The Ergodic Theorem for Random Walks: from Finite Groups, to Group Algebras, to Finite Quantum Groups

J.P. McCarthy

Cork Institute of Technology

7 September 2019
Munster Groups, WIT
<table>
<thead>
<tr>
<th>Table of contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Walks on Finite Groups</td>
</tr>
<tr>
<td>From Finite Classical Groups to Finite Quantum Groups</td>
</tr>
<tr>
<td>Random Walks on Finite Quantum Groups?</td>
</tr>
<tr>
<td>Group Algebras</td>
</tr>
<tr>
<td>An Ergodic Theorem for Random Walks on Quantum Groups?</td>
</tr>
</tbody>
</table>
Card Shuffling

Assume that the deck starts in some known order
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[ A\heartsuit, 2\heartsuit, \ldots, K\heartsuit, A\spadesuit, \ldots, K\spadesuit, A\diamondsuit, \ldots, K\clubsuit. \]
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[ A\heartsuit, 2\heartsuit, \ldots, K\heartsuit, A\clubsuit, \ldots, K\clubsuit, A\diamondsuit, \ldots, K\diamondsuit. \]

A deck is shuffled by repeatedly applying (say) \( k \) shuffles: \( \sigma_i \in S_{52} \):

\[ \sum_k := \sigma_k \cdots \sigma_1 \]
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[
A♥, 2♥, \ldots, K♥, A♠, \ldots, K♠, A♦, \ldots, K♣.
\]

A deck is shuffled by repeatedly applying (say) \( k \) shuffles: \( \sigma_i \in S_{52} \):

\[
\Sigma_k := \sigma_k \cdots \sigma_1
\]

- **Perfect Riffle Shuffle:**
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[ A♥, 2♥, \ldots, K♥, A♠, \ldots, K♠, A♦, \ldots, K♣. \]

A deck is shuffled by repeatedly applying (say) \( k \) shuffles: \( \sigma_i \in S_{52}: \)

\[ \sum_k := \sigma_k \cdots \sigma_1 \]

▷ **Perfect Riffle Shuffle:** Let \( \sigma_{PFS} \) be the perfect riffle shuffle.
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[ A\heartsuit, 2\heartsuit, \ldots, K\heartsuit, A\spadesuit, \ldots, K\spadesuit, A\diamondsuit, \ldots, K\diamondsuit. \]

A deck is shuffled by repeatedly applying (say) \( k \) shuffles: \( \sigma_i \in S_{52}: \)

\[ \Sigma_k := \sigma_k \cdots \sigma_1 \]

- **Perfect Riffle Shuffle**: Let \( \sigma_{\text{PFS}} \) be the perfect riffle shuffle.

\[ \sigma^8_{\text{PRS}} = e. \]
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[A♥, 2♥, \ldots, K♥, A♠, \ldots, K♠, A♦, \ldots, K♣.\]

A deck is shuffled by repeatedly applying (say) \(k\) shuffles: \(\sigma_i \in S_{52}\):

\[\Sigma_k := \sigma_k \cdots \sigma_1\]

- **Perfect Riffle Shuffle:** Let \(\sigma_{\text{PFS}}\) be the perfect riffle shuffle.

\[\sigma_{\text{PRS}}^8 = e.\]

A *pure* shuffle like this is not going to mix up a deck of cards. The shuffle has to be chosen according to a non-Dirac probability distribution \(\nu \in M_p(S_{52})\).
Card Shuffling

Assume that the deck starts in some known order, e.g.

\[ A♥, 2♥, \ldots, K♥, A♣, \ldots, K♣, A♦, \ldots, K♣. \]

A deck is shuffled by repeatedly applying (say) \( k \) shuffles: \( \sigma_i \in S_{52} \):

\[ \Sigma_k := \sigma_k \cdots \sigma_1 \]

► **Perfect Riffle Shuffle:** Let \( \sigma_{PFS} \) be the perfect riffle shuffle.

\[ \sigma_{PRS}^8 = e. \]

A *pure* shuffle like this is not going to mix up a deck of cards. The shuffle has to be chosen according to a non-Dirac probability distribution \( \nu \in M_p(S_{52}) \). Assume from now that all shuffles are identically but independently distributed as \( \nu \in M_p(S_{52}) \).
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

Call a shuffle ergodic if it mixes up the deck:

$$\lim_{k \to \infty} P[\Sigma_k = \sigma] = \frac{1}{52!}.$$ 

That is the distribution of $\Sigma_k$ converges to the uniform distribution.

▶ Cutting the Deck:

Is this an ergodic shuffle?

Cutting the Deck is reducible — not every order is possible.

An ergodic shuffle must be irreducible.
What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[
\mathbb{P}[\text{deck in order } \sigma \in S_{52}] = \frac{1}{52!}.
\]
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[ P[\text{deck in order } \sigma \in S_{52}] = \frac{1}{52!}. \]

Call a shuffle *ergodic* if it mixes up the deck:

\[ \lim_{k \to \infty} P[\Sigma_k = \sigma] = \frac{1}{52!}. \]
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[ \mathbb{P}[\text{deck in order } \sigma \in S_{52}] = \frac{1}{52!}. \]

Call a shuffle *ergodic* if it mixes up the deck:

\[ \lim_{k \to \infty} \mathbb{P}[\Sigma_k = \sigma] = \frac{1}{52!}. \]

That is the distribution of \( \Sigma_k \) converges to the uniform distribution.
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[ \mathbb{P}\text{[deck in order } \sigma \in S_{52}] = \frac{1}{52!}. \]

Call a shuffle \textit{ergodic} if it mixes up the deck:

\[ \lim_{k \to \infty} \mathbb{P}[\Sigma_k = \sigma] = \frac{1}{52!}. \]

That is the distribution of \( \Sigma_k \) converges to the uniform distribution.

▶ \textit{Cutting the Deck:}
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[ \mathbb{P}[\text{deck in order } \sigma \in S_{52}] = \frac{1}{52!}. \]

Call a shuffle ergodic if it mixes up the deck:

\[ \lim_{k \to \infty} \mathbb{P}[\Sigma_k = \sigma] = \frac{1}{52!}. \]

That is the distribution of \( \Sigma_k \) converges to the uniform distribution.

▶ Cutting the Deck: Is this an ergodic shuffle?
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[ \mathbb{P}[\text{deck in order } \sigma \in S_{52}] = \frac{1}{52!}. \]

Call a shuffle \textit{ergodic} if it mixes up the deck:

\[ \lim_{k \to \infty} \mathbb{P}[\Sigma_k = \sigma] = \frac{1}{52!}. \]

That is the distribution of \( \Sigma_k \) converges to the uniform distribution.

▶ \textit{Cutting the Deck:} Is this an ergodic shuffle?

\[ A\heartsuit, 3\heartsuit, 2\heartsuit, 4\heartsuit, 5\heartsuit, 6\heartsuit, \ldots, K\clubsuit? \]
Card Shuffling

What is the aim of card shuffling? What does it mean to say that a deck of cards is mixed up?

\[ \mathbb{P} \text{[deck in order } \sigma \in S_{52}] = \frac{1}{52!}. \]

Call a shuffle *ergodic* if it mixes up the deck:

\[ \lim_{k \to \infty} \mathbb{P} [\Sigma_k = \sigma] = \frac{1}{52!}. \]

That is the distribution of \( \Sigma_k \) converges to the uniform distribution.

▶ Cutting the Deck: Is this an ergodic shuffle?

\[ A\heartsuit, 3\heartsuit, 2\heartsuit, 4\heartsuit, 5\heartsuit, 6\heartsuit, \ldots, K\clubsuit? \]

Cutting the Deck is *reducible* — not every order is possible. An ergodic shuffle must be *irreducible*. 
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_\nu := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \}. \]
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_{\nu} := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \}. \]

Definition

A shuffle \( \nu \) is *irreducible* if \( S_{\nu} \) generates \( S_{52} \).
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_\nu := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \} . \]

Definition

A shuffle \( \nu \) is irreducible if \( S_\nu \) generates \( S_{52} \).

- **Adjacent Transpositions:**

There is a periodicity with:

\[ \Sigma_{2 \ell} \in A_{52} \text{, and } \Sigma_{2 \ell + 1} \text{ an odd permutation.} \]
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_\nu := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \}. \]

**Definition**

A shuffle \( \nu \) is *irreducible* if \( S_\nu \) generates \( S_{52} \).

▶ *Adjacent Transpositions*: The shuffle uniform on adjacent transpositions:

\[ \nu_{AT}((i \ i + 1)) = \frac{1}{51}, \]

is irreducible.
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_\nu := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \}. \]

Definition

A shuffle \( \nu \) is **irreducible** if \( S_\nu \) generates \( S_{52} \).

- **Adjacent Transpositions**: The shuffle uniform on adjacent transpositions:

\[ \nu_{\text{AT}}(i, i + 1) = \frac{1}{51}, \]

is irreducible. Is it an ergodic shuffle?
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_\nu := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \}. \]

**Definition**

A shuffle \( \nu \) is *irreducible* if \( S_\nu \) generates \( S_{52} \).

▶ **Adjacent Transpositions**: The shuffle uniform on adjacent transpositions:

\[ \nu_{\text{AT}}((i \ i + 1)) = \frac{1}{51}, \]

is irreducible. Is it an ergodic shuffle?

\[ \Sigma_{2\ell} = A\spadesuit, 3\spadesuit, 2\spadesuit, 4\spadesuit, 5\spadesuit, 6\spadesuit, \ldots, K\clubsuit? \]
Irreducible Shuffles and More Examples

Define the support of the shuffle by

\[ S_\nu := \{ \sigma \in S_{52} : \nu(\sigma) > 0 \}. \]

Definition

A shuffle \( \nu \) is irreducible if \( S_\nu \) generates \( S_{52} \).

