Diaconis–Shahshahani Upper Bound Lemma for Finite Quantum Groups

J.P. McCarthy

Cork Institute of Technology

30 August 2018
Irish Mathematical Society Meeting, UCD

Finite Classical Groups aka Finite Groups

A finite group is an object $G \in \mathbf{FinSet}$ together with morphisms m, e, and $^{-1}$. Associativity, identity, and inverse are given by

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times I_G} & G \times G \\ {\scriptstyle I_G \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

$$\begin{array}{ccccc} G \times G & \xrightarrow{m} & G & \xleftarrow{m} & G \times G \\ {\scriptstyle e \times I_G}\uparrow & & \| & & \uparrow{\scriptstyle I_G \times e} \\ \{\bullet\} \times G & \xleftarrow{\cong} & G & \xrightarrow{\cong} & G \times \{\bullet\} \end{array}$$

$$\begin{array}{ccccc} G \times G & \xrightarrow{m} & G & \xleftarrow{m} & G \times G \\ {\scriptstyle S \times I_G}\uparrow & & {\scriptstyle e \circ \varepsilon_G}\uparrow & & \uparrow{\scriptstyle I_G \times S} \\ G \times G & \xleftarrow{\Delta_G} & G & \xrightarrow{\Delta_G} & G \times G \end{array}$$

The $\mathbb{C}$-Functor

The $\mathbb{C}$-Functor, $\mathbb{C} : \mathbf{FinSet} \to \mathbf{FinVec}_{\mathbb{C}}$, is a covariant functor mapping a set X to a vector space $\mathbb{C}X$ (the finite-dimensional vector space with basis $\{\delta^x : x \in X\}$), and a morphism $f : X \to Y$, $x \mapsto f(x)$ to a morphism $\mathbb{C}f : \mathbb{C}X \to \mathbb{C}Y$, $\delta^x \mapsto \delta^{f(x)}$.

The $\mathbb{C}$-Functor

The $\mathbb{C}$-Functor, $\mathbb{C} : \mathbf{FinSet} \to \mathbf{FinVec}_{\mathbb{C}}$, is a covariant functor mapping a set X to a vector space $\mathbb{C}X$ (the finite-dimensional vector space with basis $\{\delta^x : x \in X\}$), and a morphism $f : X \to Y$, $x \mapsto f(x)$ to a morphism $\mathbb{C}f : \mathbb{C}X \to \mathbb{C}Y$, $\delta^x \mapsto \delta^{f(x)}$.

Applying the $\mathbb{C}$-Functor to a group G yields the *group algebra*, $\mathbb{C}G$. As the vector space is finite dimensional, $\mathbb{C}(G \times G) \cong \mathbb{C}G \otimes \mathbb{C}G$ and so $\nabla : \mathbb{C}G \otimes \mathbb{C}G \to \mathbb{C}G$, $\delta^s \otimes \delta^t \mapsto \delta^{st}$.

The $\mathbb{C}$-Functor

The $\mathbb{C}$-Functor, $\mathbb{C} : \mathbf{FinSet} \to \mathbf{FinVec}_{\mathbb{C}}$, is a covariant functor mapping a set X to a vector space $\mathbb{C}X$ (the finite-dimensional vector space with basis $\{\delta^x : x \in X\}$), and a morphism $f : X \to Y$, $x \mapsto f(x)$ to a morphism $\mathbb{C}f : \mathbb{C}X \to \mathbb{C}Y$, $\delta^x \mapsto \delta^{f(x)}$.

Applying the $\mathbb{C}$-Functor to a group G yields the *group algebra*, $\mathbb{C}G$. As the vector space is finite dimensional, $\mathbb{C}(G \times G) \cong \mathbb{C}G \otimes \mathbb{C}G$ and so $\nabla : \mathbb{C}G \otimes \mathbb{C}G \to \mathbb{C}G$, $\delta^s \otimes \delta^t \mapsto \delta^{st}$.

