Extended abstract: The membership problem for constant-sized quantum correlations is undecidable

Honghao Fu, Carl A. Miller, and William Slofstra

In a Bell test scenario, two spatially separated parties, typically called Alice and Bob, make measurements on their local systems. Their behaviour is captured by the probability $P(a,b|x,y)$ that they measure outcomes a and b on measurements x and y. Assuming that Alice (resp. Bob) has n_A (resp. n_B) measurements, each with m_A (resp. m_B) outcomes, the collection

$$P = \{P(a,b|x,y) : 0 \leq a < m_A,\ 0 \leq b < m_B,\ 0 \leq x < n_A,\ 0 \leq y < n_B\} \subseteq \mathbb{R}^{n_A n_B m_A m_B}$$

is called the correlation for their measurements. We are interested in the study of sets of correlations. We let $C_c(n_A, n_B, m_A, m_B)$ denote the set of classical correlations, although we write C_c where we can to save space. Bell's theorem states that Alice and Bob can achieve correlations outside of C_c if they share an entangled quantum state [Bel64]. This leads to the question of which correlations can be achieved in quantum mechanics. To study this question, Tsirelson introduced the set of quantum correlations [Tsi93]. There are actually several ways to define the set of quantum correlations, depending on whether we assume that all Hilbert spaces are finite-dimensional, and whether we use the tensor-product axiom or commuting-operator axiom for joint systems. This leads to four different choices for the set of quantum correlations: the finite-dimensional quantum correlations C_q, the quantum-spatial correlations C_{qs}, the quantum-approximate correlations C_{qa}, and the commuting-operator correlatons C_{qc}. We use the same convention as for classical correlations, in that C_t refers to $C_t(n_A, n_B, m_A, m_B)$ when the tuple (n_A, n_B, m_A, m_B) is clear. Tsirelson suggested that all four sets should be equal, but we now know that all four sets are different, and hence give a strictly increasing sequence $C_c \subsetneq C_q \subsetneq C_{qs} \subsetneq C_{qa} \subsetneq C_{qc}$ [Slo19, CS18, JNV+20]. The last inequality $C_{qa} \subsetneq C_{qc}$ is a very exciting consequence of the recent proof [JNV+20] that $MIP^* = RE$ by Ji, Natarajan, Vidick, Wright, and Yuen.

As the convex hull of a finite set, C_c is a polytope in $\mathbb{R}^N$, where $N = n_A n_B m_A m_B$. The sets C_t, $t \in \{q, qs, qa, qc\}$, are also convex subsets of $\mathbb{R}^N$ (in addition, C_{qa} and C_{qc} are closed), but it follows from a result of Tsirelson [Tsi87] that these sets are not polytopes. Folowing up in [Tsi93], Tsirelson asks whether the sets of quantum correlations might still have nice geometric descriptions, specifically by analytic or even polynomial inequalities. This question is significant for two reasons:

(1) (Practical) The quantum correlation set captures what is possible with quantum entanglement, and thus a description of this set tells us what is theoretically achievable in experiments and quantum technologies.

(2) (Conceptual) A nice description of the set of quantum correlations could improve our conceptual understanding of quantum entanglement, similarly to how the description of C_c as the convex hull of deterministic correlations is central to our understanding of classical correlations.

Due to the significance of this question, describing the set of quantum correlations has been a central question in the field. However, such descriptions have been hard to come by. On the geometric side, Tsirelson original results show that when $m_A = m_B = 2$, a certain linear slice of the quantum correlation set is the elliptope, a convex set described by quadratic inequalities

[Tsi87, TVC19]. Other work has focused on the case when $n_A = n_B = m_A = m_B = 2$, which is much more tractable then the general case [Lan88, WW01, Mas03, Pit08, GKW+18]. A result of Russell describes another linear slice, the synchronous correlations, in $C_q(3,3,2,2)$, but again this description does not extend to other numbers of measurements and outcomes [Rus20]. In another line, a number of authors have considered whether it's possible to give a conceptual, rather than geometric, description of the quantum correlation sets, but so far these do not give a complete description of the set of quantum correlations [BBL+06, PPK+09, NW09, FSA+13, SGAN18].

