

Testing Membership in Commutative Transformation Semigroups

Luke Elliott and Alex Levine

July 11, 2017

1 Introduction

The majority of results in this paper are taken from [1].

Throughout this paper we will use the following notations:

- We will represent the associated monoid of a semigroup S by S^1 .
- The action of elements of a semigroup on a set of states will be represented on the right.
- The identity function on a set X will be represented by id or id_X .
- The symmetric group on a set X will be denoted S_X .
- The order of an element g in a group will be denoted $o(g)$.
- The natural numbers, denoted \mathbb{N} , will be defined as the set of positive integers.

2 Commutative Transformation Semigroups

Lemma 2.1 *Let S be a commutative transformation semigroup, generated by a set A , acting on a finite set X . Let*

$$U = \bigcup_{a \in A} \text{im}(a).$$

Then S is a monoid if and only if A contains an element t such that $t \upharpoonright_U$ is a permutation of U .

In such a case, the identity of S is t^n , where n is the order of $t \upharpoonright_U$ in S_U .

Proof (\Rightarrow): Suppose S is a monoid. Then $\exists e \in S$ such that $eg = ge$, $\forall g \in S$. Let $x \in U$. We have that $\exists a \in A$, $y \in X$ such that $x = ya$. Suppose, for contradiction, that $xe \neq x$.

$$\Rightarrow yae \neq ya \Rightarrow ae \neq a,$$

a contradiction. Hence e fixes all elements of U . We have that $\exists a_1, a_2, \dots, a_k \in A$, for some $k \in \mathbb{N}$ such that

$$a_1 a_2 \cdots a_k = e \Rightarrow a_1 a_2 \cdots a_k \upharpoonright_U = \text{id}_U.$$

Since $|\text{im}(\text{id}_U)| = |U|$, we have that all the generators that product to e have image of at least the same size, when restricted to U . Since we only have $|U|$ states to map from, the sizes of the images the generators are at most $|U|$, and hence equal to U . Hence they are surjective maps from U to

U , and therefore permutations of U . In particular, we have at least one permutation of U in A , when restricting to U .

(\Leftarrow): Suppose A contains an element, t such that $t \upharpoonright_U$ is a permutation of U . Since $t \upharpoonright_U \in S_U$, the symmetric group on U , we have that $(t \upharpoonright_U)^n = \text{id}_U$ for some $n \in \mathbb{N}$, which is the order of $t \upharpoonright_U$. Define a transformation $g = t^n$ (acting on X). Let $a \in A$, $x \in X$. If $x \in U$, then

$$xg = xt^n = xt^n \upharpoonright_U = x,$$

$$\implies xga = xa,$$

If $x \notin U$, then

$$xga = xag = xat^n.$$

Since $xa \in U$, we have that t^n fixes it. Hence

$$xga = xa.$$

Hence $xga = xa$, $\forall x \in X$, $a \in A$, and hence g acts as the identity on the generators of S . Let $h \in S$. Then $\exists a_1, a_2, \dots, a_k \in A$, for some $k \in \mathbb{N}$, possibly with repeats, such that $h = a_1 a_2 \cdots a_k$. Note $a_k g = g$. Then

$$\begin{aligned} hg &= a_1 a_2 \cdots a_k g \\ &= a_1 a_2 \cdots a_k \\ &= h \end{aligned}$$

Hence g is the identity of S , and S is a monoid.

Definition 2.2 Let S be a finite semigroup, $g \in S$. Let t be the smallest non-negative integer such that $\exists k \in \mathbb{N}$ such that

$$g^t = g^{t+k}.$$

The *threshold* of g is defined to be t , and the *period* to be the smallest $p \in \mathbb{N}$ such that

$$g^t = g^{t+p}.$$

The *threshold* and *period* of S are defined to be the maximum of the thresholds and the lowest common multiple of the periods of the elements of S . If the period of S is 1, S is called *aperiodic*.

Lemma 2.3 Let A be a set of transformations of a finite set X . If the elements of A commute with one another, then $\langle A \rangle$ is commutative.

Proof Let $g, h \in \langle A \rangle$. We have that $g = a_1 \cdots a_k$, $h = b_1 \cdots b_l$, for some $k, l \in \mathbb{N}$, $a_i, b_j \in A, \forall i \leq k, j \leq l$. Then

$$gh = a_1 \cdots a_k b_1 \cdots b_l = b_1 \cdots b_l a_1 \cdots a_k = hg.$$

Lemma 2.4 Let S be a transformation semigroup, generated by a set A . Let an element $a_i \in A$ have threshold t_i and period p_i . Then for any $g \in \langle A \rangle$, with threshold t and period p , we have

$$t \leq \max_i(t_i), \quad p \mid \text{lcm}_i(p_i).$$

Proof Let $g, h \in S$ and let T be the maximum of the thresholds of g and h . Let p_g, p_h denote the periods of g, h respectively. Then

$$(gh)^{T+p_g p_h} = g^{T+p_g p_h} h^{T+p_g p_h} = g^T h^T = (gh)^T.$$

Hence the threshold of gh is less than or equal to T . Therefore, it follows that any element of S has threshold less than the maximum of the thresholds of the generators, by induction on the number of generators in the factorisation.

Let P be the lowest common multiple of the periods of the elements of A . Let $g \in S$ have threshold t and period p . Then $g = a_1 \cdots a_k$, for some $a_1, \dots, a_k \in A$.

$$g^{t+P} = a_1^{t+P} \cdots a_k^{t+P} = a_1^t \cdots a_k^t = g^t.$$

Hence $p \leq P$. Note $P - p \in \mathbb{N}_0$. We have

$$g^{t+P-p} = g^{t+P} = g^t.$$

Let $q = \left\lfloor \frac{P}{p} \right\rfloor$. Then

$$g^{t+P-qp} = g^t.$$

as $P - qp \geq 0$. Suppose $P - qp \neq 0$. Then $P - p \left\lfloor \frac{P}{p} \right\rfloor < p$, a contradiction to the minimality of p . Hence $P = qp$ and $p|P$.

Definition 2.5 Let S be a commutative semigroup acting on a finite set X . The *centraliser* of S , denoted C_S is the set of all transformations of X that commute with all elements of S .

Note that elements of the centraliser are not necessarily in S , and do not have to commute with all elements of the centraliser.

