

Nonlocal games with restricted strategies ¹

Laura Mančinska¹ David E. Roberson² Dan Stahlke³ Antonios Varvitsiotis^{1,2}

¹*Centre for Quantum Technologies, National University of Singapore*

²*School of Physical and Mathematical Sciences, Nanyang Technological University*

³*Department of Physics, Carnegie Mellon University*

Entanglement plays a central role in quantum information processing and is an essential resource for classical distributed tasks such as unconditionally secure cryptography [Eke91], randomness certification [Col06, PAM⁺10] and expansion [VV12, CY13] and others. Hence, given such a distributed task one is interested in understanding what is the optimal entangled strategy and how much and what kind of entanglement does it require. As is commonly done, we use the framework of nonlocal games to study these questions. In physics nonlocal games appear as Bell inequalities while in computer science they arise as multi-prover interactive proof-systems (MIP).

A nonlocal game consists of two separated parties, Alice and Bob, and a verifier. To play the game $G = (V, \pi)$, the verifier draws $(q, r) \in Q_A \times Q_B$ according to π and sends q to Alice and r to Bob. Alice and Bob must then respond with answers a and b from finite sets A_A and A_B respectively. The players win if they satisfy the verification predicate $V(a, b|q, r) = 1$. Alice and Bob cannot communicate after receiving the question, however they can agree on a strategy beforehand. To do so they may use their knowledge of the distribution π and the predicate V .

The goal of the players is to win with as high a probability as possible. The *classical value* of a game is the maximum winning probability over all classical strategies. Similarly, the *entangled value*, $\omega^*(G)$, of a game G is the supremum of winning probabilities taken over all entangled strategies. A *entangled strategy* allows the players to determine their answers by performing measurements on a shared entangled state. We say that an (entangled) strategy for a nonlocal game is *perfect* if it wins with probability one.

Given a nonlocal game G , one is often interested in

1. computing the entangled value $\omega^*(G)$;
2. understanding how much and what kind of entanglement is needed to achieve $\omega^*(G)$;
3. deciding if $\omega^*(G) = 1$ and if perfect success can be achieved by a finite-dimensional strategy.

Despite the efforts no algorithm is known for computing $\omega^*(G)$ or even deciding if $\omega^*(G) = 1$. Another recurrent sticking point is the achievability of $\omega^*(G)$ which relates to the more general question of whether the set of quantum correlations $p(a, b|q, r)$ is closed or not. Finally, it has remained out of reach to understand if maximally entangled state and/or projective measurements are sufficient if one is only interested in perfect strategies. In view of the lack of progress in understanding these basic questions and with the hope to get new insights, we alter the setup slightly by restricting the entangled players in one of the following two ways:

1. the players are only allowed to use projective measurements on a maximally entangled shared state;
2. the players are only allowed to use a certain subset of the quantum correlations $p(a, b|q, r)$ defined via a system of linear equations.

We give two necessary and sufficient conditions for a game to have a perfect projective strategy using a maximally entangled state. One of these conditions can be viewed as identifying a complete problem among the decision problems of the type “Does G admit a perfect projective strategy with maximally entangled state?”. In addition we give a graph-theoretic lower bound on the entangled value of a nonlocal game.

¹A technical version of this work is attached to the EasyChair submission.

1 Correlated games

As a first step we identify a class of games for which if there exists some perfect entangled strategy, there also exists one with projective measurements and the maximally entangled state.

Definition 1. A nonlocal game G is called *correlated* if it satisfies the following two properties: (i) $A_A = A_B$ and $Q_A = Q_B$; (ii) when asked the same question, the players must respond with the same answer.

In the case of correlated games, we can show that the existence of a perfect entangled strategy of a particular form.

Lemma 1. *Let G be a correlated game having a perfect entangled strategy. Then there also exists a perfect strategy for G that is projective, uses the maximally entangled state, and Bob's projectors are the transpose of the corresponding projector of Alice's.*

The above lemma is the key to analyze correlated games using the game graphs we will define below. Essentially it allows us to consider only one player's measurements instead of both.