- **Adjacent Transpositions**: The shuffle uniform on adjacent transpositions:

\[ \nu_{\text{AT}}((i \quad i + 1)) = \frac{1}{51}, \]

is irreducible. Is it an ergodic shuffle?

\[ \Sigma_{2\ell} = A\heartsuit, 3\heartsuit, 2\heartsuit, 4\heartsuit, 5\heartsuit, 6\heartsuit, \ldots, K\clubsuit? \]

There is a periodicity with:

\[ \Sigma_{2\ell} \in A_{52}, \]

and \( \Sigma_{2\ell+1} \) an odd permutation.
Some Ergodic Shuffles

- **Random Transpositions (!):**

  Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

- **Random to Top:** Consider the (random) time $T$ when all the cards have been touched. The Coupon Collector's Problem shows that $T \approx 52 \ln 52 \approx 200$.

- **Riffle Shuffle:** Bayer & Diaconis show that after six imperfect riffle shuffles the deck is 'close' to mixed up. This can be explained qualitatively using the concept of a descent.

The question of what card shuffles are ergodic goes back to Markov (1906), and Borel (1940).
Some Ergodic Shuffles

► *Random Transpositions (!):* Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. 

► *Random to Top:* Consider the (random) time $T$ when all the cards have been touched. The *Coupon Collector's Problem* shows that $T \approx 52 \ln 52 \approx 200$.

► *Riffle Shuffle:* Bayer & Diaconis show that after six imperfect riffle shuffles the deck is 'close' to mixed up. This can be explained qualitatively using the concept of a *descent*.

The question of what card shuffles are ergodic goes back to Markov (1906), and Borel (1940).
Some Ergodic Shuffles

- **Random Transpositions (!):** Let $\nu_{\text{RT}}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{\text{RT}}}$.
Some Ergodic Shuffles

- **Random Transpositions (!):** Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

- **Random to Top:**

- **Riffle Shuffle:** Bayer & Diaconis show that after six imperfect riffle shuffles the deck is 'close' to mixed up. This can be explained qualitatively using the concept of a descent. The question of what card shuffles are ergodic goes back to Markov (1906), and Borel (1940).
Some Ergodic Shuffles

- **Random Transpositions (!):** Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

- **Random to Top:** Consider the (random) time $T$ when all the cards have been touched.
Some Ergodic Shuffles

- **Random Transpositions (!):** Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

- **Random to Top:** Consider the (random) time $T$ when all the cards have been touched. The *Coupon Collector’s Problem* shows that $T \approx 52 \ln 52 \approx 200$.

---

Riffle Shuffle:
Bayer & Diaconis show that after six imperfect riffle shuffles the deck is ‘close’ to mixed up. This can be explained qualitatively using the concept of a descent.

The question of what card shuffles are ergodic goes back to Markov (1906), and Borel (1940).
Some Ergodic Shuffles

- **Random Transpositions (!):** Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

- **Random to Top:** Consider the (random) time $T$ when all the cards have been touched. The *Coupon Collector’s Problem* shows that $T \approx 52 \ln 52 \approx 200$.

- **Riffle Shuffle:**
Some Ergodic Shuffles

▶ **Random Transpositions (!):** Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

▶ **Random to Top:** Consider the (random) time $T$ when all the cards have been touched. The *Coupon Collector’s Problem* shows that $T \approx 52 \ln 52 \approx 200$.

▶ **Riffle Shuffle:** Bayer & Diaconis show that after six imperfect riffle shuffles the deck is ‘close’ to mixed up. This can be explained qualitatively using the concept of a descent.
Some Ergodic Shuffles

- **Random Transpositions (!):** Let $\nu_{RT}$ be the shuffle that independently chooses $i, j \in \{1, \ldots, 52\}$ and applies the (possibly identity) transposition $(i \ j)$. This shuffle is irreducible and avoids a periodicity with $e \in S_{\nu_{RT}}$.

- **Random to Top:** Consider the (random) time $T$ when all the cards have been touched. The Coupon Collector’s Problem shows that $T \approx 52 \ln 52 \approx 200$.

- **Riffle Shuffle:** Bayer & Diaconis show that after six imperfect riffle shuffles the deck is ‘close’ to mixed up. This can be explained qualitatively using the concept of a descent.

The question of what card shuffles are ergodic goes back to Markov (1906), and Borel (1940).
Random Walks on Finite Groups

This generalises to the study of random walks on finite groups, where, for $G$ a finite group, ‘shuffles’ $s_i \overset{\text{i.i.d.}}{\sim} \nu \in M_p(G)$ (the ‘driving probability’), and the position of the walk after $k$ steps given by:

$$\xi_k = s_k \cdots s_1.$$
Random Walks on Finite Groups

This generalises to the study of random walks on finite groups, where, for $G$ a finite group, ‘shuffles’ $s_i \overset{i.i.d.}{\sim} \nu \in M_p(G)$ (the ‘driving probability’), and the position of the walk after $k$ steps given by:

$$\xi_k = s_k \cdots s_1.$$ 

▶ Quaternion Group:
Random Walks on Finite Groups

This generalises to the study of random walks on finite groups, where, for $G$ a finite group, ‘shuffles’ $s_i \sim \nu \in M_p(G)$ (the ‘driving probability’), and the position of the walk after $k$ steps given by:

$$\xi_k = s_k \cdots s_1.$$ 

- **Quaternion Group**: If $S_\nu \subseteq \{1, -1, i, -i\}$ then the random walk is reducible because the support is concentrated on the subgroup $\langle i \rangle$. 

Random Walks on Finite Groups

This generalises to the study of random walks on finite groups, where, for \( G \) a finite group, ‘shuffles’ \( s_i \overset{\text{i.i.d.}}{\sim} \nu \in M_p(G) \) (the ‘driving probability’), and the position of the walk after \( k \) steps given by:

\[
\xi_k = s_k \cdots s_1.
\]

- **Quaternion Group**: If \( S_\nu \subseteq \{1, -1, i, -i\} \) then the random walk is reducible because the support is concentrated on the subgroup \( \langle i \rangle \).

The support of the reducible Cut the Deck shuffle is a copy of \( \mathbb{Z}_{52} < S_{52} \):
Random Walks on Finite Groups

This generalises to the study of random walks on finite groups, where, for $G$ a finite group, ‘shuffles’ $s_i \sim \nu \in M_p(G)$ (the ‘driving probability’), and the position of the walk after $k$ steps given by:

$$\xi_k = s_k \cdots s_1.$$ 

- **Quaternion Group**: If $S_\nu \subseteq \{1, -1, i, -i\}$ then the random walk is reducible because the support is concentrated on the subgroup $\langle i \rangle$.

The support of the reducible *Cut the Deck* shuffle is a copy of $\mathbb{Z}_{52} < S_{52}$:

$$S_\nu \subseteq H < G \Rightarrow \nu \text{ reducible.}$$
Random Walks on Finite Groups

▶ Walk on Even Circle:

Let \( \nu \in \mathcal{M}_p(\mathbb{Z}_2^n) \) be given by 
\[
\nu(\pm 1) = \frac{1}{2}.
\]
It is irreducible — but has a periodicity — because 
\[
S_\nu \text{ is concentrated on the coset of a normal subgroup: } S_\nu \subset 2\mathbb{Z}_2^n \{1\} \quad \text{and} \quad 2\mathbb{Z}_2^n \triangleleft \mathbb{Z}_2^n.
\]

Similarly for the Adjacent Transposition shuffle: 
\[
S_\nu \text{ AT } \subset A_{52}(1 2) \quad \text{and} \quad A_{52} \triangleleft S_{52}.
\]

Indeed, where \( \xi_k \) is the location of the walk after \( k \) steps, as 
\[
\xi_k \in N_g \cdots N_g = N_{g^k},
\]
\( S_\nu \subset N_g \) and 
\( N \triangleleft G \Rightarrow \xi_k \) has a periodicity.

These necessary conditions are in fact sufficient for ergodicity of the random walk driven by \( \nu \in \mathcal{M}_p(\mathcal{G}) \).
Random Walks on Finite Groups

- **Walk on Even Circle**: Let $\nu \in M_p(\mathbb{Z}_{2n})$ be given by $\nu(\pm 1) = \frac{1}{2}$. 

It is irreducible — but has a periodicity — because $S_{\nu}$ is concentrated on the coset of a normal subgroup: $S_{\nu} \subset 2\mathbb{Z}_{2n}$ and $2\mathbb{Z}_{2n} \vartriangleleft \mathbb{Z}_{2n}$.

Similarly for the Adjacent Transposition shuffle: $S_{\nu} \subset A_{52}(1 \ 2)$ and $A_{52} \vartriangleleft S_{52}$.

Indeed, where $\xi_k$ is the location of the walk after $k$ steps, as $\xi_k \in Ng \cdots Ng = Ng^k$, $S_{\nu} \subset Ng$ and $N \vartriangleleft G \Rightarrow \xi_k$ has a periodicity.

These necessary conditions are in fact sufficient for ergodicity of the random walk driven by $\nu \in M_p(\mathbb{Z}_{2n})$. 
Random Walks on Finite Groups

- **Walk on Even Circle**: Let \( \nu \in M_p(\mathbb{Z}_{2n}) \) be given by \( \nu(\pm 1) = \frac{1}{2} \). It is irreducible.
Walk on Even Circle: Let \( \nu \in M_p(\mathbb{Z}_{2n}) \) be given by \( \nu(\pm 1) = \frac{1}{2} \). It is irreducible — but has a periodicity — because \( S_\nu \) is concentrated on the coset of a normal subgroup:

\[
S_\nu \subset 2\mathbb{Z}_{2n}\{1\} \quad \text{and} \quad 2\mathbb{Z}_{2n} \triangleleft \mathbb{Z}_{2n}.
\]
Random Walks on Finite Groups

- **Walk on Even Circle**: Let $\nu \in M_p(\mathbb{Z}_{2n})$ be given by $\nu(\pm 1) = \frac{1}{2}$. It is irreducible — but has a periodicity — because $S_\nu$ is concentrated on the coset of a normal subgroup:

  $$S_\nu \subset 2\mathbb{Z}_{2n}\{1\} \text{ and } 2\mathbb{Z}_{2n} \triangleleft \mathbb{Z}_{2n}.$$

  Similarly for the Adjacent Transposition shuffle:

  $$S_{\nu_{\text{AT}}} \subset A_{52}(1 \ 2) \text{ and } A_{52} \triangleleft S_{52}.$$
Random Walks on Finite Groups

