Discrete Quantum Walks on the Symmetric Group

Avah Banerjee[1*]

[1*]Computer Science, Missouri S&T, 500 W 15th St., Rolla, 65401, Missouri, USA.

Corresponding author(s). E-mail(s): banerjeeav@mst.edu;

Abstract

Both the transient and limiting dynamical behavior of classical random walks on non-abelian groups have a well-developed theory utilizing non-commutative Fourier analysis. The success of the non-commutative Fourier transform in the analysis of such random walks lies in the fact that in the Fourier domain the distribution for the next step can be determined by a multiplication instead of a convolution operation, and character theory can be used to find analytical formulas for the distribution. In this paper, we initiate a study of using non-commutative Fourier transform for expressing the dynamics of discrete quantum walks in non-abelian groups. More specifically, we investigate the discrete-time quantum walk model on Cayley graphs of the symmetric group. We present the following results: 1) An expression for the probability amplitude of the walker's state using a recurrence relation in the Fourier domain; 2) A relationship between certain symmetries of the initial state, the generating set for the Cayley graph, and the state of the walker; 3) An expression for the probability amplitudes, derived for the Cayley graph with only two generators, based on a sequence that behaves like a 1-D Walsh matrix.

Keywords: Quantum Walks, Cayley Graphs, Symmetric Group, Non-commutative Fourier analysis

1 Introduction

The phenomenon of random walks on graphs has been widely studied and applied to a wide variety of problems in computational sciences. In particular, they have been instrumental in developing randomized and approximation algorithms [1]. More recently, higher-dimensional analogues of random walks (over simplicial complexes) have been proposed [2]. Propagation properties of random walks can be characterized by Markov chains. Hence, the walk is amenable to characterization using methods from spectral graph theory [3].

Unlike *classical* random walks, a *quantum walk* propagates using the principles of quantum mechanics. A few notable differences include: 1) Instead of real probabilities, the state of the walk is specified by complex amplitudes[1]. 2) The random walk coin is now replaced by a unitary transformation. The unitary evolution ensures the walk is reversible[2]. 3) Propagation of the walk generates a superposition state over all possible positions available to the walker. 4) Finally, we can sample the positions by applying suitable measurements on the state of the walker.

There are various (somewhat equivalent) models of quantum walks. The study of quantum walks has a long history, going back to the early works of Feynman, Meyer, Aharonov, Gutmann, and others [5–7]. The hope is that quantum walks can emulate the success of random walks in the development of classical algorithms for creating quantum algorithms. Quantum or classical walks[3] have been primarily used as generative models for probability distributions. Hence, two of the most important properties to study are the kinds of distributions they can generate and their converging behavior. In general, quantum walks do not converge to a stationary distribution. However, their time-averaged distribution (introduced later) does converge. Quantum walks have been shown to generalize Grover's diffusion-based search on graphs. They have been used to obtain currently best-known quantum algorithms for certain problems. Most notable among them are element distinctness, triangle finding, faster simulation of Markov chains, expansion testing, etc. [8–10].

1.1 Results

In this paper, we focus on a discrete-time model of quantum walk. The model we study originated in the seminal paper by Aharonov et al.[11]. The model is also referred to as the coined discrete-time quantum walk (DTQW) [4]. We study DTQWs on Cayley graphs of the symmetric group with appropriate generating sets. There have only been a few studies of DTQWs for Cayley graphs generated from non-abelian groups. As far as we are aware, no such studies have been published for the alternating group, symmetric group, and the general

[1] However, in some cases, if the amplitudes are constrained to be in $\mathbb{R}$, working with them becomes slightly simpler.

[2] For open systems, the walk operator need not be unitary. Interspersing walking with measurements also leads to non-unitary dynamics[4]

[3] Henceforth, we will refer to classical random walks simply as classical walks.

[4] Even though all discrete quantum walks use some type of coin space to make the walk operator unitary, the coin space may be implicitly constructed, such as in scattering quantum walks[12].

linear group. This seems partly due to the fact that non-commutativity makes the dynamical behavior, loosely speaking, information theoretically *incompressible.* That is, to determine the state of the walker after t steps, one has to remember all the paths that lead to that state from the starting state, which are exponentially many. However, as we show, certain properties can be determined about the walks relative to some simplifying assumptions. We present the following results.

1. An expression derived for the probability amplitude of the walker's state, using a recurrence relation in the Fourier domain.
2. A relationship between certain symmetries of the initial state, the generating set for the Cayley graph, and the state of the walker. Specifically, if the generating set is closed under conjugation, the distribution is uniform over the conjugacy classes when the initial state of the walker in the coin-basis is the uniform superposition state.
3. An expression for the probability amplitudes, derived for the Cayley graph with only two generators $((12), (1 \cdots n))$, is based on a sequence that behaves like a 1-D Walsh matrix. This graph was chosen due to: 1) its simplicity - it is the Cayley graph with the least degree for the symmetric group, 2) its lower expansion rate compared to graphs constructed from other generating sets, and 3) its out-degree of 2, which allows us to use the Hadamard coin operator. Even in this simple setting, the dynamical behavior of the walk is highly non-trivial and somewhat validates why not much progress has been made in studying DTQWs on non-abelian Cayley graphs.

2 Preliminaries

2.1 Cayley Graphs

Let $(G, \circ)$ be any finite group, and S be a generator of G. We take $|G| = N$ and $|S| = d$. The Cayley graph of the pair $\Gamma(G, S)$ is a directed graph Γ defined as follows. The vertex set $V(\Gamma) = G$. The edge set is defined as

$$E(\Gamma) = \{(g, h), g, h \in G \mid \; g^{-1} \circ h \in S\}$$

Henceforth, we omit the "$\circ$" and simply write $g \circ h$ as gh, where $g, h \in G$. If S is closed under inverse, that is $s \in S \implies s^{-1} \in S$ then Γ is undirected. We use $\mathbb{e}$ to denote the identity element of G. If $\mathbb{e} \notin S$ then Γ does not have any self-loops. Clearly Γ is d-regular. This allows for a reversible walk operator with a fixed-sized coin space (defined shortly), which is a requirement for unitary quantum evolution. In this paper we associate G with the symmetric group $\mathcal{S}_n$ of all n-permutations. Some typical generators of G are - the set of all transpositions, $\{(12), (13), \ldots, (1n)\}, \{(ij), (1 \cdots n)\}$ where $gcd(|i-j|, n) = 2$ etc. Later, we will study the Cayley graph, denoted as Γ_n, with respect to the last generator (specifically $\{(12), (1 \cdots n)\}$). Figure 1 shows Γ_4. For $n \geq 3$, Γ_n is directed with in-degree and out-degree of two. The element $\mu = (12)$ is of order 2 and hence the pair of edges $(g, g\mu)$ and $(g\mu, g)$ could be taken together as an undirected edge. These edges form perfect matchings. On the other hand, the element $\sigma = (1 \cdots n)$ creates directed n-cycles. We say S is *conjugate invariant*, if it is a union of one or more conjugacy classes. For example, $S =$ set of all transpositions.

