ADVANCES IN APPLIED MATHEMATICS **19,** 251–281 (1997)
ARTICLE NO. AM970547

On Calculating the Krohn–Rhodes Decomposition of Automata

Sunil Talwar

ELSE (UCL), Gower Street, London WC1E 6BT, United Kingdom

Received December 3, 1996; accepted December 30, 1996

DEDICATED TO M.-P. SCHÜTZENBERGER

The Krohn–Rhodes prime decomposition theorem determines the *building blocks* and their combination so as to *mimic* any given automaton. This result leads to an intuitively appealing, integer valued measure of the complexity of an automaton. It is a long-standing open question as to whether complexity is *decidable*. In this article, we show that complexity 1 is decidable. We exhibit an application to *game theory*.

1. INTRODUCTION

The celebrated Krohn–Rhodes prime decomposition theorem (1965) states:

> Each finite-state automaton can be simulated by a series parallel connection of two state reset automata and simple group automata. Moreover, no smaller set of components will suffice.

An automaton M is a tuple $(A, B, Q, q^1, \lambda, \mu)$, where $A = \{\alpha_1, \dots, a_n\}$ is the input alphabet, $B = \{b_1, \dots, b_m\}$ is the output alphabet, Q is a finite set of states, $q^1 \in Q$ is the initial state, λ: $Q \to B$ is the output function, and μ: $Q \times A \to Q$ is the transition function. An automaton M_1 is said to simulate an automaton M_2 ($M_2 \prec M_1$) if M_1 produces the same output as M_2 on the same sequence of inputs. An automaton is said to be a group automaton if each input induces a permutation of states. The two state reset automaton is simply an on–off switch, with the addition of the identity transformation (see Fig. 1). By series and parallel we mean the usual as in Fig. 2. The proof of Krohn and Rhodes [14] is algorithmic. A

0196-8858/97 $25.00

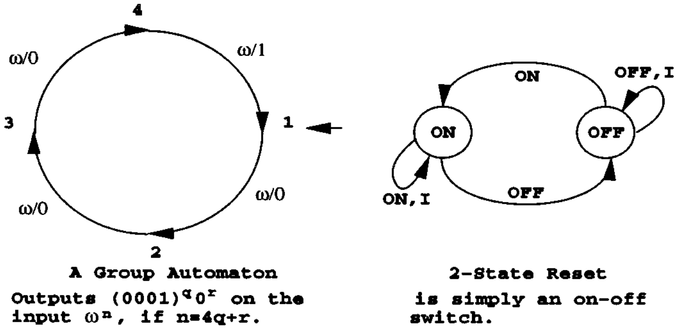


FIG. 1.

simple application of this algorithm to Tweedledee (nice) [3] in Fig. 3 yields the (series) decomposition in Fig. 4. Krohn and Rhodes pose the question of minimality [15], which is best addressed by Zeiger's proof of Krohn and Rhodes [30]. Zeiger discovered that the composition of automata in series and parallel could be subsumed in the portmanteau way of combining automata shown in Fig. 5.

THEOREM 1 (Zeiger [30]). *Each finite state automaton can be simulated by a cascade of two state reset automata and simple group automata. Moreover, no smaller set of components will suffice.*

It turns out that a cascade of group automata yields a group automaton. On gathering together all adjacent group automata to form one group automaton, we can state:

THEOREM 2. *Each automaton can be simulated by an alternating cascade of group automata and blocks of reset automata.*

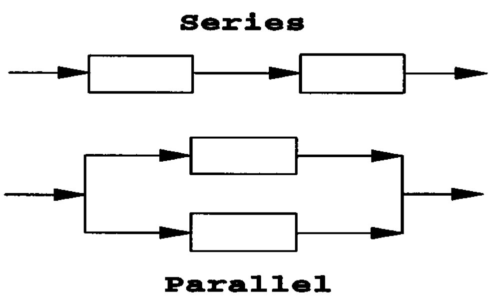


FIG. 2.

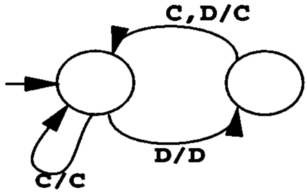


FIG. 3.

Such a simulation is denoted by

$$M \prec A \ltimes G_1 \ltimes A \ltimes G_2 \ltimes \cdots \ltimes A \ltimes G_n \ltimes A,$$

where A denotes some block of reset automata and G_i denote group automata. For the sake of consistency with Figure 5, such a simulation should be read from right to left.

The (group) complexity of an alternating cascade simulation is defined as the number of group automata, in that simulation and the complexity $M\mathbf{c}$ of an automaton M are defined as the minimum over all alternating cascade simulations of the complexity of the simulation.

Decomposition of automata can also be expressed algebraically. The transition function of M determines the elementary functions $qf_{a_i} = \mu(q, a_i)$, $q \in Q$, $i = 1, \ldots, n$. These in turn generate (under composition of functions) the (finite) transition semigroup

$$T(M) = \langle f_{a_1}, \ldots, f_{a_n} \rangle.$$

We shall assume everything in sight to be finite. Elements of $T(M)$ act naturally on the right of the set Q by evaluation. That is,

$$(qf)g = q(fg), \qquad q \in Q, f, g \in T(M).$$

The pair $(Q, T(M))$ is called the transformation semigroup of the automaton M. The algebraic proof [9] of Krohn and Rhodes "decomposes"

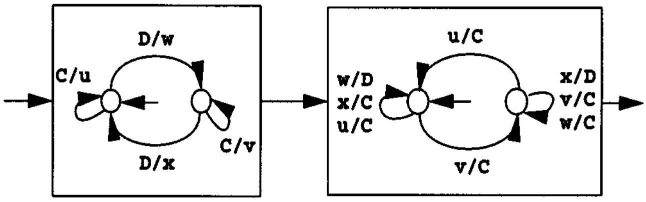
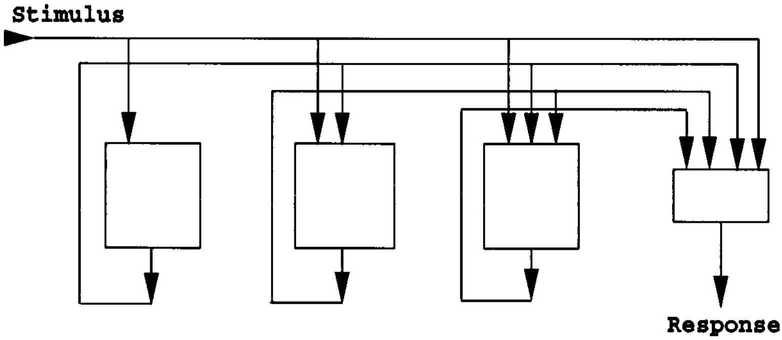


FIG. 4.



Cascade Combination of three machines

FIG. 5.

$(Q, T(M))$. There is a natural concept of simulation for transformation semigroups.

DEFINITION 1. A transformation semigroup (Q', T') is said to simulate another (Q, T) if there exists a subset $P \subseteq Q'$ and a surjective function θ: $P \to Q$ such that for each $t \in T$ there exists a $t' \in T'$ with $Pt' \subseteq P$ and the following diagram commutes:

$$\begin{array}{ccc} p & \xrightarrow{t'} & p \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ Q & \xrightarrow{t} & Q \end{array}$$

The important tie-up between the machine and algebraic concepts of simulation is

$$M_2 \prec M_1 \quad \text{if and only if} \quad (Q_2, T(M_2)) \prec (Q_1, T(M_1)).$$

The transition semigroup associated with a two state reset automaton is denoted by U_3. It consists of the matrices

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

under matrix multiplication, acting on the right of the set $\mathbf{2} = \{(1, 0), (0, 1)\}$. The transition semigroup associated with a group automaton is called a transformation group and is denoted by (X, G). It consists of a group G acting by permutations on the set X.

Cascade composition of machines corresponds to the following combination of transformation semigroups: let (Q_1, T_1) and (Q_2, T_2) be transformation semigroups. Their *wreath product* is the transformation semigroup

$$T_1 \ltimes T_2 = \left(Q_1 \times Q_2, T_1^{Q_2} \times T_2\right),$$

where $T_1^{Q_2}$ is the set of functions from Q_2 to T_1 and the multiplication is given by

$$(f,t)(g,t') = ((-)f(-t)g, tt').$$

Algebraically, this composition is not as odd as it first appears. Let $\mathrm{Mat}_{|Q_2|}(T_1)$ denote the semigroup of row-monomial matrices with entries from T_1. It is easy to see that each element (f,t) corresponds to a unique element of $\mathrm{Mat}_{|Q_2|}(T_1)$, and the composition $(f,t)(g,t')$ corresponds to matrix multiplication.

