On the power of quantum, one round, two prover interactive proof systems

Alex Rapaport and Amnon Ta-Shma
Department of Computer Science
Tel-Aviv University
Israel 69978.
email: rapapo,amnon@post.tau.ac.il. *

September 23, 2007

Abstract

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.

1 Introduction

Classical interactive proof systems allow an interaction between an efficient verifier and an all powerful prover. Classical interactive proof systems are quite powerful: one prover can prove theorems in PSPACE to an efficient verifier [14, 15] while two or more powerful provers that cannot interact between themselves can prove the whole of NEXP [2].

Kitaev and Watrous [12] 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 probably not as powerful as classical two provers (PSPACE $\subseteq$ QIP $\subseteq$ EXP). Moreover they show that in the quantum case 3 communication messages are enough (QIP = 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 limited entanglement and in the third they can share unlimited entanglement. Kobayashi and Matsumoto [13] prove that without entanglement quantum multiprover proofs are as powerful as classical. They also prove that

*This research was supported by USA-Israel BSF grant 2004390 and by the EU integrated project QAP.

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 prover quantum interactive proofs with unlimited prior entanglement and one round of communication. Let $\mathrm{QMIP}^*(2,1)$ denote the class of languages having such a protocol (for a formal definition see Section 2.2). The power of $\mathrm{QMIP}^*(2,1)$ is little understood. On the one hand more entanglement potentially gives the provers power to prove more languages to the verifier, so it might be the case that $\mathrm{QMIP}^*(2,1)$ is much stronger than MIP = NEXP. In fact, we are not aware of any known upper bound on the power of the class $\mathrm{QMIP}^*(2,1)$, and as far as we know the class might contain undecidable languages. On the other hand, entanglement also gives the provers more power to cheat, so it is also possible that $\mathrm{QMIP}^*(2,1)$ is strictly weaker than MIP.

In $\mathrm{QMIP}^*(2,1)$ given a language L we have freedom to choose a good quantum interactive protocol for it. The related question of *nonlocal games* addresses the case of a *specific* given protocol. In a non-local game Alice and Bob play as provers against a fixed verifier. The provers' goal is to make the verifier accept. The value of the game is the probability the 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. In other word, local games are like interactive proofs except that we study a fixed protocol.

For non-local games, [6] and [1] showed several games in which quantum provers outperform the classical provers and violate Bell inequalities for classical correlation between noninteracting parties. In some cases (e.g., the Magic Square game of [1]) there is even a perfect quantum strategy that achieves game value 1. This demonstrates that for certain protocols entanglement can weaken the soundness and make a good classical protocol completely useless.

Another demonstration of this phenomenon was given for the class $\bigoplus \mathrm{MIP}^*$ of languages having a one round, two prover protocol with *classical communication*, provers who share *unlimited entanglement*, and with the additional requirement that each prover gives a binary answer and the value of the protocol is the XOR of the two answer bits. [6] prove (based on previous work on PCP) that without entanglement this class equals the class NEXP. Yet, in the same paper it is proved that with unlimited entanglement $\bigoplus \mathrm{MIP}^*$ is contained in NEXP, and this was first improved by the same authors [7] to EXP using semi-definite programming, and then by [18] to $\mathrm{QIP}(2) \subseteq \mathrm{EXP}$ ($\mathrm{QIP}(2)$ is the class of languages having a quantum interactive proof with a *single* prover and two messages).

Yet, the power of *general* quantum two prover interactive proofs is still a mystery. The only result about $\mathrm{QMIP}^*(2,1)$ we are aware of is that of [10] showing that NEXP is contained in $\mathrm{QMIP}^*(3,1)$ (i.e., three provers, one round) with a small gap between completeness and soundness, namely, the protocol has perfect completeness and $1-2^{-poly(n)}$ soundness. They also show that PSPACE has a two prover system with prefect completeness and $1-1/poly(n)$ 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 [4], superdense coding [5] and the above non-local games). There is also a natural measure for measuring the amount of entanglement in *pure states* [3]. Yet, there is no *single* good measure

for the amount of entanglement in *mixed states*. 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 [12] 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 [11], 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. We also present some hypotheses about our characterization and give their implications on the power of the proof system.

2 Preliminaries and Background

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 $\mathcal{H}$. A *superoperator* $T : L(\mathcal{H}_1) \to L(\mathcal{H}_2)$ 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*

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

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

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

and that

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

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

2.2 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.

A proof system for a language L has *soundness* s and *completeness* c, if for every input x in the language L, there exists a strategy for the provers such that the verifier accepts with probability at least c, while for every input x not in the language, for every strategy the provers use, the verifier accepts with probability at most s.