Definition 2.6 Let X be a finite set. The *full transformation monoid* on X , denoted T_X , is the set of all transformations from X to X , together with the binary operation of composition of functions.

Lemma 2.7 Let S be a commutative transformation semigroup, generated by a set A acting on a finite set X . Let $f \in T_X$. Then

$$f \in C_S \iff af = fa, \quad \forall a \in A.$$

Proof (\Rightarrow): Suppose $f \in C_S$. Then f commutes with all elements of S , and hence all elements of A , since $A \subseteq S$.

(\Leftarrow): Suppose $af = fa, \forall a \in A$. Let $g \in S$. We have that $\exists a_1, a_2, \dots, a_k \in A$, for some $k \in \mathbb{N}$ such that

$$g = a_1 a_2 \cdots a_k.$$

Hence

$$fg = fa_1 a_2 \cdots a_k = a_1 f a_2 \cdots a_k = \cdots = a_1 a_2 \cdots a_k f = gf.$$

Hence f commutes with g and it follows that $f \in C_S$.

3 The Induced Aperiodic Semigroup

Definition 3.1 Let S be a transformation semigroup acting on a finite set X . Given a state $x \in X$, define the *strongly connected component (SCC)* of x , denoted \bar{x} , by

$$\bar{x} = \{y \in X : \exists g, h \in S^1 \text{ such that } x = yg, y = xh\}.$$

The set of all SCCs of S will be denoted

$$\bar{X} = \{\bar{x} : x \in X\}.$$

Lemma 3.2 *Let S be a transformation semigroup acting on a finite set X . The SCCs of the elements of X partition X .*

Proof Define the relation \sim on X , for $x, y \in X$ by,

$$x \sim y \text{ if } y \in \bar{x}.$$

Note for any $x \in X$, we have $x = x * e = e * x$, where e is the identity of S^1 , so $x \in \bar{x}$ and hence $x \sim x$ and \sim is reflexive.

Let $x, y \in X$ such that $x \sim y$. Hence $\exists g, h \in S^1$ such that

$$x = yg, \quad y = xh.$$

Hence $x \in \bar{y}$ and we have that $y \sim x$, so \sim is symmetric.

Let $x, y, z \in X$, such that $x \sim y, y \sim z$. Then $\exists g_1, g_2, h \in S^1$, such that

$$x = yg_1, \quad y = xg_2, \quad y = zh.$$

$$\implies x = zhg_2, \quad z = xg_2h.$$

Since S^1 is closed, we have that $hg_2, g_2h \in S^1$. Hence $z \in \bar{x}$ and we have that $x \sim z$ and \sim is transitive.

Hence \sim is an equivalence relation, and therefore it partitions X into equivalence classes. The equivalence class of a given $x \in X$ is

$$\{y \in X : y \in \bar{x}\} = \bar{x},$$

so the equivalence classes are the SCCs.

Proposition 3.3 *Let S be a commutative semigroup acting on a finite set X . We have that*

$$\forall x \in X, g \in C_S, \quad \bar{x}g \subseteq \overline{xg}.$$

Let $g \in C_S$. We have that there exists a transformation \bar{g} of \bar{X} , such that $\forall x \in X, \bar{x}\bar{g} = \overline{xg}$. In addition, there is a homomorphism that maps every $g \in C_S$ to the corresponding \bar{g} .

Proof Let $x \in X, g \in C_S$. We have

$$y \in \bar{x}g \implies \exists z \in \bar{x} \text{ such that } y = zg.$$

Since $z \in \bar{x}$, $\exists f, h \in S$ such that $z = xf, x = zh$.

$$\implies y = zg = xfg = xgf, \quad xg = zhg = zgh = yh.$$

So $y \in \bar{x}g$ and it follows that $\bar{x}g \subseteq \bar{x}\bar{g}$.

Define \bar{g} as a transformation of \bar{X} as follows. For any $x \in X$, $\bar{x}\bar{g} = \overline{xg}$. We will show this function is well-defined. Let $x, y \in X$ such that $\bar{x} = \bar{y}$. Since \bar{X} is a partition of X , and $\bar{x}\bar{g}, \bar{y}\bar{g}$ are SCCs, we have that they are equal if they are not disjoint.

$$xg \in \bar{x}g \subseteq \overline{xg} = \bar{x}\bar{g}$$

$$xg \in \bar{y}g \subseteq \overline{xg} = \bar{y}\bar{g}$$

Hence $xg \in \bar{y}\bar{g} \cap \bar{x}\bar{g}$, and it follows that $\bar{x}\bar{g} = \bar{y}\bar{g}$.

Let $g, h \in C_S, \bar{x} \in \bar{X}$. We have

$$\bar{x}\bar{g}\bar{h} = \overline{xg\bar{h}} = \overline{xgh} = \bar{x}\overline{gh}.$$

So the map that sends an element $g \in C_S$ to \bar{g} is a homomorphism.

Lemma 3.4 *A commutative transformation semigroup acting on a finite set is aperiodic if and only if all of its SCCs are singletons.*

Proof Let S be a commutative transformation semigroup acting on a finite set X .

(\Rightarrow): Suppose S is aperiodic. Let $x, y \in X$, $x \neq y$. Suppose, for contradiction, that $x, y \in \bar{x}$. Then $\exists g, h \in S^1$ such that $x = yg, y = xh$. Let T be the maximum of the thresholds of g, h . We have

$$ygh = y \implies y = y(gh)^T = yg^T h^T \implies xg^T h^T g = x \implies yg^{T+1} h^T = x \neq y.$$

We therefore have that $g^T \neq g^{T+1}$, so the threshold of g is greater than T , a contradiction.

(\Leftarrow): Suppose all the SCCs of S are singletons. Let $g \in S$, $x \in X$. Let $n = |X|$. Let t be the threshold of g . Then $xg^t = xg^j$, for some $j \leq n, t < j$, and let j be minimal. We have

$$xg^{t+1} = xg^t g,$$

and

$$xg^t = xg^j = xg^{t+1} g^{j-t-1},$$

which implies $xg^t, xg^{t+1} \in \overline{xg^t}$. Since this is a singleton, we have that $xg^t = xg^{t+1}$ and hence the period of g is 1, so S is aperiodic.