THEOREM 3 (Krohn–Rhodes decomposition). *Each transformation semigroup $D = (Q, T)$ admits a decomposition $D \prec D_1 \ltimes \cdots \ltimes D_n$, where for each index $1 \leq i \leq n$ either $D_i = (\mathbf{2}, U_3)$ or $D_i = (X_i, G_i)$, and G_i is a simple group with $G_i \prec T$.*

It turns out that the wreath product of two transformation groups is also a transformation group. Thus Krohn–Rhodes may be written in an alternating form,

$$(Q,T) \prec A \ltimes G_1 \ltimes A \cdots \ltimes G_n \ltimes A,$$

where each A is some block of U_3s and the G_i are groups. The (*group*) *complexity* of a semigroup is defined as

$$(Q,T)\mathbf{c} = \min\{n\colon n = \text{the number of groups used in any}$$
$$\text{alternating decomposition of } T\}.$$

The surprising result is that if M is a reduced automaton and $M\mathbf{c}$ denotes its group complexity as defined earlier, then

$$M\mathbf{c} = (Q, T(M))\mathbf{c},$$

where the right-hand side is defined as before. Moreover, every decomposition of $(Q, T(M))$ into wreath product of groups and U_3s yields an equivalent cascade decomposition of the automaton M into group automata and reset automata and vice versa.

It is a long-standing open question as to whether complexity is decidable. It is known to the Rhodes' school [16] that to decide complexity 1, it is sufficient to show that complexity 1 is decidable for regular semigroups, with three nonzero J-classes in a strict J-chain. In this article we show that complexity 1 is decidable for such semigroups.

The article is organised as follows. We first exhibit an application to game theory. In Section 3, by utilising the Rhodes expansion, we reduce the question of decidability to an amenable (to calculation) class of semigroups. In Section 4 we use Morita theory to quickly arrive at two representations. In Section 5 we use these to observe the necessary invariants (designs) to calculate a family of pointlikes. Finally, we use the presentation lemma to arrive at our result.

2. APPLICATIONS TO GAME THEORY

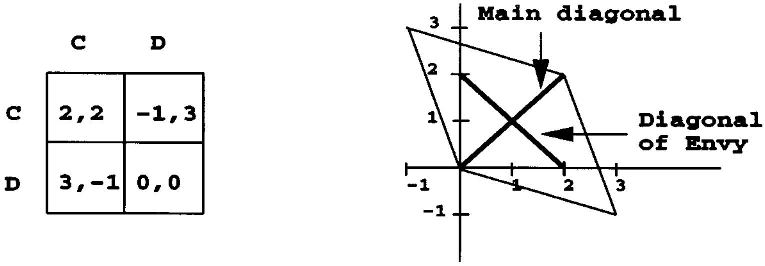
Rhodes, in a little known book, outlined an application of complexity to game theory [23]. He defined the complexity of a game as the minimum complexity of automata which can play the game perfectly (so as to achieve the von Neumann value of the game). Rhodes lends credibility to the intuitive appeal of the measure. He calculated

Game	Complexity
Trivial	0
Tic-tac-toe	1
Nim	1
7×7 Hex	≤ 24
Go	≤ 200

where Trivial is the game of placing coins of the same size flat on a round table, with the loser being the first not to be able to place a coin.

The proofs of the previous text (coupled with his sense) led Rhodes to conjecture that the complexity of a game is of the order of the typical number of moves in a game between expert players. We refer the reader to [23] for further examples, results, and conjectures.

The economist Aumann [4] pointed out the usefulness of automata for modelling bounded rationality. The use of automata now pervades numerous diverse disciplines [3, 10, 13, 17–20, 25]. Abreu and Rubinstein [1] further explored the idea of using automata for repeated games. They characterised *Nash equilibrium* automata for symmetric 2×2 stage games, when repeated game payoffs are evaluated according to the limit of means and implementation costs (number of states) enter preferences lexicographically. They found that all Nash equilibrium (N.E.) payoffs must lie on one of the two "diagonals" of the payoff matrix. On the *main diagonal* the players have equal payoffs, and on the *diagonal of envy* the payoffs are unequal (see Fig. 6).



The Prisoner's Dilemma

N.E. payoffs in this version of the game are the rational points lying on the cross.

FIG. 6.

Among 2 × 2 stage games, the Prisoner's Dilemma is the most famous. Its rise to cult status has been well documented by Sigmund [24] in "Games of Life" and Dawkins [8] in "The Selfish Gene." Sigmund described the game as follows:

> Game theorists, like gamblers and children, can become addicted to iterated games. Their classic example is the *Prisoner's Dilemma*, whose diabolical simplicity has given rise to thousands of scientific publications. Here is how it goes. Two players are engaged in the game. They have to choose between two options, which we term *Cooperate* or *Defect*. If both cooperate, they can earn three points apiece as *Reward*. If both defect, they get only one point each, which is the *Punishment* for failing to join forces. If one player defects while the other cooperates, then the defector receives five points (this is *Temptation*) while the trusting cooperator receives no points at all (this is the *Sucker's payoff*).

A moment's thought reveals that a rational player will always defect, no matter what the opponent does. Hence, two rational players end up with only one point each. However, mutual cooperation would have resulted in three points apiece!

In the infinitely repeated Prisoner's Dilemma, the same players simply repeat the ordinary game. As Dawkins [8] comments, "The successive rounds of the game give us the opportunity to build up trust or mistrust, to reciprocate or placate, forgive or avenge."

In [28] we completely characterised the complexity of the Abreu–Rubinstein automata. We found that on the main diagonal the complexity is 0, 1, or 2. This turned out to be in stark contrast to the diagonal of envy. We say that a line segment is a *place of folly* if the complexity can be arbitrarily large in an arbitrary neighbourhood of an arbitrary point. We showed that the diagonal of envy is a place of folly.

It has been observed that "In spite of the advances to which it had led, game theory is still in its infancy. Perhaps the leading obstacle to further progress is the equilibrium selection problem." The decidability of complexity 1 allows us to give meaning to the "complexity 1 automatic game" and so address this problem. In this game the players are restricted to automata of complexity 1, but otherwise the game is the same as the Abreu–Rubinstein formulation of the automatic game. In [28] we show that all N.E. payoffs for this formulation, lie on the main diagonal. In [11] we use this result, in conjunction with a large number of calculations on a computer, to demonstrate the subtlety of the measure.

3. AN AMENABLE SUFFICIENCY CLASS FOR DECIDABILITY OF COMPLEXITY

The Krohn–Rhodes decomposition states that a semigroup S can be simulated by

$$A \ltimes G \ltimes A \ltimes \cdots \ltimes G \ltimes A.$$

It is apparent that one should seek a solution to the decidability problem by utilising such a simulation. Indeed, the Rhodes expansion [9] is precisely such a tool. Rhodes defined

$$\mathbb{E}(\mathcal{L}, S) = \{[s_n, \ldots, s_1]: n \geq 1, s_{i+1} <_{\mathcal{L}} s_i, s_j \in S\}$$

with product

$$[s_n, \ldots, s_1][t_m, \ldots, t_1] = \operatorname{Red}([s_n t_m, \ldots, s_1 t_m, t_m, \ldots, t_1]),$$

where Red$(-)$ is the chain obtained recursively by reading from right to left and cancelling each element that is $\mathcal{L}$-equivalent to its successor. By considering $<_{\mathcal{R}}$, we can define the right Rhodes expansion $\mathbb{E}(\mathcal{R}, S)$.

Margolis and Rhodes independently proved that $\mathbb{E}(\mathcal{L}, S)$ is *embedded* in a Krohn–Rhodes decomposition. Birget formulated the following:

DEFINITION 2 [5]. An order $\leq$ on a set X is said to be unambiguous if for all $x, y, z \in X$, $z \leq x$ and $z \leq y$ imply either $x \leq y$ or $y \leq x$. A semigroup S is said to be $\mathcal{L}$-unambiguous (except at 0) if the $\mathcal{L}$-order of $S \backslash \{0\}$ is unambiguous. Similarly, we may define $\mathcal{R}$-unambiguous. If both the $\mathcal{R}$ and $\mathcal{L}$-orders of $S \backslash \{0\}$ are unambiguous, then S is said to be an unambiguous semigroup.

THEOREM 4 [5]. *Let S be a finite semigroup. Then the following hold*:

1. $\mathbb{E}(\mathcal{L}, S)$ $(\mathbb{E}(\mathcal{R}, S))$ *is a finite $\mathcal{L}$-unambiguous ($\mathcal{R}$-unambiguous) semigroup.*

2. *There exists a natural surjective homomorphic* $\eta^{\mathcal{L}}\colon \mathbb{E}(\mathcal{L}, S) \to S$ $(\eta^{\mathcal{R}}\colon \mathbb{E}(\mathcal{R}, S) \to S)$ *such that the restriction to any subgroup is injective and the inverse image of a regular* $\mathcal{R}$- $(\mathcal{L})$-*class of* S *is a unique regular* $\mathcal{R}$- $(\mathcal{L})$-*class of* $\mathbb{E}(\mathcal{L}, S)$ $(\mathbb{E}(\mathcal{R}, S))$.

3. $S\mathbf{c} = \mathbb{E}(\mathcal{L}, S)\mathbf{c} = \mathbb{E}(\mathcal{R}, S)\mathbf{c}$.

4. *S is regular if and only if* $\mathbb{E}(\mathcal{L}, S)$ $(\mathbb{E}(\mathcal{R}, S))$ *is regular*.

5. *For a regular semigroup S the semigroup* $\mathbb{E}(\mathcal{R}, \mathbb{E}(\mathcal{L}, S))$ *is regular, unambiguous and* $\mathbb{E}(\mathcal{R}, \mathbb{E}(\mathcal{L}, S))\mathbf{c} = S\mathbf{c}$.