As the group axioms are commutative diagrams, the group axioms are translated into "$\mathbb{C}$"-group axioms. For example, associativity:

$$\begin{array}{ccc} \mathbb{C}G \otimes \mathbb{C}G \otimes \mathbb{C}G & \xrightarrow{\nabla \times I_{\mathbb{C}G}} & \mathbb{C}G \otimes \mathbb{C}G \\ \Big\downarrow{\scriptstyle I_{\mathbb{C}G} \times \nabla} & & \Big\downarrow{\scriptstyle \nabla} \\ \mathbb{C}G \times \mathbb{C}G & \xrightarrow{\nabla} & \mathbb{C}G \end{array}$$

The Dual Endofunctor

The Dual Endofunctor, $\mathcal{D} : \mathbf{FinVec}_{\mathbb{C}} \to \mathbf{FinVec}_{\mathbb{C}}$, is a *contravariant* functor mapping a vector space U to its dual U^* (recall everything is in finite dimensions), and a morphism (linear map) $T : U \to V$, to its transpose ($\varphi \in V^*$):

$$\mathcal{D}(T) : V^* \to U^*, \qquad \varphi \mapsto \varphi \circ T.$$

The Dual Endofunctor

The Dual Endofunctor, $\mathcal{D} : \mathbf{FinVec}_{\mathbb{C}} \to \mathbf{FinVec}_{\mathbb{C}}$, is a *contravariant* functor mapping a vector space U to its dual U^* (recall everything is in finite dimensions), and a morphism (linear map) $T : U \to V$, to its transpose ($\varphi \in V^*$):

$$\mathcal{D}(T) : V^* \to U^*, \qquad \varphi \mapsto \varphi \circ T.$$

Applying the Dual Endofunctor to a group algebra $\mathbb{C}G$ yields the *algebra of functions on* G, $F(G)$, with basis $\{\delta_g : g \in G\}$. This carries a commutative $\mathbb{C}^*$-algebra structure, but inherits from the group axioms — via the functor composition $\mathcal{Q} := \mathcal{D} \circ \mathbb{C}$ — an encoding of the group axioms.

The Dual Endofunctor

The Dual Endofunctor, $\mathcal{D} : \mathbf{FinVec}_{\mathbb{C}} \to \mathbf{FinVec}_{\mathbb{C}}$, is a *contravariant* functor mapping a vector space U to its dual U^* (recall everything is in finite dimensions), and a morphism (linear map) $T : U \to V$, to its transpose ($\varphi \in V^*$):

$$\mathcal{D}(T) : V^* \to U^*, \qquad \varphi \mapsto \varphi \circ T.$$

Applying the Dual Endofunctor to a group algebra $\mathbb{C}G$ yields the *algebra of functions on* G, $F(G)$, with basis $\{\delta_g : g \in G\}$. This carries a commutative $\mathbb{C}^*$-algebra structure, but inherits from the group axioms — via the functor composition $\mathcal{Q} := \mathcal{D} \circ \mathbb{C}$ — an encoding of the group axioms.

This encoding has maps, the *comultiplication*, $\Delta := \mathcal{Q}m$; the *counit*, $\varepsilon := \mathcal{Q}e$; and the *antipode*, $S := \mathcal{Q}(^{-1})$, that satisfy three commutative diagrams that encode associativity, identity, and inverses.

The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

The *comultiplication*, for example: $\Delta : F(G) \to F(G) \otimes F(G)$ is a linear map

$$\Delta(\delta_g) = \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t.$$

The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

The *comultiplication*, for example: $\Delta : F(G) \to F(G) \otimes F(G)$ is a linear map

$$\Delta(\delta_g) = \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t.$$

The group axiom of associativity is, for example, encoded by *coassociativity* (note the reversal of arrows):

$$\begin{array}{ccc} F(G) & \xrightarrow{\quad\Delta\quad} & F(G) \otimes F(G) \\ \Delta \downarrow & & \downarrow \Delta \otimes I_{F(G)} \\ F(G) \otimes F(G) & \xrightarrow[I_{F(G)} \otimes \Delta]{} & F(G) \otimes F(G) \otimes F(G) \end{array}$$

The encoded group axioms are called *Hopf-algebra axioms*.

