ALGEBRAIC COMBINATORICS

Arvind Ayyer & Benjamin Steinberg

Random walks on rings and modules

Random walks on rings and modules

Arvind Ayyer & Benjamin Steinberg

ABSTRACT We consider two natural models of random walks on a module V over a finite commutative ring R driven simultaneously by addition of random elements in V, and multiplication by random elements in R. In the coin-toss walk, either one of the two operations is performed depending on the flip of a coin. In the affine walk, random elements $a \in R, b \in V$ are sampled independently, and the current state x is taken to $ax + b$. For both models, we obtain the complete spectrum of the transition matrix from the representation theory of the monoid of all affine maps on V under a suitable hypothesis on the measure on V (the measure on R can be arbitrary).

1. INTRODUCTION

Random walks driven simultaneously by addition and multiplication of the form $X_{n+1} = a_n X_n + b_n$, where a_n, b_n are independent, have been considered in the past. Such chains seem to have been first studied by Chung, Diaconis and Graham [22] on the field $\mathbb{Z}/p\mathbb{Z}$, where p is a prime. The motivation for their study came from the quest for efficient generation of quasirandom numbers, and those authors studied the mixing times of these chains for special choices of the distributions of a_n and b_n. For different choices of these distributions, Hildebrand [29, 30, 31] has also calculated the mixing times. Asci and Hildebrand–McCollum generalized some of these results to the vector space $(\mathbb{Z}/p\mathbb{Z})^d$ [2, 4, 3, 32] with the restriction that a_n is a deterministic matrix. In a slightly different direction, questions of convergence of affine random walks with real vectors are considered in [5].

Another class of random walks driven by both these operations has the flavor

$$(1) \qquad X_{n+1} = \begin{cases} X_n + b_n & \text{with probability } \alpha, \\ a_n X_n & \text{with probability } 1 - \alpha, \end{cases}$$

where again a_n and b_n are chosen independently from some distribution. Bate and Connor [13] have determined the mixing times of such chains on $\mathbb{Z}/m\mathbb{Z}$ with m odd and the probability $1 - \alpha$ decreasing to zero as m increases. Ayyer and Singla [11] have considered such chains on a finite commutative ring R where the distribution for

b_n is uniform on R and that of a_n is arbitrary. They have determined the stationary distribution, the spectrum of the transition matrix and the mixing time for finite chain rings.

We consider here the more abstract setting of random walks on finite left R-modules V over finite commutative rings R. Our methods will work both for the chains of the form $X_{n+1} = a_n X_n + b_n$, which we call the affine random walk, as well as those of the chain described in (1), which we call a coin-toss walk. In both cases, a_n and b_n are independent elements of R and V respectively. A word about notation: we shall use the phrase 'random walk' to talk about such chains even though these chains are not reversible. Technically, random walks refer to reversible Markov chains, but this terminology has been established by various authors working on random walks on monoids (cf. [10, 16, 18, 19, 20, 24, 37, 38, 42, 43, 44]) and in the context of random affine mappings [13, 22] and so we shall continue to use it. In this work, we focus on the spectral properties of these walks. We plan to take up the study of probabilistic properties of our walks, such as the stationary distribution and the mixing time, in future. In particular, part of the motivation for our work is a systematic study of irreversible Markov chains. The intuition is that irreversible chains have faster mixing than reversible ones [21, 25, 33, 34].

In this paper the term 'ring' means unital ring. Let R be a finite commutative ring and V a finite left R-module. For both walks, we need probability distributions P on V and Q on R. As we shall see below, Q can be arbitrary, but P will have to satisfy a condition. The state space for both random walks will be the module V.

Coin-toss walk. At each step of the walk, we flip a coin which comes up heads with probability α and tails with probability $1 - \alpha$. If the result is heads, we move from $x \in V$ to $x + b$ with probability $P(b)$ and if the result is tails, we move from x to ax with probability $Q(a)$.

Affine walk. At each step of the walk, we independently choose $a \in R$ with probability $Q(a)$ and $b \in V$ with probability $P(b)$ and move to $ax + b$. In other words, one step consists of first multiplying by an element of R chosen randomly according to Q and then adding an element of V chosen according to P.

Both of these Markov chains can be viewed as random walks for the *affine monoid* $\mathrm{Aff}(V)$ of V where $\mathrm{Aff}(V)$ is the monoid of all mappings on V of the form $x \mapsto ax + b$ with $a \in R$ and $b \in V$ with composition as the binary operation. So the product of $ax + b$ and $cx + d$ is $acx + ad + b$. Note that $\mathrm{Aff}(V)$ is the semidirect product of the multiplicative monoid $M(R)$ of R with the additive group V, that is, $\mathrm{Aff}(V) = V \rtimes M(R)$, where $M(R)$ acts on V via scalar multiplication. We can view P as a probability on $\mathrm{Aff}(V)$ supported on the translations $x \mapsto x + b$ and Q as a probability on $\mathrm{Aff}(V)$ supported on the dilations $x \mapsto ax$. The first model is then the random walk of $\mathrm{Aff}(V)$ on V driven by the probability $\alpha P + (1 - \alpha)Q$ and the second model is the random walk of $\mathrm{Aff}(V)$ on V driven by the probability PQ (where the product is convolution of measures).

To state our results, we need some definitions and notation. Recall that the set of invertible elements in a ring R forms a group, known as the *group of units*. Denote by $U(R)$ the group of units of R. We make the convention that $R = \{0\}$ is a unital ring and that $U(R) = \{0\}$ is the trivial group. Note that the only module over the zero ring is the zero module. Two elements $r_1, r_2 \in R$ are *associates* if $r_1 = ur_2$ with $u \in U(R)$. It therefore seems natural to generalize this terminology to the module V and so we say that $v_1, v_2 \in V$ are *associates* if $v_1 = uv_2$ for some $u \in U(R)$. We shall in both models impose the additional assumption that associates are equally

probable under P, that is, P is constant on associates. For example, this trivially holds for the uniform distribution. One can think of $V/U(R)$ as 'projective space' and then we are asking that P be a pullback of a measure on projective space. We can also view $V/U(R)$ as the space of cyclic submodules of V, since, for a finite module V, $v_1, v_2 \in V$ are associates if and only if $Rv_1 = Rv_2$, that is, if and only if v_1, v_2 generate the same cyclic submodule. Although this fact can be deduced from [12, Lemma 6.4], we provide a proof of this for the reader's convenience that does not require as much background.

PROPOSITION 1.1. *Let V be a finite module over a finite ring R. Then, for $v, w \in V$, one has $Rv = Rw$ if and only if $U(R)v = U(R)w$ where $U(R)$ is the group of units of R.*

We give a proof of Proposition 1.1 that relies only on the Krull–Schmidt theorem, following the second author's MathOverflow answer [41].

Proof of Proposition 1.1. Clearly, if $U(R)v = U(R)w$, then $Rv = Rw$. Turning to the converse, let $r, s \in R$ with $rv = w$ and $sw = v$. Since R is finite, there exists $n > 0$ such that $f = (rs)^n$ and $e = (sr)^n$ are idempotent ($n = |R|!$ will do). Note that $ev = v$ and $fw = w$. Let $r' = fre$ and $s' = esf$. Notice that $r'v = w$. Moreover, $s'r' = esfre = es(rs)^n re = esr(sr)^n e = (sr)^{3n+1} = (sr)^{n+1}$ and so $Rs'r' = Re$. Therefore, as $s' \in Rf$, right multiplication by r' gives a surjective R-module homomorphism $Rf \to Re$. Similarly right multiplication by s' gives a surjective R-module homomorphism $Re \to Rf$. By finiteness of R we conclude that both these homomorphisms are isomorphisms. It follows from the Krull–Schmidt theorem [14, Theorem 1.4.6] and the isomorphisms $Re \cong Rf$ and $Re \oplus R(1 - e) \cong R \cong Rf \oplus R(1 - f)$ that $R(1 - f) \cong R(1 - e)$. Such an isomorphism $R(1 - f) \to R(1 - e)$ is given via right multiplication by an element $x \in (1 - f)R(1 - e)$.

Consider $u = r' + x$. Then u is a unit since right multiplication by u gives an isomorphism from $R = Rf \oplus R(1-f)$ to $R = Re \oplus R(1-e)$ (as it is the direct sum of the two isomorphisms $Rf \to Re$ and $R(1 - f) \to R(1-e)$) and in a finite ring an element with a one-sided inverse is invertible. Also $uv = (r'+x)v = (r'+x)ev = r'ev = r'v = w$ because $x \in (1 - f)R(1 - e)$ implies $xe = 0$. Thus $w \in U(R)v$. This completes the proof. $\square$

Notice that Proposition 1.1 implies that the natural map $U(R) \to U(R/I)$ is surjective for any ideal I as the generators of the cyclic module R/I are the units of R/I.

Denote by $\widehat{A}$ the group of characters of an abelian group A, i.e. $\widehat{A} = \mathrm{Hom}(A, U(\mathbb{C}))$. We shall denote by $\mathbf{1}_A$ the *trivial character* of A mapping all of A to 1. More generally, $\mathbf{1}_G$ will denote the *trivial representation* of any (not necessarily abelian) group G.

We write $\widehat{V}$ for the character group of the additive group $(V, +)$ and $\widehat{U(R)}$ for the group of characters of the multiplicative group $U(R)$. Since the correspondence $A \mapsto \widehat{A}$ is contravariantly functorial and R is commutative, the action of R on V by multiplication induces an action of R on $\widehat{V}$ by endomorphisms. More precisely, if $\chi \in \widehat{V}$ and $r \in R$, then $r\chi \colon V \to U(\mathbb{C})$ is given by $(r\chi)(v) = \chi(rv)$ for $v \in V$. In fact, this action turns $\widehat{V}$ into a (finite) R-module since $(r + r')\chi(v) = \chi((r + r')v) = \chi(rv + r'v) = \chi(rv)\chi(r'v) = r\chi(v) \cdot r'\chi(v)$. Note that the abelian group structure of the module $\widehat{V}$ is being written multiplicatively because the operation is pointwise multiplication. We call $\widehat{V}$ the *dual module* of V. Of course, $|\widehat{V}| = V$ and $\widehat{\widehat{V}}$ is naturally isomorphic to V. See [45] for more on the Pontryagin dual of a finite module.

Finally, recall that the *transition matrix* of a Markov chain on a finite state space $\Omega = \{\omega_1, \ldots, \omega_n\}$ (in some ordering) is the $n \times n$ matrix whose (i, j)-entry is given by the one-step probability of making a transition from ω_i to ω_j. Since the rows of the transition matrix sum to 1, it is said to be *row-stochastic*. The next proposition gives sufficient conditions for the walks we are considering to be irreducible and aperiodic. They are by no means necessary.

PROPOSITION 1.2. *Let P be a probability distribution on V and Q a probability distribution on R.*

  (1) *In the coin-toss walk with heads probability $0 < \alpha < 1$, if the support of P generates the additive group of V, the walk is irreducible. If, in addition, the monoid generated by the support of Q contains 0, then the coin-toss walk is aperiodic.*
  (2) *If the support of P generates the additive group of V and the support of Q contains 1, then the affine walk is irreducible. If, moreover, the submonoid generated by the support of Q contains 0, then the walk is aperiodic.*

Proof. For the first item, one can get from v_1 to v_2 with non-zero probability because the translation $x \mapsto x + v_2 - v_1$ is in the support of some convolution power of $\lambda = \alpha P + (1-\alpha)Q$ by our assumption on P. If, in addition, 0 is in the submonoid generated by the support of Q, then some convolution power of λ contains a constant map in its support and hence, by irreducibility, there is a convolution power of λ that contains all the constant maps in its support, cf. [10, Proposition 2.5]. The corresponding power of the transition matrix will be strictly positive. The argument for the second item is nearly identical, the assumption that 1 is in the support of Q being required to guarantee we can get any translation in the support of some convolution power of PQ. $\square$

Since all the entries in the transition matrix are non-negative and at most 1, all eigenvalues will have absolute value bounded above by 1.