It follows from the foregoing text that to decide the complexity of regular semigroups, it is sufficient to decide the complexity of regular unambiguous semigroups. If we now perceive the Krohn–Rhodes decomposition as simulation by representation and we keep the Schützenberger representation in mind, then surely we must proceed as follows:

Let S be a semigroup and let J be a noncombinatorial $\mathcal{J}$-class of S. The following equivalence relation on S is folklore [2],

$$s \equiv_J t \quad \text{iff for all } x \in J^0, \qquad xs = xt,$$

where we understand $0s = s0 = 0$ and $ab = 0$ if ab does not belong to J. This is clearly a congruence on S. Let Θ_J denote the natural map from S onto $S/\equiv_J$.

LEMMA 1 (Rhodes). *Let S be noncombinatorial. Then the following hold*:

1. $S\mathbf{c} = \max\{(S\Theta_J)\mathbf{c}\colon J$ *a noncombinatorial* $\mathcal{J}$ *class*$\}$. *In particular there exists a noncombinatorial* $\mathcal{J}$-*class J such that* $(S\Theta_J)\mathbf{c} = S\mathbf{c}$.

2. *In* $S\Theta_J$, *the image of J under* Θ_J *is itself a* $\mathcal{J}$-*class, and is such that* $I = J\Theta_J \cup \{0\}$ *or* $I = J\Theta_J$ *is a unique* 0-*minimal ideal, and J is* $\mathcal{J}$-*least among the* $\mathcal{J}$-*classes whose images lie in* $J\Theta_J$.

3. $S\Theta_J$ *acts faithfully on the right of its* 0-*minimal ideal*.

It follows from Theorem 4 and Lemma 1 that to decide the complexity of a semigroup S it is enough to decide the complexity of each $\mathbb{E}(\mathcal{L}, S)\Theta_J$. It is also easy to see that $\mathbb{E}(\mathcal{L}, S)\Theta_J$ is $\mathcal{L}$-unambiguous.

DEFINITION 3. We say that a semigroup S is a *G-semigroup* if S has a unique 0-minimal ideal I with maximal subgroup G, and S acts faithfully on the right of I.

THEOREM 5. *To decide the complexity of regular semigroups, it is sufficient to decide the complexity of regular unambiguous G-semigroups*.

Proof. By Theorem 4 the semigroup $\mathbb{E}(\mathcal{R}, \mathbb{E}(\mathcal{L}, S)\Theta_J)$ has the same complexity as $\mathbb{E}(\mathcal{L}, S)\Theta_J$ and is $\mathcal{R}$-unambiguous. We note that $\mathbb{E}(\mathcal{L}, S)\Theta_J$

is regular, $\mathcal{L}$-unambiguous, and under the natural surjective homomorphism

$$\eta^{\mathcal{R}}: \mathbb{E}(\mathcal{R}, \mathbb{E}(\mathcal{L}, S)\Theta_J) \to \mathbb{E}(\mathcal{L}, S)\Theta_J,$$

the inverse image of a regular $\mathcal{L}$-class of the latter is a unique regular $\mathcal{L}$-class of the former. Hence, $\mathbb{E}(\mathcal{R}, \mathbb{E}(\mathcal{L}, S)\Theta_J)$ is also $\mathcal{L}$-unambiguous. That it is a G-semigroup follows directly from the definition of the Rhodes expansion.

4. SOME REPRESENTATIONS VIA MORITA THEORY

In [26], we developed Morita theory for semigroups. We now use the Morita theorems to arrive at two different representations of S. We shall later exploit the interplay between these two representations to arrive at the necessary invariants for calculating pointlikes.

Let S be a regular three $\mathcal{J}$-class unambiguous G-monoid with $\mathcal{J}$-class structure $J_2 > J_1 > J_0$. We choose an idempotent from each $\mathcal{J}$-class and denote them, respectively, by e_2, e_1, and e_0. Also let K, H, and G be the respective maximal subgroups. For $n = 0, 1$ let $I_n = Se_nS$ and $R_n = e_nSe_n$. It is easy to see that I_n is Morita equivalent [26] to R_n via the unitary context

$$\langle I_n, R_n, Se_n, e_nS, \langle\ ,\ \rangle, [\ ,\ ]\rangle,$$

where $[\ ,\ ]$: $Se_n \otimes_{R_n} e_nS \to I_n$ is defined by $[se_n, e_nt] = se_nt$ and $\langle\ ,\ \rangle$: $e_nS \otimes_{S_n} Se_n \to R_n$ is defined by $\langle e_ns, te_n\rangle = e_nste_n$.

We have the table

	e_2Se_2	
$\mathrm{End}_{I_1}I_1$	$I_1 \sim R_1$	$\mathrm{End}_{R_1}e_1S$
$\mathrm{End}_{I_0}I_0$	$I_0 \sim R_0$	$\mathrm{End}_{R_0}e_0S$

where $\sim$ denotes Morita equivalence and the entries in the first and last column are isomorphic. The last two rows of the table share a remarkable similarity. For any semigroup T and positive integer m let $M_m(T)$ denote the semigroup of $m \times m$ row-monomial matrices over T.

THEOREM 6 [26]. *Let I be a completely 0-simple semigroup with maximal subgroup G, l $\mathcal{L}$-classes and r $\mathcal{R}$-classes. Then*

$$I \cong Ie_0 \otimes_G e_0I \cong \coprod_{k=1}^{r} \alpha_k^0 e_0G \otimes_G \coprod_{k=1}^{l} Ge_0\beta_k^0,$$

with multiplication defined by the matrix, $\langle\ ,\ \rangle$ *and*

$$\mathrm{End}_I I \cong \mathrm{End}_G \coprod_{k=1}^{l} Ge_0\,\beta_k^0 \cong M_l(G).$$

Since S acts faithfully on I, we arrive at the Schützenberger representation of S in $\mathrm{End}_I I \cong M_l(G)$.

4.1. *The Schützenberger Representation of* R_1

Let $[J_0, H] = \{e_0\,\beta_k^0\colon e_0\,\beta_k^0 e_1 = e_0\,\beta_k^0\}$. The Schützenberger representation of R_1, represents elements by matrices which are zero in all columns not belonging to $[J_0, H]$. Hence, R_1 embeds in $M_{\|[J_0, H]\|}(G)$. Further, the set $[J_0, H]$ is a right H-set: for $h \in H$ the action can be realised by the matrix $\bar{h}$ obtained from h by replacing any nonzero entry by the identity of G. Let

$$B(H)_i = \left\{b_{ij}^0\colon j = 1, \ldots, o(i)\right\}, \qquad i = 1, \ldots, o(H),$$

denote the orbits of H. Since $R_1 - H$ is a completely 0-simple semigroup, we find the classical visualisation of R_1:

H

$GB(H)_1$	$GB(H)_2$	$\cdots$	$GB(H)_{o(K)}$
$\vdots$			

where $\boxed{GB(H)_i}$ represents the H-classes

Gb_{i1}^0	Gb_{i2}^0	$\cdots$	$Gb_{io(i)}^0$

.

Let $A(R_1 - H) = \{a_i^0\colon i = 1, \ldots, n\}$ index the R-classes of $R_1 - H$. Then an element of $R_1 - H$ is of the form $a_i^0 \otimes gb_{jk}^0$, and so is represented in $M_{\|[J_0, H]\|}(G)$ as a row-monomial matrix with at most one nonzero column. An element of H is represented as a row and column-monomial matrix with a nonzero entry in each row. We now partition the matrices into blocks labelled by the orbits. For each element $r \in R_1$, we colour in a block if the block contains a nonzero entry. We denote the resulting pattern by $\mathbf{F}(r)$, and call it the *block form* of r. For $h \in H$ we find that $\mathbf{F}(h)$ is block diagonal (see Fig. 7). The elements of $R_1 - H$ determine block forms $\mathbf{F}(a^0 \otimes gb_{jk}^0)$ of the type in Fig. 8.

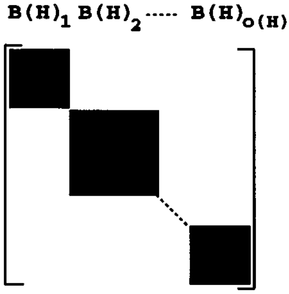


FIG. 7.

4.2. *Inducing by the Schützenberger Representation*

Since I_1 is a regular unambiguous semigroup, we find that there exist idempotents f'_k such that ${}_{I1}I_1 = \coprod_{k=1}^{l'_1} I_1 f'_k$ and ${}_{R_1}e_1 I_1 = \coprod_{k=1}^{l'_1} e_1 I_1 f'_k$.

LEMMA 2 [26]. *There exist idempotents f_k in R_1 such that*

$$ {}_{R_1}e_1 I_1 \cong \coprod_{k=1}^{l'_1} R_1 f_k \quad \textit{and} \quad \mathrm{End}_{I_1} I_1 \cong \mathrm{End}_{R_1} \coprod_{k=1}^{l'_1} R_1 f_k \cong M_{l'_1}(R_1). $$

Moreover, because $I \subset I_1$, we find that S also embeds in $\mathrm{End}_{I_1} I_1 \cong M_{l'_1}(R_1)$. We now explore the relationship between this representation and the one in $M_l(G^0)$. We first proceed along the lines of the proof of the synthesis theorem [27].

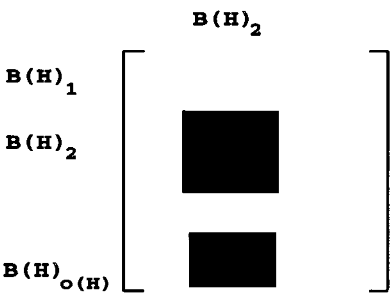


FIG. 8.

