Characterization of Binary Constraint System Games *

Richard Cleve[1] and Rajat Mittal[2]

[1] Institute for Quantum Computing and School of Computer Science, University of Waterloo
[2] Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo

Abstract. We investigate a simple class of multi-prover interactive proof systems (classical non-local games), called *binary constraint system (BCS) games*, and characterize those that admit a perfect entangled strategy (i.e., a strategy with value 1 when the provers can use shared entanglement). Our characterization is in terms of a system of matrix equations. One application of this characterization is that, combined with a recent result of Arkhipov, it leads to a simple algorithm for determining whether certain *restricted* BCS games have a perfect entangled strategy, and, for the instances that do not, for bounding their value strictly below 1. An open question is whether, for the case of *general* BCS games, making this determination is computationally decidable. Our characterization might play a useful role in the resolution of this question.

Keywords: Quantum information, entanglement, binary constraint systems.

1 Introduction

Constraint systems and various two-player non-local games associated with them have played an important role in computational complexity theory (probabilistic interactive proof systems [7,5,12,4] and the hardness of approximation [12]) as well as quantum information (pertaining to the power of entanglement [6,8,18,9]).

We investigate the computational complexity of determining the value of a game given its description. Quantumly (when the players are allowed to possess any entangled state at the beginning), it is not even currently known that the problem is computable. This is the current state of affairs even for gapped versions of the problem, where $\varepsilon > 0$ and the goal is to distinguish between these cases: (a) the existence of a perfect strategy (i.e., with value 1); and (b) all strategies have value $\leq 1 - \varepsilon$. We refer to [9] for a detailed introduction to quantum non-local games and quantum strategies.

For a very special class of non-local games, called *XOR games*, a characterization in terms of semidefinite programs exists that makes the problem of

* Full version is available at `http://arxiv.org/abs/1209.2729`

J. Esparza et al. (Eds.): ICALP 2014, Part I, LNCS 8572, pp. 320–331, 2014.

approximating their value tractable (see [9] and references therein). Also, an XOR game has a perfect quantum strategy if and only if it has a perfect classical strategy—which can be characterized by a linear system of equations. Thus, it is easy to determine whether or not an XOR game has a perfect entangled strategy.

We consider a generalization of XOR games known as *binary constraint system (BCS)* games. For such games, even determining the existence of a perfect strategy is not currently known to be computable. We characterize perfect strategies for BCS games in terms of solutions to certain systems of equations in which the variables are binary observables (involutory matrices). The known entangled strategies for BCS games have been based on such binary observables, and our main result is to shows that *any* perfect strategy for *any* BCS game must be based on such binary observables.

A parity BCS game is a BCS game where the constraints can be expressed as parities of variables. Recently, Arkhipov [3] gave an elegant algorithm for determining if a certain restricted type of parity BCS game (where every variable appears in at most two constraints) has a perfect entangled strategy. Arkhipov's methodology uses our characterization in that it assumes that any perfect entangled strategy is based on binary observables. The methodology in [3] apparently does not generalize to unrestricted parity BCS games (without the above restriction). The problem determining whether a parity BCS game has a perfect entangled strategy is not currently known to be computable.

We also give a method that upper bounds the value of BCS games strictly below 1 in certain cases of interest (but we do not know how to do this in general).

1.1 Binary Constraint System Games

A *binary constraint system (BCS)* consists of n binary variables, $v_1, v_2, \dots, v_n$, and m constraints, $c_1, c_2, \dots, c_m$, where each c_j is a binary-valued function of a subset of the variables. For convenience, we may write the constraints as equations. An example of a BCS (with $n = 9$ and $m = 6$) is

$$\begin{aligned} v_1 \oplus v_2 \oplus v_3 &= 0 & \qquad v_1 \oplus v_4 \oplus v_7 &= 0 \\ v_4 \oplus v_5 \oplus v_6 &= 0 & \qquad v_2 \oplus v_5 \oplus v_8 &= 0 \\ v_7 \oplus v_8 \oplus v_9 &= 0 & \qquad v_3 \oplus v_6 \oplus v_9 &= 1 \end{aligned} \tag{1}$$

(this BCS is related to the version of Bell's theorem introduced by Mermin [14], that is discussed further in the next section). If, as in this example, all the constraints are functions of the parity of a subset of variables we call the system a *parity BCS*. A BCS is *satisfiable* if there exists a truth assignment to the variables that satisfies every constraint. The above example is easily seen to be unsatisfiable (since summing all the equations modulo 2 yields $0 = 1$).

