A Prime Decomposition of Probabilistic Automata

Gunnar Carlsson
Department of Mathematics
Stanford University

Jun Yu
Institute for Computational & Mathematical Engineering
Stanford University

Contents

1 Introduction 2

2 Automata and Semigroups 2
  2.1 Deterministic Automata 2
  2.2 Probabilistic Automata 3

3 Local Structure of Probabilistic Automata 4
  3.1 Green-Rees Theory 4
  3.2 Local Structure of Transition Semigroups 6

4 Global Structure of Probabilistic Automata 10
  4.1 Krohn-Rhodes Theory 10
  4.2 Global Structure of Transition Semigroups 12

5 Representation Theory of Probabilistic Automata 13
  5.1 Munn-Ponizovskii Theory 13
  5.2 Holonomy Decomposition 16
  5.3 Representation Theory of Reduced Holonomy Monoid 19

References 21

This paper is based on the second author’s doctoral thesis written under the direction of the first author.
1 Introduction

Krohn-Rhodes theorem asserts that every deterministic automaton can be decomposed into cascades of irreducible automata. Algebraically, this implies that a finite semigroup acting on a finite set factors into a finite wreath product of finite simple groups and a semigroup of order 3 consisting of the identity map and constant maps on a set of order 2. The semigroups in this factorization are prime under the semidirect product.

In Section 2, we formulate a definition of probabilistic automata in which a statement analogous to the prime decomposition follows directly from Krohn-Rhodes theorem.

Section 3 deals with Green-Rees theory. We determine Green’s relations on the monoid of stochastic matrices in order to characterize the local structure of probabilistic automata.

Krohn-Rhodes theory is introduced in Section 4. The prime decomposition is presented as a framework to study the global structure of probabilistic automata.

Section 5 discusses Munn-Ponizovskii theory. We prove that irreducible representations of a probabilistic automaton are determined by those of finite groups in its holonomy decomposition, which is a variant of the prime decomposition.

2 Automata and Semigroups

2.1 Deterministic Automata

Given a set $X$, $F_X$ denotes the monoid of all maps $X 	o X$. If $X$ is of order $n$, we can index $X$ by

$$n = \{i \mid 0 \leq i < n\}$$

with a bijection $X \to n$, and write $F_n \cong F_X$.

Definition 2.1. A deterministic automaton is a triple $(X, \Sigma, \delta)$ consisting of finite sets $X$ and $\Sigma$ along with a map $\delta : X \times \Sigma \to X$. We call $X$ a state set, $\Sigma$ an alphabet, and $\delta$ a transition function.

Let $\Sigma^*$ be the free monoid on $\Sigma$. We can define a right action of $\Sigma^*$ on $X$ by $xa = \delta(x, a)$, where $x \in X$ and $a \in A$. This action may not be faithful, and hence we consider the canonical homomorphism $\sigma : \Sigma^* \to F_X$. If $\Sigma^+$ is the free semigroup on $A$, then

$$S = \Sigma^+ \sigma$$

acts faithfully on $X$. Since $F_X$ is finite, so is $S$.

Definition 2.2. A transformation semigroup is a pair $(X, S)$ in which a finite semigroup $S$ acts faithfully on $X$ from the right.

In case $S$ is a monoid such that $1_S = 1_X$, we refer to $(X, S)$ as a transformation monoid. If, in addition, $S$ is a group, $(X, S)$ is called a transformation group.
If $S$ is not a monoid, we can adjoin an identity element $1$ in a natural way to form a monoid $S^1$. It is understood that $S^1 = S$ when $S$ is a monoid. Similarly, in its absence, adjunction of a zero element $0$ defines a new semigroup $S^0$. We write $\text{FSgp}$ for the category of finite semigroups.

2.2 Probabilistic Automata

Let $X$ be a finite set. Then $\mathbb{P}X$ is the set of all probability distributions on $X$. An element $\mu \in \mathbb{P}X$ is written as a formal sum
\[ \mu = \sum_{x \in X} \mu(x)x. \]
We can regard $\mathbb{P}X$ as a subset of the free $\mathbb{R}$-module on $X$, although $\mathbb{P}X$ itself does not have an additive structure.

**Definition 2.3.** A probabilistic automaton is a quadruple $(X, \Sigma, \delta, \mathbb{P})$ consisting of finite sets $X$ and $\Sigma$ along with a map $\delta : X \times \Sigma \to X$ and its extension $\mathbb{P}\delta : \mathbb{P}X \times \mathbb{P}\Sigma \to \mathbb{P}X$ defined by
\[ \mathbb{P}\delta(\pi, \mu) = \sum_{(x,a) \in X \times \Sigma} \pi(x)\mu(a)\delta(x,a) \]
for $\pi \in \mathbb{P}X$ and $\mu \in \mathbb{P}\Sigma$.

For a subset $\Omega$ of $\mathbb{P}\Sigma$, the quintuple $(X, \Sigma, \delta, \mathbb{P}, \Omega)$ is an instance of $(X, \Sigma, \delta, \mathbb{P})$, in which case $\mathbb{P}\delta$ is restricted to $\mathbb{P}X \times \Omega'$, where $\Omega'$ denotes the closure of the set generated by $\Omega$. When $\Omega$ is finite, $(X, \Sigma, \delta, \mathbb{P}, \Omega)$ resembles the classical definition of a probabilistic automaton [16].

Again, set $S = \Sigma^+\sigma$, where $\sigma : \Sigma^* \to F_X$ is the canonical homomorphism. Given $\mu \in \mathbb{P}A$, we abuse notation by writing $\mu$ for its corresponding distribution in $\mathbb{P}S$, so that for any $s \in S$,
\[ \mu(s) = \sum_{a \sigma = s} \mu(a). \]
Then $\mathbb{P}S$ is closed under convolution, which is given by
\[ (\mu \ast \nu)(s) = \sum_{a \sigma = s} \mu(t)\nu(u) \]
for $\mu, \nu \in \mathbb{P}S$, and hence $\mathbb{P}S$ forms a semigroup under convolution. Since $S$ is finite, as a topological semigroup, $\mathbb{P}S$ is compact Hausdorff.

**Definition 2.4.** A transition semigroup is a triple $(X, S, \mathbb{P})$ in which $S$ is a finite semigroup acting faithfully on a finite set $X$ from the right, inducing a right action of $\mathbb{P}S$ on $\mathbb{P}X$ defined by
\[ \pi \mu = \sum_{xs = y} \pi(x)\mu(s)y \]
for $\pi \in \mathbb{P}X$ and $\mu \in \mathbb{P}S$. 

3
For $Q \subseteq P S$, the quadruple $(X, S, P, Q)$ is an instance of $(X, S, P)$, in which case the action of $P S$ on $P X$ is restricted to $Q'$, where $Q'$ denotes the closure of the set generated by $Q$.

It is easy to see that $\pi_\mu \in P X$. Although we require that $S$ acts faithfully on $X$, the same is not true of the action of $P S$ on $P X$. We refer to $(X, S, P)$ as a *transition monoid* if $(X, S)$ is a transformation monoid. A *transition group* is defined accordingly.

### 3 Local Structure of Probabilistic Automata

#### 3.1 Green-Rees Theory

We introduce the work of Green and Rees as presented by Clifford & Preston [1] and Rhodes & Steinberg [2].

A subset $I \neq \emptyset$ of a semigroup $S$ is a *left ideal* if $SI \subseteq I$. A *right ideal* is defined dually. We say $I$ is an *ideal* if it is both a left and right ideal. Moreover, $S$ is *left simple*, *right simple*, or *simple* if it does not contain a proper left ideal, right ideal, or ideal. For any $s \in S$, we refer to $L(s) = S^1 s$, $R(s) = s S^1$, and $J(s) = S^1 s S^1$, respectively, as the principal left ideal, principal right ideal, and principal ideal generated by $s$.

**Definition 3.1.** Let $S$ be a semigroup. Then the quasiorders on $S$ given by

1. $s \leq_1 t$ if and only if $L(s) \subset L(t)$,
2. $s \leq_e t$ if and only if $R(s) \subset R(t)$,
3. $s \leq_i t$ if and only if $J(s) \subset J(t)$,
4. $s \leq_h t$ if and only if $s \leq_1 t$ and $s \leq_e t$ induce equivalence relations $\sim_1$, $\sim_e$, $\sim_h$, and $\sim_i$, respectively, on $S$. Furthermore, the relation $\emptyset = 1 \circ r = r \circ 1$ in $S \times S$ defines an equivalence relation $\sim_\emptyset$ on $S$. These five equivalence relations on $S$ are known as Green’s relations.

