Cambridge University Press & Assessment
978-1-009-34573-6 — Compact Matrix Quantum Groups and Their Combinatorics
Amaury Freslon
Excerpt
More Information

1
Introducing Quantum Groups

The purpose of the first part of this text is to introduce objects called *compact quantum groups* and to deal in full detail with their algebraic aspects and in particular their representation theory. It turns out that many interesting examples of compact quantum groups fall into a specific subclass called *compact matrix quantum groups*. This subclass has the advantage of being more intuitive, as well as allowing for a simplified treatment of the whole theory. We will therefore restrict to it, and the connection with the more general setting of compact quantum groups will be briefly explained in Appendix C.

We believe that there is no better way of introducing a new concept than giving examples. We will therefore spend some time introducing one of the most important families of examples of compact matrix quantum groups, first defined by S. Wang in [72], called the *quantum permutation groups*.

1.1 The Graph Isomorphism Game

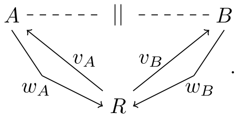
There are several ways of motivating the definition of quantum permutation groups, because these objects are related to several important notions like quantum isometry groups in the sense of non-commutative geometry (see, for instance, [22] or [7]) or quantum exchangeability in the sense of free probability (see, for instance, [50]). In this text, we will start from a recent connection, first made explicit in [53], between quantum permutation groups and quantum information theory. That connection appears through a *game* which we now describe.

As always in quantum information theory, the game is played by two players named *Alice* (denoted by A) and *Bob* (denoted by B). In this so-called *graph isomorphism game*, they cooperate to win against the *Referee* (denoted by R)

leading the game. The rules are given by two finite graphs,[1] X and Y, with vertex sets $V(X)$ and $V(Y)$ respectively having the same cardinality, which are known to A and B. At each round of the game, R sends a vertex $v_A \in V(X)$ to A and a vertex $v_B \in V(X)$ to B. Each of them answers with a vertex $w_A \in V(Y)$, $w_B \in V(Y)$ of the other graph, and they win the round if the following condition is matched.

Winning condition: 'The relation[2] between v_A and v_B is the same as the one between w_A and w_B.'[3]

The crucial point is that once the game starts, A and B **cannot communicate in any way**. The situation can be summarised by the following picture:



The question one asks is then, under which condition on the graphs X and Y can the players devise a strategy which wins whatever the given vertices are? It is not very difficult to see that the answer is the following (see Exercise 8.1 for a proof).

Proposition 1.1 *There exists a perfect classical strategy if and only if X and Y are isomorphic.*

This settles the problem in classical information theory, but in the quantum world, A and B can refine their strategy without communicating through the use of *entanglement*. This means that they can set up a quantum mechanical system and then split it into two parts, such that manipulating one part instantly modifies the other one. We will not go into the details right now, but it turns out that this gives more strategies, which are said to be *quantum*.[4] By using these

[1] The following discussion concerning graphs is only intended to motivate the introduction of quantum permutation groups, hence we do not give precise definitions. A rigorous treatment will be given in Chapter 8.

[2] Here, by 'relation' we mean either being equal, being adjacent or not being adjacent.

[3] This is not the most general version of the graph isomorphism game. We refer the reader to [2] for a more comprehensive exposition.

[4] The concept of quantum strategy turns out to be quite subtle, depending on the type of operators allowed. We here use the term in a purposely vague sense and refer the reader to the discussion at the beginning of Chapter 8 for more details.

quantum strategies, the previous proposition can be improved. Before giving a precise statement, let us fix some notations.

- Given a Hilbert space H, we denote by $\mathcal{B}(H)$ the algebra of bounded (i.e. continuous) linear maps from H to H;
- Given a graph X, we denote by A_X the adjacency matrix of A.

The following result is a combination of [2, theorem 5.8] and [53, theorem 4.4].

