Embezzlement States are Universal for Non-Local Strategies

Mateus de Oliveira Oliveira

Blavatnik School of Computer Science, Tel Aviv University
mateusde@post.tau.ac.il

Abstract. We prove that the family of embezzlement states defined by van Dam and Hayden[26] is universal for both quantum and classical entangled two-prover non-local games with an arbitrary number of rounds. More precisely, we show that for each $\varepsilon > 0$ and each strategy for a k-round two-prover non-local game which uses a bipartite shared state on $2m$ qubits and makes the provers win with probability ω, there exists a strategy for the same game which uses an embezzlement state on $2m + 2m/\varepsilon$ qubits and makes the provers win with probability $\omega - \sqrt{2\varepsilon}$. Since the value of a game can be defined as the limit of the value of a maximal $2m$-qubit strategy as m goes to infinity, our result implies that the classes $QMIP^*_{c,s}[2,k]$ and $MIP^*_{c,s}[2,k]$ remain invariant if we allow the provers to share only embezzlement states, for any completeness value $c \in [0,1]$ and any soundness value $s < c$. Finally we notice that the circuits applied by each prover may be put into a very simple universal form.

1 Introduction

A k-round non-local game is an interactive procedure involving a referee, and two provers Alice and Bob. At each round the referee randomly selects two questions drawn from finite sets and sends one of them to each prover. Subsequently, each of the provers replies to her/his question. Alice and Bob are assumed to be in distinct locations and not to be able to communicate. In this way, none of them knows which question was sent to the other. At the end of the last round, the referee evaluates a publicly known predicate which depends on the whole history of questions and answers. The provers win if the predicate evaluates to true. The value of a non-local game is defined to be the maximum winning probability of Alice and Bob.

The importance of non-local games is twofold. On one hand they are intimately connected with multi-prover interactive proof systems [6]. In these systems a polynomial time verifier must decide the membership of a string x in a language L through an interactive protocol involving several provers which are not allowed to communicate. We say that a language L has a k-round two-prover interactive proof system if there exists a polynomial time function which assigns to each x a k-round game G_x in such a way that if x is in L then the value of the game G_x is above a threshold c, while if x is not in L, the value of the game G_x is below a threshold s for $s < c$. We refer to c as being the completeness of the system, and to s as being its soundness.

On the other hand, by allowing the provers to share a quantum system prepared in an arbitrary entangled state, non-local games become a suitable formalism to describe experiments that unveil the inherent non-locality of quantum mechanics. Following Bell's [4] observation that some predictions of quantum mechanics are inconsistent with local hidden variables theories, several experiments were proposed with the aim to provide a decisive test between quantum mechanics and hidden local variables theories. As an example, in the CHSH game which is based on a thought experiment of Clauser, Horne, Shimony and Holt [9], Bell's work implies that if the provers are classical the value of the game is 0.75 while if we allow the provers to share entanglement, there is a strategy which achieves a value of ≈ 0.85. In other examples of games, like the Kochen-Specker game [19, 25] and the Mermin-Peres magic square game [22, 2, 24], any classical strategy is doomed to fail with some probability while there is a quantum strategy which always allows the provers to win.

When dealing with interactive proof systems it is customary to impose limits on the computational power of the verifier, while the provers are assumed to be at most limited by the laws of physics. In this sense, it is reasonable to consider interactive proof systems in which the provers are allowed to share arbitrary quantum states. The study of how entanglement may affect the decidability properties of two-prover interactive proof systems was initiated by Cleve, Hoyer, Toner and Watrous [10]. They provide several examples of proof systems whose soundness is violated if we allow the provers to share