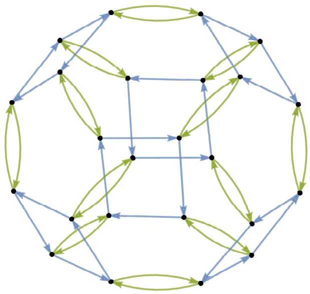


Fig. 1: The graph Γ_4. Edges corresponding to the element (12) (resp. $(1 \cdots n)$) are colored green (resp. blue). It has 24 vertices and has a diameter of 6.

2.2 Formal Description of DTQW

Physically, a particle with some internal degrees of freedom moves in superposition, as it propagates on the vertices of G. The state of such a particle at any moment is described using a vector in the Hilbert space $\mathcal{H}$ with a basis set $\{|s, g\rangle \mid s \in S \text{ and } g \in G\}$ (standard basis). Thus we can write $\mathcal{H} = \mathcal{H}_G \otimes \mathcal{H}_S$. The space $\mathcal{H}_G$ describes the position of the particle over the group elements (alternatively over the vertices of Γ). $\mathcal{H}_S$ is the coin (chiral) space, which describes the state of a particle's internal degrees of freedom (sometimes referred to as the particle's *chirality*). One step of the walk consists of applying the two unitaries $C_S \otimes I_G$ and Λ in succession. We first apply the coin operator $C \otimes I_G$ which acts trivially on $\mathcal{H}_G$. This transforms the chiral state of the particle. Then, we apply the shift operator Λ which acts on the total space $\mathcal{H}$ and performs a conditional shift of the particle's position based on its current chiral state in $\mathcal{H}_S$. Together, each step of the walk consists of applying the unitary $\boldsymbol{W} = \Lambda(C \otimes I)$ to the current state. Although there are no particular restrictions on the unitary C, in this work, we mainly consider the case when C is the Grover operator. This choice is made to keep our analysis tractable and is consistent with previous studies of DTQWs on Cayley graphs (section 3). Additionally, even when C is restricted to the Grover coin, the walk produces highly non-trivial distributions that could prove to be useful for certain sampling problems. We describe C and Λ next.

2.2.1 Coin operators

For $d \geq 3$ the Grover operator D (reflection about the mean) is defined as follows. D is also commonly known as the diffusion operator. It is defined as: $D = 2\left|\psi\right\rangle\!\left\langle\psi\right| - I$, where $\left|\psi\right\rangle = \frac{1}{\sqrt{d}}\sum_{s\in S}\left|s\right\rangle$ is the uniform superposition over the basis states in $\mathcal{H}_S$. The operator D acts only on the coin space $\mathcal{H}_S$. Let δ_{ij} be the Kronecker delta function. In the matrix notation $(i,j)^{th}$ entry of D is given by: $D_{ij} = \delta_{ij}a + (1-\delta_{ij})\,b$ where $a = \frac{2}{d} - 1$ and $b = \frac{2}{d}$. When $|S| = 2$ we consider the Hadamard operator $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ or the operator $\frac{I+iX}{\sqrt{2}}$. Here X is the not gate $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$. It has been shown that the propagation of the walk on the line when $C = \frac{I+iX}{\sqrt{2}}$ is symmetric [13] as opposed to H which has a heavy tail on one side.

2.2.2 The Λ operator

The shift operator is defined as $\Lambda = \sum_{s\in S, g\in G}\left|s, gs\right\rangle\!\left\langle s, g\right|$. In literature it is sometimes referred to as the move operator to distinguish it from some of its extensions. The operator Λ sends the walker at position g along to gs if its coin state is $\left|s\right\rangle$ ($\left|s,g\right\rangle \longmapsto \left|s, gs\right\rangle$). In the matrix form, Λ is a $dn \times dn$ block diagonal matrix with d blocks. There is a block corresponding to each $s \in S$. The block corresponding to s is the $n \times n$ permutation matrix associated with the action of s on G. A more general version of Λ also permutes the basis in $\mathcal{H}_S$. Specifically, $\Lambda_\pi = \sum_{s\in S, g\in G}\left|\pi(s), gs\right\rangle\!\left\langle s, g\right|$. In the case of the grid graph, π performing a directional flip ($\left|\uparrow\right\rangle$ to $\left|\downarrow\right\rangle$ and $\left|\leftarrow\right\rangle$ to $\left|\rightarrow\right\rangle$ and vice versa), gives rise to the so-called flip-flop walk [14].