We can associate a two-player non-local game with each BCS that proceeds as follows. There are two cooperating players, Alice and Bob, who cannot communicate with each other once the protocol starts, and a verifier. The verifier randomly (uniformly) selects one constraint c_s and one variable x_t from c_s. The verifier sends s to Alice and t to Bob. Alice returns a truth assignment to all variables in c_s and Bob returns a truth assignment to variable x_t. The verifier accepts the answer if and only if:

1. Alice's truth assignment *satisfies* the constraint c_s;
2. Bob's truth assignment for x_t is *consistent* with Alice's.

Strategies where Alice and Bob employ no entanglement are called *classical.* Strategies where they employ entanglement are called *quantum* (or *entangled*). A strategy is *perfect* if it always succeeds.

It is not too hard to see that there exists a perfect *classical* strategy for a BCS game if and only if the underlying BCS is satisfiable. It is interesting that there exist perfect entangled strategies for BCS games for some unsatisfiable BCSs.

1.2 Mermin's Quantum Strategies

Mermin [14,15] made a remarkable discovery about sets of observables with certain properties that has consequences for quantum strategies for BCS games[1] that are unsatisfiable—in particular the following two games. The left side of Fig. 1 summarizes the BCS specified by the aforementioned system of equations (1). We refer to this BCS as the *magic square.* Similarly, the right side of

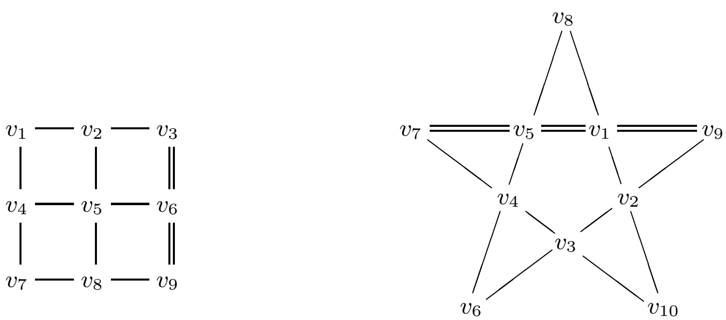

Fig. 1. Structure of two BCSs: (a) magic square (left) and (b) magic pentagram (right). Each straight line indicates a parity constraint on its variables of 0 for single lines, and 1 for double lines.

Fig. 1 summarizes another BCS consisting of ten variables and five constraints, where each constraint is related to the parity of four variables. We refer to this BCS as the *magic pentagram.*

[1] Mermin's original paper was written in the language of no-hidden-variables theorems, along the lines of the Kochen Specker Theorem; however, it discusses implications regarding Bell inequality violations, and these can be interpreted as non-local games where quantum strategies exist that outperform classical strategies. The connection is made more explicit by Aravind [1,2].

To understand Mermin's strategies, we first define a *quantum satisfying assignment* of a BCS as a relaxation of a classical satisfying assignment, in the following manner. First translate each $\{0,1\}$-variable v_j into a $\{+1,-1\}$-variable $V_j = (-1)^{v_j}$. Then the parity of any sequence of variables is their product—and, in fact, every boolean function can be uniquely represented as a multilinear polynomial over $\mathbb{R}$ (e.g., for the binary OR-function (in $\{+1,-1\}$ domain), the polynomial is $(V_1V_2 + V_1 + V_2 - 1)/2$). Now we can define a *quantum satisfying assignment* as an assignment of finite-dimensional Hermitian operators $A_1, A_2, \ldots, A_n$ to the variables $V_1, V_2, \ldots, V_n$ (respectively) such that:

(a) Each A_j is a binary observable in that its eigenvalues are in $\{+1,-1\}$ (i.e., $A_j^2 = I$).
(b) All pairs of observables, A_i, A_j, that appear within the same constraint are commuting (i.e., they satisfy $A_iA_j = A_jA_i$).
(c) The observables *satisfy* each constraint $c_s : \{+1,-1\}^k \to \{+1,-1\}$ that acts on variables $V_{i_1}, \ldots, V_{i_k}$, in the sense that the multilinear polynomial equation $c_s(A_{i_1}, \ldots, A_{i_k}) = -I$ is satisfied (since c_s is arbitrary, we can assume right hand side of the polynomial to be -1).

