Nonlocal Games and Quantum Permutation Groups*

Martino Lupini[1], Laura Mančinska[2], and David E. Roberson[3]

[1] *Mathematics Department, California Institute of Technology*
[2] *QMATH, Department of Mathematical Sciences, University of Copenhagen*
[3] *Dept. of Applied Mathematics and Computer Science, Technical University of Denmark*

March 31, 2018

Abstract

We define a notion of quantum isomorphisms of graphs based on quantum automorphisms from the theory of quantum groups, and then show that this is equivalent to the previously defined notion of quantum isomorphism corresponding to perfect quantum strategies to the isomorphism game. This connection links quantum groups to the more concrete notion of nonlocal games and physically observable quantum behaviours. In this work, we exploit this by using ideas and results from quantum information in order to prove new results about quantum automorphism groups of graphs, and about quantum permutation groups more generally. In particular, we show that asymptotically almost surely all graphs have trivial quantum automorphism group. Furthermore, we use examples of quantum isomorphic graphs from previous work to construct an infinite family of graphs which are quantum vertex transitive but fail to be vertex transitive, answering a question from the quantum permutation group literature.

Our main tool for proving these results is the introduction of orbits and orbitals (orbits on ordered pairs) of quantum permutation groups. We show that the orbitals of a quantum permutation group form a coherent configuration/algebra, a notion from the field of algebraic graph theory. We then prove that the elements of this *quantum orbital algebra* are exactly the matrices that commute with the magic unitary defining the quantum group. We furthermore show that quantum isomorphic graphs admit an isomorphism of their quantum orbital algebras which maps the adjacency matrix of one graph to that of the other.

Introduction

An isomorphism of graphs X and Y is bijection $\varphi : V(X) \to V(Y)$ which preserves both adjacency and non-adjacency. Whenever such a function exists we say that X and Y are *isomorphic* and write $X \cong Y$. An alternative definition of isomorphism can be stated in terms of the adjacency matrices of X and Y. These are 01-matrices with a 1 in the entries corresponding to the edges of the graphs. If X and Y have adjacency matrices A and B respectively, then they are isomorphic if and only if there exists a permutation matrix P such that $P^T AP = B$, or equivalently $AP = PB$.

The isomorphisms from a graph X to itself are called *automorphisms* and they form a group called the *automorphism group of* X, denoted $\mathrm{Aut}(X)$. As with isomorphisms, the automorphisms

[*] This work has been submitted to *Communications in Mathematical Physics*. A preprint is available at arXiv:1712.01820.

of a graph can be represented as permutation matrices. Furthermore, the automorphisms of X are exactly those permutations whose corresponding permutation matrix commutes with the adjacency matrix of X.

In [2], Banica introduced the *quantum automorphism group* of a graph, generalizing Wang's definition of the *quantum permutation group of a set* [4], which itself used the formalism of Woronowicz' compact quantum groups [5]. Briefly, the idea is to consider the algebra of complex-valued functions on the automorphism group of a graph. This C^*-algebra is commutative and can be generated by finitely many elements satisfying certain relations depending on the graph. By dropping the (explicit) commutativity requirement of these generators, one obtains a possibly different C^*-algebra which is by definition the "algebra of continuous functions on the *quantum* automorphism group of the graph". The generators can be arranged in a matrix U called a *magic unitary*, which satisfies $AU = UA$ where A is the adjacency matrix of the given graph. In fact, the equation $AU = UA$, along with the magic unitary property of U, defines the quantum automorphism group of the graph.

More recently, a different approach was used to define quantum analogs of graph isomorphisms which involved nonlocal games. A (2-party) nonlocal game is a game played by two players, Alice and Bob, against a referee/verifier. The referee sends each of the players some question/input and they must respond with some output. Whether the players win is determined by evaluating a binary verification function that depends on the inputs and outputs of both players. The players have full knowledge of the game beforehand: they know their input and output sets and the verification function, as well as the probability distribution used to dispense the inputs. Their goal is to to win the game with as high probability as possible. To do this, they are allowed to agree on whatever strategy they like beforehand, but are not allowed to communicate after receiving the questions.

A *classical strategy* for a nonlocal game is one in which the only resource available to the players is shared randomness. In a *quantum strategy*, the players are allowed to perform local quantum measurements on a shared entangled state. This does not allow them to communicate, but can sometimes increase their chance of winning. If players are able to win a given nonlocal game with probability greater than what is possible classically, then this is evidence that they are doing something genuinely quantum. Thus nonlocal games provide a way of certifying quantum behaviour through the observation of only classical data: the inputs and outputs of the players. Such quantum behaviour is known as *nonlocality*, and in the extreme case, when quantum players can win with probability 1 but classical players cannot, the game is called a *pseudotelepathy game* [3].

