Nonlocal games and quantum permutation groups

(Article begins on next page)

24 November 2024

Nonlocal Games and Quantum Permutation Groups

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

[1]*School of Mathematics and Statistics, Victoria University of Wellington, PO Box 600, 6140 Wellington, New Zealand*
[2]*QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark*
[3]*Department of Applied Mathematics and Computer Science, Technical University of Denmark, DK-2800 Lyngby, Denmark*

April 1, 2020

Abstract

We present a strong connection between quantum information and the theory of quantum permutation groups. Specifically, 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. Moreover, we show that two 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. 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.

We hope that this work will encourage new collaborations among the communities of quantum information, quantum groups, and algebraic graph theory.

1 Introduction

We take our graphs to be undirected, loopless, and without multiple edges. An isomorphism of graphs X and Y is function $\varphi : V(X) \to V(Y)$ which is bijective, preserves adjacency, and preserves

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 $P^T A P = B$, 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 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 [4], Banica introduced the *quantum automorphism group* of a graph[1], generalizing Wang's definition of the *quantum permutation group of a set* [28], which itself used the formalism of Woronowicz's compact quantum groups [30, 31]. Briefly, the idea is to consider the algebra of complex-valued functions on the automorphism group of a graph. This 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 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 which is called a *magic unitary*, which has the property that it commutes with the adjacency matrix 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 try to win the game with as high probability as possible. In order 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* [12].

In [2], along with others, the second and third authors introduced a family of nonlocal games called *graph 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

---

[1]We remark that a different version of the quantum automorphism group of a graph was previously introduced by Bichon [10], but the definition of Banica is the one relevant for our work.

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 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.

We remark that the connection between quantum permutation groups and quantum isomorphisms has very recently been independently noted in [25]. However, the perspective in that work is quite different from ours. While they develop a very broad, and elegant, categorical framework for working with quantum permutations and other similar notions, here we are more focused on using results and ideas from quantum information and algebraic graph theory to establish new results in the theory of quantum permutation groups. Moreover, they focus on a slightly different notion of quantum isomorphisms where the entries of projective permutation matrices are required to be finite dimensional, and which is known to be different from the more general case we consider here.

1.1 Outline

Besides proving the equivalence of our new notion of quantum isomorphism with the notion arising from isomorphism games, the main results of our work are as follows: **(1)** The orbitals of a quantum permutation group form a coherent configuration; **(2)** the value of the Haar state of a quantum permutation group on products of pairs of generators is determined by the orbitals; **(3)** 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; **(4)** there exist an infinite number of quantum vertex transitive graphs which are not vertex transitive.

In Section 2, we provide background material on the isomorphism game, quantum permutation groups, and coherent configurations/algebras, which are the three main ingredients of this work. In Section 3 we define the orbits and orbitals of an arbitrary quantum permutation group. We then show, in Section 3.1, that these definitions are equivalent to definitions based on the spaces of "fixed points" of the action of the quantum permutation group, a notion studied in the quantum group literature. Section 3.2 contains the proof of our first main result: that the orbitals of a quantum permutation group $\mathcal{Q}$ form a coherent configuration. The span of the characteristic matrices of the

classes in this configuration form a coherent algebra which we call the orbital algebra of $\mathcal{Q}$. We also show that the elements of this algebra are exactly those matrices which commute with the magic unitary defining $\mathcal{Q}$. The following Section 3.3 shows how to make this result practical by using the coherent algebra of the graph, which can be computed in polynomial time.

Section 4 is concerned with quantum isomorphisms, and using pairs of non-isomorphic but quantum isomorphic graphs to construct quantum vertex transitive graphs that fail to be vertex transitive. It begins with Section 4.3 in which we prove our second main result: that any quantum isomorphism of two graphs induces an isomorphism of their quantum orbital algebras which maps the adjacency matrix of one to that of the other. In Sections 4.4 and 4.5 we introduce two previously known constructions whose concatenation, when applied to any connected non-planar graph Z, produces a pair of non-isomorphic graphs which are nevertheless quantum isomorphic. In Section 4.6 we show that if the graph Z is vertex transitive, then at least one of the graphs produced by this construction is vertex transitive. Finally, we put this all together in Section 4.7 to show how to construct an infinite family of quantum vertex transitive graphs that are not vertex transitive. We end in Section 5 by discussing some possible future directions and interesting open problems.

The idea to use coherent configurations/algebras, a topic from algebraic graph theory, to study quantum automorphism groups is inspired by concurrent work of the second and third authors and others [23]. They consider a semidefinite relaxation of quantum isomorphisms that they call doubly nonnegative isomorphism. They show that any doubly nonnegative isomorphism of graphs X and Y induces an isomorphism of the coherent algebras of X and Y that maps the adjacency matrix of X to that of Y. Such an isomorphism of coherent algebras is called an *equivalence* of X and Y, a previously studied notion [9]. Conversely, they show that any equivalence of X and Y can be used to construct a doubly nonnegative isomorphism of X and Y. Therefore, these two relations are equivalent. This result is what motivated the consideration of coherent algebras for this work.

2 Background

We begin by giving some background about each of the three main ingredients of this work: the graph isomorphism game, quantum permutation groups, and coherent configurations/algebras.

2.1 The isomorphism game

In [2], a nonlocal game is introduced which captures the notion of graph isomorphism. In turn, by allowing entangled strategies, this allows one to define a type of quantum isomorphism in a natural way. We will give a brief description of this game and its classical/quantum strategies, but for a more thorough explanation we refer the reader to [2].

Given graphs X and Y, the (X, Y)-isomorphism game is played as follows: a referee/verifier sends each of two players (Alice and Bob) a vertex of X or Y (not necessarily the same vertex to both), and tells them which graph it is from (this is necessary if the vertex sets are not disjoint). Each of Alice and Bob must respond to the referee with a vertex of X or Y (and specify which graph it belongs to). Alice and Bob win if they meet two conditions, the first of which is:

(1) If a player (Alice or Bob) receives a vertex from X, they must respond with a vertex from Y and vice versa.

Assuming this condition is met, Alice either receives or responds with a vertex of X, which we will call x_A, and either responds with or receives a vertex of Y, which we will call y_A. We can similarly define x_B and y_B for Bob. The second condition they must meet in order to win is then given by

(2) $\mathrm{rel}(x_A, x_B) = \mathrm{rel}(y_A, y_B)$, where rel is a function denoting the *relationship* of two vertices, i.e., whether they are equal, adjacent, or distinct non-adjacent.

The players know the graphs X and Y beforehand and can agree on any strategy they like, but they are not allowed to communicate during the game. For simplicity we may assume that the referee sends the vertices to the players uniformly at random. We only require that Alice and Bob play one round of the game (each receive and respond with a single vertex), but we require that their strategy guarantees that they win with probability 1. We say that such a strategy is a *perfect* or *winning* strategy.

If $\varphi : V(X) \to V(Y)$ is an isomorphism, then it is not difficult to see that responding with $\varphi(x)$ for $x \in V(X)$ and $\varphi^{-1}(y)$ for $y \in V(Y)$ is a perfect strategy for the (X, Y)-isomorphism game. Conversely, any perfect deterministic classical strategy can be shown to have this form. This is what was shown in [2] and it follows that there exists a perfect classical strategy for the (X, Y)-isomorphism game if and only if $X \cong Y$. In general, classical players could use shared randomness but it is not hard to see that this would not allow them to win if they were not already able to succeed perfectly using a deterministic strategy.

In a quantum strategy, Alice and Bob have access to a shared entangled state which they are allowed to perform local quantum measurements on. This does not allow them to communicate, but may allow them to correlate their actions/responses in ways not possible for classical players. In [2], two different models for performing joint measurements on a shared state were considered: the tensor product framework and the commuting operator framework. In the tensor product framework, both Alice and Bob have their own Hilbert space on which they are allowed to make measurements, and their shared state lives in the tensor product of their Hilbert spaces. We note that for the isomorphism game, whenever there is a perfect quantum strategy in the tensor product framework, there is one that is finite dimensional (this is not known to hold for general nonlocal games, and is known not to hold if one considers non-perfect strategies [15]). In the commuting operator framework, they share a single Hilbert space in which their shared state lives, but it is required that all of Alice's measurement operators commute with all of Bob's. In either case, the shared entangled state is specified by a vector and the measurement operators are positive operators on the relevant Hilbert spaces. We remark that the commuting operator framework is the more general of the two. This follows from the fact that any tensor product strategy can be made into a commuting operator strategy by replacing each measurement operator E of Alice's with $E \otimes I$, and each measurement operator F of Bob's with $I \otimes F$. However, if we restrict both frameworks to finite dimensional Hilbert spaces then they are known to be equivalent.

In [2], they say that graphs X and Y are "quantum isomorphic" if there exists a perfect quantum strategy for the (X, Y)-isomorphism game in the tensor product framework. Similarly, they say they are "quantum commuting isomorphic" if there exists a perfect quantum strategy in the commuting operator framework. They show that these relations are distinct, and the former is finer than the latter, since the commuting framework is more general. In this work we additionally consider an even more general notion of quantum isomorphism, that we simply call *quantum isomorphism*, which corresponds to the isomorphism game having a perfect C^*-strategy as defined in [19]. This

5

definition of quantum isomorphism extends the notion of quantum graph automorphisms of Banica. Because of this, we will refer to the relation of being "quantum isomorphic" from [2] as being *quantum tensor isomorphic*, and we will use the notation '$\cong_{qt}$' for this relation. We will keep the terminology of quantum commuting isomorphism the same, and use '$\cong_{qc}$' for this.

Without going into the details of the proof, we present the following characterization of quantum tensor isomorphism proven in [2]. Recall that an operator P is an (orthogonal) *projection* if $P = P^* = P^2$.

Theorem 2.1. *Let X and Y be graphs. Then $X \cong_{qt} Y$ if and only if there exist projections P_{xy} for $x \in V(X), y \in V(Y)$ on a finite dimensional Hilbert space satisfying*

1. $\sum_{y \in V(Y)} P_{xy} = I$ *for all $x \in V(X)$;*

2. $\sum_{x \in V(X)} P_{xy} = I$ *for all $y \in V(Y)$;*

3. $P_{xy} P_{x'y'} = 0$ *if* $\text{rel}(x, x') \neq \text{rel}(y, y')$.

The projections P_{xy} in the above theorem correspond to the measurement operators used by Alice (Bob uses the transpose of these) in a perfect strategy for the isomorphism game. The element P_{xy} corresponds to Alice replying with y upon receiving x. Intuitively, this is analogous to x being mapped to y by an isomorphism of X and Y.

It is possible to "compose" strategies for isomorphism games. If P_{xy} are projectors as above for the (X, Y)-isomorphism game, and Q_{yz} are projectors for the (Y, Z)-isomorphism game, then the construction $R_{xz} := \sum_{y \in V(Y)} P_{xy} \otimes Q_{yz}$ gives projections satisfying Conditions (1)–(3) for the (X, Z)-isomorphism game (note the similarity to the definition of comultiplication in a quantum permutation group given in Section 2.2). In terms of the game, this construction corresponds to playing as follows: upon receiving $x \in V(X)$, the player acts as if they were playing the (X, Y)-isomorphism game and obtains some outcome $y \in V(Y)$. The player then acts as if y was their input for the (Y, Z)-isomorphism game and obtains some output $z \in V(Z)$ which they send to the verifier. Thinking in terms of the gameplay like this can sometimes provide one with good intuition for quantum isomorphisms.

An analogous characterization for quantum commuting isomorphism was also given in [2]:

Theorem 2.2. *Let X and Y be graphs. Then $X \cong_{qc} Y$ if and only if there exists a unital C*-algebra $\mathcal{A}$ that admits a faithful tracial state, and projections $P_{xy} \in \mathcal{A}$ for $x \in V(X), y \in V(Y)$ which satisfy Conditions (1)–(3) of Theorem 2.1.*

In Theorem 2.2 and in the following, we assume a unital C*-algebra to be nontrivial, i.e., such that its unit 1 is different from the zero element. A *state* on a unital C*-algebra $\mathcal{A}$ is a linear functional $s : \mathcal{A} \to \mathbb{C}$ such that $s(1) = 1$ and $s(A^*A) \geq 0$ for all $A \in \mathcal{A}$. The state is *tracial* if $s(AB) = s(BA)$ for all $A, B \in \mathcal{A}$. The prototypical example of a tracial state is the unique tracial state on the algebra $M_n(\mathbb{C})$ of $n \times n$ complex matrices given by $s(A) = \text{Tr}(A)/n$.

In [2], it was noted that the projections from Theorem 2.1 could be used as the entries of a matrix $U = (P_{xy}) \in M_n(\mathcal{A})$ that will satisfy $AU = UB$ where A and B are the adjacency matrices of X and Y respectively. Here and in the following, we canonically regard $M_n(\mathcal{A})$ for a unital C*-algebra $\mathcal{A}$ as an $M_n(\mathbb{C})$-bimodule. In other words, if $A = (a_{ij}) \in M_n(\mathcal{A})$ and $B = (b_{ij}) \in M_n(\mathbb{C})$, then $AB \in M_n(\mathcal{A})$ is the matrix whose (i, j)-entry is $\sum_{i=1}^{n} a_{ik} b_{kj}$, and $BA \in M_n(\mathcal{A})$ is the matrix whose (i, j)-entry is $\sum_{i=1}^{n} b_{ik} a_{kj}$.

6

It was also shown in [2] that the matrix U described above will necessarily be unitary. This motivated the definition of what they called a "projective permutation matrix", also known as *magic unitary* in the quantum group literature:

Definition 2.3. *A matrix $U = (u_{ij})_{i,j\in[n]}$ whose entries u_{ij} are elements of some unital C*-algebra is a* magic unitary *if u_{ij} is a projection for all $i, j \in [n]$ and $\sum_{j'} u_{ij'} = 1 = \sum_{i'} u_{i'j}$ for all $i, j \in [n]$. Any such matrix will be unitary, i.e., $UU^* = 1 = U^*U$.*

Note that in the case where the C*-algebra is $\mathbb{C}$, a magic unitary is simply a permutation matrix. The notion of projective permutation matrices/magic unitaries allows for the following formulation of quantum tensor isomorphism that was given in [2]:

Theorem 2.4. *Let X and Y be graphs with adjacency matrices A and B respectively. Then $X \cong_{qt} Y$ if and only if there exists a magic unitary $U = (u_{xy})_{x\in V(X),y\in V(Y)}$ whose entries are operators on a finite-dimensional Hilbert space such that $AU = UB$.*

Since any C*-algebra admits a representation as an algebra of operators on a Hilbert space, one can equivalently state Theorem 2.4 by saying that two graphs are quantum tensor isomorphic if and only if there exists a unital C*-algebra $\mathcal{A}$ that has a finite dimensional representation and magic unitary $U = (u_{xy})_{x\in V(X),y\in V(Y)}$ with entries from $\mathcal{A}$ such that $AU = UB$. Though it was not explicitly written in [2], the same reasoning allows for an analogous formulation for quantum commuting isomorphism:

Theorem 2.5. *Let X and Y be graphs with adjacency matrices A and B respectively. Then $X \cong_{qc} Y$ if and only if there exists a magic unitary $U = (u_{xy})$ whose entries are elements of a unital C*-algebra that admits a faithful tracial state such that $AU = UB$.*

The two theorems above are quantum analogs of the fact that graphs X and Y are isomorphic if and only if there exists a permutation matrix P such that $AP = PB$.

Remark 2.6. *The faithfulness of the tracial state in Theorems 2.2 and 2.5 is not really necessary. This is because given a (possibly not faithful) tracial state τ on a C*-algebra $\mathcal{A}$, one can always replace $\mathcal{A}$ with its image under the GNS representation associated with τ, which is endowed with a canonical faithful (vector) state.*

2.2 Quantum permutation groups

Here we provide some background on quantum groups. Though we aim to give a brief but thorough summary of quantum groups, the reader is not expected have have a mastery of these concepts in order to understand this work. The essential points are the definitions of the quantum symmetric group, the quantum automorphism group of a graph, and quantum permutation groups in general, along with their comultiplications, antipodes, counits, and universal actions.

We adopt the following notation. For subsets X, Y of a C*-algebra $\mathcal{A}$, we let XY be the set $\{xy : x \in X, y \in Y\}$, and $[X]$ be the closure of the linear span of X inside $\mathcal{A}$. We denote by $\mathcal{A} \otimes \mathcal{B}$ the *minimal* tensor product of C*-algebras $\mathcal{A}$ and $\mathcal{B}$. Concretely, if $\mathcal{A}, \mathcal{B}$ are realized as algebras of operators on a Hilbert space $\mathcal{H}$, then $\mathcal{A} \otimes \mathcal{B}$ can be identified with the algebra of operators on $\mathcal{H} \otimes \mathcal{H}$ generated by the elementary tensors of the form $a \otimes b$ for $a \in \mathcal{A}$ and $b \in \mathcal{B}$.

