Extended nonlocal games and monogamy-of-entanglement games

Nathaniel Johnston[1,2], Rajat Mittal[3], Vincent Russo[4], and John Watrous[4,5]

[1]*Department of Mathematics and Computer Science, Mount Allison University*
[2]*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo*
[3]*Department of Computer Science and Engineering, IIT Kanpur*
[4]*Institute for Quantum Computing and School of Computer Science, University of Waterloo*
[5]*Canadian Institute for Advanced Research, Toronto*

October 8, 2015

Abstract

We study a generalization of nonlocal games—which we call *extended nonlocal games*—in which the players, Alice and Bob, initially share a tripartite quantum state with the referee. In such games, the winning conditions for Alice and Bob may depend on outcomes of measurements made by the referee, on its part of the shared quantum state, in addition to Alice and Bob's answers to randomly selected questions. Our study of this class of games was inspired by the *monogamy-of-entanglement* games introduced by Tomamichel, Fehr, Kaniewski, and Wehner, which they also generalize. We prove that a natural extension of the Navascués–Pironio–Acín hierarchy of semidefinite programs converges to the optimal commuting operator value of extended nonlocal games, and we prove two extensions of results of Tomamichel et al. concerning monogamy-of-entanglement games.

1 Introduction

Nonlocal games

The nonlocal games model—although not always so named or defined explicitly—has been studied in theoretical physics and classical complexity theory for many years. In theoretical physics, nonlocal games provide a natural framework in which Bell inequality experiments, proposed by Bell [Bel64] in 1964 and subsequently studied by Clauser, Horne, Shimoney, and Holt [CHSH69] and many others, may be framed. In classical complexity theory, nonlocal games provide a simple, abstract model through which two-prover (or general multi-prover) interactive proof systems have often been analyzed [BOGKW88, For89, BFL91, Fei91, FK94, Raz98]. These two independent lines of research were merged in the context of quantum information and computation, and the result has been an active topic of research [CHTW04, BBT05, CSUU08, DLTW08, KR10, KRT10, KKM$^+$11, JP11, BFS13, RV13, DSV13, Vid13, CM14].

Mathematically speaking, a *nonlocal game* is a cooperative game of incomplete information played by two players, conventionally named *Alice* and *Bob*. The game is run by a *referee*, who begins the game by selecting a pair of questions (x, y) at random according to a fixed probability distribution, and then sends x to Alice and y to Bob. Communication between Alice and Bob is forbidden during the game—without knowing the other player's question (or answer), Alice and

Bob must respond with answers a and b, respectively. Upon receiving these answers, the referee evaluates a predicate $V(a,b|x,y)$ that determines whether Alice and Bob win or lose the game. (More generally, the function V may take arbitrary real values that represent pay-offs for Alice and Bob.) It is assumed that Alice and Bob have complete knowledge of the function V and of the probability distribution from which the question pairs are drawn, and are free to agree before the game starts on a joint strategy.

Different classes of strategies for nonlocal games may be considered. For instance, Alice and Bob may use a *classical strategy* in which they answer *deterministically*, with a and b determined by functions of x and y, respectively, or they may make use of *randomness* (which happens not to offer any advantages over an optimally chosen deterministic strategy when their goal is to maximize their winning probability or expected pay-off). Alternatively, one may consider *quantum strategies* for Alice and Bob, where they initially share a joint quantum system, and allow their answers a and b to be determined by the outcomes of measurements on this shared system. Within this category of strategies, one may consider different sub-classifications, including strategies in which the size of the shared quantum state available to Alice and Bob is limited, or strategies in which the more conventional bipartite tensor product structure of a quantum system shared between two individuals is relaxed to the requirement that Alice and Bob make use of *commuting measurements* on a single Hilbert space.

For each type of strategy, one may speak of the *value* of a given nonlocal game with respect to that strategy type, which is the supremum value of the probability for Alice and Bob to win (or the supremum value of Alice and Bob's expected pay-off) over all strategies of the given type.

Extended nonlocal games

In this paper, we consider a generalization of nonlocal games in which the *referee also holds a quantum system*, provided to it by Alice and Bob at the start of the game. The game begins in a similar way to a nonlocal game, with the referee selecting a pair of questions (x,y) according to a fixed probability distribution and Alice and Bob responding with a pair of answers (a,b) as before. Now, however, the outcome of the game is not directly determined as the value $V(a,b|x,y)$ of a predicate or real-valued pay-off function V, but rather by the result of a measurement performed by the referee on its share of the state initially provided to it by Alice and Bob. We will assume, more specifically, that Alice and Bob's pay-off is determined by an *observable* $V(a,b|x,y) \in \mathrm{Herm}(\mathbb{C}^m)$, where m denotes the dimension of the referee's quantum system—so if Alice and Bob's response (a,b) to the question pair (x,y) leaves the referee's system in the quantum state

$$\rho_{a,b}^{x,y} \in \mathrm{D}(\mathbb{C}^m), \tag{1}$$

then their pay-off will be the real-number value

$$\left\langle V(a,b|x,y), \rho_{a,b}^{x,y} \right\rangle \tag{2}$$

(where $\langle X, Y \rangle = \mathrm{Tr}(X^*Y)$ is the standard Hilbert–Schmidt inner product on $m \times m$ matrices). If one wishes to consider that the referee makes a binary-valued decision, representing that Alice and Bob either win or lose the game, then it may be required that each $V(a,b|x,y)$ is a measurement operator corresponding to the winning outcome, so that (2) represents the probability that Alice and Bob win conditioned on (x,y) having been answered with (a,b).

It is evident that games of this form, which we call *extended nonlocal games*, include ordinary nonlocal games as a special case; ordinary nonlocal games may be expressed as extended nonlocal

games for which $m = 1$, meaning that the referee's quantum system is a trivial, one-dimensional system.

Similar to an ordinary nonlocal game, one may consider a variety of possible strategies for Alice and Bob in an extended nonlocal game. In particular, there are classes of strategies that are analogous to classical strategies, standard quantum strategies, and commuting measurement strategies. Further details on these different classes of strategies can be found later in Section 2.

Monogamy-of-entanglement games

Extended nonlocal games also generalize *monogamy-of-entanglement games*, which were introduced by Tomamichel, Fehr, Kaniewski, and Wehner [TFKW13]; this was our primary inspiration for considering extended nonlocal games. Monogamy-of-entanglement games, which also have relevance to the problem of position-based cryptography, provide a framework to conceptualize the fundamental monogamy property exhibited by entangled qubits [CKW00]. In short, this property states that for three possibly entangled qubits X, Y, and Z, that if X and Y are maximally entangled, then Z must be completely uncorrelated with X and Y, and likewise for any permutation of these three qubits. This phenomena has been studied in a number of other works [Ter01, Ter04, KW04, OV06].