The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

The *comultiplication*, for example: $\Delta : F(G) \to F(G) \otimes F(G)$ is a linear map

$$\Delta(\delta_g) = \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t.$$

The group axiom of associativity is, for example, encoded by *coassociativity* (note the reversal of arrows):

$$\begin{array}{ccc} F(G) & \xrightarrow{\quad\Delta\quad} & F(G) \otimes F(G) \\ \Delta \downarrow & & \downarrow \Delta \otimes I_{F(G)} \\ F(G) \otimes F(G) & \xrightarrow[I_{F(G)} \otimes \Delta]{} & F(G) \otimes F(G) \otimes F(G) \end{array}$$

The encoded group axioms are called *Hopf-algebra axioms*. The interaction between this structure, and the C^*-algebra structure gives the algebra of functions on a group, $F(G)$, the structure of what is called a C^*-Hopf algebra.

Quantum Groups (Drinfeld, Jimbo, Woronowicz (1980s))

There are, however, finite dimensional spaces together with morphisms that also satisfy these axioms but are not the algebra of functions on any group — because the multiplication is no longer commutative — multi-matrix algebras.

Quantum Groups (Drinfeld, Jimbo, Woronowicz (1980s))

There are, however, finite dimensional spaces together with morphisms that also satisfy these axioms but are not the algebra of functions on any group — because the multiplication is no longer commutative — multi-matrix algebras.

These are the algebras of functions on (finite) *quantum groups*:

$$\begin{array}{ccc} F(G) & \xrightarrow{\mathcal{Q}(\text{group axioms) but not } ab=ba} & F(\mathbb{G}) \\ \mathcal{Q}\uparrow & & \uparrow\mathcal{Q} \\ G & & \mathbb{G} \end{array}$$

These quantum spaces do not actually exist — and are referred to as *virtual objects*

Quantum Groups (Drinfeld, Jimbo, Woronowicz (1980s))

There are, however, finite dimensional spaces together with morphisms that also satisfy these axioms but are not the algebra of functions on any group — because the multiplication is no longer commutative — multi-matrix algebras.

These are the algebras of functions on (finite) *quantum groups*:

$$\begin{array}{ccc} F(G) & \xrightarrow{\mathcal{Q}\text{(group axioms) but not } ab=ba} & F(\mathbb{G}) \\ \mathcal{Q}\uparrow & & \uparrow\mathcal{Q} \\ G & & \mathbb{G} \end{array}$$

These quantum spaces do not actually exist — and are referred to as *virtual objects* — yet many questions that can be posed and resolved in the classical setting may also be posed and hopefully resolved in the quantum case.

Classical Random Walks (Markov (1906); Borel (1940))

Given a finite group, G, and G-valued random variables $\zeta_i \overset{\text{iid}}{\sim} \nu \in M_p(G)$, the sequence of random variables $\{\xi_i\}_{i=1}^k$ given by

$$\xi_i := \zeta_i \cdot \cdots \cdot \zeta_2 \cdot \zeta_1,$$

is called a *(right-invariant) random walk on G driven by ν*.

Classical Random Walks (Markov (1906); Borel (1940))

Given a finite group, G, and G-valued random variables $\zeta_i \overset{\text{iid}}{\sim} \nu \in M_p(G)$, the sequence of random variables $\{\xi_i\}_{i=1}^k$ given by

$$\xi_i := \zeta_i \cdot \cdots \cdot \zeta_2 \cdot \zeta_1,$$

is called a *(right-invariant) random walk on G driven by ν*.