This is a relaxation of the standard "classical" notion of a satisfying assignment (which corresponds to the case of one-dimensional observables). Quantum satisfying assignments for the two BCSs in Figure 1 are shown in Figure 2.

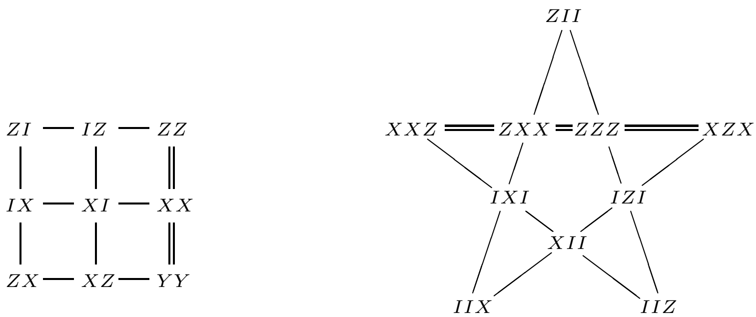

Fig. 2. Quantum satisfying assignments for: (a) magic square (left) and (b) magic pentagram (right). (X, Y, and Z are the usual 2×2 Pauli matrices, and juxtaposition means tensor product.)

There is a construction (implicit in [14] and explicit in [2] for the magic square) that converts these quantum satisfying assignments into perfect strategies—and this is easily extendable to any quantum satisfying assignment of a BCS. For completeness, we summarize the known construction. The entanglement is of the form $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{j=1}^{d} |j\rangle|j\rangle$, where d is the dimension of the observables. Alice associates observables $A_1, A_2, \ldots, A_n$ with the variables and Bob associates their transposes $A_1^T, A_2^T, \ldots, A_n^T$ (with respect to the computational basis) with the variables. On input s, Alice measures her observables that correspond to the variables in constraint c_s. At this point, it should be noted that this is a well-defined measurement since condition (b) implies that these observables are mutually commuting. Also, on input t, Bob measures his observable A_t^T. Condition (c) implies that Alice's output satisfies the constraint. Finally, Alice and Bob give consistent values for variable v_t because $\langle\psi|A_t \otimes A_t^T|\psi\rangle = \langle\psi|A_t \cdot A_t \otimes I|\psi\rangle = \langle\psi|\psi\rangle = 1$. The first equality follows from the fact that for the maximally entangled $|\psi\rangle$, $B \otimes A^T|\psi\rangle = B \cdot A \otimes I|\psi\rangle$.

1.3 General BCS Games

A natural computational problem is: given a description of a BCS as input, determine whether or not it has a perfect entangled strategy. A more general problem is to compute the maximum (or supremum) value of all entangled strategies.

For *classical* strategies, the problem of determining whether or not a perfect strategy exists is the same as finding out whether the underlying constraint system is feasible or not. It is NP-hard for general BCS games and in polynomial time for parity BCS games (where the problem reduces to solving a system of linear equations in modulo 2 arithmetic). For *quantum* strategies, we are currently not aware of *any* algorithm that determines whether or not an arbitrary parity BCS game has a perfect strategy (i.e., presently we do not even know that the problem is *decidable*).

In Section 2, we prove a converse to the construction of entangled strategies from quantum satisfying assignments in Section 1.2. Namely, we show that any perfect quantum strategy that uses countable-dimensional entanglement implies the existence of a quantum satisfying assignment.

It can be easily seen that not all BCS games have perfect quantum strategies, by this example

$$v_1 \oplus v_2 = 0 \qquad\qquad v_1 \oplus v_2 = 1. \tag{2}$$

First note that no generality is lost if we assume that Alice returns only a value for v_1 (since the value of v_2 is then uniquely determined by the constraint). The only case when they need to output different bits is when Alice is asked the second constraint and Bob is asked the second variable. Labelling the constraints as $\{0,1\}$ for Alice and variables as $\{0,1\}$ for Bob, it is not hard to see that such a game is equivalent to the so-called CHSH game [8], which is known to admit no perfect quantum strategy [18] (even though the quantum success probability is higher than the classical success probability [8]). In Section 3, we show how to derive upper bounds strictly below 1 on the entangled value of many parity BCSs.

