Structure of the Invertible CA Transformations Group

Leo Liberti\textsuperscript{1}

E-mail: l.liberti@ic.ac.uk

March 1998

Abstract

We describe the structure of the group of all invertible CA transformations acting on 1-dimensional finite-length cellular automata defined on a finite states set. It turns out that the group is a direct product of semidirect products of cyclic and symmetric groups. The analysis of this group has been carried out by means of an isomorphic image of the invertible CA transformations group, which was easier to handle. A presentation of the group by generators and relations is also supplied. Most of the results obtained can also be applied to analyse the automorphism group of any finite one-to-one dynamical system.

Contents

1 Introduction \hfill 1

2 Inner Structure of an Invertible CA Transformation \hfill 3
   2.1 Orbits \hfill 3
   2.2 Permutative Effect \hfill 5
   2.3 Shifting Effect \hfill 6

3 The CA Group Isomorphism \hfill 6
   3.1 CA Group Product \hfill 7
   3.2 The Main Theorem \hfill 7
   3.3 CA Group Generators \hfill 8
      3.3.1 Normal Form \hfill 9
   3.4 CA Group Relations \hfill 10
   3.5 A Simple Example \hfill 12

4 Conclusion \hfill 13

1 Introduction

Normally research about CAs is performed with a special mind to computation; that is, all sorts of “brute force” and statistical approaches to the problems are tried. Finite States Machines, and in particular Cellular\footnote{Correspondence address: Centre for Process Systems Engineering, Imperial College, London SW7 2BY, U.K.}
Automata, are often considered as a Computer Scientist’s rather than a Mathematician’s tools. In most cases where a mathematical approach is employed, attention is normally limited to linear CAs, i.e. to all those CA transformations which can be represented as $n \times n$ matrices acting on automata of length $n$. As $n$ gets larger, this means that the near totality of CAs are ignored. This is excessively restrictive, if we keep in mind that the most useful CA transformations (for cryptography, for example) are in fact the nonlinear ones. On the other hand, it is this author’s opinion that a systematic algebraic study of CAs should not restrict itself to a certain class of CAs, but should from the beginning try to aim at generality, even at the expense of immediate practical applications. This is the reason why throughout this paper a general algebraic approach has been tried, rather than a specific computational one.

A 1-dimensional finite cellular automaton is a shift-commuting, 1-dimensional, finite discrete dynamical system. More precisely, it is a couple $(\psi, \sigma)$ consisting of a finite sequence $\psi$ of length $n$ defined on a (finite or infinite) states set $R$ together with a transformation $\sigma : R^n \to R^n$ such that $\sigma$ commutes with the shift. The shift is a function $R^n \to R^n$ that moves every sequence in $R^n$ one step towards the left with “wrap-around” effect on the contour, i.e.

$$(v_1, v_2, \ldots, v_n) \alpha = (v_2, v_3, \ldots, v_n, v_1)$$

Notice that throughout this paper we shall use the “right hand side” notation when applying a function to a sequence or to a vector, i.e. $\psi \alpha$ and not $\alpha(\psi)$. We can also picture the shift as the effect of the permutation $(12\ldots n)$ on the indices of the components of the sequences. We will limit our discussion to those cellular automata (CA) defined on finite states sets $R$.

The most fundamental properties of CAs (indeed the reason why they are useful) is that their associated transformation can be localized. To every shift-commuting CA transformation $\sigma : R^n \to R^n$ there corresponds a function $\phi : R^m \to R$ where $m \leq n$. $\phi$ is applied to $\psi$ component-wise, in the following fashion: let $v_i^t$ be the $i$-th component of $\psi$ at timestep $t$, and let $V(v_i^t)$ be the neighbourhood of $m$ components to the left of and including the $i$-th position (the shape of the neighbourhood is entirely arbitrary; it is possible to choose any neighbourhood of length $m$, but to each neighbourhood there corresponds a different $\phi$). Then

$$v_i^{t+1} = \phi(V(v_i^t))$$

The difference between the action of $\sigma$ and of $\phi$ is shown graphically in the picture below. Localization makes it very easy to compute the evolution of a CA: it is sufficient to make fast calculations in parallel for each cell of the CA.

$$
\begin{array}{cc}
\sigma & \phi \\
\hline
\begin{array}{ccc}
\square & \ldots & \square \\
\downarrow & & \downarrow \\
\square & \ldots & \square \\
\end{array}
&
\begin{array}{ccc}
\square & \ldots & \square \\
\end{array}
\end{array}
$$

Cellular automata are often used in gas simulations. We know from thermodynamics that the transformations involved are microscopically reversible but macroscopically irreversible. In order to simulate gas behaviour with CAs, we must find appropriate reversible transformations and then apply them to the automaton grid for a number of times. We therefore focus the attention on two fundamental topics: reversible transformations, which we shall also call invertible transformations, and the concept of applying many times the same transformation to a cellular automaton. To this end we need to introduce a product $\ast$ of transformations defined by the composition of transformations: for all $\psi$ in $R^n$ and for CA transformations $\sigma$ and $\tau$

$$\psi (\sigma \ast \tau) = ((\psi \sigma) \tau)$$

Let $A^n(R)$ be the set of all CA transformations $\sigma$ acting on $R^n$. By shift commutativity it is easy to show that the algebraic structure $(A^n(R), \ast)$ has an identity and is closed and associative. In short, it is a monoid. We are now interested in finding out what the structure of the group $G^n(R)$ contained in $A^n(R)$ and consisting of all invertible CA transformations is like. Notice that the inverse of a CA transformation is still a
2 Inner Structure of an Invertible CA Transformation

