HOLONOMY THEOREM FOR FINITE SEMIGROUPS

JOHN RHODES, ANNE SCHILLING, AND PEDRO V. SILVA

Abstract. We provide a simple proof of the Holonomy Theorem using a new Lyndon–Chiswell length function on the Karnofsky–Rhodes expansion of a semigroup. Unexpectedly, we have both a left and a right action on the Chiswell tree by elliptic maps.

1. Introduction

The following problem is at the heart of the global theory of finite semigroups. Let $S, T, U$ be finite semigroups. Consider a product of the form $T \star U$ (direct, semidirect, wreath, block, triple – see [RS09]) admitting a projection morphism on $U$. When does $S$ divide $T \star U$ (i.e. $S$ is a homomorphic image of some subsemigroup of $T \star U$)? The standard technique consists of proving that, for a given generating set $A$ of $S$, each $a \in A$ can be lifted to some $\overline{a} \in T \star U$. Examples include the $V \cup T$ proof of the Krohn–Rhodes Theorem (see [RS09]) or the alternative proof by Zeiger [Zei68, Til76a, Til76b], called the Holonomy Theorem proof.

Denoting by $\overline{S}$ the subsemigroup of $T \star U$ generated by $\{ \overline{a} \mid a \in A \}$, these theorems prove that $S$ is a homomorphic image of $\overline{S}$. But sometimes it takes decades to discover the exact nature of $\overline{S}$. Rhodes’ first attempt for the case of the Holonomy theorem was the Rhodes expansion $(S, A)^R$ (see [Til76a, Til76b]) on the way to proving the Fundamental Lemma of Complexity of finite semigroups (surmorphisms which are one-to-one on subgroups preserve complexity, see [RS09]).

A better version is the right Karnofsky–Rhodes expansion $KR_{right}(S, A)$ used in this paper. If we denote by $T_n$ the semigroup of transformations of an $n$-set, then, for $n \geq 3$, $T_n$ is not a subsemigroup of any nontrivial product. So $T_n$ must be expanded by taking preimages to become a subsemigroup of a wreath product and is intuitively the “smallest” one. We note that $KR_{left}(S, A)$ (for left acting semigroups, note the right/left reversal) relates to coupling from the past in Markov chains [PW96, RS19].

In this paper, the Holonomy Theorem is proved via Lyndon–Chiswell theory of semigroups acting on trees (created by Rhodes in [Rho91] and developed by Rhodes and Silva in [RS12]). We use that $KR_{right}(S, A)$ acts faithfully as elliptic maps on a tree, elliptic maps being an abstraction of wreath products. A key idea is that $KR_{right}(S, A)$ has many more useful surmorphisms, namely when $KR_{right}(S, A)$ is proved to consist of elliptic maps: restricting the elliptic maps to all vertices of bounded depth gives a surmorphism.

Another key idea is that the $J$-order comes explicitly into the definition of the Lyndon–Chiswell function, and $KR_{right}(S, A)$ carries more information than the Rhodes expansion $(S, A)^R$. This extra information makes the proof in this paper much easier in comparison with [Rho91, RS12]. Also we obtain an extra action we need to understand more fully.

Passing from elliptic maps to wreath products is not difficult: one just needs to number the edges leaving level $j$ with some index set $X_j$. The Lyndon–Chiswell construction does not yield uniform branching, but simply adds “fake” edges and leaves the function undefined on those. This leads to a wreath product of partial transformation semigroups.

Date: December 5, 2021.

2010 Mathematics Subject Classification. 20M30, 20M05, 20M17.

Key words and phrases. Holonomy theorem, Karnofsky–Rhodes expansion, Lyndon–Chiswell length function.
Zeiger coding (see [Zei68, Til76a, Til76b]) becomes the following. Suppose that \( v_1, v_2 \) are vertices of the tree at the same level such that \( v_1 r_{12} = v_2 \) and \( v_2 r_{21} = v_1 \), where \( r_{12} \) and \( r_{21} \) are elliptic maps representing elements of \( \text{KR}_{\text{right}}(S, A) \). Then if real edges \( E_1, \ldots, E_d \) descending from \( v_1 \) are labeled \( 1, \ldots, d \) by the index set, then the distinct \( E_1 r_{12}, \ldots, E_d r_{12} \) edges get labeled \( 1, \ldots, d \) also by the index function. As mentioned in the first two paragraphs, elliptic maps arise in studying the Zeiger proof of the Krohn–Rhodes Theorem and determining \( S \).

We plan to apply the results of this paper to Markov chains [RS19, ASST15b, ASST15a], where the tree is associated to a statistic and strings running through the tree determine the stationary distribution and mixing time.

At the moment, it is very mysterious how the \( J \)-order plays such a key role in both the semigroup theory and the Markov chain theory. In a future paper [RSS] we will compare the Chiswell–Lyndon trees of the Karnofsky–Rhodes and Rhodes expansions, leading to various new statistics for the finite Markov chain.

This paper is organized as follows. In Section 2, we review the Karnofsky–Rhodes expansion of the Cayley graph of a semigroup with a finite set of generators. In Section 3, we introduce the Dedekind height function and our new Lyndon–Chiswell length function. The Lyndon–Chiswell length function is used in the Chiswell construction, which provides a rooted tree associated to the Karnofsky–Rhodes expansion of the semigroup. The Chiswell construction in turn establishes the Holonomy Theorem (see Theorem 3.11). We conclude in Section 4 with several examples.

Acknowledgments. The authors are grateful to the anonymous referee for suggested corrections and improvements.

AS was partially supported by NSF grants DMS–1760329, DMS–1764153, and DMS–2053350. PVS was partially supported by CMUP, which is financed by national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., under the project with reference UIDB/00144/2020.

2. The Karnofsky–Rhodes expansion

Let \( A \) be a finite alphabet and let \( A^+ \) (respectively \( A^* \)) denote the free semigroup (respectively the free monoid) on \( A \). If \( \theta : A^+ \to S \) is a semigroup morphism onto a semigroup \( S \), we say that \( S \) is generated by \( A \). We usually view \( A \) as a subset of \( S \). The reference to the morphism is omitted whenever possible and we use the notation \((S, A)\) to describe this situation.

