Non-local games in quantum information theory

organized by
Michael Brannan, Vern Paulsen, Ivan Todorov, and Anna Vershynina

Workshop Summary

The theory of non-local games crosses the boundaries of mathematics, theoretical physics and computer science, and has undergone a vigorous development in the past decade, showing the non-closure of the set of quantum correlations [slofstra$_JAMS$], $leadingtoaresolutionofthelong$-$standingTsirelsonproblemonquantumcorrelations[jnpp]and, dueto[jnvwy, ozawa], oftheConnesEmbedd$

Monday, May 17: Thomas Vidick and William Slofstra

Tuesday, May 18: Andreas Winter and Christopher Schafhauser

Wednesday, May 19: David Perez-Garcia and Samuel Harris

Thursday, May 20: Henry Yuen and David Roberson

Friday, May 21: Magdalena Musat and Marius Junge.

The following problem topics were brought forward during the Problem Session, held on Monday afternoon:

(i) Quantum input - quantum output games
(ii) Self-testing
(iii) Optimal synchronous strategies
(iv) Parallel repetition of non-local games
(v) Quantum graph isomorphisms
(vi) Algebras of games
(vii) Pseudo-telepathy games
(viii) Flip games

After voting, topics (vi)-(viii) did not gather sufficient participation for them to be isolated in separate discussion rooms. A summary of the proceedings in the rest of the discussion groups follows.

I. Quantum input - quantum output games

A first line of work was to unify the *apparently* different notions of games with quantum inputs and quantum outputs that were available. On the one hand, the more mathematical one presented in the talk by Samuel Harris on Wednesday 19th (let's call it Definition 1). On the other hand, the operational definition that goes back to the work [D. Leung, B. Toner, J. Watrous, Coherent state exchange in multi-prover quantum interactive proof systems]. A game is defined there as follows (Definition 2):

(1) The referee prepares three quantum registers (R, S, T) in some chosen state and send register S to Alice and register T to Bob.
(2) Alice and Bob act locally, (maybe using some extra shared entangled state), obtaining registers A and B respectively that are sent back to the referee

(3) The referee performs a binary-valued measure on the registers (R, A, B). The outcome 1 means that Alice and Bob win the game, the outcome 0 means that they lose

We managed to show that Definition 1 is included in Definition 2. A second line of work was motivated by a question of Henry Yuen, regarding the utility of quantum-XOR games or rank-one quantum games (as the simplest examples of games with quantum inputs or outputs) in the context of self-testing. Those games were introduced respectively in the papers [O. Regev, T. Vidick, Quantum XOR Games] and [T. Cooney, M. Junge, C. Palazuelos, and D. Perez-Garcia. Rank-one quantum games]. In particular the question was whether there exists a family of such games G_n, where n is the dimension of the input quantum register, so that the entangled value is $= 1$ and to achieve a value $\geq 1 - \varepsilon$ (ε independent of n) one requires an entangled state of dimension $d \geq 2^{\mathrm{poly}(n)}$. Using the embezzlement state as in the seminal construction [O. Regev, T. Vidick, Elementary Proofs of Grothendieck's Theorems for Completely Bounded Norms], we realized that answering this problem in the positive would require going beyond the current version of the operator space Grothendieck inequality of [U. Haagerup and M. Musat, The Effros-Ruan conjecture for bilinear forms on C*- algebras]. Since this seemed an extremely hard question, we then shifted the problem to the case of arbitrary quantum input and output games, but unfortunately without any success (so far).