We can now state the main result of this article.

THEOREM 1.3. *Let R be a finite commutative ring, V a finite R-module, P a probability on V that is constant on associates and Q a probability on R. Then the eigenvalues for the transition matrices of both the coin-toss walk and the affine walk on V are indexed by pairs (W, ρ) where:*

  (1) *$W = R\chi$ is a cyclic R-submodule of $\widehat{V}$;*
  (2) *and $\rho \in U(\widehat{R/\operatorname{ann}}(W))$.*

The corresponding eigenvalue for the coin-toss walk is $\alpha \widehat{P}(\chi) + (1-\alpha)\widehat{Q}(\rho)$ and for the affine walk is $\widehat{P}(\chi)\widehat{Q}(\rho)$ where

$$\widehat{P}(\chi) = \sum_{b \in V} P(b)\chi(b)$$

$$\widehat{Q}(\rho) = \sum_{a \in U(R) + \operatorname{ann}(W)} Q(a)\rho(a + \operatorname{ann}(W)).$$

In both cases, the eigenvalue occurs with multiplicity one.

Note that in the above theorem statement, the value $P(\chi)$ depends only on the cyclic submodule generated by χ and not on χ itself. It is an immediate corollary that, for generic choices of the parameters, the transition matrix is diagonalizable.

The proof of Theorem 1.3 is based on a careful analysis of the representation theory of the affine monoid $\operatorname{Aff}(V)$. The use of monoid representation theory (outside of groups) to analyze Markov chains began with the work of Bidigare, Hanlon and

Rockmore [15], followed by work of Brown and Diaconis [18, 19, 20] and then others [6, 7, 8, 9, 10, 16, 17, 23, 38, 42, 43, 44]. An introduction to these methods can be found in [44, Chapter 14]. All the papers cited above exploit the feature that the monoids in question only have one-dimensional irreducible representations over the field of complex numbers (or, equivalently, are faithfully representable by upper triangular matrices over the complex numbers [1, 44]). One novel element in this work is that the monoid in question, the affine monoid, has irreducible representations of higher dimensions. This is the first article, to the best of our knowledge, to use the representation theory of a monoid that is neither a group, nor faithfully representable by upper triangular matrices, to analyze Markov chains.

We give an example to demonstrate Theorem 1.3.

EXAMPLE 1.4. Let R be the field $\mathbb{Z}/2\mathbb{Z}$ and V the vector space R^2. Order the elements of V as $((0,0),(0,1),(1,0),(1,1))$. The probability distribution on R is $Q = (q_0, q_1)$ and that on V is $P = (p_{i,j})_{0 \leqslant i,j \leqslant 1}$. Being constant on associates forces no condition on P for this simple example. So the transition matrix of the affine walk is

$$\begin{pmatrix} p_{0,0} & p_{0,1} & p_{1,0} & p_{1,1} \\ q_0 p_{0,0} + q_1 p_{0,1} & q_1 p_{0,0} + q_0 p_{0,1} & q_0 p_{1,0} + q_1 p_{1,1} & q_1 p_{1,0} + q_0 p_{1,1} \\ q_0 p_{0,0} + q_1 p_{1,0} & q_0 p_{0,1} + q_1 p_{1,1} & q_1 p_{0,0} + q_0 p_{1,0} & q_1 p_{0,1} + q_0 p_{1,1} \\ q_0 p_{0,0} + q_1 p_{1,1} & q_0 p_{0,1} + q_1 p_{1,0} & q_1 p_{0,1} + q_0 p_{1,0} & q_1 p_{0,0} + q_0 p_{1,1} \end{pmatrix},$$

and its eigenvalues are given by

$$(1-\alpha)q_1 \left(p_{0,0} + p_{0,1} - p_{1,0} - p_{1,1} \right), q_1 \left(p_{0,0} - p_{0,1} + p_{1,0} - p_{1,1} \right),$$
$$q_1 \left(p_{0,0} - p_{0,1} - p_{1,0} + p_{1,1} \right) \text{ and } 1.$$

The transition matrix of the coin-toss walk is

$$\begin{pmatrix} (1-\alpha) + \alpha p_{0,0} & \alpha p_{0,1} & \alpha p_{1,0} & \alpha p_{1,1} \\ (1-\alpha)q_0 + \alpha p_{0,1} & (1-\alpha)q_1 + \alpha p_{0,0} & \alpha p_{1,1} & \alpha p_{1,0} \\ (1-\alpha)q_0 + \alpha p_{1,0} & \alpha p_{1,1} & (1-\alpha)q_1 + \alpha p_{0,0} & \alpha p_{0,1} \\ (1-\alpha)q_0 + \alpha p_{1,1} & \alpha p_{1,0} & \alpha p_{0,1} & (1-\alpha)q_1 + \alpha p_{0,0} \end{pmatrix},$$

and its eigenvalues are 1,

$$\alpha \left(p_{0,0} + p_{0,1} - p_{1,0} - p_{1,1} \right) + (1-\alpha)q_1,$$
$$\alpha \left(p_{0,0} - p_{0,1} + p_{1,0} - p_{1,1} \right) + (1-\alpha)q_1,$$
$$\text{and } \alpha \left(p_{0,0} - p_{0,1} - p_{1,0} + p_{1,1} \right) + (1-\alpha)q_1.$$

Theorem 1.3 has a nice reformulation for Frobenius rings when V is the ring R itself. This includes rings of the form $\mathbb{Z}/n\mathbb{Z}$. Recall that an Artinian ring R (with Jacobson radical $J(R)$) is *Frobenius* if $R/J(R)$ is isomorphic to the socle of R as a left module and as a right module. (Recall that the socle of a module is its largest semisimple submodule.) It is shown in [45] that a finite ring R is Frobenius if and only if $R \cong \widehat{R}$ as a left R-module. A character $\chi \in \widehat{R}$ such that $r \mapsto r\chi$ is an R-module isomorphism is called a *generating character* [45]. For example, $R = \mathbb{Z}/n\mathbb{Z}$ is Frobenius and a generating character is given by $\chi(m) = e^{2\pi i m/n}$ for $m \in \mathbb{Z}/n\mathbb{Z}$.

THEOREM 1.5. *Let R be a finite commutative Frobenius ring, P a probability on R that is constant on associates and Q a probability on R. Let $\chi \in \widehat{R}$ be a generating character. Then the eigenvalues for the transition matrices of both the coin-toss walk and the affine walk on R are indexed by pairs (W, ρ) where:*

(1) *$W = Rb$ is a principal ideal;*
(2) *and $\rho \in U(\widehat{R/\operatorname{ann}}(b))$.*

The corresponding eigenvalue for the coin-toss walk is

$$\alpha \cdot \sum_{r \in R} P(r)\chi(br) + (1 - \alpha) \cdot \sum_{r \in U(R) + \mathrm{ann}(b)} Q(r)\rho(r + \mathrm{ann}(b))$$

and for the affine walk is

$$\left(\sum_{r \in R} P(r)\chi(br) \right) \cdot \left(\sum_{r \in U(R) + \mathrm{ann}(b)} Q(r)\rho(r + \mathrm{ann}(b)) \right).$$

In both cases, the eigenvalue occurs with multiplicity one.

EXAMPLE 1.6. Let R be the ring $\mathbb{Z}/4\mathbb{Z}$, which we order as $(0, 1, 2, 3)$, and let $V = R$. Since 1 and 3 are associates, we set $p_3 = p_1$. The transition graphs of the coin-toss walk and the affine walk are shown in Figure 1. The eigenvalues of their respective transition matrices are

$$\alpha \left(p_0 - p_2 \right) + (1 - \alpha) \left(q_1 - q_3 \right), \alpha \left(p_0 - p_2 \right) + (1 - \alpha) \left(q_1 + q_3 \right),$$
$$\alpha \left(p_0 - 2p_1 + p_2 \right) + (1 - \alpha) \left(q_1 + q_3 \right) \text{ and } 1,$$

and

$$\left(p_0 - p_2 \right) \left(q_1 - q_3 \right), \left(p_0 - p_2 \right) \left(q_1 + q_3 \right), \left(p_0 - 2p_1 + p_2 \right) \left(q_1 + q_3 \right) \text{ and } 1.$$
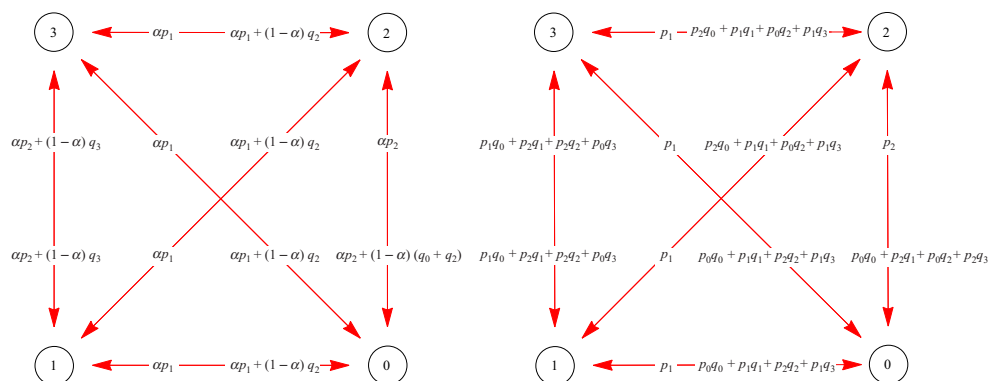
FIGURE 1. The transition graphs of the coin-toss and affine walk on $\mathbb{Z}/4\mathbb{Z}$.

The plan of the rest of the paper is as follows. In Section 2, we review first the representation theory of groups followed by that of monoids, emphasizing the parts that are relevant to this study. In Section 3, we study the structure of the affine monoid and use the results in the previous section to understand the representation theory of this monoid. Finally, we prove Theorem 1.3 and examine various special cases of this general result in Section 4.

2. PRELIMINARIES ON GROUP AND MONOID REPRESENTATION THEORY

The book [44] serves as a basic reference for those aspects of the representation theory of monoids that we shall need. If M is a finite monoid, then $\mathbb{C}M$ denotes the *monoid algebra* of M. It consists of all formal linear combinations of elements of M with the obvious addition operation and with product

$$\sum_{m \in M} c_m m \cdot \sum_{m \in M} d_m m = \sum_{m,n \in M} c_m d_n mn.$$

Finite dimensional $\mathbb{C}M$-modules (which are the only kind we consider) correspond to finite dimensional matrix representations of M over $\mathbb{C}$. A probability P on M can be identified with the element $\sum_{m \in M} P(m)m \in \mathbb{C}M$ and the product of two probabilities in $\mathbb{C}M$ corresponds to their convolution.

If V is a $\mathbb{C}M$-module, the *character* of V is the mapping $\chi_V \colon M \to \mathbb{C}$ given by sending $m \in M$ to the trace of the operator on V given by $v \mapsto mv$. It is not in general true that a module is determined by its character but semisimple modules are, cf. [36]. The character of a simple module is called an *irreducible character*. The irreducible characters of a monoid form a linearly independent set of mappings [44, Theorem 7.7].

