Snapshots of modern mathematics
from Oberwolfach

№ 4/2023

Algebras and quantum games

Vern I. Paulsen [1]

Everyone loves a good game, but when the players can access the counterintuitive world of quantum mechanics, watch out!

"God does not play dice with the universe" – Albert Einstein

"Not only does God play dice but... he sometimes throws them where they cannot be seen." – Stephen Hawking

1 Playing games with quantum assistance

When one performs a measurement of a quantum system, the outcome is random and the probabilities to obtain the different outcomes turn out to have some very counterintuitive properties. In this snapshot we will discuss some games where using quantum mechanics to "randomly roll the dice" leads to much higher probabilities of winning than our classical intuition tells us is possible. *Classical* means here not *quantum*: anything that can be explained or understood without the notions from quantum physics will be deemed classical.

We will also look at *prover systems*, which are games that are designed to test if a solution to a problem has been found. Players can find strategies to win these games with certainty using classical methods, if and only if a solution to the related problem can be found. Prover systems can be used in situations where there are so many equations and so many variables that it is impractical to write down all the values of all the variables and check that they satisfy all the equations. Instead, if players keep giving correct answers each time that they play a round of a prover system game, then the "Referee" can feel fairly

[1] Vern Paulsen is supported by NSERC.

certain that the players have indeed solved the problem. Surprisingly, there are many prover systems for which quantum-assisted players can design a strategy that will always succeed, even when no actual solution exists! So players that have access to quantum phenomena can fool a prover system.

The games that we will look at all involve three parties. There are two players, who we will call Alice and Bob. Alice and Bob are not competing, but instead they cooperate in an attempt to return correct answers to questions posed by the third party, who we will call the Referee. The questions are called the *inputs* and the answers are called the *outputs* of the game.

One property of these games is that whether or not the pair of answers given by Alice and Bob is correct depends on the pair of questions Alice and Bob received, and not just on the question each of them received individually. So although Alice and Bob both know the rules, that is, they both know which pairs of answers are right for a pair of questions, they must both give their replies without knowing what question the other was asked. Formally, this is what is meant by saying that they are *non-communicating*. It is easiest to imagine that they are in separated soundproof rooms so that they cannot hear what the Referee tells the other player or what the other player tells the Referee. A schematic view of the situation can be seen in Figure 1. We will now look at a famous example of one of these games – the CHSH game – to illustrate these ideas.

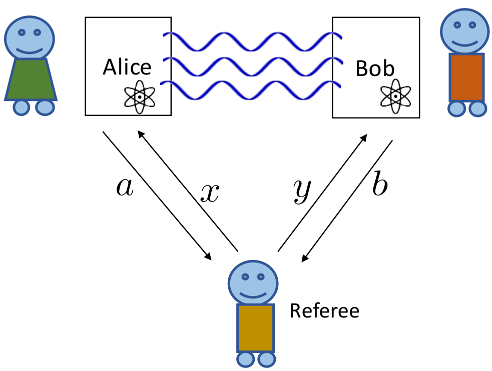

Figure 1: General depiction of a quantum game with three parties: Alice, Bob and the Referee. The variables a, b, x and y encode the information exchanged between them.

2 A practical example: the CHSH game

The name of the game introduced here will probably sound quite cryptic to the reader; it is refering to the “CHSH inequality”, which, roughly speaking, can be used to distinguish classical and quantum behaviors in a physical system. This inequality was derived jointly by Clauser, Holt, Shimony, and Horne [2], hence the name CHSH. The CHSH game was designed to illustrate that this inequality could be used to experimentally show that “entanglement” – a peculiar phenomena which we will touch upon later – is an actual phenomena and not a mere artefact of the theory [3].

In this game, Alice and Bob are each given a number by the Referee that can be either a 0 or a 1; we will denote this number by x for Alice and y for Bob. Alice and Bob must also return binary numbers (0 or 1), which will be denoted respectively by a and b. They will win the CHSH game if the sum of their numbers $a + b$ is of the same parity as the product $x\,y$. That is, they win if the quantity $a + b - x\,y$ yields an even number.

Suppose that Alice and Bob also know that the Referee will pick one of the four possible input pairs $(0, 0), (0, 1), (1, 0), (1, 1)$ randomly and with equal probability of $1/4$. A good strategy for Alice and Bob is to agree that no matter what they receive they will always answer with a 0. We would then have $a+b = 0$, which means that the game is won when $x\,y = 0$. Such values are obtained with three different pairs of input values: $(0, 0), (0, 1)$, and $(1, 0)$. The last pair $(1, 1)$ gives $x\,y = 1$, in which case they lose. This strategy therefore has a winning probability (or “value”) of $3/4$.