The majority of our results apply directly to correlated games. However, in order to apply our results to a general nonlocal game G , we define a *correlated extension* of G , denoted \tilde{G} , for which we are able to prove the following:

Lemma 2. *A game G has a perfect projective strategy with maximally entangled state if and only if \tilde{G} has a perfect entangled strategy.*

One consequence of this lemma is that if one were able to show that a nonlocal game G admits a perfect entangled strategy if and only if its correlated extension admits an perfect entangled strategy, then they would have shown that one can restrict to projective measurements and the maximally entangled state when searching for perfect quantum strategies. This could potentially make the question of the existence of perfect quantum strategies much more manageable.

2 Game graphs and projective packings

Given a correlated game G with question and answer sets Q and A respectively, we associate to G its *game graph*, which we denote $X(G)$. The graph $X(G)$ has vertex set $A \times Q$ such that (a, q) is adjacent to (a', q') if this pair of questions and answers result in a loss for Alice and Bob.

The game graph allows us to use tools from the field of graph theory to obtain two necessary and sufficient conditions for the existence of a perfect entangled strategy for a correlated game. We are also able to use it to prove a lower bound on the entangled value of a correlated game.

A *projective packing* [Rob13] of a graph is an assignment of d -dimensional projectors to its vertices such that adjacent vertices are assigned orthogonal projectors. The value of a projective packing is the sum of the ranks of the projectors divided by the dimension d . The projective packing number of a graph X , denoted $\alpha_p(X)$ is the supremum of values over all projective packings of X . Using Lemma 1, we are able to prove the following:

Lemma 3. *Let G be a correlated game with question set Q . Then G has a perfect entangled strategy if and only if $X(G)$ has a projective packing of value $|Q|$.*

We are also able to provide a lower bound on the entangled value of a correlated game through the use of projective packings:

Theorem 1. *Let G be a correlated game with uniform input distribution, question set Q , answer set A and let $X = X(G)$ be the associated game graph. Then, $\omega^*(G) \geq \left(\frac{\alpha_p(X)}{|Q|}\right)^2$.*

3 Game graphs and quantum independence number

An independent set in a graph is a set of pairwise nonadjacent vertices. The independence number of a graph X is the maximum size of an independent set of X .

The quantum independence number [RM14] of a graph X , denoted $\alpha_q(X)$, is defined via a nonlocal game as follows: Alice and Bob receive questions $i, j \in [k]$ respectively and must answer with vertices u, v of X . In order to win, they must both output the same vertex if they receive the same input, and they must output distinct nonadjacent vertices if they receive different inputs. Maximizing over k such that there exists a perfect entangled strategy yields the quantum independence number.

Note that the independent set game is a correlated game. It turns out that this is in fact the “hardest” correlated game² in a sense made rigorous by the following lemma:

Lemma 4. *Let G be a correlated game with question set Q . Then G has a perfect entangled strategy if and only if $\alpha_q(X(G)) = |Q|$.*

By this lemma, any algorithm which can determine if the independent set game has a perfect entangled strategy could be used to determine if any correlated game has a perfect entangled strategy.

Using Lemma 2, we can obtain results similar to Lemma 3 and Lemma 4 for arbitrary nonlocal game.

Theorem 2. *Let G be a game with question sets Q_A and Q_B for Alice and Bob respectively, and let \tilde{G} be its correlated extension. Then the following are equivalent:*

1. *the game G has a perfect projective strategy with maximally entangled state;*
2. *the graph $X(\tilde{G})$ has a projective packing of value $|Q_A| + |Q_B|$;*
3. *it holds that $\alpha_q(X(\tilde{G})) = |Q_A| + |Q_B|$.*

4 Approximate Homomorphisms

Given sets Q and A , a correlation $p(a, b|q, r)$ is *synchronous*[PSS⁺14] if $p(a = b|q = r) = 1$ for all $q, r \in Q$ and $a, b \in A$. Let $\mathcal{L}^s(Q, A)$ denote the set of classical synchronous correlations and $\mathcal{Q}^s(Q, A)$ denote the set of quantum synchronous correlations.