A *composition series* for a $\mathbb{C}M$-module V is a series of submodules

$$(2) \qquad\qquad V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_n = 0$$

such that the *composition factor* V_i/V_{i+1} is simple for $i = 0, \ldots, n-1$. The Jordan-Hölder theorem [14, Theorem 1.1.4] guarantees that the length of any two composition series for V is the same and, moreover, that if S is a simple $\mathbb{C}M$-module, then the number $[V : S]$ of composition factors isomorphic to S is the same for any two composition series. The isomorphism class of a module V shall be written $[V]$.

2.1. GROUP REPRESENTATION THEORY. The reader is referred to [39] for the basics of group representation theory. If G is a finite group, then $\mathbb{C}G$ is called the *group algebra* of G. It is a semisimple algebra and hence every finite dimensional $\mathbb{C}G$-module V is a direct sum of simple $\mathbb{C}G$-modules, which are in fact its composition factors (with multiplicity). If V is a $\mathbb{C}G$-module and S is a simple $\mathbb{C}G$-module, then

$$(3) \qquad\qquad \dim \mathrm{Hom}_{\mathbb{C}G}(S, V) = \dim \mathrm{Hom}_{\mathbb{C}G}(V, S) = [V : S].$$

The irreducible characters of a finite group G form an orthonormal set for the inner product on $\mathbb{C}^G$ given by

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}.$$

This is called the *first orthogonality relations*. If θ is the character of a $\mathbb{C}G$-module V and χ is the character of a simple $\mathbb{C}G$-module S, then $\langle \theta, \chi \rangle = [V : S]$.

An important consequence of Schur's lemma is that if a belongs to the center of $\mathbb{C}G$ and V is a simple $\mathbb{C}G$-module, then a acts on V via multiplication by a scalar.

If $H \leqslant G$ is a subgroup and V is a $\mathbb{C}H$-module, then $\mathrm{Ind}_H^G V = \mathbb{C}G \otimes_{\mathbb{C}H} V$ is a $\mathbb{C}G$-module called an *induced module*. Note that

$$\dim \mathrm{Ind}_H^G V = [G : H] \cdot \dim V.$$

Also, $\mathrm{Ind}_H^G \mathbf{1}_H$ is isomorphic to the permutation module $\mathbb{C}[G/H]$. If W is a $\mathbb{C}G$-module, then $\mathrm{Res}_H^G W$ is the $\mathbb{C}H$-module obtained by restricting scalars.

THEOREM 2.1 (Frobenius reciprocity). *Let $H \leqslant G$ be a subgroup and let V be a $\mathbb{C}H$-module and W a $\mathbb{C}G$-module. Then the isomorphism*

$$\mathrm{Hom}_{\mathbb{C}G}(\mathrm{Ind}_H^G V, W) \cong \mathrm{Hom}_{\mathbb{C}H}(V, \mathrm{Res}_H^G W)$$

holds.

The Mackey decomposition theorem describes how an induced representation from one subgroup restricts to another. Let $K \leqslant G$ be a subgroup and let V be a $\mathbb{C}K$-module. If $g \in G$, then V^g is the $\mathbb{C}[gKg^{-1}]$-module with underlying vector space V and action given by $xv = g^{-1}xgv$ for $x \in gKg^{-1}$. With this notation, the Mackey decomposition theorem says the following.

THEOREM 2.2 (Mackey decomposition). *Let G be a group and let H, K be subgroups of G. Let T be a complete set of representatives of the double cosets $H \backslash G / K$. If V is a $\mathbb{C}K$-module, then the decomposition*

$$\operatorname{Res}_H^G \operatorname{Ind}_K^G V \cong \bigoplus_{t \in T} \operatorname{Ind}_{H \cap tKt^{-1}}^H \operatorname{Res}_{H \cap tKt^{-1}}^{tKt^{-1}} V^t$$

holds.

If $\varphi \colon G \to K$ is a group homomorphism and V is a $\mathbb{C}K$-module, then it is also a $\mathbb{C}G$-module, called the *inflation* of V along φ, via $gv = \varphi(g)v$ for $g \in G$ and $v \in V$.

PROPOSITION 2.3. *Let $\varphi \colon G \to K$ be a surjective homomorphism, $H \leqslant K$ and V a $\mathbb{C}H$-module. Putting $H' = \varphi^{-1}(H)$, the inflation of $\operatorname{Ind}_H^K V$ along φ is isomorphic to $\operatorname{Ind}_{H'}^G V$ (where V is a $\mathbb{C}H'$-module via inflation).*

Proof. It is easily verified that there is a surjective homomorphism of $\mathbb{C}G$-modules $\psi \colon \mathbb{C}G \otimes_{\mathbb{C}H'} V \to \mathbb{C}K \otimes_{\mathbb{C}H} V$ given by $g \otimes v \mapsto \varphi(g) \otimes v$ on basic tensors. Since $\dim \operatorname{Ind}_{H'}^G V = [G : H'] \cdot \dim V = [K : H] \cdot \dim V = \dim \operatorname{Ind}_H^K V$, we conclude that ψ is an isomorphism. $\qquad\square$

2.2. MONOID REPRESENTATION THEORY. Just as for rings, the set of invertible elements (known as units) in a monoid forms a group. The *group of units* (invertible elements) of a monoid M will be denoted $U(M)$ throughout. An *idempotent* of a monoid M is an element $e \in M$ such that $e^2 = e$. Denote by $E(M)$ the set of idempotents of M. If M is a monoid and $e \in E(M)$ is an idempotent, then eMe is a monoid with identity e. The group of units $U(eMe)$ of eMe is called the *maximal subgroup* of M at e.

We recall the definition of Green's relations [28] on a monoid M. We write $m \mathcal{J} n$ if $MmM = MnM$, $m \mathcal{R} n$ if $mM = nM$ and $m \mathcal{L} n$ if $Mm = Mn$. We write $m \leqslant_{\mathcal{J}} n$ if $MmM \subseteq MnM$. A $\mathcal{J}$-class is called *regular* if it contains an idempotent. The regular $\mathcal{J}$-classes of M form a poset via the ordering $J \leqslant J'$ if $MJM \subseteq MJ'M$. If e and f are $\mathcal{J}$-equivalent idempotents, then $eMe \cong fMf$ and hence $U(eMe) \cong U(fMf)$. See [44, Corollary 1.2].

Let us first recall some basic facts about the representation theory of monoids. If $e \in E(M)$ and V is a $\mathbb{C}M$-module, then eV is a $\mathbb{C}U(eMe)$-module. We say that e is an *apex* for the simple $\mathbb{C}M$-module S if $eS \neq 0$ and $mS = 0$ for all $m \in eMe \smallsetminus U(eMe)$. This is equivalent to $mS = 0$ for all m such that $e \notin MmM$. The fundamental theorem of Clifford–Munn–Ponizovskii theory says the following. See [27] or [44, Theorem 5.5] for details.

THEOREM 2.4. *Let M be a finite monoid and $e_1, \ldots, e_s$ form a complete set of idempotent representatives of the regular $\mathcal{J}$-classes of M. Then the isomorphism classes of simple $\mathbb{C}M$-modules are parameterized by pairs $(e_i, [V])$ with V a simple $\mathbb{C}U(e_iMe_i)$-module. The corresponding simple module $V^\sharp$ is characterized up to isomorphism by the properties that e_i is an apex for $V^\sharp$ and $e_iV^\sharp \cong V$ as a $\mathbb{C}U(e_iMe_i)$-module.*

McAlister [35] gave a general method to compute the composition factors of a module from its character by inverting the character table of the monoid. In practice, it can be quite unwieldy to implement this method. A simpler method was given by the second author in [43] in the case of a monoid whose idempotents form a submonoid. The reader is referred to [40] for the Möbius function of a poset.

THEOREM 2.5. *Let M be a finite monoid whose idempotents form a submonoid. Fix an idempotent e_J from each regular $\mathcal{J}$-class J. Let χ be an irreducible character of*

$U(e_J M e_J)$ *corresponding to the simple module S and let V be a finite dimensional $\mathbb{C}M$-module with character θ. Then*

$$[V : S^\sharp] = \frac{1}{|U(e_J M e_J)|} \sum_{g \in U(e_J M e_J)} \chi(g) \sum_{J' \leqslant J} \overline{\theta(e_{J'} g e_{J'})} \mu(J', J)$$

where J' runs over regular $\mathcal{J}$-classes and μ is the Möbius function of the poset of regular $\mathcal{J}$-classes of M.

2.3. MONOID RANDOM WALKS. Let M be a finite monoid acting on the left of a finite set Ω and let P be a probability on M. Then the *random walk* of M on Ω driven by P is the Markov chain with state space Ω and with transitions $x \mapsto mx$ with probability $P(m)$.

The vector space $\mathbb{C}\Omega$ is then a left $\mathbb{C}M$-module by extending the action of M on the basis Ω linearly. If we identify P with the element

$$\sum_{m \in M} P(m)m \in \mathbb{C}M,$$

then the transition matrix of the random walk is the transpose of the matrix of the operator P acting on the vector space $\mathbb{C}\Omega$ with respect to the basis Ω. See [44, Chapter 14] or [10, 18, 19] for details. Note that the tranpose arises here because we are using row stochastic matrices for the transition matrix but left actions for the random walk.

3. THE AFFINE MONOID

As before, fix a finite commutative ring R and a finite R-module V. We continue to use $\mathrm{Aff}(V)$ to denote the affine monoid of V. Observe that

$$U(\mathrm{Aff}(V)) = \{ax + b \mid a \in U(R), b \in V\}$$

and, in fact, $U(\mathrm{Aff}(V)) = V \rtimes U(R)$ is a semidirect product of abelian groups.

3.1. THE ALGEBRAIC STRUCTURE OF THE AFFINE MONOID. If $e \in E(R)$, then $1-e \in E(R)$ and the internal direct sum

$$R = Re \oplus R(1 - e)$$

is a direct product decomposition as rings (note that Rf is a unital ring with identity f for any $f \in E(R)$). All direct sum decompositions $R = R_1 \oplus R_2$ into a direct product of unital rings arise in this way (take e to be the identity of R_1). There is a corresponding direct sum decomposition $V = eV \oplus (1-e)V$ and note that eV is annihilated by $R(1-e)$ and $(1-e)V$ is annihilated by Re. Also, eV is an Re-module. Denote by

$$\varphi_e \colon R = Re \oplus R(1-e) \to Re$$

the projection. It is a surjective homomorphism of unital rings given by $\varphi_e(r) = re$. Notice that $re = 0$ if and only if $r(1-e) = r$ and so $Re \cong R/R(1-e)$. We also have a surjective homomorphism of R-modules $\pi_e \colon V \to eV$ given by $\pi_e(v) = ev$, which has kernel $(1-e)V$.

PROPOSITION 3.1. *Let $e \in E(R)$ and let $\varphi_e \colon R \to Re$ be the projection $\varphi_e(r) = re$.*

(1) *For $a \in R$, $\varphi_e(a) \in U(Re)$ if and only if $Ra \supseteq Re$.*
(2) *The restriction $\varphi_e \colon U(R) \to U(Re)$ is surjective.*

Proof. To prove the first item, let $Ra \supseteq Re$ and write $e = ya$. Then $e = yeae = ye\varphi_e(a)$ and so $\varphi_e(a) \in U(Re)$. Conversely, if $ae \in U(Re)$, then $e = uae$ with $u \in U(Re)$ and hence $e = uea \in Ra$. Thus $Ra \supseteq Re$.

