# Playing games with quantum mechanics

Laura Mančinska

The discovery of quantum mechanics revolutionized our understanding of how the natural world behaves at the level of atoms and subatomic particles. It turns out that these small scale particles are governed by strange laws, rather different to the ones we observe in the macroscopic world. From the very beginning the city of Copenhagen has been inextricably linked to the development of quantum theory. Just think of Niels Bohr's pioneering contributions to understanding the structure of atoms and the Copenhagen interpretation of quantum mechanics.

Quantum mechanics has brought about much of the modern technology that surrounds us. Yet despite these fundamental applications of quantum theory to areas like electronics and chemistry, we are only starting to understand its consequences for information processing. In the past few decades we have seen that quantum effects can be harnessed to achieve functionalities which lie beyond the reach of classical information processing. Prime examples here include schemes for unconditionally secure cryptography, certified randomness generation, and polynomial-time factorization. One of the quantum effects I focus on in my research is the phenomenon of quantum entanglement. I am interested in understanding the mathematical structure of entanglement-assisted strategies and developing new entanglement-enhanced protocols for operational and cryptographic tasks.

Mathematically, a quantum state shared between two parties, lets call them Alice and Bob, is represented by a unit vector, $\psi$, that lives in a tensor product space $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ and we think of the first tensor as belonging to Alice and the second one to Bob. In this distributed setting, useful quantum states correspond to vectors which cannot be expressed as $\alpha \otimes \beta$ and we call such states *entangled*. One particularly useful model for studying entanglement, rooted both in theoretical computer science and foundational physics, is the framework of nonlocal games. In such a game two collaborating but non-communicating provers, Alice and Bob, engage in an interactive protocol with a verifier. The two provers aim to convince the verifier of the veracity of some mathematical statement and we are interested to see if the provers can perform better when allowed to use shared entanglement.

For instance, given a a graph $G$ and a number of colors $c$, the statement could be that $G$ is $c$-colorable (*i.e.*, it is possible to assign a color from the set $\{1, \ldots, c\}$ to each of the vertices of $G$ so that any pair of adjacent vertices receive different colors). To check this, the verifier would randomly select two vertices of $G$, say $v_A, v_B \in V(G)$, and ask Alice and Bob to assign one of the $c$ colors to their respective vertices. If the two vertices, $v_A$ and $v_B$, of $G$ were adjacent, the verifier checks that $c_A \neq c_B$, as in a valid coloring such vertices must receive different colors. If, on the other hand, $v_A = v_B$ then the verifier checks that $c_A = c_B$ (see Figure 1). Alice and Bob win the game if their answers pass these checks and their goal is to agree on a strategy that would maximize their chances of winning. In the classical case (no shared entanglement), Alice and Bob can win with probability one if and only if the graph $G$ is indeed $c$-colorable. Analogously, we define a graph to be *quantum $c$-colorable* if Alice and Bob can succeed with certainty when provided with an

entangled state of their choosing. Curiously, there are graphs which are not $c$-colorable despite being quantum $c$-colorable.

The above coloring game has been extensively studied in the literature and there are many graphs known to be quantumly but not classically $c$-colorable. This includes a family of graphs for which entanglement allows for exponential savings in the number of colors needed. Together with D. Roberson, we generalized this game to the case where the two provers aim to convince the verifier that a graph $G$ admits a homomorphism to a graph $H$. A graph homomorphism is an adjacency-preserving map $\varphi : V(G) \to V(H)$; in other words, if $xy \in E(G)$ then $\varphi(x)\varphi(y) \in E(H)$. Whenever such a $\varphi$ exists we say that $G$ admits a homomorphism to $H$ and write $G \to H$ to denote this. Just as before, we will say that $G$ admits a *quantum homomorphism* to $H$ and write $G \xrightarrow{q} H$ if there exists an entanglement-assisted strategy that allows Alice and Bob to succeed at the homomorphism game with certainty. It turns out that quantum homomorphisms are natural mathematical objects endowed with nice structure. For instance, quantum homomorphisms can be composed: If we know that $G \xrightarrow{q} H$ and $H \xrightarrow{q} K$ then it follows that $G \xrightarrow{q} K$. Also, the celebrated Lovász theta function, $\vartheta$, can be shown to give rise to a quantum homomorphism monotone. Specifically, we showed that $G \xrightarrow{q} H$ implies that $\vartheta(\overline{G}) \leq \vartheta(\overline{H})$, where $\overline{X}$ denotes the complement of a graph $X$. Finally, in a certain sense quantum homomorphisms can be seen as non-commuting operator relaxations of graph homomorphisms.