- **Walk on Even Circle:** Let $\nu \in M_p(\mathbb{Z}_{2n})$ be given by $\nu(\pm 1) = \frac{1}{2}$. It is irreducible — but has a periodicity — because $S_\nu$ is concentrated on the coset of a normal subgroup:

  $$S_\nu \subset 2\mathbb{Z}_{2n}\{1\} \text{ and } 2\mathbb{Z}_{2n} \triangleleft \mathbb{Z}_{2n}.$$ 

  Similarly for the Adjacent Transposition shuffle:

  $$S_{\nu_{AT}} \subset A_{52}(1 \ 2) \text{ and } A_{52} \triangleleft S_{52}.$$ 

  Indeed, where $\xi_k$ is the location of the walk after $k$ ‘steps’, as $\xi_k \in Ng \cdots Ng = Ng^k$,

  $$S_\nu \subset Ng \text{ and } N \triangleleft G \Rightarrow \xi_k \text{ has a periodicity.}$$
Walk on Even Circle: Let $\nu \in M_p(\mathbb{Z}_{2n})$ be given by $\nu(\pm 1) = \frac{1}{2}$. It is irreducible — but has a periodicity — because $S_\nu$ is concentrated on the coset of a normal subgroup:

$$S_\nu \subset 2\mathbb{Z}_{2n}\{1\} \text{ and } 2\mathbb{Z}_{2n} \triangleleft \mathbb{Z}_{2n}.$$  

Similarly for the Adjacent Transposition shuffle:

$$S_{\nu_{AT}} \subset A_{52}(1 \ 2) \text{ and } A_{52} \triangleleft S_{52}.$$  

Indeed, where $\xi_k$ is the location of the walk after $k$ ‘steps’, as $\xi_k \in Ng \cdots Ng = Ng^k$,

$$S_\nu \subset Ng \text{ and } N \triangleleft G \Rightarrow \xi_k \text{ has a periodicity.}$$  

These necessary conditions are in fact sufficient for ergodicity of the random walk driven by $\nu \in M_p(G)$. 

Ergodic Theorem for Random Walks on Finite Groups

Theorem

A random walk is ergodic iff the support is not concentrated on a proper subgroup nor the coset of a normal subgroup.

Proof Illustration ([McC10] for more): Consider the quaternion group, $Q_8$, with generators $S =: S = \{i, j\}$. 

Define $L_S(e)$ as the set of minimal $S$-presentations of $e$. 

$L_S(e) = \{i^4, \ldots, (ij)^2i^2, ji^3, ji, (ij)^4, (ji)^4\}$. 
Ergodic Theorem for Random Walks on Finite Groups

Theorem
A random walk is ergodic iff the support is not concentrated on a proper subgroup nor the coset of a normal subgroup.

Proof Illustration ([McC10] for more): Consider the quaternion group, $Q_8$, with generators $S_\nu =: S = \{i, j\}$. Define $L_S(e)$ as the set of minimal $S$-presentations of $e$. 

$L_S(e) = \{i^4, \ldots, (ij)^2, i^2, ji^3, ji^4, \ldots, (ij)^4, (ji)^4\}$. 

Ergodic Theorem for Random Walks on Finite Groups

Theorem

A random walk is ergodic iff the support is not concentrated on a proper subgroup nor the coset of a normal subgroup.

Proof Illustration ([McC10] for more): Consider the quaternion group, $Q_8$, with generators $S_\nu =: S = \{i, j\}$. Define $L_S(e)$ as the set of minimal $S$-presentations of $e$.

$$L_S(e) = \{i^4, \ldots, (ij)^2i^2, ji^3ji, \ldots, (ij)^2j^2, (ij)^4, (ji)^4\}.$$
Ergodic Theorem for Random Walks on Finite Groups

Theorem

A random walk is ergodic iff the support is not concentrated on a proper subgroup nor the coset of a normal subgroup.

Proof Illustration ([McC10] for more): Consider the quaternion group, $Q_8$, with generators $S_\nu =: S = \{i, j\}$. Define $L_S(e)$ as the set of minimal $S$-presentations of $e$. 

$$L_S(e) = \{i^4, \ldots, (ij)^2 i^2, ji^3 ji, \ldots, (ij)^2 j^2, (ij)^4, (ji)^4\}.$$
Ergodic Theorem for Random Walks on Finite Groups

Let $L$ be the set of word lengths of $L_S(e)$, and $P := \gcd L$; so that e.g. $L = \{4, 6, 8\}$ and $P = 2 \neq 1$. 
Ergodic Theorem for Random Walks on Finite Groups

Let $L$ be the set of word lengths of $L_S(e)$, and $P := \gcd L$; so that e.g. $L = \{4, 6, 8\}$ and $P = 2 \neq 1$. It can be shown in this case that the support is concentrated on the coset of a proper normal subgroup.
Let $L$ be the set of word lengths of $L_S(e)$, and $P := \gcd L$; so that e.g. $L = \{4, 6, 8\}$ and $P = 2 \neq 1$. It can be shown in this case that the support is concentrated on the coset of a proper normal subgroup. The following uses $P = 2$ for ease of illustration.

Let $N_2 \subset Q_8$ be the subgroup of elements with a length $2 \cdot \ell S$-presentation.
Ergodic Theorem for Random Walks on Finite Groups

Let $L$ be the set of word lengths of $L_S(e)$, and $P := \gcd L$; so that e.g. $L = \{4, 6, 8\}$ and $P = 2 \neq 1$. It can be shown in this case that the support is concentrated on the coset of a proper normal subgroup. The following uses $P = 2$ for ease of illustration.

Let $N_2 \subset Q_8$ be the subgroup of elements with a length $2 \cdot \ell$ $S$-presentation. Let $t \in Q_8$ have a length $k$ $S$-presentation so that $t^{-1} = e$ has a length $2 \cdot \ell_e$.
Ergodic Theorem for Random Walks on Finite Groups

Let $L$ be the set of word lengths of $L_S(e)$, and $P := \gcd L$; so that e.g. $L = \{4, 6, 8\}$ and $P = 2 \neq 1$. It can be shown in this case that the support is concentrated on the coset of a proper normal subgroup. The following uses $P = 2$ for ease of illustration.

Let $N_2 \subset Q_8$ be the subgroup of elements with a length $2 \cdot \ell$ $S$-presentation. Let $t \in Q_8$ have a length $k$ $S$-presentation so that

\[
\begin{align*}
t &\quad t^{-1} = e \\
\text{length } k &\quad \text{length } 2 \cdot \ell_e
\end{align*}
\]

This means that $t^{-1}$ has a length $(2 \cdot \ell_e - k)$ $S$-presentation.
Ergodic Theorem for Random Walks on Finite Groups

Let $L$ be the set of word lengths of $L_S(e)$, and $P := \gcd L$; so that e.g. $L = \{4, 6, 8\}$ and $P = 2 \neq 1$. It can be shown in this case that the support is concentrated on the coset of a proper normal subgroup. The following uses $P = 2$ for ease of illustration.

Let $N_2 \subset Q_8$ be the subgroup of elements with a length $2 \cdot \ell$ $S$-presentation. Let $t \in Q_8$ have a length $k$ $S$-presentation so that

$$t^{-1} = e$$

length $k$  \hspace{1cm}  length $2 \cdot \ell_e$

This means that $t^{-1}$ has a length $(2 \cdot \ell_e - k)$ $S$-presentation. Consider for $g \in N_2$

$$t^{-1}, \quad g, \quad t \in N_2$$

length $2 \cdot \ell_e - k$  \hspace{1cm}  length $2 \cdot \ell_g$  \hspace{1cm}  length $k$

as it has a length $2 \cdot (\ell_e + \ell_g)$ $S$-presentation. Thus $N_2$, in this case $\langle k \rangle$, is normal.
Ergodic Theorem for Random Walks on Finite Groups

Let \( \sigma_1 \in S \) and suppose \( \sigma_1 \in N_2 \) has length \( 2 \cdot \ell \):

\[
\sigma_1 \quad \overbrace{\sigma_1^{-1}}^{\text{length } 2 \cdot \ell_{e-1}} \quad \overset{!}{=} \quad e \quad \overbrace{\text{length } 2 \cdot \ell_e},
\]

which is impossible.
Ergodic Theorem for Random Walks on Finite Groups

Let $\sigma_1 \in S$ and suppose $\sigma_1 \in N_2$ has length $2 \cdot \ell$:

$$\begin{align*}
\sigma_1 & \quad \sigma_1^{-1} \quad \equiv \\
\text{length } 2 \cdot \ell & \quad \text{length } 2 \cdot \ell_{e-1}
\end{align*}$$

which is impossible.

Therefore $N_2$ is proper and consider for $\sigma_2 \in S$:

$$\begin{align*}
\sigma_2 & \quad \sigma_1^{-1} \quad \in \\
\text{length } 1 & \quad \text{length } 2 \cdot \ell - 1
\end{align*}$$
Let $\sigma_1 \in S$ and suppose $\sigma_1 \in N_2$ has length $2 \cdot \ell$: 

$$
\begin{array}{ccc}
\sigma_1 & \sigma_1^{-1} & \equiv \\
\text{length } 2 \cdot \ell & \text{length } 2 \cdot \ell - 1 & \text{length } 2 \cdot \ell
\end{array}
$$

which is impossible.

Therefore $N_2$ is proper and consider for $\sigma_2 \in S$: 

$$
\begin{array}{ccc}
\sigma_2 & \sigma_1^{-1} & \in N_2 \Rightarrow S \subset N_2 \sigma_1.
\end{array}
$$
Ergodic Theorem for Random Walks on Finite Groups

Let $\sigma_1 \in S$ and suppose $\sigma_1 \in N_2$ has length $2 \cdot \ell$:

$$
\begin{align*}
\sigma_1 & \quad \sigma_1^{-1} \quad \overset{!}{=} \quad e \\
\text{length } 2 \cdot \ell & \quad \text{length } 2 \cdot \ell_e - 1 & \quad \text{length } 2 \cdot \ell_e
\end{align*}
$$

which is impossible.