Green’s relations coincide in a commutative semigroup, while each relation is trivial for a group. In $S \times S$,

$$h = 1 \cap r \subseteq 1 \cup r \subseteq \emptyset \subseteq j.$$ 

Moreover, $\sim_1$ is a right congruence and $\sim_e$ is a left congruence. We write the $t$-class of $s \in S$ as

$$L_s = \{ t \in S \mid s \sim_1 t \},$$

and define $R_s$, $J_s$, $H_s$, and $D_s$ analogously.

**Proposition 3.2.** If $e$ is an idempotent in a semigroup $S$, then

1. $Se \cap J_e = L_e$,
2. $e S \cap J_e = R_e$, and
3. $e S \cap J_e = H_e$.

For any $u \in S$, the *left translation* by $u$ is the map $\lambda_u : S \to S$ defined by $s \lambda_u = us$. Its dual, denoted $\rho_u$, is the *right translation* by $u$. Green [6] used translations to construct bijections $L_s \to L_t$ and $R_s \to R_t$ when $s \sim_\emptyset t$. 


Lemma 3.3 (Green). Suppose \( s, t \in S \), where \( S \) is a semigroup.

1. If \( us = t \) and \( vt = s \) for \( u, v \in S^1 \), so that \( s \sim_l t \), then the maps \( \lambda_u |_{R_s} \) and \( \lambda_v |_{R_t} \) are inverses of one another.

2. If \( su = t \) and \( tv = s \) for \( u, v \in S^1 \), so that \( s \sim_r t \), then the maps \( \rho_u |_{L_s} \) and \( \rho_v |_{L_t} \) are inverses of one another.

Koch & Wallace [8] formulated a sufficient condition for \( d \) - and \( j \) -relations to agree with one another. A semigroup \( S \) is said to be stable if

1. \( s \sim_l ts \) if and only if \( s \sim_j ts \),
2. \( s \sim_r st \) if and only if \( s \sim_j st \)
for any \( s, t \in S \). This ensures that \( D_s = J_s \) for every \( s \in S \). In particular, finite semigroups, commutative semigroups, and compact semigroups are stable. For stable semigroups, Lemma 3.3 implies that \( l \)-classes contained in the same \( j \)-class have identical cardinality. The same is true of \( r \) - and \( h \)-classes.

We say \( s \in S \) is regular, in the sense of von Neumann, if there exists \( t \in S \) such that \( sts = s \). If, in addition, \( tst = t \), \( t \) is an inverse of \( s \). A regular element always has an inverse, and so \( s \) is regular if and only if \( s \) has an inverse. We call \( S \) a regular semigroup if each of its elements are regular. If every element has a unique inverse, then \( S \) is an inverse semigroup.

Definition 3.4. Given sets \( \Lambda \) and \( \Gamma \), a \( \Lambda \times \Gamma \) Rees matrix over a group \( G \) is a map \((u_{\lambda \rho}): \Lambda \times \Gamma \to G\). A Rees semigroup of matrix type is a set

\[ M(G, \Gamma, \Lambda, (u_{\lambda \rho})) = \{(\rho, g, \lambda) \mid g \in G, \rho \in \Gamma, \lambda \in \Lambda\} \]

endowed with a product defined by the rule

\[ (\rho, g, \lambda)(\gamma, h, \alpha) = (\rho, gu_{\lambda \gamma} h, \alpha). \]

We call \( G \) the structure group of \( M(G, \Gamma, \Lambda, (u_{\lambda \rho})) \).

It is easy to see that \( M(G, \Gamma, \Lambda, (u_{\lambda \rho})) \) is indeed a semigroup. By convention, we write

\[ M^0(G, \Gamma, \Lambda, (u_{\lambda \rho})) = M(G^0, \Gamma, \Lambda, (u_{\lambda \rho})). \]

Moreover, \((u_{\lambda \rho})\) is called regular if every row and column has a nonzero entry, which is the same as saying \( M^0(G, \Gamma, \Lambda, (u_{\lambda \rho})) \) is regular as a semigroup.

Suppose \( 0 \in S \) and \( S^0 \neq 0 \). Then \( S \) said to be 0-simple if it does not contain a nonzero proper ideal. It is easy to see that if \( 0 \notin S \), then \( S \) is simple if and only if \( S^0 \) is 0-simple. Under the stability assumption, Rees [17] classified 0-simple semigroups in terms of Rees matrices.

Theorem 3.5 (Rees). A stable semigroup \( S \) is 0-simple if and only if

\[ S \cong M^0(G, \Gamma, \Lambda, (u_{\lambda \rho})) \]

such that \( G \) is a group and \((u_{\lambda \rho})\) is regular.
Assume $S$ is stable. If $s \in S$ is regular, then every element of $J_s$ is regular. Moreover, there exists an idempotent $e \in J_s$ such that $H_e$ is a maximal subgroup of $S$ with $e$ as identity, and $H_e \cong H_f$ for any idempotent $f \in J_s$.

For every $s \in S$, set $I(s) = J(s) - J_s$. Then $I(s)$ is an ideal of $J(s)$ unless it is empty. The principal factor of $S$ at $s$ is the semigroup

$$J^0_s = \begin{cases} J(s)/I(s) & \text{if } J_s \text{ is not the minimal ideal}, \\ J_s \cup 0 & \text{otherwise}. \end{cases}$$

Alternatively, we can think of $J^0_s$ as the set $J_s \cup 0$ endowed with a product given by the rule

$$tu = \begin{cases} tu & \text{if } tu \in J_s, \\ 0 & \text{otherwise}. \end{cases}$$

If $S$ is stable, $J_s$ is regular if and only if $J^0_s$ is 0-simple, in which case, by Theorem 3.5, there is an isomorphism $J^0_s \to \mathcal{M}^0(G, \Gamma, \Lambda, (u_{\lambda \rho}))$. If $J_s$ is nonregular, then $J^0_s$ is a null semigroup in which $tu = 0$ for all $t, u \in J_s$.

### 3.2 Local Structure of Transition Semigroups

Any matrix over $\mathbb{R}$ is said to be stochastic if all entries are nonnegative and each row sums to unity. We write $S(n, \mathbb{R})$ for the monoid of $n \times n$ stochastic matrices over $\mathbb{R}$. A stochastic matrix is bistochastic if each column sums to unity. The submonoid of bistochastic matrices in $S(n, \mathbb{R})$ is denoted $B(n, \mathbb{R})$. We can also define a stochastic matrix over any proper unitary subring of $\mathbb{R}$. In particular, $S(n, \mathbb{Z})$ is the monoid of maps $n \to n$ and $B(n, \mathbb{Z})$ is the group of permutations on $n$.

We associate with each $s \in S$ a matrix $(s_{xy}) : X \times X \to [0, 1]$ with $(x, y) \mapsto \delta^y_{xs}$, where $\delta^y_x$ is the Kronecker delta on $X \times X$. Clearly, $(s_{xy})$ is row monomial, and hence

$$(\mu_{xy}) = \sum_{s \in S} \mu(s) \cdot (s_{xy})$$

is stochastic for any $\mu \in \mathbb{P}S$. It is readily verified that

$$(\mu * \nu)_{xy} = (\mu_{xy})(\nu_{xy}).$$

For any finite semigroup $S$, $\mathbb{P}S$ is isomorphic to a subsemigroup of $\mathbb{F}F_n \cong S(n, \mathbb{R})$, and so we first study Green’s relations on $S(n, \mathbb{R})$. Schwarz [22] showed that every maximal subgroup is isomorphic to a symmetric group $S_k$ for some $1 \leq k \leq n$. Wall [23] characterized $t$- and $r$-relations for regular elements of $S(n, \mathbb{R})$. Green’s relations on $B(n, \mathbb{R})$ were resolved by Montague & Plemmons [12].

Let $(s_{ij}) \in S(n, \mathbb{R})$. In block matrix form, 0 and 1, respectively, stand for the zero and identity matrices of suitable size. There exists $(p_{ij}) \in B(n, \mathbb{Z})$ such that

$$(p_{ij})(s_{ij}) = \begin{pmatrix} s^0_{ij} \\ s^1_{ij} \end{pmatrix}.$$
where rows of $s_0^t$ are linearly independent vectors that generate the same convex cone as rows of $(s_{ij})$. A row echelon form of $(s_{ij})$ is any matrix of the form
\[
\begin{pmatrix}
1 & 0 \\
u & 0
\end{pmatrix}(p_{ij})(s_{ij}),
\]
where $u$ is stochastic. We call $s_0^t$ a reduced row echelon form of $(s_{ij})$, which is unique up to row permutation. A pair of elements of $S(n, \mathbb{R})$ is row equivalent if they have identical reduced row echelon form up to row permutation.

