Random Motion on Finite Rings, II: Noncommutative Rings

Arvind Ayyer and Pooja Singla

Abstract. We extend our previous study of Markov chains on finite commutative rings to arbitrary finite rings with identity. At each step, we either add or multiply by a randomly chosen element of the ring, where the addition (resp. multiplication) distribution is uniform (resp. conjugacy invariant). We present explicit formulas both for the eigenvalues of the transition matrix as well as the stationary distribution. For the special case of the rings $M_2(F_q)$, we prove that the mixing time is bounded by an absolute constant.

1. Introduction

Random walks on finite noncommutative groups have been a subject of extensive study. The most famous examples are perhaps those concerning random walks on the symmetric group $S_n$ under the label of card-shuffling problems. Starting with the random-transpositions model [8], a lot of progress has been made in understanding the mixing times for such random walks. In particular, most of these shuffling algorithms satisfy the so-called cutoff phenomenon. See [7] for a survey of card-shuffling random walks.

In a completely different direction, the problem of efficient generation of quasi-random integers led to the development of random walks with fast mixing properties on $\mathbb{Z}/n\mathbb{Z}$ [6, 10]. For these walks, the fact that $\mathbb{Z}/n\mathbb{Z}$ has the structure of a ring is crucial; both additive and multiplicative operations were used to define the random walks. These ideas were extended to random walks on the vector spaces $\mathbb{Z}_p^d$ [2, 1, 11]. In an earlier work, we have studied a general class of random walks on finite commutative rings [3]. This has since been extended to random walks on modules of finite commutative rings [4].

In this work, we combine these two threads of ideas and consider random walks on finite rings generalising our work on finite commutative rings. The setup is as follows. Let $R$ be a finite ring with identity. We define two probability distributions on $R$. The first, $U$ is the uniform distribution. For the second, we need some notation. We say that two elements $a, b \in R$ belong to the same similarity class if there exists a left-invertible element $u \in R$ such that $b = uau^{-1}$. One also says that in such a case $a$ and $b$ are associates. We remark that as $R$ is a finite ring, an element is left invertible if and only if it is invertible on both sides. Let $Q$ be any distribution on $R$ which is constant on similarity classes. Then define a discrete-time Markov chain $(X_t)_{t \in \mathbb{Z}^+}$ on $R$ as follows.
At each step, toss an independent coin with Heads probability \( \alpha \in (0,1) \). If the coin lands Heads, set \( X_{t+1} = X_t + Y \) where \( Y \) is chosen independently according to \( U \), and otherwise, set \( X_{t+1} = X_t \cdot Z \), where \( Z \) is chosen independently according to \( Q \). Note that if \( R \) is commutative, all similarity classes are singletons and there is no restriction on the distribution \( Q \).

Let the transition matrix of \( (X_t)_{t \in \mathbb{Z}_{\geq 0}} \) on \( R \) be denoted \( M_R \). In other words, \( M_R \) is the matrix indexed by the elements of \( R \) with \( M_R(a,b) \) is the one-step transition probability of getting from \( a \) to \( b \). Let \( 1_{|R|} \) be the column vector of length \( |R| \) with all ones. Then, we can write

\[
M_R = \frac{\alpha}{|R|} 1_{|R|} 1_{|R|}^\text{tr} + (1 - \alpha) B_R,
\]

where \( B_R \) encodes only multiplicative transitions given by

\[
B_R(a,b) = \sum_{x \in R} Q(x).
\]

It then follows that if the eigenvalues of \( B_R \) are given by \( \lambda_1 = 1, \lambda_2, \ldots, \lambda_{|R|} \), the eigenvalues of \( M_R \) are given by \( \lambda_1 = 1, (1 - \alpha) \lambda_2, \ldots, (1 - \alpha) \lambda_{|R|} \); see, for example, [9, Corollary 3.1].

The plan of the rest of the paper is as follows. We prove a formula for the eigenvalues and their multiplicities of the transition matrix \( M_R \) of the chain \( (X_t)_{t \in \mathbb{Z}_{\geq 0}} \) in Section 2. Since all entries of \( M_R \) are positive, it immediately follows that \( (X_t)_{t \in \mathbb{Z}_{\geq 0}} \) is irreducible and aperiodic, and hence has a unique stationary distribution. We will give a recursive formula for the stationary distribution in Section 3. Lastly, we will consider the example of the matrix ring \( M_2(\mathbb{F}_q) \) in detail in Section 4. In particular, we will consider the “uniform multiplication” chain \( (X_t^{(n)})_{t \in \mathbb{Z}_{\geq 0}} \), which is similar in definition to \( (X_t)_{t \in \mathbb{Z}_{\geq 0}} \), except that both \( U \) and \( V \) are chosen according to \( U \) at each step. We will then compute the stationary distribution for \( (X_t^{(n)})_{t \in \mathbb{Z}_{\geq 0}} \) in Section 4.3 and show that the chain \( (X_t^{(n)})_{t \in \mathbb{Z}_{\geq 0}} \) on \( M_2(\mathbb{F}_q) \) mixes in constant time in Section 4.4.

2. Spectrum

Let \( R \) be a finite ring with identity. The set of invertible elements of \( R \) forms a group, which we denote by \( U_R \). For \( a \in R \), let \( I_a \) denote the principal left ideal generated by \( a \). Let \( \phi \) be a fixed set of generators of distinct principal ideals of \( R \). Let \( S_a \) be the set of all elements of \( I_a \) that generate \( I_a \) as a left ideal. For \( a \in R \), let \( \text{LAnn}(a) = \{ x \in R \mid xa = 0 \} \) be the left annihilator of \( a \) and \( \text{LStab}(a) = \{ x \in U_R \mid xa = a \} \) be the set of elements of \( U_R \) that fix \( a \) by acting from the left. Then \( \text{LStab}(a) \) is a subgroup of \( U_R \) for all \( a \in R \). The set of equivalence classes of finite dimensional complex irreducible representations of \( U_R \) is denoted by \( \text{Irr}(U_R) \). The one-dimensional trivial representation of a group \( G \) is denoted by \( 1_G \). For \( a \in \phi \), we denote \( \Sigma_a \) for the set of all inequivalent
irreducible representations of $U_R$ that are constituents of $\text{Ind}_{\text{LStab}(a)}^{U_R}(1_{\text{LStab}(a)})$. In other words, $\Sigma_a$ can be written as

\begin{equation}
(2.1) \quad \Sigma_a = \{ \rho \in \text{Irr}(U_R) \mid \text{Hom}_{U_R}(\rho, \text{Ind}_{\text{LStab}(a)}^{U_R}(1_{\text{LStab}(a)})) \neq 0 \}.
\end{equation}

The group $U_R$ acts on $R$ by conjugation. For any $r \in R$, we call the set $C_r = \{ uru^{-1} \mid u \in U_R \}$ as the similarity class of $r$. If $r \in U_R$, we will also use the term conjugacy class for $C_r$. For any subset $S$ of $R$, let $C_r S = \{ ts \mid t \in C_r \text{ and } s \in S \}$. Let $\psi$ be a fixed set of similarity class representatives of $R$. For $a \in \phi$, we define the set $F_a$ as follows.

\begin{equation}
(2.2) \quad F_a = \{ x \in \psi \mid (C_x S_a) \cap S_a \neq \emptyset \}.
\end{equation}

Let $C[R]$ be the complex vector space obtained by considering the formal basis $\{ e_r \mid r \in R \}$. Further, define multiplication on basis elements of $C[R]$ by the following.