For the second item, let $u \in U(Re)$ with inverse $v \in U(Re)$, and so $uv = e$. Let $u' = u + (1 - e)$ and $v' = v + (1 - e)$. Then since $ue = u$, $ve = v$ and $e(1 - e) = 0$, we see that $u'v' = uv + u(1 - e) + v(1 - e) + (1 - e) = uv + (1 - e) = e + 1 - e = 1$ and so $u' \in U(R)$. Moreover, $\varphi_e(u') = u'e = u$. This completes the proof. $\square$

We now begin to study the affine monoid. Let $\pi \colon \mathrm{Aff}(V) \to M(R)$ be the surjective homomorphism $\pi(ax + b) = a$. A monoid is called a *left regular band* if it satisfies the identity $xyx = xy$. Left regular bands have played an important role in applications of monoids to Markov chain theory. See [15, 18, 19, 20, 24].

PROPOSITION 3.2. *Let R be a commutative ring.*

(1) $E(\mathrm{Aff}(V)) = \{ex + b \mid e \in E(R), eb = 0\}$.
(2) $E(\mathrm{Aff}(V))$ *is a submonoid of* $\mathrm{Aff}(V)$ *and a left regular band.*
(3) *If* $ex + b, fx + c \in E(\mathrm{Aff}(V))$, *then* $ex + b \leqslant_{\mathcal{J}} fx + c$ *if and only if* $Re \subseteq Rf$. *In particular,* $ex + b \mathrel{\mathcal{J}} fx + c$ *if and only if* $e = f$.
(4) *If* $e \in E(R)$, *then* $E(Re) = \{f \in E(R) \mid Rf \subseteq Re\}$.

Proof. If $f(x) = ax + b$, then $f^2(x) = a^2x + ab + b$ and so $f(x) = f^2(x)$ if and only if $a^2 = a$ and $ab = 0$. This proves the first item.

For the second item, suppose that $e, f \in E(R)$ and $eb = 0 = fc$. Let $g(x) = ex + b$ and $h(x) = fx + c$. Then $gh(x) = efx + ec + b$, $ef \in E(R)$ and $ef(ec + b) = efc + feb = 0$. Thus $gh(x)$ is an idempotent by the first item and so the idempotents form a submonoid of $\mathrm{Aff}(R)$. Moreover, $ghg(x) = efex + efb + ec + b = efx + ec + b$ as $eb = 0$. Therefore, $ghg(x) = gh(x)$ and so $E(\mathrm{Aff}(V))$ is a left regular band.

Let us prove the third item. Let $g(x) = ex + b, h(x) = fx + c \in E(\mathrm{Aff}(V))$. If $g(x) \leqslant_{\mathcal{J}} h(x)$, then $e = \pi(g(x)) \leqslant_{\mathcal{J}} \pi(h(x)) = f$. But $M(R)$ is a commutative monoid and so $Re \subseteq Rf$. Conversely, if $Re \subseteq Rf$, then $ef = e$ and so $gh(x) = efx + ec + b = ex + efc + b = ex + b = g(x)$ because $fc = 0$. Thus $g(x) \leqslant_{\mathcal{J}} h(x)$. The final statement of the third item follows because $ex + b \mathrel{\mathcal{J}} fx + c$ if and only if $Re = Rf$. But if $Re = Rf$, then $e = ef = fe = f$.

The last item follows because an idempotent f belongs to Re if and only if $fe = f$ if and only if $Rf \subseteq Re$. $\square$

Proposition 3.2 implies that the poset of regular $\mathcal{J}$-classes of $\mathrm{Aff}(V)$ is isomorphic to the poset of idempotent generated principal ideals of R. The latter is, in fact, a lattice since $Re \cap Rf = Ref$ and $Re + Rf = R(e + f - ef)$ and one readily checks $e + f - ef$ is an idempotent. In fact, the lattice of idempotent-generated principal ideals of R is a boolean algebra where the complement of Re is $R(1 - e)$ and the atoms are the ideals generated by the primitive idempotents.

COROLLARY 3.3. *The poset of regular $\mathcal{J}$-classes of* $\mathrm{Aff}(V)$ *is isomorphic to the lattice of idempotent generated principal ideals of the ring R via the mapping taking the $\mathcal{J}$-class of $ex + b$ to Re.*

The elements of the form $g(x) = ex$ with $e \in E(R)$ form a commutative submonoid of $E(\mathrm{Aff}(V))$ and a transversal of the set of regular $\mathcal{J}$-classes. Moreover, $Re \subseteq Rf$ if and only if $e = ef = fe$.

PROPOSITION 3.4. *Let $e \in E(R)$ and let $g(x) = ex$ be the corresponding idempotent of $\mathrm{Aff}(V)$. Then $g(x)\,\mathrm{Aff}(V)g(x) = \mathrm{Aff}(eV)$, where eV is viewed as an Re-module in the natural way, and hence the maximal subgroup of $\mathrm{Aff}(V)$ at $g(x)$ is $U(\mathrm{Aff}(eV))$.*

Proof. If $h(x) = ax + b$, then $ghg(x) = eaex + eb = eax + eb$. It follows that $ax + b \in g(x) \operatorname{Aff}(V) g(x)$ if and only if $ea = ae = a$ and $eb = b$, that is, $g(x) \operatorname{Aff}(V) g(x) = \operatorname{Aff}(eV)$, establishing the proposition. $\qquad\square$

It will be useful that the projections $\varphi_e \colon R \to Re$ and $\pi_e \colon V \to eV$, for $e \in E(R)$, combine to yield a homomorphism $\operatorname{Aff}(V) \to \operatorname{Aff}(eV)$.

PROPOSITION 3.5. *Let* $e \in E(R)$. *Then there is a surjective homomorphism* $\Phi_e(\operatorname{Aff}(V)) \to \operatorname{Aff}(eV)$ *given by* $\Phi_e(ax + b) = \varphi_e(a)x + \pi_e(b) = aex + eb$. *Moreover, the restriction* $\Phi_e \colon U(\operatorname{Aff}(V)) \to U(\operatorname{Aff}(eV))$ *is surjective.*

Proof. Let $g(x) = ax + b$ and $h(x) = cx + d$. Then $gh(x) = acx + ad + b$ and so $\Phi_e(gh(x)) = acex + ead + eb$. On the other hand, $\Phi_e(g(x))\Phi_e(h(x))$ is the composition of $aex + eb$ and $cex + ed$, which is $aecex + aeed + eb = acex + ead + eb$. Also $\Phi_e(1x) = ex$, which is the identity of $\operatorname{Aff}(eV)$. Therefore, Φ_e is a homomorphism. It is surjective because if $a \in Re$ and $b \in eV$, then $ae = a$ and $eb = b$, whence $\Phi_e(ax + b) = ax + b$. The final statement follows immediately from Proposition 3.1. $\qquad\square$

Note that if $e \in E(R)$, then $e\widehat{V}$ is an R-submodule of $\widehat{V}$, and hence invariant under its group of units, $U(R)$. Also note that $e\widehat{V}$ is an Re-module. So the unit group $U(Re)$ acts on $e\widehat{V}$ by automorphisms. The stabilizer in $U(Re)$ of $\chi \in e\widehat{V}$ under this action shall be denoted $\operatorname{St}_{U(Re)}(\chi)$. Notice that $\operatorname{St}_{U(Re)}(\chi) = e + \operatorname{ann}(\chi)e$, where $\operatorname{ann}(\chi)$ is the ideal of elements of R that annihilate χ; indeed, $r\chi = \chi = e\chi$ if and only if $r - e \in \operatorname{ann}(\chi)e$, if and only if $r \in e + \operatorname{ann}(\chi)e$ for $r \in Re$. Our next proposition describes $e\widehat{V}$.

PROPOSITION 3.6. *Let* R *be a finite commutative ring,* V *a finite* R-module *and* $e \in E(R)$. *Then the following are equivalent for* $\chi \in \widehat{V}$.

(1) $\chi \in e\widehat{V}$;
(2) $\chi = \gamma \circ \pi_e$ *with* $\gamma \in \widehat{eV}$;
(3) $(1 - e)V \subseteq \ker \chi$.

Proof. If $\chi \in e\widehat{V}$ and $v \in (1 - e)V$, then

$$\chi(v) = (e\chi)(v) = \chi(ev) = \chi(e(1-e)v) = \chi(0) = 1$$

and so $(1-e)V \subseteq \ker \chi$. If $(1-e)V \subseteq \ker \chi$, then χ factors through π_e as $(1-e)V = \ker \pi_e$. If $\chi = \gamma \circ \pi_e$ with $\gamma \in \widehat{eV}$, then $(e\chi)(v) = \chi(ev) = \gamma(\pi_e(ev)) = \gamma(eev) = \gamma(ev) = \gamma(\pi_e(v)) = \chi(v)$ and so $e\chi = \chi$. Therefore, $\chi \in e\widehat{V}$. $\qquad\square$

It follows that we can identify $e\widehat{V}$ with $\widehat{eV}$ and that the action of $U(Re)$ on $e\widehat{V}$ by automorphisms can be identified with the action of $U(Re)$ on $\widehat{eV}$ by automorphisms. In particular, the orbits of $U(Re)$ on $e\widehat{V}$ and $U(R)$ on $e\widehat{V}$ are the same because $\varphi_e \colon U(R) \to U(Re)$ given by $r \mapsto re$ is onto by Proposition 3.1.

3.2. THE REPRESENTATION THEORY OF THE AFFINE MONOID. Using Theorem 2.4 we can completely describe the simple $\mathbb{C}\operatorname{Aff}(V)$-modules for a finite module V over a finite commutative ring R. We take for a complete set of idempotent representatives of the regular $\mathcal{J}$-classes of $\operatorname{Aff}(V)$ the mappings $g_e(x) = ex$ with $e \in E(R)$ (this is justified by Proposition 3.2). By Proposition 3.4 we can identify the maximal subgroup at $g_e(x)$ with $U(\operatorname{Aff}(eV))$. Let $\operatorname{Sing}(\operatorname{Aff}(eV)) = \operatorname{Aff}(eV) \smallsetminus U(\operatorname{Aff}(eV))$ be the ideal of singular affine mappings. Then $\mathbb{C}U(\operatorname{Aff}(eV)) \cong \mathbb{C}\operatorname{Aff}(eV)/\mathbb{C}\operatorname{Sing}(\operatorname{Aff}(eV))$ and hence any simple $\mathbb{C}U(\operatorname{Aff}(eV))$-module W can be viewed as a simple $\mathbb{C}\operatorname{Aff}(eV)$-module via

inflation. The surjective homomorphism $\Phi_e \colon \mathrm{Aff}(V) \to \mathrm{Aff}(eV)$ from Proposition 3.5 extends to a surjective homomorphism of $\mathbb{C}$-algebras

$$\Phi_e \colon \mathbb{C}\,\mathrm{Aff}(V) \to \mathbb{C}\,\mathrm{Aff}(eV)$$

and hence W becomes a simple $\mathbb{C}\,\mathrm{Aff}(V)$-module via inflation along Φ_e. Concretely, if $w \in W$ and $ax + b \in \mathrm{Aff}(V)$, then the action of $ax + b$ on w is given by

$$(4) \qquad\qquad (ax + b)w = \begin{cases} (aex + eb)w, & \text{if } Ra \supseteq Re \\ 0, & \text{else} \end{cases}$$

in light of Proposition 3.1. Clearly, $g_e(x)$ is an apex for this $\mathbb{C}\,\mathrm{Aff}(V)$-module structure on W and $g_e(x)W = W$ as a $\mathbb{C}U(\mathrm{Aff}(eV))$-module. Therefore, all the simple $\mathbb{C}\,\mathrm{Aff}(V)$-modules are obtained in this fashion by Theorem 2.4; that is, $W^\sharp = W$ as a vector space with the module structure given by (4).