We denote by \( S^1 \) the monoid obtained by adjoining to \( S \) a (new) identity \( 1 \) (even if \( S \) is already a monoid). Green’s quasi-orders on \( S \) are defined by

- \( a \preceq_R b \) if \( a \in bS^1 \),
- \( a \preceq_L b \) if \( a \in S^1 b \),
- \( a \preceq_J b \) if \( a \in S^1 bS^1 \).

Then \( \preceq_X = \preceq_X \cap \succeq_X \) for \( X = \mathcal{R}, \mathcal{L}, \mathcal{J} \).

We denote by \( S^{op} \) the opposite semigroup of \( S \), where the binary operation \( \cdot \) on \( S \) is replaced by the binary operation \( x \circ y = y \cdot x \). Note that the \( \mathcal{L} \) relation of \( S^{op} \) is the \( \mathcal{R} \) relation of \( S \), and the \( \mathcal{R} \) relation of \( S^{op} \) is the \( \mathcal{L} \) relation of \( S \).

We define the left and right Cayley graphs of \((S, A)\), denoted respectively by \( \text{LCay}(S, A) \) and \( \text{RCay}(S, A) \), as follows:

- \( S^1 \) is the vertex set in both graphs,
- the edge set of \( \text{LCay}(S, A) \) is \( \{(s, a, as) : s \in S^1, a \in A\} \),
- the edge set of \( \text{RCay}(S, A) \) is \( \{(s, a, sa) : s \in S^1, a \in A\} \).

Note that these graphs are complete and deterministic: given a vertex \( s \) and \( u \in A^+ \), there exists a unique path with label \( u \) starting at \( s \). The following remark, which follows from the definitions, will allow us to use left-right symmetries:

Remark 2.1. \( \text{LCay}(S, A) = \text{RCay}(S^{op}, A) \).
An edge \((p, q)\) of a directed graph is called a transition edge if there exists no path from \(q\) to \(p\). This applies also to \(A\)-labeled graphs (in particular to left and right Cayley graphs), where \((s, a, s')\) is a transition edge if there is no path from \(s'\) to \(s\). Note that in a Cayley graph, edges of the form \((1, a, a)\) are always transition edges.

If \(s \xrightarrow{D} s'\) is an edge of \(\text{RCay}(S, A)\), then \(s' = sa\) and so \(s' \leq_R s\). Hence this edge is a transition edge if and only if \(s' <_R s\). Note also that if two transition edges occur in two different paths, they must occur in the same order.

The right Karnofsky–Rhodes expansion \(\text{KR}_{\text{right}}(S, A)\) of \((S, A)\) is defined as the quotient \(A^+ / \tau_r\), where \(\tau_r\) is the congruence on \(A^+\) defined as follows: \(u \tau_r v\) if \(u = v\) holds in \(S\) and the paths \(\mathbb{1} \xrightarrow{u} u\) and \(\mathbb{1} \xrightarrow{v} v\) in \(\text{RCay}(S, A)\) have the same transition edges. Then \(S\) is a homomorphic image of \(\text{KR}_{\text{right}}(S, A)\) in the obvious way.

The left Karnofsky–Rhodes expansion of \((S, A)\) can be defined by

\[
\text{KR}_{\text{left}}(S, A) = \text{KR}_{\text{right}}(S^\text{op}, A).
\]

We will be paying particular attention to \(\text{KR}_{\text{right}}^1(S, A)\), which is obtained by adjoining the (new) identity \(\mathbb{1}\) to \(\text{KR}_{\text{right}}(S, A)\). We can view \(\text{KR}_{\text{right}}^1(S, A)\) as the quotient \(A^*/(\tau_r \cup \{(1, 1)\})\). Similarly, we define \(\text{KR}_{\text{left}}^1(S, A)\).

3. The Chiswell construction

From now on, \(S\) is a fixed finite semigroup and \(A\) is a generating set of \(S\).

3.1. The Dedekind height function. We shall write \(T = \text{KR}_{\text{right}}(S, A)\) throughout this section, and let \(\varphi: T^1 \to S^1\) denote the canonical surmorphism.

The Dedekind height function \(h: S^1 \to \mathbb{N}\) is defined as

\[
h(s) = \max\{k \in \mathbb{N} \mid \text{there exists a chain } s_0 >_J \cdots >_J s_k = s \text{ in } S^1\}.
\]

This should be denoted \(h_S\), but the semigroup \(S\) is usually understood, as in Proposition 3.4 below.

Finite semigroups are known to be stable: they satisfy the equalities

\[
\leq_R \cap J = R, \quad \leq_L \cap J = L.
\]

The following result will prove useful later.

Lemma 3.1. If \(s \prec_K s'\) holds in \(S\) for \(K \in \{R, L, J\}\), then \(h(s) > h(s')\).

Proof. The result is immediate for \(J\). By symmetry, we may assume that \(s \prec_R s'\). It follows that \(s \preceq_J s'\). Now since \(S\) is stable we cannot have \(sJs'\), thus \(s \prec_J s'\) and so \(h(s) > h(s')\). \(\square\)

A semigroup \(S\) is regular if every \(s \in S\) is regular. That is, for each \(s \in S\) there exists an element \(s' \in S\) such that \(ss's = s\).

Lemma 3.2. If \(t, t' \in T^1\) satisfy \(\varphi(tt') = \varphi(t)\), then \(tt' = t\).

Proof. Let \(u, v \in A^*\) represent \(t\) and \(t'\), respectively. We have paths \(\mathbb{1} \xrightarrow{u} \varphi(t)\) and \(\mathbb{1} \xrightarrow{uvu} \varphi(tt')\) in \(\text{RCay}(S, A)\). Since \(\varphi(tt') = \varphi(t)\) and \(\text{RCay}(S, A)\) is deterministic, we actually have a loop labeled by \(vu\) at \(\varphi(t)\). Since a loop cannot contain transition edges, it follows that \(uvu \tau_r u\) and so \(tt' = t\). \(\square\)

It follows that if \(S\) is regular, then \(T^1\) is also regular.

Lemma 3.3. Assume that \(S\) is a regular semigroup and let \(t, t' \in T^1\).

(i) If \(\varphi(t) \leq_J \varphi(t')\) if and only if \(t \leq_J t'\).