A *compact quantum group* $\mathbb{G}$ is given by a unital C*-algebra $C(\mathbb{G})$ together with a unital *-homomorphism $\Delta : C(\mathbb{G}) \to C(\mathbb{G}) \otimes C(\mathbb{G})$ called *comultiplication* satisfying the following identities:

- $(\Delta \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \Delta) \circ \Delta$;

- $[\Delta \left(C(\mathbb{G})\right) \left(1 \otimes C(\mathbb{G})\right)] = [\Delta \left(C(\mathbb{G})\right) \left(C(\mathbb{G}) \otimes 1\right)] = C(\mathbb{G}) \otimes C(\mathbb{G})$.

Any (classical) compact group G gives rise canonically to a compact quantum group, where $C(G)$ is the C*-algebra of continuous complex-valued functions on G, and the comultiplication Δ is the function induced by the multiplication operation by duality. In formulas, one has that, under the identification of $C(G) \otimes C(G)$ with $C(G \times G)$, $\Delta(f)$ is the function $G \times G \to \mathbb{C}, (s, t) \mapsto f(st)$. The compact quantum groups $\mathbb{G}$ that arise in this fashion are precisely those for which the C*-algebra $C(\mathbb{G})$ is *commutative*. In the general quantum setting, the compact quantum $\mathbb{G}$ does not actually exist as a set of points, but it is defined implicitly by the unital C*-algebra $C(\mathbb{G})$ together with its comultiplication.

As a further example, one can consider a discrete group Γ, and let $C^*(\Gamma)$ be the full group C*-algebra. If one denotes by u_γ for $\gamma \in \Gamma$ the canonical generators of $C^*(\Gamma)$ one can define a comultiplication on $C^*(\Gamma)$ by

$$\Delta\left(u_\gamma\right) = u_\gamma \otimes u_\gamma.$$

This defines a compact quantum group, which is the *dual* compact quantum group $\hat{\Gamma}$ of the discrete group Γ.

One can show that any compact quantum group $\mathbb{G}$ is endowed with a canonical state $h : C(\mathbb{G}) \to \mathbb{C}$, called the *Haar state*, which is *invariant* in the sense that $(h \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes h) \circ \Delta = h$ (where we identify $\mathbb{C}$ with the scalar multiples of the identity in $C(\mathbb{G})$). In the case of classical groups, this corresponds to integration with respect to the Haar probability measure.

A (unitary) *representation* of dimension n of a compact quantum group $\mathbb{G}$ is an $n \times n$ matrix $u = [u_{ij}] \in M_n\left(C(\mathbb{G})\right)$ such that $\Delta\left(u_{ij}\right) = \sum_{k=1}^n u_{ik} \otimes u_{kj}$. One can also regard u as a linear map $u : \mathbb{C}^n \to \mathbb{C}^n \otimes C(\mathbb{G})$ defined by $u(e_i) = \sum_{j=1}^n e_j \otimes u_{ji}$. A subspace $\mathcal{K}$ of $\mathbb{C}^n$ is *invariant* for the representation u of $\mathbb{G}$ if u maps $\mathcal{K}$ to $\mathcal{K} \otimes C(\mathbb{G})$. A finite-dimensional unitary representation of $\mathbb{G}$ is called *irreducible* if it has no nontrivial invariant subspace. Every (finite-dimensional) representation of $\mathbb{G}$ can be written as a direct sum of irreducible representations. We will denote by $\mathrm{Rep}(\mathbb{G})$ the set of finite-dimensional unitary representations of $\mathbb{G}$, and by $\mathrm{Irr}(\mathbb{G}) \subset \mathrm{Rep}(\mathbb{G})$ the set of irreducible representations of $\mathbb{G}$. For $\lambda \in \mathrm{Rep}(\mathbb{G})$ we let d_λ be the corresponding dimension, and $u^\lambda \in M_{d_\lambda}(C(\mathbb{G}))$ be the matrix defining the representation. The *matrix coefficients* of a unitary representation λ of $\mathbb{G}$ are the elements of $C(\mathbb{G})$ of the form $u^\lambda_{\xi,\eta} = (\mathrm{id} \otimes \xi^*)u^\lambda(\eta)$ for $\xi, \eta \in \mathbb{C}^{d_\lambda}$.

One then lets $\mathcal{O}(\mathbb{G})$ be the subset of $C(\mathbb{G})$ given by

$$\left\{ u^\lambda_{\xi,\eta} : \lambda \in \mathrm{Rep}\left(\mathbb{G}\right), \xi, \eta \in \mathbb{C}^{d_\lambda} \right\},$$

which is a dense self-adjoint subalgebra of $C(\mathbb{G})$ invariant under the comultiplication. If $e_1, \ldots, e_{d_\lambda}$ is the canonical basis of $\mathbb{C}^{d_\lambda}$, then the comultiplication is defined by $\Delta(u^\lambda_{\xi,\eta}) = u^\lambda_{\xi,e_1} \otimes u^\lambda_{e_1,\eta} + \cdots + u^\lambda_{\xi,e_{d_\lambda}} \otimes u^\lambda_{e_{d_\lambda},\eta}$. The *-algebra $\mathcal{O}(\mathbb{G})$ is furthermore endowed with a canonical Hopf *-algebra structure, which is determined, together with the comultiplication, by the *counit* $\varepsilon : \mathcal{O}(\mathbb{G}) \to \mathbb{C}$ and *antipode* maps $S : \mathcal{O}(\mathbb{G}) \to \mathcal{O}(\mathbb{G})^{\mathrm{op}}$ given by $\varepsilon(u^\lambda_{\xi,\eta}) = \langle \xi, \eta \rangle$ and $S(u^\lambda_{\xi,\eta}) = (u^\lambda_{\eta,\xi})^*$ for $\lambda \in \mathrm{Rep}(\mathbb{G})$ and $\xi, \eta \in \mathcal{H}^\lambda$. This means that ε is a *-homomorphism and S is a conjugate linear unital anti-homomorphism satisfying

$$m \circ (S \otimes \mathrm{id}) \circ \Delta = m \circ (\mathrm{id} \otimes S) \circ \Delta = \varepsilon$$

and
$$(\varepsilon \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \varepsilon) \circ \Delta = \mathrm{id},$$
where $m : \mathcal{O}(\mathbb{G}) \otimes \mathcal{O}(\mathbb{G}) \to \mathcal{O}(\mathbb{G})$ is the linear map induced by mulitplication, and where we identify $\mathbb{C}$ with the scalar multiples of the identity within $C(\mathbb{G})$.

In the case of $C(G)$ for a classical group G, one has that $C(G) = \mathcal{O}(G)$, and the counit and antipode are given by $\varepsilon(f) = f(1_G)$ and $S(f) = f \circ \mathrm{inv}$, where 1_G is the identity element of G and inv is the function from G to itself mapping each element to its inverse. A complete reference for the theory of compact quantum groups can be found in [27].

Fix a finite set X. The *quantum symmetric group on X*, denoted $\mathcal{Q}_X$, is a compact quantum group defined by Wang [28], and can be regarded as the quantum analog of the group S_X of permutations of X. By definition, such a compact quantum group is defined by letting $C(\mathcal{Q}_X)$ be the universal C*-algebra generated by elements u_{xy} for $x, y \in X$, subject to the relation that the matrix $U = (u_{xy})$ be a magic unitary, with comultiplication defined by setting $\Delta(u_{xz}) = \sum_{y \in X} u_{xy} \otimes u_{yz}$. In this case, one has that $C(\mathcal{Q}_X)$ is the universal C*-algebra generated by $\mathcal{O}(\mathcal{Q}_X)$, and the antipode and counit extends from $\mathcal{O}(\mathcal{Q}_X)$ to bounded linear maps on $C(\mathcal{Q}_X)$ defined by $S(u_{xy}) = u_{yx}$ and $\varepsilon(u_{xy}) = \delta_{xy}$. In this case, the antipode is an involutive *-linear map, which by definition means that $\mathcal{O}(\mathcal{Q}_X)$ is a Hopf *-algebra of *Kac type*. For comparison, one should consider the C*-algebra $C(S_X)$ associated with the symmetric group S_X. This can be seen as the universal C*-algebra generated by elements u_{xy} for $x, y \in X$ subject to the relations that $U = (u_{xy})$ be a magic unitary with *pairwise commuting entries*. In this case, the canonical Hopf *-algebra structure is defined by the same formulas as in the case of $\mathcal{Q}_X$. The canonical generators u_{xy} of $C(S_X)$ can be identified with the elements given by the characteristic functions of the set of permutations mapping x to y for $x, y \in X$. When X is a finite set with n elements, we also denote S_X with S_n and $\mathcal{Q}_X$ with $\mathcal{Q}_n$.

The quantum symmetric group $\mathcal{Q}_X$ admits a natural universal property. Recall that a *compact quantum space* $\mathbb{X}$ is given by a unital C*-algebra $C(\mathbb{X})$. An *action* of a compact quantum group $\mathbb{G}$ on $\mathbb{X}$ is given by a *-homomorphism $\alpha : C(\mathbb{X}) \to C(\mathbb{X}) \otimes C(\mathbb{G})$ satisfying:

- $(\alpha \otimes \mathrm{id}) \circ \alpha = (\mathrm{id} \otimes \Delta) \circ \alpha$;

- $[(1 \otimes C(\mathbb{G})) \alpha(C(\mathbb{X}))] = C(\mathbb{X}) \otimes C(\mathbb{G})$.

Given such an action of $\mathbb{G}$ on $\mathbb{X}$, the quantum orbit space $\mathbb{X}/\mathbb{G}$ is by definition the compact quantum space such that $C(\mathbb{X}/\mathbb{G})$ is the C*-subalgebra $C(\mathbb{X})^{\mathbb{G}} = \{a \in C(\mathbb{X}) : \alpha(a) = a \otimes 1\}$ of $C(\mathbb{X})$ (*fixed point algebra*). There is a canonical *conditional expectation* (nondegenerate $C(\mathbb{X}/\mathbb{G})$-bimodular completely positive map) $\mathrm{E}_{\mathbb{X}/\mathbb{G}} : C(\mathbb{X}) \to C(\mathbb{X}/\mathbb{G})$ given by $\mathrm{E}_{\mathbb{X}/\mathbb{G}} = (\mathrm{id} \otimes h) \circ \alpha$. The action α is called *transitive* or *homogeneous* if $C(\mathbb{X}/\mathbb{G}) = C(\mathbb{X})$. More information concerning actions of compact quantum groups on compact quantum spaces can be found in [16].

Any classical compact Hausdorff space X can in particular be regarded as a compact quantum space, by considering the algebra $C(X)$ of continuous complex-valued functions on X. If G is a classical compact group, then any classical action of G on X yields an action as defined above, and all the actions arise in this fashion. In this case, $C(X/G)$ coincides with the algebra of continuous functions on the quotient space X/G defined in the usual way as the space of G-orbits endowed with the quotient topology. Furthermore, the canonical conditional expectation $\mathrm{E}_{X/G} : C(X) \to C(X/G)$ is given by averaging the G-action with respect to the Haar probability measure on G.

9

In the particular case when X is a finite space, one has that $C(X) \cong \mathbb{C}^X$. The symmetric group S_X admits a canonical action on X which has the following universal property: for every compact group G and action of G on X, there exists a unique group morphism $G \to S_X$ that intertwines the actions. Similarly, the quantum symmetric group $\mathcal{Q}_X$ admits a canonical action α_u on X, defined by $\alpha_u : \mathbb{C}^X \to \mathbb{C}^X \otimes C(\mathcal{Q}_X)$, $e_x \mapsto \sum_y e_y \otimes u_{yx}$, where $(e_x)_{x \in X}$ denotes the canonical basis of $\mathbb{C}^X$. As shown in [28], such an action satisfies an analogous universal property within the class of actions of compact quantum groups on X. If $\mathbb{G}$ is a compact quantum group, and α is an action of $\mathbb{G}$ on X, then there exists a quantum group morphism from $\mathbb{G}$ to $\mathcal{Q}_X$ that intertwines α and α_u, i.e., a unital *-homomorphism $\varphi : C(\mathcal{Q}_X) \to C(\mathbb{G})$ such that $\Delta \circ \varphi = (\varphi \otimes \varphi) \circ \Delta$ and $\alpha \circ \varphi = (\mathrm{id} \otimes \varphi) \circ \alpha_u$.

One can generalize such a construction to define the quantum automorphism groups of graphs. Suppose now that X is a finite graph with vertex set $V(X)$ and adjacency matrix A. The (classical) automorphism group $\mathrm{Aut}(X)$ of X is the subgroup of $S_{V(X)}$ consisting of permutations that map pairs of adjacent vertices in X to pairs of adjacent vertices in X. One can see that the algebra $C(\mathrm{Aut}(X))$ of continuous functions on $\mathrm{Aut}(X)$ can be regarded as the universal C*-algebra generated by elements u_{xy} for $x, y \in V(X)$ subject to the relation that $U = (u_{xy})$ is a magic unitary with pairwise commuting entries such that $AU = UA$. The latter relation is equivalent to $u_{xy} u_{x'y'} = 0$ for vertices x, x', y, y' of X such that $\mathrm{rel}(x, x') \neq \mathrm{rel}(y, y')$, as shown in [17].

The *quantum automorphism group* of X, which we denote by $\mathrm{Qut}(X)$, is a compact quantum group defined by letting $C(\mathrm{Qut}(X))$ be the universal C*-algebra generated by elements u_{xy} for $x, y \in V(X)$, subject to the relations that $U = (u_{xy})$ is a magic unitary such that $AU = UA$, with comultiplication given by $\Delta(u_{xz}) = \sum_{y \in V(X)} u_{xy} \otimes u_{yz}$ for $x, z \in V(X)$. Clearly, in the particular case when X is the graph on n vertices without edges, $\mathrm{Qut}(X)$ recovers the quantum symmetric group $\mathcal{Q}_{V(X)}$. We also denote $C(\mathrm{Qut}(X))$ by $\mathcal{A}(X)$, and call it the *quantum symmetry algebra* of the graph X. Again, in this case one has that $C(\mathrm{Qut}(X))$ is the universal C*-algebra generated by $\mathcal{O}(\mathrm{Qut}(X))$, and the counit and antipode of $\mathcal{O}(\mathrm{Qut}(X))$ extends to bounded linear maps on $C(\mathrm{Qut}(X))$. Furthermore, in this case the antipode is a *-linear map, i.e., $\mathrm{Qut}(X)$ is of Kac type. In particular, this implies that the Haar state on $\mathrm{Qut}(X)$ is *tracial*.

The canonical surjective unital *-homomorphism from $C(\mathcal{Q}_{V(X)})$ to $C(\mathrm{Qut}(X))$ commutes with the comultiplication, and witnesses that $\mathrm{Qut}(X)$ is a *quantum subgroup* of $\mathcal{Q}_{V(X)}$. For similar reasons, the (classical) automorphism group $\mathrm{Aut}(X)$ is a quantum subgroup of $\mathrm{Qut}(X)$. More generally, given a finite set X, we say that a compact quantum group $\mathbb{G}$ is a *quantum permutation group acting on* X if it is a closed quantum subgroup of $\mathcal{Q}_X$, i.e., there exists a surjective unital *-homomorphism $C(\mathcal{Q}_X) \to C(\mathbb{G})$ that is covariant with respect to the coproducts of $\mathcal{Q}_X$ and $\mathbb{G}$. In this case, we call the image of the canonical generators of $C(\mathcal{Q}_X)$ inside $C(\mathbb{G})$ the canonical generators of $C(\mathbb{G})$. We remark that these form a magic unitary $u = (u_{xy})$, which we call the magic unitary generating $C(\mathbb{G})$. The *universal action* u of $\mathbb{G}$ on X is the action of $\mathbb{G}$ on X given by $u : \mathbb{C}^X \to \mathbb{C}^X \otimes C(\mathbb{G})$, $e_x \mapsto \sum_{y \in X} e_y \otimes u_{yx}$.

One says that a finite graph X *has no quantum symmetry* if $\mathrm{Aut}(X) = \mathrm{Qut}(X)$, i.e., the canonical unital *-homomorphism from $C(\mathrm{Qut}(X))$ onto $C(\mathrm{Aut}(X))$ is injective. This is equivalent to the assertion that $C(\mathrm{Qut}(X))$ is a commutative C*-algebra. It is shown in [28] that, for $n \in \{1, 2, 3\}$ the graph with no edges and n vertices has no quantum symmetry, i.e., $\mathcal{Q}_n = S_n$. However, already for $n = 4$ one has that the group $\mathcal{Q}_n$ is not classical, and in fact $C(\mathcal{Q}_n)$ is non-commutative and infinite-dimensional. For $n \leq 3$, the lack of any quantum symmetry follows from the fact that the entries of the magic unitary necessarily commute. This is trivial for $n = 1$, and it

remains straighforward for $n = 2$ since any 2×2 magic unitary has the form

$$\begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

For $n = 3$, most papers claim that the proof is "tricky" and makes use of the Fourier transform over $\mathbb{Z}_3$ and the universal action. However, here we present a short elementary proof. Another elementary, but longer proof, can be found in [21], where it is shown that the operators used to "quantum 3-color" the endpoints of an edge must commute.

