Cellular Automata and Finite Groups
Alonso Castillo-Ramirez and Maximilien Gadouleau

May 3, 2017

Abstract

For a finite group $G$ and a finite set $A$, we study various algebraic aspects of cellular automata over the configuration space $A^G$. In this situation, the set $\text{CA}(G; A)$ of all cellular automata over $A^G$ is a finite monoid whose basic algebraic properties had remained unknown. First, we investigate the structure of the group of units $\text{ICA}(G; A)$ of $\text{CA}(G; A)$. We obtain a decomposition of $\text{ICA}(G; A)$ into a direct product of wreath products of groups that depends on the numbers $\alpha_{[H]}$ of periodic configurations for conjugacy classes $[H]$ of subgroups of $G$. We show how the numbers $\alpha_{[H]}$ may be computed using the Möbius function of the subgroup lattice of $G$, and we use this to improve the lower bound recently found by Gao, Jackson and Seward on the number of aperiodic configurations of $A^G$. Furthermore, we study generating sets of $\text{CA}(G; A)$; in particular, we prove that $\text{CA}(G; A)$ cannot be generated by cellular automata with small memory set, and, when all subgroups of $G$ are normal, we determine the relative rank of $\text{ICA}(G; A)$ on $\text{CA}(G; A)$, i.e. the minimal size of a set $V \subseteq \text{CA}(G; A)$ such that $\text{CA}(G; A) = (\text{ICA}(G; A) \cup V)$.

Keywords: Cellular automata, Invertible cellular automata, Finite groups, Finite monoids, Generating sets.

1 Introduction

Cellular automata (CA), introduced by John von Neumann and Stanislaw Ulam as an attempt to design self-reproducing systems, are models of computation with important applications to computer science, physics, and theoretical biology. In recent years, the mathematical theory of CA has been greatly enriched by its connections to group theory and topology (e.g., see [6] and references therein). The goal of this paper is to embark in the new task of exploring CA from the point of view of finite group theory and finite semigroup theory.

First of all, we review the broad definition of CA that appears in [6, Sec. 1.4]. Let $G$ be a group and $A$ a set. Denote by $A^G$ the configuration space, i.e. the set of all functions of the form $x : G \rightarrow A$. For each $g \in G$, let $R_g : G \rightarrow G$ be the right multiplication function, i.e. $(h)R_g := hg$, for any $h \in G$. We emphasise that we apply functions on the right, while in [6] functions are applied on the left.

Definition 1. Let $G$ be a group and $A$ a set. A cellular automaton over $A^G$ is a transformation $\tau : A^G \rightarrow A^G$ such that there is a finite subset $S \subseteq G$, called a memory set of $\tau$, and a local function $\mu : A^S \rightarrow A$ satisfying

$$(g)(x)\tau = ((R_g \circ x)|_S)\mu, \ \forall x \in A^G, g \in G,$$

where $(R_g \circ x)|_S$ denotes the restriction to $S$ of the configuration $R_g \circ x : G \rightarrow A$.

Most of the classical literature on CA focuses on the case when $G = \mathbb{Z}^d$, for $d \geq 1$, and $A$ is a finite set (e.g. see survey [17]).

A semigroup is a set $M$ equipped with an associative binary operation. If there exists an element $\text{id} \in M$ such that $\text{id} \cdot m = m \cdot \text{id} = m$, for all $m \in M$, the semigroup $M$ is called a monoid and $\text{id}$ an identity of $M$. Clearly, the identity of a monoid is always unique. The group of units of $M$ is the set of all invertible elements of $M$ (i.e. elements $a \in M$ such that there is $a^{-1} \in M$ with $a \cdot a^{-1} = a^{-1} \cdot a = \text{id}$).
Let CA(G; A) be the set of all cellular automata over $A^G$; by [6 Corollary 1.4.11], this set equipped with the composition of functions is a monoid. Although results on monoids of CA have appeared in the literature before (see [14, 19]), the algebraic structure of CA(G; A) remains basically unknown. In particular, the study of CA(G; A), when G and A are both finite, has been generally disregarded (except for the case when $G = \mathbb{Z}_n$, which is the study of one-dimensional CA on periodic points). It is clear that many of the classical questions on CA are trivially answered when $G$ is finite (e.g. the Garden of Eden theorems become trivial), but, on the other hand, several new questions, typical of finite semigroup theory, arise in this setting.

In this paper, we study various algebraic properties of CA(G; A) when G and A are both finite. First, in Section 2 we introduce notation and review some basic results. In Section 3 we study the group of units ICA(G; A) of CA(G; A), i.e. the group of all invertible (also known as reversible) CA over $A^G$. We obtain an explicit decomposition of ICA(G; A) into a direct product of wreath products of groups that depends on the numbers $\alpha_{[H]}$ of periodic configurations for conjugacy classes $[H]$ of subgroups $H$ of $G$.

In Section 4 we show how the numbers $\alpha_{[H]}$ may be computed using the Möbius function of the subgroup lattice of $G$, and we give some explicit formulae for special cases. Furthermore, we make a large improvement on the lower bound recently found by Gao, Jackson and Seward [11] on the number of aperiodic configurations of $A^G$.

Finally, in Section 5, we study generating sets of CA(G; A). A set $T$ of CA is called a \textit{generating set} of CA(G; A) if every CA over $A^G$ is expressible as a word in the elements of $T$. We prove that CA(G; A) cannot be generated by CA with small memory sets: every generating set $T$ of CA(G; A) must contain a cellular automaton with minimal memory set equal to $G$ itself. This result provides a striking contrast with CA over infinite groups because, in such cases, the memory set of any cellular automaton may never be equal to the whole group (as memory sets are finite by definition). Finally, when $G$ is finite abelian, we find the smallest size of a set $V \subseteq CA(G; A)$ such that ICA(G; A) $\cup$ $V$ generates CA(G; A); this number is known in semigroup theory as the \textit{relative rank} of ICA(G; A) in CA(G; A), and it turns out to be related with the number of edges of the subgroup lattice of $G$.

The present paper is an extended version of [5]. In this version, we added preliminary material in order to make the paper self-contained, we improved the exposition, we generalised several results (e.g. Corollary 2, Lemma 11 and Theorem 7), and we added the completely new Section 4.

2 Basic Results

For any set $X$, a \textit{transformation} of $X$ is a function of the form $\tau : X \to X$. Let Tran(X) and Sym(X) be the sets of all transformations and bijective transformations of $X$, respectively. Equipped with the composition of transformations, Tran(X) is known as the \textit{full transformation monoid} on $X$, while Sym(X) is the \textit{symmetric group} on $X$. When $X$ is finite and $|X| = q$, we write Tran$_q$ and Sym$_q$ instead of Tran(X) and Sym(X), respectively. A \textit{finite transformation monoid} is simply a submonoid of Tran$_q$, for some $q$. This type of monoids has been extensively studied (e.g. see [10] and references therein), and it should be noted its close relation to finite-state machines.

Recall that the \textit{order} of a group $G$ is simply the cardinality of $G$ as a set. For the rest of the paper, let $G$ be a finite group of order $n$ and $A$ a finite set of size $q$. By Definition 1 it is clear that CA(G; A) $\subseteq$ Tran($A^G$) (where we use the symbol “$\subseteq$” for the submonoid relation). We may always assume that $\tau \in$ CA(G; A) has (not necessarily minimal) memory set $S = G$, so $\tau$ is completely determined by its local function $\mu : A^G$ $\to$ $A$. Hence, $|CA(G; A)| = q^n$.

If $n = 1$, then CA(G; A) = Tran(A), while, if $q \leq 1$, then CA(G; A) is the trivial monoid with one element; henceforth, we assume $n \geq 2$ and $q \geq 2$. Without loss of generality, we identify $A$ with the set $\{0, 1, \ldots, q - 1\}$ and we denote the identity element of $G$ by $e$.

A \textit{group action} of $G$ on a set $X$ is a function $\cdot : X \times G \to X$ such that $(x \cdot g) \cdot h = x \cdot (gh)$ and $x \cdot e = x$ for all $x \in X$, $g, h \in G$ (where we denote the image of a pair $(x, g)$ by $x \cdot g$). A group $G$ acts on the configuration space $A^G$ as follows: for each $g \in G$ and $x \in A^G$, the configuration $x \cdot g \in A^G$ is defined by

$$ (h)x \cdot g = (hg^{-1})x, \quad \forall h \in G. \quad (1) $$
This indeed defines a group action because:

(i) For all \( h \in G \), \((h) \cdot e = (h)x\), so \( x \cdot e = x \).

(ii) For all \( h, g_1, g_2 \in G \),

\[
(h)(x \cdot g_1) \cdot g_2 = (h)\left(g_2^{-1}x \cdot g_1 = (h)(g_2^{-1}g_1)x = (h)x \cdot g_1g_2, \right.
\]

so \( (x \cdot g_1) \cdot g_2 = x \cdot g_1g_2 \).

Note that in equation (1), \( h \) has to be multiplied by the inverse of \( g \) and not by \( g \) itself, as property (ii) may not hold in the latter case when \( G \) is non-abelian.

**Definition 2.** A transformation \( \tau : A^G \rightarrow A^G \) is \( G \)-equivariant if, for all \( x \in A^G \), \( g \in G \),

\[
(x \cdot g)\tau = (x)\tau \cdot g.
\]

**Theorem 1.** Let \( G \) be a finite group and \( A \) a finite set. Then,

\[
CA(G; A) = \{ \tau \in \text{Tran}(A^G) : \tau \text{ is } G\text{-equivariant} \}.
\]

**Proof.** By Curtis-Hedlund Theorem (see [6, Theorem 1.8.1]), a transformation \( \tau \in \text{Tran}(A^G) \) is a cellular automaton if and only if \( \tau \) is \( G \)-equivariant and continuous in the prodiscrete topology of \( A^G \) (i.e. the product topology of the discrete topology). However, as both \( G \) and \( A \) are finite, every transformation in \( \text{Tran}(A^G) \) is continuous, and the result follows.