It is well known that for a finite semigroup S, two idempotents e and f are $\mathcal{J}$-related if and only if $Se \cong Sf$, if and only if $eS \cong fS$. Now each idempotent in the set $\{f_k\colon k = 1, \dots, l'_1\}$ is $\mathcal{J}$-related to e_1 or e_0. Hence,

$$\coprod_{k=1}^{l'_1} R_1 f_k = \coprod_{j=0}^{1} \prod_{k=1}^{l_j} R_1 e_j \beta_k = \coprod_{k=1}^{l_1} R_1 b_k^1 \coprod_{k=1}^{l_0} R_1 \bar{b}_k^0,$$

where $\beta_k\colon R_1 e_j \to R_1 f_k$ is some isomorphism, with $e_1 \beta_k = b_k^1$ and $e_0 \beta_k = \bar{b}_k^0$. Similarly,

$$I_1 e_{1R_1} = \coprod_{k=1}^{r'_1} f''_k I_1 e_1 = \prod_{j=0}^{1} \prod_{k=1}^{r_j} \alpha_k e_j R_1 = \coprod_{k=1}^{r_1} a_k^1 R_1 \coprod_{k=1}^{r_0} \bar{a}_k^0 R_1,$$

where $\alpha_k e_j R_1 \to f''_k R_1$ is some isomorphism with $a_k^1 = \alpha_k e_1$ and $\bar{a}_k^0 = \alpha_k e_0$. Now

$$I_1 \cong I_1 e_1 \otimes_{R_1} e_1 I_1 \cong \coprod_{k=1}^{r_1} a_k^1 R_1 \coprod_{k=1}^{r_0} \bar{a}_k^0 R_1 \otimes_{R_1} \coprod_{k=1}^{l_1} R_1 b_k^1 \coprod_{k=1}^{l_0} R_1 \bar{b}_k^0$$

with multiplication defined by the matrix

$$\langle\ ,\ \rangle_1\colon \coprod_{k=1}^{l_1} R_1 b_k^1 \coprod_{k=1}^{l_0} R_1 \bar{b}_k^0 \times \coprod_{k=1}^{r_1} a_k^1 R_1 \coprod_{k=1}^{r_0} \bar{a}_k^0 R_1 \to R_1.$$

We have already seen that an element of R_1 either belongs to H or is represented as $a_i^0 \otimes g b_{jk}^0$. By the unambiguity of S, it easily follows [27] that $\coprod_{k=1}^{l} G e_0 \beta_k$ can be decomposed as

$$\coprod_{j=1}^{o(K)} \coprod_{k=1}^{1(j)} \coprod_{k'=1}^{o(H)} \coprod_{j'=1}^{0(k')} G b_{j'k'}^0 b_{jk}^1 \coprod_{k=1}^{l_0} G \bar{b}_k^0.$$

We will now make better sense of the representation of S in $M_l(G^0)$ in the following manner: Let $[J_1, K] = \{b_k^1\colon k = 1, \dots, l_1\}$ and $[J_0, K] = \{\bar{b}_k^0\colon k = 1, \dots, l_0\}$. Then the sets $[J_1, K]$ and $[J_0, K]$ are right K-sets. For $k \in K$ the action can be realised by the matrix $\bar{k}$ obtained from k by replacing any nonzero entry by the identity of H or G. Let

$$B(K)_i = \left\{b_{ij}^1\colon j = 1, \dots, 1(i)\right\}, \qquad i = 1, \dots, o(K),$$

$$\bar{B}(K)_m = \left\{\bar{b}_{mj}^0\colon j = 1, \dots, \bar{0}(m)\right\}, \qquad m = 1, \dots, \bar{o}(K),$$

K

$HB(K)_1$	$HB(K)_2$	$\cdots$	$HB(K)_{o(K)}$
$\vdots$			

$GB(H)_1B(K)_1$	$\cdots$	$GB(H)_{o(H)} \times B(K)_1$	$GB(H)_1B(K)_2$	$\cdots$	$GB(H)_{o(H)} \times B(K)_{o(K)}$	$G\bar{B}(K)_1$	$\cdots$	$G\bar{B}(K)_{o(K)}$
$\vdots$								

.

denote the respective orbits of K. We rearrange the $\mathcal{L}$-classes of S into blocks as follows:

At a moment's reflection we arrive at:

THEOREM 7. *The representation of S in $M_l(G^0)$ is given by first embedding S in $M_{l'_1}(R_1)$ and then identifying elements of R_1 in the $[J_1, K] \times [J_1, K]$ block, with their Schützenberger representation in $M_{\|[J_0, H]\|}(G^0)$. Further, if we partition the matrices into blocks as shown in the preceding visualisation of J_0, then elements of K have the block form shown in Fig.* 9, *and elements of J_1 have the block form shown in Fig.* 10. *Elements of J_0 are of course nonzero in just one column.*

This result is fundamental to our proof of decidability and we highlight it by denoting the image of S in $M_l(G^0)$ by $\mathrm{Mat}^G(S)$. On letting $B = \{b^0_{j'k'} b^1_{jk}\} \cup \{\bar{b}^0_k\} \cup \{0\}$ we arrive at the transformation semigroup $(B, \mathrm{Mat}^G(S))$.

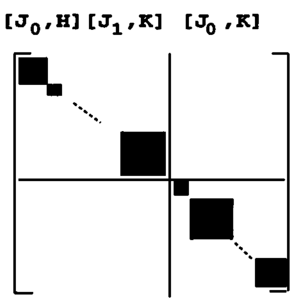


FIG. 9.

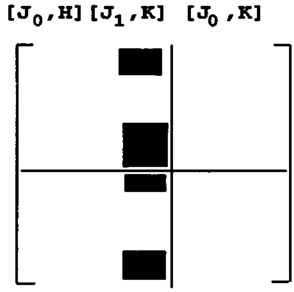


FIG. 10.

5. POINTLIKES AND INVARIANT DESIGNS OF $\langle\ ,\ \rangle_1$

Rhodes noted that for a transformation semigroup (B, S) there is a particularly important family of subsets of B. A set $X \subseteq B$ is said to be a *pointlike* if, for every relational morphism (θ, ϕ): $(B, S) \to (Y, A)$ with A combinatorial, there exists $y \in Y$ such that $X \subseteq \theta^{-1}(y)$.

LEMMA 3 [22]. *Let (θ, ϕ): $(B, S) \to (Y, A)$ be a relational morphism with A combinatorial. Then for any subgroup H of S, there exists on idempotent e in A such that $H \subseteq \phi^{-1}(e)$ and for any $b \in B$ the orbit bH is a pointlike.*

COROLLARY 1. *For the transformation semigroup $(B, \mathrm{Mat}^G(S))$ the sets $B(H)_i B(K)_j$ and $\overline{B}(K)_k$ are pointlike, where $i = 1, \ldots, o(H)$, $j = 1, \ldots, o(K)$, and $k = 1, \ldots, \overline{o}(K)$.*

Proof. By Lemma 3, each $B(H)_i$ is a pointlike and is contained in $\theta^{-1}(y)$ for some $y \in Y$. Let $b \in B(K)_j$, $b' \in \phi(b)$, and $e_2' \in \phi(e_2)$. Then

$$\theta^{-1}(yb'e_2') \supseteq \theta^{-1}(y)\phi^{-1}(b')\phi^{-1}(e_2') \supseteq B(H)_i bK = B(H)_i B(K)_j.$$

5.1. *A Larger Family of Pointlikes*

Let $[K, J_1] = \{a_k^1 \colon\ k = 1, \ldots, r_1\}$. We now consider the matrix block $\langle [J_1, K], [K, J_1] \rangle_1$ of $\langle\ ,\ \rangle_1$. We shall now observe an invariant form of this block and use it to determine a larger family of pointlikes.

Recall that each $\langle b, a\rangle_1 \in \langle [J_1, K], [K, J_1]\rangle_1$ is an element of R_1 and has been identified with its image in $M_{\llbracket J_0, H\rrbracket}(G^0)$. We obtain the *design* of the matrix $\langle\ ,\ \rangle_1$ by identifying each entry with its block form; that is,

$$\mathbf{D}\langle b, a\rangle_1 = \mathbf{F}\langle b, a\rangle_1.$$

Since H is represented by block diagonal matrices, it follows that $\mathbf{D}\langle [J_1, K], [K, J_1]\rangle_1$ is invariant under the change of coordinates within an H-class of J_1. It is easy to see that $[K, J_1]$ is a left K-set and decomposes into orbits $(K)A_i$, $i = 1, \dots, (K)o$. Thus we have a partition of $\langle [J_1, K], [K, J_1]\rangle_1$ into *(upper) cells* $\langle B(K)_i, (K)A_j\rangle_1$.

We note that the group K bears heavily on the design of a cell due to

$$\mathbf{F}\langle bk, a\rangle_1 = \mathbf{F}\langle b, ka\rangle_1.$$

In particular, if $a, a' \in (K)A_i$ and $b \in B(K)_j$, then there exists $b' \in B(K)_j$ such that

$$\mathbf{F}\langle b, a\rangle_1 = \mathbf{F}\langle b', a'\rangle_1.$$

For example if $K = \mathbb{Z}_3$ and H has three orbits, then a possible design for a cell indexed by $\{b_1^1, b_2^1, b_3^1\}$ and $\{a_1^1, a_2^1, a_3^1\}$ is as shown in Fig. 11.

