where $\pi$ is the set of distinct orbits of $Q$ defined by $\Gamma$, and $\Gamma$ is the transformation group defined by $\Gamma$.

*Proof* Let $Q = K_1 \cup \ldots \cup K_n$ be the decomposition of $Q$ into the orbits defined by $\Gamma$, and let $k_i \in K_i$ be fixed orbit representatives. Then $Q = \bigcup_{i=1}^{n} k_i\Gamma$. The elements of $\Gamma$ act as fixed point free permutations of $Q$, for if $\gamma \in \Gamma$, $q\gamma = q$ and we choose any $q' \in Q$ then $q' = qs$ for some $s \in S$ and $q'\gamma = qs\gamma = q\gamma s = qs = q'$ which makes $\gamma$ equal to $1_Q$. The partition $\pi = \{k_i\Gamma\}_{i=1,\ldots,n}$ is admissible. Putting $K = \{k_1, \ldots, k_n\}$, $\Gamma = \{\gamma_1, \ldots, \gamma_r\}$ and using the fact that the elements of $\Gamma$ are fixed point free, we see that $\tau = \{K\gamma_1, \ldots, K\gamma_r\}$ is another partition satisfying the relationship $\pi \cap \tau = 1_Q$. We can then apply 3.3.2 to obtain a covering of $A$. However it is quicker to proceed directly.

Let $\phi : \Gamma \times \pi \to Q$ be defined by

$$\phi(\gamma, k_i\Gamma) = k_i\gamma^{-1} \quad \text{for } \gamma \in \Gamma,\ k_i\Gamma \in \pi.$$

This is a surjective function onto $Q$. Now choose any $s \in S$, then $s$ defines an element $[s]$ of the semigroup of $\mathscr{A}/\langle\pi\rangle$. Let $f_s : \pi \to \Gamma$ be the function defined by

$$f_s(k_i\Gamma) = \bar{\gamma}^{-1}$$

where $k_i s \in K\bar{\gamma}$ for a unique $\bar{\gamma} \in \Gamma$.

Now choose $s \in S$, $\gamma \in \Gamma$, $k_i\Gamma \in \pi$ then

$$\begin{aligned}\phi((\gamma, k_i\Gamma)(f_s, [s])) &= \phi(\gamma * f_s(k_i\Gamma), k_i\Gamma[s])\\ &= \phi(\gamma * (\bar{\gamma})^{-1}, k_t\Gamma) \quad \text{where } k_i s = k_t\bar{\gamma}\\ &= k_t(\gamma * (\bar{\gamma})^{-1})^{-1}\\ &= k_t\bar{\gamma}\gamma^{-1}.\end{aligned}$$

Also $\phi(\gamma, k_i\Gamma)s = k_i\gamma^{-1}s = k_i s\gamma^{-1} = k_t\bar{\gamma}\gamma^{-1}$ and this establishes the required covering. □

To extend this result to transformation semigroups which are not connected we introduce the following concept due to Shibata [1972].

Let $\mathscr{A} = (Q, S)$ be a transformation semigroup and suppose that $\varnothing \neq Q' \subseteq Q$ satisfies the condition that given $q', q_1' \in Q$ there exist $s, s' \in S$ such that $q_1' = q's$ and $q' = q_1's'$. We call $Q'$ a *connected subset of* $Q$. A *stage* of $Q$ is a maximal connected subset. Suppose that

$$Q = Q_1 \cup \ldots \cup Q_n$$

is a disjoint union of stages of $Q$, we call this a *stage description of* $Q$. Generally it is possible that $Q_i S \not\subseteq Q_i$ for some $i \in \{1, \ldots, n\}$, however in the situation where $Q_i S \subseteq Q_i$ for each $i \in \{1, \ldots, n\}$ we may establish the following result.



*Theorem 3.7.5*

Let $\mathscr{A} = (Q, S)$ be a transformation semigroup and $Q = Q_1 \cup \ldots \cup Q_n$ a stage description of $Q$. Suppose that $Q_i S \subseteq Q_i$ for each $i \in \{1, \ldots, n\}$. Let $\Gamma = \mathbf{Aut}_S Q$ and $N = \{\gamma \in \Gamma \mid Q_i\gamma = Q_i$ for each $i = 1, \ldots, n\}$. For each $i \in \{1, \ldots, n\}$ define $\bar{G}_i = \{\gamma \in \Gamma \mid Q_i\gamma = Q_i\}$ and $G_i = \{\gamma|_{Q_i} \mid \gamma \in \bar{G}_i\}$, that is the elements of $G_i$ are the automorphisms of $Q$ in $\bar{G}_i$ restricted to $Q_i$. Each stage $Q_i$ generates a transformation semigroup $\mathscr{A}_i = (Q_i, S_i)$ where $S_i$ is a quotient semigroup of $S$, $i = 1, \ldots, n$ and $G_i = \mathbf{Aut}_{S_i} Q_i$ for $i = 1, \ldots, n$. Let $Q_i = q_{i1}G_i \cup \ldots \cup q_{ir_i}G_i$ be an orbit decomposition for $Q_i$ with respect to $G_i$ $(i = 1, \ldots, n)$. Put

$$\pi = \bigcup_{i=1}^{n} \bigcup_{j=1}^{r_i} \{q_{ij}G_i\}.$$

This is an admissible partition on $Q$ and

$$\mathscr{A} \leq \mathscr{N} \circ \mathscr{A}/\langle\pi\rangle.$$

*Proof* $G_i \subseteq \mathbf{Aut}_{S_i} Q_i$ is immediate. Let $h_i \in \mathbf{Aut}_{S_i} Q_i$, then $h_i : Q_i \to Q_i$. Define $l : Q \to Q$ by

$$l(q) = \begin{cases} h_i(q) & \text{if } q \in Q_i\\ q & \text{otherwise.}\end{cases}$$

It is clear that $l \in \Gamma$ and in fact $l \in \bar{G}_i$ and $h_i = l|_{Q_i}$. Thus $h_i \in G_i$. Now let $q_{ij}G_i \in \pi$ and $s \in S$, then $q_{ij}s \in Q_i$ and so $q_{ij}s = q_{ik}g_i$ for some $g_i \in G_i$ and $k \in \{1, \ldots, r_i\}$. Then $q_{ij}G_i s = q_{ij}sG_i = q_{ik}g_iG_i = q_{ik}G_i$. Hence $\pi$ is admissible. We now establish the covering $\mathscr{A} \leq \mathscr{N} \circ \mathscr{A}/\langle\pi\rangle$. Let $\phi : N \times \pi \to Q$ be defined by

$$\phi(n, q_{ij}G_i) = q_{ij}n^{-1}$$

where $n \in N$, $q_{ij}G_i \in \pi$. For $s \in S$ define $[s]$ to be the element of $S(\mathscr{A}/\langle\pi\rangle)$ induced by $s$ and define $f_s : \pi \to N$ by $f_s(q_{ij}G_i) = \bar{n}$ where $\bar{n} : Q \to Q$ is defined by

$$q\bar{n} = \begin{cases} qg_i^{-1} & \text{if } q \in Q_i \text{ and } q_{ij}s = q_{it}g_i \quad \text{for } g_i \in G_i,\ t \in \{1, \ldots, r_i\}\\ q & \text{otherwise.}\end{cases}$$

Now for $n \in N$, $q_{ij}G_i \in \pi$, $s \in S$ we have

$$\phi(n, q_{ij}G_i)s = q_{ij}n^{-1}s = q_{ij}sn^{-1}$$

and

$$\begin{aligned}
&\phi((n, q_{ij}G_i)(f_s, [s])) \\
&= \phi(n * \bar{n}, q_{ii}G_i) \quad \text{where } q_{ij}s = q_{ii}g_i \text{ and } q\bar{n} = qg_i^{-1} \text{ for } q \in Q_i \\
&= q_{ii}(n * \bar{n})^{-1} \\
&= q_{ii}(\bar{n})^{-1}n^{-1} \\
&= q_{ij}sg_i^{-1}(\bar{n})^{-1}n^{-1} \\
&= q_{ij}sn^{-1} \quad \text{as required.}
\end{aligned}$$
□

Further results are possible in this direction but we will now turn our attention to a final method of decomposing transformation semigroups and state machines.

### 3.8 Admissible subset system decompositions

There is a natural generalization of the concept of an admissible partition of a state machine.

Let $\mathcal{M} = (Q, \Sigma, F)$ be a state machine and suppose that $\pi = \{H_i\}_{i \in I}$ is a collection of subsets of $Q$ such that $Q = \bigcup_{i \in I} H_i$ and if $i \in I$ and $\sigma \in \Sigma$ there is $j \in I$ with $(H_i)F_\sigma \subseteq H_j$.

We call $\pi$ an *admissible subset system for Q*. This definition is very similar to the definition of an admissible partition, but we no longer require the collection $\{H_i\}_{I \in I}$ to be mutually disjoint. (An *admissible subset system* for a transformation semigroup is defined analogously, so that if $\mathcal{A} = (Q, S)$ and $\pi = \{H_i\}_{i \in I}$ then $Q = \bigcup_{i \in I} H_i$ and given $i \in I$, $s \in S$ there exists $j \in I$ satisfying $H_i s \subseteq H_j$.) Notice that if $i \in I$ and $\sigma \in \Sigma$ then there may be more than one element $j \in I$ such that $(H_i)F_\sigma \subseteq H_j$ so the uniqueness property associated with admissible partitions no longer applies in this situation. We can however construct a decomposition of $\mathcal{M}$ using an admissible subset system.

For each $i \in I$ and $\sigma \in \Sigma$ choose an element

$$j(i, \sigma) \in I$$

such that

$$(H_i)F_\sigma \subseteq H_{j(i,\sigma)}.$$

Now construct a machine $\mathcal{M}^* = (Q^*, \Sigma, F^*)$ where

$$Q^* = \{(q, H_i) \mid q \in H_i, i \in I\}$$

and

$$(q, H_i)F_\sigma^* = (qF_\sigma, H_{j(i,\sigma)}).$$



Define a partition $\pi^*$ on $\mathcal{M}^*$ by

$$\pi^* = \{(H_i, H_i) \mid i \in I\}.$$

This is an admissible partition on $\mathcal{M}^*$ since

$$(H_i, H_i)F_\sigma^* \subseteq (H_{j(i,\sigma)}, H_{j(i,\sigma)})$$

for $\sigma \in \Sigma$, $i \in I$.

We are now in a position to prove our last decomposition result. As before we use $\mathbf{max}(\pi)$ to indicate the size of a maximal $\pi$-block.

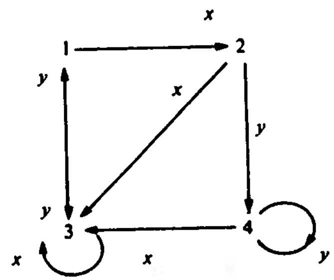
*Theorem 3.8.1*
Let $\mathcal{M} = (Q, \Sigma, F)$ be a state machine and $\pi = \{H_i\}_{i \in I}$ an admissible subset system on $Q$. There is a state machine $\mathcal{N} = (Q', \Sigma', F')$ such that

$$\mathcal{M} \leq \mathcal{N} \omega \mathcal{M}^* / \pi^* \quad \text{and} \quad |Q'| = \mathbf{max}(\pi).$$

*Proof* First we note that theorem 3.3.1 can be applied to the state machine $\mathcal{M}^*$ and so $\mathcal{M}^* \leq \mathcal{N} \omega \mathcal{M}^* / \pi^*$ for some state machine $\mathcal{N}$. Next note that $\mathcal{M} \leq \mathcal{M}^*$ under the covering $\phi : Q^* \to Q$ defined by $\phi(q, H_i) = q$ for each $(q, H_i) \in Q^*$. Then $(\phi(q, H_i))F_\sigma \subseteq qF_\sigma$ and $\phi((q, H_i)F_\sigma^*) = \phi((qF_\sigma, H_{j(i,\sigma)})) = qF_\sigma$ for $\sigma \in \Sigma$, $(q, H_i) \in Q^*$. Thus $\mathcal{M} \leq \mathcal{M}^* \leq \mathcal{N} \omega \mathcal{M}^* / \pi^*$. □

*Corollary 3.8.2*
$\mathbf{TS}(\mathcal{M}) \leq \mathbf{TS}(\mathcal{N}) \circ \mathbf{TS}(\mathcal{M}^* / \pi^*)$.

*Example 3.8*
Consider the state machine $\mathcal{M}$ given by




Let $H_1 = \{1, 2, 3\}$, $H_2 = \{2, 3, 4\}$, $H_3 = \{1, 3, 4\}$ and $\pi = \{H_1, H_2, H_3\}$. Then

$$(H_1)F_x = \{2, 3\}, (H_2)F_x = \{3\}, (H_3)F_x = \{2, 3\},$$
$$(H_1)F_y = \{1, 3, 4\}, (H_2)F_y = \{1, 4\}, (H_3)F_y = \{1, 3, 4\}.$$

Therefore $\pi$ is an admissible subset system. Let us define

$$j(1, x) = 2, j(2, x) = 3, j(3, x) = 1,$$
$$j(1, y) = 3, j(2, y) = 3, j(3, y) = 3,$$

then an $\mathcal{M}^*$ may be defined.

Notice however that the semigroup of $\mathcal{M}^*$ is not equal to the semigroup of $\mathcal{M}$, for $F_{x^2} \equiv F_{yx^2}$ yet $(1, H_1)F^*_{x^2} = (2, H_2)F^*_x = (3, H_3)$ and $(1, H_1)F^*_{yx^2} = (3, H_3)F^*_{x^2} = (3, H_1)F^*_x = (3, H_2)$ and so $F^*_{yxx} \not\equiv F^*_{xx}$. However, in general $S(\mathcal{M})$ is a quotient of $S(\mathcal{M}^*)$ since $F^*_\alpha \equiv F^*_\beta \Rightarrow F_\alpha \equiv F_\beta$ for $\alpha, \beta \in \Sigma^*$.

The last result can now be applied to obtain a decomposition of an arbitrary state machine.

Let $\mathcal{M} = (Q, \Sigma, F)$ be a state machine with $|Q| = n$. Put $\pi = \{H \in \mathcal{P}(Q) \,|\, |H| = n - 1\}$ where $\mathcal{P}(Q)$ denotes the set of all subsets of $Q$. This is a finite collection of proper subsets of $Q$ and it is clearly admissible since $|(H)F_\sigma| \leq n - 1$ for any $\sigma \in \Sigma$ and for any $H \in \pi$ and so $(H)F_\sigma \subseteq H'$ for some $H' \in \pi$. Then $\mathcal{M} \leq \mathcal{N}\omega\mathcal{M}^*/\pi^*$ where $\mathcal{N}$ has $n - 1$ states by 3.8.1. Now either $|(Q)F_\sigma| = n$ or $|(Q)F_\sigma| < n$ for each $\sigma \in \Sigma$ and so either the input $\sigma \in \Sigma$ permutes the elements of $Q$ and is thus a permutation in $\mathcal{M}^*/\pi^*$ or $(Q)F_\sigma \subseteq H$ for some $H \in \pi$ which implies that $\sigma$ acts as a reset for $\mathcal{M}^*/\pi^*$. Thus $\mathcal{M}^*/\pi^*$ is a permutation–reset machine. This leads to:

*Theorem 3.8.3*
Let $\mathcal{M}$ be a state machine, then

$$\mathcal{M} \leq \mathcal{P}_1\omega_1\mathcal{P}_2\omega_2 \ldots \omega_{n-1}\mathcal{P}_n$$

where each $\mathcal{P}_i$ is a permutation–reset machine of smaller state size than $\mathcal{M}$.

*Proof* We simply apply the above process, first putting $\mathcal{P}_n = \mathcal{M}^*/\pi^*$ and then applying it again to $\mathcal{N}$ and continue in this way. □

*Theorem 3.8.4*
Let $\mathcal{M}$ be a state machine, then

$$\mathcal{M} \leq \mathcal{P}_1\omega_1\mathcal{P}_2\omega_2 \ldots \omega_{n-1}\mathcal{P}_n$$

where each $\mathcal{P}_i$ is either
(i) a simple grouplike machine, or
(ii) a two-state reset machine.

*Proof* We combine 3.8.3 with 3.5.6. □



*Corollary 3.8.5*
Let $\mathscr{A} = (Q, S)$ be a transformation semigroup, then $\mathscr{A} \leq \mathscr{B}_1 \circ \mathscr{B}_2 \circ \ldots \circ \mathscr{B}_n$ where each $\mathscr{B}_i$ is either
(i) of the form $\mathscr{G}_i$ for some simple group $G_i$, or
(ii) a finite direct product of $\bar{\mathbf{2}}^\cdot$.

*Proof* Apply 3.8.4 to $SM(\mathscr{A})$ to get

$$SM(\mathscr{A}) \leq \mathscr{X}_1\omega_1\mathscr{X}_2\omega_2 \ldots \omega_{n-1}\mathscr{X}_n$$
$$\mathscr{A} = TS(SM(\mathscr{A})) \leq TS(\mathscr{X}_1) \circ TS(\mathscr{X}_2) \circ \ldots \circ TS(\mathscr{X}_n)$$

and if $\mathscr{X}_i$ is a two-state reset machine then $TS(\mathscr{X}_i) \leq \bar{\mathbf{2}}^\cdot$ and if $\mathscr{X}_i$ is a simple grouplike machine defined by the simple group $G_i$ then $TS(\mathscr{X}_i) \leq \mathscr{G}_i$. □

This theorem is a special case of the Krohn–Rhodes theorem. We do not, as yet, know much about the simple groups that arise in the decomposition, in fact they divide the semigroup of the original machine, but the proof of this is a little involved. Furthermore the construction of the decomposition outlined in the above is very inefficient, much simpler and more practical decompositions are available. We will study these in chapter 4.

