DIACONIS–SHAHSHAHANI UPPER BOUND LEMMA FOR FINITE QUANTUM GROUPS

J.P. MCCARTHY

Abstract. A central tool in the study of ergodic random walks on finite groups is the Upper Bound Lemma of Diaconis and Shahshahani. The Upper Bound Lemma uses the representation theory of the group to generate upper bounds for the distance to random and thus can be used to determine convergence rates for ergodic walks. The representation theory of quantum groups is remarkably similar to the representation theory of classical groups. This allows for a generalisation of the Upper Bound Lemma to an Upper Bound Lemma for finite quantum groups. The Upper Bound Lemma is used to study the convergence of ergodic random walks on the dual group $\hat{S}_n$ as well as on the truly quantum groups of Sekine.

Introduction

Let $\sigma_1, \sigma_2, \ldots, \sigma_k$ be a sequence of shuffles of a deck of cards. If the deck starts in some known order, the order of the deck after these $k$ shuffles is given by

$$\Sigma_k = \sigma_k \cdots \sigma_2 \cdot \sigma_1.$$ 

Suppose the shuffles are random variables independently and identically distributed as $\sigma_i \sim \nu \in M_p(S_{52})$, the set of probability distributions on $S_{52}$, then $\Sigma_k \sim \nu^k$ where $\nu^k$ is defined inductively as

$$\nu^k = \sum_{t \in G} \nu(\{st^{-1}\})\nu^k(\{t\}).$$

If $\nu$ is not concentrated on a subgroup, nor a coset of a normal subgroup of $S_{52}$, then as $k \to \infty$, $\nu^k \to \pi_{S_{52}}$, the uniform or random distribution on $S_{52}$.

This generalises to arbitrary finite groups. Given given independent and identically distributed $s_i \sim \nu \in M_p(G)$, not concentrated on a subgroup, nor a coset of a normal subgroup, as $k \to \infty$:

$$\xi_k = s_k \cdots s_2 \cdot s_1 \sim \nu^k \to \pi,$$

the random distribution on $G$. In this case the random walk is said to be ergodic.

2000 Mathematics Subject Classification. 46L53 (60J05, 20G42).

Key words and phrases. random walks, finite quantum groups, representation theory.
In the previous statement, convergence is with respect to the total variation distance:

$$\|\nu^k - \pi\| := \sup_{S \subset G} |\nu^k(S) - \pi(S)|.$$ 

The inspiration for this work, which is the subject of the author’s PhD thesis [10], is the following result of Diaconis and Shahshahani [4]:

**Theorem.** (Upper Bound Lemma). Let $\nu$ be a probability on a finite group $G$ and $k \in \mathbb{N}$. Then

$$\|\nu^k - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \text{Irr}(G) \setminus \tau} d_{\alpha} \text{Tr}((\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k) \quad \bullet$$

The sum is over non-trivial irreducible representations and $\hat{\nu}(\alpha)$ is the Fourier transform of $\nu$ at the representation $\rho^\alpha$

$$\hat{\nu}(\alpha) = \sum_{t \in G} \nu(t) \rho^\alpha(t).$$

As an application, Diaconis and Shahshahani show that $k_n = \frac{1}{2} n \ln n$ random transpositions is necessary and sufficient to ‘mix up’ a deck of $n$ cards. This result comprises two elements: an upper bound at $k_n + c n$ derived using the Upper Bound Lemma, as well as a lower bound at $k_n - c n$ derived using a carefully selected test set. A phenomenon occurs in this example that as $n \to \infty$, the lower bound for $k_n - c n$ tends to one for large $c$, and the upper bound for $k_n + c n$ approaches zero for large $c$. Note that $\frac{2c n}{k_n} \to 0$ so that as $n \to \infty$, the convergence from far from random to close to random is abrupt. This behaviour, called the cut-off phenomenon, occurs in a number of examples of random walks on finite groups. Saloff-Coste [15] is an excellent survey that includes more ideas even than the excellent monograph of Diaconis [3]. The author’s MSc thesis [11] also comprises a leisurely introduction to the subject.

Finite quantum groups are a noncommutative or ‘quantum’ generalisation of finite groups, and the central result of this work is that the Diaconis–Shahshahani Upper Bound Lemma also holds for finite quantum groups.

Considered as a research programme, quantum probability is concerned with generalising, where possible, objects in the study of classical probability to quantum objects in the study of quantum probability theory. It is under this programme that this work lies: the study of random walks on finite groups uses classical probability theory — a study of random walks on quantum groups should be the corresponding area of study in quantum probability.
Therefore, this work is concerned with a generalisation of a generalisation of card shuffling: generalising, where possible, the ideas and results of Diaconis and Shahshahani to the case of finite quantum groups. While the central object of card shuffling — the set of shuffles — is generalised to that of a set of elements of a group, the generalisation to quantum groups moves away from a ‘set of points’ interpretation.

However, in the study of random walks on finite quantum groups at least, the quantum theory generalises so nicely from the classical setup that it can be fruitful to refer to the virtual object that is a quantum group as if it really exists. At the very least this approach gives a most pleasing notation for quantum objects. At its very best it can inspire the noncommutative geometer to make good choices in terms of definitions, etc.

One of the most exciting and potentially lucrative aspects of quantum probability, or rather more specifically quantum group theory, is that theorems about finite groups may in fact be true for quantum groups also. For example, the classical finite Peter–Weyl Theorem concerning the matrix elements of representations of classical groups is exactly the same as the finite Peter–Weyl Theorem for finite quantum groups in the sense that replacing in the classical statement ‘finite group’ with ‘finite quantum group’ yields the quantum statement. What this really means is that the classical finite Peter–Weyl Theorem is actually just a special case of the quantum finite Peter–Weyl Theorem.

This is rather comforting on the conceptional level — these quantum objects behave so much like their ‘set of points’ classical counterparts — but in this study it is on the pragmatic level of proving results about these quantum objects that this principle really comes to the fore. On the one hand, some theorems concerning the theory of finite groups are just corollaries to results about quantum groups. On this other, pragmatic, hand, there is a translation principle: any proof of a classical group theorem, written without regard to any of the points in the ‘set of points’, may be directly translatable into a proof of the corresponding quantum group theorem.

For example, the Haar state, $h$, can allow classical ‘sum over points’ arguments and statements about the algebra of functions on a finite classical group to be translated:

$$\frac{1}{|G|} \sum_{t \in G} f(t) \quad = \quad h(f).$$

Representation Theory and ‘sum over points’ arguments, therefore, are translatable and it is precisely these ideas that play a central role in the representation-theoretic approach of Diaconis and Shahshahani to analysing the rate of convergence of random walks on finite groups. Once the quantum versions of the various objects and maps used by Diaconis and Shahshahani are established, it is largely straightforward to derive and prove the quantum Diaconis–Shahshahani Upper Bound Lemma.
The restriction to finite quantum groups is for two reasons. Firstly the classical work that this work is building upon is the Diaconis–Shahshahani Theory approach to random walks on finite groups. Secondly, the approach to finding the quantum versions of classical objects in this work — extolled in Section 1.1 — requires the isomorphism $\mathbb{C}(X \times Y) \cong \mathbb{C}X \otimes \mathbb{C}Y$ for sets $X$ and $Y$, and this holds only when $X$ and $Y$ are finite.

However, the classical Diaconis–Shahshahani Theory has been extended to possibly-infinite compact groups by Rosenthal [14]. Freslon [7, 8] has also extended this work on finite quantum groups, developed during the author’s PhD studies, to the far more technically-involved case of compact quantum groups, where the algebras are no longer necessarily finite dimensional. Freslon presents many interesting examples of random walks on compact quantum groups — with the cut-off phenomenon — and also addresses, particularly in [7], a number of concerns not answered or addressed in the author’s PhD thesis. As there is a generalisation of the classical finite symmetric group that is infinite dimensional for $n \geq 4$, it would be remiss not to point out that the restriction to finite quantum groups is more than a little unnatural, and also brushes many technical difficulties under the carpet.

Therefore this work should be considered a first, pioneering, attempt at a quantum generalisation of the work of Diaconis and Shahshahani, with Freslon’s papers a far more accomplished and reaching generalisation.

The paper is organised as follows. In Section 1, category theory language is used to motivate the definition of a finite quantum group. Results concerning the dual of a finite quantum group that are used in the sequel are presented at this point. Finally the definition of a random walk on a finite quantum group is given. In Section 2, the total variation distance, used for measuring the ‘distance to random’ of a random walk, is introduced. The central result is contained in Section 3; this leans so heavily on the work of Van Daele, that the author calls it by Diaconis–Van Daele Theory. In Section 4, two applications of the Upper Bound Lemma are presented: to a random walk on the dual of $S_n$; and to a random walk on the truly quantum groups of Sekine. In neither example is the cut-off phenomenon exhibited, and in the case of the random walk on the quantum groups of Sekine it is shown the cut-off phenomenon does not occur.

1. Preliminaries

1.1. Finite Quantum Groups. The following approach to introducing finite quantum groups is a brief summary of the approach outlined in detail in Section 2.2 of [10].

A finite classical group $G$ is an object in the category of finite sets, and the group multiplication $G \times G \to G$, inclusion of the unit, and inverse $G \to G$, are morphisms in this category. The three group axioms are given by three commutative diagrams.
Let $\mathbb{C}G$ be the complex vector space with basis elements $\{\delta^s : s \in G\}$. The map $G \mapsto \mathbb{C}G$ is a covariant functor, the $\mathbb{C}$ functor, from the category of finite sets to the category of finite dimensional complex vector spaces. The image of the group multiplication is a multiplication, $\nabla : \mathbb{C}G \otimes \mathbb{C}G \to \mathbb{C}G$ given by $\nabla(\delta^s \otimes \delta^t) = \delta^{st}$. The presence of the tensor product comes via the isomorphism $\mathbb{C}(G \times G) \cong \mathbb{C}G \otimes \mathbb{C}G$ which does not hold if $G$ is infinite. This gives $\mathbb{C}G$ the structure of a complex associative algebra called the \textit{group algebra} of $G$. The image of the three commutative diagrams (which comprise the group axioms) under the functor $\mathbb{C}$ give relations that hold in $\mathbb{C}G$, and if $\varphi = \sum_{t \in G} \alpha_t \delta^t$, then the involution

$$\varphi^* = \sum_{t \in G} \overline{\alpha_t} \delta^{t^{-1}}$$

gives the group algebra the structure of a $^*$-algebra.