This strategy is an example of a “deterministic” strategy. *Deterministic* means that Alice and Bob have a rule (function) that determines their output depending on the input they receive. Another deterministic strategy with the same value would be where Alice and Bob agree to always return 1. For this game it is straightforward to list all the possible deterministic strategies, that is, the different pairs of functions, and to check that the strategies of always returning 0 or of always returning 1 are the two strategies with the highest probability of winning.

Next we want to introduce the idea of *random strategies*. With a random strategy a player might give different outputs for the same input received in two different rounds of the game. For example, a random strategy applied to the CHSH game could lead Alice to send $a = 0$ after receiving $x = 0$ in the first round, and $a = 1$ after receiving $x = 0$ again in the second round. Now let us talk about a specific class of such random strategies for the CHSH game: the *classical shared random strategy*. An example of such a strategy works as follows: Alice and Bob have a collection of deterministic strategies and at each round they choose one of them based on an additional shared random input. For example, the Referee might roll a die and tell them both the number on the die when he gives them their inputs. It can be shown that the highest winning probability of this strategy is still 3/4. Roughly speaking, this is because at each round they are still selecting a deterministic strategy. Now suppose that instead of a roll of the die, the external input is given by a pair of laser beams emitted by the Referee's device, one beam shining into each players' room. Each player designs two quantum experiments that can be performed with the laser beam they receive, and each measurement has two possible outcomes which we can label with a 0 and a 1. Such measurements can only be described by quantum theory, which is a theory giving probabilistic predictions on the outcomes of such experiments. Alice and Bob will perform one experiment or the other, depending on the input they receive from the Referee. Once the experiment is performed, they report their outcome back to the Referee. In this way, they randomly generate two outputs for their given inputs.

We now need to define a very important notion from quantum physics which we evoked earlier: *entanglement*. A quantum system can have the weird property of being entangled with another one. When this happens, it is impossible to completely describe this system without considering the other system it is entangled with. Acting on one of the two entangled systems will immediately affect the other system, even if they are separated by thousands of kilometers! This is a purely quantum property without classical equivalent that has been puzzling physicists since the birth of the quantum theory. Even Albert Einstein himself was bothered by this effect, as this instantaneous action at a distance seems to clash with his theory of relativity. Nowadays, entanglement is better understood but it remains one of the key features that contributes to the strangeness of quantum physics.

Coming back to the CHSH game, if the two laser beams are not entangled – in other words, if we are playing the "classical game", then the optimal winning probability is still 3/4. But if the laser beams are entangled in just the right way – that is, if we now play the quantum game – the winning probability can be as large as about 85%: $\cos^2(\pi/8)$ to be precise. Roughly speaking, this happens because when the lasers are entangled the outcome of the experiment performed on one laser influences the outcome of the experiment realised on the other laser. It is no wonder that Einstein referred to entanglement as a "spooky action at a distance".

It is important to emphasize that the laser beams contain no information about the questions that were asked by the Referee; that is, they do not vary with the different inputs the Referee can send. The lasers are just constantly in the same entangled state. This particular entangled state and the experiments that Alice and Bob will perform are chosen to achieve this higher winning probability for this particular game.

In practice, a pair of laser beams sold by a manufacturer as entangled can be tested by conducting an experiment that mimics the CHSH game. This is a way to ensure that they really are entangled. One can design a set of experiments and if the players consistently beat the highest classical probability of winning when performing measurements on the beams, then this gives evidence that they are indeed entangled. This is one way that the theory of these games can be used in a practical manner.

3 Quantum probability densities and Connes's embedding problem

One natural question would be: what mathematics can help us explain the features of the CHSH game? One way to answer this question is to invoke“quantum correlations”. Suppose that we play a game very many times, then eventually, from observations we can estimate the probability that if Alice and Bob receive the input pair (x, y) they will produce the output pair (a, b). This is called a *conditional probability density* and this fraction is generally denoted $p(a, b|x, y)$. The set of all such densities that can be obtained from classical shared random strategies, as described in Section 2, is called the set of *local conditional densities* and is denoted C_{loc}. The set of all such densities that can be obtained by quantum measurements on possibly entangled states is called the set of *quantum correlations*, and is denoted C_q.