It thus remains to describe the representation theory of $\mathbb{C}U(\mathrm{Aff}(M))$ for a finite module M over a finite commutative ring S. The case of interest for us will be rings of the form $S = Re$ and modules of the form $M = eV$ with $e \in E(R)$. This is a very special case of the representation theory of semidirect products of the form $A \rtimes G$ with A an abelian group and G an arbitrary group that can be found in standard texts on group representation theory (cf. [39]). Here we use the semidirect product decomposition $U(\mathrm{Aff}(M)) = M \rtimes U(S)$.

The group $U(S)$ acts on $\widehat{M}$ via $(s\chi)(v) = \chi(sv)$ for $s \in U(S)$ and $v \in M$. If $\chi \in \widehat{M}$, let $\mathrm{St}_{U(S)}(\chi)$ be the stabilizer of χ in $U(S)$. If $\rho \in \widehat{\mathrm{St}_{U(S)}(\chi)}$, then we can define a degree one character $\chi \otimes \rho \colon M \rtimes \mathrm{St}_{U(S)}(\chi) \to U(\mathbb{C})$ by $(\chi \otimes \rho)(ax + b) = \chi(b)\rho(a)$ for $a \in \mathrm{St}_{U(S)}(\chi)$ and $b \in M$.

THEOREM 3.7. *Let M be a finite S-module with S a finite commutative ring. Let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be the orbits of $U(S)$ on $\widehat{M}$ and fix $\chi_i \in \mathcal{O}_i$. Then a complete set of representatives of the isomorphism classes of simple $\mathbb{C}U(\mathrm{Aff}(M))$-modules is given by the modules*

$$W_{(\mathcal{O}_i, \rho)} = \mathrm{Ind}_{M \rtimes \mathrm{St}_{U(S)}(\chi_i)}^{U(\mathrm{Aff}(M))} \chi_i \otimes \rho$$

with $\rho \in \widehat{\mathrm{St}_{U(S)}(\chi_i)}$.

Proof. This is the specialization to $U(\mathrm{Aff}(M)) = M \rtimes U(S)$ of the general theory of irreducible representations of semidirect products $A \rtimes G$ with A abelian described in [39, Proposition 25]. $\qquad\square$

Let $f \in E(S)$. Then $U(\mathrm{Aff}(fM))$ acts transitively on fM by permutations via the natural action $g(v) = av + b$ for $g(x) = ax + b \in U(\mathrm{Aff}(fM))$ and $v \in fM$. Hence $U(\mathrm{Aff}(M))$ acts transitively on fM by permutations via inflation along the surjective homomorphism $\Phi_f \colon U(\mathrm{Aff}(M)) \to U(\mathrm{Aff}(fM))$ given by $\Phi_f(ax + b) = afx + fb$, cf. Proposition 3.5. Notice that $ax + b \in U(\mathrm{Aff}(M))$ stabilizes 0 under this action if and only if $fb = 0$, which occurs if and only if $b \in (1 - f)M$. Hence $\mathrm{St}_{U(\mathrm{Aff}(M))}(0) = (1 - f)M \rtimes U(S)$. Therefore, the corresponding permutation module $\mathbb{C}fM$ for $\mathbb{C}U(\mathrm{Aff}(M))$ is the induced module

$$\mathrm{Ind}_{(1-f)M \rtimes U(S)}^{U(\mathrm{Aff}(M))} \mathbf{1}_{(1-f)M \rtimes U(S)}$$

where we recall that $\mathbf{1}_G$ denotes the trivial representation of a group G. We record this as the first item of the following proposition.

PROPOSITION 3.8. *Let S be a finite commutative ring, M a finite S-module and $f \in E(S)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_t$ be the orbits of $U(S)$ on $f\widehat{M}$ (which is a $U(\mathrm{Aff}(M))$-invariant subgroup of $\widehat{M}$) and let $\chi_i \in \mathcal{O}_i$.*

(1) *The module* $\mathbb{C}fM = \mathrm{Ind}_{(1-f)M \rtimes U(S)}^{U(\mathrm{Aff}(M))} \mathbf{1}_{(1-f)M \rtimes U(S)}$.

(2) *The decomposition of* $\mathbb{C}fM$ *into simple* $\mathbb{C}U(\mathrm{Aff}(M))$-*modules is given by*

$$\mathbb{C}fM = \bigoplus_{i=1}^{t} W_{(\mathcal{O}_i, \mathbf{1}_{\mathrm{St}_{U(S)}(\chi_i)})}$$

(retaining the notation of Theorem 3.7*).*

Proof. The first item was proved in the discussion immediately preceding the statement of the proposition. To prove the second item, we apply Frobenius reciprocity and the Mackey decomposition. Let $\chi \in \widehat{M}$, $\rho \in \widehat{\mathrm{St}_{U(S)}(\chi)}$ and let $\mathcal{O}$ be the orbit χ under $U(S)$. To decongest notation, we shall identify M with the subgroup of translations and $U(S)$ with the subgroup of dilations and use the notation of internal semidirect products. Then by Frobenius reciprocity we have

$$(5) \quad \left[\mathrm{Ind}_{(1-f)M \cdot U(S)}^{U(\mathrm{Aff}(M))} \mathbf{1}_{(1-f)M \cdot U(S)} : W_{(\mathcal{O}, \rho)} \right]$$
$$= \left[\mathrm{Res}_{(1-f)M \cdot U(S)}^{U(\mathrm{Aff}(M))} W_{(\mathcal{O}, \rho)} : \mathbf{1}_{(1-f)M \cdot U(S)} \right].$$

To compute the right hand side of (5), we apply the Mackey decomposition to

$$W_{(\mathcal{O}, \rho)} = \mathrm{Ind}_{M \cdot \mathrm{St}_{U(S)}(\chi)}^{U(\mathrm{Aff}(M))} \chi \otimes \rho.$$

Let $h(x) \in U(\mathrm{Aff}(M))$. Then, since M is a normal subgroup of $U(\mathrm{Aff}(M))$, we have

$$(1-f)M \cdot U(S)h(x)M \cdot \mathrm{St}_{U(S)}(\chi)$$
$$= (1-f)M \cdot U(S) \cdot Mh(x)\,\mathrm{St}_{U(S)}(\chi) = U(\mathrm{Aff}(M)),$$

and so there is only one double coset. Therefore, using the Mackey decomposition and that

$$((1-f)M \cdot U(S)) \cap (M \cdot \mathrm{St}_{U(S)}(\chi)) = (1-f)M \cdot \mathrm{St}_{U(S)}(\chi)$$

yields

$$(6) \quad \mathrm{Res}_{(1-f)M \cdot U(S)}^{U(\mathrm{Aff}(M))} \mathrm{Ind}_{M \cdot \mathrm{St}_{U(S)}(\chi)}^{U(\mathrm{Aff}(M))} \chi \otimes \rho$$
$$= \mathrm{Ind}_{(1-f)M \cdot \mathrm{St}_{U(S)}(\chi)}^{(1-f)M \cdot U(S)} \mathrm{Res}_{(1-f)M \cdot \mathrm{St}_{U(S)}(\chi)}^{M \cdot \mathrm{St}_{U(S)}(\chi)} \chi \otimes \rho.$$

Another application of Frobenius reciprocity to (6) shows that the right hand side of (5) is equal to

$$\left[\mathrm{Res}_{(1-f)M \cdot \mathrm{St}_{U(S)}(\chi)}^{(1-f)M \cdot U(S)} \mathbf{1}_{(1-f)M \cdot U(S)} : \mathrm{Res}_{(1-f)M \cdot \mathrm{St}_{U(S)}(\chi)}^{M \cdot \mathrm{St}_{U(S)}(\chi)} \chi \otimes \rho \right],$$

which is 1 if $(1-f)M \subseteq \ker \chi$ and $\rho = \mathbf{1}_{\mathrm{St}_{U(S)}}(\chi)$ and 0, otherwise. By Proposition 3.6, $(1-f)M \subseteq \ker \chi$ if and only if $\chi \in \widehat{fM}$. This completes the proof. $\square$

REMARK 3.9. We remark that if $e \in E(S)$ and $f \in E(Se)$, then the $\mathbb{C}\,\mathrm{Aff}(M)$-module structure on $\mathbb{C}fM$ is the inflation along $\Phi_e \colon \mathrm{Aff}(M) \to \mathrm{Aff}(eM)$ of the $\mathbb{C}\,\mathrm{Aff}(eM)$-module $\mathbb{C}feM = \mathbb{C}fM$. To relate the decomposition in (5) over $\mathrm{Aff}(M)$ with the corresponding decomposition over $\mathrm{Aff}(eM)$, we should identify $\widehat{fM}$ with $\widehat{feM}$ (both of which are isomorphic to $\widehat{fM}$) and use Proposition 2.3.

It will also be convenient to decompose a module of the form $W_{(\mathcal{O}, \mathbf{1}_{\mathrm{St}_{U(S)}(\chi)})}$ with $\chi \in \mathcal{O}$ over $U(S)$.

PROPOSITION 3.10. *Let $\mathcal{O}$ be an orbit of $U(S)$ on $\widehat{M}$ and $\chi \in \mathcal{O}$. Then*

$$\operatorname{Res}_{U(S)}^{U(\operatorname{Aff}(M))} W_{(\mathcal{O}, \mathbf{1}_{\operatorname{St}_{U(S)}(\chi)})} = \bigoplus_{\substack{\rho \in \widehat{U(S)}, \\ \operatorname{St}_{U(S)}(\chi) \subseteq \ker \rho}} \rho.$$

Proof. We again identify M with the subgroup of translations and $U(S)$ with the subgroup of dilations and use internal semidirect product notation. If $h(x) \in U(\operatorname{Aff}(M))$, then the double coset

$$U(S)h(x)M \cdot \operatorname{St}_{U(S)}(\chi) = U(S) \cdot Mh(x) \cdot \operatorname{St}_{U(S)}(\chi) = U(\operatorname{Aff}(M))$$

by normality of M and so there is only one double coset. The Mackey decomposition and the equality $U(S) \cap M \cdot \operatorname{St}_{U(S)}(\chi) = \operatorname{St}_{U(S)}(\chi)$ then yield

$$(7) \qquad \operatorname{Res}_{U(S)}^{U(\operatorname{Aff}(M))} \operatorname{Ind}_{M \cdot \operatorname{St}_{U(S)}(\chi)}^{U(\operatorname{Aff}(M))} \chi \otimes \mathbf{1}_{\operatorname{St}_{U(S)}} = \operatorname{Ind}_{\operatorname{St}_{U(S)}(\chi)}^{U(S)} \mathbf{1}_{\operatorname{St}_{U(S)}(\chi)}.$$

Applying Frobenius reciprocity to (7) shows that the multiplicity of $\rho \in \widehat{U(S)}$ as a summand in the right hand side of (7) is 1 if $\rho|_{\operatorname{St}_{U(S)}(\chi)} = \mathbf{1}_{\operatorname{St}_{U(S)}(\chi)}$ and 0, otherwise. This completes the proof. $\qquad \square$

Let us return now to our original finite commutative ring R and a finite R-module V. We wish to find the composition factors of $\mathbb{C}V$ as a $\mathbb{C}\operatorname{Aff}(V)$-module. The module structure on $\mathbb{C}V$ is just the linear extension of the natural action where $h(x) = ax + b$ acts on $v \in V$ by $h(v) = av + b$. The character θ of this module is given by

$$\theta(ax + b) = |\{v \in V \mid av + b = v\}|.$$

Let μ denote the Möbius function of the lattice $\Lambda(R)$ of idempotent generated principal ideals of R and ζ its zeta function. Note that if $e, f \in E(R)$, then $Re = Rf$ if and only if $e = f$ and $Rf \subseteq Re$ if and only if $f = ef = fe$. We shall need the following observation. If $\chi \in \widehat{V}$ and if $e\chi = \chi = f\chi$, then $ef\chi = \chi$. Hence, there exists $e_\chi \in E(R)$ such that $e_\chi \chi = \chi$ and, for all $f \in E(R)$, $f\chi = f$ if and only if $Re_\chi \subseteq Rf$. Also note that if χ and χ' are in the same $U(R)$ orbit, then $e_\chi = e_{\chi'}$ because $f\chi = \chi$ if and only if $f\chi' = \chi'$. Thus we put $e_\mathcal{O} = e_\chi$ for any χ in the orbit $\mathcal{O}$ of $U(R)$ on $\widehat{V}$.

