

Tel Aviv University  
Raymond and Beverly Sackler  
Faculty of Exact Sciences  
School of Computer Sciences

# Quantum Two Provers Interactive Proof Systems

by

**Alex Rapaport**

The research work has been conducted  
under the supervision of  
**Dr. Amnon Ta-Shma**

Submitted as partial fulfillment of the requirements  
towards the M.Sc. degree

April 2007

## Abstract

In this thesis we analyze quantum two prover one round interactive proof systems, in which noninteracting provers can share unlimited entanglement. The maximum acceptance probability is characterized as a superoperator norm. We get some partial results and in particular we analyze the "rank one" case. For solving it we give a bound on the trace norm of a product of matrices which, to the best of our knowledge, is new.

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
<b>2</b>	<b>Preliminaries</b>	<b>6</b>
2.1	Basic Notation . . . . .	6
2.2	Quantum Computation . . . . .	7
<b>3</b>	<b>Quantum Interactive Proofs</b>	<b>8</b>
3.1	Classical Interactive Proof Systems . . . . .	8
3.2	Quantum Interactive Proof Systems . . . . .	9
3.3	An Example of a Nonlocal Strategy . . . . .	11
<b>4</b>	<b>QIP(3) and the Diamond Norm</b>	<b>13</b>
4.1	Diamond norm . . . . .	13
4.2	QIP(3) Characterization . . . . .	14
<b>5</b>	<b>QMIP*(2, 1) and the Product Norm</b>	<b>14</b>
5.1	The Product Norm . . . . .	14
5.2	QMIP*(2, 1) . . . . .	16
5.3	Acceptance Probability for a Given Verifier . . . . .	16
<b>6</b>	<b>Trace Norm of a Product and Product Norm of Rank 1 Matrices</b>	<b>18</b>
6.1	A Bound on the Trace Norm of a Product . . . . .	18
6.2	Product Norm of Rank 1 Matrices . . . . .	19
6.3	Failed Attempts to Characterize the Product Norm . . . . .	20
<b>7</b>	<b>Directions for Further Research</b>	<b>20</b>
7.1	Superoperator Product Norm of the Tensor . . . . .	22
7.2	Additional Open Questions . . . . .	23

# 1 Introduction

Quantum computation is one of the few physical processes that seem to violate the efficient Church-Turing thesis, which states that any reasonable model of computation can be *efficiently* simulated by a probabilistic Turing machine. The quantum model is based on the laws of quantum mechanics and as such gives a more fundamental and natural representation of a computational process.

Although a full scale quantum computer is yet to be built, experimental quantum computations on a small number of bits give hope for a future practical use of the model.

Since the definition of quantum computation, many results suggest that it has considerably more power than the classical. Most notably, in [Sho97] Shor presents a polynomial time quantum algorithm for factorization. There is no similar result in the classical world.

An interactive proof in the context of the classical world is an interaction between an efficient verifier and an all powerful prover. One prover can prove hard theorems (in PSPACE) to an efficient verifier [Sha92]. Two or more powerful provers that cannot interact between themselves can prove the whole of NEXP [BFL91].

In the quantum world the interaction is complicated by the possibility of entanglement. Even in the one prover case the communication between the two parties may create a situation in which their private qubits are entangled. This creates a possibility of non-local interference that affects soundness, completeness and the number of communication messages needed for the proof.

Kitaev and Watrous [KW00] studied the power of interaction between an efficient quantum verifier and a single prover. They prove that such a proof system is at least as powerful as a classical one prover proof system but not as powerful as classical two provers ( $\text{PSPACE} \subseteq \text{QIP} \subseteq \text{EXP}$ ). Moreover they show that in the quantum case 3 communication messages is enough ( $\text{QIP} = \text{QIP}(3)$ ). They also show how to achieve perfect completeness and parallel amplification for the model.

The quantum multiprover case is more complicated. As in the classical case the provers cannot interact between themselves. There are three models concerning the initial state of the provers private qubits. In one model they are not allowed to share any prior entanglement at all, in the second they are allowed to share a limited entangled qubits and in the third they can share unlimited entanglement. Kobayashi and Matsumoto [KM03] prove that without entanglement quantum multiprover proofs are as powerful as classical.

They also prove that if we limit prior entanglement to be polynomial in the input size the power of the proof can only decrease.

In this paper we concentrate on the case of two quantum provers with unlimited prior entanglement and one round of communication. The power of such proofs is not known. On the one hand more entanglement gives the provers power to prove more languages to the verifier, but on the other hand it gives them more power to cheat the verifier. So it may be more or less or something else in relation with NEXP. The only prior result we are aware is that of Kempe and Vidick [KV06] that prove that such provers can prove NP to a verifier whose space is limited to be logarithmic in the input size with perfect completeness and some non-negligible soundness.

The problem we are facing touches the basic question of what entanglement can achieve, and how to quantify it. There are many demonstrations of the power of entanglement (e.g., teleportation [BBC<sup>+</sup>93] and superdense coding [BW92]). There is also a natural measure for measuring the amount of entanglement in pure states [PR97]. Yet, there is no good measure for the amount of entanglement in mixed states.

Another demonstration of the power of entanglement are nonlocal games. In those games Alice and Bob play as provers against a fixed verifier. Their goal is to make him accept. The value of the game is the probability a verifier accepts when Alice and Bob play optimally. Alice and Bob cannot interact during the game but in the quantum model they may share prior entanglement. The CHSH and the Magic Square games are two examples presented in [CHTW04] and [Ara02] for games in which quantum provers outperform the classical provers and violate Bell inequalities for classical correlation between noninteracting parties. In the case of the Magic Square game there is even a perfect quantum strategy that achieves game value 1. The problem we work on is a far reaching generalization of quantum nonlocal games.

It is fair to say that entanglement is far from being understood. In particular, we don't even understand whether infinite entanglement gives additional power over limited entanglement, and this is the core of the problem we try to deal with in this work.

Our approach is to generalize the direction Watrous and Kitaev [KW00] took with the quantum single prover case. They gave an algebraic characterization for the maximum acceptance probability of a fixed verifier in terms of the diamond superoperator norm. Then they used a nice algebraic property of the diamond norm, proved previously by Kitaev [KVS02], to get strong results about quantum single prover proofs.

We manage to get an algebraic characterization of one-round, two-prover

games. We define a "product superoperator norm" and use it to characterize the maximum acceptance probability of a fixed verifier in the quantum two prover, one round case. However, we are unable to analyze it algebraically. We get some partial results and in particular we analyze the "rank one" case. Even this case is nontrivial, and for solving it we give a bound on the trace norm of a product of matrices which to the best of our knowledge is new. We also present some hypotheses about our characterization and give their implications on the power of the proof system.

## 2 Preliminaries

### 2.1 Basic Notation

For a Hilbert space  $\mathcal{H}$  with dimension  $\dim(\mathcal{H})$  we denote by  $L(\mathcal{H})$  the set of all linear operators over  $\mathcal{H}$  and by  $U(\mathcal{H})$  the set of all unitary operators over  $\mathcal{H}$ .  $I_{\mathcal{H}}$  denotes the identity operator over  $\mathcal{H}$ .

We use the Dirac notation (standard in quantum computation) to represent vectors in a Hilbert space. For  $u, v \in \mathcal{H}$  denote  $|u\rangle = u$ ,  $\langle v| = v^\dagger$ ,  $|u, v\rangle = u \otimes v$  and  $\langle u|v\rangle$  their inner product. A vector  $v \in \mathcal{H}_1 \otimes \mathcal{H}_2$  is a *product vector* if  $|v\rangle = |v_1, v_2\rangle$  for some  $v_1 \in \mathcal{H}_1$ ,  $v_2 \in \mathcal{H}_2$ . Any vector that can not be represented in such a way is an *entangled vector*.

