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)

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

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:

$$\begin{tikzcd}
A \arrow[r, dashed, no head] \arrow[dr, bend right, "w_A"'] & \| \arrow[r, dashed, no head] & B \arrow[dl, bend left, "w_B"] \\
& R \arrow[ul, "v_A"'] \arrow[ur, "v_B"] &
\end{tikzcd}.$$

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

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

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.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

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. $\square$

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

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 $c_{ij}\colon S_N \to \mathbf{C}$ 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

$$\pi_{\mathrm{ab}}\colon \begin{cases} \mathcal{A}_s(N) & \to & F(S_N) \\ p_{ij} & \mapsto & c_{ij}, \end{cases}$$

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 $\ell = \ell + 1$

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

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

$F(S_N) \times F(S_N)$, 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:

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

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

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.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

To show linear independence, let us consider for some fixed $(i,j) \in I \times J$ the unique linear map

$$\varphi_{ij} \colon \mathcal{F}(V \times W) \to \mathbf{C}$$

sending (v,w) to $e_i^*(v) \times e_j^*(w)$ and all other basis vectors to 0. By construction, the kernel of φ_{ij} contains $\mathcal{I}(V,W)$, hence it factors through the quotient map $\pi \colon \mathcal{F}(V \times W) \to V \otimes W$ to a linear map $\psi_{ij} \colon V \otimes W \to \mathbf{C}$. It then follows that

$$\psi_{ij}(e_{i'} \otimes f_{j'}) = \delta_{ii'}\delta_{jj'},$$

and this clearly implies that the family is linearly independent, concluding the proof. □

As a consequence, we can elucidate the tensor product construction for finite-dimensional vector spaces.

Corollary 1.13 *Let V and W be vector spaces of dimension n and m respectively. Then, $V \otimes W$ has dimension $n \times m$.*

In particular, the dimension issue with the direct product disappears when considering tensor products. Back to our problem now, we want to prove that $F(S_N \times S_N)$ is isomorphic to $F(S_N) \otimes F(S_N)$. We will do this in greater generality, since we may need similar results later on in slightly diffferent contexts. We will consider algebras of the form $\mathcal{O}(X) = \mathbf{C}[X_1, \cdots, X_N]/I$ for some ideal I.[6]

Proposition 1.14 *Let $I \subset \mathbf{C}[X_1, \cdots, X_n]$ and $J \subset \mathbf{C}[Y_1, \cdots, Y_m]$ be ideals. Then, the map*

$$\Phi \colon (a + I, b + J) \mapsto ab + (I + J)$$

factors through a linear isomorphism

$$\mathbf{C}[X_1, \cdots, X_n]/I \otimes \mathbf{C}[Y_1, \cdots, Y_m]/J \simeq \mathbf{C}[X_1, \cdots, X_n, Y_1, \cdots, Y_m]/(I+J).$$

Proof To lighten notations, let us denote by A_n the complex polynomial algebra on n indeterminates. If $a \in A_n$, $b \in A_m$, $x \in I$ and $y \in J$, then

$$(a + x)(b + y) = ab + ay + xb + xy$$

and $ay + xb + xy \in I + J$ so that there is a well-defined linear map

$$\widetilde{\Phi} \colon \mathcal{F}(A_n/I \times A_m/J) \to A_{n+m}/(I + J).$$

[6] The notation here is the standard one from commutative algebra, since we are now considering algebras of *commutative polynomials*.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

One easily checks that $\mathcal{I}(A_n/I, A_m/J) \subset \ker(\widetilde{\Phi})$, hence there is a well-defined induced map

$$\Phi\colon\ (A_n/I) \otimes (A_m/J) \to A_{n+m}/(I+J).$$

Conversely, let us set for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$

$$\widetilde{X}_i = \overline{X}_i \otimes 1 \in (A_n/I) \otimes (A_m/J)\,,$$
$$\widetilde{Y}_j = 1 \otimes \overline{Y}_j \in (A_n/I) \otimes (A_m/J)\,,$$

where the bar denotes the image in the quotient. Because these elements commute, there exists by universality a unique $*$-homomorphism

$$\widetilde{\Psi}\colon A_{n+m} \to (A_n/I) \otimes (A_m/J)$$

such that $\widetilde{\Psi}(X_i) = \widetilde{X}_i$ and $\widetilde{\Psi}(Y_j) = \widetilde{Y}_j$ for all $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$. Obviously, $\widetilde{\Psi}$ vanishes on I and J, hence on $I+J$, allowing us to factor it through a map

$$\Psi\colon A_{n+m}/(I+J) \to (A_n/I) \otimes (A_m/J)\,.$$

Now, applying $\Phi \circ \Psi$ and $\Psi \circ \Phi$ to the basis vectors $\overline{X}_i^k \overline{Y}_j^\ell$ and $\overline{X}_i^k \otimes \overline{Y}_j^\ell$ respectively shows that both compositions are the identity, concluding the proof. $\square$

The result is quite satisfying, except that we do not want to deal with vector spaces but with algebras. The construction is, however, easy to generalise. First note that, if A and B are algebras, then there is an algebra structure on $A \otimes B$ defined by

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

The fact that this corresponds to a well-defined bilinear map can be checked, for instance on a basis using Proposition 1.12. If, moreover, A and B are $*$-algebras, then there is a $*$-algebra structure on $A \otimes B$ given by

$$(a \otimes b)^* = a^* \otimes b^*.$$

We can now state and prove our main result:

Theorem 1.15 *Let $I \subset A_n$ and $J \subset A_m$ be $*$-ideals. Then, the map*

$$(a + I, b + J) \mapsto ab + (I + J)$$

factors through an algebra $*$-isomorphism

$$(A_n/I) \otimes (A_m/J) \simeq A_{n+m}/(I+J).$$

Proof One simply has to check that the linear isomorphisms Φ and Ψ from Proposition 1.14 are algebra $*$-homomorphisms, which is straightforward. $\square$

Applying this to the case of the algebra of functions on S_N is a good way to understand what precisely is going on.