(ii) \(\varphi(t) <_J \varphi(t')\) if and only if \(t <_J t'\).
Proof. (i) If $\varphi(t) \leq_{\mathcal{J}} \varphi(t')$, there exist $p, q \in T^1$ such that $\varphi(t) = \varphi(pt'q)$. On the other hand, since $S$ is regular, we have $\varphi(t) = \varphi(tzt)$ for some $z \in T$. Hence

$$\varphi(t) = \varphi(tzt) = \varphi(tztzt) = \varphi(tzpt'qzt)$$

and it follows from Lemma 3.2 that $t = tzpt'qzt$. Therefore $t \leq_{\mathcal{J}} t'$.

The converse implication follows from $\varphi$ being a homomorphism.

(ii) Assume that $\varphi(t) <_{\mathcal{J}} \varphi(t')$. By (i), we obtain $t \leq_{\mathcal{J}} t'$. Since $\leq_{\mathcal{J}}$ is preserved by homomorphisms, $t \mathcal{J} t'$ implies $\varphi(t) \mathcal{J} \varphi(t')$, a contradiction. Thus $t <_{\mathcal{J}} t'$.

Conversely, assume that $t <_{\mathcal{J}} t'$. Hence $\varphi(t) <_{\mathcal{J}} \varphi(t')$. Since $\varphi(t) \mathcal{J} \varphi(t')$ implies $t \mathcal{J} t'$ by (i), we get $\varphi(t) <_{\mathcal{J}} \varphi(t')$.  \hfill $\Box$

**Proposition 3.4.** Assume that $S$ is a regular semigroup and let $t \in T^1$. Then $h(t) = h(\varphi(t))$.

**Proof.** By Lemma 3.3(ii), we have a chain

$$t_1 >_{\mathcal{J}} \cdots >_{\mathcal{J}} t_k = t$$

in $T$ if and only if we have a chain

$$\varphi(t_1) >_{\mathcal{J}} \cdots >_{\mathcal{J}} \varphi(t_k) = \varphi(t)$$

in $S$. Thus $h(t) = h(\varphi(t))$. \hfill $\Box$

**Remark 3.5.** If $(S, A)$ is not regular, computing $h(t)$ for $t \in T$ can be more challenging sometimes.

### 3.2. The Lyndon–Chiswell length function.

Write

$$\ell = 2 \max \{ h(s) \mid s \in S^1 \}.$$ 

Denote by $t(E)$ the endpoint of an edge $E$ of a directed graph.

Let $\alpha, \beta \in T^1$. Let $(E_1, \ldots, E_m)$ and $(E'_1, \ldots, E'_n)$ be the corresponding sequences of transition edges. Since any edge starting at $1$ is a transition edge, we have $m = 0$ if and only if $\alpha = 1$. Let

$$\xi(\alpha, \beta) = \max \{ i \in \{0, \ldots, m\} \mid E_i = E'_1, \ldots, E_i = E'_i \}.$$ 

Hence $\xi(\alpha, \beta)$ counts the maximum number of transition edges consecutively shared by $\alpha$ and $\beta$, when we start with the first and proceed in order. If $\xi(\alpha, \beta) = k > 0$, we write also $\eta(\alpha, \beta) = E_k = E'_k$.

**Lemma 3.6.** For all $\alpha, \beta, \gamma \in T^1$, we have:

(i) $\xi(\alpha, \beta) = \xi(\beta, \alpha)$;

(ii) $\xi(\alpha \gamma, \beta \gamma) \geq \xi(\alpha, \beta)$;

(iii) $\xi(\alpha, \gamma) \geq \min(\xi(\alpha, \beta), \xi(\beta, \gamma))$.

**Proof.** (i) follows from the symmetry of equality.

(ii) follows from the following fact: the sequence of transition edges of $\alpha \gamma$ starts with the sequence of transition edges of $\alpha$.

For (iii), we may assume that $\min(\xi(\alpha, \beta), \xi(\beta, \gamma)) = k > 0$. Let $(E_1, \ldots, E_m)$, $(E'_1, \ldots, E'_n)$ and $(E''_1, \ldots, E''_p)$ be the sequences of transition edges corresponding to $\alpha$, $\beta$ and $\gamma$. Then $E_1 = E'_1, \ldots, E_k = E'_k$ and also $E'_1 = E''_1, \ldots, E_k = E''_k$. Hence $E_1 = E''_1, \ldots, E_k = E''_k$ and so $\xi(\alpha, \gamma) \geq k$ as required. \hfill $\Box$

We prove also the following result:

**Lemma 3.7.** Let $\alpha, \beta, \gamma \in T^1$ be such that $\xi(\alpha, \beta) > 0$. Then:

(i) $\xi(\gamma \alpha, \gamma \beta) > 0$;

(ii) $t(\eta(\gamma \alpha, \gamma \beta)) \leq_{\mathcal{R}} \varphi(\gamma) t(\eta(\alpha, \beta))$ \hfill $\leq_{\mathcal{L}} t(\eta(\alpha, \beta))$. 


Proof. We may assume that \( \gamma \neq 1 \).

(i) Since the first letter of a word representing \( \gamma \) must necessarily label a transition edge of \( \gamma \) (or \( \gamma \alpha \), or \( \gamma \beta \)), it follows that \( \xi(\gamma \alpha, \gamma \beta) > 0 \).

(ii) Let \((E_1, \ldots, E_m), (E'_1, \ldots, E'_n)\) and \((E''_1, \ldots, E''_p)\) be the sequences of transition edges corresponding to \( \alpha \), \( \beta \) and \( \gamma \), respectively. Let \( \xi(\alpha, \beta) = k \), so that \( \eta(\alpha, \beta) = E_k = E'_k \). What are the possible transition edges of \( \gamma \)? Clearly, \( E''_1, \ldots, E''_p \) are all transition edges of \( \gamma \).

Write \( S^1 = A^* / \sigma \) and \( T^1 = A^* / \tau \). Let \( u = e_1 u_1 \ldots e_m u_m \) and \( u' = e'_1 u'_1 \ldots e'_n u'_n \) be words representing \( \alpha \) and \( \beta \), respectively, where \( e_i \) and \( e'_j \) denote the labels of \( E_i \) and \( E'_j \). Write \( e_i = e_1 u_1 \ldots e_i u_i \) and \( e'_j = e'_1 u'_1 \ldots e'_j u'_j \) for all \( 0 \leq i \leq m \) and \( 0 \leq j \leq n \). Let \( \gamma = w \tau \).

