Efficient exhaustive listings of reversible one dimensional cellular automata

Tim Boykett*

Time's Up Research Department,
Industriezeile 33b, A-4020 Linz, Austria
and
Department of Algebra, Johannes Kepler Universität,
A-4040 Linz, Austria

This paper looks at an algebraic formulation of one dimensional cellular automata. Using the formulation, certain properties become apparent and connections to combinatorial structures and graph theory become clear. Strong results about uniqueness and isomorphism allows us to outline effective algorithms for the generation of exhaustive lists of reversible one dimensional cellular automata, and to count the number of distinct examples that exist.

1. Introduction

This paper looks at closely related algebraic, combinatoric, graph theoretical and matrix theoretical interpretations of one dimensional cellular automata and describes an algorithm for the efficient enumeration of examples. The technique of using the various equivalent models of the structures leads to some interesting insights. The strength of connections also allows us to move theorem proving to the model where the proofs are most clear. One of the problematic aspects of cellular automata research is the unwieldy language. The approach used here, where we quickly move away from traditional cellular automata language allows us to use tools that exist in the algebraic, combinatorial and graph theoretic contexts to obtain clearer results.

Several connections between computational theory and algebraic theory exist. One of the aims of looking at reversible computation, that is, computations where the question can be derived from the answer, or better said, where no information is lost, is that there is (significant) extra structure involved. This structure is comparable to the differences between semigroups of transformations and groups where the transformations are invertible. This added structure allows the re-

*Email: tim@timesup.org

searcher to say more about the structures than would be possible in the non reversible case. That reversibility is no restriction on computational power has been amply demonstrated by such papers as [1].

The paper begins by looking at an algebraic structure, semicentral bigroupoids, related to the central groupoids investigated in the late 1960s and early 1970s. We show that semicentral bigroupoids can be represented as a permutation and an idempotent semicentral bigroupoid. We then describe a coordinatisation of this algebraic structure, and then derive an interesting combinatorial object. The following sections show that the combinatorial object is directly equivalent to an idempotent semicentral bigroupoid.

We break to show that semicentral bigroupoids are equivalent to reversible one dimensional cellular automata using the technique of Pedersen [25]. This section forms the bridge to cellular automata theory, and emphasises that the algebraic tools that become available through this connection are of value.

A further model of the algebraic and combinatorial structure as a pair of matrices or graphs is introduced and shown to be equivalent. We then look at isomorphism between semicentral bigroupoids, determining exactly when two semicentral bigroupoids are isomorphic and develop techniques for counting the number of distinct semicentral bigroupoids that can be lifted from a given idempotent semicentral bigroupoid. Then we look at a technique of building semicentral bigroupoids piece by piece, showing that we can generate all examples using this technique. More importantly, using the uniqueness results, and borrowing the ideas of orderly algorithms from e.g. [29], we look at an algorithm for the exhaustive generation of rectangular structures. Using the results on isomorphism we can then calculate the number of distinct semicentral bigroupoids and thus cellular automata rules that can be derived from that structure.

We finish off by looking at some further questions that remain unanswered, looking to possible future developments.

This paper summarises the work that formed the body of my thesis [2].

2. Central Groupoids

The structures have been first seen in a more refined form in the late sixties, as the central groupoids of Evans and Knuth [6, 12].

Let's follow the development. Evan's work started with [6] where he investigated the various products that could be defined on the set $S = A \times A$ for some set A. A well–known example of such a construction is the rectangular semigroup [20], where one takes a pair of sets A, B, forms the product $S = A \times B$ and the product $(a, b) * (c, d) = (a, d)$. It is quite easy to show that this is an idempotent semigroup satisfying the axiom $a * b * a = a$ for all $a, b \in S$, and every semigroup satisfying this equation is of this form.

Evans looked at all the possible products on $S = A \times A$, and found that other than the rectangular semigroups, the only other interesting examples were defined by

$$(a, b) \bullet (c, d) = (b, c). \tag{1}$$

This operation satisfies an interesting equation $(a \bullet b) \bullet (b \bullet c) = b$.

Definition 1. A *Central Groupoid* is a (2)-algebra $(S, \bullet)$ satisfying the axiom:

$$(a \bullet b) \bullet (b \bullet c) = b \tag{2}$$

The examples used by Evans are referred to as the *natural* central groupoids, as they were the first to be noted. All natural central groupoids have, by construction, order equal to a square. Surprisingly, this carries across to the general case.

If we take A to be $\{a, b\}$, then look at the multiplication table, writing ab for the ordered pair (a, b) we note some interesting things.

$\bullet$	aa	ab	ba	bb
aa	aa	aa	ab	ab
ab	ba	ba	bb	bb
ba	aa	aa	ab	ab
bb	ba	ba	bb	bb

(3)

We see that two elements are idempotent. In general, in a natural central groupoid, we will see that $(a, b) \bullet (a, b) = (a, b)$ iff $a = b$, thus we have $|A|$ idempotents in a natural central groupoid of order $|A|^2$. This is also a general result for central groupoids.

Theorem 1 (Evans, Knuth) *If $(S, \circ)$ is a finite central groupoid, then $|S| = n^2$ for some integer n. For every positive integer n there exists a central groupoid of order n^2. In any finite central groupoid of order n^2, the number of idempotents is n.*

Note that the first result appears as Corollary 17, the second follows from the example above. The third result is very difficult to show in an algebraic setting, we need to move over to a matrix theoretic setting in order to prove it, see [12].

Later, in [12], Knuth investigated various aspects of central groupoids. He showed, for instance, that the natural central groupoids can be defined by a single axiom ([12, Theorem 5]):

$$(a \bullet ((b \bullet c) \bullet d)) \bullet (c \bullet d) = c \tag{4}$$

so we know that any groupoid satisfying this axiom is a natural central groupoid.

Most importantly, Knuth's work found two models for central groupoids, one being a digraph model, the other being a model based upon the $\{0,1\}$–matrices that are the incidence matrices of these digraphs. The incidence matrices made an interesting contribution to a question posed by Hoffman in [10]: which $\{0,1\}$–matrices A have the property that $A^2 = J$, where J is the matrix consisting entirely of ones?

In [31] Shader demonstrates that non–natural central groupoids exists for all orders n^2, $n \geq 3$. The question of an exhaustive list of central groupoids, or equivalently an exhaustive list of matrices A with $A^2 = J$, is still open.

The result about idempotents fails in the infinite case, Evans has shown (presented in [12]) that the free central groupoid on any number of generators contains no idempotents.

Later we will see that many results about central groupoids can be shown as corollaries of our work, also we will see that central groupoids form a useful class of examples, counter examples and special cases for consideration.

3. A Generalisation

In this section I introduce the algebraic structure that we will be concerned with for this paper. First we will look at some basic results, and build up some machinery. In particular the *lifting* operation introduced in this section plays an important role in later developments, as do the partitions introduced in Section 3.4.

Historically, these structures evolved from looking at reversible cellular automata. Here we look at them purely as algebraic objects, therefore we cannot give some nice starting point as we had in the central groupoids, rather we view them simply as generalisations of central groupoids. This is, incidentally, the reason for the name.

3.1 Definition and Simple Results

Definition 2. A *Semicentral Bigroupoid* is a $(2,2)$-algebra $(S,\bullet,\circ)$ satisfying the following axioms:

$$(a \bullet b) \circ (b \bullet c) = b \tag{5}$$

$$(a \circ b) \bullet (b \circ c) = b \tag{6}$$

If $(S,\bullet)$ is a central groupoid, then $(S,\bullet,\bullet)$ is a semicentral bigroupoid, so this is a proper generalisation.

Note also that the definition is completely symmetric in $\bullet$ and $\circ$, i.e. $(S,\circ,\bullet)$ is a semicentral bigroupoid iff $(S,\bullet,\circ)$ is. The *dual* of a semicentral bigroupoid $(S,\bullet,\circ)$ is $(S,\circ,\bullet)$. Thus it is often not necessary to prove results for both operations, as they carry across by duality.

Any set S can be seen as a semicentral groupoid by taking

$$a \bullet b = a, a \circ b = b. \tag{7}$$

This is a trivial semicentral bigroupoid, the $\bullet$–left–constant semicentral bigroupoid on a set S.

Example 2. Let A,B be two sets, and let $Q = A \times B$. Define

$$(a_1, b_1) \bullet (a_2, b_2) = (a_1, b_2) \tag{8}$$

$$(a_1, b_1) \circ (a_2, b_2) = (a_2, b_1) \tag{9}$$

Then $(Q, \bullet, \circ)$ is a semicentral bigroupoid.

In the above, $(Q, \bullet)$ defines a rectangular semigroup. In some sense this is the case that corresponds to the natural central groupoids, in that it can be constructed as a "product of points". This is correlated by the lifting operation, see Lemma 7. In Section 3.3 we will see that it is the only associative semicentral bigroupoid.

Some interesting properties of rectangular semigroups carry across to semicentral bigroupoids. For instance, rectangular semigroups are anti–commutative, i.e. $ab = ba \Leftrightarrow a = b$, which can be shown by calculation.

Lemma 3. If $(S, \bullet, \circ)$ is a semicentral bigroupoid then both the operations are anti-commutative, that is, $a \bullet b = b \bullet a \Rightarrow a = b$ and similarly for $\circ$.

Now to look at some other "usual" abstract algebraic properties, in this case the existence of identities.

Lemma 4. There exists some $1 \in S$ such that $1 \bullet x = x$ for all x, iff $x \bullet y = y$ for all y and $x \circ y = x$ for all x.

This follows by calculation. This result restricts our choice of operations for our algebra. For instance, now we cannot use groups or monoid structures, not even loops for either of the operations.

Other standard algebraic properties such as idempotence can apply, but have certain properties.

Lemma 5. Let $(S, \bullet, \circ)$ be a semicentral bigroupoid. Then $a \bullet a = a$ iff $a \circ a = a$. Thus $(S, \bullet)$ is idempotent iff $(S, \circ)$ is idempotent.

This result also follows by direct calculation. In the following, we will often omit $\bullet$ and represent the operation by juxtaposition.

3.2 Liftings

We can take any semicentral bigroupoid and "bend" it a little to get another semicentral bigroupoid. This method can be used to find new examples of semicentral bigroupoids.

Proposition 6. If $(S, \bullet, \circ)$ is a semicentral bigroupoid, and $\phi : S \to S$ is a permutation of S, then the algebra $(S, *, +)$ with

$$a * b = \phi^{-1}(a) \bullet \phi^{-1}(b) \tag{10}$$

and

$$a + b = \phi(a \circ b) \tag{11}$$

is also a semicentral bigroupoid.

The calculation behind this result is mechanical. Note that the new semicentral bigroupoid will in general not be isomorphic to the old one. This can be made rigorous; see Section 7 on uniqueness, in particular Lemma 29.

Definition 3. The *lifting* of $(S, \bullet, \circ)$ by ϕ is the algebra $(S, *, +)$ defined above. The *square map* $\phi_\bullet$ of $(S, \bullet, \circ)$ is $\phi_\bullet : x \mapsto x \bullet x$

The square map, $\phi_\bullet : a \mapsto aa$ is a permutation:

$$\phi_\bullet(a) = \phi_\bullet(b) \tag{12}$$
$$\Rightarrow a \bullet a = b \bullet b \tag{13}$$
$$\Rightarrow (a \bullet a) \circ (a \bullet a) = (b \bullet b) \circ (b \bullet b) \tag{14}$$
$$\Rightarrow a = b \tag{15}$$

Note that if we lift by the square map then the derived operation $*$ is idempotent:

$$a * a = \phi_\bullet^{-1}(a \bullet a) = \phi_\bullet^{-1}\phi_\bullet(a) = a. \tag{16}$$

This will be referred to as the *idempotent lifting* of a semicentral bigroupoid.