$$e_r e_s = e_{rs}, \quad \text{for all } r, s \in R.$$ 

By extending this multiplication linearly to all elements of $C[R]$ we obtain that $C[R]$ is a finite dimensional associative algebra which is not necessarily commutative. Every element of ring $R$ belongs to some principal ideal, therefore $R = \cup_{a \in \phi} I_a$ clearly. Further it is easy to see that $S_a = I_a \setminus \sum_{I_b \subseteq I_a} I_b$. This in particular gives the following.

\begin{equation}
(2.3) \quad C[R] = \bigoplus_{a \in \phi} C[S_a],
\end{equation}

where $C[S_a]$ is a subspace of $C[R]$ with formal basis $\{ e_r \mid r \in S_a \}$. Similarly the spaces $C[I_a]$ and $C[U_R]$ are defined, where the latter coincides with the usual group algebra of $U_R$. We have the following relation between $U_R$ and the elements of $S_a$

**Lemma 2.1** ([4, 4, Appendix A]). For any $x, y \in S_a$, there exists $u \in U_R$ such that $ux = y$.

In particular, Lemma 2.1 implies that the group $U_R$ acts transitively on $S_a$ by permuting its elements. Therefore the set $S_a$ is in bijective correspondence with the set of left coset representatives of $U_R/\text{LStab}(a)$ via $u \mapsto ua$. This bijection preserves the $U_R$-action. Therefore as representations of $U_R$, we have $C[S_a] \cong \text{Ind}_{\text{LStab}(a)}^{U_R}(1_{\text{LStab}(a)})$.

Given a representation $\rho : U_R \to \text{GL}(V)$ of $U_R$, we define a representation $\tilde{\rho} : C[U_R] \to \text{End}(V)$ of group algebra $C[U_R]$ by $\tilde{\rho}(\sum g a_g e_g) = \sum g a_g \rho(g)$. This in particular endows $V$ with a $C[U_R]$-module structure. It is easy to see that $\rho$ is an irreducible representation of $U_R$ if and only if $V$ is an irreducible $C[U_R]$-module under the above defined action of $C[U_R]$. We are now in a position to describe the spectrum of the transition matrix $B_R$.

**Theorem 2.2.** For every $a \in \phi$, the following results hold.

- For every $x \in F_a$, there exists a class function $F_{x,a} \in C[U_R]$ such that $F_{x,a} e_a = \left( \sum_{y \in C_x} y \right) e_a$ in the quotient space $C[I_a] / \sum_{I_b \subseteq I_a} C[I_b]$. 

• For every $\rho \in \Sigma_a$, we obtain an eigenvalue $\lambda_\rho$ of $B_R$ given by,

$$\lambda_\rho = \sum_{x \in F_a} \beta_x \frac{\text{Tr}(\beta(F_{x,a}))}{\text{dim}(\rho)}.$$  

Conversely, every eigenvalue of $B_R$ is of this form for some $\rho \in \Sigma_a$.
• For $b \in R$, let $m_b(\rho)$ be the multiplicity of $\rho$ as a $U_R$-irreducible subrepresentation of $\mathbb{C}[S_b]$. For every $\rho \in \Sigma_a$, the algebraic multiplicity, $m(\lambda_\rho)$ of $\lambda_\rho$ for $\rho \in \Sigma_a$, is given by

$$m(\lambda_\rho) = \sum_{\{b \in \phi|F_b = F_a, \rho \in \Sigma_a\}} (m_b(\rho) \text{dim}(\rho)).$$

Proof. It is well known that eigenvalues of $B_R$ are the same as that of the operator of the semigroup algebra $\mathbb{C}[R]$ obtained by multiplying on the left by $\sum_{x \in R} \beta_x x$ (see [5, Section 7], for example). Further, by the definition of $\beta_x$, we have $\sum_{x \in R} \beta_x x = \sum_{x \in \psi} \beta_x (\sum_{v \in C_x} v)$. For $x \in \psi$, define $H_x := \sum_{v \in C_x} v$ and consider it as an operator of $\mathbb{C}[R]$ obtained by multiplying on the left. To obtain our result we show that there exists a basis of $\mathbb{C}[R]$ with respect to which matrix of $H_x$ for all $x \in \psi$, is upper triangular with diagonal entries of the form $\frac{\text{Tr}(\beta(F_{x,a}))}{\text{dim}(\rho)}$ for every irreducible constituent $\rho$ of $\text{Ind}_{L_{\text{Stab}(a)}}(1_{L_{\text{Stab}(a)}})$ with appropriate multiplicity.

To this end, we restrict the action of $H_x$ to $\mathbb{C}[I_a]$ and $\mathbb{C}[S_a]$ respectively and observe that although $H_x$ is an endomorphism of $\mathbb{C}[I_a]$, it need not be an endomorphism of $\mathbb{C}[S_a]$. Let $P_a : \mathbb{C}[I_a] \to \mathbb{C}[S_a]$ be a projection that commutes with the $U_R$-action. The existence of such $P_a$ is guaranteed because both $\mathbb{C}[I_a]$ and $\mathbb{C}[S_a]$ are semi-simple as $U_R$-modules. Let $H_{x,a} = H_x|_{S_a}$ and define $H'_{x,a} : \mathbb{C}[S_a] \to \mathbb{C}[S_a]$ by $H'_{x,a} = P_a \circ H_{x,a}$. Then, by definition $H'_{x,a}$ is a vector space endomorphism of $\mathbb{C}[S_a]$.

We define a partial order on $\phi$ by $a \leq b$ if and only if $I_b \subseteq I_a$. For each $a \in \phi$, we fix an ordered basis $B_a$ of $\mathbb{C}[S_a]$. We fix an ordered basis for $\mathbb{C}[R]$ where elements of $B_a$ appear before $B_b$ if $a \leq b$. We note that for every $a \in \phi$ and every $z \in \mathbb{C}[S_a]$, we have $\sum_{x \in \psi} H_{x,z} = \sum_{x \in \psi} H_{x,a} z + \omega$ for some $\omega \in \sum_{I_b \subseteq I_a} \mathbb{C}[I_b]$. Thus, the matrix of $H_x$ in the above basis is block upper-triangular. Our goal is to show that there exists a choice of basis of $B_a$ such that the diagonal blocks are in fact diagonal with the desired entries.

First, we show that for every $x \in F_a$, there exists $F_{x,a} \in \mathbb{C}[U_R]$ such that the following hold.

1. The element $F_{x,a} \in \mathbb{C}[U_R]$ is a class function.
2. The action of $H'_{x,a}$ on $\mathbb{C}[S_a]$ coincides with that of $F_{x,a}$ on $\mathbb{C}[S_a]$. 