The distribution of ξ_k — all of interest in this work — is given by

$$\underbrace{\nu \star \cdots \star \nu \star \nu}_{k \text{ copies}} =: \nu^{\star k},$$

where (noting $\mathbb{E}_\nu(\delta_g) = \nu(g)$)

$$(\nu \star \nu)(g) := \sum_{t \in G} \nu(gt^{-1})\nu(t) = \underbrace{(\mathbb{E}_\nu \otimes \mathbb{E}_\nu)\Delta}_{=:\mathbb{E}_\nu \star \mathbb{E}_\nu}(\delta_g).$$

Classical Random Walks (Markov (1906); Borel (1940))

Given a finite group, G, and G-valued random variables $\zeta_i \overset{\text{iid}}{\sim} \nu \in M_p(G)$, the sequence of random variables $\{\xi_i\}_{i=1}^k$ given by

$$\xi_i := \zeta_i \cdot \cdots \cdot \zeta_2 \cdot \zeta_1,$$

is called a *(right-invariant) random walk on G driven by ν*.

The distribution of ξ_k — all of interest in this work — is given by

$$\underbrace{\nu \star \cdots \star \nu \star \nu}_{k \text{ copies}} =: \nu^{\star k},$$

where (noting $\mathbb{E}_\nu(\delta_g) = \nu(g)$)

$$(\nu \star \nu)(g) := \sum_{t \in G} \nu(gt^{-1})\nu(t) = \underbrace{(\mathbb{E}_\nu \otimes \mathbb{E}_\nu)\Delta}_{=:\mathbb{E}_\nu \star \mathbb{E}_\nu}(\delta_g).$$

Denote by $\pi \in M_p(G)$ the uniform distribution; which is *invariant* in the sense that for any $\nu \in M_p(G)$, $\nu \star \pi = \pi = \pi \star \nu$.

Quantum Random Walks (Franz & Gohm (2005))

A probability $\nu \in M_p(G)$ gives rise to a *state* (norm one, positive linear functional) on $F(G)$: $f \mapsto \sum_{t\in G} f(t)\,\nu(t) =: \mathbb{E}_\nu(f)$.

Therefore the quantum probabilistic identifications are made:

$$\nu \in M_p(\mathbb{G}) \longleftrightarrow \text{a state } \mathbb{E}_\nu \text{ on } F(\mathbb{G});$$

$$\text{(distribution of) random walk on } \mathbb{G} \longleftrightarrow \{\mathbb{E}_{\nu^{\star k}}\} := \{\mathbb{E}_\nu^{\star k}\}$$

Quantum Random Walks (Franz & Gohm (2005))

A probability $\nu \in M_p(G)$ gives rise to a *state* (norm one, positive linear functional) on $F(G)$: $f \mapsto \sum_{t\in G} f(t)\,\nu(t) =: \mathbb{E}_\nu(f)$.

Therefore the quantum probabilistic identifications are made:

$$\nu \in M_p(\mathbb{G}) \longleftrightarrow \text{a state } \mathbb{E}_\nu \text{ on } F(\mathbb{G});$$

$$\text{(distribution of) random walk on } \mathbb{G} \longleftrightarrow \{\mathbb{E}_{\nu^{\star k}}\} := \{\mathbb{E}_\nu^{\star k}\}$$

Note that for $f \in F(G)$:

$$\mathbb{E}_\pi(f) = \sum_{t\in G} f(t)\pi(t) = \frac{1}{|G|}\sum_{t\in G} f(t) = \overline{f},$$

the average — *over all points* $t \in G$ — of f.

Quantum Random Walks (Franz & Gohm (2005))

A probability $\nu \in M_p(G)$ gives rise to a *state* (norm one, positive linear functional) on $F(G)$: $f \mapsto \sum_{t\in G} f(t)\,\nu(t) =: \mathbb{E}_\nu(f)$.