THEOREM 3.11. *Let R be a finite commutative ring, V a finite R-module and $e \in E(R)$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_s$ be the orbits of $U(Re)$ on $\widehat{eV}$, which we may identify with $\widehat{eV}$. Let $\chi_i \in \mathcal{O}_i$. Then the composition factors of $\mathbb{C}V$ with apex e are exactly those $W_{(\mathcal{O}_i, \mathbf{1}_{\operatorname{St}_{U(Re)}(\chi_i)})}^{\sharp}$ with*

$$\mathcal{O}_i \subseteq \widehat{eV} \smallsetminus \bigcup_{\substack{Rf \subsetneq Re, \\ f \in E(R)}} \widehat{fV},$$

that is, with $e_{\mathcal{O}_i} = e$ and they each appear with multiplicity one.

Proof. Let γ be the character of $W_{(\mathcal{O}_i, \rho)}$. We again put $g_f(x) = fx$ for $f \in E(R)$. Note that if $h(x) = ax + b$, then $g_f h g_f(x) = g_f h(x) = afx + fb$. Since $E(\operatorname{Aff}(V))$ is a submonoid by Proposition 3.2, Theorem 2.5 yields that $[\mathbb{C}V : W_{(\mathcal{O}_i, \rho)}^{\sharp}]$, with $\rho \in \widehat{\operatorname{St}_{U(Re)}(\chi_i)}$, is given by

$$(8) \qquad \frac{1}{|\operatorname{Aff}(eV)|} \sum_{h(x) \in U(\operatorname{Aff}(eV))} \gamma(h(x)) \sum_{Rf \subseteq Re} \overline{\theta(g_f h(x) g_f)} \mu(Rf, Re).$$

But note that $\theta(g_f h(x) g_f) = \theta(g_f h(x)) = \theta(\Phi_f(h(x)))$, for $Rf \subseteq Re$, where

$$\Phi_f \colon U(\operatorname{Aff}(eV)) \to U(\operatorname{Aff}(fV))$$

is the surjective homomorphism $\Phi_f(ax + b) = afx + fb$, cf. Proposition 3.5. Set $S = Re$ and put $M = eV$, which is an S-module. Note that $afv + fb = v$ implies that $v \in fV = fM$ and so $\theta \circ \Phi_f$ is the character of the $\mathbb{C}S$-module $\mathbb{C}fM$ of Proposition 3.8. Thus, applying the first orthogonality relations, (8) becomes

$$(9) \qquad \sum_{Rf \subseteq Re} \mu(Rf, Re) \frac{1}{|\operatorname{Aff}(eV)|} \sum_{h(x) \in U(\operatorname{Aff}(eV))} \gamma(h(x)) \overline{\theta(\Phi_f(h(x)))}$$

$$= \sum_{Rf \subseteq Re} [\mathbb{C}fM : W_{(\mathcal{O}_i, \rho)}] \mu(Rf, Re).$$

But Proposition 3.8 shows that this multiplicity is zero unless $\mathcal{O}_i \subseteq \widehat{fM} = \widehat{fV}$ (under the identification of both with $\widehat{fV}$, cf. Remark 3.9) and $\rho = \mathbf{1}_{\operatorname{St}_{U(Re)}(\chi_i)}$, in which case it is one. Therefore, the right hand side of (9) equals zero unless $\rho = \mathbf{1}_{\operatorname{St}_{U(Re)}(\chi_i)}$, in which case it is

$$(10) \qquad \sum_{Re_{\mathcal{O}_i} \subseteq Rf \subseteq Re} \zeta(Re_{\mathcal{O}_i}, Rf) \mu(Rf, Re).$$

But the quantity in (10) is zero unless $e_{\mathcal{O}_i} = e$, in which case it is one. This completes the proof of the theorem. $\qquad \square$

4. Eigenvalues

Fix a finite commutative ring R and a finite R-module V. Our goal is to prove Theorem 1.3. We shall, in fact, prove a more general result about the eigenvalues of certain elements of $\mathbb{C}\operatorname{Aff}(V)$ acting on $\mathbb{C}V$. Let us begin with a description of how an operator supported on translations and constant on associates acts under an irreducible representation.

PROPOSITION 4.1. *Let $P \in \mathbb{C}V$ be constant on associates. View P as an element of $\mathbb{C}\operatorname{Aff}(V)$ supported on translations. Let $W_{(\mathcal{O}, \rho)}^{\sharp}$ be a simple $\mathbb{C}\operatorname{Aff}(V)$-module with apex e, whence $\mathcal{O} = U(Re)\chi$ is an orbit of $U(Re)$ on $\widehat{eV}$ (which we identify with $\widehat{eV}$ and hence we identify $\mathcal{O}$ with $U(R)\chi$) and ρ is a character of $\operatorname{St}_{U(Re)}(\chi)$. Then P acts on $W_{(\mathcal{O}, \rho)}^{\sharp}$ via scalar multiplication by*

$$\widehat{P}(\chi) = \sum_{b \in V} P(b)\chi(b).$$

Proof. Note that $P \in \mathbb{C}U(\operatorname{Aff}(V))$. Moreover, notice that two translations $g(x) = x + b$ and $h(x) = x + c$ are conjugate in $U(\operatorname{Aff}(V))$ if and only if b, c are associates. Indeed, conjugating a translation by a translation does nothing. On the other hand, conjugating $g(x) = x + b$ by $h(x) = ux$ with $u \in U(R)$ yields $hgh^{-1}(x) = x + ub$. Thus P belongs to the center of $\mathbb{C}U(\operatorname{Aff}(V))$. Therefore, P acts via a scalar on any simple $\mathbb{C}U(\operatorname{Aff}(V))$-module by Schur's lemma.

Let $\Phi_e \colon U(\operatorname{Aff}(V)) \to U(\operatorname{Aff}(eV))$ be the canonical homomorphism. We saw at the beginning of Subsection 3.2 that the restriction of $W_{(\mathcal{O}, \rho)}^{\sharp}$ to $U(\operatorname{Aff}(V))$ is the inflation of $W_{(\mathcal{O}, \rho)}$ along Φ_e. As Φ_e is surjective by Proposition 3.5, this is a simple $\mathbb{C}U(\operatorname{Aff}(V))$-module. In fact, it is the simple module $W_{(\mathcal{O}, \rho\varphi_e)}$, where $\varphi_e \colon U(R) \to U(Re)$ is the projection and we view $\mathcal{O}$ as an orbit of $U(Re)$ on $\widehat{eV}$, by Proposition 2.3. It remains to understand the restriction of $W_{(\mathcal{O}, \rho\varphi_e)}$ to V (viewed as the group of translations in $U(\operatorname{Aff}(V))$).

As $U(R)$ is a set of coset representatives for the normal subgroup V of $U(\operatorname{Aff}(V))$, conjugation of a translation $h(x) = x + b$ by a dilation $g(x) = ux$ corresponds to

multiplying b by u and $(\chi \otimes \rho\varphi_e)|_V = \chi$, the Mackey decomposition yields that as a $\mathbb{C}V$-module $W_{(\mathcal{O}, \rho\varphi_e)}$ is the direct sum of the characters in the orbit $\mathcal{O}$ of χ. Each of these characters give the same Fourier transformation of P because P is constant on associates. Thus P acts on $W_{(\mathcal{O}, \rho\varphi_e)}$ via scalar multiplication by $\widehat{P}(\chi)$. This completes the proof. $\qquad\square$

We remark that it is almost never the case that P belongs to the center of $\mathbb{C}\operatorname{Aff}(V)$. Indeed, if $z(x) \in \operatorname{Aff}(V)$ is the zero mapping, then $zP = z$. But if P is not a point mass at 0, then $Pz = \sum_{b \in V} P(b)(0x + b) \neq z$. Thus we are using in an essential way the observation, implicit in the above proof, that each irreducible representation of $\operatorname{Aff}(V)$ remains irreducible when restricted to the group of units $U(\operatorname{Aff}(V))$ in order to apply Schur's lemma and deduce that P acts as a scalar matrix under irreducible representations of $\operatorname{Aff}(V)$.

Let $p(x, y) \in \mathbb{C}[x, y]$ be a polynomial and let $P, Q \in \mathbb{C}\operatorname{Aff}(V)$ with P supported on translations and Q supported on dilations, i.e. P is supported on V and Q is supported on $M(R)$ under the semidirect product decomposition $\operatorname{Aff}(V) = V \rtimes M(R)$. We further assume that P is constant on associates. Then we compute the eigenvalues of $A = p(P, Q)$ on the module $\mathbb{C}V$. More precisely, we prove the following theorem.

THEOREM 4.2. *Let $p(x, y) \in \mathbb{C}[x, y]$ be a polynomial and let $P, Q \in \mathbb{C}\operatorname{Aff}(V)$ with P supported on translations and Q supported on dilations. We further assume that P is constant on associates. Put $A = p(P, Q)$. Then the eigenvalues for A on $\mathbb{C}V$ are indexed by triples $(e, \mathcal{O}, \rho)$ where:*

(1) *$e \in E(R)$;*
(2) *$\mathcal{O} = U(R)\chi$ is an orbit of $U(R)$ on*

$$e\widehat{V} \smallsetminus \bigcup_{\substack{Rf \subsetneq Re, \\ f \in E(R)}} f\widehat{V},$$

that is, $e_{\mathcal{O}} = e$;
(3) *and $\rho \in \widehat{U(Re)}$ such that $\operatorname{St}_{U(Re)}(\chi) \subseteq \ker \rho$.*

The corresponding eigenvalue is $p(\widehat{P}(\chi), \widehat{Q}(\rho))$, where

$$\widehat{P}(\chi) = \sum_{b \in V} P(b)\chi(b)$$
$$\widehat{Q}(\rho) = \sum_{Ra \supseteq Re} Q(a)\rho(ae),$$

and it occurs with multiplicity one.