## 3.9 Complexity

If we start with an arbitrary transformation semigroup $\mathscr{A} = (Q, S)$ we can cover $\mathscr{A}$ with a wreath product involving transformation groups and transformation semigroups of reset machines. These latter transformation semigroups can be covered by direct products of the transformation semigroup $\bar{\mathbf{2}}^\cdot$ by 3.5.6. We introduce a class of transformation semigroups that is a generalization of the class of reset transformation semigroups. A transformation semigroup $\mathscr{A} = (Q, S)$ is *aperiodic* if

$$\mathscr{A} \leq \bar{\mathbf{2}}^\cdot \circ \bar{\mathbf{2}}^\cdot \circ \ldots \circ \bar{\mathbf{2}}^\cdot$$

that is if $\mathscr{A}$ can be covered by a *finite* wreath product of the transformation semigroup $\bar{\mathbf{2}}^\cdot$.

Now the proofs of 3.8.4 and 3.8.5 allow us to deduce that any transformation semigroup can be covered by a wreath product involving two types of transformation semigroups, namely

transformation groups of the form $\mathscr{G}$

and

aperiodic transformation semigroups.

Suppose that

$$\mathcal{A} = (Q, S) \text{ and } \mathcal{A} \leq \mathcal{A}_1 \circ \mathcal{G}_1 \circ \mathcal{A}_2 \circ \mathcal{G}_2 \circ \ldots \circ \mathcal{A}_k \circ \mathcal{G}_k \circ \mathcal{A}_{k+1}$$

where $G_1, \ldots, G_k$ are groups and $\mathcal{A}_1, \ldots, \mathcal{A}_{k+1}$ are aperiodic transformation semigroups. Such a decomposition can be found using 3.8.5 but it may not be the only such decomposition involving groups and aperiodic transformation semigroups. The smallest value of $k$ arising from such a decomposition is an indication of how complicated $\mathcal{A}$ is.

We define the *complexity of* $\mathcal{A}$, $\mathrm{C}(\mathcal{A})$ to be the smallest integer $k$ such that

$$\mathcal{A} \leq \mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{A}_k \circ \mathcal{G}_k \circ \mathcal{A}_{k+1}$$

is a decomposition with the $\mathcal{A}_i$ aperiodic and the $G_i$ groups.

A natural convention would be to define the complexity of $\mathcal{A}$ to be zero if $\mathcal{A}$ is aperiodic.

The groups $G_1, \ldots, G_k$ arising in the decomposition are free from any restrictions, they need not be simple nor divisors of $S$.

Notice that $\mathbf{1}^{\cdot}$ is aperiodic and for any transformation semigroup $\mathcal{A}$ we have $\mathcal{A} = \mathbf{1}^{\cdot} \circ \mathcal{A} = \mathcal{A} \circ \mathbf{1}^{\cdot}$. Thus the complexity of a transformation group $\mathcal{G}$ does not exceed 1 since $\mathcal{G} \leq \mathbf{1}^{\cdot} \circ \mathcal{G} \circ \mathbf{1}^{\cdot}$.

*Example 3.9*

From examples 3.2 and 3.4 we see that the cyclic transformation semigroup $\mathcal{C}_{(3,3)} \leq [(\bar{\mathbf{2}} \circ \mathcal{C}) \circ \mathcal{C}] \times \mathbf{Z}_3$. Since the transformation semigroup $\mathcal{C} \leq \bar{\mathbf{2}}^{\cdot}$ we have $\mathcal{C}_{(3,3)} \leq \mathcal{A}_1 \times \mathbf{Z}_3$ and so the complexity $\mathrm{C}(\mathcal{C}_{(3,3)}) \leq 1$.

From example 3.5 this transformation semigroup is covered by $\bar{\mathbf{Z}}_2 \circ \mathbf{Z}_2$, and $\bar{\mathbf{Z}}_2 \leq \bar{\mathbf{2}}^{\cdot} \circ \mathbf{Z}_2$ by 3.4.2 so we have complexity of at most 1.

Finally example 3.6 yields the covering by

$$(\bar{\mathbf{2}} \times \bar{\mathbf{2}})^{\cdot} \circ \mathbf{Z}_3 \leq (\bar{\mathbf{2}}^{\cdot} \times \bar{\mathbf{2}}^{\cdot}) \circ \mathbf{Z}_3$$

again of complexity of at most 1.

One basic problem with calculating the complexity of a transformation semigroup is that, while it is usually easy enough to find upper bounds by describing a suitable decomposition, it is often far from easy to establish that no shorter such decompositions exist. Our first result in this direction will be to show that if $G$ is any non-trivial group then $\mathrm{C}(\mathcal{G}) = 1$.

To achieve this we will assume that $\mathrm{C}(\mathcal{G}) = 0$, that is $\mathcal{G}$ is aperiodic. We first need the following result.

*Theorem 3.9.1*

Let $\mathcal{A} = (Q, S)$ be aperiodic and complete, there exists an integer $n \geq 0$ such that $s^{n+1} = s^n$ for all $s \in S$.



*Proof* We first establish that if $\mathcal{A} \leq \bar{\mathbf{2}}^{\cdot}$ then $s^2 = s$ for all $s \in S$. Suppose that $\bar{\mathbf{2}}^{\cdot} = (R, U)$ and $\phi : R \to Q$ is the covering partial function. Let $s \in S$, then there exists $u \in U$ such that

$$\phi(r)s \subseteq \phi(ru) \quad \text{for all } r \in R.$$

Let $q \in Q$, there exists $r \in R$ such that $q = \phi(r)$, then $qs = \phi(r)s = \phi(ru)$ since $\mathcal{A}$ is complete. Now $qs^2 = \phi(r) \cdot ss = \phi(ru)s = \phi(ru^2) = \phi(ru)$ since $u^2 = u$ for all $u \in U$.

Thus $qs^2 = qs$ and since $q$ is arbitrary $s^2 = s$. Now let us assume that if $\mathcal{A} \leq (\bar{\mathbf{2}}^{\cdot})^k$, that is if $\mathcal{A} \leq \bar{\mathbf{2}}^{\cdot} \circ \ldots \circ \bar{\mathbf{2}}^{\cdot}$ where there are $k$ elements in the product, then

$$s^{k+1} = s^k \quad \text{for all } s \in S.$$

Suppose that $\mathcal{A} \leq (\bar{\mathbf{2}}^{\cdot})^{k+1}$, we will show that $s^{k+2} = s^{k+1}$ for $s \in S$. Let $\mathcal{A} \leq \mathcal{B} \circ \bar{\mathbf{2}}^{\cdot}$ where $\mathcal{B} = (P, T) = (\bar{\mathbf{2}}^{\cdot})^k$. We know that for $t \in T$, $t^{k+1} = t^k$. If $\phi : P \times R \to Q$ is the covering partial function and for $s \in S$ we have $(f_s, u_s)$ covering $s$ with $f_s : R \to T$, then $\phi(p, r)s = \phi((p, r)(f_s, u_s))$. Choose any $q \in Q$, there exist $p \in P$, $r \in R$ with $q = \phi(p, r)$. Let $s \in S$, then

$$\begin{aligned}
qs^{k+2} &= \phi(p, r)s^{k+2} \\
&= \phi((p, r)(f_s, u_s)) \cdot s^{k+1} \\
&= \phi(pf_s(r), ru_s)s^{k+1} \\
&= \phi(pf_s(r) \cdot f_s(ru_s), ru_su_s)s^k \\
&= \phi(pf_s(r)f_s(ru_s), ru_s)s^k \\
&\;\;\vdots \\
&= \phi(pf_s(r)(f_s(ru_s))^{k+1}, ru_s) \\
&= \phi(pf_s(r)(f_s(ru_s))^k, ru_s) \\
&= \phi(pf_s(r), ru_s)s^k \\
&= \phi(p, r)s^{k+1} \\
&= qs^{k+1}.
\end{aligned}$$

Hence $s^{k+2} = s^{k+1}$.

The result now follows by induction. □

*Corollary 3.9.2*

Let $G$ be a group. If $G \neq \{1\}$ then

$\mathrm{C}(\mathcal{G}) = 1$.

*Proof* We have $\mathrm{C}(\mathcal{G}) \leq 1$. Let $\mathrm{C}(\mathcal{G}) = 0$, then $\mathcal{G}$ is aperiodic and so there exists $n \geq 0$ such that $g^{n+1} = g^n$ for all $g \in G$. Then $g = 1$, a contradiction. □

*Theorem 3.9.3*

Let $\mathcal{A} = (Q, S)$, $\mathcal{B} = (P, T)$ be transformation semigroups.

(i) If $\mathcal{A} \le \mathcal{B}$ then $\mathbf{C}(\mathcal{A}) \le \mathbf{C}(\mathcal{B})$.

(ii) $\mathbf{C}(\mathcal{A} \circ \mathcal{B}) \le \mathbf{C}(\mathcal{A}) + \mathbf{C}(\mathcal{B})$.

(iii) $\mathbf{C}(\mathcal{A} \times \mathcal{B}) \le \max\{\mathbf{C}(\mathcal{A}), \mathbf{C}(\mathcal{B})\}$.

(iv) If $\pi$ is an admissible partition on $\mathcal{A}$ then $\mathbf{C}(\mathcal{A}/\langle\pi\rangle) \le \mathbf{C}(\mathcal{A})$.

(v) If $\pi$ and $\tau$ are orthogonal partitions on $\mathcal{A}$ with $\pi \cap \tau = 1_Q$ then $\mathbf{C}(\mathcal{A}/\langle\pi\rangle) = \mathbf{C}(\mathcal{A})$ or $\mathbf{C}(\mathcal{A}/\langle\tau\rangle) = \mathbf{C}(\mathcal{A})$.

*Proof* (i) Let $\mathbf{C}(\mathcal{B}) = n$, then $\mathcal{B} \le \mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}$ with the $G_i$ groups and the $\mathcal{A}_i$ aperiodic transformation semigroups. Clearly $\mathcal{A} \le \mathcal{B} \le \mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}$ and so $\mathbf{C}(\mathcal{A}) \le n$.

(ii) Let $\mathbf{C}(\mathcal{A}) = n$, $\mathbf{C}(\mathcal{B}) = m$, then

$$\mathcal{A} \le \mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}$$

$$\mathcal{B} \le \mathcal{A}'_1 \circ \mathcal{G}'_1 \circ \ldots \circ \mathcal{G}'_m \circ \mathcal{A}'_{m+1}$$

where $G_1, \ldots, G_n$, $G'_1, \ldots, G'_m$ are groups and $\mathcal{A}_1, \ldots, \mathcal{A}_{n+1}$, $\mathcal{A}'_1, \ldots, \mathcal{A}'_{m+1}$ are aperiodic.

Now $\mathcal{A} \circ \mathcal{B} \le \mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1} \circ \mathcal{A}'_1 \circ \mathcal{G}'_1 \circ \ldots \circ \mathcal{G}'_m \circ \mathcal{A}'_{m+1}$ and since $\mathcal{A}_{n+1} \circ \mathcal{A}'_1$ is aperiodic we have $\mathbf{C}(\mathcal{A} \circ \mathcal{B}) \le n + m$.

(iii) Let $\max\{\mathbf{C}(\mathcal{A}), \mathbf{C}(\mathcal{B})\} = n$, and for the sake of argument let $\mathbf{C}(\mathcal{A}) = n$, $\mathbf{C}(\mathcal{B}) = m \le n$.

Now

$$\mathcal{A} \le \mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}$$

$$\mathcal{B} \le \mathcal{A}'_1 \circ \mathcal{G}'_1 \circ \ldots \circ \mathcal{G}'_m \circ \mathcal{A}'_{m+1}$$

and

$$\begin{aligned}
\mathcal{A} \times \mathcal{B} &\le (\mathcal{A}_1 \circ \mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}) \times (\mathcal{A}'_1 \circ \mathcal{G}'_1 \circ \ldots \circ \mathcal{G}'_m \circ \mathcal{A}'_{m+1}) \\
&\le (\mathcal{A}_1 \times \mathcal{A}'_1) \circ [(\mathcal{G}_1 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}) \\
&\qquad \times (\mathcal{G}'_1 \circ \ldots \circ \mathcal{G}'_m \circ \mathcal{A}'_{m+1})] \\
&\le (\mathcal{A}_1 \times \mathcal{A}'_1) \circ (\mathcal{G}_1 \times \mathcal{G}'_1) \circ [(\mathcal{A}_2 \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}) \\
&\qquad \times (\mathcal{A}'_2 \circ \ldots \circ \mathcal{G}'_m \circ \mathcal{A}'_{m+1})] \\
&\;\;\vdots \\
&\le (\mathcal{A}_1 \times \mathcal{A}'_1) \circ (\mathcal{G}_1 \times \mathcal{G}'_1) \circ (\mathcal{A}_2 \times \mathcal{A}'_2) \circ \ldots \circ (\mathcal{G}_m \times \mathcal{G}'_m) \\
&\qquad \circ (\mathcal{A}_{m+1} \times \mathcal{A}'_{m+1}) \circ \mathcal{G}_{m+1} \circ \mathcal{A}_{m+2} \circ \ldots \circ \mathcal{G}_n \circ \mathcal{A}_{n+1}
\end{aligned}$$

and so $\mathbf{C}(\mathcal{A} \times \mathcal{B}) \le n$.

(iv) Since $\mathcal{A}/\langle\pi\rangle \le \mathcal{A}$ we have $\mathbf{C}(\mathcal{A}/\langle\pi\rangle) \le \mathbf{C}(\mathcal{A})$ by (i).

(v) $\mathcal{A} \le \mathcal{A}/\langle\pi\rangle \times \mathcal{A}/\langle\tau\rangle$ and so $\mathbf{C}(\mathcal{A}) \le \max(\mathbf{C}(\mathcal{A}/\langle\pi\rangle), \mathbf{C}(\mathcal{A}/\langle\tau\rangle))$. But $\mathbf{C}(\mathcal{A}/\langle\pi\rangle) \le \mathbf{C}(\mathcal{A})$ and $\mathbf{C}(\mathcal{A}/\langle\tau\rangle) \le \mathbf{C}(\mathcal{A})$ and so $\mathbf{C}(\mathcal{A}) = \mathbf{C}(\mathcal{A}/\langle\pi\rangle)$ or $\mathbf{C}(\mathcal{A}/\langle\tau\rangle)$. □



*Example 3.10*

We are now in a position to establish that all the examples in example 3.9 have complexity equal to 1. Thus $\mathbf{C}(\mathcal{C}_{3,3}) = \mathbf{C}(\mathbf{Z}_3) = 1$ by 3.9.3(v) and 3.9.2. From example 3.5 we see that $\alpha^2 = 1$ and so by 3.9.1 this transformation semigroup cannot be aperiodic. Finally in example 3.6, $\sigma^3 = 1$ and again this cannot be aperiodic.

Our next aim is to show that complexity is really a semigroup concept rather than a transformation semigroup or state machine concept. We will establish that if $\mathcal{A} = (Q, S)$ then $\mathbf{C}(\mathcal{A}) = \mathbf{C}(\mathcal{S})$.

First we need:

*Theorem 3.9.4*

Let $\mathcal{A} = (Q, S)$ be a transformation semigroup where $S$ is not a monoid. Then

$$\mathcal{A} \le (Q, \varnothing)^{\cdot} \times (S^{\cdot}, S) \times \mathcal{C}.$$

*Proof* Let $\mathcal{C} = (\{a, b\}, \{\sigma\})$ where $a\sigma = a$, $b\sigma = a$.

Define $\phi : Q \times S^{\cdot} \times \{a, b\} \to Q$ by

$$\phi(q, s, a) = qs \quad \text{if } s \ne e \text{, the adjoined identity in } S^{\cdot}$$

$$\phi(q, e, b) = q.$$

For $s' \in S$ let us consider the triple $(1_Q, s', \sigma)$. Then for $s' \in S$, $\phi(q, s, a) \cdot s' = qss'$ and

$$\phi((q, s, a) \cdot (1_Q, s', \sigma)) = \phi(q, ss', a\sigma) = qss'$$

furthermore

$$\phi(q, e, b) \cdot s' = qs'$$

and

$$\phi((q, e, b) \cdot (1_Q, s', \sigma)) = \phi(q, s', a) = qs'.$$

Thus $(1_Q, s', \sigma)$ covers $s'$. □

*Theorem 3.9.5*

Let $\mathcal{A} = (Q, S)$ be a transformation semigroup which is not a transformation monoid but such that $S$ is a monoid. Then

$$\mathcal{A} \le (Q, \varnothing)^{\cdot} \times (S, S) \times \mathcal{C} \times \mathcal{C}.$$

*Proof* We first construct a semigroup $S^*$ as follows.

Let $e \in S$ be the identity in $S$. Choose an element $f$ which does not belong to $S$ and form $S^* = S \cup \{f\}$. This is a semigroup when we extend the multiplication in $S$ to $S^*$ along with the identities $f \cdot s = s = s \cdot f$ for all $s \in S^*$. Furthermore $(S^*, S)$ is a transformation semigroup. Now define $\phi : S \times \{a, b\} \to S^*$ by

$$\phi(s, a) = s \quad \text{for } s \in S$$
$$\phi(e, b) = f.$$

Then $\phi$ is a surjective partial function. We will show that, given $s' \in S$ the pair $(s', \sigma)$ covers $s'$. Now

$$\phi(s, a) \cdot s' = ss' = \phi((s, a)(s', \sigma))$$

and

$$\phi(e, b) \cdot s' = fs' = s' = \phi(s', a) = \phi((e, b)(s', \sigma)).$$

Thus $(S^*, S) \le (S, S) \times \mathscr{C}$.

We next show that $\mathscr{A} \le (Q, \varnothing)^{\cdot} \times (S^*, S) \times \mathscr{C}$ by defining $\phi : Q \times S^* \times \{a, b\} \to Q$ by

$$\phi(q, s, a) = qs$$
$$\phi(q, f, b) = q.$$

This is surjective and if $s' \in S$ we will cover it with $(1_Q, s', \sigma)$ so that

$$\phi(q, s, a)s' = qss' = \phi((q, s, a)(1_Q, s', \sigma))$$

and

$$\phi(q, f, b)s' = qs' = \phi((q, s', a)) = \phi((q, f, b)(1_Q, s', \sigma)).$$

Finally $\mathscr{A} \le (Q, \varnothing)^{\cdot} \times (S, S) \times \mathscr{C} \times \mathscr{C}$. □

*Theorem 3.9.6*
Let $\mathscr{A} = (Q, S)$ be a complete transformation semigroup, then $\mathbf{C}(\mathscr{A}) = \mathbf{C}(\mathscr{S})$.

