Parallelization, amplification, and exponential time simulation of quantum interactive proof systems

Alexei Kitaev[*] John Watrous[†]

ABSTRACT

In this paper we consider quantum interactive proof systems, which are interactive proof systems in which the prover and verifier may perform quantum computations and exchange quantum information. We prove that any polynomial-round quantum interactive proof system with two-sided bounded error can be parallelized to a quantum interactive proof system with exponentially small one-sided error in which the prover and verifier exchange only 3 messages. This yields a simplified proof that PSPACE has 3-message quantum interactive proof systems. We also prove that any language having a quantum interactive proof system can be decided in deterministic exponential time, implying that single-prover quantum interactive proof systems are strictly less powerful than multiple-prover classical interactive proof systems unless EXP = NEXP.

1. INTRODUCTION

Interactive proof systems were introduced by Babai [3] and Goldwasser, Micali, and Rackoff [17] in 1985. In the same year, Deutsch [10] gave the first formal treatment of quantum computation. Since then, both subjects have received a great deal of attention and have generated a number of exciting results, perhaps most notably the IP = PSPACE characterization of Lund, Fortnow, Karloff, and Nisan [25] and Shamir [26], and the polynomial-time quantum algorithms for factoring and discrete logarithms due to Shor [28].

In this paper we consider quantum interactive proof systems, which merge notions from these two subjects. A quantum interactive proof system consists of two parties—a prover with unbounded quantum computational power and a quantum polynomial-time verifier—that communicate through a quantum channel. As in the case of classical interactive proof systems, the prover attempts to prove to the verifier that a given input string satisfies some specified property, while the verifier tries to determine the validity of this proof. A language L is said to have a quantum interactive proof system if there exists a quantum verifier V such that (i) there exists a quantum prover P that can always convince V to accept when the input is in L, and (ii) no quantum prover P can convince V to accept with nonnegligible probability when the input is not in L.

Quantum interactive proof systems were first studied in a paper by one of us [30], wherein it was shown that every PSPACE language has a quantum interactive proof system, with exponentially small one-sided error, in which the prover and verifier exchange a total of only 3 messages. This implies that any classical interactive proof system can be parallelized to require just 3 messages in the quantum setting, which is a task that cannot be accomplished classically unless the polynomial-time hierarchy collapses to AM [3; 18]. In this paper we prove the following stronger result: any *quantum* interactive proof system can be parallelized to a 3-message quantum protocol with exponentially small one-sided error. In order to achieve exponentially small error in the 3-message case, we prove the somewhat surprising fact that entanglement among parallel repetitions of a 3-message quantum interactive proof system gives a cheating prover absolutely no increase in success probability. Our result simplifies the proof that PSPACE has 3-message quantum interactive proof systems, in the sense that it treats any classical protocol for a given PSPACE language as a black-box.

While (single-prover) classical interactive proof systems recognize precisely those languages in PSPACE, it was shown by Babai, Fortnow, and Lund [4] that any language in nondeterministic exponential time (NEXP) has a two-prover interactive proof system, wherein the two provers are not permitted to communicate with one another during the protocol. A sequence of papers [9; 13; 24] led to a result of Feige and Lovász [14] that any language in NEXP has a two-prover interactive proof system requiring just one round of communication (meaning that the verifier sends one question to each of the provers in parallel, then receives their responses). A natural question to ask is whether NEXP has single-prover quantum interactive proof systems, or equivalently whether single-prover quantum interactive proof systems can simulate multiple classical provers. We show that this is not likely to be the case, as any language having a quantum interactive proof system is necessarily contained in determin-

[*] Microsoft Research, One Microsoft Way, Redmond, WA 98052, e-mail: kitaev@microsoft.com. On leave from L.D. Landau Institute for Theoretical Physics

[†] Department of Computer Science, University of Calgary, 2500 University Drive NW, Calgary (Alberta), Canada T2N 1N4, e-mail: jwatrous@cpsc.ucalgary.ca.

istic exponential time (EXP); under the assumption EXP $\neq$ NEXP, multiple-prover classical interactive proof systems are strictly more powerful than single-prover quantum interactive proof systems. Our proof of this fact relies on the technique of semidefinite programming.

The remainder of this paper is organized as follows. In section 2 we review necessary background information and define the quantum interactive proof system model. In section 3 we prove that two-sided error quantum interactive proof systems can be converted to one-sided error quantum interactive proofs by adding one round of communication to the protocol, in section 4 we prove that any polynomial-message (one-sided error) quantum interactive proof system can be parallelized to a 3-message protocol, and in section 5 we prove that parallel executions of a given 3-message quantum interactive proof system result in an exponential decrease in error probability. In section 6 we prove that any language having a quantum interactive proof system is contained in EXP. We conclude with section 7, which summarizes the relations we have proved and mentions a number of open questions regarding quantum interactive proofs.

2. PRELIMINARIES

We begin by mentioning some of the basic notation used in this paper. As usual, $\mathbb{N}$, $\mathbb{Z}^+$, and $\mathbb{C}$ denote the positive integers, the nonnegative integers, and complex numbers, respectively. For a given complex number z, $\Re(z)$ denotes the real part of z. We let *poly* denote the class of functions $f : \mathbb{Z}^+ \to \mathbb{N}$ satisfying the following two properties: (i) there exists a polynomial p such that $f(n) \leq p(n)$ for all $n \in \mathbb{Z}^+$, and (ii) $f(n)$ is computable in time polynomial in n. We also write $poly^{-1}$, 2^{-poly}, etc., to denote classes of functions derived from functions in *poly* in the obvious ways. The length of a given string x is denoted $|x|$, and we assume all strings are over the alphabet $\Sigma = \{0, 1\}$. Given a finite set S, $\ell_2(S)$ denotes the Hilbert space of dimension $|S|$ whose elements are mappings from S to $\mathbb{C}$. All Hilbert spaces considered in this paper will be finite dimensional, and this assumption will be made hereafter without explicit mention. For any positive semidefinite operator A acting on a given Hilbert space, there exists a unique positive semidefinite operator denoted by $\sqrt{A}$ that satisfies $(\sqrt{A})^2 = A$.

2.1 Quantum formalism

Next we briefly review various facts and notation from quantum computation and quantum information theory. We will not attempt to provide a comprehensive review, as this has been done elsewhere. (See, for instance, the surveys of Berthiaume [8] and Kitaev [23].)

For given Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, $\mathbf{L}(\mathcal{H}, \mathcal{K})$ denotes the set of linear operators mapping $\mathcal{H}$ to $\mathcal{K}$, $\mathbf{L}(\mathcal{H})$ denotes $\mathbf{L}(\mathcal{H}, \mathcal{H})$, $\mathbf{D}(\mathcal{H})$ denotes the set of positive semidefinite operators on $\mathcal{H}$ having unit trace, $\mathbf{U}(\mathcal{H})$ denotes the set of unitary operators on $\mathcal{H}$, and $\mathbf{P}(\mathcal{H})$ denotes the set of projection operators on $\mathcal{H}$. Finally, $\mathbf{T}(\mathcal{H}, \mathcal{K})$ denotes the set of linear mappings from $\mathbf{L}(\mathcal{H})$ to $\mathbf{L}(\mathcal{K})$, viewing $\mathbf{L}(\mathcal{H})$ and $\mathbf{L}(\mathcal{K})$ as linear spaces in the usual way, and $\mathbf{T}(\mathcal{H})$ denotes $\mathbf{T}(\mathcal{H}, \mathcal{H})$. The identity elements of $\mathbf{L}(\mathcal{H})$ and $\mathbf{T}(\mathcal{H})$ are denoted $I_{\mathcal{H}}$ and $I_{\mathbf{L}(\mathcal{H})}$, respectively.

A *pure state* or *superposition* of a quantum system having (finite) classical state set S is a unit vector in the Hilbert space $\mathcal{H} = \ell_2(S)$. We use the Dirac notation to represent elements of Hilbert spaces: for each $s \in S$, $|s\rangle$ represents the unit vector corresponding to the map that takes s to 1 and each $s' \neq s$ to 0. Arbitrary vectors will be denoted $|\psi\rangle$, $|\phi\rangle$, etc., even though the symbols ψ, ϕ, etc., are not used alone, and may be specified by linear combinations of elements in the orthonormal basis $\{|s\rangle : s \in S\}$. Corresponding to each $|\psi\rangle$ is a linear functional $\langle\psi|$ that maps each vector $|\phi\rangle$ to the inner product $\langle\psi|\phi\rangle$ (conjugate-linear in the first argument).

A *mixed state* of a quantum system is a state that may be described by a distribution on (not necessarily orthogonal) pure states. A collection $\{(p_k, |\psi_k\rangle)\}$ such that $0 \leq p_k$, $\sum_k p_k = 1$, and each $|\psi_k\rangle$ is a pure state is called a *mixture*: for each k, the system is in superposition $|\psi_k\rangle$ with probability p_k. With a given mixture $\{(p_k, |\psi_k\rangle)\}$, we associate a *density operator* $\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k|$. Necessary and sufficient conditions for a given operator $\rho \in \mathbf{L}(\mathcal{H})$ to be a density operator (i.e., to represent some mixed state) are (i) ρ must be positive semidefinite, and (ii) ρ must have unit trace. (Thus, $\mathbf{D}(\mathcal{H})$ denotes the set of density operators over a given space $\mathcal{H}$.) Different mixtures may yield identical states, in the sense that no measurement can distinguish the mixtures even in a statistical sense. Two mixtures yielding different density operators can be statistically distinguished however, and for this reason we interpret a given density operator ρ as being a canonical representation of a given mixed state.