For this we note that by the definition of $\mathcal{H}_x$, $\mathcal{H}_{x,a}$ and Lemma 2.1, there exists $\sum_{u \in U_R} h_u u \in \mathbb{C}[U_R]$ such that

\begin{equation}
\mathcal{H}_{x,a}(e_a) = \left( \sum_{u \in U_R} h_u u \right) e_a + w, \text{ for some } w \in \sum_{h \leq I_a} \mathbb{C}[I_b].
\end{equation}

Therefore, by the definition of $\mathcal{H}'_{x,a}$, the following holds.

\begin{equation}
\mathcal{H}'_{x,a}(e_a) = \left( \sum_{u \in U_R} h_u u \right) (e_a),
\end{equation}

We also note that $\mathcal{H}_{x,a} u' = u' \mathcal{H}_{x,a}$ for all $u' \in U_R$. Therefore $h_{u' u} = h_{u u'}$, for all $u, u' \in U_R$. Define $\mathcal{F}_{x,a} \in \mathbb{C}[U_R]$ by $\mathcal{F}_{x,a} = \sum_{u \in U_R} h_u u$, where $h_u$ are as in (2.5). Then as shown above $\mathcal{F}_{x,a} \in \mathbb{C}[U_R]$ is a class function, and moreover on the generating set $\{ e_{u a} \mid u \in U_R \}$, the action of $\mathcal{F}_{x,a}$ and $\mathcal{H}'_{x,a}$ coincide.

Let $\mathbb{C}[S_a] \cong V_1 \oplus V_2 \oplus \cdots \oplus V_t$ be a decomposition of $\mathbb{C}[S_a]$ into its irreducible constituents such that $d_i = \dim(V_i)$. Consider an ordered basis $B_a = \{ v_{1,1}, \ldots, v_{1,d_1}, v_{2,1}, v_{2,2}, \ldots, v_{t,d_t} \}$ of $\mathbb{C}[S_a]$ such that $v_{i,j} \in V_i$ for $1 \leq j \leq d_j$. The function $\mathcal{F}_{x,a} \in \mathbb{C}[U_R]$ is a class function. This in particular implies that if $V$ is an irreducible $U_R$-submodule of $\mathbb{C}[U_R]$, then $V$ is $\mathcal{F}_{x,a}$-invariant and the action of $\mathcal{F}_{x,a}$ on $V$ is multiplication by a scalar. Therefore we obtain that matrix of $\mathcal{F}_{x,a}$ with respect to $B_a$, as an endomorphism of $\mathbb{C}[S_a]$, is a diagonal matrix with diagonal entries given by $\lambda_{j} = \frac{\Tr(\tilde{\mathcal{F}}_{x,a})}{\dim(\rho)}$ for each irreducible constituent $\rho$ of $\text{Ind}_{\mathcal{LStab}(a)}^{U_R}(1_{\mathcal{LStab}(a)})$. Let $\rho$ be an irreducible sub-representation of $\text{Ind}_{\mathcal{LStab}(a)}^{U_R}(1_{\mathcal{LStab}(a)})$ such that $\text{Hom}_{U_R}(\text{Ind}_{\mathcal{LStab}(a)}^{U_R}(1_{\mathcal{LStab}(a)}), \rho) = m_{\rho}(\rho)$. Then, by this choice of basis, it follows that the algebraic multiplicity of $\lambda_{\rho}$ as an eigenvalue of $\mathcal{H}'_{x,a}$ (as an endomorphism of $\mathbb{C}[S_a]$) is $m_{\rho}(\dim(\rho))$ for every $a \in \phi$. Combining this result with the fact that $\sum_{x \in R} \beta_x = \sum_{x \in \psi} \beta_x \mathcal{H}_x$, we obtain our result.

3. Stationary distribution

We now give a recursive formula for the stationary distribution $\pi$ of the chain. The formula is a special case of the one for arbitrary Markov chains [13] and is very similar in spirit to the commutative case [3, Theorem 2.4].

Proposition 3.1. For $a, b \in R$ such that $S_b = S_a$, we have that $\pi(a) = \pi(b)$.

Proof. There exists an element $u \in U_R$ such that $u a = b$ by Lemma 2.1. Therefore, left multiplication by $u$ is an inner automorphism of $R$ which takes $a$ to $b$. Moreover, for any $c, d \in R$,

$$B_R(u,c,d) = \sum_{x \in R \atop xc = ud} Q(x) = \sum_{y \in R \atop yc = d} Q(y) = B_R(c,d).$$
Therefore, all transition rates are unchanged, and the automorphism causes only a relabelling of rows and columns of \( M_R \). 

For any \( x, y \in R \), let \( R_{x,y} = \{ r \mid ry = x \} \). Then \( R_{x,y} \neq \emptyset \) if and only if \( I_x \subseteq I_y \). Further, in case \( R_{x,y} \neq \emptyset \) then we must have \( |R_{x,y}| = |\text{LAnn}_R(y)| \). For any \( x \in R \), we use \( U_x \subseteq U_R \) to denote the set of distinct coset representatives of \( \text{LStab}(x) \) in \( U_R \). In case \( R \) is commutative the set \( U_x \) has a group structure however this does not hold for the case of non-commutative ring \( R \).

We now state the main theorem of this section. Recall that \( \phi \) is a set of generators of distinct principal ideals of \( R \).

**Theorem 3.2.** Let \( R \) be a finite ring. The stationary probability \( \pi(x) \) for \( x \in R \) in \( (X_t)_{t \in \mathbb{Z}_{\geq 0}} \) is given by

\[
\pi(x) = \frac{\alpha}{|R|} + (1 - \alpha) \sum_{y \in \phi, I_x \subseteq I_y} \left( \sum_{u \in U_y, r \in R_{x,y}} Q(ru^{-1}) \right) \pi(y) 
\]

\[
1 - (1 - \alpha) \sum_{u \in U_x, r \in R_{x,x}} Q(ru^{-1})
\]

**Proof.** The strategy of proof is essentially identical to that of the proof of Theorem 2.4 in [3], and we will be a lot more sketchy.

The stationary distribution satisfies the master equation,

\[
\pi(x) = \sum_{y \in R} \mathbb{P}(y \rightarrow x) \pi(y).
\]

Now, \( \mathbb{P}(y \rightarrow x) \geq \alpha/|R| \) for all \( y \in R \) because of the addition transition. To keep track of when multiplicative transitions can occur, we look at the poset of principal ideals, and we see that

\[
\pi(x) = \frac{\alpha}{|R|} + (1 - \alpha) \sum_{y \in R, I_x \subseteq I_y} B_R(y,x) \pi(y).
\]

Now, we split the sum on the right hand side depending on whether \( I_y = I_x \) or not. Using Lemma 2.1 and Proposition 3.1 we find that

\[
\sum_{y \in R, I_x = I_y} B_R(y,x) \pi(y) = \pi(x) \sum_{u \in U_x, r \in R_{x,x}} Q(ru^{-1}),
\]

and

\[
\sum_{y \in \phi, I_x \subseteq I_y} B_R(y,x) \pi(y) = \sum_{y \in \phi} \pi(y) \sum_{u \in U_y, r \in R_{x,y}} Q(ru^{-1}).
\]

Substituting the last two identities in the previous sum gives us the desired result. \( \square \)
As a corollary, we obtain the stationary distribution for $(X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}$. Somewhat surprisingly, the answer is identical to that of the commutative case (Corollary 2.5) in [3].

**Corollary 3.3.** Let $R$ be a finite ring. The stationary probability $\pi(x)$ for $x \in R$ in $(X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}$ is given by

$$\pi_U(x) = \frac{\alpha + (1 - \alpha) \sum_{y \in \phi, I_x \subseteq I_y} |U_y| |LAnn_R(y)| \pi_U(y)}{|R| - (1 - \alpha)|U_x| |LAnn_R(x)|}.$$

**Proof.** This immediately follows from Theorem 3.2 and the fact that $|R_{x,y}| = |LAnn_R(y)|$ for every $x, y \in R$ such that $I_x \subseteq I_y$. □

The formula for the stationary probability of units can then be derived immediately.