Suppose that $U = (u_{ij})_{i,j \in [3]}$ is a magic unitary. It suffices to show that u_{ij} and $u_{\ell k}$ commute for $i \neq \ell$ and $j \neq k$, because all other pairs must commute (their product in either direction is zero) by the definition of magic unitaries. Since we can permute the rows and columns of a magic unitary independently and always produce a magic unitary, it suffices to show that $u_{11}u_{22} = u_{22}u_{11}$. We have that

$$u_{11}u_{22} = u_{11}u_{22}(u_{11} + u_{12} + u_{13}) = u_{11}u_{22}u_{11} + u_{11}u_{22}u_{13},$$

but

$$u_{11}u_{22}u_{13} = u_{11}(1 - u_{21} - u_{23})u_{13} = u_{11}u_{13} = 0.$$

Therefore $u_{11}u_{22} = u_{11}u_{22}u_{11}$ and thus $u_{22}u_{11} = u_{11}u_{22}$ by applying $*$ to this equation.

2.3 Coherent configurations/algebras

A *coherent configuration* [20] on a set X is a partition $\mathcal{R} = \{R_i : i \in \mathcal{I}\}$ of $X \times X$ into the *relations* (or *classes*) R_i satisfying the following:

1. There is a subset $\mathcal{D} \subseteq \mathcal{I}$ of the index set such that $\{R_d : d \in \mathcal{D}\}$ is a partition of the diagonal $\{(x, x) : x \in X\}$. These are called the *diagonal relations*.

2. For each R_i, its converse $\{(y, x) : (x, y) \in R_i\}$ is a relation, say $R_{i'}$, in $\mathcal{R}$. Note that $R_{i'} = R_i$ is possible.

3. For all $i, j, k \in \mathcal{I}$ and any $(x, z) \in R_k$, the number of $y \in X$ such that $(x, y) \in R_i$ and $(y, z) \in R_j$ is a constant p_{ij}^k that does not depend on x and z. We refer to the p_{ij}^k as the *intersection numbers* of $\mathcal{R}$.

The motivation here is that the orbits on $X \times X$ of any permutation group acting on X gives a coherent configuration, but the converse does not necessarily hold.

Given any coherent configuration, one can construct the matrices A^i for $i \in \mathcal{I}$ such that

$$A^i_{x,y} = \begin{cases} 1 & \text{if } (x, y) \in R_i \\ 0 & \text{otherwise.} \end{cases}$$

We will refer to the matrices A^i as the *characteristic matrices* of the configuration. One can consider the linear span of the matrices A^i, and it turns out that this will be a *coherent algebra*: a self-adjoint, unital algebra containing the all ones matrix and which is closed under Schur (entrywise) product. It is easy to see that most of these properties follow from the definition of a coherent configuration, with the possible exception of the fact that the span of the A^i is indeed closed under

matrix multiplication. This closure follows from property (3) above which can be written in terms of the characteristic matrices as $A^i A^j = \sum_k p_{ij}^k A^k$ for all $i, j \in \mathcal{I}$.

Conversely, it is a short exercise to show that any coherent algebra necessarily has a unique basis of 01-matrices (this follows from being closed under Schur product) which define a partition of $X \times X$ (since a coherent algebra contains the all ones matrix). It is then straightforward to check that this partition satisfies the conditions of being a coherent configuration. Thus, coherent configurations and coherent algebras are really just two perspectives on the same idea.

An important case of coherent configurations/algebras is the coherent algebra of a graph. It is not difficult to see that the intersection of two coherent algebras is again a coherent algebra. In terms of coherent configurations, the intersection of the algebras corresponds to the join (in the sense of partitions) of the two initial coherent configurations. Because of this, there is a unique smallest coherent algebra containing the adjacency matrix of a given graph, and this is called the coherent algebra of the graph. In terms of configurations, this is the coarsest coherent configuration such that the edge set of the graph is a union of its relations. We remark that this coherent algebra can be computed in polynomial time via the (2-dimensional) Weisfeiler-Leman method [29].

3 Quantum orbits and orbitals

Given a group Γ acting on a finite set X via the action $(\gamma, x) \mapsto \gamma \cdot x$, one can define its orbit equivalence relation $\sim$ on X as $x \sim y$ if there exists $\gamma \in \Gamma$ such that $\gamma \cdot x = y$. It is easy to see that this is an equivalence relation whose equivalence classes are the orbits of Γ. Moreover, the action of Γ on X induces *diagonal action* on $X \times X$ given by $\gamma \cdot (x, y) = (\gamma \cdot x, \gamma \cdot y)$. One can similarly define the orbits of this action, and these are often referred to as the *orbitals* of the Γ-action on X. We aim to define and investigate analogs of orbits and orbitals for the quantum automorphism groups of graphs.

Definition 3.1. *Suppose X is a finite set and $\mathcal{Q}$ is a quantum permutation group acting on X. Let $U = (u_{xy})_{x,y \in X}$ be a magic unitary defining $C(\mathcal{Q})$. Define the relations $\sim_1$ and $\sim_2$ on X and $X \times X$ respectively as follows:*

- *$x \sim_1 y$ if $u_{xy} \neq 0$;*

- *$(x, x') \sim_2 (y, y')$ if $u_{xy} u_{x'y'} \neq 0$.*

Of course, $x \sim_1 y$ is meant to be analogous to there being some permutation that maps x to y, and similarly $(x, x') \sim_2 (y, y')$ is meant to be analogous to there being some permutation that maps x to y while also mapping x' to y'. We will see that the analogy is fairly strong.

We will show that $\sim_1$ and $\sim_2$ are equivalence relations, and then define the orbits/orbitals of $\mathcal{Q}$ on X as their equivalence classes. In the course of the proof, we will use the Hopf *-algebra structure of $\mathcal{O}(\mathcal{Q})$ and the fact that the canonical generators u_{xy} belong to $\mathcal{O}(\mathcal{Q})$.

Lemma 3.2. *Given a quantum permutation group $\mathcal{Q}$ acting on a finite set X, the relation $\sim_1$ defined above is an equivalence relation.*

Proof. To see that $\sim_1$ is reflexive, recall that the counit, ε, of a quantum permutation group is given by $\varepsilon(u_{xy}) = \delta_{xy}$, and is a *-homomorphism. Therefore, $\varepsilon(u_{xx}) = 1$ implies that $u_{xx} \neq 0$. Therefore $x \sim_1 x$.

To see that $\sim_1$ is symmetric, recall that the antipode S of $\mathcal{Q}$ is given by $S(u_{xy}) = u_{yx}$, and it is an involutive anti-homomorphism. Therefore, if $u_{xy} \neq 0$, then $S^2(u_{xy}) = u_{xy} \neq 0$ implies that $u_{yx} = S(u_{xy}) \neq 0$. In other words, $x \sim_1 y$ implies that $y \sim_1 x$.

Now suppose that $u_{xy} \neq 0$ and $u_{yz} \neq 0$. Recall that the comultiplication $\Delta : C(\mathcal{Q}) \to C(\mathcal{Q}) \otimes C(\mathcal{Q})$ of $\mathcal{Q}$ is a $*$-homomorphism defined as $\Delta(u_{xz}) = \sum_w u_{xw} \otimes u_{wz}$. Thus

$$(u_{xy} \otimes u_{yz})\Delta(u_{xz}) = (u_{xy} \otimes u_{yz}) \sum_w u_{xw} \otimes u_{wz}$$

$$= \sum_w u_{xy}u_{xw} \otimes u_{yz}u_{wz} = u_{xy} \otimes u_{yz} \neq 0.$$

Therefore $\Delta(u_{xz}) \neq 0$ and so $u_{xz} \neq 0$. This shows that if $x \sim_1 y$ and $y \sim_1 z$, then $x \sim_1 z$, i.e., the relation $\sim_1$ is transitive.

Altogether, the above implies that $\sim_1$ is an equivalence relation as desired. $\qquad \square$

The above lemma allows us to give the following definition:

Definition 3.3. *Given a quantum permutation group $\mathcal{Q}$ acting on a finite set X, the* orbits *of $\mathcal{Q}$ are the equivalence classes of the relation $\sim_1$ defined above. In the case where $\mathcal{Q}$ is the quantum automorphism group of a graph X, we will sometimes refer to its orbits as the* quantum orbits *of X, in order to distinguish them from the orbits of its (classical) automorphism group.*

We remark that orbits of quantum permutation groups were independently introduced and studied by Banica and Freslon in the recent paper [8]. To our knowledge, this is the first time that orbitals have been considered in the quantum setting.

Now we will show that $\sim_2$ is an equivalence relation as we did for $\sim_1$.

Lemma 3.4. *Given a quantum permutation group $\mathcal{Q}$ acting on a finite set X, the relation $\sim_2$ defined above is an equivalence relation.*

Proof. Since $\varepsilon(u_{xx}u_{yy}) = \varepsilon(u_{xx})\varepsilon(u_{yy}) = 1 \cdot 1 = 1$, we have that $u_{xx}u_{yy} \neq 0$. Therefore $(x, y) \sim_2 (x, y)$, i.e., $\sim_2$ is reflexive.

If $(x, x') \sim_2 (y, y')$, then $u_{xy}u_{x'y'} \neq 0$ and hence $u_{x'y'}u_{xy} = (u_{xy}u_{x'y'})^* \neq 0$. Since the antipode S is an involution, this implies that

$$0 \neq S(u_{x'y'}u_{xy}) = u_{yx}u_{y'x'}$$

and thus $(y, y') \sim_2 (x, x')$. So we have shown that $\sim_2$ is symmetric.

Now suppose that $(x, x') \sim_2 (y, y')$ and $(y, y') \sim_2 (z, z')$, i.e., that $u_{xy}u_{x'y'} \neq 0 \neq u_{yz}u_{y'z'}$. Then

$$\Delta(u_{xz}u_{x'z'}) = \Delta(u_{xz})\Delta(u_{x'z'}) = \left(\sum_w u_{xw} \otimes u_{wz}\right)\left(\sum_{w'} u_{x'w'} \otimes u_{w'z'}\right) = \sum_{w,w'} u_{xw}u_{x'w'} \otimes u_{wz}u_{w'z'}.$$

Therefore,

$$(u_{xy} \otimes u_{yz})\Delta(u_{xz}u_{x'z'})(u_{x'y'} \otimes u_{y'z'}) = \sum_{w,w'} u_{xy}u_{xw}u_{x'w'}u_{x'y'} \otimes u_{yz}u_{wz}u_{w'z'}u_{y'z'}$$

$$= u_{xy}u_{x'y'} \otimes u_{yz}u_{y'z'} \neq 0$$

13

since each factor in the tensor product is nonzero by assumption. This implies that $\Delta(u_{xz}u_{x'z'}) \neq 0$ and therefore $u_{xz}u_{x'z'} \neq 0$, i.e., $(x, x') \sim_2 (z, z')$. This shows that $\sim_2$ is transitive and thus we have shown it is an equivalence relation. $\qquad\square$

Now we can consider the following:

Definition 3.5. *Given a quantum permutation group $\mathcal{Q}$ acting on a finite set X, the* orbitals *of $\mathcal{Q}$ are the equivalence classes of the relation $\sim_2$ defined above. In the case where $\mathcal{Q}$ is the quantum automorphism group of a graph X, we will sometimes refer to its orbitals as the* quantum orbitals *of X.*

Remark 3.6. *Using the fact that $u_{xy}^2 = u_{xy}$, we have that the relation $\sim_1$ "agrees" with $\sim_2$, when X is identified with the diagonal of $X \times X$. Since the diagonal is invariant with respect to $\sim_2$, one can say that the orbits are precisely the orbitals contained in the diagonal.*

3.1   An equivalent definition

In this section, we verify that the notion of quantum orbits from the previous subsection coincides with the usual notion of quantum orbits for an action of a compact quantum group on a compact (quantum) space. This has also been shown in [8]. Here we additionally provide an analogous characterization of the orbitals. This might be surprising, as in general the "quantum orbital space" of a compact quantum group action is not well defined, as there does not exist in general a quantum analog of the "diagonal action" associated with a given action.

Let $\mathcal{Q}$ be a quantum permutation group on a set X, and let $U = (u_{ij})$ be the magic unitary whose entries are the canonical generators of $C(\mathcal{Q})$. Recall that the *universal action* $u : \mathbb{C}^X \to \mathbb{C}^X \otimes C(\mathcal{Q})$ of $\mathcal{Q}$ is the linear map defined on the standard basis vectors as

$$u(e_i) = \sum_{j \in X} e_j \otimes u_{ji}.$$

The corresponding quantum orbit space is given by the selfadjoint subalgebra $(\mathbb{C}^X)^{\mathcal{Q}}$ of $\mathbb{C}^X$ defined as those elements $f \in \mathbb{C}^X$ such that $u(f) = f \otimes 1$. We say that $(\mathbb{C}^X)^{\mathcal{Q}}$ is *trivial* if it only contains the scalar multiples of $1 \in \mathbb{C}^X$ (the vector with all entries equal to one). As u is a $*$-homomorphism, $(\mathbb{C}^X)^{\mathcal{Q}}$ is a C*-subalgebra of $\mathbb{C}^X$, and therefore has a unique basis of 01-vectors which corresponds to a partition of X. We will show that the classes of this partition are precisely the orbits of $\mathcal{Q}$ as defined in the previous section. We note that $(\mathbb{C}^X)^{\mathcal{Q}}$ can be also seen as the space $\mathrm{Hom}(1, u)$ of intertwiners from the trivial representation 1 to u.

Lemma 3.7. *Let $\mathcal{Q}$ be a quantum permutation group on a set X, with universal action u. Then $u(f) = f \otimes 1$ is equivalent to f being constant on the orbits of $\mathcal{Q}$.*

Proof. Letting f_i be the ith component of f, we have that

$$u(f) = \sum_i f_i u(e_i) = \sum_{i,j} f_i e_j \otimes u_{ji} = \sum_j e_j \otimes \left(\sum_i f_i u_{ji} \right);$$
$$f \otimes 1 = \sum_j e_j \otimes f_j 1.$$

These two expressions are equal if and only if $\sum_i f_i u_{ji} = f_j 1$ for all $j \in X$. Multiplying both sides of this equation by u_{jk} for some fixed $k \in X$, we see that a necessary condition for it holding is that $f_k u_{jk} = f_j u_{jk}$ for all $k \in X$. This implies that $f_k = f_j$ must hold for all j, k such that $u_{jk} \neq 0$, i.e., that f must be constant on the orbits of $\mathcal{Q}$.

On the other hand, if f is constant on the orbits of $\mathcal{Q}$, then $f_i = f_j$ unless $u_{ji} = 0$. Therefore, $\sum_i f_i u_{ji} = \sum_i f_j u_{ji} = f_j \sum_i u_{ji} = f_j 1$ for all $j \in X$. Thus we have proven the lemma. $\qquad\square$

As a special case of the above, we see that the notion of transitivity of a quantum permutation group coincides with the more combinatorial definition of there being a single orbit.

Corollary 3.8. *Let $\mathcal{Q}$ be a quantum permutation group acting on a finite set X. The following are equivalent:*

1. *$\mathcal{Q}$ acts transitively on X, i.e., the fixed point algebra $(\mathbb{C}^X)^{\mathcal{Q}}$ is trivial;*

2. *$\mathcal{Q}$ has only one orbit on X;*

3. *there exists $x \in X$ such that $u_{xy} \neq 0$ for all $y \in X$;*

4. *$u_{xy} \neq 0$ for all $x, y \in X$.*

We can also prove an analog of Lemma 3.7 for orbitals as well. For this, we need to consider the tensor square of the representation u, which is the representation $u^{\otimes 2}$ of $\mathcal{Q}$ on $\mathbb{C}^X \otimes \mathbb{C}^X$ defined on the standard basis elements by:

$$u^{\otimes 2}(e_i \otimes e_{i'}) = \sum_{j,j'} (e_j \otimes e_{j'}) \otimes u_{ji} u_{j'i'}.$$

The space of fixed points of $u^{\otimes 2}$ is defined in the same manner as for u:

$$\mathrm{Hom}(1, u^{\otimes 2}) = \{f \in \mathbb{C}^X \otimes \mathbb{C}^X : u^{\otimes 2}(f) = f \otimes 1\}.$$

Such a representation can be seen as the analog of the diagonal action, even though $u^{\otimes 2}$ is not in general an action. Nonetheless, we will show that $\mathrm{Hom}(1, u^{\otimes 2})$ is a selfadjoint subalgebra of $\mathbb{C}^X \otimes \mathbb{C}^X$, whose corresponding equivalence relation on $X \times X$ has the orbitals as classes.