A *superoperator*  $T : L(\mathcal{H}_1) \rightarrow L(\mathcal{H}_2)$  is a linear mapping from  $L(\mathcal{H}_1)$  to  $L(\mathcal{H}_2)$ .

**Definition 1.** *The trace out operator is a superoperator from  $L(\mathcal{H}_1 \otimes \mathcal{H}_2)$  to  $L(\mathcal{H}_1)$  defined by*

$$\text{Tr}_{\mathcal{H}_2}(A \otimes B) = \text{Tr}(B) \cdot A$$

for  $A \in L(\mathcal{H}_1)$  and  $B \in L(\mathcal{H}_2)$  and extended linearly to all of  $L(\mathcal{H}_1 \otimes \mathcal{H}_2)$ .

It can be checked that for  $X \in L(\mathcal{H}_1 \otimes \mathcal{H}_2)$ ,  $\text{Tr}_{\mathcal{H}_2}(X)$  is independent of the representation  $X = \sum_i A_i \otimes B_i$ . Also it is easy to check that

$$\text{Tr}(\text{Tr}_{\mathcal{H}_2}(X)) = \text{Tr}(X) \tag{1}$$

and that

$$\text{Tr}_{\mathcal{H}_2}((C \otimes I)X) = C \text{Tr}_{\mathcal{H}_2}(X) \tag{2}$$

for any  $C \in L(\mathcal{H}_1)$ .

## 2.2 Quantum Computation

A *pure quantum state* over  $q$  qubits is a unit vector  $|\psi\rangle \in \mathcal{H} = \mathbb{C}^{2^q}$ . A *mixed quantum state* is a probabilistic distribution over pure states  $\{(p_i, |\psi_i\rangle)\}$  with  $p_i \geq 0$  and  $\sum_i p_i = 1$ . A convenient way to represent a mixed state is by a density matrix  $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ . This representation is not unique, but it can be shown that two mixed states with the same density matrix cannot be distinguished by any quantum computational process.

A quantum computation evolves by either applying a unitary operator or a measurement. A unitary operator  $U$  transforms the pure state  $|\psi\rangle$  to the pure state  $|U\psi\rangle$  and the mixed state  $\rho$  to the mixed state  $U\rho U^\dagger$ . A general *quantum measurement* (POVM) is defined by a set  $\{M_i\} \subseteq L(\mathcal{H})$  such that  $\sum_i M_i^\dagger M_i = I$  and when it is applied on the state  $|\psi\rangle$  we collapse to the state  $\frac{|M_i\psi\rangle}{|M_i\psi|}$  with probability  $p_i = |M_i\psi|^2$ . On a mixed state  $\rho$  the measurement is the transformation  $\rho \rightarrow \sum_i M_i \rho M_i^\dagger$ . Let us notice that a unitary transformation  $U$  is also a measurement since  $U^\dagger U = I$ . For a density matrix  $\rho \in L(\mathcal{H}_1 \otimes \mathcal{H}_2)$ , if we want to ignore the  $\mathcal{H}_2$  register we look at the reduced density matrix  $\text{Tr}_{\mathcal{H}_2}(\rho)$ . The effect is similar to measuring  $\mathcal{H}_2$  in the (standard) basis.

A *quantum circuit* is composed of local gates from the universal basis  $\{CNOT, H, T\}$  and measurements in the standard basis. The complexity of a quantum circuit is defined by the number of gates that compose it. Any unitary transformation on  $q$  qubits can be  $\varepsilon$  approximated by a quantum circuit that uses  $\tilde{O}(4^q \text{poly}(\frac{1}{\varepsilon}))$  gates. A collection of quantum circuits  $\{C_n\}_{n \in \mathbb{N}}$  is *t(n) time uniform* if there exists a deterministic Turing machine that given  $n$  outputs  $C_n$  in at most  $t(n)$  steps. The complexity class *BQP* consists of all the languages that can be decided with good probability by a polynomial time, uniform quantum circuit.

Two useful principles are the locality principle and the safe storage principle. The *locality principle* states that for any quantum state over  $\mathcal{H}_1 \otimes \mathcal{H}_2$ , a local operation on  $\mathcal{H}_2$  can not change the statistics of a measurement on  $\mathcal{H}_1$ . In symbols, for any measurement  $\{M_i\}$  on  $\mathcal{H}_2$  defining the superoperator  $T(\sigma) = \sum_i M_i \sigma M_i^\dagger$  it holds that the reduced density matrix on  $\mathcal{H}_1$  stays the same, i.e.,  $\text{Tr}_{\mathcal{H}_2}((I \otimes T)(\rho)) = \text{Tr}_{\mathcal{H}_2}(\rho)$ . Thus  $\mathcal{H}_2$  can not affect  $\mathcal{H}_1$  without interaction.

The *safe storage principle* allows us to postpone all the measurements to the end of the circuit with a polynomial increase in the number of used qubits. It makes circuits easier to analyze. This is done as follows. Any measurement  $\{M_i\}$  on  $|\psi\rangle \in \mathcal{H}_1$  can be accomplished by adding an ancillary register  $\mathcal{H}_2$ , applying the unitary transformation  $|\psi, 0\rangle \rightarrow \sum_i |M_i\psi, i\rangle$ , and

measuring  $\mathcal{H}_2$  in the standard basis. By the locality principle we can ignore the  $\mathcal{H}_2$  register instead of measuring it.

### 3 Quantum Interactive Proofs

In this section we look at the notion of a proof in the classical and quantum worlds and review single and multiprover proof systems.

#### 3.1 Classical Interactive Proof Systems

An interactive proof system is a protocol that determines the rules of interaction between a verifier and a prover. At the end of the protocol the verifier decides whether to accept or reject. Usually the verifier is a probabilistic polynomial time Turing machine and the prover has unbounded computational power.

An interactive proof system proves a language  $L$  to a verifier  $V$  with completeness parameter  $c$  and soundness parameter  $s$  if:

1. If  $x \in L$  there exist a prover that convinces  $V$  with probability at least  $c$ .
2. If  $x \notin L$  then no prover can convince  $V$  with probability greater than  $s$ .

IP is the class of languages that can be proved to a probabilistic polynomial time verifier, with a polynomial number of communication rounds, when  $c = \frac{2}{3}$  and  $s = \frac{1}{3}$ .  $IP(k)$  is the same as the above except that the number of communication rounds is limited by  $k$ . Shamir proved in [Sha92] that  $IP = PSPACE$ . In MA there is only one communication message from the prover to a probabilistic polynomial time verifier.  $AM(k)$  is defined as  $IP(k)$  with an additional condition that the coins are public. In this model the prover knows what are the random bits the verifier uses. In [GS86] it is proven that  $IP(k) \subseteq AM(k + 2)$  and in [BM88] that for any constant  $k$ ,  $AM(k) = AM(1)$ . It follows from this that private coins have no advantage over public coins.

$MIP(k, r)$  is a generalization of IP with  $k$  isolated provers and  $r$  communication rounds. The provers do not exchange information during the protocol, but they can agree on a strategy in advance. It is proved in [BFL91] that  $MIP(poly, poly) = MIP(2, 1) = NEXP$ .

Another version of MIP allows the provers to share a common random string. This does not change the power of the class. To see that notice that

in the case of shared randomness, a random strategy is a distribution over deterministic strategies, and the provers can only improve the acceptance probability by using the best deterministic strategy.

All the classical interactive proof models mentioned above have the following parallel amplification property. Let  $V$  be a verifier for a language  $L$ . Consider the verifier  $V^{poly}$  that applies the verification procedure of  $V$  a polynomial number of times in parallel. For every question  $V$  sends to the prover,  $V^{poly}$  sends a polynomial number of independently prepared questions and receives a polynomial number of answers. At the end of the protocol  $V^{poly}$  has a polynomial number of results, based on which he accepts or rejects. For classical interactive proof systems parallel amplification reduces the error exponentially fast (see [Gol99] for the easy single prover case and [Raz98] for the complicated multiprover case).