**Corollary 3.4.** Let $R$ be a finite ring. The stationary probability $\pi(u)$ for $u \in U_R$ in $(X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}$ is given by

$$\pi_U(u) = \frac{\alpha}{n - u + u\alpha}.$$

The above result is identical to that obtained for commutative rings [3].

**Example 3.5.** For the ring $M_2(\mathbb{F}_2)$, the multiplicative part of the transition matrix $B_R$ in the lexicographically ordered basis,

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\},$$

is given by

$$\begin{pmatrix} 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 4 \\ 4 & 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 4 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 4 \end{pmatrix}.$$
The stationary probability of the units is
\[ \pi \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \pi \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \pi \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pi \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \pi \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \pi \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \pi \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{\alpha}{2(3\alpha + 5)}. \]
of the nonzero non-units is
\[ \pi \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \pi \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \pi \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \pi \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \pi \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \pi \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \pi \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \frac{2\alpha}{(3\alpha + 1)(3\alpha + 5)}. \]
and of zero is
\[ \pi \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \frac{5 - 3\alpha}{(3\alpha + 1)(3\alpha + 5)}. \]

4. The matrix ring \( M_2(\mathbb{F}_q) \)

Let \( R = M_2(\mathbb{F}_q) \) be the ring of \( 2 \times 2 \) matrices with entries over the finite field \( \mathbb{F}_q \), where \( q > 2 \). For \( q = 2 \), the description of conjugacy classes of \( \text{GL}_2(\mathbb{F}_q) \) is slightly different, but the computations are similar.

Recall that \( U_R = \text{GL}_2(\mathbb{F}_q) \) is the group of \( 2 \times 2 \) invertible with entries from \( \mathbb{F}_q \) and \(|U_R| = (q^2 - 1)(q^2 - q)\). To avoid any confusion, in this section we will use uppercase letters to denote elements of \( R \) and lowercase letters for the field \( \mathbb{F}_q \).

The set
\[
\phi = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & z \\ 0 & 0 \end{pmatrix}, \right\}_{z \in \mathbb{F}_q}
\]
is a set of representatives of distinct principal ideals of \( R \). The set
\[
\psi = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, \right\}_{x \in \mathbb{F}_q} \bigcup \left\{ \begin{pmatrix} x & 0 \\ 1 & x \end{pmatrix}, \right\}_{x \in \mathbb{F}_q} \bigcup \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \right\}_{x \neq y \in \mathbb{F}_q} \bigcup \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}, \right\}_{\alpha \in \mathbb{F}_q^2 \setminus \mathbb{F}_q}
\]
is a set of representatives of similarity classes of \( M_2(\mathbb{F}_q) \). Further, we say a similarity class is \textit{invertible} if it is contained in \( \text{GL}_2(\mathbb{F}_q) \). Otherwise we call a similarity class \textit{non-invertible}. We note that this does not depend on the similarity class representative. The set of non-invertible similarity classes, denoted \( \psi^0 \), is given by
\[
\psi^0 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \right\}_{x \in \mathbb{F}_q^\times}.
\]
We denote the set of invertible classes as \( \psi^x = \psi \setminus \psi^0 \). Next, for each \( A \in \phi \), we describe below the set of generators of the principal ideal generated by \( A \), denoted by \( S_A \), and the (left) stabilizer of \( A \) in \( U_R \), denoted by \( \text{LStab}(A) \). Recall that \( \text{LStab}(A) \) is the set of elements \( X \in U_R \) such that \( XA = A \).

### Table 1

| \( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) | \( \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \) | \( \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \) | GL\(_2\)(\( F_q \)) | \( \psi^0 \) |
|---|---|---|---|---|
| \begin{align*}
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \in \phi \\
S_A & = \text{GL}_2(\mathbb{F}_q) \\
\text{LStab}(A) & = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
F_A & \cap \psi^0 = \emptyset
\end{align*}
| \begin{align*}
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \in \phi \\
S_A & = \{ (0, a) \mid a \neq (0,0) \} \\
\text{LStab}(A) & = \{ (1, y) \mid y \in \mathbb{F}_q, w \in \mathbb{F}_q^\times \} \\
F_A & \cap \psi^0 = \emptyset
\end{align*}
| \begin{align*}
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \in \phi \\
S_A & = \{ (a, za) \mid a \neq (0,0) \} \\
\text{LStab}(A) & = \{ (1, y) \mid y \in \mathbb{F}_q, w \in \mathbb{F}_q^\times \} \\
F_A & \cap \psi^0 = \emptyset
\end{align*}

\( A \in \phi \) and \( F_{X,A} \). We now describe \( F_A \), defined in (2.2), for every \( A \in \phi \). For any \( x \in \psi \) such that \( s \) is invertible, we have \( xS_A \subseteq S_A \). Therefore \( \psi^x \subseteq F_A \) for each \( A \in \phi \). It remains to determine \( F_A \cap \psi^0 \). We give the representatives of similarity classes that are contained in \( F_A \cap \psi^0 \) in Table 1 for every \( A \in \phi \).

Our next step is, for each \( A \in \phi \) and \( X \in F_A \), to identify \( F_{X,A} \) satisfying the hypothesis of Theorem 2.2. To that end, consider the operator \( \mathcal{H}_{X,A} = \sum_{V \in U_R} XVV^{-1} : \mathbb{C}[t_A] \to \mathbb{C}[S_A] \) and \( \mathcal{H}'_{X,A} : \mathbb{C}[S_A] \to \mathbb{C}[S_A] \), obtained by composing \( \mathcal{H}_A \) with the natural inclusion and projection. For case \( X \in F_A \cap \psi^x \), the function \( F_{X,A} = \mathcal{H}'_{X,A} \) itself works. Therefore, we now focus on the case where \( X \in F_A \cap \psi^0 \), and we explicitly describe \( F_{X,A} \). The existence of these was proved in Theorem 2.2. For \( A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \), the function \( F_{X,A} = |C_X|e_{(1, 0)} \) itself works for all \( X \in F_A \cap \psi^0 \). We are left to deal with the cases for all \( A \in \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 1 & z \\ 0 & 0 \end{pmatrix} \right\} \subseteq \mathbb{F}_q^\times \).

For simplicity, we use the notation,

\[
Y_t = \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{for} \ t \in \mathbb{F}_q^\times \quad \text{and} \quad Y_0 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.
\]
We obtain the following by direct computations and these work uniformly for all such \( A \).

\[
\mathcal{F}_{Y_t,A} = \sum_{v \in C \left( \frac{1}{1} \right)} e_v + e_{\left( \begin{smallmatrix} 0 & t \\ 0 & 1 \end{smallmatrix} \right)},
\]

(4.1)

\[
\mathcal{F}_{Y_0,A} = \sum_{v \in C \left( \frac{1}{1} \right)} e_v - (q - 1) e_{\left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)}.
\]

4.2. Description of \( \Sigma_A \). Next, for every \( A \in \phi \), we describe \( \Sigma_A \), defined in (2.1). Thus \( \Sigma_A \) consists of inequivalent irreducible constituents of \( \text{Ind}_{\text{LStab}(A)}^U(\mathbb{1}_{\text{LStab}(A)}) \).