Lemma 3.9. *Let $\mathcal{Q}$ be a quantum permutation group on a set X, with universal action u. Then $u^{\otimes 2}(f) = f \otimes 1$ if and only if f is constant on the orbitals of $\mathcal{Q}$.*

Proof. We have that

$$u^{\otimes 2}(f) = \sum_{x,x'} f_{xx'} u(e_x \otimes e_{x'}) = \sum_{x,x',y,y'} f_{xx'}(e_y \otimes e_{y'}) \otimes u_{yx} u_{y'x'} = \sum_{y,y'} (e_y \otimes e_{y'}) \otimes \left(\sum_{x,x'} f_{xx'} u_{yx} u_{y'x'}\right);$$

$$f \otimes 1 = \sum_{y,y'} (e_y \otimes e_{y'}) \otimes f_{yy'} 1.$$

These two expressions are equal if and only if $\sum_{x,x'} f_{xx'} u_{yx} u_{y'x'} = f_{yy'} 1$ for all $y, y' \in X$. Multiplying both sides of this equation on the left by u_{yz} and on the right by $u_{y'z'}$ for some $z, z' \in X$, we see that a necessary condition for it to hold is that $f_{zz'} u_{yz} u_{y'z'} = f_{yy'} u_{yz} u_{y'z'}$ for all $z, z' \in X$.

This implies that $f_{zz'} = f_{yy'}$ whenever $u_{yz}u_{y'z'} \neq 0$, i.e., whenever (y, y') and (z, z') are in the same orbital of $\mathcal{Q}$. This proves that if $u^{\otimes 2}(f) = f \otimes 1$, then f is constant on the orbitals of $\mathcal{Q}$.

Conversely, if f is constant on the orbitals of $\mathcal{Q}$, then $f_{xx'} = f_{yy'}$ whenever $u_{yx}u_{y'x'} \neq 0$. Therefore,

$$\sum_{x,x'} f_{xx'}u_{yx}u_{y'x'} = \sum_{x,x'} f_{yy'}u_{yx}u_{y'x'} = f_{yy'}\sum_{x,x'} u_{yx}u_{y'x'} = f_{yy'}1$$

as desired. □

3.2 A coherent configuration

Given a group Γ acting on a set X, it is well known that the orbitals of Γ form a coherent configuration on X. Indeed, this was part of the original motivation for studying coherent configurations. Here we will show that the same holds for the orbitals of a quantum permutation group.

Theorem 3.10. *Let $\mathcal{Q}$ be a quantum permutation group $\mathcal{Q}$ acting on a set X, and let $U = (u_{xy})_{x,y \in X}$ be the magic unitary defining $\mathcal{Q}$. Then for a scalar matrix M we have that $MU = UM$ if and only if M is constant on the orbitals of $\mathcal{Q}$. As a consequence, the orbitals of $\mathcal{Q}$ form a coherent configuration.*

Proof. Consider the canonical linear isomorphism from $\mathbb{C}^X \otimes \mathbb{C}^X$ to $\text{End}(\mathbb{C}^X)$ taking $e_x \otimes e_y \mapsto e_x e_y^T$. By Frobenius reciprocity this restricts to a linear isomorphism from $\text{Hom}(1, u^{\otimes 2})$ to $\text{End}_{\mathcal{Q}}(U) = \{M \in \text{End}(\mathbb{C}^X) : MU = UM\}$. By Lemma 3.9, it immediately follows that $M \in \text{End}_{\mathcal{Q}}(U)$ if and only if M is constant on the orbitals of $\mathcal{Q}$. Thus we have proven the first claim.

For the second claim, first note that if $M, N \in \text{End}_{\mathcal{Q}}(U)$, then $(MN)U = MUN = U(MN)$ and thus $MN \in \text{End}_{\mathcal{Q}}(U)$. Moreover, $\text{End}_{\mathcal{Q}}(U)$ is obviously closed under linear combinations and contains the identity, thus $\text{End}_{\mathcal{Q}}(U)$ is a unital algebra. Next, a consequence of the first claim is that $\text{End}_{\mathcal{Q}}(U)$ is the linear span of the characteristic matrices of the orbitals of $\mathcal{Q}$. As these are 01-matrices, this implies that $\text{End}_{\mathcal{Q}}(U)$ is closed under Schur product. We also have that the constant matrix J is necessarily constant on the orbitals of $\mathcal{Q}$, and thus $J \in \text{End}_{\mathcal{Q}}(U)$. Lastly, if $M \in \text{End}_{\mathcal{Q}}(U)$, then $M^*U = (U^*M)^* = (U^*MUU^*)^* = (U^*UMU^*)^* = (MU^*)^* = UM^*$, i.e., $M^* \in \text{End}_{\mathcal{Q}}(U)$. Together these properties show that $\text{End}_{\mathcal{Q}}(U)$ is a coherent algebra, and thus its *unique* basis of 01-matrices form the characteristic matrices of a coherent configuration. But by the first claim we have that this coherent configuration is precisely the set of orbitals of $\mathcal{Q}$. □

Due to the above theorem, we give the following definition:

Definition 3.11. *Let X be a graph with quantum automorphism group $\text{Qut}(X)$. We define the* quantum orbital configuration/algebra *of X as the coherent configuration/algebra produced by the orbitals of $\text{Qut}(X)$ acting on $V(X)$.*

We will similarly refer to the coherent configuration/algebra produced by the orbitals of $\text{Aut}(X)$ as the *orbital configuration/algebra* of X. We note that the orbital configuration is a (possibly trivial) refinement of the quantum orbital configuration or, equivalently, the quantum orbital algebra is a subalgebra of the orbital algebra. This follows from the fact that $\text{Aut}(X)$ is a quantum subgroup of $\text{Qut}(X)$. More concretely, for any $\sigma \in \text{Aut}(X)$ the mapping $u_{x\sigma(x)} \mapsto 1$ and $u_{xy} \mapsto 0$ for all $y \neq \sigma(x)$ gives a representation of the quantum symmetry algebra of X. Thus if $\sigma(x) = y$ and

16

$\sigma(x') = y'$, then $u_{xy}u_{x'y'} \neq 0$ since its image is nonzero in this representation. Therefore, if (x, x') and (y, y') are in the same (classical) orbital of X, they are in the same quantum orbital as well.

We remark here that the coherent configuration of a graph can "detect" many properties of the graph. More precisely, the classes of the configuration can detect properties of the pairs of vertices they correspond to. For instance, if X is a graph with adjacency matrix A, then for all $\ell \in \mathbb{N}$ the power A^ℓ of A is in the coherent algebra of X, and the entries of A^ℓ record the number of walks of length ℓ between pairs of vertices. Thus if two pairs of vertices have a different number of walks of length ℓ between them, then they must be in different classes of the coherent configuration (since A^ℓ must lie in the span of the characteristic matrices of the classes). It is not too hard to see that this also means that pairs of vertices at different distances cannot be in the same class, and one can similarly find many other properties of pairs of vertices that are detected by the coherent configuration of the graph. For instance, this implies the adjacency matrix of the d-distance graph of X is contained in its coherent algebra for all d. Since this holds for the coherent configuration of X, it also holds for the quantum orbital configuration of X. It is an interesting question what additional properties are detected by the latter configuration.

We also remark that, in the classical case, the permutations in the automorphism group of a graph can be represented as permutation matrices. These permutation matrices are exactly those that commute with the adjacency matrix of the graph, but they will also commute with the characteristic matrices of the orbitals of the automorphism group. In fact, the orbital algebra of X is exactly the commutant of $\mathrm{Aut}(X)$ when considered as a subgroup of the permutation matrices. Of course Theorem 3.10 represents the quantum analog of this fact.

We cannot help but mention that Higman introduced coherent algebras in order to 'do group theory without groups', and here we are constructing coherent algebras from quantum groups, which are another approach to studying group theory without groups.

3.3   Using the coherent algebra of a graph

One purpose of the Theorem 3.10 is to provide more information about the quantum automorphism group of a graph. However, one might argue that it could be difficult or impossible to determine the quantum orbitals of a given graph, and so Theorem 3.10 may not be of much use. But, as we mentioned previously, one can efficiently compute the coherent configuration of a graph. In this section we will see that this is a useful tool for studying the quantum automorphism group of a graph.

Recall from the end of Section 3.2, that the quantum orbital algebra of a graph X is a subalgebra of the orbital algebra of X, i.e., the orbital configuration of X is a refinement of the quantum orbital configuration of X. On the other hand, the quantum orbital algebra of a graph must contain its adjacency matrix, since $(x, x') \sim_2 (y, y')$ (i.e. $u_{xy}u_{x'y'} \neq 0$) is not possible if one of the pairs form an edge and the other does not. Therefore, the quantum orbital algebra of a graph X must contain the coherent algebra of X, and thus the classes of the coherent configuration of X must be unions of the orbitals of $\mathrm{Qut}(X)$. From this we obtain the following two corollaries:

Corollary 3.12. *Let X be a graph with adjacency matrix A. Then a magic unitary U that commutes with A also commutes with every element of the coherent algebra of X.*

Corollary 3.13. *Let X be a graph with adjacency matrix A. If U is a magic unitary that commutes with A, then $u_{xy}u_{x'y'} = 0$ unless (x, x') and (y, y') are in the same class of the coherent configuration*

17

of X.

Using the second corollary above, we can show that almost all graphs have trivial quantum automorphism group.

Theorem 3.14. *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.*

Proof. Let U be the magic unitary defining $\mathrm{Qut}(X)$. It is known (it follows from Theorem 4.1 of [3] for instance) that almost all graphs have coherent algebras equal to the full matrix algebra. As the coherent algebra of a graph is contained in its quantum orbital algebra, the latter is also the full matrix algebra for almost all graphs. This implies that the magic unitary U defining $\mathrm{Qut}(X)$ commutes with any scalar matrix and thus $U = 1 \otimes 1$ by the double commutant theorem. It follows that $\mathrm{Qut}(X)$ is trivial. □

Though the above result is not surprising (it is well known that it holds for classical automorphisms), it is not immediately obvious how to prove this in the quantum case. Thus the above theorem exhibits the usefulness of coherent configurations/algebras in the study of quantum permutation groups. In Section 5, we will discuss a possible application of Theorem 3.10 for showing that certain graphs have no quantum symmetry.

4 Quantum Isomorphism

In Section 2.1, we introduced the notions of quantum tensor isomorphism and quantum commuting isomorphism. Here we will define a notion of quantum isomorphism that fits naturally with the already existing notion of quantum automorphism.

Definition 4.1. *We say that graphs X and Y with adjacency matrices A and B are* quantum isomorphic, *and write $X \cong_q Y$, if there exists a Hilbert space $\mathcal{H}$, a magic unitary $U = (u_{xy})$ with $u_{xy} \in \mathcal{B}(\mathcal{H})$ for all $x \in V(X), y \in V(Y)$ such that $AU = UB$ or, equivalently, $u_{xy}u_{x'y'} = 0$ if $\mathrm{rel}(x, x') \neq \mathrm{rel}(y, y')$.*

Because of the correspondence between C^*-algebras and algebras of bounded linear operators on a Hilbert space, the above is easily seen to be equivalent to the definition of quantum commuting isomorphism given by Theorem 2.5, except without the requirement of a tracial state. Therefore, $X \cong_{qc} Y$ implies $X \cong_q Y$ for any graphs X and Y. We have already mentioned that $X \cong_{qt} Y \Rightarrow X \cong_{qc} Y$, and so we have the following chain of implications:

$$X \cong Y \ \Rightarrow \ X \cong_{qt} Y \ \Rightarrow \ X \cong_{qc} Y \ \Rightarrow \ X \cong_q Y.$$

The fact that the first two implications cannot be reversed was proven in [2]. In Section 4.2, we will show that the last implication can be reversed, thus quantum isomorphism and quantum commuting isomorphism are the same relation.

It also follows from the above that the non-isomorphic but quantum tensor isomorphic graphs constructed in [2] provide us with examples of non-isomorphic but quantum isomorphic graphs. We do not contribute anything more on this front, but we will see later that we can use these examples to construct graphs which are quantum vertex transitive but not vertex transitive, answering a question from the quantum permutation group literature. First, we will show that if two graphs

18

are quantum isomorphic, then there is an isomorphism of their quantum orbital algebras that maps the adjacency matrix of one to that of the other. This result is inspired by results in an upcoming work [23] of Varvitsiotis and the second and third authors, in which they show that a certain semidefinite relaxation of quantum tensor/commuting isomorphism is equivalent to the existence of an isomorphism of the coherent algebras of two graphs which maps the adjacency matrix of one to the other.

4.1   The Haar state

In this section, we will compute the value of the Haar state of a quantum permutation group on products of pairs of generators. We will see that the value depends only on the sizes of the orbitals of the quantum permutation groups.

Theorem 4.2. *Let $\mathcal{Q}$ be a quantum permutation group on a set X. Let $U = (u_{xy})$ be the magic unitary defining $C(\mathcal{Q})$ and 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*

$$h(u_{xy}u_{x'y'}) = \begin{cases} 1/|R_i| & \text{if } (x, x'), (y, y') \in R_i; \\ 0 & \text{if } (x, x') \not\sim_2 (y, y'). \end{cases}$$

Proof. Note that the $(x, x') \not\sim_2 (y, y')$ case is trivial since in this case $u_{xy}u_{x'y'} = 0$ by definition.

So suppose that $(x, x'), (y, y'), (z, z') \in R_i$. We will show that $h(u_{xy}u_{x'y'}) = h(u_{xz}u_{x'z'})$, i.e., changing the second indices to another pair of vertices in the same orbital does not change the value of h. Recall from Section 2.2 that $(h \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes h)\Delta = h(\cdot)1$. Therefore, we have that

$$h(u_{xz}u_{x'z'})1 = (h \otimes \mathrm{id})\Delta(u_{xz}u_{x'z'}) = (h \otimes \mathrm{id})\Delta(u_{xz})\Delta(u_{x'z'})$$

$$= (h \otimes \mathrm{id})\left(\left(\sum_{w \in X} u_{xw} \otimes u_{wz}\right)\left(\sum_{w' \in X} u_{x'w'} \otimes u_{w'z'}\right)\right)$$

$$= (h \otimes \mathrm{id})\left(\sum_{w, w' \in X} u_{xw}u_{x'w'} \otimes u_{wz}u_{w'z'}\right)$$

$$= (h \otimes \mathrm{id})\left(\sum_{(w, w') \in R_i} u_{xw}u_{x'w'} \otimes u_{wz}u_{w'z'}\right)$$

$$= \sum_{(w, w') \in R_i} h(u_{xw}u_{x'w'})u_{wz}u_{w'z'}.$$

Multiplying this equation on the left by u_{yz} and on the right by $u_{y'z'}$, we obtain

$$h(u_{xz}u_{x'z'})u_{yz}u_{y'z'} = h(u_{xy}u_{x'y'})u_{yz}u_{y'z'}.$$

Since $(y, y'), (z, z') \in R_i$, we have that $u_{yz}u_{y'z'} \neq 0$, and therefore $h(u_{xz}u_{x'z'}) = h(u_{xy}u_{x'y'})$. This shows that for $(x, x') \in R_i$, we have that $h(u_{xw}u_{x'w'})$ is constant for all $(w, w') \in R_i$ (and is zero otherwise).

Now, again fixing $(x, x')(y, y') \in R_i$, we have that

$$1 = h(1) = h\left(\sum_{w,w' \in X} u_{xw} u_{x'w'}\right) = \sum_{w,w' \in X} h(u_{xw} u_{x'w'}) = \sum_{(w,w') \in R_i} h(u_{xw} u_{x'w'}) = |R_i| h(u_{xy} u_{x'y'}).$$

Thus $h(u_{xy} u_{x'y'}) = 1/|R_i|$, and $(x, x'), (y, y')$ were arbitrary elements of R_i so we are done. $\qquad\square$

As a consequence of the above and Remark 3.6, we have the following:

Corollary 4.3. *Let $\mathcal{Q}$ be a quantum permutation group on a set X. Let $U = (u_{xy})$ be the magic unitary defining $C(\mathcal{Q})$ and let h denote the Haar state on $C(\mathcal{Q})$. If $O_1, \dots, O_m \subseteq X$ are the orbits of $\mathcal{Q}$ on X, then*

$$h(u_{xy}) = \begin{cases} 1/|O_i| & \text{if } x, y \in O_i; \\ 0 & \text{if } x \not\sim_1 y. \end{cases}$$

4.2 Quantum isomorphism and quantum commuting isomorphism are the same

In the beginning of Section 4, we noted that $X \cong_{qc} Y$ implies that $X \cong_q Y$ for any graphs X and Y. Here we will show that this implication can be reversed, thus proving that these two relations are equivalent.