In other words, the previous result means that \( CA(G; A) \) is the endomorphism monoid of the \( G \)-set \( A^G \). This result allows us to study \( CA(G; A) \) form a pure algebraic perspective.

We review a few further basic concepts on group actions (see [9, Ch. 1]). For \( x \in A^G \), denote by \( G_x \) the stabiliser of \( x \) in \( G \):

\[
G_x := \{ g \in G : x \cdot g = x \}.
\]

**Remark 1.** For any subgroup \( H \leq G \) there exists \( x \in A^G \) such that \( G_x = H \); namely, we may define \( x : G \rightarrow A \) by

\[
(g)x := \begin{cases} 
1 & \text{if } g \in H, \\
0 & \text{otherwise, } \forall g \in G.
\end{cases}
\]

For any \( x \in A^G \), denote by \( xG \) the \( G \)-orbit of \( x \) on \( A^G \):

\[
xG := \{ x \cdot g : g \in G \}.
\]

Let \( O(G; A) \) be the set of all \( G \)-orbits on \( A^G \):

\[
O(G; A) := \{ xG : x \in A^G \}.
\]

It turns out that \( O(G; A) \) forms a partition of \( A^G \). The following result is known as the Orbit-Stabiliser Theorem (see [9, Theorem 1.4A.]).

**Theorem 2.** Let \( G \) be a finite group and \( A \) a finite set. For any \( x \in A^G \),

\[
|xG| = \frac{|G|}{|G_x|}.
\]

Moreover, if \( x = y \cdot g \) for some \( x, y \in A^G \), \( g \in G \), then \( G_x = g^{-1}G_yg \).

In general, when \( X \) is a set and \( \mathcal{P} \) is a partition of \( X \), we say that a transformation monoid \( M \leq \text{Tran}(X) \) preserves the partition if, for any \( P \in \mathcal{P} \) and \( \tau \in M \) there is \( Q \in \mathcal{P} \) such that \( (P)\tau \subseteq Q \).
Lemma 1. For any $x \in A^G$ and $\tau \in \text{ICA}(G; A)$,

$$(xG)\tau = (x)\tau G.$$ 

In particular, $\text{ICA}(G; A)$ preserves the partition $O(G; A)$ of $A^G$.

Proof. The result follows by the $G$-equivariance of $\tau \in \text{ICA}(G; A)$. □

A configuration $x \in A^G$ is called constant if $(g)x = k \in A$, for all $g \in G$. In such case, we usually denote $x$ by $k \in A^G$.

Lemma 2. Let $\tau \in \text{ICA}(G; A)$ and let $k \in A^G$ be a constant configuration. Then, $(k)\tau \in A^G$ is a constant configuration.

Proof. Observe that $x \in A^G$ is constant if and only if $x \cdot g = x$, for all $g \in G$. By $G$-equivariance,

$$(k)\tau = (k \cdot g)\tau = (k)\tau \cdot g, \quad \forall g \in G.$$ 

Hence, $(k)\tau$ is constant. □

A subshift of $A^G$ is a subset $X \subseteq A^G$ that is $G$-invariant, i.e. for all $x \in X$, $g \in G$, we have $x \cdot g \in X$, and closed in the prodiscrete topology of $A^G$. As $G$ and $A$ are finite, the subshifts of $A^G$ are simply unions of $G$-orbits in $A^G$.

The actions of $G$ on two sets $X$ and $Y$ are equivalent if there is a bijection $\lambda : X \rightarrow Y$ such that, for all $x \in X, g \in G$, we have $(x \cdot g)\lambda = (x)\lambda \cdot g$.

Two subgroups $H_1$ and $H_2$ of $G$ are conjugate in $G$ if there exists $g \in G$ such that $g^{-1} H_1 g = H_2$. This defines an equivalence relation on the subgroups of $G$. Denote by $[H]$ the conjugacy class of $H \leq G$. If $y$ and $z$ are two configurations in the same $G$-orbit, then by Theorem 2 we have $[G_y] = [G_z]$.

We use the cyclic notation for the permutations of $\text{Sym}(A^G)$. If $B \subseteq A^G$ and $a \in A^G$, we define the idempotent transformation $(B \rightarrow a) \in \text{Tran}(A^G)$ by

$$(x)(B \rightarrow a) := \begin{cases} a & \text{if } x \in B, \\ x & \text{otherwise,} \end{cases} \quad \forall x \in A^G.$$ 

When $B = \{b\}$ is a singleton, we write $(b \rightarrow a)$ instead of $(\{b\} \rightarrow a)$.

3 The Structure of ICA($G; A$)

Denote by ICA($G; A$) the group of all invertible cellular automata:

$$\text{ICA}(G; A) := \{ \tau \in \text{ICA}(G; A) : \exists \tau^{-1} \in \text{ICA}(G; A) \text{ such that } \tau \tau^{-1} = \tau^{-1} \tau = \text{id} \}.$$ 

As the inverse of a bijective $G$-equivariant map is also $G$-equivariant, it follows by Theorem 1 that ICA($G; A$) = CA($G; A$) $\cap$ Sym($A^G$).

The following is an essential result for our description of the structure of the group of invertible cellular automata.

Lemma 3. Let $G$ be a finite group of order $n \geq 2$ and $A$ a finite set of size $q \geq 2$. Let $x, y \in A^G$ be such that $xG \neq yG$. Then, there exists $\tau \in \text{ICA}(G; A)$ such that $(x)\tau = y$ if and only if $G_x = G_y$.

Proof. Suppose first that there is $\tau \in \text{ICA}(G; A)$ such that $(x)\tau = y$. Let $g \in G_x$. Then, $y \cdot g = (x)\tau \cdot g = (x \cdot g)\tau = (x)\tau = y$, so $g \in G_y$. This shows that $G_x \leq G_y$. Now, let $h \in G_y$. Then, $x \cdot h = (y)\tau^{-1} \cdot h = (y \cdot h)\tau^{-1} = (y)\tau^{-1} = x$, where $\tau^{-1} \in \text{ICA}(G; A)$ is the inverse of $\tau$, so $h \in G_x$. Therefore, $G_x = G_y$.

Suppose now that $G_x = G_y$. We define a map $\tau : A^G \rightarrow A^G$ as follows:

$$(z)\tau := \begin{cases} y \cdot g & \text{if } z = x \cdot g, \\ x \cdot g & \text{if } z = y \cdot g, \\ z & \text{otherwise,} \end{cases} \quad \forall z \in A^G.$$
We check that \( \tau \) is well-defined:

\[
x \cdot g = x \cdot h \Leftrightarrow gh^{-1} \in G_x = G_y \Leftrightarrow y \cdot g = y \cdot h;
\]

therefore, every element of \( A^G \) has a unique image under \( \tau \). Clearly, \( \tau \) is \( G \)-equivariant and invertible (in fact, \( \tau = \tau^{-1} \)). Hence \( \tau \in \text{ICA}(G; A) \), and it satisfies \( (x)\tau = y \).

**Corollary 1.** Under the assumptions of Lemma 1 there exists \( \tau \in \text{ICA}(G; A) \) such that \( (xG)\tau = yG \) if and only if \( [G_x] = [G_y] \).

**Proof.** Suppose that \( (xG)\tau = yG \). Then, \( (x)\tau = y \cdot g \), for some \( g \in G \). By Lemma 1 \( G_x = G_yg \).

However, note that \( G_yg = g^{-1}G_yg \), so \( [G_x] = [G_y] \). Conversely, if \( [G_x] = [G_y] \), then \( G_x = g^{-1}G_yg = G_yg \), for some \( g \in G \). By Lemma 1 there exists \( \tau \in \text{ICA}(G; A) \) such that \( (x)\tau = y \cdot g \), and by Lemma 1 \( (xG)\tau = yG \).

A subgroup \( H \leq G \) is normal if \( [H] = \{ H \} \) (i.e. \( g^{-1}Hg = H \) for all \( g \in G \)).

**Corollary 2.** Suppose that \( G \) is a finite group whose subgroups are all normal. For any \( x, y \in A^G \), there exists \( \tau \in \text{ICA}(G; A) \) such that \( (xG)\tau = yG \) if and only if \( G_x = G_y \).

Groups whose subgroups are all normal are called Dedekind groups. Clearly, abelian groups are always Dedekind. The finite non-abelian Dedekind groups (also known as finite Hamiltonian groups) were classified by Richard Dedekind in [8] and have the form \( Q_8 \times (Z_2)^n \times H \), where \( Q_8 \) is the quaternion group (i.e. the group of units of the quaternions \( \mathbb{H} \)), \( n \geq 0 \), and \( H \) is a finite abelian group of odd order. Several of their stronger results on \( \text{CA}(G; A) \) will hold when \( G \) is a finite Dedekind group.