QIP(m) (Quantum IP) is the class of languages that can be proved to a quantum verifier with completeness $c = \frac{2}{3}$ and soundness $s = \frac{1}{3}$ 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.

We now turn to *two prover proof systems*. An important parameter of the system is the maximal amount of entangled qubits the provers are allowed to share (if at all) in the initial state of $\mathcal{P}_1 \otimes \mathcal{P}_2$. 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 2.1. *Fix functions $m(|x|), q(|x|) \geq 0$. QMIP$(2, m, q)$ is the class of languages L for which there is an interactive proof system with*

- *two 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, P_2 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, P_2 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

$$\begin{aligned} \mathrm{QMIP}(2, m) &= \mathrm{QMIP}(2, m, 0) \\ \mathrm{QMIP}^{poly}(2, m) &= \mathrm{QMIP}(2, m, poly) \\ \mathrm{QMIP}^{*}(2, m) &= \mathrm{QMIP}(2, m, \infty) \end{aligned}$$

Kobayashi and Matsumoto prove in [13] that

$$\mathrm{QMIP}(2, poly) = \mathrm{MIP}(2, poly) = \mathrm{NEXP}$$

Also, they proved that if the provers have $poly(|x|)$-prior-entanglement then we can assume that $\dim(\mathcal{P}_i) = 2^{poly(|x|)}$ and therefore $\mathrm{QMIP}^{poly}(2, poly) \subseteq \mathrm{NEXP}$. It is possible that the containment is strict.

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

2.3 The Diamond Norm

In this section we survey Kitaev and Watrous [12] characterization of QIP(3) using the diamond norm.

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

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

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

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

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

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

$$\| T \otimes I_N \|_. \leq \left\| T \otimes I_{f(n)} \right\|_.$$

where I_m is the identity super-operator over $L(H_m)$, and H_m is a dimension m Hilbert space.

If $f(n) = 0$ we say that $\| \ \|_.$ 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 $A = \sum_{i,j} |i, i\rangle\langle j, j|$, $\| A \|_{\mathrm{tr}} = 2$ but $\| T \otimes I_1(A) \|_{\mathrm{tr}} = 4$, and so $\| T \otimes I_1 \|_1 \geq 2$.

Fortunately Kitaev [11] proved that $\| \ \|_1$ 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 [17] gave a simpler proof of that. This allows one to define the diamond norm.

Definition 5. *Let $T : L(\mathcal{H}_1) \to L(\mathcal{H}_2)$ 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 [11]. The $\| \ \|_\diamond$ is indeed stable. Kitaev [11] 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.

2.4 QIP(3) Characterization by the diamond norm

Denote 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 Π_{init} and the accepting projection Π_{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

$$\text{MAP}(B_1, B_2) = \| T \|_\diamond^2$$

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

As a corollary of the above characterization and the fact that the diamond norm is multiplicative Kitaev and Watrous showed that QIP$(3, s, 1)$ has perfect parallel amplification.

3 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.

3.1 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*

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

Claim 1. $\| \ \|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$ *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.

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 $\| A \|_{\text{tr}} = Tr(UA)$ 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 basis for any $L(\mathcal{H})$. Pauli matrices are one example to such a basis when $\mathcal{H}$ has dimension that is a power of two, and generalized Pauli matrices (presented, e.g., in [16]) do the job for general dimensions. Thus $Tr(UA) = \sum_i a_i Tr((W_i \otimes V_i)A) = 0$ and so $\| A \|_{\text{tr}} = 0$ and $A = 0$. □

We notice that

$$\| \operatorname{Tr}_{\mathcal{V}_2}(A) \|_{\mathrm{tr}} \leq \| A \|_{\mathcal{V}_1 \otimes \mathcal{V}_2} \leq \| A \|_{\mathrm{tr}} \tag{3}$$

The left inequality follows from Equations (1) and (2) because $\operatorname{Tr}((U_1 \otimes U_2)A) = \operatorname{Tr}(U_1 \operatorname{Tr}_{\mathcal{V}_2}((I \otimes U_2)A))$. The right inequality follows from the fact that $\max_{U_i \in U(\mathcal{V}_i)} |Tr((U_1 \otimes U_2)A)| \leq \max_{U \in U(\mathcal{V}_1 \otimes \mathcal{V}_2)} |\operatorname{Tr}(UA)|$. Those inequalities can be strict, for example for A of the form $A = |u\rangle\langle v|$. For any such A, $\| A \|_{\mathrm{tr}} = 1$ 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 $|epr\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$). Another example is $A = |00\rangle\langle 11|$ with the partition $\mathcal{V}_1 = \mathcal{V}_2 = \mathbb{C}^2$. On the one hand $\| \operatorname{Tr}_{\mathcal{V}_2}(A) \|_{\mathrm{tr}} = 0$, but as we will show later $\| A \|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = 1$.