If $(s_{ij})$ has a pair of nonzero columns in the same direction, then they appear as the first two columns of $(s_{ij})(p_{ij})$ for some $(p_{ij}) \in B(n, \mathbb{Z})$. Their sum, whose direction remains unchanged, is the first column of
\[
(s_{ij})(p_{ij})\begin{pmatrix}e & 0 \\0 & 1\end{pmatrix},
\]
where the leftmost entries of $e \in B(2, \mathbb{Z})$ are unity. We can repeat this process of adding up columns in the same direction until the matrix is in column echelon form
\[
(s_0 & s_1),
\]
where nonzero columns are pairwise in different directions and columns of $s_0$, which are linearly independent, generate the same convex cone as columns of $(s_{ij})$. The reduced column echelon form of $(s_{ij})$, which is unique up to column permutation, is obtained by removing any zero columns from $a_1$. When a pair of elements of $S(n, \mathbb{R})$ have identical reduced column echelon form up to column permutation, we say that they are column equivalent.

The echelon form of $(s_{ij})$ is the row echelon form of the column echelon form of $(s_{ij})$. This is the same as the column echelon form of the row echelon form of $(s_{ij})$ as matrix multiplication is associative. If the reduced echelon form is defined accordingly, then it is unique up to row and column permutations. A pair of elements of $S(n, \mathbb{R})$ is called equivalent if they have identical reduced echelon form up to row and column permutations.

**Proposition 3.6.** If $(s_{ij}), (t_{ij}) \in S(n, \mathbb{R})$, then

1. $(s_{ij}) \sim_l (t_{ij})$ if and only if $(s_{ij})$ and $(t_{ij})$ are row equivalent,
2. $(s_{ij}) \sim_r (t_{ij})$ if and only if $(s_{ij})$ and $(t_{ij})$ are column equivalent,
3. $(s_{ij}) \sim_e (t_{ij})$ if and only if $(s_{ij})$ and $(t_{ij})$ are equivalent,
4. $(s_{ij}) \sim_h (t_{ij})$ if and only if $(s_{ij})$ and $(t_{ij})$ are row and column equivalent.

**Proof.** (1) Suppose $(s_{ij}) \sim_l (t_{ij})$. Then the rows of $(s_{ij})$ and $(t_{ij})$ generate the same convex cone, and so they must be row equivalent.

Conversely, if $(s_{ij})$ and $(t_{ij})$ are row equivalent, then there exists $(p_{ij}), (q_{ij}) \in B(n, \mathbb{Z})$ such that
\[
(p_{ij})(s_{ij}) = \begin{pmatrix}s_0^t \\
s_1^t\end{pmatrix} \quad \text{and} \quad (q_{ij})(t_{ij}) = \begin{pmatrix}t_0^t \\
t_1^t\end{pmatrix}.
\]
are in row echelon form with $rs_0^t = t_0^t$ for some permutation $r$. Moreover, every row of $t_1^t$ is contained in the convex hull generated by the rows of $s_0^t$, so that we can find $u$ that is stochastic and satisfies $us_0^t = t_1^t$. Similarly, $vs_0^t = s_1^t$, where $v$ is stochastic. Therefore

$$
(q_{ij})^t \begin{pmatrix} r & 0 \\ u & 0 \end{pmatrix} (p_{ij})(s_{ij}) = (t_{ij}) \quad \text{and} \quad (p_{ij})^t \begin{pmatrix} r^t & 0 \\ v & 0 \end{pmatrix} (q_{ij})(t_{ij}) = (s_{ij}),
$$

and so we are done.

(2) If the first two columns of $(s_{ij})(p_{ij})$ are in the same direction, then for any $u \in S(2, \mathbb{R})$ of rank one, we can always find $v \in S(2, \mathbb{R})$ of rank one such that

$$
(s_{ij})(p_{ij}) \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} = (s_{ij})(p_{ij}).
$$

This shows that $(s_{ij})$ and its column echelon form are $r$-related.

Let $(s_{ij}) \sim_r (t_{ij})$. We can assume $(s_{ij})$ and $(t_{ij})$ are in column echelon form. Then there exist $(u_{ij}), (v_{ij}) \in S(n, \mathbb{R})$ such that

$$
(s_0, s_1) = (t_0, t_1) \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \quad \text{and} \quad (t_0, t_1) = (s_0, s_1) \begin{pmatrix} v_{00} & v_{01} \\ v_{10} & v_{11} \end{pmatrix}.
$$

We can now write

$$
s_0 = t_0 u_{00} + t_1 u_{10}.
$$

Columns of $s_0$ generate the same convex cone as those of $t_0$, and hence $s_0 = t_0 dp$, where $d$ is diagonal and $p$ a permutation. Furthermore, columns of $t_1$ are properly contained in the convex cone generated by those of $t_0$, so that $t_1 = t_0 w$ for some $w$ that has at least two positive entries in every column. This implies that $u_{10} = 0$, whence $t_0(dp - u_{00}) = 0$. As columns of $t_0$ are linearly independent, it follows that $u_{00} = dp$. By a similar reasoning for

$$
t_0 = s_0 v_{00} + s_1 v_{10},
$$

we can deduce that $v_{00} = p^d d^{-1}$ and $v_{10} = 0$. This shows $d = 1$, or else $(u_{ij})$ or $(v_{ij})$ fails to be stochastic. It is immediate that $u_{01} = v_{01} = 0$, and so $s_1 = t_1 u_{11}$ and $t_1 = s_1 v_{11}$. If nonzero columns of $s_1$ and $t_1$ are linearly independent, we are done. Otherwise, we can repeat this argument for $s_1$ and $t_1$. This process ends in finite steps, and thus the result follows.

(3) By stability, $(s_{ij}) \sim_r (t_{ij})$ if and only if there exists $(u_{ij}) \in S(n, \mathbb{R})$ such that $(s_{ij}) \sim_r (u_{ij})$ and $(u_{ij}) \sim_r (t_{ij})$, which is the same as saying the reduced column echelon form of the reduced row echelon form of $(s_{ij})$ is identical to the reduced column echelon form of the reduced row echelon form of $(t_{ij})$ up to row and column permutations.

(4) This is a direct consequence of (1) and (2).

Every compact semigroup contains an idempotent, so that $J_\mu$ is regular for some $\mu \in \mathbb{P} S$. Doob [3] identified all idempotent elements in $S(n, \mathbb{R})$.  

8
Theorem 3.7 (Doob). If \((e_{ij}) \in S(n, \mathbb{R})\) is of rank \(k\) with \(1 \leq k \leq n\), then \((e_{ij})\) is idempotent if and only if there exists \((p_{ij}) \in B(n, \mathbb{Z})\) such that
\[
(p_{ij})(e_{ij})(p_{ij})^t = \begin{pmatrix} e_{ij} & 0 \\ 0 & e_{ij} \end{pmatrix},
\]
where \(s\) is stochastic and \(e\) is of the form
\[
e = \begin{pmatrix} e_1 \\ \vdots \\ e_k \end{pmatrix}
\]
such that \(e_i\) is rank one and stochastic for \(1 \leq i \leq k\).

We can count the number of distinct regular \(j\)-classes in \(S(n, \mathbb{R})\) once it is known which idempotent elements belong to the same \(j\)-class.

Corollary 3.8. If \((e_{ij})\) and \((f_{ij})\) are idempotent in \(S(n, \mathbb{R})\), then \((e_{ij}) \sim_j (f_{ij})\) if and only if \(\text{rank}(e_{ij}) = \text{rank}(f_{ij})\).

Proof. Suppose \((e_{ij})\) is of rank \(k\). It follows from Theorem 3.7 that there exists \((p_{ij}) \in B(n, \mathbb{Z})\) such that the reduced echelon form of \((p_{ij})(e_{ij})(p_{ij})^t\) is an identity in \(S(k, \mathbb{Z})\). This completes the proof. \(\Box\)

It is immediate from Corollary 3.8 that there are \(n\) regular \(j\)-classes in \(S(n, \mathbb{R})\). In general, we cannot say that if \((e_{ij}) \sim_j (f_{ij})\) in \(S(n, \mathbb{R})\), then \((e_{ij}) \sim_j (f_{ij})\) in a proper subsemigroup of \(S(n, \mathbb{R})\). Consider, for example, the subsemigroup
\[
\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\}
\]
of \(S(3, \mathbb{R})\). It is true, however, that if \(t\) and \(u\) are regular in a subsemigroup \(T\) of \(S\), then \(t \sim_u u\) in \(T\) if and only if \(t \sim_u u\) in \(S\). Analogous statements hold for \(r\)- and \(h\)-relations.