Theorem 4.4. *Let X and Y be graphs. Then $X \cong_q Y$ if and only if $X \cong_{qc} Y$.*

Proof. We only need to show that if $X \cong_q Y$, then $X \cong_{qc} Y$. So suppose that the former holds. By taking complements if necessary, we may assume that X is connected. It follows from Corollary 4.7 that Y is also connected. Let $Z = X \cup Y$ be the disjoint union of X and Y. Also, let $U = (u_{wz})$ for $w, z \in V(Z)$ be the magic unitary defining $C(\mathrm{Qut}(Z))$. We will show that $u_{xy} u_{x'x''} = 0$ for all $y \in V(Y)$ and $x, x', x'' \in V(X)$.

Since X is connected, the distance in Z between $x, x' \in V(X)$ is finite. On the other hand, there is no path between y and x'' in Z. This implies that (x, x') and (y, x'') cannot be in the same class of the coherent configuration of Z (see the discussion at the end of Section 3.2). Since the classes of the quantum orbital configuration are refinements of the classes of the coherent configuration, we see that (x, x') and (y, x'') cannot be in the same orbital of $\mathrm{Qut}(Z)$. Therefore, $u_{xy} u_{x'x''} = 0$ as desired.

Now, for each $x \in V(X)$, define the projection $p_x = \sum_{y \in V(Y)} u_{xy}$. We will show that $p_x = p_{x'}$ for all $x, x' \in V(X)$. From the above, we have that

$$p_x(1 - p_{x'}) = p_x\left(\sum_{x'' \in V(X)} u_{x'x''}\right) = 0.$$

So $p_x = p_x p_{x'}$, and similarly we can show that $p_{x'} = p_x p_{x'}$. Thus $p_x = p_{x'}$ as desired. Similarly, we can define $p_y = \sum_{x \in V(X)} u_{xy}$, and these will all be equal. Next we want to show that $p_x = p_y$. We have that

$$|V(X)| p_x = \sum_{x \in V(X)} p_x = \sum_{x \in V(X), y \in V(Y)} u_{xy} = \sum_{y \in V(Y)} p_y = |V(Y)| p_y.$$

20

This implies that p_x is proportional to p_y, but since they are both projections, we must have that $p_x = p_y$. Since all of these projections are equal, we will refer to them simply as p from now on.

Next, we want to show that $p \neq 0$. Since $X \cong_q Y$, we have that there are operators v_{xy} for $x \in V(X)$, $y \in V(Y)$ on some Hilbert space such that the matrix $V = (v_{xy})$ is a magic unitary and $v_{xy}v_{x'y'} = 0$ whenever $\mathrm{rel}(x, x') \neq \mathrm{rel}(y, y')$. Then it is easy to see that mapping u_{xy} to v_{xy} for $x \in V(X)$, $y \in V(Y)$ and mapping all other u_{wz} to zero is a representation of $C(\mathrm{Qut}(X))$. Moreover, in this representation, the element p is mapped to $\sum_{y \in V(Y)} v_{xy} = 1$. Since p is mapped to a nonzero element in this representation, we have that $p \neq 0$ in $C(\mathrm{Qut}(Z))$. Note that this implies that for any $x \in V(X)$, there exists some $y \in V(Y)$ such that x and y are in the same orbit of $\mathrm{Qut}(Z)$.

Now let $\mathcal{A}$ be the C^*-subalgebra of $C(\mathrm{Qut}(Z))$ generated by the elements u_{xy} for $x \in V(X)$, $y \in V(Y)$. Note that p is the identity in $\mathcal{A}$, since

$$u_{xy}p = u_{xy} \sum_{y' \in V(Y)} u_{xy'} = u_{xy}^2 = u_{xy},$$

and similarly $pu_{xy} = u_{xy}$. This means that the matrix $\hat{U} = (u_{xy})$ for $x \in V(X)$, $y \in V(Y)$ is a magic unitary over $\mathcal{A}$. Moreover, we have that $u_{xy}u_{x'y'} = 0$ if $\mathrm{rel}(x, x') \neq \mathrm{rel}(y, y')$, since this was true in $C(\mathrm{Qut}(Z))$. Thus, $\hat{U}$ is a magic unitary such that $A\hat{U} = \hat{U}B$ where A and B are the adjacency matrices of X and Y respectively. This only shows that $X \cong_q Y$, which we had already assumed, and so we still need to construct a tracial state on $\mathcal{A}$.

Let h be the Haar state on $C(\mathrm{Qut}(Z))$, and recall that this is tracial, i.e., $h(ab) = h(ba)$ for all $a, b \in C(\mathrm{Qut}(Z))$. It is easy to see that the restriction of h to $\mathcal{A}$ satisfies all of the conditions of being a tracial state on $\mathcal{A}$, except that it may not evaluate to one on the identity p. Recall from above that for any $x \in V(X)$ there is some $y \in V(Y)$ such that x and y are in the same orbit of $\mathrm{Qut}(Z)$. Thus, by definition of p and Corollary 4.3 we have that $h(p) > 0$, and so we can define $\hat{h}(\cdot) = h(\cdot)/h(p)$. This is our tracial state on $\mathcal{A}$, and so by Theorem 2.5 and Remark 2.6 we are done. $\qquad\square$

Note that in the above, the only place where we used the fact that $X \cong_q Y$ was to assume without loss of generality that X and Y are both connected and to show that $p \neq 0$. The latter happens if and only if there exists $x \in V(X)$ and $y \in V(Y)$ such that $u_{xy} \neq 0$. Therefore, we immediately have the following:

Theorem 4.5. *Let X and Y be connected graphs. Then $X \cong_{qc} Y$ if and only if there exists $x \in V(X)$ and $y \in V(Y)$ that are in the same orbit of $\mathrm{Qut}(X \cup Y)$.*

Since any graph is either connected or has a connected complement, and connected graphs can only be quantum isomorphic to connected graphs, the above reduces the question of quantum isomorphism to the determination of the orbits of a quantum permutation group, which is exactly analogous to the classical case.

4.3 Isomorphisms of coherent algebras

Given coherent algebras $\mathcal{C}$ and $\mathcal{C}'$, an isomorphism $\Phi : \mathcal{C} \to \mathcal{C}'$ is a linear bijection which, for any $M, N \in \mathcal{C}$, satisfies

- $\Phi(MN) = \Phi(M)\Phi(N)$;

- $\Phi(M^*) = \Phi(M)^*$;

- $\Phi(M \circ N) = \Phi(M) \circ \Phi(N)$, where $\circ$ denotes Schur product;

- $\Phi(I) = I$ and $\Phi(J) = J$.

Consider the coherent configurations $\mathcal{R} = \{R_i : i \in \mathcal{I}\}$ and $\mathcal{R}' = \{R'_i : i \in \mathcal{I}'\}$ corresponding to $\mathcal{C}$ and $\mathcal{C}'$. Suppose that $\mathcal{R}$ and $\mathcal{R}'$ have intersection numbers p_{ij}^k for $i, j, k \in \mathcal{I}$ and q_{ij}^k for $i, j, k \in \mathcal{I}'$ respectively. It is well known and not too difficult to see that an isomorphism from $\mathcal{C}$ to $\mathcal{C}'$ is equivalent to a bijection $f : \mathcal{I} \to \mathcal{I}'$ such that $p_{ij}^k = q_{f(i)f(j)}^{f(k)}$ for all $i, j, k \in \mathcal{I}$. The corresponding isomorphism Φ will then map the characteristic matrix of R_i to that of $R'_{f(i)}$ for all $i \in \mathcal{I}$.

It is obvious that isomorphic graphs have isomorphic orbital algebras. The isomorphism is given by conjugation with a permutation matrix encoding the isomorphism of the two graphs. However, the converse does not hold: there are graphs with isomorphic orbital algebras which are not isomorphic themselves. An example would be the Paley and Peisert graphs of the same order.

Here we show that quantum isomorphic graphs have isomorphic quantum orbital algebras, in analogy with the fact for isomorphic graphs.

Theorem 4.6. *Suppose that X and Y are quantum isomorphic graphs with adjacency matrices A and B. Then there exists an isomorphism Φ of their quantum orbital algebras such that $\Phi(A) = B$.*

Proof. Let $\mathcal{R} = \{R_i : i \in \mathcal{I}\}$ and $\mathcal{R}' = \{R'_i : i \in \mathcal{I}'\}$ be the quantum orbital configurations of X and Y respectively, with intersection numbers p_{ij}^k and q_{ij}^k. Let $V = (v_{xy})$ be the magic unitary witnessing the quantum isomorphism of X and Y. Assume that $V(X)$ and $V(Y)$ are disjoint and define a relation $\sim_v$ on $(V(X) \times V(X)) \cup (V(Y) \times V(Y))$ by $(x, x') \sim_v (y, y')$ if $v_{xy}v_{x'y'} \neq 0$. We will think of this relation as defining a bipartite graph W with parts $V(X) \times V(X)$ and $V(Y) \times V(Y)$. We will show that this relation gives rise to a bijection $f : \mathcal{I} \to \mathcal{I}'$ that provides us with the required isomorphism.

First, we will use our quantum isomorphism of X and Y to construct a magic unitary that commutes with A. Let $U = (u_{yy'})$ for $y, y' \in V(Y)$ be the magic unitary defining the quantum symmetry algebra of Y. Consider the matrix $\hat{V} = (\hat{v}_{xx'})$ for $x, x' \in V(X)$ defined as

$$\hat{v}_{xx'} = \sum_{y, y' \in V(Y)} v_{xy} \otimes u_{yy'} \otimes v_{x'y'}.$$

Intuitively, this is capturing the idea of composing an isomorphism from X to Y with an automorphism of Y and then followed by an isomorphism from Y back to X. It is easy to see that $\hat{v}_{xx'} = \hat{v}_{xx'}^*$ for all $x \in x' \in V(X)$. Moreover,

$$\hat{v}_{xx'}^2 = \sum_{y, y', w, w' \in V(Y)} v_{xy}v_{xw} \otimes u_{yy'}u_{ww'} \otimes v_{x'y'}v_{x'w'} = \sum_{y, y'} v_{xy} \otimes u_{yy'} \otimes v_{x'y'} = \hat{v}_{xx'},$$

since $v_{xy}v_{xw} = 0$ unless $w = y$ and $v_{x'y'}v_{x'w'} = 0$ unless $w' = y'$. We also have that

$$\sum_{x' \in V(X)} \hat{v}_{xx'} = \sum_{x' \in V(X), y, y' \in V(Y)} v_{xy} \otimes u_{yy'} \otimes v_{x'y'}$$

$$= \sum_{y, y' \in V(Y)} v_{xw} \otimes u_{yy'} \otimes \left(\sum_{x'} v_{x'w} \right)$$

$$= \sum_{y \in V(Y)} v_{xy} \otimes \left(\sum_{y'} u_{yy'} \right) \otimes 1$$

$$= \sum_{y \in V(Y)} v_{xy} \otimes 1 = 1,$$

and similarly $\sum_x \hat{v}_{xx'} = 1$. Thus $\hat{V}$ is a magic unitary.

Now suppose that $\mathrm{rel}(x', x'') \neq \mathrm{rel}(x^*, x^{**})$. Then

$$\hat{v}_{x'x^*}\hat{v}_{x''x^{**}} = \sum_{y', y^*, y'', y^{**} \in V(Y)} v_{x'y'}v_{x''y''} \otimes u_{y'y^*}u_{y''y^{**}} \otimes v_{x^*y^*}v_{x^{**}y^{**}} = 0,$$

since any nonzero term in the sum would require $\mathrm{rel}(x', x'') = \mathrm{rel}(y', y'') = \mathrm{rel}(y^*, y^{**}) = \mathrm{rel}(x^*, x^{**})$, a contradiction. Therefore, $A\hat{V} = \hat{V}A$ as desired.

Now suppose that $(x_1, x_1'), (x_2, x_2') \in V(X) \times V(X)$ and that there exist $(y_1, y_1'), (y_2, y_2')$ in the *same* quantum orbital of Y such that both $(x_1, x_1') \sim_v (y_1, y_1')$ and $(x_2, x_2') \sim_v (y_2, y_2')$. In other words, we have that $v_{x_1y_1}v_{x_1'y_1'} \neq 0$, $v_{x_2y_2}v_{x_2'y_2'} \neq 0$, and $u_{y_1y_2}u_{y_1'y_2'} \neq 0$. Then

$$\hat{v}_{x_1x_2}\hat{v}_{x_1'x_2'} = \sum_{y, y', w, w' \in V(Y)} v_{x_1y}v_{x_1'w} \otimes u_{yy'}u_{ww'} \otimes v_{x_2y'}v_{x_2'w'},$$

and thus

$$\left(v_{x_1y_1} \otimes 1 \otimes v_{x_2y_2} \right) \left(\hat{v}_{x_1x_2}\hat{v}_{x_1'x_2'} \right) \left(v_{x_1'y_1'} \otimes 1 \otimes v_{x_2'y_2'} \right) = v_{x_1y_1}v_{x_1'y_1'} \otimes u_{y_1y_2}u_{y_1'y_2'} \otimes v_{x_2y_2}v_{x_2'y_2'} \neq 0.$$

Therefore we have that $\hat{v}_{x_1x_2}\hat{v}_{x_1'x_2'} \neq 0$ and so (x_1, x_1') and (x_2, x_2') must be in the same quantum orbital of X.

So we have shown that if we fix a quantum orbital, say R_i', of Y, then the elements of R_i' can be adjacent in W only to elements of R_j for some fixed j. It can similarly be shown that the same holds with X and Y swapped. Moreover, every vertex of Y has at least one neighbor since $\sum_{y_1, y_2} v_{xy_1}v_{x'y_2} = \sum_{x_1, x_2} v_{x_1y}v_{x_2y'} = 1$ for all $x, x' \in V(X)$ and $y, y' \in V(Y)$. Thus there is a bijection $f : \mathcal{I} \to \mathcal{I}'$ such that the elements of R_i are adjacent in W only to elements of $R_{f(i)}'$, i.e., $v_{xy}v_{x'y'} = 0$ unless $(x, x') \in R_i$ and $(y, y') \in R_{f(i)}'$ for some $i \in \mathcal{I}$.

Now we must show that the function f has the property that $p_{ij}^k = q_{f(i)f(j)}^{f(k)}$ for all $i, j, k \in \mathcal{I}$. Suppose that $(x, x') \in R_k$ for some $k \in \mathcal{I}$, and let $i, j \in \mathcal{I}$. Define $S = \{w \in V(X) : (x, w) \in R_i, (w, x') \in R_j\}$, and note that $|S| = p_{ij}^k$. There must exist $y, y' \in V(Y)$ such that $v_{xy}v_{x'y'} \neq 0$ and furthermore we must have that $(y, y') \in R_{f(k)}'$. Define $S' = \{z \in V(Y) : (y, z) \in R_{f(i)}', (z, y') \in$

23

$R'_{f(j)}\}$ and note that $|S'| = q'^{f(k)}_{f(i)f(j)}$. We see that

$$p^k_{ij} v_{xy} v_{x'y'} = v_{xy} \left(\sum_{w \in S} 1 \right) v_{x'y'}$$

$$= v_{xy} \left(\sum_{w \in S, z \in V(Y)} v_{wz} \right) v_{x'y'}$$

$$= v_{xy} \left(\sum_{w \in S, z \in S'} v_{wz} \right) v_{x'y'} \quad \left(\text{here we used } z \notin S' \Rightarrow v_{xy} v_{wz} = 0 \text{ or } v_{wz} v_{x'y'} = 0 \right)$$

$$= v_{xy} \left(\sum_{w \in V(X), z \in S'} v_{wz} \right) v_{x'y'}$$

$$= q'^{f(k)}_{f(i)f(j)} v_{xy} v_{x'y'}.$$

Since $v_{xy} v_{x'y'} \neq 0$ by assumption, we have that $p^k_{ij} = q'^{f(k)}_{f(i)f(j)}$ as desired.

Let A^i and B^i be the characteristic matrices of the relations R_i and R'_i respectively. Letting Φ be linear extension to span$\{A^i : i \in \mathcal{I}\}$ of the map taking A^i to $B^{f(i)}$ gives the isomorphism of the coherent algebras corresponding to $\mathcal{R}$ and $\mathcal{R}'$. The fact that $\Phi(A) = B$ is immediate from the fact that $v_{xy} v_{x'y'} = 0$ when rel$(x, x') \neq$ rel(y, y') and thus f maps indices corresponding to edges of X to indices corresponding to edges of Y and vice versa. $\square$

As with the classical case, we do not expect that the converse of the above theorem holds. In fact, following the initial submission of this work, it was shown in [11] and [22] that in order to go in the other direction one must assume an isomorphism of all *intertwiner spaces* of the graphs X and Y, whereas the quantum orbital algebra is only the space of $(1,1)$-intertwiners. With this additional assumption one obtains an equivalence with quantum isomorphism. Moreover, one can use the work of [22] to show that the Paley and Peisert graphs on 49 vertices are not quantum isomorphic since they contain a different number of complete subgraphs of order four. However, there is an isomorphism of the orbital algebras of these graphs mapping the adjacency matrix of one to the other, and moreover the orbital algebras of these graphs are equal to their coherent algebras and thus to their quantum orbital algebras. Thus these two graphs form an explicit counterexample to the converse of Theorem 4.6.