2 Characterization of Perfect Strategies by Observables

Theorem 1. *For any binary constraint system, if there exists a perfect quantum strategy for the corresponding BCS game that uses finite or countably-infinite dimensional entanglement, then it has a quantum satisfying assignment.*

Proof. We start with an arbitrary binary constraint system that has variables $v_1, v_2, \ldots, v_n$ and constraints $c_1, c_2, \ldots, c_m$. Assume that there is a perfect entangled protocol for this system that uses entanglement

$$|\psi\rangle = \sum_{i=1}^{l} \alpha_i |\phi_i\rangle|\psi_i\rangle, \tag{3}$$

where $\{|\phi_1\rangle, \ldots, |\phi_l\rangle\}$ and $\{|\psi_1\rangle, \ldots, |\psi_l\rangle\}$ are orthonormal sets, $\alpha_1, \ldots, \alpha_l > 0$, and $\sum_{i=1}^{l} |\alpha_i|^2 = 1$. Here l is the Schmidt rank of the shared state—which can be set to ∞ to indicate a countably infinite set.

We consider two separate cases for Alice's strategy. In the first case, she applies an arbitrary *projective* measurement to the first register of $|\psi\rangle$. In the second case, Alice can apply an arbitrary POVM measurement to the first register of $|\psi\rangle$. For the definition and differences between these two measurements, we refer the reader to [16].

We will prove that quantum satisfying assignment exists in the first case. Then we will show that the second case can be reduced to first one, hence proving the theorem.

Case 1: Projective Measurements for Alice. For each $s \in \{1, 2, \ldots, m\}$, let c_s be a constraint consisting of r_s variables. Therefore, the set of outcomes for Alice is $\{0,1\}^{r_s}$. These can be associated with orthogonal projectors Π_a^s ($a \in \{0,1\}^{r_s}$). From these projectors, we can define the r_s individual bits of the outcome as the binary observables

$$A_s^{(j)} = \sum_{a \in \{0,1\}^{r_s}} (-1)^{a_j} \Pi_a^s, \tag{4}$$

for $j \in \{1, \ldots, r_s\}$ (Here we adopt the notation that observable $A_s^{(j)}$ corresponds to the variable in position j of constraint s). It is easy to check that $\{A_s^{(j)} : j \in \{1, \ldots, r_s\}\}$ is a set of commuting binary observables. We have defined a binary observable for Alice for each variable in the context of each constraint that includes it. For example, in the case of the magic square (Eqns. (1)), there is a binary observable $A_3^{(1)}$ for v_7 in the context of the third constraint and a binary observable $A_4^{(3)}$ for v_7 in the context of the fourth constraint. We have not yet shown that $A_3^{(1)} = A_4^{(3)}$ (constraint independent).

The measurements for Bob are (without loss of generality) binary observables B_t for each variable v_t ($t \in \{1, 2, \ldots, n\}$).

We need to show that the observables for Alice are the same, regardless of the constraint that they arise from (for example, for the magic square game, $A_3^{(1)} = A_4^{(3)}$). We shall use the following lemma.

Lemma 1. *Let $-I \preceq C_1, C_2, B \preceq I$ be Hermitian matrices on some Hilbert space $\mathcal{H}$. Let $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ be of the form*

$$|\psi\rangle = \sum_{i=1}^{l} \alpha_i |\phi_i\rangle|\psi_i\rangle, \tag{5}$$

where $\{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_l\rangle\}$ *and* $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_l\rangle\}$ *are orthonormal bases for* $\mathcal{H}$*,* $\alpha_1, \alpha_2, \ldots, \alpha_l > 0$*, and* $\sum_{i=1}^{l} |\alpha_i|^2 = 1$*. Then, for the Hermitian matrices* $\{B, C_1, C_2\}$*, if* $\langle\psi|B \otimes C_1|\psi\rangle = \langle\psi|B \otimes C_2|\psi\rangle = 1$ *then* $C_1 = C_2$*.*