5.2. *Content of a Cell and Its Derivations*

For elements $\langle b, a\rangle_1$, $\langle b', a'\rangle_1$ of a cell $\langle B(K)_i, (K)A_j\rangle_1$, we let $\mathbf{F}\langle b, a\rangle_1 + \mathbf{F}\langle b', a'\rangle$ be the pattern obtained by superimposing $\mathbf{F}\langle b, a\rangle_1$ on $\mathbf{F}\langle b', a'\rangle_1$. The *content* of a cell $\langle B(K)_i, (K)A_j\rangle_1$ is defined as

$$\mathbf{C}(i, j) = \sum_{\langle B(K)_i, (K)A_j\rangle_1} \mathbf{F}\langle b, a\rangle_1.$$

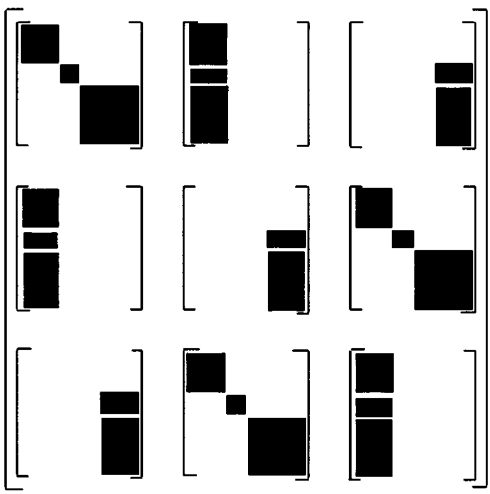


FIG. 11.

For example, the content of the preceding cell (we fix our notation) is

	$B(H)_1$	$B(H)_2$	$B(H)_3$
$B(H)_1$	■		
$B(H)_2$	■	■	■
$B(H)_3$	■		■

. (1)

An enlargement of a content by $B(H)_i$ is obtained by introducing a new row and a new column labelled by $B(H)_i$ and nonzero blocks as before.

A *derivation* of $\mathbf{C}(i, j)$ is any pattern which can be obtained from $\mathbf{C}(i, j)$ by some enlargement, some reordering of the border, and removal of nonzero blocks. For example,

	2	3	1
2	■	■	
3			
1			

and

	2	3	1
2	■		
3		■	■
1			

(2)

are two derivations of the content in (1), where $i = 1, 2, 3$ refer to the index of $B(H)_i$. We are now in a position to calculate a larger family of pointlikes.

5.3. *Calculation*

A content is said to be *complete* if each diagonal block of the content is nonzero. Since J_1 is a regular $\mathcal{J}$-class, we find that in each row and column of upper contents, there is at least one complete content.

Let $\boldsymbol{B}(H) = \{B(H)_i : i = 1, \ldots, o(H)\}$. An m-tuple

$$[B(H)_{p_1}, B(H)_{p_2}, \ldots, B(H)_{p_m}], \qquad B(H)_i \in \boldsymbol{B}(H),$$

is said to be a *calculation chain* if there exists a sequence $\mathbf{C}(i_k, j_k)$, $k = 1, \ldots, m-1$, of (not necessarily distinct) complete contents such that

	p_1	p_2	$\cdots$	p_k	p_{k+1}	$\cdots$
p_1	■				$*$	
p_2		■			$*$	
			■		$*$	
p_k				■	$*$	
p_{k+1}						

is a derivation of $\mathbf{C}(i_k, j_k)$, with one of the starred blocks nonzero. For example, $[B(H)_2, B(H)_3, B(H)_1]$ is a calculation chain for the content in (1) due to the derivations in (2).

A chain $[B(H)_{p_1}, \dots, B(H)_{p_n}]$ is said to be a block of the chain $[B(H)_{i_1}, B(H)_{i_2}, \dots, B(H)_{i_m}]$ if there exists an i_q such that $B(H)_{p_k} = B(H)_{i_{q+k}}$ for $k = 1, \dots, n$. A chain is reduced recursively by identifying any two like consecutive blocks. We let RC denote the set of reduced chains. By a well known result in combinatorics we have

$$|\mathrm{RC}| \leq \sum_{k=1}^{o(H)} C_k^{o(H)} \prod_{i=1}^{k-1} (k - i + 1)^{2^i}.$$

Henceforth, the term "chain" will refer to reduced chain.

LEMMA 4. *Let* $[B(H)_{p_1}, B(H)_{p_2}, \dots, B(H)_{p_m}]$ *be a calculation chain. Then for each* $j = 1, \dots, o(K)$, *the set* $\bigcup_{i=1}^{m} B(H)_{p_i} B(K)_j$ *is a pointlike.*

Proof. Let (θ, ϕ): $(B, \mathrm{Mat}^G(S)) \to (Y, A)$ be a relational morphism with A combinatorial. Also let $\mathbf{C}(i_k, j_k)$, $k = 1, \dots, m-1$, be a sequence of contents associated with the given chain. By Corollary 1 we know that $B(H)_{p_1} B(K)_{i_1}$ is a pointlike, and so let $B(H)_{p_1} B(K)_{i_1} \subseteq \theta^{-1}(y)$. For fixed elements $b \in B(K)_j$ and $a \in (K)A_{j_1}$, let $b' \in \phi(b)$ and $a' \in \phi(a)$. Then

$$\begin{aligned} \theta^{-1}(ye_2' a' e_1' b' e_2') &\supseteq \theta^{-1}(y) \phi^{-1}(e_2') \phi^{-1}(a') \phi^{-1}(e_1') \phi^{-1}(b') \phi^{-1}(e_2') \\ &\supseteq B(H)_{p_1} B(K)_{i_1} KaHbK \\ &\supseteq B(H)_{p_1} B(K)_{i_1} (K) A_{i_1} HB(K)_j \\ &\supseteq B(H)_{p_1} B(K)_j \cup B(H)_{p_2} B(K)_j. \end{aligned}$$

The last statement follows from the fact that $\mathbf{C}(i_1, j_1)$ has a derivation

	1	2	$\cdots$
1	$\blacksquare$	$\blacksquare$	
2			

However, now $\bigcup_{i=1}^{2} B(H)_{p_i} B(K)_j$ is a pointlike for arbitrary j and in particular for $j = i_2$. Also, $\mathbf{C}(i_2, j_2)$ has the derivation

	p_1	p_2	p_3
p_1	■		$*$
p_2		■	$*$
p_3			

and the result follows by recursion.

5.4. *Partition Due to Complete Contents*

Calculation chains allow us to define an equivalence relation on the set $B(H)$. We say $B(H)_1$ is equivalent to $B(H)_2$, denoted as $B(H)_1 \sim B(H)_2$, if there exists chains

$$[B(H)_1, \dots, B(H)_2] \quad \text{and} \quad [B(H)_2, \dots, B(H)_1].$$

This is indeed an equivalence relation. Suppose there exist chains

$$[B(H)_1, B(H)_{p_1}, \dots, B(H)_{p_n}, B(H)_2],$$
$$[B(H)_2, B(H)_{q_1}, \dots, B(H)_{q_m}, B(H)_3].$$

Then there exists a sequence of contents

	1	p_1	$\cdots$
1	■	■	
p_1			

,

	1	p_1	p_2
1	■		$*$
p_1		■	$*$
p_2			

$\dots$,

	1	p_1	$\cdots$	p_n	2	$\cdots$
1	■				$*$	
p_1		■			$*$	
			■		$*$	
p_n				■	$*$	
2						

due to the first chain. We also have a sequence of contents,

	2	q_1	$\cdots$
2	■	■	
q_1			

,

	2	q_1	q_2
2	■		$*$
q_1		■	$*$
q_2			

, $\cdots$

	2	q_1	$\cdots$	q_m	3	$\cdots$
2	■				$*$	
q_1		■			$*$	
			■		$*$	
q_m				■	$*$	
3						

due to the second chain. However, all chains are formed using complete contents. Thus we may view

	2	q_1	$\cdots$
2	■	■	
q_1			

as

	1	p_1	$\cdots$	p_n	2	q_1
1	■					
p_1		■				
			■			
p_n				■		
2					■	■

.

Continuing in this fashion, we see that there exists a chain $[B(H)_1, \ldots, B(H)_3]$.

Let $P_1, \ldots, P_n$ denote the equivalence classes. Suppose $P_1 = \{B(H)_{1_1}, \ldots, B(H)_{1_n}\}$ and $P_2 = \{B(H)_{2_1}, \ldots, B(H)_{2_m}\}$. We shall write

		1	2	$\cdots$	
		1	■	■	
		2			

if there exists a content such that the $P_1 \times P_2$ block contains a nonzero $B(H)_{1_i} \times B(H)_{2_j}$ block. For example,

	2_1	2_2	$\cdots$	2_m
1_1				
1_2	■			
			■	
1_n				

.

An m-tuple $[P_{p_1}, P_{p_2}, \ldots, P_{n_n}]$ is said to be P-chain if there exists a sequence of derivations

	p_1	p_2
p_1		■

,

	p_1	p_2	p_3	
p_1				
p_2			■	

$\cdots$,

	p_1	p_2	$\cdots$	p_n
p_1				
p_2				
p_{n-1}				■

in complete contents.

