Rank-one and Quantum XOR games*

Tom Cooney Marius Junge Carlos Palazuelos David Pérez-García
Oded Regev Thomas Vidick

Initiated by the work of Bell [Bel64], the quantitative study of the nonlocal correlations predicted by quantum mechanics has more recently been pursued using the powerful framework of *multiplayer games*. The simplest such games, XOR games [CHTW04], correspond to the simplest and most widely studied class of Bell inequalities, the so-called correlation inequalities. In an XOR game, two players have a one-round interaction with a referee. The referee asks each player a question, to which they have to reply with a single bit each. The referee then makes an accept/reject decision based on the parity of the two received bits alone.

The constrained format of XOR games makes them uniquely amenable to mathematical [Tsi87, Gro53] and algorithmic [CHTW04] treatment, while also offering the possibility for experimental demonstrations [ADR82]. As a result, they have been the object of extensive study both in the physics [CHSH69, Tsi80] and computer science [CHTW04, CSUU08, PWP$^+$08] literature. Simplicity, however, comes at a cost: XOR games only reflect limited aspects of the nonlocality of entanglement. For instance, the largest advantage of entangled over unentangled players in an XOR game can be at most a small constant multiplicative factor, making experiments based on those games particularly vulnerable to detection loopholes. It is also known that finite-dimensional maximally entangled states are always an optimal resource; this is no longer true in more general scenarios [JP11, Reg12].

These limitations make the study of more general classes of games all the more desirable. Going beyond the well-understood framework of XOR games, however, has proved challenging. Extensions to larger answer sizes [JPP$^+$10, JP11, BRSdW11, Reg12] and more than two players [PWP$^+$08, BV12] have been considered, and specific families of games discovered that demonstrate the richness of general multiplayer games, further motivating their study. Unfortunately, although these investigations have uncovered interesting connections with functional analysis and theoretical computer science, a systematic analysis of general multiplayer games has so far proved elusive: possibly, the class of games considered has now become too wide for any substantial mathematical treatment to be possible.

Games with quantum messages. In this paper we propose new extensions of XOR games, in a different direction: we allow the exchange of quantum messages between the referee and the players.[1] We consider two simple classes of games with quantum messages:

1. *Quantum XOR games* are games in which the referee's questions to the players are quantum states, but, just as in classical XOR games, the player's answers are classical bits and the referee bases

*This QIP 2013 submission combines two separate papers, the first on rank-one quantum games [CJPP11] and the second on quantum XOR games [RV12]. The results contained in both papers are for the most part disjoint, and were obtained independently. However, due to the close relationship between the two models, we believe that merging the two papers for the purposes of a QIP presentation could only benefit the audience.

[1]While games with quantum messages have been previously considered in the context of interactive proofs [KM03], to the best of our knowledge such games had not been studied in the context of "Bell inequality violations" (see however recent related work by Buscemi [Bus12]).

his decision on their parity alone. Given a quantum XOR game G, we introduce its bias $\omega(G)$, maximally entangled bias $\omega^{me}(G)$, and entangled bias $\omega^*(G)$, which are defined as twice the maximum success probability, minus one, achievable by players respectively sharing no entanglement, a maximally entangled state of arbitrary dimension, or an arbitrary entangled state,

2. *Rank-one quantum games* are games in which both the referee's questions, and the players' answers, are quantum states, but the referee's final decision is restricted to be given by the outcome of a rank-one projection performed on the players' (quantum) answers, as well as the referee's own private space. Given a rank-one quantum game G, its entangled value $\omega^*(G)$ is defined as the maximum success probability of players sharing arbitrary entanglement.

Although seemingly quite different, these two models share many properties. In particular, we show that there exists a simple transformation mapping games of one form into games of the other in a way that preserves (up to a simple scaling) the quantity $\omega^*(G)$.

Our main results demonstrate that both models are a fruitful class of two-player games to study in two complementary ways. First, we provide diverse examples of games that fall in either model and exhibit diverse properties of entanglement that could not be observed in the context of classical XOR games, showing that our quantum games provide a *richer* model. Second, we show that, in spite of this greater generality, and in stark contrast with previously considered extensions, both rank-one and quantum XOR games remain *tractable* models. In particular, we show the existence of efficient approximation algorithms for each of the quantities $\omega(G), \omega^{me}(G)$ and $\omega^*(G)$ introduced above.

Families of games. We briefly describe two families of games that exemplify the rich behavior of rank-one and quantum XOR games. More examples can be found in the full papers.