Definition 3.5 Let S be a commutative transformation semigroup, acting on a finite set X . The *induced aperiodic semigroup* of S , denoted \bar{S} , is defined by

$$\bar{S} = \{\bar{g} : g \in S\},$$

together with the binary operation composition of functions.

Corollary 3.6 *Let S be a commutative transformation semigroup, generated by a set A acting on a finite set X . The induced aperiodic semigroup of S is a commutative aperiodic semigroup, generated by the set $\bar{A} = \{\bar{g} : g \in A\}$.*

Proof Since mapping any $g \in S$ to \bar{g} is a homomorphism, and \bar{S} is the homomorphic image of this homomorphism, we have that \bar{S} is a semigroup.

Let $\alpha, \beta \in \bar{S}$. Then $\exists g, h \in S$ such that $\alpha = \bar{g}$, $\beta = \bar{h}$. We have

$$\alpha\beta = \bar{g}\bar{h} = \overline{gh} = \overline{hg} = \bar{h}\bar{g} = \beta\alpha,$$

and therefore \bar{S} is commutative.

To show \bar{S} is aperiodic, it suffices to show that the SCCs of \bar{S} are singletons, by Lemma 3.4. Let $x \in X$. Suppose that $\exists y \in X$, $g, h \in S$ such that

$$\bar{y} = \bar{x}\bar{g}, \quad \bar{x} = \bar{y}\bar{h}.$$

$$\implies xg \in \bar{y}.$$

Hence $\exists f_1 \in S$ such that $y = xgf_1$. We also have

$$yh \in \bar{x}.$$

It therefore follows that $\exists f_2 \in S$ such that $x = yhf_2$. Together with $y = xgf_1$, we conclude that $x, y \in \bar{x}$ and hence $\bar{x} = \bar{y}$, recalling that \bar{X} is a partition of X by Lemma 3.2. Hence the SCC that \bar{x} is in, with respect to \bar{S} is a singleton.

Let $g \in S$. Since $S = \langle A \rangle$, $\exists a_1, \dots, a_n \in A$ such that $g = a_1 \cdots a_n$. Since mapping any $h \in S$ to \bar{h} is a homomorphism, we have

$$\bar{g} = \overline{a_1 \cdots a_n} = \bar{a}_1 \cdots \bar{a}_n.$$

So \bar{g} can be written as a product of elements of \bar{A} , and hence

$$\bar{S} = \langle \bar{A} \rangle.$$

4 Stabilisers of Strongly Connected Components

Definition 4.1 Let S be a transformation semigroup, acting on a finite set X . Let $\bar{x} \in \bar{S}$. A transformation $g \in S$ *stabilises* \bar{x} , if $\bar{x}\bar{g} = \bar{x}$. The *stabiliser* of \bar{x} , denoted $\text{Stab}(\bar{x})$, is the set of all elements of S that stabilise \bar{x} .

Definition 4.2 Let G be a permutation group acting on a finite set X . The group G is *transitive* if $\forall x, y \in X$, $\exists g \in G$ such that $y = xg$. If, in addition, this g is always unique, then G has *regular action*.

Lemma 4.3 *Every transitive abelian group has regular action.*

Proof Let G be a transitive abelian group, acting on a set X . Let $x, y \in X$. By transitivity of G , $\exists g \in G$ such that $y = xg$. Suppose $\exists h \in G$ such that $y = xh$. Then $xh = xg$. Let $z \in X$. By transitivity $\exists f \in G$ such that $x = zf$. Therefore,

$$xg = xh \implies zfg = zfh \implies zgf = zhf \implies zg = zh.$$

Hence $zh = zf$, $\forall z \in X$, so $g = h$.

Proposition 4.4 *Let S be a commutative transformation semigroup, generated by a set A , acting on a finite set X . Let $x \in X$. If $\text{Stab}(\bar{x})$ is non-empty, then the restriction of $\text{Stab}(\bar{x})$ to the SCC \bar{x} is an abelian permutation group with regular action, generated by $\text{Stab}(\bar{x}) \cap A$.*

Proof Let $x \in X$, $g, h \in \text{Stab}(\bar{x})$. We therefore have that $\bar{x}g = \bar{x}$, $\bar{x}h = \bar{x}$ so $\bar{x}gh = \bar{x}h = \bar{x}$ and hence $gh \in \text{Stab}(\bar{x})$.

Let $y, z \in \bar{x}$. We have that $\exists g \in S^1$ such that $y = zg$. Let $w \in \bar{x}$. Hence $\exists h \in S^1$ such that $w = yh$. By Proposition 3.3, we have

$$\begin{aligned} \bar{w}g &\subseteq \bar{w}g \\ \implies \bar{x}g &\subseteq \bar{w}g. \end{aligned}$$

Note that $y \in \bar{x}$ and $y = zg$ so $y \in \bar{x}g \subseteq \bar{w}g$. Hence $y \in \bar{x} \cap \bar{w}g$. Since these are both SCCs, and SCCs are disjoint or equal, because \bar{X} partitions X , it follows that $\bar{w}g = \bar{x}$. In particular $wg \in \bar{x}$ and hence $g \in \text{Stab}(\bar{x})$. We therefore have that the maps that send elements of an SCC to each other, as mentioned in the definition of an SCC, are in the stabiliser of that SCC.

Let $g_1 \in \text{Stab}(\bar{x})$. Let $y = xg_1$. We have that $\exists g_2 \in \text{Stab}(\bar{x})$ such that $x = yg_2$. Let $z \in \bar{x}$. We have that $\exists h \in \text{Stab}(\bar{x})$ such that $z = xh$. Then

$$zg_2g_1 = zg_1g_2 = xhg_1g_2 = xg_1g_2h = yg_2h = xh = z,$$

and hence g_2g_1 acts as the identity on \bar{x} and hence is the identity of $\text{Stab}(\bar{x})$, when restricted to \bar{x} . We also have that g_2 is the inverse of g_1 , on \bar{x} . Since it has an inverse, g_1 must be injective, when restricted to \bar{x} , and since it is a transformation of a finite set, we have that g_1 is a permutation of \bar{x} .

Therefore $\text{Stab}(\bar{x})$ is a permutation group, when restricted to \bar{x} . Since the transformation that maps any element of the \bar{x} to any other is always in $\text{Stab}(\bar{x})$, it follows that $\text{Stab}(\bar{x})$ is transitive.