Let's apply this to a central groupoid. As mentioned beforehand, if $(S, \bullet)$ is a central groupoid, then $(S, \bullet, \bullet)$ is a semicentral bigroupoid. Take the example of the natural central groupoid of order 4 defined in (3). The square map is the permutation $\sigma = (ab\ ba)$. This is the permutation that reverses the entries in the product, i.e. $\sigma : xy \mapsto yx$. If we construct the multiplication tables for the lifting by σ, then we obtain the following:

*	aa	ab	ba	bb
aa	aa	ab	aa	ab
ab	aa	ab	aa	ab
ba	ba	bb	ba	bb
bb	ba	bb	ba	bb

+	aa	ab	ba	bb
aa	aa	aa	ba	ba
ab	ab	ab	bb	bb
ba	aa	aa	ba	ba
bb	ab	ab	bb	bb

(17)

We see that this lifting is an idempotent semicentral bigroupoid, in fact an associative one.

In general one can make the following statement.

Lemma 7. The idempotent lifting of a natural central groupoid is an associative semicentral bigroupoid.

Proof: This result follows as a result of some simple calculations. Let $(S, \bullet)$ be the natural central groupoid on the set A. Considering S as a semicentral bigroupoid $(S, \bullet, \bullet)$, we have the square map $\sigma : (a, b) \mapsto (a, b) \bullet (a, b) = (b, a)$. Then

$$
\begin{aligned}
((a,b) * (c,d)) * (e,f) &= ((b,a) \bullet (d,c)) * (e,f) && (18)\\
&= (a,d) * (e,f) && (19)\\
&= (d,a) \bullet (f,e) && (20)\\
&= (a,f) && (21)\\
(a,b) * ((c,d) * (e,f)) &= (a,b) * ((d,c) \bullet (f,e)) && (22)\\
&= (a,b) * (c,f) && (23)\\
&= (b,a) \bullet (f,c) && (24)\\
&= (a,f) && (25)
\end{aligned}
$$

So the associativity identity holds in $(S, *)$ a similar argument shows that it holds in $(S, +)$.

□

We will look more at associative semicentral bigroupoids in the next section, in a very strong sense they play the equivalent role to the natural central groupoids.

Since the lifting map is a permutation, we can take its inverse $\varphi = \phi_\bullet^{-1}$ and find that the lifting via φ of the idempotent lifting of $(S, \bullet, \circ)$ is isomorphic to $(S, \bullet, \circ)$.

Let $(S, *, +)$ be the idempotent lifting of $(S, \bullet, \circ)$, and let $(S, \cdot, \times)$ be the lifting of $(S, *, +)$ by φ. Then

$$
\begin{aligned}
a \cdot b &= \varphi^{-1}(a) * \varphi^{-1}(b) && (26)\\
&= \phi_\bullet^{-1}\varphi^{-1}(a) \bullet \phi_\bullet^{-1}\varphi^{-1}(b) && (27)\\
&= a \bullet b && (28)
\end{aligned}
$$

and similarly $a \times b = a \circ b$.

Thus we see that the lifting operation is invertible (a similar argument shows this for any lifting and its inverse), and we see that every semicentral bigroupoid is the lifting of an idempotent semicentral bigroupoid by a permutation that becomes the inverse of the square map in the lifting.

That we can have any permutation as the square map in a semicentral bigroupoid, and thus any number of idempotents, is a contrast to the case for a central groupoid, where there are exactly $\sqrt{|S|}$ idempotents for S finite.

We see the following.

Proposition 8. Every semicentral bigroupoid $(S,\bullet,\circ)$ can be uniquley represented as an idempotent semicentral bigroupoid and a permutation in $Symm(S)$. Conversely, every such pair gives a semicentral bigroupoid that is idempotent iff the permutation is trivial.

In Proposition 28 we will see exactly when two semicentral bigroupoids are isomorphic, based upon the isomorphism of their idempotent representatives and relations between their square maps.

There is a *dual lifting*. Given a semicentral bigroupoid$(S,\bullet,\circ)$ and a permutation ϕ, define $(S,*,+)$ with

$$a * b = \phi^{-1}(a \bullet b) \tag{29}$$

$$a + b = \phi a \ \circ \ \phi b \tag{30}$$

All the statements about liftings carry across for the dual lifting. On occasion this version is better to discuss details. Note that the dual lifting of a semicentral bigroupoid S by ϕ is the dual of the lifting by ϕ^{-1} of the dual of S.

But we find that, in another sense, all the liftings are equivalent. In the study of quasigroupoid and other general algebraic structures, a more general idea of equivalence is found to be relevant. This is the concept of *isotropism* [26].

Definition 4. Two groupoids $(A,*)$ and $(B,\circ)$ are called *isotropic* if there are three bijections $f,g,h : A \to B$ such that

$$f(a) \circ g(b) = h(a * b) \tag{31}$$

for all $a,b \in A$.

Isomorphism is a special case of isotropism. The lifting operation is also an isotropism. We know that there are two nonisomorphic idempotent semicentral bigroupoids that are isotropic of order 6, so isotropism classes are larger than lifting classes.

We will focus upon idempotent semicentral bigroupoids for now.

3.3 Associative Semicentral Bigroupoids

Before we go too much further, it would be useful to look at the most accessible class of semicentral bigroupoids, namely those that are associative. I say these are accessible since most abstract algebra deals with operations that are associative.

In Lemma 3 above, we saw that the operations in a semicentral bigroupoid are anticommutative. In [20], McLean shows that the only anticommutative semigroups are the rectangular semigroups.

Thus if we start out with one of the semicentral bigroupoid operations, say $\bullet$, associative, we know that $(S,\bullet)$ is a rectangular semigroup.

Thus there are two sets A, B and an operation $*$ on $A \times B$,

$$(a_1, b_1) * (a_2, b_2) = (a_1, b_2) \tag{32}$$

such that $(S, \bullet)$ is isomorphic to $(A \times B, *)$. Thus the $\circ$ operation can be extended to $A \times B$, and we can say

$$\begin{aligned}(a_1, b_1) \circ (a_2, b_2) &= ((a_1, b_3) * (a_2, b_1)) \circ ((a_2, b_1) * (a_3, b_2)) &(33)\\ &= (a_2, b_1) &(34)\end{aligned}$$

giving us a description of all associative semicentral bigroupoids:

Lemma 9. All associative semicentral bigroupoids $(S, \bullet, \circ)$ are defined by two sets A, B with

$$\begin{aligned}S &= A \times B &(35)\\ (a_1, b_1) \bullet (a_2, b_2) &= (a_1, b_2) &(36)\\ (a_1, b_1) \circ (a_2, b_2) &= (a_2, b_1) &(37)\end{aligned}$$

3.4 Partitioning

In this section, we show that we can "coordinatise" our algebra using some term function voodoo.

Definition 5. For any $x \in S$ define

$$\begin{aligned}\mu_x : S^2 &\to S^2 &(38)\\ (a, b) &\mapsto (ax, xb) &(39)\end{aligned}$$

then

$$\begin{aligned}\rho : S &\to \mathcal{P}(S^2) &(40)\\ x &\mapsto \mu_x(S^2) &(41)\end{aligned}$$

Where $\mathcal{P}(X)$ denotes the power set of X.

Lemma 10. $\rho(S) = \{\rho(s) | s \in S\}$ is a partition of S^2.

Proof: First note that for $(ax, xb) \in \rho(x)$, $(ax) \circ (xb) = x$, so $\rho(x) \cap \rho(y) = \emptyset$ unless $x = y$. So the $\{\rho(s) | s \in S\}$ form a set of non–intersecting subsets of S^2. Then, for some $(a, b) \in S^2$, let $x = a \circ b$. Then

$$\begin{aligned}\mu_x(b \circ a, b \circ a) &= ((b \circ a) \bullet (a \circ b), (a \circ b) \bullet (b \circ a)) &(42)\\ &= (a, b) &(43)\end{aligned}$$

so $(a, b) \in \rho(x)$, thus the $\{\rho(s) | s \in S\}$ cover S^2 and form a partition. □

Lemma 11. For every $x \in S$ there exists $A, B \subseteq S$ such that

- $\rho(x) = A \times B$.
- $|A \cap B| = 1$.
- $B \circ A = S$.

Proof: $A = S \bullet x$, $B = x \bullet S$, so

$$\begin{aligned}\rho(x) &= \{(ax, xb) | a, b \in S\} && (44)\\ &= \{(ax) | a \in S\} \times \{(xb) | b \in S\} && (45)\\ &= A \times B. && (46)\end{aligned}$$

Suppose $y \in A \cap B$. Then $y = ax = xb$ for some $a, b \in S$. Thus $y \circ y = (ax) \circ (xb) = x$. Since $x \mapsto x \circ x$ is a permutation, y must be unique. Thus $|A \cap B| = 1$.

Obviously $B \circ A \subseteq S$. But $S = \{(xa) \circ (ax) | a \in S\} \subseteq B \circ A$, so $B \circ A = S$.

□

So the ρ map breaks S down into a collection of cartesian products, *rectangles*, that form a partition. The last result shows that every one of these rectangles, in some sense, holds all of S inside it.

In this way we find a coordinatisation of S in terms of a pair of trivially intersecting sets, taking some $\rho(x) = A \times B$, every element x of S can be uniquely represented as a pair (b, a) with $a \circ b = x$.

Corollary 12. Let $(S, \bullet, \circ)$ be a semicentral bigroupoid. If $a \circ b = c \circ d = x$, then $a \circ d = c \circ b = x$, and similarly for $\bullet$.

Proof: By Lemma 11 above, $\rho(x) = A \times B$, $A = Sx$, $B = xS$. Then

$$a = (a \circ a) \bullet (a \circ b) = (a \circ a) \bullet x \in Sx \quad (47)$$

similarly $c \in Sx$, $b, d \in xS$. Then $A \circ B = Sx \circ xS = \{x\}$, so

$$a \circ d \in A \circ B \Rightarrow a \circ d = x \quad (48)$$

$$c \circ b \in A \circ B \Rightarrow c \circ b = x \quad (49)$$

□

3.5 Rectangles

In the above we saw a "breakdown" of an algebraic structure into various sets. We investigate the structure of this collection of sets.

Let $\mathcal{R}^\circ = \{(Sx, xS) | x \in S\}$ be a set of ordered pairs of sets. It is the set of "rectangles" in the table of $\circ$, i.e. $\mathcal{R}^\circ = \{R^\circ_x = \{(a, b) | a \circ b = x\} | x \in S\}$.

What is the structure of this $\mathcal{R}^\circ$? First, it is a partition, so

$$\text{For all } (a, b) \in S^2\ \exists! R = (R_1, R_2) \in \mathcal{R}^\circ \text{ s.t. } a \in R_1, b \in R_2. \quad (50)$$

This follows from Lemma 10 above. Then,

$$\text{For any pair of rectangles } Q, R \in \mathcal{R}^\circ, |Q_1 \cap R_2| = 1. \tag{51}$$

To see this, note that there are some $x, y \in S$ such that $Q_1 = S \bullet x, R_2 = y \bullet S$. If $a \in Q_1 \cap R_2$, then $a = b \bullet x = y \bullet c$ for some $b, c \in S$. Then by Corollary 12 above, $a = y \bullet x$, that is, $Q_1 \cap R_2 = \{y \bullet x\}$.

So we see that an idempotent semicentral bigroupoid $(S, \bullet, \circ)$ has the structure of a set of rectangles satisfying a pair of identities (50), (51). The next section demonstrates that this process is, in some sense "reversible," i.e. given a set of such rectangles (and some permutation on the state alphabet), one obtains an idempotent semicentral bigroupoid.