For any integer \( \alpha \geq 2 \) and any group \( C \), the wreath product of \( C \) by \( \text{Sym}_\alpha \) is the set

\[
C \wr \text{Sym}_\alpha := \{(v; \phi) : v \in C^\alpha, \phi \in \text{Sym}_\alpha\}
\]

equipped with the operation

\[
(v; \phi) \cdot (w; \psi) = (vw^{\phi}; \phi\psi), \quad \text{for all } v, w \in C^\alpha, \phi, \psi \in \text{Sym}_\alpha,
\]

where \( \phi \) acts on \( w \) by permuting its coordinates:

\[
w^{\phi} = (w_1, w_2, \ldots, w_\alpha)^{\phi} := (w_1^{(1)\phi}, w_2^{(2)\phi}, \ldots, w_\alpha^{(\alpha)\phi}).
\]

In fact, as may be seen from the above definitions, \( C \wr \text{Sym}_\alpha \) is equal to the external semidirect product

\[
C^\alpha \rtimes_\varphi \text{Sym}_\alpha,
\]

where \( \varphi : \text{Sym}_\alpha \to \text{Aut}(C^\alpha) \) is given by \( (w)(\phi) := w^{\phi} \) for all \( w \in C^\alpha, \phi \in \text{Sym}_\alpha \). For a more detailed description of the wreath product of groups, see [9, Sec. 2.6].

Let \( O \in \mathcal{O}(G; A) \) be a \( G \)-orbit. If \( G_{(O)} \) is the pointwise stabiliser of \( O \), i.e. \( G_{(O)} := \cap_{x \in O} G_x \), the group \( G^O := G/G_{(O)} \) is isomorphic to a subgroup of \( \text{Sym}(O) \) (as the homomorphism \( \rho : G \to \text{Sym}(O) \) given by \( (x)(g)\rho = x \cdot g \), for all \( x \in O, g \in G \), has kernel \( G_{(O)} \); see [9, p. 17] for more details). Abusing the notation, we also write \( G^O \) for the isomorphic copy of \( G^O \) inside \( \text{Sym}(O) \). Define the group

\[
\text{ICA}(O) := \{ \tau \in \text{Sym}(O) : \tau \text{ is } G\text{-equivariant}\}.
\]

Note that \( \text{ICA}(O) \) is isomorphic to the centraliser of \( G^O \) in \( \text{Sym}(O) \):

\[
\text{ICA}(O) \cong C_{\text{Sym}(O)}(G^O).
\]

Let \( H \) be a subgroup of \( G \) and \( [H] \) its conjugacy class. Define

\[
B_{[H]}(G; A) := \{ x \in A^G : [G_x] = [H] \}.
\]

Note that \( B_{[H]}(G; A) \) is a subshift of \( A^G \) (i.e. a union of \( G \)-orbits) and, by Theorem 2, all the \( G \)-orbits contained in \( B_{[H]}(G; A) \) have equal sizes. Define

\[
\alpha_{[H]}(G; A) := \left| \{ O \in \mathcal{O}(G, A) : O \subseteq B_{[H]}(G; A) \} \right|.
\]

If \( r \) is the number of different conjugacy classes of subgroups of \( G \), observe that

\[
B := \{ B_{[H]}(G; A) : H \leq G \}
\]

is a partition of \( A^G \) into \( r \) blocks. When \( G \) and \( A \) are clear from the context, we write simply \( B_{[H]} \) and \( \alpha_{[H]} \) instead of \( B_{[H]}(G; A) \) and \( \alpha_{[H]}(G; A) \), respectively.
Remark 2. For any \( G \) and \( A \), we have \( B_{|G|}(G; A) = \{ x \in A^G : x \text{ is constant} \} \) and \( \alpha_{|G|}(G; A) = |A| \).

Example 1. Let \( G \cong \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \) be a cyclic group of order \( n \geq 2 \) and let \( A \) be a finite set of size \( q \geq 2 \). Any configuration \( x : \mathbb{Z}_n \to A \) may be represented by a \( n \)-tuple \((x_1, x_2, \ldots, x_n)\) such that \( x_i := (i-1)x \). The action of \( \mathbb{Z}_n \) on \( A^G \) correspond to cyclic shifts of the \( n \)-tuples; for example,

\[
(x_1, x_2, \ldots, x_n) \cdot 1 = (x_n, x_1, x_2, \ldots, x_{n-1}).
\]

As \( \mathbb{Z}_n \) has a unique subgroup \( \mathbb{Z}_d \) for each \( d \mid n \), we have

\[
\alpha_{|\mathbb{Z}_d|}(\mathbb{Z}_n; A) = \left| \left\{ O \in \mathcal{O}(\mathbb{Z}_n, A) : |O| = \frac{n}{d} \right\} \right|.
\]

This number may be determined by "counting necklaces", and we shall discuss how to do this in the next section (see Lemma [7]).

Example 2. Let \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \) be the Klein four-group and \( A = \{0, 1\} \). As \( G \) is abelian, \( [H] = \{H\} \), for all \( H \leq G \). The subgroups of \( G \) are

\[
H_1 = G, \quad H_2 = \langle (1, 0) \rangle, \quad H_3 = \langle (0, 1) \rangle, \quad H_4 = \langle (1, 1) \rangle, \quad \text{and} \quad H_5 = \langle (0, 0) \rangle,
\]

where \( \langle (a, b) \rangle \) denotes the subgroup generated by \( (a, b) \in G \). Any configuration \( x : G \to A \) may be written as a \( 2 \times 2 \) matrix \((x_{i,j})\) where \( x_{i,j} := (i-1, j-1)x \), \( i, j \in \{1, 2\} \). The \( G \)-orbits on \( A^G \) are

\[
O_1 := \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}, \quad O_2 := \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}, \quad O_3 := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},
\]

\[
O_4 := \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \right\}, \quad O_5 := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},
\]

\[
O_6 := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}, \quad O_7 := \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.
\]

Hence,

\[
B_{|H_1|} := O_1 \cup O_2, \quad B_{|H_2|} := O_3, \quad B_{|H_3|} := O_4, \quad B_{|H_4|} := O_5, \quad B_{|H_5|} := O_6 \cup O_7;
\]

\[
\alpha_{|H_i|}(G; A) = 2, \text{ for } i \in \{1, 5\}, \quad \text{and} \quad \alpha_{|H_i|}(G; A) = 1, \text{ for } i \in \{2, 3, 4\}.
\]

For any \( H \leq G \), let \( N_G(H) := \{ g \in G : H = g^{-1}Hg \} \leq G \) be the normaliser of \( H \) in \( G \). Note that \( H \) is always normal in \( N_G(H) \). The following result determines the structure of the group \( \text{ICA}(G; A) \), and it is a refinement of [1] Lemma 4 (c.f. [19] Theorem 9) and [7] Theorem 7.2).

**Theorem 3** (Structure of \( \text{ICA}(G; A) \)). Let \( G \) be a finite group and \( A \) a finite set of size \( q \geq 2 \). Let \( [H_1], \ldots, [H_r] \) be the list of all different conjugacy classes of subgroups of \( G \). Then,

\[
\text{ICA}(G; A) \cong \prod_{i=1}^{r} (\text{CG}(H_i)/|\text{Sym}_H|),
\]

where \( \alpha_i := \alpha_{|H_i|}(G; A) \).

**Proof.** Let \( B_i := B_{|H_i|} \), and note that all these subshifts are nonempty because of Remark 1. By Corollary 1, any \( \tau \in \text{ICA}(G; A) \) maps configurations inside \( B_i \) to configurations inside \( B_i \); hence, \( \text{ICA}(G; A) \) is contained in the group

\[
\prod_{i=1}^{r} \text{Sym}(B_i) = \text{Sym}(B_1) \times \text{Sym}(B_2) \times \cdots \times \text{Sym}(B_r).
\]
For each \(1 \leq i \leq r\), fix a \(G\)-orbit \(O_i \subseteq B_i\), and let \(O_i\) be the set of \(G\)-orbits contained in \(B_i\) (so \(O_i \in \mathcal{O}_i\)). Note that \(O_i\) is a uniform partition of \(B_i\) (i.e., all the blocks in the partition have the same size). For any \(\tau \in \ICA(G; A)\), Lemma [1] implies that the projection of \(\tau\) to \(\Sym(B_i)\) is contained in the group that preserves this uniform partition, i.e., the projection of \(\tau\) is contained in

\[ S(B_i, O_i) := \{ \phi \in \Sym(B_i) : \forall P \in O_i, \ (P)\phi \in O_i \}. \]

By [2] Lemma 2.1(iv),

\[ S(B_i, O_i) \cong \Sym(O_i) \triangleleft \Sym_{\alpha_i}. \]

It is well-known that \(\Sym_{\alpha_i}\) is generated by its transpositions. As the invertible cellular automaton constructed in the proof of Lemma [3] induces a transposition \((xG, yG) \in \Sym_{\alpha_i}\), with \(xG, yG \in O_i\), we deduce that \(\Sym_{\alpha_i} \leq \ICA(G; A)\). Now it is clear that the projection of \(\ICA(G; A)\) to \(\Sym(B_i)\) is exactly \(\ICA(O_i) \triangleleft \Sym_{\alpha_i}\). By [9] Theorem 4.2A (i), it follows that

\[ C_{\Sym(O_i)}(G^{O_i}) \cong N_G(H_i)/H_i. \]

The result follows because \(\ICA(O_i) \cong C_{\Sym(O_i)}(G^{O_i})\).

**Corollary 3.** Let \(G\) be a finite Dedekind group and \(A\) a finite set of size \(q \geq 2\). Let \(H_1, \ldots, H_r\) be the list of different subgroups of \(G\). Then,

\[ \ICA(G; A) \cong \prod_{i=1}^r \left( (G/H_i) \triangleleft \Sym_{\alpha_i} \right), \]

where \(\alpha_i := \alpha_{[H_i]}(G; A)\).

