Near-Optimal and Explicit Bell Inequality Violations

Harry Buhrman* Oded Regev† Giannicola Scarpa‡ Ronald de Wolf§

Abstract

Bell inequality violations correspond to behavior of entangled quantum systems that cannot be simulated classically. We give two new two-player games with Bell inequality violations that are stronger, fully explicit, and arguably simpler than earlier work. The first game is based on the Hidden Matching problem of quantum communication complexity, introduced by Bar-Yossef, Jayram, and Kerenidis. This game can be won with probability 1 by a quantum strategy using a maximally entangled state with local dimension n (e.g., $\log n$ EPR-pairs), while we show that the winning probability of any classical strategy differs from $\frac{1}{2}$ by at most $O(\log n/\sqrt{n})$. The second game is based on the integrality gap for Unique Games by Khot and Vishnoi and the quantum rounding procedure of Kempe, Regev, and Toner. Here n-dimensional entanglement allows to win with probability $1/(\log n)^2$, while the best classical winning probability is $1/n$. This near-linear ratio ("Bell inequality violation") is near-optimal, both in terms of the local dimension of the entangled state and in terms of the number of possible outputs.

1 Introduction

One of the most striking features of quantum mechanics is the fact that *entangled* particles can exhibit correlations that cannot be reproduced or explained by classical physics (i.e., by "local hidden-variable theories"). This was first noted by Bell, in response to Einstein-Podolsky-Rosen's challenge to the completeness of quantum mechanics. Experimental realization of such correlations is the strongest proof we have that nature does not behave according to classical physics.

Here we study quantitatively how much such "quantum correlations" can deviate from what is achievable classically. The setup for a game G is as follows. Two space-like separated parties, called Alice and Bob, receive inputs x and y according to some fixed and known probability distribution π, and are required to produce outputs a and b. There is a predicate specifying which outputs a, b "win" the game on inputs x, y. The goal is to design games where quantum strategies have much higher winning probability than the best classical strategy.

Quantum strategies start out with some fixed entangled state $|\psi\rangle$, say with local dimension n; a typical example would be $\log n$ shared EPR-pairs. For each input x, Alice has a set of measurement operators $\{A_x^a\}$ and for each y, Bob has measurement operators $\{B_y^b\}$. They apply the measurement corresponding to x and y to the entangled state $|\psi\rangle$, producing outputs a and b, respectively. No communication takes place between them. Depending on which is more convenient for the game G at hand, we will define its *entangled value* $\omega^*(G)$ as either the maximum winning probability, or the

*CWI and U of Amsterdam, buhrman@cwi.nl. Supported by a Vici grant from NWO, and EU-grant QCS.
†Tel Aviv University and ENS Paris, odedr@post.tau.ac.il.
‡CWI Amsterdam, g.scarpa@cwi.nl. Supported by a Vidi grant from NWO, and EU-grant QCS.
§CWI Amsterdam, rdewolf@cwi.nl. Supported by a Vidi grant from NWO, and EU-grant QCS.

maximum *advantage* (winning probability minus losing probability) among all quantum strategies for it. When restricting to strategies that use entanglement of local dimension n, the value is denoted $\omega_n^*(G)$. This should be contrasted with the *classical value* $\omega(G) = \omega_0^*(G)$ of the game, which is the maximum winning probability among all classical, non-entangled strategies.

It is well-known that there are games G where $\omega_n^*(G)$ is higher than $\omega(G)$. Such examples are known as "Bell inequality violations"; the CHSH game is a famous one with $n = 2$. We are interested in designing games G maximizing the ratio between quantum and classical values. The larger this ratio, the larger the "difference" between quantum and classical worlds, and the larger the "noise-resistance" of the violation. The ratio can be analyzed in two different ways:

1. $\max \frac{\omega_n^*(G)}{\omega(G)}$ as a function of n, the local dimension of the entangled state
2. $\max \frac{\omega^*(G)}{\omega(G)}$ as a function of k, the number of possible outputs each of Alice and Bob can give

In two recent papers, Junge et al. [3, 2] studied both settings using tools from Banach space and operator space theory. They proved that the first ratio cannot be larger than $O(n)$, and (implicitly) showed the existence of a game where the ratio is $\Omega(\sqrt{n}/\log n)$. For the second ratio, Junge and Palazuelos [2] recently showed an upper bound of $O(k)$, and they showed the existence of a game where the ratio is $\Omega(\sqrt{k}/\log k)$. Theirs is an existence proof, involving a random choice of signs and hence not fully explicit, though they in fact show that almost all choices of signs will work.

In this paper we exhibit two stronger and more explicit Bell inequality violations.

2 The Hidden Matching game

The "Hidden Matching" problem was introduced by Bar-Yossef et al. [1], and many variants of it were subsequently studied. The original version is as follows. Let n be a power of 2. Alice is given input $x \in \{0,1\}^n$ and Bob is given a perfect matching M (i.e., a partition of $[n]$ into $n/2$ disjoint pairs (i, j)). Both are uniformly distributed. We allow one-way communication from Alice to Bob, and Bob outputs an $(i, j) \in M$ and $v \in \{0,1\}$. They win if $v = x_i \oplus x_j$. Using tools from Fourier analysis, we show that if Alice sends Bob a c-bit message, then their optimal winning probability is $\frac{1}{2} + \Theta(\frac{c}{\sqrt{n}})$. Bar-Yossef et al. [1] earlier proved this for $c \sim \sqrt{n}$, using information theory.