Therefore the quantum probabilistic identifications are made:

$$\nu \in M_p(\mathbb{G}) \longleftrightarrow \text{a state } \mathbb{E}_\nu \text{ on } F(\mathbb{G});$$

$$\text{(distribution of) random walk on } \mathbb{G} \longleftrightarrow \{\mathbb{E}_{\nu^{\star k}}\} := \{\mathbb{E}_\nu^{\star k}\}$$

Note that for $f \in F(G)$:

$$\mathbb{E}_\pi(f) = \sum_{t\in G} f(t)\pi(t) = \frac{1}{|G|}\sum_{t\in G} f(t) = \overline{f},$$

the average — *over all points* $t \in G$ — of f.

Note that a (finite) quantum group also has a "uniform distribution". Given by the *Haar state*, $\mathbb{E}_\pi$, it is also invariant in the sense that $\mathbb{E}_\pi \star \mathbb{E}_\nu = \mathbb{E}_\pi = \mathbb{E}_\nu \star \mathbb{E}_\pi$ for all $\nu \in M_p(\mathbb{G})$.

Classical Distance to Random

Classical Random Walks of interest are primarily those in which the $\nu^{\star k}$ converge to uniform, to *random*. Thus, the question is posed: *when* is $\nu^{\star k}$ 'close to random'?

Classical Distance to Random

Classical Random Walks of interest are primarily those in which the $\nu^{\star k}$ converge to uniform, to *random*. Thus, the question is posed: *when* is $\nu^{\star k}$ 'close to random'? The distance to random is given by

$$\|\nu^{\star k} - \pi\| = \sup_{S \subset G} |\nu^{\star k}(S) - \pi(S)| = \sup_{S \subset G} |\mathbb{E}_{\nu^{\star k}}(\mathbb{1}_S) - \mathbb{E}_{\pi}(\mathbb{1}_S)|.$$

Classical Distance to Random

Classical Random Walks of interest are primarily those in which the $\nu^{\star k}$ converge to uniform, to *random*. Thus, the question is posed: *when* is $\nu^{\star k}$ 'close to random'? The distance to random is given by

$$\|\nu^{\star k} - \pi\| = \sup_{S \subset G} |\nu^{\star k}(S) - \pi(S)| = \sup_{S \subset G} |\mathbb{E}_{\nu^{\star k}}(\mathbb{1}_S) - \mathbb{E}_{\pi}(\mathbb{1}_S)|.$$

Probabilities $\nu \in M_p(G)$ have *densities*, that is there is an element $f_\nu \in F(G)$ such that $\mathbb{E}_\nu(f) = \mathbb{E}_\pi(f_\nu\, f)$ for all $f \in F(G)$ (indeed $f_\nu(g) = |G|\, \nu(g)$).

Classical Distance to Random

Classical Random Walks of interest are primarily those in which the $\nu^{\star k}$ converge to uniform, to *random*. Thus, the question is posed: *when* is $\nu^{\star k}$ 'close to random'? The distance to random is given by

$$\|\nu^{\star k} - \pi\| = \sup_{S \subset G} |\nu^{\star k}(S) - \pi(S)| = \sup_{S \subset G} |\mathbb{E}_{\nu^{\star k}}(\mathbb{1}_S) - \mathbb{E}_{\pi}(\mathbb{1}_S)|.$$

Probabilities $\nu \in M_p(G)$ have *densities*, that is there is an element $f_\nu \in F(G)$ such that $\mathbb{E}_\nu(f) = \mathbb{E}_\pi(f_\nu\, f)$ for all $f \in F(G)$ (indeed $f_\nu(g) = |G|\,\nu(g)$). Where

$$\|f\|_1 = \frac{1}{|G|} \sum_{t \in G} |f(t)| = \mathbb{E}_\pi(|f|),$$

Theorem

$$\|\nu^{\star k} - \pi\| = \frac{1}{2}\, \|f_{\nu^{\star k}} - f_\pi\|_1 \qquad \bullet$$

The presence of this one-norm allows a Cauchy–Schwarz inequality to be used: this becomes crucial.