We know that $c$-colorability is a computationally hard problem; in particular, even determining if a given graph is 3-colorable is an NP-complete problem. However, if one is not concerned with efficiency then it is always possible to check all different assignments of colors to vertices to determine if a graph $G$ admits a valid $c$-coloring or not. Things become more complicated in case of quantum colorings. This is not only because there are infinitely many possible strategies that use a fixed shared entangled state $\psi \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$, but mostly due to there being no a priori upper bound on the dimensions $d_A$ and $d_B$ that could be needed. In fact, very recently for a related class of games W. Slofstra has shown that it is undecidable to determine if there exists an entanglement-assisted strategy that would ensure the provers' success. Therefore, unsurprisingly, there is no known algorithmic way of checking if a graph is quantum $c$-colorable. Luckily, in some cases we can use even efficiently computable criteria to conclude that a quantum coloring cannot exist. One such efficiently testable criterion follows directly from the monotonicity result of the Lovász theta function we saw above. Since $c$-colorability is a special case graph homomorphism, it can be shown that quantum $c$-coloring is impossible whenever $\vartheta(\overline{G}) > c$.

Since its first introduction in 2012, our notion of quantum homomorphisms has appeared in works in rather different areas of quantum information ranging from optimization (M. Laurent and T. Piovesan) to operator algebras (C. Ortiz and V. Paulsen), and category theory (S. Abramsky, R. S. Barbosa, N. de Silva, and O. Zapata).

In this short note I chose to tell you a bit about just one of the research directions I have worked on in the past. If you are interested to find out more about playing games with quantum mechanics or other questions I spend my days thinking about, come find me in 04.2.03 (or catch me by the 4th floor coffee machine).

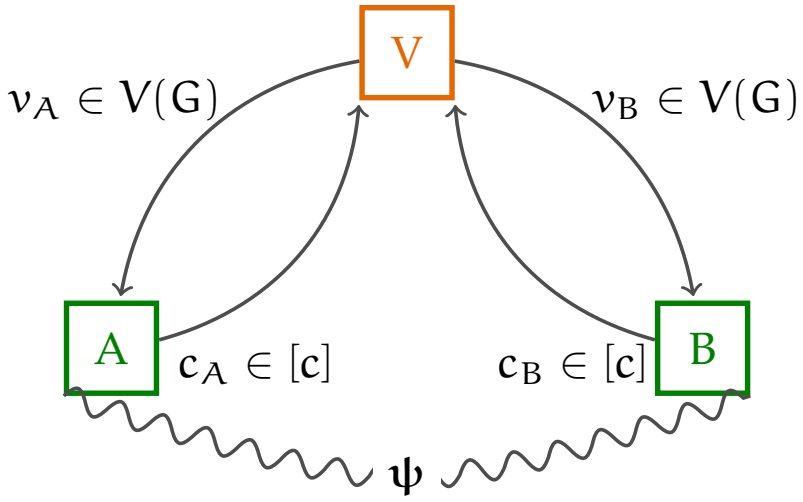


Figure 1: Verifier randomly selects two vertices and sends one of them to Alice and the other one to Bob. The two provers respond by assigning colors, $c_A$ and $c_B$, to their respective vertices. Upon receiving the answers the verifier checks if $c_A = c_B$ in case $v_A = v_B$ and he checks that $c_A \neq c_B$ in case $v_A$ and $v_B$ are adjacent. If the provers' answers pass these checks they win the game.