The fact that by using quantum experiments we can increase our probability of winning the CHSH game is a proof that $C_{loc} \subsetneq C_q$. This means that C_{loc} is a (strictly smaller) subset of C_q. However, there are actually three possible mathematical models for describing the sets of quantum correlations. One is the standard model, so we will still denote that set by C_q. The other two sets of densities, obtained from more exotic models, will be denoted by C_{qa} and C_{qc}. We still don't know which of these sets C_q, C_{qa} or C_{qc}, if any, is exactly the set of conditional densities that can be obtained from the quantum world. Consequently there is some ambiguity in the literature about which of these three sets is meant by the term “quantum correlation”.

Mathematicians working with algebras of operators became interested in this question after it was shown that the two “exotic” models gave exactly the same set of densities, namely $C_{qa} = C_{qc}$, if and only if a famous problem in the area of operator algebras had a positive solution [9, 12]. This problem, “Connes's Embedding Problem”, was originally posed in 1967 by the Fields medallist Alain Connes [5].

The first person to show that C_q and C_{qa} are different sets of densities was William Slofstra [13]. He demonstrated it by using a prover system game for solving systems of linear equations, which we will describe later on. His proof showed the difference between these sets for a large number of inputs. Later the difference between C_q and C_{qc} was also shown to hold for small numbers of inputs and outputs [6, 4], and currently there are only a few remaining cases of input-output numbers for which the difference is unknown. Very recently the paper [8] (still under review at the time of writing this snapshot) has shown that C_{qa} and C_{qc} are different by using these types of games, providing a negative answer to Connes Embedding Problem.

4 Mermin's magic square and linear constraint games

The type of prover-system game used by Slofstra originates in games built around solving systems of linear equations over the binary field $\mathbb{Z}_2 = \{0, 1\}$. Suppose that we are given a set of m linear equations in n variables over the binary field $\mathbb{Z}_2$. We can write this in matrix form as $Mx = c$, where M is an $m \times n$ matrix with entries from $\mathbb{Z}_2$ (that is, a table with m lines and n columns of numbers equal to either 0 or 1), c is an n-tuple with entries also from $\mathbb{Z}_2$ and x is the vector of unknowns – the variables. We can create a game from such a system as follows: The Referee sends Alice an integer i between 1 and m, representing one of the equations, and sends Bob another integer j between 1 and n, representing a variable. Alice replies with a binary n-tuple $a = (a_1, \ldots, a_n)$ and Bob replies with a single bit b, that is, an element of $\mathbb{Z}_2$. They win the game if Alice's n-tuple is a solution to the i-th equation and if $a_j = b$, that is, if Bob correctly predicted the j-th entry of Alice's solution.

Given a conditional probability density $p(a, b|x, y)$, we will say that it is a *perfect* density for the game if $p(a, b|x, y) = 0$ whenever (a, b) is a losing pair of outputs for the input pair (x, y). Thus, a perfect density never produces a losing output pair. If it follows a perfect density, the game described above turns out to be a prover system. That is, the game has a perfect deterministic strategy if and only if the system of equations has an actual solution.

However, there are many linear systems for which this game has been shown to have a perfect quantum density while there is no classical solution. That is, by using entanglement, Alice and Bob can produce correct answers for every round, even though there is no solution to the system of equations.

A famous example of this phenomena is "Mermin's magic square game" [11]. This is a system of six equations with nine variables, which is best pictured by arranging the variables in a square:

$$\begin{matrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6. \\ x_7 & x_8 & x_9 \end{matrix}$$

The equations are given by the requirement that the sum of each row should yield an even number, while each column should have an odd sum. It turns out that it is impossible to find a solution to these equations.[2] Nonetheless, using entanglement, there is a perfect quantum strategy for this game so that no matter what row or column Alice is given and no matter what variable Bob is given, Alice and Bob will always give replies that will satisfy the rules.

Besides entanglement, one other key feature that allows these strange outcomes is that our games are *memoryless*. That is, if at some round Alice assigns the value 1 to a particular variable, then there is nothing that prevents her from assigning the value 0 to the same variable at some later round.

Slofstra [13] showed that two sets of quantum correlations are different by implicitly creating a linear system with about 200 equations in about 200 variables that had a perfect density in the set C_{qa} but not in C_q.