**Proof.** As every subgroup of \(G\) is normal, the results follows because \([H_i] = \{H_i\}\) and \(N_G(H_i) = G\) for all \(1 \leq i \leq r\).

**Example 3.** For any \(n \geq 2\),

\[ \ICA(Z_n; A) \cong \prod_{i=1}^r \left( (Z_{d_i} : \Sym_{\alpha_i}) \right), \]

where \(d_1, d_2, \ldots, d_r\) are the divisors of \(n\), and \(\alpha_i := \alpha_{Z_{d_i}}(Z_n; A)\).

**Example 4.** Let \(G = \mathbb{Z}_2 \times \mathbb{Z}_2\) and \(A = \{0, 1\}\). By Example [2]

\[ \ICA(G; A) \cong (\mathbb{Z}_2)^4 \times (G \triangleleft \Sym_2). \]

### 4 Aperiodic Configurations

In this section, we shall determine the integers \(\alpha_{[H]}(G; A)\), for each \(H \leq G\), as they play an important role in the decomposition of \(\ICA(G; A)\) given by Theorem [3].

The following elementary result links the integers \(\alpha_{[H]}(G; A)\) with the sizes of the subshifts \(B_{[H]}(G; A)\).

**Lemma 4.** Let \(G\) be a finite group of order \(n \geq 2\) and \(A\) a finite set of size \(q \geq 2\). Let \(H\) be a subgroup of \(G\) of order \(m\). Then,

\[ \alpha_{[H]} \cdot n = m \cdot |B_{[H]}|. \]

**Proof.** The set of \(G\)-orbits contained in \(B_{[H]}\) forms a partition of \(B_{[H]}\) into \(\alpha_{[H]}\) blocks. The result follows as each one of these \(G\)-orbits has size \(\frac{n}{m}\) by Theorem [2].

Denote by \([G : H]\) the index of \(H\) in \(G\) (i.e., the number of cosets of \(H\) in \(G\)). It is well-known that when \(G\) is finite, \([G : H] = \frac{|G|}{|H|}\). The following result characterises the situations when \(B_{[H]}\) contains a unique \(G\)-orbit and will be useful in Section [5,2].

**Lemma 5.** Let \(G\) be a finite group and \(A\) a finite set of size \(q \geq 2\). Then, \(\alpha_{[H]}(G; A) = 1\) if and only if \([G : H] = 2\) and \(q = 2\).
Proof. Suppose first that \([G : H] = q = 2\). The subgroup \(H\) is normal because it has index 2, so \(Hg = gH\) for every \(g \in G\). Fix \(s \in G \setminus H\), and define \(x \in A^G\) by
\[
(g)x = \begin{cases} 
0 & \text{if } g \in H \\
1 & \text{if } g \in sH = Hs.
\end{cases}
\]
Clearly, \(G_x = H\) and \(x \in B_{|H|}\). Let \(y \in B_{|H|}\). As \(H\) is normal, \([H] = \{H\}\), so \(G_y = H\). For any \(h \in H\),
\[
(h)y = (e)y \cdot h^{-1} = (e)y \quad \text{and} \quad (sh)y = (s)y \cdot h^{-1} = (s)y,
\]
so \(y\) is constant on the cosets of \(H\). Therefore, either \(y = x\), or
\[
(g)y = \begin{cases} 
1 & \text{if } g \in H \\
0 & \text{if } g \in sH = Hs.
\end{cases}
\]
In the latter case, \(y \cdot s = x\) and \(y \in xG\). This shows that there is a unique \(G\)-orbit contained in \(B_{|H|}\), so \(\alpha_{|H|}(G; A) = 1\).
Conversely, suppose that \([G : H] \neq 2\) or \(q \geq 3\). If \([G : H] = 1\), then \(G = H\) and \(\alpha_{|H|}(G; A) = q \geq 2\).
Now we prove the two cases separately.

**Case 1:** \([G : H] \geq 3\). Define configurations \(x_1, x_2 \in A^G\) by
\[
(g)x_1 = \begin{cases} 
1 & \text{if } g \in H \\
0 & \text{otherwise}.
\end{cases}
\]
\[
(g)x_2 = \begin{cases} 
0 & \text{if } g \in H \\
1 & \text{otherwise}.
\end{cases}
\]
It is clear that \(x_1, x_2 \in B_{|H|}\) because \(G_{x_1} = G_{x_2} = H\). Furthermore, \(x_1\) and \(x_2\) are not in the same \(G\)-orbit because the number of preimages of 1 under \(x_1\) and \(x_2\) is different (as \([G : H] \geq 3\)).
Hence, \(\alpha_{|H|}(G; A) \geq 2\).

**Case 2:** \(q \geq 3\). Define a configuration \(x_3 \in B_{|H|}\) by
\[
(g)x_3 = \begin{cases} 
2 & \text{if } g \in H \\
0 & \text{otherwise},
\end{cases}
\]
and consider the configuration \(x_1 \in B_{|H|}\) defined in Case 1. Clearly, \(x_1\) and \(x_3\) are not in the same \(G\)-orbit because 2 \(\in A\) is not in the image of \(x_1\). Hence, \(\alpha_{|H|}(G; A) \geq 2\).

\(\square\)

For any \(H \leq G\), consider the set of \(H\)-periodic configurations:
\[
\text{Fix}(H) := \{ x \in A^G : x \cdot h = x, \forall h \in H \} = \{ x \in A^G : H \leq G_x \}.
\]
By [6] Corollary 1.3.4., we have
\[
|\text{Fix}(H)| = q^{|G:H|}.
\]
By the Cauchy-Frobenius lemma ([9] Theorem 1.7A)), the total number of \(G\)-orbits on \(A^G\) is
\[
|O(G; A)| = \frac{1}{|G|} \sum_{g \in G} q^{|\langle g \rangle|},
\]
where \(|g| := |\langle g \rangle|\) is the order of the element \(g\). However, we need a somewhat more sophisticated machinery in order to count the number of orbits inside \(B_{|H|}(G; A)\).
The Möbius function of a finite poset \((P, \leq)\) is a map \(\mu : P \times P \to \mathbb{Z}\) defined inductively by the following equations:

\[
\mu(a, a) = 1, \quad \forall a \in P,
\]

\[
\mu(a, b) = 0, \quad \forall a > b,
\]

\[
\sum_{a \leq c \leq b} \mu(a, c) = 0, \quad \forall a < b.
\]

If \(L(G)\) is the set of subgroups of \(G\), the poset \((L(G), \subseteq)\) is called the subgroup lattice of \(G\). Let \(\mu : L(G) \times L(G) \to \mathbb{Z}\) be the Möbius function of the subgroup lattice of \(G\). In particular, \(\mu(H, H) = 1\) for any \(H \leq G\), and \(\mu(H, K) = -1\) if \(H\) is a maximal subgroup of \(K \leq G\).

For any \(H \leq G\) of order \(m\), let \(p_H\) be the smallest order of a subgroup between \(H\) and \(G\) (note that \(p_G \geq 2m\)):

\[
p_H := \min\{|K| : H < K \leq G\},
\]

and define

\[
S_H := \{K : H < K \leq G, \ |K| = p_H\}.
\]

By convention, \(p_G = n\) and \(S_G = \emptyset\).

In the next result we use the following asymptotic notation: write \(f(n) = o(g(n))\), with \(g(n)\) not identically zero, if \(\lim_{n \to 0} \frac{f(n)}{g(n)} = 0\).

**Theorem 4.** Let \(G\) be a finite group of order \(n \geq 2\) and \(A\) a finite set of size \(q \geq 2\). Let \(H\) be a subgroup of \(G\) of order \(m\).

(i) \(|B[H]| = |[H]| \sum_{K \leq G} \mu(H, K) \cdot q^{n/|K|} |B[K]| \).

(ii) Using asymptotic notation by fixing \(G\) and considering \(q = |A|\) as a variable, we have

\[
\frac{|B[H]|}{|[H]|} = q^{n/m} - (|S_H| + o(1))q^{n/p_H}.
\]

**Proof.** In order to prove part (i), observe that

\[
|\text{Fix}(H)| = \sum_{H \leq K \leq G} \frac{1}{|K|} |B[K]|.
\]

By Möbius inversion (see [18, 4.1.2]), we obtain that

\[
|B[H]| = |[H]| \sum_{K \leq G} \mu(H, K) \cdot |\text{Fix}(K)|.
\]

The result follows as \(|\text{Fix}(K)| = q^{n/|K|}\).

Now we prove part (ii). The result is clear for \(H = G\). Otherwise, we have

\[
\frac{|B[H]|}{|[H]|} = \sum_{H \leq K \leq G} \mu(H, K)q^{n/|K|}
\]

\[
= q^{n/m} - |S_H|q^{n/p_H} + \sum_{K \notin S_H} \mu(H, K)q^{n/|K|}
\]

\[
= q^{n/m} - (|S_H| - \sum_{K \notin S_H} \mu(H, K)q^{n/|K| - n/p_H})q^{n/p_H}.
\]

The result follows as \(q^{n/|K| - n/p_H} = o(1)\). \(\square\)
As the Möbius function of the subgroup lattice of $G$ is not easy to calculate in general, we shall give a few more explicit results by counting the number of so-called aperiodic configurations:

$$ac(G; A) := \left| \{ x \in A^G : Gx = \{ e \} \} \right| = |B_{\{e\}}(G; A)|.$$

Part of our motivation to study this number is that, when $H$ is a normal subgroup of $G$, the size of the subshift $B_H$ is equal to the number of aperiodic configurations with respect to $G/H$.