In [1], along with others, the second and third authors introduced a family of nonlocal games called *isomorphism games*, and investigated the classical and quantum strategies that win the game perfectly (with probability 1). They showed that the game can be won perfectly by a classical strategy if and only if the corresponding graphs are isomorphic. This motivated the definition of quantum isomorphic graphs: those for which the game can be won perfectly by a quantum strategy. They characterized quantum isomorphism in terms of an object they referred to as a *projective permutation matrix.* The entries of this matrix correspond to the quantum measurement operators used to win the game. They showed that if the graphs used in the game had adjacency matrices A and B respectively, then they were quantum isomorphic if and only if there exists projective permutation matrix $\mathcal{P}$ such that $A\mathcal{P} = \mathcal{P}B$. This is a quantum analog of the adjacency matrix formulation of classical isomorphism, since replacing $\mathcal{P}$ with a permutation matrix P recovers the classical definition.

It turns out that the notions of magic unitaries and projective permutation matrices are essentially the same. The only difference is that in the theory of quantum groups the entries are allowed to be elements of any unital C^*-algebra, whereas in quantum information the entries are required to be elements of a unital C^*-algebra that *admits a trace*. Thus, in this work we define a relaxed notion of quantum isomorphism in which the required projective permutation matrix/magic unitary has entries from some unital C^*-algebra, which does not necessarily admit a trace. This is the natural extension of quantum automorphisms from quantum group theory to the setting of isomorphisms. Surprisingly, we show that this is equivalent to the original notion: the existence of a perfect quantum strategy for the isomorphism game. Moreover, we show that connected graphs X and Y are quantum isomorphic if and only if there exists $x \in V(X)$ and $y \in V(Y)$ that are in the same orbit of the quantum automorphism group of the disjoint union of X and Y, in perfect analogy to the classical case. Thus the quantum information theoretic notion of quantum isomorphisms can be rephrased completely in terms of quantum automorphism groups.

Main Results

In addition to establishing a connection between quantum permutation groups and quantum information, we also show that relations among the generators of a quantum permutation group can be used to define orbits and orbitals (orbits on ordered pairs) analogously to the classical case. The following result shows that the orbitals of a quantum permutation group form a highly regular structure that arises in group theory and algebraic graph theory:

Result 1. *If $\mathcal{Q}$ is a quantum permutation group acting on a set X, then the orbitals of $\mathcal{Q}$ form a coherent configuration.*

This turns out to be a useful tool for studying quantum isomorphisms/automorphisms. Indeed, we use this to prove the following result:

Result 2. *Let X be a random graph on n vertices. The probability that X has nontrivial quantum automorphism group goes to zero as n goes to infinity.*

Moreover, we prove the following necessary condition for two graphs to be quantum isomorphic:

Result 3. *Let X and Y be graphs. If X and Y are quantum isomorphic, then there is an isomorphism of their quantum orbital algebras that maps the adjacency matrix of X to that of Y.*

We also show that the previously defined notion of *quantum vertex transitivity* [2] of a graph X is equivalent to the quantum automorphism group of X having only one orbit, which is analogous to the classical case. Using this we are able to prove the following, resolving an open question from the quantum permutation group literature.

Result 4. *There exist an infinite number of quantum vertex transitive graphs which are not vertex transitive.*

Finally, we show that the Haar state of a quantum permutation group is uniform on its orbitals:

Result 5. *Let $\mathcal{Q}$ be a quantum permutation group on a set X, and let u_{xy} for $x, y \in X$ be the generators defining $C(\mathcal{Q})$, the algebra of continuous functions on $\mathcal{Q}$. Also let h denote the Haar state on $C(\mathcal{Q})$. If $R_1, \ldots, R_m \subseteq X \times X$ are the orbitals of $\mathcal{Q}$ on X, then*

$$h(u_{xy}u_{x'y'}) = \begin{cases} 1/|R_i| & \textit{if } (x,x'),(y,y') \in R_i; \\ 0 & \textit{o.w.} \end{cases}$$

References

[1] Albert Atserias, Laura Mančinska, David E. Roberson, Robert Šámal, Simone Severini, and Antonios Varvitsiotis. Quantum and non-signalling graph isomorphisms. 2016. arXiv:1611.09837v3.

[2] Teodor Banica. Quantum automorphism groups of homogeneous graphs. *Journal of Functional Analysis*, 224(2):243 – 280, 2005. doi:10.1016/j.jfa.2004.11.002.

[3] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, Nov 2005. doi:10.1007/s10701-005-7353-4.

[4] Shuzhou Wang. Quantum symmetry groups of finite spaces. *Communications in Mathematical Physics*, 195(1):195–211, Jul 1998. doi:10.1007/s002200050385.

[5] Stanisław L. Woronowicz. Compact matrix pseudogroups. *Comm. Math. Phys.*, 111(4):613–665, 1987. doi:10.1007/BF01219077.