Now apply the contravariant dual endofunctor to the group algebra. The dual endofunctor maps a finite dimensional complex vector space $U$ to its dual $U^*$, and a morphism $T : U \to V$ to a morphism $V^* \to U^*$ given by $f \mapsto f \circ T$. The dual of the group algebra is the algebra of functions on $G$, $F(G)$, with dual basis $\{\delta_s : s \in G\}$ such that $\delta_s(\delta^t) = \delta_{s,t}$, and involution $f^*(\delta^s) = \overline{f(\delta^s)}$. The composition of the $\mathbb{C}$ functor and the dual endofunctor gives a functor $G \mapsto F(G)$ and the images of the group multiplication, inverse, and inclusion of the unit, under this functor composition give structure maps on $F(G)$. These structure maps are called the \textit{comultiplication}, an algebra homomorphism $\Delta : F(G) \to F(G) \otimes F(G)$, $\delta_s \mapsto 1_{m^{-1}(s)} \equiv \sum_{t \in G} \delta_{st^{-1}} \otimes \delta_t$ (for finite $G$); the counit, $\varepsilon : F(G) \to \mathbb{C}$, $\delta_s \mapsto \delta_{s,1}$; and the antipode, $S : F(G) \to F(G)$, $\delta_s \mapsto \delta_{s^{-1}}$. The associativity, inverse, and identity group axiom commutative diagrams, under this functor, give \textit{coassociativity}, the \textit{counital property}, and the \textit{antipodal property}:

$$\begin{align*}
(\Delta \otimes I_{F(G)}) \circ \Delta &= (I_{F(G)} \otimes \Delta) \circ \Delta \\
(\varepsilon \otimes I_{F(G)}) \circ \Delta &= I_{F(G)} = (I_{F(G)} \otimes \varepsilon) \circ \Delta \\
M \circ (S \otimes I_{F(G)}) \circ \Delta &= \eta_{F(G)} \circ \varepsilon = M \circ (I_{F(G)} \otimes S) \circ \Delta
\end{align*}$$

Here $M : F(G) \otimes F(G) \to F(G)$ is pointwise multiplication and $\eta_{F(G)}$ is the inclusion of the unit, $1_G$. With the fact that $f^* f = 0$ if and only if $f = 0$, $F(G)$ can be given the structure of a finite dimensional $C^*$-algebra. It is a unital commutative algebra and the group axioms are encoded by these relations. Note furthermore that $\Delta$ satisfies $\Delta(f^*) = \Delta(f)^*$, where the involution in $F(G) \otimes F(G)$ is given by $(f \otimes g)^* = f^* \otimes g^*$. 
A finite dimensional C*-algebra $A$ with a *-homomorphism $\Delta : A \to A \otimes A$, and maps $\varepsilon : A \to \mathbb{C}$, and $S : A \to A$, that satisfies the above relations, but is not necessarily commutative is thus considered the algebra of functions on a finite quantum group. Such an algebra is called a C*-Hopf algebra.

**Definition 1.1.** An algebra of functions on a finite quantum group, is a unital C*-Hopf algebra $A$; that is a C*-algebra $A$ with a *-homomorphism $\Delta$, a counit $\varepsilon$, and an antipode $S$, satisfying the relations (1).

Denote an algebra of functions on a finite quantum group by $A =: F(G)$ and refer to $G$ as a finite quantum group, with unit denoted by $1_G$, and note that $S$ is an involution (not necessarily true for infinite $G$, see remark to Theorem 2.2, [21]). Timmermann presents in Chapter 1 further properties of Hopf algebras, for example the fact that the counit is a *-homomorphism (used in the sequel). The simplest noncommutative example of an algebra of functions on a finite quantum group is $C(S_3)$, where $S_3$ is the classical symmetric group on three elements, where the comultiplication is given by $\Delta_{C(S_3)}(\delta^\sigma) = \delta^\sigma \otimes \delta^\sigma$, and is the dual of the pointwise multiplication in $F(S_3)$. Where $\tau$ is the flip map $a \otimes b \mapsto b \otimes a$, this comultiplication has the property that $\tau \circ \Delta_{C(S_3)} = \Delta_{C(S_3)}$. Algebras of functions on finite quantum groups, $F(C)$, whose comultiplications have this property, $\tau \circ \Delta = \Delta$ are said to be cocommutative, and are of the form $F(C) = C G$ for $G$ a classical finite group. Similarly a commutative algebras of functions on a finite quantum group is the algebra of functions on some classical finite group (can be inferred from Theorem 3.3, [19]).

For the remainder of this work, unless explicitly stated otherwise, $G$ is a quantum group, and assumed finite. There are well established notions of compact and locally compact quantum groups. See, for example, Timmermann [18] for more.

### 1.2. The Dual of a Quantum Group.

Where $\pi$ is the random/uniform distribution on a classical group $G$, consider the functional on $F(G)$:

$$ f \mapsto \int_G f(t) \, d\pi(t) = \frac{1}{|G|} \sum_{t \in G} f(t). $$

This is a normalised, positive functional, invariant in the sense that for each $s \in G$,

$$ \int_G f(t) \, d\pi(t) = \int_G f(st) \, d\pi(t) = \int_G f(ts) \, d\pi(t) $$

$$ \Rightarrow 1_G \cdot \int_G f = \left( I_{F(G)} \otimes \int_G \right) \Delta(f) = \left( \int_G \otimes I_{F(G)} \right) \Delta(f). \quad (f \in F(G)) $$

This normalised, invariant, positive functional is called a Haar state, it is unique, and is denoted by $\int_G$ (earlier $h$ was used).
A finite quantum group also has a unique Haar state (Theorem 1.3, [21]), denoted by \( \int_G \). Invariance of the Haar state is given by (2) and furthermore it is tracial: \( \int_G ab = \int_G ba \) (Theorem 2.2, [21]).

Consider the space, \( \hat{A} \), of linear functionals on \( A := F(G) \) of the form \( b \mapsto \int_G ba \). As \( F(G) \) is finite dimensional, the continuous and algebraic duals coincide. Furthermore, the Haar state is faithful and so \( \langle a, b \rangle := \int_G a^* b \) defines an inner product making \( F(G) \) a Hilbert space. Via the Riesz Representation Theorem for Hilbert spaces, for every element \( \varphi \in F(G)' \), there exists a density \( a^*_\varphi \in F(G) \) such that:

\[
\varphi(b) = \langle a^*_\varphi, b \rangle = \int_G a^*_\varphi b, \quad (b \in F(G))
\]

so that \( F(G)' = \hat{A} \). This space can be given the structure of an algebra of functions on a finite quantum group by employing the contravariant dual functor to \( F(G) \) and its structure maps. The dual functor maps the object \( F(G) \) to \( \hat{A} \); the comultiplication \( \Delta : F(G) \to F(G) \otimes F(G) \) to an associative multiplication \( \nabla : \hat{A} \otimes \hat{A} \to \hat{A} \); and the multiplication \( M : F(G) \otimes F(G) \to F(G) \) to a comultiplication \( \hat{\Delta} : \hat{A} \to \hat{A} \otimes \hat{A} \) (see [10], Section 2.5 for more). The \( * \)-involution on \( \hat{A} \) is given by:

\[
\varphi^*(a) = \overline{\varphi(S(a)^*)}. \quad (\varphi \in \hat{A}, a \in F(G))
\]

The finite quantum group formed in this way is called the dual of the quantum group \( G \), and is denoted by \( \hat{G} \). An invariant, positive functional on \( F(\hat{G}) \) is given by \( \hat{h}(\varphi) = \varepsilon(a_\varphi) \).

In the case of a classical group \( G \), \( F(\hat{G}) = \mathbb{C}G \).

The analogue of a probability distribution on a classical group is a state on the algebra of functions on a quantum group, that is a positive functional of norm one. Denote the states on \( F(G) \) by \( M_p(G) \) and note that \( M_p(G) \) is a subset of \( F(\hat{G}) \). A density \( a_\nu \) defines a state \( \nu \in M_p(G) \) if and only if \( a_\nu \) is positive and \( \int_G a_\nu = 1 \). There are Convolution and Plancherel Theorems for \( F(\hat{G}) \) that will be used to prove the Upper Bound Lemma. The Convolution Theorem is well presented by Bhowmick, Skalski, and Soltan (Section 1.1, [2]), which heavily cites Van Daele [20, 21, 22, 23]; while the Plancherel Theorem is well presented by Timmermann (Section 2.3, [18]), which also cites Van Daele [21].
The convolution product on $F(G)$ is given by:

\[ a \otimes b = \left( \int_G \otimes I_{F(G)} \right) \left( ((S \otimes I_{F(G)}) \Delta(b)) (a \otimes 1_G) \right). \]

There is a Convolution Theorem relating this convolution to a convolution in $F(\hat{G})$:

\[ \varphi_1 \ast \varphi_2 := (\varphi_1 \otimes \varphi_2) \Delta. \quad (\varphi_1, \varphi_2 \in F(\hat{G})) \]

Within the proof of Proposition 3.11 of \[22\], Van Daele proves the following identity:

\[ S \left( \left( I_{F(G)} \otimes \int_G \right) (\Delta(a) (1_G \otimes b)) \right) = \left( I_{F(G)} \otimes \int_G \right) ((1_G \otimes a) \Delta(b)) \cdot (a, b \in F(G)) \]

This identity can be used to prove the following (see Section 1.1 of \[2\]):

**Theorem 1.2.** (Van Daele’s Convolution Theorem) For $\varphi_1, \varphi_2 \in F(\hat{G})$

\[ a_{\varphi_1 \ast \varphi_2} = a_{\varphi_1} \otimes a_{\varphi_2} \]

Timmerman (Lemma 2.3.8, \[18\]) presents a proof of the following lemma.