Proof (Lemma 1). Consider the vectors $w = B \otimes I|\psi\rangle$, $u_1 = I \otimes C_1|\psi\rangle$, and $u_2 = I \otimes C_2|\psi\rangle$. These are vectors with length at most 1 and we have $w \cdot u_1 = w \cdot u_2 = 1$, which implies that $u_1 = w = u_2$. Therefore,

$$0 = I \otimes C_1|\psi\rangle - I \otimes C_2|\psi\rangle \tag{6}$$

$$= (I \otimes (C_1 - C_2)) \left(\sum_{i=1}^{l} \alpha_i |\phi_i\rangle|\psi_i\rangle \right) \tag{7}$$

$$= \sum_{i=1}^{l} \alpha_i |\phi_i\rangle (C_1 - C_2)|\psi_i\rangle, \tag{8}$$

which implies that $(C_1 - C_2)|\phi_i\rangle = 0$, for all $i \in \{1, 2, \ldots\}$. This implies that $C_1 = C_2$, which completes the proof of the lemma. □

Returning to the proof of Theorem 1, let $t \in \{1, 2, \ldots, n\}$ and $A_s^{(j)}$ and $A_{s'}^{(j')}$ be any two observables of Alice corresponding to the same variable v_t. Since Alice's binary observables associated with constraint c_s are commuting, we can assume that Alice begins her measurement process by measuring $A_s^{(j)}$, while Bob measures B_t. Since these two measurements must yield the same outcome, we have $\langle\psi|A_s^{(j)} \otimes B_t|\psi\rangle = 1$. Similarly, $\langle\psi|A_{s'}^{(j')} \otimes B_t|\psi\rangle = 1$. Therefore, applying Lemma 1, we have $A_s^{(j)} = A_{s'}^{(j')}$, which establishes that Alice's observables are constraint independent.

In addition to consistency between Alice and Bob, Alice's output bits must satisfy the constraint c_s (recall that c_s can be expressed as a multilinear polynomial over $\mathbb{R}$). That is,

$$\langle\psi|c_s(A_s^{(1)}, \ldots, A_s^{(r_s)}) \otimes I|\psi\rangle = -1. \tag{9}$$

By invoking Lemma 1 again, with $C_1 = -c_s(A_s^{(1)}, \ldots, A_s^{(r_s)})$, $C_2 = I$, $B = I$, we can deduce that $c_s(A_s^{(1)}, \ldots, A_s^{(r_s)}) = -I$.

At this point, it is convenient to rename Alice's observables to A_t, for each $t \in \{1, 2, \ldots, n\}$ (which we can do because we proved they are constraint independent). The observables associated with each constraint commute and their product has the required parity.

We will finally prove that a finite-dimensional set of observables must exist. If l is finite then there is nothing to prove, so assume it is countably infinite. Since, for all $t \in \{1, 2, \ldots, n\}$, $\langle\psi|A_t \otimes B_t|\psi\rangle = \langle\psi\,(A_t \otimes I)\,|\,(I \otimes B_t)\,\psi\rangle = 1$, we have $A_t \otimes I|\psi\rangle = I \otimes B_t|\psi\rangle$, so

$$\sum_{i=1}^{\infty} \alpha_i \left(A_t|\phi_i\rangle\right)|\psi_i\rangle = \sum_{i=1}^{\infty} \alpha_i |\phi_i\rangle \left(B_t|\psi_i\rangle\right). \tag{10}$$

Both sides of Eq. (10) are Schmidt decompositions of the same quantum state. Now we can use the fact that the Schmidt decomposition is unique up to a change of basis for the subspace associated with each distinct Schmidt coefficient. Consider any Schmidt coefficient with multiplicity d (each Schmidt coefficient appears with finite multiplicity because $\sum_{i=1}^{\infty} |\alpha_i|^2 = 1$). Suppose, without loss of generality, that $\alpha_1 = \alpha_2 = \cdots = \alpha_d = \alpha$. Then the span of $\{A_t|\phi_i\rangle : i \in \{1, 2, \ldots, d\}\}$ equals the span of $\{|\phi_i\rangle : i \in \{1, 2, \ldots, d\}\}$. In other words, A_t leaves the subspace spanned by $\{|\phi_i\rangle : i \in \{1, 2, \ldots, d\}\}$ fixed. By similar reasoning, B_t leaves the subspace spanned by $\{|\psi_i\rangle : i \in \{1, 2, \ldots, d\}\}$ fixed. Therefore, there exist bases in which A_t and B_t have block decompositions of the form

$$A_t = \begin{pmatrix} A'_t & 0 & 0 & \ldots \\ 0 & A''_t & 0 & \ldots \\ 0 & 0 & A'''_t & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \qquad B_t = \begin{pmatrix} B'_t & 0 & 0 & \ldots \\ 0 & B''_t & 0 & \ldots \\ 0 & 0 & B'''_t & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \tag{11}$$

with one block for the subspace of each Schmidt coefficient. We can take, say, the d-dimensional observables from the first block $\{A'_t : t \in \{1, 2, \ldots, n\}\}$ as a quantum satisfying assignment (which changes the effective entanglement to a d-dimensional maximally entangled state).