A monogamy-of-entanglement game is a game played in a similar way to an extended nonlocal game, as described above. Specifically, Alice and Bob initially supply the referee with a quantum system, the referee selects a single question $x \in X$ at random, sends this question to both Alice and Bob, performs a measurement

$$\left\{ \Pi_a^x \,:\, a \in A \right\} \tag{3}$$

on its quantum system, and declares Alice and Bob winners if and only if they both respond with the same outcome $a \in A$ that the referee's measurement produced. Such a game is represented as an extended nonlocal game by taking $Y = X$ and $B = A$ and setting $V(a, a|x, x) = \Pi_a^x$ for each choice of $x \in X$ and $a \in A$, as well as $V(a, b|x, x) = 0$ for $a \neq b$. In addition one may define $V(a, b|x, y)$ arbitrarily for all $x \neq y$ and all $a, b \in A$; these matrices are irrelevant to the description of the game because the referee never asks a question pair (x, y) where $x \neq y$ in a monogamy-of-entanglement game.

Motivation and summary of results

By defining and studying extended nonlocal games we hope to identify commonalities between nonlocal games and monogamy-of-entanglement games, and to potentially gain insights on both models through this type of generalization. In addition to introducing the extended nonlocal games model and investigating some of its basic properties, we prove the following results:

1. An extension of the NPA hierarchy of semidefinite programs to extended nonlocal games.

Navascués, Pironio, and Acín [NPA07, NPA08] proved that the *commuting operator value* of a nonlocal game can be expressed through a sequence of semidefinite programs. The optimum values of the semidefinite programs in this sequence are nonincreasing, each establishes an upper-bound on the value of the given game, and the sequence of optimum values necessarily converges to the true commuting operator value of the game. By extending this method, we describe a sequence of semidefinite programs, for a given extended nonlocal game, that upper-bounds and converges to the commuting operator value of the extended nonlocal game in a similar way.

2. Results on monogamy-of-entanglement games with two questions.

We prove two facts about monogamy-of-entanglement games for the case in which the question set X contains just two elements that extend results of Tomamichel, Fehr, Kaniewski, and Wehner. First, we prove that Alice and Bob can always achieve the quantum value of such a game by using a strategy that does not require them to store quantum information: they provide the referee with a chosen state at the start of the game, but act classically thereafter. We also provide an example of a monogamy-of-entanglement game, in which the question set X has 4 elements and the answer set A has 3 elements, for which Alice and Bob must store quantum information to play optimally, implying that this result on two-question monogamy-of-entanglement games does not generalize to larger question sets. Second, we prove that a bound of Tomamichel, Fehr, Kaniewski, and Wehner concerning parallel repetition of monogamy-of-entanglement games defined by projective measurements is tight for two-question games, implying a strong parallel repetition property for such games.

Organization of the paper

In Section 2 we formally introduce the extended nonlocal game model, and consider the types of strategies that Alice and Bob may use. In Section 3, we present our extension of the NPA hierarchy, that allows us to place upper bounds on the quantum value of extended nonlocal games. In Section 4, we consider the class of monogamy-of-entanglement-games and prove some results on monogamy-of-entanglement-games with two questions. Finally, in Section 5, we conclude with some open problems.

2 Extended nonlocal games

As was summarized in the introduction, an *extended-nonlocal game* G is defined by a pair (π, V), where π is a probability distribution of the form

$$\pi : X \times Y \to [0,1] \tag{4}$$

on the Cartesian product of two finite and nonempty sets X and Y, and V is a function of the form

$$V : A \times B \times X \times Y \to \mathrm{Herm}(\mathbb{C}^m), \tag{5}$$

for X and Y as above, A and B being finite and nonempty sets, and m being a positive integer. The sets X and Y represent sets of questions asked to Alice and Bob, A and B represent Alice and Bob's sets of answers, and m represents the size of the quantum system initially provided to the referee by Alice and Bob. We write $\mathcal{R} = \mathbb{C}^m$ to denote its corresponding complex vector space for convenience.

As a result of Alice and Bob responding to the question pair (x, y) with the answer pair (a, b), the referee's quantum system will be left in a quantum state

$$\rho_{a,b}^{x,y} \in \mathrm{D}(\mathcal{R}), \tag{6}$$

which is an $m \times m$ density operator. The pay-off for Alice and Bob in this situation is given by the real number

$$\left\langle V(a,b|x,y), \rho_{a,b}^{x,y} \right\rangle. \tag{7}$$

Standard quantum strategies

As suggested in the introduction, there are multiple classes of strategies that may be considered for extended nonlocal games. We will begin with *standard quantum strategies*, which represent what is arguably the most natural form of quantum strategy for the players Alice and Bob in an extended nonlocal game. A strategy of this form consists of finite-dimensional complex Hilbert spaces $\mathcal{A}$ and $\mathcal{B}$ for Alice and Bob, respectively, a quantum state $\rho \in \mathrm{D}(\mathcal{R} \otimes \mathcal{A} \otimes \mathcal{B})$, and two collections of measurements,

$$\big\{ A_a^x \,:\, a \in A \big\} \subset \mathrm{Pos}(\mathcal{A}) \quad \text{and} \quad \big\{ B_b^y \,:\, b \in B \big\} \subset \mathrm{Pos}(\mathcal{B}), \tag{8}$$

for each $x \in X$ and $y \in Y$, respectively. That is, one has that

$$\sum_{a \in A} A_a^x = \mathbb{1}_{\mathcal{A}} \quad \text{and} \quad \sum_{b \in B} B_b^y = \mathbb{1}_{\mathcal{B}} \tag{9}$$

for each $x \in X$ and $y \in Y$.

When the game is played, Alice and Bob present the referee with a quantum system so that the three parties share the state ρ. The referee chooses $(x, y) \in X \times Y$ at random, according to the probability distribution π, and sends x to Alice and y to Bob. Alice measures her portion of ρ with respect to the measurement $\{A_a^x : a \in A\}$, and sends the result $a \in A$ of this measurement to the referee. Bob does likewise, sending the outcome $b \in B$ of the measurement $\{B_b^y : b \in B\}$ to the referee. Finally, the referee measures its quantum system and assigns a pay-off, as specified by the observable $V(a, b|x, y)$. The expected pay-off for such a strategy in the game $G = (\pi, V)$ is given by

$$\sum_{(x,y) \in X \times Y} \pi(x, y) \sum_{(a,b) \in A \times B} \Big\langle V(a, b|x, y) \otimes A_a^x \otimes B_b^y, \rho \Big\rangle. \tag{10}$$

It is a simple consequence of Naimark's theorem that any strategy for Alice and Bob that makes use of non-projective measurements can be simulated by a projective measurement strategy, so there is no loss of generality in restricting one's attention to projective measurements $\{A_a^x : a \in A\}$ and $\{B_b^y : b \in B\}$ for Alice and Bob.