Corollary 1.16 *The map $\imath\colon F(S_N) \otimes F(S_N) \to F(S_N \times S_N)$ sending $f \otimes g$ to the map*

$$(\sigma, \tau) \mapsto f(\sigma)g(\tau)$$

extends to a $*$-algebra isomorphism.

Proof Let I be the ideal of $A = \mathbf{C}[X_{ij} \mid 1 \leqslant i, j \leqslant N]$ generated by the polynomials giving the relations of Definition 1.6, so that $A/I = F(S_N)$ by Exercise 1.3. Theorem 1.15 yields an isomorphism

$$F(S_N) \otimes F(S_N) \to \mathbf{C}[X_{ij}, Y_{ij} \mid 1 \leqslant i, j \leqslant N]/\widetilde{I},$$

where $\widetilde{I}$ is generated by the two copies of I and the image of $P \otimes Q$ is $P \times Q$. Any element of the right-hand side can be written as a linear combination of products $P \times Q$ and therefore defines a function on $S_N \times S_N$ so that the map induces a surjection onto $F(S_N \times S_N)$. By equality of the dimensions, such a surjection must be an isomorphism, concluding the proof. $\square$

As a conclusion, we can identify canonically $F(S_N \times S_N)$ with $F(S_N) \otimes F(S_N)$, so that we have an analogue of the algebra of functions on pairs of quantum permutation matrices, which is simply $\mathcal{A}_s(N) \otimes \mathcal{A}_s(N)$.

Now that we are talking about tensor products, let us take the occasion to define the corresponding construction on linear maps, so that it is ready for use in the next chapters.

Exercise 1.4 Let V_i, W_i be vector spaces for $i \in \{1, 2\}$ and let $T_i\colon V_i \to W_i$ be linear maps. Prove that there exists a unique linear map

$$T_1 \otimes T_2\colon V_1 \otimes V_2 \to W_1 \otimes W_2$$

such that for any $(v_1, v_2) \in V_1 \otimes V_2$,

$$(T_1 \otimes T_2)(v_1 \otimes v_2) = T_1(v_1) \otimes T_2(v_2).$$

Solution We can define a map

$$T_1 \odot T_2\colon \mathcal{F}(V_1 \times V_2) \to \mathcal{F}(W_1 \times W_2) \to W_1 \otimes W_2$$

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

by the formula

$$(T_1 \odot T_2)(v_1, v_2) = T_1(v_1) \otimes T_2(v_2).$$

Then, the linearity of T_1 and T_2 implies that $T_1 \odot T_2$ vanishes on $\mathcal{I}(V_1, V_2)$, hence it factors through $V_1 \otimes V_2$, yielding the result. $\square$

1.2.3 Coproduct

Back to our formula for the product, we can now write, making the isomorphism implicit,

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

Considering the elements p_{ij} as 'coefficient functions', this suggests to encode a kind of 'group law' through the map

$$\Delta\colon p_{ij} \to \sum_{k=1}^{N} p_{ik} \otimes p_{kj}. \tag{1.1}$$

But for this to work, one must first prove that such a map Δ exists.

Proposition 1.17 *There exists a unique $*$-homomorphism*

$$\Delta\colon \mathcal{A}_s(N) \to \mathcal{A}_s(N) \otimes \mathcal{A}_s(N)$$

satisfying formula (1.1).

Proof Let us set, for $1 \leqslant i, j \leqslant N$,

$$q_{ij} = \sum_{k=1}^{N} p_{ik} \otimes p_{kj}.$$

We claim that the q_{ij}'s satisfy Conditions (1) to (3) of Definition 1.6. The existence of Δ then follows from the universal property. $\square$

Exercise 1.5 Prove the claim in the preceding proof.

Solution It is clear that $q_{ij}^* = q_{ij}$. Let us now compute the square

$$\begin{aligned} q_{ij}^2 &= \sum_{k,\ell=1}^{N} p_{ik}p_{i\ell} \otimes p_{kj}p_{\ell j} \\ &= \sum_{k,\ell=1}^{N} \delta_{k\ell}p_{ik} \otimes p_{kj} \\ &= q_{ij}. \end{aligned}$$

We have therefore checked Condition (1). Moreover,

$$\begin{aligned}\sum_{i=1}^{N} q_{ij} &= \sum_{k,i=1}^{N} p_{ik} \otimes p_{kj} \\ &= \sum_{k=1}^{N} \left(\sum_{i=1}^{N} p_{ik}\right) \otimes p_{kj} \\ &= \sum_{k=1}^{N} 1 \otimes p_{kj} \\ &= 1 \otimes 1,\end{aligned}$$

hence Condition (2) also is satisfied. Eventually, for $j \neq j'$,

$$q_{ij}q_{ij'} = \sum_{k,\ell=1}^{N} p_{ik}p_{i\ell} \otimes p_{kj}p_{\ell j'}.$$

The first tensor in the sum vanishes unless $k = \ell$, but in that case the second one vanishes and Condition (3) follows. The argument for $i \neq i'$ is similar. □

The map Δ is called the *coproduct* and is a reasonable substitute for matrix multiplication (i.e. the group law of a matrix group). In particular, it satisfies an analogue of the associativity property of the group law, called *coassociativity*, which reads

$$(\Delta \otimes \mathrm{id}) \circ \Delta = (\mathrm{id} \otimes \Delta) \circ \Delta. \tag{1.2}$$

Exercise 1.6 Prove that the coproduct on $\mathcal{A}_s(N)$ is indeed coassociative. Check also that the corresponding equation on the coefficient functions in S_N is equivalent to the associativity of the composition of permutations.