As before, a P-chain is reduced recursively by identifying any two consecutive like blocks. Henceforth, "P-chain" will refer to reduced P-chain.

LEMMA 5. *Let* $[P_{p_1}, P_{p_2}, \ldots, P_{p_n}]$ *be a* P*-chain. Then the set*

$$\bigcup_{i=1}^{n} P_{p_i} B(K)_j$$

is pointlike for all $j = 1, \ldots, o(K)$.

Proof. We know that there exists a sequence of contents with the foregoing derivations. Suppose $B(H)_1 \in P_{p_1}$, $B(H)_2 \in P_{p_2}$, and the $B(H)_1 \times B(H)_2$ block is nonzero. Then $[B(H)_1, B(H)_2]$ is a calculation chain. Also, there exists a calculation chain containing all elements of P_{p_1} and ending in $B(H)_1$, and a calculation chain containing all elements of

P_{p_2} and beginning with $B(H)_2$. Hence, there exists a chain containing all elements of $P_{p_1} \cup P_{p_2}$. The result follows by induction.

The following is a fundamental property of P-chains.

LEMMA 6. *Suppose* $[P_1, P_2]$ *is a* P*-chain. Then there is no chain in which* P_2 *appears to the left of* P_1.

Proof. Let $[P_1, P_2]$ be a P-chain. Then there exists a content with the $B(H)_1 \times B(H)_2$ block nonzero, and $B(H)_1 \in P_1$, $B(H)_2 \in P_2$. However, since the content is complete, we also find that the $B(H)_1 \times B(H)_1$ block of the content is nonzero. Thus, $[B(H)_1, B(H)_2]$ is a calculation chain.

Now suppose there exists a P-chain of the form $[\dots, P_2, \dots, P_1, \dots]$. Then by definition of P-chain it is easy to see that if we cut this chain on the left up to P_2, and on the right from P_1, then we arrive at another P-chain of the form $[P_2, \dots, P_1]$. However, this implies that there exists a calculation chain starting with an element of P_2 and ending with an element of P_1. That is, $P_2 = P_1$.

The *cuts* of a chain $[P_{p_1}, P_{p_2}, \dots, P_{p_{n-1}}, P_{p_n}]$, are the chains

$$\begin{gathered}
\left[P_{p_1}, P_{p_2}, \dots, P_{p_{n-1}}, P_{p_n}\right], \\
\left[P_{p_1}, P_{p_2}, \dots, P_{p_{n-1}}\right], \\
\vdots \\
\left[P_{p_1}, P_{p_2}\right], \\
\left[P_{p_1}\right].
\end{gathered}$$

There is a natural partial order on P-chains:

$$X_1 \le X_2 \quad \text{if } X_2 = [X_1, \dots].$$

We shall be interested in the set Max consisting of all maximal P-chains and their cuts. Let $\mathrm{Max}(P_i)$ be the set of all chains in Max which end in P_i and their cuts. We note that if $[P_1, P_2]$ is a P-chain, then $\mathrm{Max}(P_1) \subset \mathrm{Max}(P_2)$, because any P-chain in Max ending in P_1 is below a chain of the form $[\dots, P_1, P_2]$. Moreover, for $X_1, X_2, X_3 \in \mathrm{Max}$ with $X_1 \le X_2$ and $X_1 \le X_3$, we find that $\bigcup P_i B(K)_j$ is pointlike, where the union is taken over all the P_i appearing in X_2 and X_3.

5.5. *Lower Contents*

The cells $\langle \overline{B}(K)_i, (K)A_j \rangle_1$ will be referred to as the lower cells and their contents as the lower contents. We note that any $\langle b, a \rangle_1 \in \langle \overline{B}(K)_i, (K)A_j \rangle_1$ is $\mathcal{R}$-related to e_0, and on partitioning a lower content into blocks labelled by the $P_1, \ldots, P_n$, we see that the nonempty rows are nonzero in the same columns. For example,

	p_1	p_2	$\cdots$	p_n
p_1		■		■
p_2		■		■
p_n				

.

We define the range of $\langle \overline{B}(K)_i, (K)A_j \rangle_1$ to be the set of columns in which the content is nonzero and denote this set by $\mathrm{Ran}(i, j)$.

LEMMA 7. *The sets* $\mathrm{Ran}(i, j)X$ *are pointlike for* $X \in \{B(K)_j, \overline{B}(K)_j\}$.

Now the sets $\mathrm{Ran}(i, j)$ can be ordered by inclusion. Let M Ran denote the set of maximal sets. We now extend the set of maximal P-chains. Given a maximal P-chain of the form $[P_1, \ldots]$, we form new chains whose first element is any maximal set in M Ran which contains P_1, and the rest of the chain is left as it is. For example, let $\{P_1, P_2\}$ and $\{P_1, P_3\}$ be in M Ran. Then the chain $[P_1, P_4]$ gives rise to the chains $[\{P_1, P_2\}, P_4]$ and $[\{P_1, P_3\}, P_4]$.

We are now in a position to utilise the presentation lemma [22].

6. THE PRESENTATION LEMMA

We need some definitions from [22]: Let $\mathrm{Diag}_l(G^0)$ denote the set of diagonal matrices with entries from G^0. Then G acts naturally on the left of $\mathrm{Diag}_l(G^0)$ by

$$g \cdot \mathrm{diag}(g_1, \ldots, g_l) = \mathrm{diag}(gg_1, \ldots, gg_n), \qquad g_i \in G^0.$$

Denote the orbit of $\partial = \mathrm{diag}(g_1, \ldots, g_n)$ by $[\partial]$. An orbit $[\partial']$ is said to be an aspect of $[\partial]$ if $[\partial']$ can be derived from $[\partial]$ by replacing some of the g_is by zero. The support of $[\partial]$ is the set $\sigma[\partial] = \{i\colon g_i \neq 0\}$.

An orbit $[\partial]$ is said to be a *cross section* for $\mathrm{Mat}_l^G(S)$, if it has a representative ∂ satisfying

$$\text{for all } b_1, b_2 \in \sigma[\partial] \text{ and } s \in \mathrm{Mat}_l^G(S), \text{ if } b_1 \cdot s = b_2 \cdot s \neq 0,$$
$$\text{then } \partial(b_1)s_{b_1} = \partial(b_2)s_{b_2}.$$

Note that cross sections are well defined. For $s \in \mathrm{Mat}^G(S)$, we denote the entry in the ith row of s by s_i. Let $\mathrm{diag}(s) = \mathrm{diag}(s_1, \dots, s_l)$ be the diagonal matrix. An aspect of a cross section is a cross section and S acts naturally on the right of its cross sections by

$$[\partial]s = [\mathrm{diag}(\partial s)].$$

An element s of S is said to map $[\partial]$ into $[\partial']$ if $[\partial]s$ is an aspect of $[\partial']$.

Let $X_1, X_2 \subseteq B$ and let Π_1, Π_2 be partitions of X_1 and X_2, respectively. Call the equivalence classes $X_i^1, \dots, X_i^{n(i)}$ of Π_i the blocks of this partition. A function ϕ: $X_1 \to X_2 \cup \{0\}$ is said to 0-*inject* Π_1 into Π_2 if ϕ induces a well defined injective map from the set of Π_1-blocks X_1^j for which $\phi(X_1^j) \neq 0$ to the set of Π_2-blocks.

THEOREM 8 [22]. *If* $\mathrm{Mat}_l^G(S)\mathbf{c} \geq 1$, *then the following hold*:

1. *There exists a relational morphism* (θ, ϕ): $(B^0, \mathrm{Mat}_l^G(S)) \to (Y, T)$, *such that* $\phi^{-1}(T) = \mathrm{Mat}_l^G(S)$ *and* $\theta^{-1}(Y) = B^0$.
2. (Y, T) *is a faithful transformation semigroup.*
3. *For each* $y \in Y$ *there exists a partition* Π_y *of* $\theta^{-1}(y)$ *with the property*: *If* $s\phi t$, *then* $\cdot s$: $\theta^{-1}(y) \to \theta^{-1}(y \cdot t)$ *is a* 0-*injection of the partition* Π_y *into* $\Pi_{y \cdot t}$.
4. *Denote the equivalence classes of* Π_y *by* $X_y^1, \dots, X_y^{k(y)}$. *Each* Π_y *has a family of cross sections* $[\partial_y^i]$ *with* $\sigma[\partial_y^i] = X_y^i$ *such that whenever* $s\phi t$ *and* $X_y^i \cdot s \neq 0$, *then* s *maps* $[\partial_y^i]$ *into* $[\partial_{y\cdot t}^j]$, *where* $X_y^i \cdot s \subseteq X_{y\cdot t}^j \cup \{0\}$.
5. $T\mathbf{c} < \mathrm{Mat}_l^G(S)\mathbf{c}$.

Statements 1, 2, 3, 4 are said to constitute a *presentation of* $\mathrm{Mat}_l^G(S)$ *of degree* $T\mathbf{c}$. There is also a converse of this result. For $s \in \mathrm{Mat}^G(S)$ let $\bar{s}$ be the matrix with all nonzero entries replaced by the identity of G. Let $\mathrm{diag}(s) = \mathrm{diag}(s_1, \dots, s_l)$ be the diagonal matrix, with all zero entries replaced by the identity of G. Then $s = \mathrm{diag}(s)\bar{s}$ and $s \mapsto \bar{s}$ is a homomorphism. On denoting the image by $\mathrm{Mat}^1(S)$, we arrive at the transformation semigroup $(B, \mathrm{Mat}^1(S))$.