Theorem 3.9. Suppose \((X, S, P)\) is a transition semigroup such that \(\varphi : PS \to T\) is an isomorphism, where \(n = |X|\) and \(T\) is a subsemigroup of \(S(n, \mathbb{R})\). For any idempotent \(e \in PS\), define \(\Lambda = \{ \lambda \in T \mid \lambda \sim\varphi e\varphi \}\) and \(\Gamma = \{ \rho \in T \mid \rho \sim\varphi e\varphi \}\). If \(G = H_{e\varphi}\), then
\[
J_\varphi^0 \cong M^0(G, \Gamma, \Lambda, (u_{\lambda\rho})),
\]
where \((u_{\lambda\rho}) : \Lambda \times \Gamma \to G^0\) is given by
\[
u_{\lambda\rho} = \begin{cases} \lambda\rho & \text{if } \lambda\rho \in G, \\ 0 & \text{otherwise}. \end{cases}
\]
Here, \((\rho, g, \lambda) = 0\) in \(M^0(G, \Gamma, \Lambda, (u_{\lambda\rho}))\) whenever \(g = 0\).

Proof. This follows directly from Theorem 3.5 and Proposition 3.6. \(\Box\)

Theorem 3.9 carries over to an instance \((X, S, P, Q)\) of \((X, S, P)\) since \(Q'\) is compact, and hence stable.
4 Global Structure of Probabilistic Automata

4.1 Krohn-Rhodes Theory

A pair of transformation semigroups \((X, S)\) and \((Y, T)\) are said to be isomorphic, written \((X, S) \cong (Y, T)\), if there exists a bijective map \(\varphi : Y \rightarrow X\) such that

1. \(\varphi s \varphi^{-1} \in T\) for all \(s \in S\),
2. \(\varphi^{-1} t \varphi \in S\) for all \(t \in T\).

It is easy to see that this implies \(S\) is isomorphic to \(T\).

**Definition 4.1.** Let \((X, S)\) and \((Y, T)\) be transformation semigroups. If there exists a surjective partial map \(\varphi : Y \rightarrow X\) such that for every \(s \in S\), \(\varphi s = t \varphi\) for some \(t \in T\), so that the diagram

\[
\begin{array}{ccc}
Y & \xrightarrow{t} & Y \\
\downarrow \varphi & & \downarrow \varphi \\
X & \xrightarrow{s} & X
\end{array}
\]

commutes, then \((X, S)\) is said to divide \((Y, T)\) by \(\varphi\). We write

\((X, S) \prec (Y, T)\)

to mean \((X, S)\) is a divisor of \((Y, T)\), and refer to \(\varphi\) as a covering.

If \(T\) is not a monoid, a homomorphism \(\varphi : T \rightarrow S\) has a natural extension \(\varphi^1 : T^1 \rightarrow S^1\) given by

\[
t \varphi^1 = \begin{cases} 1 & \text{if } t = 1, \\ t \varphi & \text{otherwise.} \end{cases}
\]

In case \(T\) is a monoid, set \(\varphi^1 = \varphi\). We often identify \(S\) with the transformation semigroup \((S^1, S)\), and say that \(T\) covers \(S\) when there is a covering \(\varphi^1\), so that \(T\) covers \(S\) as transformation semigroups.

If \(x \in X\), \(\bar{x}\) stands for the constant map \(X \rightarrow X\) onto \(x\). The semigroup of all such maps is denoted \(\bar{X}\). The **closure** of \((X, S)\) is the transformation semigroup

\[
\overline{(X, S)} = (X, S \cup \bar{X}).
\]

As the empty set is vacuously a semigroup, \(X\) can be identified with the transformation semigroup \((X, \emptyset)\), in which case \(\bar{X} = (X, \bar{X})\). In addition, we associate to \((X, S)\) the transformation monoid

\[
(X, S)^1 = (X, S \cup 1_X),
\]

which means \(S^1 = (S^1, S^1)\).
Definition 4.2. Let \((X, S)\) and \((Y, T)\) be transformation semigroups. Suppose that the action of \(t \in T\) on \(f \in S^Y\) is given by \(ytf = ytf\) for any \(y \in Y\). Then the wreath product of \((X, S)\) by \((Y, T)\) is the transformation semigroup
\[
(X, S) \wr (Y, T) = (X \times Y, S^Y \rtimes T),
\]
where \((x, y)(f, t) = (x(yf), yt)\) for any \((x, y) \in X \times Y\) and \((f, t) \in S^Y \rtimes T\).

Let \(\text{TSGp}\) denote the category in which objects are transformation semigroups and morphisms are coverings of objects. Evidently, \((X, S) \cong (Y, T)\) if and only if \((X, S) \prec (Y, T)\) and \((Y, T) \prec (X, S)\), whence \(\prec\) is a partial order on \(\text{TSGp}\). In Definition 4.2, it is routine to check that \(S^Y \rtimes T\) is a semigroup acting faithfully on \(X \times Y\). It follows that isomorphism classes of \(\text{TSGp}\) form a monoid under the binary operation \(\wr\) with unity \(1^1\). A decomposition of \((X, S)\) is an inequality in \(\text{TSGp}\) of the form
\[
(X, S) \prec (X_1, S_1) \wr \cdots \wr (X_n, S_n)
\]
such that either \(X_i\) is strictly smaller than \(X\) or \(S_i\) is strictly smaller than \(S\) for all \(1 \leq i \leq n\).

Proposition 4.3. Let \((X, S)\) be a transformation semigroup.
(1) If \(G\) is a maximal subgroup of \(S\), then
\[
(X, S) \prec (X, S \setminus G)^1 \wr G.
\]
(2) If \(S = I \cup T\), where \(I\) is a left ideal in \(S\) and \(T\) a subsemigroup of \(S\), then
\[
(X, S) \prec (X, I)^1 \wr (T \cup 1_X, T).
\]

Every finite group admits a composition series, which determines a unique collection of simple group divisors. Jordan-Hölder decomposition accounts for all simple group divisors.

Theorem 4.4 (Jordan-Hölder). If \(G\) is a finite group, then
\[
G \prec G_1 \wr \cdots \wr G_n,
\]
where \(G_i\) is a simple group divisor of \(G\) for \(1 \leq i \leq n\).

By Proposition 4.3, we can view Theorem 4.4 as a decomposition for transformation groups. Krohn-Rhodes decomposition generalizes Jordan-Hölder decomposition to transformation semigroups. Krohn and Rhodes [10] first showed that a finite semigroup is either cyclic, left simple, or the union of a proper left ideal and a proper subsemigroup, and then argued inductively by showing that any transformation semigroup admits a decomposition in \(\text{TSGp}\).

Theorem 4.5 (Krohn-Rhodes). If \((X, S)\) is a transformation semigroup, then
\[
(X, S) \prec (X_1, S_1) \wr \cdots \wr (X_n, S_n),
\]
where either \((X_i, S_i) = \mathbf{T}^1\) or \((X_i, S_i)\) is a simple group divisor of \(S\) for \(1 \leq i \leq n\).

In \(\text{FSgp}\), we say \(S\) is prime if \(S \prec T \rtimes U\) implies that either \(S \prec T\) or \(S \prec U\). The prime semigroups are precisely the divisors of \(\mathbf{T}^1\) and the finite simple groups. The decomposition of Theorem 4.5 is called the prime decomposition.
4.2 Global Structure of Transition Semigroups

Let $X$ and $Y$ be finite sets. If $\varphi : Y \to X$ is a partial map, we define its extension to be a partial map $P\varphi : PY \to PX$ given by

$$
\pi(P\varphi) = \begin{cases}
\sum_{x \in X} \sum_{y \varphi = x} \pi(y)x & \text{if } y\varphi \neq \emptyset \text{ whenever } \pi(y) > 0, \\
\emptyset & \text{otherwise}
\end{cases}
$$

for any $\pi \in PY$.

**Definition 4.6.** Let $(X,S,P)$ and $(Y,T,P)$ be transition semigroups. If there exists a surjective partial map $\varphi : Y \to X$ with extension $P\varphi : PY \to PX$ such that for every $\mu \in PS$, $(P\varphi)\mu = \nu(P\varphi)$ for some $\nu \in PT$, so that the diagram

$$
\begin{array}{ccc}
PY & \xrightarrow{\nu} & PY \\
P\varphi \downarrow & & \downarrow P\varphi \\
PX & \xrightarrow{\mu} & PX
\end{array}
$$

commutes, then $(X,S,P)$ is said to divide $(Y,T,P)$ by $P\varphi$. We write

$$(X,S,P) \prec (Y,T,P)$$

to mean $(X,S,P)$ is a divisor of $(Y,T,P)$, and refer to $\varphi$ as a covering.