Therefore $N_2$ is proper and consider for $\sigma_2 \in S$:

$$
\begin{align*}
\sigma_2 & \quad \sigma_1^{-1} \quad \overset{!}{\in} \quad N_2 \\
\text{length } 1 & \quad \text{length } 2 \cdot \ell - 1 & \quad \text{length } 2 \cdot \ell
\end{align*}
$$

This argument shows that if $\gcd L =: P > 1$, $N_P$ is a proper normal subgroup,
Ergodic Theorem for Random Walks on Finite Groups

Let \( \sigma_1 \in S \) and suppose \( \sigma_1 \in N_2 \) has length \( 2 \cdot \ell \):

\[
\sigma_1 \quad \sigma_1^{-1} \quad e
\]

\[
\text{length } 2 \cdot \ell \quad \text{length } 2 \cdot \ell - 1 \quad \text{length } 2 \cdot \ell
\]

which is impossible.

Therefore \( N_2 \) is proper and consider for \( \sigma_2 \in S \):

\[
\sigma_2 \quad \sigma_1^{-1} \quad e
\]

\[
\text{length } 1 \quad \text{length } 2 \cdot \ell - 1 \quad \text{length } 2 \ell
\]

\( \in N_2 \Rightarrow S \subset N_2 \sigma_1 \).

This argument shows that if \( \gcd L =: P > 1 \), \( N_P \) is a proper normal subgroup, and \( S \) is concentrated on a coset of it.
Ergodic Theorem for Random Walks on Finite Groups

Therefore assume that \( \gcd L = P = 1 \).
Ergodic Theorem for Random Walks on Finite Groups

Therefore assume that $\gcd L = P = 1$. For example $S_3$ with $S = \{(1 \ 2), (1 \ 3 \ 2)\}$:
Therefore assume that $\gcd L = P = 1$. For example $S_3$ with $S = \{(1 \ 2), (1 \ 3 \ 2)\}$:

Recall $L$ is, essentially, the set of lengths of loops in this Cayley graph. Note that $\gcd L = P = 1$. Take a subset $\{\ell_1, \ldots, \ell_m\}$ of $L$ with a gcd of one, e.g. $\{\ell_1, \ell_2\} = \{2, 3\}$. 

Ergodic Theorem for Random Walks on Finite Groups

Therefore assume that $\gcd L = P = 1$. For example $S_3$ with $S = \{(1 \ 2), (1 \ 3 \ 2)\}$:

Recall $L$ is, essentially, the set of lengths of loops in this Cayley graph. Note that $\gcd L = P = 1$. Take a subset $\{\ell_1, \ldots, \ell_m\}$ of $L$ with a gcd of one, e.g. $\{\ell_1, \ell_2\} = \{2, 3\}$. Using Bezout’s Identity, there exist integers $k_1, k_2$ such that

$$\ell_1 k_1 + \cdots + \ell_m k_m = 1,$$
Ergodic Theorem for Random Walks on Finite Groups

Therefore assume that $\gcd(L) = P = 1$. For example $S_3$ with $S = \{(1 \ 2), (1 \ 3 \ 2)\}$:

Recall $L$ is, essentially, the set of lengths of loops in this Cayley graph. Note that $\gcd(L) = P = 1$. Take a subset $\{\ell_1, \ldots, \ell_m\}$ of $L$ with a gcd of one, e.g. $\{\ell_1, \ell_2\} = \{2, 3\}$. Using Bezout’s Identity, there exist integers $k_1, k_2$ such that

$$\ell_1k_1 + \cdots + \ell_mk_m = 1,$$

for example $2(-1) + 3(1) = 1$. 
Ergodic Theorem for Random Walks on Finite Groups

From this we can construct a number $M$ such that for all $N \geq M$, \( e \) has a length-$N$ $S$-presentation.

Let $N = rM + a$ with $r \geq 1$, and $0 \leq a < r$:

$$N = rM + a \left( m \sum_{i=1}^{\infty} \ell_{i_k} \right) = m \sum_{i=1}^{\infty} \left( \ell_{i_k} (r |k_i| + ak_i) \right) > 0$$

Observe there are loops of length $\ell_{i_k}$, and so $e$ has a length-$N$ $S$-presentation. So, for e.g. $N = 5, 6, 7, ...$; $e \in S_3$ has a length-$N$ $S$-presentation.
Ergodic Theorem for Random Walks on Finite Groups

From this we can construct a number $M$ such that for all $N \geq M$, $e$ has a length-$N$ $S$-presentation. It is

$$M = \sum_{i=1}^{m} \ell_i |k_i|,$$

e.g.

$$M = 2|−1| + 3|1| = 5.$$
From this we can construct a number $M$ such that for all $N \geq M$, $e$ has a length-$N$ $S$-presentation. It is

$$M = \sum_{i=1}^{m} \ell_i |k_i|,$$

e.g.

$$M = 2|−1| + 3|1| = 5.$$

Let $N = rM + a$ with $r \geq 1$, and $0 \leq a < r$:

$$N = rM + a \left( \sum_{i=1}^{m} \ell_i k_i \right) = \sum_{i=1}^{m} \left[ \ell_i (r |k_i| + ak_i) \right]_{>0}.$$
Ergodic Theorem for Random Walks on Finite Groups

From this we can construct a number $M$ such that for all $N \geq M$, $e$ has a length-$N S$-presentation. It is

$$M = \sum_{i=1}^{m} \ell_i |k_i|,$$

e.g.

$$M = 2|-1| + 3|1| = 5.$$

Let $N = rM + a$ with $r \geq 1$, and $0 \leq a < r$:

$$N = rM + a \left( \sum_{i=1}^{m} \ell_i k_i \right) = \sum_{i=1}^{m} \left[ \ell_i (r|k_i| + ak_i) \right] > 0$$

Observe there are loops of length $\ell_i$, and so $e$ has a length-$N S$-presentation. So, for e.g. $N = 5, 6, 7, \ldots; e \in S_3$ has a length-$N S$-presentation.
Ergodic Theorem for Random Walks on Finite Groups

Assuming irreducibility, each element $s$ has a length-$n_s$ $S$-presentation.

Let $n^*$ be the maximum of these and consider:

$M, M + 1, \ldots, M + n^* - n_s, \ldots, M + n^* =: M^*$.

Every group element has a length $M^*$ $S$-presentation. Simply loop back to $e$ after $M + n^* - n_s$ steps, and then take $n_s$ more.

For $S_3$, $M = 5$ and $M^* = 7$:

Thus for every element $s$, there is a non-zero probability of $\xi_{M^*} = s$. Markov Chain machinery shows this implies ergodicity.
Assuming irreducibility, each element $s$ has a length-$n_s$ $S$-presentation. Let $n^*$ be the maximum of these and consider:

$$M, M + 1, \ldots, M + n^* - n_s, \ldots, M + n^* =: M^*.$$
Ergodic Theorem for Random Walks on Finite Groups

Assuming irreducibility, each element $s$ has a length-$n_s$ $S$-presentation. Let $n^*$ be the maximum of these and consider:

$$M, M + 1, \ldots, M + n^* - n_s, \ldots, M + n^* =: M^*.$$ 

Every group element has a length $M^*$ $S$-presentation. Simply loop back to $e$ after $M + n^* - n_s$ steps, and then take $n_s$ more.
Ergodic Theorem for Random Walks on Finite Groups

Assuming irreducibility, each element $s$ has a length-$n_s$ $S$-presentation. Let $n^*$ be the maximum of these and consider:

$$M, M + 1, \ldots, M + n^* - n_s, \ldots, M + n^* =: M^*.$$ 

Every group element has a length $M^*$ $S$-presentation. Simply loop back to $e$ after $M + n^* - n_s$ steps, and then take $n_s$ more.

For $S_3$, $M = 5$ and $M^* = 7$: 

![Diagram showing a random walk on $S_3$ with nodes and arrows indicating transitions.](image_url)
Ergodic Theorem for Random Walks on Finite Groups

Assuming irreducibility, each element $s$ has a length-$n_s$ $S$-presentation. Let $n^*$ be the maximum of these and consider:

$$M, M + 1, \ldots, M + n^* - n_s, \ldots, M + n^* =: M^*.$$  

Every group element has a length $M^*$ $S$-presentation. Simply loop back to $e$ after $M + n^* - n_s$ steps, and then take $n_s$ more.

For $S_3$, $M = 5$ and $M^* = 7$:

Thus for every element $s$, there is a non-zero probability of $\xi_{M^*} = s$. Markov Chain machinery shows this implies ergodicity.
Finite Classical Groups aka Finite Groups

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

$$G \times G \times G \xrightarrow{m \times I_G} G \times G$$

$$I_G \times m \downarrow \quad m \downarrow$$

$$G \times G \xrightarrow{m} G$$

$$G \times G \xrightarrow{m} G \leftarrow m \quad G \times G$$

$$G \leftarrow \cong \quad \cong \rightarrow G \times \{\bullet\}$$

$$G \times G \xrightarrow{m} G \leftarrow m \quad G \times G$$

$$G \leftarrow \cong \quad \cong \rightarrow G \times \{\bullet\}$$

$$G \times G \xrightarrow{m} G \leftarrow m \quad G \times G$$

$$G \leftarrow \Delta_G \quad \Delta_G \rightarrow G \times G$$

$$G \times G \leftarrow \Delta_G \quad G \xrightarrow{\Delta_G} G \times G$$

$$S \times I_G \uparrow \quad e \circ \varepsilon \uparrow \quad I_G \times S \uparrow$$

$$G \times G \quad \text{and} \quad G \times \{\bullet\}$$
The $\mathbb{C}$-Functor

The $\mathbb{C}$-Functor, $\mathbb{C} : \text{FinSet} \rightarrow \text{FinVec}_\mathbb{C}$, 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 $f : X \rightarrow Y$, $x \mapsto f(x)$ to a morphism $\mathbb{C}f : \mathbb{C}X \rightarrow \mathbb{C}Y$, $\delta^x \mapsto \delta^{f(x)}$. 