Quantum Distance to Random

There is a one-to-one correspondence between subsets $S \subset G$ and projections $p \in F(G)$ — $S \leftrightarrow \mathbb{1}_S$ — and so for $\nu \in M_p(G)$

$$\|\nu^{\star k} - \pi\| = \sup_{p \in F(G),\ \text{a projection}} |\mathbb{E}_{\nu^{\star k}}(p) - \mathbb{E}_{\pi}(p)|. \qquad (1)$$

Quantum Distance to Random

There is a one-to-one correspondence between subsets $S \subset G$ and projections $p \in F(G)$ — $S \leftrightarrow \mathbb{1}_S$ — and so for $\nu \in M_p(G)$

$$\|\nu^{\star k} - \pi\| = \sup_{p \in F(G),\ \text{a projection}} |\mathbb{E}_{\nu^{\star k}}(p) - \mathbb{E}_{\pi}(p)|. \qquad (1)$$

Probabilities $\nu \in M_p(\mathbb{G})$ also have densities, that is there is an element $a_\nu \in F(\mathbb{G})$ such that $\mathbb{E}_\nu(a) = \mathbb{E}_\pi(a_\nu a)$ for all $a \in F(\mathbb{G})$.

Quantum Distance to Random

There is a one-to-one correspondence between subsets $S \subset G$ and projections $p \in F(G)$ — $S \leftrightarrow \mathbb{1}_S$ — and so for $\nu \in M_p(G)$

$$\|\nu^{\star k} - \pi\| = \sup_{p \in F(G),\ \text{a projection}} |\mathbb{E}_{\nu^{\star k}}(p) - \mathbb{E}_{\pi}(p)|. \qquad (1)$$

Probabilities $\nu \in M_p(\mathbb{G})$ also have densities, that is there is an element $a_\nu \in F(\mathbb{G})$ such that $\mathbb{E}_\nu(a) = \mathbb{E}_\pi(a_\nu a)$ for all $a \in F(\mathbb{G})$.

Theorem

In the quantum case, the total variation distance is also equal to half the one norm:

$$\|\nu^{\star k} - \pi\| = \frac{1}{2}\,\|a_{\nu^{\star k}} - a_\pi\|_1 := \frac{1}{2}\,\mathbb{E}_\pi(|a_{\nu^{\star k}} - a_\pi|).$$

(Freslon (2018))

Quantum Distance to Random

There is a one-to-one correspondence between subsets $S \subset G$ and projections $p \in F(G)$ — $S \leftrightarrow \mathbb{1}_S$ — and so for $\nu \in M_p(G)$

$$\|\nu^{\star k} - \pi\| = \sup_{p \in F(G),\ \text{a projection}} |\mathbb{E}_{\nu^{\star k}}(p) - \mathbb{E}_{\pi}(p)|. \qquad (1)$$

Probabilities $\nu \in M_p(\mathbb{G})$ also have densities, that is there is an element $a_\nu \in F(\mathbb{G})$ such that $\mathbb{E}_\nu(a) = \mathbb{E}_\pi(a_\nu a)$ for all $a \in F(\mathbb{G})$.

Theorem

In the quantum case, the total variation distance is also equal to half the one norm:

$$\|\nu^{\star k} - \pi\| = \frac{1}{2}\,\|a_{\nu^{\star k}} - a_\pi\|_1 := \frac{1}{2}\,\mathbb{E}_\pi(|a_{\nu^{\star k}} - a_\pi|).$$

(Freslon (2018))

This one norm also has an associated Cauchy–Schwarz inequality, and this allows (1) to be used in the quantum case.

Classical Diaconis–Shahshahani Theory

Every group representation $\rho : G \to \mathrm{GL}(V)$ splits into a direct sum of irreducible representations where $\rho^\alpha : G \to \mathrm{GL}(V_\alpha)$ with $\dim(V_\alpha) =: d_\alpha$.