The above theorem gives us a necessary condition for two graphs to be quantum isomorphic. However, as with Theorem 3.10, it may be difficult or impossible to make use of this since we may not be able to compute the quantum orbitals of a given graph. But as we did before, we can fall back on the coherent algebras of the graphs to find a more useable necessary condition.

Corollary 4.7. *Suppose that X and Y are quantum isomorphic graphs with adjacency matrices A and B. Then there exists an isomorphism Φ of their coherent algebras such that $\Phi(A) = B$.*

Proof. Let Φ be the isomorphism of the quantum coherent algebras of X and Y satisfying $\Phi(A) = B$ guaranteed by Theorem 4.6. It is easy to see that the restriction $\hat{\Phi}$ of Φ to the coherent algebra of X has as its image a coherent algebra. Moreover, since $\Phi(A) = B$, we have that this image must contain the coherent algebra of Y. If the image of $\hat{\Phi}$ is strictly larger than the coherent algebra

24

of Y, then the image of the restriction of Φ^{-1} to the coherent algebra of Y would necessarily be strictly smaller than the coherent algebra of X. However, this is a contradiction since this image must contain the coherent algebra of X by the same reasoning as with the image of $\hat{\Phi}$. Therefore, $\hat{\Phi}$ is an isomorphism of the coherent algebras of X and Y such that $\hat{\Phi}(A) = B$. $\qquad\square$

As mentioned in the introduction, the existence of an isomorphism Φ of the coherent algebras of X and Y which maps A to B is a previously studied relation known as graph *equivalence* [9], and the map Φ is said to be an equivalence of X and Y. It is also known that two graphs are equivalent if and only if they cannot be distinguished by the (2-dimensional) Weisfeiler-Leman algorithm. Since this algorithm runs in polynomial time, this provides us with an efficiently testable necessary condition for quantum isomorphism.

Graphs X and Y being equivalent implies further necessary conditions. For instance, it is known that such graphs must be cospectral, not just with respect to their adjacency matrices, but with respect to several other matrices often associated to graphs such as the Laplacian, signless Laplacian, normalized Laplacian, etc. In fact, if Φ is an equivalence of X and Y, then for any Hermitian matrix M in the coherent algebra of X, the matrix $\Phi(M)$ will be cospectral to M. Equivalent graphs must also have the same diameter and radius, and share many other structural properties [18]. Also, an equivalence of graphs X and Y maps the adjacency matrix of the d-distance graph of X to that of Y, and this further implies that these distance graphs are equivalent. Similarly, quantum isomorphic graphs have quantum isomorphic d-distance graphs. This last fact follows from similar techniques as those presented here, but we do not give a full proof.

Recall that the relation of graph equivalence has been shown to be equivalent *doubly nonnegative isomorphism*, a semidefinite relaxation of quantum tensor/commuting isomorphism defined in [23]. The above corollary shows that this is also a relaxation of quantum isomorphism. They also show in [23] that doubly nonnegative isomorphism is not equivalent to quantum tensor/commuting isomorphism. We remark here that the same proof shows that it is not equivalent to quantum isomorphism as defined here.

We note here that the notion of quantum isomorphism can be used to find graphs that are quantum vertex transitive but not vertex transitive. First, one should observe that there exist graphs X, Y, one of which is vertex transitive, that are quantum isomorphic but not isomorphic. This will be proved later in this section. Granted this, one can take their disjoint union, which will be quantum vertex transitive but not vertex transitive.

4.4   Linear Binary Constraint Systems

A linear binary constraint system (LBCS) is simply a system of linear equations (constraints) over $\mathbb{F}_2$. More formally, an LBCS $\mathcal{F}$ consists of a family of binary variables $x_1, \ldots, x_n$ and constraints $C_1, \ldots, C_m$, where each C_ℓ takes the form $\sum_{x_i \in S_\ell} x_i = b_\ell$ for some $S_\ell \subseteq \{x_1, \ldots, x_n\}$ and $b_\ell \in \mathbb{F}_2$. An LBCS is said to be satisfiable if there is an assignment of values from $\mathbb{F}_2$ to the variable x_i such that every constraint C_ℓ is simultaneously satisfied.

$$
\begin{array}{lll}
& x_1 + x_2 + x_3 = 0 & \qquad x_1 + x_4 + x_7 = 0 \\
(1) & x_4 + x_5 + x_6 = 0 & \qquad x_2 + x_5 + x_8 = 0 \\
& x_7 + x_8 + x_9 = 0 & \qquad x_3 + x_6 + x_9 = 1
\end{array}
$$

where we stress again that the equations are over $\mathbb{F}_2$. It is not too difficult to see that the LBCS above is not satisfiable. This is because every variable appears in exactly two constraints and thus adding up all of them we obtain $0 = 1$.

There is an important alternative formulation of LBCS's that we will briefly mention. One can replace each constraint $\sum_{x_i \in S_\ell} x_i = b_\ell$ with $\prod_{x_i \in S_\ell} x_i = (-1)^{b_\ell}$, and allow the variables to take values in $\{-1, 1\}$ to obtain an equivalent system of equations which we will call the multiplicative form of the LBCS. This form is used in the work of Cleve and Mittal [14], where they construct a nonlocal game based on LBCS's (actually they do it even for nonlinear binary constraint systems). In the game, Alice is asked a constraint and Bob a variable in her constraint. In order to win, Alice must respond with an assignment of values to all of the variables in her constraint such that it is satisfied, and Bob must assign his variable a value so that it agrees with Alice. Cleve and Mittal show that this game can be won perfectly with a quantum strategy in the tensor product framework if and only if there exists a finite dimensional operator solution to the (multiplicative form of the) LBCS. An *operator solution* is an assignment of selfadjoint operators X_i on some Hilbert space $\mathcal{H}$ to the variables x_i such that $X_i^2 = I$ for all $i \in [n]$, and such that all of the operators appearing in a constraint commute with each other (this removes any ambiguity in the order of the multiplication in the constraint). Furthermore, on the right-hand sides the $(-1)^{b_\ell}$ is replaced with $(-1)^{b_\ell} I$. Such an operator solution is *finite-dimensional* if $\mathcal{H}$ is finite-dimensional. The nonlocal game corresponding to the LBCS in (1) is the well known Mermin-Peres magic square game [24], which can be won perfectly with a quantum strategy, and thus such a finite-dimensional operator solution does in fact exist.

The results of [14] were extended to the quantum commuting framework in [13]. Specifically, they showed that the game corresponding to an LBCS has a perfect quantum strategy in the commuting framework if and only if the LBCS has a possibly infinite dimensional operator solution.

In [2], the authors introduce a construction that takes any LBCS $\mathcal{F}$ and produces a graph $X(\mathcal{F})$. They show that, if $\mathcal{F}_0$ is the LBCS obtained from $\mathcal{F}$ by changing the right-hand side of every constraint in $\mathcal{F}$ to 0 (known as the *homogeneous* version of $\mathcal{F}$), then the graphs $X(\mathcal{F})$ and $X(\mathcal{F}_0)$ are quantum commuting isomorphic if and only if $\mathcal{F}$ has an operator solution, and quantum tensor isomorphic if and only if $\mathcal{F}$ has a finite-dimensional operator solution. Moreover, $X(\mathcal{F})$ and $X(\mathcal{F}_0)$ are isomorphic if and only if $\mathcal{F}$ is satisfiable. This allowed them to construct non-isomorphic graphs which are nevertheless quantum tensor/commuting isomorphic. This is (part of) the construction we will use to find quantum vertex transitive graphs which are not vertex transitive, thus we now give a description of this construction.

Let $\mathcal{F}$ be an LBCS with constraints C_ℓ given by $\sum_{x_i \in S_\ell} x_i = b_\ell$ for $\ell \in [m]$. Then the graph $X(\mathcal{F})$ has as its vertices pairs (ℓ, f) where $\ell \in [m]$ and $f : S_\ell \to \mathbb{F}_2$ is an assignment of values to the variables in C_ℓ such that it is satisfied. There is an edge between two vertices (ℓ, f) and (k, f') if they are *inconsistent*, i.e., if there exists $x_i \in S_\ell \cap S_k$ such that $f(x_i) \neq f'(x_i)$. Note that this implies that the vertices of the form (ℓ, f) for fixed $\ell \in [m]$ form a clique in $X(\mathcal{F})$.

Letting $\mathcal{F}$ be the LBCS in (1), one obtains the two graphs from figures 1 and 2, which were first considered in [2], and are quantum tensor isomorphic but not isomorphic. As was mentioned in [2], both of these graphs are vertex transitive, and even Cayley graphs. Moreover, if one removes the edges among the cliques corresponding to each constraint, the graphs remain quantum isomorphic but not isomorphic, and also become arc transitive (the automorphism groups act transitively on ordered pairs of adjacent vertices). In the next section we will introduce a construction of Arkhipov [1] which takes a connected non-planar graph and produces a LBCS with a (finite

26

dimensional) operator solution but no classical solution. This construction is the other half of our construction of quantum vertex transitive graphs that are not vertex transitive.
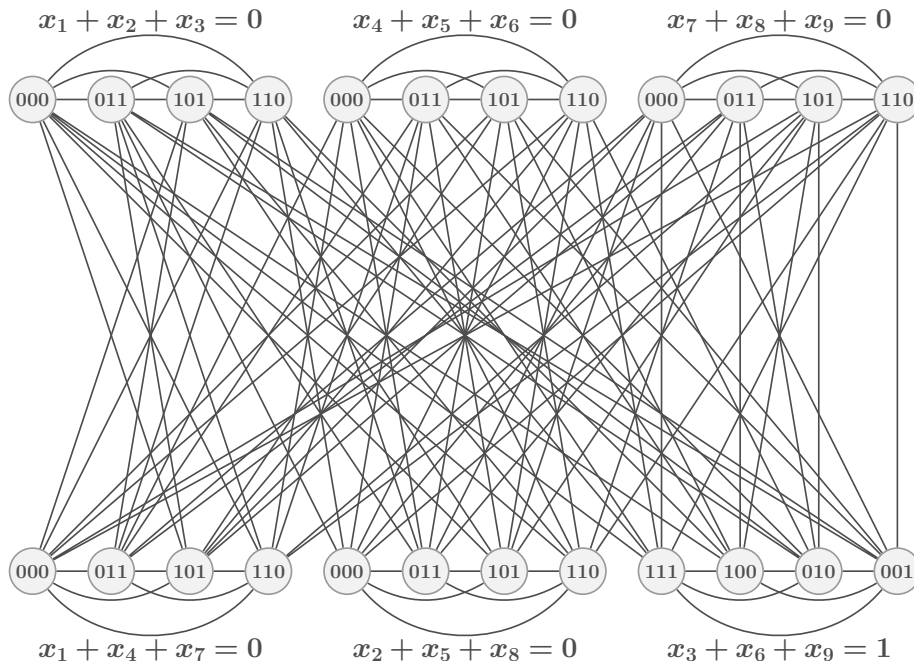

Figure 1: $X(\mathcal{F})$ for the Mermin magic square game (1).

4.5 The construction of Arkhipov

In [1], Arkhipov finds a correspondence between graphs and LBCS's in which every variable appears in exactly two equations. In the case of connected graphs, he shows that the corresponding LBCS is never satisfiable, but has an operator solution if and only if the graph is non-planar, in which case the operator solution is in finite dimension (even dimension at most eight). The construction is as follows: Let Z be a connected graph with vertex set $[m]$ and label the edges $1, \ldots, n := |E(X)|$. Pick a vertex $\ell^* \in [m]$. Create an LBCS $\mathcal{F}$ which will have a constraint C_ℓ for each $\ell \in [m]$ and variable x_i for each edge $i \in [n]$. Let $S_\ell = \{x_i : \text{edge } i \text{ is incident to vertex } \ell\}$, and define C_ℓ to be the constraint $\sum_{x_i \in S_\ell} x_i = 0$ for all $\ell \neq \ell^*$, and define C_{ℓ^*} to be $\sum_{x_i \in S_{\ell^*}} x_i = 1$.

We remark that though the LBCS constructed depends on the choice of ℓ^*, the satisfiability (classical or quantum) does not. In fact Arkhipov showed that the satisfiability only depends on the parity of the number of constraints whose right-hand side is 1. We will mainly be interested in the case where the graph Z used to construct the LBCS is vertex transitive, so even the LBCS will not depend on the choice of ℓ^* (up to relabelling).

The two prototypical non-planar graphs are the complete graph K_5 and complete bipartite graph $K_{3,3}$. For $Z = K_{3,3}$, the corresponding LBCS is the Mermin-Peres magic square one from (1). For $Z = K_5$, the LBCS corresponds to the related magic pentagram game.

To construct quantum vertex transitive graphs which are not vertex transitive, we will concatenate Arkhipov's construction of an LBCS with the reduction from [2] of an LBCS to graph
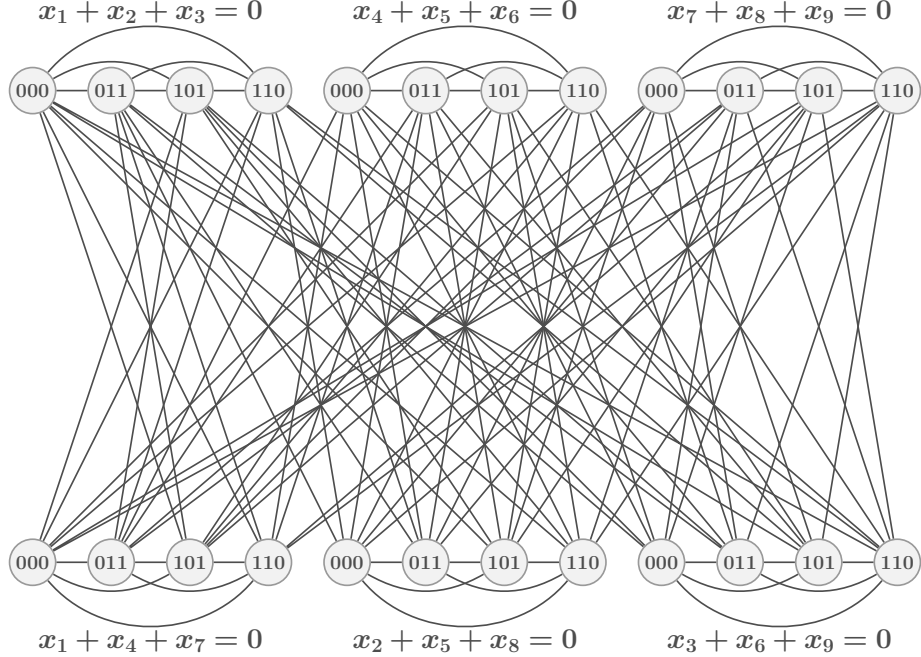
Figure 2: $X(\mathcal{F}_0)$ for the Mermin magic square game (1).

isomorphism. It is thus helpful to give a direct description of the resulting two graphs based on the input graph to Arkhipov's construction.

Definition 4.8. *Given a connected graph Z with marked vertex ℓ^*, we define two graphs $X(Z, \ell^*)$ and $X_0(Z)$ as follows. The vertices of $X(Z, \ell^*)$ are ordered pairs (ℓ, S) where $\ell \in V(Z)$ and S is a subset of edges incident to ℓ which has even parity if $\ell \neq \ell^*$ and odd parity otherwise. Two vertices (ℓ, S) and (k, T) are adjacent if ℓ and k are adjacent and the edge ℓk is in exactly one of S and T. The graph $X_0(Z)$ is defined in the same way except that the subset S must have even parity for all vertices (ℓ, S) of $X_0(Z)$ (thus it does not depend on ℓ^*). In cases where the choice of ℓ^* is not of particular importance, such as when Z is vertex transitive, we will sometimes simply write $X(Z)$.*

The following is merely the concatenation of results from [1] and [2]:

Theorem 4.9. *Let Z be a connected non-planar graph. Then the graphs $X_0(Z)$ and $X(Z, \ell^*)$ are quantum tensor isomorphic but not isomorphic for any choice of $\ell^* \in V(Z)$.*

4.6 Vertex transitivity of $X_0(Z)$

In this section we will show that if Z is vertex transitive, then $X_0(Z)$ is also vertex transitive. The first lemma shows that the automorphisms of Z can be used to construct certain automorphisms of $X_0(Z)$. To state this lemma as simply as possible, we will use the convention that if $e = \ell k$ is an edge of Z and σ an automorphism of Z, then $\sigma(e)$ is defined as the edge $\sigma(\ell)\sigma(k)$. Moreover, if S is a subset of edges, then $\sigma(S) := \{\sigma(e) : e \in S\}$.