Since the letters occurring in the \( u_i \) label no transition edges in the path \( 1 \rightarrow \sigma \) u in \( \text{RCay}(S, A) \), there exists a path \( v_i \sigma \xrightarrow{} (v_i, \epsilon_{i+1}) \sigma \) in \( \text{RCay}(S, A) \) for \( i = 1, \ldots, m \). Hence \( (v_i, \epsilon_{i+1}) \tau = (v_i, \epsilon_i) \tau \) and so \( (w v_i x_i) \tau = (w v_i x_i v_i, \epsilon_i) \tau \) for \( i = 1, \ldots, m \). Thus the only possible transition edges of \( \gamma \alpha \) beyond \( E''_1, \ldots, E''_p \) are of the form \( (w v_i x_i) \sigma \xrightarrow{} (w v_i x_i v_i, \epsilon_i) \sigma \) for some \( i \in \{1, \ldots, m\} \). Similarly, the only possible transition edges of \( \gamma \beta \) beyond \( E''_1, \ldots, E''_p \) are of the form \( (w v_i x_i v_i) \sigma \xrightarrow{} (w v_i x_i v_i, \epsilon_i) \sigma \) for some \( i \in \{1, \ldots, n\} \).

Let \( I = \{i \in \{1, \ldots, k\} \mid (w v_i x_i) \sigma \xrightarrow{} (v_i, \epsilon_{i+1}) \sigma \) is a transition edge of \( \text{RCay}(S, A) \} \).

Note that \( I \) needs not to contain all the integers between 1 and \( r \). Suppose first that \( I \neq \emptyset \) and let \( r = \max I \). Since \( (v_i, \epsilon_{i+1}) \sigma = E_i = E'_i = (v'_i, \epsilon'_i) \sigma \) for \( i = 1, \ldots, k \), we get \((w v_i x_i) \sigma, e_i, (w v_i x_i v_i) \sigma) = ((w v'_i x'_i) \sigma, e'_i, (w v'_i x'_i v'_i) \sigma)\) as well. Hence \( \gamma \alpha \) and \( \gamma \beta \) share the same transition edges up to \((w v_i x_i) \sigma, e_i, (w v_i x_i v_i) \sigma) = (w v'_i x'_i) \sigma, e'_i, (w v'_i x'_i v'_i) \sigma\) at least. Now since \( r = \max I \) there are no more transition edges between \((w v_i x_i) \sigma, e_i, (w v_i x_i v_i) \sigma) \) in \( \text{RCay}(S, A) \). Hence

\[
\tau(\eta(\gamma, \alpha, \beta)) \leq_R (w v_r x_r) \sigma R (w v_k x_k) \sigma = \varphi(\gamma) \tau(\eta(\alpha, \beta)).
\]

We reach the same conclusion in the case \( I = \emptyset \), replacing the edge \( E_i \) in the above argument by \( E^p \) (note that \( p \geq 1 \) since we are assuming \( \gamma \neq 1 \)).

Finally, \( \gamma \tau(\eta(\alpha, \beta)) \leq_L \tau(\eta(\alpha, \beta)) \) holds trivially. \( \square \)

Let \((E_1, \ldots, E_m)\) and \((E'_1, \ldots, E'_n)\) be the sequences of transition edges corresponding to \( \alpha \) and \( \beta \), respectively. Let \( k = \xi(\alpha, \beta) \). If \( k > 0 \), we have \( \eta(\alpha, \beta) = E_k = E'_k \). We define the Lyndon–Chiswell length function \( D : T^1 \times T^1 \rightarrow \mathbb{N} \) by

\[
D(\alpha, \beta) = \begin{cases} 
\ell & \text{if } \alpha = \beta, \\
0 & \text{if } \alpha \neq \beta \text{ and } k = 0, \\
2h((E_k)) & \text{if } 0 < k < m, n \text{ and } t(E_{k+1}) = t(E'_{k+1}), \\
2h((E_k)) - 1 & \text{in all remaining cases}.
\end{cases}
\]

Note that \( \text{im}(h) = \{0, 1, \ldots, \ell\} \) implies \( \text{im}(D) \subseteq \{0, 1, \ldots, \ell\} \). We show now that

\[(\alpha \neq \beta \land \xi(\alpha, \beta) < \xi(\alpha, \gamma)) \Rightarrow D(\alpha, \beta) < D(\alpha, \gamma) \]

holds for all \( \alpha, \beta, \gamma \in T^1 \).

Assume that \( \xi(\alpha, \beta) < \xi(\alpha, \gamma) \). We may assume that \( \xi(\alpha, \beta) > 0 \), otherwise \( D(\alpha, \beta) = 0 \). Then \( \tau(\eta(\alpha, \beta)) \geq_R \tau(\eta(\alpha, \gamma)) \) because there exists in \( \text{RCay}(S, A) \) a path from \( \tau(\eta(\alpha, \beta)) \) to \( \tau(\eta(\alpha, \gamma)) \) containing transition edges. By Lemma 3.1, we get \( h(\tau(\eta(\alpha, \beta))) \leq h(\tau(\eta(\alpha, \gamma))) \), yielding \( D(\alpha, \beta) < D(\alpha, \gamma) \). Thus (3.1) holds.

The following properties go a little beyond those of [Rho91, Fact 1.9]. We provide a full proof.

Lemma 3.8. The Lyndon-Chiswell length function satisfies the following properties for all \( \alpha, \beta, \gamma \in T^1 \):
(i) \( D(\alpha, \beta) = D(\beta, \alpha) \);
(ii) \( D(\alpha \gamma, \beta \gamma) \geq D(\alpha, \beta) \);
(iii) \( D(\gamma \alpha, \gamma \beta) \geq D(\alpha, \beta) \);
(iv) **(isoperimetric inequality)** \( D(\alpha, \gamma) \geq \min(D(\alpha, \beta), D(\beta, \gamma)) \).