An *admissible transformation* from $\mathbf{D}(\mathcal{H})$ to $\mathbf{D}(\mathcal{K})$ is a mapping T for which there exists a some collection $\{A_1, \ldots, A_k\}$ of operators in $\mathbf{L}(\mathcal{H}, \mathcal{K})$ such that (i) $T(\rho) = \sum_{j=1}^k A_j \rho A_j^\dagger$ for every ρ, and (ii) $\sum_{j=1}^k A_j^\dagger A_j = I_{\mathcal{H}}$. It is a straightforward exercise to verify that such mappings preserve both trace and the property of a operator being positive semidefinite. Admissible transformations are precisely those transformations that can (in principle) be realized physically. We identify admissible transformations with elements of $\mathbf{T}(\mathcal{H}, \mathcal{K})$ as follows: $T(X) = \sum_{j=1}^k A_j X A_j^\dagger$ for each $X \in \mathbf{L}(\mathcal{H})$.

For any Hilbert space $\mathcal{H}$ there is exactly one admissible transformation $T \in \mathbf{T}(\mathcal{H}, \mathbb{C})$, which necessarily satisfies $T(X) = \mathrm{tr}(X)$ for every $X \in \mathbf{L}(\mathcal{H})$. To perform this transformation on some part of a quantum system essentially means that this part of the system is discarded or not further considered. When necessary we refer to this transformation as the *trace-out* operation, and more commonly we say that some part of a given system is *traced-out* to mean that this operation is performed on that part of the system. The *partial trace* is defined as follows: given a density operator $\rho \in \mathbf{D}(\mathcal{H} \otimes \mathcal{K})$ and any orthonormal basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$ of $\mathcal{K}$, define

$$\mathrm{tr}_{\mathcal{K}}\, \rho = \sum_{j=1}^n (I_{\mathcal{H}} \otimes \langle e_j|) \rho (I_{\mathcal{H}} \otimes |e_j\rangle).$$

Alternately we may define the partial trace by taking the tensor product of the identity transformation and the trace-out operation.

Any unitary operator $U \in \mathbf{U}(\mathcal{H})$ gives rise to an admissible transformation $T_U \in \mathbf{T}(\mathcal{H})$ given by $T_U(\rho) = U\rho U^\dagger$. Any transformation that can be expressed in this way will be called a *unitary transformation.* When describing unitary transformations, it is sufficient (and often more convenient) to describe the transformation in question in terms of its action on pure states: in case T is a unitary transformation we write $T(|\phi\rangle) = |\psi\rangle$ to mean $T(|\phi\rangle\langle\phi|) = |\psi\rangle\langle\psi|$.

It is helpful to note the following alternate characterization of admissible transformations. A transformation T from $\mathbf{D}(\mathcal{H})$ to $\mathbf{D}(\mathcal{K})$ is admissible if and only if there exist Hilbert spaces $\mathcal{F}$, $\mathcal{G}$, and $\mathcal{L}$ satisfying $\mathcal{L} \cong \mathcal{H} \otimes \mathcal{F} \cong \mathcal{K} \otimes \mathcal{G}$, a unitary operator $U \in \mathbf{U}(\mathcal{L})$, and an arbitrary vector $|\psi\rangle \in \mathcal{F}$ such that $T(\rho) = \operatorname{tr}_{\mathcal{G}} U(\rho \otimes |\psi\rangle\langle\psi|)U^{\dagger}$ for every $\rho \in \mathbf{D}(\mathcal{H})$. It can be proved (see [23]) that if T is admissible then we may take $\mathcal{L}$ such that $\dim(\mathcal{L}) \leq \dim(\mathcal{H})\dim(\mathcal{K})$.

An important concept in quantum physics is that of a *measurement*. Although measurements may be treated as particular types of admissible transformations, it is helpful to formalize them somewhat differently. Any collection of operators $\{A_1, \ldots, A_k\}$ satisfying $\sum_{j=1}^{k} A_j^{\dagger} A_j = I$ defines a measurement. If a system in a mixed state ρ is observed via such a measurement, then the following happens: (i) for each $j \in \{1, \ldots, k\}$ the result of the measurement is j with probability $\operatorname{tr}(A_j \rho A_j^{\dagger})$, and (ii) the state of the system is changed to one represented by the density operator $A_j \rho A_j^{\dagger} / \operatorname{tr}(A_j \rho A_j^{\dagger})$ for whichever j resulted in (i). In case $\{A_1, \ldots, A_k\}$ is a collection of orthonormal projections, the measurement is a *projection* or *von Neumann* measurement. When we say that a system is observed in a particular basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$, we mean that is observed according to the projection measurement given by $\{|e_1\rangle\langle e_1|, \ldots, |e_n\rangle\langle e_n|\}$.

We define the following norms on $\mathbf{L}(\mathcal{H})$ and $\mathbf{T}(\mathcal{H}, \mathcal{K})$: for $X \in \mathbf{L}(\mathcal{H})$ define $\|X\|_{\mathrm{tr}} = \operatorname{tr}\sqrt{X^{\dagger}X}$ and

$$\|X\| = \sup_{|\psi\rangle \in \mathcal{H} \setminus \{0\}} \frac{\|X|\psi\rangle\|}{\||\psi\rangle\|}$$

(with $\|\cdot\|$ denoting the ℓ_2-norm), and for $T \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ define

$$\|T\|_{\diamond} = \inf\left\{\|A\|\,\|B\| \;:\; T(\cdot) = \operatorname{tr}_{\mathcal{F}}(A \,\cdot\, B^{\dagger})\right\}.$$

Here, the infimum is taken over all $A, B \in \mathbf{L}(\mathcal{H}, \mathcal{K} \otimes \mathcal{F})$ with $\dim(\mathcal{H})\dim(\mathcal{K}) \leq \dim(\mathcal{F})$. In general, the norm $\|\cdot\|_{\mathrm{tr}}$ (known as the *trace norm*) is appropriate for measuring distance between density operators, while $\|\cdot\|_{\diamond}$ (called the *diamond norm*) is appropriate for measuring distances between admissible transformations. The norm $\|\cdot\|_{\mathrm{tr}}$ may also be extended to $T \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ as

$$\|T\|_{\mathrm{tr}} = \sup_{X \in \mathbf{L}(\mathcal{H}) \setminus \{0\}} \frac{\|T(X)\|_{\mathrm{tr}}}{\|X\|_{\mathrm{tr}}}.$$

Given two density operators $\rho, \xi \in \mathbf{D}(\mathcal{H})$, we also define the *fidelity* between ρ and ξ, denoted $F(\rho, \xi)$, as follows:

$$F(\rho, \xi) = \left\|\sqrt{\rho}\sqrt{\xi}\right\|_{\mathrm{tr}}^{2}.$$

Some of the proofs contained in this paper rely on the facts stated in the following theorem.

THEOREM 1. *The following relations hold:*

1. *For* $X \in \mathbf{L}(\mathcal{H})$, $\|X\|_{\mathrm{tr}} = \max\{|\operatorname{tr}(UX)| \,:\, U \in \mathbf{U}(\mathcal{H})\}$.
2. *Let* $T \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ *and let* $\mathcal{L}$ *be a Hilbert space satisfying* $\dim(\mathcal{L}) \geq \dim(\mathcal{H})$. *Then* $\|T\|_{\diamond} = \|T \otimes I_{\mathbf{L}(\mathcal{L})}\|_{\mathrm{tr}}$.
3. *Let* $T_1, T_2 \in \mathbf{T}(\mathcal{H}, \mathcal{K})$. *Then* $\|T_1 \otimes T_2\|_{\diamond} = \|T_1\|_{\diamond}\|T_2\|_{\diamond}$.
4. *Let* $\mathcal{H}$ *and* $\mathcal{K}$ *be Hilbert spaces with* $\dim(\mathcal{H}) \leq \dim(\mathcal{K})$ *and let* $\rho, \xi \in \mathbf{D}(\mathcal{H})$. *Then* $F(\rho, \xi) = \max\left\{|\langle\phi|\psi\rangle|^2\right\}$, *where the maximum is taken over all* $|\phi\rangle, |\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ *satisfying* $\operatorname{tr}_{\mathcal{K}} |\psi\rangle\langle\psi| = \rho$ *and* $\operatorname{tr}_{\mathcal{K}} |\phi\rangle\langle\phi| = \xi$. *Equivalently, for* $\epsilon = \min\{\||\phi\rangle - |\psi\rangle\|\}$ *(over the same set of values for* $|\psi\rangle$ *and* $|\phi\rangle$*) we have* $F(\rho, \xi) = (1 - \epsilon^2/2)^2$.
5. *Let* $\rho, \xi \in \mathbf{D}(\mathcal{H})$. *Then*
$$2 - 2\sqrt{F(\rho, \xi)} \leq \|\rho - \xi\|_{\mathrm{tr}} \leq 2\sqrt{1 - F(\rho, \xi)}.$$
6. *If* $|\phi\rangle, |\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ *satisfy* $\operatorname{tr}_{\mathcal{K}} |\phi\rangle\langle\phi| = \operatorname{tr}_{\mathcal{K}} |\psi\rangle\langle\psi|$, *then there exists* $U \in \mathbf{U}(\mathcal{K})$ *such that* $(I \otimes U)|\phi\rangle = |\psi\rangle$.