A CA transformation belongs to the group $G^n(R)$ if and only if it is invertible; since $R$ has a finite number of elements we can say that a CA transformation is invertible if and only if it permutes the elements of $R^n$. In order to determine whether a given CA transformation is a permutation we need to know its effect over all the elements of $R^n$. The way a CA transformation acts on the sequences of $R^n$ is intimately linked to the way $\alpha$ (the shift transformation) partitions $R^n$ into orbits. Let $\sigma$ be a CA transformation. Since for all $j$

$$( \alpha^j \sigma ) \sigma = ( \sigma \alpha ) \alpha^j$$

it follows that is sufficient to calculate the effect of $\sigma$ on a representative (say $v$) of the orbit

$$O(v) = \{ \alpha^j \sigma \mid j \in \mathbb{Z}_n \}$$

in order to know the effect of $\sigma$ over all elements of $O(v)$. This implies that it is sufficient to know what the restriction of $\sigma$ to a set of representatives of the orbits looks like in order to describe $\sigma$ completely.

We shall see that if $\sigma$ is an invertible CA transformation its effect can be viewed as being split in two definite parts: the permutation of the orbits of $R^n$ under the shift and the shifting of the successions of $R^n$.

2.1 Orbits

We need to introduce some definitions. Let $G$ be any group. We call a set $X$ a $G$-set if there is a product between the elements of $G$ and the elements of $X$ such that for all $x \in X$ and being $1$ the identity of $G$ we have $x1 = x$ and such that for all $g, h \in G$ and for all $x \in X$ we have $x(gh) = (xg)h$. For each element $x$ in $X$ we define the orbit of $x$ as $xG = \{ xg \mid g \in G \}$. We call $|xG|$ the length or period of the orbit.

We now consider the cyclic group $C_n = \{ \alpha^i \mid i < n \}$ of order $n$ acting on the set $R^n$.

2.1 Proposition

For each $v \in R^n$ we have that $|vC_n|$ divides $n$.

Proof. We define a product $\times$ on the orbit $vC_n$ such that

$$(v\alpha^i) \times (v\alpha^j) = v\alpha^{i+j}$$

The product $\times$ is obviously closed, $v1$ is the identity and for each $i$ we have

$$(v\alpha^i) \times (v\alpha^{n-i}) = v1$$

hence $(vC_n, \times)$ is a group. We now define the map $\phi : C_n \rightarrow vC_n$ given by $\alpha^i \phi = v\alpha^i$. $\phi$ is clearly a surjective group homomorphism, therefore $\text{Im} \phi = vC_n$ is isomorphic to a subgroup of $C_n$. By Lagrange’s theorem we then have that $|vC_n|$ divides $|C_n|$ and hence

$$\forall v \in R^n \ (|vC_n| \mid n)$$
The converse is also true.

2.2 Proposition
If $|R| \geq 2$, for each divisor $d$ of $n$ there is an orbit of length $d$.

Proof. Let $a, b \in R$ such that $a \neq b$. Then

$$
\nu_0 = \left( a, b, \ldots, a, b, \ldots, a, b, \ldots, b \right)
$$

is clearly such that $\nu_0 \alpha^d = \nu_0$ and $\nu_i \alpha^i \neq \nu_0$ for each $i$ in the range $0 < i < d$. □

Hence for each divisor $d$ of $n$ there are orbits of length $n$ and those are the only lengths orbits of $R^n$ can have. We indicate with $\delta(n)$ the number of divisors of $n$. It is easy to show that if $n = p_1^{e_1} \cdots p_t^{e_t}$ is the unique prime factorization of $n$, then

$$
\delta(n) = \prod_{i=1}^t (e_i + 1)
$$

We are now interested in how many orbits of length $d$ there are in $R^n$. We define two functions:

$$
\Omega_R(d) = \text{number of sequences in } R^n \text{ of period } d
$$

$$
\omega_R(d) = \text{number of orbits in } R^n \text{ of period } d
$$

Notice that $\omega_R(d) = \frac{1}{d} \Omega_R(d)$ because in $R^n$ there are $\Omega_R(d)$ sequences having period $d$ partitioned in disjoint orbits of length $d$.

2.3 Proposition
For each integer $n$ and for each $d | n$,

$$
\omega_R(d) = \frac{1}{d} \sum_{t | d} \mu(t) |R|^\frac{d}{t}
$$

where $\mu$ is the Möbius arithmetic function defined as

$$
\mu(m) = \begin{cases} 
1 & \text{if } m = 1 \\
(-1)^k & \text{if } m \text{ is a product of } k \text{ distinct primes} \\
0 & \text{otherwise}
\end{cases}
$$

Proof. First of all observe that $R^d$ is composed by all sequences belonging to orbits of period $t$ for all divisors $t$ of $d$. We can write this with

$$
|R|^d = \sum_{t | d} \Omega_R(t) = \sum_{t | d} t \omega_R(t)
$$

By the Möbius inversion formula we then have

$$
d \omega_R(d) = \sum_{t | d} \mu(t) |R|^\frac{d}{t}
$$

and hence

$$
\omega_R(d) = \frac{1}{d} \sum_{t | d} \mu(t) |R|^\frac{d}{t}
$$

\footnote{The proof to proposition (2.3) was suggested by Prof. Umberto Cerruti, of the Dept. of Mathematics of University of Turin.}
Now we take into account a CA transformation $\tau \in \mathcal{A}^n(R)$ and given an orbit $\underline{u}C_n$ we examine the length of the orbit $(\underline{u}\tau)C_n$.

### 2.4 Proposition
For each $\tau \in \mathcal{A}^n(R)$ and each $\underline{u} \in R^n$ the length of the orbit $(\underline{u}\tau)C_n$ divides the length of the orbit $\underline{u}C_n$.