**Proof.** (i) It follows easily from Lemma 3.6(i).

(ii) We may assume that \( \alpha \gamma \neq \beta \gamma \), otherwise \( D(\alpha \gamma, \beta \gamma) = \ell \) is maximum. Hence \( \alpha \neq \beta \) as well. We may also assume that \( \xi(\alpha, \beta) > 0 \), otherwise \( D(\alpha, \beta) = 0 \).

Let \( (E_1, \ldots, E_m) \) and \( (E'_1, \ldots, E'_n) \) be the sequences of transition edges corresponding to \( \alpha \) and \( \beta \). Let \( k = \xi(\alpha, \beta) > 0 \), so that \( E_1 = E'_1, \ldots, E_k = E'_k \). By the proof of Lemma 3.6(ii), the sequences of transition edges corresponding to \( \alpha \gamma \) and \( \beta \gamma \) are of the form \((E_1, \ldots, E_m, F_1, \ldots, F_r)\) and \((E'_1, \ldots, E'_n, F'_1, \ldots, F'_s)\). Suppose that \( \xi(\alpha \gamma, \beta \gamma) > \xi(\alpha, \beta) = k \). Then either \( m = k < n \) and \( F_1 = E'_{k+1}, \) or \( n = k < m \) and \( E_{k+1} = F'_1 \), or \( m = n = k \) and \( F_1 = F'_1 \). In any case, we have \( t(\eta(\alpha \gamma, \beta \gamma)) <_\mathcal{R} t(\eta(\alpha, \beta)) \). Now it follows from Lemma 3.1 that \( h(t(\eta(\alpha \gamma, \beta \gamma))) > h(t(\eta(\alpha, \beta))) \).

Thus \( D(\alpha \gamma, \beta \gamma) > D(\alpha, \beta) \).

Therefore we may assume by Lemma 3.6(ii) that \( \xi(\alpha \gamma, \beta \gamma) = \xi(\alpha, \beta) = k \), which means that \( D(\alpha \gamma, \beta \gamma) \) and \( D(\alpha, \beta) \) differ by at most 1. Hence we may also assume that \( t(E_{k+1}) = t(E'_{k+1}) \) (the case where we do not subtract 1). Since \( E_1, \ldots, E_{k+1} \) and \( E'_1, \ldots, E'_{k+1} \) are the first \( k+1 \) transition edges corresponding to \( \alpha \gamma \) and \( \beta \gamma \), respectively, we immediately get \( D(\alpha \gamma, \beta \gamma) = D(\alpha, \beta) \).

(iii) Similarly to the proof of (ii), we may assume that \( \gamma \alpha \neq \gamma \beta \) and \( \xi(\alpha, \beta) > 0 \). By Lemma 3.7(ii), we have \( t(\eta(\alpha \gamma, \beta \gamma)) \leq_\mathcal{J} t(\eta(\alpha, \beta)) \).

Suppose first that \( t(\eta(\alpha \gamma, \beta \gamma)) <_\mathcal{J} t(\eta(\alpha, \beta)) \). Then Lemma 3.1 yields \( h(t(\eta(\alpha \gamma, \beta \gamma))) > h(t(\eta(\alpha, \beta))) \) and so

\[
D(\gamma \alpha, \gamma \beta) > 2h(t(\eta(\alpha \gamma, \beta \gamma))) - 1 > 2h(t(\eta(\alpha, \beta))) \geq D(\alpha, \beta).
\]

Thus we may assume that \( t(\eta(\gamma \alpha, \gamma \beta)) \notin \mathcal{J} t(\eta(\alpha, \beta)) \), so that \( h(t(\eta(\gamma \alpha, \gamma \beta))) = h(t(\eta(\alpha, \beta))) \). We may also assume that \( D(\alpha, \beta) \) is even, so that \( k < m, n \) and \( t(E_{k+1}) = t(E'_{k+1}) \).

Recall from the proof of Lemma 3.7 the words \( u = e_1 u_1 \ldots e_m u_m \) and \( u' = e'_1 u'_1 \ldots e'_n u'_n \) representing \( \alpha \) and \( \beta \), and all the associated notation. By Lemma 3.7(ii), we get

\[
t(\eta(\gamma \alpha, \gamma \beta)) \leq_\mathcal{R} \varphi(\gamma) t(\eta(\alpha, \beta)) = (wv_{k-1} e_k) \sigma.
\]

Thus

\[
(wv_k e_{k+1}) \sigma \leq_\mathcal{S} (w_k e_{k+1}) \sigma <_\mathcal{R} (v_k e_{k+1}) \sigma = t(\eta(\alpha, \beta)) \mathcal{J} t(\eta(\gamma \alpha, \gamma \beta)) \leq_\mathcal{R} (wv_k e_{k+1}) \sigma \mathcal{R} (wv_k) \sigma.
\]

Since finite semigroups are stable, the relation \( <_\mathcal{R} \) is contained in \( <_\mathcal{J} \), hence \( (wv_k e_{k+1}) \sigma \notin \mathcal{J} (wv_k) \sigma \). Since \( (wv_k e_{k+1}) \sigma \leq_\mathcal{R} (wv_k) \sigma \), it follows that \( (wv_k e_{k+1}) \sigma \notin \mathcal{R} (wv_k) \sigma \). Hence

\[
(wv_k) \sigma \xrightarrow{e_{k+1}} (wv_k e_{k+1}) \sigma
\]

is a transition edge, in fact the first transition edge of \( \gamma \alpha \) which is not shared with \( \gamma \beta \). Similarly,

\[
(wv'_k) \sigma \xrightarrow{e'_{k+1}} (wv'_k e'_{k+1}) \sigma
\]

is the first transition edge of \( \gamma \beta \) which is not shared with \( \gamma \alpha \). Now

\[
(v_k e_{k+1}) \sigma = t(E_{k+1}) = t(E'_{k+1}) = (v'_k e'_{k+1}) \sigma
\]

yields \( (wv_k e_{k+1}) \sigma = (wv'_k e'_{k+1}) \sigma \) and so

\[
D(\gamma \alpha, \gamma \beta) = 2h(t(\eta(\gamma \alpha, \gamma \beta))) = 2h(t(\eta(\alpha, \beta))) = D(\alpha, \beta).
\]

Therefore (iii) holds.