Because of the apparent difficulty in describing quantum correlation sets, it makes sense to ask if there are obstacles to having nice descriptions. One way to examine this question is by looking at the problem of computing the quantum value of a nonlocal game, which amounts to optimizing a linear functional over the sets C_{qa} or C_{qc}. The difficulty of this task is closely related to the computational complexity class MIP^*, and prior to this year there has been series of deep works showing that even the approximate version of this optimization problem is very difficult [IV12, RUV13, Ji17, NV18, NV17, FJVY19, NW19]. In the exact (rather than approximate) case, results of the last author imply that the decision problems

(PerfectStrategy_t) Given a tuple (n_A, n_B, m_A, m_B) and a nonlocal game G with n_A and n_B questions and m_A and m_B answers, does G have a perfect strategy in C_t?

are undecidable for $t \in \{q, qs, qa, qc\}$ (whether or not a nonlocal game has a perfect strategy corresponds to asking whether a certain linear functional takes value 1 on the set C_t) [Slo19, Slo20]. Ultimately, in the approximate case, the proof that $MIP^* = RE$ shows that a gapped version ($\text{GappedPerfectStrategy}_t$) of ($\text{PerfectStrategy}_t$) is also undecidable for $t \in \{q, qs, qa\}$ [JNV+20].

Rather than looking at nonlocal games, a more straightforward way to study the difficulty of describing quantum correlation sets is to look at the membership problem for these sets. Specifically, we can look at the decision problems

($\text{Membership}_{t,\mathbb{K}}$) Given a tuple (n_A, n_B, m_A, m_B) and a correlation $P \in \mathbb{K}^{n_A n_B m_A m_B}$, is $P \in C_t(n_A, n_B, m_A, m_B)$?

for $t \in \{q, qs, qa, qc\}$ and subfields $\mathbb{K} \subseteq \mathbb{R}$. The point of restricting to correlations in $\mathbb{K}^{n_A n_B m_A m_B}$ rather than $\mathbb{R}^{n_A n_B m_A m_B}$ is that it is not possible to describe all real numbers in a finite fashion. We are primarily interested in fields, such as $\mathbb{Q}$, where it is practical to work with elements of the field on a computer. For our results we actually need to take a larger field than $\mathbb{Q}$, so in what follows we'll set $\mathbb{K} = \overline{\mathbb{Q}} \cap \mathbb{R}$ unless otherwise noted, where $\overline{\mathbb{Q}}$ is the algebraic closure of the rationals.[1] The questions ($\text{Membership}_{t,\mathbb{K}}$) are a very general way of studying descriptions of the sets C_t for $t \in \{q, qs, qa, qc\}$, since we don't restrict to any particular form of description, but instead just look at a basic functionality that we would hope to have from any nice description, namely a way of being able to distinguish elements inside the set from those outside. The decision problems ($\text{Membership}_{t,\mathbb{K}}$) are not equivalent to the problems (PerfectStrategy_t) or ($\text{GappedPerfectStrategy}_t$), since nonlocal games do not necessarily have unique perfect strategies in C_t. Nonetheless, the two families of decision problems are closely related. Indeed, Coudron and the last author show that the methods used in [Slo20] to prove the undecidability of ($\text{PerfectStrategy}_{qc}$) also imply the undecidability of ($\text{Membership}_{qc,\mathbb{K}}$) [CS19]. The methods of [Slo19] can be adapted to show the undecidability of ($\text{Membership}_{t,\mathbb{K}}$) for $t \in \{q, qs, qa\}$ in similar fashion (although some work is needed for the case $t = q$). The undecidability of ($\text{GappedPerfectStrategy}_t$) can be used to get the stronger result that ($\text{Membership}_{t,\mathbb{Q}}$) is undecidable for $t \in \{q, qs, qa\}$ [JNV+20]. Taken together, these

[1] Since $\overline{\mathbb{Q}}$ is computable, it is possible to work with $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}} \cap \mathbb{R}$ on a computer, and indeed support for this is included in Mathematica and other computer algebra packages.

undecidability results put very strong restrictions on what descriptions of the quantum correlation sets are possible. For instance, they imply that there is no Turing machine which takes tuples (n_A, n_B, m_A, m_B) as inputs, and output a description of $C_t(n_A, n_B, m_A, m_B)$ in terms of a finite list of polynomial inequalities, since such a Turing machine would allow us to decide $(\text{Membership}_{t,\mathbb{K}})$. Similarly, these results also imply that there can be no finite set of principles, independent of (n_A, n_B, m_A, m_B), such that we can decide whether a correlation satisfies every principle, and such that a correlation satisfies all the principles if and only if it belongs to $C_t(n_A, n_B, m_A, m_B)$.