*Proof* If $\mathscr{A}$ is a transformation monoid then by exercise 3.7 we have $\mathscr{A} \le (Q, \varnothing)^{\cdot} \times \mathscr{S}$. Generally $\mathscr{A} \le (Q, \varnothing)^{\cdot} \times \mathscr{S} \times \mathscr{C} \times \mathscr{C}$ from 3.9.4 and 3.9.5. Now suppose that $\mathbf{C}(\mathscr{S}) = n$ and $\mathscr{S} \le \mathscr{A}_1 \circ \mathscr{G}_1 \circ \ldots \circ \mathscr{G}_n \circ \mathscr{A}_{n+1}$, then

$$\mathscr{A} \le (Q, \varnothing)^{\cdot} \times (\mathscr{A}_1 \circ \mathscr{G}_1 \circ \ldots \circ \mathscr{G}_n \circ \mathscr{A}_{n+1}) \times \mathscr{C} \times \mathscr{C}$$
$$\le ((Q, \varnothing)^{\cdot} \times \mathscr{A}_1) \circ \mathscr{G}_1 \circ \ldots \circ \mathscr{G}_n \circ (\mathscr{A}_{n+1} \times \mathscr{C} \times \mathscr{C})$$

and since $(Q, \varnothing)^{\cdot} \times \mathscr{A}_1$ and $\mathscr{A}_{n+1} \times \mathscr{C} \times \mathscr{C}$ are aperiodic we have $\mathbf{C}(\mathscr{A}) \le n$. We now show that $\mathscr{S} \le \prod^k \mathscr{A}$, the direct product of $k$ copies of $\mathscr{A}$, where $k = |Q|$. Let $Q = \{q_1, \ldots, q_k\}$. Define $\phi : Q \times \ldots \times Q \to S^{\cdot}$ by

$$\phi((q_{i1}, \ldots, q_{ik})) = s \quad \text{if } q_j s = q_{ij}, j \in \{1, \ldots, k\}$$
$$\phi((q_1, \ldots, q_k)) = e$$



and

$$\phi((q_{i1}, \ldots, q_{ik})) = \varnothing \quad \text{otherwise.}$$

so that

$$\phi((q_1 s, \ldots, q_k s)) = s,$$
$$\phi((q_1, \ldots, q_k)) = e$$

and all other values of $\phi((q_{i1}, \ldots, q_{ik}))$ are undefined, where $q_{i1}, \ldots, q_{ik} \in Q$. Let $s' \in S$ and consider $(s', \ldots, s') \in S^k$. Then for $s' \in S$ we have $\phi((q_{i1}, \ldots, q_{ik})) \cdot s' = \varnothing$

or

$$\phi((q_{i1}, \ldots, q_{ik})) \cdot s' = ss' \subseteq \phi((q_{i1}s', \ldots, q_{ik}s')) = ss'$$

or

$$\phi((q_1, \ldots, q_k)) \cdot s' = es' = \phi((q_1 s'_1, \ldots, q_k s')) = s'$$

and the covering is established.

Then by 3.9.3(iii) $\mathbf{C}(\mathscr{S}) \le \mathbf{C}(\mathscr{A})$ and so

$$\mathbf{C}(\mathscr{S}) = \mathbf{C}(\mathscr{A}).$$ □

Finally we show that if $\mathscr{A}$ is incomplete then $\mathbf{C}(\mathscr{A}) = \mathbf{C}(\mathscr{A}^c)$. First we need the following result:

*Theorem 3.9.7*
If $\mathscr{A} \le \mathscr{B}$ and $\mathscr{B}$ is complete then $\mathscr{A}^c \le \mathbf{2}^{\cdot} \times \mathscr{B}$.

*Proof* Let $\mathscr{A} = (Q, S)$, $\mathscr{B} = (P, T)$, $\mathbf{2}^{\cdot} = (\{a, b\}, \{1\})$, $\mathscr{A}^c = (Q \cup \{r\}, S)$. Suppose that $\phi : P \to Q$ is the covering partial function giving $\mathscr{A} \le \mathscr{B}$. Let $\psi : \{a, b\} \times P \to Q \cup \{r\}$ be defined by

$$\psi(a, p) = \phi(p)$$
$$\psi(b, p) = r, \quad p \in P.$$

If $s \in S$ let $t$ be such that $t$ covers $s$ with respect to $\phi$. Now for $s \in S$,

$$\psi(a, p)s = \phi(p)s \subseteq \phi(pt) = \psi(a, pt) = \psi((a, p)(1, t))$$
$$\psi(b, p)s = rs = r = \psi(b, pt) = \psi((b, p)(q, t)).$$

Hence $\psi$ is the required covering. □

*Theorem 3.9.8*
If $\mathscr{A} = (Q, S)$ is any transformation semigroup

$$\mathbf{C}(\mathscr{A}^c) = \mathbf{C}(\mathscr{A}).$$

*Proof* If $\mathscr{A}$ is complete, $\mathscr{A}^c = \mathscr{A}$. If $\mathscr{A}$ is not complete then $\mathscr{A} \le \mathscr{A}^c$ and so $\mathbf{C}(\mathscr{A}) \le \mathbf{C}(\mathscr{A}^c)$. Suppose that $\mathbf{C}(\mathscr{A}) = n$, then

$$\mathscr{A} \le \mathscr{A}_1 \circ \mathscr{G}_1 \circ \ldots \circ \mathscr{G}_n \circ \mathscr{A}_{n+1}$$

and we may assume that all of the $\mathscr{A}_i$ and $\mathscr{G}_i$ are complete.

Hence by 3.9.7

$$\begin{aligned}\mathscr{A}^c &\le \mathbf{2}^{\cdot} \times (\mathscr{A}_1 \circ \mathscr{G}_1 \circ \ldots \circ \mathscr{G}_n \circ \mathscr{A}_{n+1})\\ &\le (\mathbf{2}^{\cdot} \times \mathscr{A}_1) \circ \mathscr{G}_1 \circ \ldots \circ \mathscr{G}_n \circ \mathscr{A}_{n+1}\end{aligned}$$

and since $\mathbf{2}^{\cdot} \times \mathscr{A}_1$ is aperiodic we have

$$\mathbf{C}(\mathscr{A}^c) \le n = \mathbf{C}(\mathscr{A}). \qquad \square$$

It can be shown that transformation semigroups of an arbitrary complexity exist. The proof of this fact is far from easy, it uses a considerable amount of the theory of semigroups and we do not have the space available for such a discussion. However, the interested reader may study the appropriate literature for the details (Eilenberg [1976]). We will close with the following unproved statement.

Let $n \ge 0$ be an integer, then $\mathbf{C}(\overline{(2, S_2)} \circ \overline{(3, S_3)} \circ \ldots \circ \overline{(n, S_n)}) = n - 1$, where $S_k$ is the symmetric group on $k$ symbols.

Now $(k, S_k) \le \bar{\mathbf{k}}^{\cdot} \circ \mathscr{S}_k$ by 3.4.3, $\bar{\mathbf{k}}^{\cdot}$ is aperiodic and $S_k$ is a group and so $\mathbf{C}(\overline{(2, S_2)} \circ \overline{(3, S_3)} \circ \ldots \circ \overline{(n, S_n)}) \le n - 1$. It can be shown that $\mathbf{C}(\overline{(2, S_2)} \circ \overline{(3, S_3)} \circ \ldots \circ \overline{(n, S_n)}) = n - 1$.

Other important results in the theory of complexity also involve sophisticated techniques in semigroup theory and we shall have to leave the subject here.

The implications of complexity theory in the applications of state machines centre around the use of the complexity of a machine as a measure of how complicated the machine is. There are other possible measures, one of which involves finding the shortest chain of admissible partitions in the machine. We say that $\mathscr{M} = (Q, \Sigma, F)$ has an *admissible series* of length $n$ if there exists a sequence

$$1_Q = \pi_0 < \pi_1 < \pi_2 < \ldots < \pi_n = \{Q\}$$

of admissible partitions on $Q$ such that no admissible partition $\tau$ exists satisfying $\pi_i < \tau < \pi_{i+1}$ for $0 \le i < n$.

The *dimension*, $\mathbf{D}(\mathscr{M})$, is then defined to be the smallest number that is the length of an admissible series of $\mathscr{M}$. Clearly $\mathbf{D}(\mathscr{M}) = 1$ if and only if $\mathscr{M}$ is irreducible. The dimension is a measure of the functional stability of the machine and is particularly valuable in some biological examples



where functional stability is an evolutionary more important factor than minimal complexity. For example the machine of the Krebs cycle (example 2.10) is irreducible, it has complexity 2.

### 3.10 Exercises

3.1 Prove theorems 3.1.2 and 3.1.3.

3.2 Let $Q$ be a finite set with $|Q| = n > 1$. Prove that

$$(Q, \varnothing) \le \prod^{k} \bar{\mathbf{2}} = \bar{\mathbf{2}} \times \bar{\mathbf{2}} \times \ldots \times \bar{\mathbf{2}} \quad (k \text{ times})$$

where $k$, as a function of $n$, satisfies the formula

$$k(2) = 1$$
$$k(n) = 1 + k\{[(n+1)/2]\}, \quad n > 2.$$

Here $[(n+1)/2]$ means the largest integer less than or equal to $(n+1)/2$. Another way of expressing this is $k(n) = [\log_2(n-1)] + 1$.

3.3 Prove Theorem 3.3.3. Prove the state machine analogue of 3.5.2 and 3.5.3.

3.4 Let $(Q, G)$ be a connected transformation group, let $q \in Q$ and put $H = \{g \in G \mid qg = q\}$. Prove that $(Q, G) \le (G/H, G/H^G)$.

3.5 Prove that a connected transformation group is primitive if and only if it is irreducible.

3.6 Show that the set of all endomorphisms of an irreducible transformation semigroup $\mathscr{A} = (Q, S)$ equals $G \cup \{\bar{q}\}$ or $G$, where $G$ is a group, according as $\mathscr{A}$ has a sink state $q$ or not.

3.7 Let $\mathscr{A} = (Q, S)$ be a transformation monoid. Show $\mathscr{A} \le (Q, \varnothing)^{\cdot} \times \mathscr{S}$.

3.8 If $\mathscr{A}$ is complete and $\mathscr{B} \le \mathscr{A}$ then $\mathscr{B}^c \le \mathbf{2}^{\cdot} \times \mathscr{A}$.

# 4

## The holonomy decomposition

The aim of this chapter is the description of a method for decomposing an arbitrary transformation semigroup into a wreath product of 'simpler' transformation semigroups, namely aperiodic ones and transformation groups. The origin of this theory is the theorem due to Krohn and Rhodes which gave an algorithmic procedure for such a decomposition. There are now various proofs of this result extant, some are set in the theory of transformation semigroups and others are concerned with the theory of state machines. In the light of the close connections between the two theories forged in chapter 2 we can expect a similar correspondence between the two respective decomposition theorems. The proof of the decomposition theorem for state machines has the advantage that it can be motivated the more easily, but at the expense of some elegance. Recently Eilenberg has produced a new, and much more efficient, decomposition and it is this theory that we will now study. It is set in the world of transformation semigroups.

Before we embark on the details let us pause for a moment and consider how we could approach the problem of finding a suitable decomposition. Let $\mathcal{M}=(Q,\Sigma,F)$ be a state machine and let $|Q|=n$. Consider the collection $\pi$ of all subsets of $Q$ of order $n-1$. Then $\pi$ is an admissible subset system, and we may construct a well-defined quotient machine $\mathcal{M}/\pi$. This state machine is a permutation–reset machine and $\mathcal{M}$ may be covered by a cascade product of $\mathcal{M}/\pi$ and a smaller state machine. We then repeat the procedure until we have $\mathcal{M}$ covered by a cascade product of permutation–reset machines. These can then be covered by cascade products of reset machines and group machines. This yields a Krohn–Rhodes type decomposition but the proof of the fact that the groups of the group machines are covered by the semigroup of $\mathcal{M}$ remains to be done, and is not easy.



There are other drawbacks with this approach. The admissible subset system $\pi$ is very wasteful. One better choice for $\pi$ would be the collection of all the maximal images of the machine $\mathcal{M}$. This is the direction that we take here, although we will develop the theory with reference to transformation semigroups rather than state machines. There are certain technical and notational advantages in this approach, but it would be possible to adapt much of the following theory to the state machine case.

We will prove the holonomy decomposition theorem which involves some quite difficult arguments. Once we have this result, however, we will be in a position to decompose a transformation semigroup much more efficiently than the traditional methods would allow.

The theory begins with a close study of admissible subset systems, their possible quotients and their coverings.

### 4.1 Relational coverings

If $\mathcal{A}=(Q,S)$ is a transformation semigroup and $\pi=\{H_i\}_{i\in I}$ is an admissible subset system then a quotient transformation semigroup $\mathcal{A}/\langle\pi\rangle$ may be defined in various ways. They are all based on the pair $(\pi,S)$. We define an operation $\circledast:\pi\times S\to\pi$, which is an action of $S$ on $\pi$ by: $H_i\circledast s=H_j$ where $H_j$ is chosen so that $H_is\subseteq H_j$, for $i,j\in I$, $s\in S$. (Since $H_is$ may belong to more than one element of $\pi$ we have to make a specific choice of one particular element of $\pi$. This means that the operation $\circledast$ is not always uniquely specified, there is a collection of such operations.) To make the triple $(\pi,S,\circledast)$ into a transformation semigroup we must now ensure that $S$ acts faithfully on $\pi$ under $\circledast$. This is done in the usual way by defining the relation $\sim$ on $S$ by: $s\sim s_1\Leftrightarrow H_i\circledast s=H_i\circledast s_1$ for all $H_i\in\pi$. Then $(\pi,S/\sim)$ becomes a transformation semigroup under the operation induced by $\circledast$. We will denote this transformation semigroup by $\mathcal{A}/\langle\pi\rangle$ when the operation $\circledast$ is understood. (We will also use the symbol $\circledast$ for the induced operation in $\mathcal{A}/\langle\pi\rangle$.)

*Example 4.1*

Let $\mathcal{A}=(Q,S)$ be the transformation monoid generated by the state machine:

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| 0 | $a$ | $a$ | $c$ |
| 1 | $b$ | $b$ | $b$ |

where $Q=\{a, b, c\}$, $S=\{\Lambda, 0, 1, 10\}$. The monoid $S$ has the table:

| $S$ | $\Lambda$ | 0 | 1 | 10 |
|---|---|---|---|---|
| $\Lambda$ | $\Lambda$ | 0 | 1 | 10 |
| 0 | 0 | 0 | 1 | 10 |
| 1 | 1 | 10 | 1 | 10 |
| 10 | 10 | 10 | 1 | 10 |

If $\pi=\{\{a, b\}, \{b, c\}, \{a, c\}\}$ we may check that $\pi$ is an admissible subset system for $\mathscr{A}$. Write $H_1=\{a, b\}$, $H_2=\{b, c\}$, $H_3=\{a, c\}$. There are several quotient transformation monoids that may be defined; we consider two possibilities:

| $\circledast$ | $H_1$ | $H_2$ | $H_3$ |
|---|---|---|---|
| $\Lambda$ | $H_1$ | $H_2$ | $H_3$ |
| 0 | $H_1$ | $H_3$ | $H_3$ |
| 1 | $H_1$ | $H_2$ | $H_2$ |
| 10 | $H_1$ | $H_3$ | $H_3$ |

| $\circledast'$ | $H_1$ | $H_2$ | $H_3$ |
|---|---|---|---|
| $\Lambda$ | $H_1$ | $H_2$ | $H_3$ |
| 0 | $H_3$ | $H_3$ | $H_3$ |
| 1 | $H_1$ | $H_1$ | $H_1$ |
| 10 | $H_3$ | $H_3$ | $H_1$ |

The monoids $S/\sim$ are $\{[\Lambda], [0], [1]\}$ and $S$ respectively. Thus $\mathscr{A}/\langle\pi\rangle$ may be defined in several different ways. Similar things happen with transformation semigroups.

What is the connection between $\mathscr{A}$ and the various quotients $\mathscr{A}/\langle\pi\rangle$? Notice that we may define a function $\alpha: \pi \to \mathscr{P}(Q)$ by $\alpha(H_i)=H_i$ where $i\in I$. This defines a relation from the state set of any $\mathscr{A}/\langle\pi\rangle$ onto the state set of $\mathscr{A}$. We cannot expect, in general, that $\mathscr{A}/\langle\pi\rangle$ covers $\mathscr{A}$ in the traditional sense. But if we examine the properties of the relation $\alpha$ we see that $\alpha(H_i)s \subseteq \alpha(H_i \circledast [s])$ for all $s\in S$, $i\in I$. This is very similar to the requirement that $[s]$ covers $s$ with respect to $\alpha$, but now $\alpha$ is a relation and not necessarily a function. This leads us to the following concept.

Let $\mathscr{A}=(Q, S)$, $\mathscr{B}=(P, T)$ be transformation semigroups. A relation $\alpha: P \rightsquigarrow Q$ is called a *relational covering of $\mathscr{A}$ by $\mathscr{B}$* if

(i) $\alpha$ is surjective

(ii) given any $s\in S$ there exists a $t\in T$

such that

$$\alpha(p)\cdot s \subseteq \alpha(p\cdot t) \quad \text{for all } p\in P. \qquad (*)$$

We then write $\mathscr{A} \lhd_\alpha \mathscr{B}$, or just $\mathscr{A} \lhd \mathscr{B}$ if a specific reference to the relation $\alpha$ is unnecessary. In the inequality $(*)$ the element $t$ is said to *cover s*.



If we recall that $\alpha$ is a completely additive relation the first condition yields $\bigcup_{p\in P}\alpha(p)=Q$. Each image $\alpha(p)$, $p\in P$, is a subset of $Q$ and the collection of the distinct such images covers $Q$ in the set-theoretical sense. Condition (ii) tells us, further, that the collection $\{\alpha(p) \mid p\in P\}$, of images under $\alpha$, forms an admissible subset system. To see the connection between relational coverings, admissible subset systems and related quotient transformation semigroups we introduce a new concept.