When analyzing a strategy for Alice and Bob as described above, it is convenient to define a function $K : A \times B \times X \times Y \to \mathrm{Pos}(\mathcal{R})$ as

$$K(a, b|x, y) = \mathrm{Tr}_{\mathcal{A} \otimes \mathcal{B}} \Big(\big(\mathbb{1}_{\mathcal{R}} \otimes A_a^x \otimes B_b^y \big) \rho \Big) \tag{11}$$

for each $x \in X$, $y \in Y$, $a \in A$, and $b \in B$. The operators output by this function represent the *unnormalized* states of the referee's quantum system when Alice and Bob respond to the question pair (x, y) with the answer pair (a, b). In particular, one has that $\mathrm{Tr}(K(a, b|x, y))$ is the probability with which Alice and Bob answer (a, b) for the question pair (x, y), and normalizing this operator (assuming it is nonzero) yields the state

$$\rho_{a,b}^{x,y} = \frac{K(a, b|x, y)}{\mathrm{Tr}(K(a, b|x, y))} \tag{12}$$

of the referee's system conditioned on this question and answer pair. Note that the function K, which we will refer to as a *quantum correlation function*, completely determines the performance of Alice and Bob's strategy for G. In particular, Alice and Bob's expected pay-off is represented as

$$\sum_{(x,y) \in X \times Y} \pi(x, y) \sum_{(a,b) \in A \times B} \Big\langle V(a, b|x, y), K(a, b|x, y) \Big\rangle. \tag{13}$$

For a given extended nonlocal game $G = (\pi, V)$, we write $\omega^*(G)$ to denote the *quantum value* of G, which is the supremum value of Alice and Bob's expected pay-off over all standard quantum strategies for G.

Unentangled strategies

Next we consider a much more restricted form of strategy called an *unentangled strategy*. These are standard quantum strategies for which the state $\rho \in \mathrm{D}(\mathcal{R} \otimes \mathcal{A} \otimes \mathcal{B})$ initially prepared by Alice and Bob is fully separable, meaning that it takes the form

$$\rho = \sum_{j=1}^{N} p_j \, \rho_j^{\mathsf{R}} \otimes \rho_j^{\mathsf{A}} \otimes \rho_j^{\mathsf{B}} \tag{14}$$

for a probability vector $(p_1, \ldots, p_N)$ and density operators

$$\rho_1^{\mathsf{R}}, \ldots, \rho_N^{\mathsf{R}} \in \mathrm{D}(\mathcal{R}), \quad \rho_1^{\mathsf{A}}, \ldots, \rho_N^{\mathsf{A}} \in \mathrm{D}(\mathcal{A}), \quad \text{and} \quad \rho_1^{\mathsf{B}}, \ldots, \rho_N^{\mathsf{B}} \in \mathrm{D}(\mathcal{B}). \tag{15}$$

One may prove that any unentangled strategy is equivalent to one in which Alice and Bob store only classical information once the referee's quantum system has been provided to it. Indeed, any such strategy is equivalent to one given by a convex combination of *deterministic strategies*, in which Alice and Bob initially provide the referee with a fixed pure state $\rho = uu^* \in \mathrm{D}(\mathcal{R})$, and respond to questions deterministically, with Alice responding to $x \in X$ with $a = f(x)$ and Bob responding to $y \in Y$ with $b = g(y)$ for functions $f : X \to A$ and $g : Y \to B$.

For a given game $G = (\pi, V)$, we write $\omega(G)$ to denote the *unentangled value* of G, which is the supremum value for Alice and Bob's expected pay-off in G over all unentangled strategies. It follows by convexity that this supremum value is necessarily achieved by some deterministic strategy, and can be represented as

$$\omega(G) = \max_{f,g} \left\| \sum_{(x,y) \in X \times Y} \pi(x,y) V\big(f(x), g(y) | x, y\big) \right\| \tag{16}$$

where the maximum is over all functions $f : X \to A$ and $g : Y \to B$.

Commuting operator strategies

The last type of strategy we consider for Alice and Bob in an extended nonlocal game is a *commuting operator strategy*, which is a (potentially) more general type of strategy than a standard quantum strategy. A commuting operator strategy is similar to a standard quantum strategy, except now the bipartite tensor product space $\mathcal{A} \otimes B$ shared by Alice and Bob is replaced by a single (possibly infinite-dimensional) Hilbert space $\mathcal{H}$. Alice and Bob initially prepare a quantum state

$$\rho \in \mathrm{D}(\mathcal{R} \otimes \mathcal{H}) \tag{17}$$

and give to the referee its portion of this state. Alice and Bob's measurements on $\mathcal{A}$ and $\mathcal{B}$ are replaced by measurements on the space $\mathcal{H}$, so that

$$\big\{ A_a^x \,:\, x \in X,\, a \in A \big\} \quad \text{and} \quad \big\{ B_b^y \,:\, y \in Y,\, b \in B \big\} \tag{18}$$

are collections of positive semidefinite operators on $\mathcal{H}$, representing measurements for each choice of $x \in X$ and $y \in Y$. It is required that each of Alice's measurements commutes with each of Bob's measurements, meaning that

$$\big[A_a^x, B_b^y \big] = 0 \tag{19}$$

for all $x \in X$, $y \in Y$, $a \in A$, and $b \in B$. Similar to standard quantum strategies, there is no generality lost in considering only projective measurements for Alice and Bob.

The expected pay-off for a commuting operator strategy, as just described, in an extended nonlocal game $G = (\pi, V)$, is given by

$$\sum_{(x,y)\in X\times Y} \pi(x,y) \sum_{(a,b)\in A\times B} \big\langle V(a,b|x,y) \otimes A_a^x B_b^y, \rho \big\rangle. \tag{20}$$

The *commuting operator value* of G, which is denoted $\omega_c(G)$, is the supremum value of the expected pay-off of G taken over all commuting operator strategies for Alice and Bob.

Along similar lines to standard quantum strategies, a commuting operator strategy as above defines a function $K : A \times B \times X \times Y \to \mathrm{Pos}(\mathcal{R})$ as

$$K(a,b|x,y) = \mathrm{Tr}_{\mathcal{H}}\Big(\big(\mathbb{1}_{\mathcal{R}} \otimes A_a^x B_b^y\big)\rho \Big) \tag{21}$$

for each $x \in X$, $y \in Y$, $a \in A$, and $b \in B$. Any such function will be called a *commuting operator correlation function*. We do not know whether every commuting operator correlation function K is also a quantum correlation function, realized in a similar way by a standard quantum strategy.

3 The NPA hierarchy for extended nonlocal games

In this section we describe how the semidefinite programming hierarchy of Navascués, Pironio, and Acín [NPA07, NPA08] may be generalized to extended nonlocal games. We will begin by describing the construction of the hierarchy, and then prove that the hierarchy converges to the commuting operator value of an extended nonlocal game.

Construction of the extended NPA hierarchy

Assume that finite and nonempty question and answer sets X, Y, A, and B, as well as a positive integer m representing the dimension of the referee's quantum system, have been fixed. We first introduce three alphabets:

$$\Sigma_A = X \times A, \quad \Sigma_B = Y \times B, \quad \text{and} \quad \Sigma = \Sigma_A \cup \Sigma_B. \tag{22}$$

Here, $\cup$ denotes the disjoint union, meaning that Σ_A and Σ_B are to be treated as disjoint sets when forming Σ. For every nonnegative integer k, we will write $\Sigma^{\leq k}$ to denote the set of strings over the alphabet Σ having length at most k, we write Σ^* to denote the set of all strings (of finite length) over Σ, and we write ε to denote the empty string.