**Lemma 6.** Let $G$ be a finite group, $A$ a finite set, and $H$ a normal subgroup of $G$. Then,

$$|B_H(G; A)| = ac(G/H; A).$$

**Proof.** As $H$ is normal, then $G/H$ is a group. By [6, Proposition 1.3.7.], there is a $G/H$-equivariant bijection between the configuration space $A^{G/H}$ and $\text{Fix}(H)$. Hence, configurations in $A^{G/H}$ with trivial stabiliser correspond to configurations in $\text{Fix}(H)$ with stabiliser $H$. □

The following result gives some formulae for the number of aperiodic configurations of various finite groups.

**Lemma 7.** Let $G$ be a finite group of order $n \geq 2$ and $A$ a finite set of size $q \geq 2$.

(i) $$ac(G; A) = \sum_{K \leq G} \mu(\{e\}, K) \cdot q^{n/|K|}.$$  

(ii) If $G \cong \mathbb{Z}_n$ is a cyclic group, then

$$ac(\mathbb{Z}_n, A) = \sum_{d|n} \mu(1, d) \cdot q^{n/d},$$

where $\mu$ is the classic Möbius function of the poset $(\mathbb{N}, |)$.

(iii) If $G$ is a $p$-group and $\mathcal{H} := \{ H \leq G : H \text{ is elementary abelian} \}$, then

$$ac(G; A) = \sum_{H \in \mathcal{H}} (-1)^{\log_p |H|} p^{\left( \frac{\log_p |H|}{2} \right)} q^{n/|H|}.$$  

(iv) If $G \cong \mathbb{Z}_p^m$ is an elementary abelian group, then

$$ac(\mathbb{Z}_p^m, A) = q^{p^m} + \sum_{r=1}^m (-1)^r q^{p^m-r} p^{(r-1)/2} \binom{m}{r}_p.$$  

where $\binom{m}{r}_p$ is the Gaussian binomial coefficient:

$$\binom{m}{r}_p := \frac{(1 - p^m)(1 - p^{m-1}) \ldots (1 - p^{m-r+1})}{(1 - p^r)(1 - p^{r-1}) \ldots (1 - p)}.$$  

**Proof.** Part (i) follows by Lemma 4 (iii). Part (ii) follows because the subgroup lattice of the cyclic group $\mathbb{Z}_n$ is isomorphic to the lattice of divisors of $n$.

We prove part (iii). If $G$ is a $p$-group, by [15, Corollary 3.5.], for any $H \leq G$ we have

$$\mu(\{e\}, H) = \begin{cases} (-1)^{\log_p |H|} p^{\left( \frac{\log_p |H|}{2} \right)} & \text{if } H \text{ is elementary abelian}, \\ 0 & \text{otherwise}. \end{cases}$$

So the result follows by part (i).
Finally, we prove part (iv). Denote by $\mathcal{H}_r$ the set of elementary abelian subgroups of $G$ of order $p^r$. Then,

$$ac(G; A) = \sum_{r=0}^{m} (-1)^r |\mathcal{H}_r| p^r m / p^r$$

$$= \sum_{r=0}^{m} (-1)^r q^r m / p^r (r-1)/2 |\mathcal{H}_r|.$$ 

The result follows because the Gaussian binomial coefficient $\binom{m}{r}_p$ gives precisely the number of subgroups of order $p^r$ of $\mathbb{Z}_p^m$ (see [3 Section 9.2]).

As constant configurations are never aperiodic, the following obvious upper bound of $ac(G; A)$ is obtained:

$$ac(G; A) \leq q^n - q$$

This upper bound is achieved if and only if $n$ is a prime number (so $G$ is a cyclic group). The following lower bound bound of $ac(G; A)$ was obtained by Gao, Jackson and Seward [11 Corollary 1.7.2.]:

$$q^n - q^{n-1} \leq ac(G; A),$$

which is achieved for small values of $n$ and $q$, as for example, when $n = q = 2$, or when $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $q = 2$ (see Example 2).

For any $d \mid n$, define $G^{(d)} := \{ g \in G : |\langle g \rangle| = d \}$. In the next result we improve the known estimates of $ac(G; A)$.

**Theorem 5** (Lower bound on aperiodic configurations). Let $G$ be a finite group of order $n \geq 2$ and $A$ a finite set of size $q \geq 2$. Let $p$ be the smallest prime dividing $n$. Then:

(i) $ac(G; A) = q^n - \left(\frac{|G^{(p)}|}{p-1} + o(1)\right) q^{n/p}$.

(ii) We have the following lower bound:

$$q^n - (n-1)q^{n/p} \leq ac(G; A).$$

**Proof.** By Theorem 4 (ii) with $H = \{e\}$, we have

$$ac(G; A) = q^n - (|S_{\{e\}}| + o(1)) q^{n/p(a)}.$$ 

In this case, $p_{\{e\}}$ is the smallest order of a non-identity element in $G$, which, by Sylow’s theorem, is equal to $p$, the smallest prime dividing $n$. Furthermore, $|S_{\{e\}}|$, the number of subgroups of $G$ of order $p$, is $|G^{(p)}|/(p-1)$, so part (i) follows.

In order to prove part (ii), let $t_1, \ldots, t_r$ be the generators of the minimal subgroups of $G$ (all of which are cyclic groups of prime order). Then,

$$ac(G; A) = q^n - \left| \bigcup_{i=1}^{r} \text{Fix}(\{t_i\}) \right| \geq q^n - \sum_{i=1}^{r} q^{n/|t_i|} \geq q^n - (n-1)q^{n/p}. $$

The lower bound of Theorem 5 (ii) is much tighter than the one given by [11 Corollary 1.7.2.].

**5 Generating Sets of CA($G; A$)**

For a monoid $M$ and a subset $T \subseteq M$, denote by $\langle T \rangle$ the submonoid generated by $T$, i.e. the smallest submonoid of $M$ containing $T$. Say that $T$ is a generating set of $M$ if $M = \langle T \rangle$; in this case, every element of $M$ is expressible as a word in the elements of $T$ (we use the convention that the empty word is the identity).
5.1 Memory Sets of Generators of CA(G; A)

A large part of the classical research on CA is focused on CA with small memory sets. In some cases, such as the elementary Rule 110, or John Conway’s Game of Life, these CA are known to be Turing complete. In a striking contrast, when G and A are both finite, CA with small memory sets are insufficient to generate the monoid CA(G; A).

**Theorem 6** (Minimal memory set of generators of CA(G; A)). Let G be a finite group of order n ≥ 2 and A a finite set of size q ≥ 2. Let T be a generating set of CA(G; A). Then, there exists τ ∈ T with minimal memory set $S = G$.

**Proof.** Suppose that T is a generating set of CA(G; A) such that each of its elements has minimal memory set of size at most $n - 1$. Consider the idempotent $σ := (0 → 1) ∈ CA(G; A)$, where $0, 1 ∈ G^A$ are different constant configurations. Then, $σ = τ_1 τ_2 ... τ_t$, for some $τ_i ∈ T$. By the definition of $σ$ and Lemma 2, there must be $1 ≤ j ≤ ℓ$ such that $|(A_G^G)τ_j| = q - 1$ and $(A_G^G)τ_j = A_{nc}^G$, where

$$A_c^G := \{k ∈ G^A : k \text{ is constant}\} \quad \text{and} \quad A_{nc}^G := \{x ∈ G^A : x \text{ is non-constant}\}.$$  

Let $S ⊆ G$ and $μ : A^S → A$ be the minimal memory set and local function of $τ := τ_j$, respectively. By hypothesis, $s := |S| < n$. Since the restriction of $τ$ to $A^G_c$ is a bijection, there exists $k ∈ A^G_c$ (defined by $(g)k := k ∈ A$, ∀g ∈ G) such that $k ∉ (A_G^G)τ_j$.

For any $x ∈ G^A$, define the $k$-weight of $x$ by

$$|x|_k := |\{g ∈ G : (g)x \neq k\}|.$$  

Consider the sum of the $k$-weights of all non-constant configurations of $A^G$:

$$w := \sum_{x ∈ A_{nc}^G} |x|_k = \sum_{x ∈ A^G} |x|_k − \sum_{x ∈ A^G_c} |x|_k = n(q - 1)q^{n-1} − n(q - 1) = n(q - 1)(q^{n-1} - 1).$$

In particular, $\frac{w}{n}$ is an integer not divisible by $q$.

For any $x ∈ G^A$ and $y ∈ A^S$, define

$$\text{Sub}(y, x) := |\{g ∈ G : y = x|sg\}|;$$

this counts the number of times that $y$ appears as a subconfiguration of $x$. Then, for any fixed $y ∈ A^S$,

$$N_y := \sum_{x ∈ A_{nc}^S} \text{Sub}(y, x) = \begin{cases} nq^{n-s} & \text{if } y ∈ A_{nc}^S, \\ n(q^{n-s} - 1) & \text{if } y ∈ A_c^S. \end{cases}$$

To see why the previous equality holds, fix $g ∈ G$ and count the number of configurations $x ∈ A_{nc}^G$ such that $y = x|sg$: there are $q^{n-s}$ such configurations if $y$ is non-constant, and $q^{n-s} - 1$ if $y$ is constant. The equality follows by counting this for each one of the $n$ elements of $G$.