### 3.2 Quantum Interactive Proof Systems

In quantum interactive proof systems the verifier and the provers are quantum players. The protocol lives in  $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k \otimes \mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$  where  $\mathcal{V}$  is the verifier private register,  $\mathcal{M}_i$  is the message register between the verifier and the  $i$ 'th prover and  $\mathcal{P}_i$  is the  $i$ 'th prover private register.  $\mathcal{V}$  and  $\mathcal{M}_i$  are of size polynomial in the input length. In every round of the proof the verifier applies a unitary transformation on  $\mathcal{V} \otimes \mathcal{M}_1 \otimes \cdots \otimes \mathcal{M}_k$  after which the  $\mathcal{M}_i$  register is sent to the  $i$ 'th prover who applies a unitary transformation on  $\mathcal{M}_i \otimes \mathcal{P}_i$  and sends  $\mathcal{M}_i$  back to the verifier. Because of the safe storage and the locality principle it is convenient to assume without loss of generality that there is only one measurement done by the verifier at the end, based on which he accepts or rejects.

QIP( $m$ ) (Quantum IP) is the class of languages that can be proved to a quantum verifier with  $c = \frac{2}{3}$  and  $s = \frac{1}{3}$  by a single quantum prover with at most  $m$  messages passed between the prover and the verifier. Note that in the quantum model we usually count the actual number of passed messages in each direction and not the number of rounds, as is customary in the classical model.

Kitaev and Watrous [KW00] proved that  $\text{PSPACE} \subseteq \text{QIP} = \text{QIP}(3) \subseteq \text{EXP}$ . There is no similar result in classical IP. They also showed that any language in QIP(3) has a proof with perfect completeness. Also QIP(3) has perfect parallel amplification.

QMA is the quantum analogue of MA where the proof is a quantum state  $|\psi\rangle$  and the verifier runs in BQP. QMA has a parallel amplification scheme. Furthermore, Marriott and Watrous [MW05] show an amplification

scheme (that is not parallel) that *does not increase the proof size*. They also define the class QMAM in which the verifier is allowed to send only uniformly random classical questions to the prover with three messages allowed. They prove that  $\text{QMAM} = \text{QIP} = \text{QIP}(3)$ .

We now turn to *multiprover proof systems*. An important parameter of multiprover quantum interactive proof systems is the maximal amount of entangled qubits the provers are allowed to share (if at all) in the initial state of  $\mathcal{P}_1 \otimes \cdots \otimes \mathcal{P}_k$ . We say that the provers have  $q(|x|)$ -prior-entanglement if all the provers hold at most  $q(|x|)$  entangled qubits in the initial state.

**Definition 3.1.** Fix functions  $k(|x|), m(|x|), q(|x|) \geq 0$ .  $\text{QMIP}(k, m, q)$  is the class of languages  $L$  for which there is an interactive proof system with

- $k$  quantum provers.
- $m$  communication rounds.
- The initial state  $|\psi\rangle$ , between the provers is  $q(|x|)$ -prior-entangled.

such that

1. If  $x \in L$  then there exist quantum provers  $P_1, \dots, P_k$  and  $|\psi\rangle$  for which  $V_x$  accepts with probability at least  $\frac{2}{3}$ .
2. If  $x \notin L$  then for all quantum provers  $P_1, \dots, P_k$  and  $|\psi\rangle$ ,  $V_x$  accepts with probability at most  $\frac{1}{3}$ .

Note that we define  $m$  as the number of communication rounds, and not as the number of communication messages. Since we study only the case of one round two messages, the classical convention is more appropriate in this case.

Denote

$$\begin{aligned} \text{QMIP}(k, m) &= \text{QMIP}(k, m, 0) \\ \text{QMIP}^{\text{poly}}(k, m) &= \text{QMIP}(k, m, \text{poly}) \\ \text{QMIP}^*(k, m) &= \text{QMIP}(k, m, \infty) \end{aligned}$$

Kobayashi and Matsumoto prove in [KM03] that

$$\text{QMIP}(\text{poly}, \text{poly}) = \text{MIP}(\text{poly}, \text{poly}) = \text{NEXP}$$

Also, they proved that if the provers have  $\text{poly}(|x|)$ -prior-entanglement then we can assume that  $\dim(\mathcal{P}_i) = 2^{\text{poly}(|x|)}$  and therefore  $\text{QMIP}^{\text{poly}}(\text{poly}, \text{poly}) \subseteq \text{QMIP}(\text{poly}, \text{poly})$ . This is not necessarily an equality, because potentially,

more entanglement may be used by the provers to cheat the verifier. It is possible that there are languages that can be proved without entanglement and can not be proved with it.

Thus the main difference between the quantum and the classical models is that the provers can use prior-entanglement to their advantage, and otherwise  $\text{QMIP} = \text{MIP}$ .

The power of  $\text{QMIP}^*(poly, poly)$  is a mystery, the provers are stronger and thus it might seem that they may prove more languages. However the provers are also less trustworthy so there might be some languages that the classical provers can prove but quantum provers with entanglement can not. Thus, it is not even known that  $\text{QMIP}^*(poly, poly) \subseteq \text{NEXP}$  or  $\text{NEXP} \subseteq \text{QMIP}^*(poly, poly)$ .

In [KV06] Kempe and Vidick expand the definition of  $\text{QMIP}(k, 1)$  to  $\text{QMIP}_{\log n, c, s}(k, 1)$ , the class of languages that have a QMIP proof with the verifiers complexity and the message registers logarithmic in the input size. They prove that  $\text{NP} \subseteq \text{QMIP}_{\log n, 1, 1-2^{-O(n)}}^*(2, 1)$ . This implies that even if the provers have unlimited entanglement they can not cheat perfectly. Recently, this result have been improved to  $1 - \frac{1}{poly(n)}$  soundness. By applying the padding argument this can be expanded to  $\text{NEXP} \subseteq \text{QMIP}_{poly(n), 1, 1-2^{-poly(n)}}^*(2, 1)$ .

### 3.3 An Example of a Nonlocal Strategy

In a game the verifier has no input. We still have, as before a protocol, and the provers goal is to make the verifier accept. A nonlocal strategy is a strategy used by two or more isolated provers. We are interested in the case the two provers share entanglement in a one round game. In this model the verifier picks questions  $(s, t)$  at random and sends  $s$  to  $P_1$  and  $t$  to  $P_2$ .  $P_1$  and  $P_2$  answer with  $a, b \in \{0, 1\}$  and the verifier accepts if  $V(s, t, a, b) = 1$  where  $V(s, t, a, b)$  is a predicate. The *value of a game* is the maximum probability a honest verifier accepts when the provers play optimally.

**Claim 1.** *The best prover strategy for any classical nonlocal game is deterministic.*

*Proof.* Consider  $P_1$  and  $P_2$  that use random strategies. The resulting strategy is a distribution over deterministic strategies. The  $i$ 'th deterministic strategy has some success probability  $p_i$ , and the value of the game is the expectation of  $p_i$  over this distribution. By choosing the deterministic strategy that achieves the maximal value we can only increase the value of the game.  $\square$

We present two examples from [CHTW04] that show how shared quantum entanglement can be utilized to improve the acceptance probability.

Consider the *CHSH game*: The verifier picks  $s, t \in \{0, 1\}$  at random, sends  $s$  to  $P_1$  and  $t$  to  $P_2$ .  $P_1$  and  $P_2$  answer with  $a, b \in \{0, 1\}$  and the verifier accepts if  $V(s, t, a, b) = 1$ , where

$$V(s, t, a, b) = \begin{cases} 1, & a \oplus b = s \wedge t \\ 0, & \text{else} \end{cases}$$

Since the best classical strategy is deterministic it can be checked that the classical value of the CHSH game is  $\frac{3}{4}$ . However there is a quantum strategy that achieves probability  $\cos^2(\pi/8) \approx 0.85$ .