Next, define $\sim$ to be the equivalence relation on Σ^* generated by the following rules:

1. $s\sigma t \sim s\sigma\sigma t$ (for every $s, t \in \Sigma^*$ and $\sigma \in \Sigma$).
2. $s\sigma\tau t \sim s\tau\sigma t$ (for every $s, t \in \Sigma^*$, $\sigma \in \Sigma_A$, and $\tau \in \Sigma_B$).

That is, two strings are equivalent with respect to the relation $\sim$ if and only if one can be obtained from the other by a finite number of applications of the above rules.

Now, a function of the form

$$\phi : \Sigma^* \to \mathbb{C} \tag{23}$$

will be said to be *admissible* if and only if the following conditions are satisfied:

1. For every choice of strings $s, t \in \Sigma^*$ it holds that

$$\sum_{a \in A} \phi(s(x,a)t) = \phi(st) \quad \text{and} \quad \sum_{b \in B} \phi(s(y,b)t) = \phi(st) \tag{24}$$

   for every $x \in X$ and $y \in Y$.

2. For every choice of strings $s, t \in \Sigma^*$, it holds that

$$\phi(s(x,a)(x,a')t) = 0 \quad \text{and} \quad \phi(s(y,b)(y,b')t) = 0 \tag{25}$$

   for every choice of $x \in X$ and $a, a' \in A$ satisfying $a \neq a'$, and every choice of $y \in Y$ and $b, b' \in B$ satisfying $b \neq b'$, respectively.

3. For all strings $s, t \in \Sigma^*$ satisfying $s \sim t$ it holds that $\phi(s) = \phi(t)$.

Along similar lines, a function of the form

$$\phi : \Sigma^{\leq k} \to \mathbb{C} \tag{26}$$

is said to be *admissible* if and only if the same conditions listed above hold, provided that s and t are sufficiently short so that ϕ is defined on the arguments indicated within each condition.

Finally, for each positive integer k (representing a level of approximation in the hierarchy to be constructed), we consider the set of all block matrices of the form

$$M^{(k)} = \begin{pmatrix} M_{1,1}^{(k)} & \cdots & M_{1,m}^{(k)} \\ \vdots & \ddots & \vdots \\ M_{m,1}^{(k)} & \cdots & M_{m,m}^{(k)} \end{pmatrix}, \tag{27}$$

where each of the blocks takes the form

$$M_{i,j}^{(k)} : \Sigma^{\leq k} \times \Sigma^{\leq k} \to \mathbb{C}, \tag{28}$$

and for which the following conditions are satisfied:

1. For every choice of $i, j \in \{1, \ldots, m\}$, there exists an admissible function

$$\phi_{i,j} : \Sigma^{\leq 2k} \to \mathbb{C} \tag{29}$$

   such that

$$M_{i,j}^{(k)}(s,t) = \phi_{i,j}(s^R t) \tag{30}$$

   for every choice of strings $s, t \in \Sigma^{\leq k}$. (Here, the notation s^R means the *reverse* of the string s.)

2. It holds that

$$M_{1,1}^{(k)}(\varepsilon,\varepsilon) + \cdots + M_{m,m}^{(k)}(\varepsilon,\varepsilon) = 1. \tag{31}$$

3. The matrix $M^{(k)}$ is positive semidefinite.

Matrices of the form (27) obeying the listed constraints will be called *k-th order admissible matrices*. For such a matrix, we write $M^{(k)}(s,t)$ to denote the $m \times m$ complex matrix

$$M^{(k)}(s,t) = \begin{pmatrix} M_{1,1}^{(k)}(s,t) & \cdots & M_{1,m}^{(k)}(s,t) \\ \vdots & \ddots & \vdots \\ M_{m,1}^{(k)}(s,t) & \cdots & M_{m,m}^{(k)}(s,t) \end{pmatrix}, \tag{32}$$

for each choice of strings $s, t \in \Sigma^{\leq k}$. With respect to this notation, the second and third conditions on $M^{(k)}$ imply that $M^{(k)}(\varepsilon, \varepsilon)$ is an $m \times m$ density matrix.

We observe that an optimization over all k-th order admissible matrices can be represented by a semidefinite program: a matrix of the form (27) is a k-th order admissible matrix if and only if it is positive semidefinite and satisfies a finite number of linear constraints imposed by the first two conditions on $M^{(k)}$. In particular, for an extended nonlocal game $G = (\pi, V)$, where π is a distribution over $X \times Y$ and V is a function $V : A \times B \times X \times Y \to \mathrm{Herm}(\mathbb{C}^m)$, one may consider the maximization of the quantity

$$\sum_{x,y,a,b} \pi(x,y) \Big\langle V(a,b|x,y), M^{(k)}((x,a),(y,b)) \Big\rangle \tag{33}$$

subject to $M^{(k)}$ being a k-th order admissible matrix.

We also note that the hierarchy of Navascués, Pironio, and Acín corresponds precisely to the $m = 1$ case of the hierarchy just described.

Convergence of the extended NPA hierarchy

Now, for a fixed choice of sets X, Y, A, and B, as well as positive integers m and k, let us consider the set of all functions of the form

$$K : A \times B \times X \times Y \to \mathrm{L}(\mathbb{C}^m) \tag{34}$$

for which there exists a k-th order admissible matrix $M^{(k)}$ that satisfies

$$K(a,b|x,y) = M^{(k)}((x,a),(y,b)) \tag{35}$$

for every $x \in X$, $y \in Y$, $a \in A$, and $b \in B$. The set of all such functions will be called *k-th order pseudo-correlation functions*.

Theorem 3.1. *Let X, Y, A, and B be finite sets, let m be a positive integer, and let*

$$K : A \times B \times X \times Y \to \mathrm{L}(\mathbb{C}^m) \tag{36}$$

be a function. The following statements are equivalent:

1. *The function K is a commuting operator correlation function.*
2. *The function K is a k-th order pseudo-correlation function for every positive integer k.*

Proof. The simpler implication is that statement 1 implies statement 2. Under the assumption that statement 1 holds, it must be that K is defined by a strategy in which Alice and Bob use projective measurements, $\{A_a^x : a \in A\}$ for Alice and $\{B_b^y : b \in B\}$ for Bob, on a shared Hilbert space $\mathcal{H}$, along with a pure state $u \in \mathcal{R} \otimes \mathcal{H}$. Let $u_1, \ldots, u_m \in \mathcal{H}$ be vectors for which

$$u = \sum_{j=1}^{m} e_j \otimes u_j. \tag{37}$$

Also let Π_c^z denote A_c^z if $z \in X$ and $c \in A$, or B_c^z if $z \in Y$ and $c \in B$. With respect to this notation, one may consider the k-th order admissible matrix $M^{(k)}$ defined by

$$M_{i,j}^{(k)}(s,t) = \phi_{i,j}(s^R t), \tag{38}$$

where the functions $\{\phi_{i,j}\}$ are defined as

$$\phi_{i,j}\big((z_1,c_1)\cdots(z_\ell,c_\ell)\big) = u_i^* \Pi_{c_1}^{z_1} \cdots \Pi_{c_\ell}^{z_\ell} u_j \tag{39}$$

for every string $(z_1,c_1)\cdots(z_\ell,c_\ell) \in \Sigma^{\leq 2k}$. A verification reveals that this matrix is consistent with K, and therefore K is a k-th order pseudo-correlation function.