**Proof.** We use the product $\times$ defined in the previous proposition (2.1), where we also proved that $(\underline{u}C_n, \times)$ is a group. We now define a function $\theta : \underline{u}C_n \rightarrow (\underline{u}\tau)C_n$ such that $(\underline{u}\alpha^i)\theta = (\underline{u}\alpha^i)\tau$. $\theta$ is well-defined because $\tau$ is a shift transformation. Furthermore, $\theta$ is a group homomorphism: given elements $\underline{u}\alpha^i$ and $\underline{u}\alpha^j$ in $\underline{u}C_n$ we have

$$( (\underline{u}\alpha^i)\theta \times (\underline{u}\alpha^j) = (\underline{u}\alpha^{i+j})\tau$$

Since $\tau \in \mathcal{A}^n(R)$ it commutes with all powers of the shift transformation, i.e., with $\alpha^j$ for all $j$, hence

$$(\underline{u}\alpha^{i+j})\tau = (\underline{u}\tau)\alpha^{i+j} = ((\underline{u}\tau)\alpha^i) \times ((\underline{u}\tau)\alpha^j)$$

Again by shift commutation this equals

$$( (\underline{u}\alpha^i)\tau \times (\underline{u}\alpha^j)\tau = ( (\underline{u}\alpha^i)\theta \times (\underline{u}\alpha^j)\theta)$$

We now check inverses. For each $i$,

$$(\underline{u}\alpha^{-i})\theta = (\underline{u}\alpha^{-i})\tau = (\underline{u}\tau)\alpha^{i-1} = ((\underline{u}\tau)\alpha^i)^{-1} = ((\underline{u}\alpha^i)\tau)^{-1} = (\underline{u}\alpha^i)\theta^{-1}$$

Furthermore $\theta$ is surjective: let $\underline{u} \in (\underline{u}\tau)C_n$; then for some $i$

$$\underline{u} = (\underline{u}\tau)\alpha^i = (\underline{u}\alpha^i)\tau = (\underline{u}\alpha^i)\theta$$

Hence the image of $\theta$ is $(\underline{u}\tau)C_n$, which implies that $(\underline{u}\tau)C_n$ is isomorphic to a subgroup of $\underline{u}C_n$. By Lagrange’s theorem the result follows. \qed

Now we restrict the attention to $\tau \in \mathcal{G}^n(R)$, i.e., let $\tau$ be invertible.

### 2.5 Proposition
Let $\tau \in \mathcal{A}^n(R)$. If $\tau$ is invertible then for each $\underline{v} \in R^n$ we have

$$| (\underline{v}\tau)C_n | = | \underline{v}C_n |$$

**Proof.** Let $\theta : \underline{u}C_n \rightarrow (\underline{v}\tau)C_n$ given by $(\underline{v}\alpha^i)\theta = (\underline{v}\alpha^i)\tau$ for each $i$. We have shown in the proof of proposition (2.4) that $\theta$ is a group homomorphism. Since $\tau$ is invertible we conclude that $\theta$ is an isomorphism. This concludes the proof. \qed

### 2.2 Permutative Effect

We are now in the position to start investigating the effect of an invertible CA transformation $\sigma$ on the orbits of $R^n$ under the shift. For simplicity of notation let’s agree to set $k = \delta(n)$, the number of divisors of $n$, and $z_i = \omega_R(d_i)$, the number of orbits of length $d_i$ in $R^n$, where $d_i$ is the $i$-th divisor of $n$ in ascending order. Let $O^n$ be the set of orbits of $R^n$, i.e.,

$$O^n = \{ \underline{u}C_n \mid \underline{u} \in R^n \}$$

Now define the restriction $\bar{\sigma}$ of $\sigma$ to $O^n$:

$$(\underline{v}C_n)\bar{\sigma} = (\underline{v}\sigma)C_n$$

5
Basically all this restriction does is concentrate on the action $\sigma$ has on the orbits, rather than on single successions. The restriction is well-defined because all CA transformations commute with the shift.

We have shown in proposition (2.5) that if $\sigma$ is invertible, $\bar{\sigma}$ necessarily sends every orbit into an orbit of the same period. So for all $i \leq k$ and for all $j \leq z_i$ we have

\[(\mathcal{U}_{i,j} C_n) \bar{\sigma} = \mathcal{U}_{i,\bar{\sigma}(j)} C_n\]

for some function $\bar{\sigma}_i$ (which clearly depends on $\bar{\sigma}$) defined on the set \{1, \ldots, z_i\}. Hence $\bar{\sigma}$ can be described by a $k$-tuple $(\bar{\sigma}_1, \ldots, \bar{\sigma}_{z_i})$ where each of the $\bar{\sigma}_i$ specifies the effect of $\bar{\sigma}$ within each class of orbits having the same period.

**2.6 Proposition**
The restriction $\bar{\sigma}$ is invertible if and only if, for each $i$ such that $1 \leq i \leq k$, $\bar{\sigma}_i$ is a permutation of the set \{1, \ldots, $z_i$\}, i.e. $\bar{\sigma}_i \in S_{z_i}$.

**Proof.** ($\Leftarrow$): every permutation in $S_{z_i}$ is also a function \{1, \ldots, $z_i$\} $\rightarrow$ \{1, \ldots, $z_i$\}.