In one extreme case, \( \text{LStab}(A) = \text{GL}_2(F_q) \), we have \( U_R = \text{LStab}(a) \) and therefore \( \text{Ind}_{\text{LStab}(A)}^U(\mathbb{1}_{\text{LStab}(a)}) \) is the trivial representation of \( \text{GL}_2(F_q) \). In the other extreme, \( \text{LStab}(A) = \left( \begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right) \) and \( \text{Ind}_{\text{LStab}(A)}^U(\mathbb{1}_{\text{LStab}(a)}) \) is the regular representation of \( \text{GL}_2(F_q) \) and therefore \( \Sigma_A \) in this set consists of all inequivalent irreducible representations of \( \text{GL}_2(F_q) \). For the reader’s convenience, we have given a description of all irreducible representations of \( \text{GL}_2(F_q) \) along with their character values in Appendix A.

Let \( P \) be the subgroup of \( \text{GL}_2(F_q) \) consisting of matrices of the form \( \left( \begin{smallmatrix} 1 & y \\ 0 & w \end{smallmatrix} \right) \), where \( w \in F_q^\times \). Then, from Table 1 we see that \( P \) is \( \text{LStab}(A) \) for some \( A \in \phi \). So, we need to describe the irreducible constituents of \( \text{Ind}_P^{\text{GL}_2(F_q)}(\mathbb{1}_P) \). The trivial representation of the group \( F_q^\times \) is denoted by \( \mathbb{1}_q \) for simplification. We use the notation of Appendix A to give this description.

Proposition 4.1. The space \( \text{Ind}_P^{\text{GL}_2(F_q)}(\mathbb{1}_P) \) has the following decomposition into \( \text{GL}_2(F_q) \)-irreducible constituents.

(4.2) \[
\text{Ind}_P^{\text{GL}_2(F_q)}(\mathbb{1}_P) \cong \mathbb{1}_{\text{GL}_2(F_q)} \oplus \rho_{\mathbb{1}_q} \oplus \rho_{\chi,\mathbb{1}_q},
\]

where \( \rho_{\mathbb{1}_q} \) and \( \rho_{\chi,\mathbb{1}_q} \) are given in Table 4.

Proof. Let \( S \) be the set of all irreducible constituents listed on the right side of (4.2).

We first note that both \( \text{Ind}_P^G(\mathbb{1}_P) \) and \( \mathbb{1}_G \oplus \rho_{\mathbb{1}_q} \oplus \rho_{\chi,\mathbb{1}_q} \) have dimension \((q^2 - 1)\). Thus, to complete the proof it is enough to show that any \( \rho \in S \) is indeed a constituent of \( \text{Ind}_P^{\text{GL}_2(F_q)}(\mathbb{1}_P) \). By Frobenius reciprocity, this is equivalent to proving that the restriction of \( \rho \) to \( P \) for each \( \rho \in S \) has a \( P \)-fixed vector, that is \( \text{Hom}_P(\text{Res}_P^{\text{GL}_2(F_q)}(\rho), \mathbb{1}_P) \neq 0 \), where \( \text{Res}_P^{\text{GL}_2(F_q)}(\rho) \) denotes the restriction of \( \rho \) to \( P \). The space \( \text{Hom}_G(\rho_1, \rho_2) \) of
intertwiners between two representations \( \rho_1 \) and \( \rho_2 \) of \( G \) is given by

\[
\dim(C(\text{Hom}_G(\rho_1, \rho_2))) = \frac{1}{|G|} \sum_{x \in G} \frac{\text{Tr}(\rho_1(x))\text{Tr}(\rho_2(x))}{\text{dim}(\rho_1)\text{dim}(\rho_2)}.
\]

(4.3)

Therefore, \( \text{Hom}_{\mathcal{P}}(\text{Res}_P^G(\rho), \mathbb{1}_P) \neq 0 \) for any \( \rho \in \mathcal{S} \) is equivalent to the fact that

\[
\frac{1}{|P|} \sum_{x \in P} \text{Tr}(\rho(x)) \neq 0.
\]

We further note that

\[
\sum_{x \in P} \text{Tr}(\rho(x)) = \text{Tr}\left(\rho\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + (q-1)\text{Tr}\left(\rho\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) + q\sum_{x \in \mathbb{F}_q^\times \setminus 1} \text{Tr}\left(\rho\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\right).
\]

Using the character values from Table 4, we obtain the following for each \( \rho \in \mathcal{S} \):

\[
\begin{align*}
\rho = \mathbb{1}_{\text{GL}_2(\mathbb{F}_q)} & : \sum_{x \in P} \text{Tr}(\rho(x)) = 1 + (q-1) + q(q-2) = q(q-1). \\
\rho = \rho_{1_q} & : \sum_{x \in P} \text{Tr}(\rho(x)) = q + q(q-2) = q(q-1). \\
\rho = \rho_{\chi,1_q} & : \sum_{x \in P} \text{Tr}(\rho(x)) = (q+1) + (q-1) + q\left(\sum_{x \in \mathbb{F}_q^\times \setminus 1} (\chi(x) + 1)\right) \\
& = 2q + q\sum_{x \in \mathbb{F}_q^\times} \chi(x) + q(q-3).
\end{align*}
\]

For every \( \mu \in \hat{\mathbb{F}_q^\times} \setminus 1_q \), we have \( \text{Hom}_{\mathbb{F}_q^\times}(\mu, 1_q) = 0 \). From (4.3), it is easy to see that \( \sum_{x \in \mathbb{F}_q^\times} \mu(x) = 0 \) for every \( \mu \in \hat{\mathbb{F}_q^\times} \setminus 1_q \). Therefore for every \( \rho \in \mathcal{S} \), we have

\[
\frac{1}{|P|} \sum_{x \in P} \text{Tr}(\rho(x)) \neq 0.
\]

This proves the equivalence given in (4.2). \( \square \)

We summarize all of this information of \( F_A \) and \( \Sigma_A \) for \( A \in \phi \) in Table 2.

Using Table 2 along with the description of \( F_{X,A} \) as given in Section 4.1, the character table in Table 4 and Theorem 2.2, we obtain a complete description of the eigenvalues of \( B_R \). We now describe the eigenvalues. Recall from Theorem 2.2 that for each \( A \in \phi \) and \( \rho \in \Sigma_A \), the eigenvalue \( \lambda_\rho \) is given by

\[
\lambda_\rho = \sum_{X \in F_A} \beta_X \frac{\text{Tr}(\tilde{\rho}(\mathbb{F}_{X,A}))}{\text{dim}(\rho)}.
\]

(a) For \( A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) and \( \rho \in \Sigma_A \), we have

\[
\lambda_\rho = \sum_{X \in \psi^\times} \beta_X |C_X| \chi_\rho(X),
\]
and the multiplicity of each $\lambda_\rho$ in this case is $\dim(\rho)^2$.

(b) For any $A \in \begin{bmatrix} 0&1 \\ 0&0 \end{bmatrix} \bigcup \begin{bmatrix} 1&z \\ 0&0 \end{bmatrix}_{z \in \mathbb{F}_q}$ and $\rho \in \Sigma_A$, we have:

$$\dim(\rho)(\lambda_\rho) = \sum_{X \in \psi^\times} \beta_X |C_X| \chi_\rho(X) + \beta_Y \left( (q^2 - 1) \chi_\rho \left( \begin{array}{ll} 1 & 1 \\ 0 & 1 \end{array} \right) - (q - 1) \chi_\rho \left( \begin{array}{ll} 1 & 0 \\ 0 & 1 \end{array} \right) \right)$$

$$+ \sum_{t \in \mathbb{F}_q^\times} \beta_Y \left( (q^2 - 1) \chi_\rho \left( \begin{array}{ll} t & 1 \\ 0 & t \end{array} \right) + \chi_\rho \left( \begin{array}{ll} t & 0 \\ 0 & t \end{array} \right) \right),$$

(4.4)

and each eigenvalue above appears with multiplicity $(q + 1)\dim(\rho)$.