We now have that $\text{Stab}(\bar{x})$ is a transitive abelian group, when acting on \bar{x} . By Lemma 4.3, it has regular action.

To prove that $\text{Stab}(\bar{x})$ is generated by $\text{Stab}(\bar{x}) \cap A$, we will proceed by contradiction. Let $g \in \text{Stab}(\bar{x})$ be expressed as a product of elements of A by

$$g = a_1^{\gamma_1} a_2^{\delta_2} \cdots a_k^{\gamma_k} b_1^{\delta_1} b_2^{\delta_2} \cdots b_l^{\delta_l},$$

where $k, l \in \mathbb{N}$, and the generators denoted a_i for some $i \in \mathbb{N}$ are elements of $\text{Stab}(\bar{x})$, and the generators denoted b_i for some $i \in \mathbb{N}$ are not. Let $h = b_1^{\delta_1-1} b_2^{\delta_2} \cdots b_l^{\delta_l}$. We have

$$\bar{x} = \bar{x}g = \bar{x}b_1\bar{h}.$$

Since $b_1 \notin \text{Stab}(\bar{x})$, $\bar{x}b_1 \neq \bar{x}$ but $\bar{x}b_1h_1 = \bar{x}$, which means that \bar{x} and $\bar{x}b_1$ are non-equal, but in the same SCC of \bar{S} . This contradicts \bar{S} being aperiodic, and therefore only having singleton SCCs, by Corollary 3.6.

Corollary 4.5 *Let S be a commutative transformation semigroup acting on a finite set X . Let $x \in X, g \in S$. If g stabilises \bar{x} , then g acts as a permutation on \bar{x} .*

Proof Let g stabilise \bar{x} . By Proposition 4.4, we have that since $\text{Stab}(\bar{x})$ is a permutation group, when restricted to \bar{x} , we have that $g \upharpoonright_{\bar{x}}$ is a permutation.

Corollary 4.6 *Let S be a commutative transformation semigroup acting on a finite set X . Let $g \in S$. The thresholds of g and \bar{g} are equal.*

Proof Let t be the threshold of g and p be the period. Let u be the threshold of \bar{g} . Let $x \in X$. We have

$$\bar{x}\bar{g}^t = \bar{x}\bar{g}^t = \overline{xg^t},$$

since the map that sends every $f \in C_S$ to \bar{f} is a homomorphism. It therefore follows that

$$\bar{x}\bar{g}^{t+p} = \overline{xg^{t+p}} = \overline{xg^t} = \bar{x}\bar{g}^t,$$

and hence $u \leq t$.

Note also that

$$\overline{xg^u} = \bar{x}\bar{g}^u = \bar{x}\bar{g}^u\bar{g} = \overline{xg^u\bar{g}},$$

so g stabilises $\overline{xg^u}$. By Corollary 4.5, g permutes $\overline{xg^u}$. We have

$$xg^u \in \overline{xg^u} \implies xg^u g^{o(g \upharpoonright_{\overline{xg^u}})} = xg^u,$$

and hence $t \leq u$.

Definition 4.7 Let S be a commutative transformation semigroup acting on a finite set X . A state $x \in X$ is a *source* if $\forall y \in X \setminus \{x\}, g \in S, yg \neq x$. A *source-SCC* is defined to be a source of \bar{S} . The set of all source-SCCs of S will be denoted \bar{Y} , the union of all source-SCCs will be denoted Y .

Lemma 4.8 *Let S be a commutative transformation semigroup acting on a finite set. Let $f, g \in C_S$. If*

$$zg = zf, \quad \forall z \in Y,$$

then $f = g$.

Proof Let X be the set that S acts on. We already have that f, g coincide on all states in source-SCCs. Let $\bar{x} \in \bar{X} \setminus \bar{Y}$. Then there $\exists \bar{z} \in \bar{X}, \bar{g} \in \bar{S}$ such that $\bar{x} = \bar{z}\bar{g}$. If \bar{z} is a source-SCC, we have a sequence of maps in \bar{S} that take a source-SCC to \bar{x} . Otherwise apply this process to \bar{z} , and continue until a source-SCCs is reached.

This must happen after a finite number of steps, since \bar{X} is finite, and no repeats can appear in the sequence. This is because \bar{S} is aperiodic, and hence all of its SCCs are singletons, by Lemma 3.4. If we can get from one SCC to another by an element of \bar{S} , and back again, then these two element are in the same SCC of \bar{S} , a contradiction. We also have that there is a sequence of maps

in S that when the homomorphism $\psi : h \mapsto \bar{h}$ is applied to them, we obtain the sequence of maps in \bar{S} that take a source-SCC to \bar{x} . Let these maps be

$$h_1, h_2, \dots, h_k,$$

where $k \in \mathbb{N}$. Let $w \in X$, such that \bar{w} is a source SCC such that

$$\bar{x} = \bar{w}\bar{h}_1\bar{h}_2 \cdots \bar{h}_k.$$

Let

$$v = wh_1h_2 \cdots h_k.$$

Note $v \in \bar{x}$. Let $z \in \bar{x}$. Then $\exists l \in S$ such that $vl = z$. Hence

$$z = wh_1h_2 \cdots h_kl.$$

$$zf = wh_1h_2 \cdots h_klf = wfh_1h_2 \cdots h_kl = wgh_1h_2 \cdots h_kl = wh_1h_2 \cdots h_klg = zg,$$

and we have that f and g coincide on all states that are not in source-SCCs, and hence must be equal.

5 The Source Action Group

Definition 5.1 Let S be a commutative transformation semigroup acting on a finite set X , $f \in S$. For a transformation $g \in \bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x})$, define the *source action transformation* of g with respect to f , denoted \hat{g}_f , by

$$\hat{g}_f : X \rightarrow X$$

$$x \mapsto \begin{cases} xg & \bar{x} \in \bar{Y}\bar{f} \\ x & \text{otherwise} \end{cases}.$$

Define the *source action group* of f , denoted \hat{S}_f by

$$\hat{S}_f = \left\{ \hat{g}_f : g \in \bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \right\} \cup \{\text{id}\}.$$

Define

$$\hat{A}_f = \left\{ \hat{g}_f : g \in A \cap \left(\bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \right) \right\} \cup \{\text{id}\}.$$

Lemma 5.2 Let S be a commutative transformation semigroup acting on a finite set X , $f \in S$. The source action group of f is an abelian group, generated by \hat{A}_f , and isomorphic to

$$\bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \cup \{\text{id}\},$$

restricted to Yf . It has regular action when restricted to any $\bar{x} \in \bar{Y}\bar{f}$.