Let $\mathscr{A} \lhd_\alpha \mathscr{B}$ be a relational covering, where $\mathscr{A}=(Q, S)$ and $\mathscr{B}=(P, T)$. Define $T_\alpha$ to be the set of elements of $T$ that cover some element of $S$ with respect to $\alpha$, so $T_\alpha=\{t\in T \mid \exists s\in S$ such that $\alpha(p)s\subseteq\alpha(pt)$ for all $p\in P\}$. We say that the relation $\alpha$ is *close* if:

$$\alpha(p)=\alpha(p') \Rightarrow \alpha(pt)=\alpha(p't) \quad \text{for all } t\in T_\alpha, \text{ where } p, p'\in P.$$

It should be noted that although close coverings abound in the theory, by no means are all relational coverings close.

*Theorem 4.1.1*

Let $\mathscr{A}=(Q, S)$, $\mathscr{B}=(P, T)$ be transformation semigroups. If $\mathscr{A} \lhd_\alpha \mathscr{B}$ is a relational covering then $\{\alpha(p) \mid p\in P\}$ is an admissible subset system. If $\pi$ is an admissible subset system and $\mathscr{A}/\langle\pi\rangle$ is a chosen quotient defined by $\pi$ then $\mathscr{A} \lhd \mathscr{A}/\langle\pi\rangle$. If $\mathscr{A} \lhd_\alpha \mathscr{B}$ is a close relational covering and $\pi=\{\alpha(p), p\in P\}$ then there exists a quotient $\mathscr{A}/\langle\pi\rangle$ such that $\mathscr{A}/\langle\pi\rangle \leq \mathscr{B}$. If $\pi$ is a partition then $\mathscr{A}/\langle\pi\rangle \leq \mathscr{B}$.

*Proof* The first two statements are immediate. Suppose now that $\mathscr{A} \lhd_\alpha \mathscr{B}$ is close. Let $\alpha(p)\in\pi$ and $s\in S$. There exists a $t\in T$ such that $\alpha(p)s\subseteq\alpha(pt)$ for all $p\in P$. We define an operation $\circledast$ of $S$ on $\pi$ by putting $\alpha(p)\circledast s=\alpha(pt)$ for each $\alpha(p)\in\pi$, $s\in S$. This operation is well-defined, for if $\alpha(p)=\alpha(p')$, $p, p'\in P$, then $\alpha(pt)=\alpha(p't)$ for all $t\in T_\alpha$. Hence $\alpha(p)\circledast s=\alpha(pt)=\alpha(p')\circledast s$. We now turn the pair $(\pi, S)$ into a transformation semigroup $\mathscr{A}/\langle\pi\rangle$ by finding a quotient of $S$ that acts faithfully on $\pi$. Then $\alpha: P\to\pi$ is a mapping such that $\mathscr{A}/\langle\pi\rangle \leq \mathscr{B}$. If $\pi$ is a partition then $\circledast$ is well-defined anyway.

*Example 4.2*

Let $\mathscr{A}$ and $\mathscr{B}$ be the transformation semigroups defined by the state machines

| | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|---|---|---|---|---|---|---|
| 0 | $a$ | $c$ | $b$ | $e$ | $c$ | $c$ |
| 1 | $c$ | $b$ | $a$ | $b$ | $f$ | $f$ |

and

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 0 | B | A | D | C | A |
| 1 | A | B | C | A | C |

The relation $\alpha(A)=\alpha(B)=\{a,b,c\}$, $\alpha(C)=\alpha(E)=\{b,e,f\}$, $\alpha(D)=\{c,d\}$, defines a relational covering $\mathcal{A}\lhd_\alpha\mathcal{B}$ which is not close. If $\pi$ is the admissible subset system defined by $\alpha$ then $\pi$ is $\{\{a,b,c\},\{b,e,f\},\{c,d\}\}$. If we denote $\{a,b,c\}$ by $X$, $\{b,e,f\}$ by $Y$ and $\{c,d\}$ by $Z$ we can then find the possible quotient transformation semigroups $\mathcal{A}/\langle\pi\rangle$. There are two of these defined by

| | $X$ | $Y$ | $Z$ |
|---|---|---|---|
| 0 | $X$ | $X$ | $Y$ |
| 1 | $X$ | $Y$ | $X$ |

and

| | $X$ | $Y$ | $Z$ |
|---|---|---|---|
| 0 | $X$ | $Z$ | $Y$ |
| 1 | $X$ | $Y$ | $X$ |

In neither case does $\mathcal{A}/\langle\pi\rangle\le\mathcal{B}$ hold, and so theorem 4.1.1 is not true for all relational coverings.

### 4.2 The skeleton and height functions

If $\mathcal{A}=(Q,S)$ is a transformation semigroup and $s\in S$ then $Qs=\{qs\mid q\in Q\}$ will be called the *image under s*. The collection of all these images constitutes a very important subset of the power set $\mathcal{P}(Q)$. In many ways the properties of this set of images reflect the structure of $\mathcal{A}$. A natural ordering exists on this set of images, but first we extend the set slightly. Define

$$\mathrm{I}(\mathcal{A})=\Big(\bigcup_{s\in S}\{Qs\}\Big)\cup\{Q\}\cup\Big(\bigcup_{q\in Q}\{\{q\}\}\Big)\cup\{\varnothing\}.$$

Thus $\mathrm{I}(\mathcal{A})$ consists of the set of all the images under the elements of $S$, together with the set $Q$ and $\varnothing$ and the singleton subsets of $Q$. If $1_Q\in S$ then it is not necessary to adjoin the set $Q$ in this way. Similarly each reset map in $S$ will give rise to the appropriate singleton in $Qs$, so that if $1_Q\in S$ and $\mathcal{A}$ is closed then $\mathrm{I}(\mathcal{A})=\bigcup_{s\in S}\{Qs\}\cup\{\varnothing\}$.

Now let $A,B\in\mathrm{I}(\mathcal{A})$, we write $A\le B$ if and only if either $A\subseteq B$ or $A\subseteq Bs$ for some $s\in S$. (The existence of the identity $1_Q$ in $S$ will ensure that the first condition follows from the second.) This ordering on the set $\mathrm{I}(\mathcal{A})$ satisfies the following properties:



4.2.1(i) $A\le A$

4.2.1(ii) $A\le B$ and $B\le C\Rightarrow A\le C$.

We further define $A<B$ to mean $A\le B$ but $B\not\le A$. Then $(\mathrm{I}(\mathcal{A}),\le)$ is seen to be a pre-ordered set. We call $(\mathrm{I}(\mathcal{A}),\le)$ the *skeleton* of $\mathcal{A}$. Notice, however, that distinct transformation semigroups may have identical skeletons, so that although the skeleton gives us much information about $\mathcal{A}$ it cannot tell us everything about it.

In the usual way we construct an equivalence relation on $\mathrm{I}(\mathcal{A})$ by defining

$A\equiv B$ if and only if $A\le B$ and $B\le A$.

We immediately obtain the following information.

*Proposition 4.2.1*

If $A,B\in\mathrm{I}(\mathcal{A})$ then

(i) $A\le B\Rightarrow|A|\le|B|$

(ii) $A\equiv B\Rightarrow|A|=|B|$

*Proof* Both follow from the simple observation that $|Bs|\le|B|$ since $|B|$ is finite. □

*Example 4.3*

Returning to the transformation semigroup $\mathcal{A}$ defined in example 4.1 we will calculate $\mathrm{I}(\mathcal{A})$. We get $\mathrm{I}(\mathcal{A})=\{Q,\{a,c\},\{a\},\{b\},\{c\},\varnothing\}$. The ordering on $\mathrm{I}(\mathcal{A})$ will be displayed in diagrammatic form, with $A\le B$ being replaced by an arrow $A\to B$. (We usually omit $\varnothing$ from the diagram.)

$$\begin{tikzcd}
 & Q & \\
 & \{a,c\} \arrow[u] & \\
\{a\} \arrow[ur] \arrow[r, leftrightarrow] & \{b\} \arrow[u] \arrow[r] & \{c\} \arrow[ul]
\end{tikzcd}$$

Then $\{a\}\equiv\{b\}$, but $\{b\}<\{c\}$ and $\{a\}<\{c\}$.

*Example 4.4*

Let $|Q|=n$ ($n$ a positive integer) and let $S$ be the set of all functions from $Q$ to $Q$. Then $\mathcal{A}=(Q,S)$ is a transformation semigroup.

Now $\mathbf{I}(\mathscr{A}) = \mathscr{P}(Q)$ and if $A, B \subseteq Q$ then $A \leq B \Leftrightarrow |A| \leq |B|$, furthermore $A \equiv B \Leftrightarrow |A| = |B|$.

In this example we notice that $A \equiv B$ implies the existence of an element $s \in S$ such that $B = As$. An element $s' \in S$ also exists satisfying $A = Bs'$ and such that for any $a \in A$, $b \in B$, $ass' = a$, $bs's = b$. This last property is in fact a feature of any transformation semigroup.

*Proposition 4.2.2*

Let $\mathscr{A} = (Q, S)$ be a transformation semigroup. $A, B \in \mathbf{I}(\mathscr{A})$ with $A \equiv B$. There exist elements $s, \bar{s} \in S \cup \{1_Q\}$ such that

$$B = As, \quad A = B\bar{s},$$

and for all $a \in A$, $b \in B$,

$$as\bar{s} = a, \quad b\bar{s}s = b.$$

*Proof* Since $A \leq B$ and $B \leq A$ there exist elements $s, t \in S \cup \{1_Q\}$ such that $B \subseteq As$, $A \subseteq Bt$. As $|A| = |B|$ we have $B = As$ and $A = Bt$. Then $B = Bts$, $A = Ast$. Therefore $ts$ and $st$ are permutations on $B$ and $A$ respectively. If $st$ is an 'identity' on $A$, that is, if $ast = a$ for all $a \in A$, then for each $b \in B$ there exists an $a_1 \in A$ such that $b = a_1 s$. Then $bts = a_1 sts = a_1 s = b$, and thus $ts$ is an identity on $B$ and we may choose $\bar{s} = t$. If $st$ is not an identity on $A$ then $(st)^n$ is an identity on $A$ for some $n > 1$. Then we choose $\bar{s} = t(st)^{n-1}$ and note that $B\bar{s} = Bt(st)^{n-1} = A(st)^n = A$. Also, for $a \in A$, $as\bar{s} = a(st)^n = a$, and for $b \in B$, $b\bar{s}s = bt(st)^{n-1}s = a_1 st(st)^{n-1}s$ (where $b = a_1 s \in As$) $= a_1 s = b$. □

This result enables us to move easily between two equivalent images $A$ and $B$. If any input $\bar{s}$ acts as a permutation on the image set $A$ then $s'\bar{s}s$ will act as a permutation on the image set $B$. Since we are going to be interested in the permutations on these image sets later, this fact will prove useful. It will sometimes be convenient and suggestive to write $s$ as $(B/A)$ and $\bar{s}$ as $(A/B)$. Then $as\bar{s} = a(B/A)\cdot(A/B) = a$ and $b\bar{s}s = b(A/B)\cdot(B/A) = b$ for $a \in A$, $b \in B$.

In the example 4.4 the skeleton has a particularly nice form, it is arranged naturally in 'layers' with sets of equal cardinality arranged in the same layer. It is tempting to expect that we can do the same with a more general transformation semigroup, with, perhaps the equivalent sets arranged in the same layer. This is in fact the case but we can do much more; we will define a general height function that maps the skeleton in an order-preserving fashion into the set of integers. The



main requirements of the height function, apart from respecting the order on $\mathbf{I}(\mathscr{A})$, are that the function maps all singletons to zero and that there are 'no gaps in the image of it'. Formally we define a ***height function*** for $\mathscr{A} = (Q, S)$ to be any function $h: \mathbf{I}(\mathscr{A}) \to \mathbf{Z}$ satisfying:

(i) $h(\{q\}) = 0$ for all $q \in Q$, $h(\varnothing) = -1$.

(ii) $A \equiv B \Rightarrow h(A) = h(B)$.

(iii) $A < B$ and $|B| > 1 \Rightarrow h(A) < h(B)$.

(iv) If $0 \leq i \leq h(Q)$ then $\exists A \in \mathbf{I}(\mathscr{A})$ such that $h(A) = i$.

The last condition is just there to prevent the function from being 'too wasteful'. We cannot expect $A < B \Rightarrow h(A) < h(B)$ in all circumstances since we are also requiring the height of a singleton to be zero and this may conflict with the ordering on $\mathbf{I}(\mathscr{A})$. We have already seen example (4.3) where $\{a\} < \{c\}$ for $a, c \in Q$. This difficulty vanishes if the restriction $|B| > 1$ is imposed.

There may be various functions that satisfy these conditions for a given transformation semigroup. One always exists and is constructed in the following way. Given the skeleton $(\mathbf{I}(\mathscr{A}), \leq)$ of the transformation semigroup $\mathscr{A}$, let $A \in \mathbf{I}(\mathscr{A})$ with $|A| > 1$. Suppose that $A_1 < A_2 < \ldots < A_n = A$ is the longest chain in $\mathbf{I}(\mathscr{A})$ satisfying $|A_1| > 1$. We define $h(A) = n$. For $A \in I(\mathscr{A})$ satisfying $|A| = 1$ we put $h(\mathscr{A}) = 0$ and $h(\varnothing) = -1$. In this way we may now associate an integer with every element of $\mathbf{I}(\mathscr{A})$, and so define a function $h: \mathbf{I}(\mathscr{A}) \to \mathbf{Z}$.

To show that $h$ satisfies the four conditions is fairly straightforward. For example let $A, B \in \mathbf{I}(\mathscr{A})$ with $A \equiv B$. If $|A| = |B| = 1$ then $h(A) = h(B) = 0$. Let $|A| > 1$, $|B| > 1$. Suppose that $h(A) = n$, $h(B) = m$ then there exist chains

$$A_1 < A_2 < \ldots < A_n = A, \quad B_1 < B_2 < \ldots < B_m = B$$

each of maximal length subject to the requirement $|A_1| \neq 1$, $|B_1| \neq 1$. Then $A \leq B$ and $B \leq A$, yielding $A_{n-1} < B$ and $B_{m-1} < A$. If $m > n$ we obtain the longer chain $B_1 < \ldots < B_{m-1} < A$ of length $m$ for $A$ which is false. Similarly $n > m$ is incorrect and so $m = n$. The height function just defined is called the ***minimal height function*** for the transformation semigroup. The ***height of*** $\mathscr{A}$ is defined to be $h(Q)$ where $h$ is this minimal height function (we sometimes write the height of $\mathscr{A}$ as $h(\mathscr{A})$ also).

Given the minimal height function various other height functions may then be defined. For example let $\{A_{ij}\}$ $(j = 1, \ldots, m_i)$ be the distinct $\equiv$-equivalence classes of $\mathbf{I}(\mathscr{A})$ of minimal height $i \geq 1$. Put $l(A_{ij}) = \sum_{k=1}^{i-1} m_k + j$. This yields a height function $l: I(\mathscr{A}) \to \mathbf{Z}$ when we define $l(\{q\}) = 0$ for all $q \in Q$ and $l(\varnothing) = 0$. It is a maximal height function in the sense that $l(Q)$ is a maximum, but is not unique with respect to this property in general, since it depends on the order in which the equivalence classes of height $i$ are enumerated.

Now we consider an arbitrary transformation semigroup $\mathscr{A}=(Q,S)$ together with a height function $h:\mathrm{I}(\mathscr{A})\to\mathbf{Z}$. Suppose that $\mathscr{B}=(P,T)$ is a transformation semigroup such that $\mathscr{A}\lhd_\alpha\mathscr{B}$. The subsets $\alpha(p)$, $p\in P$ may not be images in $\mathscr{A}$ but we will be particularly interested in the occasions when they are. We say that the relational covering $\mathscr{A}\lhd_\alpha\mathscr{B}$ is of *rank* $i$ (with respect to $h$) if:

(i) $\alpha(p)\in\mathrm{I}(\mathscr{A})$ for all $p\in P$,

(ii) $h(\alpha(p))\le i$ for all $p\in P$ and $h(\alpha(p))=i$ for at least one $p\in P$ where $0\le i\le h(Q)$.

We will consider an example shortly, but before we do note that a relational covering of rank 0 is merely a covering since the image $\alpha(p)$ is a singleton for all $p\in P$, and thus $\alpha$ is a mapping. (The fact that the only elements of the skeleton that have height zero are singletons follows from condition (iii) of the height function.)

*Example 4.5*

Let $\mathscr{A}=(Q,S)$ be an arbitrary transformation semigroup with height function $h$, and suppose that $h(Q)=n$. Consider the 'proper maximal images' in $\mathrm{I}(\mathscr{A})$. Formally define

$$\mathrm{M}(Q)=\{A\in\mathrm{I}(\mathscr{A})\mid A\ne Q \text{ and } A\subseteq C\subseteq Q \text{ with } C\in\mathrm{I}(\mathscr{A}) \Rightarrow \text{either } C=A \text{ or } C=Q\}.$$

We show that $\mathrm{M}(Q)$ forms an admissible subset system for $\mathscr{A}$. First note that if $q\in Q$ then either $\{q\}\in\mathrm{M}(Q)$ or $q\in A$ for some $A\in\mathrm{M}(Q)$ and so the subsets in $\mathrm{M}(Q)$ cover $Q$. Further let $A\in\mathrm{M}(Q)$ and $s\in S$. Since $A=Qs_1$ for some $s_1\in S$ we have $As=Qs_1s\in\mathrm{I}(\mathscr{A})$ and either $As\in\mathrm{M}(Q)$ or $As\subseteq A_1$ for some $A_1\in\mathrm{M}(Q)$. Therefore $\mathrm{M}(Q)$ is an admissible subset system for $\mathscr{A}$. Now consider the way in which the elements of $S$ act on the subsets in $\mathrm{M}(Q)$. If $s$ is a permutation of $Q$ then $s$ is also a permutation on the set $\mathrm{M}(Q)$. First let $A\in\mathrm{M}(Q)$ then $As\in\mathrm{I}(\mathscr{A})$ and let $C\in\mathrm{I}(\mathscr{A})$ with $As\subseteq C\subseteq Q$. If $s\ne 1_Q$ then $s^m=1_Q$ for some $m>1$ and we see that $A=Ass^{m-1}\subseteq Cs^{m-1}\subseteq Qs^{m-1}=Q$. Therefore $Cs^{m-1}=A$ or $Cs^{m-1}=Q$, that is $C=Cs^m=As$ or $C=Q$. Thus $As\in\mathrm{M}(Q)$. If $s$ is not a permutation of $Q$ then $Qs\subset Q$ and $Qs\subseteq A$ for some $A\in\mathrm{M}(Q)$. Now let $B\in\mathrm{M}(Q)$, then $Bs\subseteq Qs\subseteq A$ so $s$ has the effect of sending each element of $\mathrm{M}(Q)$ to the element $A$. We now define a transformation semigroup using the elements of $\mathrm{M}(Q)$ as the states. Let $s\in S$, then either $Qs=Q$ or $Qs\subseteq B$ for some $B\in\mathrm{M}(Q)$. Suppose that for each $s$ satisfying $Qs\ne Q$ we select a $B_s\in\mathrm{M}(Q)$ such that $Qs\subseteq B_s$, now define for $B'\in\mathrm{M}(Q)$ the operation:

$$B'\circledast s=\begin{cases} B's & \text{if } Qs=Q\\ B_s & \text{if } Qs\ne Q,\ Qs\subseteq B_s \text{ and } B_s \text{ is the chosen element}\\ & \text{of } \mathrm{M}(Q) \text{ associated with } s.\end{cases}$$

The pair $(\mathrm{M}(Q),S)$ gives rise to a transformation semigroup $(\mathrm{M}(Q),S/{\sim})$ under the operation $\circledast$ in the same way as section 4.1. Therefore this transformation semigroup may be denoted by $\mathscr{A}/\langle\pi\rangle$ where $\pi=\mathrm{M}(Q)$.