Solution Because Δ is a $*$-algebra homomorphism, it is enough to check coassociativity on the generators,

$$\begin{aligned}(\Delta \otimes \mathrm{id}) \circ \Delta(p_{ij}) &= \sum_{k=1}^{N} \Delta(p_{ik}) \otimes p_{kj} \\ &= \sum_{k,\ell=1}^{N} p_{i\ell} \otimes p_{\ell k} \otimes p_{kj} \\ &= \sum_{\ell=1}^{N} p_{i\ell} \otimes \Delta(p_{\ell j}) \\ &= (\mathrm{id} \otimes \Delta) \circ \Delta(p_{ij}).\end{aligned}$$

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

As for the second assertion, we have already seen that

$$\Delta(c_{ij})(\sigma_1, \sigma_2) = c_{ij}(\sigma_1\sigma_2).$$

Thus,

$$(\Delta \otimes \mathrm{id}) \circ \Delta(c_{ij})(\sigma_1, \sigma_2, \sigma_3) = \Delta(c_{ij})(\sigma_1\sigma_2, \sigma_3) = c_{ij}((\sigma_1\sigma_2)\sigma_3)$$

while

$$(\mathrm{id} \otimes \Delta) \circ \Delta(c_{ij})(\sigma_1, \sigma_2, \sigma_3) = \Delta(c_{ij})(\sigma_1, \sigma_2\sigma_3) = c_{ij}(\sigma_1(\sigma_2\sigma_3))$$

so that coassociativity is equivalent to $f((\sigma_1\sigma_2)\sigma_3) = f(\sigma_1(\sigma_2\sigma_3))$ for all $f \in \mathcal{F}(S_N)$ and $\sigma_1, \sigma_2, \sigma_3 \in S_N$, which is, in turn, equivalent to the associativity of the group law. □

The coproduct certainly indicates that we are on the right track to produce a group-like structure on the quantum permutation algebra. However, we still need a neutral element and an inverse. But instead of trying to translate each of them, we will take advantage of the fact that we are considering a matrix group. Indeed, for any permutation σ, the corresponding matrix is orthogonal, hence

$$\sum_{k=1}^{N} c_{ik}(\sigma)c_{jk}(\sigma) = \delta_{ij} = \sum_{k=1}^{N} c_{ki}(\sigma)c_{kj}(\sigma). \tag{1.3}$$

Since this holds for any σ, it can be written as an equality of functions in $F(S_N)$, and it turns out that the same equality holds in $\mathcal{A}_s(N)$.

Proposition 1.18 *For any* $1 \leqslant i, j \leqslant N$,

$$\sum_{k=1}^{N} p_{ik}p_{jk} = \delta_{ij} = \sum_{k=1}^{N} p_{ki}p_{kj}. \tag{1.4}$$

Proof This is a direct consequence of Conditions (1) to (3). □

This means that the quantum permutation algebra is somehow 'made of orthogonal quantum matrices' (see the beginning of Subsection 1.3.3 for a more precise statement), and this property should contain all information about the unit and the inverse. Another way to state this is that the matrix $P = (p_{ij})_{1\leqslant i,j\leqslant N} \in M_N(\mathcal{A}_s(N))$ is orthogonal in the sense that its inverse equals its transpose. As a conclusion, the algebra $\mathcal{A}_s(N)$ with its generators $(p_{ij})_{1\leqslant i,j\leqslant N}$ seem to have all the properties one can expect for a group-like object. It therefore deserves the name of *quantum group* that we will define in the next section.

The fact that Condition (1.4) yields a full group-like structure can be encoded in the two following maps, whose existence follows from the universal property of $\mathcal{A}_s(N)$.

- The *antipode* $S\colon \mathcal{A}_s(N) \to \mathcal{A}_s(N)$, which is the unique $*$-antihomomorphism induced by
$$p_{ij} \mapsto p_{ji}.$$
Since the transpose of P is its inverse, this plays the role of the inverse map.
- The *counit* $\varepsilon\colon \mathcal{A}_s(N) \to \mathbf{C}$, which is the unique $*$-homomorphism induced by
$$p_{ij} \mapsto \delta_{ij}.$$
Since the matrix $(\delta_{ij})_{1\leqslant i,j\leqslant N}$ is the identity, this plays the role of the neutral element.

Exercise 1.7 Prove the existence of the maps S and ε.

Solution 1. We start with the antipode S. The uniqueness is clear, and we have to prove existence. Let us denote by $\mathcal{A}$ the opposite algebra of $\mathcal{A}_s(N)$, that is to say, the algebra with the same underlying vector space but such that $a \times_{\mathcal{A}} b = ba$. Let us also consider the elements $q_{ij} = p_{ji}$ in $\mathcal{A}$. Then, the matrix $(q_{ij})_{1\leqslant i,j\leqslant N}$ is a quantum permutation matrix and its coefficients generate $\mathcal{A}$, hence there is a surjective $*$-homomorphism
$$\widetilde{S}\colon \mathcal{A}_s(N) \to \mathcal{A}$$
such that $\widetilde{S}(p_{ij}) = q_{ij}$. Composing with the identity map seen as a linear isomorphism $I\colon \mathcal{A} \to \mathcal{A}_s(N)$ yields a map $S = I \circ \widetilde{S}\colon \mathcal{A}_s(N) \to \mathcal{A}_s(N)$. By construction, $S(p_{ij}) = p_{ji}$ and, moreover,
$$\begin{aligned} S(p_{ij}p_{k\ell}) &= I \circ \widetilde{S}(p_{ij}p_{k\ell}) \\ &= I(q_{ij} \times_{\mathcal{A}} q_{k\ell}) \\ &= I(q_{k\ell}q_{ij}) \\ &= p_{\ell k}p_{ji} \\ &= S(p_{k\ell})S(p_{ij}) \end{aligned}$$
so that S is anti-multiplicative.