Denote  $|\phi(\theta)\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ . The quantum provers  $P_1$  and  $P_2$  prepare the entangled state

$$|epr\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

with the left register in  $P_1$ 's possession and the right in  $P_2$ 's. The provers perform local measurements to determine the output  $a(s), b(t)$ .  $P_1$  measures his register in the  $\{|\phi(\alpha_s)\rangle, |\phi(\alpha_s)\rangle^\perp\}$  basis for  $\alpha_s = s \cdot (\pi/4)$ .  $P_2$  measures his in the  $\{|\phi(\beta_t)\rangle, |\phi(\beta_t)\rangle^\perp\}$  basis for  $\beta_t = (-1)^t \cdot (\pi/8)$ . It can be checked that the provers success probability is  $\cos^2(\pi/8)$ . It can also be proven that the above strategy is optimal.

The *Magic Square game* is presented and described in details by Aravind in [Ara02]. The verifier picks random questions  $s = (c, k) \in \{0, 1\} \times \{1, 2, 3\}$  and  $t = (i, j) \in \{1, 2, 3\}^2$  with the constraint that if  $c = 0$  then  $i = k$  and  $j = k$  otherwise. He sends  $s$  to  $P_1$  and  $t$  to  $P_2$ .  $P_1$  and  $P_2$  answer with  $a = (a_1, a_2, a_3) \in \{0, 1\}^3$  and  $b \in \{0, 1\}$  respectively. The verifier accepts iff

$$(a_1 \oplus a_2 \oplus a_3 = c) \wedge ((c = 0 \Rightarrow b = a_j) \vee (c = 1 \Rightarrow b = a_i))$$

We can think of this game as follows. The verifier asks  $P_1$  for a row (if  $c = 0$ ) or a column (if  $c = 1$ ) of a 3x3 binary matrix, and asks  $P_2$  for an entry  $(i, j)$  from that row or column. The verifier checks that the answers are consistent and that a row has even parity and a column has an odd parity.

It is easy to see that there is no 3x3 binary matrix with the property that each row has an even parity and each column has an odd parity. It follows from this that without entanglement there is a constant probability for the verifier to reject. The classical value of the game is in fact  $\frac{17}{18}$ . Remarkably there is a perfect quantum strategy (with entanglement) that achieves the value 1. The strategy is presented in [Ara02] and we do not describe it here.

## 4 QIP(3) and the Diamond Norm

In this section we survey Kitaev and Watrous [KW00] characterization of QIP(3) using the diamond norm.

### 4.1 Diamond norm

**Definition 2.** *The Trace Norm of an operator  $A \in L(\mathcal{H})$  is*

$$\|A\|_{\text{tr}} = \max_{U \in U(\mathcal{H})} |\text{Tr}(UA)|$$

If  $A$  is a normal matrix with eigenvalues  $\{\lambda_i\}$  then  $\|A\|_{\text{tr}} = \sum_i |\lambda_i|$ . For a general  $A$  it can be checked that  $\|A\|_{\text{tr}} = \text{Tr}(|A|) = \text{Tr}(\sqrt{AA^\dagger})$ . Also  $\|A\|_{\text{tr}} = \sum_i s_i(A)$  where  $s_1(A) \geq \dots \geq s_n(A)$  are the singular values of  $A$ .

The natural generalization of the  $\|\cdot\|_{\text{tr}}$  to superoperators is

**Definition 3.** *Let  $T : L(\mathcal{H}_1) \rightarrow L(\mathcal{H}_2)$  be a superoperator. The  $l_1$  norm  $\|T\|_1$  is*

$$\|T\|_1 = \max_{A: \|A\|_{\text{tr}}=1} \|T(A)\|_{\text{tr}}$$

**Definition 4.** *A superoperator norm  $\|\cdot\|$  is  $f(n)$ -stable iff for any  $T : L(\mathcal{H}_1) \rightarrow L(\mathcal{H}_2)$  having  $\dim(\mathcal{H}_1) = n$  and every  $N \geq 0$  it holds that*

$$\|T \otimes I_N\| \leq \|T \otimes I_{f(n)}\|$$

If  $f(n) = 0$  we say that  $\|\cdot\|$  is *stable*. The  $l_1$  norm is not stable. For example consider the superoperator on  $L(\mathbb{C}^2)$

$$T(|i\rangle\langle j|) = |j\rangle\langle i|, (i, j = 0, 1)$$

On the one hand  $\|T\|_1 = 1$ . On the other hand for  $A = \sum_{i,j} |i, i\rangle\langle j, j|$ ,  $\|A\|_{\text{tr}} = 2$  but  $\|T \otimes I_1(A)\|_{\text{tr}} = 4$ , and so  $\|T \otimes I_1\|_1 \geq 2$ . Fortunately Kitaev [KVS02] proved that  $\|\cdot\|_1$  is  $n$ -stable. For any  $N \geq 0$  and  $n = \dim(\mathcal{H}_1)$  it holds that  $\|T \otimes I_N\|_1 \leq \|T \otimes I_n\|_1$ . Watrous [Wat05] gave a simpler proof of that. This allows to define the diamond norm.

**Definition 5.** *Let  $T : L(\mathcal{H}_1) \rightarrow L(\mathcal{H}_2)$  be a superoperator and  $n = \dim(\mathcal{H}_1)$  then the diamond norm  $\|T\|_\diamond$  is*

$$\|T\|_\diamond = \|T \otimes I_n\|_1$$

This defines a norm [KVS02]. The  $\|\cdot\|_\diamond$  is indeed stable. Kitaev [KVS02] also proved that the diamond norm is multiplicative, i.e.,  $\|T \otimes R\|_\diamond = \|T\|_\diamond \|R\|_\diamond$ . He also gave other equivalent mathematical formulations to it.

## 4.2 QIP(3) Characterization

Denote  $\text{QIP}(3, s, c)$  the class of languages with a QIP proof system with three messages, soundness  $s$  and completeness  $c$ . Let  $L \in \text{QIP}(3, s, 1)$  proved to a verifier  $V$ . The protocol is characterized by the unitary operators  $V_1, V_2$  the verifier applies in each round, the initial state projection  $\Pi_{init}$  and the accepting projection  $\Pi_{acc}$ . Denote  $B_1 = V_1 \Pi_{init}, B_2 = \Pi_{acc} V_2$ . Let  $\text{MAP}(B_1, B_2)$  denote the maximal acceptance probability of the verifier. Kitaev and Watrous proved that

$$\text{MAP}(B_1, B_2) = \|T\|_{\diamond}$$

where  $T(X) = \text{Tr}_{\mathcal{V}}(B_1 X B_2^\dagger)$  giving a neat algebraic characterization of the game.

Kitaev and Watrous used the above characterization in [KW00] to show that parallel amplification works in  $\text{QIP}(3, s, 1)$ .

**Theorem 4.1.** *Let  $p(n)$  be a polynomial and  $s(n) \in [0, 1]$  be any function. Then  $\text{QIP}(3, s, 1) \subseteq \text{QIP}(3, s^p, 1)$ .*

*Proof.* Consider the verifier  $V'$  that runs  $p$  copies of the protocol of  $V$  in parallel. The new verifier is characterized by  $B'_1 = B_1^{\otimes p}$  and  $B'_2 = B_2^{\otimes p}$ . The resulting superoperator is  $T^{\otimes p}$  and the maximum acceptance probability is therefore  $\text{MAP}(B'_1, B'_2) = \|T^{\otimes p}\|_{\diamond} = \|T\|_{\diamond}^p$  because the diamond norm is multiplicative. Thus, if  $x \in L$  then  $\text{MAP}(B'_1, B'_2) = 1$  and if  $x \notin L$  then  $\text{MAP}(B'_1, B'_2) \leq s^p$ .  $\square$

## 5 QMIP\*(2, 1) and the Product Norm

In this section we define a product operator norm and a product superoperator norm and later prove that the maximum acceptance probability for a given verifier in quantum one round two prover protocol can be described in terms of it.