(c) For $A = \begin{bmatrix} 0&0 \\ 0&0 \end{bmatrix}$ and $\rho \in \Sigma_A$, we have:

$$\lambda_\rho = \sum_{X \in \psi} \beta_X |C_X| = 1,$$

and this occurs with multiplicity one, as expected by Proposition 4.2.

Therefore we have a total of

$$|\text{GL}_2(\mathbb{F}_q)| + (q + 1) + q + (q - 2)(q + 1) + 1 = q^4 = |M_2(\mathbb{F}_q)|$$

eigenvalues of $B_R$, as expected. Recall from the paragraph immediately following 1.2 that the eigenvalues of $M_R$ are easily obtained from those of $B_R$.

4.3. Stationary distribution.
Proposition 4.2. The stationary distribution of $(X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}$ has the following formula:

$$
\pi(x) = \begin{cases} 
\frac{\alpha}{q^3 + q^2 - q - (q^2 - 1)(q^2 - q)\alpha}, & x \in U_R, \\
\frac{q^2\alpha}{(1 + (q^2 - 1)\alpha)(q^3 + q^2 - q - (q^2 - 1)(q^2 - q)\alpha)}, & x \notin U_R, x \neq 0, \\
\frac{q^3 + q^2 - q(q^2 - 1)\alpha}{(1 + (q^2 - 1)\alpha)(q^3 + q^2 - q - (q^2 - 1)(q^2 - q)\alpha)}, & x = 0.
\end{cases}
$$

Proof. The formula for units can be obtained by directly from Corollary 3.4. If $x$ is a nonzero nonunit, the only other ideal it belongs to is the one generated by 1. Therefore, from Corollary 3.3 it follows that

$$
\pi(x) = \frac{\alpha + (1 - \alpha)|U_R|\pi(1)}{|R| - (1 - \alpha)q^2(q^2 - 1)} = \frac{\alpha + (1 - \alpha)(q^2 - 1)(q^2 - q)\pi(1)}{q^4 - (1 - \alpha)q^2(q^2 - 1)},
$$

where we have used the fact that $|U_x| = |U_R/L\text{Stab}(x)| = q^2 - 1$ and $|L\text{Ann}(x)| = q^2$ for any nonzero nonunit $x$ by similar computations as those done in Table 1. A little simplification gives the result. The formula for the zero matrix is then a consequence of the total probability being 1. □

4.4. Mixing times. We will now prove that $(X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}$ on the matrix ring $R = M_2(\mathbb{F}_q)$ mixes in finite time. Let $M_R$ be the transition matrix of the chain, and $\pi$ be the stationary distribution.

We now define two vectors $v_1$ and $v_2$ on $\mathbb{C}[R]$ as follows:

$$
v_1(x) = \begin{cases} 
0 & x \in U_R, \\
1 & x \notin U_R, x \neq 0, \\
-(n - u - 1) & x = 0,
\end{cases}
$$

and

$$
v_2(x) = \begin{cases} 
-1/(q - 1) & x \in U_R, \\
1 & x \notin U_R, x \neq 0, \\
-(q^2 - 1) & x = 0.
\end{cases}
$$

Proposition 4.3. The row vectors $v_1$ and $v_2$ are eigenvectors of $M_R$ satisfying

$$
v_1M_R = \frac{(q^2 - 1)}{q^4}(1 - \alpha)v_1, \quad v_2M_R = \frac{(q - 1)(q^2 - 1)}{q^3}(1 - \alpha)v_2.
$$
Proof. The only ingredient needed is a formula for \((M_R)_{a,b}\) for different values of \(a\) and \(b\). The following table gives the values

| \(a \in U_R\) | \(b \in U_R\) | \(b \notin U_R, b \neq 0\) | \(b = 0\) |
|----------------|----------------|-----------------|-------|
| \(\alpha n\)  | \(\alpha n\)  | \(\frac{\alpha n}{n} + \frac{q^2(1-\alpha)}{n}\) | \(\frac{\alpha n}{n} + \frac{q^2(1-\alpha)}{n}\) |
| \(\alpha n\)  | \(\alpha n\)  | \(\frac{\alpha n}{n}\) | \(\frac{\alpha n}{n} + \frac{q^2(1-\alpha)}{n}\) |
| \(a = 0\)    | \(\alpha n\)  | \(\alpha n\) | \(1 - \frac{(n-1)\alpha}{n}\) |

Most of the entries here are clear. Only the last two entries in the second row need some explanation. For these, we note that for \(R = M_2(\mathbb{F}_q)\), if \(a, b \in R \setminus U_R\) then there exists \(r \in R\) such that \(ra = b\) if and only if either \(S_a = S_b\) or \(b = 0\). For any such \(b\) we obtain, by direct calculations similar to the ones we do for Table 1, \(|R_{a,b}| = |\text{LAnn}_R(a)| = q^2\).

We then compute \(v_iM_R\) for \(i = 1, 2\) entrywise by splitting the sum into these three cases. This is a purely computational exercise and we omit the proof.

Recall that \(e_0 \in \mathbb{C}[R]\) is the vector with 1 in the position indexed by the zero matrix and 0 elsewhere. The following result is then purely computational.

**Proposition 4.4.** The vector \(e_0\) can be expressed in terms of eigenvectors of \(M_R\) as

\[
e_0 = \pi - \frac{\alpha}{q(1 + (q^2 - 1)\alpha)}v_1 + \frac{(q - 1)\alpha}{n - u + u\alpha}v_2
\]

We are now in a position to state and prove the result for the mixing time of the chain \((X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}\).

**Theorem 4.5.** The mixing time for the chain \((X_t^{(u)})_{t \in \mathbb{Z}_{\geq 0}}\) with \(X_0^{(u)} = 0\) is bounded above by the constant

\[
t_{\text{mix}}(\epsilon) \leq \frac{\log \left(\frac{\epsilon \alpha}{8}\right)}{\log \left(\frac{3}{4}(1 - \alpha)\right)}.
\]

This says in particular that for values of \(\alpha\) close to 1, the mixing time is very small. In that case, most of the transitions take place by addition and the subgraph of the transition graph comprising of addition-transition is a complete graph with equal rates.