Let $δ : A^2 → \{0, 1\}$ be the Kronecker’s delta function. Since $(A_{nc}^G)τ = A_{nc}^G$, we have

$$w = \sum_{x ∈ A_{nc}^G} |(x)τ|_k = \sum_{y ∈ A^S} N_y(1 - δ(y)μ,k) = nq^{n-s} \sum_{y ∈ A_{nc}^S} (1 - δ(y)μ,k) + n(q^{n-s} - 1) \sum_{y ∈ A_c^S} (1 - δ(y)μ,k).$$

Because $k ∉ (A_G^G)τ$, we know that $(y)μ ≠ k$ for all $y ∈ A_c^S$. Therefore,

$$\frac{w}{n} = q^{n-s} \sum_{y ∈ A_{nc}^S} (1 - δ(y)μ,k) + (q^{n-s} - 1)q.$$  

As $s < n$, this implies that $\frac{w}{n}$ is an integer divisible by $q$, which is a contradiction. □
5.2 Relative Rank of $\ICA(G; A)$ in $\ICA(G; A)$

One of the fundamental problems in the study of a finite monoid $M$ is the determination of the cardinality of a smallest generating subset of $M$; this is called the rank of $M$ and denoted by $\text{Rank}(M)$:

$$\text{Rank}(M) := \min\{|T| : T \subseteq M \text{ and } \langle T \rangle = M\}.$$

It is well-known that, if $X$ is any finite set, the rank of the full transformation monoid $\text{Tran}(X)$ is 3, while the rank of the symmetric group $\text{Sym}(X)$ is 2 (see [11] Ch. 3). Ranks of various finite monoids have been determined in the literature before (e.g. see [12, 13, 14, 16]).

In [11], the rank of $\ICA(\mathbb{Z}_n; A)$, where $\mathbb{Z}_n$ is the cyclic group of order $n$, was studied and determined when $n \in \{p, 2^k, q^k : k \geq 1, p \text{ odd prime}\}$. Moreover, the following problem was proposed:

**Problem 1.** For any finite group $G$ and finite set $A$, determine $\text{Rank}(\ICA(G; A))$.

For any finite monoid $M$ and $U \subseteq M$, the relative rank of $U$ in $M$, denoted by $\text{Rank}(M : U)$, is the minimum cardinality of a subset $V \subseteq M$ such that $\langle U \cup V \rangle = M$. For example, for any finite set $X$,

$$\text{Rank}(\text{Tran}(X) : \text{Sym}(X)) = 1,$$

as any $\tau \in \text{Tran}(X)$ with $|(X)\tau| = |X| - 1$ satisfies $\langle \text{Sym}(X) \cup \{\tau\} \rangle = \text{Tran}(X)$. One of the main tools used to determine $\text{Rank}(\ICA(G; A))$ is based on the following result (see [2, Lemma 3.1]).

**Lemma 8.** Let $M$ be a finite monoid and let $U$ be its group of units. Then,

$$\text{Rank}(M) = \text{Rank}(M : U) + \text{Rank}(U).$$

We shall determine the relative rank of $\ICA(G; A)$ in $\ICA(G; A)$ for any finite abelian group $G$ and finite set $A$. In order to achieve this, we prove two lemmas that hold even when $G$ is nonabelian and have relevance in their own right.

**Lemma 9.** Let $G$ be a finite group and $A$ a finite set of size $q \geq 2$. Let $\tau \in \ICA(G; A)$ and $x \in A^G$. If $(x)\tau \in xG$, then $\tau|_{xG} \in \text{Sym}(xG)$.

**Proof.** It is enough to show that $(xG)\tau = xG$ as this implies that $\tau|_{xG} : xG \to xG$ is surjective, so it is bijective by the finiteness of $xG$. Since $(x)\tau \in xG$, we know that $(x)\tau G = xG$. Hence, by Lemma 11, $(xG)\tau = (x)\tau G = xG$.

**Remark 3.** Recall that a Garden of Eden (GoE) of $\tau \in \ICA(G; A)$ is a configuration $x \in A^G$ such that $x \notin (A^G)\tau$. As $A^G$ is finite in our setting, note that $\tau$ is non-invertible if and only if it has a GoE. Moreover, by $G$-equivariance, $x$ is a GoE of $\tau$ if and only if $xG$ is a GoE of $\tau$, so we shall talk about $G$-E orbits, rather than GoE configurations.

Denote by $\mathcal{C}_G$ the set of conjugacy classes of subgroups of $G$. For any $[H_1], [H_2] \in \mathcal{C}_G$, write $[H_1] \leq [H_2]$ if $H_1 \leq g^{-1}H_2g$, for some $g \in G$.

**Remark 4.** The relation $\leq$ defined above is a well-defined partial order on $\mathcal{C}_G$. Clearly, $\leq$ is reflexive and transitive. In order to show antisymmetry, suppose that $[H_1] \leq [H_2]$ and $[H_2] \leq [H_1]$. Then, $H_1 \leq g^{-1}H_2g$ and $H_2 \leq f^{-1}H_1f$, for some $f, g \in G$, which implies that $|H_1| \leq |H_2|$ and $|H_2| \leq |H_1|$. As $H_1$ and $H_2$ are finite, $|H_1| = |H_2|$, and $H_1 = g^{-1}H_2g$. This shows that $[H_1] = [H_2]$.

**Lemma 10.** Let $G$ be a finite group and $A$ a finite set of size $q \geq 2$. Let $x, y \in A^G$ be such that $xG \neq yG$. There exists a non-invertible $\tau \in \ICA(G; A)$ such that $(x)\tau = y$ if and only if $G_x \subseteq G_y$.

**Proof.** In general, for any $\tau \in \ICA(G; A)$ such that $(x)\tau = y$, we have $G_x \leq G_y$, because we may argue as in the first line of the proof of Lemma 3. Conversely, suppose that $G_x \leq G_y$. We define an idempotent transformation $\tau_{x,y} : A^G \to A^G$ as follows:

$$(z)\tau_{x,y} := \begin{cases} y \cdot g & \text{if } z = x \cdot g, \\ z & \text{otherwise}, \end{cases} \quad \forall z \in A^G.$$

Note that $\tau_{x,y}$ is well-defined because $x \cdot g = x \cdot h$, implies that $gh^{-1} \in G_x \leq G_y$, so $y \cdot g = y \cdot h$. Clearly, $\tau_{x,y}$ is non-invertible and $G$-equivariant, so $\tau_{x,y} \in \ICA(G; A) \setminus \ICA(G; A)$. 

\end{document}
Corollary 4. Let $G$ be a finite group and $A$ a finite set of size $q \geq 2$. Let $x, y \in A^G$ be such that $xG \neq yG$. There exists a non-invertible $\tau \in \text{CA}(G; A)$ such that $(xG)\tau = yG$ if and only if $|G_x| \leq |G_y|$.

Consider the directed graph $(C_G, \mathcal{E}_G)$ with vertex set $C_G$ and edge set

$$\mathcal{E}_G := \{(|H_i|, |H_j|) \in C_G^2 : |H_i| \leq |H_j|\}.$$ 

When $G$ is abelian, this graph coincides with the subgroup lattice of $G$.

Remark 5. Lemma 10 may be restated in terms of $(C_G, \mathcal{E}_G)$. By Lemma 9 loops $([H_i], |H_i|)$ do not have corresponding non-invertible CA when $\alpha_{|H_i|}(G; A) = 1$.

Recall that an action of $G$ on a set $X$ is transitive if for any $x, y \in X$ there exists $g \in G$ such that $x \cdot g = y$ (i.e. $X = xG$, for any $x \in X$). The following result will be useful in order to prove the main theorem of this section.

Lemma 11. Let $G$ be a finite group and $A$ a finite set of size $q \geq 2$. Then $\text{ICA}(G; A)$ is transitive on every $G$-orbit on $A^G$ if and only if $G$ is a finite Dedekind group.

Proof. Let $x \in A^G$ be a configuration. By Theorem 7 the group $\text{ICA}(G; A)$ acts on $xG$ as the group $N_G(G_x)/G_x$ via the action $x \cdot (G_xg) := x \cdot g$, for any $G_xg \in N_G(G_x)/G_x$. Note that $N_G(G_x)/G_x$ is transitive on $xG$ if and only if $G = N_G(G_x)$, which holds if and only if $G_x$ is normal in $G$. As any subgroup of $G$ occurs as a stabiliser of a configuration, this shows that $\text{ICA}(G; A)$ is transitive on $xG$, for all $x \in A^G$, if and only if every subgroup of $G$ is normal.

Remark 6. It is obvious, by definition, that $G$ is transitive on a $G$-orbit $xG$. However, Lemma 11 establishes a criterion for the transitivity of the group $\text{ICA}(G; A)$ on $xG$.

Theorem 7 (Relative rank of $\text{ICA}(G; A)$ on $\text{CA}(G; A)$). Let $G$ be a finite group and $A$ a finite set of size $q \geq 2$. Let $I_2(G)$ be the set of subgroups of $G$ of index 2:

$$I_2(G) = \{H \leq G : [G : H] = 2\}.$$ 

Then,

$$\text{Rank}(\text{CA}(G; A) : \text{ICA}(G; A)) \geq \begin{cases} |\mathcal{E}_G| - |I_2(G)| & \text{if } q = 2, \\ |\mathcal{E}_G| & \text{otherwise,} \end{cases}$$

with equality if and only if $G$ is a finite Dedekind group.