($\Rightarrow$): In order for $\bar{\sigma}$ to be invertible, each of the $\bar{\sigma}_i$ must be invertible, hence the $\bar{\sigma}_i$ are permutations defined on the set \{1, \ldots, $z_i$\}, i.e. elements of the symmetric group $S_{z_i}$.

\[\square\]

**2.3 Shifting Effect**

We now extend $\bar{\sigma}$ back to the function $\sigma : R^n \rightarrow R^n$ by adding back the structure relative to the shifts. Let $S$ be a double-indexed list of representatives of the orbits

\[S = \{\mathcal{U}_{i,1}, \ldots, \mathcal{U}_{i,z_i}, \ldots, \mathcal{U}_{k,1}, \ldots, \mathcal{U}_{k,z_k}\}\]

such that $\mathcal{U}_{i,j}$ is a representative of the $j$-th orbit having period $d_i$. For each $\mathcal{U}_{i,j}$ we need to specify what power of the shift we should apply to it:

\[\mathcal{U}_{i,j}^{\sigma} = \mathcal{U}_{i,\sigma(i)}^{\sigma_{i,j}}\]

Notice that $0 \leq e_{i,j} < d_i$ as the vector $\mathcal{U}_{i,j}$ belongs to an orbit with period $d_i$.

Hence we can completely describe $\sigma$ by means of the $k$ permutations $\bar{\sigma}_i \in S_{z_i}$ and the powers of the shift $e_{i,j} \in Z_{d_i}$ where $1 \leq i \leq k$ and $1 \leq j \leq z_i$. I.e., to each $\sigma \in \mathcal{G}^n(R)$ we can associate a $k$-tuple of the form

\[((e_{1,1}, \ldots, e_{1,z_1}), \bar{\sigma}_1), \ldots, (e_{k,1}, \ldots, e_{k,z_k}), \bar{\sigma}_k)\]

where $e_{i,j} \in Z_{d_i}$ and $\bar{\sigma}_i \in S_{z_i}$. It is evident that given such a $k$-tuple we can find the invertible CA transformation that corresponds to it, so this is a bijection.

For each $i$, let $G_i = Z_{d_i}^2 \times S_{z_i}$. We have constructed a special bijection between $\mathcal{G}^n(R)$ and the set $\prod_{i=1}^k G_i$. In the next section we shall show that this bijection is really a group isomorphism.

**3 The CA Group Isomorphism**

Call $\Gamma$ the bijection we have just defined, i.e., for each $i \leq k$ let $G_i = Z_{d_i}^2 \times S_{z_i}$, let $X = \prod_{i=1}^k G_i$ and let

\[\Gamma : \mathcal{G}^n(R) \rightarrow X\]

so that for $\sigma \in \mathcal{G}^n(R)$, $\sigma \Gamma$ is the $k$-tuple described in equation (2). In order to show that $\Gamma$ is a group isomorphism, we define a suitable product in $X$ and then we need only prove that given $x, y \in X$,

\[(xy)\Gamma^{-1} = (x\Gamma^{-1})(y\Gamma^{-1})\]

\[\text{(3)}\]
3.1 CA Group Product

Recall that $X$ is a direct product of the sets $G_i$. The product on $X$ will be defined quite naturally as the “cartesian product of the products” on the sets $G_i$; we shall therefore define the product on the set $G_i$. We have already seen that the set $G_i$ is given by

$$\{(e_{i,1}, \ldots, e_{i,z_i}), \pi_i \mid \forall j \ e_{i,j} \in \mathbb{Z}_{d_i}, \pi_i \in S_{z_i} \}$$

Let $x_i, y_i$ be generic elements in $G_i$:

$$x_i = ((e_{i,1}, \ldots, e_{i,z_i}), \pi_i)$$  \hspace{1cm} (4)

$$y_i = ((f_{i,1}, \ldots, f_{i,z_i}), \pi_i)$$  \hspace{1cm} (5)

The product on $G_i$ is defined by

$$x_i y_i = \{(e_{i,1}, \ldots, e_{i,z_i}), \pi_i \mid \forall j \ \pi_j \in S_{z_j} \}$$

$$= ((e_{i,1}, \ldots, e_{i,z_i}) + (f_{i,1}, \ldots, f_{i,z_i}) \pi_i, \pi_i)$$

$$= ((e_{i,1} + f_{i,1}, \ldots, e_{i,z_i} + f_{i,z_i}), \pi_i)$$  \hspace{1cm} (6)

where the sums are intended mod $d_i$. Notice that this product is a semi-direct product of cyclic and symmetric groups, i.e.

$$G_i \cong C_{d_i} \rtimes S_{z_i}$$

In practice the product in the second component is an ordinary permutation product, whereas the product in the first component depends on the second component (the permutation) of the first term. Notice that the semi-direct product involved depends on the first term only because we agreed to use right function application, as in $xf$. If we were using left function application, as in $f(x)$, this would be the second term.

Now let $x, y$ be generic elements of $X$:

$$x = (x_1, \ldots, x_k)$$  \hspace{1cm} (7)

$$y = (y_1, \ldots, y_k)$$  \hspace{1cm} (8)

where each of the $x_i, y_i$ is defined as in equations (4), (5). We define the product on $X$ by means of the products on the $G_i$, so that

$$xy = (x_1 y_1, \ldots, x_k y_k)$$

where each of the $x_i y_i$ is given by equation (6).

3.2 The Main Theorem

In this section we shall show that the equation (3) holds, which will immediately imply that $G^n(R)$ and $X$ are isomorphic.