**Lemma 1.3.** Let $\varphi_1, \varphi_2 \in F(\hat{G})$. Then

\[ \hat{h}(\varphi_1 \varphi_2) = \varphi_1(S^{-1}(a_{\varphi_2})) \]

**Theorem 1.4.** (Plancherel Theorem) Let $G$ be a quantum group and $\varphi \in F(\hat{G})$. Then

\[ \hat{h}(\varphi^* \varphi) = \int_G a_{\varphi}^* a_{\varphi}. \]

**Proof.** Applying the previous lemma to the left-hand side:

\[ \hat{h}(\varphi^* \varphi) = \varphi^* (S^{-1}(a_{\varphi})) = \overline{\varphi(S(S^{-1}(a_{\varphi})))^*} \]

\[ = \varphi(a_{\varphi}^*) = \int_G a_{\varphi}^* a_{\varphi} = \int_G a_{\varphi}^* a_{\varphi} , \]

where the traciality of $\int_G$ was used.
1.3. Random Walks on Finite Quantum Groups. Early work on quantum stochastic processes by various authors led to random walks on duals of compact groups (particularly Biane, see [5] for references), and other examples, but Franz and Gohm [5] defined with clarity a random walk on a finite quantum group. Given a random walk on a finite classical group $G$, by applying the functor composition referenced in Section 1.1 to the random variables $\xi_k : G^k \to G$, random variables on the level of $F(G)$, $j_k : F(G) \to \otimes_k$ copies $F(G)$ can be defined by:

$$j_k(f) = f \circ \delta^{\xi_k},$$

and the generalisation to random walks on finite quantum groups can be made in this way. It is also possible to generalise from classical to quantum random walks using stochastic operators, and also $F(G)$ analogues of the random variables $s_i$ (denoted by $k_i$ by Franz and Gohm and $z_i$ by the author in [10]).

In Section 3.2 of [10], this generalisation of Franz and Gohm from random walks on finite classical groups to random walks on finite quantum groups is explored in detail, and concludes with Franz and Gohm’s assertion that a random walk on a finite quantum group $G$ driven by a state $\nu \in M_p(G)$ is essentially the same thing as the semigroup of convolution powers, $\{\nu^*\}$, defined inductively through

$$\nu^{*(k+1)} = (\nu \otimes \nu^*) \circ \Delta.$$

Indeed, Amaury Freslon defines a random walk on a (compact) quantum group simply as a state on $C(G)$, and proceeds to study the semigroup of convolution powers without mentioning the random variables $j_k$ nor $z_i$, only mentioning the stochastic operator $P_\nu = (\nu \otimes 1_{F(G)}) \circ \Delta$ for analytical reasons (see Section 4.2, [7]).

2. Total Variation Distance

In the classical case, the distance between $\nu$ and $\mu \in M_p(G)$ is given by the total variation distance:

$$\|\nu - \mu\| := \sup_{S \subseteq G} |\nu(1_S) - \mu(1_S)|.$$

Given a subset $S \subseteq G$, the indicator function on $S$, $1_S = \sum_{s \in S} \delta_s$, is a projection, and all projections in $F(G)$ are formed in this way, and so there is a one-to-one correspondence between projections in $F(G)$ and subsets of $G$. Using this correspondence, this definition can be extended to quantum groups:

$$\|\nu - \mu\| := \sup_{p \in F(G) \text{ a projection}} |\nu(p) - \mu(p)|.$$
The Haar state is a normal, faithful trace, therefore non-commutative $L^p$ machinery can be used to put $p$-norms on $F(G)$:

$$
\|a\|_p := \left( \int_G |a|^p \right)^{1/p} \quad (a \in F(G))
$$

Set the infinity norm equal to the operator norm.

**Proposition 2.1.** Let $G$ be a quantum group and $\nu, \mu \in M_p(G)$:

$$
\|\nu - \mu\| = \frac{1}{2} \|a_\nu - a_\mu\|_1.
$$

**Proof.** Standard non-commutative $L^p$ machinery from [13] shows that:

$$
\|a_\nu - a_\mu\|_1 = \sup_{\phi \in F(G): \|\phi\|_\infty \leq 1} \left| \int_G ((a_\nu - a_\mu) \phi) \right| = \sup_{\|\phi\|_\infty \leq 1} |\nu(\phi) - \mu(\phi)|.
$$

Embed the algebra of functions $F(G)$ into a matrix algebra. As everything is in finite dimensions, the supremum on the right is actually a maximum. Suppose that the two states $\nu$ and $\mu$ are given by density matrices: $\nu = \text{Tr}(\rho_\nu \cdot)$ and $\mu = \text{Tr}(\rho_\mu \cdot)$, and $\theta := \rho_\nu - \rho_\mu$ so that

$$
\|a_\nu - a_\mu\|_1 = \max_{\|\phi\|_\infty \leq 1} |\text{Tr}(\rho_\nu - \rho_\mu)\phi| = \max_{\|\phi\|_\infty \leq 1} |\text{Tr}(\theta\phi)|.
$$

Using the $M_n(\mathbb{C})$ inequality ($\|A\|_1 = \text{Tr}(|A|)$, $|A| := \sqrt{A^*A}$, $\text{Tr}(AB) \leq \|A\|_1 \|B\|_\infty$),

$$
\|a_\nu - a_\mu\|_1 = \max_{\|\phi\|_\infty \leq 1} |\text{Tr}(\theta\phi)|
$$

$$
\leq \max_{\|\phi\|_\infty \leq 1} \|\theta\|_1 \|\phi\|_\infty = \|\theta\|_1.
$$

Note that $\theta$ is self-adjoint so that there exists a polar decomposition $\theta = U|\theta|$ such that $U$ is self-adjoint. Consider $\phi = U$, the phase of $\theta$, so that $U\theta = |\theta|$, and so

$$
\text{Tr}(\theta U) = \text{Tr}(|\theta|) = \|\theta\|_1.
$$

that is equality is achieved at the self-adjoint unitary $U$:

$$
\|a_\mu - a_\nu\|_1 = |\nu(U) - \mu(U)|.
$$

Consider $q = \frac{1 + \sqrt{1 + 4U}}{2}$. The self-adjointness of $U$ gives $q = q^*$, and the fact $U$ is also a unitary implies that $U$ is an involution. This implies that $q = q^2$ and so $q$ is a projection. The projection distance satisfies

$$
\|\nu - \mu\| \geq |\nu(q) - \mu(q)| = \frac{1}{2} |\nu(U) - \mu(U)| = \frac{1}{2} \|a_\nu - a_\mu\|_1.
$$
Now suppose the projection distance is attained at \( p \) and consider the infinity-norm-one element \( \phi = 2p - 1_G \in F(G) \):

\[
\|a_\nu - a_\mu\|_1 \geq |\nu(2p - 1_G) - \mu(2p - 1_G)| = 2|\nu(p) - \mu(p)| = 2\|\mu - \nu\|
\]

\[
\Rightarrow \|\nu - \mu\| \leq \frac{1}{2}\|a_\nu - a_\mu\|_1
\]

This proof takes advantage of the finite dimensionality of \( F(G) \). Amaury Freslon ([7], Lemma 2.6) states and proves a similar result for \( \|\nu - \int_G\| \) which holds for not-necessarily finite-dimensional compact quantum groups whenever \( \nu \) is a state on \( L^\infty(G) \) that has an \( L^1(G) \)-density \( a_\nu \), which is not always the case in infinite dimensions.

The total variation distance defined using projections has three properties that suggest it is a suitable generalisation of the classical variation distance.

Firstly, in the case of a classical group, \( G \), the one-to-one correspondence between projections and subsets, and between probability measures on \( G \) and states on \( F(G) \), means that there is agreement in the classical case. Furthermore, there is a one-to-one correspondence between representations of a classical group \( G \) and corepresentations of \( F(G) \) and this implies that estimates of the distance to random are the same whether the classical or quantum Upper Bound Lemmas are used.

The Upper Bound Lemma is a formula for a two norm, and thus requires a Cauchy–Schwarz inequality to relate back to the total variation distance. Such an inequality for total variation distance is provided for by non-commutative \( \mathcal{L}^p \) machinery (see [13]):

\[
\|ab\|_1 \leq \|a\|_2\|b\|_2, \quad (a, b \in F(G))
\]

applied to

\[
\|\nu - \mu\|^2 = \frac{1}{4}\|a_\nu - a_\mu\|_1^2 = \frac{1}{4}\|(a_\nu - a_\mu)1_G\|_1^2
\]

\[
\leq \frac{1}{4}\|a_\nu - a_\mu\|_2^2\|1_G\|_2^2 = \frac{1}{4}\hat{h}((\nu - \mu)^* * (\nu - \mu))
\]

The final equality here is the Plancherel Theorem [13].

Finally, to establish lower bounds, the total variation distance has a presentation(s) as a supremum:

\[
(3) \quad \|\nu - \mu\| = \sup_{p \in F(G) \text{ a projection}} |\nu(p) - \mu(p)| = \frac{1}{2} \sup_{\|\phi\|_{\infty} \leq 1} |\nu(\phi) - \mu(\phi)|
\]
3. Diaconis–Van Daele Theory

3.1. Corepresentation Theory.

Definition 3.1. A corepresentation of the algebra of functions on a quantum group $G$ on a complex vector space $V$ is a linear map $\kappa : V \rightarrow V \otimes F(G)$ that satisfies:

\[
(\kappa \otimes I_{F(G)}) \circ \kappa = (I_V \otimes \Delta) \circ \kappa \quad \text{and} \quad (I_V \otimes \varepsilon) \circ \kappa = I_V.
\]

If $V$ is equipped with a Hermitian inner product, $\langle , \rangle_V$, define for $v, w \in V$, and $a, b \in F(G)$

\[
\langle v \otimes a, w \otimes b \rangle_{F(G)} = \langle v, w \rangle_V \cdot a^* b.
\]

A representation $\kappa$ on such a vector space is said to be unitary if $\langle \kappa(v), \kappa(w) \rangle_{F(G)} = \langle v, w \rangle_V \cdot 1_G$.