28

Lemma 4.10. *Let Z be a connected graph. If $\sigma \in \mathrm{Aut}(Z)$, then the map $(\ell, S) \mapsto (\sigma(\ell), \sigma(S))$ is an automorphism of $X_0(Z)$.*

Proof. Let us call the map described in the lemma statement $\hat{\sigma}$. First, we must show that this maps vertices of $X_0(Z)$ to vertices of $X_0(Z)$. However, this is clear since if e is an edge incident to ℓ, then $e = \ell k$ for some $k \in V(Z)$ and then $\sigma(e) = \sigma(\ell)\sigma(k)$ is incident to $\sigma(\ell)$. Thus $\sigma(S)$ is a subset of edges incident to $\sigma(\ell)$ whenever S was a subset of edges incident to ℓ. Moreover, σ is a bijection on the vertices as well as the edges, and thus $|\sigma(S)| = |S|$. So $\sigma(S)$ has the same parity as S. This shows that the map $\hat{\sigma}$ does in fact map vertices of $X_0(Z)$ to vertices of $X_0(Z)$. Moreover, this map is a bijection, which is straightforward to see.

Next we must show that it preserves the adjacency of vertices in $X_0(Z)$. For this, suppose that (ℓ, S) and (k, T) are adjacent. Then $e = \ell k$ is an edge of Z and without loss of generality we have that $e \in S \setminus T$. From here we see that $\sigma(e) = \sigma(\ell)\sigma(k)$ is an edge of Z and that $\sigma(e) \in \sigma(S) \setminus \sigma(T)$ since σ is a bijection on the edges of Z. Therefore, $(\sigma(\ell), \sigma(S))$ is adjacent to $(\sigma(k), \sigma(T))$ in $X_0(Z)$. Since $\hat{\sigma}$ is a bijection that preserves adjacency, it also preserves non-adjacency and is therefore a bijection. $\square$

The above lemma shows that if there is an automorphism of Z mapping ℓ to k, then there is an automorphism of $X_0(Z)$ which maps the subset of vertices with first coordinate ℓ to the subset of vertices with first coordinate k. The next lemma shows that we can use the even subgraphs of Z to construct some automorphisms of $X_0(Z)$ which fix the first coordinate. An *even subgraph* is a subgraph in which every vertex has even degree. We use the notation $S \triangle T$ to denote the symmetric difference of sets S and T. We will also use $E(\ell)$ to denote the set of edges incident to the vertex ℓ.

Lemma 4.11. *Let Z be a connected graph and F the edge set of some even subgraph of Z. Then the map $(\ell, S) \mapsto (\ell, S \triangle (E(\ell) \cap F))$ is an automorphism of $X_0(Z)$.*

Proof. Let f denote the map describe in the lemma statement. The idea here is the even subgraphs of Z correspond exactly to the solutions to the homogeneous version of the LBCS constructed from Z via Arkhipov's method. The sum of two solutions to a homogeneous LBCS is a solution, and this addition corresponds to symmetric difference in subset language.

First we show that f is indeed a map from the vertices of $X_0(Z)$ to the vertices of $X_0(Z)$. Since F is the edge set of an even subgraph of Z, we have that $E(\ell) \cap F$ has even parity for all $\ell \in V(Z)$. Therefore, if S is an even subset of $E(\ell)$, then $S \triangle (E(\ell) \cap F)$ must have even parity since the parity of the symmetric difference is the sum of the parities. Thus f is a map from $V(X_0(Z))$ to itself, and then it is easy to see that it must be a bijection, since taking symmetric difference with a fixed set is a bijection on subsets. In fact, f is a bijection on the vertices with fixed first coordinate.

Next we must show that f preserves adjacency. For this suppose that (ℓ, S) and (k, T) are adjacent vertices of $X_0(Z)$. As in the proof of the previous lemma we have that $e = \ell k$ is an edge of Z and without loss of generality we have that $e \in S \setminus T$. Note that $e \in E(\ell)$ and $e \in E(k)$. If $e \notin F$, then $e \notin E(\ell) \cap F$ and thus $e \in S \triangle (E(\ell) \cap F)$ but $e \notin T \triangle (E(k) \cap F)$. If $e \in F$, then $e \in E(\ell) \cap F$ and $e \in E(k) \cap F$, thus $e \notin S \triangle (E(\ell) \cap F)$ but $e \in T \triangle (E(k) \cap F)$. In either case we see that $(\ell, S \triangle (E(\ell) \cap F))$ is adjacent to $(k, T \triangle (E(k) \cap F))$, and so f preserves adjacency and we are done. $\square$

In the case where Z has no cut-vertex, we can use the above to show that any vertex (ℓ, S) of $X_0(Z)$ can be mapped to a vertex of the form (ℓ, T) by an automorphism of $X_0(Z)$. A cut-vertex of a connected graph is a vertex whose removal disconnects the graph.

Lemma 4.12. *Let Z be a connected graph with no cut-vertex. If (ℓ, S) and (ℓ, T) are two vertices of $X_0(Z)$, then there is an automorphism σ of $X_0(Z)$ such that $\sigma(\ell, S) = (\ell, T)$.*

Proof. First we will show that the lemma holds when $|S \triangle T| = 2$. One can then compose such automorphisms to prove the result for any $|S \triangle T|$.

Suppose that $S \triangle T = \{e, f\}$ for edges e, f incident to ℓ, and let $j, k \in V(Z)$ be such that $e = \ell j$ and $f = \ell k$. Consider the graph Z' obtained from Z by removing vertex ℓ. Since ℓ is not a cut-vertex by assumption, the graph Z' is connected, and therefore there exists a path P from j to k in Z'. This path does not contain any edge incident to ℓ since these edges are not in Z'. In Z, the path P along with edges e, f and vertex ℓ form a cycle C. Let F be the edge set of this cycle and note that $E(\ell) \cap F = \{e, f\}$. Since C is a cycle, it is an even subgraph of Z. Therefore, by Lemma 4.11, the map $(k, R) \mapsto (k, R \triangle (E(k) \cap F))$ is an automorphism of Z. It is easy to see that $S \triangle (E(\ell) \cap F) = S \triangle \{e, f\} = T$, and therefore this automorphism maps (ℓ, S) to (ℓ, T) as desired.

For $|S \triangle T| > 2$, we will still have that this cardinality is even (since S and T are even), and so we can partition $S \triangle T$ into pairs $\{e_i, f_i\}$ for $i = 1, \ldots, |S \triangle T|/2$. Defining $S_0 = S$ and letting $S_i = S_{i-1} \triangle \{e_i, f_i\}$, it is easy to see that $|S_{i-1} \triangle S_i| = |\{e_i, f_i\}| = 2$ for all i, and $S_{|S \triangle T|/2} = T$. Therefore we can compose automorphisms mapping (ℓ, S_{i-1}) to (ℓ, S_i) guaranteed by the above argument to obtain an automorphism mapping (ℓ, S) to (ℓ, T). $\qquad\square$

We actually only needed to assume that ℓ was not a cut-vertex in the above lemma, but the statement as is suffices for our results.

So Lemma 4.10 provides us with automorphisms of $X_0(Z)$ that change the first coordinate (and possibly the second coordinate), and Lemma 4.11 provides us with automorphisms that fix the first coordinate but change the second coordinate. Combining these we can prove the following:

Theorem 4.13. *Let Z be a connected vertex transitive graph. Then $X_0(Z)$ is vertex transitive.*

Proof. We must prove that Z has no cut-vertex and then it will follow easily from the above lemmas. Since Z is connected, it has a spanning tree $\mathcal{T}$. Consider a leaf (vertex of degree 1) ℓ of $\mathcal{T}$, which must exist. Removing ℓ from $\mathcal{T}$ creates a smaller tree $\mathcal{T}'$ which must be connected since it is a tree. Since $\mathcal{T}'$ is a subgraph of the graph Z' obtained by removing ℓ from Z, we have that Z' must be connected as well. Therefore, ℓ was not a cut-vertex. However, Z is vertex transitive, so if ℓ is not a cut-vertex, then no vertex of Z is a cut-vertex.

Now consider vertices (ℓ, S) and (k, T) of $X_0(Z)$. Since Z is vertex transitive, there exists an automorphism $\sigma \in \mathrm{Aut}(Z)$ such that $\sigma(\ell) = k$. By Lemma 4.10, there is an automorphism σ_1 of $X_0(Z)$ such that $\sigma_1(\ell, S) = (k, T')$ where $T' = \sigma(S)$. Now, since Z has no cut-vertex, Lemma 4.12 says that there is an automorphism σ_2 of $X_0(Z)$ such that $\sigma_2(k, T') = (k, T)$. Therefore, the composition $\sigma_2 \circ \sigma_1$ is an automorphism of $X_0(Z)$ that maps (ℓ, S) to (k, T). Since these vertices were arbitrary, this implies that $X_0(Z)$ is vertex transitive as desired. $\qquad\square$

Corollary 4.14. *If Z is a connected vertex transitive non-planar graph, then $X(Z, \ell^*)$ is quantum vertex transitive for any choice of ℓ^*.*

Proof. Under these conditions, the graphs $X_0(Z)$ and $X(Z)$ are quantum isomorphic by Theorem 4.9. This implies that they have the same number of quantum orbits. However, $X_0(Z)$ is vertex transitive by Theorem 4.13 and so it has only one orbit and therefore only one quantum orbit. Thus $X(Z)$ has one quantum orbit, i.e., is quantum vertex transitive. $\qquad\square$

It would be interesting to find a connected non-planar graph Z such that exactly one of $X_0(Z)$ and $X(Z)$ was vertex transitive.

4.7   Quantum vertex transitivity of the disjoint union

In this section we aim to show that if Z is a connect non-planar vertex transitive graph, then the disjoint union of $X_0(Z)$ and $X(Z)$ is quantum vertex transitive but not vertex transitive. To begin we need the following lemma:

Lemma 4.15. *Let X and Y be quantum isomorphic graphs which are both quantum vertex transitive. Then the disjoint union of X and Y is quantum vertex transitive.*

Proof. We denote by A_X and A_Y the adjacency matrices of X and Y, respectively. Let Z denote the disjoint union of X and Y, and let $U = (u_{xx'})$ and $V = (v_{yy'})$ be the magic unitaries whose entries are the canonical generators of $\mathcal{A}(X)$ and $\mathcal{A}(Y)$ respectively. Define $W = (w_{zz'}) = U \oplus V$ as

$$
w_{zz'} = \begin{cases} u_{zz'} \otimes 1_{\mathcal{A}(Y)}, & \text{if } z, z' \in V(X) \\ 1_{\mathcal{A}(X)} \otimes v_{zz'}, & \text{if } z, z' \in V(Y) \\ 0, & \text{otherwise.} \end{cases}
$$

It is easy to see that this is a magic unitary. Now we show that it commutes with the adjacency matrix of the disjoint union of X and Y. The adjacency matrix of this disjoint union is $A := A_X \oplus A_Y$, and thus

$$
AW = (A_X \oplus A_Y)(U \oplus V) = A_X U \oplus A_Y V = U A_X \oplus V A_Y = (U \oplus V)(A_X \oplus A_Y) = WA,
$$

where we have used the fact that U and V commute with A_X and A_Y respectively. Since W commutes with A, if $w_{zz'} \neq 0$, then $z \sim_1 z'$, i.e., z and z' are in the same quantum orbit of Z. By assumption we have that both X and Y are quantum vertex transitive, i.e., have one quantum orbit. Therefore, $u_{xx'} \neq 0$ for all $x, x' \in V(X)$ and $v_{yy'} \neq 0$ for all $y, y' \in V(Y)$. Therefore $w_{xx'} \neq 0$ for all $x, x' \in V(X)$ and $w_{yy'} \neq 0$ for all $y, y' \in V(Y)$, i.e., every vertex of X is in the same quantum orbit of Z and every vertex of Y is in the same quantum orbit of Z.

It now only remains to show that $x \sim_1 y$ for some $x \in V(X)$ and $y \in V(Y)$. Since we assumed that X and Y are quantum isomorphic, there exists a unital C*-algebra $\mathcal{A}$ and magic unitary $\hat{W} = (\hat{w}_{xy})$ for $x \in V(X)$, $y \in V(Y)$ such that $A_X \hat{W} = \hat{W} A_Y$. We define

$$
\tilde{W} = \begin{pmatrix} 0 & \hat{W} \\ \hat{W}^* & 0 \end{pmatrix}.
$$

Then,

$$
A\tilde{W} = \begin{pmatrix} A_X & 0 \\ 0 & A_Y \end{pmatrix} \begin{pmatrix} 0 & \hat{W} \\ \hat{W}^* & 0 \end{pmatrix} = \begin{pmatrix} 0 & A_X \hat{W} \\ A_Y \hat{W}^* & 0 \end{pmatrix} = \begin{pmatrix} 0 & \hat{W} A_Y \\ \hat{W}^* A_X & 0 \end{pmatrix},
$$

as $A_Y \hat{W}^* = (\hat{W} A_Y)^* = (A_X \hat{W})^* = \hat{W}^* A_X$. Further,

$$\tilde{W} A = \begin{pmatrix} 0 & \hat{W} \\ \hat{W}^* & 0 \end{pmatrix} \begin{pmatrix} A_X & 0 \\ 0 & A_Y \end{pmatrix} = \begin{pmatrix} 0 & \hat{W} A_Y \\ \hat{W}^* A_X & 0 \end{pmatrix}.$$

Therefore, $\tilde{W}$ is a magic unitary which commutes with A. Moreover, by its definition, for any vertex $x \in V(X)$, there must be at least one vertex $y \in V(Y)$ such that $\tilde{w}_{xy} \neq 0$. Thus these two vertices are in the same quantum orbit, and combining this with the above we see that there is only one quantum orbit of Z, i.e, it is quantum vertex transitive. □

We can now prove our main result of this section:

Theorem 4.16. *Let X and Y be quantum vertex transitive graphs which are quantum isomorphic but not isomorphic. Then the disjoint union of X and Y are quantum vertex transitive but not vertex transitive.*

Proof. By Lemma 4.15, we have that the disjoint union of X and Y is quantum vertex transitive. So it is only left to show that it is not vertex transitive. It is easy to see that a graph is vertex transitive if and only if all of its connected components are vertex transitive and isomorphic to each other (since automorphism must map connected components to connected components). Thus, if the disjoint union of X and Y is vertex transitive, then X and Y must have both been the disjoint union of (a possibly different) number of copies of a common connected vertex transitive graph Z. However, since we assumed that X and Y were not isomorphic, this implies that the number of copies of Z used was different for X and Y. This implies that X and Y have a different number of vertices, and therefore cannot be quantum isomorphic, a contradiction to our assumption. Therefore the disjoint union of X and Y cannot be vertex transitive and we are done. □

As a corollary we obtain the following which allows us to construct an infinite number of graphs which are quantum vertex transitive but not vertex transitive.

Corollary 4.17. *Let Z be a connected, vertex transitive, non-planar graph. Then the disjoint union of $X_0(Z)$ and $X(Z)$ is quantum vertex transitive but not vertex transitive.*

The smallest possibility for Z in the above corollary is the graph K_5, but the resulting graphs $X_0(Z)$ and $X(Z)$ are actually larger (40 vertices) than those obtained from letting $Z = K_{3,3}$ which have 24 vertices and are shown in Figures 1 and 2. By Kuratowski's theorem, any other non-planar graph must contain one of $K_{3,3}$ or K_5 as a minor and so these are indeed the smallest graphs that can be obtained by this construction. As we mentioned previously, if one removes the edges contained in the cliques corresponding to the constraints of the LBCS, then the graphs in Figures 1 and 2 remain quantum isomorphic but not isomorphic, and now become arc-transitive. Therefore, their disjoint union will be quantum arc-transitive, but not arc-transitive, or even edge-transitive.

There are infinitely many connected, vertex transitive, non-planar graphs and so the above corollary does in fact give us infinitely many examples of graphs which are quantum vertex transitive but not vertex transitive. Indeed, any vertex transitive graph with degree at least six is non-planar since it is known that any planar graph has some vertex of degree less than six.

We remark that if one would prefer an example of a *connected* graph which is quantum vertex transitive but not vertex transitive, then they may simply take the complement of the examples generated by Corollary 4.17.

As we mentioned, the above corollary answers an unresolved question raised (at least implicitly) in the quantum permutation group literature (see e.g. [4, 5]). Perhaps the examples provided by this corollary will have some new interesting quantum permutation groups. Unfortunately it seems that the currently known techniques to compute quantum automorphism groups are not sufficient to handle graphs of this size. Hopefully this will change with the increased interest in this area from members of the quantum information and graph theory community, which we hope this work encourages.

5 Discussion

Here we discuss some possible further directions and open questions.