Proofs of the facts comprising Theorem 1 can be found as follows: 1. see page 430 of [20], 2. and 3. see [1] or [23], 4. see [22], 5. see [15], and 6. see [21].

2.2 Quantum circuits

The computational model upon which quantum interactive proof systems are based is the (acyclic) quantum circuit model. See [1; 8; 23; 31] for background information regarding quantum circuits.

A family $\{Q_x\}$ of quantum circuits is said to be *polynomial-time uniformly generated* if there exists a deterministic procedure that, on input x, outputs a description of Q_x and runs in time polynomial in x. It is assumed that the circuits in such a family are composed only of gates in what has been called the *Shor basis*: Hadamard gates, $\sqrt{\sigma_z}$ gates, and Toffoli gates [27]. Furthermore, it is assumed that the number of gates in any circuit is not more than the length of that circuit's description (i.e., no compact descriptions of large circuits are allowed), so Q_x must have size polynomial in $|x|$. Often we identify a circuit Q_x with the unitary operator it induces.

A few notes are in order regarding polynomial-time uniformly generated families of quantum circuits. First, we note that the above notion of uniformity is somewhat nonstandard, since we allow an input x to be given to the procedure generating the circuits rather than just $|x|$ written in unary. This does not change the computational power for the resulting class of quantum circuits, and we find that it is more convenient to describe the quantum interactive proof system model using this notion. The second note regards our choice of the Shor basis. This collection of gates is universal (in the sense described in [5; 6; 11; 12], for instance); see [23] for a proof of this fact. While our results hold for any other reasonable choice for a universal set of gates, we have chosen this basis for definiteness and convenience; by allowing reversible computations and Hadamard transforms to be performed without error, we avoid the need to including negligible error terms in some calculations.

The actions performed by the interacting parties in a quantum interactive proof system will be described by quantum circuits. In the case of the verifier, whose computational power is assumed to be limited, actions essentially correspond to polynomial-time uniformly generated families of circuits; this will be made more precise in the next subsection. In the case of the prover we allow circuits composed of arbitrary unitary gates, as we do not place restrictions on the complexity or precision of the prover's actions. (Note, however, that the prover must of course obey the restrictions imposed by the laws of quantum physics.) One may instead view the prover as simply applying some arbitrary unitary transformation to a collection of qubits rather than applying a particular circuit.

Our model does not change if we consider the more general class of quantum circuits one obtains if gates are permitted to correspond to arbitrary admissible transformations on collections of qubits (rather than just the unitary gates in the Shor basis, which perform only unitary transformations). This follows from the characterization of admissible transformations mentioned above—for a detailed discussion of the equivalence of the unitary vs. non-unitary quantum circuit models, see [1]. Often we will describe quantum circuits in a high-level manner that suggests that measurements are performed at various times as the circuits are applied to some collection of qubits. In fact, as all of our circuits are assumed to be unitary, such measurements do not occur, but rather are assumed to be simulated by unitary gates as described in [1].

2.3 Quantum interactive proof systems

In this section we define the quantum interactive proof system model. It is assumed the reader is familiar with classical interactive proof systems, which have been discussed in detail in a number of works (see, e.g., [16] and the references therein).

As in the classical case, a quantum interactive proof system consists of two parties, a prover with unlimited computation power and a computationally bounded verifier, that receive a common input string and have an interaction that determines whether or not the verifier is to accept the input. The goal of the prover is to convince the verifier that the input satisfies some particular property, while the goal of the verifier is to decide whether the prover's argument is valid. Quantum interactive proofs differ from classical interactive proofs in that the prover and verifier may send and process quantum information (i.e., qubits). This may result in a situation in which the prover's qubits and verifier's qubits are *entangled*. While the verifier in a quantum interactive proof system gains the advantage of being able to perform quantum computations over classical computations, it seems to be the case that this is secondary to cryptographic advantages offered by entanglement.

We now formalize the notion of a quantum interactive proof system using the quantum circuit model. We begin by describing separately the two parties.

A quantum verifier is a polynomial-time computable mapping of the form $V : \Sigma^* \to \Sigma^*$. For each $x \in \Sigma^*$, $V(x)$ is interpreted as a $k(|x|)$-tuple $(V(x)_1, \ldots, V(x)_{k(|x|)})$, for some polynomial bounded function k, with each $V(x)_j$ a description of a quantum circuits acting on $q_{\mathcal{V}}(|x|) + q_{\mathcal{M}}(|x|)$ qubits (for $q_{\mathcal{V}}$ and $q_{\mathcal{M}}$ polynomial bounded functions to be discussed shortly). It is assumed that these circuit descriptions satisfy the properties of polynomial-time uniformly generated circuits discussed in the previous subsection; each circuit $V(x)_j$ is of size polynomial in $|x|$, and each circuit $V(x)_j$ is composed only of gates in the Shor basis. The qubits upon which each circuit $V(x)_j$ acts are divided into two sets: $q_{\mathcal{V}}(|x|)$ qubits that are private to the verifier, and $q_{\mathcal{M}}(|x|)$ qubits that represent the communication channel between the prover and verifier. One of the verifier's private qubits is designated as the output qubit.

A prover is a mapping P that maps each input $x \in \Sigma^*$ to an $l(|x|)$-tuple $(P(x)_1, \ldots, P(x)_{l(|x|)})$ of quantum circuits, for some function l, with each circuit acting on $q_{\mathcal{M}}(|x|)+q_{\mathcal{P}}(|x|)$ qubits. No restrictions are placed on the complexity of the mapping P, the gates of which each $P(x)_j$ is composed, or on the size of each $P(x)_j$ (i.e., each $P(x)_j$ may simply be viewed as a unitary transformation). As in the case of the verifier, the qubits upon which each $P(x)_j$ acts are divided into two sets: $q_{\mathcal{P}}(|x|)$ qubits that are private to the prover, and $q_{\mathcal{M}}(|x|)$ qubits representing the communication channel. A verifier V and a prover P are compatible if for all inputs x we have (i) each $V(x)_i$ and $P(x)_j$ agree on the number $q_{\mathcal{M}}(|x|)$ of message qubits upon which they act, and (ii) $k(|x|) = \lfloor m(|x|)/2 + 1 \rfloor$ and $l(|x|) = \lfloor m(|x|)/2 + 1/2 \rfloor$ for some $m(|x|)$ (representing the number of messages exchanged). We say that V is an m-message verifier and P is an m-message prover in this case. Whenever we discuss an interaction between a prover and verifier, we naturally assume they are compatible.

Given a verifier V, a prover P, and an input x, we define a circuit $(V(x), P(x))$ acting on $q(|x|) = q_{\mathcal{V}}(|x|) + q_{\mathcal{M}}(|x|) + q_{\mathcal{P}}(|x|)$ qubits as follows. If $m(|x|)$ is odd, circuits

$$P(x)_1, V(x)_1, \ldots, P(x)_{(m(|x|)+1)/2}, V(x)_{(m(|x|)+1)/2}$$

are applied in sequence, each to the $q_{\mathcal{M}}(|x|) + q_{\mathcal{P}}(|x|)$ message and prover qubits or to the $q_{\mathcal{V}}(|x|) + q_{\mathcal{M}}(|x|)$ verifier and message qubits accordingly. If $m(|x|)$ is even the situation is similar, except that the verifier applies the first circuit; circuits

$$V(x)_1, P(x)_1, V(x)_2, \ldots, P(x)_{m(|x|)/2}, V(x)_{m(|x|)/2+1}$$

are applied in sequence similar to the above case. This situation is illustrated in Figure 1 for the case $m(|x|) = 4$.

Now, for a given input x, the probability that the pair (V, P) accepts x is defined to be the probability that an observation of the output qubit (in the $\{|0\rangle, |1\rangle\}$ basis) yields the value 1, after the circuit $(V(x), P(x))$ is applied to a collection of $q(|x|)$ qubits each initially in the $|0\rangle$ state.

Finally, we define a number of classes of languages based on quantum interactive proof systems.

Definition 1. For functions $m : \mathbb{Z}^+ \to \mathbb{N}$ and $a, b : \mathbb{Z}^+ \to [0, 1]$, let $\mathrm{QIP}(m, a, b)$ denote the class of languages L for which there exists an m-message verifier V such that

1. There exists an m-message prover P such that for any $x \in L$, (V, P) accepts x with probability at least $a(|x|)$.
2. For all m-message provers P and all $x \notin L$, (V, P) accepts x with probability at most $b(|x|)$.

We also let $\mathrm{QIP}(\mathit{poly}, a, b)$ denote the union of the classes $\mathrm{QIP}(m, a, b)$ over all $m \in \mathit{poly}$.