Let $\kappa$ be a corepresentation on a vector space $V$. Denote by $V^*$ the conjugate vector space of $V$ and by $v \mapsto \overline{v}$ the canonical conjugate-linear isomorphism. Since $\Delta$ and $\varepsilon$ are $\ast$-homomorphisms, the map $\kappa : V \rightarrow V \otimes F(G), \ e_j \mapsto \sum e_i \otimes \rho_{ij}^*$, is a representation again, called the conjugate of $\kappa$.

Denoting the map $a_\varphi \mapsto \varphi$ by $F$, so that $F(a_\varphi) = \varphi$, for each $a_\varphi \in F(G)$ define the map $\widehat{a_\varphi} \in L(V)$:

\[
\widehat{a_\varphi}(\kappa) = (I_V \otimes F(a_\varphi)) \circ \overline{\kappa} = (I_V \otimes \varphi) \circ \overline{\kappa}.
\]

Proposition 3.2. For $a_{\varphi_1}, a_{\varphi_2} \in F(G)$ and $\kappa$ a representation of $G$ on $V$

\[
\widehat{a_{\varphi_1} \ast \varphi_2}(\kappa) = \widehat{a_{\varphi_1}}(\kappa) \circ \widehat{a_{\varphi_2}}(\kappa).
\]

Furthermore, if $\kappa$ is unitary then

\[
\widehat{a_{\varphi^*}}(\kappa) = \widehat{a_\varphi}(\kappa)^*.
\]

Note the first involution is in $F(\hat{G})$ and the second is in $L(V)$.

Proof. The proposition is that the map $F(\hat{G}) \rightarrow L(V), \varphi \mapsto \widehat{a_\varphi}(\kappa)$ is a $\ast$-homomorphism. See Timmermann for a proof (Proposition 3.1.7 ii. and v., [18]) •

The following result is presented by Timmermann (Proposition 3.29 and Theorem 3.2.12, [18]), but is due to Woronowicz [25].
Theorem 3.3. (Finite Quantum Peter–Weyl Theorem) Let $\mathcal{I} = \text{Irr}(G)$ be an index set for a family of pairwise-inequivalent irreducible unitary representations of $G$. If $d_\alpha$ is the dimension of the vector space on which $\rho_\alpha$ acts ($\alpha \in \mathcal{I}$), 

$$\{\rho_\alpha^{ij} | i, j = 1 \ldots d_\alpha, \alpha \in \mathcal{I}\},$$

the set of matrix elements of $\mathcal{I}$, is an orthogonal basis of $F(G)$ with respect to the inner product

$$\langle a, b \rangle := \int_G a^* b, \quad (a, b \in F(G))$$

such that $\langle \rho_\alpha^{ij}, \rho_\alpha^{ij} \rangle = 1/d_\alpha$.

3.2. Fourier Transform. The following definition is similar to that of Simeng Wang ((2.5), [24]) save for a choice of left-right. As remarked upon by Simeng Wang, his definition is similar to earlier definitions of Kahng and also Caspers save for the presence of the conjugate representation $\kappa_\alpha$ rather than $\kappa_\alpha$ itself. As Wang explains, the conjugate representation is used to be compatible with standard definitions in classical analysis on compact groups and hence most welcome for this work.

Definition 3.4. (The Fourier Transform) Let $G$ be a quantum group with representation notation as before. Then the Fourier transform is a map:

$$F(G) \rightarrow \bigoplus_{\alpha \in \text{Irr}(G)} L(\overline{V}_\alpha), \quad a_\varphi \mapsto \hat{a}_\varphi,$$

defined for each $\alpha \in \text{Irr}(G)$:

$$\hat{a}_\varphi(\alpha) = (I_{\overline{V}_\alpha} \otimes F(a_\varphi)) \circ \overline{\kappa}_\alpha = (I_{\overline{V}_\alpha} \otimes \varphi) \circ \overline{\kappa}_\alpha.$$

Each $\hat{a}_\varphi(\alpha)$ is called the Fourier transform of $a_\varphi$ at the representation $\kappa_\alpha$. For $\varphi \in F(\hat{G})$:

$$\hat{\varphi}(\alpha) := \hat{a}_\varphi(\alpha) = (I_{\overline{V}_\alpha} \otimes \varphi) \circ \overline{\kappa}_\alpha,$$

so $\hat{\varphi}$ is identified with $\hat{a}_\varphi$.

The maps $\{\hat{a}_\varphi(\alpha) : \alpha \in \text{Irr}(G)\}$ play a key role in the sequel.

Theorem 3.5. (Diaconis–Van Daele Inversion Theorem) Let $\varepsilon$ be the counit of a quantum group $G$ and $\varphi \in F(\hat{G})$. Then

$$\hat{h}(\varphi) := \varepsilon(a_\varphi) = \sum_{\alpha \in \text{Irr}(G)} d_\alpha \text{Tr}(\hat{a}_\varphi(\alpha)),$$

where the sum is over the irreducible unitary representations of $F(G)$. 

Proof. Both sides are linear in $a_\varphi$ so it suffices to check $a_\varphi = \rho_\beta^\beta$ for $\beta \in \text{Irr}(G)$. The left-hand side reads

$$\varepsilon \left( \rho_\beta^\beta \right) = \delta_{k,l}.$$ 

To calculate the right-hand-side, calculate for a given representation the trace of $\hat{\rho}_\beta^\beta(\alpha)$. Let $\overline{e}_j \in \overline{V}_\alpha$ and calculate

$$\hat{\rho}_\beta^\beta(\alpha) \overline{e}_j = \left( I_{\overline{V}_\alpha} \otimes \mathcal{F} \left( \rho_\beta^\beta \right) \right) \sum_i \overline{e}_i \otimes (\rho^\alpha_{ij})^* = \sum_i \mathcal{F} \left( \rho_\beta^\beta \right) (\rho^\alpha_{ij})^* \overline{e}_i = \frac{1}{d_\beta} \delta_{j,k} \overline{e}_k$$

This is zero unless $\alpha \equiv \beta$. If $\alpha \equiv \beta$ then

$$\Rightarrow \text{Tr} \left( \hat{\rho}_\beta^\beta(\beta) \right) = \sum_j \langle \overline{e}_j, \hat{\rho}_\beta^\beta(\beta) \overline{e}_j \rangle_{\overline{V}_\beta} = \sum_j \langle \overline{e}_j, \frac{1}{d_\beta} \delta_{j,k} \overline{e}_k \rangle = \frac{1}{d_\beta} \delta_{k,l}.$$ 

Multiply this by $d_\beta$ to get $\delta_{k,l}$. 

Theorem 3.6. (Diaconis–Van Daele Convolution Theorem) For a representation $\kappa_\alpha$ of $G$ and $a_{\varphi_1}, a_{\varphi_2} \in F(G)$

$$a_{\varphi_1} \star a_{\varphi_2} (\alpha) = \hat{a}_{\varphi_1} (\alpha) \circ \hat{a}_{\varphi_2} (\alpha).$$

Proof. Recalling the identifications $\hat{a}_\varphi(\alpha) =: \mathcal{F}(a_\varphi)(\alpha) = \hat{\varphi}(\alpha)$, and that

$$\left( a_{\varphi_1} \star a_{\varphi_2} \right) (\alpha) = \left( I_{\overline{V}_\alpha} \otimes \mathcal{F} \left( a_{\varphi_1} \otimes a_{\varphi_2} \right) \right) \kappa_\alpha = \left( I_{\overline{V}_\alpha} \otimes \mathcal{F} \left( a_{\varphi_1 \star \varphi_2} \right) \right) \kappa_\alpha = \hat{a}_{\varphi_1 \star \varphi_2}(\alpha) = \hat{a}_{\varphi_1}(\alpha) \circ \hat{a}_{\varphi_2}(\alpha).$$

The second equality uses Van Daele’s Convolution Theorem [1,2] and final equality is Proposition 3.2. 

Lemma 3.7. Where the sum is over unitary irreducible representations,

$$\hat{h}(\varphi_1 \star \varphi_2) = \sum_{\alpha \in \text{Irr}(G)} d_\alpha \text{Tr} \left( \hat{a}_{\varphi_1}(\alpha) \hat{a}_{\varphi_2}(\alpha) \right). \quad (\varphi_1, \varphi_2 \in F(\hat{G}))$$
Proof. The proof uses the convolution theorem of Van Daele and the definition of $\hat{h}$ to find
\[ \hat{h} \left( \mathcal{F}(a_{\varphi_1}) \ast \mathcal{F}(a_{\varphi_2}) \right) = \hat{h} \left( \mathcal{F}(a_{\varphi_1} \circledast a_{\varphi_2}) \right) = \varepsilon \left( a_{\varphi_1} \circledast a_{\varphi_2} \right). \]
Now use the Diaconis–Van Daele Inversion Theorem 3.5 and the Diaconis–Van Daele Convolution Theorem 3.2
\[ \varepsilon \left( a_{\varphi_1} \circledast a_{\varphi_2} \right) = \sum_{\alpha \in \text{Irr}(G)} d_\alpha \Tr \left( \hat{a}_{\varphi_1} (\alpha) \hat{a}_{\varphi_2} (\alpha) \right). \]

Proposition 3.8. Suppose that $\nu \in M_p(G)$. If $\kappa_\tau$ is the trivial representation, $\lambda \mapsto \lambda \otimes 1_G$, then $\hat{a}_\nu (\tau) = I_\mathcal{G}$.