Proof Let

$$G = \left\{ g \downarrow_{Yf} : g \in \bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \cup \{\text{id}\} \right\}.$$

Define the mapping

$$\begin{aligned} \phi : G &\rightarrow \hat{S}_f \\ g &\mapsto \hat{g}_f \end{aligned}$$

As an intersection of abelian groups, we have that G is an abelian group, using Proposition 4.4, when restricted to Yf . We have, by definition of \hat{S}_f , that ϕ is surjective. Let $g, h \in S$ such that $g \downarrow_{Yf}, h \downarrow_{Yf} \in G$ and $\phi(g) = \phi(h)$. Let $x \in Yf$. We have

$$\hat{g}_f = \hat{h}_f \implies xg = xh \implies g \downarrow_{Yf} = h \downarrow_{Yf}.$$

Hence ϕ is injective. Let $g, h \in S$ such that $g \downarrow_{Yf}, h \downarrow_{Yf} \in G$. Let $x \in Yf$. We have

$$\begin{aligned} (x)\phi(g \downarrow_{Yf} h \downarrow_{Yf}) &= x\widehat{gh}_f \\ &= xgh \\ &= x\hat{g}_f\hat{h}_f \\ &= (x)\phi(g \downarrow_{Yf})\phi(h \downarrow_{Yf}) \end{aligned}$$

Hence ϕ is a homomorphism. We conclude that ϕ is an isomorphism from G to \hat{S}_f , and hence \hat{S}_f is a group. Since G is abelian, we have that \hat{S}_f is an abelian group. By Proposition 4.4, we have that $G \downarrow_{\bar{x}}$ has regular action, for any $\bar{x} \in \bar{Y}\bar{f}$. Let $x, y \in \bar{x}$. By regularity of the action of $G \downarrow_{\bar{x}}$, there is a unique $g \in G$ such that $xg = y$. Note that, since $x \in Yf$, we have

$$xg = y \implies x\hat{g}_f = y,$$

so $\hat{S}_f \downarrow_{\bar{x}}$ is transitive. As a transitive abelian group, we have that $\hat{S}_f \downarrow_{\bar{x}}$ has regular action, by Lemma 4.3.

Let $g \in G$, such that $g = hk$ for some $h, k \in S \downarrow_{\bar{Y}\bar{f}}$. Let $\bar{x} \in \bar{Y}\bar{f}$. Suppose, for contradiction, that $\bar{x}\bar{h} = \bar{y} \neq \bar{x}$. Then, since $\bar{x}\bar{g} = \bar{x}$, as $g \in \text{Stab}(\bar{x})$, we have that $\bar{y}\bar{k} = \bar{x}$. Hence \bar{x}, \bar{y} are strongly connected, a contradiction to the fact that they are SCCs. Therefore, the list of generators in A that product to g all stabilise all $\bar{x} \in \bar{Y}\bar{f}$. Hence G is generated by

$$\left\{ g \downarrow_{Yf} : g \in A \cap \left(\bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \right) \cup \{\text{id}\} \right\}.$$

Applying ϕ to this gives

$$\left\{ \hat{g}_f : g \in A \cap \left(\bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \right) \cup \{\text{id}\} \right\} = \hat{A}_f.$$

6 Membership Testing in Semilattices

Definition 6.1 Let S be a semigroup. An element $g \in S$ is an *idempotent* if $g^2 = g$. A *semilattice* is a commutative semigroup, such that every element is an idempotent.

Lemma 6.2 Let S be a transformation semilattice acting on a finite set X , and generated by a set A . Let $f \in C_S$. Let

$$B = \{a \in A : af = f\}.$$

Then $\exists C \subseteq A$, such that

$$f = \prod_{c \in C} c,$$

and

$$f \neq \prod_{c \in C \cup \{d\}} c,$$

for any $d \in A \setminus C$. In addition, $C = B$.

Proof Define C to be the union of all subsets $D \subseteq A$ such that

$$f = \prod_{d \in D} d.$$

Let D_1 be one of these subsets. We have that $C = D_1 \cup C \setminus D_1$ and that

$$f = \prod_{d \in D_1} d.$$

Let $g \in C \setminus D_1$. Then $\exists D_2 \subseteq A$ which products to f and contains g .

$$g \prod_{d \in D_1} d = gf = g \prod_{d \in D_2} d = \prod_{d \in D_2} d = f.$$

By repeating this, it follows that C products to f , due to the finiteness of A . Let $h \in A \notin C$. As h is not in any factorisation of f , we have that

$$f \neq \prod_{c \in C \cup \{h\}} c.$$

Let $b \in B$. We have that $bf = f$ and hence

$$f = \prod_{c \in C \cup \{b\}} c,$$

which implies $b \in C$. Hence $B \subseteq C$.

Let $c \in C$. Then

$$cf = c \prod_{c \in C} c = \prod_{c \in C} c = f,$$

so $c \in B$, and we have that $C \subseteq B$. Hence $B = C$.

Theorem 6.3 *Let S be a transformation semilattice acting on a finite set X , and generated by a set A . Let $f \in C_S$. Let*

$$B = \{a \in A : af = f\}.$$

Then $f \in S$ if and only if

$$f = \prod_{b \in B} b.$$

Proof (\Rightarrow): Suppose $f \in S$. By Lemma 6.2, we have that $B = C$, which is a factorisation of f over A .

(\Leftarrow): We have that $f \in S$, since f is a product of elements of S .

Algorithm 6.4 Let S be a transformation semilattice acting on a finite set X , and generated by a set A . Let $f \in C_S$. The following algorithm shows how to test if $f \in S$. The time complexity of this algorithm is $O(mn)$, where $m = |X|$, $n = |A|$.

1. Calculate B , as defined in Theorem 6.3.

2. Check if

$$f = \prod_{b \in B} b.$$

If so $f \in S$. Otherwise $f \notin S$.