3.1 Theorem
For all $x, y \in X$

$$(xy)\Gamma^{-1} = (x\Gamma^{-1})(y\Gamma^{-1})$$

Proof. We have seen in equation (1) that for $\sigma \in G^n(R)$ and for each representative of the orbits $\mathcal{U}_{i,j}$ we have

$$\mathcal{U}_{i,j} \sigma = \mathcal{U}_{i,\sigma_{i,j}} \alpha_{\sigma_{i,j}}$$

where $\sigma_i$ is the $i$-th permutation in $S_{z_i}$ associated with $\sigma$. Let $x, y \in X$ be defined as in equations (7), (8). We have

$$xy = (x_1 y_1, \ldots, x_k y_k)$$
where
\[ x_i y_i = ((e_{i_1} + f_{i_1}, i_1), \ldots, e_{i_k} + f_{i_k}, i_k, \sigma_i, \tau_i) \]
so that, for each representative of the orbits \( \psi_{i,j} \) we have
\[ \psi_{i,j}(x y) = \psi_{i,j}(\sigma_i, \tau_j) \quad \alpha^{e_{i,j} + f_i, \tau_i} \]
On the other hand,
\[ \psi_{i,j}(x \Gamma^{-1}) = \psi_{i,j}(\sigma_i, \tau_j) \alpha^{e_{i,j}} \]
\[ \psi_{i,j}(y \Gamma^{-1}) = \psi_{i,j}(\sigma_i, \tau_j) \alpha^{f_i, \tau_i} \]
which implies
\[ \psi_{i,j}(x \Gamma^{-1})(y \Gamma^{-1}) = (\psi_{i,j}(\sigma_i, \tau_j) \alpha^{e_{i,j}})(y \Gamma^{-1}) \]
\[ = (\psi_{i,j}(\sigma_i, \tau_j)(y \Gamma^{-1}) \alpha^{e_{i,j}}) \]
\[ = \psi_{i,j}(\sigma_i, \tau_j) \alpha^{f_i, \tau_i} \alpha^{e_{i,j}} \]
\[ = \psi_{i,j}(\sigma_i, \tau_j) \alpha^{e_{i,j} + f_i, \tau_i} \]
which is the same as (9). This completes the proof. \( \square \)

### 3.3 CA Group Generators

We shall now find a minimal set of generators for each of the groups \( G_i \); the direct product of these generators will result in the generators for the group \( X \) which is isomorphic to \( G^n(R) \). We remind the reader that \( G_i \approx C_{d_i} \times S_{z_i} \).

It is a well-known fact that the \( z_i - 1 \) two-cycles \((1, 2), (1, 3), \ldots, (1, z_i)\) are a minimal set of generators for the symmetric group \( S_{z_i} \). Let’s agree to call these two-cycles \( \gamma_1, \ldots, \gamma_{z_i-1} \) (so that \( \gamma_j = (1, j + 1) \)) and the identity of the symmetric group \( \eta \). Now notice that given a generic element \((e_{i_1}, \ldots, e_{i_{z_i}}, \pi_i)\) in \( G_i \) where \( \pi_i \) is a product of two-cycles \( \gamma_{j_1} \cdots \gamma_{j_k} \), the following relation holds:
\[ ((e_{i_1}, \ldots, e_{i_{z_i}}, \pi_i)) = \]
\[ = [((1, 0, \ldots, 0), \eta)^{e_{i_1}} \cdots ((0, \ldots, 0, 1), \eta)^{e_{i_{z_i}}} \prod_{j=1}^{q} ((0, \ldots, 0, \gamma_{j_k}))] \quad (10) \]
(also see paragraph (3.3.1) for a more detailed discussion of this relation). Hence if \( \alpha_i = (12 \ldots z_i) \) and
\[ x_{i,j} = ((1, 0, \ldots, 0, \alpha_i^j, \eta) \quad \forall \quad j \leq z_i \]
\[ y_{i,f} = ((0, \ldots, 0, \gamma_f) \quad \forall \quad f \leq z_i - 1 \]
we obtain that \( G_i \) is generated by all \( x_{i,j}, y_{i,f} \). This set, however, is not minimal. Notice that for each \( j \leq z_i \), if \( f \) is such that the permutation \( \gamma_f \) moves \( j \),
\[ y_{i,f} x_{i,j} y_{i,f}^{-1} = \]
\[ = ((0, \ldots, 0, \gamma_f)((1, 0, \ldots, 0, \alpha_i^j, \eta)((0, \ldots, 0), \gamma_f^{-1}) = \]
\[ = ((1, 0, \ldots, 0) \alpha_i^j \gamma_f, \gamma_f)((0, \ldots, 0), \gamma_f^{-1}) = \]
\[ = ((1, 0, \ldots, 0) \alpha_i^j \gamma_f, \eta) = x_{i, \gamma_f(j)} \]
and hence, in particular, conjugating one of the \( g_{i,j} \), say \( g_{i,1} \), with all the \( h_{i,f} \) whose associated permutation moves 1, we obtain all the other \( g_{i,j} \). Thus we define

\[
x_i = x_{i,1} = ((1,0,\ldots,0),\eta)
\]

and we claim that the set

\[
M_i = \{y_{i,f} \mid 1 \leq f \leq z_i - 1\} \cup \{x_i\}
\]

is a minimal set of generators for the group \( G_i \).

### 3.2 Proposition

*Provided the length of the automaton, \( n_i \), is greater than 1, the set \( T_i \) is a minimal set of generators for the group \( G_i \).*

**Proof.** We have already verified that \( M_i \) is a set of generators. Now we have to show that it is minimal. Suppose there is an integer \( c \) such that \( M_i \setminus \{y_{i,c}\} \) is a set of generators. Hence \( S_{z_i} \) is generated by all the two-cycles but \((1,c+1)\), which is a contradiction. Now suppose that \( M_i \setminus \{x_i\} \) is a set of generators: we then have

\[
G_i = \{(0,\ldots,0,\gamma_f) \mid 1 \leq f \leq z_i - 1\} \cong S_{z_i}
\]

This implies \( d_i = 1 \), which means that the \( i \)-th orbit has period 1; i.e., \( i = k \) and \( n = 1 \), the trivial case, which, again, is a contradiction. The result follows. \( \square \)