4. Rectangular Structures

In this section we show that a rectangular structure as derived at the end of the last section is equivalent to an idempotent semicentral bigroupoid (Proposition 14). This helps us express and see some results about the internal structure of the multiplication table of a semicentral bigroupoid (Proposition 13), the interdependence of the two operations of a semicentral bigroupoid (Corollary 15) and shows that the first theorem of Evan's paper reduces to a simple calculation (Corollary 17).

The definition here is based directly upon the two statements (50) and (51) above.

Definition 6. A *Rectangular Structure* on a set S, called the *base set*, is a collection $\mathcal{R}$ of ordered pairs of subsets, called *rectangles*, of S, such that

$$\forall (s,t) \in S^2 \ \exists! \ R \in \mathcal{R} \text{ such that } (s,t) \in R \tag{52}$$

$$\forall R, Q \in \mathcal{R}, |R_1 \cap Q_2| = 1 \tag{53}$$

where we identify $R = (R_1, R_2) = R_1 \times R_2$.

We say two rectangular structures are *isomorphic* if there is an invertible map between the base sets that preserves rectangles.

A simple example is to take some set A, and to define the rectangles as $\{a\} \times A$ for each $a \in A$. Taking any pair $(s,t) \in S^2$, (s,t) is uniquely in the rectangle $\{s\} \times A$. For any pair of rectangles R, Q, the intersection $R_1 \cap Q_2$ is a singleton. Such a rectangular structure will be called a *Dagwood*, owing to the layered, or sandwich–like structure of it.

A somewhat more general example is the following. Take two sets A, B. Define $S = A \times B$, and for all $(a,b) \in S$ define $R_{(a,b)} = (\{a\} \times$

$B, A \times \{b\})$. Then

$$\mathcal{R} = \{R_{(a,b)} | a \in A, b \in B\} \tag{54}$$

is a rectangular structure on S. For any $((a,b),(c,d)) \in S^2$, we see that $((a,b),(c,d)) \in R_{(a,d)}$, and this is obviously unique. Let $R = R_{(a,b)}$, $Q = R_{(c,d)}$ be two rectangles in $\mathcal{R}$. Then $R_1 = \{a\} \times B$ and $Q_2 = A \times \{d\}$, so $|R_1 \cap Q_2| = |\{\{a\} \times \{d\}\}| = 1$. This is a slight generalisation of the Dagwood. Since this is a very simple construction, we will refer to it as the *vanilla* rectangular structure on A, B.

Of course, every semicentral bigroupoid gives us a rectangular structure, as demonstrated in the previous section.

The two axioms are not redundant. Consider the following simple examples. Take Π to be some partition of a set S, $|S| \geq 2$. Then the set $\mathcal{T} = \{(P,Q) | P, Q \in \Pi\}$ satisfies (52) since for every $s, t \in S$ there are unique $P, Q \in \Pi$ such that $s \in P$ and $t \in Q$, so $(s,t) \in (P,Q)$ uniquely. Equation (53) is however not satisfied. Take $P \neq Q \in \Pi$. Then $R = (P,Q) \in \mathcal{T}$ but $R_1 \cap R_2 = \emptyset$. In the case that Π has a single element P, that take $R = (P,P)$ and note that $P \cap P = P = S$ and $|S| \geq 2$ contradicts (53).

Alternatively, for some base set S with $|S| \geq 2$ and some element $a \in S$, the set $\mathcal{T} = \{\{a\},\{a\}\}$ satisfies (53) trivially, but does not satisfy (52) for $(s,t) \neq (a,a)$.

4.1 A General Structural Result

In this section I want to present a result that demonstrates that these combinatoric objects, although easily defined, have strong symmetrical structure buried within them. Though it is rather technical, the result shows that rectangular structures are very well–behaved combinatorial structures, open to considerable analysis.

The "format" of a rectangle (A, B) is the ordered pair $(|A|, |B|)$.

Proposition 13. If $\mathcal{R}$ is a rectangular structure with base set S, and $R = (R_1, R_2) \in \mathcal{R}$ is some rectangle, then $|R_1||R_2| = |S| = |\mathcal{R}|$. Moreover, for any other rectangle $Q = (Q_1, Q_2) \in \mathcal{R}$, $|R_1| = |Q_1|$, i.e. all rectangles have the same format.

Proof. Define the map:

$$d : \mathcal{R} \to S \tag{55}$$

$$R \mapsto r \text{ where } \{r\} = R_1 \cap R_2 \tag{56}$$

This map is well defined since for every $R \in \mathcal{R}$, $|R_1 \cap R_2| = 1$ by (53) above, so $R_1 \cap R_2 = \{r\}$ for some unique r.

By (52) above, (r,r) is in a unique rectangle, so this map is bijective and $|\mathcal{R}| = |S|$.

For some fixed rectangle $R \in \mathcal{R}$ define:

$$r_R : \mathcal{R} \to R_2 \times R_1 \tag{57}$$
$$Q \mapsto (Q_1 \cap R_2, Q_2 \cap R_1) \tag{58}$$

where $(\{a\},\{b\})$ and (a,b) are equated to simplify notation. Suppose $r_R(Q) = r_R(P) = (a,b)$ for some $P, Q \in \mathcal{R}$. Then $a \in P_1, Q_1$ and $b \in P_2, Q_2$, i.e. $(a,b) \in P, Q$, so by the uniqueness in (52) $P = Q$ and r_R is injective. (52) also forces surjectivity since for every $(s,t) \in R$, there is some $Q \in \mathcal{R}$ with $(t,s) \in Q$. Thus r_R is a bijection and $|R| = |R_1||R_2| = |\mathcal{R}|$.

Fix $s \in S$ and define

$$\mathcal{Q} = \{Q \in \mathcal{R} | s \in Q_1\}. \tag{59}$$

Take a rectangle $R \in \mathcal{R}$, for all $Q \in \mathcal{Q}$, $|Q_2 \cap R_1| = 1$. Thus the mapping

$$\mathcal{Q} \to R_1 \tag{60}$$
$$Q \mapsto q \text{ where } \{q\} = Q_2 \cap R_1 \tag{61}$$

is well–defined. For any $Q, T \in \mathcal{Q}$,

$$t \in Q_2 \cap T_2 \neq \emptyset \Rightarrow (s,t) \in Q, (s,t) \in T \Rightarrow Q = T \tag{62}$$

Thus the mapping is injective. Since for every $t \in R_1$, there is some $Q \in \mathcal{R}$ such that $(s,t) \in Q$, the mapping is surjective, thus bijective, giving $|R_1| = |\mathcal{Q}|$. Since $\mathcal{Q}$ is independent of R, $|R_1|$ is thus fixed, as is $|R_2|$, for all rectangles $R \in \mathcal{R}$. ■

This leads to some simplifications. Suppose $|S|$ is prime. Then the only rectangular structures definable on S are the Dagwoods.

4.2 An Abstract Algebra

From a rectangular structure $\mathcal{R}$, using the bijection d from equation (55) above and denoting by $R(s,t)$ the unique rectangle on the pair (s,t) guaranteed by (52), define

$$\bullet : S \times S \to S \tag{63}$$
$$(s,t) \mapsto u \text{ where } \{u\} = (d^{-1}(s))_2 \cap (d^{-1}(t))_1$$
$$\circ : S \times S \to S \tag{64}$$
$$(s,t) \mapsto u \text{ where } \{u\} = d(R(s,t))$$

as binary operations on S.

As an example consider the vanilla rectangular structure on A, B. In this case

$$d(R_{(a,b)}) = (a,b) \tag{65}$$
$$R((a,b),(c,d)) = R_{(a,d)} \tag{66}$$

thus

$$(a,b)\bullet(c,d)=(b,c) \tag{67}$$
$$(a,b)\circ(c,d)=(a,d) \tag{68}$$

In general

Proposition 14. The algebra $(S,\bullet,\circ)$, with operations defined as in (63),(64) above, is an idempotent semicentral bigroupoid.

Proof. This is pure calculation.

$$\begin{aligned}(a\bullet b)\circ(b\bullet c) &= (d^{-1}(a)_2\cap d^{-1}(b)_1)\circ(d^{-1}(b)_2\cap d^{-1}(c)_1) &(69)\\ &= k\circ l \text{ for some } k,l\in S &(70)\\ &= d(R(k,l)) &(71)\end{aligned}$$

But $k\in d^{-1}(b)_1$ and $l\in d^{-1}(b)_2$. Let $B=d^{-1}(b)$. Then $(k,l)\in B$, thus $R(k,l)=B$, thus $k\circ l=d(B)=b$.

Now for the dual.

$$\begin{aligned}(a\circ b)\bullet(b\circ c) &= d(R(a,b))\bullet d(R(b,c)) &(72)\\ &= d^{-1}(d(R(a,b)))_2\cap d^{-1}(d(R(b,c)))_1 &(73)\\ &= R(a,b)_2\cap R(b,c)_1 &(74)\end{aligned}$$

Since $b\in R(a,b)_2$, $b\in R(b,c)_1$ and their intersection is unique,

$$R(a,b)_2\cap R(b,c)_1=\{b\}. \tag{75}$$

Thus the two axioms of a semicentral bigroupoid are satisfied. Since $a\circ a=d(R(a,a))=a$ for all $a\in S$ we see that the $\circ$ operation is idempotent, thus by Lemma 5 above, both operations are idempotent. ■

In the example from a vanilla rectangular structure above, we can see that the algebra $(S,\bullet)$ is a rectangular semigroup, as is $(S,\circ)$. It has been shown in Section 3.3 that all *associative* semicentral bigroupoids are of this form. In some sense this is the "simplest" semicentral bigroupoid that is not trivial. The trivial semicentral bigroupoid defined by equation (7) can be seen to be derived from the Dagwood rectangular structure by the same process as above. It also belongs to the class of examples described here, as it is associative. To see this, take one of the sets A,B above as trivial, i.e. $|A|=1$ or $|B|=1$.

That the whole structure of the associative semicentral bigroupoids is forced from the associativity of just one operation is not an isolated case. In general, one operation follows from the other uniquely.

Corollary 15. Given the table for $(S,\bullet)$, one obtains the table for $(S,\circ)$ uniquely.

Proof. From the table of $(S, \bullet)$, one can find the rectangular structure associated with the algebra, thus the idempotent semicentral bigroupoid that corresponds to it. The permutation of the elements defined by the square map $a \mapsto a \bullet a$ is also apparent in $(S, \bullet)$. These are all that are necessary to define the $\circ$ operation. ∎

If we call the format of an operation table the format of the derived rectangular structure, we get the following.

Corollary 16. If $(S, \bullet, \circ)$ is a semicentral bigroupoid with format (a, b) for the $\bullet$ operation table, then the format of the $\circ$ operation table is (b, a).

Proof. Let (c, d) be the format of the $\circ$ operation table. For any $x \in S$, $\rho(x) = S \bullet x \times x \bullet S$ is the rectangle filled with x in the $\circ$ operation table. Thus $d = |x \bullet S|$, so there are d rectangles in the x row of the $\bullet$ operation table, all of which have the same format (a, b). Thus $db = |S|$. But $|S| = ab$ so $a = d$. Similarly $b = c$, i.e. the format of the $\circ$ operation table is (b, a). ∎

This result gives a corollary that comes from the early work on central groupoids.

Corollary 17 ([6] Theorem 1) *A finite central groupoid* $(S, \bullet)$ *has square order.*

Proof. If $(S, \bullet)$ is a central groupoid, then $(S, \bullet, \bullet)$ is a bicentral groupoid. Thus the formats of the operations are (a, b) and (b, a), but these are identical, so $a = b$ and $|S| = ab = a^2$. ∎

5. Reversibility of cellular automata

I presume that the reader knows the basic ideas of cellular automata. We will use alphabet A, f to represent the cellular automata rule or local map, F to represent the global map. A cellular automaton with a global map F is called *reversible* if the map F has an inverse F^{-1} such that $F \circ F^{-1} = F^{-1} \circ F$ is the identity map on $A^{\mathbb{Z}}$. We call this a *reversible cellular automata* (RCA). A rather thorough review of the state of reversible cellular automata is given in [33], which covers the theory and some applications of reversible cellular automata.