Note that B is a factorisation for f into the generators of S .

7 Membership Testing for Transformations of Threshold 1

Lemma 7.1 *Let S be an commutative aperiodic transformation semigroup, generated by a set $A = \{a_1, a_2, \dots, a_n\}$, acting on a finite set X . Let t_1, t_2, \dots, t_n be the thresholds of a_1, a_2, \dots, a_n , respectively. Let $f \in C_S$ be an idempotent. Then $f \in S$ if and only if*

$$f \in \langle a_1^{t_1}, a_2^{t_2}, \dots, a_n^{t_n} \rangle.$$

Proof (\Rightarrow): Suppose $f \in S$. Then $f = a_1^{i_1} \cdots a_k^{i_k}$, for some $a_1, \dots, a_k \in A$, $i_1, \dots, i_k \in \mathbb{N}$. Let $b \in \{a_1, \dots, a_k\}$. Suppose $bf \neq f$. WLOG let $b = a_1$. We have that $\exists x \in X$ such that $xf a_1 \neq xf$. Let $y = xf$, $z = xf a_1$. We have

$$\begin{aligned} y &= xf \\ &= xf^2 \\ &= xfa_1^{i_1} a_2^{i_2} \cdots a_k^{i_k} \\ &= xfa_1 a_1^{i_1-1} a_2^{i_2} \cdots a_k^{i_k} \\ &= za_1^{i_1-1} a_2^{i_2} \cdots a_k^{i_k} \end{aligned}$$

By definition of y , z , we have that $ya_1 = z$. Together with the above, we have that y and z are in the same SCC of S , a contradiction to Lemma 3.4.

Therefore, we have that $bf = f$.

$$\implies a_1^{t_1-i_1} f = f$$

$$\begin{aligned} &\implies a_1^{t_1-i_1} f \cdot a_k^{t_k-i_k} f = f \\ &\implies f = a_1^{t_1-i_1} f \cdot a_k^{t_k-i_k} a_1^{i_1} \cdots a_k^{i_k} = a_1^{t_1} \cdots a_k^{t_k} \in \langle a_1^{t_1}, \dots, a_n^{t_n} \rangle. \end{aligned}$$

(\Leftarrow): Suppose $f \in \langle a_1^{t_1}, \dots, a_n^{t_n} \rangle$. Since this is a subset of S , we have that $f \in S$.

Lemma 7.2 *Let $f \in T_X$ for some finite set X . Then f has threshold less than or equal to 1 if and only if f permutes $\text{im } f$.*

Proof (\Rightarrow): Suppose f has threshold less than or equal to 1. Let p be the period of f , $x \in \text{im } f$. Hence $x = yf$ for some $y \in X$ and $f^{p+1} = f$. We have

$$f = f^{p+1} \implies yf = yf^{p+1} \implies x = xf^p.$$

Hence $f^p \upharpoonright_{\text{im } f} = \text{id}_{\text{im } f}$, and therefore $f \upharpoonright_{\text{im } f}$ is a permutation, since

$$|\text{im } f \upharpoonright_{\text{im } f}| = \cdots = |\text{im } f^p \upharpoonright_{\text{im } f}|, \quad \text{im } f^p \subseteq \cdots \subseteq \text{im } f.$$

(\Leftarrow): Suppose $f \upharpoonright_{\text{im } f}$ is a permutation. Then $(f \upharpoonright_{\text{im } f})^{o(f \upharpoonright_{\text{im } f})} = \text{id}_{\text{im } f}$. Let $x \in X$. We have that $xf \in \text{im } f$. Hence

$$xf \cdot f^{o(f \upharpoonright_{\text{im } f})} = xf.$$

Therefore

$$f = f \cdot f^{o(f \upharpoonright_{\text{im } f})} = f^{o(f \upharpoonright_{\text{im } f})+1}.$$

Hence the threshold of g is less than or equal to 1. Since we know that $g \neq \text{id}$, we have that g has threshold less than or equal to 1.

Theorem 7.3 *Let S be a commutative transformation semigroup, generated by a set A , acting on a finite set X . Let $f \in C_S$ have threshold less than or equal to 1. Suppose $\exists \lambda_f \in S^1$ such that $\bar{\lambda}_f = \bar{f}$. Then $f \in S^1$ if and only if $\hat{\mu}_f \in \hat{S}$ such that*

$$yf = y\lambda_f\hat{\mu}_f, \quad \forall y \in Y.$$

Proof (\Rightarrow): Suppose $f \in S^1$. By Corollary 4.6, we have that the threshold of \bar{f} is less than or equal to 1. Since \bar{f} is aperiodic, it follows that \bar{f} is an idempotent. Let \bar{Y} denote the set of source-SCCs of S . We have $\forall \bar{x} \in \bar{Y}$ that

$$\bar{x}\bar{f}^2 = \bar{x}\bar{f} \implies \bar{x}f \subseteq \bar{x}f^2.$$

Since f is a permutation on its image, by Lemma 7.2, we have that $\bar{x}f = \bar{x}$, $\forall \bar{x} \in \bar{Y}\bar{f}$, and hence $f \in \text{Stab}(\bar{x})$, $\forall \bar{x} \in \bar{Y}\bar{f}$. Note that since $\bar{\lambda}_f = \bar{f}$, we have that the threshold of λ_f is also less than or equal to 1, and hence $\lambda_f \in \text{Stab}(\bar{x})$, $\forall \bar{x} \in \bar{Y}\bar{f}$. Try $\hat{\mu} = \hat{f}_f(\hat{\lambda}_f)^{-1}$. Let $y \in Y$. We have

$$\begin{aligned} y\lambda_f\hat{\mu} &= y\lambda_f\hat{f}_f(\hat{\lambda}_f)^{-1} \\ &= y\lambda_f f(\hat{\lambda}_f)^{-1} \\ &= yf\lambda_f(\hat{\lambda}_f)^{-1} \\ &= yf\hat{\lambda}_f(\hat{\lambda}_f)^{-1} \\ &= yf \end{aligned}$$

(\Leftarrow): Suppose $\exists \lambda_f \in S^1$, $\hat{\mu}_f \in \hat{S}^1$ such that

$$\bar{f} = \bar{\lambda}_f, \quad yf = y\lambda_f\hat{\mu}_f, \quad \forall y \in Y.$$