Applying the $\mathbb{C}$-Functor to a group $G$ yields the group algebra $\mathbb{C}G$. Consider the multiplication morphism $m : G \times G \rightarrow G$ and its image under the $\mathbb{C}$-Functor, $\nabla := \mathbb{C}m$:

$\delta(g, h) \nabla \mapsto \delta^{m(g, h)} = \delta^{gh}$.

As the vector space is finite dimensional, $\mathbb{C}(G \times G) \sim = \mathbb{C}G \otimes \mathbb{C}G$ and so $\nabla : \mathbb{C}G \otimes \mathbb{C}G \rightarrow \mathbb{C}G$, $\delta_s \otimes \delta_t \mapsto \delta_{st}$.

The morphisms are extended linearly, so, for example, for the quaternion group:

$\nabla[(2 \delta_i + 3 \delta_j) \otimes (\delta_k - 2 \delta_l)] = 2 \delta_{-j} - 4 \delta_{-i} + 3 \delta_i - 6 \delta_{-j}$.
The \( \mathbb{C} \)-Functor

The \( \mathbb{C} \)-Functor, \( \mathbb{C} : \text{FinSet} \to \text{FinVec}_\mathbb{C} \), 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, \( \mathbb{C}G \). Consider the multiplication morphism \( m : G \times G \to G \) and its image under the \( \mathbb{C} \)-Functor, \( \nabla := \mathbb{C}m \):

\[
\delta(g,h) \xrightarrow{\nabla} \delta^{m(g,h)} = \delta^{gh}.
\]
The $\mathbb{C}$-Functor

The $\mathbb{C}$-Functor, $\mathbb{C}: \text{FinSet} \to \text{FinVec}_\mathbb{C}$, 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, $\mathbb{C}G$. Consider the multiplication morphism $m: G \times G \to G$ and its image under the $\mathbb{C}$-Functor, $\nabla := \mathbb{C}m$:

$$\delta(g,h) \xrightarrow{\nabla} \delta^{m(g,h)} = \delta^{gh}.$$ 

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, $\mathbb{C} : \text{FinSet} \to \text{FinVec}_\mathbb{C}$, 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, $\mathbb{C}G$. Consider the multiplication morphism $m : G \times G \to G$ and its image under the $\mathbb{C}$-Functor, $\nabla := \mathbb{C}m$:

$$\delta(g,h) \xmapsto{\nabla} \delta^{m(g,h)} = \delta^{gh}.$$  

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 morphisms are extended linearly, so, for example, for the quaternion group:

$$\nabla \left[(2\delta^i + 3\delta^j) \otimes (\delta^k - 2\delta^{-1})\right] = 2\delta^{-j} - 4\delta^{-i} + 3\delta^i - 6\delta^{-j}.$$
The $\mathbb{C}$-Functor

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

\[
\begin{align*}
\mathbb{C} G \otimes \mathbb{C} G \otimes \mathbb{C} G & \xrightarrow{\nabla \times I_{\mathbb{C} G}} \mathbb{C} G \otimes \mathbb{C} G \\
I_{\mathbb{C} G} \times \nabla & \downarrow \quad \nabla \\
\mathbb{C} G \times \mathbb{C} G & \xrightarrow{\nabla} \mathbb{C} G
\end{align*}
\]
The \( \mathbb{C} \)-Functor

As the group axioms are commutative diagrams, the group axioms are translated into “\( \mathbb{C}G \)”-group axioms. For example, associativity:

\[
\begin{array}{ccc}
\mathbb{C}G \otimes \mathbb{C}G \otimes \mathbb{C}G & \xrightarrow{\nabla \times l_{\mathbb{C}G}} & \mathbb{C}G \otimes \mathbb{C}G \\
\downarrow l_{\mathbb{C}G} \times \nabla & & \downarrow \nabla \\
\mathbb{C}G \times \mathbb{C}G & \xrightarrow{\nabla} & \mathbb{C}G 
\end{array}
\]

Recall that the dual, \( V^* \), of a finite dimensional vector space \( V \), is the vector space of all linear maps, functionals:

\[
V \rightarrow \mathbb{C}.
\]
The \( \mathbb{C} \)-Functor

As the group axioms are commutative diagrams, the group axioms are translated into “\( \mathbb{C}G \)”-group axioms. For example, associativity:

\[
\begin{align*}
\mathbb{C}G \otimes \mathbb{C}G \otimes \mathbb{C}G & \xrightarrow{\nabla \times l_{\mathbb{C}G}} \mathbb{C}G \otimes \mathbb{C}G \\
\mathbb{C}G \times \mathbb{C}G & \xrightarrow{\nabla} \mathbb{C}G
\end{align*}
\]

Recall that the dual, \( V^* \), of a finite dimensional vector space \( V \), is the vector space of all linear maps, \textit{functionals}:

\[
V \rightarrow \mathbb{C}.
\]

The dual of \( \mathbb{C}G \) is \( F(G) \) — the vector space of complex-valued functions on \( G \).
The $\mathbb{C}$-Functor

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

\[
\begin{array}{c}
\mathbb{C}G \otimes \mathbb{C}G \otimes \mathbb{C}G \\
\downarrow l_{\mathbb{C}G} \otimes \nabla \\
\mathbb{C}G \times \mathbb{C}G \\
\downarrow \nabla \\
\mathbb{C}G
\end{array}
\]

Recall that the dual, $V^*$, of a finite dimensional vector space $V$, is the vector space of all linear maps, functionals:

\[
V \to \mathbb{C}.
\]

The dual of $\mathbb{C}G$ is $F(G)$ — the vector space of complex-valued functions on $G$. As functionals are linear maps, elements of $(\mathbb{C}G)^*$ are determined by their values on basis elements; so that for an $\varphi \in (\mathbb{C}G)^*$

\[
\varphi(\delta^g) \cong \varphi(g).
\]
The Dual Endofunctor

The Dual Endofunctor, $\mathcal{D} : \text{FinVec}_\mathbb{C} \to \text{FinVec}_\mathbb{C}$, 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 ($\varphi \in V^*$):

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

The Dual Endofunctor, $\mathcal{D} : \text{FinVec}_\mathbb{C} \to \text{FinVec}_\mathbb{C}$, is a \textit{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 ($\varphi \in V^*$):

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

Applying the Dual Endofunctor to a group algebra $\mathbb{C}G$ yields the \textit{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 $Q := \mathcal{D} \circ \mathbb{C}$ — an encoding of the group axioms.
The Dual Endofunctor

The Dual Endofunctor, $\mathcal{D} : \text{FinVec}_C \to \text{FinVec}_C$, 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 ($\varphi \in V^*$):

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

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 $Q := \mathcal{D} \circ \mathbb{C}$ — an encoding of the group axioms.

This encoding has maps, the comultiplication, $\Delta := Qm$; the counit, $\varepsilon := Qe$; and the antipode, $S := Q(-1)$, that satisfy three commutative diagrams that encode associativity, identity, and inverses.
The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

The comultiplication, $\Delta := D(\nabla)$, for example:

$\Delta : F(G) \rightarrow F(G) \otimes F(G)$ is a linear map

$\Delta(\delta_g)(\delta^s \otimes \delta^t) = \delta_g(\nabla(\delta^s \otimes \delta^t)) = \delta_g(\delta^{st})$
The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

The \textit{comultiplication}, $\Delta := D(\nabla)$, for example:

$\Delta : F(G) \to F(G) \otimes F(G)$ is a linear map

$\Delta(\delta_g)(\delta^s \otimes \delta^t) = \delta_g(\nabla(\delta^s \otimes \delta^t)) = \delta_g(\delta^{st})$

$\Rightarrow \Delta(\delta_g) = \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t.$
The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

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

$$\Delta(\delta_g)(\delta^s \otimes \delta^t) = \delta_g(\nabla(\delta^s \otimes \delta^t)) = \delta_g(\delta^{st})$$

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

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

$$F(G) \xrightarrow{\Delta} F(G) \otimes F(G)$$

The encoded group axioms are called *Hopf-algebra axioms*. 
The Encoded Group Axioms (Hopf (1940s); Kac (1960s))

The comultiplication, $\Delta := D(\nabla)$, for example:

$\Delta : F(G) \rightarrow F(G) \otimes F(G)$ is a linear map

$\Delta(\delta_g)(\delta^s \otimes \delta^t) = \delta_g(\nabla(\delta^s \otimes \delta^t)) = \delta_g(\delta^{st})$

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

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

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:

\[
\begin{array}{c}
F(G) \\
G
\end{array} \overset{Q(\text{group axioms) but not } ab=ba}{\longrightarrow} \begin{array}{c}
F(G) \\
G
\end{array}
\]

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:

\[
F(G) \xrightarrow{Q \text{(group axioms) but not } ab=ba} F(G)
\]

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.
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by $\nu \in M_p(G)$. Firstly $\xi_1 \sim \nu$. For $g \in G$, what is $P[\xi_2 = g]$?

The walk can go to any $t \in G$ and onto $g \in G$: $e \rightarrow \xi_1 \rightarrow t \rightarrow \xi_2 = gt^{-1} \rightarrow g$.

Thus $P[\xi_2 = g] = \sum_{t \in G} \nu(gt^{-1}) \nu(t) = (\nu \otimes \nu)(\sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t)$.