II. Self-testing

Self-testing is a method for inferring the underlying quantum mechanical description of a system merely from classical observations. This method is usually applied in the context of some Bell scenario, where non-communicating parties, Alice and Bob, interact with a classical verifier. Alice and Bob collaborate in an attempt to win a certain game or produce a specific correlation (joint conditional probability distribution). A quantum strategy for Alice and Bob can be described by a triple $\mathcal{S} = (\psi, \{A_{xa}\}, \{B_{yb}\})$, where $\psi \in \mathbb{C}^d \otimes \mathbb{C}^d$ is the shared quantum state and $\{A_{xa}\}_{a \in A}$ specify a quantum measurement that Alice performs upon receiving question $x \in X$ and, similarly, $\{B_{yb}\}_{b \in B}$ are the measurements performed by Bob. In its most common form, a self-testing theorem asserts that *any* quantum strategy $\mathcal{S}$ which produces correlation $\tilde{p}$ can be seen as arising from a single *canonical* quantum strategy $\tilde{S}$. Specifically, given any $\mathcal{S} = (\psi, \{A_{xa}\}, \{B_{yb}\})$ which produces $\tilde{p}$, we can find a local isometry $V := V_A \otimes V_B$ such that for all x, y, a, b and some state ψ_{aux} we have

$$V(A_{xa} \otimes B_{yb})\psi = \left((\tilde{A}_{xa} \otimes \tilde{B}_{yb})\tilde{\psi}\right) \otimes \psi_{\mathrm{aux}},$$

where $\tilde{\mathcal{S}}$ is the canonical strategy. In practice we care about *robust* self-testing, where any strategy $\mathcal{S}$ producing a correlation ϵ-close to $\tilde{p}$ can be shown to satisfy the above equation up to some $f(\epsilon)$.

Most self-testing results are obtained using ad hoc techniques. One notable exception is a general method for obtaining *robust* self-testing results by leveraging the Gowers-Hatami theorem which guarantees the existence of an exact group representation near any approximate representation. The downside of this method is that it is only applicable in situations, where the game or correlation in question has an underlying group structure. A recent work by Mančinska, Prakash, and Schafhauser [MPS] suggests that similar stability results might hold for algebras. If true in general, this would allow to apply the previously mentioned proof strategy for games with an underlying algebra structure. The weak point of the stability

result obtained in [MPS] is that it is non-constructive and not efficient. We discussed how recent results by either Paul-Paddock or Vidick [Vid] on almost synchronous correlations could be used to promote the approximately tracial state in the hypothesis of the stability theorem from [MPS] to an exactly tracial state. We further discussed some ideas of how this tracial state could then help to eliminate the non-constructive elements in the proof and pave way to an efficient stability result for the algebras considered in [MPS].

We also discussed how self-testing could be defined in the commuting operator framework and if that relates in any way to a strategy being non-degenerate. A strategy is non-degenerate if there is no (nontrivial) projection Π that commutes with both Alice and Bobs projections and for which the state is invariant (i.e. $\Pi|\psi\rangle = |\psi\rangle$). The notion of non-degenerate strategies seems to go back to Tsirelson [Tsi], and is subsequently mentioned in [Slo].

III. Optimal synchronous strategies

For two person cooperative games there is a well developed theory that studies the optimal expected value of the game over various families of conditional probability densities. But this theory has not been developed for families of synchronous probability densities. A density is synchronous, if whenever both players receive the same input, the probability that they give different outputs is 0.

Synchronous densities are known to correspond to traces on C*-algebras and it is known that the proof that Connes' Embedding Problem has a negative answer passes through the theory of synchronous games. So a better understanding of synchronous values of games could lead to some simplifications of this result.

During the workshop, this theory was developed a bit, especially for games based around the colouring of graphs. Examples of synchronous games were found whose synchronous value was strictly smaller than their non-synchronous value. A famous theorem in the theory of games says that if the value of a game is less than one, then when the game is played n times in parallel, the value must decay to 0 as n grows. In stark contrast, a game was found whose synchronous value was monotone increasing in n.

IV. Parallel repetition of non-local games

One of the breakout sessions focused on the subject of "parallel repetition of games", which is about understanding the maximum success probability (i.e. the value) of the *parallel repeated* game G^k, as a function of the value of G (the "base" game) and the number of repetitions k. The behaviour of parallel repeated games (at least in the two-player setting) is well-understood in the case of classical strategies, but the case of quantum strategies (both finite-dimensional and commuting-operator) remain rather mysterious.