The following claim was communicated to us by the anonymous referee. It asserts that $\| A \|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$ is not only the maximum over all unitaries $U_i \in U(\mathcal{V}_i)$, but in fact is also the maximum over all linear operators of norm at most 1 in $L(\mathcal{V}_i)$. More precisely,

Claim 2. *[8] For Hilbert spaces $\mathcal{V}_1, \mathcal{V}_2$ and a matrix $A \in L(\mathcal{V}_1 \otimes \mathcal{V}_2)$*

$$\| A \|_{\mathcal{V}_1 \otimes \mathcal{V}_2} = \max_{Z_i \in L(\mathcal{V}_i) \,:\, ||Z_i|| \leq 1} |Tr((Z_1 \otimes Z_2)A)| \tag{4}$$

Proof. We look at the RHS of (4). Z_1 can be expressed as $Z_1 = NU$ for some unitary U and some normal matrix N of norm at most 1 (in fact, N can be made positive semi-definite but we do not care about that). Expressing N as $N = \sum \lambda_i v_i v_i^*$ for some orthonormal basis $\{v_i\}$, we see that the RHS (4) can only be improved by changing each λ_i to $\lambda_i' = \frac{w_i^*}{|w_i|}$ where $w_i = \operatorname{Tr}((v_i v_i^* U \otimes Z_2)A)$. The matrix $\sum \lambda_i' v_i v_i^*$ is, however, *unitary*.

Thus, we have shown that for any fixed A and Z_2 the maximum in the RHS of (4) may be obtained by some *unitary* Z_1. The same reasoning is then applied to Z_2 showing that the maximum may be obtained by some unitaries Z_1, Z_2 and therefore equals $\| A \|_{\mathcal{V}_1 \otimes \mathcal{V}_2}$. □

3.2 The Superoperator Product Norm

Next, we define a superoperator product norm.

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

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

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 3.

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

Proof. Any A satisfying $\| A \|_{\mathrm{tr}} = 1$ 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

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

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

Claim 4. *For any two superoperators $T : L(\mathcal{H}_1) \to L(\mathcal{V}_1 \otimes \mathcal{V}_2)$ and $R : L(\mathcal{H}_2) \to L(\mathcal{W}_1 \otimes \mathcal{W}_2)$ 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.

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

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 $B \in L(\mathcal{H}_2)$.

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

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

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

□

In particular it follows from above that

$$\| T \|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr} \leq \| T \otimes I_{\mathcal{W}_1 \otimes \mathcal{W}_2} \|_{(\mathcal{V}_1 \otimes \mathcal{W}_1) \otimes (\mathcal{V}_2 \otimes \mathcal{W}_2), tr}$$

Next 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 3.1. *$A \| \|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr}$ is $f(n)$-stable iff for any $T : L(\mathcal{H}) \to L(\mathcal{V}_1 \otimes \mathcal{V}_2)$ having $\dim(\mathcal{H}) = n$ and every $N \geq 0$ it holds that*

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

The $\| \ \|_{\mathcal{V}_1 \otimes \mathcal{V}_2, tr}$ norm is not 0 stable. Consider the superoperator $T : L(\mathbb{C}^4) \to L(\mathbb{C}^2 \otimes \mathbb{C}^2)$ 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 $\| A \|_{\mathrm{tr}} = 4$, 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 $\| T \otimes I_4 \|_{(\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathbb{C}^2 \otimes \mathbb{C}^2), tr} \leq \| T \|_\diamond = 4$.

3.3 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 $\Pi_{init} = |0\rangle\langle 0|$ 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 $\Pi_{acc} = |0\rangle\langle 0|$ 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

$$((\Pi_{acc} V_2) \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)((V_1 \Pi_{init}) \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})\,|\psi\rangle$$

3.4 Acceptance Probability for a Given Verifier

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

$$\mathrm{MAP}(B_1, B_2) = \max_{U_i \in U(\mathcal{M}_i \otimes \mathcal{P}_i), |\psi\rangle} \| (B_2 \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})(I_{\mathcal{V}} \otimes U_1 \otimes U_2)(B_1 \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2})\,|\psi\rangle \|^2 \quad (5)$$

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

Theorem 3.2. *$MAP(B_1, B_2) = \| T \otimes I_{\mathcal{P}_1 \otimes \mathcal{P}_2} \|^2_{(\mathcal{M}_1 \otimes \mathcal{P}_1) \otimes (\mathcal{M}_2 \otimes \mathcal{P}_2), tr}$*

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

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

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

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

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

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

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

Since this is a scalar number we can insert trace

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

By Equation (1)

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

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.