**Proof.** Begin by applying \(M_R^t\) to (4.7) and use the result of Proposition 4.3 to obtain

\[
e_0M_R^t = \pi - c_1e_1^tv_1 + c_2e_2^tv_2,
\]
where
\[
\begin{align*}
    c_1 &= \frac{\alpha}{q(1 + (q^2 - 1)\alpha)}, \quad c_2 = \frac{(q - 1)\alpha}{n - u + u\alpha}, \\
    e_1 &= \frac{(q^2 - 1)}{q^2}(1 - \alpha), \quad e_2 = \frac{(q - 1)(q^2 - 1)}{q^3}(1 - \alpha).
\end{align*}
\]

By definition, the total variation distance \(d_t\) between \(e_0 M^t_R\) and \(\pi\) is given by
\[
d_t := \frac{1}{2} || e_0 M^t_R - \pi ||_1 = \frac{1}{2} || -c_1 e_1^t v_1 + c_2 e_2^t v_2 ||_1.
\]

A quick computation shows that \(||v_1||_1 = ||v_2||_1 = 2(q^2 - 1)(q + 1)\) and the triangle inequality gives
\[
d_t \leq (q^2 - 1)(q + 1)(c_1 + c_2) e_1^t,
\]
where we have used the fact that \(e_2 < e_1\). It then follows that if
\[
t \geq \log \epsilon - \log ((q^2 - 1)(q + 1)(c_1 + c_2)),
\]
then \(d_t \leq \epsilon\). Since \(c_1 + c_2\) behaves like \(q^3\) for large \(q\), it is clear that \((q^2 - 1)(q + 1)(c_1 + c_2)\) can be bounded above. In particular, one can show that
\[
(q^2 - 1)(q + 1)(c_1 + c_2) \leq 2 \left(1 + \frac{1}{\alpha}\right).
\]

Using this and the fact that \((q^2 - 1)/q^2 \geq 3/4\), one obtains that
\[
t \geq \frac{\log \epsilon \alpha}{2(1 + \alpha) \log 3/4(1 - \alpha)}
\]
should suffice, completing the proof. \(\square\)

Acknowledgements

The authors were partially supported by the UGC Centre for Advanced Studies. AA was also partly supported by Department of Science and Technology grant EMR/2016/006624.

Appendix A. Irreducible representations of \(\text{GL}_2(\mathbb{F}_q)\)

In this section, we briefly describe the irreducible representations and the character table of \(\text{GL}_2(\mathbb{F}_q)\) for the sake of completeness. This is well known in the literature and can be found in many texts. Here we shall refer to [12] for all the details. For an abelian group \(A\), we use \(\hat{A}\) to denote the set of its all one-dimensional representations of \(A\). For a group \(G\), we use \(\mathbb{1}_G\) to denote the trivial one-dimensional representation of \(G\).
A.1. **Principal series representations of** \( \text{GL}_2(\mathbb{F}_q) \). Let \( U = \left\{ \left( \begin{array}{cc} 1 & w \\ 0 & 1 \end{array} \right) \right\} \) be the subgroup of \( \text{GL}_2(\mathbb{F}_q) \) consisting of all unipotent upper triangular matrices. An irreducible representation of \( \text{GL}_2(\mathbb{F}_q) \) is called a **principal series representation** if it is an irreducible constituent of \( \text{Ind}_{U}^{\text{GL}_2(\mathbb{F}_q)}(\mathbb{I}_U) \). Now we describe all of the principal series representations of \( \text{GL}_2(\mathbb{F}_q) \).

Let \( B = \left\{ \left( \begin{array}{cc} u & w \\ 0 & v \end{array} \right) \right\} \) be the subgroup of \( \text{GL}_2(\mathbb{F}_q) \) consisting of all upper triangular matrices. Let \( \mu_1, \mu_2 \in \widehat{\mathbb{F}_q^\times} \). Define the one-dimensional representation \( \mu_{1,2} \) of \( B \) by

\[
\mu_{1,2} : B \to \mathbb{C}^\times ; \ \mu_{1,2} \left( \begin{array}{cc} u & w \\ 0 & v \end{array} \right) = \mu_1(u)\mu_2(v).
\]

Let \( \rho_{\mu_1,\mu_2} = \text{Ind}_B^G(\mu_{1,2}) \) be the corresponding induced representation of \( \text{GL}_2(\mathbb{F}_q) \). Then we have the following result regarding their mutual relation.

**Proposition A.1.** For \( \mu_1, \mu_2 \in \widehat{\mathbb{F}_q^\times} \), the following hold.

1. \( \dim_{\mathbb{C}}(\text{Hom}_G(\rho_{\mu_1,\mu_2}, \rho_{\mu'_1,\mu'_2})) \neq 0 \) if and only if \( \{\mu_1, \mu_2\} = \{\mu'_1, \mu'_2\} \).
2. For \( \mu_1 \neq \mu_2 \), the representations \( \rho_{\mu_1,\mu_2} \) are irreducible.
3. For \( \mu_1 = \mu_2 \), we have \( \dim_{\mathbb{C}}(\text{End}_G(\rho_{\mu_1,\mu_1})) = 2 \).

The last part of the above proposition implies that for every \( \mu \in \widehat{\mathbb{F}_q^\times} \) the representation \( \rho_{\mu,\mu} \cong W_{\mu_1}^\mu \oplus W_{\mu_2}^\mu \), where \( W_{\mu_1}^\mu \) and \( W_{\mu_2}^\mu \) are inequivalent representations of \( G \). Next we describe one of the constituents of \( \rho_{\mu,\mu} \). The other one is the complement and is easily obtained. For every \( \mu \in \widehat{\mathbb{F}_q^\times} \), define the one-dimensional representation \( \det_{\mu} : \text{GL}_2(\mathbb{F}_q) \to \mathbb{C}^\times \) by \( \det_{\mu}(X) = \mu(\det(X)) \). Then it is easy to see that one of the constituents of \( \rho_{\mu,\mu} \) is isomorphic to the one-dimensional representation \( \det_{\mu} \). For notational convenience, we shall denote \( \mathbb{I}^\times_{\mathbb{F}_q} \) by \( \mathbb{I}_q \). We note that \( \det_{\mu_1} = \mathbb{I}_{\text{GL}_2(\mathbb{F}_q)} \). Now onwards, we shall use \( \rho_{\mu} \) to denote a complement of \( \det_{\mu} \) in \( \rho_{\mu,\mu} \).

Collecting all this information together, we obtain \( 2(q-1) + \frac{(q-1)(q-2)}{2} \) inequivalent irreducible representations of \( \text{GL}_2(\mathbb{F}_q) \). We know that the total number of inequivalent irreducible representations of a finite group is equal to the number of its conjugacy classes. Therefore, at this point it is good to compare the number of irreducible representations constructed above with the number of conjugacy classes of \( \text{GL}_2(\mathbb{F}_q) \) so that we know exactly how many more irreducible representations exist for the group \( \text{GL}_2(\mathbb{F}_q) \). This we do in the Table 3.
Conjugacy class type | Representative | Number of classes
---|---|---
central semisimple | \((x \ 0)\ (0 \ x)_{x \in \mathbb{F}_q^*}\) | \(q - 1\)
unitary | \((x \ 1)\ (0 \ x)_{x \in \mathbb{F}_q^*}\) | \(q - 1\)
on central semisimple | \((x \ 0)\ (0 \ y)_{x,y \in \mathbb{F}_q^* \ x \neq y}\) | \(\frac{(q-1)(q-2)}{2}\)ananisotropic | \((\alpha \ 0)\ (0 \ \bar{\alpha})_{\alpha \in \mathbb{F}_{q^2} \ \setminus \mathbb{F}_q}\) | \(\frac{q^2-q}{2}\)

Table 3. Conjugacy class types of \(\text{GL}_2(\mathbb{F}_q)\) along with their representatives and the number of each type.

This table along with the above discussion on construction of principal series irreducible representations of \(\text{GL}_2(\mathbb{F}_q)\) implies that, we still need to construct \((q^2 - q)/2\) irreducible representations of \(\text{GL}_2(\mathbb{F}_q)\). This we obtain in the next section.