2.2.3 Initial states and evolution

We use $\left|\psi_t\right\rangle = \alpha_{s,t}(g)\left|s,g\right\rangle$ to denote the state of the walker after t steps. $\left|\psi_0\right\rangle$ is the initial state. We can write,

$$\left|\psi_t\right\rangle = \boldsymbol{W}^t\left|\psi_0\right\rangle$$

Then the probability of observing a particle at g when measured on the standard basis $\{\left|s,g\right\rangle\}$ is

$$P_t[g \mid \psi_0] = \sum_s \left|\alpha_{s,t}(g)\right|^2$$

Since $\boldsymbol{W}$ is unitary, $\left|\psi_t\right\rangle$ is periodic with respect to t [11] as long as $\left|\psi_0\right\rangle$ is not an eigenvector of $\boldsymbol{W}$. In general P_t does not converge. However the time averaged distribution (defined below) does.

$$\overline{P}_T[g \mid \psi_0] = \frac{1}{T}\sum_{t=0}^{T-1} P_t[g \mid \psi_0]$$

$\overline{P}_T$ can be interpreted as the expected value of the distribution P_t when t is selected uniformly at random from the set $\{0, \ldots, T-1\}$. If the amplitudes are all real then to study the convergence of $\overline{P}_T$ it suffices to study the amplitudes only. Let $\pi[\ \mid \psi_0]$ be the limiting distribution of the walk starting from the initial state $|\psi_0\rangle$. Convergence is measured via the total variation distance $\parallel P - \pi \parallel = \frac{1}{2}\sum_g |P[g] - \pi[g]|$. Various convergence parameters have been introduced in the literature. Notable among them is the *mixing time* of the walk. The mixing time itself can be defined in several way. We use the definition from [11] which can be thought of as the average mixing time.

$$M_\epsilon = \min\{t \mid \ \forall T \geq t, |s,g\rangle : \parallel \overline{P}_T[\cdot \ \mid |s,g\rangle] - \pi[\cdot \ \mid |s,g\rangle] \parallel \leq \epsilon\}$$

We also consider the mixing time starting from a specific state $|\phi\rangle$ as defined below.

$$M_\epsilon^\phi = \min\{t \mid \ \forall T \geq t : \parallel \overline{P}_T[\ \mid |\phi\rangle] - \pi[\ \mid |\phi\rangle] \parallel \leq \epsilon\}$$

When estimating the mixing time via numerical simulation it is easier to compute M_ϵ^ϕ than M_ϵ, where the former gives a lower bound for the latter.

3 Previous Work

Over the past two decades, there has been significant research on various aspects of DTQWs. To maintain the relevance of our review, we will first briefly discuss the seminal paper that introduced the DTQW model under study. This will be followed by an examination of papers that conduct analytical investigations of DTQWs on Cayley graphs.

Aharonov et al. [11] were the first to propose a discrete time model of quantum walks using a coin operator. They characterized the convergence behavior of walks on abelian groups. They show that the time-averaged distribution converges to the uniform distribution whenever the eigenvalues of U are all distinct. They also gave an $O(\frac{n \log n}{\epsilon^3})$ upper bound on the mixing time for $\mathbb{Z}_n$ (the cycle graph). Some lower bounds were also proved in terms of the graph's conductance.

Following their introduction, DTQWs has been studied for several graph families. Nayak and Vishwanath [15] gave a detailed analysis for the line using Fourier analysis. They were able to show that the Hadamard walk mixes almost uniformly with only $O(t)$ steps, giving a quadratic speedup over its classical counterpart. Moor and Russell [16] analyzed the Grover walk on the Cayley graph of $\mathbb{Z}_2^n$ (a.k.a the hypercube). They show an instantaneous mixing time of $O(n)$, which again beats the classical $\Omega(n \log n)$ bound. Acevedo and Gobron studied quantum walks for certain Cayley graphs and, in particular, gave several results for graphs generated by free groups [17]. D'Ariano et. al. investigated the case where the group is virtually abelian [18]. Virtual abelianity allowed them to reduce the problem to an equivalent one on an abelian group with a larger chiral space dimension and use the Fourier method of [15]. More recently, DTQWs has been studied for the Dihedral group D_n by [19] Dai et. al. Since, D_n is isomorphic to the semi-direct product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$; (again) the Fourier approach introduced in [15] carries over. Using which authors gave spectral decomposition of U for the Grover walk. A detailed survey about various types of quantum walks including DTQWs can be found in [20] and the reference therein. A recent survey of DTQWs on Cayley graphs can be found in [21][5].

Finally, we mention the continuous time quantum walk model studied in [22] by Gerhardt and Watrous. In the continuous setting the walk operator $\boldsymbol{W}(t) = e^{itA}$ is determined by the adjacency matrix of the Cayley graph. When S is the set of transpositions, they show, the time averaged distribution is far from the uniform distribution. They explicitly calculate the probability of reaching a n-cycle starting from $\mathbb{e}$ by expressing the eigenstates of $\boldsymbol{W}$ using the characters of $\mathcal{S}_n$. Unfortunately, in the discrete time model an analogous description of $\boldsymbol{W}$ seems elusive.

4 Results via Representation Theory

We use representation theory to express the amplitudes $\alpha_{s,t}(g)$ using a sum over the irreducible characters. Let $|\psi_0\rangle$ be the initial state of the walk. After t steps the state is $|\psi_t\rangle$ where,

$$|\psi_t\rangle = \sum_{s,g} \alpha_{s,t}(g) \, |s, g\rangle$$

Since $\alpha_{s,t}(g)$'s are functions from G to $\mathbb{C}$ which enables us to apply the non-commutative Fourier transformation to get their duals:

$$\hat{\alpha}_{s,t}(\rho) = \sum_{g \in G} \alpha_{s,t}(g)\rho(g) \tag{1}$$

for every $\rho \in \hat{G}$, the set of all irreducible representations of G. Where $\rho : G \to GL(V)$ is a homomorphism from G to the space of linear maps on some vector space V satisfying the following. For all $g, h \in G$, $\rho(g)\rho(h) = \rho(gh)$ and $\rho(\mathbb{e}) = I$. We denote by d_ρ, the dimension of V, as the dimension of ρ. The

[5] We were unable to get complete bibliographical information for this reference.

character of a representation ρ is defined as $\chi_\rho(g) = tr(\rho(g))$. Here $tr()$ is the trace operator. Following properties of χ_ρ will be useful:

1. $\chi_\rho(\mathbb{e}) = d_\rho$
2. $\forall g, h \in G: \ \chi_\rho(gh) = \chi_\rho(hg)$ (cyclic property)
3. $\forall g, h \in G: \ \chi_\rho(hgh^{-1}) = \chi_\rho(g)$ (χ_ρ is constant over the conjugacy classes)

Additionally, we have $\rho(g^{-1}) = \rho(g)^\dagger$, where $A^\dagger$ is the adjoint of the operator A. Here we assume the representations are unitary. Proof of the above relations directly follows from the definition of χ_ρ and ρ. For further information and introduction to representation theory, especially in the context of random walks, we refer the reader to the monograph by Diaconis [23]. The book by Terras [24] gives a comprehensive introduction to non-commutative Fourier analysis.