The more difficult implication is that statement 2 implies statement 1. The basic methodology of the proof is similar to the $m = 1$ case proved in [NPA08], and we will refer to arguments made in that paper when they extend to the general case. For every positive integer k, let $M^{(k)}$ be a k-th order admissible matrix satisfying $K(a,b|x,y) = M^{(k)}((x,a),(y,b))$ for every $x \in X$, $y \in Y$, $a \in A$, and $b \in B$.

First, one may observe that for every choice of $k \geq 1$, it holds that

$$\left|M_{i,j}^{(k)}(s,t)\right| \leq 1 \tag{40}$$

for every choice of $i,j \in \{1,\ldots,m\}$ and $s,t \in \Sigma^{\leq k}$. To see that this is so, observe first that

$$\left|M_{i,j}^{(k)}(s,t)\right| \leq \sqrt{M_{i,i}^{(k)}(s,s)}\sqrt{M_{j,j}^{(k)}(t,t)} \tag{41}$$

for each $i,j \in \{1,\ldots,m\}$ and $s,t \in \Sigma^*$, which is a consequence of the fact that each 2×2 submatrix

$$\begin{pmatrix} M_{i,i}^{(k)}(s,s) & M_{i,j}^{(k)}(s,t) \\ M_{j,i}^{(k)}(t,s) & M_{j,j}^{(k)}(t,t) \end{pmatrix} \tag{42}$$

of $M^{(k)}$ is positive semidefinite. It therefore suffices to prove that

$$M_{i,i}^{(k)}(s,s) \leq 1 \tag{43}$$

for every $i \in \{1,\ldots,m\}$ and $s \in \Sigma^{\leq k}$. The bound (43) may be proved by induction on the length of s. For the base case, one has that $M_{i,i}^{(k)}(\varepsilon,\varepsilon) \leq 1$ by the constraint (31), along with the fact that the diagonal entries of $M^{(k)}$ are nonnegative. For the general case, one has that for any string $t \in \Sigma^*$ and any choice of $(z,c) \in \Sigma$, it holds that

$$\begin{aligned} M_{i,i}^{(k)}((z,c)t,(z,c)t) &\leq \sum_d M_{i,i}^{(k)}((z,d)t,(z,d)t) = \sum_d \phi_{i,i}^{(k)}(t^R(z,d)(z,d)t) \\ &= \sum_d \phi_{i,i}^{(k)}(t^R(z,d)t) = \phi_{i,i}^{(k)}(t^R t) = M_{i,i}^{(k)}(t,t), \end{aligned} \tag{44}$$

where the sums are over all $d \in A$ or $d \in B$ depending on whether $z \in X$ or $z \in Y$, respectively. By the hypothesis of induction the required bound (43) follows.

Next, reasoning in the same way as [NPA08] through the use of the Banach–Alaoglu theorem, one finds that there must exist an infinite matrix of the form

$$M = \begin{pmatrix} M_{1,1} & \cdots & M_{1,m} \\ \vdots & \ddots & \vdots \\ M_{m,1} & \cdots & M_{m,m} \end{pmatrix}, \tag{45}$$

where

$$M_{i,j} : \Sigma^* \times \Sigma^* \to \mathbb{C} \tag{46}$$

for each $i, j \in \{1, \ldots, m\}$, satisfying similar constraints to the finite matrices $M^{(k)}$. In particular, it must hold that

$$M_{i,j}(s,t) = \phi_{i,j}(s^R t) \tag{47}$$

for a collection of admissible functions $\{\phi_{i,j}\}$ taking the form

$$\phi_{i,j} : \Sigma^* \to \mathbb{C}, \tag{48}$$

it must hold that all finite submatrices of M are positive semidefinite, and it must hold that $M_{1,1}(\varepsilon,\varepsilon) + \cdots + M_{m,m}(\varepsilon,\varepsilon) = 1$. Consequently, there must exist a collection of vectors

$$\big\{u_{i,s} \,:\, i \in \{1,\ldots,m\},\ s \in \Sigma^*\big\} \subset \mathcal{H} \tag{49}$$

chosen from a (separable) Hilbert space $\mathcal{H}$ for which it holds that

$$M_{i,j}(s,t) = \big\langle u_{i,s}, u_{j,t} \big\rangle \tag{50}$$

for every choice of $i, j \in \{1, \ldots, m\}$ and $s, t \in \Sigma^*$. Furthermore, it must hold that

$$K(a,b|x,y) = M((x,a),(y,b)) \tag{51}$$

where, as for the matrices $M^{(k)}$, we write

$$M(s,t) = \begin{pmatrix} M_{1,1}(s,t) & \cdots & M_{1,m}(s,t) \\ \vdots & \ddots & \vdots \\ M_{m,1}(s,t) & \cdots & M_{m,m}(s,t) \end{pmatrix} \tag{52}$$

for each $s, t \in \Sigma^*$. There is no loss of generality in assuming $\mathcal{H}$ is spanned by the vectors (49), for otherwise $\mathcal{H}$ can simply be replaced by the (possibly finite-dimensional) subspace spanned by these vectors.

Now we will define a commuting operator strategy for Alice and Bob certifying that K is a commuting operator correlation function. The state initially prepared by Alice an Bob, and shared with the referee, will be the pure state corresponding to the vector

$$u = \sum_{j=1}^{m} e_j \otimes u_{j,\varepsilon} \in \mathbb{C}^m \otimes \mathcal{H}. \tag{53}$$

This is a unit vector, as a calculation reveals:

$$\|u\|^2 = \sum_{j=1}^{m} \langle u_{j,\varepsilon}, u_{j,\varepsilon} \rangle = M_{1,1}(\varepsilon,\varepsilon) + \cdots + M_{m,m}(\varepsilon,\varepsilon) = 1. \tag{54}$$

Next we define projective measurements on $\mathcal{H}$ for Alice and Bob. For each $(z,c) \in \Sigma$, define Π_c^z to be the projection operator onto the span of the set

$$\big\{u_{j,(z,c)s} \,:\, j \in \{1,\ldots,m\},\ s \in \Sigma^*\big\}. \tag{55}$$

It must, of course, be proved that these projections do indeed form projective measurements, and that Alice's measurements commute with Bob's. Toward these goals, consider any choice of $i, j \in \{1, \ldots, m\}$, $s, t \in \Sigma^*$, and $(z,c) \in \Sigma$, and observe that

$$\begin{aligned} \big\langle u_{i,(z,c)t}, u_{j,s} \big\rangle &= M_{i,j}((z,c)t, s) = \phi_{i,j}(t^R(z,c)s) \\ &= \phi_{i,j}(t^R(z,c)(z,c)s) = M_{i,j}((z,c)t,(z,c)s) = \big\langle u_{i,(z,c)t}, u_{j,(z,c)s} \big\rangle. \end{aligned} \tag{56}$$