Classical Diaconis–Shahshahani Theory

Every group representation $\rho : G \to \mathrm{GL}(V)$ splits into a direct sum of irreducible representations where $\rho^\alpha : G \to \mathrm{GL}(V_\alpha)$ with $\dim(V_\alpha) =: d_\alpha$.

Definition: (used by Diaconis) The *Fourier Transform of* $\nu \in M_p(G)$ is a linear map:

$$\widehat{\nu} \in \bigoplus_{\alpha \in \mathrm{Irr}(G)} L(V_\alpha);$$

where the *Fourier Transform of* ν at *the representation* ρ^α is

$$\widehat{\nu}|_{V_\alpha} =: \widehat{\nu}(\alpha) = \sum_{t \in G} \nu(t)\rho^\alpha(t).$$

Classical Diaconis–Shahshahani Theory

Every group representation $\rho : G \to \mathrm{GL}(V)$ splits into a direct sum of irreducible representations where $\rho^\alpha : G \to \mathrm{GL}(V_\alpha)$ with $\dim(V_\alpha) =: d_\alpha$.

Definition: (used by Diaconis) The *Fourier Transform of* $\nu \in M_p(G)$ is a linear map:

$$\widehat{\nu} \in \bigoplus_{\alpha \in \mathrm{Irr}(G)} L(V_\alpha);$$

where the *Fourier Transform of* ν at *the representation* ρ^α is

$$\widehat{\nu}|_{V_\alpha} =: \widehat{\nu}(\alpha) = \sum_{t \in G} \nu(t)\rho^\alpha(t).$$

Upper Bound Lemma: Where τ is the *trivial representation*,

$$\|\nu^{\star k} - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \mathrm{Irr}(G)\setminus\{\tau\}} d_\alpha \mathrm{Tr}\left[\left(\widehat{\nu}(\alpha)^*\right)^k \widehat{\nu}(\alpha)^k\right].$$

(Diaconis & Shahshahani (1981))

Applications

- Simple Random Walk on Circle, $\mathbb{Z}_n$ — step left/right with equal probability; close to random in about $k = n^2$ steps.
- Random Walk on the Hypercube, $\mathbb{Z}_2^n$ — stick or move to one of the nearest neighbours with equal probability, $\frac{1}{n+1}$; close to random in $k = \frac{1}{4} n \ln n$ steps.
- Random Transposition Shuffle of S_n — swap two cards chosen at random; close to random in $k = \frac{1}{2} n \ln n$ steps ($k \approx 102$ for $n = 52$).

Diaconis (1988)

Quantum Diaconis–Shahshahani Theory? (Wills, (2010))

Consider again the Upper Bound Lemma:

$$\|\nu^{\star k} - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \mathsf{Irr}(G)\setminus\{\tau\}} d_\alpha \mathsf{Tr}\left[\left(\widehat{\nu}(\alpha)^*\right)^k \widehat{\nu}(\alpha)^k\right].$$

Note there is no reference to points in the space G. While it appears that $\widehat{\nu}(\alpha)$ is defined with respect to points, it is actually a sum over *all* points, a rôle played by the Haar state $\mathbb{E}_\pi$:

$$\underbrace{\frac{1}{|G|}\sum_{t\in G} f(t)}_{\text{classical: references points } t\in G} \quad = \quad \underbrace{\mathbb{E}_\pi(f)}_{\text{quantum: no reference to points}} .$$

Quantum Diaconis–Shahshahani Theory? (Wills, (2010))

Consider again the Upper Bound Lemma:

$$\|\nu^{\star k} - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \mathsf{Irr}(G) \setminus \{\tau\}} d_\alpha \mathsf{Tr}\left[\left(\widehat{\nu}(\alpha)^* \right)^k \widehat{\nu}(\alpha)^k \right].$$