The following result is quite important, as it removes the possibility of the inverse of a reversible cellular automata not being a cellular automata.

Lemma 18 (Richardson [28]) *If a cellular automata is reversible, then its inverse is a cellular automata.*

In 1993 J. Kari showed that for cellular automata of higher dimension, the reversibility question is undecidable [11], in contrast to the situation for one dimensional cellular automata. Happily, this need not concern us, as there are enough interesting aspects of one dimensional reversible cellular automata to be investigated. For instance, Morita and others have demonstrated that reversible universal computable cellular automata exist [23].

John Pedersen's work in [25] shows that we can treat all one dimensional cellular automata local functions as binary by using a shift and chunking. In the literature these are often referred to as radius one–half rules.

The construction is as follows. If we have a local map f of radius r, thus arity $2r+1$ (assuming symmetry for simplicity) on a state set A. The global state is then taken from $A^{\mathbb{Z}}$ and the global map is $(F(a))_i = f(a_{i-r}, a_{i-r+1}, \ldots, a_{i+r})$. We see that the dynamics of the cellular automaton is not changed by multiplying by σ^r where σ is the shift operation. The rule $\sigma^r f$ is then one sided, with $(F(a))_i = f(a_i, a_{i+1}, \ldots, a_{i+2r})$.

We can then define an equivalent cellular automaton with state set $S = A^{2r}$ and local rule

$$\begin{aligned} h &: S \times S \to S && (76)\\ &(a,b) \mapsto (f(a_1, a_2, \ldots, a_{2r}, b_1),\\ &\qquad f(a_2, a_3, \ldots, a_{2r}, b_1, b_2),\\ &\qquad \ldots,\\ &\qquad f(a_{2r}, b_1, b_2, \ldots, b_{2r})) && (77) \end{aligned}$$

As a result we get a cellular automaton with a binary operation as the local map, which can be treated as a groupoid operation. That is, (S,h) is a groupoid, a (2)-algebra. Such operations are more intuitive and enable us to apply the tools of algebra in a clearer fashion. Such operations are also known in general algebra, see e.g. [15].

Now taking a reversible cellular automata, we can apply this treatment in both forward and reverse time. It is easy to see that if $\bar{f}$ is a local map on a state set A and $\bar{g}$ is the reverse map, then by suitably shifting the maps (in opposite directions) and taking the state set S to be a product of A, we can derive an algebra (S,f,g) where f and g are binary operations. As the cellular automaton is reversible, there will be certain equalities.

In forward time, the global function is $(F(a))_i = f(a_i, a_{i+1})$. In reverse time, the global function is $(G(a))_i = g(a_{i-1}, a_i)$. By reversibility, we mean that $FG(a) = a$ and $GF(a) = a$, or locally,

$$a_i = f(g(a_{i-1}, a_i), g(a_i, a_{i+1})) \qquad (78)$$

$$a_i = g(f(a_{i-1}, a_i), f(a_i, a_{i+1})) \qquad (79)$$

which we can rewrite in general as

$$a = f(g(b,a), g(a,c)) \tag{80}$$
$$a = g(f(b,a), f(a,c)) \tag{81}$$

which, by rewriting using infix notation with $\bullet$ for f and $\circ$ for g,

$$a = (b \circ a) \bullet (a \circ c) \tag{82}$$
$$a = (b \bullet a) \circ (a \bullet c) \tag{83}$$

which we can recognise as the axioms for a semicentral bigroupoid.

Thus we see that semicentral bigroupoids are an appropriate tool for investigating reversible one dimensional cellular automata.

Cellular automata with a binary local map are also known as *radius one–half* cellular automata, see for example [9] where similar results to those obtained in this paper are obtained, but with much more work. It is surprising to see the amount of effort he had to go through to derive these results using pure cellular automata theoretic techniques, compared to the simplicity with which the results follow using this generalisation of Pedersen's technique. Some other papers have appeared using the ideas of Pedersen, see for instance [3, 4, 21, 22], but I am sure that there will be many more, as this algebraic approach offers much in the way of rigour and more tools for cellular automata theoreticians. For instance, additive cellular automata can be analysed simply using these techniques, see [2] for details, comparing with e.g. [16] or [34].

6. Graph and Matrix Models

In this section we will look at some models of semicentral bigroupoids using more traditional mathematical constructs. Matrix theory and graph theory are very universal fields of study, encroaching nearly everywhere. Here we will see that we can equate semicentral bigroupoids with a class of matrix pairs and with a class of graph pairs. Similar connections are to be found in the theory of central groupoids, see [12]. Note that in this section, we will treat eneral semicentral bigroupoids, not just idempotent ones.

6.1 Matrices

Let M, N be a pair of 0–1 matrices under normal integer addition and multiplication, such that

$$MN = J_1 \tag{84}$$
$$NM = J_2 \tag{85}$$

where J_i is the matrix consisting of 1 in every place, of appropriate sizes.

Every pair of such matrices can be converted to a rectangular structure and vice versa. First note that if M is a $k \times l$ matrix, and N is $m \times n$, then by equation (84), $l = m$, and by equation (85), $k = n$, so we know they are $m \times n$ and $n \times m$ matrices respectively. Define sets M_i, N_i for $i = 1 \ldots n$ by

$$j \in M_i \Leftrightarrow M_{i,j} = 1 \tag{86}$$

$$j \in N_i \Leftrightarrow N_{j,i} = 1 \tag{87}$$

Then define

$$\mathcal{R} = \{(M_i, N_i) | i = 1, \ldots, n\} \tag{88}$$

Proposition 19. $\mathcal{R}$ is a rectangular structure on $S = \{1, \ldots, m\}$. Conversely every rectangular structure on S defines a matrix pair satisfying (84) and (85).

Proof. For axiom (52) take the first set in one rectangle, M_i for some i, and the second set of some other rectangle, N_j for some j. Note that $k \in M_i \cap N_j$ if and only if $M_{i,k} = N_{k,j} = 1$. Since

$$(MN)_{i,j} = 1 = \sum_l M_{i,l} N_{l,j} \tag{89}$$

we know that there is some unique l for which $M_{i,l} N_{l,j} = 1$, and this is the (unique) element in the intersection $M_i \cap N_j$.

Now for (53). Take any pair $(a, b) \in S$. Then

$$\begin{aligned} (NM)_{b,a} = 1 &\Rightarrow \exists! k \; N_{b,k} = M_{k,a} = 1 &(90)\\ &\Rightarrow a \in M_k, \quad b \in N_k &(91)\\ &\Rightarrow (a, b) \in R_k = (M_k, N_k) &(92) \end{aligned}$$

Thus there is a rectangle containing (a, b). It is unique since if it were not, then $(NM)_{b,a}$ would be greater than 1.

Thus every such matrix pair leads to a rectangular structure.

For the converse, start with a rectangular structure $\mathcal{R} = \{R_1, \ldots, R_m\}$ on $\{1, \ldots, m\}$ and construct matrices M, N by

$$M_{i,j} = \begin{cases} 1 & \text{if } j \in (R_i)_1 \\ 0 & \text{o/w} \end{cases} \tag{93}$$

$$N_{i,j} = \begin{cases} 1 & \text{if } i \in (R_j)_2 \\ 0 & \text{o/w} \end{cases} \tag{94}$$

It is then simple to show that this pair of matrices satisfies the equations (84) and (85) above.

$$(MN)_{i,j} = \sum_k M_{i,k} N_{k,j} \tag{95}$$

$$\begin{aligned} \text{Now } M_{i,k} N_{k,j} = 1 &\Leftrightarrow M_{i,k} = N_{k,j} = 1 \\ &\Leftrightarrow k \in (R_i)_1, \; k \in (R_j)_2 &(96) \end{aligned}$$

By axiom (53) there is a unique such k, so we find that $(MN)_{i,j} = 1$.

$$(NM)_{i,j} = \sum_k N_{i,k} M_{k,j} \tag{97}$$

$$\begin{aligned}\text{Now } N_{i,k}M_{k,j} = 1 &\Leftrightarrow N_{i,k} = M_{k,j} = 1\\ &\Leftrightarrow (j,i) \in R_k = (M_k, N_k)\end{aligned} \tag{98}$$

By axiom (52) there is a unique such k, so we find that $(NM)_{i,j} = 1$, and we are done. ■

Note that rectangular structure results then show that $n = m$, so every such pair of matrices is square. We also find that the rows and columns are evenly weighted. Note that several matrices could be defined dependinh upon th eordering of the rectangles in the set $\mathcal{R}$.

These are generalisations of the matrices introduced by Hoffman in [10] and later investigated by Knuth in [12], where 0–1 matrices A such that $A^2 = J$ are investigated. There has been some interesting work done on these, with some generating algorithms developed by Leslie Shader [31].

Examples of such matrix pairs can be combined to create new pairs. For instance, forming the Kronecker product.

Proposition 20. If M, N and M', N' are pairs of matrices satisfying (84) and (85), then the Kronecker products $M \otimes M', N \otimes N'$ are also such a matrix pair.

We omit a proof by calculation as it is overly technical. A more direct proof of this will be possible later as we build up more connections and realise that forming the Kronecker product of two such matrices is equivalent to the conjunction of the graphs with these incidence matrices which is in turn equivalent to forming the direct product of the two semicentral bigroupoids associated with the graphs.

Other results of interest, such as the relationship of the lifting operation to the matrices, can be found in [2].

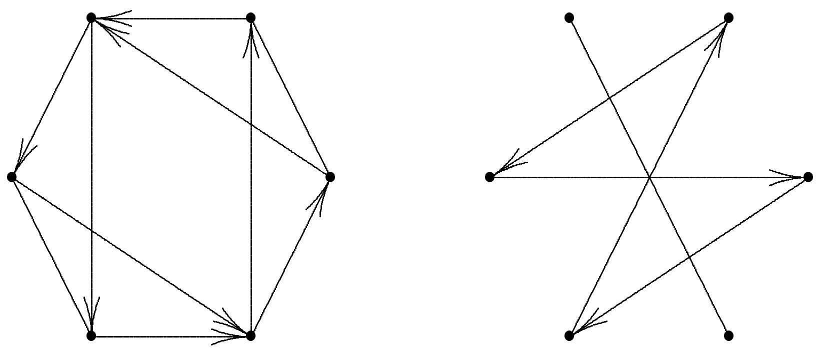
6.2 Digraphs

In this section, we see that the matrix pairs defined above are the incidence matrices for some nicely structured graph pairs.

Take a fixed set of vertices, and look at two directed graphs on this set, G_R and G_B. Call these as the red and blue graphs respectively. The problem is to arrange these graphs such that, when we superimpose them, there is a unique directed path of length 2 coloured blue-red between any two nodes, and a unique directed path coloured red-blue.

As an example consider the pair of graphs in Figure 1, with loop arcs of both colours on every node not drawn in.

Take the left graph to be red, the right one to be blue. One notices a few things about these graphs. The symmetry apparent in the graphs



(99)

Figure 1. An example of a red and blue graph pair, omitting loop arcs.

is quite striking. Both graphs are regular, the red graph has valency three (including the unseen loop arcs) while the blue has valency two. We will see that these observations are, in fact, general to this class of graph–pairs.

A general class of such examples can be simply constructed as grids. Take any rectangle in the plane $\mathbb{Z} \times \mathbb{Z}$ as the node set, and join all nodes in a horizontal line with red arcs, and all nodes in a vertical line with blue arcs. Then to get from one node to another along a red–blue path, one first travels horizontally along a red arc to the correct vertical line, then travels along a blue arc to the correct node, somewhat like the Manhattan street map. One finds the blue–red path from one node to another similarly by moving first vertically then horizontally.