It follows that $u_{j,s}$ and $u_{j,(z,c)s}$ have the same inner product with every vector in the image of Π_c^z. As every vector in the orthogonal complement of the image of Π_c^z is obviously orthogonal to $u_{j,(z,c)s}$, as this vector is contained in the image of Π_c^z, it follows that

$$\Pi_c^z u_{j,s} = u_{j,(z,c)s}. \tag{57}$$

This formula greatly simplifies the required verifications. For instance, one has

$$\big\langle u_{i,(z,c)t}, u_{j,(z,d)s} \big\rangle = M_{i,j}((z,c)t,(z,d)s) = \phi_{i,j}(t^R(z,c)(z,d)s) = 0 \tag{58}$$

for all $i,j \in \{1,\ldots,m\}$, $s,t \in \Sigma^*$, and $(z,c),(z,d) \in \Sigma$ for which $c \neq d$, and therefore $\Pi_c^z \Pi_d^z = 0$ whenever $(z,c),(z,d) \in \Sigma$ satisfy $c \neq d$. For each $x \in X$, and each $i,j \in \{1,\ldots,m\}$ and $s,t \in \Sigma^*$, it holds that

$$\sum_{a\in A} \big\langle u_{i,s}, \Pi_a^x u_{j,t} \big\rangle = \sum_{a\in A} \big\langle u_{i,s}, u_{j,(x,a)t} \big\rangle = \sum_{a\in A} \phi_{i,j}(s^R(x,a)t) = \phi_{i,j}(s^R t) = \big\langle u_{i,s}, u_{j,t} \big\rangle \tag{59}$$

and therefore

$$\sum_{a\in A} \Pi_a^x = \mathbb{1}, \tag{60}$$

for each $x \in X$, and along similar lines one finds that

$$\sum_{b\in B} \Pi_b^y = \mathbb{1} \tag{61}$$

for each $y \in Y$. Finally, for every $i,j \in \{1,\ldots,m\}$, $s,t \in \Sigma^*$, $(x,a) \in \Sigma_A$, and $(y,b) \in \Sigma_B$ we have

$$\begin{aligned} \Big\langle u_{i,s}, \Pi_a^x \Pi_b^y u_{j,t} \Big\rangle &= \big\langle u_{i,(x,a)s}, u_{j,(y,b)t} \big\rangle = \phi_{i,j}\big(s^R(x,a)(y,b)t\big) \\ &= \phi_{i,j}\big(s^R(y,b)(x,a)t\big) = \big\langle u_{i,(y,b)s}, u_{j,(x,a)t} \big\rangle = \big\langle u_{i,s}, \Pi_b^y \Pi_a^x u_{j,t} \big\rangle, \end{aligned} \tag{62}$$

and therefore $\big[\Pi_a^x, \Pi_b^y\big] = 0$.

It remains to observe that the strategy represented by the pure state u and the projective measurements $\{\Pi_a^x\}$ and $\{\Pi_b^y\}$ yields the commuting operator correlation function K. This is also evident from the equation (57), as one has

$$M_{i,j}((x,a),(y,b)) = \big\langle u_{i,(x,a)}, u_{j,(y,b)} \big\rangle = \Big\langle \Pi_a^x \Pi_b^y, u_{j,\varepsilon} u_{i,\varepsilon}^* \Big\rangle, \tag{63}$$

and therefore

$$K(a,b|x,y) = \mathrm{Tr}_{\mathcal{H}}\Big(\big(\mathbb{1} \otimes \Pi_a^x \Pi_b^y\big) uu^* \Big) \tag{64}$$

for every choice of $x \in X$, $y \in Y$, $a \in A$, and $b \in B$. □

4 Monogamy-of-entanglement games

As suggested in the introduction, a monogamy-of-entanglement game is specified by a pair $G = (\pi, R)$ where $\pi : X \to [0,1]$ is a probability vector defined over a finite, nonempty set X and R is a function of the form $R : A \times X \to \mathrm{Pos}(\mathbb{C}^m)$ satisfying

$$\sum_{a\in A} R(a|x) = \mathbb{1} \tag{65}$$

for every $x \in X$, where A is a finite and nonempty set. The function R specifies a collection of measurements, one for each choice of $x \in X$, each having outcomes in A.

Recall that in a monogamy-of-entanglement game, Alice and Bob prepare a state, and then share it with the referee. The referee randomly selects a single question $x \in X$, performs a measurement on its portion of the state with an operator $R(a|x)$, and then sends x to both Alice and Bob. The game is won if and only if the responses that Alice and Bob give agree with the outcome of the referee's measurement.

Because Alice and Bob only win when their output is the same, the optimal winning probability for an entangled strategy making use of a specific choice of measurements $\{A_a^x\}$ and $\{B_b^y\}$ for Alice and Bob is given by

$$\left\| \sum_{x \in X} \pi(x) \sum_{a \in A} R(a|x) \otimes A_a^x \otimes B_a^x \right\|. \tag{66}$$

The unentangled value of a monogamy-of-entanglement game may be expressed as

$$\omega(G) = \max_{f : X \to A} \left\| \sum_{x \in X} \pi(x) R(f(x)|x) \right\|. \tag{67}$$

As an example of a monogamy-of-entanglement game, we consider the BB84 monogamy game, which was also introduced in [TFKW13].

Example 4.1 (BB84 monogamy game)**.** Let $m = 2$, let $X = A = \{0, 1\}$, and define

$$R(0|0) = |0\rangle\langle 0|, \quad R(1|0) = |1\rangle\langle 1|, \quad R(0|1) = |+\rangle\langle +|, \quad \text{and} \quad R(1|1) = |-\rangle\langle -|. \tag{68}$$

Also define $\pi(0) = \pi(1) = 1/2$, and define the BB84 monogamy-of-entanglement game $G_{\mathsf{BB84}} = (\pi, R)$. It was observed in [TFKW13] that

$$\omega(G_{\mathsf{BB84}}) = \omega^*(G_{\mathsf{BB84}}) = \cos^2(\pi/8). \tag{69}$$

Entangled versus unentangled strategies for monogamy-of-entanglement games

The phenomenon that entanglement does not help in the BB84 monogamy-of-entanglement game is not limited to that game. We show that for any monogamy-of-entanglement game G for which $|X| = 2$, it must hold that $\omega(G) = \omega^*(G)$.

Theorem 4.1. *Let G be any monogamy-of-entanglement game for which it holds that the question set X satisfies $|X| = 2$. It holds that*

$$\omega(G) = \omega^*(G). \tag{70}$$

Proof. It is evident that $\omega(G) \leq \omega^*(G)$, as this is so for every monogamy-of-entanglement game, so it remains to prove the reverse inequality.