Theorem 1.2 (Atserias–Lupini–Mančinska–Roberson–Šamal–Severini–Varvitsiotis) *There is a perfect* quantum *strategy if and only if there exists a matrix* $P = (p_{ij})_{1\leqslant i,j\leqslant N}$ *with coefficients in* $\mathcal{B}(H)$ *for some Hilbert space* H*, such that*

- p_{ij} *is an orthogonal projection for all* $1 \leqslant i, j \leqslant N$*;*
- $\displaystyle\sum_{k=1}^{N} p_{ik} = \mathrm{Id}_H = \sum_{k=1}^{N} p_{kj}$ *for all* $1 \leqslant i, j \leqslant N$*;*
- $A_X P = P A_Y$.

The proof of this result involves several tools coming from quantum information theory, graph theory and compact quantum group theory. For those reasons, we postpone it to Chapter 8.

Remark 1.3 From the perspective of quantum physics, this definition is at least reasonable. Indeed, a family of orthogonal projections summing up to one is a particular instance of a *Positive Operator Valued Measure* (see Definition 8.1). We are therefore considering a collection of such objects with compatibility conditions coming from the graphs.

Remark 1.4 It is not straightforward to produce a pair of graphs for which there is a perfect quantum strategy but no classical one. The first example, given in [2, section 6.2], has 24 vertices and is the smallest known at the time of this writing.

An intriguing point of Theorem 1.2 is the operator-valued matrices which appear in the statement. To understand them, let us consider the case $H = \mathbf{C}$. Then, the coefficients are scalars, and since they are projections, they all equal either 0 or 1. Moreover, the sum over any row is 1, hence there is exactly one non-zero coefficient on each row. The same being true for the columns, we have a permutation matrix! We should therefore think of the operator-valued matrices as quantum versions of permutations, and this leads to the following definition.

Definition 1.5 Let H be a Hilbert space. A *quantum permutation matrix* in H is a matrix $P = (p_{ij})_{1\leqslant i,j\leqslant N}$ with coefficients in $\mathcal{B}(H)$ such that

- p_{ij} is an orthogonal projection for all $1 \leqslant i, j \leqslant N$;
- $\displaystyle\sum_{k=1}^{N} p_{ik} = \mathrm{Id}_H = \sum_{k=1}^{N} p_{kj}$ for all $1 \leqslant i, j \leqslant N$.

Moreover, with this point of view the last point of Theorem 1.2 has a nice interpretation. To explain it, let us first do a little computation.

Exercise 1.1 Let X, Y be graphs on N vertices and let $\sigma \in S_N$. Numbering the vertices from 1 to N, σ induces a bijection between the vertex sets of X and Y. Prove this is a graph isomorphism if and only if

$$A_X P_\sigma = P_\sigma A_Y.$$

Solution Denoting by $E(X)$ and $E(Y)$ the edge sets of X and Y respectively, the (i, j)-th coefficient of $A_X P_\sigma$ is

$$\begin{aligned}\sum_{k=1}^{N}(A_X)_{ik}(P_\sigma)_{kj} &= \sum_{k=1}^{N}\delta_{(i,k)\in E(X)}\delta_{\sigma(k)j}\\ &= \delta_{(i,\sigma^{-1}(j))\in E(X)},\end{aligned}$$

while the corresponding coefficient of $P_\sigma A_Y$ is

$$\begin{aligned}\sum_{k=1}^{N}(P_\sigma)_{ik}(A_X)_{kj} &= \sum_{k=1}^{N}\delta_{(k,j)\in E(Y)}\delta_{\sigma(i)k}\\ &= \delta_{(\sigma(i),j)\in E(Y)}.\end{aligned}$$

These are equal if and only if

$$(i, \sigma^{-1}(j)) \in E(X) \Leftrightarrow (\sigma(i), j) \in E(Y).$$

Setting $k = \sigma^{-1}(j)$, the condition is equivalent to

$$(i, k) \in E(X) \Leftrightarrow (\sigma(i), \sigma(k)) \in E(Y),$$

which precisely means that σ induces a graph automorphism. □

In view of this, the last point of Theorem 1.2 can be interpreted as saying that the quantum permutation respects the edges of the graphs, so that one says that the graphs are *quantum isomorphic*.