an entangled state. Furthermore they provide evidences that entanglement may significantly interfere in the decidability properties of multi-prover interactive proof systems. Let $\oplus MIP_{c,s}[2,1]$ denote the class of languages which can be decided by two prover interactive proof systems in which the final decision of the verifier is taken solely based on the XOR of the 1-bit answers of the provers, and $\oplus MIP^*_{c,s}[2,1]$ be its entangled version. Cleve et al. [10] show that $\oplus MIP^*_{c,s}[2,1] \subseteq EXP$, while in the classical case, it follows from works of Håstad [13] and Bellare, Goldreich and Sudan [5] that $\oplus MIP_{c,s}[2,1] = NEXP$ for certain completeness and soundness values. Indeed, by combining a result of Wehner [27] and Jain, Upadhyay and Watrous [14], it is possible to refine the first inclusion to $\oplus MIP^*[2,1] \subseteq PSPACE$. Thus unless, $PSPACE = NEXP$ entanglement indeed can weaken the decidability properties of XOR games. Entangled non local games were generalized and studied as well in the scenario in which the verifier is allowed to be quantum [16, 15, 17]. In particular, some positive aspects of entanglement are explored in [16], where the authors provide some evidence that prior entanglement may be useful for honest provers.

In order to make the study of entangled games slightly easier, it is reasonable to ask whether the bipartite state shared by the provers may be restricted to a class of states which is easy to describe and to work with. The aim of this work is to show that the embezzlement family of states defined by van Dam and Hayden[26], satisfy these criteria. More precisely, in Theorem 2 we prove that the family of embezzlement states is universal for two-prover non-local games with any number of rounds, in the sense that any strategy for a two-prover non-local game which yields a value ω may be replaced by a strategy for the same game that uses an embezzlement state and that yields a value of at least $\omega - \sqrt{2\varepsilon}$ for any ε with $0 < \varepsilon < 1$ with only a linear, in $1/\varepsilon$, overhead on the number of qubits to be shared. Since the value ω of a game can be defined as the limit of the value of a maximal $2m$-qubit strategy as m goes to infinity, this implies that ω itself is not changed when only embezzlement states are considered. As a consequence, the classes $QMIP^*_{c,s}[2,k]$ and $MIP^*_{c,s}[2]$ remain invariant through our restriction (Corollary 1). Finally, as an observation, we note in Theorem 3 that the circuits applied by the provers may also be put into a very simple universal form.

While in the classical case a series of results [3, 8, 20, 11, 12] established the relation $MIP[2,k] = MIP[2,1] = NEXP$ for any k, in the setting in which the provers share entanglement it makes sense to consider interactive proof systems with an arbitrary number of rounds because in this case it is not known whether $MIP^*[2,k] = MIP^*[2,1]$ for $k \geq 2$. It is also worth noting that the embezzlement family has been already considered (and generalized to any constant number of provers) by Leung, Toner and Watrous [21] and used to prove that if we allow the referee to be quantum, then there are one-round games whose value cannot be achieved by means of strategies that share a finite amount of entanglement. Nevertheless, the embezzlement family seems to have passed unnoticed as a universal family of states for non-local games, and in some of the literature concerning entangled multiprover interactive proof systems, the existence of such family is implicitly stated as an open problem [18].

The rest of this paper is organized as follows: In Section 2 we provide a formal definition of non-local games. In Section 3 we introduce van Dam and Hayden's embezzlement family and prove our universality results (Theorems 2 and 3, and Corollary 1).

2 Non-Local Games

A k-round two-prover non-local game is an interactive procedure undertaken by a verifier and two provers which we call Alice and Bob. The game proceeds as follows: Given two sets of questions S and T, two sets of answers A and B, and a predicate $V \subseteq S^k \times T^k \times A^k \times B^k$, at round i the verifier choses a pair of questions $(s_i, t_i) \in S \times T$ accordingly to a probability distribution π_i defined on $S \times T$ and sends the question s_i to Alice and the question t_i to Bob. Alice replies with an answer $a_i \in A$ and Bob replies with an answer $b_i \in B$. The provers win the game if the history $(s_1...s_k, t_1...t_k, a_1...a_k, b_1...b_k)$ of all questions and answers satisfies the predicate V. The goal of the provers is to follow a strategy that maximizes their winning probability. We note that the probability distribution π_i with which the verifier choses the questions at round i may depend on the questions and answers from previous rounds. We denote a k-round non-local game by $G = (V, \pi)$ where π is a set of probability distributions over $S \times T$

$$\pi = \{\pi_i(s_1...s_i, t_1...t_i, a_1...a_i, b_1...b_i) | 1 \leq i \leq k-1\} \tag{1}$$

