Extended Abstract

One fantastic implication of quantum mechanics is that measurements made on quantum mechanical systems can produce correlated outcomes irreproducible by any classical system. This observation is at the heart of Bell's celebrated 1964 inequality [2] and has since found applications in cryptography [1, 14, 28, 10], delegated computing [24] and short depth circuits [4, 30, 16], among others. Recent results have shown the sets of correlations producible by measuring quantum states are incredibly difficult to characterize [21, 13, 19, 11, 26, 9].

In this work, we present a result in the opposite direction. We consider a natural question concerning existence of quantum correlations which has been open for decades and is comparable to the one shown to be undecidable in [26]. We show it can be answered in polynomial time. Furthermore we show that when these correlations can be produced, they can be produced by simple measurements of a finite dimensional quantum state. We begin by reviewing some necessary background.

Nonlocal Games. Nonlocal games describe experiments which test the correlations that can be produced by measurements of quantum systems. A nonlocal game involves a *referee* (also called the *verifier*) and $k \geq 1$ *players* (also called *provers*). In a round of the game, the verifer selects a vector of questions $q = (q_1, q_2, ..., q_k)$ randomly from a set S of possible questions, then sends player i question q_i. Each player responds with an answer a_i. The players cannot communicate with each other when choosing their answers. After receiving an answer from each player, the verfier computes a *score* $V(a_1, a_2, ..., a_k|q_1, q_2, ..., q_k)$ which depends on the questions selected and answers recieved. The players know the set of possible questions S and the scoring function V. Their goal is to chose a *strategy* for responding to each possible question which maximizes their score in expectation. The difficulty for the players lies in the fact that in a given round each player only has partial information about the questions sent to other players.

For a given game G, the supremum of the expected scores achievable by players is called the *value* of the game. The value depends on the resources available to the players. If players are restricted to classical strategies, the value is called the *classical value* and denoted $\omega(G)$. If players can make measurements on a shared quantum state (but still can't communicate) the value can be larger and is called the *entangled value*. More specifically, if the players shared state lives in a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_k$ and the i-th player makes a measurement on the i-th Hilbert space, the supremum of the scores the players can obtain is called the *tensor product value*, denoted ω^*_{tp}. If the players share an arbitrary state and the only restriction placed on their measurements is that the measurement operators commute (enforcing no-communication), the supremum of the achievable scores is called the *commuting operator value*, denoted ω^*_{co}. When the state shared by the players is finite dimensional these definitions coincide. In the infinite dimensional case $\omega^*_{tp} \leq \omega^*_{co}$, and there exist games for which the inequality is strict [19, 26, 13].

Bounds On the Value. The commuting operator and tensor product values of a game are in general uncomputable [19, 26]. Intuitively, this is because the nonlocal games formalism places no restriction on the dimension of the state shared by the players, and so a brute force search over strategies will never terminate. However, such a search can provide a lower bound on the value of a game. Given a game G, let $\omega^*_d(G)$ denote the maximum score achievable by players using states of dimension at most d. This value lower bounds the tensor product (hence, commuting operator) value, and converges to the tensor product value in the limit as $d \to \infty$ [25], so $\sup_{d<\infty} \{\omega^*_d\} = \omega^*_{tp}$. Given a fixed d, ω^*_d can be computed by exhaustive search. Computing ω^*_d for an increasing sequence of d's produces a sequence of lower bounds that converge to ω^*_{tp} from below.

It is also possible to bound the commuting operator value of a nonlocal game from above, via a convergent hierarchy of semidefinite programs known as the *NPA hierarchy* [22, 12]. When run to a finite level, this hierarchy gives an upper bound on the commuting operator value of a game. However there is no guarantee that this bound can be achieved by any commuting operator strategy, hence no guarantee that the upper bound matches the true commuting operator value. In general all that can be said is that this hierarchy is complete, meaning that the bound computed necessarily converges to the commuting operator value of the game. Because of the previously mentioned undecidability results, no general bounds can be put on this rate of convergence.