Assume without loss of generality that $X = \{0, 1\}$, assume that $G = (\pi, R)$ for $\pi(0) = \lambda$ and $\pi(1) = 1 - \lambda$. Consider any choice of projective measurements

$$\left\{A_a^0 : a \in A\right\} \quad \text{and} \quad \left\{A_a^1 : a \in A\right\} \tag{71}$$

on $\mathcal{A}$ for Alice and

$$\left\{B_a^0 : a \in A\right\} \quad \text{and} \quad \left\{B_a^1 : a \in A\right\} \tag{72}$$

on $\mathcal{B}$ for Bob. The winning probability for a strategy using these measurements is given by

$$\left\| \lambda \sum_{a \in A} R(a|0) \otimes A_a^0 \otimes B_a^0 + (1-\lambda) \sum_{a \in A} R(a|1) \otimes A_a^1 \otimes B_a^1 \right\| \tag{73}$$

for an optimal choice of the initial state. For any choice of positive semidefinite operators $P \leq Q$ it holds that $\|P\| \leq \|Q\|$, from which it follows that (73) is upper-bounded by

$$\begin{aligned} &\left\| \lambda \sum_{a \in A} R(a|0) \otimes A_a^0 \otimes \mathbb{1} + (1-\lambda) \sum_{b \in A} R(b|1) \otimes \mathbb{1} \otimes B_b^1 \right\| \\ &\qquad = \left\| \sum_{a \in A} \sum_{b \in B} \big(\lambda R(a|0) + (1-\lambda) R(b|1) \big) \otimes A_a^0 \otimes B_b^1 \right\| \\ &\qquad = \max_{a,b \in A} \big\| \lambda R(a|0) + (1-\lambda) R(b|1) \big\|. \end{aligned} \tag{74}$$

The second equality follows from the fact that $\{A_a^0 \otimes B_b^1 \,:\, a, b \in A\}$ is a collection of pairwise orthogonal projection operators. The final expression of (74) is equal to the unentangled value $\omega(G)$ of G. Because the projective measurements (71) and (72) were chosen arbitrarily, and every entangled strategy is equivalent to one in which Alice and Bob use projective measurements, it follows that $\omega^*(G) \leq \omega(G)$ as required. □

An operational interpretation of this result was suggested to us by Thomas Vidick. To convert a quantum strategy into a classical strategy, we can assign one question to each player (say 0 to Alice and 1 to Bob). Even before the referee asks the question, Alice can measure her part of the state with $\{A_a^0\}$ and Bob with $\{B_a^1\}$. They exchange their answers and then are separated. If the referee asks the question 0 (or 1) then they answer according to Alice (respectively Bob).

It turns out that monogamy-of-entanglement games for which there are more than two questions can exhibit an advantage of entangled over unentangled strategies. The following example describes such a game.

Example 4.2. Let $\zeta = e^{\frac{2\pi i}{3}}$ and consider the following four mutually unbiased bases:

$$\begin{aligned} \mathcal{B}_0 &= \{|0\rangle, |1\rangle, |2\rangle\}, \\ \mathcal{B}_1 &= \left\{ \frac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + \zeta^2|1\rangle + \zeta|2\rangle}{\sqrt{3}}, \frac{|0\rangle + \zeta|1\rangle + \zeta^2|2\rangle}{\sqrt{3}} \right\}, \\ \mathcal{B}_2 &= \left\{ \frac{|0\rangle + |1\rangle + \zeta|2\rangle}{\sqrt{3}}, \frac{|0\rangle + \zeta^2|1\rangle + \zeta^2|2\rangle}{\sqrt{3}}, \frac{|0\rangle + \zeta|1\rangle + |2\rangle}{\sqrt{3}} \right\}, \\ \mathcal{B}_3 &= \left\{ \frac{|0\rangle + |1\rangle + \zeta^2|2\rangle}{\sqrt{3}}, \frac{|0\rangle + \zeta^2|1\rangle + |2\rangle}{\sqrt{3}}, \frac{|0\rangle + \zeta|1\rangle + \zeta|2\rangle}{\sqrt{3}} \right\}. \end{aligned} \tag{75}$$

Define a monogamy-of-entanglement game $G = (\pi, R)$ so that

$$\pi(0) = \pi(1) = \pi(2) = \pi(3) = \frac{1}{4} \tag{76}$$

and R is such that

$$\big\{ R(0|x),\ R(1|x),\ R(2|x) \big\} \tag{77}$$

represents a measurement with respect to the basis $\mathcal{B}_x$, for each $x \in \{0,1,2,3\}$. An exhaustive search over all unentangled strategies reveals that

$$\omega(G) = \frac{3+\sqrt{5}}{8} \approx 0.6545, \tag{78}$$

while a computer search over quantum strategies has revealed that

$$\omega^*(G) \geq 0.660986, \tag{79}$$

which is strictly larger than the unentangled value of this game. (This strategy is available for download from the software repository [JR15].) We do not know if this strategy is optimal—the first level of the extended NPA hierarchy of Section 3 gives an upper bound of $2/3$ on the commuting operator value of this game.

Parallel repetition of monogamy-of-entanglement games

Tomamichel et al. [TFKW13] proved the following upper bound on the value of monogamy-of-entanglement games when they are repeated in parallel, under the assumption that the distribution π is uniform over the question set X. They also proved that this bound is tight for the BB84 monogamy-of-entanglement game.

Theorem 4.2 (Tomamichel, Fehr, Kaniewski, and Wehner)**.** *Let $G = (\pi, R)$ be a monogamy-of-entanglement game for which π is uniform over X, define*

$$c(G) = \max_{\substack{x,y \in X \\ x \neq y}} \max_{a,b \in A} \left\| \sqrt{R(a|x)}\sqrt{R(b|y)} \right\|^2, \tag{80}$$

and let G^n denote the game G played n times in parallel. It holds that

$$\omega^*(G^n) \leq \left(\frac{1}{|X|} + \frac{|X|-1}{|X|}\sqrt{c(G)} \right)^n. \tag{81}$$

We prove that this bound is, in fact, tight for all monogamy-of-entanglement games for which $|X| = 2$, the questions are chosen uniformly, and the referee's measurements are projective. This is a consequence of the following proposition.

Proposition 4.1. *Let $G = (\pi, R)$ be a monogamy-of-entanglement game for which $X = \{0,1\}$, π is uniform over X, and $R(a|x)$ is a projection operator for each $x \in X$ and $a \in A$. It holds that*

$$\omega(G) = \frac{1}{2} + \frac{1}{2} \max_{a,b \in A} \left\| R(a|0)\, R(b|1) \right\|. \tag{82}$$

The proof of this proposition makes use of the following lemma.