The provers' strategies can be described by Positive Operator Valued Measurements (POVM's). Formally, a POVM in $\mathbb{C}^n$ with outcomes in $\mathcal{I}$ is a family of n-dimensional operators $M = \{M_i\}_{i \in \mathcal{I}}$

satisfying $\sum M_i^\dagger M_i = I_n$, where I_n is the identity in $\mathbb{C}^n$. Measuring a quantum system prepared in a state $|\psi\rangle \in \mathbb{C}^n$ according to M, yields the outcome i with probability $\langle\psi|M_i^\dagger M_i|\psi\rangle$ and post-measurement state $M_i|\psi\rangle/\langle\psi|M_i^\dagger M_i|\psi\rangle$ [23].

In a quantum strategy, the provers share a quantum register consisting of $2m$ qubits prepared in a bipartite state $|\psi\rangle \in \mathbb{C}^{2^m} \otimes \mathbb{C}^{2^m}$ in such a way that each prover holds m of the qubits. The state shared by the provers can be assumed to be pure, for if it were mixed, we could simply consider a pure state in a higher dimensional Hilbert space. For each question $s_i \in S$ and history of questions and answers $(s_1...s_{i-1}, a_1...a_{i-1})$, Alice has a POVM $\{X^{a_1...a_{i-1}|a_i}_{s_1...s_{i-1}|s_i}\}_{a_i \in A}$ with outcomes in A. Similarly, for each question $t_i \in T$ and history of questions and answers $(t_1...t_{i-1}, b_1...b_{i-1})$, Bob has a POVM $\{Y^{b_1...b_{i-1}|b_i}_{t_1...t_{i-1}|t_i}\}_{b_i \in B}$ with outcomes in B. In a slight abuse of notation we simply write $\{X^{a_i}_{s_i}\}_{a_i \in A}$ and $\{Y^{b_i}_{t_i}\}_{b_i \in B}$ whenever the history of the previous rounds is clear. A strategy on $2m$-qubits is completely determined by a triple $(|\psi\rangle_{2m}, X, Y)$ where $|\psi\rangle$ is the shared state, X is the collection of all POVM's of Alice and Y of all POVM's of Bob. Let $|\psi\rangle = |\psi_1\rangle$ be the initial state shared by the provers and $|\psi_i\rangle$ be the state shared by the provers at the i-th round. The probability with which Alice and Bob reply respectively a_i and b_i at the i-th round when questioned with s_i and t_i is given by

$$\langle\psi_i|(X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i})^\dagger X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i}|\psi_i\rangle \tag{2}$$

and the new state becomes

$$|\psi_{i+1}\rangle = \frac{X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i}|\psi_i\rangle}{\langle\psi_i|(X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i})^\dagger X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i}|\psi_i\rangle}\ . \tag{3}$$

As a convention we let boldface letters range over k-tuples of elements: $\mathbf{s} \in S^k$, $\mathbf{t} \in T^k$, $\mathbf{a} \in A^k$ and $\mathbf{b} \in B^k$. The value of the strategy $(|\psi\rangle, X, Y)$ for the game is defined as

$$\omega_G(|\psi\rangle, X, Y) = \sum_{\mathbf{s},\mathbf{t},\mathbf{a},\mathbf{b}} V(\mathbf{s},\mathbf{t},\mathbf{a},\mathbf{b}) \prod_{i=1}^{k} \pi_i(s_i,t_i) \prod_{i=1}^{k} \langle\psi_i|(X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i})^\dagger X^{a_i}_{s_i} \otimes Y^{b_i}_{t_i}|\psi_i\rangle, \tag{4}$$

which by using Equations (2) and (3), can be rewritten explicitly as a function of the initial shared state $|\psi\rangle$ as

$$\omega_G(|\psi\rangle_{2m}, X, Y) = \sum_{\mathbf{s},\mathbf{t},\mathbf{a},\mathbf{b}} \left[V(\mathbf{s},\mathbf{t},\mathbf{a},\mathbf{b}) \prod_{i=1}^{k} \pi_i(s_i,t_i) \right] \langle\psi| \left(X^{a_1}_{s_1}...X^{a_k}_{s_k} \otimes Y^{b_1}_{t_1}...Y^{b_k}_{t_k} \right)^\dagger X^{a_1}_{s_1}...X^{a_k}_{s_k} \otimes Y^{b_1}_{t_1}...Y^{b_k}_{t_k}|\psi\rangle. \tag{5}$$