A minimal set of generators for \( X \) is therefore

\[
M = M_1 \times \ldots \times M_k.
\]

### 3.3.1 Normal Form

It will be useful to see how we can express a generic element of \( G_i \) in terms of the generators found in the previous section. We shall call this expression the **normal form** for an element of \( G_i \). This in fact is just a restatement of equation (10), which bears a deep significance to this issue. Consider a general element of \( G_i \), say \((e_{i,1},\ldots,e_{i,z_i}),\pi_i\). This, as we already noted, can be written as follows:

\[
((e_{i,1},\ldots,e_{i,z_i}),\pi_i) = \left( ((1,0,\ldots,0),\eta)^{e_{i,1}} \cdots ((0,\ldots,0,1),\eta)^{e_{i,z_i}} \right) \prod_{j=1}^{q} ((0,\ldots,0,\gamma_{y_j}) \quad \right)
\]

\[
= \left( (x_i^{e_{i,1}}) (y_{i,1} x_i y_{i,1}^{-1})^{e_{i,2}} \cdots (y_{i,z_i-1} x_i y_{i,z_i-1}^{-1})^{e_{i,z_i}} \right) \prod_{j=1}^{q} y_{i,j} 
\]

We can write the above equation in a more compact form as

\[
((e_{i,1},\ldots,e_{i,z_i}),\pi_i) = x_i^{e_{i,1}} \left[ \prod_{j=1}^{z_i-1} (y_{i,j} x_i y_{i,j}^{-1})^{e_{i,j+1}} \right] \prod_{j=1}^{q} y_{i,j}.
\]

It is worth noting that the normal form is unique.
3.4 CA Group Relations

We aim to give a presentation of the group $G^n(R)$ by means of generators and relations. We found a minimal set of generators $M$ for $X$ in the previous section; we now find the relations between them. For clarity of notation, we get rid of the index $i$, which only refers to $G_i$. We shall agree to set $G = G_i$, $x = z_i$, $y_f = y_i, f$, $z = z_i$ and $d = d_i$. We also set $y_0 = (0, \ldots , 0, \eta)$ as the identity of $G$.

1. Notice first that the $\gamma_f$ generate $S_z$. This implies all the relations on $y_f$ which define the symmetric group $S_z$.

2. We have observed earlier on (see eqn. (10)) that

$$((1, 0, \ldots , 0, \eta))^m = ((m, 0, \ldots , 0, \eta))$$

for each integer $m$. Hence,

$$x^d = 1$$

3. Again from eqn. (10) we have

$$(y_f z) = ((1, 0, \ldots , 0) \gamma_f, \gamma_f)$$

$$((y_f z)^2) = ((1, 0, \ldots , 0) + (1, 0, \ldots , 0) \gamma_f, \eta)$$

$$((y_f z)^3) = ((1, 0, \ldots , 0) + (2, 0, \ldots , 0) \gamma_f, \gamma_f)$$

$$((y_f z)^4) = ((2, 0, \ldots , 0) + (2, 0, \ldots , 0) \gamma_f, \eta)$$

$$
\vdots
$$

$$(y_f z)^{2d} = ((d, 0, \ldots , 0) + (d, 0, \ldots , 0) \gamma_f, \eta) =$$

$$= ((0, \ldots , 0) + (0, \ldots , 0) \gamma_f, \eta) = ((0, \ldots , 0), \eta) = 1$$

4. Since $G \cong C_d \times S_z$, there is a subgroup of $G$ which is isomorphic to $C_d^2$. More precisely, the set

$$\{(e_1, \ldots , e_z, \eta) \mid e_j \in \mathbb{Z}_d \}$$

under the product defined on $G$ is a subgroup of $G$ which is isomorphic to $C_d^2$. Since $C_d^2$ is abelian, we want to express the fact that the elements of $G$ having $\eta$ (the identity) as the permutation in the second position all commute. By equations (10) and (11), noticing that

$$(y_f z y_f^{-1})^m = (y_f z y_f^{-1}) \cdots (y_f z y_f^{-1}) = y_f z y_f^{-1}$$

and recalling that $\gamma_f$ is the 2-cycle $(1, f + 1)$ we can express $x_{z} = ((e_1, \ldots , e_z, \eta))$ as

$$x_{z} = \prod_{f=0}^{z-1} (y_f z y_f^{-1})$$

The relation we want is therefore

$$\forall e_{z} \in \mathbb{Z}_d (x_{z} = x_{z})$$

By reducing the relation to the basic "building blocks" $x, y_f$ of the group $G$ it suffices to impose the following:

$$\forall f < z, w < z \quad (y_f z y_f^{-1}) (y_w z y_w^{-1}) = (y_w z y_w^{-1}) (y_f z y_f^{-1})$$

5. Let $x_{z} = ((e_1, \ldots , e_z, \eta))$ as above and $y_{\pi} = ((0, \ldots , 0), \pi)$. Notice that $y_{\pi} x_{z} = x_{\pi(z)} y_{\pi}:

$$((0, \ldots , 0), \pi)((e_1, \ldots , e_z, \eta)) = ((e_1, \ldots , e_z, \pi, \pi)) =$$

$$= ((e_{\pi(1)}, \ldots , e_{\pi(z)}), \pi) =$$

$$= ((e_{\pi(1)}, \ldots , e_{\pi(z)}), \eta)((0, \ldots , 0), \pi).$$

As before, we reduce the relation so that it only includes the building blocks $x, y_f$. Again recall that $\gamma_f$ is the 2-cycle $(1, f + 1)$. It then suffices to impose

$$\forall f < z, w < z \quad y_f (y_w x y_w^{-1}) = (y_{\gamma_f(z+1)} x y_{\gamma_f(z+1)}^{-1} y_f)$$