The non-local game based on this is as follows: the inputs x and M are the same as before, but now Alice and Bob don't communicate. Instead, Alice outputs an $a \in \{0,1\}^{\log n}$, Bob outputs $b \in \{0,1\}^{\log n}$ and $(i, j) \in M$, and they *win* the game if the outputs satisfy the relation $(a \oplus b) \cdot (i \oplus j) = x_i \oplus x_j$, where the left-hand side is the inner product of two $\log n$-bit strings modulo 2. As stated, Alice has n possible outputs while Bob has $O(n^3)$. However, one can massage the problem such that there are only n possible outputs for Bob as well.

A classical strategy that wins this non-local game induces a protocol for the original Hidden Matching problem with communication $c = \log n$ bits and the same winning probability. Hence our bound for the original problem implies that no classical strategy can win with probability greater than $\frac{1}{2} + O(\frac{\log n}{\sqrt{n}})$. In contrast, there is a strategy that wins with probability 1 using $\log n$ EPR-pairs. By defining the value of the game as the advantage of the best strategy (rather than its winning probability), we get entangled value $\omega_n^*(G) = 1$ and classical value $\omega(G) = O(\frac{\log n}{\sqrt{n}})$. This gives a Bell inequality violation of order $\sqrt{n}/\log n$. This order is similar to the one of Junge et al. [3, 2], but our game is simple and fully explicit. Clearly, explicitness is a prerequisite for any future experimental realization.

3 The Khot-Vishnoi game

Our second non-local game derives from the work of Khot and Vishnoi [5] on the famous *Unique Games Conjecture*. They exhibited a large integrality gap for the SDP-relaxation of certain specific Unique Games. We use essentially the same game, though for our purposes we won't have to worry about SDPs or the UGC. Consider the group $\{0,1\}^n$ of all n-bit strings with bitwise addition mod 2, and let H be the subgroup containing the n Hadamard codewords. This subgroup partitions $\{0,1\}^n$ into $2^n/n$ cosets of n elements each. Alice receives a uniformly random coset x as input, which we can think of as $u+H$ for uniformly random $u \in \{0,1\}^n$. Bob receives a coset y obtained from Alice's by adding a string of low Hamming weight, namely $y = x + z = u + z + H$, where each bit of $z \in \{0,1\}^n$ is set to 1 with probability η, independently of the other bits. Notice that addition of z gives a natural bijection between the two cosets, mapping each element of the first coset to a relatively nearby element of the second coset; namely, the distance between the two elements is the Hamming weight of z, which is typically around ηn. Each player is supposed to output one element from its coset, and their goal is for their elements to match under the bijection. In other words, Alice outputs an element $a \in x$, Bob outputs $b \in y$, and they win the game iff $a + b = z$.[1]

Based on the integrality gap analysis of Khot and Vishnoi, we show that no classical strategy can win this game with probability greater than $1/n^{\eta/(1-\eta)}$. In contrast, using a simple version of the "quantum rounding" technique of [4], we exhibit a quantum strategy that uses the maximally entangled state in n dimensions and wins with probability at least $(1-2\eta)^2$. Accordingly, we have entangled value $\omega_n^*(G) \geq (1-2\eta)^2$ and classical value $\omega(G) \leq 1/n^{\eta/(1-\eta)}$ for this game. Setting the noise-rate to $\eta = 1/2 - 1/\log n$, we obtain a Bell inequality violation of order $n/(\log n)^2$. This is near-optimal both in terms of the local dimension of the entangled state, and in terms of the number of possible outputs of the two players.

Full version: See `http://arxiv.org/abs/1012.5043`

References

[1] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM J. on Computing*, 38(1):366–384, 2008.

[2] M. Junge and C. Palazuelos. Large violation of Bell inequalities with low entanglement. To appear in *Comm. Math. Physics*. arXiv:1007.3043v2, 2010.

[3] M. Junge, C. Palazuelos, D. Pérez-Garcia, I. Villanueva, and M. Wolf. Operator space theory: a natural framework for Bell inequalities. *PRL*, 104(170405), 2010. arXiv:0912.1941.

[4] J. Kempe, O. Regev, and B. Toner. Unique games with entangled provers are easy. In *Proc. of 49th FOCS*, pages 457–466, 2008. arXiv:0710.0655.

[5] S. Khot and N. Vishnoi. The unique games conjecture, integrality gap for cut problems and embeddability of negative type metrics into ℓ_1. In *Proc. of 46th FOCS*, pages 53–62, 2005.

[1] Note that the winning condition for this game is a "randomized predicate", as there are n possible predicates (one for each z in $x+y$) corresponding to each pair of inputs x, y. However, it is easy to see that with very high probability exactly one of these n constraints dominates (namely, the one corresponding to a z of Hamming weight around ηn). This allows one to modify the game in a straightforward manner, making the predicate deterministic.