This relates to the inter–processor communication graphs in [8], with added notions of symmetry. There, the author is interested in digraphs that can be coloured so that between every pair of vertices (a, b) there is a unique directed path from a to b coloured red–blue, but not the dual (a unique path coloured blue–red). The graph pairs he advocates are of the grid form, since they are simple to implement, one could use a single broadcast medium such as ethernet as the connections along horizontal or vertical lines. We see here that other options would be possible.

6.3 Connections

In this section we see that the digraph (with loop nodes), matrix (with full diagonal), combinatorial and (idempotent) algebraic structures are all equivalent. We also se that the unrestricted digraph, matrix and algebraic structures are also equivalent.

From graph pairs, one constructs the incidence matrix R for the red graph and B for the blue graph. That is $R_{i,j} = 1$ iff there is a directed red edge from vertex i to vertex j, and is 0 otherwise. B is constructed similarly from the blue edges. Then R and B form a pair of 0–1 matrices as described above. This follows since $(RB)_{i,j}$ counts the number of directed red–blue paths from i to j. By construction, we have a unique path between every pair of nodes, thus this value is always one. Similarly $(BR)_{i,j}$ counts the number of directed blue–red paths from i to j, which is also one.

This argument not only shows that each such pair of graphs defines a pair of matrices as above, but also that the graphs defined by taking the matrices as incidence matrices are all of the appropriate form. In a strong sense the graph pairs and the matrix pairs are equivalent.

For instance, the matrices derived from the above graph pair are:

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{100}$$

Another connection is that these digraphs appear for all semicentral bigroupoids. In some sense we can equate semicentral bigroupoids and these graph pairs. Secondly, the relation between direct products of semicentral bigroupoids and direct products of graphs is a very direct one, allows us to draw an isomorphism between the category of these graphs and the category of semicentral bigroupoids.

Example 21 (Construction) *When one takes any semicentral bigroupoid, one finds that the relations $a \rightarrow_{blue} b$ and $a \rightarrow_{red} b$ are defined as*

$$a \rightarrow_{red} b \Leftrightarrow a \bullet c = b \; \exists c \tag{101}$$

$$a \rightarrow_{blue} b \Leftrightarrow a \circ c = b \; \exists c \tag{102}$$

Thus we can define a graph pair from any semicentral bigroupoid.

Conversely, given a graph pair we can define a semicentral bigroupoid from it. Let S be the vertex set of the graphs. For any $a, b \in S$, let c_r, c_b be the vertices on the path between a and b:

$$a \rightarrow_{red} c_r \rightarrow_{blue} b \tag{103}$$

$$a \rightarrow_{blue} c_b \rightarrow_{red} b \tag{104}$$

These are uniquely defined by the graph property. Then define

$$a \bullet b = c_r \tag{105}$$

$$a \circ b = c_b \tag{106}$$

and we have a semicentral bigroupoid $(S, \bullet, \circ)$.

These constructions are the inverses of one another.

Thus from a semicentral bigroupoid we can define a graph pair quite simply, by defining the arcs as above on the node set that are the elements of S. Note that if some element a is idempotent, then $a \bullet a = a$ so there is a red loop arc on the node a, similarly a blue loop arc. Thus if S were idempotent, every node would be a loop node, as seen in the case above.

If $(V_1, R_1), (V_1, B_1)$ and $(V_2, R_2), (V_2, B_2)$ are two pairs of graphs as described above, then the *conjunction* of these is the graph pair $(V_1 \times V_2, R), (V_1 \times V_2, B)$ with $((a,b),(c,d)) \in R$ iff $(a,c) \in R_1$ and $(b,d) \in R_2$ and $((a,b),(c,d)) \in B$ iff $(a,c) \in B_1$ and $(b,d) \in B_2$.

Lemma 22 ([7], 2.2) *The class of graphs defined above is closed under the conjunction operation.*

Proof. Given two points (a,b) and (c,d) in $V_1 \times V_2$, we get the pair (e,f) with $a \rightarrow_{blue} e \rightarrow_{red} c$ for the graph on V_1, and $b \rightarrow_{blue} f \rightarrow_{red} d$ for the graph on V_2. Thus this path exists, and a similar argument shows a red–blue path exists between (a,b) and (c,d).

The uniqueness follows by considering that if a different "way–point" (e', f') existed for a blue–red path, then that would imply that there was a different blue–red path in graph V_1, which there is not, by the definition. Similarly there cannot be another red–blue path. ∎

Let's look more closely at the connection between semicentral bigroupoids and these graph pairs. We see that that the two classes are completely identical, in a categoric sense.

Consider two categories, $\mathcal{S}$ of semicentral bigroupoids, and $\mathcal{G}$ of graph pairs satisfying the constraint above. Consider the functor from $\mathcal{S}$ to $\mathcal{G}$ as described in Example 21 above, and take an exact sequence $A \rightarrow_f B \rightarrow_g C$ in $\mathcal{S}$. Since the mappings f, g operate on elements of the semicentral bigroupoids, they then operate on vertices of the graphs under the functor, carrying arcs across with them. Thus $range(f) = ker(g)$ in $\mathcal{G}$, so the functor is exact. Thus we get the result:

Lemma 23. Isomorphic semicentral bigroupoids give isomorphic graph pairs by the construction in Example 21 above.

Thus the correspondence between graph pairs and semicentral bigroupoids is an equivalence. Moreover the conjunction of graphs equates to the Kronecker product of their incidence matrices, as mentioned above. In the next section we look at the equivalence amongst the graphs, matrices and semicentral bigroupoids a little more closely.

The following shows that the automorphism group of a semicentral bigroupoid can be obtained using the automorphism groups of the associated graphs, a well–studied problem in combinatorics.

Lemma 24. If G_b, G_r are the graphs defined by a semicentral bigroupoid S, then

$$Aut(S) = Aut(G_b) \cap Aut(G_r) \tag{107}$$

Proof. Note that automorphisms are already bijections. Thus we can concentrate upon structural coherence.

($\subseteq$): Take $\phi \in Aut(S)$. Take any red edge $a \to_{red} b$, so there is some c such that $a \bullet c = b$.

$$\phi a \bullet \phi c = \phi(a \bullet c) = \phi b \tag{108}$$

So $\phi a \to_{red} \phi b$, so $\phi \in Aut(G_r)$. Similarly $\phi \in Aut(G_b)$ and we are done.

($\supseteq$): Take some $\phi \in Aut(G_b) \cap Aut(G_r)$, $a, b \in S$ and $c = a \bullet b$ so $a \to_{red} c \to_{blue} b$. Then

$$\phi \in Aut(G_r) \Rightarrow \phi a \to_{red} \phi c \tag{109}$$

$$\phi \in Aut(G_b) \Rightarrow \phi c \to_{blue} \phi b \tag{110}$$

Then by uniqueness of the path

$$\phi a \to_{red} (\phi a \bullet \phi b) \to_{blue} \phi b \tag{111}$$

$$\phi a \to_{red} (\phi a) \bullet (\phi b) \to_{blue} \phi b \tag{112}$$

we know that $\phi c = \phi(a \bullet b) = \phi a \bullet \phi b$ and similarly $\phi(a \circ b) = \phi a \circ \phi b$ so $\phi \in Aut(S)$. ■

It is thus possible to use the algorithms developed for determining the automorphisms of graphs to easily determine the automorphism groups of semicentral bigroupoids. This is a particular problem in relation to the results later regarding the uniqueness of liftings of semicentral bigroupoids and moreover it is also of considerable worth in the construction of examples of rectangular structures that we will look at in section 9.

7. Uniqueness of Semicentral Bigroupoids

In this section we can now investigate the notion of isomorphism, and a clear method of determining isomorphism between semicentral bigroupoids is arrived at. This can even be extended to a counting method so that given exhaustive lists of idempotent semicentral bigroupoids of a given size we can then count exactly how many semicentral bigroupoids of that order exist. In the following section we will look at this problem of exhaustive generation, and the determination of isomorphism is fundamental there.

In this section I wish to look at some general results dealing with the uniqueness of semicentral bigroupoids up to isomorphism. For ease of notation I will use the dual lifting formulation.

Once again duality and symmetry make our work easier.

Lemma 25. If $(S, \bullet, \circ)$ is a semicentral bigroupoid and ϕ is a $\bullet$–isomorphism, then it is a $\circ$–isomorphism.

Proof. As usual, we use a coordinatisation argument. Note first that

$$\{a \circ b\} = \{x|yx = a\} \cap \{x|xy = b\} \tag{113}$$

Then compute for a $\bullet$–isomorphism ϕ:

$$\begin{aligned} \{\phi(a \circ b)\} &= \{\phi x|yx = a\} \cap \{\phi x|xy = b\} && (114)\\ &= \{\phi x|\phi y\phi x = \phi a\} \cap \{\phi x|\phi x\phi y = \phi b\} && (115)\\ &= \{x|yx = \phi a\} \cap \{x|xy = \phi b\} && (116)\\ &= \{\phi a \circ \phi b\} && (117) \end{aligned}$$

so ϕ is a $\circ$–morphism, and we are done. ∎

Thus in order to show that a mapping ϕ on semicentral bigroupoid S is an isomorphism we need only show it for one operation, the other follows automatically. Note that the above argument does not work for general morphisms.

We have seen that every semicentral bigroupoid is a lifting of an idempotent one. We also have:

Lemma 26. Every semicentral bigroupoid $(S, \bullet, \circ)$ has an associated rectangular structure that is constant across liftings.

Proof. Suppose $(S, *, +)$ is a lifting of $(S, \bullet, \circ)$ by ϕ. Define the rectangular structures as follows:

$$\mathcal{R}^\bullet = \{R^\bullet_x = \{(a, b)|a \bullet b = x\}|x \in S\} \tag{118}$$

$$\mathcal{R}^* = \{R^*_x = \{(a, b)|a * b = x\}|x \in S\} \tag{119}$$

These are rectangular structures as they are derived from semicentral bigroupoids.

Take $(a, b), (c, d) \in R \in \mathcal{R}^\bullet$, two pairs in some rectangle. Thus $a \bullet b = c \bullet d = x$ for some $x \in S$. But $a * b = \phi^{-1}(a \bullet b) = \phi^{-1}(c \bullet d) = c * d$ so (a, b) and (c, d) are in the same rectangle in $\mathcal{R}^*$. Thus the rectangular structures are the same for both semicentral bigroupoids. ∎

Proposition 27. Two idempotent semicentral bigroupoids are isomorphic iff the associated rectangular structures are isomorphic.

Proof. ($\Rightarrow$) Let the semicentral bigroupoids be $(S, \bullet, \circ)$ and $(T, *, +)$, with isomorphism $\beta : S \to T$. Take $\mathcal{R}^\bullet, \mathcal{R}^*$ as above, and take $R \in \mathcal{R}^\bullet$. Then

$$\begin{aligned} \beta(R) &= \{(\beta a, \beta b)|(a, b) \in R\} && (120)\\ &= \{(\beta a, \beta b)|a \bullet b = x\} \text{ for some } x \in S && (121)\\ &= \{(\beta a, \beta b)|\beta a * \beta b = \beta(a \bullet b) = \beta(x)\} && (122)\\ &= \{(a, b)|a * b = \beta x\} && (123) \end{aligned}$$

which is a rectangle in $\mathcal{R}^*$. Similarly one shows that $\beta^{-1} : T \to S$ respects rectangles, so β is a rectangular structure isomorphism.