Case 2: POVM Measurements for Alice. A POVM measurement can be expressed as a projective measurement in a larger Hilbert space that includes ancillary qubits, as shown in Figure 3. Again we can define binary observables for j^{th} variable in a constraint s as in Case 1.

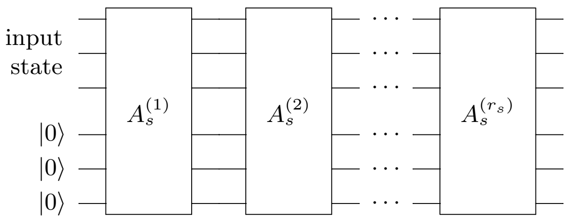

Fig. 3. Alice's POVM measurement on receiving input s expressed in Stinespring form (Case 2)

$$A_s^{(j)} = \sum_{a \in \{0,1\}^{r_s}} (-1)^{a_j} \Pi_a, \tag{12}$$

these observables act on the larger Hilbert space $\mathcal{H}_s \otimes \mathcal{H}_p$. Here $\mathcal{H}_s$ ($\mathcal{H}_p$) represents the Hilbert space for the entangled (private) qubits. Like before, the

$\{A_s^{(j)} : j \in \{1, \ldots, r_s\}\}$ is a set of commuting binary observables. Since these observables commute, without loss of generality, any of the corresponding variables can be measured first by Alice.

We will focus on the first measurement done by Alice given some constraint. Let us suppress the superscript and subscript for brevity of notation. Say, Alice uses observable A for the first measurement corresponding to variable t. This defines a projective measurement ($\Pi_0 = \frac{A+I}{2}, \Pi_1 = \frac{I-A}{2}$) on $\mathcal{H}_s \otimes \mathcal{H}_p$.

Suppose that the reduced entangled state on Alice's side is ρ. Then Alice's strategy is to apply the channel which adds the ancilla qubits to ρ and then applies the measurement (Π_0, Π_1). Using the Kraus operators of this channel, we can come up with *equivalent* POVM elements E_0, E_1 acting on the Hilbert space $\mathcal{H}_s$. Here equivalent means, for all $i \in \{0,1\}$ and $|\phi\rangle \in \mathcal{H}_s$,

$$\langle \phi, 00\ldots 0|\Pi_i|\phi, 00\ldots 0\rangle = \langle \phi|E_i|\phi\rangle. \tag{13}$$

Similarly, Bob has POVM elements (F_0, F_1) to measure variable t. Since their strategy is perfect, they always answer with same bit when asked for the variable t, which implies

$$\langle \psi|E_0 \otimes F_0|\psi\rangle + \langle \psi|E_1 \otimes F_1|\psi\rangle = 1. \tag{14}$$

This can be simplified to

$$\langle \psi|(E_0 - E_1) \otimes (F_0 - F_1)|\psi\rangle = 1. \tag{15}$$

Now we use the following lemma to prove that (E_0, E_1) is actually a projective measurement (similarly (F_0, F_1) is projective).

Lemma 2. *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be such that $|\psi\rangle = \sum_{i=1}^n \alpha_i|\phi_i\rangle|\psi_i\rangle$, where $\alpha_1, \alpha_2, \ldots, \alpha_n > 0$. If we have two POVM measurements, (E_0, E_1) on $\mathcal{H}_A$ and (F_0, F_1) on $\mathcal{H}_B$, such that*

$$\langle \psi|(E_0 - E_1) \otimes (F_0 - F_1)|\psi\rangle = 1 \tag{16}$$

then (E_0, E_1) and (F_0, F_1) are projective measurements.

Proof (Lemma 2). We will prove that (E_0, E_1) is a projective measurement. The proof for (F_0, F_1) is the same.