1.2 The Quantum Permutation Algebra

1.2.1 Universal Definition

The brief discussion of Section 1.1 suggests that quantum permutation matrices are interesting objects which require further study. However, their definition lacks several important features of classical permutation matrices. In particular, there is no obvious way to 'compose' quantum permutation matrices, especially if they do not act on the same Hilbert space, so that one could recover an analogue of the group structure of permutations. To overcome this problem, it is quite natural from an (operator) algebraic point of view to introduce a universal object associated to quantum permutation matrices. Note that, in order to translate the fact that the operators p_{ij} are orthogonal projections, it is convenient to use the natural involution on $\mathcal{B}(H)$ given by taking adjoints. For this purpose, we will consider $*$-*algebras*, that is to say, complex algebras $\mathcal{A}$ endowed with an anti-linear and anti-multiplicative involution $x \mapsto x^*$.

Definition 1.6 Let $\mathcal{A}_s(N)$ be the universal $*$-algebra[5] generated by N^2 elements $(p_{ij})_{1\leqslant i,j\leqslant N}$ such that

1. $p_{ij}^2 = p_{ij} = p_{ij}^*$;
2. For all $1 \leqslant i, j \leqslant N$, $\displaystyle\sum_{k=1}^{N} p_{ik} = 1 = \sum_{k=1}^{N} p_{kj}$;
3. For all $1 \leqslant i, j, k, \ell \leqslant N$, $p_{ij}p_{ik} = \delta_{jk}p_{ij}$ and $p_{ij}p_{\ell j} = \delta_{i\ell}p_{ij}$.

This will be called the *quantum permutation algebra* on N points.

Remark 1.7 The third condition in the definition may seem redundant since it is automatically satisfied for projections in a Hilbert space. However, a $*$-algebra may not have a faithful representation on a Hilbert space, hence Condition (3) does not necessarily follow from the two other ones.

Definition 1.6 refers to a so-called *universal object* and we will give a few details about it for the sake of completeness. This roughly means that we want the 'largest possible' algebra generated by elements that we call p_{ij} and such that the relations in the statement are satisfied. Proving that such an object exists and is well-behaved is not very difficult but requires a bit of abstraction. The intuition is to start with a full algebra of *non-commutative* polynomials and

[5] As the following relations show, we are in fact considering, here and throughout the text, universal *unital* algebras. For convenience we will drop the term 'unital' because we will never consider non-unital algebras.

then quotient by the desired relations. As for usual polynomials, it is easier to use a definition based on sequences.

Definition 1.8 Given a set I, we denote by $\mathcal{U}_I$ the complex vector space of all finite linear combinations of finite sequences of elements of I. It is endowed with the algebra structure induced by the concatenation of sequences, with the empty sequence acting as a unit.

If we denote by X_i the sequence (i), then the elements $(X_i)_{i\in I}$ generate $\mathcal{U}_I$ and any element can therefore be written as a linear combination of products of these generators, the latter products being called *monomials*. Note that this decomposition is unique up to the commutativity of addition. We therefore may, and should (and will) see $\mathcal{U}_I$ as the algebra of all non-commutative polynomials over the set I, and denote it by $\mathbf{C}\langle X_i \mid i \in I\rangle$. For our purpose, we will turn this into a $*$-algebra by setting $X_i^* = X_i$ for all $i \in I$.

Assuming now that we have a subset $\mathcal{R} \subset \mathbf{C}\langle X_i \mid i \in I\rangle$ called *relations*, here is how we can build our universal object.

Definition 1.9 The *universal $*$-algebra* generated by $(X_i)_{i\in I}$ with the relations $\mathcal{R}$ is the quotient of $\mathbf{C}\langle X_i \mid i \in I\rangle$ by the intersection of all the $*$-ideals containing $\mathcal{R}$. We will again denote its generators by $(X_i)_{i\in I}$.