($\Leftarrow$) Take two idempotent semicentral bigroupoids $(S, \bullet, \circ)$ and $(T, *, +)$, and suppose $\beta : S \to T$ preserves the rectangles of the associated rectangular structures $\mathcal{R}^\bullet, \mathcal{R}^*$. Take some $a, b \in S$. Then $a \bullet b = x = x \bullet x$ for some x. Thus (a, b) and (x, x) are in the same rectangle in $\mathcal{R}^\bullet$, and thus $(\beta a, \beta b)$ and $(\beta x, \beta x)$ are in the same rectangle in $\mathcal{R}^*$. Thus

$$\beta(a) * \beta(b) = \beta(x) * \beta(x) = \beta(x) = \beta(a \bullet b) \tag{124}$$

so β is an isomorphism of the algebras. ■

The construction of a rectangular structure from a semicentral bigroupoid above and the reverse construction in Proposition 14 are complementary in that given an idempotent semicentral bigroupoid $(S, *, +)$, the semicentral bigroupoid $(S, \bullet, \circ)$ derived from the associated rectangular structure is the same, i.e. $a * b = a \bullet b,\ a + b = a \circ b$.

We now know that given a collection of non–isomorphic rectangular structures, we cannot get isomorphic idempotent semicentral bigroupoids out of them, and vice versa. Rectangular structures and idempotent semicentral bigroupoids are essentially equivalent. This contrasts with many generation procedures for algebraic objects where non–isomorphic combinatorial structures lead to isomorphic algebraic structures, or vice versa.

Note also that the forward implication in the proposition above does not use the idempotence, so we know that isomorphic semicentral bigroupoids have isomorphic rectangular structures in all cases.

Now to look at a similar result for non–idempotent semicentral bigroupoids.

Proposition 28. Two semicentral bigroupoids $(S, \bullet, \circ)$ and $(T, *, +)$ are isomorphic, with isomorphism $\beta : S \to T$, iff their idempotent liftings are isomorphic by β, and $\beta\phi_\bullet = \phi_*\beta$ for the square maps $\phi_\bullet$ and ϕ_*.

Proof. In this proof, I will use the symbol $\bar{\bullet}$ for the idempotent lifting of the $\bullet$ operation, i.e. $a \bar{\bullet} b = \phi_\bullet^{-1}(a \bullet b)$.

($\Rightarrow$) We know from the forward half of Proposition 27 above that the rectangular structures are isomorphic, thus the idempotent semicentral bigroupoids generated from the rectangular structures are isomorphic by some bijection β.

Now for all $a, b \in S$:

$$\beta(a \bar{\bullet} b) = \beta(\phi_\bullet^{-1}(a \bullet b)) \tag{125}$$
$$\text{and } \beta(a \bar{\bullet} b) = \beta(a) \bar{*} \beta(b) \tag{126}$$
$$= \phi_*^{-1}(\beta(a) * \beta(b)) \tag{127}$$
$$= \phi_*^{-1}(\beta(a \bullet b)) \tag{128}$$
$$\text{thus } \phi_*^{-1}\beta = \beta\phi_\bullet^{-1} \tag{129}$$
$$\Rightarrow \beta\phi_\bullet = \phi_*\beta \tag{130}$$

($\Leftarrow$) The converse follows directly by computation.

$$\beta(a \bullet b) = \beta\phi_\bullet\phi_\bullet^{-1}(a \bullet b) \tag{131}$$
$$= \phi_*\beta(a \bar{\bullet} b) \tag{132}$$
$$= \phi_*(\beta(a) \bar{*} \beta(b)) \tag{133}$$
$$= \phi_*\phi_*^{-1}(\beta(a) * \beta(b)) \tag{134}$$
$$= \beta(a) * \beta(b) \tag{135}$$

So β is a semicentral bigroupoid isomorphism. ■

For the following, S_S is the symmetric group on S, $Symm_{RS}(S)$ is the symmetry group of the rectangular structure of $(S, \bullet, \circ)$, and $[a, b]$ is the commutator of a and b.

Lemma 29. A lifting of a semicentral bigroupoid $(S, \bullet, \circ)$ by ϕ is an isomorphism iff $\phi \in [\phi_\bullet, Symm_{RS}(S)]$

Proof. The square map in the lifting $(S, *, +)$ is

$$\phi_*(x) = x * x = \phi^{-1}(x \bullet x) = \phi^{-1}\phi_\bullet(x) \tag{136}$$

We know that rectangular structures are preserved by lifting (Lemma 26), so we need only look at the second condition in the last proposition.

The lifting is isomorphic, with isomorphism α, if α is an automorphism of the rectangular structure associated with S and

$$\alpha\phi_\bullet = \phi_*\alpha \tag{137}$$
$$\Leftrightarrow \alpha\phi_\bullet = \phi^{-1}\phi_\bullet\alpha \tag{138}$$
$$\Leftrightarrow \phi = \phi_\bullet\alpha\phi_\bullet^{-1}\alpha^{-1} \tag{139}$$
$$\text{that is, } \phi \in [\phi_\bullet, Symm_{RS}(S)] \tag{140}$$

■

Proposition 30. Two liftings of an idempotent semicentral bigroupoid by $\phi, \bar{\phi}$ are isomorphic iff the $\phi, \bar{\phi}$ are conjugate by an element from $Symm_{RS}(S)$.

Proof. Let $(S_1, \bullet_1, \circ_1)$(resp. $(S_2, \bullet_2, \circ_2)$) be the lifting by ϕ (resp. $\bar{\phi}$), that is

$$a \bullet_1 b = \phi^{-1}(a \bullet b) \tag{141}$$
$$a \bullet_2 b = \bar{\phi}^{-1}(a \bullet b) \tag{142}$$

Note that $\phi_{\bullet_1}(x) = x \bullet_1 x = \phi^{-1}(x \bullet x) = \phi^{-1}(x)$ so $\phi_{\bullet_1} = \phi^{-1}$, similarly $\phi_{\bullet_2} = \bar{\phi}^{-1}$.

S_2 is a lifting of S_1 by $(\phi^{-1}\bar{\phi})$,

$$a \bullet_2 b = \bar{\phi}^{-1}(a \bullet b) \tag{143}$$
$$= \bar{\phi}^{-1}\phi(a \bullet_1 b) \tag{144}$$
$$= (\phi^{-1}\bar{\phi})^{-1}(a \bullet_1 b) \tag{145}$$

Thus $\alpha \in Symm_{RS}(S)$ is an isomorphism $S_1 \to S_2$

$$\Leftrightarrow \phi^{-1}\bar{\phi} = \phi_{\bullet_1}\alpha\phi_{\bullet_1}^{-1}\alpha^{-1} \tag{146}$$
$$= \phi^{-1}\alpha\phi\alpha^{-1} \tag{147}$$
$$\Leftrightarrow \bar{\phi} = \alpha\phi\alpha^{-1} \tag{148}$$

i.e. iff ϕ and $\bar{\phi}$ are conjugate by an element of $Symm_{RS}(S)$. ■

In order to catalogue (all) semicentral bigroupoids of some specified size, we need only determine (all) rectangular structures of that size, find their symmetry groups, take representatives of the conjugacy classes in S_S and $Symm_{RS}(S)$, and we are done.

8. Counting semicentral bigroupoids

In this section we demonstrate how to count the number of nonisomorphic liftings of a given idempotent semicentral bigroupoid.

Given a rectangular structure $\mathcal{R}$, we find its symmetry group $G = Symm(\mathcal{R}) < S_S$. This can be easily done by finding the automorphism group of the idempotent semicentral bigroupoid via the graph model method of Lemma 24. These automorphisms act upon S_S by conjugation. By the previous section, each orbit then corresponds to an isomorphism class of the liftings of the idempotent semicentral bigroupoid on the rectangular structure $\mathcal{R}$. The problem is to count the number of orbits.

We formulate this problem in terms of permutation groups. Let $G := S_n$ for some n, and take some subgroup $K \leq G$. How many orbits does G have under the action of K by conjugation? Using Burnside's Lemma, we see that

$$t|K| = \sum_{k \in K} |F_G(k)| \tag{149}$$

where t is the number of orbits and $F_G(k)$ is the set of elements of G fixed by k. Now

$$F_G(k) = \{g \in G | kgk^{-1} = g\} = \{g \in G | kg = gk\} = C_G(k) \quad (150)$$

If we look at G acting upon itself by conjugation, we see

$$|C_G(k)||Gk| = |G| \quad (151)$$

where Gk is the orbit of k under G.

Note that Gk is the collection of all elements of G conjugate to k, and this is the collection of all elements of G with the same cycle structure as k. If k has a cycle structure of t_i cycles of length a_i, including cycles of length 1, we find that

Lemma 31.

$$|Gk| = \frac{n!}{\prod_i (t_i!) a_i^{t_i}} \quad (152)$$

Proof. We can lay out the cycles and fill in the n places in $n!$ combinations. The question is about equivalent ones.

First we have "external" symmetries, where we can arrange the t_i cycles of length a_i in any order. There are $t_i!$ possibilities for each i, thus $\prod_i t_i!$ in all.

Then we have "internal" symmetries where each cycle can be "spun" to any internal position. That is, the cycle $(\alpha_1, \ldots, \alpha_{a_i})$ is equivalent to the cycle $(\alpha_j, \ldots, \alpha_{a_i}, \alpha_1, \ldots, \alpha_{j-1})$ for any j. For a cycle of length a_i there are a_i such possibilities. Since we have t_i cycles of length a_i, we know there are $\prod_i a_i^{t_i}$ possibilities.

By dividing the number of raw possibilities $n!$ by the product of these symmetry counts, we get the expression above. ∎

Thus we find that

$$|C_G(k)| = \frac{|G|}{|Gk|} = \prod_i t_i! a_i^{t_i} \quad (153)$$

To find the number of orbits, we need only sum $|C_G(k)|$ for each element $k \in K$, and calculate

$$\text{num. orbits } = t = \frac{\sum_{k \in K} |C_G(k)|}{|K|} \quad (154)$$

Thus we have shown the following.

Proposition 32. If K is the symmetry group of a semicentral bigroupoid S of order n, and $G = S_n$ is the symmetric group on n points, then the number of non–isomorphic liftings of S is

$$\frac{\sum_{k \in K} |G_k|}{|K|} \quad (155)$$

This concludes our investigation into the uniqueness with respect to isomorphism. Given a rectangular structure, respectively an idempotent semicentral bigroupoid, we can easily compute the symmetry group of the object and thus determine the number of pairwise non-isomorphic liftings.

9. Generating Rectangular Structures

We look at a method of comprehensively constructing all examples with a given format using an incremental process. These methods makes use of internal symmetry and other structure to reduce the search space significantly and to avoid or remove isomorphic examples. The first method investigated is a two–phase method, generating then removing isomorphic copies. We then look at a more complex method that generates no isomorphic copies by keeping track of possible branches in the generation tree. We compare these two algorithms to see where efficiencies lie. Both techniques use a branching generation tree to generate examples piece by piece. The trade–off lies between increasing complexity in the generation tree algorithm and increasing effort in removing isomorphic copies in the thus generated lists.

If we are not after exhaustive listings, there are many other sources of examples. Special cases from affine planes and k-nets described in [2], the matrices from Shader's work [31], and various classes of matrices considered by people constructing special solutions to Hoffman's matrix question, see for instance [30, 13, 14, 35, 36, 17, 24] for general results.

9.1 Partial Rectangular Structures

In this section I want to look at a method of exhaustively enumerating all rectangular structures of a certain format. This method works by building up examples from simpler incomplete ones, in a branching process where each incomplete example can be built up in a number of different ways. Methods are outlined to reduce unnecessary branching by using only canonical extensions, the positive one–step extensions and by removing isomorphic extensions. We then look at techniques to sort the list, sieving out duplicates. The definitions here will be of relevance for the second technique as well.

Definition 7. For positive integers n, m, an $n \times m$ *rectangle* is a pair of sets (R_1, R_2) with $|R_1| = n, |R_2| = m$, $R_i \subset \{1, \dots, (nm)\}$, $|R_1 \cap R_2| = 1$

For instance $(\{1,4\},\{1,2,3,5\})$, $(\{1,2\},\{2,3,4,5\})$ are examples of 2×4 rectangles.