The *entangled value* of G is defined as the limit of the maximum value among all n-qubit strategies as n goes to infinity.

$$\omega^e_G = \lim_{m\to\infty} \max_{|\psi\rangle_{2m}, X, Y} \omega^e_G(|\psi\rangle_{2m}, X, Y). \tag{6}$$

Non-local games can be further generalized to the case in which the verifier has quantum capabilities. In this case the communication with the provers proceeds through the exchange of quantum registers.

Definition 1 (Quantum Entangled Non-Local Games). *A k-round 2-prover entangled quantum game $G(V_1, ..., V_k)$ is defined by a verifier strategy $(V_1, ..., V_k, V_{k+1})$ where each V_i is a quantum circuit acting on three quantum registers: A private quantum register $priv_V$ and two quantum communication registers com_X and com_Y. A $2m$-qubit strategy for G consists of a bipartite quantum state $|\psi\rangle \in \mathbb{C}^{2^m} \otimes C^{2^m}$, and two sequences of quantum circuits $X = (X_1, ..., X_k)$ and $Y = (Y_1, ..., Y_k)$ (prover's circuits), where each X_i acts on the quantum communication register com_X and on a private quantum register $priv_X$, and each Y_i is a quantum circuit acting on the communication register com_Y and on a private quantum register $priv_Y$.*

The game proceeds as follows: At the start, $priv_V$, com_X and com_Y are initialized to $|0\rangle$ while $priv_X$ and $priv_Y$ are initialized to the bipartite state $|\psi\rangle$. The j-th round of the game consists in the application of the circuit V_j followed by the application of X_j and Y_j to their respective registers. After the k-th round, V_{k+1} is applied and the first private qubit q of the verifier is measured in the computational basis.

The quantum value $\omega_q(|\psi\rangle_{2m}, X, Y)$ of a strategy $(|\psi\rangle_{2m}, X, Y)$ is defined as the probability with which the measured qubit q is $|1\rangle$. Similarly to the classical entangled case, the value of a k-round quantum game $G = (V_1, ..., V_k, V_{k+1})$ is defined as

$$\omega_G^q = \lim_{m\to\infty} \max_{|\psi\rangle_{2m}, X, Y} \omega_G^q(|\psi\rangle_{2m}, X, Y). \tag{7}$$

In the most general case, the circuits corresponding to both the verifier and the provers may contain any kind of physically realisable operations. However such circuits may be efficiently simulated by quantum circuits consisting only of unitary operations followed by a single measurement [1]. Furthermore, by considering higher dimensional Hilbert spaces, we may assume that the state shared by the provers is pure.

Classical entangled games may be cast as a subclass of quantum entangled games: Each verifier circuit consists of a measurement of the communication registers com_X and com_Y in the computational basis, followed by the application of a permutation of the basis states. The formulation of classical entangled two-prover non-local games in terms of predicates is more natural, and allow us to define the value of the entangled game by a closed formula, which is completely circuit independent. Nevertheless the reformulation of classical entangled games as a special case of quantum entangled games is more suitable for the goals of this paper. In particular, the proof of Theorem 2 turns out to be much simpler in this setting.

Definition 2 (Quantum (Classical) Entangled Multiprover Interactive Proof Systems). *A language L over an alphabet Σ can be decided by a k-round quantum (classical) entangled two-prover interactive proof system with completeness c and soundness s if there exists a deterministic polynomial time algorithm P that on input $x \in \Sigma^*$ constructs the description of the circuits of a quantum (classical) entangled k-round two-prover non-local game $G = (V_1, ..., V_k, V_{k+1})$, such that if $x \in L$ then $\omega_G^q \geq c$ ($\omega_G^e \geq c$) and if $x \notin L$ then $\omega_G^q \leq s$ ($\omega_G^e \leq s$).*

We denote by $QMIP^*_{c,s}[2,k]$ and $MIP^*_{c,s}[2,k]$ the classes of all languages that have a quantum, resp. classical, entangled k-round two-prover interactive proof system with completeness c and soundness s.