Is this expression familiar? $P[\xi_2 = g] = (\nu \otimes \nu)\Delta(\delta_g) =: (\nu \ast \nu)(\delta_g)$, and inductively $\xi_k \sim \nu \ast k$, the distribution of the random walk after $k$ steps is given by the $k$-fold convolution $\nu \ast k$. 
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by $\nu \in M_p(G)$. Firstly $\xi_1 \sim \nu$. What is the distribution of $\xi_2$? For $g \in G$, what is $\mathbb{P}[\xi_2 = g]$?
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by \( \nu \in M_p(G) \). Firstly \( \xi_1 \sim \nu \). What is the distribution of \( \xi_2 \)? For \( g \in G \), what is \( \mathbb{P}[\xi_2 = g] \)? The walk can go to any \( t \in G \) and onto \( g \in G \):

\[
\begin{align*}
\epsilon &\rightarrow \underbrace{\xi_1}_{s_1=t} \rightarrow \underbrace{\xi_2}_{s_2=gt^{-1}} \rightarrow g.
\end{align*}
\]
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by \( \nu \in M_p(G) \). Firstly \( \xi_1 \sim \nu \). What is the distribution of \( \xi_2 \)? For \( g \in G \), what is \( P[\xi_2 = g] \)? The walk can go to any \( t \in G \) and onto \( g \in G \):

\[
\begin{align*}
& e \xrightarrow{} t \quad \xrightarrow{} \xi_1 \quad \xrightarrow{} \xi_2 \quad \xrightarrow{} g,
& s_1 = t \\
& s_2 = gt^{-1}
\end{align*}
\]

Thus

\[
P[\xi_2 = g] = \sum_{t \in G} \nu(gt^{-1})\nu(t) = (\nu \otimes \nu) \left( \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t \right).
\]
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by \( \nu \in M_p(G) \). Firstly \( \xi_1 \sim \nu \). What is the distribution of \( \xi_2 \)? For \( g \in G \), what is \( \mathbb{P}[\xi_2 = g] \)? The walk can go to any \( t \in G \) and onto \( g \in G \):

\[
\begin{align*}
e & \xrightarrow{\xi_1} t \quad \xrightarrow{\xi_2} g.
\end{align*}
\]

Thus

\[
\mathbb{P}[\xi_2 = g] = \sum_{t \in G} \nu(gt^{-1})\nu(t) = (\nu \otimes \nu) \left( \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t \right).
\]

Is this expression familiar?
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by $\nu \in \text{M}_p(G)$. Firstly $\xi_1 \sim \nu$. What is the distribution of $\xi_2$? For $g \in G$, what is $\mathbb{P}[\xi_2 = g]$? The walk can go to any $t \in G$ and onto $g \in G$:

$$
\begin{align*}
e & \rightarrow \xi_1 \quad \xi_1 \rightarrow \xi_2 \\
s_1 = t & \rightarrow t \quad s_2 = gt^{-1} \rightarrow g.
\end{align*}
$$

Thus

$$
\mathbb{P}[\xi_2 = g] = \sum_{t \in G} \nu(gt^{-1})\nu(t) = (\nu \otimes \nu) \left( \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t \right).
$$

Is this expression familiar?

$$
\mathbb{P}[\xi_2 = g] = (\nu \otimes \nu) \Delta(\delta_g) =: (\nu \ast \nu)(\delta_g),
$$

and $\xi_2 \sim \nu^2$
The Distribution of a Random Walk

Consider a random walk on a finite, classical group, driven by \( \nu \in M_p(G) \). Firstly \( \xi_1 \sim \nu \). What is the distribution of \( \xi_2 \)? For \( g \in G \), what is \( \mathbb{P}[\xi_2 = g] \)? The walk can go to any \( t \in G \) and onto \( g \in G \):

\[
\begin{align*}
& e \xrightarrow{\xi_1} t \xrightarrow{\xi_2} g. \\
& s_1 = t \quad s_2 = gt^{-1}
\end{align*}
\]

Thus

\[
\mathbb{P}[\xi_2 = g] = \sum_{t \in G} \nu(gt^{-1})\nu(t) = (\nu \otimes \nu) \left( \sum_{t \in G} \delta_{gt^{-1}} \otimes \delta_t \right).
\]

Is this expression familiar?

\[
\mathbb{P}[\xi_2 = g] = (\nu \otimes \nu) \Delta(\delta_g) =: (\nu * \nu)(\delta_g),
\]

and \( \xi_2 \sim \nu^2 \), and inductively \( \xi_k \sim \nu^k \), the distribution of the random walk after \( k \) steps is given by the \( k \)-fold convolution \( \nu^k \).
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_\nu$ on $F(G)$. 

How? 

$E_\nu(f) = \sum_{t \in G} f(t) \nu(t)$.

What is a state on $F(G)$?

▶ a linear map $E_\nu: F(G) \to C$ aka an element of $F(G)^*$ that is ▶ positive: $E_\nu(f) \geq 0$ if $f \geq 0$, and ▶ normalised: $E_\nu(1_G) = 1$.

There is a bijective correspondence between probabilities $\nu \in M_p(G)$ and states $E_\nu$ on $F(G)$. This means that there are analogues of probabilities on finite quantum groups — states on the algebras of functions. .. and also analogues of convolution: $\nu \star \nu = (\nu \otimes \nu) \Delta$. 

Take a $\nu \in M_p(G)$ and study $\nu \star k$!
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $\mathbb{E}_\nu$ on $F(G)$. How?
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_\nu$ on $F(G)$. How?

$$E_\nu(f) = \sum_{t \in G} f(t)\nu(t).$$
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_\nu$ on $F(G)$. How?

$$E_\nu(f) = \sum_{t \in G} f(t)\nu(t).$$

What is a state on $F(G)$?

▶ a linear map $E_\nu : F(G) \to \mathbb{C}$ aka an element of $F(G)^*$ that is
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $\mathbb{E}_\nu$ on $F(G)$. How?

$$\mathbb{E}_\nu(f) = \sum_{t \in G} f(t)\nu(t).$$

What is a state on $F(G)$?

- a linear map $\mathbb{E}_\nu : F(G) \to \mathbb{C}$ aka an element of $F(G)^*$ that is
- positive: $\mathbb{E}_\nu(f) \geq 0$ if $f \geq 0$
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_{\nu}$ on $F(G)$. How?

$$E_{\nu}(f) = \sum_{t \in G} f(t)\nu(t).$$

What is a state on $F(G)$?

- a linear map $E_{\nu} : F(G) \to \mathbb{C}$ aka an element of $F(G)^*$ that is
- positive: $E_{\nu}(f) \geq 0$ if $f \geq 0$, and
- normalised: $E_{\nu}(1_G) = 1$. 

There is a bijective correspondence between probabilities $\nu \in M_p(G)$ and states $E_{\nu}$ on $F(G)$.

This means that there are analogues of probabilities on finite quantum groups — states on the algebras of functions.

... and also analogues of convolution: $\nu \ast \nu = (\nu \otimes \nu)\Delta$. 

Take a $\nu \in M_p(G)$ and study $\nu \ast k!$.
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_\nu$ on $F(G)$. How?

$$E_\nu(f) = \sum_{t \in G} f(t)\nu(t).$$

What is a state on $F(G)$?

- a linear map $E_\nu : F(G) \to \mathbb{C}$ aka an element of $F(G)^*$ that is
- positive: $E_\nu(f) \geq 0$ if $f \geq 0$, and
- normalised: $E_\nu(1_G) = 1$.

There is a bijective correspondence between probabilities $\nu \in M_p(G)$ and states $E_\nu$ on $F(G)$. 

Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_\nu$ on $F(G)$. How?

$$E_\nu(f) = \sum_{t \in G} f(t)\nu(t).$$

What is a state on $F(G)$?

- a linear map $E_\nu : F(G) \to \mathbb{C}$ aka an element of $F(G)^*$ that is
- positive: $E_\nu(f) \geq 0$ if $f \geq 0$, and
- normalised: $E_\nu(1_G) = 1$.

There is a bijective correspondence between probabilities $\nu \in M_p(G)$ and states $E_\nu$ on $F(G)$.

This means that there are analogues of probabilities on finite quantum groups.
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $\mathbb{E}_\nu$ on $F(G)$. How?

$$\mathbb{E}_\nu(f) = \sum_{t \in G} f(t)\nu(t).$$

What is a state on $F(G)$?

- a linear map $\mathbb{E}_\nu : F(G) \rightarrow \mathbb{C}$ aka an element of $F(G)^*$ that is
- positive: $\mathbb{E}_\nu(f) \geq 0$ if $f \geq 0$, and
- normalised: $\mathbb{E}_\nu(1_G) = 1$.

There is a bijective correspondence between probabilities $\nu \in M_p(G)$ and states $\mathbb{E}_\nu$ on $F(G)$.

This means that there are analogues of probabilities on finite quantum groups — states on the algebras of functions.
Random Walks on... Quantum Groups?

Probabilities \( \nu \in M_p(G) \) give states \( E_\nu \) on \( F(G) \). How?

\[
E_\nu(f) = \sum_{t \in G} f(t) \nu(t).
\]

What is a state on \( F(G) \)?

- a linear map \( E_\nu : F(G) \to \mathbb{C} \) aka an element of \( F(G)^* \) that is
- positive: \( E_\nu(f) \geq 0 \) if \( f \geq 0 \), and
- normalised: \( E_\nu(1_G) = 1 \).

There is a bijective correspondence between probabilities \( \nu \in M_p(G) \) and states \( E_\nu \) on \( F(G) \).

This means that there are analogues of probabilities on finite quantum groups — states on the algebras of functions... and also analogues of convolution:
Random Walks on... Quantum Groups?

Probabilities \( \nu \in M_p(G) \) give states \( \mathbb{E}_\nu \) on \( F(G) \). How?

\[
\mathbb{E}_\nu(f) = \sum_{t \in G} f(t) \nu(t).
\]

What is a state on \( F(G) \)?

- a linear map \( \mathbb{E}_\nu : F(G) \to \mathbb{C} \) aka an element of \( F(G)^* \) that is
- positive: \( \mathbb{E}_\nu(f) \geq 0 \) if \( f \geq 0 \), and
- normalised: \( \mathbb{E}_\nu(1_G) = 1 \).

There is a bijective correspondence between probabilities \( \nu \in M_p(G) \) and states \( \mathbb{E}_\nu \) on \( F(G) \).

This means that there are analogues of probabilities on finite quantum groups — states on the algebras of functions... and also analogues of convolution: \( \nu * \nu = (\nu \otimes \nu)\Delta \).
Random Walks on... Quantum Groups?

Probabilities $\nu \in M_p(G)$ give states $E_\nu$ on $F(G)$. How?

\[ E_\nu(f) = \sum_{t \in G} f(t)\nu(t). \]

What is a state on $F(G)$?

- a linear map $E_\nu : F(G) \to \mathbb{C}$ aka an element of $F(G)^*$ that is
- positive: $E_\nu(f) \geq 0$ if $f \geq 0$, and
- normalised: $E_\nu(1_G) = 1$.

There is a bijective correspondence between probabilities $\nu \in M_p(G)$ and states $E_\nu$ on $F(G)$.