Proof. A calculation:
\[ \hat{a}_\nu (\tau) \lambda = (I_\mathcal{G} \otimes \nu) \overline{\kappa_\tau} (\lambda) = (I_\mathcal{G} \otimes \nu) (\lambda \otimes 1) = \lambda \otimes 1 \equiv \lambda \]

Proposition 3.9. Suppose that $\kappa_\alpha$ is a non-trivial and irreducible unitary representation, then $\hat{1}_G (\alpha) = 0$.

Proof. Another calculation:
\[ \hat{1}_G (\alpha) \overline{\epsilon}_j = (I \otimes \mathcal{F}(1_G)) \sum_i \overline{\epsilon}_i \otimes (\rho_{ij}^\alpha)^* = \sum_i \overline{\epsilon}_i \mathcal{F}(1_G) (\rho_{ij}^\alpha)^* = \sum_i \int_G ((\rho_{ij}^\alpha)^* \cdot \overline{\epsilon}_i). \]
Note that $1_G$ is the matrix element of the trivial representation and $\alpha$ is not equivalent to the trivial representation. Therefore, by the orthogonality relation $\hat{1}_G (\alpha) = 0$.

3.3. The Upper Bound Lemma. At this point, to mirror the classical notation, use $\pi$ for $\int_G$. Recall, from Section 2, that
\[ \| \nu - \pi \|^2 \leq \frac{1}{4} \hat{h} ((\nu - \pi)^* (\nu - \pi)). \quad (\nu, \mu \in F(\hat{G})) \]

Lemma 3.10. (Diaconis–Shahshahani Upper Bound Lemma) Let $\nu \in M_p(G)$. Then
\[ \| \nu^k - \pi \|^2 \leq \frac{1}{4} \sum_{\alpha \in \text{Irr}(G) \setminus \{\tau\}} d_\alpha \Tr \left[ (\hat{\nu}(\alpha))^k (\hat{\nu}(\alpha))^k \right], \]
where the sum is over all non-trivial irreducible unitary representations.
Proof. Noting that $a_\pi = 1_G$ write
\[
\hat{h} ((\nu - \pi) \ast (\nu - \pi)) = \hat{h} (\mathcal{F} (a_\nu - 1_G)^* \mathcal{F} (a_\nu - 1_G)).
\]
Now using Lemma 3.7 and (4), this is equal to
\[
\hat{h} ((\nu - \pi) \ast (\nu - \pi)) = \sum_{\alpha \in \text{Irr}(G)} d_\alpha \text{Tr} \left[ \widehat{(a_\nu - 1_G)} (\alpha)^* (a_\nu - 1_G)(\alpha) \right].
\]
Now note that
\[
\widehat{(a_\nu - 1_G)} (\alpha) = \hat{a}_\nu (\alpha) - \hat{1}_G (\alpha).
\]
If $\alpha = \tau$, the trivial representation, then this yields zero as both terms are the identity on $\mathbb{C}$. If $\alpha$ is non-trivial, then $\hat{1}_G (\alpha) = 0$ and thus (using the notation $\hat{a}_\nu (\alpha) = \hat{\nu}(\alpha)$):
\[
\|\nu - \pi\|^2 \leq \frac{1}{4} \hat{h} ((\nu - \pi) \ast (\nu - \pi)) = \frac{1}{4} \sum_{\alpha \in \text{Irr}(G) \setminus \{\tau\}} d_\alpha \text{Tr} [\hat{\nu} (\alpha)^* \hat{\nu} (\alpha)].
\]
Apply the Diaconis–Van Daele Convolution Theorem 3.6 $k$ times $\bullet$

Note this is exactly the same as the classical Diaconis–Shahshahani Upper Bound Lemma.

3.4. Lower Bounds.

Lemma 3.11. (Lower Bound Lemma) Suppose that $\nu \in M_p(G)$ and $\rho$ the matrix element of a non-trivial one dimensional representation. Then
\[
\|\nu^* - \pi\| \geq \frac{1}{2} |\nu(\rho)|^k.
\]
Proof. Starting with (3), note that the argument from Proposition 3.9 shows that $\rho$ has zero expectation under the random distribution. Note also that $\rho$ is unitary (Proposition 3.1.7 v., [18]), thus norm one and thus a suitable test function.

Note that for a one dimensional representation, by the Convolution Theorem 3.6
\[
|\nu^k(\rho)| = |\nu^k(\rho)| = |\nu^k(\rho)| = |\nu(\rho)|^k = |\nu(\rho)|^k \cdot
\]
4. Examples

4.1. Random Walks on Dual Groups. Consider the dual quantum group, $\hat{G}$, of a not-necessarily abelian group, $G$, given by $F(\hat{G}) := CG$. States on $F(\hat{G})$ are given by positive definite functions $u \in F(G) = \hat{CG}$ (see Bekka, de la Harpe and Valette (Proposition C.4.2., [1])). Furthermore, there is a correspondence between positive definite functions and unitary representations on $G$ together with a vector. In particular, for each positive definite function $u$ there exists a unitary representation $\rho : G \to GL(V)$ and a vector $\xi \in V$ such that

\begin{equation}
    u(s) = \langle \rho(s)\xi, \xi \rangle,
\end{equation}

and for each unitary representation and vector (5) defines a positive definite function on $G$. For $u$ to be a state it is required that $u(e) = 1$ and so $\langle \xi, \xi \rangle = 1$; i.e. $\xi$ is a unit vector. Therefore probabilities on $\hat{G}$ can be chosen by selecting a given representation and unit vector.

Since $\Delta(\delta^s) = \delta^s \otimes \delta^s$, it follows that $\kappa_s(\lambda) = \lambda \otimes \delta^s$ defines a (co)representation (with $\tau = \kappa_e$), and thus all irreducible representations are of this form by counting. This makes the application of the upper bound lemma straightforward. Let $u \in M_p(\hat{G})$ so that $\hat{u}(\kappa_s) = u(s)$ and so

\[ \hat{u}(\kappa_s)^* \hat{u}(\kappa_s) = |u(s)|^2. \]

Therefore the upper bound lemma yields:

\[ \|u^{*k} - \pi\|^2 \leq \frac{1}{4} \sum_{t \in G \setminus \{e\}} |u(t)|^{2k}. \]

4.1.1. A Walk on $\hat{S}_n$. Consider the quantum group $\hat{S}_n$ (given by $F(\hat{S}_n) := CS_n$) with a state $u \in M_p(\hat{S}_n)$ given by the permutation representation on $\mathbb{C}^n$ given by $\pi(\sigma)(e_i) = e_{\sigma(i)}$ together with the unit vector $\xi$ with components

\[ \alpha_i = \sqrt{n^{n-i} - 1}. \]

This vector is such that the $\alpha_i$ are in geometric progression with common ratio $\frac{1}{\sqrt{n}}$. For large $n$, this vector is approximately given by:

\[ \xi \approx \left(1, \frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n^2}}, \cdots \right) \approx (1, 0, 0, \ldots). \]

Following this through

\[ u(\sigma) \approx \begin{cases} 
1 & \text{if } \sigma(1) = 1, \\
0 & \text{otherwise.} 
\end{cases} \]
To establish the upper bound some elementary inequalities will be used.

**Lemma 4.1.** The following hold for $n \geq 5$:

(6) \[ \left( \frac{4}{n} \right)^k (n-1) \leq 1, \text{ for } k > n^{n-1} \ln(n)/2, \]

(7) \[ \sqrt{\ln(n-1) - n + 2} \leq 0, \]

(8) \[ A_n = \frac{(n-1)(\sqrt{n}-1)^2}{n^{n-1}} \rightarrow 1^{-} \text{ monotonically,} \]

(9) \[ g(n) = \frac{(\sqrt{n}-1)^2}{n^{n-1}} \rightarrow 1^{-} \text{ monotonically.} \]

**Proof.** For (6), note that $k > n^{n-1} \ln(n)/2$ and thus $\left( \frac{4}{n} \right)^k (n-1) \leq n \left( \frac{4}{n} \right)^{n^2 \ln(n)/2} := h(n)$.

Note that $h(5) < 1$ and

\[ \frac{d}{dn} \ln(h(n))) = n^2 \ln(n) \left[ \ln \left( \frac{4}{n} \right) \right] + n^2 \left[ \ln \left( \frac{2e^{1/n^2}}{n} \right) \right] < 0, \]

while (7) is trivial. Note that $A_n \rightarrow 1$ and

\[ \frac{(n^n-1)^2}{n^{n-3}(\sqrt{n}-1)} \frac{dA_n}{dn} = n^n(n-2) + n^2 \sqrt{n(n^{n-2}-(\ln n+1))} + n \ln n(n-1) \]
\[ + n(n-2) + \sqrt{n(n \ln n-1)} + n\sqrt{n} + 2 > 0 \]

for $n \geq 3$, and so the convergence is monotonic. Also $g(n) \rightarrow 1$ and

\[ \frac{(n^n-1)^2}{n^{n-5/2}(\sqrt{n}-1)} g'(n) = n^2(n^{n-2}\sqrt{n}-(\ln n+1)) + \sqrt{n(n \ln n+n-1)} > 0 \]

for $n \geq 3$.

**Upper Bounds.** For $k = \alpha n^{n-1} \ln(n)/2 + cn^{n-2}$, $\alpha > 1$, and $n$ large

\[ \| u^*k - \pi \|^2 \leq \frac{1}{2} e^{-2Ac} \]

where $A$ can be chosen to be any $A < 1$ for $n$ sufficiently large.