### 5.1 The Product Norm

**Definition 6.** *For Hilbert spaces  $\mathcal{V}_1, \mathcal{V}_2$  and a matrix  $A \in L(\mathcal{V}_1 \otimes \mathcal{V}_2)$  the product norm of  $A$  is*

$$\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = \max_{U_i \in U(\mathcal{V}_i)} |\text{Tr}((U_1 \otimes U_2)A)|$$

**Claim 1.**  $\|\cdot\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$  is a norm.

*Proof.* The following things are simple.

1.  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \geq 0$ .
2.  $\|cA\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = c\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$ .
3. Triangle inequality.
4. If  $A = 0$  then  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = 0$ .

We are left with showing that if  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = 0$  then  $A = 0$ . Assume  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = 0$ . Then  $\|A\|_{\text{tr}} = \text{Tr}(UA)$  for some  $U \in U(\mathcal{V}_1 \otimes \mathcal{V}_2)$ . The transformation  $U$  can be represented as

$$U = \sum_i a_i (W_i \otimes V_i)$$

where  $W_i \in U(\mathcal{V}_1), V_i \in U(\mathcal{V}_2)$ . This is true because there is a unitary product basis for  $\mathcal{V}_1 \otimes \mathcal{V}_2$ . Thus  $\text{Tr}(UA) = \sum_i a_i \text{Tr}((W_i \otimes V_i)A) = 0$  and so  $\|A\|_{\text{tr}} = 0$  and  $A = 0$ .  $\square$

Let us notice that

$$\|\text{Tr}_{\mathcal{V}_2}(A)\|_{\text{tr}} \leq \|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \leq \|A\|_{\text{tr}} \quad (3)$$

The left inequality follows from Equations (1) and (2) because  $\text{Tr}((U_1 \otimes U_2)A) = \text{Tr}(U_1 \text{Tr}_{\mathcal{V}_2}((I \otimes U_2)A))$ . The right follows from the fact that  $\max_{U_i \in U(\mathcal{V}_i)} |\text{Tr}((U_1 \otimes U_2)A)| \leq \max_{U \in U(\mathcal{V}_1 \otimes \mathcal{V}_2)} |\text{Tr}(UA)|$ . Those inequalities can be strict, for example for  $A$  of the form  $A = |u\rangle\langle v|$ . For any such  $A$ ,  $\|A\|_{\text{tr}} = 1$  but we will show later that for  $A = |epr\rangle\langle 00|$  it holds that  $\|A\|_{\mathbb{C}^2 \otimes \mathbb{C}^2} = \frac{1}{\sqrt{2}}$  (where  $|epr\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ).

Next, we define a superoperator product norm.

**Definition 7.** For Hilbert spaces  $\mathcal{V}, \mathcal{V}_1, \mathcal{V}_2$  and superoperator  $T : L(\mathcal{V}) \rightarrow L(\mathcal{V}_1 \otimes \mathcal{V}_2)$  the superoperator product norm is

$$\|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} = \max_{\|A\|_{\text{tr}}=1} \|T(A)\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$$

It is easy to check that this is a norm and that  $\|I\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} = 1$ . Also, it follows from Equation (3) that  $\|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} \leq \|T\|_{\diamond}$ . A useful fact is:

**Claim 2.**

$$\|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} = \max_{|u\rangle, |v\rangle \in \mathcal{V}} \|T(|u\rangle\langle v|)\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$$

*Proof.* Any  $A$  satisfying  $\|A\|_{\text{tr}} = 1$  has a singular value decomposition  $A = \sum_i s_i |u_i\rangle\langle v_i|$  for  $s_i \geq 0$  and  $\sum_i s_i = 1$ . Thus

$$\begin{aligned} \|T(A)\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} &= \left\| T\left(\sum_i s_i |u_i\rangle\langle v_i|\right) \right\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \\ &\leq \sum_i s_i \|T(|u_i\rangle\langle v_i|)\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \\ &\leq \max_i \|T(|u_i\rangle\langle v_i|)\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \end{aligned}$$

Thus the maximum is always achieved on some rank one matrix  $|u\rangle\langle v|$ .  $\square$

## 5.2 QMIP\*(2, 1)

In this section we focus on QMIP\*(2, 1). The protocol is applied on the registers  $\mathcal{V} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2 \otimes \mathcal{P}_1 \otimes \mathcal{P}_2$  where  $\mathcal{V}$  is the verifier's private register.  $\mathcal{M}_1, \mathcal{M}_2$  are the registers passed between  $V$  and  $P_1, P_2$  respectively.  $\mathcal{P}_1, \mathcal{P}_2$  are the private registers of the provers. The initial quantum state is some  $|\psi\rangle$  of an arbitrary length chosen as part of the prover strategy.

The protocol proceeds as follows:

1. The verifier applies a measurement defined by  $\Pi_{\text{init}} = |0\rangle\langle 0|$  on  $\mathcal{V} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2$ . If the outcome is not  $|0\rangle$  he rejects. This step checks the initial state.
2. The verifier applies a unitary transformation  $V_1$  on  $\mathcal{V} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2$ . This prepares the questions to the two provers.
3. Prover  $i$  applies a unitary  $U_i$  on  $\mathcal{M}_i \otimes \mathcal{P}_i$ .
4. The verifier applies a unitary  $V_2$  on  $\mathcal{V} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2$ , followed by a measurement defined by  $\Pi_{\text{acc}} = |0\rangle\langle 0|$  on the first qubit of  $\mathcal{V}$  and accepts iff the outcome is  $|0\rangle$ .

If the provers are successful in convincing the verifier the final (unnormalized) state of the system is thus  $((\Pi_{\text{acc}} V_2) \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)((V_1 \Pi_{\text{init}}) \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})|\psi\rangle$

## 5.3 Acceptance Probability for a Given Verifier

Let  $V$  be a verifier.  $V$ 's strategy is defined by  $B_1 = V_1 \Pi_{\text{init}}$  and  $B_2 = \Pi_{\text{acc}} V_2$ . Let  $\text{MAP}(B_1, B_2)$  denote the maximum acceptance probability of  $V$ , when  $V$  plays with the optimal provers. I.e.,

$$\text{MAP}(B_1, B_2) = \max_{U_i \in U(\mathcal{M}_i \otimes \mathcal{P}_i), |\psi\rangle} |(B_2 \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})|\psi\rangle|^2 \quad (4)$$

We now relate  $\text{MAP}(B_1, B_2)$  to the superoperator product norm. We claim that:

**Theorem 5.1.**  $\text{MAP}(B_1, B_2) = \|T \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2}\|_{(\mathcal{M}_1 \otimes \mathcal{P}_1) \otimes (\mathcal{M}_2 \otimes \mathcal{P}_2), tr}^2$

where  $T : L(\mathcal{V} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2) \rightarrow L(\mathcal{M}_1 \otimes \mathcal{M}_2)$  is defined by  $T(X) = \text{Tr}_{\mathcal{V}}(B_1 X B_2)$ .