2. We now turn to the counit ε. Noticing that the identity matrix is a quantum permutation matrix, the universal property of $\mathcal{A}_s(N)$ directly yields a

$*$-homomorphism $\varepsilon\colon \mathcal{A}_s(N) \to \mathbf{C}$ sending p_{ij} to the corresponding coefficient of the identity matrix, which is δ_{ij}. □

It is worth working out the analogues of these maps for the classical permutation group to be convinced that they encode the complete group structure.

Exercise 1.8 Write down the explicit form of the analogues of the counit ε and antipode S for $F(S_N)$ in terms of permutations.

Solution The functions corresponding to the p_{ij}'s are the functions $c_{ij} : \sigma \mapsto \delta_{\sigma(i)j}$. Thus,

$$S(c_{ij})(\sigma) = c_{ji}(\sigma) = \delta_{\sigma(j)i} = \delta_{\sigma^{-1}(i)j} = c_{ij}(\sigma^{-1})$$

so that S is induced by the inverse map on S_N. Similarly,

$$\varepsilon(c_{ij}) = \delta_{ij} = c_{ij}(\mathrm{id})$$

so that ε corresponds to the identity permutation. □

With these maps, Equation (1.4) becomes

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

where $m\colon \mathcal{A}_s(N) \otimes \mathcal{A}_s(N) \to \mathcal{A}_s(N)$ is the multiplication map. Our focus in this text is on the matricial aspect of quantum groups, and we will therefore never use these maps.[7] Note, however, that $(\mathcal{A}_s(N), \Delta, \varepsilon, S)$ is what is called a *Hopf algebra*. The theory of Hopf algebras is vast and has many connections to other fields. The reader may, for instance, read [62] for a detailed introduction or [48] for more categorical aspects and important applications.

1.3 Compact Matrix Quantum Groups

Our study of the quantum permutation algebra has given us enough motivation to introduce a notion of compact quantum group. There is a nice and complete theory of these objects, which was developed by S. L Woronowicz in [77]. There are two published books explaining this theory in detail, [69] and [60] to which the reader may refer for alternative expositions emphasising other aspects.

[7] This is a lie. We will use them at some point to get a computationally tractable description of representations, but in a way which has no consequence for the remainder of the development of the theory.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

1.3.1 A First Definition

The purpose of this text is to give some examples of the interaction between the combinatorics of partitions and the theory of compact quantum groups. The most striking examples involve compact quantum groups which belong to a specific class which is, in a sense, simpler to define and handle. It was introduced by S. L Woronowicz in [75] as a generalisation of compact groups of matrices and as a first attempt at a definition of compact quantum groups. We will therefore focus on this class, even though our definition differs from [75, definition 1.1] and is closer to [70, definition 2.1’].

Before giving the definition, we have to give an important warning. We will use throughout this text a specific assumption on all compact quantum groups which is somehow hidden in the definition. In plain terms, all the objects that we will consider will be of so-called *Kac type*. However, for simplicity and because this is a consequence of our axioms, we will never mention that specificity again. But the reader should be aware that our terminology does not exactly match the literature, because one should, any time the words ‘compact quantum group’ are written hereafter, add the words ‘of Kac type’ (for more comments on this, see the end of Appendix C).

Definition 1.19 An *orthogonal compact matrix quantum group* of size N is given by a $*$-algebra $\mathcal{A}$ generated by N^2 elements $(u_{ij})_{1\leqslant i,j\leqslant N}$ such that

1. $u_{ij} = u_{ij}^*$ for all $1 \leqslant i, j \leqslant N$;
2. For all $1 \leqslant i, j \leqslant N$,
$$\sum_{k=1}^{N} u_{ik}u_{jk} = \delta_{ij} = \sum_{k=1}^{N} u_{ki}u_{kj};$$
3. There exists a $*$-homomorphism $\Delta\colon \mathcal{A} \to \mathcal{A}\otimes\mathcal{A}$ such that for all $1 \leqslant i, j \leqslant N$,
$$\Delta(u_{ij}) = \sum_{k=1}^{N} u_{ik}\otimes u_{kj}.$$

Denoting by $u \in M_N(\mathcal{A})$ the matrix with coefficients $(u_{ij})_{1\leqslant i,j\leqslant N}$, we will denote the orthogonal compact matrix quantum group by $(\mathcal{A}, u)$.

By analogy with our reasoning on S_N, $\mathcal{A}$ will be thought of as the algebra of functions on a non-existent ‘quantum space’. However, if we consider general ‘compact quantum spaces’, we cannot use all the functions like for S_N. Here our crucial intuition will be that compact groups of matrices are completely determined by their algebra of *regular functions*, that is to say, functions which are polynomial in the matrix coefficients (see the beginning of Section 5.1 for some details on this). The usual notation for this is $\mathcal{O}(G)$, whence the notation $\mathcal{A} = \mathcal{O}(\mathbb{G})$ if $\mathbb{G} = (\mathcal{A}, u)$ denotes the orthogonal compact matrix quantum group. We can now formalise the properties of the quantum permutation algebras established in Section 1.2.

Definition 1.20 For any integer N, the pair $(\mathcal{A}_s(N), P)$ is an orthogonal compact matrix quantum group, where $P = (p_{ij})_{1\leqslant i,j\leqslant N}$. It is called the *quantum permutation group* on N points and is usually referred to using the notation S_N^+.

Consequently, we may from now on write $\mathcal{O}(S_N^+)$ instead of $\mathcal{A}_s(N)$. This quantum group was first defined by S. Wang in [72]. It is natural (and crucial for our purpose) to wonder whether this is really different from S_N.