A recurrence for $\alpha_{s,t}(g)$.

Let $|\psi'_t\rangle = (D \otimes I)|\psi_t\rangle$ and $|\psi_{t+1}\rangle = \Lambda|\psi'_t\rangle$ so that $|\psi_{t+1}\rangle = \boldsymbol{W}|\psi_t\rangle$. Applying the Grover operator D on the basis states in $\mathcal{H}_S$ we get,

$$|s\rangle \to a|s\rangle + \sum_{s' \in S, s \neq s'} b|s'\rangle$$

This gives $|\phi'_t\rangle$ as the intermediate state just after applying the coin operator.

$$|\psi'_t\rangle = \sum_{s,g} \alpha_{s,t}(g) \left(a|s\rangle + \sum_{s' \in S, s \neq s'} b|s'\rangle \right) |g\rangle$$

After applying Λ we get the state after completing a full step of the walk.

$$\begin{aligned} |\psi_{t+1}\rangle &= \sum_{s,g} \alpha_{s,t}(g) \left(\sum_{s' \in S, s' \neq s} b|s', gs'\rangle + a|s, gs\rangle \right) \\ &= \sum_{s,g} \left(a\alpha_{s,t}(gs^{-1}) + b \sum_{s' \in S, s' \neq s} \alpha_{s',t}(gs^{-1}) \right) |s, g\rangle \end{aligned}$$

The above gives a recurrence relation for the amplitude after t steps:

$$\alpha_{s,t}(g) = a\alpha_{s,t-1}(gs^{-1}) + b \sum_{s' \in S, s' \neq s} \alpha_{s',t-1}(gs^{-1})$$

Now we expand Eq. 1, giving

$$\hat{\alpha}_{s,t}(\rho) = \sum_{g \in G} \alpha_{s,t}(g)\rho(g) = \sum_{g \in G} \left(a\alpha_{s,t-1}(gs^{-1}) + b \sum_{s \neq s'} \alpha_{s',t-1}(gs^{-1}) \right) \rho(g)$$

$$= \sum_{g \in G} \left(a\alpha_{s,t-1}(g) + b \sum_{s \neq s'} \alpha_{s',t-1}(g) \right) \rho(gs) \tag{2}$$

$$= \left(a\hat{\alpha}_{s,t-1}(\rho) + b \sum_{s \neq s'} \hat{\alpha}_{s',t-1}(\rho) \right) \rho(s) \tag{3}$$

Due to the dependence on $\rho(s)$ the above recurrence does not have a closed form solution. However, $\alpha_{s,t}(g)$ can be expressed as a sum of characters. We derive this next.

Lemma 1 *Given the Grover operator acting on $\mathcal{H}_S$ and the initial state $|\psi_0\rangle = \frac{1}{\sqrt{d}} \sum_s |s, \mathbb{e}\rangle$ we have for $t > 0, d > 2$:*

$$\alpha_{s,t}(g) = \frac{1}{\sqrt{d}N} \sum_{k=0}^{t-1} (a^{t-k-1} b^k) \left(\sum_{\rho \in \hat{G}, r \in R_{k,t,s}} d_\rho \chi_\rho(g^{-1}r) \right). \tag{4}$$

where every $r \in R_{k,t,s}$ has a generating sequence of the following form:

$$R_{k,t,s} \ni r = \begin{cases} s^t & \text{if } k = 0 \\ s_k^{p_k} s_{k-1}^{p_{k-1}} \ldots s_1^{p_1} s & \text{otherwise} \end{cases}$$

satisfying - 1) $\forall i \in \{0, \ldots, k-1\}, s_i \neq s_{i+1} (s_0 = s)$ and 2) $\sum_i p_i = t - 1$.

Proof We prove this by induction on t. For the base case we take $t = 1$. From Eq. 2 we get:

$$\begin{aligned} \hat{\alpha}_{s,1}(\rho) &= \left(a\hat{\alpha}_{s,0}(\rho) + b \sum_{s \neq s'} \hat{\alpha}_{s',0}(\rho) \right) \rho(s) \\ &= \left(a \sum_{g' \in G} \alpha_{s,0}(g')\rho(g') + b \sum_{s \neq s'} \sum_{g' \in G} \alpha_{s',0}(g')\rho(g') \right) \rho(s) \\ &= \left(a\alpha_{s,0}(\mathbb{e})\rho(\mathbb{e}) + b \sum_{s \neq s'} \alpha_{s',0}(\mathbb{e})\rho(\mathbb{e}) \right) \rho(s) = \frac{\rho(s)}{\sqrt{d}}(a + (d-1)b) = \frac{\rho(s)}{\sqrt{d}} \end{aligned}$$

The inverse Fourier transform of $\hat{\alpha}_{s,t}$ is given by [25]:

$$\alpha_{s,t}(g) = \frac{1}{N} \sum_{\rho \in \hat{G}} d_\rho Tr(\rho^\dagger(g)\hat{\alpha}_{s,t}(\rho))$$

For $t = 1$ we get:

$$\alpha_{s,1}(g) = \frac{1}{N\sqrt{d}} \sum_{\rho \in \hat{G}} d_\rho Tr(\rho(g^{-1}s))$$

For the inductive case, assume Eq. 2 holds upto $t - 1$. Let $\frac{1}{N\sqrt{d}} = \beta$. Then,

$$\alpha_{s,t}(g) = a\alpha_{s,t-1}(gs^{-1}) + b \sum_{s' \neq s} \alpha_{s',t-1}(gs^{-1})$$

$$
\begin{aligned}
&= \beta \sum_{k=0}^{t-2} (a^{t-k-1} b^k) \sum_{\rho, r \in R_{k,t-1,s}} d_\rho \chi_\rho (s g^{-1} r) \\
&+ \beta \sum_{s' \neq s} \sum_{k=0}^{t-2} (a^{t-k-2} b^{k+1}) \sum_{\rho, r \in R_{k,t-1,s'}} d_\rho \chi_\rho (s g^{-1} r) \\
&= \beta \sum_{k=0}^{t-2} (a^{t-k-1} b^k) \sum_{\substack{\rho,\ r \in R_{k,t,s} \\ r = ps,\ p \in R_{k,t-1,s}}} d_\rho \chi_\rho (g^{-1} r) \\
&+ \beta \sum_{k=0}^{t-2} (a^{t-k-2} b^{k+1}) \sum_{s' \neq s} \sum_{\substack{\rho,\ r \in R_{k+1,t,s} \\ r = qs,\ q \in R_{k,t-1,s'}}} d_\rho \chi_\rho (g^{-1} r)
\end{aligned}
$$