If we define a relation $\alpha:\pi\rightsquigarrow Q$ by

$$\alpha(B)=B \quad \text{for } B\in\pi$$

we obtain a relational covering $\mathscr{A}\lhd_\alpha\mathscr{A}/\langle\pi\rangle$ of rank $n-1$. Because of the special choice of the quotient $\mathscr{A}/\langle\pi\rangle$ we may cover $\mathscr{A}/\langle\pi\rangle$ with a particularly useful transformation semigroup. Notice that the semigroup $S/{\sim}$ of $\mathscr{A}/\langle\pi\rangle$ is generated by a quotient of the maximal subgroup $G$ of $S$ and some reset elements. Then $S/{\sim}\subseteq Sg\langle(G/{\sim})\cup(\bigcup_{B\in\pi}\bar{B})\rangle$ where each $\bar{B}$ is the reset map $\bar{B}:B'\to B$ for all $B'\in\pi$. The inclusion may be strict in some cases. The group $G/{\sim}$ is called the *holonomy group of* $Q$ and it is to this that we now turn our attention.

### 4.3 The holonomy groups

Let $A\in\mathrm{I}(\mathscr{A})$ with $|A|>1$. First we define the *maximal image space* (or *paving*) of $A$ to be the set

$$\mathrm{M}(A)=\{B\in\mathrm{I}(\mathscr{A})\mid B\subset A,\ B\ne A \text{ and } B\subseteq C\subseteq A \text{ with } C\in\mathrm{I}(\mathscr{A})\Rightarrow\text{either } C=A \text{ or } C=B\}.$$

The elements $B$ of $\mathrm{M}(A)$ are called the *maximal images* (or *bricks*) of $A$. The collection $\mathrm{M}(A)$ forms a covering of the set $A$, for if $a\in A$ then $\{a\}\in\mathrm{I}(\mathscr{A})$ and either $\{a\}\in\mathrm{M}(A)$ or $\{a\}\subseteq B$ for some $B\in\mathrm{M}(A)$.

Put $\mathrm{G}(A)=\{s\in S\mid As=A\}$, the set of all elements of $S$ that act as permutations on the set $A$. Naturally $\mathrm{G}(A)$ may be empty. We have:

*Proposition 4.3.1*

For $A\in\mathrm{I}(\mathscr{A})$ with $|A|>1$, each element of $\mathrm{G}(A)$ acts as a permutation on the set $\mathrm{M}(A)$.

*Proof* Let $s\in\mathrm{G}(A)$ and $B\in\mathrm{M}(A)$. Then $Bs\subset A$ and $Bs\in\mathrm{I}(\mathscr{A})$. Suppose that $Bs\subseteq C\subseteq A$. There exists some integer $n\ge 1$ such that $s^n$ acts as the identity on $A$. Either $Bs=B$ or $B=Bss^{n-1}\subset Cs^{n-1}\subseteq As^{n-1}=A$. Therefore $B=Cs^{n-1}$ or $A=Cs^{n-1}$ and so $Bs=C$ or

$A = C$. Hence $Bs \in \mathbf{M}(A)$. Clearly $s^{n-1} \in \mathbf{G}(A)$ and the inverse of $s$ on $\mathbf{M}(A)$ is $s^{n-1}$. □

By considering only the *distinct* permutations of $\mathbf{M}(A)$ given by the elements of $\mathbf{G}(A)$ we may define a transformation group $(\mathbf{M}(A), \mathbf{H}(A))$, providing of course that $\mathbf{G}(A) \neq \emptyset$. (Thus $\mathbf{H}(A)$ is a quotient of $\mathbf{G}(A)$.) If $\mathbf{G}(A) = \emptyset$ then we consider the *generalized* transformation group $(\mathbf{M}(A), \emptyset)$. This can only occur if $S$ does not contain the identity $1_Q$. In this case we will also write $\mathbf{H}(A) = \emptyset$.

The generalized transformation group $\mathcal{H}(A) = (\mathbf{M}(A), \mathbf{H}(A))$ is called the *holonomy transformation group of* $A$. The group $\mathbf{H}(A)$ is the *holonomy group of* $A$ (if $\mathbf{H}(A) \neq \emptyset$).

We may, by referring back to example 4.5 notice that the transformation semigroup $\mathcal{A}/\langle\pi'\rangle$ chosen there may be covered by the closure of the *holonomy* transformation group of $Q$ and thus $\mathcal{A} \prec_\alpha \overline{\mathcal{H}(Q)}$ is of rank $n-1$ where $n$ is the height of $\mathcal{A}$ with respect to the given height function. Notice also that the covering $\alpha$ is close.

Our next aim is to improve the relational covering constructed in example 4.5. Before we do this, however, we will dispose of three useful technical results concerned with maximal image spaces and holonomy groups.

*Proposition 4.3.2*

Let $\mathcal{A} = (Q, S)$ be a transformation semigroup, $h: \mathbf{I}(\mathcal{A}) \to \mathbf{Z}$ a height function and $h(Q) = n \geq 1$. Then we have:

(i) If $h(A) = n$ for some $A \in \mathbf{I}(\mathcal{A})$ then $A = Q$.

(ii) If $A, B \in \mathbf{I}(\mathcal{A})$ with $A \subsetneq B$ and $|B| > 1$ then $h(A) < h(B)$.

(iii) If $A, B \in \mathbf{I}(\mathcal{A})$ with $A \equiv B$ and $s, \bar{s} \in S$ satisfying the hypothesis of 4.2.2, then $\mathbf{M}(B) = \mathbf{M}(A)s$ and $\mathbf{M}(A) = \mathbf{M}(B)\bar{s}$.

*Proof* (i) $A \subseteq Q$ and so $h(A) \leq h(Q)$. Suppose that $A \subsetneq Q$, then $Q \leq A$ implies that $Q \subseteq As$ for some $s \in S$, so $|Q| \leq |As| \leq |A| \leq |Q|$ which yields a contradiction. Hence $A < Q$ and so $h(A) < h(Q)$. Therefore $h(A) = n \Rightarrow A = Q$.

(ii) This is proved in a similar way to (i).

(iii) Let $A = B\bar{s}$ and $B = As$ with $as\bar{s} = a$ for all $a \in A$, $b\bar{s}s = b$ for all $b \in B$. Consider $K \in \mathbf{M}(A)$, then $Ks \in \mathbf{I}(\mathcal{A})$. Let $Ks \subseteq C \subseteq B$ for some $C \in \mathbf{I}(\mathcal{A})$, then $K = Ks\bar{s} \subseteq C\bar{s} \subseteq B\bar{s} = A$ and $C\bar{s} \in \mathbf{I}(\mathcal{A})$ which implies $C\bar{s} = K$ or $C\bar{s} = A$ and thus $C = Ks$ or $C = B$. Therefore $Ks \in \mathbf{M}(B)$. Now let $L \in \mathbf{M}(B)$, then $L\bar{s}s = L$ and $L\bar{s} \subsetneq A$. Let us choose any $D \in \mathbf{I}(A)$ with $L\bar{s} \subseteq D \subseteq A$, then $L = L\bar{s}s \subseteq Ds \subseteq As = B$ and so $Ds = L$ or $Ds = B$, which gives $D = L\bar{s}$ or $D = A$. Therefore $\mathbf{M}(B) = \mathbf{M}(A) \cdot s$. The other result is proved similarly. □



*Proposition 4.3.3*

If $A \equiv B$ then $\mathcal{H}(A) \cong \mathcal{H}(B)$.

*Proof* $\mathcal{H}(A) = (\mathbf{M}(A), \mathbf{H}(A))$, $\mathcal{H}(B) = (\mathbf{M}(B), \mathbf{H}(B))$. There is a mapping $\phi: \mathbf{M}(A) \to \mathbf{M}(B)$ defined by $\phi(K) = Ks$ where $K \in \mathbf{M}(A)$ and $s \in S$ is such that $B = As$. Then $A = B\bar{s}$ for a suitable $\bar{s} \in S$ and so $\phi$ is invertible with inverse $\psi: \mathbf{M}(B) \to \mathbf{M}(A)$ defined by $\psi(L) = L\bar{s}$ for $L \in \mathbf{M}(B)$. Now we choose a $g \in \mathbf{G}(A)$ which satisfies $Ag = A$ and so $B(\bar{s}gs) = Ags = As = B$ which allows us to define a mapping $\xi: \mathbf{G}(A) \to \mathbf{G}(B)$ by $\xi(g) = \bar{s}gs$ for all $g \in G(A)$. The mapping $\eta: \mathbf{G}(B) \to \mathbf{G}(A)$ defined by $\eta(g') = sg'\bar{s}$ for all $g' \in \mathbf{G}(B)$ is the inverse of $\xi$. Finally we notice that for $g, g_1 \in \mathbf{G}(A)$,

$$B(\bar{s}gs)(\bar{s}g_1s) = B$$

and for $b \in B$,

$$b\xi(g)\xi(g_1) = b\bar{s}gs\bar{s}g_1s = b\bar{s}gg_1s = b\xi(gg_1)$$

and therefore $\xi$ is an isomorphism of groups. The factor groups $\mathbf{H}(A)$ and $\mathbf{H}(B)$ must also be isomorphic since $A \equiv B$. □

Now we may return to the central problem of improving the relational covering of example 4.4. So we let $\mathcal{A} = (Q, S)$ be a transformation semigroup and $h: \mathbf{I}(\mathcal{A}) \to \mathbf{Z}$ a height function. Suppose that $\pi$ is an admissible subset system with the property that each subset $A \in \pi$ also belongs to the skeleton $\mathbf{I}(\mathcal{A})$ and the maximum height of an element of $\pi$ is $i$. Such an admissible subset system is said to have *rank* $i$. We may now produce an admissible subset system $\pi'$ of rank $i-1$ with $\pi' \leq \pi$ (assuming that $i \geq 1$).

First let $\mathcal{X} = \{A \in \pi \mid h(A) < i\}$ and $\mathcal{Y} = \{A \in \pi \mid h(A) = i\}$. Then we define $\pi' = \mathcal{X} \cup (\bigcup_{Y \in \mathcal{Y}} \mathbf{M}(Y))$ where, as before, $\mathbf{M}(Y)$ is the maximal image space of $Y$. Clearly $\pi' \leq \pi$ and the rank of $\pi'$ equals $i-1$; we have to establish the fact that $\pi'$ is an admissible subset system, so we let $B \in \pi'$ and $s \in S$. If $B \in \mathcal{X}$ then $B \in \pi$ and so $Bs \subseteq A$ for some $A \in \pi$. This leads to two cases:

Case (i): $A \in \mathcal{X}$, in which case $Bs$ is contained in a subset of $\pi'$.

Case (ii): $Bs \subseteq A$ with $A \in Y$. Since $Bs \leq B$ and $h(B) < i$ then $h(Bs) < i$ and so there exists $C \in \mathbf{M}(A)$ such that $Bs \subseteq C$. Therefore $Bs$ is contained in an element of $\pi'$.

If $B \in \mathbf{M}(Y)$ for some $Y \in \mathcal{Y}$ then $Bs \subseteq Ys$. We have three further cases to consider:

Case (iii): $Ys \subseteq A$ for some $A \in \mathcal{X}$ and then $Bs \subseteq A$.

Case (iv): $Ys \subsetneq A$ for some $A \in \mathcal{Y}$, then $Ys \subseteq C$ for some $C \in \mathbf{M}(A)$ and so $Bs \subseteq C$ with $C \in \pi'$.

Case (v): $Ys \in \mathcal{Y}$. Now $Ys \leq Y$ and $h(Ys) = h(Y) = i$, hence $Ys \equiv Y$. By 4.3.2(iii) $\mathbf{M}(Ys) = \mathbf{M}(Y)s$ and so $Bs \in \mathbf{M}(Y')$ and thus $Bs \in \pi'$.

This result is stated as:

*Theorem 4.3.4*

Let $\mathcal{A} = (Q, S)$ be a transformation semigroup and $h: \mathbf{I}(\mathcal{A}) \to \mathbf{Z}$ a height function. Let $\pi$ be an admissible subset system of rank $i$. There exists an admissible subset system $\pi'$ of rank $i-1$ with $\pi' \leq \pi$.

In this way we may start with an admissible subset system of $\mathcal{A}$ of rank equal to the height of $\mathcal{A}$ and successively reduce the rank of the covering. First let $\pi^n$ be the trivial admissible subset system $\{Q\}$ where $n = h(Q)$ then $(\pi^n)'$ is the admissible subset system of example 4.4. Putting $\pi^{n-1} = (\pi^n)'$, $\pi^{n-2} = (\pi^{n-1})', \ldots$ we obtain a sequence $\pi^n > \pi^{n-1} > \pi^{n-2} > \ldots$ of admissible subset systems. We call this the *derived sequence* of $\mathcal{A}$. The rank of $\pi^n$ equals the height $n$ of $\mathcal{A}$, the rank of $\pi^{n-1}$ equals $n-1$, and in general $\pi^j$ has rank $j$. We will use the derived sequence as a means of defining a relational covering of $\mathcal{A}$ using transformation groups. Notice that if we can associate a suitable relational covering of $\mathcal{A}$ with the admissible subset system $\pi^j$ then there may be a natural candidate for a relational covering associated with $\pi^{j-1}$.

Suppose that $\pi^j = \mathcal{X} \cup \mathcal{Y}$ where the elements of $\mathcal{X}$ are of height less than $j$ and the height of the elements of $\mathcal{Y}$ is $j$. The definition of $\pi^{j-1}$ is $\mathcal{X} \cup \bigcup_{Y \in \mathcal{Y}} \mathbf{M}(Y)$. The sets $\mathbf{M}(Y)$ are the underlying sets of the holonomy transformation groups $\mathcal{H}(Y)$. We have seen that when $j = n$ the closure of the holonomy transformation group $\mathcal{H}(Q)$ yields a relational covering of $\mathcal{A}$ of rank $n-1$. (Here $n$ is the height of $Q$.) Can we build on this to produce an inductive method of generating relational coverings of smaller rank?

Let $1 \leq j \leq n$ where $n = h(Q)$. The set of elements of the skeleton of height $j$ may be partitioned by the equivalence relation $\equiv$. Let $A^j_1, \ldots, A^j_{r_j}$ be a set of representatives of the distinct equivalence classes. We form the holonomy transformation groups $\mathcal{H}(A^j_1), \ldots, \mathcal{H}(A^j_{r_j})$ and then take their join $\mathcal{H}(A^j_1) \vee \ldots \vee \mathcal{H}(A^j_{r_j})$. This is also denoted by $\mathcal{H}^\vee_j(\mathcal{A})$. The state set of this transformation semigroup must be defined with care, for we need the individual state sets of $\mathcal{H}(A^j_k)$ to be disjoint if we are going to form the join. To ensure this we will consider the state set of $\mathcal{H}(A^j_k)$ to be $\{k\} \times \mathbf{M}(A^j_k)$. So a typical element of the state set of $\mathcal{H}^\vee_j(\mathcal{A})$ is $(k, B^j_k)$ where $1 \leq k \leq r_j$, $B^j_k \in \mathbf{M}(A^j_k)$.



We now state our main inductive result.

*Theorem 4.3.5*

Let $\mathcal{A} \lhd_{\alpha_j} \mathcal{B}$ be a relational covering of rank $j$ such that the image of $\alpha_j$ is $\pi^j$. There exists a relational covering $\mathcal{A} \lhd_{\alpha_{j-1}} \mathcal{H}^\vee_j(\mathcal{A}) \circ \mathcal{B}$ such that

(i) the rank of $\alpha_{j-1}$ is $j-1$,

(ii) the image of $\alpha_{j-1}$ is $\pi^{j-1}$.