*Proof.* Denote  $\mathcal{P} = \mathcal{P}_1 \otimes \mathcal{P}_2$ . We start with Equation (4).

$$\sqrt{\text{MAP}(B_1, B_2)} = \max_{U_1, U_2, \psi} |(B_2 \otimes I_{\mathcal{P}})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}})|\psi\rangle|$$

Since we maximize over the unit vector  $|\psi\rangle$  we can replace the vector norm with the operator norm

$$\sqrt{\text{MAP}(B_1, B_2)} = \max_{U_1, U_2} \|(B_2 \otimes I_{\mathcal{P}})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}})\|$$

The operator norm of the matrix is the largest singular value, and so

$$\sqrt{\text{MAP}(B_1, B_2)} = \max_{U_1, U_2, v, u} |\langle v | (B_2 \otimes I_{\mathcal{P}})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}}) |u\rangle|$$

Since this is a scalar number we can insert trace

$$\begin{aligned} \sqrt{\text{MAP}(B_1, B_2)} &= \max_{U_1, U_2, v, u} |\text{Tr}(\langle v | (B_2 \otimes I_{\mathcal{P}})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}}) |u\rangle)| \\ &= \max_{U_1, U_2, v, u} |\text{Tr}((I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}}) |u\rangle \langle v | (B_2 \otimes I_{\mathcal{P}}))| \end{aligned}$$

By Equation (1)

$$\sqrt{\text{MAP}(B_1, B_2)} = \max_{U_1, U_2, v, u} |\text{Tr}(\text{Tr}_{\mathcal{V}}((I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}}) |u\rangle \langle v | (B_2 \otimes I_{\mathcal{P}})))|$$

By Equation (2) we can carry the operators that do not affect  $\mathcal{V}$  out, use the definition of  $T$  and then use Claim 2.

$$\begin{aligned} \sqrt{\text{MAP}(B_1, B_2)} &= \max_{U_1, U_2, u, v} |\text{Tr}((U_1 \otimes U_2) \text{Tr}_{\mathcal{V}}((B_1 \otimes I_{\mathcal{P}}) |u\rangle \langle v | (B_2 \otimes I_{\mathcal{P}})))| \\ &= \max_{U_1, U_2, u, v} |\text{Tr}((U_1 \otimes U_2)(T \otimes I_{\mathcal{P}})(|u\rangle \langle v|))| \\ &= \|T \otimes I_{\mathcal{P}}\|_{(\mathcal{M}_1 \otimes \mathcal{P}_1) \otimes (\mathcal{M}_2 \otimes \mathcal{P}_2), tr} \end{aligned}$$

□

## 6 Trace Norm of a Product and Product Norm of Rank 1 Matrices

In this section we prove a useful bound on  $\|BC\|_{\text{tr}}$  and use it to show what is the product norm for rank 1 matrices.

### 6.1 A Bound on the Trace Norm of a Product

**Lemma 6.1.** *Fix arbitrary matrices  $B$  and  $C$  with  $s_1(B) \geq \dots \geq s_n(B) \geq 0$  the singular values of  $B$ , and  $s_1(C) \geq \dots \geq s_n(C) \geq 0$  the singular values of  $C$ . Then*

$$\|BC\|_{\text{tr}} \leq \sum_i s_i(B)s_i(C)$$

The bound appearing in ([KVS02], page 99) and in many other places is  $\|BC\|_{\text{tr}} \leq \|B\| \|C\|_{\text{tr}}$ , i.e.,  $\|BC\|_{\text{tr}} \leq s_1(B) \sum_i s_i(C)$ . We are not aware of a better upper bound appearing elsewhere. The above lemma gives the tighter bound  $\|BC\|_{\text{tr}} = \sum_i s_i(BC) \leq \sum_i s_i(B)s_i(C)$ . Notice also that this is tight for normal commuting matrices  $B$  and  $C$ .

*Proof.* Let us denote the singular value decomposition of  $C$ ,  $C = UDV$  with the unitaries  $U, V$  and  $D = \text{diag}(s_1(C), \dots, s_n(C))$ . Thus

$$\|BC\|_{\text{tr}} = \text{Tr}(|BC|) = \text{Tr}(|BUDV|) = \text{Tr}(|BUD|)$$

Let  $P_k$  denote the projection  $P_k = \sum_{i=1}^k |i\rangle\langle i|$ . It can be checked that  $D = s_n(C)P_n + \sum_{i=1}^{n-1} (s_i(C) - s_{i+1}(C))P_i$ . Thus

$$\text{Tr}(|BC|) \leq s_n(C) \text{Tr}(|BUP_n|) + \sum_{i=1}^{n-1} (s_i(C) - s_{i+1}(C)) \text{Tr}(|BUP_i|)$$

We have used the fact that  $s_i(C) - s_{i+1}(C) \geq 0$  and that  $\text{Tr}(|X+Y|) \leq \text{Tr}(|X|) + \text{Tr}(|Y|)$  since the trace-norm is a norm. However,

$$\text{Tr}(|BUP_k|) = \sum_{i=1}^n s_i(BUP_k) = \sum_{i=1}^k s_i(BUP_k)$$

because  $\text{rank}(BUP_k) \leq \text{rank}(P_k) = k$  since  $P_k$  is a projection. By [Bha97]

(Problem III.6.2 page 75)  $s_i(BUP_k) \leq \|P_k\| s_i(BU) = s_i(B)$ . It follows that

$$\begin{aligned} \|BC\|_{\text{tr}} = \text{Tr}(|BC|) &\leq s_n(C) \sum_{j=1}^n s_j(B) + \sum_{i=1}^{n-1} (s_i(C) - s_{i+1}(C)) \sum_{j=1}^i s_j(B) \\ &= \sum_{i=1}^n s_i(B) s_i(C) \end{aligned}$$

□

Originally we had a different proof and proved something weaker. We are grateful to Zeph Landau for suggesting the idea of reducing the singular values of  $C$  to  $P_k$ .

## 6.2 Product Norm of Rank 1 Matrices

We now look at the special case of rank 1 matrices.

**Theorem 6.2.** *Let  $A$  be a rank 1 matrix over  $\mathcal{V}_1 \otimes \mathcal{V}_2$ . Thus  $A = |u\rangle\langle v|$  for some  $u, v \in \mathcal{V}_1 \otimes \mathcal{V}_2$ . Suppose the Schmidt decomposition of  $u$  is  $|u\rangle = \sum_i \alpha_i |x_i\rangle \otimes |y_i\rangle$ , and of  $v$  is  $|v\rangle = \sum_i \beta_i |w_i\rangle \otimes |z_i\rangle$  with  $\alpha_i, \beta_i \geq 0$  sorted in descending order. Then*

$$\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = \sum_i \alpha_i \beta_i$$

*Proof.* We can assume without loss of generality that  $|x_i\rangle = |y_i\rangle = |w_i\rangle = |z_i\rangle = |i\rangle$  because  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_1} = \|(U_1 \otimes U_2)A(V_1 \otimes V_2)\|_{\mathcal{V}_1 \otimes \mathcal{V}_1}$  for any unitaries  $U_1, V_1 \in U(\mathcal{V}_1)$  and  $U_2, V_2 \in U(\mathcal{V}_2)$ . Thus

$$A = |u\rangle\langle v| = \sum_{i,j} \alpha_i \beta_j |i, i\rangle\langle j, j|$$

and

$$\begin{aligned} \text{Tr}((U_1 \otimes U_2)A) &= \sum_{i,j} \alpha_i \beta_j \langle j| U_1 |i\rangle \langle j| U_2 |i\rangle \\ &= \sum_{i,j} \alpha_i (U_1)_{j,i} \cdot \beta_j (U_2)_{j,i} \end{aligned}$$

We can look at this sum of products as a standard matrix inner product. Let us denote the matrices  $C$  and  $B$  as follows,  $C_{j,i} = \alpha_i (U_1)_{j,i}$  and  $B_{j,i} = \beta_j (U_2)_{j,i}$ . Then

$$\text{Tr}((U_1 \otimes U_2)A) = \sum_{i,j} B_{i,j} C_{i,j} = \text{Tr}(B^t C)$$

By Lemma 6.1,  $|\text{Tr}(B^t C)| \leq \|B^t C\|_{\text{tr}} \leq \sum_i \alpha_i \beta_i$ , because  $C = U_1 \text{diag}(\alpha_1, \dots, \alpha_n)$ ,  $B = \text{diag}(\beta_1, \dots, \beta_n) U_2$ , and so  $s_i(C) = \alpha_i$  and  $s_i(B) = \beta_i$ . Finally, this upper bound can be achieved by  $U_1 = U_2 = I$ .  $\square$

### 6.3 Failed Attempts to Characterize the Product Norm

We could have hoped that  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$  is a function of the singular values of  $A$ , but this is not the case. Consider for example  $A = |00\rangle\langle 11|$  and the unitary transformation  $U = |01\rangle\langle 00| + |epr\rangle\langle 11| + |10\rangle\langle 01| + |epr^\perp\rangle\langle 10|$ . It follows from the Theorem 6.2 that  $\|UAU^\dagger\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = \||01\rangle\langle epr|\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = \frac{1}{\sqrt{2}}$  and so  $\|UAU^\dagger\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \neq \|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$ . Hence  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$  is not unitarily invariant and not a function of the singular values of  $A$ .