3 Universality of the Family of Embezzlement States

Embezzlement states were defined in [26] as follows:

$$|\mu\rangle_{2n} = \frac{1}{C}\sum_{j=1}^{2^n} \frac{1}{\sqrt{j}}|j\rangle_n|j\rangle_n \qquad C = \sqrt{\sum_{j=1}^{2^n}\frac{1}{j}}. \tag{8}$$

Let $|\psi\rangle_{2n} = \sum_{i=1}^{2^m} \alpha_i|\theta_i\rangle|\theta_i\rangle$ be a bipartite $2m$-qubit state written according to its Schmidt decomposition. Then the state $|\mu\rangle \otimes |\psi\rangle$ admits a Schmidt decomposition of the form

$$\sum_{j,i} \gamma_{j,i}|j\rangle|j\rangle|\theta_i\rangle|\theta_i\rangle \tag{9}$$

Let $\gamma_{j_1,i_1} \geq \gamma_{j_2,i_2} \geq ... \geq \gamma_{j_N,i_N}$ be the $N = 2^n$ largest coefficients of the above Schmidt decomposition. Then define the $n-th$ embezzled version of $|\psi\rangle$ to be the state

$$|E(\psi)\rangle_{2n,2m} = \sum_{r=1}^{2^n} \frac{1}{\sqrt{r}}|j_r\rangle|j_r\rangle|\theta_{i_r}\rangle|\theta_{i_r}\rangle. \tag{10}$$

We note that Alice and Bob may transform the state $|\mu\rangle_{2n}$ into the state $|E(\psi)\rangle_{2n,2m}$ by performing only local operations and without communication. First each prover prepares a local ancilla register of size m in the state $|1\rangle_m$, so that $|\mu\rangle_{2n}$ becomes $|\mu\rangle_{2n} \otimes |1\rangle_m|1\rangle_m$. Subsequently both Alice and Bob apply a unitary U that maps each basis state $|j\rangle_n|1\rangle_m$ to the basis state $|j_r\rangle_n|\theta_{i_r}\rangle_m$, thus transforming $|\mu\rangle_{2n} \otimes |1\rangle_m|1\rangle_m$ into $|E(\psi)\rangle_{2n,2m}$. Surprisingly, as stated in the next theorem, by increasing n the state $|E(\psi)\rangle_{2n,2m}$ can be made arbitrarily close to $|\mu\rangle_{2n} \otimes |\psi\rangle_{2m}$.

Theorem 1 (Embezzlement [26]). *Let* $|\psi\rangle_{2m} = \sum_{j=1}^{2^m} \alpha_i |\theta_i\rangle|\theta_i\rangle$ *be a* $2m$ *qubit bipartite state written according to its Schmidt decomposition,* ε *be such that* $0 < \varepsilon < 1$*; and* $n, m \in \mathbb{N}$ *be such that* $n \geq \frac{m}{\varepsilon}$*. Then* $(\langle\mu|_{2n} \otimes \langle\psi|_{2m})|E(\psi)\rangle_{2n,2m} \geq 1 - \varepsilon$.

To show our main theorem, we need some more notation: The trace distance between two states $|\psi\rangle$ and $|\phi\rangle$ in $\mathbb{C}^n$ is defined as $D(|\psi\rangle, |\phi\rangle) = \frac{1}{2} tr|(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|)|$ where $|A| \equiv \sqrt{A^\dagger A}$. If $\{M_i\}_{i\in\mathcal{I}}$ is a POVM with outcomes in $\mathcal{I}$ and $p_i = \langle\psi|M_i^\dagger M_i|\psi\rangle$ and $q_i = \langle\phi|M_i^\dagger M_i|\phi\rangle$ are the probability distributions induced by the measurement on $|\psi\rangle$ and $|\phi\rangle$ respectively, then $D(p_i, q_i) \leq D(|\psi\rangle, |\phi\rangle)$ where $D(p_i, q_i) = \frac{1}{2}\sum_i |p_i - q_i|$ is the classical total variance distance between the probability distributions p_i and q_i (see for example theorem 9.1 of [23] for a proof). In other words if two quantum states are close in trace distance, then any measurement performed on those states will give rise to probability distributions which are close in the classical sense. Also it can be proved that $D(|\psi\rangle, |\phi\rangle) \leq \sqrt{1 - \langle\psi|\phi\rangle^2}$ and thus if $\langle\psi|\phi\rangle \geq 1 - \varepsilon$, then $D(|\psi\rangle, |\phi\rangle) < \sqrt{2\varepsilon}$.