*Proof* Let $\mathcal{A} = (Q, S)$ and $\mathcal{B} = (P, T)$. If $s \in S$ there exists $t_s \in T$ such that

$$\alpha_j(p) \cdot s \subseteq \alpha_j(p \cdot t_s) \quad \text{for all } p \in P.$$

To define $\alpha_{j-1}: (\bigcup_{k=1}^{r_j} (\{k\} \times \mathbf{M}(A^j_k))) \times P \rightsquigarrow Q$ consider an element $((k, B^j_k), p) \in (\bigcup_{k=1}^{r_j} (\{k\} \times \mathbf{M}(A^j_k))) \times P$ and put

$$\alpha_{j-1}((k, B^j_k), P) = \begin{cases} \alpha_j(p) & \text{if } h(\alpha_j(p)) < j \\ B^j_k \cdot (\alpha_j(p)/A^j_k) & \text{if } \alpha_j(p) \equiv A^j_k \\ \varnothing & \text{otherwise.} \end{cases}$$

From this definition we note that $\alpha_{j-1}((k, B^j_k), p)$ is an element of the skeleton of $\mathcal{A}$ of height less than $j$. Furthermore $B^j_k \cdot (\alpha_j(p)/A_k) \in \mathbf{M}(\alpha_j(p))$. Since the image of $\alpha_j$ is $\pi^j$, suppose that $Z \in \pi^{j-1}$. If $Z \in \pi^j$ we have $h(Z) < j$ and $Z = \alpha_j(p)$ for some $p \in P$ and so $\alpha_{j-1}((k, B^j_k), p) = \alpha_j(p) = Z$ for any $(k, B^j_k) \in \bigcup_{k=1}^{r_j} (\{k\} \times \mathbf{M}(A^j_k))$. Writing $\pi^j$ as $\mathcal{X} \cup \mathcal{Y}$ as in 4.3.4 we have $\pi^{j-1} = \mathcal{X} \cup (\bigcup_{Y \in \mathcal{Y}} \mathbf{M}(Y))$. If $Z \in \mathbf{M}(Y)$ for some $Y \in \mathcal{Y}$ then $Y \in \pi^j$ and $Y = \alpha_j(p)$ for some $p \in P$. Now $Y \equiv A_k$ for some $1 \leq k \leq r_j$ and $Y = A_k \cdot (Y/A_k)$. Then $Z = B \cdot (Y/A_k)$ for some $B \in \mathbf{M}(A_k)$ and $Z = \alpha_{j-1}((k, B), p)$. Hence the image of $\alpha_{j-1}$ equals $\pi^{j-1}$.

The proof of the fact that $\alpha_{j-1}$ is a relational covering now occupies our attention for a few paragraphs. The crucial part is the definition of the element of the action semigroup of $\mathcal{H}^\vee_j(\mathcal{A}) \circ \mathcal{B}$ that will cover a given element of $S$.

Let $s \in S$ and suppose that $t_s \in T$ covers $s$ with respect to the relational covering $\alpha_j$. Thus $\alpha_j(p) \cdot s \subseteq \alpha_j(p \cdot t_s)$ for all $p \in P$. Now the action semigroup of $\mathcal{H}^\vee_j(\mathcal{A}) \circ \mathcal{B}$ consists of the set of all ordered pairs $(f, t)$ where $t \in T$ and $f: P \to (\bigvee_{k=1}^{r_j} \mathbf{H}(A^j_k))$. Having chosen our element $s \in S$ we define a function $f_s : P \to \overline{(\bigvee_{k=1}^{r_j} \mathbf{H}(A_k^j))}$ in the following way. Let $p \in P$, three possibilities arise:

Case (i): $\alpha_j(p \cdot t_s) \in \mathscr{X}$, whence $f_s(p)$ is chosen arbitrarily.

Case (ii): $\alpha_j(p \cdot t_s) \in \mathscr{Y}$ and $\alpha_j(p) \cdot s \subsetneq \alpha_j(p \cdot t_s)$ then $\alpha_j(p \cdot t_s) \equiv A_k^j$ for some $1 \le k \le r_j$. Now

$$\alpha_j(p) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s)) \subsetneq \alpha_j(p \cdot t_s) \cdot (A_k^j/\alpha_j(p \cdot t_s)) = A_k^j$$

and so $\alpha_j(p) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s)) \subseteq B'$ for some $B' \in \mathbf{M}(A_k^j)$. We put $f_s(p) = \overline{(k, B')}$, the constant map.

Case (iii): $\alpha_j(p \cdot t_s) \in \mathscr{Y}$ and $\alpha_j(p) \cdot s = \alpha_j(p \cdot t_s)$, then $\alpha_j(p) \equiv \alpha_j(p \cdot t_s)$ since $\alpha_j(p) \cdot s \le \alpha_j(p)$ and yet $\alpha_j(p)$ is of height $j$ at most.

Now let $\alpha_j(p) \equiv A_k^j$ for some $1 \le k \le r_j$, then

$$A_k^j \cdot (\alpha_j(p)/A_k^j) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s)) = \alpha_j(p) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s))$$
$$= \alpha_j(p \cdot t_s)) \cdot (A_k^j/\alpha_j(p \cdot t_s)) = A_k^j.$$

The element $(\alpha_j(p)/A_k^j) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s))$ defines an element $h$ of the holonomy group $\mathbf{H}(A_k^j)$ and so we put

$$f_s(p) = h.$$

This defines the function $f : P \to \overline{\bigvee_{k=1}^{r_j} \mathbf{H}(A_k^j)}$. What remains is the task of showing that $(f_s, t_s)$ covers $s$ with respect to $\alpha_{j-1}$. Let $((l, B_l^j), p) \in (\bigcup_{k=1}^{r_j} (\{k\} \times \mathbf{M}(A_k^j))) \times P$, we will prove that

$$\alpha_{j-1}((l, B_l^j), p) \cdot s \subseteq \alpha_{j-1}(((l, B_l^j), p) \cdot (f_s, t_s)). \qquad (*)$$

In case (i), where $\alpha_j(p \cdot t_s) \in \mathscr{X}$, we have

$$\alpha_{j-1}((l, B_l^j), p) \cdot s = \alpha_j(p) \cdot s \subseteq \alpha_j(p \cdot t_s) \quad \text{if } \alpha_j(p) \in \mathscr{X},$$

and

$$\alpha_{j-1}((l, B_l^j), p) \cdot s \subseteq \alpha_j(p) \cdot s \subseteq \alpha_j(p \cdot t_s)$$

in all other cases.

Since $\alpha_j(p \cdot t_s) \in \mathscr{X}$, $f_s(p)$ is arbitrary and

$$\alpha_{j-1}(((l, B_l^j), p) \cdot (f_s, t_s)) = \alpha_{j-1}((l, B_l^j) \cdot f_s, p \cdot t_s))$$
$$= \alpha_j(p \cdot t_s).$$

Therefore the inequality $(*)$ holds in this case.

In case (ii) $\alpha_j(p \cdot t_s) \in \mathscr{Y}$ and $\alpha_j(p) \cdot s \subsetneq \alpha_j(p \cdot t_s)$. As before $\alpha_{j-1}((l, B_l^j), p) \cdot s \subsetneq \alpha_j(p) \cdot s$. Now $f_s(p) = \overline{(k, B')}$ where $B' \in \mathbf{M}(A_k^j)$ and $\alpha_j(p) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s)) \subseteq B'$, and so

$$\alpha_{j-1} \cdot (((l, B_l^j), p) \cdot (f_s, t_s)) = \alpha_{j-1}((k, B'), p \cdot t_s)$$
$$= B' \cdot (\alpha_j(p \cdot t_s)/A_k^j).$$



Now

$$\alpha_j(p) \cdot s = \alpha_j(p) \cdot s \cdot (A_k^j/\alpha_j(p \cdot t_s)) \cdot (\alpha_j(p \cdot t_s)/A_k^j)$$
$$\subseteq B' \cdot (\alpha_j(p \cdot t_s)/A_k^j)$$

and so $(*)$ holds again.

In case (iii), $\alpha_j(p \cdot t_s) \in \mathscr{Y}$ and $\alpha_j(p) \cdot s = \alpha_j(p \cdot t_s)$. If

$$\alpha_j(p) \equiv A_l^j$$

then

$$\alpha_{j-1}(((l, B_l^j), p) \cdot (f_s, t_s))$$
$$= \alpha_{j-1}((l, B_l^j \cdot (\alpha_j(p)/A_l^j) \cdot s \cdot (A_l^j/\alpha_j(p \cdot t_s))), p \cdot t_s)$$
$$= B_l^j \cdot (\alpha_j(p)/A_l^j) \cdot s \cdot (A_l^j/\alpha_j(p \cdot t_s)) \cdot (\alpha_j(p \cdot t_s)/A_l^j)$$
$$= B_l^j \cdot (\alpha_j(p)/A_l^j) \cdot s$$
$$= \alpha_{j-1}((l, B_l^j), p) \cdot s$$

and so $(*)$ holds. Finally if $\alpha_j(p) \not\equiv A^l$ then

$$\alpha_{j-1}((l, B_l^j), p) = \varnothing$$

and so

$$\alpha_{j-1}((l, B_l^j), p) \cdot s \subseteq \alpha_{j-1}(((l, B_l^j), p) \cdot (f_s, t_s))$$

as required. □

*Theorem 4.3.6*

Let $\mathscr{A}$ be a transformation semigroup and $h : \mathbf{I}(\mathscr{A}) \to \mathbf{Z}$ a height function then

$$\mathscr{A} \le \overline{\mathscr{H}_1^{\vee}(\mathscr{A})} \circ \overline{\mathscr{H}_2^{\vee}(\mathscr{A})} \circ \ldots \circ \overline{\mathscr{H}_n^{\vee}(\mathscr{A})}$$

where $n = h(\mathscr{A})$.

*Proof* We have already established in example 4.5 the relational covering $\mathscr{A} \lhd_{\alpha_{n-1}} \overline{\mathscr{H}(Q)}$ and recalling that $\mathscr{H}(Q) = \mathscr{H}_n^{\vee}(\mathscr{A})$ we have $\mathscr{A} \lhd_{\alpha_{n-1}} \overline{\mathscr{H}_n^{\vee}(\mathscr{A})}$. The above theorem leads to the relational coverings,

$$\mathscr{A} \lhd_{\alpha_{n-2}} \overline{\mathscr{H}_{n-1}^{\vee}(\mathscr{A})} \circ \overline{\mathscr{H}_n^{\vee}(\mathscr{A})}$$
$$\mathscr{A} \lhd_{\alpha_{n-3}} \overline{\mathscr{H}_{n-2}^{\vee}(\mathscr{A})} \circ \overline{\mathscr{H}_{n-1}^{\vee}(\mathscr{A})} \circ \overline{\mathscr{H}_n^{\vee}(\mathscr{A})}$$
$$\vdots$$
$$\mathscr{A} \lhd_{\alpha_0} \overline{\mathscr{H}_1^{\vee}(\mathscr{A})} \circ \ldots \circ \overline{\mathscr{H}_n^{\vee}(\mathscr{A})},$$

where $\alpha_0$ is of rank 0 and is thus a covering (i.e. a partial function). □

It is sometimes useful to have alternative holonomy decomposition theorems, especially those involving products rather than joins of the holonomy transformation groups.

As before let $A^j_1, \ldots, A^j_{r_j}$ be a set of representatives of the distinct equivalence classes of the elements of the skeleton of height $j$. Define

$$\mathcal{H}_j^\times(\mathcal{A}) = \prod_{k=1}^{r_j} \mathcal{H}(A^j_k)^\cdot,$$

the direct product of the individual holonomy transformation groups. Notice that $\mathcal{H}_j^\times(\mathcal{A})$ is a transformation group. (We need only adjoin an identity to those generalized holonomy transformation groups $\mathcal{H}(A^j_k) = (\mathbf{M}(A^j_k), \mathbf{H}(A^j_k))$ where $\mathbf{H}(A^j_k) = \varnothing$, so that the direct product may be defined in a suitable way.)

*Theorem 4.3.7*

Let $\mathcal{A} \lhd_{\beta_j} \mathcal{B}$ be a relational covering of rank $j$ such that the image of $\beta_j$ is $\pi^j$. There exists a relational covering $\mathcal{A} \lhd_{\beta_{j-1}} \mathcal{H}_j^\times(\mathcal{A}) \circ \mathcal{B}$ such that

(i) the rank of $\beta_{j-1}$ is $j-1$,
(ii) the image of $\beta_{j-1}$ is $\pi^{j-1}$.

*Proof* As before let $\mathcal{A} = (Q, S)$, $\mathcal{B} = (P, T)$ we define $\beta_{j-1} : (\prod_{k=1}^{r_j} \mathbf{M}(A^j_k)) \times P \rightsquigarrow Q$ by

$$\beta_{j-1}((B^j_1, \ldots, B^j_{r_j}), p) = \begin{cases} \beta_j(p) & \text{if } h(\beta_j(p)) < j \\ B^j_k \cdot (\beta_j(p)/A^j_k) & \text{if } \beta_j(p) \equiv A^j_k \end{cases}$$

where $(B^j_1, \ldots, B^j_{r_j}) \in \prod_{k=1}^{r_j} \mathbf{M}(A^j_k)$, $p \in P$.

With respect to this relation we will establish the covering condition

$$\beta_{j-1}((B^j_1, \ldots, B^j_{r_j}), p) \cdot s \subseteq \beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s))$$

where $s \in S$, $t_s \in T$ is such that $\beta_j(p) \cdot s \subseteq \beta_j(p \cdot t_s)$ and $g_s : P \to \prod_{k=1}^{r_j} \mathbf{H}(A^j_k)$ is chosen suitably. The definition of $g_s$ is taken in three cases; let $p \in P$.

Case (i): $\beta_j(p \cdot t_s)$ is of height less than $j$, in which case $g_s(p)$ may be defined arbitrarily.

Case (ii): $\beta_j(p \cdot t_s)$ is of height $j$ and $\beta_j(p) \cdot s \subsetneq \beta_j(p \cdot t_s)$. Now $\beta_j(p \cdot t_s) \equiv A^j_k$ for some $k \in \{1, \ldots, r_j\}$ and so $\beta_j(p) \cdot s \cdot (A^j_k/\beta_j(p \cdot t_s)) \subsetneq \beta_j(p \cdot t_s) \cdot (A^j_k/\beta_j(p \cdot t_s)) = A^j_k$ and thus $\beta_j(p) \cdot s \cdot (A^j_k/\beta_j(p \cdot t_s)) \subseteq B'$ for some $B' \in \mathbf{M}(A^j_k)$. Define $g_s(p)$ to be the transformation that sends the $k$-th coordinate of an element $(B^j_1, \ldots, B^j_{r_j})$ of $\prod_{i=1}^{r_j} \mathbf{M}(A^j_i)$ to $B'$ and is arbitrarily defined on the other coordinates, thus

$$(B^j_1, \ldots, B^j_k, \ldots, B^j_{r_j}) \cdot g_s(p) = (*, \ldots, B', \ldots, *).$$

Case (iii): $\beta_j(p \cdot t_s) = \beta_j(p) \cdot s \equiv A^j_k$ for some $k \in \{1, \ldots, r_j\}$. As before (proof of 4.3.5) the element

$$(\beta_j(p)/A^j_k) \cdot s \cdot (A^j_k/\beta_j(p \cdot t_s))$$



defines an element $h$ of the holonomy group $\mathbf{H}(A^j_k)$. The definition of $g_s(p)$ is then taken to be any element of the semigroup of $\mathcal{H}_j^\times(\mathcal{A})$ that acts like $h$ on the $k$-th coordinate, thus

$$(B^j_1, \ldots, B^j_k, \ldots, B^j_{r_j}) \cdot (g_s(p)) = (*, \ldots, B^j_k \cdot h, \ldots, *).$$

We now show that $(g_s, t_s)$ covers $s$, and to do this let

$$((B^j_1, \ldots, B^j_k, \ldots, B^j_{r_j}), p) \in \left( \prod_{k=1}^{r_j} \mathbf{M}(A^j_k) \right) \times P.$$

In case (i) $\beta_j(p \cdot t_s)$ is of height $j$ and $\beta_{j-1}((B^j_1, \ldots, B^j_{r_j}), p) \cdot s \subseteq \beta_j(p) \cdot s \subseteq \beta_j(p \cdot t_s)$ since $\beta_j$ is a relational covering and $t_s$ covers $s$. Now

$$\begin{aligned} \beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s)) &= \beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}) \cdot g_s, pt_s)) \\ &= \beta_j(p \cdot t_s) \end{aligned}$$

and so

$$\beta_{j-1}((B^j_1, \ldots, B^j_{r_j}), p) \cdot s \subseteq \beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s))$$

in this case.

In case (ii) $\beta_j(p \cdot t_s) \equiv A^j_k$ for some $k \in \{1, \ldots, r_j\}$ and $\beta_j(p) \cdot s \subsetneq \beta_j(p \cdot t_s)$. Then

$$\beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s)) = \beta_{j-1}(((*, \ldots, B', \ldots, *), p \cdot t_s))$$

where

$$B' \in \mathbf{M}(A^j_k) \quad \text{and} \quad \beta_j(p) \cdot s \cdot (A^j_k/\beta_j(p \cdot t_s)) \subseteq B'.$$

Thus

$$\beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s)) = B'(\beta_j(p \cdot t_s)/A^j_k).$$

Now

$$\begin{aligned} \beta_{j-1}((B^j_1, \ldots, B^j_{r_j}), p) \cdot s &\subseteq \beta_j(p) \cdot s \\ &= \beta_j(p) \cdot s \cdot (A^j_k/\alpha_j(p \cdot t_s)) \cdot (\beta_j(p \cdot t_s)/A^j_k) \\ &\subseteq B'(\beta_j(p \cdot t_s)/A^j_k) \\ &= \beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s)). \end{aligned}$$

Finally for case (iii), $\beta_j(p \cdot t_s) \equiv \beta_j(p) \cdot s \equiv A^j_k$ and

$$\begin{aligned} &\beta_{j-1}(((B^j_1, \ldots, B^j_{r_j}), p) \cdot (g_s, t_s)) \\ &\quad = \beta_{j-1}(((*, \ldots, B^j_k \cdot h, \ldots, *), p \cdot t_s)) \\ &\quad = B^j_k \cdot h \cdot (\beta_j(p \cdot t_s)/A^j_k) \\ &\quad = B^j_k(\beta_j(p)/A^j_k) \cdot s \cdot (A^j_k/\beta_j(p \cdot t_s)) \cdot (\beta_j(p \cdot t_s)/A^j_k) \\ &\quad = B^j_k(\beta_j(p)/A^j_k) \cdot s \\ &\quad = \beta_{j-1}((B^j_1, \ldots, B^j_{r_j}), p)) \cdot s. \end{aligned}$$

Therefore, in all cases we have $(g_s, t_s)$ covering $s$. Hence $\beta_{j-1}$ is a relational covering and the rest of the theorem follows in a similar way to theorem 4.3.5 □

*Theorem 4.3.8*

Let $\mathscr{A}$ be a transformation semigroup and $h:\mathbf{I}(\mathscr{A})\to\mathbf{Z}$ a height function, then

$$\mathscr{A}\le\overline{\mathscr{H}_1^\times(\mathscr{A})}\circ\overline{\mathscr{H}_2^\times(\mathscr{A})}\circ\ldots\circ\overline{\mathscr{H}_n^\times(\mathscr{A})}\quad\text{where } n=h(\mathscr{A}).$$

*Theorem 4.3.9*

Let $\mathscr{A}$ be a transformation semigroup and $h:\mathbf{I}(\mathscr{A})\to\mathbf{Z}$ a height function. Suppose that $h(\mathscr{A})=n$ and $\pi^{n-1}$ is the first non-trivial element of the derived sequence of $\mathscr{A}$. Then

(i) $\mathscr{A}\le\overline{\mathscr{H}_1^\vee(\mathscr{A})}\circ\ldots\circ\overline{\mathscr{H}_{n-1}^\vee(\mathscr{A})}\circ\mathscr{A}/\langle\pi^{n-1}\rangle$

(ii) $\mathscr{A}\le\overline{\mathscr{H}_1^\times(\mathscr{A})}\circ\ldots\circ\overline{\mathscr{H}_{n-1}^\times(\mathscr{A})}\circ\mathscr{A}/\langle\pi^{n-1}\rangle$

where $\mathscr{A}/\langle\pi^{n-1}\rangle$ is a suitably chosen quotient transformation semigroup.