It will be necessary in our proofs to refer to the quantum states of various subsystems of a quantum interactive proof system. We will use the following notation for this purpose. Assume we have a verifier V and a prover P, and let us fix an input x. For readability we often drop the argument x and $|x|$ in the various functions above when it is understood (e.g., we write V_j and P_j to denote $V(x)_j$ and $P(x)_j$ for each j, and we write m to denote $m(|x|)$). Let $\mathcal{V} = \ell_2(\Sigma^{q_{\mathcal{V}}})$, $\mathcal{M} = \ell_2(\Sigma^{q_{\mathcal{M}}})$, and $\mathcal{P} = \ell_2(\Sigma^{q_{\mathcal{P}}})$ denote the Hilbert spaces corresponding to the verifier's qubits, the message qubits, and the prover's qubits, respectively. At a given instant, the state of the circuit (V, P) is thus a unit vector in the space $\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$. For instance, if $|\psi_{init}\rangle$ denotes the state in which all qubits are zero, the state of the system after all of the prover's and verifier's circuits have been applied is $V_2 P_2 V_1 P_1 |\psi_{init}\rangle$ in the case $m = 3$. Here, and throughout this paper, we assume that operators acting on subsystems of a given system are extended to the entire system by tensoring with the identity—in all cases it will be clear from context upon what part of a system a given operator acts. We may also consider the mixed states

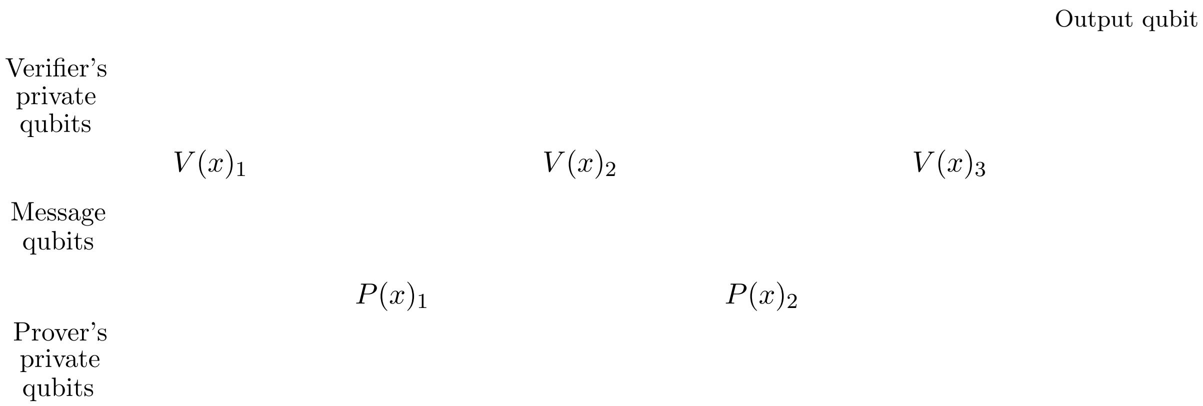

Figure 1: Quantum circuit for a 4-message quantum interactive proof system

of subsystems of circuits in the usual way; for instance, if $|\psi\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ denotes the state of (V, P) at some time, then $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}} |\psi\rangle\langle\psi| \in \mathbf{D}(\mathcal{V})$ denotes the mixed state of the verifier's qubits that results by excluding the message qubits and prover's qubits from consideration.

3. ONE-SIDED VS. TWO-SIDED ERROR

In this section we prove that any quantum interactive proof system having two-sided bounded error can be made to have one-sided bounded error at the cost of one additional round of communication.

Theorem 2. *Let $m \in poly$ and let $a : \mathbb{Z}^+ \to [0, 1]$ be such that there exists a family $\{Q_{1^n}\}$ of polynomial-time uniformly generated quantum circuits such that Q_{1^n} performs (exactly) the unitary transformation $T_{a(n)}$ having the following effect on pure states:*

$$\begin{aligned} T_{a(n)}(|0\rangle) &= \sqrt{a(n)}|0\rangle - \sqrt{1-a(n)}|1\rangle \\ T_{a(n)}(|1\rangle) &= \sqrt{1-a(n)}|0\rangle + \sqrt{a(n)}|1\rangle. \end{aligned}$$

Then for $b : \mathbb{Z}^+ \to [0, 1]$ satisfying $b(n) < a(n)$ for every n, $\mathrm{QIP}(m, a, b) \subseteq \mathrm{QIP}(m + 2, 1, 1 - (a - b)^2)$.

Proof. Let $L \in \mathrm{QIP}(m, a, b)$ for m, a, and b as in the statement of the theorem. Without loss of generality, we may assume there exists an m-message protocol for L that causes the verifier to accept with probability precisely equal to $a(|x|)$ for each input $x \in L$ (following from the fact that any nontrivial protocol can be modified to yield one in which the prover can decrease the probability that the verifier accepts by any desired quantity). In order to prove $L \in \mathrm{QIP}(m+2, 1, 1-(a-b)^2)$, we consider the modification of such a protocol as described in Figure 2.

Consider an execution of this protocol on a given input x of length n. Suppose that $|\psi\rangle$ describes the state of register $\mathbf{R}$, along with any of the prover's private registers, after the original protocol is simulated in step 1. After $\mathbf{B}$ and $\mathbf{B}'$ are incremented, the state of the entire system may be expressed as $\alpha_{acc}|00\rangle|\psi_{acc}\rangle + \alpha_{rej}|11\rangle|\psi_{rej}\rangle$, where $\alpha_{acc}, \alpha_{rej} \in [0, 1]$ and $|\psi\rangle = \alpha_{acc}|\psi_{acc}\rangle + \alpha_{rej}|\psi_{rej}\rangle$ (for $|\psi_{acc}\rangle$ and $|\psi_{rej}\rangle$ representing the normalized projections of $|\psi\rangle$ onto accepting and rejecting states). The prover now applies some transformation U to the registers of the system except $\mathbf{B}$, resulting in state $\alpha_{acc}|0\rangle U(|0\rangle|\psi_{acc}\rangle) + \alpha_{rej}|1\rangle U(|1\rangle|\psi_{rej}\rangle)$. After receiving $\mathbf{B}'$ from the prover in step 3, the verifier subtracts $\mathbf{B}$ from $\mathbf{B}'$, yielding the state $\alpha_{acc}|0\rangle|\phi_{acc}\rangle + \alpha_{rej}|1\rangle|\phi_{rej}\rangle$, where $|\phi_{acc}\rangle = U(|0\rangle|\psi_{acc}\rangle)$ and $|\phi_{rej}\rangle$ is equivalent to $U(|1\rangle|\psi_{rej}\rangle)$, but with $\mathbf{B}'$ flipped. Finally, the verifier applies transformation $T_{a(n)}$ to $\mathbf{B}$. The probability of acceptance is thus given by

---

1. Run the original protocol, except do not output accept or reject. Let $\mathbf{R}$ denote the verifier's qubits in the initial protocol after all messages have been exchanged. Assume registers $\mathbf{B}$ and $\mathbf{B}'$ (not used in the original protocol) are initially zero. Increment both $\mathbf{B}$ and $\mathbf{B}'$ if and only if the contents of $\mathbf{R}$ would cause the original verifier to reject.
2. Send $\mathbf{B}'$ and $\mathbf{R}$ to the prover.
3. Receive $\mathbf{B}'$ from the prover, subtract $\mathbf{B}$ from $\mathbf{B}'$, and perform $T_{a(|x|)}$ on $\mathbf{B}$. Observe $\mathbf{B}$: if $\mathbf{B}$ contains 0, then *accept*, otherwise *reject.*

Figure 2: Verifier's protocol for Theorem 2.

$$\left\| \alpha_{acc}\sqrt{a(n)}|\phi_{acc}\rangle + \alpha_{rej}\sqrt{1-a(n)}|\phi_{rej}\rangle \right\|^2. \qquad (1)$$

Assume $x \in L$, so that $\alpha_{acc} = \sqrt{a(n)}$ and $\alpha_{rej} = \sqrt{1-a(n)}$. The prover may choose U so that $U(|0\rangle|\psi_{acc}\rangle) = |0\rangle|\gamma\rangle$ and $U(|1\rangle|\psi_{rej}\rangle) = |1\rangle|\gamma\rangle$ for arbitrary $|\gamma\rangle$, implying that $|\phi_{acc}\rangle = |\phi_{rej}\rangle$. By (1) the probability of acceptance is therefore 1 as required.

Now assume $x \notin L$. By (1), the probability of acceptance is bounded by

$$\begin{aligned} &\left(\alpha_{acc}\sqrt{a(n)} + \alpha_{rej}\sqrt{1-a(n)}\right)^2 \\ &\qquad \leq 1 - \left(a(n) - \alpha_{acc}^2\right)^2 \leq 1 - (a(n) - b(n))^2, \end{aligned}$$

as required. ■

By definition $\mathrm{QIP}(m, a, b) \subseteq \mathrm{QIP}(m, a', b)$ whenever $a' < a$, and thus Theorem 2 implies

$$\mathrm{QIP}(m, a, b) \subseteq \mathrm{QIP}(m + 2, 1, 1 - (a' - b)^2)$$

assuming (i) $b(n) < a'(n) \leq a(n)$ for every n and (ii) $T_{a'(n)}$ can be performed by polynomial-time uniformly generated circuits. It is the case that a function a' can in fact always be chosen that is exponentially close (in a point-wise sense) to a given (polynomial-time computable) function a:

PROPOSITION 3. *Let $f \in 2^{-poly}$, let $a : \mathbb{Z}^+ \to [0,1]$ be polynomial-time computable, and assume $a(n) - f(n) \in [0,1]$ for every n. Then there exists a function $a' : \mathbb{Z}^+ \to [0,1]$ such that (i) $a'(n) \in (a(n) - f(n), a(n)]$ for every n, and (ii) there exists a family $\{Q_{1^n}\}$ of polynomial-time uniformly generated quantum circuits for exactly performing the transformation $T_{a'(n)}$.*

This proposition follows from a more general theorem regarding the accuracy to which any 2-dimensional unitary transformation can be approximated by gates in our basis. (See [23] for details.) As a result, we see that

$$\mathrm{QIP}(m,a,b) \subseteq \mathrm{QIP}(m+2,1,1-poly^{-1})$$

given that $a - b \in poly^{-1}$.