Define an order on same sized sets by ordering the elements of the sets, then ordering the sets on the words defined by the sequence of elements, using the standard order on integers. For example, given the sets $A = \{1,5,3,6\}$ and $B = \{6,5,1,2\}$, we order them and write the words $w_A = 1356$ and $w_B = 1256$. Then because these words can be lexicographically ordered, we say the sets are ordered $B \leq A$.

We can then order our rectangles

Definition 8. Two rectangles $R = (R_1, R_2)$ and $Q = (Q_1, Q_2)$ are ordered by $R \leq Q$ if $R_1 \leq Q_1$ or $R_1 = Q_1$ and $R_2 \leq Q_2$.

This is the lexicographical order.

Definition 9. A $n \times m$ *Partial Rectangular Structure* P is a collection of $n \times m$ rectangles such that

- For all $Q, R \in P, |Q_1 \cap R_2| = 1$
- For all $a, b \in \{1, \ldots, nm\}$ there is at most one $R \in P$ such that $a \in R_1, b \in R_2$.

One can easily see that a rectangular structure is a partial rectangular structure, that is, a partial rectangular structure is a generalisation of a rectangular structure along the axis of the covering requirement (equation (52)). A *full* partial rectangular structure is one with nm rectangles. This is a rectangular structure.

A simple $n \times m$ partial rectangular structure is

$$\{(\{1,2,\ldots,n\}, \{1, n+1, n+2, \ldots n+m-1\})\} \tag{156}$$

Note that this is also the minimal $n \times m$ rectangle by the ordering above. By adding the rectangle

$$(\{1,2,\ldots,n\}, \{1, n+m, n+m+1, \ldots n+2(m-1)\}) \tag{157}$$

we get a partial rectangular structure with two rectangles. This rectangle is also the smallest by the above ordering that one could add to the previous rectangle.

We can order partial rectangular structures of the same size by ordering the rectangles, then constructing the word of those rectangles, and ordering lexicographically on the words. This is particularly useful when implementing algorithms in an algebraic computer language such as GAP[5], where sets are defined as ordered lists without duplicates. Algorithms presupposing structured sets are thus no extra burden upon the system.

We let S_{nm}, the symmetric group on $\{1, \ldots, nm\}$ act on partial rectangular structures in the natural way.

Definition 10. A partial rectangular structure is *representative* if it is minimal in its orbit under S_{nm}.

There is precisely one representative for every partial rectangular structure.

Definition 11. An *extension* of a partial rectangular structure P is a partial rectangular structure P' such that $P \subset P'$. A *one–step extension* has the additional requirement that $|P'| = |P| + 1$. A *positive one–step extension* is one where the rectangle $R \in P' - P$ is greater than all the rectangles in P.

9.2 Algorithms

From here we come to a naive algorithm. Assume a function `pos_one_ext(P)` that, given a partial rectangular structure P, returns a set of all rectangles that could be added to P to form a positive one–step extension. Assembling a comprehensive list of all extensions of the minimal partial rectangular structure (156) using a depth–first branching tree, then taking the orbits under S_{mn} and selecting the minimal full partial rectangular structure in each orbit, would form a simple but incredibly slow algorithm.

A less stupid algorithm must check for aspects of isomorphism in the partial rectangular structures it has, and only expand one representative, trying to avoid multiple paths to the same (up to isomorphism) rectangular structure.

We can restrict ourselves to considering only some of the extensions of a partial rectangular structure, since we only want representative full partial rectangular structures, i.e. only representative rectangular structures.

Proposition 33. Any representative partial rectangular structure is a positive one–step extension of a representative partial rectangular structure.

Proof. Suppose the partial rectangular structure $P = \{R_1, \dots, R_{k+1}\}$ is a representative partial rectangular structure, $R_i < R_{i+1}$ for $i = 1, \dots, k$. Then P is a positive one–step extension of the partial rectangular structure $\{R_1, \dots, R_k\}$. Suppose that this is not a representative. Then there is some permutation ϕ of $\{1, \dots, nm\}$ such that

$$\phi(R_1, \dots, R_k) = \{S_1, \dots, S_k\} \leq \{R_1, \dots, R_k\}. \tag{158}$$

with $S_i < S_{i+1}$ $i = 1, \dots, k-1$. Then either

- $\phi(R_{k+1}) = S_1 \Rightarrow \exists i \in 1 \dots k$ s.t. $\phi(R_{k+1}) = S_1 = \phi(R_i) \Rightarrow R_{k+1} = R_i$, which is a contradiction.
- $\phi(R_{k+1}) < S_1$, in which case $S_1 \leq R_1$ implies $\phi(R_{k+1}) < R_1$ thus
$$\phi(P) = \phi(\{R_1, \dots, R_{k+1}\}) \leq \{R_1, \dots, R_{k+1}\} = P. \tag{159}$$
So $\phi(P)$ is the representative of P, and P was not a representative.

- $\phi(R_{k+1}) > S_1$. If $\phi(R_{k+1}) > S_k$, then

$$\phi(P) = \{S_1, \ldots, S_k, \phi R_{k+1}\} < \{R_1, \ldots, R_{k+1}\} = P. \tag{160}$$

  So P was not representative. There is some least l such that $\phi(R_{k+1}) < S_l$. So

$$S_1, \ldots, S_{l-1}, \phi R_{k-1} < R_1, \ldots, R_l \tag{161}$$

$$\phi(P) \Rightarrow S_1, \ldots, S_{l-1}, \phi R_{k+1}, S_l, \ldots, S_k < R_1, \ldots, R_{k+1} = P \tag{162}$$

  so P was not a representative.

Thus if P is not an extension of a representative, then it is not a representative itself. ■

Note that this does not say that a one step positive extension of a representative is necessarily representative, or that the representative of a one step positive extension of a partial rectangular structure P is an extension of P at all. But it does allow us to cut down many branches of our search tree, since we know that any partial rectangular structure that is not representative is a hopeless case, and that it is therefore pointless to continue to extend it since it will not give a representative rectangular structure.

From this result we can construct a more efficient algorithm. This algorithm was implemented as follows. Determine the automorphism group of the partial rectangular structure, then find the orbits of the positive one step extensions of that partial rectangular structure under the action of the automorphism group. Take the minimal element of each orbit, these are the candidate representative extensions. Rather than perform extra testing on the incomplete partial rectangular structures, let all candidates through until they become rectangular structures, then perform isomorph rejection by testing isomorphism between the examples using techniques outlined in the next section. In order to determine the automorphism group of the partial rectangular structures, I used Brendan McKay's `nauty` package [18] via Leonard Soicher's GRAPE package [32] for GAP. The graphs involved correspond exactly to the graphs defined earlier on rectangular structures, suitably generalised for the partial rectangular structure case. Similar proofs show that graph automorphism is (partial) algebra automorphism is partial rectangular structure automorphism.

```
find_allrs2(P)
  if P is a rectangular structure
    Print P
  else
    S := pos_one_ext(P)
    G := Aut(P)
    Orbs := Orbits of S under G
```

```
for o in Orbs
  rep = minimal(o)
  if rep < maximal(P)
    ignore, not a positive extension
  else
    find_all_rs2( Union( P, {rep}))
```

Definition 12. Given a partial rectangular structure $\mathcal{P}$, a rectangle R is *compatible* with $\mathcal{P}$ if $\mathcal{P} \cup \{R\}$ is a partial rectangular structure.

Lemma 34. Given a partial rectangular structure $\mathcal{P}$ and a compatible rectangle R, for all $\phi \in Aut(\mathcal{P})$, ϕR is compatible with $\mathcal{P}$.

The proof is a simple calculation.

Theorem 35. The algorithm above finds all representative partial rectangular structures.

Proof. We use induction on the size of the partial rectangular structure. For $|\mathcal{P}| = 1$ the only example is the starting rectangle, and we are done. Assume truth for size k. Take $\mathcal{P}$ of order $k+1$, a representative partial rectangular structure, $\mathcal{P} = \{R_1, \ldots, R_{k+1}\}$, $R_i < R_{i+1}$. By Proposition 33, $\mathcal{P}' = \{R_1, \ldots, R_k\}$ is representative, thu it will be found by the algorithm. Since R_{k+1} is compatible with $\mathcal{P}'$, so is ϕR_{k+1} for any $\phi \in Aut(\mathcal{P})$. Since $\mathcal{P}$ is representative, there is no $\phi \in Aut(\mathcal{P})$ such that $\phi R_{k+1} < R_{k+1}$. Thus R_{k+1} is minimal in its orbit, and is found by the algorithm. ■

Thus the resulting list is complete. The following section delves into the techniques for filtering out the isomorphic copies in the list.

9.3 Sieving the Full Partial Rectangular Structures

(This seems idiotic - needs a lot of polishing!!)

The last section showed that we can find large collections of rectangular structures. As indicated, although we have removed many branches in the search / generation tree, we still do not know whether these are all pairwise non–isomorphic, i.e. if they are all representative. In general this will not be the case. A primitive method is to compute the orbit of the full partial rectangular structure under the symmetric group on nm points and to take the minimal, i.e. representative, member of the orbit. Unfortunately, since we are dealing with sets of pairs of sets of points, the memory requirements quickly inflate to overwhelm any machine. Thus it is necessary to look at more efficient methods.

We have shown that rectangular structures are equivalent to idempotent semicentral bigroupoids, which are equivalent to the graph pairs (with loops) introduced in section 6.2. The question of isomorphism between two rectangular structures is equivalent to the question of isomorphism between two graph pairs. In the sequel, we assume that the graphs have loop edges on every arc, thus we can ignore them for the determination of isomorphism. Graph isomorphism is a rather standard problem in graph theory, the `nauty` package [18] is an efficient implementation of graph isomorphism. This package is available from GAP using the GRAPE package [32].

We are able to use these to filter the list of rectangular structures and obtain a collection of pairwise nonisomorphic structures. The algorithm runs as follows:

```
inlist := list of rectangular structures
outlist := empty list
graphlist := empty list
for RS in inlist do
  graphpair := Graph pair from RS
  if not graphpair in graphlist then
    add RS to outlist
    add graphpair to graphlist
  fi
od
```

The most exhaustive part is testing the existence of the graph pair in the list of graph pairs. Although `nauty` manages the automorphism problem well, it is still the most complex part of the algorithm. Using combinatorial properties of the rectangular structure can remove the necessity to check graph isomorphism. We can also combine the two graphs into one graph, the isomorphism of two graph pairs being equivalant to the isomorphism of two combined graphs. If the graph pair is A, B on node set $\{1,\ldots,n\}$, then using the labels a and b we construct a graph with nodes

$$\{(a,x),(b,x)|x\in\{1,\ldots,n\}\} \tag{163}$$

and edges

$$\{((a,x),(a,y))|(x,y)\in Edges(A)\}\cup\{((b,x),(b,y))|(x,y)\in Edges(B)\}\cup\{((a,x),(b,x))|x\in\{1,\ldots,n\}\}\}\cup\{((a,x),(a,x))|x\in\{1,\ldots,n\}\} \tag{164}$$

where we ignore the loop edges in the graphs A and B. It is easy to see that the graphs so constructed from two graph pairs are isomorphic iff the graph pairs are isomorphic.

9.4 Orderly algorithms

An alterbative approach is to ensure that the branching generation prcess does not generate isomorphic examples, thus removing the filtering step of the process described above. With careful bookkeeping, this can be done. Such generation processes have been called "orderly" in [27]. McKay has developed a general structure for such algorithms [19] and Royle has developed a simplified algorithm, [29] upon which we base ours.

This section introduces Royle's approach, then describes the functions necessary for this algorithm. We then look at the use of combinatorial identities to speed up the algorithm.