This means that there are analogues of probabilities on finite quantum groups — states on the algebras of functions... and also analogues of convolution: $\nu \star \nu = (\nu \otimes \nu)\Delta$.

Take a $\nu \in M_p(G)$ and study $\nu^*k$!
Ergodicity for Random Walks on Finite Groups

In the classical case, where $\pi$ is the uniform distribution:

$$\pi(g) = \frac{1}{|G|},$$

A random walk is ergodic if for $\nu \in M_p(G)$,

$$\nu \star k \to \pi.$$
Ergodicity for Random Walks on Finite Groups

In the classical case, where \( \pi \) is the uniform distribution:

\[
\pi(g) = \frac{1}{|G|},
\]

a random walk is ergodic if for \( \nu \in M_p(G) \),

\[
\nu^k \to \pi.
\]
Ergodicity for Random Walks on Finite Groups

In the classical case, where $\pi$ is the uniform distribution:

$$\pi(g) = \frac{1}{|G|},$$

a random walk is ergodic if for $\nu \in M_p(G)$,

$$\nu^* \rightarrow \pi.$$

The uniform distribution gives rise to a unique Haar state, the unique state on $F(G)$ such that for all states $\mu$ on $F(G)$:

$$\pi \star \mu = \pi = \mu \star \pi.$$
Ergodicity for Random Walks on Finite Groups

In the classical case, where $\pi$ is the uniform distribution:

$$\pi(g) = \frac{1}{|G|},$$

a random walk is ergodic if for $\nu \in M_p(G)$,

$$\nu^k \to \pi.$$

The uniform distribution gives rise to a unique Haar state, the unique state on $F(G)$ such that for all states $\mu$ on $F(G)$:

$$\pi \ast \mu = \pi = \mu \ast \pi.$$

Finite quantum groups also have such an invariant state, $\pi$, such that, for all states on $F(G)$,

$$(\pi \otimes \mu) \circ \Delta =: \pi \ast \mu = \pi = \mu \ast \pi := (\mu \otimes \pi)\Delta.$$
Ergodicity for Random Walks on Finite Groups

In the classical case, where $\pi$ is the uniform distribution:

$$\pi(g) = \frac{1}{|G|},$$

a random walk is ergodic if for $\nu \in M_{p}(G)$,

$$\nu^{\ast k} \to \pi.$$

The uniform distribution gives rise to a unique Haar state, the unique state on $F(G)$ such that for all states $\mu$ on $F(G)$:

$$\pi \ast \mu = \pi = \mu \ast \pi.$$

Finite quantum groups also have such an invariant state, $\pi$, such that, for all states on $F(G)$,

$$(\pi \otimes \mu) \circ \Delta =: \pi \ast \mu = \pi = \mu \ast \pi := (\mu \otimes \pi)\Delta.$$

Therefore, an ergodic random walk on a quantum group $\mathbb{G}$ is given by a state $\nu$ on $F(\mathbb{G})$ such that

$$\nu^{\ast k} \to \pi.$$
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. 
Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

$$\Delta_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g,$$

$$\varepsilon_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}, \quad \delta^g \mapsto \delta_{g,e},$$

$$S_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}.$$
Group Algebras

Consider \( \mathbb{C}G \) for a finite group \( G \). Consider the following maps:

\[
\Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g,
\]

\[
\varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}, \quad \delta^g \mapsto \delta^g_e,
\]

\[
S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}.
\]

The algebra \( \mathbb{C}G \) — with these maps — is the algebra of functions on a quantum group.
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

- $\Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G$, \( \delta^g \mapsto \delta^g \otimes \delta^g \),
- $\varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}$, \( \delta^g \mapsto \delta^g_e \),
- $S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G$, \( \delta^g \mapsto \delta^{g^{-1}} \).

The algebra $\mathbb{C}G$ — with these maps — is the algebra of functions on a quantum group. If $G$ is non-abelian, $\mathbb{C}G$ is noncommutative and the quantum group is a virtual object.
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

$$
\Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g,
$$

$$
\varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}, \quad \delta^g \mapsto \delta^g,e,
$$

$$
S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}.
$$

The algebra $\mathbb{C}G$ — with these maps — is the algebra of functions on a quantum group. If $G$ is non-abelian, $\mathbb{C}G$ is noncommutative and the quantum group is a virtual object and write $\mathbb{C}G =: F(\hat{G})$.
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

\[ \Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g, \]
\[ \varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}, \quad \delta^g \mapsto \delta^g e, \]
\[ S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}. \]

The algebra $\mathbb{C}G$ — with these maps — is the algebra of functions on a quantum group. If $G$ is non-abelian, $\mathbb{C}G$ is noncommutative and the quantum group is a virtual object and write $\mathbb{C}G =: F(\hat{G})$, $\hat{G}$ is called the dual group of $G$. 

A probability on $\hat{G}$ is a state on $F(\hat{G}) = \mathbb{C}G$. They are functionals in the dual of $\mathbb{C}G$ — but $\mathbb{C}G^* = F(G)$. Let

\[ v = \sum_{t \in G} c_t \delta_t \in F(G). \]
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

\[ \Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g, \]
\[ \varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}, \quad \delta^g \mapsto \delta^g, e, \]
\[ S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}. \]

The algebra $\mathbb{C}G$ — with these maps — is the algebra of functions on a quantum group. If $G$ is non-abelian, $\mathbb{C}G$ is noncommutative and the quantum group is a virtual object and write $\mathbb{C}G \equiv F(\hat{G})$, $\hat{G}$ is called the dual group of $G$.

A probability on $\hat{G}$ is a state on $F(\hat{G}) = \mathbb{C}G$. 
Group Algebras

Consider \( \mathbb{C}G \) for a finite group \( G \). Consider the following maps:

\[
\Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g,
\]

\[
\varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}, \quad \delta^g \mapsto \delta_{g,e},
\]

\[
S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}.
\]

The algebra \( \mathbb{C}G \) — with these maps — is the algebra of functions on a quantum group. If \( G \) is non-abelian, \( \mathbb{C}G \) is noncommutative and the quantum group is a virtual object and write \( \mathbb{C}G =: F(\hat{G}) \), \( \hat{G} \) is called the dual group of \( G \).

A probability on \( \hat{G} \) is a state on \( F(\hat{G}) = \mathbb{C}G \). They are functionals in the dual of \( \mathbb{C}G \).
Group Algebras

Consider \( \mathbb{C}G \) for a finite group \( G \). Consider the following maps:

\[
\Delta_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g,
\]
\[
\varepsilon_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}, \quad \delta^g \mapsto \delta^g_e,
\]
\[
S_{\mathbb{C}G} : \mathbb{C}G \to \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}.
\]

The algebra \( \mathbb{C}G \) — with these maps — is the algebra of functions on a quantum group. If \( G \) is non-abelian, \( \mathbb{C}G \) is noncommutative and the quantum group is a virtual object and write \( \mathbb{C}G =: F(\hat{G}) \), \( \hat{G} \) is called the dual group of \( G \).

A probability on \( \hat{G} \) is a state on \( F(\hat{G}) = \mathbb{C}G \). They are functionals in the dual of \( \mathbb{C}G \) — but \( \mathbb{C}G^* = F(G) \).
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

$\Delta_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}G \otimes \mathbb{C}G$, \hspace{1em} $\delta g \mapsto \delta g \otimes \delta g$,

$\varepsilon_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}$, \hspace{1em} $\delta g \mapsto \delta g, e$,

$S_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}G$, \hspace{1em} $\delta g \mapsto \delta g^{-1}$.

The algebra $\mathbb{C}G$ — with these maps — is the algebra of functions on a quantum group. If $G$ is non-abelian, $\mathbb{C}G$ is noncommutative and the quantum group is a virtual object and write $\mathbb{C}G =: F(\hat{G})$, $\hat{G}$ is called the dual group of $G$.

A probability on $\hat{G}$ is a state on $F(\hat{G}) = \mathbb{C}G$. They are functionals in the dual of $\mathbb{C}G$ — but $\mathbb{C}G^* = F(G)$. Let

$$v = \sum_{t \in G} c_t \delta_t \in F(G).$$
Group Algebras

Consider $\mathbb{C}G$ for a finite group $G$. Consider the following maps:

$$\Delta_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}G \otimes \mathbb{C}G, \quad \delta^g \mapsto \delta^g \otimes \delta^g,$$

$$\varepsilon_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}, \quad \delta^g \mapsto \delta^g,e,$$

$$S_{\mathbb{C}G} : \mathbb{C}G \rightarrow \mathbb{C}G, \quad \delta^g \mapsto \delta^{g^{-1}}.$$

The algebra $\mathbb{C}G$ — with these maps — is the algebra of functions on a quantum group. If $G$ is non-abelian, $\mathbb{C}G$ is noncommutative and the quantum group is a virtual object and write $\mathbb{C}G =: F(\hat{G})$, $\hat{G}$ is called the dual group of $G$.

A probability on $\hat{G}$ is a state on $F(\hat{G}) = \mathbb{C}G$. They are functionals in the dual of $\mathbb{C}G$ — but $\mathbb{C}G^* = F(G)$. Let

$$\nu = \sum_{t \in G} c_t \delta_t \in F(G).$$

The involution is given by:

$$\nu^* = \sum_{t \in G} c_t \delta_{t^{-1}}.$$
Ergodic Theorem for Random Walks on Dual Groups

Positive elements in $\mathbb{C}G$ are of the form $u = \nu^* \nu$ and are called positive definite functions.
Ergodic Theorem for Random Walks on Dual Groups

Positive elements in $\mathbb{C}G$ are of the form $u = \nu^*\nu$ and are called *positive definite functions*. This gives positivity.
Ergodic Theorem for Random Walks on Dual Groups

Positive elements in $\mathbb{C}G$ are of the form $u = \nu^* \nu$ and are called *positive definite functions*. This gives positivity.

For group algebras, $\mathbbm{1}_{\hat{G}} = \delta^e$, and so to be normalised,

$$u(\delta^e) \leq u(e) = 1.$$
Ergodic Theorem for Random Walks on Dual Groups

Positive elements in $\mathbb{C}G$ are of the form $u = \nu^* \nu$ and are called *positive definite functions*. This gives positivity.