4. PARALLELIZATION OF QUANTUM INTERACTIVE PROOF SYSTEMS

Next, we prove that any one-sided error quantum interactive proof system in which the prover and verifier exchange a polynomial number of messages can be parallelized to one in which the prover and verifier exchange just 3 messages.

THEOREM 4. *Let $m \in poly$ and let $\epsilon : \mathbb{Z}^+ \to [0,1]$ be any function. Then*

$$\mathrm{QIP}(m,1,1-\epsilon) \subseteq \mathrm{QIP}\left(3,1,1-\frac{\epsilon^2}{4m^2}\right).$$

For convenience we restrict our attention to quantum interactive proofs in which m is odd, implying that the prover sends the first message. (A quantum protocol with even m can trivially be simulated by one with odd m in which the verifier rejects if the first message does not consist of all zero-valued qubits.) Since there is nothing to prove in case $m \leq 3$, we will assume $m > 3$. For a given fixed input x, we let k denote $(m+1)/2$, so the prover and verifier alternately apply circuits $P_1, \ldots, P_k$ and $V_1, \ldots, V_k$ on this input. We define $\mathrm{MAP}(V_1, \ldots, V_k)$ (the maximum acceptance probability of $V_1, \ldots, V_k$) as follows:

$$\mathrm{MAP}(V_1,\ldots,V_k) = \max\left\{\|\Pi_{acc} V_k P_k \cdots V_1 P_1 |\psi_{init}\rangle\|^2\right\},$$

where the maximum is over all $P_1, \ldots, P_k \in \mathbf{U}(\mathcal{M} \otimes \mathcal{P})$ and Π_{acc} denotes the projection onto accepting states (i.e., states for which the output qubit is 1). Let Π_{init} denote the projection onto those states for which the verifier's qubits are all in the state $|0\rangle$.

In order to prove Theorem 4 we require the following lemma.

LEMMA 5. *Let $\rho_1, \ldots, \rho_k \in \mathbf{D}(\mathcal{V} \otimes \mathcal{M})$ and $V_1, \ldots, V_k \in \mathbf{U}(\mathcal{V} \otimes \mathcal{M})$ satisfy $\rho_k = (V_k^\dagger \Pi_{acc} V_k)\rho_k(V_k^\dagger \Pi_{acc} V_k)$, $\rho_1 = \Pi_{init}\, \rho_1\, \Pi_{init}$, and $\mathrm{MAP}(V_1, \ldots, V_k) < 1 - \epsilon$. Then*

$$\sum_{j=1}^{k-1} \sqrt{F\left(\mathrm{tr}_{\mathcal{M}}\, V_j \rho_j V_j^\dagger, \mathrm{tr}_{\mathcal{M}}\, \rho_{j+1}\right)} \;\leq\; (k-1) - \frac{\epsilon^2}{8(k-1)}.$$

Proof. Let $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ be such that $\mathrm{tr}_{\mathcal{P}}\, |\psi_j\rangle\langle\psi_j| = \rho_j$, and write

$$F\left(\mathrm{tr}_{\mathcal{M}}\, V_j \rho_j V_j^\dagger, \mathrm{tr}_{\mathcal{M}}\, \rho_{j+1}\right) \;=\; \left(1 - \frac{\eta_j^2}{2}\right)^2$$

for $\eta_1, \ldots, \eta_{k-1} \geq 0$. By Theorem 1 (item 4) there exist vectors $|\xi_j\rangle, |\gamma_j\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ such that $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}\, |\xi_j\rangle\langle\xi_j| = \mathrm{tr}_{\mathcal{M}}\, V_j \rho_j V_j^\dagger$, $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}\, |\gamma_j\rangle\langle\gamma_j| = \mathrm{tr}_{\mathcal{M}}\, \rho_{j+1}$, and $\||\xi_j\rangle - |\gamma_j\rangle\| \leq \eta_j$, for $1 \leq j \leq k-1$. For each j we have $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}\, |\gamma_j\rangle\langle\gamma_j| = \mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}\, |\psi_{j+1}\rangle\langle\psi_{j+1}|$, and thus by Theorem 1 (item 6) there exists $Q_{j+1} \in \mathbf{U}(\mathcal{M}\otimes\mathcal{P})$ such that $Q_{j+1}|\gamma_j\rangle = |\psi_{j+1}\rangle$. Similarly, as $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}\, V_j|\psi_j\rangle\langle\psi_j|V_j^\dagger = \mathrm{tr}_{\mathcal{M}\otimes\mathcal{P}}\, |\xi_j\rangle\langle\xi_j|$, there exists $R_{j+1} \in \mathbf{U}(\mathcal{M}\otimes\mathcal{P})$ such that $R_{j+1}V_j|\psi_j\rangle = |\xi_j\rangle$. Define $P_{j+1} = Q_{j+1}R_{j+1}$ for $1 \leq j \leq k-1$. As $\rho_1 = \Pi_{init}\, \rho_1\, \Pi_{init}$, we may also define P_1 such that $P_1|\psi_{init}\rangle = |\psi_1\rangle$. Now, for $1 \leq j \leq k-1$ we have

$$\|P_{j+1}V_j|\psi_j\rangle - |\psi_{j+1}\rangle\| = \||\xi_j\rangle - |\gamma_j\rangle\| \leq \eta_j,$$

and consequently

$$\begin{aligned} &\|P_k V_{k-1} \cdots P_1|\psi_{init}\rangle - |\psi_k\rangle\| \\ &\quad = \;\; \|P_k V_{k-1} \cdots P_2 V_1|\psi_1\rangle - |\psi_k\rangle\| \;\leq\; \sum_{j=1}^{k-1} \eta_j. \end{aligned}$$

Since $\rho_k = (V_k^\dagger \Pi_{acc} V_k)\rho_k(V_k^\dagger \Pi_{acc} V_k)$, it follows that $\|\Pi_{acc} V_k|\psi_k\rangle\| = 1$, and thus

$$\|\Pi_{acc} V_k P_k \cdots V_1 P_1|\psi_{init}\rangle\| \geq 1 - \sum_{j=1}^{k-1} \eta_j.$$

As $\mathrm{MAP}(V_1, \ldots, V_k) < 1 - \epsilon$, we therefore have $\sum_{j=1}^{k-1} \eta_j \geq 1 - \sqrt{1-\epsilon} \geq \epsilon/2$. The lemma now follows by noting that the maximum of $\sum_{j=1}^{k-1}(1 - \eta_j^2/2)$ subject to the constraint $\sum_{j=1}^{k-1} \eta_j \geq \epsilon/2$ is as stated. ■

Proof of Theorem 4. Fix an input x, and let $V_1, \ldots, V_k \in \mathbf{U}(\mathcal{V}\otimes\mathcal{M})$ describe the verifier's circuits for this input. Also let $P_1, \ldots, P_k \in \mathbf{U}(\mathcal{M}\otimes\mathcal{P})$ be an optimal sequence of unitary transformations for the prover, and let Π_{init} and Π_{acc} be as above.

In Figure 3, we describe the verifier's 3-message protocol. In step 1, the verifier effectively measures $(\mathbf{V}_1, \mathbf{M}_1)$ and

1. Receive registers $\mathbf{V}_1, \ldots, \mathbf{V}_k$ and $\mathbf{M}_1, \ldots, \mathbf{M}_k$ from the prover. Reject if $\mathbf{V}_1$ does not contain all zeroes. Perform V_k on $(\mathbf{V}_k, \mathbf{M}_k)$, reject if $(\mathbf{V}_k, \mathbf{M}_k)$ does not contain an accepting state, and then perform $V_k^\dagger$ on $(\mathbf{V}_k, \mathbf{M}_k)$.
2. Prepare $(\mathbf{B}, \mathbf{B}')$ in state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and choose $r \in \{1, \ldots, k-1\}$ uniformly at random. Apply V_r to $(\mathbf{V}_r, \mathbf{M}_r)$, perform a controlled-swap between $\mathbf{V}_r$ and $\mathbf{V}_{r+1}$ with control bit $\mathbf{B}$, and send $\mathbf{M}_r$, $\mathbf{M}_{r+1}$, $\mathbf{B}'$, and r to the prover.
3. Receive $\mathbf{B}'$ from the prover, perform a controlled-not operation on $(\mathbf{B}, \mathbf{B}')$, and perform a Hadamard transform on $\mathbf{B}$. Accept if $\mathbf{B}$ contains 0, and reject otherwise.

Figure 3: Verifier's parallelization protocol.

$(\mathbf{V}_k, \mathbf{M}_k)$ corresponding to projections Π_{init} and $V_k^\dagger \Pi_{acc} V_k$, respectively. Under the assumption that the verifier does not reject in step 1, the state of the entire system is projected according to Π_{init} and $V_k^\dagger \Pi_{acc} V_k$ appropriately.