**Proof.** Note that

\[ u(\sigma) = \langle \xi, \pi(\sigma)\xi \rangle = \frac{n^{n+1} - n^n}{n^n - 1} \sum_{i=1}^{n} \frac{1}{\sqrt{n^{i+\sigma(i)}}}. \]
Therefore, using the Upper Bound Lemma,
\[ \|u^k - \pi\|^2 \leq \frac{1}{4} \left( \frac{n^{n+1} - n^n}{n^n - 1} \right)^{2k} \sum_{\sigma \in S_n \setminus \{e\}} \left[ \sum_{i=1}^{n} \frac{1}{\sqrt{n^{i+\sigma(i)}}} \right]^{2k}. \]

Define for \( a_i = \frac{1}{\sqrt{n^i}} \)
\[ S(\sigma) = \sum_{i=1}^{n} a_i a_{\sigma(i)}. \]

An inversion is an ordered pair \((j, k)\) with \(j, k \in \{1, \ldots, n\}\) with \(j < k\) and \(\sigma(j) > \sigma(k)\). All non-identity permutations have at least one inversion.

Taking the approach of Steele ([17], P. 79), for any inversion \((j, k)\) define a new permutation by
\[ \tau_1(i) := (j \ k)\sigma(i) = \begin{cases} \sigma(i) & \text{if } i \neq j, k, \\ \sigma(j) & \text{if } i = k, \\ \sigma(k) & \text{if } i = j. \end{cases} \]

Steele shows that
\[ S(\sigma) \leq S(\tau_1). \]

That is, multiplying by \((j \ k)\), whenever \((j, k)\) is an inversion, in this fashion, increases the number of fixed points, reduces the number of inversions and increases \(S\). This can always be done until \(\tau_r = e\). If the maximising \(\sigma \in S_n / \{e\}\) were not a transposition, then it would be the product of at least two transpositions. Take one of the transpositions \((j \ k)\): it is certainly an inversion. By the referenced calculation, \(\tau_i := (j \ k)\sigma\) has \(S(\tau_i) \geq S(\sigma)\). Therefore, no matter what the starting permutation \(\sigma\), \(\tau_{r-1}\) is a transposition and therefore to maximise \(S\) on \(S_n \setminus \{e\}\) one just maximises over transpositions.

The one-step differences between the \(a_i\) is decreasing in \(i\) and so the smallest one-step difference is between \(a_{n-1}\) and \(a_n\). Let \((j \ k)\) be a transposition with \(j < k\). Note that
\[ S((n-1 \ n)) - S((j \ k)) = a_j^2 + a_k^2 + 2a_{n-1}a_n - a_{n-1}^2 - a_n^2 - 2a_ja_k = (a_j - a_k)^2 - (a_n - a_{n-1})^2 \geq 0, \]
so that \(S\) is maximised at \((n-1 \ n)\).

Partition \(S_n \setminus \{e\}\) into \(F_1\) and \(F_1^C\) where \(F_1\) is the set of permutations with \(\sigma(1) = 1\). On \(F_1\),
\[ S(\sigma) \leq S((n-1 \ n)) = \frac{1}{n} \frac{n^n - n^2}{n-1} + \frac{2\sqrt{n}}{n^n} =: f_0. \]
Now consider the maximum of $S$ on $F_1^C$. From Steele's argument [17], it is known that strictly increasing the number of fixed points (by multiplying by suitably chosen transpositions), increases $S$. Also, if written in the disjoint cycle notation, elements of $F_1^C$ must contain a cycle of the form $(1 \ i_2 \ldots \ i_N)$. By multiplying by suitably chosen transpositions, any disjoint cycle not containing 1 may be factored out whilst increasing $S$. Then write

$$(1 \ i_2 \ldots \ i_N) = (1 \ i_N)(1 \ i_{N-1})\ldots(1 \ i_2),$$

so that the maximum of $S$ on $F_1^C$ occurs at an element of the form

$$\sigma = \prod_{k=N}^{2} (1 \ i_k).$$

All transpositions are inversions therefore can be removed — all the time increasing $S$ — until one gets a transposition of the form $(1 \ i)$. The maximum must occur at such a transposition. Note that

$$S((1 \ 2)) - S((1 \ i)) = 2a_1a_2 + a_1^2 - 2a_1a_i - a_i^2 = (a_1 - a_i)^2 - (a_1 - a_2)^2 \geq 0.$$ 

Therefore $S(1 \ i) \leq S(1 \ 2)$ and for any $\sigma \in F_1^C$:

$$S(\sigma) \leq S(1 \ 2) = \frac{2\sqrt{n}}{n^2} + \frac{1}{n^2 n(n-1)} =: f_1.$$ 

For $n \geq 4$, $f_1 \leq 2f_0/\sqrt{n}$ as

$$\frac{2}{\sqrt{n}}f_0 - f_1 \leq \frac{1}{n^2 n(n-1)} [n^3 \sqrt{n}((n^3 - 2) + n^{n-4}(n - \sqrt{n})) + n^2 (4n - 3)] \geq 0.$$ 

Therefore the Upper Bound Lemma yields:

$$\|u^k - \pi\|^2 \leq \frac{1}{4} \left( \frac{n^{n+1} - n^n}{n^{n-1}} \right)^{2k} \left( \sum_{\sigma \in F_1} S(\sigma)^{2k} + \sum_{\sigma \in F_1^C} S(\sigma)^{2k} \right).$$

It is shown in the author’s PhD thesis ([10], p. 93) that this yields:

(10)

$$\|u^k - \pi\|^2 \leq \frac{1}{4} \left( 1 - \frac{(n-1)(\sqrt{n} - 1)^2}{n^{n-1}} \right)^{2k} \sqrt{n - 1}(n - 1)^{n-1} e^{2-n} \left[ 1 + \left( \frac{4}{n} \right)^k (n - 1) \right].$$

Using (6), and $(1 - x) \leq \exp(-x)$, a rewriting yields:

$$\|u^k - \pi\|^2 \leq \frac{1}{2} \exp \left( -2k \frac{(n-1)(\sqrt{n} - 1)^2}{n^{n-1}} + (n - 1) \ln(n - 1) \right) \times \exp \left( \ln(\sqrt{n} - 1) - n + 2 \right).$$
By (7) the second exponential is less than one. Writing \( k = \alpha n^{n-1} \ln(n)/2 + c n^{n-2} \) and rewriting again

\[
\|u^k - \pi\| \leq \frac{1}{2} \exp\left(-2c \frac{(n-1)(\sqrt{n} - 1)^2}{n^n - 1}\right) \times \\
\exp\left((n-1) \ln(n-1) - \alpha(n-1) \ln(n) \left(\frac{\sqrt{n} - 1)^2}{n^n - 1}\right)\right)
\]

Note that for \( \alpha > 1 \) and \( n \) sufficiently large by (9)

\[
(n-1) \ln(n-1) (1 - \alpha g(n)) \leq 0
\]

\[
\Rightarrow (n-1) \ln(n-1) \leq \alpha (n-1) \ln(n-1) g(n)
\]

\[
\Rightarrow (n-1) \ln(n-1) - \alpha (n-1) \ln(n) g(n) \leq 0,
\]

and the result follows.

If there were an effective lower bound for the total variation distance for \( k = n^{n-1} \ln(n)/2 - c n^{n-2} \), and if such a bound approached one for large \( c \), then the cut-off phenomenon would be exhibited for this random walk. Unfortunately no such result is at hand, but the following gives a partial result, showing that the random walk is still far from random for small multiples of \( n^{n-2} \). The following will be used.

**Lemma 4.2.** The following hold for, respectively, \( 0 < x < 1/2 \) and \( n \geq 2 \):

1. \( 1 - x \geq e^{-x^2 - x} \),
2. \( B_n = \frac{n^n}{n^n - 1} \left(\frac{n^2}{n^n - 1} + 1\right) \rightarrow 1^+ \) monotonically.

**Proof.** The bound (11) is (10), Lemma 5.5.1 with \( n = 1 \). Note that \( B_n \rightarrow 1, B_2 > 1 \), and note

\[
\frac{(n^n - 1)^3 dB_n}{n^n} = n^n[2n - (1 + \ln n)(n^2 + 1)] - (1 + \ln n)n^2 - (2n - (1 + \ln n)) < 0
\]
Lower Bounds. For \( k = \alpha n^{-2} \), \( \alpha > 0 \), and \( n \) large
\[
\| u^* - \pi \| \geq \frac{1}{2} e^{-Bn}
\]
where \( B \) can be chosen to be any \( B > 1 \) for sufficiently large \( n \).

**Proof.** Using the Lower Bound Lemma 3.11 with the matrix element \( \delta^{(n-1)} \), using a calculation from the PhD thesis \([10]\), p. 95), together with (11),
\[
\| u^* - \pi \| \geq \frac{1}{2} \left| 1 - \frac{(n-1)(\sqrt{n-1})^2}{n^{n-1}} \right|^{\alpha n^{-2}}
\]
\[
\geq \frac{1}{2} \exp \left[ \left( -\frac{(n-1)^2(\sqrt{n-1})^2}{n^{n-1}} - \frac{(n-1)(\sqrt{n-1})^2}{n^{n-1}} \right) \alpha n^{-2} \right]
\]
\[
\geq \frac{1}{2} \exp \left[ \left( -\frac{n^2 n^n}{(n-1)^2} - \frac{n^n}{n-1} \right) \alpha \right]
\]
\[
= \frac{1}{2} \exp \left[ \left( \frac{n^n}{n-1} - \left( \frac{n^n}{n-1} + 1 \right) \right) \alpha \right] = B_n
\]


4.2. A Family of Walks on the Sekine Quantum Groups.

4.2.1. Sekine Quantum Groups. Y. Sekine \([16]\) introduced a family of finite quantum groups of order \( 2n^2 \) that are neither commutative nor cocommutative.

The following follows the presentation of Franz and Skalski \([6]\) rather than of Sekine. Let \( n \geq 3 \) be fixed and \( \zeta_n = e^{2\pi i/n} \) and
\[
\mathbb{Z}_n = \{0, 1, \ldots, n-1\},
\]
with addition modulo \( n \).