Although the undecidability results mentioned in the last two paragraphs go a long way to showing that the quantum correlation sets C_t do not have nice descriptions, there is a gap: they leave open the possibility that every set $C_t(n_A, n_B, m_A, m_B)$ has a nice description, but it's just not possible to have a Turing machine which outputs these descriptions as a function of (n_A, n_B, m_A, m_B). Of course, without a way to get the descriptions of the sets C_t, it would be difficult to use the existence of such descriptions for a practical purpose. Nonetheless, if we knew that, for instance, $C_t(n_A, n_B, m_A, m_B)$ had a description by quadratic polynomial inequalities, it would tell us a lot about the geometry and character of that set, even if we couldn't find the inequalities. Our main result is that, for large enough number of measurements and measurement outcomes, nice descriptions of the sets $C_t(n_A, n_B, m_A, m_B)$ aren't possible, at least for $t \in \{qa, qc\}$. Specifically, we look at the membership problems

$$(\text{Membership}(n_A, n_B, m_A, m_B)_{t,\mathbb{K}}) \quad \text{Given } p \in \mathbb{K}^{n_A n_B m_A m_B}, \text{ is } p \in C_t(n_A, n_B, m_A, m_B)?$$

for $t \in \{q, qs, qa, qc\}$ with (n_A, n_B, m_A, m_B) fixed. We show:

Theorem 0.1. *(Informal version) There is an integer α_0 such that the decision problem $(\text{Membership}(n_A, n_B, m_A, m_B)_{t,\mathbb{K}})$ is undecidable for $t \in \{qa, qc\}$ and $n_A, n_B, m_A, m_B > \alpha_0$.*

This implies that for $t \in \{qa, qc\}$ and large enough (n_A, n_B, m_A, m_B), there is no description of $C_t(n_A, n_B, m_A, m_B)$ that would allow us to decide membership in this set. This rules out a large class of descriptions, including descriptions by a finite list of polynomial inequalities. As mentioned above, in this theorem $\mathbb{K}$ is the intersection $\overline{\mathbb{Q}} \cap \mathbb{R}$. However, the proof of this theorem does not rely on writing down very complicated elements of $\overline{\mathbb{Q}}$. In fact, $\mathbb{K}$ could be replaced with $\mathbb{K}_0 \cap \mathbb{R}$, where $\mathbb{K}_0$ is the subfield of $\overline{\mathbb{Q}}$ generated by roots of unity.

To prove Theorem 0.1, we combine techniques from [Slo19, Slo20] with self-testing methods from [Fu19]. Specifically, [Fu19] shows that it is possible to self-test a maximally entangled state of arbitrary dimension, using constant-sized correlations. This is done by self-testing a relation $T^p = 1$ for a certain word T in the observables used in the correlation, and a chosen integer p. The methods used in [Slo19, Slo20] are group-theoretic, and involve reducing from nonlocal games to the word problem for groups. We combine these approaches by using families of finitely-presented groups, where the presentation includes the relation $T^p = 1$, and the outcome of the word problem for a certain known element depends on the choice of p.

Finally, it is interesting to consider upper bounds on the problems $(\text{Membership}(n_A, n_B, m_A, m_B)_{t,\mathbb{K}})$. When $t = qc$, this problem is contained in coRE, and Theorem 0.1 actually shows that this problem is coRE-complete (for large enough n_A, n_B, m_A, m_B). When $t = q$ or $t = qs$, this problem is contained in RE, but when $t = qa$, the best known upper bound on this decision problem is Π_2^0. In this case, Theorem 0.1 only shows that $(\text{Membership}(n_A, n_B, m_A, m_B)_{qa,\mathbb{K}})$ is coRE-hard, so this lower bound is not necessarily tight. Recently, Mousavi, Nezhadi, and Yuen have shown that the three-player version of $(\text{PerfectStrategy}_{qa})$ is Π_2^0-complete [MNY20], and it seems reasonable to conjecture that $(\text{Membership}(n_A, n_B, m_A, m_B)_{qa,\mathbb{K}})$ is also Π_2^0-complete for large enough n_A, n_B, m_A, m_B. We leave this as an open problem.

References

[BBL+06] G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, and F. Unger. A limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96(250401), 2006. URL: https://link.aps.org/doi/10.1103/PhysRevLett.96.250401, doi:10.1103/PhysRevLett.96.250401.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964. URL: https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195, doi:10.1103/PhysicsPhysiqueFizika.1.195.