Let $g \in \bigcap_{\bar{x} \in \bar{Y}\bar{f}} \text{Stab}(\bar{x}) \cup \{\text{id}\}$ be such that $\hat{g}_f = \hat{\mu}_f$. Let $y \in Y$. We have

$$\bar{y}\bar{f} = \bar{y}\bar{\lambda}_f, \quad \bar{y}\bar{f}\bar{g} = \bar{y}\bar{f},$$

since g is a transformation which stabilises every SCC in $\bar{Y}\bar{f}$. We also have that

$$y\lambda_f \in \bar{y}\bar{\lambda}_f = \bar{y}\bar{f} \in \bar{Y}\bar{f}.$$

Hence

$$yf = y\lambda_f\hat{\mu}_f = y\lambda_f\hat{g}_f = y\lambda_fg.$$

By Lemma 4.8, we have $f = \lambda_fg$. Therefore $f \in S^1$.

Algorithm 7.4 Let S be a commutative transformation semigroup, generated by a set A , acting on a finite set X . Let $f \in T_X$ have threshold less than or equal to 1. The following algorithm shows how to test if $f \in S$ in polynomial time.

1. Check if f acts as the identity on S . If so, check if A contains an element that permutes the set $\bigcup_{a \in A} \text{im } a$. If so and f is equal to the identity of S , then $f \in S$. Otherwise $f \notin S$.
2. Check if $af = fa$, $\forall a \in A$. If not $f \notin S$.
3. Build $\bar{X}, Y, \bar{A}, \hat{A}_f$.
4. Check if $\bar{f} \in \bar{S}$. If not $f \notin S$. If so find a $\lambda_f \in S^1$, written as a product of elements of A , such that $\bar{f} = \bar{\lambda}_f$.
5. Construct a spanning tree T , with root xf for some $x \in X$, of the digraph with vertex set Yf , and an edge from any $y \in Yf$ to any $z \in Yf$, if $\exists a \in \hat{A}$ such that $ya = z$.
6. For each element of \bar{y} of \bar{Y} and any $x \in \bar{y}$, find the path in T that takes $x\lambda_f$ to the root, xf , and define $\hat{\mu}_f$, on this subset of Yf to be the product of the sequence of generators in this path.
7. Check if $yf = y\lambda_f\hat{\mu}_f$, $\forall y \in Y$. If not $f \notin S$.
8. Check if $\hat{\mu}_f \in \hat{S}_f$. If so $f \in S$. Otherwise $f \notin S$.

If f acts as the identity on S , then Step 1 checks if S is a monoid, and if so, checks if f is the identity of S . This allows subsequent steps to assume S is a monoid. This uses Lemma 2.1.

Step 2 checks if $f \in C_S$, using Lemma 2.7.

Step 3 constructs the generating sets of the induced aperiodic semigroup and source action group of S , with respect to f . This uses Corollary 3.6 and Lemma 4.8.

Step 4 requires membership testing and factorisation in a semilattice. We have that \bar{f} is aperiodic and has threshold less than or equal to 1, by Corollary 4.6. Therefore \bar{f} is an idempotent. By Lemma 7.1, it suffices to check if \bar{f} is in the semigroup generated by the generators of \bar{S} , raised to the power of their thresholds, which is a semilattice. Since the membership testing algorithm for semilattices in Algorithm 6.4 yields a factorisation, we can obtain a factorisation for \bar{f} into powers of the generators of \bar{S} . Since the mapping $g \mapsto \bar{g}$ is a homomorphism, we can obtain a λ_f by producting and powering the generators in A , that are sent to the generators in \bar{A} , in the factorisation of \bar{f} .

Steps 5 and 6 are used to construct a transformation $\hat{\mu}_f$. It suffices to check one element of each SCC, because of the regular action of \hat{S}_f on each SCC in $\bar{Y}\bar{f}$. Together with λ_f , we potentially have the conditions mentioned in Theorem 7.3, provided $yf = y\lambda_f\hat{\mu}_f$, $\forall y \in Y$.

Step 7 checks if $f = \lambda_f\hat{\mu}_f$, $\forall y \in Y$. Step 8 checks if $\hat{\mu}_f \in \hat{S}_f$. This can be done in polynomial time, using the Schreier-Sims algorithm.

8 Testing Membership in Semigroups of Threshold 1

Definition 8.1 A semigroup S is *regular* if $\forall g \in S$, $\exists h \in S$ such that $ghg = g$.

Note that this is not the same as having regular action.

Lemma 8.2 Let S be a regular commutative transformation semigroup acting on a finite set. Then S has threshold less than or equal to 1.

Proof Let $g \in S$. Then $\exists h \in S$ such that $ghg = g$. Hence $g^2h = g$. Let $x \in \text{im } g$. We have $(xg)h = x$, $(x)g = (xg)$, and hence x, xg are in the same SCC. Therefore $\bar{g} = \bar{g}^2$, so \bar{g} has threshold less than or equal to 1. By Corollary 4.6 we have that the threshold of g is less than or equal to 1.

Definition 8.3 A semigroup S is *completely regular* if every element of S lies in a subgroup of S .

Lemma 8.4 Every completely regular semigroup is regular.

Proof Let S be a completely regular semigroup. Let $g \in S$ be in a subgroup $G \leq S$. Let $h \in S$ be the element that acts as the inverse of g in G . Then

$$g = ghg.$$

Definition 8.5 A regular semigroup S is a *Clifford semigroup* if its idempotents are central.

Algorithm 8.6 Let S be a commutative transformation semigroup, acting on a finite set X , of threshold less than or equal to 1. Let $f \in T_X$. The following algorithm tests if $f \in S$ in polynomial time.

1. Check if f permutes its image. If not $f \notin S$.
2. Run Algorithm 7.4 to test if $f \in S$.

Step 1 uses Lemma 7.2 to test if f has threshold less than or equal to 1. Step 2 can therefore assume that f has threshold 1, and use Algorithm 7.4.

9 Counter-Example to Algorithm in [1]

Throughout this section, a transformation f of the set $\{1, \dots, n\}$ will be represented as the list $(1f \dots nf)$. The notation used throughout the paper will be mostly the same as the notation in [1].

