezzlement. We thank Richard Cleve for additional discussions on embezzlement.

References

[1] K. AUDENAERT: A sharp continuity estimate for the von Neumann entropy. *Journal of Physics A: Mathematical and Theoretical*, 40(28):8127–8136, 2007. 11

[2] L. BABAI, L. FORTNOW, AND C. LUND: Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991. 2

[3] D. BECKMAN, D. GOTTESMAN, M. NIELSEN, AND J. PRESKILL: Causal and localizable quantum operations. *Physical Review A*, 64(5):52309, 2001. 11

[4] J. BELL: On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964. 2

[5] M. BEN-OR, S. GOLDWASSER, J. KILIAN, AND A. WIGDERSON: Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pp. 113–131, 1988. 2

[6] C. BENNETT AND G. BRASSARD: Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984. 2

[7] C. BENNETT, G. BRASSARD, C. CRÉPEAU, R. JOZSA, A. PERES, AND W. WOOTTERS: Teleporting an unknown quantum state via dual classical and EPR channels. *Physical Review Letters*, 70(12):1895–1899, 1993. 1

[8] C. BENNETT, D. DIVINCENZO, J. SMOLIN, AND W. WOOTTERS: Mixed state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996. 2

[9] C. BENNETT, P. SHOR, J. SMOLIN, AND A. THAPLIYAL: Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48(10):2637–2655, 2002. 1

[10] C. BENNETT AND S. WIESNER: Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992. 1

[11] G. BRASSARD: Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003. 2

[12] J. F. CLAUSER, M. A. HORNE, A. SHIMONY, AND R. A. HOLT: Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969. 2

[13] R. CLEVE, D. GAVINSKY, AND R. JAIN: Entanglement-resistant two-prover interactive proof systems and non-adaptive PIRs. *Quantum Information and Computation*, 9(7&8):648–656, 2009. 2

[14] R. CLEVE, P. HØYER, B. TONER, AND J. WATROUS: Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*, pp. 236–249, 2004. 2, 8

[15] R. CLEVE, W. SLOFSTRA, F. UNGER, AND S. UPADHYAY: Perfect parallel repetition theorem for quantum XOR proof systems. *Computational Complexity*, 17:282–299, 2008. 2

[16] T. COONEY, M. JUNGE, C. PALAZUELOS, AND D. PÉREZ-GARCÍA: Rank-one quantum games. Available as arXiv.org e-Print 1112.3563, 2011. 3, 4

[17] S. DAFTUAR AND M. KLIMESH: Mathematical structure of entanglement catalysis. *Physical Review A*, 64(4):042314, 2001. 12

[18] W. VAM DAM AND P. HAYDEN: Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003. 3, 5, 7, 11

[19] I. DEVETAK, A. HARROW, AND A. WINTER: A family of quantum protocols. *Physical Review Letters*, 93(23):230505, 2004. 2

[20] A. EKERT: Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991. 2

[21] M. FANNES: A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31(4):291–294, 1973. 11

[22] C. FUCHS AND J. VAN DE GRAAF: Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999. 10

[23] N. GISIN: Bell inequalities: many questions, a few answers. *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle*, 73:125–138, 2009. 2

[24] A. HARROW, P. HAYDEN, AND D. LEUNG: Superdense coding of quantum states. *Physical Review Letters*, 92(18):187901, 2004. 1

[25] T. ITO AND T. VIDICK: A multi-prover interactive proof for NEXP sound against entangled provers. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science*, 2012. 2, 3

[26] D. JONATHAN AND M. PLENIO: Entanglement-assisted local manipulation of pure quantum states. *Physical Review Letters*, 83(17):3566–3569, 1999. 7, 12

[27] J. KEMPE, H. KOBAYASHI, K. MATSUMOTO, B. TONER, AND T. VIDICK: Entangled games are hard to approximate. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, 2008. 2

[28] J. KEMPE, H. KOBAYASHI, K. MATSUMOTO, AND T. VIDICK: Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18:273–307, 2009. 3, 12, 14

[29] J. KEMPE, O. REGEV, AND B. TONER: Unique games with entangled provers are easy. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, pp. 457–466, 2008. 2

[30] A. KITAEV AND J. WATROUS: Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pp. 608–617, 2000. 3, 12

[31] H. KOBAYASHI AND K. MATSUMOTO: Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3), 2003. 2

[32] H.-K. LO AND H. F. CHAU: Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999. 2

[33] O. REGEV AND T. VIDICK: Quantum XOR games. Available as arXiv.org e-Print 1207.4939, 2012. 3, 4

[34] P. SHOR AND J. PRESKILL: Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000. 2

[35] G. VIDAL, D. JONATHAN, AND M. NIELSEN: Approximate transformations and robust manipulation of bipartite pure state entanglement. *Physical Review A*, 62:012304, 2000. 10

[36] T. VIDICK: Three-player entangled XOR games are NP-hard to approximate. In *54th Annual IEEE Symposium on Foundations of Computer Science*, 2013. To appear. 3

[37] S. WEHNER: Entanglement in interactive proof systems with binary answers. In *Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science*, volume 3884 of *Lecture Notes in Computer Science*, pp. 162–171. Springer, 2006. 2

[38] R. DE WOLF: Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002. 2

AUTHORS

Debbie Leung
Department of Combinatorics and Optimization
University of Waterloo
wcleung@uwaterloo.ca
http://www.math.uwaterloo.ca/~wcleung

Ben Toner*
School of Physics
University of Melbourne
bentoner@bentoner.com
http://bentoner.com

John Watrous
School of Computer Science
University of Waterloo
john.watrous@uwaterloo.ca
http://www.cs.uwaterloo.ca/~watrous

*This research was done while the author was at Centrum Wiskunde & Informatica, Amsterdam, The Netherlands