[CS18] Andrea Coladangelo and Jalex Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. *arXiv preprint arXiv:1804.05116*, 2018.

[CS19] Matthew Coudron and William Slofstra. Complexity lower bounds for computing the approximately-commuting operator value of non-local games to high precision. *arXiv preprint arXiv:1905.11635*, 2019.

[FJVY19] Joseph Fitzsimons, Zhengfeng Ji, Thomas Vidick, and Henry Yuen. Quantum proof systems for iterated exponential time, and beyond. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 473–480. ACM, 2019. doi:10.1145/3313276.3316343.

[FSA+13] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acin. Local orthogonality as a multipartite principle for quantum correlations. *Nature Communications*, 4(2263), 2013. doi:10.1038/ncomms3263.

[Fu19] Honghao Fu. Constant-sized correlations are sufficient to robustly self-test maximally entangled states with unbounded dimension. *arXiv preprint arXiv:1911.01494*, 2019.

[GKW+18] Koon Tong Goh, Jedrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.022104, doi:10.1103/PhysRevA.97.022104.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled provers. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 243–252. IEEE, 2012. doi:10.1109/FOCS.2012.11.

[Ji17] Zhengfeng Ji. Compression of quantum multi-prover interactive proofs. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 289–302, 2017. URL: https://doi.org/10.1145/3055399.3055441, doi:10.1145/3055399.3055441.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. $MIP^* = RE$. *arXiv preprint arXiv:2001.04383*, 2020.

[Lan88] L. J. Landau. Empirical two-point correlation functions. *Foundations of Physics*, 18:449–460, 1988. doi:10.1007/BF00732549.

[Mas03] Ll. Masanes. Necessary and sufficient condition for quantum-generated correlations. 2003. arXiv:quant-ph/0309137.

[MNY20] Hamoon Mousavi, Seyed Sajjad Nezhadi, and Henry Yuen. On the complexity of zero gap MIP. *arXiv preprint arXiv:2002.10490*, 2020.

[NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015. ACM, 2017. doi:10.1145/3055399.3055468.

[NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742. IEEE, 2018. doi:10.1109/FOCS.2018.00075.

[NW09] M. Navascues and H. Wunderlich. A glance beyond the quantum model. *Proc. Royal Soc. A*, 466:881–890, 2009. doi:10.1098/rspa.2009.0453.

[NW19] Anand Natarajan and John Wright. $NEEXP$ is Contained in MIP^*. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 510–518. IEEE, 2019. doi:10.1109/FOCS.2019.00039.

[Pit08] I. Pitowsky. Geometry of quantum correlations. *Physical Review A*, 77:062109, 2008. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.022104, doi:10.1103/PhysRevA.97.022104.

[PPK+09] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Zukowski. Information causality as a physical principle. *Nature*, 461:1101–1104, 2009. doi:10.1038/nature08400.

[Rus20] Travis B. Russell. Geometry of the set of synchronous quantum correlations. *Journal of Mathematical Physics*, 61:052201, 2020. doi:10.1063/1.5115010.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456, 2013. doi:10.1038/nature12035.

[SGAN18] Ana Belén Sainz, Yelena Guryanova, Antonio Acín, and Miguel Navascués. Almost-quantum correlations violate the no-restriction hypothesis. *Phys. Rev. Lett.*, 120:200402, May 2018. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.200402, doi:10.1103/PhysRevLett.120.200402.

[Slo19] William Slofstra. The set of quantum correlations is not closed. In *Forum of Mathematics, Pi*, volume 7. Cambridge University Press, 2019. doi:10.1017/fmp.2018.3.

[Slo20] William 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. doi:10.1090/jams/929.

[Tsi87] B.S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987. doi:10.1007/BF01663472.

[Tsi93] B.S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329–345, 1993.

[TVC19] Le Phuc Thinh, Antonios Varvitsiotis, and Yu Cai. Geometric structure of quantum correlators via semidefinite programming. *Phys. Rev. A*, 99:052108, May 2019. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.052108, doi:10.1103/PhysRevA.99.052108.

[WW01] R. F. Werner and M. M. Wolf. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64:032112, Aug 2001. URL: https://link.aps.org/doi/10.1103/PhysRevA.64.032112, doi:10.1103/PhysRevA.64.032112.