Algorithm 9.1 The following algorithm is given in [1] as a general algorithm for membership testing in a commutative transformation semigroup. We have adapted the notation to be consistent with the notation defined throughout this paper. Here the semigroup in question will be S , generated by a set A , and acting on a finite set X . The test transformation will be $f \in T_X$.

1. Test whether $af = fa$ for every $a \in A$.
2. Build \bar{X} , \bar{Y} , \bar{A} , \hat{A}_f , the latter two generate the semigroups \bar{S} , \hat{S}_f .
3. Test whether $\bar{f} \in \bar{S}$. If so, find a $\lambda_f \in S$ such that $\bar{\lambda}_f = \bar{f}$.
4. Build a transformation $\hat{\mu}_f$ such that for every $x \in Y$, $x\lambda_f\hat{\mu}_f = xf$.
5. Test whether $\hat{\mu}_f \in \hat{S}_f$.

Example 9.2 Here we will give a counter-example to Algorithm 9.1.

Let $X = \{1, \dots, 7\}$. Let $A = \{a, b, c\}$, where

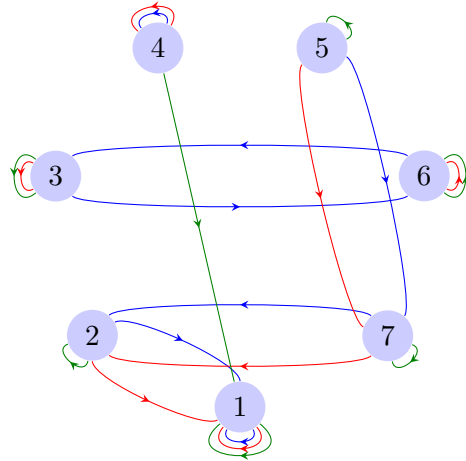
$$a = (1 \ 1 \ 6 \ 4 \ 7 \ 3 \ 2), \ b = (1 \ 1 \ 3 \ 4 \ 7 \ 6 \ 2), \ c = (1 \ 2 \ 3 \ 1 \ 5 \ 6 \ 7).$$

Let $S = \langle A \rangle$. Note that

$$ab = (1 \ 1 \ 6 \ 4 \ 2 \ 3 \ 1) = ba, \ ac = (1 \ 1 \ 6 \ 1 \ 7 \ 3 \ 2) = ca, \ bc = (1 \ 1 \ 3 \ 1 \ 7 \ 6 \ 2) = cb.$$

Hence S is commutative. Let $f = (1 \ 1 \ 3 \ 1 \ 7 \ 6 \ 2)$. We have

$$af = (1 \ 1 \ 6 \ 1 \ 2 \ 3 \ 1) = fa, \ bf = (1 \ 1 \ 3 \ 1 \ 2 \ 6 \ 1) = fb, \ cf = (1 \ 1 \ 3 \ 1 \ 7 \ 6 \ 2) = fc,$$



We therefore have that the set of SCCs is

$$\bar{X} = \{\{1\}, \{3, 6\}, \{4\}, \{5\}, \{7\}\},$$

and the set of source-SCCs is

$$\bar{Y} = \{\{3, 6\}, \{4\}, \{5\}\}.$$

Note that

$$\bar{f} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{7} \\ \bar{1} & \bar{1} & \bar{3} & \bar{1} & \bar{7} & \bar{2} \end{pmatrix},$$

$$\bar{a} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{7} \\ \bar{1} & \bar{1} & \bar{3} & \bar{4} & \bar{7} & \bar{2} \end{pmatrix}, \quad \bar{b} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{7} \\ \bar{1} & \bar{1} & \bar{3} & \bar{4} & \bar{7} & \bar{2} \end{pmatrix}, \quad \bar{c} = \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{7} \\ \bar{1} & \bar{2} & \bar{3} & \bar{1} & \bar{5} & \bar{7} \end{pmatrix}.$$

Hence $\bar{Y}\bar{f} = \{\bar{3}, \bar{1}, \bar{7}\}$ and $Yf = \{1, 3, 6, 7\}$. The only $a \in A$ which fixes all SCCs in $\bar{Y}\bar{f}$ is $c = (1\ 2\ 3\ 1\ 5\ 6\ 7)$. Note that $\hat{c}_f = id$. Hence $\hat{S}_f = \langle id \rangle = \{id\}$.

The elements of S are

$$(1\ 1\ 6\ 4\ 7\ 3\ 2), (1\ 1\ 3\ 4\ 7\ 6\ 2), (1\ 2\ 3\ 1\ 5\ 6\ 7), (1\ 1\ 3\ 4\ 2\ 6\ 1), (1\ 1\ 6\ 4\ 2\ 3\ 1),$$

$$(1\ 1\ 6\ 1\ 7\ 3\ 2), (1\ 1\ 3\ 1\ 7\ 6\ 2), (1\ 1\ 6\ 4\ 1\ 3\ 1), (1\ 1\ 3\ 4\ 1\ 6\ 1),$$

$$(1\ 1\ 3\ 1\ 2\ 6\ 1), (1\ 1\ 6\ 1\ 2\ 3\ 1), (1\ 1\ 6\ 1\ 1\ 3\ 1), (1\ 1\ 3\ 1\ 1\ 6\ 1).$$

Therefore, the only potential candidates for λ_f , as mentioned in [1], are

$$(1\ 1\ 6\ 1\ 7\ 3\ 2), (1\ 1\ 3\ 1\ 7\ 6\ 2),$$

the latter one being f .

Try taking $\lambda_f = (1\ 1\ 6\ 1\ 7\ 3\ 2)$. The algorithm in [1], suggests that $\exists \hat{\mu}_f \in \hat{S}_f$ such that $\forall y \in Y, yf = y\lambda_f\hat{\mu}_f$. However, since the only potential candidate for $\hat{\mu}_f$ is id , we have that

$$3\lambda_f\hat{\mu}_f = 6 \neq 3f, \quad \forall \hat{\mu}_f \in \hat{S}_f.$$

Therefore by the algorithm in [1], it should follow that $f \notin S$, which is not true.

References

- [1] Martin Beaudry. Membership testing in commutative transformation semigroups. *Information and Computing*, 79:84–93, October 1988.
- [2] J. D. Mitchell et al. *Semigroups - GAP package, Version 3.0.3*, Jun 2017.