Consider \( n^2 \) one-dimensional spaces \( \mathbb{C} e_{(i,j)} \) spanned by elements indexed by \( \mathbb{Z}_n \times \mathbb{Z}_n \), \( \{ e_{(i,j)} : i, j \in \mathbb{Z}_n \} \). Together with a copy of \( \mathbb{M}_n(\mathbb{C}) \), spanned by elements \( E_{ij} \) indexed by \( \{(i,j) : i, j = 1, \ldots, n, 0 \equiv n \} \), a direct sum of these \( n^2 + 1 \) spaces, the \( 2n^2 \) dimensional space
\[
A_n = \left( \bigoplus_{i,j \in \mathbb{Z}_n} \mathbb{C} e_{(i,j)} \right) \oplus \mathbb{M}_n(\mathbb{C}),
\]
can be given the structure of the algebra of functions on a finite quantum group denoted by $Y_n$ (so that $A_n = F(Y_n)$). On the one dimensional elements the comultiplication is given by, for $i, j \in \mathbb{Z}_n$:

$$\Delta(e_{(i,j)}) = \sum_{\ell, m \in \mathbb{Z}_n} (e_{(\ell,m)} \otimes e_{(i-\ell,j-m)}) + \frac{1}{n} \sum_{\ell, m = 1}^n (\zeta_n^{(i-\ell)m} E_{\ell,m} \otimes E_{\ell+j,m+j}) \cdot$$

On the matrix elements in the $M_n(\mathbb{C})$ factor:

$$\Delta(E_{i,j}) = \sum_{\ell, m \in \mathbb{Z}_n} (e_{(-\ell,-m)} \otimes \zeta_n^{(i-j)} E_{i-m,j-m}) + \sum_{\ell, m \in \mathbb{Z}_n} (\zeta_n^{(j-i)} E_{i-m,j-m} \otimes e_{(\ell,m)})$$

The antipode is given by $S(e_{(i,j)}) = e_{(-i,-j)}$ on the one dimensional factors and the transpose for the $M_n(\mathbb{C})$ factor. Sekine does not give the counit but by noting that $u(0,0) = I_n$ (where $U \in M_n(M_n(\mathbb{C}))$ is defined in Sekine’s original paper), it can be seen that the coefficient of the $e_{(0,0)}$ one-dimensional factor satisfies the counital property. The Haar state $\int_{Y_n} \in M_p(Y_n)$ is given by:

$$\int_{Y_n} \left( \sum_{i,j \in \mathbb{Z}_n} x_{(i,j)} e_{(i,j)} + a \right) = \frac{1}{2n^2} \left( \sum_{i,j \in \mathbb{Z}_n} x_{(i,j)} + n \cdot \text{Tr}(a) \right).$$

Although Sekine restricts the construction to $n \geq 3$, for $n = 1$ and $n = 2$ the construction still satisfies the conditions of Kac and Paljutkin and so are algebras of functions of quantum groups. Sekine does not clarify but the construction for $n = 2$ does not give the celebrated Kac–Paljutkin quantum group of order eight and indeed $Y_2$ is commonly mistaken for the Kac–Paljutkin quantum group in the literature. In fact, $Y_2$ is the dual group $\hat{D}_4$ while $Y_1$ is the classical group $\mathbb{Z}_2$.

To use the quantum Diaconis–Shahshahani Upper Bound Lemma, the representation theory of the quantum group must be well understood. The representation theory of the Sekine quantum groups changes according to the parity of the parameter $n$ and the below restricts to $n$ odd.

4.2.2. Representation Theory for $n$ Odd. For $n$ odd there are $2n$ one dimensional representations and $\binom{n}{2}$ two dimensional representations. Consider the convolution algebra $(F(Y_n), \ast_{F(Y_n)})$. Sekine gives $2n$ minimal one-dimensional central projections, $\binom{n}{2}$ minimal two-dimensional central projections, and matrix units in the two-dimensional subspaces. Sébastien Palcoux (private communication, March 2016) suggests a connection between projections and matrix units in the convolution algebra and the comultiplication in the algebra of functions. Palcoux’s approach uses slightly different Fourier transforms and convolutions — and the language of planar algebras (see [12]) — therefore his results could not be used directly. However it was possible to show that the one-dimensional central projections in $(F(Y_n), \ast_{F(Y_n)})$ were the matrix elements of the one dimensional
representations, while the two-dimensional central projections were, up to a factor of two, the matrix elements of the irreducible two-dimensional representations (see the appendix to [10] for the brute-force verification). As far as the author knows this was not explicitly stated in the existing literature.

Let \( \ell \in \{0, 1, \ldots, n - 1\} \). Then

\[
\rho_{\ell}^{\pm} = \sum_{i,j \in \mathbb{Z}_n} \zeta_n^{i\ell} e_{(i,j)} \pm \sum_{m=1}^{n} E_{m,m+\ell},
\]

are the \( 2n \) matrix elements of the one dimensional representations so that

\[
\kappa_{\ell}^{\pm}(\lambda) = \lambda \otimes \rho_{\ell}^{\pm} \quad \text{and} \quad \Delta(\rho_{\ell}^{\pm}) = \rho_{\ell}^{\pm} \otimes \rho_{\ell}^{\pm}.
\]

Note that \( \rho_{0}^{+} = 1_{Y_{n}} \) is the matrix element of the trivial representation.

Now let \( u \in \{0, 1, \ldots, n - 1\} \) and \( v \in \{1, 2, \ldots, (n - 1)/2\} \). Each pair gives a two-dimensional representation \( \kappa_{u,v} : \mathbb{C}^2 \to \mathbb{C}^2 \otimes F(Y_{n}) \) with matrix elements:

\[
\begin{pmatrix}
\rho_{11}^{u,v} & \rho_{12}^{u,v} \\
\rho_{21}^{u,v} & \rho_{22}^{u,v}
\end{pmatrix} = \begin{pmatrix}
\sum_{i,j \in \mathbb{Z}_n} \zeta_n^{iu+jv} e_{(i,j)} & \sum_{m=1}^{n} \zeta_n^{-mv} E_{m,m+u} \\
\sum_{m=1}^{n} \zeta_n^{mv} E_{m,m+u} & \sum_{i,j \in \mathbb{Z}_n} \zeta_n^{iu-jv} e_{(i,j)}
\end{pmatrix}.
\]

4.2.3. States on the Sekine Quantum Groups. Consider the basis of \( F(\hat{Y}_{n}) \) dual to \( \{e_{(i,j)} : i, j \in \mathbb{Z}_n\} \cup \{E_{i,j} : i, j = 1, 2, \ldots, n\} \) given by

\[
e_{(i,j)} e_{(r,s)} = \delta_{i,r} \delta_{j,s} \quad \text{and} \quad E_{i,j} e_{(r,s)} = 0,
\]

and

\[
e_{(i,j)} E_{r,s} = 0, \quad E_{i,j} E_{r,s} = \delta_{i,r} \delta_{j,s}.
\]

Let \( \mu \in F(\hat{Y}_{n}) \):

\[
\mu = \sum_{i,j \in \mathbb{Z}_n} x_{(i,j)} e_{(i,j)} + \sum_{p,q=1}^{n} a_{p,q} E^{p,q}.
\]

Franz and Skalski [6] show that \( \mu \in M_{p}(Y_{n}) \) if and only if

- \( x_{(i,j)} \geq 0 \) for all \( i, j \in \mathbb{Z}_n \),
- the matrix \( A = (a_{pq}) \) is positive,
- \( \text{Tr}(\mu) := \sum_{i,j \in \mathbb{Z}_n} x_{(i,j)} + \sum_{p=1}^{n} a_{p,p} = 1 \).
4.2.4. A Random Walk. Where \( n \) is odd, and \( J_n = \sum_{p,q=1}^n E_{p,q} \in M_n(\mathbb{C}) \) the matrix of all ones, consider the state

\[
\nu = \frac{1}{8} (e^{(0,1)} + e^{(1,0)} + e^{(-1,0)} + e^{(0,-1)}) + \frac{1}{2n} J_n \in M_p(Y_n).
\]

The Diaconis–Shahshahani Upper Bound Lemma gives:

\[
\|\nu^{*k} - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \text{Irr}(Y_n) \setminus \{\tau\}} d_{\alpha} \text{Tr} \left[ (\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k \right]
\]

**Proposition 4.3.** For \( k = \alpha n^2 \), with \( \alpha > 1/20 \) and \( n \geq 3 \)

\[
\frac{1}{2} e^{-\alpha \pi^2/2} \leq \|\nu^{*k} - \pi\| \leq c_n e^{-\alpha \pi^2/4},
\]

with \( c_n \to 1 \) as \( n \to \infty \).

**Proof.** For the Upper Bound, consider first the one-dimensional representations \( \kappa_\ell^\pm \) (except the trivial representation \( \kappa_0^+ \)).

\[
\nu(\rho_\ell^\pm) = \frac{1}{8} (\zeta_n^\ell + \zeta_{-n}^\ell + 2) \pm 2 = \begin{cases} 
\frac{1}{2} \left( \cos^2 \left( \frac{\pi \ell}{n} \right) + 1 \right) & \text{if } \pm = + \\
-\frac{1}{2} \sin^2 \left( \frac{\pi \ell}{n} \right) & \text{if } \pm = - \\
0 & \text{for } \kappa_\ell^\pm = \kappa_0^-
\end{cases}.
\]

Note that the \( \kappa_\ell^+ \) will dominate to such an extent that very trivial bounds may be used on the other terms.