(iv) We may assume that \( \alpha, \beta, \gamma \) are all different. Let \( (E''_1, \ldots, E''_p) \) be the sequence of transition edges corresponding to \( \gamma \).
If \( \xi(\alpha, \beta) > \xi(\beta, \gamma) \), we can exchange \( \alpha \) and \( \gamma \) in view of (i), and so Lemma 3.6(i) allows us to assume that \( \xi(\alpha, \beta) \leq \xi(\beta, \gamma) \). Now Lemma 3.6(iii) yields \( \xi(\alpha, \gamma) \geq \xi(\alpha, \beta) \). Since \( \xi(\alpha, \gamma) > \xi(\alpha, \beta) \) immediately implies our objective in view of (3.1), we are now restricted to the case

\[
0 < k = \xi(\alpha, \gamma) = \xi(\alpha, \beta) \leq \xi(\beta, \gamma).
\]

It follows that \( E_i = E'_i = E''_i \) for \( i = 1, \ldots, k \).

Unless \( t(E_{k+1}) = t(E'_{k+1}) \), we get \( D(\alpha, \beta) = 2h(t(E_k)) - 1 \) and we are done. Hence we may assume that \( t(E_{k+1}) = t(E'_{k+1}) \). Now, unless \( t(E''_{k+1}) = t(E'_k) \), we get \( D(\beta, \gamma) = 2h(t(E_k)) \) and we are done as well. But then \( t(E_{k+1}) = t(E''_{k+1}) \) and so \( D(\alpha, \gamma) = 2h(t(E_k)) = D(\alpha, \beta) \).

Therefore (iv) holds.

**Remark 3.9.** In view of these properties, \( D \) can indeed be called a length function for (unexpectedly) both a left and right action because of Lemma 3.8 (ii) and (iii).

3.3. Representations as elliptic maps on a rooted tree. Let \( \Gamma = (V, E) \) be a simple undirected graph. Then \( \Gamma \) is a tree if it is connected and admits no cycles (i.e. no closed paths of the form \( v_1 \rightarrow \cdots \rightarrow v_n \rightarrow v_1 \) with \( n \geq 3 \) different vertices). If we distinguish a vertex \( v_0 \in V \), we get the **rooted tree** \( \Gamma \).

Given a rooted tree \( \Gamma \), we get a **depth function** \( \delta : V \to \mathbb{N} \) as follows: \( \delta(v) \) is the edge length of the shortest path connecting \( v \) to \( v_0 \). An **endomorphism** of the rooted tree \( \Gamma \) is a function \( \varphi : V \to V \) such that:

- \( \delta(\varphi(v)) = \delta(v) \) for every \( v \in V \);
- if \( v \rightarrow w \) is an edge of \( \Gamma \), so is \( \varphi(v) \rightarrow \varphi(w) \).

Endomorphisms of rooted trees are also known as **elliptic maps**. We denote by \( \text{EM}(\Gamma, v_0) \) the monoid of all elliptic maps of \( \Gamma \).

A **representation** of a monoid \( M \) as elliptic maps on a rooted tree \( \Gamma \) is a monoid homomorphism \( \theta : M \to \text{EM}(\Gamma, v_0) \). The representation is **faithful** if \( \varphi \) is one-to-one.

3.4. The Chiswell construction and the holonomy theorem. We adapt next the Chiswell construction described in [Rho91, Proof of Theorem 1.12] and [RS12, Proof of Theorem 4.7] (see also [Chi76]).

Let \( T = \text{KR}_{\text{right}}(S, A) \) and let \( D : T^1 \times T^1 \to \mathbb{N} \) be the Lyndon–Chiswell length function defined before (with maximum value \( \ell \)). Write

\[
C = \{(k, \alpha) \mid 0 \leq k \leq \ell, \alpha \in T^1\}.
\]

We define a relation \( \sim \) on \( C \) by \( (k, \alpha) \sim (k', \beta) \) if:

- \( k = k' \);
- \( D(\alpha, \beta) \geq k \).

It follows from Lemma 3.8(i) and (iv) that \( \sim \) is indeed an equivalence relation on \( C \). Note that \( (0, \alpha) \sim (0, \beta) \) for all \( \alpha, \beta \in T^1 \).

Denote by \( [k, \alpha] \) the equivalence class of \( (k, \alpha) \in C \). Define an undirected graph \( C \) with vertices \( [k, \alpha] \) and edges \( [k, \alpha] \rightarrow [k+1, \alpha] \) when \( 0 \leq k < \ell \) and \( \alpha \in T^1 \). Note that

\[
\text{if } [k, \beta] \rightarrow [k+1, \alpha] \text{ is an edge of } C \text{ then } [k, \beta] = [k, \alpha].
\]

Indeed, if there exists such an edge then there exists some \( \gamma \in T^1 \) such that \( [k, \beta] = [k, \gamma] \) and \( [k+1, \alpha] = [k+1, \gamma] \). It follows that \( D(\alpha, \gamma) \geq k+1 > k \). Hence \( [k, \alpha] = [k, \gamma] \) and (3.2) holds.

With minimal adaptations from [Rho91] and [RS12], we prove the following lemma for the sake of completeness.

**Lemma 3.10.** \( (C, [0, 1]) \) is a rooted tree.
Proof. We have a path

\[ [0, 1] = [0, \alpha] \rightarrow [1, \alpha] \rightarrow \cdots \rightarrow [k, \alpha] \]

for every vertex \([k, \alpha]\), hence \(C\) is connected.

Suppose that

\[ [k_0, \alpha_0] \rightarrow [k_1, \alpha_1] \rightarrow \cdots \rightarrow [k_n, \alpha_n] = [k_0, \alpha_0] \]

is a cycle in \(C\). We may assume that \(k_0 \geq k_i\) for every \(0 \leq i \leq n\). Then \(k_1 = k_{n-1} = k_0 - 1\) and it follows from (3.2) that \([k_1, \alpha_1] = [k_0 - 1, \alpha_0] = [k_{n-1}, \alpha_{n-1}]\), a contradiction. Therefore \(C\) is a tree as required. \(\square\)

This rooted tree is the Chiswell tree induced by the Lyndon–Chiswell length function \(D : T^1 \times T^1 \rightarrow \mathbb{N}\). Note that the depth function is given by \(\delta([k, \alpha]) = k\).