No quantum symmetry. In the study of quantum automorphism groups of graphs, it seems an important case is when the graph has no quantum symmetry, i.e., its quantum symmetry algebra is commutative. Indeed, many of the small graphs whose quantum automorphism groups have been computed [6, 7] have this property. The most direct way to show this is to show that all of the entries u_{ij} of the magic unitary U defining the given quantum automorphism group commute. However, in the known examples a different strategy is followed. The most common technique seems to be to use the universal action.

Suppose that $\mathcal{Q}$ is a quantum permutation group on the set $[n]$ with universal action u. It was shown in [4] that the magic unitary U commutes with the projection onto a subspace K of $\mathbb{C}^n$ if and only if K is invariant for u, i.e. $u(K) \subseteq K \otimes C(\mathcal{Q})$. If $\mathcal{Q} = \mathrm{Qut}(X)$ for some graph X with adjacency matrix A, then the corresponding magic unitary U commutes with A and therefore any polynomial expression in A. This includes the projections onto the eigenspaces of A. Thus if $f_1, \ldots, f_d$ is a basis of one of these eigenspaces, then $u(f_j) = \sum_{i=1}^d f_i \otimes a_{ij}$ for some elements $a_{ij} \in C(\mathcal{Q})$. Since the image of u is dense in $\mathcal{Q}$, if all of the a_{ij} (as well as those for the other eigenspaces) commute, then $\mathcal{Q}$ is commutative and therefore X has no quantum symmetry. Our results show that one does not necessarily need to consider the eigenspaces of the adjacency matrix, but instead could use any Hermitian matrix in the coherent algebra of the graph. This will often allow for smaller eigenspaces than considering the adjacency matrix alone.

The above method has been particularly useful for *circulants*: graphs X with vertex set $\mathbb{Z}_n$ such that $i \sim j$ if $i - j \in C$ for some inverse closed subset $C \subseteq \mathbb{Z}_n \setminus \{0\}$. The reason this approach works so well for these graphs is because they always have a basis of eigenvectors that is closed under entrywise product. Specifically, if $f \in \mathbb{C}^n$ is the vector whose i^{th} entry is ω^i for a primitive n^{th} root of unity ω, then the entrywise powers f^j for $j = 0, \ldots, n-1$ are an orthonormal basis of $\mathbb{C}^n$ consisting of eigenvectors of (the adjacency matrix of) X. It is known that the vectors f^j and f^{n-j} always correspond to the same eigenvalue for these graphs. It was shown in [4] that if these are the only common eigenvalues among the vectors f^j for $j = 0, \ldots, n-1$ then the graph X has no quantum symmetry (unless $n = 4$). Here again, our results could be of use. In the case of circulants, the resulting coherent algebra only contains symmetric matrices, and therefore is a *symmetric association scheme*. This means that all of its elements commute and therefore have a common eigenbasis. In fact the common eigenbasis is exactly the one described above consisting of the f^j. It is known that there will be a matrix in the coherent algebra with different eigenvalues for f^j and f^i whenever $i \notin \{j, n-j\}$ if and only if there are $\lfloor n/2 \rfloor + 1$ classes in the coherent algebra. In this case the classes are exactly the distance relations of the cycle of length n. Thus, if

the coherent configuration of a circulant has $\lfloor n/2 \rfloor + 1$ classes then the circulant has no quantum symmetry.

Unfortunately, using coherent algebras does not provide any further information for a certain class of graphs: strongly regular graphs. The coherent configurations of these graphs have only three classes: the vertices, edges, and non-edges. Thus the coherent algebra is simply the span of the identity I, the adjacency matrix A, and the adjacency matrix of the complement $\overline{A} = J - I - A$. This means that Corollary 3.13 is just a restatement of the relations defining the quantum automorphism group. It may be possible that the quantum orbitals are finer than this, but we do not know how to compute these in general. Moreover, it is possible that the classes of the coherent configuration and the (classical) orbitals of the graph coincide, and therefore so do the quantum orbitals.

Higher order orbits. In this work we defined the orbits of a quantum permutation group on points and ordered pairs of points. One could also define a relation $\sim_m$ on ordered m-tuples of points such that $(x_1, \ldots, x_m) \sim_m (y_1, \ldots, y_m)$ whenever $u_{x_1 y_1} \ldots u_{x_m y_m} = 0$, and then used this to define orbits of m-tuples for quantum permutation groups. We could have defined such a relation, but even for $m = 3$ we do not see how to show that it would be transitive (and do not believe it will be in general). It seems that things work for $m \leq 2$ because we can multiply on both the left and the right, but for $m \geq 3$ we cannot multiply "in the middle" since we do not have commutativity. But what about the equivalent definitions of orbits and orbitals given in Section 3.1 using the canonical action? Is it possible to extend this in order to define orbits on m-tuples for $m \geq 3$?

Let $U = (u_{ij})$ be a magic unitary whose entries are the canonical generators of $C(\mathcal{Q})$ from some quantum permutation group $\mathcal{Q}$. The m-th tensor power of the action u of $\mathcal{Q}$ is a linear map $u^{\otimes m} : (\mathbb{C}^n)^{\otimes m} \to (\mathbb{C}^n)^{\otimes m} \otimes C(\mathcal{Q})$ defined on the standard basis vectors as

$$u^{\otimes m}(e_{i_1} \otimes \ldots \otimes e_{i_m}) = \sum_{j_1, \ldots, j_m} (e_{j_1} \otimes \ldots \otimes e_{j_m}) \otimes u_{j_1 i_1} \ldots u_{j_m i_m}.$$

As with u and $u^{\otimes 2}$, we can consider the space of fixed points of $u^{\otimes m}$:

$$\mathrm{Hom}(1, u^{\otimes m}) = \{f \in (\mathbb{C}^n)^{\otimes m} : u^{\otimes m}(f) = f \otimes 1\}.$$

In the case of $m = 2$, we saw that $\mathrm{Hom}(1, u^{\otimes 2})$ is a selfadjoint subalgebra of $\mathbb{C}^X \otimes \mathbb{C}^X$, and the same holds for $m = 1$ since u is an action. Moreover, we could define the orbits as the parts of the partition corresponding to $\mathrm{Hom}(1, u)$, and the orbitals as the parts of the partition corresponding to $\mathrm{Hom}(1, u^{\otimes 2})$. Unfortunately, we do not know whether $\mathrm{Hom}(1, u^{\otimes m})$ is a selfadjoint subalgebra of $(\mathbb{C}^X)^{\otimes m}$. Thus we leave it as an open question how to define orbits of a quantum permutation group on m-tuples for general m.

Quantum groups vs. quantum behaviour. Let Z be the graphs consisting of a single edge plus two additional isolated vertices. In [26] it is shown (and it is not hard to see) that the quantum symmetry algebra of Z is generated by a magic unitary of the form

$$\begin{pmatrix} a & 1-a & 0 & 0 \\ 1-a & a & 0 & 0 \\ 0 & 0 & b & 1-b \\ 0 & 0 & 1-b & b \end{pmatrix}$$

where a and b are free projectors. Obviously, this is not commutative since a and b do not commute in general. Thus the graph Z has some "non-classical" automorphisms. Does this mean that we can construct a perfect quantum strategy for the (Z, Z)-isomorphism game (henceforth referred to as the Z-automorphism game) which is not classical? It depends on what exactly it means for a strategy to not be classical. For any choice of finite dimensional projectors a and b, we can construct a perfect strategy for the Z-automorphism game in which the measurements used by the players will correspond to the rows and columns of the magic unitary above, and the shared state will be the maximally entangled state. This is of course not a classical strategy since it uses quantum measurements, but this does not mean that the corresponding behaviour of the players, i.e., the correlations of their inputs and outputs in the game, cannot be explained classically.

To be more precise, any fixed strategy (classical, quantum, or otherwise) for a nonlocal game has a corresponding *correlation* or joint conditional probability distribution. This is a function p mapping tuples of Alice and Bob's inputs and outputs to $[0, 1]$, where $p(y, y'|x, x')$ is the probability that Alice and Bob reply with y and y' respectively, upon receiving x and x'. In the deterministic case, this is either 0 or 1, but access to shared randomness allows classical players to construct strategies whose correlations are any convex combination of deterministic ones. In the quantum commuting framework, the probability $p(y, y'|x, x')$ is given by the value of a tracial state s on the product of the the projector corresponding to Alice outputting y upon receiving x and the projector corresponding to Bob outputting x' upon receiving y'. In the case of the Z-automorphism game, this means that all of the correlation probabilities are determined by the value of $s(ab) \in [0, 1]$. We do not present the proof here, but we have shown that no matter what value is chosen for this, the resulting correlation can be obtained by a classical strategy. Therefore, there is no perfect quantum strategy for the Z-automorphism game which actually exhibits non-classical behaviour in this sense.

One could therefore consider the problem of which graphs not only have quantum symmetries, but such quantum symmetries that give rise to strategies for the automorphism game of the graph whose corresponding correlations can *not* be obtained via a classical strategy. Such a quantum strategy is said to exhibit *nonlocality*, since its behavior cannot be explained by a local hidden variable model. There are three different degrees of nonlocality that can be exhibited by a quantum correlation p: nonlocality, logical nonlocality, and pseudotelepathy/strong nonlocality. The first is as we defined it above: there is no classical strategy that produces p. Logical nonlocality occurs when there is no classical correlation q such that $q(y, y'|x, x') = 0$ if and only if $p(y, y'|x, x') = 0$. Strong nonlocality is defined as there being no classical correlation q such that $q(y, y'|x, x') = 0$ whenever $p(y, y'|x, x') = 0$, even allowing for q to be zero in places where p is not. For any quantum correlation p exhibiting strong nonlocality, one can construct a nonlocal game which is won perfectly by p but by no classical strategy: define the game so that the players lose on input/output tuples where p is 0. This ability to perfectly win a game which has no perfect classical strategy is what motivates the term pseudotelepathy, since it appears as if the players are telepathic.

In the case of the isomorphism game, pseudotelepathy occurs exactly when there is a pair of non-isomorphic graphs X, Y that are quantum tensor/commuting isomorphic. This means that the X-automorphism game is never a pseudotelepathy game, since every graph has the trivial automorphism. However, it is possible for an automorphism game to exhibit nonlocality. Computations by the third author and Robert Šámal show that already the complete graph on five vertices (and thus any larger number of vertices) admits quantum tensor automorphisms whose correlations are not classical. We do not know whether the complete graph on four vertices has this property.

It is also possible for an automorphism game to exhibit logical nonlocality. This happens exactly when there are pairs of vertices (x, x') and (y, y') that are in different (classical) orbitals of X, but there is a quantum correlation p which wins the automorphism game perfectly and $p(y, y'|x, x') > 0$. Since the Haar state is tracial, the correlation $p(y, y'|x, x') = h(u_{xy}u_{x'y'})$ is quantum commuting correlation which wins the X-automorphism game perfectly. Moreover, by Theorem 4.2, we have that $h(u_{xy}u_{x'y'}) \neq 0$ if and only if $u_{xy}u_{x'y'} \neq 0$ if and only if (x, x') and (y, y') are in the same orbital of $\mathrm{Qut}(X)$. Thus the correlation arising from the Haar state for $\mathrm{Qut}(X)$ exhibits logical nonlocality if and only if the orbitals and quantum orbitals of X differ. Examples of such graphs can be constructed by taking the disjoint union of any pair of non-isomorphic but quantum isomorphic graphs.

Acknowledgements

References

[1] Alex Arkhipov. Extending and characterizing quantum magic games. 2012. `arXiv:1209.3819`.

[2] Albert Atserias, Laura Mančinska, David E. Roberson, Robert Šámal, Simone Severini, and Antonios Varvitsiotis. Quantum and non-signalling graph isomorphisms. *Journal of Combinatorial Theory, Series B*, 136:289–328, 2019. `doi:10.1016/j.jctb.2018.11.002`.

[3] László Babai and Ludik Kucera. Canonical labelling of graphs in linear average time. In *Foundations of Computer Science, 1979, 20th Annual Symposium on*, pages 39–46. IEEE, 1979. `doi:10.1109/SFCS.1979.8`.

[4] 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`.

[5] Teodor Banica. Quantum automorphism groups of small metric spaces. *Pacific journal of mathematics*, 219(1):27–51, 2005. `doi:10.1016/j.jfa.2004.11.002`.

[6] Teodor Banica and Julien Bichon. Quantum automorphism groups of vertex-transitive graphs of order ≤ 11. *Journal of Algebraic Combinatorics*, 26(1):83, 2007. `doi:10.1007/s10801-006-0049-9`.

[7] Teodor Banica, Julien Bichon, and Gaëtan Chenevier. Graphs having no quantum symmetry. *Annales de l'Institut Fourier*, 57(3):955–971, 2007. `doi:10.5802/aif.2282`.

[8] Teodor Banica and Amaury Freslon. Modeling questions for quantum permutations. *Infinite Dimensional Analysis, Quantum Probability and Related Topics*, 21(02):1850009, 2018. `doi:10.1142/S0219025718500091`.

[9] Amir Rahnamai Barghi and Ilya Ponomarenko. Non-isomorphic graphs with cospectral symmetric powers. *The Electronic Journal of Combinatorics*, 16(1):R120, 2009.

[10] Julien Bichon. Quantum automorphism groups of finite graphs. *Proceedings of the American Mathematical Society*, 131(3):665–673, 2003. `doi:10.1090/S0002-9939-02-06798-9`.

[11] Michael Brannan, Alexandru Chirvasitu, Kari Eifler, Samuel Harris, Vern Paulsen, Xiaoyu Su, and Mateusz Wasilewski. Bigalois extensions and the graph isomorphism game. *Communications in Mathematical Physics*, pages 1–33, 2019. `doi:10.1007/s00220-019-03563-9`.

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

[13] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017. `doi:10.1063/1.4973422`.

[14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In *International Colloquium on Automata, Languages, and Programming*, pages 320–331. Springer, 2014. `arXiv:1209.2729`.

[15] Andrea Coladangelo and Jalex Stark. Unconditional separation of finite and infinite-dimensional quantum correlations. 2018. `arXiv:1804.05116`.

[16] Kenny De Commer. Actions of compact quantum groups. In *Topological quantum groups*, volume 111 of *Banach Center Publ.*, pages 33–100. Polish Acad. Sci. Inst. Math., Warsaw, 2017. `doi:10.4064/bc111-0-2`.

[17] Melanie Fulton. *The quantum automorphism group and undirected trees*. PhD thesis, Virginia Polytechnic Institute and State University, 2006.

[18] Martin Fürer. On the combinatorial power of the Weisfeiler-Lehman algorithm. In *International Conference on Algorithms and Complexity*, pages 260–271. Springer, 2017. `doi:10.1007/978-3-319-57586-5_22`.

[19] William Helton, Kyle P. Meyer, Vern I. Paulsen, and Matthew Satriano. Algebras, synchronous games, and chromatic numbers of graphs. *New York Journal of Math*, 25:328–361, 2019.

[20] D.G. Higman. Coherent algebras. *Linear Algebra and its Applications*, 93:209 – 239, 1987. `doi:10.1016/S0024-3795(87)90326-0`.

[21] Zhengfeng Ji. Binary constraint system games and locally commutative reductions. 2013. `arXiv:1310.3794`.

[22] Laura Mančinska and David E. Roberson. Quantum isomorphism is equivalent to equality of homomorphism counts from planar graphs. 2019. `arXiv:1910.06958`.

[23] Laura Mančinska, David E. Roberson, and Antonios Varvitsiotis. Semidefinite relaxations of quantum isomorphism. In progress, 2017.

[24] Nathaniel D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65:3373–3376, 1990. `doi:10.1103/PhysRevLett.65.3373`.

[25] Benjamin Musto, David Reutter, and Dominic Verdon. A compositional approach to quantum functions. *Journal of Mathematical Physics*, 59(8):081706, 2018. `doi:10.1063/1.5020566`.

[26] Simon Schmidt and Moritz Weber. Quantum symmetries of graph C^*-algebras. *Canadian Mathematical Bulletin*, 61(4):848–864, 2018. `doi:10.4153/CMB-2017-075-4`.

[27] Thomas Timmermann. *An invitation to quantum groups and duality: From Hopf algebras to multiplicative unitaries and beyond*. EMS Textbooks in Mathematics. European Mathematical Society, 2008. `doi:10.4171/043`.

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

[29] Boris Weisfeiler. *On construction and identification of graphs*, volume 558 of *Lecture Notes in Mathematics*. Springer-Verlag, 1976. With contributions by A. Lehman, G. M. Adelson-Velsky, V. Arlazarov, I. Faragev, A. Uskov, I. Zuev, M. Rosenfeld and B. Weisfeiler.

[30] Stanisław L. Woronowicz. Compact matrix pseudogroups. *Communications in Mathematical Physics*, 111(4):613–665, 1987. `doi:10.1007/BF01219077`.

[31] Stanisław L Woronowicz. Compact quantum groups. *Symétries quantiques (Les Houches, 1995)*, 845(884):98, 1998.