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

□

Let us notice that this proof is almost identical to the proof of QIP(3) characterization by Kitaev and Watrous [12]. The main difference is that here we have a product norm instead of the trace norm as a target. This is because the initial state of the provers in QMIP$^*(2, 1)$ can be viewed as the first message and so we actually have three messages instead of two.

4 Product Norm of Rank 1 Matrices

We start with a useful bound on $\| BC \|_{\mathrm{tr}}$ and use it to show what is the product norm for rank 1 matrices.

Lemma 4.1. *Fix arbitrary matrices B and C with $s_1(B) \geq \cdots \geq s_n(B) \geq 0$ the singular values of B, and $s_1(C) \geq \cdots \geq s_n(C) \geq 0$ the singular values of C. Then*

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

The above claim appears in [9] (page 182, Exercise 4). Notice also that this is tight for normal commuting matrices B and C.

With that we prove:

Theorem 4.2. *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

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

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

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

By Lemma 4.1, $|\mathrm{Tr}(B^t C)| \leq \| B^t C \|_{\mathrm{tr}} \leq \sum_i \alpha_i \beta_i$, because $C = U_1 \mathrm{diag}(\alpha_1, \ldots \alpha_n)$, $B = \mathrm{diag}(\beta_1, \ldots \beta_n) U_2$, and so $s_i(C) = \alpha_i$ and $s_i(B) = \beta_i$. Finally, this upper bound can be achieved by $U_1 = U_2 = I$. □

5 Directions for Further Research

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

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

Claim 5. *Under hypothesis 1 QMIP*(2,1) $\subseteq$ NEXP = MIP.*

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

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

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

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

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 $\mathrm{QMIP}^*(2,1) \subseteq \mathrm{QMIP}^{poly}(2,1)$ and we already mentioned that Kobayashi and Matsumoto proved in [13] that $\mathrm{QMIP}^{poly}(2,1) \subseteq$ NEXP. □

Another hypothesis is the following. Kitaev and Watrous proved in [12] that QIP ⊆ EXP by showing a reduction from distinguishing between the case of $\mathrm{MAP}(B_1, B_2) = 1$ and $\mathrm{MAP}(B_1, B_2) \leq \frac{1}{2}$ to a semidefinite programming problem of an exponential size (in the number of qubits).

Hypothesis 2. *For $T : L(\mathcal{H}) \to L(\mathcal{V}_1 \otimes \mathcal{V}_2)$ 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 6. *If both hypotheses are true then $QMIP^*(2,1) \subseteq EXP$.*

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

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

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

Acknowledgements

We thank Julia Kempe, Ashwin Nayak and Oded Regev for interesting discussions on the subject. We thank Zeph Landau for helping us prove Lemma 4.1, Ashwin Nayak for an alternative proof and Oded Regev for providing us with the reference in [9] where the lemma is proved. We thank the anonymous referee for communicating Claim 2 to us and for other helpful comments.

References

[1] P.K Aravind. A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities. *Arxiv preprint quant-ph/0206070*, 2002.

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

[3] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53(4):2046–2052, Apr 1996.

[4] 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.

[5] 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.

[6] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity*, pages 236–249, 2004.

[7] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. Presentation at Computational Complexity, 2004.

[8] Communication from the anonymous referee.

[9] R.A. Horn and C.R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, 1994.

[10] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. On the power of entangled provers: Immunizing games against entanglement, 2007.

[11] A. Kitaev, M. Vyalyi, and A. Shen. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[12] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. *STOC*, pages 608–617, 2000.

[13] 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.

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

[15] A. Shamir. IP = PSPACE. *J. ACM*, 39:869–877, 1992.

[16] K.G.H. Vollbrecht and R.F. Werner. Why Two Qubits Are Special. *Arxiv preprint quant-ph/9910064*, pages 6–7, 1999.

[17] J. Watrous. Notes on super-operator norms induced by schatten norms. *Arxiv preprint quant-ph/0411077*, 2005.

[18] S. Wehner. Entanglement in interactive proof systems with binary answers. In *STACS*, pages 162–171, 2006.