First let us assume $\mathrm{MAP}(V_1, \ldots, V_k) = 1$. We now define a prover that causes the (3-message) verifier to accept with certainty. The prover initially prepares registers $(\mathbf{V}_j, \mathbf{M}_j, \mathbf{P}_j)$, $1 \leq j \leq k$, as follows: $(\mathbf{V}_1, \mathbf{M}_1, \mathbf{P}_1)$ is prepared in state $P_1|\psi_{init}\rangle$, and $(\mathbf{V}_{j+1}, \mathbf{M}_{j+1}, \mathbf{P}_{j+1})$ is prepared in state $P_{j+1}V_jP_j \cdots V_1P_1|\psi_{init}\rangle$ for $j \geq 1$. For whichever r the verifier sends in step 2, the prover performs P_{r+1} to $(\mathbf{M}_r, \mathbf{P}_r)$ and then performs a controlled-swap on $(\mathbf{M}_r, \mathbf{P}_r)$ and $(\mathbf{M}_{r+1}, \mathbf{P}_{r+1})$ using control bit $\mathbf{B}'$. The prover then sends $\mathbf{B}'$ back to the verifier. Assuming that $\mathrm{MAP}(V_1, \ldots, V_k) = 1$ and $P_1, \ldots, P_k$ is an optimal sequence of transformations in the m-message case, it is routine to show that the 3-message verifier accepts with certainty.

Now consider the case that $\mathrm{MAP}(V_1, \ldots, V_k) < 1 - \epsilon$. For each j, let $\rho_j \in \mathbf{D}(\mathcal{V} \otimes \mathcal{M})$ denote the state of the registers $(\mathbf{V}_j, \mathbf{M}_j)$ received from the prover in step 1, assuming all other registers are traced out. We claim that the probability that the verifier accepts for each choice of r is at most

$$p_r := \frac{1}{2} + \frac{1}{2}\sqrt{F\left(\mathrm{tr}_{\mathcal{M}} V_r \rho_r V_r^\dagger, \mathrm{tr}_{\mathcal{M}} \rho_{r+1}\right)}.$$

Since r is chosen uniformly, this will imply that the total probability that the verifier accepts is bounded by

$$\sum_{r=1}^{k-1} \frac{p_r}{k-1} \leq 1 - \frac{\epsilon^2}{16(k-1)^2} = 1 - \frac{\epsilon^2}{4(m-1)^2}$$

by Lemma 5. To account for the possibility that we have added 1 to m to handle the case that m was initially even, we obtain the bound given in the statement of the theorem.

It remains to prove that p_r bounds the probability that the verifier accepts for given r. Consider the state of the entire system immediately after the controlled-not in step 3 has been performed. We may denote this state by $(|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle)/\sqrt{2}$ for unit vectors $|\phi_0\rangle, |\phi_1\rangle \in \mathcal{V} \otimes \mathcal{K}$, where the $\mathcal{V}$ component of each vector describes the state of $\mathbf{V}_r$ and the $\mathcal{K}$ component describes all registers of the system besides $\mathbf{B}$ and $\mathbf{V}_r$. Note that by Theorem 1 (item 4) we must have $|\langle\phi_0|\phi_1\rangle|^2 \leq F\left(\mathrm{tr}_{\mathcal{M}} V_r \rho_r V_r^\dagger, \mathrm{tr}_{\mathcal{M}} \rho_{r+1}\right)$, as $\mathrm{tr}_{\mathcal{K}} |\phi_0\rangle\langle\phi_0| = \mathrm{tr}_{\mathcal{M}} V_r \rho_r V_r^\dagger$ and $\mathrm{tr}_{\mathcal{K}} |\phi_1\rangle\langle\phi_1| = \mathrm{tr}_{\mathcal{M}} \rho_{r+1}$. The verifier applies a Hadamard transform to $\mathbf{B}$ and accepts if the resulting bit is 0. The probability of acceptance is thus given by

$$\left\|\frac{1}{2}|0\rangle(|\phi_0\rangle + |\phi_1\rangle)\right\|^2 = \frac{1}{2} + \frac{1}{2}\Re\langle\phi_0|\phi_1\rangle,$$

which is bounded by $\frac{1}{2} + \frac{1}{2}\sqrt{F(\mathrm{tr}_{\mathcal{M}} V_r \rho_r V_r^\dagger, \mathrm{tr}_{\mathcal{M}} \rho_{r+1})}$ as required. ■

5. AMPLIFICATION OF 3-MESSAGE PROTOCOLS

The simplest way to (potentially) reduce the error probability of a quantum interactive proof system is to perform the protocol many times in parallel and to allow the verifier to make its decision to accept or reject based on the outcomes of the individual executions. In case the original protocol has one-sided error, the verifier simply accepts if and only if every one of the parallel executions accepts. For the case of two-sided error, the verifier may choose to accept or reject based on the ratio of acceptance to rejection of the parallel executions.

One might expect that there is the possibility that this method will not work, since a malicious prover might entangle its responses among the parallel executions, perhaps in a way that biases the outcome of a particular execution based on the outcome of another. We prove, however, that in the case of one-sided error 3-message protocols this cannot happen; the prover gains no advantage whatsoever by entangling parallel executions.

Theorem 6. *Let $p \in poly$ and let $b : \mathbb{Z}^+ \rightarrow [0, 1]$ be any function. Then* $\mathrm{QIP}(3, 1, b) \subseteq \mathrm{QIP}(3, 1, b^p)$.

The proof of this theorem is based on the following lemma, which relates the maximum acceptance probability of an interactive proof system to the diamond norm of a mapping based only the specification of the verifier.

Lemma 7. *Let operators $V_1, V_2 \in \mathbf{U}(\mathcal{V} \otimes \mathcal{M})$ and projections Π_{init} and Π_{acc} be as defined previously. Define $W_1, W_2 \in \mathbf{L}(\mathcal{V} \otimes \mathcal{M})$ as $W_1 = V_1\Pi_{init}$ and $W_2 = V_2^\dagger\Pi_{acc}$, and define $T \in \mathbf{T}(\mathcal{V} \otimes \mathcal{M}, \mathcal{M})$ as $T(X) = \mathrm{tr}_{\mathcal{V}} W_1XW_2^\dagger$. Then* $\mathrm{MAP}(V_1, V_2) = \|T\|_\diamond^2$.

Proof. First note that

$$\mathrm{MAP}(V_1, V_2) = \max\left\{\left|\langle\phi|W_2^\dagger UW_1|\psi\rangle\right|^2\right\},$$

where the maximum is over all $|\psi\rangle$, $|\phi\rangle$, and $U \in \mathbf{U}(\mathcal{M} \otimes \mathcal{P})$, where $|\psi\rangle, |\phi\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ are unit vectors.

Now, for $\mathcal{P}$ of sufficiently large dimension, by Theorem 1 (item 2) we have that

$$\|T\|_\diamond = \|T \otimes I_{\mathbf{L}(\mathcal{P})}\|_{\mathrm{tr}} = \max\left\{\|T \otimes I_{\mathbf{L}(\mathcal{P})}(Y)\|_{\mathrm{tr}}\right\},$$

where the maximum is taken over all $Y \in \mathbf{L}(\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P})$ satisfying $\|Y\|_{\mathrm{tr}} = 1$. Any $Y \in \mathbf{L}(\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P})$ satisfying $\|Y\|_{\mathrm{tr}} = 1$ can be written as $\sum_j \alpha_j|\psi_j\rangle\langle\phi_j|$ where $\sum_j |\alpha_j| = 1$ and each $|\psi_j\rangle, |\phi_j\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ is a unit vector. Thus, it must be the case that the maximum of $\|T \otimes I_{\mathbf{L}(\mathcal{P})}(Y)\|_{\mathrm{tr}}$ is obtained on an operator of the form $|\psi\rangle\langle\phi|$ (again for $|\psi\rangle$ and $|\phi\rangle$ unit vectors). We therefore have

$$\begin{aligned}\|T\|_\diamond &= \max\left\{\|T \otimes I_{\mathbf{L}(\mathcal{P})}(|\psi\rangle\langle\phi|)\|_{\mathrm{tr}}\right\} \\ &= \max\left\{\|\,\mathrm{tr}_{\mathcal{V}} W_1|\psi\rangle\langle\phi|W_2^\dagger\|_{\mathrm{tr}}\right\},\end{aligned}$$

with both maximums being taken over all choices for unit vectors $|\psi\rangle, |\phi\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$. By Theorem 1 (item 1) we therefore have

$$\|T\|_\diamond^2 = \max\left\{\left|\mathrm{tr}\left(U\,\mathrm{tr}_{\mathcal{V}} W_1|\psi\rangle\langle\phi|W_2^\dagger\right)\right|\right\}^2$$

for $U \in \mathbf{U}(\mathcal{M} \otimes \mathcal{P})$. Simplifying this equality, we have

$$\begin{aligned}\|T\|_\diamond^2 &= \max\left\{\left|\mathrm{tr}\left(UW_1|\psi\rangle\langle\phi|W_2^\dagger\right)\right|\right\}^2 \\ &= \max\left\{\left|\langle\phi|W_2^\dagger UW_1|\psi\rangle\right|\right\}^2 \\ &= \mathrm{MAP}(V_1, V_2)\end{aligned}$$

as required. ■

Proof of Theorem 6. Let $L \in \mathrm{QIP}(3, 1, b)$ and let V be a verifier witnessing this fact. Fix an input string x and define $T \in \mathbf{T}(\mathcal{V} \otimes \mathcal{M}, \mathcal{M})$ as in Lemma 7. If $x \in L$ we have $\|T\|_\diamond^2 = 1$, while if $x \notin L$ we have $\|T\|_\diamond^2 \leq b$. Now let V' be a verifier that runs p copies of the protocol of V in parallel and accepts if and only if every one of the p copies accepts. The operators corresponding to the actions of V' are described by $V_i' = V_i \otimes \cdots \otimes V_i$ (p times) for $i = 1, 2$, while the projections Π'_{init} and Π'_{acc} corresponding to the initial and accepting conditions of V' are given by $\Pi'_{init} = \Pi_{init} \otimes \cdots \otimes \Pi_{init}$ and $\Pi'_{acc} = \Pi_{acc} \otimes \cdots \otimes \Pi_{acc}$ (p times each). Consequently, defining T' for V' as in Lemma 7 we have $T' = T \otimes \cdots \otimes T$. By Item 3 in Theorem 1 we have $\|T'\|_\diamond = \|T \otimes \cdots \otimes T\|_\diamond = \|T\|_\diamond^p$. Thus, if $x \in L$ then $\mathrm{MAP}(V_1', V_2') = 1$, while if $x \notin L$ then $\mathrm{MAP}(V_1', V_2') \leq b^p$. ■

We note that a simple modification of the proof of this theorem implies that 1-message and 2-message quantum interactive proofs can be amplified in a similar way (although there is a much simpler proof in the 1-message case).