The contribution to (15) from the \( \kappa_\ell^+ \) is given by

\[
\frac{1}{4} \sum_{\alpha = \kappa_\ell^+} d_{\alpha} \text{Tr} \left[ (\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k \right] = \frac{1}{4} \sum_{\ell=1}^{n-1} |\nu(\rho_\ell^+)|^{2k} = \frac{1}{4} \sum_{\ell=1}^{n-1} \left( \frac{1}{2} \left( \cos^2 \left( \frac{\pi \ell}{n} \right) + 1 \right) \right)^{2k}.
\]

Using the symmetry of \( \cos^2(x) \) about \( x = \pi/2, \cos x \leq e^{-x^2/2} \) on \([0, \pi/2] \) (Theorem 2, p. 26, [3]), and employing the following inequality:

\[
\frac{1}{2} (\cos^2 x + 1) \leq \frac{1}{2} (\cos x + 1) = \left( \cos \left( \frac{x}{2} \right) \right)^2 \leq \left( e^{-x^2/2}/2 \right)^2 = e^{-x^2/4},
\]

\[
\Rightarrow \frac{1}{4} \sum_{\alpha = \kappa_\ell^+} d_{\alpha} \text{Tr} \left[ (\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k \right] \leq \frac{1}{2} \sum_{\ell=1}^{n-1} e^{-\pi^2 \ell^2 \alpha/2}.
\]
A similar sum occurs in the analysis of the classical walk on $\mathbb{Z}_n$. See p.26 of Diaconis [3] to see how such sums are handled (details teased out in Section 3.4 of [11]):

$$\frac{1}{4} \sum_{\alpha=\kappa_\ell} d_\alpha \text{Tr} \left[ (\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k \right] \leq e^{-\alpha \pi^2/2}$$

for $\alpha \geq 1/20$

With the dominant term identified, the other terms can be bound crudely. In particular,

$$\frac{1}{4} \sum_{\alpha=\kappa_\ell} d_\alpha \text{Tr} \left[ (\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k \right] = \frac{1}{4} \sum_{\ell=1}^{n-1} \frac{1}{4^k} \sin^4 \left( \frac{\pi \ell}{n} \right) \leq \frac{1}{4} \sum_{\ell=1}^{n-1} \frac{1}{4^k} = \frac{1}{4} \frac{n-1}{4^{\alpha n^2}} \cdot \frac{e^{\alpha \pi^2/2}}{\sin^4 \left( \frac{\pi \ell}{n} \right)} \leq \left( \frac{n}{4} \cdot e^{\alpha \pi^2/2} \right) e^{-\alpha \pi^2/2} \leq \left( \frac{n}{4} \cdot e^{\alpha(n^2-\pi^2/2)} \right) e^{-\alpha \pi^2/2} \leq \alpha \geq 1/20 \left( \frac{n}{4} \cdot e^{-(n^2-\pi^2/2)/20} \right) e^{-\alpha \pi^2/2} =: d(n) \cdot e^{-\alpha \pi^2/2}.$$

Note that $\hat{\nu}(\kappa_{u,v})$ is real and diagonal:

$$\hat{\nu}(\kappa_{u,v}) = \frac{1}{2} \left( \cos \left( \frac{2\pi u}{n} \right) + \cos \left( \frac{2\pi v}{n} \right) \right) I_2$$

$$\Rightarrow \text{Tr}[(\hat{\nu}(\kappa_{u,v})^*)^k \hat{\nu}(\kappa_{u,v})^k] = 2^{4k} \left( \cos \left( \frac{2\pi u}{n} \right) + \cos \left( \frac{2\pi v}{n} \right) \right)^{2k}$$

Using the trivial $|\cos(x) + \cos(y)| \leq 2$ bound,

$$\frac{1}{4} \sum_{\alpha=\kappa_{u,v}} d_\alpha \text{Tr} \left[ (\hat{\nu}(\alpha)^*)^k \hat{\nu}(\alpha)^k \right] \leq \frac{1}{4^k} \sum_{u=0,...,n-1}^{v=1,...,\frac{n}{2}} 2^{2k} \frac{n(n-1)}{4^k} = \frac{2^{2k} n(n-1)}{4^{2k}} \cdot \frac{1}{2} \frac{n^2 e^{-\alpha(n^2-\pi^2/2)}}{4^{\alpha n^2}} \leq \frac{1}{2} \frac{n^2 e^{-\alpha(n^2-\pi^2/2)}}{4^{\alpha n^2}} \leq 2n \cdot d(n) \cdot e^{-\alpha \pi^2/2}.$$

Putting these bounds together gives the result with

$$c_n = \sqrt{1 + d(n) + 2n \cdot d(n)}$$
Consider the Lower Bound Lemma 3.11 with $\rho_1^+$:

$$\|\nu^k - \pi\| \geq \frac{1}{2} \left| \cos^2 \left( \frac{\pi}{n} \right) + 1 \right|^k.$$ 

Consider $h(x) = \ln \left( \frac{1}{2} (\cos^2 x + 1) e^{x^2/2} \right)$. Note $h(0) = h'(0) = h''(0) = 0$ but

$$h''(x) = \frac{(1 - \cos^2 x)(3 - \cos^2 x)}{(\cos^2 x + 1)^2} > 0,$$

for $x \in (0, \pi)$. Therefore $\frac{1}{2} (\cos^2 x + 1) \geq e^{-x^2/2}$ and

$$\|\nu^k - \pi\| \geq \frac{1}{2} e^{-\pi^2 k/2n^2} = \frac{1}{2} e^{-\alpha \pi^2 / 2}.$$ 

Note that $c_n \to 1$ very rapidly. Below the bounds are plotted for $c_n = 1$:

**Figure 1.** Note that for $k = n^2/5$ the distance to random is bounded above by $3/5$ and bounded below away from zero. However at $k = 3n^2/5$ the distance to random is still bounded away from zero. Therefore the cut-off phenomenon is not exhibited.
Acknowledgements. I would like to thank Adam Skalski; Example 4.2 was developed during a visit to Adam at the Institute of Mathematics of the Polish Academy of Sciences (IMPAN), Warsaw, Poland. This trip was financially supported by IMPAN and also Cork Institute of Technology. I would like to thank Uwe Franz for assisting with Proposition 2.1. I would like to thank Amaury Freslon for encouragement and helpful comments; in particular for help in greatly improving the presentation of the bounds for the random walk on $\tilde{S}_n$. The rest of the paper was developed during the author’s PhD study at University College Cork, under the supervision of Stephen Wills.

References

[1] Bekka, B. and de la Harpe, P. and Valette, A., Kazhdans Property (T), New Math. Monogr. 11, Cambridge Univ. Press, Cambridge, 2008.
[2] Bhowmick, J., Skalski, A., Sołtan, Quantum group of automorphisms of a finite quantum group, Journal of Algebra, 423, 514-537, 2015.
[3] Diaconis, P., Group Representations in Probability and Statistics, IMS: Hayward, CA, 1988.
[4] Diaconis, P. and Shahshahani, M., Generating a random permutation with random transpositions, Z. Wahrscheinlichkeitstheorie Verw. Gebiete 57, 159-179, 1981.
[5] Franz, U. and Gohm, R., Random Walks on Finite Quantum Groups, Quantum Independent Increment Processes II, volume 1866 of Lecture Notes in Math., pages 1-32. Springer, Berlin, 2006.
[6] Franz, U. and Skalski, A., On Idempotent States on Quantum Groups, Journal of Algebra 322, (5) 1774-1802, 2009.
[7] Freslon, A., Cut-off phenomenom for random walks on free orthogonal free groups, to appear in Probab. Theory Related Fields, 2018.
[8] Freslon, A., Quantum reflections, random walks and cut-off, arXiv:1802.09402, 2018.
[9] Kac, G.I. and Paljutkin, V.G., Finite Group Rings, Trudy Moskov. Mat. Obšč. 15:224-261, 1966. Translated in Trans. Moscow Math. Soc. (1967), 251-284., 1996.
[10] McCarthy, J.P., Random walks on finite quantum groups : Diaconis-Shahshahani theory for quantum groups, PhD thesis, 2017, arXiv:1709.09357
[11] McCarthy, J.P., The cut-off phenomenon in random walks on finite groups, MSc thesis, 2010, arXiv:1504.05387
[12] Palcoux, S., Ore’s theorem for cyclic subfactor planar algebras and beyond, Pacific J. Math. 292-1, 203-221, 2018.
[13] Pisier, G. and Xu, Q., Non-commutative $L^p$-spaces, Handbook of the Geometry of Banach Spaces, Volume 2, William B. Johnson and Joram Lindenstrauss, North Holland, Amsterdam, 34, 1459-1517, 2003.
[14] Rosenthal, J.S., Random Rotation: Characters and Random Walks on SO(N), Ann. Probab. 22, no. 1, 398-423, 1997.
[15] Saloff-Coste, L., *Random Walks on Finite Groups (Probability on Discrete Structures)*, p.263-346, Springer, Berlin, 2004.

[16] Sekine, Y., *An example of finite-dimensional Kac algebras of Kac–Paljutkin type*, Proc. Amer. Math. Soc. **124**, no.4, 1139-1147, 1996.

[17] J. M. Steele, *The Cauchy–Schwarz Master Class: An Introduction to the Art of Mathematical Inequalities*, Cambridge University Press, New York, NY, USA, 2004.

[18] Timmermann, T., *An Invitation to Quantum Groups and Duality*, Eur. Math. Soc., 2008.

[19] Vainermann, L. I. and Kac, G. I., *Nonunimodular ring groups and Hopf–von Neumann algebras*, Dokl. Akad., Nauk SSSR **211**, 194-225; English transl. Math. USSR Sb. **23** (1974), 170-181, 1973.

[20] Van Daele, A., *Multiplier Hopf algebras*, Trans. Amer. Math. Soc., **342**, no 2, 917-932, 1994.

[21] Van Daele, A., *The Haar Measure on Finite Quantum Groups*, Proc. Amer. Math. Soc. **125**, no.12, 3489-3500, 1997.

[22] Van Daele, A., *An Algebraic Framework for Group Duality*, Adv. Math. **140**, (2) 323-366, 1998.

[23] Van Daele, A., *The Fourier transform for group duality*, Arxiv preprint, arXiv:math/0609502, 2007.

[24] Wang, Simeng, *$L_p$-improving convolution operators on finite quantum groups*, Indiana Univ. Math. J., **65**, no.5, 1609-1637, 2016.

[25] Woronowicz, S.L., *Compact matrix pseudogroups*, Comm. Math. Phys. **111**, 613-665, 1987.

Department of Mathematics, Cork Institute of Technology, Cork, Ireland.

E-mail address: jeremiah.mccarthy@cit.ie