In the first breakout session, Laura Mancinska raised the interesting question if there are "genuinely quantum" counterexamples to parallel repetition. One formalisation of this question is the following: are there games G for which $val_c(G) < val_q(G) < 1$, where val_c denotes classical value and val_q denotes the quantum value, and $val_q(G^k)$ is different from both $val_q(G)^k$ and $val_c(G^k)$? This could indicate that optimal strategies for the repeated game G^k are using entanglement to "slow down" the rate of parallel repetition in an interesting way.

For the remainder of the breakout session (and also in the second meeting about parallel repetition), it was explored whether existing proofs for quantum parallel repetition can be

adapted to the infinite-dimensional (i.e. commuting operator) setting. Such a result would be interesting in its own right (it is not known whether the commuting operator value of general games decay at all), and also would have interesting complexity-theoretic applications (for example, it would be a useful for understanding the complexity of approximating the commuting-operator value). Specifically, discussions centred around the appropriate infinite-dimensional analogues of "reduced density matrix", "relative entropy", "data processing inequality", and so on. Based on the discussion, the prospect of adapting the proof techniques to the infinite-dimensional setting seems promising.

V. Quantum graph isomorphisms

The notion of quantum isomorphism is based on a *nonlocal game* in which two players, Alice and Bob, attempt to convince a referee that they know an isomorphism between two given graphs G and H. Formally, each player is given a vertex of one of the graphs and must respond with a vertex of the other. Thus Alice must either receive or respond with a vertex of G, say g_A. Similarly one can define h_A, g_B, and h_B. Alice and Bob win the game if g_A and g_B are related to each other (either equal, adjacent, or distinct non-adjacent) in the same way as h_A and h_B. Classically, this game can be won (with probability 1) if and only if the graphs G and H are isomorphic. Motivated by this, graphs are said to be *quantum isomorphic* if the corresponding isomorphism game can be won perfectly using a quantum strategy [qiso1], i.e., a strategy in which the players are allowed to share an entangled quantum state and each perform local measurements on their part of the state. This turns out to have an elegant formulation in terms of *quantum permutation matrices* (known as *magic unitaries* in the quantum group literature. A quantum permutation matrix is an $n \times n$ matrix $\mathcal{P} = (p_{ij})$ whose entries are elements of a C^*-algebra and satisfy

(1) $p_{ij} = p_{ij}^2 = p_{ij}^*$, i.e., the p_{ij} are projections;
(2) $\sum_k p_{ik} = \mathbf{1} = \sum_\ell p_{\ell j}$ for all $i, j \in [n]$.

Graphs G and H are quantum isomorphic if and only if there is a quantum permutation matrix $\mathcal{P}$ such that $A_G\mathcal{P} = \mathcal{P}A_H$, where A_G and A_H are the adjacency matrices of G and H. There is furthermore a way to reformulate quantum isomorphism purely in terms of quantum automorphism groups (despite the similar name, the latter concept arose in a completely different context in the area of noncommutative mathematics). It was shown in [qperms] that connected graphs G and H are quantum isomorphic if and only if there is an orbit of the quantum automorphism group of $G \cup H$ containing both a vertex from G and a vertex from H.

In addition to the relationship to quantum automorphism groups mentioned above, quantum isomorphism has been shown to have surprising and deep connections to other areas of mathematics, such as Morita equivalence, monoidal equivalence, and graph homomorphism counts. In our group we discussed the connection between quantum isomorphism and quantum/operator solutions of binary linear systems introduced by Cleve and Mittal. Given a linear system $Mx = b$ of m equations and n variables over $\mathbb{Z}_2$, a quantum solution to the system is an assignment $x_i \mapsto A_i$ of *self-adjoint* bounded linear operators on a Hilbert space such that

(1) $A_i^2 = I$ for all $i \in [n]$;
(2) $A_iA_j = A_jA_i$ if there exists $k \in [m]$ such that $M_{ki} = M_{kj} = 1$;
(3) $\prod_{i\in[n]} A_i^{M_{ki}} = (-1)^{b_k} I$ for all $k \in [m]$.