10
Let $\overline{T} = \langle g, h_f \mid 1 \leq f < z \rangle$ be the free group generated by $g, h_1, \ldots, h_f$. Let relations $R_1, \ldots, R_6$ be defined so that

- $R_1$ is the set of relations given by $\langle h_f \rangle \cong S_z$.
- $R_2$ is given by $g^d = 1$.
- $R_3$ is the set of relations so that for all $f < z$ we have $(h_f g)^{2d} = 1$.
- $R_4$ is the set of relations given by
  \[
  \forall f < z, w < z \quad (h_f g h_f^{-1})(h_w g h_w^{-1}) = (h_w g h_w^{-1})(h_f g h_f^{-1}).
  \]
- $R_5$ is the set of relations given by
  \[
  \forall f < z, w < z \quad h_f(h_w g h_w^{-1}) = (h_{\gamma_f(w+1)} g h_{\gamma_f(w+1)-1})h_f.
  \]

Notice that it is consistent to talk about $\gamma_f$ because of relation $R_1$ (i.e., by $R_1$ we can rig up an isomorphism between the group generated by the $h_f$ and the group generated by the $\gamma_f$).

Now let $T = \overline{T}/(R_1 \cup R_2 \cup R_3 \cup R_4 \cup R_5)$. We claim that $G \cong T$. Let $\vartheta : G \to T$ be given by

\[
\vartheta(e) = g \\
\vartheta(g) = h_f \quad \forall f < z
\]

and extend $\vartheta$ to the whole of $G$ by using the normal form and the fact that $(h_f g h_f^{-1})^m = (h_f g^n h_f^{-1})$, i.e.,

\[
\vartheta((e_1, \ldots, e_z, \pi)) = g^{e_1} \left( \prod_{f=1}^{z-1} (h_f g^{e_{f+1} + t_f h_f^{-1}}) \right)^{t_\pi} \prod_{j=1}^{t_\pi} h_{f_j}
\]

where $\pi = \prod_{j=1}^{t_\pi} \gamma_{f_j}$.

We shall prove $\vartheta$ is an isomorphism in three steps. First, we shall show that it is a group homomorphism. Then we shall show that it is injective, and lastly that it is surjective.

**3.3 Lemma**

$\vartheta$ is a group homomorphism.

**Proof.** We have to show that $\vartheta(\xi_1 \xi_2) = \vartheta(\xi_1) \vartheta(\xi_2)$ for all $\xi_1, \xi_2 \in G$. Let $\xi_1 = (e, \pi)$ and $\xi_2 = (l, \rho)$, where $e = (e_1, \ldots, e_z)$ and $l = (l_1, \ldots, l_z)$. Now,

\[
\vartheta((e, \pi)(l, \rho)) = \vartheta((e + l \pi, \pi \rho)) = g^{e_1 + t_\pi} \left( \prod_{f=1}^{z-1} (h_f g^{e_{f+1} + t_f (h_f h_{f-1})}) \right)^{t_\pi} \prod_{j=1}^{t_\pi} h_{f_j} =
\]

\[
= g^{e_1} g^{e_1} (h_1 g^{e_1} h_1^{-1})(h_1 g^{e_1} h_1^{-1}) \cdots (h_{z-1} g^{e_1} h_{z-1}^{-1})(h_{z-1} g^{e_1} h_{z-1}^{-1}) \prod_{j=1}^{t_\pi} h_{f_j} \prod_{j=1}^{t_\pi} h_{f_j}
\]

Now we use the commutativity of the terms having the identity permutation (relation $R_4$),

\[
= \left[ g^{e_1} (h_1 g^{e_1} h_1^{-1}) \cdots (h_{z-1} g^{e_1} h_{z-1}^{-1}) \right] \left[ g^{e_1} (h_1 g^{e_1} h_1^{-1}) \cdots (h_{z-1} g^{e_1} h_{z-1}^{-1}) \right] \prod_{j=1}^{t_\pi} h_{f_j} \prod_{j=1}^{t_\pi} h_{f_j} =
\]

\[
= \left[ g^{e_1} \prod_{f=1}^{z-1} (h_f g^{e_{f+1} h_f^{-1}}) \right] \left[ g^{e_1} \prod_{f=1}^{z-1} (h_f g^{e_{f+1} h_f^{-1}}) \right] \prod_{j=1}^{t_\pi} h_{f_j} \prod_{j=1}^{t_\pi} h_{f_j}.
\]

11
Finally we use the partial commutativity of relation $R_5$.

$$\left[ g^{e_1} \prod_{f=1}^{z-1} (h_f g^t h_f^{-1}) \prod_{j=1}^{t_r} h_{f_j} \right] \left[ g^{e_1} \prod_{f=1}^{z-1} (h_f g^t h_f^{-1}) \prod_{j=1}^{t_r} h_{f_j} \right] = \vartheta((e, \pi)) \vartheta((l, \rho))$$

as claimed. \(\square\)

### 3.4 Corollary
\(\vartheta\) is injective.

**Proof.** This follows because \(\vartheta\) is a group homomorphism and because of uniqueness of the normal form. \(\square\)

### 3.5 Corollary
\(\vartheta\) is surjective.

**Proof.** Let \(t \in T\). Then \(t\) is a product of \(g, h_1, \ldots, h_{z-1}\). Say \(t = \text{prod}(g, h_1, \ldots, h_{z-1})\). Since by definition of \(\vartheta\) we have \(\vartheta(x) = g\) and \(\vartheta(y_f) = h_f\) for all \(f < z\), \(t = \text{prod}(\vartheta(x), \vartheta(y_1), \ldots, \vartheta(y_{z-1}))\). Now, since \(\vartheta\) is a group homomorphism, \(t = \vartheta(\text{prod}(x, y_1, \ldots, y_{z-1}))\). Hence \(\vartheta\) is surjective. \(\square\)

So we have proved the following theorem.