Next we prove our main theorem. It says that the value of a quantum strategy for a quantum entangled non-local game in which the provers share a pure state $|\psi\rangle$ on $2m$ qubits can be arbitrarily approximated by the value of a strategy in which the provers share an embezzlement state. Since classical entangled games can be regarded as a special case of quantum entangled games, Theorem 2 holds also in the classical entangled setting.

Theorem 2. *Let* $(|\psi\rangle_{2m}, X, Y)$ *be a* $2m$*-qubit quantum strategy for a* k*-round two-prover non-local game* $G(V_1, ..., V_k, V_{k+1})$*. Then for any* ε *with* $0 < \varepsilon < 1$ *there exists a* $2m(1 + 1/\varepsilon)$*-qubit strategy* $(|\mu\rangle_{2m/\varepsilon} \otimes |1\rangle_m|1\rangle_m, X', Y')$ *such that* $\omega_G^q(|\mu\rangle_{2m/\varepsilon}|1\rangle_m|1\rangle_m, X', Y') \geq \omega_G^q(|\psi\rangle_{2m}, X, Y) - \sqrt{2\varepsilon}$.

Proof. Let $(|\mu\rangle_{2m/\varepsilon} \otimes |\psi\rangle_{2m}, \overline{X}, \overline{Y})$ be a strategy for G where $|\mu\rangle_{2m/\varepsilon}$ is the embezzlement state and $\overline{X}$ and $\overline{Y}$ are obtained by tensoring each circuit in X and each circuit in Y with the identity on m/ε qubits acting on half of the qubits of $|\mu\rangle_{2m/\varepsilon}$. Then clearly $\omega_G^q(|\mu\rangle_{2m/\varepsilon} \otimes |\psi\rangle_{2m}, \overline{X}, \overline{Y}) = \omega_G^q(|\psi\rangle_{2m}, X, Y)$. By Definition 1, the interplay of the verifier's strategy with the provers's strategies, prior to the final measurement of the verifier, may be regarded as the application of a single unitary U_G to a pure state. Let $|E(\psi)\rangle_{2m/\varepsilon,2m}$ be the embezzled version of $|\psi\rangle$ as defined in Equation (10) and set $|\phi\rangle = U_G|E(\psi)\rangle_{2m/\varepsilon,2m}$ and $|\phi'\rangle = U_G|\mu\rangle_{2m/\varepsilon} \otimes |\psi\rangle$. Since by Theorem 1, $(\langle\mu|_{2m/\varepsilon,2m} \otimes \langle\psi|_{2m})|E(\psi)\rangle_{2m/\varepsilon,2m} \geq 1 - \varepsilon$, we have $\langle\phi|\phi'\rangle \geq 1 - \varepsilon$ and the trace distance $D(|\psi\rangle, |\phi\rangle) < \sqrt{2\varepsilon}$. Let $\{M_i\}_{i\in\mathcal{I}}$ be the POVM measurement made by the verifier in the end of the k-th round and let $p_i = \langle\phi|M_i^\dagger M_i|\phi\rangle$ and $q_i = \langle\phi'|M_i^\dagger M_i|\phi'\rangle$. Then $D(p_i, q_i) \leq D(|\phi\rangle, |\phi'\rangle) \leq \sqrt{2\varepsilon}$. Finally there is a unitary U such that $U \otimes U|E(\psi)\rangle_{2m/\varepsilon,2m} = |\mu\rangle_{2m/\varepsilon} \otimes |1\rangle_m|1\rangle_m$ where one of the U's acts on Alice's qubits and the other on Bob's qubits. Then the final strategy is $(|\mu\rangle_{2m/\varepsilon,2m}, X', Y')$ where $X' = U\overline{X}U^\dagger$ and $Y' = U\overline{Y}U^\dagger$. □