XOR Games. XOR games are one family of games for which more concrete results are known. These are nonlocal games where each question q_j is drawn from an alphabet of size n, player's responses are single bits $a_i \in \{0, 1\}$ and the scoring function checks if the the overall parity of the responses matches a desired parity s_j associated with the question, that is

$$V(a_1, a_2, ..., a_k|q_1, q_2, ..., q_k) = \begin{cases} 1 \text{ if } \sum_i a_i = s_j \pmod 2 \\ 0 \text{ otherwise.} \end{cases} \tag{0.1}$$

We refer to an XOR game with k players as a kXOR Game. It is helpful to think of an kXOR game as testing satisfiabiliy of a set of clauses:

$$\hat{X}^{(1)}_{q_{11}} + \hat{X}^{(2)}_{q_{12}} + ...\hat{X}^{(k)}_{q_{1k}} = s_1,\ \hat{X}^{(1)}_{q_{21}} + \hat{X}^{(2)}_{q_{22}} + ...\hat{X}^{(k)}_{q_{2k}} = s_2,\ ...,\ \hat{X}^{(1)}_{q_{m1}} + \hat{X}^{(2)}_{q_{m2}} + ...\hat{X}^{(k)}_{q_{mk}} = s_m,$$

where each clause $\hat{X}^{(1)}_{q_{j1}} + ... + \hat{X}^{(k)}_{q_{jk}} = s_j$ corresponds to a question vector $(q_{j1}, q_{j2}, ..., q_{jk})$ with associated parity bit s_j. If question vectors are chosen uniformly at random, the classical value of the game corresponds to the maximum fraction of simultaneously satisfiable clauses. The tensor product and commuting operator values have no such interpretation, and may be larger.

2XOR games are well understood. In 1987, Tsirelson showed the optimal value for any 2XOR game can always be achieved by a finite dimensional strategy which can be found in polynomial time [27]. As a consequence $\omega^*_{co} = \omega^*_{tp}$ for any 2XOR game.

For kXOR games with $k > 2$ the situation is more opaque. There exist polynomial time algorithms that can compute ω^*_{co} and ω^*_{tp} in special cases [29, 31]. On the other hand it is NP-hard to compute the classical value of a 3XOR game [17], and there is no known upper bound on the runtime required to compute the commuting operator or tensor product value of a kXOR game when $k \geq 3$. Furthermore, the commuting operator and tensor product values of a k-XOR game are not known to coincide. One natural and efficiently solvable problem involving kXOR games is identifying games with perfect classical value $\omega = 1$. This is equivalent to asking if the corresponding set of clauses is exactly solvable, so can be answered in polynomial time using Gaussian elimination.

Interestingly, there exist XOR games with $\omega^*_{tp} = 1$ and $\omega < 1$; the sets of clauses associated with these games appear perfectly solvable when the game is played by players sharing an entangled state, despite the clauses having no actual solution. The most famous of these XOR *pseudotelepathy games* [3] is the GHZ game, a 3XOR game with 4 clauses and classical value $\omega = 3/4$. There is a perfect value tensor product strategy for this game involving measurements of the GHZ state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ so $\omega^*_{tp}(\text{GHZ}) = \omega^*_{co}(\text{GHZ}) = 1$ [15, 20].

The relative difficulty of computing the classical value of kXOR games compared to the ease of identifying kXOR games with perfect classical value motivates an analogous question concerning the entangled values. Does there exist a non-commutative analogue of Gaussian elimination that can easily identify kXOR games with ω^*_{co} or $\omega^*_{tp} = 1$? How hard is it to identify XOR pseudotelepathy games?

Bias. XOR games can also be characterized by their *bias* $\beta(G)$, defined by $\beta(G) = 2\omega(G) - 1$.[1] The *entangled biases* β^*_{co} and β^*_{tp} are defined analogously. A completely random strategy for answering an XOR game will achieve a score of $1/2$, hence $\omega(G) \geq 1/2$ and $\beta(G) \in [0, 1]$, with identical bounds holding on the other biases. When comparing classical and entangled biases, the quantity usually considered is the ratio $\beta^*_{tp}(G)/\beta(G)$ (or $\beta^*_{co}(G)/\beta(G)$), called the quantum-classical gap.