### 3.6 Theorem
\(G\) is isomorphic to \(T\).

The relations on the group \(G^n(R)\) are all the relations on each of the groups \(G_i\) for \(1 \leq i \leq k\).

### 3.5 A Simple Example

Let’s now see a worked out example. We shall analyse one of the simplest possible cases: consider the set of cellular automata defined on \(\mathbb{Z}_2\) having length 3. In our model, this corresponds to sequences of three elements of \(\mathbb{Z}_2\), i.e. \(R = \mathbb{Z}_2\) and \(n = 3\). We shall find the structure of the group \(G^3(\mathbb{Z}_2)\).

1. Calculate \(k\), i.e. the number of divisors of 3. In this case \(k\) is obviously equal to 2. Hence \(G^3(\mathbb{Z}_2) \cong G_1 \times G_2\).

2. For each \(i \leq 2\), find the structure of \(G_i\). First we have to calculate the parameters \(d_i\) (the \(i\)-th divisor) and \(z_i\) (the number of orbits having period \(d_i\)).

   - We have \(d_1 = 1\) and \(z_1 = 2\). Consequently
     
     \[ G_1 = \{(e_{1,1}, e_{1,2}), \pi_i) \mid e_{1,1}, e_{1,2} \in \mathbb{Z}_2, \pi_i \in S_2) \} \cong (0,0), \pi_i \mid \pi_i \in S_2 \cong S_2 \cong C_2 \]

   - We have \(d_2 = 3\) and \(z_2 = 2\). Consequently
     
     \[ G_2 = \{(e_{2,1}, e_{2,2}), \pi_i) \mid e_{2,1}, e_{2,2} \in \mathbb{Z}_2, \pi_i \in S_2) \} \cong C_3^2 \times S_2 \]

   with presentation
   
   \[ G_2 = \langle g, h \mid g^3 = h^2 = (gh)^6 = 1, (gh)^2 = (hg)^2 \rangle \]

   where \(g = ((1,0), \eta)\) and \(h = ((0,0), \pi)\) with \(\pi = (1 2)\). The structure of this group is not so simple, as one can verify from the following multiplication tables.
\[
\begin{array}{|c|c|c|c|c|c|c|}
\hline
\{0, 0\} & \{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} \\
\hline
\{0, 0\} & \{0, 0\} & \{0, 0\} & \{0, 0\} & \{0, 0\} & \{0, 0\} & \{0, 0\} \\
\hline
\{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} & \{0, 1\} \\
\hline
\{0, 2\} & \{0, 2\} & \{0, 2\} & \{0, 2\} & \{0, 2\} & \{0, 2\} & \{0, 2\} \\
\hline
\{0, 3\} & \{0, 3\} & \{0, 3\} & \{0, 3\} & \{0, 3\} & \{0, 3\} & \{0, 3\} \\
\hline
\hline
\{1, 0\} & \{1, 0\} & \{1, 0\} & \{1, 0\} & \{1, 0\} & \{1, 0\} & \{1, 0\} \\
\hline
\{1, 1\} & \{1, 1\} & \{1, 1\} & \{1, 1\} & \{1, 1\} & \{1, 1\} & \{1, 1\} \\
\hline
\{1, 2\} & \{1, 2\} & \{1, 2\} & \{1, 2\} & \{1, 2\} & \{1, 2\} & \{1, 2\} \\
\hline
\{1, 3\} & \{1, 3\} & \{1, 3\} & \{1, 3\} & \{1, 3\} & \{1, 3\} & \{1, 3\} \\
\hline
\{2, 0\} & \{2, 0\} & \{2, 0\} & \{2, 0\} & \{2, 0\} & \{2, 0\} & \{2, 0\} \\
\hline
\{2, 1\} & \{2, 1\} & \{2, 1\} & \{2, 1\} & \{2, 1\} & \{2, 1\} & \{2, 1\} \\
\hline
\{2, 2\} & \{2, 2\} & \{2, 2\} & \{2, 2\} & \{2, 2\} & \{2, 2\} & \{2, 2\} \\
\hline
\{2, 3\} & \{2, 3\} & \{2, 3\} & \{2, 3\} & \{2, 3\} & \{2, 3\} & \{2, 3\} \\
\hline
\end{array}
\]

where \(\eta, \pi \cong S_2 \cong C_2\). Notice also that since we’re using right function application, when calculating a product \(ab\) one would have to look for \(a\) on the top row and for \(b\) on the leftmost column.

3. Hence we conclude that

\[G^3(Z_2) \cong C_2 \times (C_3 \times C_2)\]

4 Conclusion

Although a practical application of the concepts exposed herein may seem far-fetched, an algorithm for CA transformation product was designed and implemented; the tables above are a direct application of the program. Although the code has (for the present) only been used as an aid to theoretical research, the way it deals with CAs may offer good insight to very specific problems about CAs, like for example estimating the length of the period of a particular CA transformation (this can be used to investigate convergence).

One possible way forward in this research would be to find convenient faithful representations of this group and devise a way to build its character table. This should offer a deeper knowledge of the group structure and the way elements interact with each other.

It is also worth pointing out that the analysis carried out in this paper is actually applicable to other finite dynamical systems, not just cellular automata. The CA behaviour of the dynamical system is only used at the beginning to analyse the numbers of orbits of different lengths under the shift. Most of the work about the CA transformation group only takes orbit lengths into account, hence the results obtained and the techniques developed here may also be employed in the study of the automorphism group of any finite one-to-one dynamical system.

References