As pointed out in the introduction, Leung, Toner and Watrous [21] showed that there are quantum entangled games whose value is never attained by a strategy whose shared state has a constant number of qubits, and thus the limit in Equation (7) is fundamental. It is still not known whether the same situation holds for classical entangled games. Despite the fact that Theorem 2 concerns only strategies with a finite number of qubits, it is still possible to prove that the limit in Equations 6 and 7 does not change if we consider only embezzlement states. This in particular implies that the classes $QMIP^*_{c,s}[2,k]$ and $MIP^*_{c,s}[2,k]$ remain invariant if we allow the provers to share only embezzlement states. Let $QMIP^{E^*}_{c,s}[2,k]$ ($MIP^{E^*}[2,k]$) be the class of languages that can be decided by quantum (classical) entangled k-round two-prover interactive proof systems whose provers are only allowed to share embezzlement states.

Corollary 1. *For any completeness value* $c \in [0,1]$ *and any soundness value* $s < c$, $QMIP^{E^*}_{c,s}[2,k]$ *(*$MIP^{E^*}_{c,s}[2,k]$*) is equal to* $QMIP^*_{c,s}[2,k]$ *(*$MIP^*_{c,s}[2,k]$*).*

Proof. Let L be a language in $QMIP^*_{c,s}[2,k]$ ($MIP^*_{c,s}[2,k]$). It is enough to prove that for any $x \in L$ the value of the game G_x associated to x remains the same if we restrict the state shared by the provers to belong to the embezzlement family. Since the proof holds both for classical entangled and for quantum entangled games, we write simple ω_{G_x} for the value of G_x. If ω_{G_x} is reached by a strategy in which the provers share a finite dimensional state $|\psi\rangle_{2m}$, then by Theorem 2 there exist a sequence of strategies

sharing states $|\mu\rangle_{2n} \otimes |1\rangle_m |1\rangle_m$ whose value approaches ω_{G_x} as $n \to \infty$. Now suppose that there is no finite dimensional strategy whose value is ω_{G_x}, and let $\omega_2, \omega_4, ..., \omega_{2m}, ...$ be an infinite sequence where ω_{2m} is the maximum value among strategies sharing a quantum states on $2m$ qubits. Then by Theorem 2, for any two such consecutive values $\omega_{2(m-1)}$ and ω_{2m}, and for a small enough ε, there exists a strategy on $2(1+1/\varepsilon)m$ qubits whose value $\omega \geq \omega_{2m} - \sqrt{2\varepsilon}$ is between $\omega_{2(m-1)}$ and ω_{2m}. □

In Theorem 3 we state a dual of Theorem 2 which says that the circuits applied by the provers can be put into a universal form.

Theorem 3 (Universal Strategy). *For each k and each $\varepsilon > 0$ there is a universal set of k-round circuits $\{(\mathcal{X}_M, \mathcal{Y}_M)\}_{M \in \mathbb{N}}$ such that for each k-prover non-local game G and each strategy $(|\psi\rangle_{2m}, X, Y)$, there is a $M \in \mathbb{N}$ and a state $|\psi\rangle_{2m} |A\rangle_M |B\rangle_M$, such that*

$$\omega_G(|\psi\rangle_{2m} |A\rangle_M |B\rangle_M, \mathcal{X}_M, \mathcal{Y}_M) \geq \omega_G(|\psi\rangle_{2m}, X, Y) - \varepsilon.$$