Notation for transformation semigroups naturally carry over to transition semigroups. Therefore

$$(X,S,P) = (X,S \cup \bar{X},P) \text{ and } (X,S,P)^{1} = (X,S \cup 1_{X},P).$$

We also identify $(X,P)$ with $(X,\emptyset,P)$ and $(S,P)$ with $(S^{1},S,P)$.

**Lemma 4.7.** If $(X,S,P)$ and $(Y,T,P)$ are transition semigroups, then $(X,S,P)$ divides $(Y,T,P)$ if and only if $(X,S)$ divides $(Y,T)$.

**Proof.** Suppose $(X,S,P)$ divides $(Y,T,P)$ by $P\varphi$. Fix $s \in S$. Then $(P\varphi)s = \nu(P\varphi)$ for some $\nu \in PY$. This means

$$y\varphi s = \sum_{t \in T} \nu(t)yt\varphi$$

for any $y \in Y$ such that $y\varphi \neq \emptyset$. We conclude $\varphi s = t\varphi$ for some $t \in T$ with $\nu(t) > 0$.

Conversely, assume $(X,S)$ divides $(Y,T)$ by $\varphi$. Given $\mu \in PS$, choose $t \in T$ such that $\varphi s = t\varphi$ for every $s \in S$ with $\mu(s) > 0$. Let $U \subset T$ be the collection of all such selections. Define $\nu \in PT$ by

$$
\nu(t) = \begin{cases}
\sum_{\varphi s = t\varphi} \mu(s) & \text{if } t \in U, \\
0 & \text{otherwise}.
\end{cases}
$$

12
Then we can write
\[ \pi(\mathcal{P}_\varphi)\mu = \sum_{x \in X} \sum_{y: y \varphi = x} \pi(y)\mu(s)x = \sum_{x \in X} \sum_{y: y \varphi = x} \pi(y)\nu(t)x = \pi\nu(\mathcal{P}_\varphi), \]
where \( \pi \in \mathcal{P}Y \).

To extend Definition 4.2 to transition semigroups, we take the wreath product of \((X, S)\) by \((Y, T)\), and consider the right action of \(\mathcal{P}(S^Y \times T)\) on \(\mathcal{P}(X \times Y)\).

**Definition 4.8.** Let \((X, S, \mathcal{P})\) and \((Y, T, \mathcal{P})\) be transition semigroups. The wreath product of \((X, S, \mathcal{P})\) by \((Y, T, \mathcal{P})\) is the transition semigroup
\[ (X, S, \mathcal{P}) \wr (Y, T, \mathcal{P}) = (Z, U, \mathcal{P}), \]
where \((Z, U) = (X, S) \wr (Y, T)\).

It is clear that \((Z, U, \mathcal{P})\) is well-defined since \((X, S) \wr (Y, T)\) is a transformation semigroup in its own right.

**Theorem 4.9.** If \((X, S, \mathcal{P})\) is a transition semigroup, then
\[ (X, S, \mathcal{P}) \preceq (X_1, S_{1}, \mathcal{P}) \wr \cdots \wr (X_n, S_n, \mathcal{P}), \]
where either \((X_i, S_i) \preceq \mathbb{2}\) or \((X_i, S_i)\) is a simple group divisor of \(S\) for \(1 \leq i \leq n\).

**Proof.** This is an immediate consequence of Theorem 4.5 and Lemma 4.7.

We define a transition semigroup \((X, S, \mathcal{P})\) to be prime if \((X, S)\) is prime as a transformation semigroup. Theorem 4.9 provides a way to classify any set of stochastic matrices. If \(T\) is any semigroup of \(S(n, \mathbb{R})\), then \(S = \text{supp}(T)\) is a set of row monomial binary matrices isomorphic to a subsemigroup of \(F_n\). Set \(n = X\). Then each matrix in \(T\) is an instance in \((X, S, \mathcal{P})\).

## 5 Representation Theory of Probabilistic Automata

### 5.1 Munn-Ponizovskii Theory

Let \(A\) be an associative algebra with unity. We denote by \(\text{Mod-}A\) the category of right \(A\)-modules. Put \(J = \text{Rad}(A)\). For any primitive idempotent \(e\) of \(A\), \(eJ\) is the unique maximal submodule of \(eA\) in \(\text{Mod-}A\). Assume further that \(A\) is noetherian or artinian. This ensures that there exists a collection of pairwise orthogonal central idempotents \(e_1, \cdots, e_n \in A\) such that \(1_A = e_1 + \cdots + e_n\), or equivalently,
\[ A_A = e_1A \oplus \cdots \oplus e_nA. \]
Moreover, $M \in \text{Mod}-A$ is simple if and only if $M \cong e_i A/e_i J$ for some $1 \leq i \leq n$, and hence there is a one-to-one correspondence between isomorphism classes of irreducible modules and that of principal indecomposable modules.

For any idempotent $e$ of $A$, set $B = eAe$. Then $B$ is a subalgebra of $A$. We define restriction as the covariant functor $\text{Res}_B^A : \text{Mod}-A \to \text{Mod}-B$ given by

$$\text{Res}_B^A(M) = Me$$

and induction as its left adjoint functor $\text{Ind}_B^A : \text{Mod}-B \to \text{Mod}-A$ given by

$$\text{Ind}_B^A(M) = M \otimes_B eA.$$

Then $\text{Res}_B^A$ is exact and $\text{Ind}_B^A$ is left exact.

**Theorem 5.1** (Green). Let $e \neq 0$ be an idempotent of an associative algebra $A$.

1. If $M \in \text{Mod}-A$ is simple, then $\text{Res}_{eAe}^A(M) \in \text{Mod}-eAe$ is either trivial or simple.

2. If $N \in \text{Mod}-eAe$ is simple, then the quotient of $\text{Ind}_{eAe}^A(N)$ by its unique maximal submodule

$$\left\{ m \in \text{Ind}_{eAe}^A(N) \mid mAe = 0 \right\}$$

is the unique simple $M \in \text{Mod}-A$ such that $\text{Res}_{eAe}^A(M) = N$.

Consequently, there is a one-to-one correspondence between simple $A$-modules that are not annihilated by $e$ and simple $B$-modules.

Around the same time, Munn [14] & Ponizovski˘ı [15] independently furthered the work of Clifford [1] by characterizing irreducible representations of a finite semigroup by those of its principal factors. Lallement & Petrich [11], and later Rhodes & Zalcstein [19], provided a precise construction based on Theorem 3.5. We closely follow the arguments of Ganyushkin, Mazorchuk & Steinberg [5] in which the same results are recovered by virtue of Theorem 5.1.

Let $S$ be a finite semigroup. For a field $K$, $KS$ is artinian, so that the notions of semisimplicity and semiprimitivity coincide. It is evident that $KS$ need not be semisimple. Consider, for instance, $K\bar{X}$ for any finite set $X$. For $M \in \text{Mod}-KS$, we denote by $\text{Ann}_S(M)$ the ideal of $S$ consisting of elements that annihilate $M$.

**Definition 5.2.** Let $M \in \text{Mod}-KS$, where $K$ is a field and $S$ a finite semigroup. If $e$ is an idempotent of $S$ satisfying

$$\text{Ann}_S(M) = \{ s \in S \mid J_e \subset J(s) \},$$

then $J_e$ is said to be the apex of $M$.

Suppose $M \in \text{Mod}-KS$ is simple. Then there exists a unique apex $J_e$ of $M$. Set $I = \text{Ann}_S(M)$. We identify $M$ with the unique simple $N \in \text{Mod}-KS/KI$ such that $Ne \neq 0$. By Proposition 3.2,

$$e(KS/KI)e \cong K(eSe)/K(eIe) \cong KH_e.$$
Let $E(S)$ be a collection of idempotent class representatives of regular $j$-classes of $S$. We also write $\text{Res}_{H_e}^S(M)$ and $\text{Ind}_{H_e}^S(M)$, respectively, to mean the restriction and induction functors.

**Theorem 5.3** (Munn-Ponizovski˘ı). Let $K$ be a field. Suppose $e \in E(S)$, where $S$ is a finite semigroup.

1. If $M \in \text{Mod-}KS$ is simple with apex $J_e$, then $\text{Res}_{H_e}^S(M) \in \text{Mod-}KH_e$ is simple.
2. If $N \in \text{Mod-}KH_e$ is simple, then the quotient of $\text{Ind}_{H_e}^S(N)$ by its unique maximal submodule
   \[ \left\{ m \in \text{Ind}_{H_e}^S(N) \mid mKSe = 0 \right\} \]
   is the unique simple $M \in \text{Mod-}KS$ with apex $J_e$ such that $\text{Res}_{H_e}^S(M) = N$.