Exercise 1.9 Prove that for $N = 1, 2, 3$, $S_N^+ = S_N$ in the sense that π_{ab} is injective. Prove moreover that for any $N \geqslant 4$, $\mathcal{O}(S_N^+)$ is non-commutative, hence not isomorphic to $F(S_N)$.

Solution For $N = 1$, $\mathcal{A}_s(1)$ is generated by one self-adjoint projection, hence is isomorphic to $\mathbf{C} = F(S_1)$. For $N = 2$, observe that the relations force

$$P = \begin{pmatrix} p_{11} & 1 - p_{11} \\ 1 - p_{11} & p_{11} \end{pmatrix}$$

making $\mathcal{A}_s(2)$ abelian, hence equal to $F(S_2)$.

For $N = 3$, we must again prove that $\mathcal{A}_s(3)$ is abelian. Here is a simple argument from [53]. It is enough to prove that p_{11} commutes with p_{22}, since any independent permutation of the rows and columns of P yields an automorphism of $\mathcal{A}_s(N)$ by the universal property. We start by observing that

$$\begin{aligned} p_{11}p_{22} &= p_{11}p_{22}\left(p_{11} + p_{12} + p_{13}\right) \\ &= p_{11}p_{22}p_{11} + p_{11}p_{22}p_{13}. \end{aligned}$$

But

$$\begin{aligned} p_{11}p_{22}p_{13} &= p_{11}\left(1 - p_{21} - p_{23}\right)p_{13} \\ &= p_{11}p_{13} - p_{11}p_{21}p_{13} - p_{11}p_{23}p_{13} \\ &= 0, \end{aligned}$$

hence

$$\begin{aligned} p_{11}p_{22} &= p_{11}p_{22}p_{11} \\ &= (p_{11}p_{22}p_{11})^* \\ &= (p_{11}p_{22})^* \\ &= p_{22}^*p_{11}^* \\ &= p_{22}p_{11}. \end{aligned}$$

For $N \geqslant 4$, let p and q be the orthogonal projections onto the lines spanned by the vectors $(0, 1)$ and $(1, 1)$ respectively in $\mathbf{C}^2$, so that $pq \neq qp$. Then, consider the matrix

$$\begin{pmatrix} p & 1-p & 0 & 0 \\ 1-p & p & 0 & 0 \\ 0 & 0 & q & 1-q \\ 0 & 0 & 1-q & q \end{pmatrix}$$

and complete it to an $N \times N$ matrix by putting it in the upper left corner, setting the other diagonal coefficients to 1 and all the other coefficients to 0. This yields a quantum permutation matrix, hence a $*$-homomorphism $\pi \colon \mathcal{O}(S_N^+) \to \mathcal{B}(H)$. Because $\pi(u_{11}) = p$ and $\pi(u_{33}) = q$ do not commute, we infer that $\mathcal{O}(S_N^+)$ is not commutative. □

To get a better understanding of Definition 1.19, it is worth working out the link with the classical case. This requires the identification of the kernel of a tensor product of linear maps, that we give here as a lemma.

Lemma 1.21 *Let $T_1 \colon V_1 \to W_1$ and $T_2 \colon V_2 \to W_2$ be linear maps. Then,*

$$\ker(T_1 \otimes T_2) = \ker(T_1) \otimes V_2 + V_1 \otimes \ker(T_2).$$

Proof We may assume without loss of generality that the maps are surjective. Moreover, we have decompositions

$$V_i = \ker(T_i) \oplus V_i'$$

such that the maps restrict to isomorphisms on V_i'. Let us denote by $\widetilde{T_i}$ the projection onto V_i' parallel to $\ker(T_i)$. It is easy to see that we have a decomposition

$$V_1 \otimes V_2 = (\ker(T_1) \otimes \ker(T_2)) \oplus (\ker(T_1) \otimes V_2') \oplus (V_1' \oplus \ker(T_2)) \oplus (V_1' \otimes V_2').$$

By definition, $\widetilde{T_1} \otimes \widetilde{T_2}$ vanishes on the first three summands and is the identity on the last one so that its kernel is

$$(\ker(T_1) \otimes \ker(T_2)) \oplus (\ker(T_1) \otimes V_2') \oplus (V_1' \oplus \ker(T_2)) = \ker(T_1) \otimes V_2 + V_1 \otimes \ker(T_2).$$

The result now follows from the fact that

$$T_1 \otimes T_2 = (\mathrm{id} \oplus T_{1|V_1'}) \otimes (\mathrm{id} \oplus T_{2|V_2'}) \circ (\widetilde{T}_1 \otimes \widetilde{T}_2)$$

has the same kernel as $\widetilde{T}_1 \otimes \widetilde{T}_2$. □

We would like now to describe all orthogonal compact matrix quantum groups $(\mathcal{A}, u)$ where $\mathcal{A}$ is a commutative $*$-algebra, and to prove that they come from compact groups of orthogonal matrices. However, there is a rather non-trivial step in such a proof: one needs to prove that for a given $*$-ideal $I \subset \mathbf{C}[X_{ij} \mid 1 \leqslant i, j \leqslant N]$, any polynomial vanishing on the intersection of all the zeros if elements of I is again in I. This is reminiscent of the famous Nüllstelensatz from algebraic geometry, and taking this path would lead us to showing that some $*$-algebra does not contain nilpotent elements, which is difficult. There is, nevertheless, another way around, using operator algebras. But this will only be possible once the connection between our algebraic framework and functional analysis is made in Chapter 5 (see, more precisely, Corollary 5.18). We will therefore restrict ourselves to partial results hereafter, hoping that they nontheless give enough motivation to the reader to keep reading this text.