Where the second equality follows from the cyclic property of characters and rearranging the sums in the second term. Substituting $k+1$ for k in the above and rearranging the summations in the second term we get

$$
\begin{aligned}
\alpha_{s,t}(g) = \beta \sum_{k=0}^{t-2} (a^{t-k-1} b^k) \sum_{\substack{\rho \in \hat{G} \\ r \in P}} d_\rho \chi_\rho (g^{-1} r) \\
+ \beta \sum_{k=1}^{t-1} (a^{t-k-1} b^k) \sum_{s' \neq s} \sum_{\substack{\rho \in \hat{G} \\ r \in Q_{s'}}} d_\rho \chi_\rho (g^{-1} r)
\end{aligned} \tag{5}
$$

Where,

$$
\begin{aligned}
P &= \{ r \in R_{k,t,s} \mid \ \exists p \in R_{k,t-1,s} \ r = ps \} \text{ and} \\
Q_{s'} &= \{ r \in R_{k,t,s} \mid \ \exists q \in R_{k-1,t-1,s'} \ r = qs \wedge \ s' \neq s \}
\end{aligned}
$$

Since $R_{k,t,s} = P \cup \left(\bigcup_{s \neq s'} Q_{s'} \right)$ we can combine the two terms in Eq. 5 to get,

$$
\alpha_{s,t}(g) = \beta \sum_{k=0}^{t-1} (a^{t-k-1} b^k) \sum_{\rho \in \hat{G},\ r \in R_{k,t,s}} d_\rho \chi_\rho (g^{-1} r)
$$

□

Theorem 2 *Defining,*

$$
\#_{k,t,s}(g) = \left| \{ r \in R_{k,t,s} \mid r = g \} \right| \tag{6}
$$

we have

$$
\alpha_{s,t}(g) = \frac{1}{\sqrt{d}} \sum_{k=0}^{t-1} (a^{t-k-1} b^k) \#_{k,t,s}(g)
$$

Proof Recall,

$$
\sum_{\rho \in \hat{G}} d_\rho \chi_\rho (g) = \begin{cases} N & g = \mathbb{e} \\ 0 & \text{otherwise} \end{cases}
$$

Substituting this in Eq. 4 we have,

$$\begin{aligned}
\alpha_{s,t}(g) &= \frac{1}{\sqrt{d}N}\sum_{k=0}^{t-1}(a^{t-k-1}b^k)\sum_{\rho\in\hat{G},\ r\in R_{k,t,s}} d_\rho\chi_\rho(g^{-1}r)\\
&= \frac{1}{\sqrt{d}N}\sum_{k=0}^{t-1}(a^{t-k-1}b^k)\sum_{\substack{r\in R_{k,t,s}\\ g^{-1}r=\mathbb{e}}}\sum_{\rho\in\hat{G}} d_\rho\chi_\rho(\mathbb{e}) = \frac{1}{\sqrt{d}N}\sum_{k=0}^{t-1}(a^{t-k-1}b^k)\sum_{\substack{r\in R_{k,t}\\ g^{-1}r=\mathbb{e}}} N\\
&= \frac{1}{\sqrt{d}}\sum_{k=0}^{t-1}(a^{t-k-1}b^k)\#_{k,t,s}(g)
\end{aligned}$$

□

4.1 When S is Conjugate Invariant

Recall that a generating set S is *conjugate invariant* if it is a union of one or more conjugacy classes.

Corollary 3 *If the generating set S is conjugate invariant then the walk is uniform over the conjugacy classes of G. Specifically, the distribution $P_t[\ |_{\psi_0}]$ after t steps is a class function.*

Proof Suppose the elements g, h are from the same conjugacy class. Let $h = \tau g\tau^{-1}$ for some $\tau \in G$. Then,

$$\alpha_{s,t}(h) = \alpha_{s,t}(\tau g\tau^{-1}) = \frac{1}{\sqrt{d}}\sum_{k=0}^{t-1}(a^{t-k-1}b^k)\#_{k,t,s}(\tau g\tau^{-1}) \tag{7}$$

We note that for any $\tau \in G$ the function $\tau^{-1}()\tau : S \to S$ is an automorphism. This implies it is also an isomorphism from $R_{k,t,s}$ to $R_{k,t,\tau^{-1}s\tau}$. To show this take $r = s_k^{p_k} s_{k-1}^{p_{k-1}} \cdots s_1^{p_1} s$. Then,

$$\tau^{-1}r\tau = \tau^{-1}s_k^{p_k}\tau\tau^{-1}s_{k-1}^{p_{k-1}}\tau\cdots\tau^{-1}s\tau = s'^{p_k}_{k}\, s'^{p_{k-1}}_{k-1}\ldots s'^{p_1}_{1}\tau^{-1}s\tau = r' \in R_{k,t,\tau^{-1}s\tau} \tag{8}$$

where $s'_i = \tau^{-1}s_i\tau$. The last containment follows from the fact that $s_i \neq s_{i+1} \iff s'_i \neq s'_{i+1}$. To show injectivity we note that $\tau^{-1}r\tau = \tau^{-1}r'\tau \implies r = r'$. Then,

$$\#_{k,t,s}(\tau g\tau^{-1}) = \left|\{r \in R_{k,t,s} \mid r = \tau g\tau^{-1}\}\right| = \left|\{r \in R_{k,t,\tau^{-1}s\tau} \mid r = g\}\right| = \#_{k,t,\tau^{-1}s\tau}(g)$$

Substituting the above in Eq. 7 we have,

$$\alpha_{s,t}(h) = \frac{1}{\sqrt{d}}\sum_{k=0}^{t-1}(a^{t-k-1}b^k)\#_{k,t,\tau^{-1}s\tau}(g) = \alpha_{\tau^{-1}s\tau,t}(g)$$

Finally,

$$P_t[\tau g\tau^{-1}\ |_{\psi_0}] = \sum_{\tau^{-1}s\tau\in S}\left|\alpha_{\tau^{-1}s\tau,t}(g)\right|^2 = \sum_{s\in S}|\alpha_{s,t}(g)|^2 = P_t[g\ |_{\psi_0}].$$

□

Remark 1 From the above it follows that the time average distribution $\overline{P}[|\ \psi_0]$ is also a class function.