Proof. Let $[H_1], [H_2], \ldots, [H_r]$ be the list of different conjugacy classes subgroups of $G$ with $H_1 = G$. Suppose further that this is ordered such that

$$|H_1| \geq |H_2| \geq \cdots \geq |H_r| \quad (3)$$

For each $1 \leq i \leq r$, let $\alpha_i := \alpha_{|H_i|}(G; A)$ and $B_i := \alpha_{|H_i|}(G; A)$. Fix orbits $x_iG \subseteq B_i$ such that $G_{x_i} < G_{x_j}$ whenever $[H_i] < [H_j]$. For every $\alpha_i \geq 2$, fix orbits $y_iG \subseteq B_i$ such that $x_iG \neq y_iG$. Consider the set

$$V := \{\tau_{x_i, x_j} : G_{x_i} < G_{x_j}\} \cup \{\tau_{x_i, y_i} : \alpha_i \geq 2\},$$

and $\tau_{x_i, x_j}$ and $\tau_{x_i, y_i}$ are the idempotents that map $x_i$ to $x_j$ and $x_i$ to $y_i$, respectively, as defined in Lemma 10. Observe that

$$|V| = |\mathcal{E}_G| - \sum_{i=1}^{n} \delta(\alpha_i, 1) = \begin{cases} |\mathcal{E}_G| - |I_2(G)| & \text{if } q = 2, \\ |\mathcal{E}_G| & \text{otherwise,} \end{cases}$$

where the last equality follows by Lemma 5.

Claim. The relative rank of $\text{ICA}(G; A)$ on $\text{CA}(G; A)$ is at least $|V|$.
Proof. Suppose there exists $W \subseteq CA(G; A)$ such that $|W| < |V|$ and 

$$\langle ICA(G; A) \cup W \rangle = CA(G; A).$$

Let $\tau \in CA(G; A)$. We say that $\tau$ is a Unique-Garden-of-Eden CA (UCA) of type $(B_i, B_j)$ if the following holds:

($\ast$) $\tau$ has a unique Garden of Eden $G$-orbit $O_i$ (i.e. $(A^G)\tau = A^G \setminus O_i$), and it satisfies $O_i \subseteq B_i$ and $(O_i)\tau \subseteq B_j$.

Note that UCA of type $(B_i, B_j)$ only exist when there are at least two different orbits in $B_i$, i.e. $\alpha_i \geq 2$.

For example, the idempotents $\tau_{x_i, y_i} \in V$, with $\alpha_i \geq 2$, are UCA of type $(B_i, B_i)$, while the idempotents $\tau_{x_i, x_j}$, with $G_{x_i} < G_{x_j}$, are UCA of type $(B_i, B_j)$ with $O_i = x_iG$. Note that $\tau \in CA(G; A)$ is a UCA of type $(B_i, B_j)$ if and only if $(ICA(G; A), \tau)$ contains a UCA of type $(B_i, B_j)$ if and only if all non-invertible elements of $(ICA(G; A), \tau)$ are UCA of type $(B_i, B_j)$ (because any $\phi \in ICA(G; A)$ always satisfies $\phi(B_k) = B_k$ for all $k$, by Corollary 1).

As $|W| < |V|$, and $V$ has exactly one UCA of each possible type (see Lemma [10]), there must be $\tau \in V$ such that there is no UCA in $W$ of the same type as $\tau$. Without loss of generality, suppose that the type of $\tau$ is $(B_i, B_j)$. We finish the proof of the claim by showing that there is no UCA of type $(B_i, B_j)$ in $(ICA(G; A) \cup W)$, contradicting that $\langle ICA(G; A) \cup W \rangle = CA(G; A)$.

Assume that $\omega := \omega_1 \ldots \omega_\ell \in W$, with $\omega_m \in W$, $\forall m = 1, \ldots, \ell$, (4)

is a UCA of type $(B_i, B_j)$. First note that, as $\omega$ has no GoE in $B_k$, for all $k \neq i$, then $(B_k)\omega = B_k$.

Hence,

$$(B_k)\omega_m = B_k$$

because $\omega_m$ cannot map any $G$-orbit of $B_k$ to a different subshift $B_i$, as there is no CA mapping back $B_k$ to $B_k$ (see Lemmas [10] and [3], and $\omega_m$ does not have GoE inside $B_k$ because this would be a GoE for $\omega$ inside $B_k$.

Now, observe that each non-invertible $\omega_m$ that appears in (4) has a unique GoE orbit $\Omega_m$ (inside $B_i$ because of (5)). This is true because if $\Omega_m$ consists of more than one orbit, then $(A^{G})\omega_m = A^{G} \setminus \Omega_m$ implies that the size of $(A^{G})\omega$ is strictly smaller than $|A^{G} \setminus \Omega_m|$, where $O_i \subseteq B_i$ is the unique GoE $G$-orbit of $\omega$.

Let $\omega'$ the the first non-invertible CA that appears in (4). We finish the proof by showing that $(\Omega_\ell)\omega_\ell \subseteq B_j$. Let $\Omega'_s = (\Omega_s)\omega_{s-1} \ldots \omega_1$. There are three possibilities:

Case 1: $(\Omega_s)\omega_s = P_c \subseteq B_c$ for $c \neq i, j$. Then:

$$(\Omega'_s)\omega = (\Omega_s)\omega_s \ldots \omega_\ell = (P_c)\omega_{s+1} \ldots \omega_\ell \subseteq B_c,$$

where the last contention is because of (5). However, as $\omega$ maps all orbits of $B_i$ to $B_i \cup B_j$, this case is impossible.

Case 2: $(\Omega_s)\omega_s \subseteq B_i$. If $i = j$, then $\omega_s$ is a UCA of the same type as $\omega$. Hence, let $i \neq j$. By the uniqueness of $\Omega_s$, $(B_i \setminus \Omega_s)\omega_s = (B_i \setminus \Omega_s)$, so there exists a $G$-orbit $Q \subseteq B_i$, $Q \neq \Omega_s$, such that $(\Omega_s)\omega_s = (Q)\omega_s$. Let $Q' = (Q)\omega_{s-1} \ldots \omega_1$. Then,

$$(\Omega'_s)\omega = (\Omega_s)\omega_s \ldots \omega_\ell = (Q)\omega_s \ldots \omega_\ell = (Q')\omega.$$

However, as $\omega$ maps its only GoE orbit to $B_j$, it does not collapse orbits in $B_i$. So this case, with $i \neq j$ is impossible.

Case 3: $(\Omega_s)\omega_s \subseteq B_j$. In this case, $\omega_s$ is a UCA of type $(B_i, B_j)$.

In any case, we obtain a contradiction with the assumption that $W$ has no UCA of type $(B_i, B_j)$. Therefore, $\langle W \rangle$ has no UCA of type $(B_i, B_j)$. \qed
**Claim.** If $G$ is a Dedekind group, then $\text{Rank}(\text{CA}(G; A) : \text{ICA}(G; A)) = |V|$.

*Proof.* We will show that

$$\text{CA}(G; A) = M := (\text{ICA}(G; A) \cup V).$$

For any $\sigma \in \text{CA}(G; A)$, consider $\sigma_i \in \text{CA}(G; A)$, $1 \leq i \leq r$, defined by

$$(x)\sigma_i = \begin{cases} (x)\sigma & \text{if } x \in B_i \\ x & \text{otherwise.} \end{cases}$$

By Lemmas 3 and 10, we know that $G_x \leq G_{(x)\sigma}$, for all $x \in A^G$, so $(B_i)\sigma \subseteq \bigcup_{j \leq i} B_j$ for all $i$ (recall the order given by 3). Hence, we have the decomposition

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r.$$

We shall prove that $\sigma_i \in M$ for all $1 \leq i \leq r$. For each $\sigma_i$, decompose $B_i = B_i' \cup B_i''$, where

$$B_i' := \bigcup \{ P \in \mathcal{O}(G; A) : P \subseteq B_i \text{ and } (P)\sigma_i \subseteq B_j \text{ for some } j < i \},$$

$$B_i'' := \bigcup \{ P \in \mathcal{O}(G; A) : P \subseteq B_i \text{ and } (P)\sigma_i \subseteq B_i \}.$$

If $\sigma_i'$ and $\sigma_i''$ are the CA that act as $\sigma_i$ on $B_i'$ and $B_i''$, respectively, and fix everything else, then $\sigma_i = \sigma_i' \circ \sigma_i''$. We shall prove that $\sigma_i' \in M$ and $\sigma_i'' \in M$.

1. We show that $\sigma_i' \in M$. For any orbit $P \subseteq B_i'$, the orbit $Q := (P)\sigma_i'$ is contained in $B_j$ for some $j < i$. By Theorem 3, there exists an involution

$$\phi \in \left( (N_G(G_{x_i}) / G_{x_i}) \wr \text{Sym}_{\alpha_i} \right) \times \left( (N_G(G_{x_j}) / G_{x_j}) \wr \text{Sym}_{\alpha_j} \right) \leq \text{ICA}(G; A)$$

that induces the double transposition $(x_i, G, P)(x_j, G, Q)$. By Lemma 11, ICA($G; A$) is transitive on $x_iG$ and $x_jG$ (as $G$ is Dedekind), so we may take $\phi$ such that $(x_i)\phi\sigma_i' = (x_j)\phi$. Then,

$$(z)\sigma_i'(z) = (z)\phi\tau_{x_i,x_j}\phi, \quad \forall z \in P = (x_iG)\phi.$$ 

As $\sigma_i'$ may be decomposed as a product of CA that only move one orbit in $B_i'$, this shows that $\sigma_i' \in M$.

2. We show that $\sigma_i'' \in M$. In this case, $\sigma_i'' \in \text{Tran}(B_i)$. In fact, as $\sigma_i''$ preserves the partition of $B_i$ into $G$-orbits, Lemma 3 and Lemma 2.1 (i) imply that $\sigma_i'' \in (G / G_{x_i}) \wr \text{Tran}_{\alpha_i}$. If $\alpha_i \geq 2$, the monoid $\text{Tran}_{\alpha_i}$ is generated by $\text{Sym}_{\alpha_i} \leq \text{ICA}(G; A)$ together with the idempotent $\tau_{x_i, y_i}$. Hence, $\sigma_i'' \in M$.