**A.2. Cuspidal representations of \(\text{GL}_2(\mathbb{F}_q)\).** An irreducible representation \(\rho\) of \(G\) is called *cuspidal* if it is not a principal series representation. These representations are slightly more complicated to define as compared to those of the principal series. Here we outline their construction just enough to explain the entries of the character table of \(\text{GL}_2(\mathbb{F}_q)\) and urge the interested reader to look at [12] for more details.

Let \(\mathbb{F}_{q^2}\) be a degree two extension field of \(\mathbb{F}_q\). Then the map \(\sigma : x \mapsto x^q\) is a field automorphism of \(\mathbb{F}_{q^2}\) of order two with the property that \(\sigma(x) = x\) implies \(x \in \mathbb{F}_q\). Then the Norm map \(N : \mathbb{F}_{q^2}^\times \rightarrow \mathbb{F}_q^\times\) defined by \(x \mapsto x\sigma(x)\) is easily seen to be a surjective group homomorphism. Next, for every \(\nu \in \hat{\mathbb{F}_{q^2}}\), we define \(\sigma(\nu) \in \hat{\mathbb{F}_{q^2}}\) by \(\sigma(\nu)(x) = \nu(\sigma(x))\).

A one-dimensional representation \(\nu\) of \(\mathbb{F}_{q^2}^\times\) is called *non-decomposable* if \(\nu \neq \sigma(\nu)\). It turns out that cuspidal representations are parametrized by the set of non-decomposable characters of \(\mathbb{F}_{q^2}^\times\). More specifically, the following result is true.

**Theorem A.2.** There exists an irreducible representation \(\rho_\nu\) of \(\text{GL}_2(\mathbb{F}_q)\) of dimension \((q-1)\) for each non-decomposable character \(\nu\) of \(\mathbb{F}_{q^2}^\times\). Furthermore \(\rho_\nu \cong \rho_{\nu'}\) if and only if \(\nu' \in \{\nu, \sigma(\nu)\}\).

It is easy to see that the number of non-decomposable characters of \(\mathbb{F}_{q^2}^\times\) is \(q^2 - q\). Further by Theorem [A.2] for non-decomposable characters \(\nu\) of \(\mathbb{F}_{q^2}^\times\), there exists exactly one non-decomposable character \(\nu'\) of \(\mathbb{F}_{q^2}^\times\) such that \(\nu \neq \nu'\) and \(\rho_\nu \cong \rho_{\nu'}\). So we obtain exactly \((q^2 - q)/2\) inequivalent irreducible representations of \(\text{GL}_2(\mathbb{F}_q)\) this way. This
implies that the set of representations $\rho_\nu$ together with principal series irreducible representations form a complete set of irreducible representations of $GL_2(\mathbb{F}_q)$. It is possible to describe all these cuspidal representations precisely. We refer the reader to [12, Section 13] for more details.

A.3. Character table of $GL_2(\mathbb{F}_q)$. Now we are in a position to describe the character table of $GL_2(\mathbb{F}_q)$. By definition if $\rho : G \to GL(V)$ is a finite dimensional representation of $G$, the character of $\rho$, denoted $\chi_\rho$, is a complex valued function defined by $\chi_\rho(g) = \text{Tr}(\rho(g))$. It is well-known that the character of a representation is an invariant of a representation determined up to equivalence of representation. Further, two irreducible representations of a finite group are equivalent if and only if their characters are equal. Therefore, the character table encodes important information about the irreducible representations of a group. Note that $\chi_\rho(s) = \chi_\rho(t)$, whenever $s$ and $t$ are conjugate. So we shall describe character values only on the conjugacy class representatives of $GL_2(\mathbb{F}_q)$.

The character table is given in Table 4.

| Character $\chi$ | $\chi(x)^2$ | $\chi(x)^2$ | $\chi(x)\chi(y)$ | $\chi(\alpha\bar{\alpha})$ |
|-----------------|-------------|-------------|-------------------|--------------------------|
| $\det_\rho$     | $\chi(x)^2$| $\chi(x)^2$| $\chi(x)\chi(y)$| $\chi(\alpha\bar{\alpha})$|
| $\rho_{\lambda_1,\lambda_2}$ | $(q+1)\lambda_1(x)\lambda_2(x)$ | $\lambda_1(x)\lambda_2(x)$ | $\lambda_1(x)\lambda_2(y) + \lambda_1(y)\lambda_2(x)$ | 0 |
| $\rho_\nu$      | $(q-1)\nu(x)$ | $\nu(x)$ | 0 | $-\nu(\alpha) - \nu(\bar{\alpha})$ |

Table 4. The character table of $GL_2(\mathbb{F}_q)$.

The conjugacy classes of $GL_2(\mathbb{F}_q)$ are described in Table 3. The first three rows of the character table in Table 4 correspond to the principal series irreducible representations and can be obtained by using the character formula for induced representations. The last row corresponds to the cuspidal character and uses the explicit description of cuspidal irreducible representations of $GL_2(\mathbb{F}_q)$ as given in [12, Section 13].

References

[1] C. Asci, Asymptotic behavior of an affine random recursion in $\mathbb{Z}_p^k$, defined by a matrix with an eigenvalue of size 1, Statist. Probab. Lett., 79 (2009), pp. 1421–1428.
[2] , Generating uniform random vectors in $\mathbb{Z}_p^k$: the general case, J. Theoret. Probab., 22 (2009), pp. 791–809.
[3] A. Ayyer and P. Singla, Random motion on finite rings, I: noncommutative rings, arXiv preprint arXiv:1605.05089, (2016).
[4] A. Ayyer and B. Steinberg, Random walks on rings and modules, arXiv preprint arXiv:1708.04223, (2017).
[5] K. S. Brown, Semigroups, rings, and Markov chains, J. Theoret. Probab., 13 (2000), pp. 871–938.
[6] F. R. K. Chung, P. Diaconis, and R. L. Graham, Random walks arising in random number generation, Ann. Probab., 15 (1987), pp. 1148–1165.
[7] P. Diaconis, Group representations in probability and statistics, Lecture Notes-Monograph Series, 11 (1988), pp. i–192.
[8] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions, Z. Wahrsch. Verw. Gebiete, 57 (1981), pp. 159–179.
[9] J. Ding and A. Zhou, Eigenvalues of rank-one updated matrices with some applications, Appl. Math. Lett., 20 (2007), pp. 1223–1226.
[10] M. Hildebrand, Random processes of the form \(X_{n+1} = a_nX_n + b_n \pmod{p}\), Ann. Probab., 21 (1993), pp. 710–720.
[11] M. Hildebrand and J. McCollum, Generating random vectors in \((\mathbb{Z}/p\mathbb{Z})^d\) via an affine random process, J. Theoret. Probab., 21 (2008), pp. 802–811.
[12] I. Piatetski-Shapiro, Complex representations of GL(2, \(K\)) for finite fields \(K\), vol. 16 of Contemporary Mathematics, American Mathematical Society, Providence, R.I., 1983.
[13] J. Rhodes and A. Schilling, Unified theory for finite markov chains, arXiv preprint arXiv:1711.10689, (2017).
[14] B. Steinberg, In modules over finite rings \(Rv = Rw \iff R^xv = R^xw\). MathOverflow.
URL:https://mathoverflow.net/q/211739 (version: 2017-06-14).

AA: Department of Mathematics, Indian Institute of Science, Bangalore 560012, India.
E-mail address: arvind@iisc.ac.in

PS: Department of Mathematics, Indian Institute of Science, Bangalore 560012, India.
E-mail address: pooja@iisc.ac.in