Consequently, there is a one-to-one correspondence between irreducible representations of $S$ and those of $H_e$ for $e \in E(S)$.

Again, by Proposition 3.2, we know $e(KS/KI) \cong R_e$, from which it follows that
\[ \text{Ind}_{H_e}^S(N) \cong N \otimes_{KH_e} KR_e \]
for any $N \in \text{Mod-}KH_e$, where $e \in E(S)$.

Schützenberger [20, 21] studied the action of $S$ on $L_s$ and $R_s$ for any $s \in S$. First define $\Lambda(H_s)$ to be the quotient of the right action of the monoid
\[ \{ u \in S^1 \mid uH_s \subset H_s \} \]
on $H_s$ by its kernel. Then $\Lambda(H_s)$ is isomorphic to the group of all maps of the form $\lambda_u|_{H_s} : H_s \to H_s$, and acts freely on $R_s$ from the left. We call $\Lambda(H_s)$ the left Schützenberger group of $H_s$. Its orbit space $\Lambda(H_s) \backslash R_s$ consists of $h$-classes in $R_s$. Moreover, $\Lambda(H_s) \cong \Lambda(H_t)$ if $s \sim t$. A dual statement holds for the right Schützenberger group $\Gamma(H_s)$. In particular, $\Lambda(H_s) \cong \Gamma(H_s)_{\text{op}}$.

Suppose $\Lambda(H_s) \backslash R_s$ consists of $n$ number of $h$-classes. Choose a class representative for each $h$-class, so that we can write
\[ \Lambda(H_s) \backslash R_s = \{ H_{s_1}, \ldots, H_{s_n} \}. \]
Let $1 \leq i \leq n$. Given $t \in S$, if $s_i t \in R_s$, then $s_i t \in H_{s_i}$ for some $1 \leq j \leq n$, and so there exists $h \in \Lambda(H_s)$ such that $s_i t = h s_j$. The right Schützenberger representation is a map $\rho : S \to M_n(\Lambda(H_s))$ defined by
\[ \rho(t)_{ij} = \begin{cases} h & \text{if } s_i t = h s_j, \\ 0 & \text{otherwise.} \end{cases} \]
The dual construction leads to the left Schützenberger representation $\lambda : S \to M_n(\Gamma(H_s))$. 15
5.2 Holonomy Decomposition

The original proof of Theorem 4.5 by Krohn & Rhodes [10] is purely algebraic. Based on the work of Zeiger [24, 25], Eilenberg [4] devised a decomposition that retains the combinatorial structure of a transformation semigroup.

Let \((X, S)\) be a transformation semigroup. We can extend the action of \(S\) on \(X\) to \(S^1\) by requiring that \(x1 = x\) for any \(x \in X\). Set

\[
XS = \{xs \mid s \in S^1 \cup \bar{X}\} \cup \{\emptyset\}.
\]

Write \(a \leq b\) if \(a \subset bs\) for some \(s \in S^1\). Then the quasiorder \(\leq\) induces an equivalence relation \(\sim\) given by \(a \sim b\) if and only if \(a \leq b\) and \(b \leq a\). We write \(a < b\) to mean \(a \leq b\) and not \(b \leq a\). A height function is a map \(\eta : XS \to \mathbb{Z}\) satisfying

1. \(\eta(\emptyset) = -1,\)
2. \(\eta(x) = 0\) if \(x \in X,\)
3. \(a \sim b\) implies \(\eta(a) = \eta(b),\)
4. \(a < b\) implies \(\eta(a) < \eta(b),\)
5. \(\eta(a) = i\) for some \(a \in XS\) if \(0 \leq i \leq \eta(X).\)

The height of \((X, S)\), denoted \(\eta(X, S)\), is defined as \(\eta(X)\). We can always define a height function on \(XS\) by assigning \(\eta(a) = i\), where \(a_0 < \cdots < a_i\) is a maximal chain in \(XS\) such that \(a_0 \in X\) and \(a_i = a\).

Assume \(|a| > 1\) for \(a \in XS\). Consider the set \(X_a\) of all maximal proper subsets of \(a\) contained in \(XS\). We call an element of \(X_a\) a brick of \(a\). If \(s = a\), then \(X_a s = X_a\), so that \(s\) permutes \(X_a\). Let \(G_a\) denote the coimage of

\[
\{s \in S \mid as = s\} \to \text{Sym}(X_a).
\]

Clearly, \(G_a \acts S\). If \(G_a \neq \emptyset\), \((X_a, G_a)\) is a transformation group. Furthermore, \(a \sim b\) implies \((X_a, G_a) \cong (X_b, G_b)\). In case \(G_a = \emptyset\), put \(G_a = 1\).

Suppose \(\eta\) admits \(j\) elements, say \(a_1, \cdots, a_j\), of height \(k\) in \(XS/\sim\). Then we call \(X_k = X_{a_1} \times \cdots \times X_{a_j}\) the \(k\)th paving and \(G_k = G_{a_1} \times \cdots \times G_{a_j}\) the \(k\)th holonomy group. The \(k\)th holonomy is the transformation semigroup

\[
\text{Hol}_k(X, S) = (X_k, G_k).
\]

This is well-defined since \(G_k\) is independent of the choice of \(a_1, \cdots, a_j\) in \(XS/\sim\).

**Theorem 5.4** (Eilenberg). If \((X, S)\) is a transformation semigroup with a height function \(\eta : XS \to \mathbb{Z}\) such that \(\eta(X, S) = n\), then

\[
(X, S) \prec \text{Hol}_1(X, S) \prec \cdots \prec \text{Hol}_n(X, S),
\]

where \(\text{Hol}_i(X, S)\) is the \(i\)th holonomy for \(1 \leq i \leq n\).

The decomposition in Theorem 5.4 is known as the holonomy decomposition of \((X, S)\) induced by \(\eta\). For brevity, we write

\[
\text{Hol}_i(X, S) = \text{Hol}_1(X, S) \prec \cdots \prec \text{Hol}_n(X, S).
\]
Since \( \bar{n}^1 \) embeds in \( n \) direct copies of \( \bar{2}^1 \), applying Theorem 4.4 to Theorem 5.4 indeed leads to a prime decomposition of \((X, S)\). If \( \text{Hol}_e(X, S) = (Y, T) \), then \( T \) is called the holonomy monoid of \((X, S)\).

**Definition 5.5.** Let \((X, S)\) and \((Y, T)\) be transformation semigroups. If there exists a surjective relation \( \varphi : Y \to X \) such that for every \( s \in S \),

\[
\varphi s \subset t \varphi
\]

for some \( t \in T \), then \((Y, T)\) is said to cover \((X, S)\) by \( \varphi \). We write

\[
(X, S) \prec_{\text{rel}} (Y, T)
\]

to mean \((Y, T)\) is a cover of \((X, S)\), and refer to \( \varphi \) as a relational covering.

If \( Y \varphi \subset XS \), then the rank of \( \varphi \) is the smallest integer \( k \geq 0 \) such that \( \eta(y \varphi) \leq k \) for all \( y \in Y \). Note that \((X, S)\) divides \((Y, T)\) when \( \varphi \) is of rank 0.

**Sketch of proof of Theorem 5.4.** It suffices to show that if \( \varphi : Y \to X \) is of rank \( k \), then there exists a map \( \psi : X_k \times Y \to X \) of rank \( k - 1 \) such that

\[
(X, S) \prec_{\text{rel}} \text{Hol}_1(X, S) \wr (Y, T)
\]

by \( \psi \), for \( 1 \) covers \((X, S)\) by the unique relation \( 1 \to X \) of rank \( n \).

Let \( a_1, \ldots, a_j \) represent elements of height \( k \) in \( XS/\sim \). If \( \eta(y \varphi) = k \), then \( y \varphi \sim a_i \) for a unique \( 1 \leq i \leq j \), so that we can find \( u_y, v_y \in S \) such that

\[
a_i u_y = y \varphi \quad \text{and} \quad y \varphi v_y = a_i.
\]

Assume such a selection has been made for all \( y \in Y \) such that \( \eta(y \varphi) = k \). We write a projection map as \( \pi_i : (X_k, G_k) \to (X_{a_i}, G_{a_i}) \). Define \( \psi : X_k \times Y \to X \) by

\[
(b, y) \psi = \begin{cases} 
  y \varphi & \text{if } \eta(y \varphi) < k, \\
  b \pi_i u_y & \text{if } y \varphi \sim a_i.
\end{cases}
\]

It is easy to see that \( \psi \) is of rank \( k - 1 \) with \( \text{Im}(\psi) \subset XS \).