That this is the correct definition is confirmed by the following *universal property*.

Exercise 1.2 Let $\mathcal{A}$ be a $*$-algebra generated by elements $(x_i)_{i\in I}$ and let $\mathcal{R} \subset \mathbf{C}\langle X_i \mid i \in I\rangle$. Prove that if $P(x_i) = 0$ for all $P \in \mathcal{R}$, then there exists a unique surjective $*$-homomorphism from the universal $*$-algebra generated by $(X_i)_{i\in I}$ with the relations $\mathcal{R}$ to $\mathcal{A}$ mapping X_i to x_i.

Solution We first construct a $*$-homomorphism from $\mathbf{C}\langle X_i \mid i \in I\rangle$. The requirements of the statements force $\pi(X_i) = x_i$, and the fact that π is a $*$-algebra homomorphism uniquely determines it on the whole of $\mathbf{C}\langle X_i \mid i \in I\rangle$, that is,

$$\pi(X_{i_1} \cdots X_{i_n}) = x_{i_1} \cdots x_{i_n}.$$

Note that this makes sense because, by definition, the monomials are a basis of $\mathbf{C}\langle X_i \mid i \in I\rangle$. Moreover, it is surjective because the x_i's are generators. By assumption, $\ker(\pi)$ is a $*$-ideal containing $\mathcal{R}$, hence it also contains the intersection J of all the $*$-ideals containing it. As a consequence, π factors through $\mathbf{C}\langle X_i \mid i \in I\rangle/J$, which is precisely the universal $*$-algebra. □

We now have a nice object to study, but the link to the classical permutation group is somewhat blurred. To clear it up, let us consider the functions $c_{ij} : S_N \to \mathbf{C}$ defined by

$$c_{ij}(\sigma) = \delta_{\sigma(i)j}.$$

This is nothing but the function sending the permutation matrix of σ to its (i, j)-th coefficient. In particular, c_{ij} always takes the value 0 or 1, hence

$$c_{ij}^* = c_{ij} = c_{ij}^2.$$

Similarly, it is straightforward to check that Conditions (2) and (3) of Definition 1.6 are satisfied. Hence, by the universal property of Exercise 1.2, there is a unique $*$-homomorphism

$$\pi_{\text{ab}} : \left\{ \begin{array}{ccc} \mathcal{A}_s(N) & \to & F(S_N) \\ p_{ij} & \mapsto & c_{ij}, \end{array} \right.$$

where $F(S_N)$ is the algebra of all functions from S_N to $\mathbf{C}$. Moreover, since the functions c_{ij} obviously generate the whole algebra $F(S_N)$, π_{ab} is onto. The subscript 'ab' is meant to indicate that π_{ab} is, in fact, the abelianisation map, that is to say, the quotient by the ideal generated by all commutators. In other words, we are claiming that $F(S_N)$ is the largest possible commutative $*$-algebra satisfying the defining relations of $\mathcal{A}_s(N)$. The proof of that fact is an easy exercise that we leave to the curious reader.

Exercise 1.3 Let $\mathcal{B}_N$ be the universal $*$-algebra generated by N^2 elements $(p_{ij})_{1\leqslant i,j\leqslant N}$ satisfying Conditions (1), (2) and (3) as well as the relations

$$p_{ij}p_{k\ell} = p_{k\ell}p_{ij},$$

for all $1 \leqslant i, j, k, \ell \leqslant N$.

1. For a permutation $\sigma \in S_N$, we set

$$p_\sigma = \prod_{i=1}^{N} p_{i\sigma(i)}.$$

Prove that $(p_\sigma)_{\sigma\in S_N}$ spans $\mathcal{B}_N$.