Such a quantum solution exists if and only if the corresponding linear system game can be won perfectly with a quantum strategy. Following the work of Cleve and Mittal, the important notion of the *solution group* of a binary linear system was introduced by Cleve, Liu, and Slofstra. For a given system $Mx = b$ with m equations and n variables, its solution group is generated by elements $g_1, \ldots, g_n$ and J that satisfy the following relations:

(1) $J^2 = e$ and $g_i^2 = e$ for all $i \in [n]$;
(2) $Jg_i = g_i J$ for all $i \in [n]$ and $g_i g_j = g_j g_i$ if there is $k \in [m]$ such that $M_{ki} = M_{kj} = 1$;
(3) $\prod_{i \in [n]} g_i^{M_{ki}} = J^{b_k}$.

Cleve, Liu, and Slofstra showed that quantum solutions are representations of the solution group where J is not mapped to the identity. This reformulation in terms of groups is in some ways analogous to the reformulation of quantum isomorphism in terms of quantum groups.

The connection between quantum isomorphism and binary linear systems was already established in the work where the former was introduced [qiso1]. Specifically, a construction was given which associates a graph $G(M, b)$ to any binary linear system $Mx = b$, and these graphs have the property that $G(M, b)$ is quantum isomorphic to $G(M, 0)$ if and only if $Mx = b$ has a quantum solution. It follows from this reduction that the group algebra of the solution group of a binary linear system $Mx = b$ is contained in the algebra associated to the isomorphism game for $G(M, b)$ and $G(M, 0)$. This means that the algebras associated to isomorphism games are in a certain sense at least as general as those associated to linear system games. Essentially this means that properties exhibited by linear system games (such as having quantum correlation sets that are not closed) can also be exhibited by isomorphism games. The main question addressed in our group was whether the converse was true.

We specifically sought a way to embed the algebra associated to an isomorphism game into the algebra of a linear system game. The algebra of the isomorphism game for G and H is the universal C^*-algebra generated by elements p_{gh} for $g \in V(G)$, $h \in V(H)$ such that $p_{gh} = p_{gh}^2 = p_{gh}^*$, and $p_{gh} p_{g'h'} = 0$ if g and g' are not related in the same way as h and h'. The main approach discussed was to try to use the generators p_{gh} to construct self-adjoint elements which square to the identity and generate the full algebra. Moreover, these elements would need to satisfy the relations of a solution group. For each $g \in V(G)$, $h \in V(H)$, the element $1 - 2p_{gh}$ is self-adjoint and squares to the identity, and the set of these elements generates the full algebra, but it is unclear how to find a solution group whose relations are satisfied by these elements. Unfortunately we were not able to solve this problem during the workshop.

Bibliography

[jnvwy] Z. Ji, A. Natarajan, T. Vidick, J. Wright and H. Yuen. MIP*=RE. preprint (2020), arXiv:2001.04383.

[jnpp] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. Scholz and R.F. Werner. Connes' emnedding problem and Tsirelson's problem. *J. Math. Phys.* 52, 012102 (2011), 12 pages.

[qiso1] A. Atserias, L. Mančinska, D. E. Roberson, R. Šámal, S. Severini and A. Varvitsiotis. Quantum and non-signalling graph isomorphisms. *J. Comb. Theory B* 136 (2019), 289-328.

[qperms] M. Lupini, L. Mančinska and D. E. Roberson. Nonlocal games and quantum permutation groups. *J. Funct. Anal.* 279 (2020), no. 5, 108592.

[MPS] L. Mančinska, J. Prakash, and C. Schafhauser. Constant-sized robust self- tests for states and measurements of unbounded dimension. *arXiv:2103.01729*, 2021.

[ozawa] N. Ozawa. About the Connes embedding conjecture: algebraic approaches. *Jpn. J. Math.* 8 (2013), no. 1, 147-183.

[Vid] T. Vidick. Almost synchronous quantum correlations. *arXiv:2103.02468*, 2021.

[Tsi] B. S. Tsirelson. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *J. Soviet Math.* 36 (1987), no. 4, 557-570.

[Slo] W. Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *arXiv:1007.2248*, 2010.

[slofstra$_J$*AMS*]*W.Slofstra.Tsirelson′sproblemandanembeddingtheoremforgroupsarisingfromnon*−*localgames.J. Amer. Math. Soc.*33(2020), *no.*1, 1 − 56.