Exercise 1.10 Let $(\mathcal{A}, u)$ be an orthogonal compact matrix quantum group such that $\mathcal{A}$ is commutative. We set

$$\mathcal{O}(M_N(\mathbf{C})) = \mathbf{C}[X_{ij} \mid 1 \leqslant i, j \leqslant N].$$

1. Show that there exists a surjective $*$-homomorphism $\pi\colon \mathcal{O}(M_N(\mathbf{C})) \to \mathcal{A}$. We set $I = \ker(\pi)$.
2. Let us set

$$G = \{M \in M_N(\mathbf{C}) \mid P(M) = 0 \text{ for all } P \in I\}.$$

   Prove that G is a closed subgroup of O_N. *Hint: a compact bisimplifiable semigroup is a group (see, for instance, [60, example 1.1.2] for a proof).*
3. We now set

$$J = \{P \in \mathcal{O}(M_N(\mathbf{C})) \mid P(M) = 0 \text{ for all } M \in G\},$$

   so that $\mathcal{O}(G) = \mathcal{O}(M_N(\mathbf{C}))/J$. Check that $I \subset J$.
4. We now assume that $\mathcal{A}$ is finite-dimensional.
   (a) Show that G is then finite.
   (b) Conclude that $\mathcal{A} = \mathcal{O}(G)$.
5. We assume instead that for any $x \in \mathcal{A}\backslash\{0\}$, there exists a $*$-homomorphism $f\colon \mathcal{A} \to \mathbf{C}$ such that $f(x) \neq 0$. Conclude again that $\mathcal{A} = \mathcal{O}(G)$.

Solution 1. This follows from the fact that $\mathcal{O}(M_N(\mathbf{C}))$ is the universal $*$-algebra generated by N^2 self-adjoint pairwise commuting variables, so that setting $\pi(X_{ij}) = u_{ij}$ works.

2. We first note that G is closed by definition and consists of orthogonal matrices because u is orthogonal. Let us therefore prove that G is stable under product, which is enough according to the hint. Let us start by observing that the elements

$$Y_{ij} = \sum_{k=1}^{N} X_{ik} \otimes X_{kj}$$

are self-adjoint and pairwise commute, hence there exists a unique $*$-homomorphism $\Delta\colon \mathcal{O}(M_N(\mathbf{C})) \to \mathcal{O}(M_N(\mathbf{C}))\otimes\mathcal{O}(M_N(\mathbf{C}))$ such that $\Delta(X_{ij}) = Y_{ij}$. If now $P \in I$, we have

$$(\pi \otimes \pi) \circ \Delta(P) = \Delta \circ \pi(P) = 0,$$

so that by Lemma 1.21 we can write

$$\Delta(P) = \sum_i P_i \otimes Q_i \in \mathcal{O}(M_N(\mathbf{C})) \otimes \mathcal{O}(M_N(\mathbf{C}))$$

such that, for all i, either P_i or Q_i belongs to I. Thus, for any $M_1, M_2 \in G$,

$$\begin{aligned} P(M_1M_2) &= \Delta(P)(M_1, M_2) \\ &= \sum_i P_i(M_1)Q_i(M_2) \\ &= 0 \end{aligned}$$

and $M_1M_2 \in G$.

3. By definition of G, $P(M) = 0$ for any $M \in G$ if $P \in I$, hence the inclusion.

4. (a) Because $\mathcal{O}(G)$ is a quotient of $\mathcal{A}$, it is also finite-dimensional and our strategy will be to prove that if G is infinite, then $\mathcal{O}(G)$ is infinite-dimensional. To do this, let us first define, for $M \in O_N$,

$$P_M(X_{ij}) = \sum_{1\leqslant i,j\leqslant N} (X_{ij} - M_{ij})^*(X_{ij} - M_{ij}).$$

This is a polynomial and $P_M(M') = 0$ if and only if $M' = M$. Therefore, if $F \subset G$ is a finite set, we can define the polynomial

$$P_{M,F}(X_{ij}) = \frac{1}{\displaystyle\prod_{M'\in F\setminus\{M\}} P_{M'}(M)} \prod_{M'\in F\setminus\{M\}} P_{M'}(X_{ij})$$

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

for any $M \in F$. That polynomial evaluates to 1 on M and 0 on all other elements of F. As a consequence, the family $(\pi(P_{M,F}))_{M\in F}$ is linearly independent in $\mathcal{O}(G)$, proving that

$$\dim(\mathcal{O}(G)) \geqslant |F|.$$

If now G is infinite, it contains arbitrary large finite subsets, hence $\dim(\mathcal{O}(G)) = +\infty$.

(b) We have to prove that $I = J$. Observe that by the previous question the polynomials $(P_{M,G})_{M\in G}$ span a complement of J in $\mathcal{O}(M_N(\mathbf{C}))$. Therefore, any $P \in I$ can be written as

$$P = Q + \sum_{M\in G} \lambda_M P_M$$

for some $Q \in J$ and $\lambda_M \in \mathbf{C}$ for all $M \in G$. Then, for any $M \in G$ evaluating the previous expression at M yields

$$\sum_{N\in G\setminus\{M\}} \lambda_N = 0$$

and the only solution to this linear system is $\lambda_M = 0$ for all $M \in G$. Therefore, $I = J$ and the proof is complete.