For 2XOR games this gap can be related to the Grothendieck inequality, with

$$\beta^*_{co}(G)/\beta(G) = \beta^*_{tp}(G)/\beta(G) \leq K^{\mathbb{R}}_G \tag{0.2}$$

where $K^{\mathbb{R}}_G$ is the real Grothendieck constant[2]. For 3XOR games no such bound holds [23, 6], and there exist families of games $\{G_n\}_{n\in\mathbb{N}}$ with

$$\lim_{n\to\infty} \beta^*_{tp}(G_n)/\beta(G_n) = \infty. \tag{0.3}$$

Our Main Results. This paper considers perfect commuting operator strategies for XOR games. We first show a link between XOR games and algebraic combinatorics: proving a kXOR game has value $\omega^*_{co} = 1$ iff an instance of the subgroup membership problem on a group corresponding to the kXOR game has no for an answer. For kXOR games with $k \geq 3$, the corresponding class of groups has undecidable subgroup membership problem. A priori, it is not clear whether or not the instances determining if a game has value $\omega^*_{co} = 1$ are decidable. We resolve the 3XOR case by proving an algebraic result, showing the instances of the subgroup membership problem determining the value of 3XOR games are equivalent to instances on a simpler group G/K obtained from G by modding out a particular normal subgroup K. This equivalence lets us construct a polynomial time algorithm that determines if 3XOR games do or do not have value $\omega^*_{co} = 1$. Previously this problem was not known to be decidable.

Combining this result with arguments from [29] shows 3XOR games with $\omega^*_{co} = 1$ also have perfect value tensor product strategies, with the players sharing a three qubit GHZ state. Combining that observation with the known bounds on the quantum-classical gap for strategies using a GHZ state [23, 5] shows that 3XOR games with $\omega^*_{co} = 1$ have classical value bounded a constant distance above $1/2$. In other words, when $\omega^*_{co} = 1$, how well quantum bias outperforms classical bias is bounded. This is in contrast with the behavior, see Equation (0.3), of not perfect games.

These results completely characterize 3XOR correlations, and dramatically simplify our understanding of the resources required to generate them. Additionally, the equivalence we show between perfect value XOR games and the subgroup membership problem allows for new analysis of k player XOR games and may be extendable to study other nonlocal games.

Comparison with Other Work. Our result shares high-level structure with the work of Cleve and coauthors [8, 7] and followup work by Slofstra [26] concerning linear systems games, though our work comes to a very different conclusion than theirs. In both that work and ours, perfect value commuting operator strategies are shown to exist for a family of nonlocal games iff an algebraic property is satisfied on a related group. In [26], Slofstra showed that the algebraic property associated with linear systems games was undecidable, implying existence of a linear systems game whose only perfect value strategies were incredibly complicated (infinite dimensional). Here we show the algebraic property associated with perfect value 3XOR games can be checked in polynomial time, and give a finite dimensional strategy, called a MERP strategy, that achieves value 1 whenever a perfect value commuting operator strategy exists.

[1] Some definitions vary by a factor of 2, defining $\beta(G) = \omega(G) - 1/2$

[2] Because $\omega^*_{co} = \omega^*_{tp}$ for 2XOR games, we also have $\beta^*_{co} = \beta^*_{tp}$

The MERP strategy is a variant of the GHZ strategy that has been considered before. In [31] this strategy was shown to be optimal for kXOR games with two questions per player. In [29] this strategy was shown to be optimal for a restricted class of XOR games (symmetric kXOR games)[3] with perfect value. In [18] a quantum circuit closely related to this strategy was used as a subroutine in short depth circuits.