Proof. Any unitary matrix acting on d qubits can be ε-approximated by a circuit with $poly(2^d, \log 1/\varepsilon)$ gates from the universal set of gates $\{CNOT, H, \pi/8\}$ [7]. By adding the $SWAP$ gate to this set, such circuits can be put into a nearest neighbor configuration, in which the $CNOT$ and $SWAP$ operate only on adjacent pair of qubits. Alice and Bob hold two registers each: one working register with $d = m + v$ qubits, where v is the size of the communication register with the verifier, and an ancilla register of size $M = k \cdot poly(2^d, \log k/\varepsilon)$ divided into k regions with equal number of qubits. Each prover regards the state of the j-th region of her/his ancilla register as a program which will determine the unitary that will be applied to her/his working register at the j-th round. More precisely, each prover applies a circuit of the form $C_M C_{M-1} ... C_1$ where each C_i is a controlled gate which applies one of the four gates $SWAP, CNOT, I \otimes H$ or $I \otimes \pi/8$ to qubits $2i (\bmod d)$ and $2i+1 (\bmod d)$ [1] of the working register depending whether the state of qubits $2i$ and $2i+1$ of the ancilla register is $|00\rangle, |01\rangle, |10\rangle$ or $|11\rangle$ respectively. For some configuration of $|A\rangle, |B\rangle$ of the ancillae registers of Alice and Bob respectively, each unitary in $\mathcal{X}_M$ (resp. $\mathcal{Y}_M$) will be ε/k-close to its corresponding unitary in X (resp. Y). Since there are k rounds and the errors accumulate additively, $\omega_G(|\psi\rangle |A\rangle |B\rangle, \mathcal{X}_M, \mathcal{Y}_M) \geq \omega(|\psi\rangle, X, Y) - \varepsilon$. □

4 Acknowledgements

The author thanks Julia Kempe and Thomas Vidick for their valuable revisions on drafts of this paper, and André Chailloux, Iordanis Kerenidis and Frédérick Magniez, for useful discussions. The author also acknowledges support by Julia Kempe's Israel Science Foundation grant and by Julia Kempe's European Research Council (ERC) Starting Grant QUCO as well as by the Wolfson Family Charitable Trust.

References

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

[2] P. K. Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72:1303–1307, 2004.

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

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

[5] Bellare, Goldreich, and Sudan. Free bits, PCPs, and nonapproximability–towards tight results. *SICOMP: SIAM Journal on Computing*, 27, 1998.

[6] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 113–131, 1988.

[7] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 486–494. Society Press, 1999.

[8] J.-Y. Cai, A. Condon, and R. J. Lipton. On bounded round multi-prover interactive proof systems. In *Prooceedings of the Structure in Complexity Theory Conference (CoCo)*, pages 45–54, 1990.

[1] For simplicity we assume that the first and last qubits of the working register are adjacent.

[9] J. Clausser, M. Horne, A. Shimony, and R. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[10] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Conference on Computational Complexity (CCC)*, pages 236–249. IEEE Computer Society, 2004.

[11] U. Feige. On the success probability of the two provers in one-round proof systems. In *Proceedings of the Structure in Complexity Theory Conference (CoCo)*, pages 116–123, 1991.

[12] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing (STOC)*, pages 733–744, 1992.

[13] J. Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001.

[14] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. In *Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC)*, pages 573–582, 2010.

[15] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 447–456, 2008.

[16] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18(2):273–307, 2009.

[17] J. Kempe, O. Regev, and B. Toner. Unique games with entangled provers are easy. *SICOMP*, 39(17):3207–3229, 2010.

[18] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. Syst. Sci*, 66(3):429–450, 2003.

[19] S. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967.

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

[21] D. Leung, B. Toner, and J. Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. Avaliable at arXiv.org eprint archive, arXiv:0804.4118v1 [quant-ph].

[22] N. D. Mermin. Quantum mysteries revisited. *American Journal of Physics*, 58:731–734, 1990.

[23] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[24] A. Peres. Incompatible results of quantum measurements. *Physical Review Letters A*, 151:107–108, 1990.

[25] N. Straumann. A simple proof of the Kochen-Specker theorem on the problem of hidden variables. *Annalen der Physik*, 19:121–127, 2009.

[26] W. van Dam and P. Hayden. Universal entanglement transformations without communication. *Phys. Rev. A*, 67(6):060302, Jun 2003.

[27] S. Wehner. Entanglement in interactive proof systems with binary answers. In *Proceedings of the 23rd Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171. Springer, 2006.