5. If $f\colon \mathcal{A} \to \mathbf{C}$ is a $*$-homomorphism, then we claim that the matrix $\widehat{f} = (f(u_{ij}))_{1\leqslant i,j\leqslant N}$ is in G. Indeed, if $P \in I$, then

$$P(\widehat{f}) = (f(P(u_{ij}))_{1\leqslant i,j\leqslant N} = 0.$$

As a consequence, f is nothing but the evaluation map at $\widehat{f}$. Therefore, if

$$\pi'\colon \mathcal{A} \to \mathcal{A}/\pi(J) = \mathcal{O}(G)$$

is the canonical surjection and $x \in \ker(\pi')$, then

$$f(x) = \pi'(x)(\widehat{f}) = 0$$

and the condition in the question ensures that $\ker(\pi') = 0$, hence $\mathcal{A} = \mathcal{O}(G)$. □

1.3.2 The Quantum Orthogonal Group

Before delving into the general theory of compact quantum groups, let us give another fundamental example which is also due to S. Wang, but earlier in [70]. After a look at Definition 1.19, it is natural to wonder about the largest possible orthogonal compact matrix quantum group. Its definition relies on the following simple fact.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

Exercise 1.11 Let N be an integer and let $\mathcal{A}_o(N)$ be the universal $*$-algebra generated by N^2 elements $(U_{ij})_{1\leqslant i,j\leqslant N}$ such that

- $U_{ij}^* = U_{ij}$ for all $1 \leqslant i, j \leqslant N$;
- $\displaystyle\sum_{k=1}^{N} U_{ik}U_{jk} = \delta_{ij} = \sum_{k=1}^{N} U_{ki}U_{kj}$.

Then, there exists a unique $*$-homomorphism

$$\Delta\colon \mathcal{A}_o(N) \to \mathcal{A}_o(N) \otimes \mathcal{A}_o(N)$$

such that for all $1 \leqslant i, j \leqslant N$,

$$\Delta(U_{ij}) = \sum_{k=1}^{N} U_{ik} \otimes U_{kj}.$$

Solution The proof is similar to that of Proposition 1.17. We set

$$V_{ij} = \sum_{k=1}^{N} U_{ik} \otimes U_{kj}$$

and have to check that the corresponding matrix V is orthogonal. Indeed,

$$\begin{aligned}
\sum_{k=1}^{N} V_{ik}V_{jk} &= \sum_{k,\ell,m=1}^{N} U_{i\ell}U_{jm} \otimes U_{\ell k}U_{mk} \\
&= \sum_{\ell,m=1}^{N} U_{i\ell}U_{jm} \otimes \left(\sum_{k=1}^{N} U_{\ell k}U_{mk}\right) \\
&= \sum_{\ell,m=1}^{N} U_{i\ell}U_{jm} \otimes \delta_{\ell m} \\
&= \sum_{\ell=1}^{N} U_{i\ell}U_{j\ell} \otimes 1 \\
&= \delta_{ij} 1 \otimes 1.
\end{aligned}$$

The other equality is proved similarly, and it then follows from universality that there exists a $*$-homomorphism sending U_{ij} to V_{ij}. □

Denoting by U the matrix $(U_{ij})_{1\leqslant i,j\leqslant N} \in M_N(\mathcal{A}_o(N))$, this motivates the following definition.

Definition 1.22 The pair $(\mathcal{A}_o(N), U)$ is an orthogonal compact matrix quantum group called the *quantum orthogonal group*. It is usually referred to using the notation O_N^+.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

As the name suggests, O_N^+ is linked to the orthogonal group. Indeed, if $c_{ij}\colon O_N \to \mathbf{C}$ are the matrix coefficient functions, then there is a surjective $*$-homomorphism

$$\pi_{\mathrm{ab}}\colon \mathcal{O}(O_N^+) \to \mathcal{O}(O_N)$$

sending U_{ij} to c_{ij}. Thus, O_N^+ is a quantum version of O_N just in the same way as S_N^+ is a quantum version of S_N.

Remark 1.23 The preceding comments, as well as the notation π_{ab}, suggest that $\mathcal{O}(O_N)$ is the largest abelian quotient of $\mathcal{O}(O_N^+)$. This would be easy to prove if we knew that any orthogonal compact matrix quantum group with commutative $*$-algebra comes from a group. It will therefore be a consequence of Corollary 5.18.

Note that it follows from the universal property that there is a surjective $*$-homomorphism

$$\mathcal{O}(O_N^+) \to \mathcal{O}(S_N^+),$$

so that $\mathcal{O}(O_N^+)$ is not commutative as soon as $N \geqslant 4$. However, more is true in that case.

Proposition 1.24 *The $*$-algebra $\mathcal{O}(O_N^+)$ is non-commutative as soon as $N \geqslant 2$.*

Proof Let $r_1, r_2 \in \mathcal{B}(\mathbf{C}^2)$ be two reflections with axis generated by the vectors $(1,0)$ and $(1,1)$ respectively, so that they do not commute. Then, the diagonal matrix with first coefficient r_1 and all other coefficients equal to r_2 is orthogonal, hence there exists a $*$-homomorphism

$$\pi\colon \mathcal{O}(O_N^+) \to \mathcal{B}(\mathbf{C}^2)$$

sending U_{ij} to 0 if $i \neq j$, to r_1 if $i = 1 = j$ and to r_2 otherwise. In particular, $\pi(U_{11})$ and $\pi(U_{22})$ do not commute, so that $\mathcal{O}(O_N^+)$ is not commutative. $\square$

1.3.3 The Unitary Case

The intuition that orthogonal compact matrix quantum groups generalise subgroups of O_N can be made rigorous in the following way: by universality, for any orthogonal compact matrix quantum group $\mathbb{G} = (\mathcal{O}(\mathbb{G}), u)$, there is a surjective $*$-homomorphism

$$\pi\colon \mathcal{O}(O_N^+) \to \mathcal{O}(\mathbb{G})$$

sending U_{ij} to u_{ij} and therefore satisfying

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

$$\Delta \circ \pi(x) = (\pi \otimes \pi) \circ \Delta(x)$$

for all $x \in \mathcal{O}(\mathbb{G})$. Thus, orthogonal compact matrix quantum groups are 'quantum subgroups' of O_N^+.

One may wonder whether it is possible to consider analogues of closed subgroups of the unitary group U_N instead of the orthogonal one. This is possible, but we will not need it until the last part of this text. Moreover, this more general setting involves subtleties which make some arguments tricky. This can already be seen in the following definition.