For any $n \geq 1$, let $|\psi_n\rangle$ be the maximally entangled state in n dimensions. Let T_n be the quantum XOR game in which the players are sent one of the two states $|\varphi_0\rangle = (|0\rangle|0\rangle + |\psi_n\rangle)/\sqrt{2}$ or $|\varphi_1\rangle = (|0\rangle|0\rangle - |\psi_n\rangle)/\sqrt{2}$, each chosen with probability $1/2$ by the referee, and are asked to produce answers with even parity in case the state is $|\varphi_0\rangle$, and odd parity in case it is $|\varphi_1\rangle$. Even though the two states are orthogonal, it is not a priori clear how well the players can perform in this game: can $|\varphi_0\rangle$ and $|\varphi_1\rangle$ be *locally* distinguished? Interestingly, the answer crucially depends on the resources allowed for the players. The maximum bias achievable by players who do not share any entanglement is exactly $\omega(T_n) = 1/\sqrt{n}$. In fact, even players allowed to share an arbitrary supply of EPR pairs cannot do better: $\omega^{me}(T_n) = 1/\sqrt{n}$. Surprisingly, in case the players have access to an unrestricted amount of entanglement, we have $\omega^*(T_n) = 1$: an unbounded advantage over the unentangled case. Finally, we also show that the optimal $\omega^*(T_n) = 1$ can only be achieved in the limit of infinite entanglement.

It is interesting to consider the rank-one equivalent of the game T_n: in that game, the referee prepares the state $|\eta\rangle = (|00\rangle|0\rangle + |\psi_n\rangle|1\rangle)/\sqrt{2}$, where the last register is his private register, and his accepting measurement is the rank-one projection on $|\gamma\rangle = (|\psi_n\rangle|0\rangle + |00\rangle|1\rangle)/\sqrt{2}$.[2] These games fall in a larger class which we call *Schur games*, because the reduced density of both the question state $|\eta\rangle$ and final state $|\gamma\rangle$ on the players is supported on $\{|i\rangle\langle i| \otimes |i\rangle\langle i|\}$. As we show, such games have the property that their entangled value is always at least a quarter of their *one-way value*: the maximum success probability achievable by players allowed one-way communication (say, from Alice to Bob).

For simplicity we also describe our second example as a quantum XOR game, though it was originally introduced as a rank-one quantum game. For $n \geq 1$, the game C_n is played as follows. The referee chooses a random integer $k \in \{1, \ldots, n\}$, and sends one of the two states $(|0,k\rangle \pm |k,0\rangle)/\sqrt{2}$,

[2] The game T_2, when expressed in this form, is very closely related to the coherent state exchange game of [LTW08].

each chosen with probability $1/2$, to the players. They should produce answers with even parity in case they were sent a "$+$" state, and odd in case it was a "$-$" state. We show that the games (C_n) satisfy $\omega^*(C_n) = 1/n$, while $\omega^*(C_n \otimes C_n) \geq 1/(2n) \gg (\omega^*(C_n))^2$: the entangled value of quantum XOR games does not satisfy a perfect parallel repetition theorem. This again contrasts with the setting of classical XOR games, which do satisfy perfect parallel repetition [CSUU08]. As a counterpoint to this result, we also introduce a general class of rank-one games, OH_n-games, inspired by the operator Hilbert space OH [Jun05] and for which we can prove that some form of parallel repetition holds.

Algorithms. Remarkably, despite encompassing a wide variety of behaviors, both rank-one and quantum XOR games remain tractable models, as is demonstrated by our main theorem.

Theorem. *There exists a polynomial-time algorithm which, given as input an explicit description of a quantum XOR game G, outputs two numbers $\omega^{nc}(G)$ and $\omega^{os}(G)$ such that*

$$\omega(G) \leq \omega^{me}(G) \leq \omega^{nc}(G) \leq 2\sqrt{2}\,\omega(G) \qquad \text{and} \qquad \omega^*(G) \leq \omega^{os}(G) \leq 2\,\omega^*(G). \tag{1}$$

The same algorithm can be used to obtain a factor-4 approximation to the entangled value of a rank-one game.

Thus, despite the fact that the quantities $\omega(G)$ and $\omega^*(G)$ can differ greatly, both have nontrivial efficient approximations. We are not aware of any other model with this property. Moreover, the approximations claimed in the theorem are all obtained as the optimum of a polynomial-sized semidefinite program. This property might aid in finding games that exhibit large separations between entangled and unentangled biases, say for the purposes of experimental demonstrations.

The efficient algorithm posited in the theorem also allows us to derive interesting non-algorithmic conclusions. For instance, as an immediate corollary of the first sequence of inequalities stated in the theorem we obtain that, for any quantum XOR game G, $\omega^{me}(G) \leq 2\sqrt{2}\omega(G)$: maximally entangled states only provide a bounded advantage over no entanglement at all. This is in contrast with the general entangled case: the family (T_n) shows that $\omega^*(G)$ can be arbitrarily larger than $\omega(G)$.