THEOREM 9 [22]. *If* $\mathrm{Mat}_l^G(S)$ *has a presentation of degree* d *and* $\mathrm{Mat}_l^1(S)\mathbf{c} \leq n$, *then*

$$\mathrm{Mat}_l^G(S)\mathbf{c} \leq \max\{n, d+1\}.$$

If in addition $d < \mathrm{Mat}_l^G(S)\mathbf{c}$ *and* $\mathrm{Mat}_l^1(S)\mathbf{c} = n$, *then*

$$\mathrm{Mat}_l^G(S)\mathbf{c} = \max\{n, d+1\}.$$

The previous two results are jointly referred to as the presentation lemma.

LEMMA 8 [22]. *Let* $\mathrm{Mat}_l^G(S)$ *have a presentation given by a relational morphism*

$$(\theta, \phi): \left(B^0, \mathrm{Mat}_l^G(S)\right) \to (Y, T)$$

with partitions and cross sections as in the presentation lemma. Then:

1. *Given a cross section* $[\partial]$ *with support containing some* b *and* b_0 *which are attached, there is an* $a_0 \in A(J_0)$ *such that* $\partial(b) = \langle b, a_0 \rangle \partial(b_0) \langle b_0, a_0 \rangle$.
2. *For any* $D \subseteq B$ *for which all elements of* D *are transitively attached with respect to* D, *there is at most one cross section* $[\partial]$ *with support* D.
3. *If* $\theta^{-1}(y) - \{0\} \subseteq B$, *then the partition* Π_y*-blocks* X_y^i *are unions of the equivalence classes* D_j *which are transitively attached with respect to* $\theta^{-1}(y) - \{0\}$. *Each* D_j *is transitively attached with respect to itself, and the cross section* $[\partial_j^i]$ *with support* X_y^i *has an aspect on each* $D_j \subseteq X_y^i$, *determined as in* 2.

6.1. *Some Bounds*

We now derive some standard bounds for $\mathrm{Mat}^G(S)\mathbf{c}$.

The 0-minimal $\mathcal{J}$-class of $\mathrm{Mat}^1(S)$ is combinatorial. By Lemma 2.8 of [22] a minimal length decomposition of $\mathrm{Mat}^1(S)$ is of the form $A_n \ltimes G_n \ltimes \cdots \ltimes A_0$ with A_n nontrivial. We can now state:

THEOREM 10. *The map* $s \mapsto (\mathrm{diag}(s), s)$ *is an embedding of* $\mathrm{Mat}^G(S)$ *in* $G \ltimes \mathrm{Mat}^1(S)$ *and*

$$\mathrm{Mat}^1(S)\mathbf{c} \le \mathrm{Mat}^G(S)\mathbf{c} \le 1 + \mathrm{Mat}^1(S)\mathbf{c}.$$

As always, Tilson's theorem will prove to be indispensible.

THEOREM 11 (Tilson [29]). *The complexity of a semigroup with at most two* $\mathcal{J}$*-classes is decidable*.

Since the 0-minimal $\mathcal{J}$-class of $\mathrm{Mat}^1(S)$ is combinatorial, we can apply the fundamental lemma of complexity [9] to arrive at:

COROLLARY 2. *The complexity of* $\mathrm{Mat}^1(S)$ *is decidable, and if* $\mathrm{Mat}^1(S)\mathbf{c} = 2$, *then* $\mathrm{Mat}^G(S)\mathbf{c} \ge 2$.

7. DECIDABILITY FOR COMPLETE CONTENTS

For the sake of clarity, we first show that complexity 1 is decidable for those semigroups in which every upper content is complete. We shall construct a combinatorial monoid (Y, C) (control monoid), which will allow us to bound a Turing machine testing for possible presentations for $\mathrm{Mat}^G(S)$. We propose to take each element $s \in \mathrm{Mat}^G(S)$ and construct a new matrix. We first form copies of the set Max, one for each $B(K)_i$, and denote them by Max^i. The control monoid will consist of matrices whose rows and columns are divided into 3-blocks. The first block will be labelled by elements of $\mathrm{Max}^1, \dots, \mathrm{Max}^{o(K)}$; the second block will be labelled by the $\overline{B}(K)_m$, $m = 1, \dots, \bar{o}(K)$; finally, the third block will be labelled by $*_0$. We now construct a relational morphism. For $k \in K$ we define $\phi(k) =$ identity matrix. For $a \otimes hb \in J_1$ with $b \in B(K)_j$, we define $\phi(a \otimes hb)$ to be nonzero only in the columns in $\{\mathrm{Max}^j\}$, and the first block will be

$$
\begin{array}{c}
\\
\{\mathrm{Max}^j\} \\
\vdots \\
\{\mathrm{Max}^{o(K)}\} \\
\\
\end{array}
\begin{array}{c}
\begin{array}{cccc} \cdots & \{\mathrm{Max}^j\} & \cdots & \{\mathrm{Max}^{o(K)}\} \end{array} \\
\left(\begin{array}{cccc}
 & I & & \\
 & I & & \\
 & & & \\
 & I & & \\
 & I & &
\end{array}\right)
\end{array},
$$

where I is the $|\mathrm{Max}| \times |\mathrm{Max}|$ identity matrix.

For $i = 1, \dots, \bar{o}(K)$ the $\overline{B}(K)_i \times \{\mathrm{Max}^j\}$ block will be a fixed constant function on one of the elements of M Ran which contains $\mathrm{Ran}(i, l)$, where $a \in (K)A_l$. Finally, the $(*_0, *_0)$ entry will be 1. For $s \in J_0$ with the right-hand coordinate of s in $P_i B(K)_j$, we define $\phi(s)$ to be the set of constant functions on all chains in Max^j ending in P_i and a 1 in the $(*_0, *_0)$ position. We also define

$$\theta \colon B \to Y = \bigcup_{j=1}^{o(K)} \{\mathrm{Max}^j\} \cup \bigcup_{i=1}^{\bar{o}(K)} \overline{B}(K)_i \cup \{*_0\},$$

$$\theta(b) = \begin{cases} \overline{B}(K)_j \cup \{*_0\}, & \text{if } b \in \overline{B}(K)_j, \\ \mathrm{Max}(P_i)^j \cup \{*_0\}, & \text{if } b \in P_i B(K)_j, \\ Y, & \text{if } b = 0. \end{cases}$$

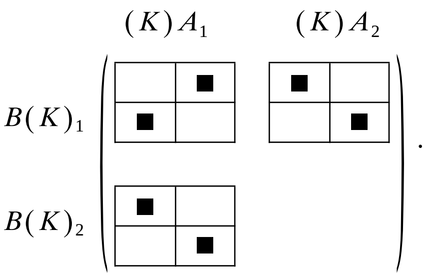
It is now easy to check that (θ, ϕ) is a relational morphism. Suppose then that $S\mathbf{c} = 1$. Then by the presentation lemma there exists a presentation of degree 0. However, the inverse image of any point under θ is pointlike and so restricting the partitions and cross sections for the original presentation yields partitions and cross sections for (θ, ϕ). It follows that if $S\mathbf{c} = 1$, then S has a presentation of degree 0 with

$$(\theta, \phi): (B, S) \to (Y, C).$$

So to decide whether or not $S\mathbf{c} = 1$, it suffices to check all possible combinations of partitions and cross sections for (θ, ϕ), and determine whether or not they give a presentation for S.

8. NONCOMPLETE CONTENTS

Our immediate problem is to deal with the following example of matrix of contents.



If we define (Y, C) as before, then we see that C is noncombinatorial and our decision procedure no longer allows us to decide the complexity of S. To remedy this situation we proceed as follows: Given a noncomplete content, we partition its rows and columns into blocks labelled by $P_1, \ldots, P_n$. We say that the content $B(K)_1 \times (K)A_1$ contains a permutation pair (P_1, P_2) if the content has the form

	P_1	P_2
P_1		■
P_2	■	

.

Let $P_1 = \{B(H)_1, \ldots, B(H)_{1_n}\}$ and $P_2 = \{B(H)_{2_1}, \ldots, B(H)_{2_m}\}$ and suppose

	2_1	$\cdots$	2_j	$\cdots$	2_m
1_1					
1_i			■		
1_n					

	1_1	$\cdots$	$1_{j'}$	$\cdots$	1_n
2_1					
$2_{i'}$			■		
2_m					

.