Lemma 4.1. *Let Π_0 and Π_1 be nonzero projection operators on $\mathbb{C}^n$. It holds that*

$$\|\Pi_0 + \Pi_1\| = 1 + \|\Pi_0 \Pi_1\|. \tag{83}$$

Proof. For every choice of unit vectors $u_0, u_1 \in \mathbb{C}^n$, one has the formula

$$\left\| u_0 u_0^* + u_1 u_1^* \right\| = 1 + \left| \langle u_0, u_1 \rangle \right|, \tag{84}$$

which follows from the observation that the Hermitian operator $u_0 u_0^* + u_1 u_1^*$ has (at most) two nonzero eigenvalues $1 \pm \left| \langle u_0, u_1 \rangle \right|$. Letting $\mathcal{S}$, $\mathcal{S}_0$, and $\mathcal{S}_1$ denote the unit spheres in the spaces $\mathbb{C}^n$, $\mathrm{im}(\Pi_0)$, and $\mathrm{im}(\Pi_1)$, respectively, one has

$$\begin{aligned}
\left\| \Pi_0 + \Pi_1 \right\| &= \max\Big\{ v^*(\Pi_0 + \Pi_1)v \,:\, v \in \mathcal{S} \Big\} \\
&= \max\Big\{ \|\Pi_0 v\|^2 + \|\Pi_1 v\|^2 \,:\, v \in \mathcal{S} \Big\} \\
&= \max\Big\{ \left|\langle u_0, v \rangle\right|^2 + \left|\langle u_1, v \rangle\right|^2 \,:\, v \in \mathcal{S},\, u_0 \in \mathcal{S}_0,\, u_1 \in \mathcal{S}_1 \Big\} \\
&= \max\Big\{ v^*\big(u_0 u_0^* + u_1 u_1^*\big)v \,:\, v \in \mathcal{S},\, u_0 \in \mathcal{S}_0,\, u_1 \in \mathcal{S}_1 \Big\} \\
&= \max\Big\{ \left\| u_0 u_0^* + u_1 u_1^* \right\| \,:\, u_0 \in \mathcal{S}_0,\, u_1 \in \mathcal{S}_1 \Big\} \\
&= \max\Big\{ 1 + \left|\langle u_0, u_1 \rangle\right| \,:\, u_0 \in \mathcal{S}_0,\, u_1 \in \mathcal{S}_1 \Big\} \\
&= 1 + \left\| \Pi_0 \Pi_1 \right\|,
\end{aligned} \tag{85}$$

which proves the lemma. □

Proof of Proposition 4.1. We observe that the unentangled value of G is given by

$$\omega(G) = \max_{a,b \in A} \left\| \frac{R(a|0) + R(b|1)}{2} \right\| = \frac{1}{2} + \frac{1}{2} \max_{a,b \in A} \Big\| R(a|0)\, R(b|1) \Big\| \tag{86}$$

as claimed. □

The reason that the proposition just proved implies the tightness of the bound in Theorem 4.2 for a monogamy-of-entanglement game of the type specified in Proposition 4.1 is that Alice and Bob can simply play, n times in parallel, an optimal strategy for G. This implies that

$$\omega^*(G^n) \geq \omega(G^n) \geq \left(\frac{1}{2} + \frac{1}{2} \max_{a,b \in A} \Big\| R(a|0)\, R(b|1) \Big\| \right)^n = \left(\frac{1}{2} + \frac{1}{2} \sqrt{c(G)} \right)^n, \tag{87}$$

which matches the upper-bound of Theorem 4.2.

5 Conclusion

We conclude with a few open questions.

1. We observed that a monogamy-of-entanglement game defined by a set of four mutually unbiased bases in three dimensions allows Alice and Bob to perform better if they adopt an entangled strategy instead of an unentangled strategy. This is the smallest example of a monogamy-of-entanglement game we were able to find having this property. Is there an example having fewer questions and/or answers? Under what conditions does a monogamy-of-entanglement game based on mutually unbiased bases admit an entangled over unentangled strategy advantage?

2. Is there a natural extension of Proposition 4.1 for monogamy-of-entanglement games having nonuniform distributions of questions and non-projective measurements?
3. It is an open question whether standard quantum strategies and commuting operator strategies are equivalent for nonlocal games. Does there exist an extended nonlocal game for which these two types of strategies differ?

Acknowledgments

We thank Richard Cleve, Debbie Leung, Li Liu, Matt McKague, Jamie Sikora, Marco Tomamichel, Thomas Vidick, and Elie Wolfe for helpful discussions. We acknowledge Michael Grant and Stephen Boyd for their convex optimization software CVX [GBY08]. RM is supported by the INSPIRE fellowship. He would like to thank the Institute for Quantum Computing at the University of Waterloo for its hospitality while contributing to this work. VR is supported by NSERC and the US Army Research Office. JW is supported by NSERC.

References

[BBT05] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005.

[Bel64] John Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[BFS13] Harry Buhrman, Serge Fehr, and Christian Schaffner. On the parallel repetition of multi-player games: The no-signaling case. *arXiv preprint arXiv:1312.7455*, 2013.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 113–131. ACM, 1988.

[CHSH69] John Clauser, Michael Horne, Abner Shimony, and Richard Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[CHTW04] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.

[CKW00] Valerie Coffman, Joydip Kundu, and William Wootters. Distributed entanglement. *Physical Review A*, 61(5):052306, 2000.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, volume 8572 of *Lecture Notes in Computer Science*, pages 320–331. Springer Berlin Heidelberg, 2014.

[CSUU08] Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. *Computational Complexity*, 17(2):282–299, 2008.

[DLTW08] Andrew Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *Computational Complexity, 2008. CCC'08. 23rd Annual IEEE Conference on*, pages 199–210. IEEE, 2008.

[DSV13] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. *Computational Complexity*, 24:201–254, 2013.

[Fei91] Uriel Feige. On the success probability of the two provers in one-round proof systems. In *Structure in Complexity Theory Conference, 1991., Proceedings of the Sixth Annual*, pages 116–123. IEEE, 1991.

[FK94] Uri Feige and Joe Kilian. Two prover protocols: Low error at affordable rates. In *Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing*, pages 172–183. ACM, 1994.

[For89] Lance Fortnow. *Complexity-theoretic aspects of interactive proof systems*. PhD thesis, Massachusetts Institute of Technology, 1989.

[GBY08] Michael Grant, Stephen Boyd, and Yinyu Ye. CVX: MATLAB software for disciplined convex programming, 2008.

[JP11] Marius Junge and Carlos Palazuelos. Large violation of Bell inequalities with low entanglement. *Communications in Mathematical Physics*, 306(3):695–746, 2011.

[JR15] Nathaniel Johnston and Vincent Russo. Supplementary software for implementing the examples for the extended NPA hierarchy of semidefinite programs. https://github.org/vprusso/monogamy-of-entanglement-games, 2015.

[KKM+11] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. *SIAM Journal on Computing*, 40(3):848–877, 2011.

[KR10] Julia Kempe and Oded Regev. No strong parallel repetition with entangled and non-signaling provers. In *Computational Complexity (CCC), 2010 IEEE 25th Annual Conference on*, pages 7–15. IEEE, 2010.

[KRT10] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. *SIAM Journal on Computing*, 39(7):3207–3229, 2010.

[KW04] Masato Koashi and Andreas Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69(2):022309, 2004.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Physical Review Letters*, 98:010401, 2007.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[OV06] Tobias Osborne and Frank Verstraete. General monogamy inequality for bipartite qubit entanglement. *Physical Review Letters*, 96(22):220503, 2006.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[RV13] Oded Regev and Thomas Vidick. Quantum XOR games. In *Computational Complexity (CCC), 2013 IEEE Conference on*, pages 144–155. IEEE, 2013.

[Ter01] Barbara Terhal. A family of indecomposable positive linear maps based on entangled quantum states. *Linear Algebra and its Applications*, 323(1):61–73, 2001.

[Ter04] Barbara Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1):71–78, 2004.

[TFKW13] Marco Tomamichel, Serge Fehr, Jkedrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013.

[Vid13] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 766–775. IEEE, 2013.