References

[1] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical review letters*, 95(1):010503, 2005. [p. 1]

[2] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964. [p. 1]

[3] G. Brassard, A. Broadbent, and A. Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005. [p. 2]

[4] S. Bravyi, D. Gosset, and R. König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018. [p. 1]

[5] J. Briet, H. Buhrman, T. Lee, and T. Vidick. Multiplayer xor games and quantum communication complexity with clique-wise entanglement. *arXiv preprint arXiv:0911.4007*, 2009. [p. 3]

[6] J. Briët and T. Vidick. Explicit lower and upper bounds on the entangled value of multiplayer xor games. *Communications in Mathematical Physics*, 321(1):181–207, 2013. [p. 3]

[7] R. Cleve, L. Liu, and W. Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017. [p. 3]

[8] R. Cleve and R. Mittal. Characterization of binary constraint system games. In *International Colloquium on Automata, Languages, and Programming*, pages 320–331. Springer, 2014. [p. 3]

[9] A. Coladangelo and J. Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. *arXiv preprint arXiv:1804.05116*, 2018. [p. 1]

[10] R. Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, 2009. [p. 1]

[11] M. Coudron and W. Slofstra. Complexity lower bounds for computing the approximately-commuting operator value of non-local games to high precision. *arXiv preprint arXiv:1905.11635*, 2019. [p. 1]

[12] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 199–210. IEEE, 2008. [p. 2]

[13] K. Dykema, V. I. Paulsen, and J. Prakash. Non-closure of the set of quantum correlations via graphs. *Communications in Mathematical Physics*, 365(3):1125–1142, 2019. [p. 1]

[3] Symmetric XOR games are XOR games whose scoring function is invariant under permutations of the players. As an example, this would force $V(a_1 \oplus a_2|q_1, q_2) = V(a_2 \oplus a_1|q_2, q_1)$ for a two player symmetric XOR game.

[14] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991. [p. 1]

[15] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12):1131–1143, 1990. [p. 2]

[16] D. Grier and L. Schaeffer. Interactive shallow clifford circuits: quantum advantage against nc^1 and beyond. *arXiv preprint arXiv:1911.02555*, 2019. [p. 1]

[17] J. Håstad. Some optimal inapproximability results. *Journal of the ACM (JACM)*, 48(4):798–859, 2001. [p. 2]

[18] P. Høyer and R. Špalek. Quantum fan-out is powerful. *Theory of computing*, 1(1):81–103, 2005. [p. 4]

[19] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. Mip*= re. *arXiv preprint arXiv:2001.04383*, 2020. [p. 1]

[20] N. D. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65(15):1838, 1990. [p. 2]

[21] A. Natarajan and J. Wright. Neexp in mip. *arXiv preprint arXiv:1904.05870*, 2019. [p. 1]

[22] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. [p. 2]

[23] D. Pérez-García, M. M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge. Unbounded violation of tripartite bell inequalities. *Communications in Mathematical Physics*, 279(2):455–486, 2008. [p. 3]

[24] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013. [p. 1]

[25] V. B. Scholz and R. F. Werner. Tsirelson's problem. *arXiv preprint arXiv:0812.4305*, 2008. [p. 1]

[26] W. Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 33(1):1–56, 2020. [pp. 1, 3]

[27] B. S. Tsirel'son. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Mathematical Sciences*, 36(4):557–570, 1987. [p. 2]

[28] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. *Communications of the ACM*, 62(4):133–133, 2019. [p. 1]

[29] A. B. Watts, A. W. Harrow, G. Kanwar, and A. Natarajan. Algorithms, bounds, and strategies for entangled xor games. *arXiv preprint arXiv:1801.00821*, 2018. [pp. 2, 3, 4]

[30] A. B. Watts, R. Kothari, L. Schaeffer, and A. Tal. Exponential separation between shallow quantum circuits and unbounded fan-in shallow classical circuits. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 515–526, 2019. [p. 1]

[31] R. F. Werner and M. M. Wolf. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Physical Review A*, 64(3):032112, 2001. [pp. 2, 4]