Since P_2 is a partition block, there exists a calculation chain

$$\left[B(H)_{2_j}, \ldots, B(H)2_{i'}\right],$$

which contains all elements of P_2. Also, P_1 is a partition block and so there exists a calculation chain

$$\left[B(H)_{1_{j'}}, \ldots, B(H)_{1_i}\right],$$

which contains all elements of P_1. Let (θ, ϕ): $(B, S) \to (Y, A)$ be a relational morphism, with A combinatorial. Associated with each of the preceding calculation chains, there is a sequence of complete contents and these in turn, respectively, give rise to elements $s_1, \ldots, s_l$ and $t_1, \ldots, t_{l'}$ of A. Let $b' \in B(K)_1$ and $a' \in (K)A_1$, and choose $a \in \phi(a')$ and $b \in \phi(b')$. Then $as_1 \cdots s_l t_1 \cdots t_{l'} b \in A$, but A is combinatorial and so there exists a p such that

$$(as_1 \cdots s_l t_1 \cdots t_{l'} b)^p = (as_1 \cdots s_l t_1 \cdots t_{l'} b)^{p+1}.$$

Also, $P_1 B(K)_1$ is pointlike. Let $P_1 B(K)_1 \subseteq \theta^{-1}(y)$. It is easy to see that

$$\bigcup_{i=1}^{2} P_i B(K)_1 \subseteq \theta^{-1}\left(y(as_1 \cdots s_l t_1 \cdots t_{l'} b)^p\right).$$

Moreover, every row of contents contains a complete content, and it follows that $\bigcup_{i=1}^{2} P_i B(K)_j$ is pointlike for all $j = 1, \ldots, o(K)$.

Now suppose the $B(K)_1 \times (K)A_1$ content has the form

	P_1	P_2	P_3
P_1		■	■
P_2	■		

.

Let $P_3 = \{B(H)_{3_1}, \dots, B(H)_{3_{n'}}\}$ and suppose that the $P_1 \times P_3$ block is of the form

	3_1	$\cdots$	$3_{j''}$	$\cdots$	$3_{n'}$
1_1					
$1_{i''}$			■		
1_n					

.

Since P_3 is a partition block, there exists a chain $[B(H)_{3_{j''}}, \dots]$ which contains all elements of P_3. This chain gives rise to a sequence of complete contents which in turn give rise to elements $u_1, \dots, u_{l''}$ of A. Also $\bigcup_{i=1}^{2} P_i B(K)_1$ is pointlike and so is contained in $\theta^{-1}(y)$ for some $y \in Y$. It is then easy to see that

$$\bigcup_{i=1}^{3} P_i B(K)_1 \subseteq \theta^{-1}(yas_1 \cdots s_l t_1 \cdots t_{l'} u_1 \cdots u_{l''} b).$$

Again, we find that $\bigcup_{i=1}^{3} P_i B(K)_j$ is pointlike for all $j = 1, \dots, o(K)$.

Given $P_1, \dots, P_m$, we define $\mathrm{Ran}(P_1, \dots, P_m)$ as the set of those columns which contain a nonzero block, for rows $P_1, \dots, P_m$. Let

$$\mathrm{Ran}^2(P_1, \dots, P_m) = \mathrm{Ran}\big(\mathrm{Ran}(P_1, \dots, P_m)\big).$$

It is easy to establish that if (P_1, P_2) is a permutation pair, then there exists an n such that

$$\mathrm{Ran}^n(P_1, P_2) = \mathrm{Ran}^{n+1}(P_1, P_2),$$

and $\mathrm{Ran}^n(P_1, P_2)B(K)_j$ is pointlike for all $j = 1, \dots, o(K)$. Finally, suppose that (P_1, P_2) and (P_3, P_4) are permutation pairs in the same content, and $\mathrm{Ran}^{m'}(P_3, P_4) = \mathrm{Ran}^{m'+1}(P_3, P_4)$. Then exactly one of the following holds:

$$\mathrm{Ran}^{n}(P_1, P_2) \subseteq \mathrm{Ran}^{m'}(P_3, P_4),$$

$$\mathrm{Ran}^{m'}(P_3, P_4) \subseteq \mathrm{Ran}^{n}(P_1, P_2),$$

$$\{P_1, P_2\} \cap \mathrm{Ran}^{m'}(P_3, P_4) = \varnothing \quad \text{and} \quad \{P_3, P_4\} \cap \mathrm{Ran}^{n}(P_1, P_2) = \varnothing.$$

Thus, the content after computing the limit of ranges must have the form

	P_1	P_2		$\cdots$	P_3	P_4		$\cdots$	P_5	P_6		$\cdots$
P_1	$\ast$	$\blacksquare$	$\ast$	$\ast$	0	0	0	0	0	0	0	0
P_2	$\blacksquare$	$\ast$	$\ast$	$\ast$	0	0	0	0	0	0	0	0
	$\ast$	$\ast$	$\ast$	$\ast$	0	0	0	0	0	0	0	0
	$\ast$	$\ast$	$\ast$	$\ast$	0	0	0	0	0	0	0	0
P_3	0	0	$\ast$	$\ast$	$\ast$	$\blacksquare$	$\ast$	$\ast$	0	0	0	0
P_4	0	0	$\ast$	$\ast$	$\blacksquare$	$\ast$	$\ast$	$\ast$	0	0	0	0
	0	0	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	0	0	0	0
	0	0	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	$\ast$	0	0	0	0
P_5	0	0	$\ast$	$\ast$	0	0	$\ast$	$\ast$	$\ast$	$\blacksquare$	$\ast$	0
P_6	0	0	$\ast$	$\ast$	0	0	$\ast$	$\ast$	$\blacksquare$	$\ast$	$\ast$	0

,

where the $\ast$-blocks may be 0 or $\blacksquare$. We can now compute ranges over all noncomplete contents, pick the maximal pointlikes, and then extend the set Max as before. However, due to the preceding separation of permutation pairs, we can again construct a combinatorial monoid (Y, C) and check if S has a presentation with (Y, C).

ACKNOWLEDGMENTS

I am grateful to J. C. Birget for numerous conversations on the Rhodes expansion and indebted to J. Rhodes for introducing me to the presentation lemma. Finally, I would like to thank A. Pacheco for her careful editing and proofreading of the manuscript.

REFERENCES

1. D. Abreu and A. Rubinstein, The structure of Nash equilibrium in repeated games with finite automata, *Econometrica* **56** (1988), 1259–1281.
2. M. A. Arbib, (Ed.), "Algebraic Theory of Machines, Languages and Semigroups," Academic Press, New York, 1968.

3. K. G. Binmore and L. Samuelson, Evolutionary stability in repeated games played by finite automata, *J. Econom. Theory* **57** (1992), 278–305.
4. R. J. Aumann, Survey of repeated games, *in* "Essays in Game Theory and Mathematical Economics in Honour of Oskar Morgenstern," pp. 11–42, Bibliograph. Inst. Zurich, 1981.
5. J. C. Birget, Iteration of expansions, unambiguous semigroups, *J. Pure Appl. Algebra* **34** (1984), 1–55.
6. J. C. Birget, Arbitrary vs. regular semigroups, *J. Pure Appl. Algebra* **34** (1984), 56–115.
7. J. C. Birget, The synthesis theorem for finite regular semigroups, and its generalization, *J. Pure Appl. Algebra* **55** (1988), 1–79.
8. R. Dawkins, "The Selfish Gene," Oxford University Press, London, 1989.
9. S. Eilenberg, "Automata, Languages, and Machines," Vol. B, Academic Press, New York, 1976.
10. C. Futia, The complexity of economic decision rules, *J. Math. Econom.* **4** (1977), 289–299.
11. M. Hartshorn and S. Talwar, The automatic dilemma, preprint.
12. N. Jacobson, "Basic Algebra 2," W. H. Freeman, San Francisco, 1980.
13. E. Kalai and W. Stanford, Finite rationality and interpersonal complexity in repeated games, *Econometrica* **56** (1988), 397–410.
14. K. Krohn and J. Rhodes, Algebraic theory of machines, I, *Trans. Amer. Math. Soc.* **116** (1965), 450–464.
15. K. Krohn and J. Rhodes, Complexity of finite semigroups, *Ann. of Math.* **88** (1968), 128–160.
16. S. Margolis, private communication.
17. A. Neyman, Cooperation, repetition and automata, Discussion paper 88, Centre for Rationality and Interactive Decision Theory, Israel.
18. M. A. Nowak and K. Sigmund, A strategy of win–stay, lose–shift that outperforms tit-for-tat in the Prisoner's Dilemma game, *Nature*, **364** (1992), 56–58.
19. M. A. Nowak, K. Sigmund, and E. El-Sedy, Automata, repeated games and Noise, *J. Math. Biol.* **33** (1995), 703–722.
20. C. Papadimitriou, On players with a bounded number of states, *Games Econom. Behavior* **4** (1992), 122–131.
21. J.-E. Pin, "Varieties of Formal Languages," North Oxford Academic Publishers, Oxford, 1986.
22. J. Rhodes, B. Austin, K. Henckell, C. Nehaniv, and J. Rhodes, Subsemigroups and complexity via the presentation lemma, preprint.
23. J. Rhodes, Applications of automata theory and algebra, Department of Mathematics, University of California, Berkeley.
24. K. Sigmund, "Games of Life," Penguin Books, Baltimore, 1995.
25. A. Rubinstein, Finite automata play the repeated prisoner's dilemma, *J. Econom. Theory* **39** (1986), 83–96.
26. S. Talwar, Strong Morita equivalence and a generalisation of the Rees theorem, *J. Algebra* **181** (1996), 371–394.
27. S. Talwar, Strong Morita equivalence and the synthesis theorem, *Int. J. Algebra and Computation* **6** (1996), 123–141.
28. S. Talwar, Krohn–Rhodes: The Prisoner's Dilemma and synchronocity, submitted for publication.
29. B. Tilson, Complexity of two J-class semigroups, *Adv. in Math.* **11** (1973), 215–237.
30. H. P. Zeiger, Cascade synthesis of finite state machines, *Inform. and Control* **10** (1967), 419–433.