For group algebras, $\mathbb{1}_{\hat{G}} = \delta^e$, and so to be normalised, $u(\delta^e) \simeq u(e) = 1$. Let $u$ be a state on $F(\hat{G})$ and let us calculate:

$$(u \star \delta_e)(\delta^g) = (u \otimes \delta_e)(\delta^g \otimes \delta^g) = u(g)\delta_e(g) = \begin{cases} 1, & \text{if } g = e \\ 0, & \text{otherwise.} \end{cases} = \delta_e(\delta^g),$$

as $u(e) = 1$. 

Ergodic Theorem for Random Walks on Dual Groups

Positive elements in $\mathbb{C}G$ are of the form $u = \nu^* \nu$ and are called *positive definite functions*. This gives positivity.

For group algebras, $\mathbb{1}_{\hat{G}} = \delta^e$, and so to be normalised, $u(\delta^e) \simeq u(e) = 1$. Let $u$ be a state on $F(\hat{G})$ and let us calculate:

$$(u \star \delta_e)(\delta^g) = (u \otimes \delta_e)(\delta^g \otimes \delta^g) = u(g) \delta_e(g) = \begin{cases} 1, & \text{if } g = e \\ 0, & \text{otherwise.} \end{cases} = \delta_e(\delta^g),$$

as $u(e) = 1$. Thus $\delta_e$ is the Haar state on $F(\hat{G})$. 

Ergodic Theorem for Random Walks on Dual Groups

Positive elements in $\mathbb{C}G$ are of the form $u = \nu^* \nu$ and are called positive definite functions. This gives positivity.

For group algebras, $\mathbb{1}_{\hat{G}} = \delta^e$, and so to be normalised, $u(\delta^e) \cong u(e) = 1$. Let $u$ be a state on $F(\hat{G})$ and let us calculate:

$$(u \star \delta_e)(\delta^g) = (u \otimes \delta_e)(\delta^g \otimes \delta^g) = u(g)\delta_e(g) = \begin{cases} 1, & \text{if } g = e \\ 0, & \text{otherwise.} \end{cases} = \delta_e(\delta^g),$$

as $u(e) = 1$. Thus $\delta_e$ is the Haar state on $F(\hat{G})$.

Fix a ‘probability $u$ on $\hat{G}^*$ and consider at $u^k$:

$$u^k(\delta^g) = u \otimes^k \Delta^{(k)}(\delta^g) = u(\delta^g)^k.$$
Ergodic Theorem for Random Walks on Dual Groups

Positive elements in \( \mathbb{C}G \) are of the form \( u = \nu^* \nu \) and are called \textit{positive definite functions}. This gives positivity.

For group algebras, \( 1_{\hat{G}} = \delta^e \), and so to be normalised, \( u(\delta^e) \cong u(e) = 1 \). Let \( u \) be a state on \( F(\hat{G}) \) and let us calculate:

\[
(u \ast \delta^e)(\delta^g) = (u \otimes \delta^e)(\delta^g \otimes \delta^g) = u(g)\delta^e(g) = \begin{cases} 1, & \text{if } g = e \\ 0, & \text{otherwise.} \end{cases} = \delta^e(\delta^g),
\]

as \( u(e) = 1 \). Thus \( \delta^e \) is the Haar state on \( F(\hat{G}) \).

Fix a ‘probability \( u \) on \( \hat{G}^* \) and consider at \( u^*k \):

\[
 u^*k(\delta^g) = u \otimes^k \Delta^{(k)}(\delta^g) = u(\delta^g)^k.
\]

As \( |u(\delta^g)| \leq 1 \), the random walk driven by \( u \) is ergodic iff for all \( g \neq e \)

\[
|u(\delta^g)| < 1.
\]
Ergodic Theorem for Random Walks on Dual Groups

Recall that the classical Ergodic Theorem was given in terms of the \textit{support} of the driving probability.

Amaury Freslon [F18] has recently proven the following:

\begin{itemize}
\item the random walk on $\hat{\Gamma}$ driven by $u$ is not ergodic,
\item $u$ coincides with a character on a non-trivial subgroup $\Lambda < \Gamma$,
\item $u$ is bimodular with respect to a non-trivial subgroup $\Lambda < \Gamma$ in the sense that for any $h \in \Lambda$ and $g \in \Gamma$,
\end{itemize}

$u(gh) = u(g)u(h) = u(hg)$.

This generalises the classical result for abelian finite groups.
Recall that the classical Ergodic Theorem was given in terms of the *support* of the driving probability.

Amaury Freslon [F18] has recently proven the following:

**Theorem**

*Let $\Gamma$ be a discrete group and let $u : \Gamma \to \mathbb{C}$ a positive definite function. The following are equivalent:*

1. *the random walk on $\hat{\Gamma}$ driven by $u$ is not ergodic,*
Ergodic Theorem for Random Walks on Dual Groups

Recall that the classical Ergodic Theorem was given in terms of the *support* of the driving probability.

Amaury Freslon [F18] has recently proven the following:

**Theorem**

Let $\Gamma$ be a discrete group and let $u : \Gamma \to \mathbb{C}$ a positive definite function. The following are equivalent:

1. the random walk on $\hat{\Gamma}$ driven by $u$ is not ergodic, 
2. $u$ coincides with a character on a non-trivial subgroup $\Lambda < \Gamma$,
Ergodic Theorem for Random Walks on Dual Groups

Recall that the classical Ergodic Theorem was given in terms of the *support* of the driving probability.

Amaury Freslon [F18] has recently proven the following:

**Theorem**

Let $\Gamma$ be a discrete group and let $u : \Gamma \to \mathbb{C}$ a positive definite function. The following are equivalent:

1. The random walk on $\hat{\Gamma}$ driven by $u$ is *not* ergodic,
2. $u$ coincides with a character on a non-trivial subgroup $\Lambda < \Gamma$,
3. $u$ is bimodular with respect to a non-trivial subgroup $\Lambda < \Gamma$ in the sense that for any $h \in \Lambda$ and $g \in \Gamma$,

$$u(gh) = u(g)u(h) = u(hg).$$
Ergodic Theorem for Random Walks on Dual Groups

Recall that the classical Ergodic Theorem was given in terms of the \textit{support} of the driving probability.

Amaury Freslon [F18] has recently proven the following:

\textbf{Theorem}

Let $\Gamma$ be a discrete group and let $u : \Gamma \to \mathbb{C}$ a positive definite function. The following are equivalent:

1. the random walk on $\hat{\Gamma}$ driven by $u$ is not ergodic,
2. $u$ coincides with a character on a non-trivial subgroup $\Lambda < \Gamma$,
3. $u$ is bimodular with respect to a non-trivial subgroup $\Lambda < \Gamma$ in the sense that for any $h \in \Lambda$ and $g \in \Gamma$,

$$u(gh) = u(g)u(h) = u(hg).$$

This generalises the classical result for \textit{abelian} finite groups.
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.

As of today only partial results have been found:

- A random walk on a finite quantum group is irreducible if and only if the driving probability is not concentrated on a quasi-sub-quantum-group.
- If "e is the support of the driving probability", the random walk avoids periodicity.

There is the notion of a normal quantum subgroup $N \triangleleft G$ and one can form the quotient quantum group: $G / N$.

A probability on $G$ concentrated on a coset in the quotient quantum group should be somehow 'less' than a pure state on $\mathbb{F}(G / N)$.

... and exhibit periodicity.

This would be necessary conditions for aperiodicity.
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.

As of today only partial results have been found:

- a random walk on a finite quantum group is *irreducible* if and only if the driving probability is not concentrated on a quasi-sub(-quantum-)group

- if "e is the support of the driving probability", the random walk avoids periodicity

There is the notion of a normal quantum subgroup \( N \triangleleft G \) and one can form the quotient quantum group: \( G/N \).

A probability on \( G \) concentrated on a coset in the quotient quantum group should be somehow 'less' than a pure state on \( \mathcal{F}(G/N) \). And exhibit periodicity.

This would be necessary conditions for aperiodicity.
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.

As of today only partial results have been found:

- a random walk on a finite quantum group is *irreducible* if and only if the driving probability is not concentrated on a *quasi*-sub(-quantum-)group
- if “e is the support of the driving probability”, the random walk avoids periodicity
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.

As of today only partial results have been found:

- a random walk on a finite quantum group is *irreducible* if and only if the driving probability is not concentrated on a *quasi*-sub(-quantum-)group
- if “e is the support of the driving probability”, the random walk avoids periodicity

There is the notion of a normal quantum subgroup $\mathbb{N} \triangleright G$ and one can form the quotient quantum group: $G/\mathbb{N}$. 
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.

As of today only partial results have been found:

▶ a random walk on a finite quantum group is \textit{irreducible} if and only if the driving probability is not concentrated on a \textit{quasi}-sub(-quantum-)group

▶ if “e is the support of the driving probability”, the random walk avoids periodicity

There is the notion of a normal quantum subgroup $\mathbb{N} \triangleleft \mathcal{G}$ and one can form the quotient quantum group: $\mathcal{G}/\mathbb{N}$. A probability on $\mathcal{G}$ concentrated on a coset in the quotient quantum group should be somehow ‘less’ than a \textit{pure state} on $F(\mathcal{G}/\mathbb{N})$. 
Ergodic Theorem for Finite Quantum Groups?

An Ergodic Theorem for Finite Quantum Groups would generalise the classical result and the (finite) group algebra case.

As of today only partial results have been found:

- a random walk on a finite quantum group is *irreducible* if and only if the driving probability is not concentrated on a *quasi*-sub(-quantum-)group
- if “e is the support of the driving probability”, the random walk avoids periodicity

There is the notion of a normal quantum subgroup \( N \triangleright G \) and one can form the quotient quantum group: \( G/N \). A probability on \( G \) concentrated on a coset in the quotient quantum group should be somehow ‘less’ than a *pure state* on \( F(G/N) \) ... and exhibit periodicity.

This would be necessary conditions for aperiodicity.
References

[AF18] Freslon, *Positive definite functions and cut-off for discrete groups*.