*Proof* In the discussion of example 4.5 we defined a quotient transformation semigroup $\mathscr{A}/\langle\pi\rangle$. In the context of this section $\pi$ is denoted by $\pi^{n-1}$ and so the result follows from the fact that $\mathscr{A}/\langle\pi^{n-1}\rangle$ yields a relational covering of $\mathscr{A}$ of rank $n-1$. □

Theorems 4.3.5 and 4.3.7 are known as the *holonomy reduction theorems* and theorems 4.3.6 and 4.3.8 as the *holonomy decomposition theorems.*

It is possible to use theorem 4.3.6 to deduce another decomposition theorem. First let $\mathscr{H}_j^+(\mathscr{A})=\mathscr{H}(A_1^j)+\ldots+\mathscr{H}(A_{r_j}^j)$, where $A_1^j,\ldots,A_{r_j}^j$ are representatives of the skeletal elements of height $j$ with respect to some height function on the transformation semigroup $\mathscr{A}$. We have that $\mathscr{H}_j^\vee(\mathscr{A})\le\mathscr{H}_j^+(\mathscr{A})$ and so we may establish:

*Theorem 4.3.10*

Let $\mathscr{A}$ be a transformation semigroup and $h:\mathbf{I}(\mathscr{A})\to\mathbf{Z}$ a height function. Then

$$\mathscr{A}\le\overline{\mathscr{H}_1^+(\mathscr{A})}\circ\overline{\mathscr{H}_2^+(\mathscr{A})}\circ\ldots\circ\overline{\mathscr{H}_n^+(\mathscr{A})}$$

where $n$ is the height of $\mathscr{A}$.

We will examine some examples later, but for the moment there are some remarks that are worth making. First of all this decomposition is



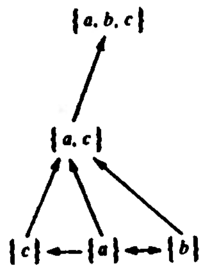
a considerable improvement on the original decomposition theorem for transformation semigroups obtained by Krohn and Rhodes [1965]. The increase in efficiency is easily demonstrated by examining some of their examples. Notice that the groups involved in the holonomy transformation semigroups are immediately seen to be divisors of the semigroup $S$. However, Eilenberg noted that it was still possible to obtain even better decompositions than those given by the holonomy decomposition theorem and it is this aspect of the theory that we turn to next. Although the proof of the holonomy decomposition theorem given here is the same as Eilenberg's we have stressed the admissible subset systems and the derived sequence. The reason for this will become apparent in the next section where we introduce an 'improved' holonomy decomposition theorem, which in many cases gives a more efficient decomposition than the standard holonomy decomposition theorem.

## 4.4 An 'improved' holonomy decomposition and examples

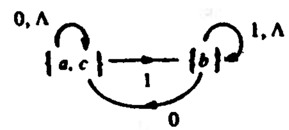
We begin with an example to motivate the discussion.

*Example 4.6*

If we recall example 4.1 we note that the transformation monoid $\mathscr{A}$ has the following skeleton:




There is a unique height function, $h(Q)=2$, $h(\{a,c\})=1$, $h(\{a\})=h(\{b\})=h(\{c\})=0$, $h(\varnothing)=-1$. The first derived admissible subset system $\pi'$ consists of the two sets $\{a,c\}$, $\{b\}$. Then $\mathscr{A}/\langle\pi'\rangle$ is given by




and so $\mathscr{A}/\langle\pi'\rangle\cong\bar{\mathbf{2}}$. Also $\mathscr{H}_2^\vee(\mathscr{A})=\mathscr{H}_2^\times(\mathscr{A})\cong(\pi',\{\Lambda\})$ and $\overline{\mathscr{H}_2^\vee(\mathscr{A})}\cong\bar{\mathbf{2}}$.

The derived system $\pi^0 = \{\{a\}, \{b\}, \{c\}\}$.

$$\mathcal{H}_1^{\vee}(\mathcal{A}) = \mathcal{H}_1^{\times}(\mathcal{A}) \cong (\mathbf{M}(\{a, c\}), \{\Lambda\})$$
$$\cong \mathbf{2}^{\cdot}.$$

Then the holonomy decomposition theorem yields

$$\mathcal{A} \le \bar{\mathbf{2}}^{\cdot} \circ \bar{\mathbf{2}}^{\cdot}.$$

Notice, however, that $\pi'$ is an *orthogonal* admissible partition, since $\pi \cap \tau = 1$ where $\tau = \{\{a, b\}, \{c\}\}$ and $\tau$ is an admissible partition. Then by theorem 3.2.1

$$\mathcal{A} \le \mathcal{A}/\langle\tau\rangle \times \mathcal{A}/\langle\pi'\rangle = \mathcal{A}/\langle\tau\rangle \times \bar{\mathbf{2}}^{\cdot}.$$

We may check that $\mathcal{A}/\langle\tau\rangle = \mathscr{C}^{\cdot}$ and thus $\mathcal{A} \le \mathscr{C}^{\cdot} \times \bar{\mathbf{2}}^{\cdot}$, which is better than $\mathcal{A} \le \bar{\mathbf{2}}^{\cdot} \circ \bar{\mathbf{2}}^{\cdot}$ for two reasons. Firstly $\mathscr{C}^{\cdot} \le \bar{\mathbf{2}}^{\cdot}$ and secondly direct products are much more efficient than wreath products. (Actually if we examine the proof of theorem 4.3.5 it becomes clear that the wreath product in this example may be replaced by the direct product since the definition of $f$ given by the theorem yields an identity in this example.)

The behaviour of this example gives us a method of approaching the problem of improving the holonomy decomposition theorem. If $\mathcal{A} = (Q, S)$ is an arbitrary transformation semigroup and $h: \mathbf{I}(\mathcal{A}) \to \mathbf{Z}$ is a given height function we may define the derived sequence $\pi^n > \pi^{n-1} > \ldots > \{1\}$ of admissible subset systems. Suppose that $\pi^p$ is the largest orthogonal admissible partition in the sequence that is non-trivial. Naturally such a $\pi^p$ may not exist and if this is the case the following theory will not lead to an improved decomposition. However in many cases there is such a $\pi^p$. Now let $\tau$ be an orthogonal admissible partition such that $\tau \cap \pi^p = \{1\}$. From theorem 3.2.1 we deduce that $\mathcal{A} \le \mathcal{A}/\langle\tau\rangle \times \mathcal{A}/\langle\pi^p\rangle$ and from theorems 4.1.1 and 4.3.5

$$\mathcal{A}/\langle\pi^p\rangle \le \overline{\mathcal{H}_{p+1}^{\vee}(\mathcal{A})} \circ \overline{\mathcal{H}_{p+2}^{\vee}(\mathcal{A})} \circ \ldots \circ \overline{\mathcal{H}_n^{\vee}(\mathcal{A})}$$

where $p$ is the rank of $\pi^p$ and $n = h(\mathcal{A})$. Therefore

$$\mathcal{A} \le \mathcal{A}/\langle\tau\rangle \times (\overline{\mathcal{H}_{p+1}^{\vee}(\mathcal{A})} \circ (\overline{\mathcal{H}_{p+2}^{\vee}(\mathcal{A})} \circ \ldots \circ \overline{\mathcal{H}_n^{\vee}(\mathcal{A})}).$$

We can now apply the holonomy decomposition theorem to the transformation semigroup $\mathcal{A}/\langle\tau\rangle$ and continue the process. So we choose a height function for $\mathcal{A}/\langle\tau\rangle$, look at its derived sequence and see if a largest non-trivial orthogonal admissible partition lies in this sequence. If one exists we repeat the above process, using theorems 3.2.1 and 4.3.5 to

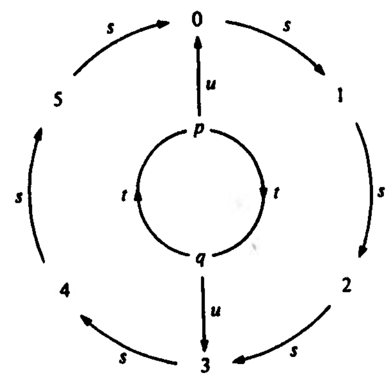


obtain an 'improved' decomposition of $\mathcal{A}/\langle\tau\rangle$. This procedure is repeated as many times as is necessary to obtain a complete decomposition of $\mathcal{A}$. That this decomposition of $\mathcal{A}$ is better than the holonomy decomposition may be established, but the details are rather complex.

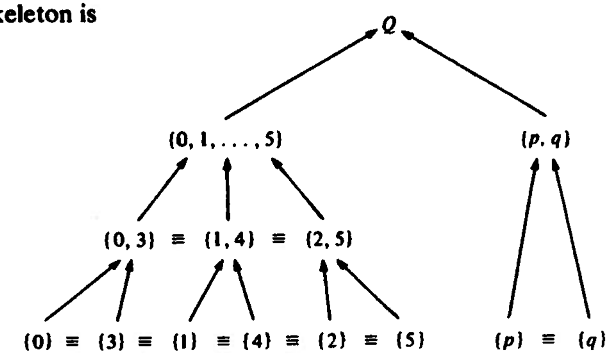
Suppose that $\mathcal{A} = (Q, S)$ is a transformation semigroup with $h: \mathbf{I}(\mathcal{A}) \to \mathbf{Z}$ a height function. Let $\pi^n > \pi^{n-1} > \ldots > \{1\}$ be the derived sequence and suppose that $\pi^p$ $(0 < p < n)$ is an orthogonal admissible partition. Let $\pi^p \cap \tau = \{1\}$ and write $\mathcal{A}/\langle\tau\rangle = \mathcal{B}$. There is a natural epimorphism $(f, g)$: $\mathcal{A} \to \mathcal{B}$ defined as follows. Let $T = S/\sim$ be the semigroup of $\mathcal{B}$, then each $t \in T$ corresponds to a set of elements from $S$. The function $g$ will send an element $s \in S$ to the equivalence class it belongs to, and this is an element of $T$. Similarly $f$ will send an element of $Q$ to the $\tau$-class it belongs to and the result is a homomorphism of $\mathcal{A}$ onto $\mathcal{B}$. In many cases the homomorphism $(f, g)$ allows us to transfer information about the transformation semigroup $\mathcal{A}$ to the transformation semigroup $\mathcal{B}$ although it is not always a straightforward procedure. For example the skeleton $\mathbf{I}(\mathcal{B})$ can be constructed using $\mathbf{I}(\mathcal{A})$ and $(f, g)$. Similarly a derived sequence may be induced on $\mathcal{B}$ from $\mathcal{A}$, but it is no longer so well behaved and this complicates matters. Similarly a height function on $\mathcal{A}$ may be used in some cases to define a height function on $\mathcal{B}$ but many difficulties arise in this theory. Some of these questions are examined in the exercises at the end of this chapter. We can now look at some examples.

*Example 4.7*

Let $\mathcal{A} = (Q, S)$ be the transformation semigroup defined by the following graph:



The skeleton is




(with $\varnothing$ omitted).

If we choose the minimal height function then $h(Q)=3$ and

$$\pi^2=\{\{0,1,\dots,5\},\{p,q\}\},\ \pi^1=\{\{0,3\},\{1,4\},\{2,5\},\{p\},\{q\}\}.$$

The holonomy decomposition is

$$\mathscr{A}\le\overline{\mathscr{H}(\{0,3\})}\circ\overline{\mathscr{H}(\{0,1,\dots,5\})\vee\mathscr{H}(\{p,q\})}\circ\overline{\mathscr{H}(Q)}.$$

Now

$$\mathscr{H}(Q)=(\{\{0,1,\dots,5\},\{p,q\}\},\varnothing)\cong\mathbf{2}$$

$$\mathscr{H}(\{0,1,\dots,5\})=(\{\{0,3\},\{1,4\},\{2,5\}\},\{s,s^2,s^3\})\cong\mathbf{Z}_3$$

$$\mathscr{H}(\{p,q\})=(\{\{p\},\{q\}\},\{t,t^2\})\cong\mathbf{Z}_2$$

$$\mathscr{H}(\{0,3\})=(\{\{0\},\{3\}\},\{s^3,s^6\})\cong\mathbf{Z}_2$$

and so

$$\mathscr{A}\le\bar{\mathbf{Z}}_2\circ(\overline{\mathbf{Z}_2\vee\mathbf{Z}_3})\circ\bar{\mathbf{2}}.$$

Now notice, however, that $\pi^2$ is a partition and if $\tau=\{\{0,p\},\{3,q\},\{1\},\{2\},\{4\},\{5\}\}$ then $\tau$ is an admissible partition and $\tau\cap\pi^2=\{1\}$. Hence we may deduce that

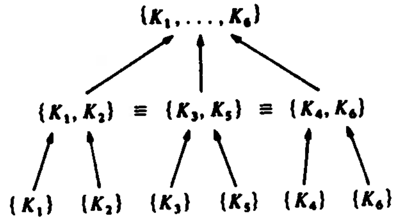
$$\mathscr{A}\le\mathscr{A}/\langle\tau\rangle\times\mathscr{A}/\langle\pi^2\rangle\le\mathscr{A}/\langle\tau\rangle\times\bar{\mathbf{2}}.$$

Now we consider the skeleton of $\mathscr{A}/\langle\tau\rangle$. For convenience we will put $K_1=\{0,p\}, K_2=\{3,q\}, K_3=\{1\}, K_4=\{2\}, K_5=\{4\}, K_6=\{5\}$ and the state table for $\mathscr{A}/\langle\tau\rangle$ is:

| | $s$ | $t$ | $u$ |
|---|---|---|---|
| $K_1$ | $K_3$ | $K_2$ | $K_1$ |
| $K_2$ | $K_5$ | $K_1$ | $K_2$ |
| $K_3$ | $K_4$ | $\varnothing$ | $\varnothing$ |
| $K_4$ | $K_2$ | $\varnothing$ | $\varnothing$ |
| $K_5$ | $K_6$ | $\varnothing$ | $\varnothing$ |
| $K_6$ | $K_1$ | $\varnothing$ | $\varnothing$ |



The skeleton is:




The first derived admissible subset system is:

$$\rho^1=\{\{K_1,K_2\},\{K_3,K_5\},\{K_4,K_6\}\},$$

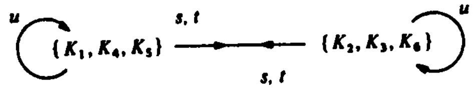
since there is only one height function available and that yields $h(\mathscr{A}/\langle\tau\rangle)=2$. Now $\rho^1$ is an orthogonal partition since the partition $\xi=\{\{K_1,K_4,K_5\},\{K_2,K_3,K_6\}\}$ is admissible and $\xi\cap\rho'=\{1\}$. Therefore

$$\mathscr{A}/\langle\tau\rangle\le(\mathscr{A}/\langle\tau\rangle)/\langle\xi\rangle\times(\mathscr{A}/\langle\tau\rangle)/\langle\rho'\rangle$$

and

$$(\mathscr{A}/\langle\tau\rangle)/\langle\rho'\rangle\le\overline{\mathscr{H}_2^{\vee}(\mathscr{A}/\langle\tau\rangle)}\cong\overline{(\rho',\{s,s^2,s^3\})}$$
$$\cong\bar{\mathbf{Z}}_3.$$

Also, $(\mathscr{A}/\langle\tau\rangle)/\langle\xi\rangle$ is




and so $(\mathscr{A}/\langle\tau\rangle)/\langle\xi\rangle\le\bar{\mathbf{Z}}_2$.

Hence $\mathscr{A}/\langle\tau\rangle\le\bar{\mathbf{Z}}_2\times\bar{\mathbf{Z}}_3$ and $\mathscr{A}\le\bar{\mathbf{Z}}_2\times\bar{\mathbf{Z}}_3\times\bar{\mathbf{2}}$.