Notice that E_0 and E_1 are simultaneously diagonalizable (they are both Hermitian and $E_0 + E_1 = I$). The dimension of the system is n which can be set to ∞ to indicate that it is countably infinite. In the basis which diagonalizes them,

$$E_0 = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix} \quad \text{and} \quad E_1 = \begin{pmatrix} 1-\lambda_1 & & & \\ & 1-\lambda_2 & & \\ & & \ddots & \\ & & & 1-\lambda_n \end{pmatrix}.$$

This implies that E_0 and E_1 can be thought of as a probability distribution on 2^n projective measurements in the following way. For each $S \subseteq [n]$, define the projectors $\Pi_0^S = \sum_{i \in S} |i\rangle\langle i|$ and $\Pi_1^S = I - \Pi_0^S$, and $p_S = \prod_{i \in S} \lambda_i \prod_{i \notin S} (1 - \lambda_i)$. Note that $\sum_{S \subseteq [n]} p_S = 1$. It is straightforward to verify that

$$E_0 = \sum_{S \subseteq [n]} p_S \Pi_0^S \quad \text{and} \quad E_1 = \sum_{S \subseteq [n]} p_S \Pi_1^S. \tag{17}$$

By Eqns. (16), (17), and linearity,

$$\sum_{S \subseteq [n]} p_S \langle \psi | (\Pi_0^S - \Pi_1^S) \otimes (F_0 - F_1) | \psi \rangle = 1. \tag{18}$$

In the above equation, p_S's sum up to 1, and the term multiplied to them is at most 1. By an averaging argument, for all S with $p_S > 0$,

$$\langle \psi | (\Pi_0^S - \Pi_1^S) \otimes (F_0 - F_1) | \psi \rangle = 1. \tag{19}$$

Using Lemma 1, the $(\Pi_0^S - \Pi_1^S)$ have to be same for all S with $p_S > 0$. Hence, there can be at most one p_S with non-zero probability. Hence (E_0, E_1) is a projective measurement.

□

Now we know that (E_0, E_1) is a projective measurement. Also, using Eq. (13), any eigenvector $|\phi\rangle$ of E_i can be converted into an eigenvector $|\phi, 00 \cdots 0\rangle$ for Π_i with same eigenvalue. Then, in the basis where eigenvectors of the form $|\phi, 00 \cdots 0\rangle$ are listed first,

$$\Pi_0 = \left(\begin{array}{c|c} E_0 & 0 \ \cdots \ 0 \\ \hline 0 & \\ \vdots & M_0 \\ 0 & \end{array}\right) \quad \text{and} \quad \Pi_1 = \left(\begin{array}{c|c} E_1 & 0 \ \cdots \ 0 \\ \hline 0 & \\ \vdots & M_1 \\ 0 & \end{array}\right). \tag{20}$$

It is given that the observables $\Pi_0 - \Pi_1$ corresponding to different variables in the same context commute. It follows that the observables $E_0 - E_1$ corresponding to different variables in the same context also commute. Hence the proof for Case 2 follows from Case 1.

□

From the argument at the end of the first case, it follows that if we have a perfect strategy using countably infinite entanglement then it can be converted into a strategy having finite entanglement. The generic conversion (Sec. 1.2) of quantum satisfying assignments to a quantum strategy uses maximally entangled state. Hence Theorem 1 shows that if there is a perfect strategy for a BCS game then there exist a perfect strategy which uses maximally entangled state.

3 Proving Gaps on the Maximum Success Probability

Due to space constraints, the content of this section is omitted; however, it is available in the full version of this paper [10], which can be accessed at `http://arxiv.org/abs/1209.2729`.

The main result in this section is an upper bound below 1 on the entangled value of some BCS games of interest, under the assumption that the entanglement is a maximally mixed state (of arbitrarily high dimension).

4 Related Work

After the results of this article were made public, Arkhipov [3] studied the restricted case of parity BCS games where every variable appears in at most two constraints. He showed that these games have a perfect entangled strategy if and only if a related *dual* graph of the game is non-planar. The result combines elegant techniques with Kuratowski's theorem and our characterization of perfect strategies (in the sense that [3] makes use of our characterization).

More recently, Ji [13] showed that interesting examples like quantum chromatic number and Kochen-Specker sets can be described in the BCS game framework. He used special gadgets, called *commutativity* gadgets, to show reductions between various BCS's which preserve satisfiability using quantum assignments. Also, he showed that, for all k, there exists a parity BCS game which requires at least k entangled qubits to play perfectly.