Using the notion of synchronous correlations and the homomorphism game introduced in [RM14], we define the following:

Definition 2. For graphs X and Y , let $A(X \rightarrow Y)$ be the maximum value q such that there is a $p(y, y'|x, x') \in \mathcal{L}^s(X, Y \cup \{\emptyset\})$ satisfying $p(y, y'|x, x') = 0$ for all $x \sim x'$ and $y, y' \in V(Y), y \not\sim y'$, and $p(y = \emptyset|x) = 1 - q$ for all $x \in V(X)$. Let $A(X \xrightarrow{q} Y)$ be defined similarly but over $\mathcal{Q}^s(X, Y \cup \{\emptyset\})$.

Definition 3. For graphs X and Y , let $B(X \rightarrow Y)$ be the maximum value q such that there is a $p(y, y'|x, x') \in \mathcal{L}^s(X, Y)$ satisfying $p(y \sim y'|x, x') = q$ for all $x \sim x'$. Let $B(X \xrightarrow{q} Y)$ be defined similarly but over $\mathcal{Q}^s(X, Y)$.

Another way of formulating $B(X \xrightarrow{q} Y)$ is as the optimal entangled value of the (X, Y) -homomorphism game restricted to synchronous correlations which satisfy $p(y \sim y'|x, x') = p(y \sim y'|x'', x''')$ for all $x \sim x'$ and $x'' \sim x'''$, and such that the input distribution is the uniform distribution over the edges of X . The value $A(X \xrightarrow{q} Y)$ can be similarly defined as the entangled value of a nonlocal game.

Theorem 3. *If a graph X has at least one edge, then $B(X \xrightarrow{q} K_2)$ is a function of the Lovász theta number of \bar{X} and $B(X \rightarrow K_2)$ is a function of the cubical chromatic number of [Š14].*

Theorem 4. $A(X \rightarrow K_1) = 1/\chi_f(X)$ and $A(X \xrightarrow{q} K_1) = 1/\xi_f(X)$ where χ_f is the fractional chromatic number and ξ_f is the projective rank of [RM14].

²Using a different technique a similar result has independently been obtained by Z. Ji.

Acknowledgments. LM is supported by Ministry of Education, Singapore under the Tier 3 grant MOE2012-T3-1-009. DR is supported by an NTU start-up grant awarded to D.V. Pasechnik.

References

- [Col06] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, Trinity College, University of Cambridge, 2006. [arXiv:0911.3814](#).
- [CY13] Matthew Coudron and Henry Yuen. Infinite randomness expansion and amplification with a constant number of devices. 2013. [arXiv:1310.6755](#).
- [Eke91] Artur K. Ekert. Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991. [doi:10.1103/physrevlett.67.661](#).
- [PAM⁺10] Stefano Pironio, Antonio Acín, Serge Massar, A. Boyer de La Giroday, Dzimitry N. Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T. Andrew Manning, and Cristopher Monroe. Random numbers certified by Bell’s theorem. *Nature*, 464(7291):10, 2010. [arXiv:0911.3427](#), [doi:10.1038/nature09008](#).
- [PSS⁺14] Vern I. Paulsen, Simone Severini, Dan Stahlke, Ivan G. Todorov, and Andreas Winter. Estimating quantum chromatic numbers. 2014. [arXiv:1407.6918](#).
- [RM14] David E. Roberson and Laura Mančinska. Quantum homomorphisms. To appear in *Journal of Combinatorial Theory, Series B*, 2014. [arXiv:1212.1724](#).
- [Rob13] David E. Roberson. *Variations on a Theme: Graph Homomorphisms*. PhD thesis, University of Waterloo, 2013.
- [Š14] Robert Šámal. Cubical coloring – fractional covering by cuts and semidefinite programming. 2014. [arXiv:0911.2589](#).
- [VV12] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the 44th Symposium on Theory of Computing, STOC’12*, pages 61–76, 2012. [arXiv:1111.6054](#), [doi:10.1145/2213977.2213984](#).