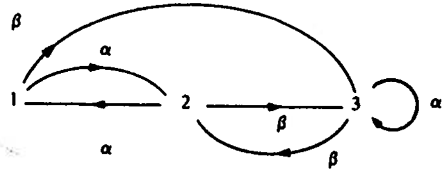
Decomposing $\mathscr{A}$ with respect to another height function does not really alter things much although the basic holonomy decomposition will not be the same. For example, let $h_1:\mathbf{I}(\mathscr{A})\to\mathbf{Z}$ be defined by $h_1(Q)=4$, $h_1(\{0,1,\dots,5\})=3$, $h_1(\{p,q\})=2$, $h_1(\{0,3\})=1$ etc. giving us $\mathscr{A}\le\bar{\mathbf{Z}}_2\circ\bar{\mathbf{Z}}_2\circ\bar{\mathbf{Z}}_3\circ\bar{\mathbf{2}}$ for the basic decomposition, but our improved decomposition is $\mathscr{A}\le\bar{\mathbf{Z}}_2\times\bar{\mathbf{Z}}_3\times\bar{\mathbf{2}}$ since we have not changed $\tau$ when changing the height function. Theorem 3.4.3 enables us to replace each transformation group of the form $(\mathbf{M}(A),\mathbf{H}(A))$ by the wreath product $(\mathbf{M}(A),\varnothing)^{\cdot}\circ(\mathbf{H}(A),\mathbf{H}(A))$ and so we have $\mathscr{A}\le(\bar{\mathbf{2}}^{\cdot}\circ\mathbf{Z}_2)\times(\bar{\mathbf{3}}^{\cdot}\circ\mathbf{Z}_3)\times\bar{\mathbf{2}}$. Now apply the identity $(\mathscr{A}\circ\mathscr{B})\times(\mathscr{C}\circ\mathscr{D})\le(\mathscr{A}\times\mathscr{C})\circ(\mathscr{B}\times\mathscr{D})$ to obtain

$$\mathscr{A}\le[(\bar{\mathbf{2}}^{\cdot}\times\bar{\mathbf{3}}^{\cdot})\circ(\mathbf{Z}_2\times\mathbf{Z}_3)]\times\bar{\mathbf{2}}$$
$$=[(\bar{\mathbf{2}}^{\cdot}\times\bar{\mathbf{3}}^{\cdot})\circ(\mathbf{Z}_2\times\mathbf{Z}_3)]\times(\bar{\mathbf{2}}\circ\mathbf{1}^{\cdot})$$
$$\le(\bar{\mathbf{2}}^{\cdot}\times\bar{\mathbf{3}}^{\cdot}\times\bar{\mathbf{2}})\circ(\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{1}^{\cdot})$$
$$=(\bar{\mathbf{2}}^{\cdot}\times\bar{\mathbf{3}}^{\cdot}\times\bar{\mathbf{2}})\circ\mathbf{Z}_6.$$

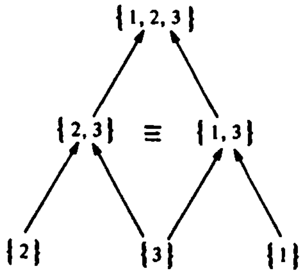
This decomposition is in the form of a wreath product $\mathscr{A}\circ\mathscr{G}$ where $\mathscr{A}$ is aperiodic and $\mathscr{G}$ is a transformation group. Thus $\mathbf{C}(\mathscr{A})\leq 1$.

*Example 4.8*

Consider the transformation semigroup $\mathscr{A}=(Q,S)$ where $Q=\{1,2,3\}$, $S=\{\alpha,\beta,\alpha^2,\beta^2,\beta\alpha,\beta^2\alpha\}$ and with generating graph:




The skeleton is:




and so the height is 2. Then $\pi'=\{\{2,3\},\{1,3\}\}$ which is not a partition and so the basic holonomy decomposition theorem must be used.

$$\mathscr{H}_n^{\vee}(\mathscr{A})=\mathscr{H}(Q)=(\{\{2,3\},\{1,3\}\},\{\alpha,\alpha^2\})\cong\mathbf{Z}_2,$$

$$\mathscr{H}(\{2,3\})=(\{\{2\},\{3\}\},\{\beta,\beta^2\})=\mathbf{Z}_2=\mathscr{H}_1^{\vee}(\mathscr{A}).$$

Thus $\mathscr{A}\leq\bar{\mathbf{Z}}_2\circ\bar{\mathbf{Z}}_2$.

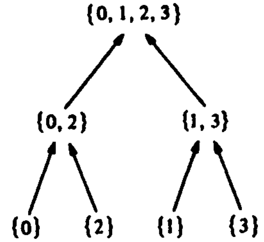
*Example 4.9*

Let $\mathscr{A}=(Q,S)$ where $Q=\{0,1,2,3\}$, $S=\{a,b,c,d\}$ given by the table:

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $a$ | 0 | 2 | 0 | 2 |
| $b$ | 2 | 0 | 2 | 0 |
| $c$ | 1 | 3 | 1 | 3 |
| $d$ | 3 | 1 | 3 | 1 |



The skeleton is:




and so $h(Q)=2$. Then $\pi'=\{\{0,2\},\{1,3\}\}$ which is a partition but is not orthogonal. Therefore we apply the basic holonomy decomposition theorem.

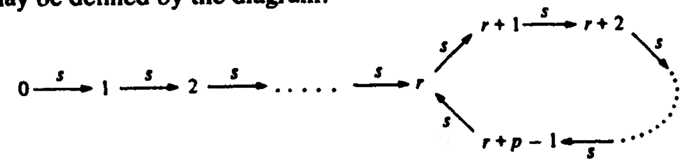
$$\mathscr{H}_2(\mathscr{A})=\mathscr{H}(Q)=(\{\{0,2\},\{1,3\}\},\varnothing)\cong\mathbf{2}$$

$\mathscr{H}(\{0,2\})=(\{\{0\},\{2\}\},\varnothing)=\mathbf{2}=\mathscr{H}(\{1,3\})$ and so $\mathscr{H}_1^{\vee}(\mathscr{A})=\mathbf{2}\vee\mathbf{2}$ and

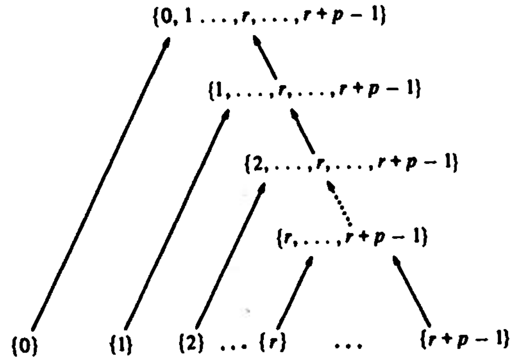
$$\mathscr{A}\leq(\overline{\mathbf{2}\vee\mathbf{2}})\circ\bar{\mathbf{2}}.$$

*Example 4.10*

We now consider the cyclic transformation semigroup $\mathscr{C}_{(p,r)}$. This may be defined by the diagram:




The skeleton is:




The height of the transformation semigroup is $r+1$ if $p>1$, and is $r$ if $p=1$. The derived sequence when $p>1$ is easily calculated from the skeleton and the one of particular interest is $\pi^1=\{\{0\},\{1\},\ldots,\{r-1\},\{r,\ldots,r+p-1\}\}$. This is an orthogonal partition. To see this suppose that $r>p$ and $r=qp+t$ where $0\le t<p$, and put

$$\begin{aligned}\tau=\{&\{0,p,\ldots,(q+1)p\},\{1,p+1,\ldots,(q+1)p+1\},\ldots,\\&\{t-1,p+t-1,\ldots,r+p-1\},\{t,p+t,\ldots,r\},\\&\{t+1,p+t+1,\ldots,qp+t+1\},\ldots,\\&\{p-1,2p-1,\ldots,(q+1)p-1\}\}.\end{aligned}$$

Then $\pi^1\cap\tau=\{1\}$ and $\tau$ is admissible. Then

$$\mathscr{C}_{(p,r)}\le\mathscr{A}/\langle\tau\rangle\times\mathscr{A}/\langle\pi^1\rangle.$$

Clearly $\mathscr{A}/\langle\tau\rangle\cong\mathbf{Z}_p$ and $\mathscr{A}/\langle\pi'\rangle=\mathscr{C}_{(1,r)}$ and so $\mathscr{C}_{(p,r)}\le\mathbf{Z}_p\times\mathscr{C}_{(1,r)}$.

If $r=p$ put $\tau=\{\{0,r\},\{1,r+1\},\ldots,\{r-1,2r-1\}\}$ then $\pi^1\cap\tau=\{1\}$ and $\tau$ is admissible. In this case

$$\mathscr{C}_{(p,r)}\le\mathbf{Z}_r\times\mathscr{C}_{(1,r)}$$

as before.

Finally let $r<p$ and choose $\tau=\{\{r\},\{r+1\},\ldots,\{p-1\},\{0,p\},\{1,p+1\}\ldots\{r-1,r+p-1\}\}$.

As before $\pi^1\cap\tau=\{1\}$ and $\tau$ is admissible, hence $\mathscr{A}\le\mathbf{Z}_p\times\mathscr{C}_{(1,r)}$.

In all cases the partition $\tau$ is defined by the relation

$$q\sim q'\Leftrightarrow q'\equiv q(\mathrm{mod}\ p),\quad q,q'\in Q.$$

Then for any $r\ge1$, the basic holonomy theorem yields

$$\mathscr{C}_{(1,r)}\le\bar{\bar{2}}^{r-1}\circ\mathscr{C}.$$

(The $\mathscr{C}$ arises if we replace the holonomy group $\mathscr{H}_r(\mathscr{C}_{(1,r)})$ by the quotient of the first element of the derived sequence – we use theorem 4.3.9(i).) Finally we obtain $\mathscr{C}_{(p,r)}\le\mathbf{Z}_p\times(\bar{\bar{2}}^{r-1}\circ\mathscr{C})$.

Contrast this result with the basic holonomy covering $\mathscr{C}_{(p,r)}\le\bar{\bar{\mathbf{Z}}}_p\circ\bar{\bar{2}}^r$, which is clearly very inferior.

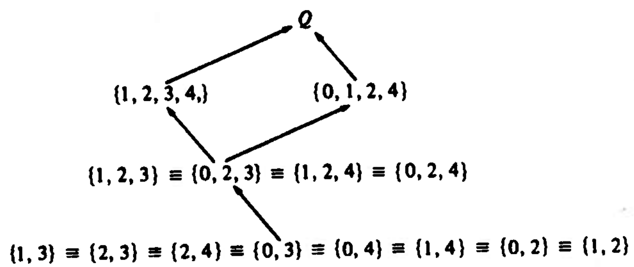
*Example 4.11*

This transformation semigroup arises from the study of the tricarboxylic acid (or Krebs) cycle in biochemistry. Let $Q=\{0,1,2,3,4\}$, and let $\mathscr{A}=(Q,S)$ be the transformation semigroup generated by the table:

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a$ | 1 | 1 | 2 | 3 | 4 |
| $b$ | 0 | 2 | 3 | 3 | 0 |
| $c$ | 0 | 1 | 2 | 4 | 4 |



The transformation semigroup is irreducible and so we must apply the basic holonomy decomposition. The skeleton is:




where the singletons and $\varnothing$ are omitted and also some of the lines indicating the $\leqslant$ relation are left out for clarity. The minimal height function $h$ yields $h(Q)=4$. The derived sequence is

$$\begin{aligned}\pi^3&=\{\{1,2,3,4\},\{0,1,2,4\},\{0,2,3\}\}\\\pi^2&=\{\{1,2,3\},\{1,2,4\},\{0,2,3\},\{1,2,4\},\{0,2,4\}\}\\\pi^1&=\{\{1,3\},\{2,3\},\{1,2\},\{0,3\},\{2,4\},\{1,4\},\{0,4\},\{0,2\}\}.\end{aligned}$$

Now $\mathscr{A}/\langle\pi^3\rangle\cong\bar{\bar{3}}$, and the holonomy groups are given by:

$$\mathscr{H}_3^{\vee}(\mathscr{A})=\mathscr{H}(\{1,2,3,4\})\vee\mathscr{H}(\{0,1,2,4\})\cong\mathbf{2}^{\cdot}\vee\mathbf{2}^{\cdot},$$
$$\mathscr{H}_2^{\vee}(\mathscr{A})\cong\mathscr{H}(\{0,2,3\})\cong\mathbf{Z}_3,\ \mathscr{H}_1^{\vee}(\mathscr{A})\cong\mathscr{H}(\{0,3\})\cong\mathbf{Z}_2$$

and so

$$\mathscr{A}\le\bar{\bar{\mathbf{Z}}}_2\circ\bar{\bar{\mathbf{Z}}}_3\circ(\bar{\bar{2}}^{\cdot}\vee\bar{\bar{2}}^{\cdot})\circ\bar{\bar{3}}.$$

Does this decomposition have a biochemical interpretation?

### 4.5 The Krohn–Rhodes decomposition

The first major result in the algebraic decomposition theory of transformation semigroups was due to Krohn and Rhodes and appeared in 1965. Since then many versions of this result have appeared. Some are set in the context of state machines, some in the context of Mealy machines and of course some occur in treatments of the theory of transformation semigroups. We will state the most relevant form of the theorem here.

*Theorem 4.5.1* (Krohn–Rhodes decomposition theorem)

Let $\mathscr{A}=(Q,S)$ be a transformation semigroup. Then $\mathscr{A}$ may be covered by a finite wreath product of transformation semigroups of the following two types:

(i) aperiodic transformation semigroups,

(ii) transformation groups $(G, G)$ where $G$ is a finite simple group and $G|S$.

*Proof* Choose a maximal height function $h:\mathrm{I}(\mathscr{A}) \to \mathbf{Z}$ for $\mathscr{A}$. We first suppose that $S \neq \varnothing$. Now $\mathscr{H}_i^{\vee}(\mathscr{A}) = \mathscr{H}(A)$ for some $A \in \mathrm{I}(\mathscr{A})$. By the basic holonomy theorem (4.3.7)

$$\mathscr{A} \le \overline{\mathscr{H}_1^{\vee}(\mathscr{A})} \circ \overline{\mathscr{H}_2^{\vee}(\mathscr{A})} \circ \ldots \circ \overline{\mathscr{H}_n^{\vee}(\mathscr{A})}$$

where $n = h(Q)$. Applying theorem 3.4.3 to each component $\overline{\mathscr{H}_i^{\vee}(\mathscr{A})}$ yields

$$\overline{\mathscr{H}_i^{\vee}(\mathscr{A})} \le \overline{(P_i, \varnothing)}^{\cdot} \circ \mathscr{H}_i$$

where $\mathscr{H}_i^{\vee}(\mathscr{A}) = (P_i, H_i)$, $P_i$ is the maximal image space of the element of height $i$ in the skeleton and $H_i$ is the holonomy group of this element. We now apply example 3.3 to get $\overline{(P_i, \varnothing)}^{\cdot} \le \prod^k \bar{\mathbf{2}}^{\cdot}$ where $|P_i| \le 2^k$ and theorem 3.5.4 to get $\mathscr{H}_i \le \mathscr{G}_{i1} \circ \ldots \circ \mathscr{G}_{im}$ where each $G_{ij}$ is a finite simple group, $j = 1, \ldots, m$ and $G_{ij} | H_i$. Finally note that $H_i | S$ by the construction of the holonomy groups.

In the case where $S = \varnothing$ then $\mathscr{A} = (Q, \varnothing) \le \prod^k \bar{\mathbf{2}}^{\cdot}$ by example 3.3. □

The corresponding theorem for state machines says that any state machine may be covered by direct and cascade products involving two-state reset machines and simple grouplike state machines whose groups are covered by the semigroup of the original machine. Proofs of theorems of this type were developed by Zeiger and then Ginzburg (see Ginzburg [1968].) Their approach was briefly sketched in the opening paragraphs of this chapter, but it has the serious disadvantage of leading to a very inefficient and lengthy decomposition process. For example, their original method would require the use of a computer to obtain a decomposition of the example 4.11.

The development of the holonomy decomposition theorem was achieved by Eilenberg [1976]. His original definition of a height function contained a small inadequacy (condition (iii)). This failing was indicated to me by T. Keville [1978]. The approach we take here, using the derived sequence, is not very far removed from Eilenberg's own treatment. The advantage of our method occurs in the 'improvement' of the holonomy decomposition in section 4.4.

The applications of this theory are likely to prove important in all those areas where automata theory can be used to model discrete systems. We have already noted how an important metabolic pathway can be compared with some simple cyclic groups and aperiodic transformation semigroups. There are many other examples, in the biological and psychological sciences, and also in computer science and engineering.



All the results of this chapter may be applied to 'pure' semigroup theory also. Recall that if $S$ is any semigroup then $(S^{\cdot}, S)$ is a transformation semigroup, and so the decomposition theory may be applied to $(S^{\cdot}, S)$. However, it is often possible to obtain better results, in this situation, by using the internal structure and techniques available in semigroup theory. In particular, the skeleton is essentially just the collection of principal left ideals of $S$ with the appropriate relation. Since there are many other algebraic structures in a semigroup, we may as well make use of them. Of particular note is the depth decomposition theorem for semigroups due to Tilson. (See Eilenberg [1976].) This often leads to a shorter decomposition of a semigroup compared to the basic holonomy decomposition applied to the semigroup.

### 4.6 Exercises

4.1 Prove that the minimal height function defined in section 4.2 satisfies all the requirements of the definition of a height function.

4.2 Calculate the skeleton and the height function for the transformation semigroup $(Q, S)$ represented by:

| | 1 | 2 | 3 |
|---|---|---|---|
| $a$ | 1 | 1 | 1 |
| $b$ | 1 | 2 | 3 |

where $Q = \{1, 2, 3\}$, $S = \{a, b\}$.

4.3 Construct the skeleton and the derived sequence for the transformation semigroup $\bar{\mathbf{2}}^{\cdot} \vee \bar{\mathbf{2}}^{\cdot}$. Show that $\pi^1$ is orthogonal and hence establish that $\bar{\mathbf{2}}^{\cdot} \vee \bar{\mathbf{2}}^{\cdot} \le \bar{\mathbf{2}}^{\cdot} \times \mathbf{2}^{\cdot}$.

4.4 Decompose example 4.4 and hence show that this transformation semigroup may be covered by a wreath product of aperiodic transformation semigroups and symmetric permutation groups.

4.5 Let $\mathscr{A} = (Q, S)$ be a state machine. Show that $\mathrm{I}(\mathscr{A}) = \mathrm{I}(\mathscr{A}^{\cdot}) = \mathrm{I}(\bar{\mathscr{A}})$ and $\mathrm{I}(\mathscr{A}^{c}) = \{B \cup \{z\} \mid B \in \mathrm{I}(\mathscr{A})\}$. If $A \in \mathrm{I}(\mathscr{A})$ show that the holonomy transformation group of $A$ regarded as an image of $\mathscr{A}^{\cdot}$ equals $\mathscr{H}(\mathscr{A})^{\cdot}$ and the holonomy transformation group of $\mathscr{A}$ regarded as an image