The partition of the space  $\mathcal{V}$  to the product  $\mathcal{V}_1 \otimes \mathcal{V}_2$  heavily influences the product norm. Therefore, we could have hoped that the product norm of  $A$  is a function of the singular values of some reduced density matrices. In fact, we see that in the case that  $\text{rank}(A) = 1$  it holds that  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = \frac{\sum_i \sqrt{s_i(\text{Tr}_{\mathcal{V}_2}(A^\dagger A)) s_i(\text{Tr}_{\mathcal{V}_2}(AA^\dagger))}}{\|A\|_{\text{tr}}}$ . We did not find a similar connection for higher ranks, and it is unlikely that such a connection depends on  $AA^\dagger$  and  $A^\dagger A$  alone. This is because the trace norm and the product norm coincide on positive matrices  $A$ , but may differ on Hermitian matrices  $A$ . However, for Hermitian  $A$ ,  $AA^\dagger$  and  $A^\dagger A$  are both equal to  $|A|$  which is positive.

We can also use our analysis of rank one matrices to show that  $\|AB\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$  may be larger or smaller than  $\|A\|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \|B\|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$ . For example for the matrices  $A = |00\rangle\langle epr|$ ,  $B = |epr\rangle\langle 00|$ ,  $C = |00\rangle\langle 00|$  and  $D = |epr\rangle\langle epr|$ , it is easy to check that  $\|AB\|_{\mathbb{C}^2 \otimes \mathbb{C}^2} > \|A\|_{\mathbb{C}^2 \otimes \mathbb{C}^2} \|B\|_{\mathbb{C}^2 \otimes \mathbb{C}^2}$  and  $\|CD\|_{\mathbb{C}^2 \otimes \mathbb{C}^2} < \|C\|_{\mathbb{C}^2 \otimes \mathbb{C}^2} \|D\|_{\mathbb{C}^2 \otimes \mathbb{C}^2}$ .

## 7 Directions for Further Research

First we expand the definition of stability to the superoperator product norm. We do this by adding to each register of the original partition  $\mathcal{V}_1, \mathcal{V}_2$  an additional register  $\mathbb{C}^N$  and applying the superoperator  $T \otimes I_N \otimes I_N$  with the identity operator over the new registers.

**Definition 7.1.**  $A \|\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr}$  is  $f(n)$ -stable iff for any  $T : L(\mathcal{H}) \rightarrow L(\mathcal{V}_1 \otimes \mathcal{V}_2)$  having  $\dim(\mathcal{H}) = n$  and every  $N \geq 0$  it holds that

$$\|T \otimes I_{N^2}\|_{(\mathcal{V}_1 \otimes \mathbb{C}^N) \otimes (\mathcal{V}_2 \otimes \mathbb{C}^N), tr} \leq \|T \otimes I_{f(n)^2}\|_{(\mathcal{V}_1 \otimes \mathbb{C}^{f(n)}) \otimes (\mathcal{V}_2 \otimes \mathbb{C}^{f(n)}), tr}$$

Consider the superoperator  $T : L(\mathbb{C}^4) \rightarrow L(\mathbb{C}^2 \otimes \mathbb{C}^2)$  that is defined by  $T(|i, j\rangle\langle k, m|) = |k, m\rangle\langle i, j|$ . Then  $\|T\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr} \leq \|T\|_1 = 1$ . On the other hand,  $\|T \otimes I_4\|_{(\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathbb{C}^2 \otimes \mathbb{C}^2), tr} = 4$ . To see that use  $A = \sum_{i,j,k,m} |i, j, i, j\rangle\langle k, m, k, m|$ . It is easy to check that  $\|A\|_{tr} = 4$ , and that by  $U|i, k\rangle = |k, i\rangle$  we have  $(U \otimes U)(T \otimes I_4)(A) = \sum_{i,j,k,m} |i, k, j, m\rangle\langle i, k, j, m| = I_{16}$  and so  $\|T \otimes I_4\|_{(\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathbb{C}^2 \otimes \mathbb{C}^2), tr} \geq 4$ . Altogether  $\|T \otimes I_4\|_{(\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathbb{C}^2 \otimes \mathbb{C}^2), tr} \leq \|T\|_{\diamond} = 4$ .

We can *not* prove that the product norm stabilizes. However we would like to check what such a result would give.

**Hypothesis 1.**  $\|\cdot\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr}$  is *poly*( $n$ )-stable.

**Claim 3.** Under hypothesis 1  $\text{QMIP}^*(2, 1) \subseteq \text{NEXP} = \text{MIP}(2, 1)$ .

*Proof.* Let  $L \in \text{QMIP}^*(2, 1)$ . Consider a verifier  $V$  for  $L$ . By Theorem 5.1 the maximum acceptance probability of  $V$  is

$$\text{MAP}(B_1, B_2) = \|T \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2}\|_{(\mathcal{M}_1 \otimes \mathcal{P}_1) \otimes (\mathcal{M}_2 \otimes \mathcal{P}_2), tr}^2$$

for  $B_1, B_2$  and  $T$  defined as before. It follows from Definitions 6,7 and Claim 2 that

$$\text{MAP}(B_1, B_2) = \text{Tr}((U_1 \otimes U_2)(T \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})(|u\rangle\langle v|))$$

for some  $U_1 \in U(\mathcal{M}_1 \otimes \mathcal{P}_1)$ ,  $U_2 \in U(\mathcal{M}_2 \otimes \mathcal{P}_2)$  and  $|u\rangle, |v\rangle \in \mathcal{V} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2 \otimes \mathcal{P}_1 \otimes \mathcal{P}_2$ . Under the hypothesis we can fix such  $U_1, U_2$  and  $|u\rangle, |v\rangle$  that live in the world of *poly*( $|x|$ ) qubits. Consider the prover strategy  $U_1 \otimes U_2$  with the initial state  $|u\rangle$ . This strategy uses only *poly*( $|x|$ ) entangled qubits in the initial state and is optimal. Thus  $\text{QMIP}^*(2, 1) \subseteq \text{QMIP}^{\text{poly}}(2, 1)$  and we already mentioned that Kobayashi and Matsumoto proved in [KM03] that  $\text{QMIP}^{\text{poly}}(2, 1) \subseteq \text{NEXP}$ .  $\square$

Another hypothesis is the following. It is not known if there exists an efficient Turing machine for approximating the  $\|\cdot\|_{\diamond}$ . However Kitaev and Watrous proved in [KW00] that  $\text{QIP} \subseteq \text{EXP}$  by showing a reduction from distinguishing between the case of  $\text{MAP}(B_1, B_2) = 1$  and  $\text{MAP}(B_1, B_2) \leq \frac{1}{2}$  to a semidefinite programming problem of an exponential size (in the number of qubits).

**Hypothesis 2.** For  $T : L(\mathcal{H}) \rightarrow L(\mathcal{V}_1 \otimes \mathcal{V}_2)$  there exists a Turing machine that approximates  $\|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr}$  in *poly*( $\dim(\mathcal{H}) + \dim(\mathcal{V}_1 \otimes \mathcal{V}_2)$ ) time.