Fix \( s \in S \). It remains to prove that there exists \( (f, t) \in (G_k \cup \bar{X}_k)^Y \rtimes T \) such that the diagram

\[
\begin{array}{ccc}
X_k \times Y & \overset{(f, t)}{\longrightarrow} & X_k \times Y \\
\psi \downarrow & & \downarrow \psi \\
X & \overset{s}{\longrightarrow} & X
\end{array}
\]

is commutative.
commutes. Choose any \( t \in T \) satisfying \( \varphi s \subset t\varphi \). We can find a map \( f : Y \to G_k \cup \bar{X}_k \) such that if \( y\varphi \sim a_i \), then

\[
    f\pi_i = \begin{cases} 
        u_{ySV}y, & \text{if } y\varphi s = yt\varphi, \\
        b_i & \text{if } y\varphi s VT \subset b_i \text{ with } b_i \in X_n. 
    \end{cases}
\]

It is routine to check that \( \psi s \subset (f,t)\psi \). □

Given \( t \in T \), \( t_i \) denotes the \( i \)th component of \( t \). In particular, if \( 1 \leq i < n \), then \( t_i \) is a map \( X_{i+1} \times \cdots \times X_n \to G_i \cup X_i \). Suppose that if either

1. there exists \( (x_{k+1}, \ldots, x_n) \in X_{k+1} \times \cdots \times X_n \) such that \( (x_{k+1}, \ldots, x_n)t_k \in G_k \) for some \( 1 < k < n \),
2. \( t_n \in G_n \) with \( k = n \),

then \( (x_{i+1}, \ldots, x_n)t_i \in G_i \) for all \( 1 \leq i < k \). Then \( t \) is said to satisfy the Zeiger property.

**Lemma 5.6.** Suppose \((X,S)\) is a transformation semigroup with a height function \( \eta : X \times S \to \mathbb{Z} \) such that \( \eta(X,S) = n \), which admits a decomposition

\[
    \text{Hol}_n(X,S) = (Y,T).
\]

Then the set \( U \) of elements of \( T \) satisfying the Zeiger property forms a submonoid of \( T \) such that \((Y,U)\) covers \((X,S)\).

**Proof.** It is easy to see that \( U \) is indeed a monoid. Assume \((x_{k+1}, \ldots, x_n)t_k \in G_k \) for \( 1 < k < n \). By construction,

\[
    (x_k, \ldots, x_n)\varphi s = (x_k, \ldots, x_n)(t_k, \ldots, t_n)\varphi,
\]

where \( \varphi : X_k \times \cdots \times X_n \to X \) is a relation of rank \( k - 1 \) such that

\[
    (X,S) \prec_{rel} \text{Hol}_k(X,S) \smile \cdots \smile \text{Hol}_n(X,S)
\]

by \( \varphi \). If \( a_1, \ldots, a_j \) are elements of height \( k \) in \( X \times S/\sim \), then \( (x_{k+1}, \ldots, x_n)\varphi \sim a_i \)

for some \( 1 \leq i \leq j \). Define \( t_{k-1} : X_k \times \cdots \times X_n \to G_{k-1} \) by

\[
    (x_k, \ldots, x_n)t_{k-1}\pi_k = u_{(x_{k+1}, \ldots, x_n)}sv_{(x_{k+1}, \ldots, x_n)}.
\]

Put \( t_{k-1}\pi_i = 1_{G_{a_i}} \) for \( i \neq k \). The case when \( k = n \) is similar. □

A height function \( \eta \) uniquely determines \( U \), which is referred to as the reduced holonomy monoid of \((X,S)\). We also write

\[
    \tilde{\text{Hol}}_n(X,S) = (Y,U),
\]

and call \((Y,U)\) the reduced holonomy decomposition of \((X,S)\) induced by \( \eta \).
5.3 Representation Theory of Reduced Holonomy Monoid

Suppose a height function \( \eta : XS \to \mathbb{Z} \) on a transformation semigroup \((X, S)\) such that \( \eta(X, S) = n \) induces the reduced holonomy decomposition

\[
\text{Hol}_\ast(X, S) = (Y, U).
\]

We wish to study the representation theory of the transition monoid \((Y, U, \mathbb{P})\). Since \(\mathbb{P}U\) does not have an additive structure, we apply Theorem 5.3 to \(\mathbb{C}U\), and consider the inclusion \(\mathbb{P}U \hookrightarrow \mathbb{C}U\).

The depth function on \(U\) is a map \(\delta : U \to \mathbb{Z}\) such that for \(u \in U\), \(\delta(u) = k\) if there exists \(0 \leq k \leq m\) satisfying

1. \(\text{Im}(u_1) \cap G_i \neq \emptyset\) for \(1 \leq i \leq k\),
2. \(\text{Im}(u_1)\) is a singleton in \(X_i\) for \(k < i \leq n\),

and \(\delta(u) = -1\) otherwise. The depth of \((X, S)\) is the largest integer \(1 \leq m \leq n\) such that \(\delta(u) = m\) for some \(u \in U\). We refer to the pair \((m, n)\) as the dimension of \((X, S)\), and write \(\text{dim}(X, S) = (m, n)\).

**Proposition 5.7.** Let \((X, S)\) be a transformation semigroup with height function \(\eta : XS \to \mathbb{Z}\), which induces a reduced holonomy decomposition

\[
\text{Hol}_\ast(X, S) = (Y, U)
\]

such that \(\text{dim}(X, S) = (m, n)\). Then \(u \in U\) is regular if and only if \(\delta(u) = k\) for some \(0 \leq k \leq m\). Therefore \(e \in U\) such that \(\delta(e) = k\) is idempotent in \(U\) if and only if

1. \((x_{i+1}, \ldots, x_n)e_i = 1_{G_i}\) for \(1 \leq i \leq k\),
2. \(e_i = \bar{x}_i\) for \(k < i \leq n\) for some \((x_{k+1}, \ldots, x_n) \in X_{k+1} \times \cdots \times X_n\).

**Proof.** If \(u \in U\) is regular, there exists \(v \in U\) such that \(uvu = u\). Fix \(1 < k \leq n\). Suppose \(\text{Im}(u_{k-1}) \subset \bar{X}_{k-1}\) and \(\text{Im}(u_k)\) is a singleton in \(\bar{X}_k\) for \(k \leq i \leq n\). Then

\[
u_{k-1}^{-1}(u_k, \ldots, u_n)\nu_{k-1}^{-1}(u_k, \ldots, u_n) u_{k-1} = u_{k-1},
\]

and so \(\text{Im}(u_{k-1})\) is also a singleton in \(\bar{X}_{k-1}\).

Conversely, assume \(u \in U\) with \(\delta(u) = k\) for some \(1 \leq k \leq m\). This means \((x_{k+1}, \ldots, x_n)u_k \in G_k\) for some \((x_{k+1}, \ldots, x_n) \in X_{k+1} \times \cdots \times X_n\). We want to find \(v \in U\) such that \(uvu = u\). Set \(v_i = \bar{x}_i\) for \(k < i \leq n\). It follows from Lemma 5.6 that \((x_{i+1}, \ldots, x_n)u_i \in G_i\) when \(1 \leq i < k\). Therefore there exists \(v_i : X_{i+1} \times \cdots \times X_n \to G_i\) such that

\[
u_i^{-1}(v_{i+1}, \ldots, v_n) u_i = 1_{G_i}
\]

for \(1 \leq i \leq k\).

Given \(1 \leq k \leq m\), denote by \(H_k\) the group acting on \(X_1 \times \cdots \times X_k\) for the transformation group

\[
(X_1, G_1) \ast \cdots \ast (X_k, G_k).
\]
For fixed $y \in Y$, define

$$E(U, y) = \{ e \in U \mid e^2 = e \text{ and } e_i = \tilde{y}_i \text{ whenever } e_i \neq 1_{G_i} \text{ for } 1 \leq i \leq n \}.$$  

Then $E(U, y)$ contains exactly one idempotent of depth $k$ for each $1 \leq k \leq m$. We also write

$$Y_i = X_{i+1} \times \cdots \times X_n$$

for $0 \leq i \leq n$, so that $Y_0 = Y$ and $Y_n = \emptyset$. Then $H_k \times \tilde{Y}_k$ is a subsemigroup of $U$ containing $e \in E(U, y)$ such that $\delta(e) = k$.