By Theorem 2, Proposition 3, Theorem 4, and Theorem 6, we obtain the following corollary:

Corollary 8. *Let $p \in poly$, $\epsilon \in poly^{-1}$, and assume $a, b : \mathbb{Z}^+ \to [0,1]$ satisfy $a(n) - b(n) \geq \epsilon(n)$ for every n. Then* $\mathrm{QIP}(poly, a, b) \subseteq \mathrm{QIP}(3, 1, 2^{-p})$.

6. EXPONENTIAL-TIME SIMULATION OF QUANTUM INTERACTIVE PROOFS

Finally, we prove the following upper bound on the power of quantum interactive proof systems: any language having a quantum interactive proof system can be decided in deterministic exponential time.

Theorem 9. $\mathrm{QIP}(3, 1, 1/2) \subseteq \mathrm{EXP}$.

Here, EXP denotes the class of languages L decidable by a deterministic Turing machine M in time bounded by 2^p for some $p \in poly$.

The method used to prove this fact is based on semidefinite programming. For information on semidefinite programming, we refer the reader to [2; 29] and the references therein.

The following problem is called the *standard semidefinite programming* (SDP) problem:

Input: $A_1, \ldots, A_k, C \in \mathbb{C}^{N \times N}$ and $b_1, \ldots, b_k \in \mathbb{C}$.

Problem: Minimize $\Re(\operatorname{tr} C^\dagger X)$ for $X \in \mathbb{C}^{N \times N}$ positive semidefinite and satisfying $\operatorname{tr} A_j^\dagger X = b_j$ for $j = 1, \ldots, k$.

It should be noted that it is generally required that the underlying field be the real numbers rather than the complex numbers for this problem. It is a fairly straightforward exercise, however, to show that the two problems are equivalent (up to a polynomial factor increase in the size of the problem). Given an accuracy bound ϵ, the SDP problem can be solved in (deterministic) time polynomial in the input size and $|\log \epsilon|$ (given that a polynomial upper-bound on the length of the solution is known) [19] (see also [2]).

Proof of Theorem 9 First we consider an optimization problem that reduces to the SDP problem. We then show that membership in a given language $L \in \mathrm{QIP}(3, 1, 1/2)$ can be decided in EXP by solving an exponential-size instance of our optimization problem.

Assume we are given positive integer parameters N_1, N_2, and M, as well as $M \times N_1$ complex matrices $B_{1,1}, \ldots, B_{1,k_1}$, and $M \times N_2$ complex matrices $B_{2,1}, \ldots, B_{2,k_2}$. Define mappings $\widetilde{T}_1, \widetilde{T}_2 : \mathbb{C}^{N_i \times N_i} \to \mathbb{C}^{M \times M}$ as follows:

$$\widetilde{T}_i(Y) = \sum_{j=1}^{k_i} B_{i,j} Y B_{i,j}^\dagger,$$

and suppose we are promised that one of the following two possibilities holds for given $\epsilon > 0$:

1. There exist positive semidefinite, trace 1 matrices Y_1 and Y_2 such that $\widetilde{T}_1(Y_1) = \widetilde{T}_2(Y_2)$.
2. For all positive semidefinite, trace 1 matrices Y_1 and Y_2, $\|\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2)\| > \epsilon$.

We wish to determine which of these two cases holds. This problem reduces to the SDP problem, as we now show.

Let $N' = N_1 + N_2 + 2M + 1$ and consider the set of all $N' \times N'$ matrices having the form

$$\begin{aligned} X = \operatorname{diag}(t, Y_1, Y_2, tI - (\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2)), \\ tI + (\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2))) \quad (2) \end{aligned}$$

(where t is a scalar) and subject to the constraints that $\operatorname{tr} Y_1 = \operatorname{tr} Y_2 = 1$ and X is positive semidefinite. For any such X we must have that t is a nonnegative real number, that Y_1 and Y_2 are positive semidefinite, and furthermore that $t \geq \|\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2)\|$. Thus, there exists an X satisfying these constraints for which $t = 0$ if and only if item 1 above is satisfied; otherwise $t > \epsilon$ for all such X, in which item 2 holds.

We will define a collection of matrices $A_1, \ldots, A_l$ and numbers $b_1, \ldots, b_l$ that, in the sense of the SDP problem, impose the constraints on a given matrix X that it be of the form (2) with $\operatorname{tr}(Y_1) = \operatorname{tr}(Y_2) = 1$. First, for each $i, j \in \{1, \ldots, N'\}$, define $E_{i,j}$ to be the $N' \times N'$ matrix having a 1 as its i, j entry and with all other entries 0. Note that $\operatorname{tr} E_{i,j}^\dagger X = X[i,j]$ for any $N' \times N'$ matrix X. Let us also define $K_1 = \{1\}$, $K_2 = \{2, \ldots, N_1 + 1\}$, $K_3 = \{N_1 + 2, \ldots, N_1 + N_2 + 1\}$, $K_4 = \{N_1 + N_2 + 2, \ldots, N_1 + N_2 + M + 1\}$, and $K_5 = \{N_1 + N_2 + M + 2, \ldots, N_1 + N_2 + 2M + 1\}$. Next, we do the following:

- For every pair i, j such that $i \in K_{m_1}$ and $j \in K_{m_2}$ for $m_1 \neq m_2$, define $U_{i,j} = E_{i,j}$ and $u_{i,j} = 0$.
- Define $V_1 = \sum_{i \in K_2} E_{i,i}$, $V_2 = \sum_{i \in K_3} E_{i,i}$, and set $v_1 = v_2 = 1$.
- For each $i, j \in \{1, \ldots, M\}$ define

  $$\begin{aligned} F_{i,j} = \sum_{i',j'=1}^{N} \Bigg[\left(\sum_{t=1}^{k_1} B_{1,t}^\dagger[i', i] B_{1,t}[j, j'] \right) E_{i'+1,j'+1} \\ - \left(\sum_{t=1}^{k_2} B_{2,t}^\dagger[i', i] B_{2,t}[j, j'] \right) E_{i'+N_1+1,j'+N_1+1} \Bigg], \end{aligned}$$

  define $G_{i,j}$ and $H_{i,j}$ as follows:

  $$\begin{aligned} G_{i,j} &= \delta_{i,j} E_{1,1} - F_{i,j} - E_{i+N_1+N_2+1,j+N_1+N_2+1}, \\ H_{i,j} &= \delta_{i,j} E_{1,1} + F_{i,j} - E_{i+N_1+N_2+M+1,j+N_1+N_2+M+1}, \end{aligned}$$

  and set $g_{i,j} = h_{i,j} = 0$.

Relabel the matrices $\{U_{i,j}\} \cup \{V_1, V_2\} \cup \{G_{i,j}\} \cup \{H_{i,j}\}$ and the numbers $\{u_{i,j}\} \cup \{v_1, v_2\} \cup \{g_{i,j}\} \cup \{h_{i,j}\}$ as $A_1, \ldots, A_l$

and $b_1, \ldots, b_l$ for appropriately chosen l, and consider the collection of all $N' \times N'$ matrices X for which we have $\operatorname{tr} A_1^\dagger X = b_1, \ \ldots, \ \operatorname{tr} A_l^\dagger X = b_l$. It may be verified that this is precisely the collection of matrices of the form (2) such that $\operatorname{tr}(Y_1) = \operatorname{tr}(Y_2) = 1$; the first item above imposes the constraint that X be of the form $\operatorname{diag}(t, Y_1, Y_2, Z_1, Z_2)$ for Y_1 an $N_1 \times N_1$ matrix, Y_2 an $N_2 \times N_2$ matrix, and Z_1 and Z_2 $M \times M$ matrices, the second item imposes the constraint $\operatorname{tr} Y_1 = \operatorname{tr} Y_2 = 1$, and the third item imposes the constraint that $Z_1 = tI - (\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2))$ and $Z_2 = tI + (\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2))$. By defining $C = E_{1,1}$, we see that the minimum of $\Re(\operatorname{tr} C^\dagger X)$ subject to the above constraints is precisely the minimum value of $\|\widetilde{T}_1(Y_1) - \widetilde{T}_2(Y_2)\|$ over all matrices Y_1, Y_2 representing density operators, and thus determines which of possibility 1 or 2 above holds.