Let V be come set, $G = Aut(V)$. We write v^g for the action of $g \in G$ on $v \in V$ and extend naturally to actions on sets. We want to find all subsets $X \subset V$ such that $P(X)$ is true for some hereditary property P, but we want only one example from each isomorphism class, with isomorphism defined by G.

We require a function Θ such that

$$\Theta : 2^V \to 2^V \tag{165}$$

$$\Theta(X) \text{ is an orbit of } G_X \text{ on } X \tag{166}$$

$$\Theta(X^g) = \Theta(X)^g \forall g \in G \tag{167}$$

where G_X is the stabiliser of X, $G_X = \{g \in G | X^g = X\}$.

Let S_k be the set of sets of size k such that $P(X)$ is true for all $X \in S_k$, with no isomorphs. The following algorithm generates a set S_{k+1} from S_k.

```
for X in S_k
  for x representative in each orbit of G_X upon V - X
    if P(X + x) and x ∈ Θ(X + x) then
      add X + x to S_{k+1}
```

Theorem 36 (Royle[29], McKay [19]) *Let S_k contains exactly one representative from each G–orbit on k–sets of V that have property P. Then the set S_{k+1} contains exactly one representative from each G–orbit on $k+1$–sets of V that have property P.*

Starting with $S_0 = \{\emptyset\}$ we obtain an orderly algorithm for constructing one representative of each subset of V with property P. The problem is to define the function Θ.

One property of the `nauty` package is that it constructs a *canonical labelling* of a graph. A canonical labelling uniquely identifies each node of a graph up to automorphisms.

Definition 13. A *canonical mapping* α takes a graph $\Gamma = (N, E)$ and maps

$$\alpha : N \times \Gamma \to \{1, \ldots |N|\} \tag{168}$$

such that for any permutation ϕ of N,

$$\alpha(n^\phi, \Gamma^\phi) = \alpha(m, \Gamma) \Leftrightarrow \exists \psi \in Aut(\Gamma), n^\psi = m \tag{169}$$

This means that if we take the orbit of the minimal labelled point in a graph under the automorphism group of the graph, that orbit will be uniquely identified no matter how we relabel the graph. This forms the simplest mechanism for creating a Θ function.

Our situation is as follows. The set V is the set of $n \times m$ rectangles. P is the property of being a partial rectangular structure. We want to find the set S_{nm} of full partial rectangular structures, i.e. rectangular structures.

We define Θ as follows. We label rectangles R by their *middle*, the element in $R_1 \cap R_2$. We take a partial rectangular structure over to a graph, take the minimal canonically labelled point that is the middle of a rectangle in the partial rectangular structure, and then take its orbit under the automorphism group of the graph, respectively the rectangular structure. If the middle of the new rectangle is in the orbit, then we accept the new rectangle, otherwise not.

Note that we assemble only rectangles that will satisfy P.

Improvements can be made in the algorithm by using easily computed combinatorial properties of the partial rectangular structures to reduce the number of candidates. We define Θ to take the orbit of the minimally labelled node from the set of middles with minimum values of some combinatorial value. For instance, we look at the counts of occurrence of the middle in the left and right sets of the rectangles, obtaining a pair of integers, which we then order lexicographically. If there is a unique minimum for the combinatorial vales, we need not use the canonical labelling algorithm, thus saving computational effort.

9.5 Results

Timings and comparisms.

We have run the algorithms for examples up to order 10. The following table compares the times required for the partial rectangular structure algorithm, an improved version (not described above) that attempted to reduce branching with some bookkeeping, but still required filtering, and the orderly algorithm described above. We have included timings for $n \times m$ and $m \times m$ in a few cases where we ran both. There is no explanation for the differences in timings.

Size	Number	PRS + filter	Prohib + filter	Orderly
2×2	3	8+4	8+11	4
2×3	9	44 + 1:02	7+5	50
3×2		8 + 14		29
2×4	53	1:39+44:08	38+11:12	10:21
4×4		3:11+16:43	1:08+7:47	10:59
3×3	184	72 hours (approx)	8:30+28:38:01	6:03:00
2×5	813	104:37:00+55:56:00		10:34:00

Although the range of values is too low to make any decent estimations of what is going on here, it seems to be apparent that the orderly approach is the more efficient, though the prohibition technique (not yet tested at 2×5) might also be effective. (DO THIS!)

In Section 7 we saw results about the uniqueness of liftings up to isomorphism. From the graph representation of a rectangular structure we obtain the automorphism group of the rectangular structure. Given the automorphism group of a rectangular structure we are able to determine representatives for the lifting actions and to determine how many distinct liftings of one idempotent semicentral bigroupoid there are. Thus we are able to generate comprehensive lists of distinct semicentral bigroupoids and realise that there are several million examples up to order 10. This wealth of examples is an embarrassment of riches, determining which examples are of interest is difficult, and must be one aim of further work.

10. Conclusion and further work

This paper has summarised the work of my thesis investigating some interesting and, it appears, productive connections between cellular automata theory, abstract algebra, combinatorics and algebraic programming. Moving from a computational model, through an algebraic formulation to a combinatoric interpretation allows us to strip away layers of structure and expose the elements that make up the structure in a clear form. Using ideas for algorithms for listing combinatorial objects that have been developed over recent years, we are able to efficiently list one dimensional reversible cellular automata.

Many questions remain open. Some date from the work of Shader, Knuth, et al in the 1970s, such as techniques to generate all central groupoids, or equivalently, to determine all 0-1 matrices A such that $A^2 = J$. It is possible that the techniques touched upon here might offer some inroads into this problem.

Other questions are more related to the structures here.

I feel that the more important questions relate to the connections between computational aspects of a given cellular automata and the algebraic and/or combinatorial properties of the semicentral bigroupoid that corresponds to it. What are the connections between computational power in a cellular automata and the algebraic structure on the semicentral bigroupoid derived from it? Is universal computability related to any algebraic property? Are ergodicity or other properties of interest to cellular automata theoretists related to any algebraic properties of semicentral bigroupoids? Is isotropism or some other form of algebraic equivalence of more relevance for cellular automata theorists than isomorphism? How much more structure is forced by requirements such as additivity?

Are the graph pairs described here of any independent relevance? Inasmuch as structure was a leading light in this research, it might be hoped that the continuous structure in cellular automata (see [28]) might be analogous to the continuous structure in algebras, where for instance this structure allowed the classification of finite simple Lie groups to be completed almost a century before the general case. Can we say more about these algebraic structures using continuity arguments?

Many questions, and many more lie just beneath the surface. Perhaps we can see here that although bridges from computational ideas to algebraic models are buildable, the techniques that are most appropriate for their analysis need to be selected more widely that simply from the armoury of classical abstract algebra.

References

[1] Charles H. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, pages 525–532, November 1973.

[2] Tim Boykett. *Algebraic Aspects of Reversible Computation*. PhD thesis, University of Western Australia, 1997.

[3] Tim Boykett and Cris Moore. Single state conserved quantities in one dimensional cellular automata. *Complex Systems*, 11:55–64, 1997.

[4] Arthur A. Drisko and Cris Moore. Alebraic properties of the block transformation on cellular automata. *Complex Systems*, 10:185–194, 1996.

[5] Martin Schönert et al. GAP, groups algorithms and programming. Technical report, Lehrshuhl D für Mathematik, RWTH Aachen, 1994.

[6] Trevor Evans. Products of points – some simple algebras and their identities. *Am. Math. Monthly*, pages 362–372, April 1967.

[7] M.A. Fiol, I. Alegra, J.L.A. Yebra, and J. Fàbrega. Digraphs with walks of equal lengths between vertices. In Y. Alavi, G. Chartrand, L. Lesnick, D.R. Lick, and C.E. Wall, editors, *Graph Theory with Applications to Algorithms and Computer Science*, pages 313–322. John Wiley, 1985.

[8] David Gelernter. Generative communication in Linda. *ACM Trans. Prog. Lang. and Sys.*, 7(1):80–112, January 1985.

[9] David Hillman. The structure of reversible one–dimensional cellular automata. *Physica A*, 52:277–292, 1991.

[10] A.J. Hoffman. Research problem 2-11. *J. Combinatorial Theory*, 2:393, 1967.

[11] J. Kari. Reversibility of 2D cellular automata is undecidable. *Physica D*, 45:379–385, 1993.

[12] Donald E. Knuth. Notes on central groupoids. *Journal of Combinatorial Theory*, 8:376–390, 1970.

[13] C.W.H. Lam. On rational circulants satisfying $A^m = dI + \lambda J$. *Lin. Alg. App.*, 12:139–150, 1975.

[14] C.W.H. Lam. On some solutions of $A^m = dI + \lambda J$. *J. Comb. Theory Ser. A*, 29:140–147, 1977.

[15] H. Länger. Induced groupoids and induced semigroups. In Hermann Kautschitsch et al., editors, *Contributions to General Algebra*, pages 177–186. Verlag Johannes Heyn, 1979.

[16] L. Le Bruyn and M. Van Den Bergh. Algebraic properties of linear cellular automata. *Linear algebra and its applications*, 157, nov 1991.

[17] S.L. Ma. On rational circulants satisfying $A^m = dI + \lambda J$. *Lin. Alg. App.*, 62:155–161, 1984.

[18] B.D. McKay. `nauty` user's guide. Technical report, Department of Computer Science, Australian National University, 1990.

[19] B.D. McKay. Isomorph-free exhaustive generation. *J Algorithms*, 26:306–324, 1998.

[20] David McLean. Idempotent semigroups. *American Math Monthly*, 64:110–113, February 1954.

[21] Cris Moore. Non–abelian cellular automata. Technical Report 95-09-081, Sante Fe Institute, 1995.

[22] Cris Moore. Quasi–linear cellular automata. *Physica D*, 103:100–132, 1997.

[23] Kenichi Morita and Masateru Harao. Computation universality of one–dimensional reversible (injective) cellular automata. *Transactions of the IEICE*, E 72(6):758–762, 1989.

[24] Otero. Extraction of the mth roots in matrix rings over fields. *Lin. Alg. App.*, 128:1–26, 1990.

[25] John Pedersen. Cellular automata as algebraic systems. *Complex Systems*, 6:237–250, 1992.

[26] Hala O. Pflugfelder. *Quasigroups and Loops: Introduction*. Number 7 in Sigma Series in Pure Mathematics. Heldermann, 1990.

[27] R.C. Read. Every one a winner. *Annals of Discrete Mathematics*, 2:107–120, 1978.

[28] D. Richardson. Tesselations with local transformations. *J. Comp. Sys. Sci.*, 6:373–388, 1972.

[29] Gordon F. Royle. An orderly algorithm and some applications in finite geometry. *Discrete Mathematics*, 185:105–115, 1998.

[30] H.J. Ryser. A generalisation of the matrix equation $A^2 = J$. *Lin. Alg. App.*, 3:451–460, 1970.

[31] Leslie E. Shader. On the existence of finite central groupoids of all possible ranks. *J. Combinat. Theory Ser A*, 16:221–229, 1974.

[32] L.H. Soicher. GRAPE: a system for computing with graphs and groups. In L. Finklestein and W.M. Kantor, editors, *Groups and Computation*, volume 11 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 287–291. A.M.S., 1993.

[33] Tommaso Toffoli and Norman H. Margolus. Invertible cellular automata: a review. *Physica D*, 45:229–253, 1993.

[34] Vorhees. A note on injectivity of additive cellular automata. *Complex Systems*, 8:151–159, 1994.

[35] K. Wang. On the matrix equation $A^m = \lambda J$. *J. Comb. Theory Ser. A*, 29:134–141, 1980.

[36] K. Wang. On the g–circulant solutions to the matrix equation $A^m = \lambda J$. *J. Comb. Theory Ser. A*, 33:287–296, 1982.