4.2 When $|\psi_0\rangle$ is a Basis State

In order to determine the mixing time we want to know the distribution starting from a basis state; that is $|\psi_0\rangle = |s_*, g_*\rangle$. R_{s_*} be the set of generating sequences beginning with s_*. We define $R_{k,t,s,+s_*} = R_{k,t,s} \cap R_{s_*}$ and $R_{k,t,s,-s_*} = R_{k,t,s} \setminus R_{k,t,s,+s_*}$. Analogous to Eq. 6 we define,

$$\#_{k,t,s,+s_*}(g) = |\{r \in R_{k,t,s,+s_*} \mid r = g\}| \text{ and } \#_{k,t,s,-s_*}(g) = |\{r \in R_{k,t,s,-s_*} \mid r = g\}|$$

Theorem 4 *Starting at $|\psi_0\rangle = |s_*, g_*\rangle$ we have,*

$$\alpha_{s,t}(g) = \sum_{k=0}^{t-1} a^{t-k-1} b^k \left(a\#_{k,t,s,+s_*}(g_*^{-1}g) + b\#_{k,t,s,-s_*}(g_*^{-1}g) \right)$$

Proof The proof is similar to Theorem 2 except the initial step which leads to a dependency on g_*, s_*. □

Taken together, the following two lemmas show that, up to a permutation of G, the distribution does not depend on the initial state $|s_*, g_*\rangle$, if S is conjugate invariant.

Lemma 5

$$P_t[g \mid_{|s_*,\pi g_*\rangle}] = P_t[\pi^{-1} g \mid_{|s_*,g_*\rangle}]$$

Proof Since $\#_{k,t,s,\pm s_*}((\pi g_*)^{-1}g) = \#_{k,t,s,\pm s_*}(g_*^{-1}\pi^{-1}g)$. □

Lemma 6 *If the generating set S is conjugate invariant and $s_* \neq s'_*$, then*

$$P_t[g \mid_{|s'_*,g_*\rangle}] = P_t[\pi g \mid_{|s_*,g_*\rangle}]$$

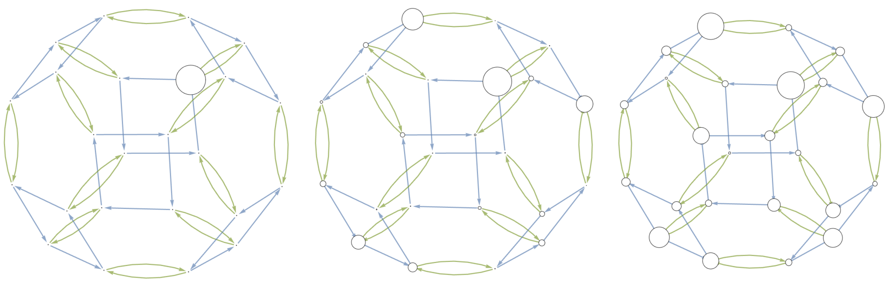
for some π acting on G.

Proof Every generator has the same order and creates cycles of the same length in Γ (if $g = \tau h \tau^{-1}$ and $g^k = \mathbb{e}$ then $h^k = \mathbb{e}$). Thus Γ is symmetric with respect to its generators. Specifically, the chirality of the initial state $|s'_*, g_*\rangle$ specifies the initial "direction" of the walk. Previous argument implies that these directions are symmetric. Hence, the distribution of the walk is same as when starting from $|s_*, g_*\rangle$ up to a permutation on the vertices of Γ. More formally, using an argument similar to that in Corollary 3 we can show $\#_{k,t,s,\pm s'_*}(g) = \#_{k,t,s,\pm s_*}(\tau g \tau^{-1})$, where $s'_* = \tau s_* \tau^{-1}$.

□

Remark 2 Unfortunately, a result analogous to Corollary 3 does not hold in this case even if we relax our definition of a class function as follows. We say, f is a class function up to some permutation iff there exists some fixed permutation π acting on G such that: $f(\pi g) = f(h)$ whenever g and h belong to the same conjugacy class. The following graph serves as a counterexample. Let $G = \mathcal{S}_4$ and $S =$ set of all transpositions of G. G has 5 conjugacy classes. However, the probability distribution after the first two steps of the walk starting from $|(1,2),\mathbb{e}\rangle$ has 6 distinct values:

$$P_t[|_{|(1,2),\mathbb{e}\rangle}] = \left(\frac{4}{9}, 0, 0, 0, 0, 0, 0, \frac{2}{27}, \frac{2}{27}, \frac{2}{27}, \frac{1}{27}, \frac{2}{27}, \frac{1}{27}, \frac{1}{27}, \frac{1}{27}, 0, 0, 0, 0, 0, 0, \frac{5}{81}, \frac{2}{81}, \frac{2}{81}\right)$$



(a) $T = 0$ (b) $T = 6$ (c) $T = 24$

Fig. 2: Time averaged distribution ($\overline{P}_T[\ |_{|0,\mathbb{e}\rangle}]$) of the Hadamard walk on Γ_4. Vertices are sized proportional to the probability of observing the particle there.