2. Deduce that there is a $*$-isomorphism $\mathcal{B}_N \to F(S_N)$ sending p_{ij} to c_{ij}.

Solution 1. Let us first observe that $\mathcal{B}_N$ is by definition spanned by monomials in the generators. Moreover, we claim that in such a monomial $p = p_{i_1j_1} \dots p_{i_kj_k}$, we may assume that $i_\ell \neq i_{\ell'}$ and $j_\ell \neq j_{\ell'}$ for all $\ell \neq \ell'$. Indeed, otherwise we can assume by commutativity that $\ell = \ell + 1$

and, without loss of generality, that $i_\ell = i_{\ell+1}$. It then follows from the defining relations that either $j_\ell = j_{\ell+1}$, in which case we can remove one of these two terms since $p_{i_\ell j_\ell}^2 = p_{i_\ell j_\ell}$, or $j_\ell \neq j_{\ell+1}$, in which case $p = 0$. A straightforward consequence of this is that, by the pigeonhole principle, $\mathcal{B}_N$ is spanned by monomials of length at most N.

Let us set denote by E the span of the elements in the statement. We will prove by induction on k that any monomial of length $N-k$ is in E, for $0 \leqslant k \leqslant N$. The case $k = 0$ follows from the observations in the previous paragraphs: since $(i_1, \ldots, i_N)$ and $(j_1, \ldots, j_N)$ are tuples of pairwise distinct elements of $\{1, \ldots, N\}$, there exists a permutation $\sigma \in S_N$ such that $j_\ell = \sigma(i_\ell)$ for all $1 \leqslant \ell \leqslant N$. Assume now that the result holds for some k and consider a monomial

$$p = p_{i_1 j_1} \cdots p_{i_{N-k-1} j_{N-k-1}}.$$

Let us choose an element $i_{N-k} \in \{1, \cdots, N\} \setminus \{i_1 \cdots i_{N-k-1}\}$. Then,

$$p = \sum_{j=1}^{N} p_{i_1 j_1} \cdots p_{i_{N-k-1} j_{N-k-1}} p_{i_{N-k} j}$$

and the proof is complete.

2. By universality, there is a surjective $*$-homomorphism $\mathcal{B}_N \to F(S_N)$ sending p_{ij} to c_{ij}. But from the first question we know that

$$\dim(\mathcal{B}_N) \leqslant N! = \dim(F(S_N)),$$

therefore the surjection must be injective. □

We will now use this link to investigate a possible ‘group-like’ structure on $\mathcal{A}_s(N)$. At the level of the coefficient functions, the group law of S_N satisfies the equation

$$c_{ij}(\sigma_1\sigma_2) = \sum_{k=1}^{N} c_{ik}(\sigma_1) c_{kj}(\sigma_2).$$

The trouble here is that the right-hand side is an element of $F(S_N \times S_N)$, which has no analogue in terms of quantum permutations so far. It would be more helpful to express the product solely in terms of $F(S_N)$. It turns out that there is an algebraic construction which exactly does this: the *tensor product*.

1.2.2 The Tensor Product

Our problem is to build the algebra of functions on $S_N \times S_N$ using only algebraic constructions on $F(S_N)$. One may try to consider the direct product

Cambridge University Press & Assessment
978-1-009-34573-6 — Compact Matrix Quantum Groups and Their Combinatorics
Amaury Freslon
Excerpt
More Information

$F(S_N) \times F(S_N)$, but it has dimension $2N!$ while $F(S_N \times S_N)$ has dimension $(N!)^2$, so that we need something else. Let us nevertheless focus on the direct product to get some insight. Given two functions P and Q on S_N, we can see PQ as a two-variable function. However, the set theoretic map

$$\Phi \colon (P, Q) \in F(S_N) \times F(S_N) \mapsto PQ \in F(S_N \times S_N)$$

fails to be linear. Indeed, we have the two following issues: first,

$$\begin{aligned}\Phi((P, Q) + (P', Q')) &= \Phi(P + P', Q + Q') \\ &= (P + P')(Q + Q') \\ &\neq PQ + P'Q' \\ &= \Phi(P, Q) + \Phi(P', Q')\end{aligned}$$

and second

$$\begin{aligned}\Phi(\lambda(P, Q)) &= \Phi(\lambda P, \lambda, Q) \\ &= \lambda^2 PQ \\ &\neq \lambda\Phi(P, Q).\end{aligned}$$

In order to remedy this, we can use a universal construction, as we already did to define $\mathcal{A}_s(N)$. In other words, we will start from the largest vector space on which the map Φ can be defined as a linear map.