**Theorem 3.11 (Holonomy Theorem).** Let \((S, A)\) be a finite semigroup \(S\) with generators \(A\). Then \(KR_{\text{right}}^1(S, A)\) and \(KR_{\text{left}}^1(S, A)\) are faithfully represented as elliptic maps on a finite rooted tree.

**Proof.** Once again, we adapt the proof from [Rho91, RS12].

Let \(\epsilon : KR_{\text{right}}^1(S, A) \rightarrow \text{EM}((C, [0, 1]))\)

be defined by

\[ \epsilon_{\alpha}([k, \beta]) = [k, \alpha \beta]. \]

First, we show that \(\epsilon_{\alpha}\) is well defined. Suppose that \([k, \beta] = [k', \beta']\). Then \(k = k'\) and \(D(\beta, \beta') \geq k\). Then \(D(\alpha \beta, \alpha \beta') \geq k\) by Lemma 3.8(iii) and so \([k, \alpha \beta] = [k', \alpha \beta']\). Thus \(\epsilon_{\alpha}\) is well defined.

It is obvious that \(\delta(\epsilon_{\alpha}([k, \beta])) = \delta([k, \beta])\). On the other hand, if \([k, \beta] \rightarrow [k+1, \beta]\) is an edge of \(C\), so is \(\epsilon_{\alpha}([k, \beta]) = [k, \alpha \beta] \rightarrow [k+1, \alpha \beta] = \epsilon_{\alpha}([k+1, \beta])\). Therefore \(\epsilon_{\alpha}\) is an elliptic map on the finite rooted tree \((C, [0, 1])\) and so \(\epsilon\) is well defined.

Given \(\alpha, \alpha' \in KR_{\text{right}}^1(S, A)\), we have

\[ \epsilon_{\alpha \alpha'}([k, \beta]) = [k, \alpha \alpha' \beta] = \epsilon_{\alpha}([k, \beta]), \]

hence \(\epsilon_{\alpha \alpha'} = \epsilon_{\alpha} \epsilon_{\alpha'}\). On the other hand, \(\epsilon_{1}([k, \beta]) = [k, \beta]\) and so \(\epsilon_{1}\) is the identity map. Thus \(\epsilon\) is a monoid homomorphism.

Finally, assume that \(\alpha \neq \alpha'\). Let \((E_1, \ldots, E_m)\) be the sequence of transition edges corresponding to \(\alpha\).

Since \(D(\alpha, \alpha') = \ell = 2\max\{h(s) \mid s \in S^2\}\), we are not subtracting 1, which implies that \(\alpha\) possesses transition edges beyond \(E_{\xi(\alpha, \alpha')}\), i.e. \(\xi(\alpha, \alpha') < m\). In view of Lemma 3.1, this contradicts the fact that \(h\) should reach its maximum value at \(t(E_{\xi(\alpha, \alpha')})\). Thus \(\alpha = \alpha'\) and so \(\epsilon\) is one-to-one. Therefore the representation is faithful.

Recall now that \(KR_{\text{left}}^1(S, A) = KR_{\text{right}}^1(S^{\text{op}}, A)\). It follows from the first part that \(KR_{\text{left}}^1(S, A)\) is also faithfully represented as elliptic maps on a finite rooted tree. \(\square\)

**Remark 3.12.** It follows easily from Lemma 3.8(ii) that we can consider a right action of \(KR_{\text{right}}^1(S, A)\) on the Chiswell tree \((C, [0, 1])\) given by

\[ [k, \beta] \alpha = [k, \beta \alpha]. \]

A straightforward adaptation of the proof of Theorem 3.11 shows that we obtain an injective monoid homomorphism

\[ \epsilon' : KR_{\text{right}}^1(S, A) \rightarrow (\text{EM}((C, [0, 1])))^{\text{op}}, \]

since here the elliptic mappings must compose from left to right.
Table 1. The left action semaphore code in $\{a,b\}^4$ associated to the ideal generated by $aaa,aab,aba,baa,bab$.

| a·  | b·  |
|-----|-----|
| $aaa$ | $baa$ |
| $aab$ | $baa$ |
| $aba$ | $bab$ |
| $aba$ | $bbab$ |
| $baa$ | $bbba$ |
| $aab$ | $bab$ |
| $bab$ | $bbba$ |
| $bab$ | $bbba$ |
| $abb$ | $bab$ |
| $bbb$ | $bbbb$ |

Remark 3.13. Note that the Lyndon-Chiswell length function on $KR^1_{right}(S^{op}, A) \times KR^1_{right}(S^{op}, A)$ would be the version of the Lyndon-Chiswell length function built from $S$ when we replace its right Cayley graph by its left Cayley graph. And Lemma 3.8(ii) ensures that left-right symmetry is preserved at all levels of the proofs, so we could replicate all the preceding proofs using $LCay(S, A)$ and $KR^1_{left}(S, A)$.

In the next paper we will expand this theory and apply it to mixing times.

4. Examples

4.1. Left action on semaphore codes. Let $A$ be a finite alphabet and let $k \geq 1$. Consider the left action $A^+ \times A^k \to A^k$ defined as follows: given $v \in A^+$ and $u \in A^k$, let $v \cdot u$ denote the prefix of length $k$ of $vu$. An equivalence relation $\rho$ on $A^k$ is a left congruence if

$$u\rho v \implies (w \cdot u)(w \cdot v)$$

holds for all $u, v \in A^k$ and $w \in A^+$. Then the set $\rho \backslash A^k$ of all $\rho$-classes becomes a left zero semigroup under the operation $(\rho u)(\rho v) = \rho u$. We denote by $LC(A^k)$ the set of left congruences on $A^k$. As shown in [RSS16a, RSS16b], every left congruence can be approximated by a special left congruence and special left congruences are in bijection with semaphore codes. A semaphore code [BPR10] is a prefix code $S$ over $A$ (i.e., all elements in the code are incomparable in prefix order) for which there is a left action in the following sense: If $a \in A$ and $u \in S$, then $au$ has a prefix in $S$. The left action $a \cdot u$ is the prefix of $au$ that is in $S$.

Remark 4.1. In fact, [RSS16a, RSS16b] use right congruences and semaphore codes are suffix codes. But as outlined in the introduction, in applications the left action is usually used. See also [RS19].