Note there is no reference to points in the space G. While it appears that $\widehat{\nu}(\alpha)$ is defined with respect to points, it is actually a sum over *all* points, a rôle played by the Haar state $\mathbb{E}_\pi$:

$$\underbrace{\frac{1}{|G|} \sum_{t \in G} f(t)}_{\text{classical: references points } t \in G} = \underbrace{\mathbb{E}_\pi(f)}_{\text{quantum: no reference to points}}.$$

...and (finite) quantum groups have a representation theory remarkably similar to that of classical groups; e.g. there is a Peter–Weyl Theorem (Woronowicz, (1987)) (their algebras of functions have *corepresentations*).

Diaconis–Van Daele Theory (McCarthy, 2017)

Using results of Van Daele (1994-2007), it can be shown that the properties of the classical Fourier Transform $\widehat{\nu}(\rho^{\alpha})$, that are used to prove the classical Upper Bound Lemma, are *also* shared by a quantum Fourier Transform $\widehat{\nu}(\kappa_{\alpha})$ (this κ_{α} is a *corepresentation*).

Diaconis–Van Daele Theory (McCarthy, 2017)

Using results of Van Daele (1994-2007), it can be shown that the properties of the classical Fourier Transform $\widehat{\nu}(\rho^{\alpha})$, that are used to prove the classical Upper Bound Lemma, are *also* shared by a quantum Fourier Transform $\widehat{\nu}(\kappa_{\alpha})$ (this κ_{α} is a *corepresentation*).

For example, the sum over irreducible representations comes from the classical

$$\nu(\delta_{e}) = \frac{1}{|G|} \sum_{\alpha \in \mathsf{Irr}(G)} d_{\alpha} \, \mathsf{Tr}\left[\widehat{\nu}(\alpha)\right];$$

which has a generalisation to finite quantum groups:

$$\widehat{h}(\nu) = \sum_{\alpha \in \mathsf{Irr}(\mathbb{G})} d_{\alpha} \, \mathsf{Tr}\left[\widehat{\nu}(\alpha)\right],$$

where $\widehat{h}$ is an unnormalised but invariant state on the dual of $F(\mathbb{G})$.

Upper Bound Lemma (McCarthy, 2017)

Leaning heavily on the finiteness assumption, the Upper Bound Lemma for Finite Quantum Groups follows in a similar manner to that of the classical result of Diaconis and Shahshahani.

In the notation that is used, the classical Upper Bound Lemma:

$$\|\nu^{\star k} - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \mathsf{Irr}(G)\setminus\{\tau\}} d_\alpha \,\mathsf{Tr}\left[\left(\widehat{\nu}\,(\alpha)^*\right)^k \widehat{\nu}\,(\alpha)^k\right],$$

and the quantum Upper Bound Lemma:

$$\|\nu^{\star k} - \pi\|^2 \leq \frac{1}{4} \sum_{\alpha \in \mathsf{Irr}(\mathbb{G})\setminus\{\tau\}} d_\alpha \,\mathsf{Tr}\left[\left(\widehat{\nu}\,(\alpha)^*\right)^k \widehat{\nu}\,(\alpha)^k\right].$$

are essentially the same thing.

References

1. Markov (1906), *Extension of the law of large numbers to dependent events*
2. Borel (1940), *Théorie Mathématique du Bridge à la Portée de Tous*
3. Diaconis & Shahshahani (1981), *Generating a Random Permutation with Random Transpositions*
4. Diaconis (1988), *Group Representations in Probability and Statistics*
5. Franz & Gohm (2005), *Random Walks on Finite Quantum Groups*
6. Freslon (2018), *Cut-off phenomenon for random walks on free orthogonal quantum groups*
7. McCarthy (2017), *Random Walks on Finite Quantum Groups: Diaconis–Shahshahani Theory for Quantum Groups*
8. Van Daele (2006), *The Fourier Transform in Quantum Group Theory*