5 Algebras and games

Finally, we very briefly describe the work done in [1, 7, 10]. For each game of a certain type, called "synchronous" games, we construct a new object that encodes the rules of the game. For those familiar with the terminology, this new object is called an "algebra". An example of a familiar algebra is the set of polynomials. These are objects we know how to perform on them various operations: add, multiply, subtract, sometimes divide; we can compare their degrees, and they have been studied extensively. In this case, we construct a parallel for polynomials by replacing the coefficients, powers, variables, etc. with elements from the games. And so we can investigate them using tools which are quite developed. We are then able to translate questions about whether or not the game possesses a perfect strategy of each of the four types, local, q, qa, or qc, into questions about this new object built from the game. This has allowed us to prove that some games have perfect strategies by showing that this object built from the game has the right properties, without ever actually constructing the density or entangled state.

Building this type of "dictionary" that translates problems about one type of object, in this case games, into problems about a totally different type of object, in this case algebras, has always been one of my favorite parts of mathematics. The first time I encountered this powerful idea was when I learned how Galois had solved the long-standing problem in Euclidean geometry, that asked if there was a geometric construction for trisecting any angle, by building a "dictionary" that turned it into a problem about finding roots of polynomials.

[2] Can you see this? Hint: Use 0 and 1 for even and odd.

In addition to solving Connes's Embedding Problem, researchers now believe that this new dictionary for going between games and algebras might be the key to solving another problem in a third area of mathematics, called the "hyperlinear groups problem".

References

[1] M. Brannan, A. Chirvasitu, K. Eifler, S. J. Harris, V. I. Paulsen, X. Su, and M. Wasilewski, *Bigalois extensions and the graph isomorphism game*, Communications in Mathematical Physics **375** (2019), 1777–1809.

[2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Physical Review Letters **23** (1969), 880.

[3] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, *Consequences and limits of non-local strategies*, in *Proceedings. 19th IEEE Annual Conference on Computational Complexity*, IEEE, 2004, pp. 236–249.

[4] A. Coladangelo and J. Stark, *Unconditional separation of finite and infinite dimensional quantum correlations*, arXiv preprint, arXiv:1804.05116 (2018).

[5] A. Connes, *Classification of injective factors. Cases* $II_1, I_\infty, III_\lambda, \lambda \neq 1$, Annals of Mathematics (2) **104** (1976), 73–115.

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

[7] W. Helton, K. P. Meyer, V. I. Paulsen, and M. Satriano, *Algebras, synchronous games, and chromatic numbers of graphs*, New York Journal of Mathematics **25** (2019), 328–361.

[8] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, *MIP*=RE*, preprint, https://arxiv.org/abs/2001.04383 (2020).

[9] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner, *Connes embedding problem and Tsirelson's problem*, Journal of Mathematical Physics **52** (2011), 012102, 12 pp.

[10] S.-J. Kim, V. I. Paulsen, C. Schafhauser, *A synchronous game for binary constraint systems*, Journal of Mathematical Physics **59** (2018), 032201, 17 pp.

[11] N. D. Mermin, *Simple unified form for the major no-hidden-variables theorems*, Physical Review Letters **65** (1990), 3373.

[12] N. Ozawa, *About the Connes embedding conjecture: algebraic approaches*, Japanese Journal of Mathematics **8** (2013), 147–183.

[13] W. Slofstra, *The set of quantum correlations is not closed*, Forum of Mathematics. Pi **7** (2019), e1 41.

Vern I. Paulsen *is a professor of pure mathematics at the University of Waterloo and a member of the Institute for Quantum Computing.*

Mathematical subjects
Analysis

Connections to other fields
Computer Science, Physics

DOI
10.14760/SNAP-2023-004-EN

Snapshots of modern mathematics from Oberwolfach provide exciting insights into current mathematical research. They are written by participants in the scientific program of the Mathematisches Forschungsinstitut Oberwolfach (MFO). The snapshot project is designed to promote the understanding and appreciation of modern mathematics and mathematical research in the interested public worldwide. All snapshots are published in cooperation with the IMAGINARY platform and can be found on www.imaginary.org/snapshots and on www.mfo.de/snapshots.

ISSN 2626-1995

Junior Editor
Jan Kohlrus
junior-editors@mfo.de

Senior Editor
Anja Randecker
senior-editor@mfo.de

Mathematisches Forschungsinstitut
Oberwolfach gGmbH
Schwarzwaldstr. 9 – 11
77709 Oberwolfach
Germany

Director
Gerhard Huisken

Mathematisches Forschungsinstitut Oberwolfach

Member of Leibniz
Leibniz Association

IMAGINARY
open mathematics