5 Open Questions

There are many questions left open by this work. We have a characterization of perfect strategies for BCS games. It shows that there always exists a perfect strategy using maximal entanglement if a perfect entangled strategy exist. Still, given a game, deciding whether it has a perfect strategy is open.

There are questions pertaining to the *optimal* values of BCS games (the maximum success probability achievable), such as problem of computing these values, or approximations of them. Another question is whether there always exists an optimal strategy for a BCS game which uses maximally entangled states.

All of the above questions can be asked for general non-local games too. For the case of XOR games, the optimal value is given by a semidefinite program [9,18]. This shows how to compute the optimal value of the game and that there always exist an optimal strategy which uses maximally entangled states [9]. It is also known for graph coloring games (like BCS games) that there always exists a perfect strategy using maximal entanglement (if a perfect entangled strategy exist) [11]. But whether this is true for general games that have perfect strategies remains open.

Acknowledgments. We are grateful for discussions about this project with many people, including Alex Arkhipov, Harry Buhrman, Sevag Gharibian, Tsuyoshi Ito, Kazuo Iwama, Zhengfeng Ji, Hirotada Kobayashi, François Le Gall, Laura Mancinska (for pointing out an error in a previous version of this manuscript pertaining to the analysis of the case of POVM measurements), Oded Regev, Florian Speelman, Sarvagya Upadhyay, John Watrous, and Ronald de Wolf. Some of this work took place while the first author was visiting Amsterdam's CWI in 2011. This work is partially supported by Canada's NSERC and CIFAR.

References

1. Aravind, P.K.: Bell's Theorem without inequalities and only two distant observers. Found. Phys. Lett. 15(4), 397–405 (2002)
2. Aravind, P.K.: Quantum mysteries revisited again. Am. J. Phys. 72, 1303–1307 (2004)
3. Arkhipov, A.: Extending and characterizing quantum magic games. arXiv:1209.3819 [quant-ph] (2012)
4. Arora, S., Lund, C., Motwani, R., Sudan, M., Szegedy, M.: Proof verification and the hardness of approximation problems. J. ACM 45(3), 501–555 (1998)
5. Babai, L., Fortnow, L., Lund, C.: Non-deterministic exponential time has two-prover interactive protocols. Computational Complexity 1, 3–40 (1991)
6. Bell, J.S.: On the Einstein-Podolsky-Rosen paradox. Physics 1, 195–200 (1964)
7. Ben-Or, M., Goldwasser, S., Kilian, J., Wigderson, A.: Multi-prover interactive proofs: How to remove intractability assumptions. In: Proc. of the 20th ACM Symp. on Theory of Computing (STOC 1988), pp. 113–131 (1988)
8. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. 23(15), 880–884 (1969)
9. Cleve, R., Høyer, P., Toner, B., Watrous, J.: Consequences and limits of nonlocal strategies. In: Proc. of the 19th IEEE Conf. on Computational Complexity (CCC 2004), pp. 236–249 (2004)
10. Cleve, R., Mittal, R.: Characterization of binary constraint system games (2013), `http://arxiv.org/abs/1209.2729`
11. Cameron, P.J., Montanaro, A., Newman, M.W., Severini, S., Winter, A.: On the quantum chromatic number of a graph. The Electronic Journal of Combinatorics [Electronic Only] 14(1):Research Paper R81, 15 (2007)
12. Feige, U., Goldwasser, S., Lovász, L., Safra, S., Szegedy, M.: Interactive proofs and the hardness of approximating cliques. J. ACM 43(2), 268–292 (1996)
13. Ji, Z.: Binary constraint system games and locally commutative reductions. arXiv:1310.3794 [quant-ph] (2013)
14. Mermin, N.D.: Simple unified form for the major no-hidden-variables theorems. Phys. Rev. Lett. 65(27), 3373–3376 (1990)
15. Mermin, N.D.: Hidden variables and the two theorems of John Bell. Rev. Mod. Phys. 65(3), 803–815 (1993)
16. Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge University Press, Cambridge (2000)
17. Speelman, F.: Personal communication (2011)
18. Cirel'son, B.S.: Quantum generalizations of Bell's inequality. Lett. in Math. Phys. 4(2), 93–100 (1980)