**Proposition 5.8.** Let $(X, S)$ be a transformation semigroup with height function $\eta : XS \to \mathbb{Z}$, which induces a reduced holonomy decomposition

$$\text{Hol}_e(X, S) = (Y, U)$$

such that $\dim(X, S) = (m, n)$. Fix $y \in Y$. If $u, v \in U$ are regular with $\delta(u) = k$, then

1. $u \sim_T v$ if and only if $\delta(u) = \delta(v)$ and $u_i = v_i$ for every $k < i \leq n$,
2. $u \sim_T v$ if and only if $\delta(u) = \delta(v)$.

For $1 \leq k \leq m$, if $e \in E(U, y)$ such that $\delta(e) = k$, then

3. $R_e \cong H_k \times \tilde{Y}_k$,
4. $H_e \cong H_k$.

**Proof.** (1) If $u \sim_T v$, then it is necessary that $\delta(u) = \delta(v)$, and hence $u_i = v_i$ for $k < i \leq n$. Assume the converse. By Lemma 5.6 and Proposition 5.7, there is $(x_{k+1}, \cdots, x_n) \in X_{k+1} \times \cdots \times X_n$ such that $(x_{i+1}, \cdots, x_n) u_i \in G_i$ for $1 \leq i \leq k$. Therefore we can find $w \in U$ such that

$$w_i (w_{i+1}, \cdots, w_n) u_i = v_i$$

for $1 \leq i \leq k$ once we set $w_i = \tilde{x}_i$ for $k < i \leq n$. This shows that $wu = v$. By symmetry, we conclude that $u \sim_T v$.

(2) Again, $u \sim_T v$ implies that $\delta(u) = \delta(v)$. Conversely, if $\delta(u) = \delta(v)$, then $u \sim_T ue$ if $e \in U$ such that $\delta(e) = k$ is an idempotent defined by

$$e_i = \begin{cases} 1_{G_i} & \text{for } 1 \leq i \leq k, \\ v_i & \text{otherwise.} \end{cases}$$

It follows from (1) that $ue \sim_T v$.

(3) Assume $u \sim_T e$. By (2), $\delta(u) = k$, which means $u_i$ is a singleton in $\tilde{X}_i$ for $k < i \leq n$. Since $ev = u$ for some $v \in U$,

$$e_i (e_{i+1}, \cdots, e_n) v_i = u_i$$

for $1 \leq i \leq k$, which shows that $u_i$ does not depend on $X_{k+1} \times \cdots \times X_n$. Similarly, $uw = e$ for some $w \in U$, and hence

$$u_i (u_{i+1}, \cdots, u_n) w_i = e_i.$$

Whenever $1 \leq i \leq k$, $\text{Im}(u_i) \subset G_i$ since $e_i = 1_{G_i}$. Therefore we can conclude that $R_e \subset H_i \times \tilde{Y}_i$. The opposite inclusion is obvious.

(4) This is an immediate consequence of (1) and (3).
Proposition 5.8 implies that there are exactly $m$ regular $j$-classes in $U$ whose maximal subgroup is determined by the first $k$ holonomy groups. We can now apply this to Theorem 5.3 to determine all irreducible representations of $U$.

**Theorem 5.9.** Let $(X, S)$ be a transformation semigroup with height function \( \eta : XS \to \mathbb{Z} \), which induces a reduced holonomy decomposition

\[
\text{Hol}_\eta(X, S) = (Y, U)
\]

such that \( \text{dim}(X, S) = (m, n) \). Fix \( y \in Y \). If $K$ is a field, then $M_i \in \text{Mod-}KU$ satisfying

\[
M_i \cong M \otimes KH_i, K(H_i \times \bar{Y}_i),
\]

where $M \in \text{Mod-}KH_i$ is simple and $H_e \cong H_i$ for $e \in E(U, y)$ with $\delta(e) = i$ for $1 \leq i \leq m$, is principal indecomposable. Furthermore, $M_i$ contains a unique maximal submodule

\[
N_i = \{ m \in M_i \mid mKUe = 0 \},
\]

so that $M_i/N_i \in \text{Mod-}KU$ is simple.

**Proof.** It is easy to see that elements $m \otimes (1_{H_i}, \bar{z})$, where $m$ is a basis of $M$ and $z \in Y_i$, form a basis of $M_i$. For any $(h, \bar{z}) \in H_i \times \bar{Y}_i$, we can write

\[
m \otimes (h, \bar{z}) = m(h, \bar{y}_i) \otimes (1, \bar{z}).
\]

This implies that $M_i$ is indecomposable. Since $M_i$ is free, it is projective, and hence principal indecomposable. The result follows from Theorem 5.3. \(\square\)

It follows from Theorem 5.3 that modules of the form $M_i/N_i$ induced by a simple right $KH_e$-module $M$, where $H_e \cong H_i$ for some $e \in E(U, y)$, account for all simple right $KU$-modules.

**References**

1. A. H. Clifford, *Matrix representations of completely simple semigroups*, Amer. J. Math. 64, (1942), 327-342.

2. A. H. Clifford, G. B. Preston, *The algebraic theory of semigroups*, vol. I, Mathematical Surveys, no. 7, American Mathematical Society, Providence, RI, 1961.

3. J. L. Doob, *Topics in the theory of Markoff chains*, Trans. Amer. Math. Soc. 52 (1942), 37-64.

4. S. Eilenberg, *Automata, languages, and machines*, vol. B, Pure and Applied Mathematics, vol. 59, Academic Press, New York, 1976.

5. O. Ganyushkin, V. Mazorchuk, B. Steinberg, *On the irreducible representations of a finite semigroup*, Proc. Amer. Math. Soc. 137 (2009), no. 11, 3585-3592.
[6] J. A. Green, *On the structure of semigroups*, Ann. of Math. (2) **54** (1951), 163-172.

[7] ______, *Polynomial representations of $GL_n$*, Lecture Notes in Mathematics, 830, Springer-Verlag, Berlin, 1980.

[8] R. J. Koch, A. D. Wallace, *Stability in semigroups*, Duke Math. J. **24** (1957), 193-195.

[9] K. Henckell, S. Lazarus, J. Rhodes, *Prime decomposition theorem for arbitrary semigroups: general holonomy decomposition and synthesis theorem*, J. Pure Appl. Algebra **55** (1988), no. 1-2, 127-172.

[10] K. Krohn, J. Rhodes, *Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines*, Trans. Amer. Math. Soc. **116** (1965) 450-464.

[11] G. Lallement, M. Petrich, *Irreducible matrix representations of finite semigroups*, Trans. Amer. Math. Soc. **139** (1969), 393-412.

[12] J. S. Montague, R. J. Plemmons, *Doubly stochastic matrix equations*, Israel J. Math. **15** (1973), 216-229.

[13] W. D. Munn, *On semigroup algebras*, Proc. Cambridge Philos. Soc. **51** (1955), 1-15.

[14] ______, *Matrix representations of semigroups*, Proc. Cambidges Philos. Soc. **53** (1957), 5-12.

[15] I. S. Ponizovski˘ı, *On matrix representations of associative systems*, Mat. Sb. (N.S.) **38**(80) (1956), 241-260 (Russian).

[16] M. O. Rabin, *Probabilistic Automata*, Information and Control **6** (1963), 230-245.

[17] D. Rees, *On semi-groups*, Proc. Cambridge Philos. Soc. **36** (1940), 387-400.

[18] J. Rhodes, B. Steinberg, *The q-theory of finite semigroups*, Springer Monographs in Mathematics, Springer, New York, 2009.

[19] J. Rhodes, Y. Zalcstein, *Elementary representation and character theory of finite semigroups and its application*, In J. Rhodes, ed., *Monoids and semigroups with applications (Berkeley, CA, 1989)*, 334-367, World Sci. Publ., River Edge, NJ, 1991.

[20] M. P. Schützenberger, *Sur la représentation monomiale des demi-groupes*, C. R. Acad. Sci. Paris **246** (1958), 865-867 (French).

[21] ______, *Dé représentation des demi-groupes*, C. R. Acad. Sci. Paris **244** (1957), 1994-1996 (French).
[22] Š. Schwarz, *On the structure of the semigroup of stochastic matrices*, Magyar Tud. Akad. Mat. Kutató Int. Közl. 9 (1964), 297-311.

[23] J. R. Wall, *Green’s relations for stochastic matrices*, Czechoslovak Math. J. 25(100) (1975), 247-260.

[24] H. P. Zeiger, *Cascade synthesis of finite state machines*, Information and Control 10 (1967), 419-433.

[25] ______, *Yet another proof of the cascade decomposition theorem for finite automata*, Math. Systems Theory 1 (1967), 225-228.