Definition 1.10 Given two vector spaces V and W, the *free vector space on* $V \times W$ is the vector space $\mathcal{F}(V \times W)$ of all finite linear combinations of elements of $V \times W$.

One must be careful that the elements of $V \times W$ form a basis of $\mathcal{F}(V \times W)$, hence

$$(v, w) + (v', w') \neq (v + v', w + w')$$

in that space. The point of this construction is that the map Φ, defined on $F(S_N) \times F(S_N)$ by $\Phi(P, Q) = PQ$, has by definition a unique extension to a linear map

$$\widetilde{\Phi} : \mathcal{F}(F(S_N) \times F(S_N)) \to F(S_N \times S_N).$$

The problem is, of course, that this map is far from injective, and we have to identify its kernel. Here are three obvious ways of building vectors on which $\widetilde{\Phi}$ vanishes:

Cambridge University Press & Assessment
978-1-009-34573-6 — Compact Matrix Quantum Groups and Their Combinatorics
Amaury Freslon
Excerpt
More Information

- $\widetilde{\Phi}((P,Q)+(P,Q')) = PQ + PQ' = P(Q+Q') = \widetilde{\Phi}(P,Q+Q')$,
- $\widetilde{\Phi}((P,Q)+(P',Q)) = PQ + P'Q = (P+P')Q = \widetilde{\Phi}(P+P',Q)$,
- $\widetilde{\Phi}(\lambda P,Q) = \lambda PQ = \widetilde{\Phi}(P,\lambda Q)$.

The main result of this section is that this is enough to generate the kernel. Before proving this, let us give a formal definition.

Definition 1.11 Given two vector spaces V and W, we denote by $\mathcal{I}(V,W)$ the linear subspace of $\mathcal{F}(V\times W)$ spanned by the vectors

- $(v,w)+(v,w')-(v,w+w')$,
- $(v,w)+(v',w)-(v+v',w)$,
- $(\lambda v,w)-(v,\lambda w)$,

for all $(v,w)\in V\times W$. Then, the *tensor product* of V and W is the quotient vector space

$$V\otimes W = \mathcal{F}(V\times W)/\mathcal{I}(V,W).$$

The image of (v,w) in this quotient will be denoted by $v\otimes w$.

This construction may seem weird at first sight, since we are quotienting a 'huge' vector space by a 'huge' vector subspace. However, it turns out that the result is very tractable and perfectly fits our requirements. Before proving this, let us elaborate a bit more on the general construction by identifying a basis.

Proposition 1.12 *Let $(e_i)_{i\in I}$ and $(f_j)_{j\in J}$ be bases of V and W respectively. Then,*

$$(e_i\otimes f_j)_{(i,j)\in I\times J}$$

is a basis of $V\otimes W$.

Proof Let $v\in V$ and $w\in W$. By assumption, they can be written as

$$v = \sum_{i\in I_v}\lambda_i e_i \text{ and } w = \sum_{j\in J_w}\mu_j f_j$$

for some finite subsets $I_v\subset I$ and $J_w\subset J$. Thus,

$$(v,w) - \sum_{(i,j)\in I_v\times J_w}\lambda_i\mu_j(e_i,f_j)\in\mathcal{I}(V,W)$$

by definition. In other words, we have in $V\otimes W$ the equality

$$v\otimes w = \sum_{(i,j)\in I_v\times J_w}\lambda_i\mu_j e_i\otimes f_j,$$

proving that the family is generating.