Definition 1.25 A *unitary compact matrix quantum group* of size N is given by a $*$-algebra $\mathcal{A}$ generated by N^2 elements $(u_{ij})_{1\leqslant i,j\leqslant N}$ such that

1. There exist a $*$-homomorphism $\Delta\colon \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}$ such that for all $1 \leqslant i$, $j \leqslant N$,
$$\Delta(u_{ij}) = \sum_{k=1}^{N} u_{ik} \otimes u_{kj};$$
2. For all $1 \leqslant i, j \leqslant N$,
$$\sum_{k=1}^{N} u_{ik}u_{jk}^* = \delta_{ij} = \sum_{k=1}^{N} u_{ki}^* u_{kj}$$
and
$$\sum_{k=1}^{N} u_{ki}u_{kj}^* = \delta_{ij} = \sum_{k=1}^{N} u_{ik}^* u_{jk}.$$

Remark 1.26 The relations in the previous definition mean that both the matrix u and its conjugate $\overline{u}$ (the matrix where each coefficient is replaced with its adjoint) are unitary. The second one does not follow from the first one in general (see [70, section 4.1] for a counter-example), so that both need to be included in the definition.

Once again, there is an obvious example obtained by considering the largest possible such quantum group at a fixed size N.

Definition 1.27 Let $\mathcal{A}_u(N)$ be the universal $*$-algebra generated by N^2 elements $(V_{ij})_{1\leqslant i,j\leqslant N}$ such that

$$\sum_{k=1}^{N} V_{ik}V_{jk}^* = \delta_{ij} = \sum_{k=1}^{N} V_{ki}^* V_{kj}$$

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

and

$$\sum_{k=1}^{N} V_{ik}^{*} V_{jk} = \delta_{ij} = \sum_{k=1}^{N} V_{ki} V_{kj}^{*}.$$

One can construct as before a compact quantum group structure on this, and by now the reader should be able to do this alone.

Exercise 1.12 1. Prove that there exists a unique $*$-homomorphism

$$\Delta\colon \mathcal{A}_u(N) \to \mathcal{A}_u(N) \otimes \mathcal{A}_u(N)$$

such that

$$\Delta(V_{ij}) = \sum_{k=1}^{N} V_{ik} \otimes V_{kj}.$$

2. Prove that $\mathcal{A}_u(N)$ is non-commutative for $N \geqslant 2$.
3. What is $\mathcal{A}_u(1)$?

Solution 1. Let us set

$$W_{ij} = \sum_{k=1}^{N} V_{ik} \otimes V_{kj}.$$

Then,

$$\begin{aligned}
\sum_{k=1}^{N} W_{ik} W_{jk}^{*} &= \sum_{k=1}^{N} \sum_{\ell,\ell'=1}^{N} V_{i\ell} V_{j\ell'}^{*} \otimes V_{\ell k} V_{\ell' k}^{*} \\
&= \sum_{\ell,\ell'=1}^{N} V_{i\ell} V_{j\ell'}^{*} \otimes \left(\sum_{k=1}^{N} V_{\ell k} V_{\ell' k}^{*} \right) \\
&= \sum_{\ell,\ell'=1}^{N} V_{i\ell} V_{j\ell'}^{*} \otimes (\delta_{\ell,\ell'}) \\
&= \sum_{\ell=1}^{N} V_{i\ell} V_{j\ell'}^{*} \\
&= \delta_{ij}.
\end{aligned}$$

The other relations are proven in a similar way.

2. Note that there is a quotient map $\pi\colon \mathcal{A}_u(N) \to \mathcal{A}_o(N)$ given by the quotient by the relations $V_{ij} = V_{ij}^{*}$ for all $1 \leqslant i, j \leqslant N$. The result therefore follows from the fact that $\mathcal{A}_o(N)$ is non-commutative for $N \geqslant 2$.

https://doi.org/10.1017/9781009345705.002 Published online by Cambridge University Press

3. Observe that $\mathcal{A}_u(1)$ is the quotient of $\mathbf{C}\langle X\rangle$ by the relations

$$XX^* = 1 = X^*X.$$

In particular, the relations make $\mathcal{A}_u(1)$ commutative, and we will show that it corresponds to the circle group

$$\mathbb{T} = \{z \in \mathbf{C} \mid |z| = 1\}.$$

Indeed, denoting by e_k the function $z \mapsto z^k$ for $k \in \mathbf{Z}$, we know that $(e_k)_{k\in\mathbf{Z}}$ is a basis of $\mathcal{O}(\mathbb{T})$. Therefore, there exists a linear map $\Phi\colon \mathcal{O}(\mathbb{T}) \to \mathcal{A}_u(1)$ sending e_k to X^k, and it is surjective by definition. Moreover, because $e_ke_\ell = e_{k+\ell}$ and $e_k^* = e_{-k}$, Φ is in fact a $*$-homomorphism. To conclude, simply observe that $\mathcal{O}(\mathbb{T})$ is generated by e_1, which satisfies $e_1^*e_1 = 1 = e_1e_1^*$, so that by universality there is a surjective $*$-homomorphism $\Psi\colon \mathcal{A}_u(1) \to \mathcal{O}(\mathbb{T})$ sending X to e_1. It is clear that Ψ is inverse to Φ, thence $\mathcal{A}_u(1) = \mathcal{O}(\mathbb{T})$. □

The pair $U_N^+ = (\mathcal{A}_u(N), U)$ is called a *quantum unitary group*. Once again, abelianisation provides a link with the classical unitary group, with the same caveat as in Remark 1.23. Even though concrete examples of unitary compact quantum groups are more difficult to deal with than orthogonal ones, most of the general theory is exactly the same (see Chapter 6). As a consequence, we will state and prove general results in the setting of unitary compact matrix quantum groups as soon as this does not entail any additional technicality in the proof. As for the other statements which require some adaptation, we will treat them in Chapter 6.