Techniques: Grothendieck inequalities. Our main theorem is proved by establishing a strong connection between rank-one and quantum XOR games on the one hand, and two deep extensions of Grothendieck's inequality on the other. The first extension, which is used to prove the sequence of inequalities surrounding ω^{nc}, is known as the *non-commutative Grothendieck inequality*. The inequality, already conjectured by Grothendieck [Gro53], was proved by Pisier [Pis78] and then in a more general form by Haagerup [Haa85]. The second one, which is used to prove the sequence of inequalities surrounding ω^{os}, is known as the *operator space Grothendieck inequality* and was proved by Pisier and Shlyakhtenko [PS02] and by Haagerup and Musat [HM08]. In fact, the connection between the models we introduced and operator space theory runs at many different levels: for instance, the class of Schur games introduced above is motivated by the role of Schur multipliers in functional analysis, and the relationship between the entangled and "one-way" value of Schur games can be deduced from the operator space Grothendieck inequality. An additional example is our proof that the inequality $\omega^*(G) \leq \omega^{os}(G)$ from (1) can be strict, which requires us to improve a weaker and highly non-explicit separation obtained in the theory of jointly completely bounded bilinear forms [HI95].

Most of the effort in establishing our main theorem goes into interpreting the aforementioned Grothendieck inequalities as statements relating biases to semidefinite programs, for which efficient algorithms are known. Our results give the first application of these inequalities to quantum information theory, and we hope that our self-contained presentations will contribute to promoting those inequalities as powerful tools in complexity theory and quantum information theory, and will lead to further applications.

References

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25):1804–1807, 1982.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BRSdW11] H. Buhrman, O. Regev, G. Scarpa, and R. de Wolf. Near-optimal and explicit Bell inequality violations. In *Proc. 26th IEEE Conf. on Computational Complexity (CCC'11)*, pages 157–166. 2011.

[Bus12] F. Buscemi. All entangled quantum states are nonlocal. *Phys. Rev. Lett.*, 108:200401, May 2012.

[BV12] J. Briët and T. Vidick. Explicit lower and upper bounds on the entangled value of multiplayer XOR games, 2012. To appear in Comm. Math. Phys. Technical report arXiv:1108.5647.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proc. 19th IEEE Conf. on Computational Complexity (CCC'04)*, pages 236–249. 2004.

[CJPP11] T. Cooney, M. Junge, C. Palazuelos, and D. Pérez-García. Rank-one quantum games, 2011. Technical report arXiv:1112.3563.

[CSUU08] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. *Comput. Complexity*, 17:282–299, 2008.

[Gro53] A. Grothendieck. Résumé de la théorie métrique des produits tensoriels topologiques. *Bol. Soc. Mat. São Paulo*, 8:1–79, 1953.

[Haa85] U. Haagerup. The Grothendieck inequality for bilinear forms on C^*-algebras. *Adv. in Math.*, 56(2):93 – 116, 1985.

[HI95] U. Haagerup and T. Itoh. Grothendieck type norms for bilinear forms on C^*-algebras. *J. Operator Theory*, 34(2):263–283, 1995.

[HM08] U. Haagerup and M. Musat. The Effros-Ruan conjecture for bilinear forms on C^*-algebras. *Invent. Math.*, 174:139–163, 2008.

[JP11] M. Junge and C. Palazuelos. Large violation of Bell inequalities with low entanglement. *Comm. Math. Phys.*, 306(3):695–746, 2011.

[JPP+10] M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, and M. Wolf. Unbounded violations of bipartite Bell inequalities via Operator Space theory. *Comm. Math. Phys.*, 300(3):715–739, 2010.

[Jun05] M. Junge. Embedding of the operator space OH and the logarithmic little Grothendieck inequality. *Invent. Math.*, 161:225–286, 2005.

[KM03] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[LTW08] D. Leung, B. Toner, and J. Watrous. Coherent state exchange in multi-prover quantum interactive proof systems, 2008. Technical report arXiv:0804.4118.

[Pis78] G. Pisier. Grothendieck's theorem for noncommutative C^*-algebras, with an appendix on Grothendieck's constants. *J. Funct. Anal.*, 29(3):397–415, 1978.

[PS02] G. Pisier and D. Shlyakhtenko. Grothendieck's theorem for operator spaces. *Invent. Math.*, 150:185–217, 2002.

[PWP+08] D. Pérez-García, M. M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge. Unbounded violation of tripartite Bell inequalities. *Comm. Math. Phys.*, 279:455, 2008.

[Reg12] O. Regev. Bell violations through independent bases games. *Quantum Information and Computation*, 12(1):9–20, 2012.

[RV12] O. Regev and T. Vidick. Quantum XOR games, 2012. Technical report arXiv:1207.4939.

[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4:93–100, 1980.

[Tsi87] B. S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *J. Soviet Math.*, 36:557–570, 1987.