Proof. Let $\mathbb{C}V = U_0 \supsetneq U_1 \supsetneq \cdots \supsetneq U_n = 0$ be a composition series for $\mathbb{C}V$ as a $\mathbb{C}\operatorname{Aff}(V)$-module. If we choose a basis $B = B_0 \cup \cdots \cup B_{n-1}$ for $\mathbb{C}V$ such that $B_i \subseteq U_i$ projects to a basis for U_i/U_{i+1} for $0 \leqslant i \leqslant n-1$, then the corresponding matrix representation of $\operatorname{Aff}(V)$ has a block upper triangular form with diagonal blocks ρ_i corresponding to the matrix representation afforded by U_i/U_{i+1} with respect to the basis that is the projection of B_i into U_i/U_{i+1}. It follows that the set of eigenvalues of A on $\mathbb{C}V$ with multiplicities is the union with multiplicities of the eigenvalues of $\rho_i(A)$ for $1 \leqslant i \leqslant n-1$, i.e. for the action of A on the composition factors of $\mathbb{C}V$. The composition factors of $\mathbb{C}V$ are described in Theorem 3.11. So it suffices to show that if $\chi \in \widehat{V}$ and $e = e_\chi$, then the eigenvalues of A on $W^\sharp_{(\mathcal{O}, \mathbf{1}_{\operatorname{St}_{U(Re)}(\chi)})}$, where $\mathcal{O}$ is the orbit of χ under $U(R)$, are of the form $p(\widehat{P}(\chi), \widehat{Q}(\rho))$ where $\rho \in \widehat{U(Re)}$ with $\operatorname{St}_{U(Re)}(\chi) \subseteq \ker \rho$.

By Proposition 4.1, P acts on $W^{\sharp}_{(\mathcal{O}, \mathbf{1}_{\mathrm{St}_{U(Re)}(\chi)})}$ as scalar multiplication by $\widehat{P}(\chi)$. It therefore suffices to show that Q is diagonalizable with eigenvalues $\widehat{Q}(\rho)$ where $\rho \in \widehat{U(Re)}$ with $\mathrm{St}_{U(Re)}(\chi) \subseteq \ker \rho$. But Q is supported on dilations and the dilation $h(x) = ax$ acts on $W^{\sharp}_{(\mathcal{O}, \mathbf{1}_{\mathrm{St}_{U(Re)}(\chi)})}$ as the element $x \mapsto aex$ of $U(Re)$ if $Ra \supseteq Re$ and as 0, else. Proposition 3.10 shows that $W_{(\mathcal{O}, \mathbf{1}_{\mathrm{St}_{U(Re)}(\chi)})}$ restricts to $U(Re)$ as a direct sum of precisely the linear characters ρ where $\rho \in \widehat{U(Re)}$ with $\mathrm{St}_{U(Re)}(\chi) \subseteq \ker \rho$ and hence on the corresponding summand Q acts as $\widehat{Q}(\rho)$. This completes the proof. $\square$

The special case where P, Q are probabilities and $p(x, y) = \alpha x + (1 - \alpha)y$ with $0 \leqslant \alpha \leqslant 1$ for the coin-toss walk and $p(x, y) = xy$ for the affine walk (cf. Subsection 2.3) yields the following formulation of Theorem 1.3.

THEOREM 4.3. *Let R be a finite commutative ring, V a finite R-module, P a probability on V that is constant on associates and Q a probability on R. Then the eigenvalues for the transition matrices of both the coin-toss walk and the affine walk on V are indexed by triples $(e, \mathcal{O}, \rho)$ where:*

   (1) *$e \in E(R)$;*
   (2) *$\mathcal{O} = U(R)\chi$ is an orbit of $U(R)$ on*

$$e\widehat{V} \smallsetminus \bigcup_{\substack{Rf \subsetneq Re, \\ f \in E(R)}} f\widehat{V};$$

   (3) *and $\rho \in \widehat{U(Re)}$ such that $\mathrm{St}_{U(Re)}(\chi) \subseteq \ker \rho$.*

The corresponding eigenvalue for the coin-toss walk is $\alpha\widehat{P}(\chi) + (1 - \alpha)\widehat{Q}(\rho)$ and for the affine walk is $\widehat{P}(\chi)\widehat{Q}(\rho)$ (where $\chi \in \mathcal{O}$) where

$$\widehat{P}(\chi) = \sum_{b \in V} P(b)\chi(b)$$

$$\widehat{Q}(\rho) = \sum_{Ra \supseteq Re} Q(a)\rho(ae).$$

This eigenvalue occurs with multiplicity one.

To see that Theorem 1.3 is a reformulation of Theorem 4.3, we need some further preliminaries. Let W be a finite R-module. If $v \in W$, then

$$\mathrm{ann}(v) = \{a \in R \mid av = 0\}$$

is the *annihilator* of v; it is an ideal of R. Note that the annihilators of v and the cyclic submodule Rv are the same and $Rv \cong R/\mathrm{ann}(v)$ as an R-module. In particular, $Rv \cong Rw$ if and only if $\mathrm{ann}(v) = \mathrm{ann}(w)$.

PROPOSITION 4.4. *Let $v \in V$ and $e \in E(R)$. Then $ev = v$ if and only if $1 - e \in E(\mathrm{ann}(v))$.*

Proof. This is obvious. $\square$

Recall that $E(R)$ is a Boolean algebra with respect to the ordering $e \leqslant f$ if $ef = e$. The operations are given by $e \wedge f = ef$, $e \vee f = e + f - ef$ and $\neg e = 1 - e$. The mapping $e \mapsto Re$ is an isomorphism of Boolean algebras.

As $ev = v$ and $fv = v$ implies $efv = v$, it follows that there is a minimal idempotent e_v with $e_v v = v$. As $e \mapsto 1 - e$ is an order reversing involution on $E(R)$, it follows from Proposition 4.4 that $e = e_v$ if and only if $1 - e$ is the maximal idempotent in $\mathrm{ann}(v)$ (which is a join subsemilattice as $0 \in \mathrm{ann}(v)$ and $e \vee f = e + f - ef$). In

particular, $\operatorname{ann}(v) = \operatorname{ann}(w)$ implies $e_v = e_w$. Also note that $Rv = Rw$ implies that $\operatorname{ann}(v) = \operatorname{ann}(w)$, whence $e_v = e_w$.

PROPOSITION 4.5. *Let $v \in W$.*

    (1) *The natural mapping $\pi_v \colon U(R) \to U(R/\operatorname{ann}(v))$ is surjective and $\pi_v(r) = \pi_v(re_v)$ for all $r \in R$.*

    (2) *Let $\rho \in \widehat{U(R)}$. Then $(1 + \operatorname{ann}(v)) \cap U(R) \subseteq \ker \rho$ if and only if ρ factors through π_v.*

    (3) *If $a \in Re_v$, then $a \in U(Re_v)$ if and only if $a + \operatorname{ann}(v) \in U(R/\operatorname{ann}(v))$.*

Proof. First note that $r - re_v = r(1 - e_v) \in \operatorname{ann}(v)$ for all $r \in R$, whence $\pi_v(r) = \pi_v(re_v)$, and so $Re_v \to R/\operatorname{ann}(a)$ is a surjective homomorphism of unital rings. It is enough to show that the natural mapping $U(Re_v) \to U(R/\operatorname{ann}(v))$ is surjective since we can then apply Proposition 3.1.

Suppose that $a + \operatorname{ann}(v)$ is a unit with inverse $b + \operatorname{ann}(v)$ with $a, b \in Re_v$. Then $ab + \operatorname{ann}(v) = 1 + \operatorname{ann}(v) = e_v + \operatorname{ann}(v)$ and so $ab = e_v + x$ with $x \in \operatorname{ann}(v)$. Then $abv = e_v v + xv = v$ and hence $(ab)^n v = v$ for all $n > 0$. As $M(R)$ is a finite monoid, we have that $(ab)^k \in E(Re_v)$ for some $k > 0$. Minimality of e_v then implies $(ab)^k = e_v$ and so $a \in U(Re_v)$. This completes the proof of the first item and also the third.

The second item follows from the first and the observation that $\ker \pi_v = (1 + \operatorname{ann}(v)) \cap U(R)$. $\qquad\square$

Proof of Theorem 1.3. By Proposition 1.1 there is a bijection between orbits of $U(R)$ on $\widehat{V}$ and cyclic submodules if $\widehat{V}$. Moreover, e is the minimal idempotent stabilizing $\chi \in \widehat{V}$ if and only if $1 - e$ is the maximal idempotent in $\operatorname{ann}(\chi)$ by Proposition 4.4. If e is the minimal idempotent stabilizing χ, then $\operatorname{St}_{U(Re)}(\chi) = e + \operatorname{ann}(\chi)e$. By Proposition 4.5, we have that if $\rho \in \widehat{U(Re)}$, then $\ker \rho$ contains $\operatorname{St}_{U(Re)}(\chi)$ if and only if ρ factors through $Re \to R/\operatorname{ann}(\chi)$. Thus the triples $(e, \mathcal{O}, \rho)$ from Theorem 4.3 correspond bijectively to the pairs (W, ρ) of Theorem 4.3. Moreover, by Proposition 3.1 and Proposition 4.5, we have that $Ra \supseteq Re$ if and only if $ae \in U(Re)$, if and only if $ae + \operatorname{ann}(\chi) = a + \operatorname{ann}(\chi) \in U(R/\operatorname{ann}(\chi))$, if and only if $a \in U(R) + \operatorname{ann}(\chi)$. It follows that the definitions of $\widehat{Q}(\rho)$ in Theorem 1.3 and in Theorem 4.3 agree (using Proposition 4.5). $\qquad\square$

We now aim to recover the results of the first author and Singla [11] for the case when $V = R$ (and hence cyclic submodules are principal ideals) and P is uniform. In this case, one has that $\widehat{P}(\chi) = 0$ for any non-trivial character χ on the additive group of R by the orthogonality relations for characters. Hence many of the eigenvalues in Theorem 1.3 will be the same. We shall first give a description of the eigenvalues that follows directly from Theorem 1.3. We shall then reformulate the result to make it apparent that it agrees with the results of [11] for $V = R$.

THEOREM 4.6. *Let R be a finite commutative ring and V a finite R-module. Let Q be a probability on R. Then the eigenvalues for transition matrix of the coin-toss random walk on V with respect to P the uniform distribution and Q, with heads probability α, are indexed by pairs $([W], \rho)$ where $[W]$ is the isomorphism class of a cyclic submodule of W of $\widehat{V}$ and ρ is a character of $U(R)$ factoring through $\pi_W \colon U(R) \to U(R/\operatorname{ann}(W))$. The corresponding eigenvalue is given by*

$$\lambda_{([W], \rho)} = \begin{cases} 1, & \text{if } W = 0 \\ (1 - \alpha) \sum_{a \in U(R) + \operatorname{ann}(W)} Q(a)\rho(u_W(a)), & \text{else} \end{cases}$$

where $u_W(a) \in U(R)$ with $u_W(a) + \operatorname{ann}(W) = a + \operatorname{ann}(W)$; it has multiplicity the number of cyclic submodules of $\widehat{V}$ isomorphic to W.

Proof. This follows from Theorem 1.3, the observation that

$$\widehat{P}(\chi) = \frac{1}{|V|} \sum_{v \in V} \chi(v) = \langle 1_V, \chi \rangle = \begin{cases} 1, & \text{if } \chi = \mathbf{1}_V \\ 0, & \text{else} \end{cases}$$

by the orthogonality relations and from Proposition 4.5. □

Our next goal is to show that we can work with cyclic submodules of V instead of $\widehat{V}$. This is necessary to recover the result as formulated in [11]. We do this by showing that the coin-toss walk with P uniform for V and $\widehat{V}$ have the same eigenvalues.

The following result can also be proved via elementary linear algebra (cf. [26]).