5 The Hadamard Walk on Γ_n

In this section we study the case when the size of the generating set is 2. Theorem 1 does not apply here directly. In fact we consider a specific case when $S = \{\mu = (12), \sigma = (1 \cdots n)\}$ and $C = H$ is the Hadamard operator. However, the principle techniques used here apply to any arbitrary C and any S with $|S| = 2$. In what follows we identify the basis vector corresponding to μ (resp. σ) as $|0\rangle$ (resp. $|1\rangle$). We can represent a generating sequence $\mu^{p_1}\sigma^{q_1} \ldots \mu^{p_l}\sigma^{q_l}$, where each p_i, q_i's are non-negative integers, as a $L = \sum_i (p_i + q_i)$ bit number $k \in [2^L]$[6]. For example $\mu^2\sigma\mu^3\sigma^2$ is represented as 00100011 = 35. By μ^p we represent the sequence $\mu \cdots \mu$, where μ is applied p times and not the corresponding group element, which is either μ or $\mathbb{e}$. Henceforth we identify μ (resp. σ) with 0 (resp. 1). We use $\hat{k}$ to denote the group element corresponding to the generating sequence k. We define a sequence W_n of length 2^n over the

[6] $[2^L] = \{0, \ldots, 2^L - 1\}$

alphabet $\{1,-1\}$. Let $\underline{W}_n$ and $\overline{W}_n$ be the first and last half of W_n respectively. Let $-W_n$ be the negation of W_n ($\forall i - W_n(i) = (-1)W_n(i)$). Then,

$$W_n = \begin{cases} [1,1] & \text{if } n = 1 \\ [W_{n-1} \ \underline{W}_{n-1} \ \ -\overline{W}_{n-1}] & \text{otherwise} \end{cases}$$

Loosely speaking, W_n's can be thought of as a vector analogue of the corresponding Walsh matrix. Here we take $W_n(k)$ to denote the k^{th} element of W_n.

Theorem 7 *If $S = \{0,1\}$ and $C = H$ then starting from the initial state $|\psi_0\rangle = |0, \mathbb{e}\rangle$ the amplitude after $t \geq 1$ steps is given by,*

$$\alpha_{s,t}(g) = \frac{1}{\sqrt{2^t}} \sum_{\substack{k \in [2^t] \\ k = \delta_{s1} \mod 2}} \delta_{\hat{k},g} W_t(k)$$

Proof First we show for $t \geq 1$,

$$|\psi_t\rangle = \frac{1}{\sqrt{2^t}} \left(\sum_{\substack{k \in [2^t] \\ k=0 \mod 2}} W_t(k) \left|0, \hat{k}\right\rangle + \sum_{\substack{k \in [2^t] \\ k=1 \mod 2}} W_t(k) \left|1, \hat{k}\right\rangle \right)$$

The proof is via induction. The base case $t = 1$ is trivial. Applying the Hadamard walk operator to $|\psi_t\rangle$ yields,

$$\begin{aligned} |\psi_{t+1}\rangle &= \frac{1}{\sqrt{2^{t+1}}} \sum_{\substack{k \in [2^t] \\ k=0 \mod 2}} (W_t(k) \left|0, \hat{k}0\right\rangle + W_t(k) \left|1, \hat{k}1\right\rangle) \\ &+ \frac{1}{\sqrt{2^{t+1}}} \sum_{\substack{k \in [2^t] \\ k=1 \mod 2}} (W_t(k) \left|0, \hat{k}0\right\rangle - W_t(k) \left|1, \hat{k}1\right\rangle) \\ &= \frac{1}{\sqrt{2^{t+1}}} \left(\sum_{\substack{k \in [2^{t+1}] \\ k=0 \mod 2}} W_{t+1}(k) \left|0, \hat{k}\right\rangle + \sum_{\substack{k \in [2^{t+1}] \\ k=1 \mod 2}} W_{t+1}(k) \left|1, \hat{k}\right\rangle \right) \end{aligned} \tag{9}$$

Where the last equality follows from the definition of W_t. The terms in Equation 9 that contribute towards $\alpha_{s,t}(g)$ are those for which $\hat{k} = g$. This immediately implies the theorem. □

Remark 3 (Spectra of $\boldsymbol{W}$) A brief remark about the spectrum of $\boldsymbol{W} = \Lambda(H \otimes I)$, where H is the Hadamard operator. The case with $C = \frac{1}{\sqrt{2}}(I + iX)$ is similar. Let P_μ and P_σ be the permutation matrices corresponding to μ and σ respectively. It is an easy exercise to show that $\boldsymbol{W} = \frac{1}{\sqrt{2}} \begin{bmatrix} P_\mu & P_\mu \\ P_\sigma & -P_\sigma \end{bmatrix}$. Unfortunately, the eigenvalues of U are not all distinct. Hence the minimum eigenvalue gap is zero and we cannot directly use Theorem 6.1 in [11] to bound the mixing time.

5.1 Simulation Results

As demonstrated in the previous section, the amplitude at any vertex depends on the path sums over generating sequences. It appears that there are no closed-form expressions for the amplitudes, and it is unclear how to derive such expressions for the mixing time either. Given these challenges, we turned to numerical simulations for further insights.

Our goal was to estimate the mixing time in order to generate a plausible hypothesis of its growth rate. We consider both the standard mixing time M_ϵ and state-dependent mixing time M_ϵ^ϕ, where we take $\epsilon = \frac{1}{4}$, a value often used in mixing time computation [26]. Figure 3 summarizes our simulation results. Based on the simulation results, we conjecture that the Hadamard walk on Γ_n mixes in $O(n^2)$ steps for a fixed ϵ.