Therefore, we have established that $\text{CA}(G; A) = (\text{ICA}(G; A) \cup V)$. \hfill \qed

**Claim.** If $G$ is not a Dedekind group, then $\text{Rank}(\text{CA}(G; A) : \text{ICA}(G; A)) > |V|$.

*Proof.* As $G$ is not Dedekind, so there is a subgroup $H \leq G$ which is not normal. Hence, $H = G_{x_i}$ for a non-constant configuration $x_i \in A^G$, and, by the proof of Lemma 11 ICA($G; A$) is not transitive on $x_iG$. Consider the idempotent $\tau_{i,1} \in V$. Then $\tau_{i,1} = (P \to x_i)$, where $P$ is the ICA($G; A$)-orbit inside $x_iG$ that contains $x_i$ and $x_1 \in A^G$ is a constant configuration. Let $Q$ be an ICA($G; A$)-orbit inside $x_iG$ such that $Q \neq P$. As there is no $\phi \in \text{ICA}(G; A)$ mapping $P$ to $Q$, we have $(Q \to x_i) \notin (\text{ICA}(G; A) \cup V)$. Therefore, the edge $([H],[G])$ of the graph on $\mathcal{C}_G$ must be counted at least twice for its contribution towards the relative rank of ICA($G; A$) on CA($G; A$). The claim follows. \hfill \qed

Using Theorem 7 we may find an upper bound for the smallest size of a generating set of CA($G; A$), when $G$ is a finite Dedekind group.
Corollary 5. Let $G$ be a finite Dedekind group and $A$ a finite set of size $q \geq 2$. Suppose that $\text{Rank}(G) = m$ and that $G$ has $r$ different subgroups. Then,

$$\text{Rank}(\text{CA}(G; A)) \leq m(r - 1) + \frac{1}{2}r(r + 5).$$

Proof. Observe that for any $\alpha \geq 3$ and any $H \leq G$, we have $\text{Rank}((G/H) \wr \text{Sym}_\alpha) \leq m + 2$ because

$$\{(g_1, e, \ldots, e); \text{id}), \ldots, ((g_m, e, \ldots, e); \text{id}), ((e, \ldots, e); (1,2)), ((e, \ldots, e); (1,2, \ldots, \alpha))\}$$

is a generating set of $(G/H) \wr \text{Sym}_\alpha$, whenever $\{g_1, \ldots, g_m\}$ is a generating set for $G$.

Let $H_1, H_2, \ldots, H_r$ be the list of different subgroups of $G$ with $H_1 = G$. For each $1 \leq i \leq r$, let $\alpha_i := \alpha_{[H_i]}(G; A)$. Thus, by Lemma 8, Corollary 3, and Theorem 7 we have:

$$\text{Rank}(\text{CA}(G; A)) = \text{Rank}(\text{ICA}(G; A)) + \text{Rank}((\text{CA}(G; A) : \text{ICA}(G; A)))$$

$$\leq \sum_{i=1}^{r} \text{Rank}((G/H_i) \wr \text{Sym}_{\alpha_i}) + |E_G|$$

$$\leq \text{Rank}((\text{Sym}_q) + \sum_{i=2}^{r} (m + 2) + \binom{r}{2} + r$$

$$\leq 2 + (r - 1)(m + 2) + \frac{1}{2}r(r - 1) + r$$

$$= m(r - 1) + \frac{1}{2}r(r + 5).$$

\[\Box\]

Figure 1: Hasse diagram of subgroup lattice of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

The bound of Corollary 5 may become tighter if we actually know $|E_G|$ and $\text{Rank}(G/H_i)$, for all $H_i \leq G$.

Example 5. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ be the Klein-four group and $A = \{0, 1\}$. With the notation of Example 2, Figure 1 illustrates the Hasse diagram of the subgroup lattice of $G$ (i.e. the actual lattice of subgroups is the transitive and reflexive closure of this graph). Hence, by Theorem 7 and Example 4

$$\text{Rank}(\text{CA}(G; A) : \text{ICA}(G; A)) = |E_G| - 3 = 12 - 3 = 9,$$

$$\text{Rank}(\text{CA}(G; A)) \leq 9 + 9 = 18, \text{ as } \text{Rank}(\text{ICA}(G; A)) \leq 9.$$

6 Conclusions

In this paper we studied the monoid $\text{CA}(G; A)$ of all cellular automata over a finite group $G$ and a finite set $A$. Our main results are the following:
1. We completely determined the structure of the group of invertible cellular automata \(ICA(G; A)\) in terms of the structure of \(G\) (Theorem 3).

2. We improved the known lower bound on the number of aperiodic configurations of \(A^G\) (Theorem 4).

3. We showed that any generating set of \(CA(G; A)\) must have at least one cellular automaton whose minimal memory set is \(G\) itself (Theorem 6).

4. We gave a lower bound for the minimal size of a set \(V \subseteq CA(G; A)\) such that \(ICA(G; A) \cup V\) generates \(CA(G; A)\), and we showed that this lower bound is achieved if and only if all subgroups of \(G\) are normal (Theorem 7).

Most of our results are particularly good for finite Dedekind groups, i.e. finite groups in which all subgroups are normal (this includes all finite abelian groups).

Some open problems and directions for future work are the following:

1. Examine further the case when \(G\) is not a Dedekind group; in particular, determine the relative rank of \(ICA(G; A)\) on \(CA(G; A)\).

2. Improve the upper bound on \(\text{Rank}(CA(G; A))\) given by Corollary 5.

3. Study generating sets of \(CA(G; A)\) when \(G\) is an infinite group.

4. Study other algebraic properties of the monoid \(CA(G; A)\).

7 Acknowledgments

This work was supported by the EPSRC grant EP/K033956/1. We kindly thank Turlough Neary and Matthew Cook for their invitation to submit this paper and for the organisation of the conference AUTOMATA 2016. We also thank the referees of this paper for their insightful suggestions.

References

[1] Araújo, J., Bentz, W., Mitchell, J.D., Schneider, C.: The rank of the semigroup of transformations stabilising a partition of a finite set. Mat. Proc. Camb. Phil. Soc. **159**, 339–353 (2015).

[2] Araújo, J., Schneider, C.: The rank of the endomorphism monoid of a uniform partition. Semigroup Forum **78**, 498–510 (2009).

[3] Cameron, P.J.: Combinatorics: Topics, Techniques, Algorithms. Cambridge University Press, Cambridge (1994).

[4] Castillo-Ramirez, A., Gadouleau, M.: Ranks of finite semigroups of one-dimensional cellular automata. Semigroup Forum **93**, no. 2, 347–362 (2016).

[5] Castillo-Ramirez, A., Gadouleau, M.: On Finite Monoids of Cellular Automata. In: Cook, M., Neary, T. (eds.) Cellular Automata and Discrete Complex Systems. LNCS **9664**, 90–104, Springer International Publishing (2016).

[6] Ceccherini-Silberstein, T., Coornaert, M.: Cellular Automata and Groups. Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg (2010).

[7] Cyr, V., Bryna, K.: The automorphism group of a shift of linear growth: beyond transitivity. Forum Math. Sigma **3**, e5, 1–27 (2015).

[8] Dedekind, R.: Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind (German) Math. Ann. **48**, no. 4, 548–561 (1897).
[9] Dixon, J.D., Mortimer, B.: Permutation Groups. Graduate Texts in Mathematics 163, Springer-Verlag, New York (1996).

[10] Ganyushkin, O., Mazorchuk, V.: Classical Finite Transformation Semigroups: An Introduction. Algebra and Applications 9, Springer-Verlag, London (2009).

[11] Gao, S., Jackson, S., Seward, B.: Group Colorings and Bernoulli Subflows. Mem. Am. Math. Soc. 241, no. 1141, 1–239 (2016).

[12] Gomes, G.M.S., Howie, J.M.: On the ranks of certain finite semigroups of transformations. Math. Proc. Camb. Phil. Soc. 101, 395–403 (1987).

[13] Gray, R.D.: The minimal number of generators of a finite semigroup. Semigroup Forum 89, 135–154 (2014).

[14] Hartman, Y.: Large semigroups of cellular automata. Ergodic Theory Dyn. Syst. 32, 1991–2010 (2012).

[15] Hawkes, T., Isaacs, I.M., Özyaydin, M.: On the M"obius Function of a Finite Group. Rocky Mt. J. Math. 19, no. 4, 1003–1034 (1989).

[16] Howie, J.M., McFadden, R.B.: Idempotent rank in finite full transformation semigroups. Proc. Royal Soc. Edinburgh 114A, 161–167 (1990).

[17] Kari, J.: Theory of cellular automata: A Survey. Theoret. Comput. Sci. 334, 3–33 (2005).

[18] Kerber, A.: Applied Finite Group Actions, 2nd ed. Algorithms and Combinatorics 19, Springer (1999).

[19] Salo, V.: Groups and Monoids of Cellular Automata. In: Kari, J. (ed.) Cellular Automata and Discrete Complex Systems. LNCS 9099, 17–45, Springer Berlin Heidelberg (2015).

A. Castillo-Ramirez (Corresponding author), Universidad de Guadalajara, CUCEI, Departamento de Matemáticas, Guadalajara, México.
Email: alonso.castillor@academicos.udg.mx

M. Gadouleau, School of Engineering and Computing Sciences, Durham University, South Road, Durham DH1 3LE, U.K.
Email: m.r.gadouleau@durham.ac.uk