**Claim 4.** If both hypotheses are true then  $\text{QMIP}^*(2, 1) \subseteq \text{EXP}$ .

*Proof.* Let  $L \in \text{QMIP}^*(2, 1)$ . Hypothesis 1 implies that  $L$  has a protocol  $\langle V, P_1, P_2 \rangle$  with maximum acceptance probability

$$\|T \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2}\|_{(\mathcal{M}_1 \otimes \mathcal{P}_1) \otimes (\mathcal{M}_2 \otimes \mathcal{P}_2), tr}^2$$

for  $T$  defined as previously and  $\dim(\mathcal{M}_1 \otimes \mathcal{P}_1 \otimes \mathcal{M}_2 \otimes \mathcal{P}_2) = 2^{\text{poly}(|x|)}$ . Hypothesis 2 implies that there is a Turing machine that approximates the maximum acceptance probability and decides if  $x \in L$  in  $\text{poly}(2^{\text{poly}(|x|)})$  time.  $\square$

## 7.1 Superoperator Product Norm of the Tensor

Another open problem is the parallel amplification of  $\text{QMIP}^*(2, 1)$ . We know from [KVS02] that  $\|T \otimes R\|_{\diamond} = \|T\|_{\diamond} \cdot \|R\|_{\diamond}$  and that implies parallel amplification for  $\text{QIP}(3)$ . What about the product superoperator norm?

**Claim 5.** *For any two superoperators  $T : L(\mathcal{H}_1) \rightarrow L(\mathcal{V}_1 \otimes \mathcal{W}_1)$  and  $R : L(\mathcal{H}_2) \rightarrow L(\mathcal{V}_2 \otimes \mathcal{W}_2)$  it holds that*

$$\|T \otimes R\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2), tr} \geq \|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} \cdot \|R\|_{\mathcal{W}_1 \otimes \mathcal{W}_2, tr}$$

*Proof.*

$$\|T \otimes R\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2), tr} = \max_{\|X\|_{tr}=1} \|(T \otimes R)(X)\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2)}$$

Let us look at the special case where  $X \in L(\mathcal{H}_1 \otimes \mathcal{H}_2)$  is product,  $X = A \otimes B$  for some  $A \in L(\mathcal{H}_1)$  and  $B \in L(\mathcal{H}_2)$ .

$$\begin{aligned} \|T \otimes R\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2), tr} &\geq \max_{\|A\|_{tr}=\|B\|_{tr}=1} \|(T \otimes R)(A \otimes B)\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2)} \\ &= \max_{\|A\|_{tr}=\|B\|_{tr}=1} \|T(A) \otimes R(B)\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2)} \\ &= \max_{\|A\|_{tr}=\|B\|_{tr}=1, U_1, U_2} \text{Tr}((U_1 \otimes U_2)(T(A) \otimes R(B))) \end{aligned}$$

for unitaries  $U_1 \in U(\mathcal{V}_1 \otimes \mathcal{W}_1)$  and  $U_2 \in U(\mathcal{V}_2 \otimes \mathcal{W}_2)$ . We again look at the special case where  $U_1$  and  $U_2$  are also products of unitaries  $U_1 = V_1 \otimes W_1$  and  $U_2 = V_2 \otimes W_2$  for  $V_1 \in U(\mathcal{V}_1)$ ,  $W_1 \in U(\mathcal{W}_1)$ ,  $V_2 \in U(\mathcal{V}_2)$ ,  $W_2 \in U(\mathcal{W}_2)$ . Then

$$\begin{aligned} &\|T \otimes R\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2), tr} \\ &\geq \max_{\|A\|_{tr}=\|B\|_{tr}=1, V_1, V_2, W_1, W_2} \text{Tr}((V_1 \otimes W_1 \otimes V_2 \otimes W_2)(T(A) \otimes R(B))) \\ &= \max_{\|A\|_{tr}=\|B\|_{tr}=1, V_1, V_2, W_1, W_2} \text{Tr}((V_1 \otimes V_2)T(A)) \cdot \text{Tr}((W_1 \otimes W_2)R(B)) \\ &= \|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} \cdot \|R\|_{\mathcal{W}_1 \otimes \mathcal{W}_2, tr} \end{aligned}$$

$\square$

In particular it follows from above that  $\|T\|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} \leq \|T \otimes I\|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2), tr}$ .

In [KVS02] it is proved that  $\|T \otimes R\|_{\diamond} = \|T\|_{\diamond} \cdot \|R\|_{\diamond}$  by showing first that  $\|T \otimes R\|_1 \geq \|T\|_1 \cdot \|R\|_1$ . The last inequality is true because  $\|T \otimes R\|_{\diamond} = \|T \otimes R \otimes I\|_1 = \|(T \otimes I)(I \otimes R)\|_1 \leq \|(T \otimes I)\|_1 \cdot \|(I \otimes R)\|_1$ . Thus a crucial fact used is that  $\|TR\|_1 \leq \|T\|_1 \cdot \|R\|_1$ . Since there is no similar result for the product norm we do not get a trivial parallel amplification scheme even under Hypothesis 1.

Consider for example the superoperators  $T, R : L(\mathbb{C}^4) \rightarrow L(\mathbb{C}^4)$  defined by  $T(|epr\rangle\langle 00|) = |00\rangle\langle 00|$ ,  $R(|00\rangle\langle 00|) = |epr\rangle\langle 00|$  and 0 on the complementary matrices of the basis. Then by Theorem 6.2  $\|T\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr} = 1$  and  $\|R\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr} = \frac{1}{\sqrt{2}}$  but it is easy to see that  $\|TR\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr} = 1$ . Thus  $\|TR\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr} > \|T\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr} \cdot \|R\|_{\mathbb{C}^2 \otimes \mathbb{C}^2, tr}$ .

## 7.2 Additional Open Questions

Additional questions that can be asked are:

1. We do not know if  $\text{QMIP}^*(2, 1)$  can be made to have perfect completeness even at the cost of adding additional communication rounds as in QIP.
2. We know that adding more communication rounds does not change the power of  $\text{MIP}(2, 1)$ . Is it so for  $\text{QMIP}^*(2, 1)$ ?
3. What if we increase the number of provers i.e look at  $(\text{QMIP}^*(k, 1))$  for  $k > 2$ ? How does this affect the proof system?

## References

- [Ara02] P.K Aravind. A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities. *Arxiv preprint quant-ph/0206070*, 2002.
- [BBC<sup>+</sup>93] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.
- [BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991.
- [Bha97] R. Bhatia. *Matrix Analysis*. Springer, 1997.

- [BM88] L. Babai and S. Moran. Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36:254–276, 1988.
- [BW92] C.H. Bennett and S.J. Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.
- [CHTW04] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. *Computational Complexity*, pages 236–249, 2004.
- [Gol99] O. Goldreich. *Modern cryptography, probabilistic proofs and pseudorandomness*, volume 17 of *Algorithms and Combinatorics*. Springer-Verlag, 1999.
- [GS86] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 59–68, 1986.
- [KM03] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66:429–450, 2003.
- [KV06] J. Kempe and T. Vidick. On the power of entangled quantum provers, 2006.
- [KVS02] A. Kitaev, M. Vyalyi, and A. Shen. *Classical and Quantum Computation*. American Mathematical Society, 2002.
- [KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. *STOC*, pages 608–617, 2000.
- [MW05] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14:122–152, 2005.
- [PR97] S. Popescu and D. Rohrlich. On the measure of entanglement for pure states. Technical report, Hewlett Packard Laboratories, 1997.
- [Raz98] R. Raz. A parallel repetition theorem. *SIAM*, 27:763–803, 1998.
- [Sha92] A. Shamir.  $IP = PSPACE$ . *J. ACM*, 39:869–877, 1992.

- [Sho97] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM*, 26:1484, 1997.
- [Wat05] J. Watrous. Notes on super-operator norms induced by Schatten norms. *Arxiv preprint quant-ph/0411077*, 2005.