Now we show that membership in a given language $L \in \mathrm{QIP}(3, 1, 1/2)$ can be reduced to an exponential-size instance of the optimization problem discussed above. Assume V is a 3-message verifier for L having one-sided error bounded by 1/2. For a given input x, we therefore wish to determine whether $\mathrm{MAP}(V_1, V_2) = 1$ or $\mathrm{MAP}(V_1, V_2) < 1/2$ holds. Recall the definitions of the spaces $\mathcal{V}$, $\mathcal{M}$, and $\mathcal{P}$ and the projections Π_{init} and Π_{acc} as defined in Section 2.3. Define $\mathcal{H}_1 = \mathcal{M}$ and define $\mathcal{H}_2$ to be $\mathcal{V} \otimes \mathcal{M}$ with the output qubit removed (i.e., $\mathcal{H}_2 = \ell_2(\Sigma^{q_\mathcal{V}-1} \times \Sigma^{q_\mathcal{M}})$). Define $T_i : \mathbf{D}(\mathcal{H}_i) \rightarrow \mathbf{D}(\mathcal{V})$ for $i = 1, 2$ as follows:

$$\begin{aligned} T_1 : \rho &\mapsto \operatorname{tr}_\mathcal{M} \left(V_1 \left(|0^{q_\mathcal{V}}\rangle\langle 0^{q_\mathcal{V}}| \otimes \rho \right) V_1^\dagger \right), \\ T_2 : \rho &\mapsto \operatorname{tr}_\mathcal{M} \left(V_2^\dagger \left(|1\rangle\langle 1| \otimes \rho \right) V_2 \right). \end{aligned}$$

We claim that if $\mathrm{MAP}(V_1, V_2) = 1$ then there exists $\rho_1 \in \mathbf{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathbf{D}(\mathcal{H}_2)$ such that $T_1(\rho_1) = T_2(\rho_2)$, and if $\mathrm{MAP}(V_1, V_2) < 1/2$ then

$$\|T_1(\rho_1) - T_2(\rho_2)\| \geq 2^{-q_\mathcal{V}-4}$$

for any $\rho_1 \in \mathbf{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathbf{D}(\mathcal{H}_2)$. If $\mathrm{MAP}(V_1, V_2) = 1$, this is straightforward. Suppose on the other hand that $\mathrm{MAP}(V_1, V_2) < 1/2$. For any $\rho_1 \in \mathbf{D}(\mathcal{H}_1)$ and $\rho_2 \in \mathbf{D}(\mathcal{H}_2)$ we may conclude

$$\sqrt{F(T_1(\rho_1), T_2(\rho_2))} \leq \frac{31}{32}$$

by Lemma 5. Consequently

$$\|T_1(\rho_1) - T_2(\rho_2)\| \geq 2^{-q_\mathcal{V}} \|T_1(\rho_1) - T_2(\rho_2)\|_{\mathrm{tr}} \geq 2^{-q_\mathcal{V}-4}$$

by Theorem 1 (item 5).

Now let $M = 2^{q_\mathcal{V}}$, $N_1 = 2^{q_\mathcal{M}}$, and $N_2 = 2^{q_\mathcal{V}+q_\mathcal{M}-1}$. It remains to be shown that a collection of $M \times N_1$ matrices $B_{1,1}, \ldots, B_{1,k_1}$ (describing an approximation $\widetilde{T}_1$ to T_1) and $M \times N_2$ matrices $B_{2,1}, \ldots, B_{2,k_2}$ (describing an approximation $\widetilde{T}_2$ to T_2) may be computed in time exponential in $|x|$ to a sufficient degree of accuracy such that the solution to the corresponding instance of SDP described above reveals whether or not $x \in L$. But under the assumption that V_1 and V_2 are polynomial-time uniformly generated circuits as discussed in Section 2, it is routine to show that in exponential time one may compute matrices $B_{i,1}, \ldots, B_{i,k_i}$ for which the inequalities $\|T_i(\rho_i) - \widetilde{T}_i(\rho_i)\|_{\mathrm{tr}} < 2^{-p(|x|)}$ $(i = 1, 2)$ hold for any fixed polynomial p and all $\rho_i \in \mathbf{D}(\mathcal{H}_i)$. (Note that this bound in precision is sufficient for our purposes, but is indeed very coarse—the error can in fact be made smaller than 2^{-2^p}, as an exponential number of bits of precision may be computed for each entry of each $B_{i,j}$ in exponential time.) Thus, taking $p = q_\mathcal{V} + 7$ for instance, we have that $x \in L$ implies $\|\widetilde{T}_1(\rho_1) - \widetilde{T}_2(\rho_2)\| \leq 2^{-(q_\mathcal{V}+6)}$ for some ρ_1, ρ_2, while $x \notin L$ implies $\|\widetilde{T}_1(\rho_1) - \widetilde{T}_2(\rho_2)\| \geq 2^{-(q_\mathcal{V}+5)}$ for every ρ_1, ρ_2. As there exist polynomial time algorithms for the SDP problem for which the solution is accurate to a polynomial number of bits of precision in the instance size, it follows that in time exponential in $|x|^{O(1)}$ we may determine whether or not $x \in L$, which completes the proof. ■

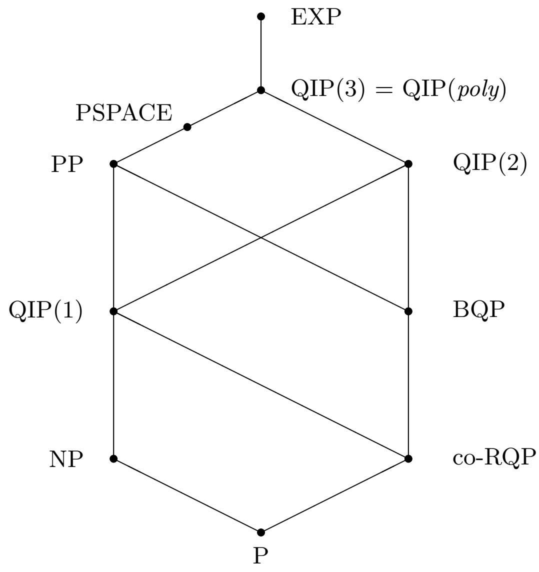

Figure 4: Relationships among quantum interactive proof system classes and some other complexity classes.

7. CONCLUSION

Figure 4 summarizes relationships among some of the classes considered in this paper. Here we let $\mathrm{QIP}(m)$ denote the one-sided error class $\mathrm{QIP}(m, 1, 1/2)$. A definition of the class BQP may be found in [7], while RQP may be defined as a one-sided error version of BQP.

A number of open questions regarding quantum interactive proof systems remain. Of particular interest is the following question: can QIP(1), QIP(2), and QIP(3) be characterized by classical complexity classes? More generally, what other relations hold among quantum interactive proof systems and classical models of computation? We know very little about QIP(2); how does this class compare to PP or to PSPACE? Finally, one may consider many variants on quantum interactive proof systems, such as quantum variants of PCPs and multiprover proof systems. How do these models compare to their classical counterparts?

Acknowledgments

Our research was supported in part by DARPA through Caltech's Quantum Information and Computation (QUIC) project administered by the Army Research Office under Grant No. DAAH04-96-1-0386, and in part by Canada's NSERC. We thank Ashwin Nayak for constructive comments on an earlier version of this paper.

REFERENCES

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[2] F. Alizadeh. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization*, 5(1):13–51, 1995.

[3] L. Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[4] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[5] A. Barenco. A universal two-bit gate for quantum computation. *Proceedings of the Royal Society of London*, 449:679–683, 1995.

[6] A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52:3457–3467, 1995.

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

[8] A. Berthiaume. Quantum computation. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 23–50. Springer, 1997.

[9] J. Cai, A. Condon, and R. Lipton. On bounded round multi-prover interactive proof systems. In *Proceedings of the Fifth Annual Conference on Structure in Complexity Theory*, pages 45–54, 1990.

[10] D. Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London*, A400:97–117, 1985.

[11] D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London*, A425:73–90, 1989.

[12] D. DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 50:1015–1022, 1995.

[13] U. Feige. On the success probability of two provers in one-round proof systems. In *Proceedings of the Sixth Annual Conference on Structure in Complexity Theory*, pages 116–123, 1991.

[14] U. Feige and L. Lovász. Two-prover one-round proof systems: their power and their problems. In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, pages 733–744, 1992.

[15] C. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[16] O. Goldreich. A taxonomy of proof systems. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 109–134. Springer-Verlag, 1997.

[17] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989. Preliminary version appeared in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[18] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. JAI Press, 1989.

[19] M. Grötschel, L. Lovász, and A. Schrijver. The ellipsoid method and its consequences in combinatorial optimization. *Combinatorica*, 1, 1981.

[20] R. Horn and C. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[21] L. Hughston, R. Jozsa, and W. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14–18, 1993.

[22] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[23] A. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[24] D. Lapidot and A. Shamir. Fully parallelized multi prover protocols for NEXP-time. In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 13–18, 1991.

[25] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[26] A. Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

[27] P. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996.

[28] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[29] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[30] J. Watrous. PSPACE has constant-round quantum interactive proof systems. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 112–119, 1999.

[31] A. Yao. Quantum circuit complexity. In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, pages 352–361, 1993.