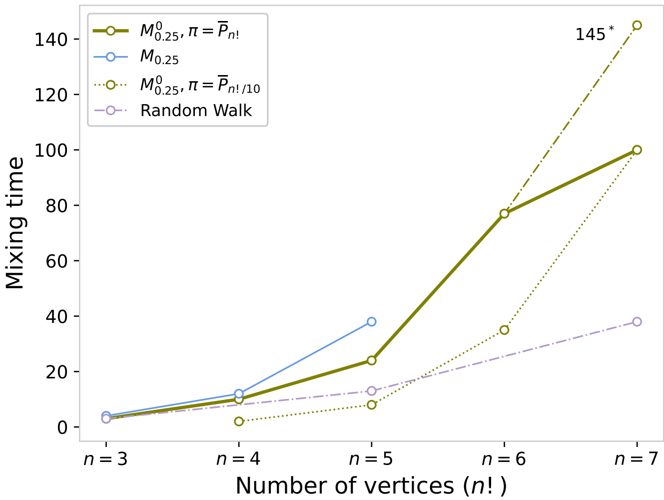


Fig. 3: The graph for various mixing times. In the figure, $M^0_{0.25}$ denotes the mixing time starting from basis state $|\mu, \mathbb{e}\rangle$. We estimate the time averaged limiting distribution π with $\overline{P}_{n!}$. However, for $n = 7$ the graph has 5040 nodes and due to hardware limitations we could only simulate it for $T = \frac{7!}{10}$. This gives us a loose lower bound for the mixing time. Hence, for Γ_7, we show both the mixing time obtained from simulation as well as its estimated value (145) using a quadratic fit. We also plot a lower bound for $M^0_{0.25}$, by estimating π with $\overline{P}_{n!/10}$. For the value of n up to 5 we also compute the worst case mixing time independent of the starting basis state. Lastly, for sake of completeness the corresponding mixing times (with $\epsilon = 0.25$) for the uniform random walk is given. Since Γ_n is bipartite when n is even the random walk on these graphs do not converge to a limiting distribution.

6 Conclusion

In this paper, using character sums of the group representation we derive expressions for the amplitudes of the state after t steps of the quantum walk. Even though this expression is not fully analytical, we can use it to infer certain properties of the generated distribution, in particular, whether they are uniform over the conjugacy classes. We also give an expression for the amplitudes, for the Cayley graph with only two generators, using a "vector" form of the Walsh matrix. However, many important questions remain open with respect to the transient behavior of the discrete quantum walks on the symmetric group. In particular , we were not able to derive a result similar to [22] on the spread of the probabilities to large cycles, as is known for the continuous case. The extra coin space of the discrete coined quantum walk creates additional challenges. This makes deriving a spectral decomposition based the irreducible representations, as was done in [22] for the continuous case, especially difficult.

7 Statements and Declarations

Acknowledgments. The author acknowledges National Science Foundation for supporting part of this research (Grant no. CCF-2246144).

Conflicts of Interest. There are no conflicts of interest or competing interest.

Data Availability. The simulations were carried out using Mathematica and the code is available here.

References

[1] Lovász, L.: Random walks on graphs. Combinatorics, Paul erdos is eighty **2**(1-46), 4 (1993)

[2] Lubotzky, A.: Ramanujan complexes and high dimensional expanders. Japanese Journal of Mathematics **9**(2), 137–169 (2014)

[3] Godsil, C., Royle, G.F.: Algebraic Graph Theory vol. 207. Springer, New York (2001)

[4] Kendon, V.: Decoherence in quantum walks–a review. Mathematical Structures in Computer Science **17**(6), 1169–1220 (2007)

[5] Aharonov, Y., Davidovich, L., Zagury, N.: Quantum random walks. Physical Review A **48**(2), 1687 (1993)

[6] Farhi, E., Gutmann, S.: Quantum computation and decision trees. Physical Review A **58**(2), 915 (1998)

[7] Meyer, D.A.: From quantum cellular automata to quantum lattice gases. Journal of Statistical Physics **85**(5), 551–574 (1996)

[8] Magniez, F., Nayak, A., Roland, J., Santha, M.: Search via quantum walk. SIAM journal on computing **40**(1), 142–164 (2011)

[9] Ambainis, A.: Quantum random walks–new method for designing quantum algorithms. In: International Conference on Current Trends in Theory and Practice of Computer Science, pp. 1–4 (2008). Springer

[10] Apers, S.: Expansion testing using quantum fast-forwarding and seed sets. Quantum **4**, 323 (2020)

[11] Aharonov, D., Ambainis, A., Kempe, J., Vazirani, U.: Quantum walks on graphs. In: Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing, pp. 50–59 (2001)

[12] Feldman, E., Hillery, M.: Modifying quantum walks: a scattering theory approach. Journal of Physics A: Mathematical and Theoretical **40**(37), 11343 (2007)

[13] Lipton, R.J., Regan, K.W.: Quantum Algorithms Via Linear Algebra: A Primer. MIT Press, Cambridge, USA (2014)

[14] Shenvi, N., Kempe, J., Whaley, K.B.: Quantum random-walk search algorithm. Physical Review A **67**(5), 052307 (2003)

[15] Nayak, A., Vishwanath, A.: Quantum walk on the line. arXiv preprint quant-ph/0010117 (2000)

[16] Moore, C., Russell, A.: Quantum walks on the hypercube. In: International Workshop on Randomization and Approximation Techniques in Computer Science, pp. 164–178 (2002)

[17] Acevedo, O.L., Gobron, T.: Quantum walks on cayley graphs. Journal of Physics A: Mathematical and General **39**(3), 585 (2005)

[18] D'Ariano, G.M., Erba, M., Perinotti, P., Tosini, A.: Virtually abelian quantum walks. Journal of Physics A: Mathematical and Theoretical **50**(3), 035301 (2016)

[19] Dai, W., Yuan, J., Li, D.: Discrete-time quantum walk on the cayley graph of the dihedral group. Quantum Information Processing **17**(12), 1–21 (2018)

[20] Venegas-Andraca, S.E.: Quantum walks: a comprehensive review. Quantum Information Processing **11**(5), 1015–1106 (2012)

[21] Knittel, M., Bassirian, R.: Quantum random walks on cayley graphs

[22] Gerhardt, H., Watrous, J.: Continuous-time quantum walks on the symmetric group. In: Approximation, Randomization, and Combinatorial Optimization.. Algorithms and Techniques, pp. 290–301 (2003)

[23] Diaconis, P.: Group representations in probability and statistics. Lecture notes-monograph series **11**, 192 (1988)

[24] Terras, A.: Fourier Analysis on Finite Groups and Applications vol. 43. Cambridge University Press, Cambridge (1999)

[25] Diaconis, P., Saloff-Coste, L.: Comparison techniques for random walk on finite groups. The Annals of Probability, 2131–2156 (1993)

[26] Levin, D.A., Peres, Y.: Markov Chains and Mixing Times vol. 107. American Mathematical Soc., Rhode Island (2017)