Given a semaphore code $S$ and the left action by $A^+$ on $S$, consider the functions $S \to S$ induced by this action. This yields a semigroup $(S, A)$. The right Cayley graph of $(S, A)$ is equal to its Karnofsky–Rhodes expansion.

Example 4.2. Let $A = \{a,b\}$ be a two letter alphabet and $I$ the ideal in $A^*$ generated by $aaa,aab,aba,baa,bab$. Then the left action prefix semaphore code in $A^4$ is given in Table 1. Hence $S$ has 11 elements. To compute $KR_{right}(S, A)$, we compute the action of the various subwords of the elements in $S$ on $S$ and record the images, see Figure 1. We have $\ell = 8$, so the Chiswell tree has 9 levels. However, the Lyndon–Chiswell length function $D$ cannot take on the values 2, 4, 6, 8. It follows that these levels are equal to their predecessors and can be omitted. The elliptic left action of $a$ on the Chiswell tree is given in Figure 2, whereas the elliptic left action of $b$ is given in Figure 3.
4.2. **Right zero semigroup with two generators.** Let \((S, A)\) be the right zero semigroup \(\text{RZ}(2)\) (that is \(xy = y\) for all \(x, y \in \text{RZ}(2)\)) with two generators \(A = \{a, b\}\). The Karnofsky–Rhodes expansion of the right Cayley graph of \((S, A)\) is depicted in Figure 4. Then the Chiswell construction
is given in Figure 5. The right and left actions of $a$ and $b$ on the Chiswell construction are given in Figures 6, 7, 8 and 9, respectively.

**Figure 4.** $\text{KR}_{\text{right}}(\text{RZ}(2), \{a, b\})$.

**Figure 5.** The Chiswell construction for $\text{KR}_{\text{right}}(\text{RZ}(2), \{a, b\})$. 
Figure 6. The left action of $a \cdot$ on the Chiswell tree for $\text{KR}_{\text{right}}(\text{RZ}(2), \{a, b\})$.

Figure 7. The left action of $b \cdot$ on the Chiswell tree for $\text{KR}_{\text{right}}(\text{RZ}(2), \{a, b\})$.

Figure 8. The right action of $\cdot a$ on the Chiswell tree for $\text{KR}_{\text{right}}(\text{RZ}(2), \{a, b\})$.

Figure 9. The right action of $\cdot b$ on the Chiswell tree for $\text{KR}_{\text{right}}(\text{RZ}(2), \{a, b\})$. 
4.3. **The monoid $T_2$ of total transformations.** Let $T_2$ denote the monoid of total transformations on the set $\{1, 2\}$. We denote $\varphi \in T_2$ by $(\varphi 1 \varphi 2)$ (so in $\psi \varphi$ the map $\varphi$ acts first). Let $A = \{a, b\}$ and let $\varphi: A^* \to S^2$ be the monoid homomorphism defined by $\varphi(a) = (2 1)$ and $\varphi(b) = (1 1)$. It is routine to check that $\varphi$ is onto and $\text{RCay}(T_2, A) = \text{LCay}(T_2^{\text{op}}, A)$ is depicted in Figure 10. The Karnofsky–Rhodes expansion is given in Figure 11, the Chiswell construction is drawn in Figure 12, and the left action of $a$ on the Chiswell tree is depicted in Figure 13.

![Figure 10. RCay$(T_2, A)$ with the transition edges in blue.](image)

![Figure 11. KR$_\text{right}(T_2, A)$.](image)

**REFERENCES**

[ASST15a] Arvind Ayyer, Anne Schilling, Benjamin Steinberg, and Nicolas M. Thiéry. Directed nonabelian sandpile models on trees. *Comm. Math. Phys.*, 335(3):1065–1098, 2015.

[ASST15b] Arvind Ayyer, Anne Schilling, Benjamin Steinberg, and Nicolas M. Thiéry. Markov chains, $\mathcal{R}$-trivial monoids and representation theory. *Internat. J. Algebra Comput.*, 25(1-2):169–231, 2015.

[BPR10] Jean Berstel, Dominique Perrin, and Christophe Reutenauer. *Codes and automata*, volume 129 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2010.

[Chi76] I. M. Chiswell. Abstract length functions in groups. *Math. Proc. Cambridge Philos. Soc.*, 80(3):451–463, 1976.

[PW96] James Gary Propp and David Bruce Wilson. Exact sampling with coupled Markov chains and applications to statistical mechanics. In *Proceedings of the Seventh International Conference on Random Structures and Algorithms* (Atlanta, GA, 1995), volume 9, pages 223–252, 1996.

[Rho91] John Rhodes. Monoids acting on trees: elliptic and wreath products and the holonomy theorem for arbitrary monoids with applications to infinite groups. *Internat. J. Algebra Comput.*, 1(2):253–279, 1991.

[RS09] John Rhodes and Benjamin Steinberg. *The q-theory of finite semigroups*. Springer Monographs in Mathematics. Springer, New York, 2009.

[RS12] John Rhodes and Pedro V. Silva. Further results on monoids acting on trees. *Internat. J. Algebra Comput.*, 22(4):1250034, 69, 2012.

[RS19] John Rhodes and Anne Schilling. Unified theory for finite Markov chains. *Adv. Math.*, 347:739–779, 2019.
John Rhodes, Anne Schilling, and Pedro V. Silva. The holonomy theorem giving statistics in Markov chains. in preparation.

John Rhodes, Anne Schilling, and Pedro V. Silva. Random walks on semaphore codes and delay de Bruijn semigroups. *Internat. J. Algebra Comput.*, 26(4):635–673, 2016.

John Rhodes, Anne Schilling, and Pedro V. Silva. The semaphore codes attached to a Turing machine via resets and their various limits. *Internat. J. Algebra Comput.*, 26(4):675–704, 2016.

Bret Tilson. *Complexity of semigroups and morphisms*, chapter XII in S. Eilenberg, Automata, Languages and Machines, Vol. B, Academic Press, New York, 1976, pages 313–384. 1976.

Bret Tilson. *Depth decomposition theorem*, chapter XI in S. Eilenberg, Automata, Languages and Machines, Vol. B, Academic Press, New York, 1976, pages 287–312. 1976.

Paul Zeiger. Yet another proof of the cascade decomposition theorem for finite automata: Correction. *Math. Systems Theory*, 2(4):381, 1968.