PROPOSITION 4.7. *Consider the coin-toss random walk on V where P is taken to be the uniform distribution on R, Q is any distribution on R and α is the probability of heads. Let $1 = \lambda_1, \lambda_2, \ldots, \lambda_k$ be the eigenvalues for the transition matrix of the random walk of the multiplicative monoid $M(R)$ on V driven by Q with multiplicities. Then the eigenvalues for the transition matrix of the coin-toss walk are*

$$1 = \lambda_1, (1 - \alpha)\lambda_2, \ldots, (1 - \alpha)\lambda_k$$

with multiplicities.

Proof. This is immediate from Theorem 4.6 once we observe that the random walk on V driven by Q is the coin-toss random walk with $\alpha = 0$. □

By Proposition 4.7, to show that the coin-toss walk with P uniform for V and $\widehat{V}$ have the same eigenvalues, it suffices to show that the random walks of the multiplicative monoid $M(R)$ on V and $\widehat{V}$ driven by Q have the same eigenvalues.

PROPOSITION 4.8. *Let V be a finite R-module and Q a probability on R. Then the transition matrix for the random walk of $M(R)$ on $\widehat{V}$ driven by Q is similar to the transpose of the transition matrix of the random walk of $M(R)$ on V driven by Q and hence both transition matrices have the same eigenvalues.*

Proof. The vector space dual of $\mathbb{C}V$, which is a $\mathbb{C}M(R)$-module, can be identified with the space of functions $f : V \to \mathbb{C}$ and the dual basis to the basis V of $\mathbb{C}V$ corresponds to the indicator functions δ_v of the singleton sets $\{v\}$ with $v \in V$. The module action of R on $\mathbb{C}^V$ is given by $(rf)(v) = f(rv)$. So the matrix of Q acting on $\mathbb{C}^V$ with respect to the basis of indicator functions is the transpose of the matrix of Q acting of $\mathbb{C}V$ with respect to the basis Ω and hence is the transition matrix of the random walk of $M(R)$ on V driven by Q (cf. Subsection 2.3). But the characters of V also form a basis for $\mathbb{C}^V$ and the matrix of Q with respect to the basis of characters is the transpose of the transition matrix of the random walk of $M(R)$ on $\widehat{V}$ driven by Q. This completes the proof. □

Using Theorem 4.6, Proposition 4.7, Proposition 4.8 and that $\widehat{\widehat{M}}$ is canonically isomorphic to M as an R-module, we then obtain the following theorem.

THEOREM 4.9. *Let R be a finite commutative ring and V a finite R-module. Let Q be a probability on R. Then the eigenvalues for transition matrix of the coin-toss random walk on V with respect to P the uniform distribution and Q, with heads probability α, are indexed by pairs $([W], \rho)$ where $[W]$ is the isomorphism class of a cyclic submodule of W of V and ρ is a character of $U(R)$ factoring through $\pi_W : U(R) \to U(R/\operatorname{ann}(W))$. The corresponding eigenvalue is*

$$\lambda_{([W], \rho)} = \begin{cases} 1, & \text{if } W = 0 \\ (1 - \alpha) \sum_{a \in U(R) + \operatorname{ann}(W)} Q(a)\rho(u_W(a)), & \text{else} \end{cases}$$

where $u_W(a) \in U(R)$ with $u_W(a) + \mathrm{ann}(W) = a + \mathrm{ann}(W)$; it has multiplicity the number of cyclic submodules of V isomorphic to W.

The special case in which $V = R$ (and hence cyclic modules are principal ideals) recovers [11, Theorem 2.3].

References

[1] Jorge Almeida, Stuart Margolis, Benjamin Steinberg, and Mikhail Volkov, *Representation theory of finite semigroups, semigroup radicals and formal language theory*, Trans. Am. Math. Soc. **361** (2009), no. 3, 1429–1461.

[2] Claudio Asci, *Generating uniform random vectors*, J. Theor. Probab. **14** (2001), no. 2, 333–356.

[3] _____, *Asymptotic behavior of an affine random recursion in $\mathbf{Z}_p^k$ defined by a matrix with an eigenvalue of size 1*, Stat. Probab. Lett. **79** (2009), no. 11, 1421–1428.

[4] _____, *Generating uniform random vectors in Z_p^k: the general case*, J. Theor. Probab. **22** (2009), no. 3, 791–809.

[5] _____, *Convergence in total variation of an affine random recursion in $[0, p)^k$ to a uniform random vector*, Markov Process. Relat. Fields **19** (2013), no. 1, 125–140.

[6] Christos A. Athanasiadis and Persi Diaconis, *Functions of random walks on hyperplane arrangements*, Adv. Appl. Math. **45** (2010), no. 3, 410–437.

[7] Arvind Ayyer, Steven Klee, and Anne Schilling, *Combinatorial Markov chains on linear extensions*, J. Algebr. Comb. **39** (2014), no. 4, 853–881.

[8] _____, *Markov chains for promotion operators*, in Algebraic Monoids, Group Embeddings, and Algebraic Combinatorics, Fields Inst. Commun., no. 71, Springer-Verlag New York, 2014, pp. 285–304.

[9] Arvind Ayyer, Anne Schilling, Benjamin Steinberg, and Nicolas M. Thiéry, *Directed nonabelian sandpile models on trees*, Commun. Math. Phys. **335** (2015), no. 3, 1065–1098.

[10] _____, *Markov chains, $\mathcal{R}$-trivial monoids and representation theory*, Int. J. Algebra Comput. **25** (2015), no. 1-2, 169–231.

[11] Arvind Ayyer and Pooja Singla, *Random motion on finite rings, I: commutative rings*, to appear in Algebr. Represent. Theory, `https://arxiv.org/abs/1605.05089`, 2016.

[12] Hyman Bass, *K-theory and stable algebra*, Publications Mathématiques de l'IHÉS **22** (1964), 5–60.

[13] Michael E. Bate and Stephen B. Connor, *Mixing time and cutoff for a random walk on the ring of integers mod n*, Bernoulli **24** (2018), no. 2, 993–1009.

[14] David J. Benson, *Representations and cohomology. I: Basic representation theory of finite groups and associative algebras*, second ed., Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1998.

[15] Pat Bidigare, Phil Hanlon, and Dan Rockmore, *A combinatorial description of the spectrum for the Tsetlin library and its generalization to hyperplane arrangements*, Duke Math. J. **99** (1999), no. 1, 135–174.

[16] Anders Björner, *Random walks, arrangements, cell complexes, greedoids, and self-organizing libraries*, in Building bridges, Bolyai Soc. Math. Stud., vol. 19, Springer, Berlin, 2008, pp. 165–203.

[17] _____, *Note: Random-to-front shuffles on trees*, Electron. Commun. Probab. **14** (2009), 36–41.

[18] Kenneth S. Brown, *Semigroups, rings, and Markov chains*, J. Theor. Probab. **13** (2000), no. 3, 871–938.

[19] _____, *Semigroup and ring theoretical methods in probability*, in Representations of finite dimensional algebras and related topics in Lie theory and geometry, Fields Inst. Commun., vol. 40, Amer. Math. Soc., Providence, RI, 2004, pp. 3–26.

[20] Kenneth S. Brown and Persi Diaconis, *Random walks and hyperplane arrangements*, Ann. Probab. **26** (1998), no. 4, 1813–1854.

[21] Ting-Li Chen and Chii-Ruey Hwang, *Accelerating reversible Markov chains*, Stat. Probab. Lett. **83** (2013), no. 9, 1956–1962.

[22] Fan R. K. Chung, Persi Diaconis, and Ronald L. Graham, *Random walks arising in random number generation*, Ann. Probab. **15** (1987), no. 3, 1148–1165.

[23] Fan R. K. Chung and Ronald L. Graham, *Edge flipping in graphs*, Adv. Appl. Math. **48** (2012), no. 1, 37–63.

[24] Persi Diaconis, *From shuffling cards to walking around the building: an introduction to modern Markov chain theory*, Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998), Doc. Math., no. Extra Vol. ICM, 1998, pp. 187–204.

[25] Persi Diaconis, Susan Holmes, and Radford M. Neal, *Analysis of a nonreversible Markov chain sampler*, Ann. Appl. Probab. **10** (2000), no. 3, 726–752.

[26] Jiu Ding and Aihui Zhou, *Eigenvalues of rank-one updated matrices with some applications*, Appl. Math. Lett. **20** (2007), no. 12, 1223–1226.

[27] Olexandr Ganyushkin, Volodymyr Mazorchuk, and Benjamin Steinberg, *On the irreducible representations of a finite semigroup*, Proc. Am. Math. Soc. **137** (2009), no. 11, 3585–3592.

[28] James A. Green, *On the structure of semigroups*, Ann. Math. (2) **54** (1951), 163–172.

[29] Martin Hildebrand, *Random processes of the form $X_{n+1} = a_n X_n + b_n$ (mod p)*, Ann. Probab. **21** (1993), no. 2, 710–720.

[30] ———, *Random processes of the form $X_{n+1} = a_n X_n + b_n$ (mod p) where b_n takes on a single value*, in Random discrete structures (Minneapolis, MN, 1993), IMA Vol. Math. Appl., vol. 76, Springer, New York, 1996, pp. 153–174.

[31] ———, *A lower bound for the Chung-Diaconis-Graham random process*, Proc. Am. Math. Soc. **137** (2009), no. 4, 1479–1487.

[32] Martin Hildebrand and Joseph McCollum, *Generating random vectors in $(\mathbb{Z}/p\mathbb{Z})^d$ via an affine random process*, J. Theor. Probab. **21** (2008), no. 4, 802–811.

[33] Lu-Jing Huang and Yong-Hua Mao, *On some mixing times for nonreversible finite Markov chains*, J. Appl. Probab. **54** (2017), no. 2, 627–637.

[34] Marcus Kaiser, Robert L. Jack, and Johannes Zimmer, *Acceleration of convergence to equilibrium in Markov chains by breaking detailed balance*, J. Stat. Phys. **168** (2017), no. 2, 259–287.

[35] Donald B. McAlister, *Characters of finite semigroups*, J. Algebra **22** (1972), 183–200.

[36] John Rhodes and Yechezkel Zalcstein, *Elementary representation and character theory of finite semigroups and its application*, in Monoids and semigroups with applications (Berkeley, CA, 1989), World Sci. Publ., River Edge, NJ, 1991, pp. 334–367.

[37] Murray Rosenblatt, *Stationary measures for random walks on semigroups*, in Semigroups (Proc. Sympos., Wayne State Univ., Detroit, Mich., 1968), Academic Press, New York, 1969, pp. 209–220.

[38] Franco Saliola, *Eigenvectors for a random walk on a left-regular band*, Adv. Appl. Math. **48** (2012), no. 2, 306–311.

[39] Jean-Pierre Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott.

[40] Richard P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 1997, With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[41] Benjamin Steinberg, *In modules over finite rings $Rv = Rw \iff R^{\times} v = R^{\times} w$*, `https://mathoverflow.net/q/211739` (version: 2017-06-14).

[42] ———, *Möbius functions and semigroup representation theory*, J. Comb. Theory, Ser. A **113** (2006), no. 5, 866–881.

[43] ———, *Möbius functions and semigroup representation theory. II. Character formulas and multiplicities*, Adv. Math. **217** (2008), no. 4, 1521–1557.

[44] ———, *Representation theory of finite monoids*, Universitext, Springer, Cham, 2016.

[45] Jay A. Wood, *Duality for modules over finite rings and applications to coding theory*, Am. J. Math. **121** (1999), no. 3, 555–575.

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

BENJAMIN STEINBERG, Department of Mathematics, City College of New York, Convent Avenue at 138th Street, New York, New York 10031, USA
E-mail : `bsteinberg@ccny.cuny.edu`