On Finite Monoids of Cellular Automata

Alonso Castillo-Ramirez* and Maximilien Gadouleau†

School of Engineering and Computing Sciences,
Durham University, South Road,
Durham, DH1 3LE
Telephone: +44 (0) 191 33 41729

January 22, 2016

Abstract

For any group G and set A, a cellular automaton over G and A is a transformation $\tau : A^G \to A^G$ defined via a finite neighborhood $S \subseteq G$ (called a memory set of τ) and a local function $\mu : A^S \to A$. In this paper, we assume that G and A are both finite and study various algebraic properties of the finite monoid $\mathrm{CA}(G, A)$ consisting of all cellular automata over G and A. Let $\mathrm{ICA}(G; A)$ be the group of invertible cellular automata over G and A. In the first part, using information on the conjugacy classes of subgroups of G, we give a detailed description of the structure of $\mathrm{ICA}(G; A)$ in terms of direct and wreath products. In the second part, we study generating sets of $\mathrm{CA}(G; A)$. In particular, we prove that $\mathrm{CA}(G, A)$ cannot be generated by cellular automata with small memory set, and, when G is finite abelian, we determine the minimal size of a set $V \subseteq \mathrm{CA}(G; A)$ such that $\mathrm{CA}(G; A) = \langle \mathrm{ICA}(G; A) \cup V \rangle$.

1 Introduction

Cellular automata (CA), first introduced by John von Neumann 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 theory of CA has been greatly enriched with its connections to group theory and topology (see [4] and references therein). One of the goals of this paper is to embark in the new task of exploring CA from the point of view of finite group and semigroup theory.

We review the broad definition of CA that appears in [4, 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 $x : G \to A$. For each $g \in G$, let $R_g : G \to G$ 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 [4] functions are applied on the left.

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

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

*Email: alonso.castillo-ramirez@durham.ac.uk
†Email: m.r.gadouleau@durham.ac.uk

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 [11]).

A *semigroup* is a set M equipped with an associative binary operation. If there exists an element $\mathrm{id} \in M$ such that $\mathrm{id} \cdot m = m \cdot \mathrm{id} = m$, for all $m \in M$, the semigroup M is called a *monoid* and id an *identity* of M. Clearly, the identity of a monoid is always unique.

Let $\mathrm{CA}(G; A)$ be the set of all cellular automata over G and A; by [4, 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 [3, 9, 12]), the algebraic structure of $\mathrm{CA}(G; A)$ remains basically unknown. In particular, the study of $\mathrm{CA}(G; A)$, when G and A are both finite, has been generally disregarded, perhaps because some of the classical questions are trivially answered (e.g. the Garden of Eden theorems become trivial). However, many new questions, typical of finite semigroup theory, arise in this setting.

In this paper, we study various algebraic properties of $\mathrm{CA}(G; A)$ 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 $\mathrm{ICA}(G; A)$ consisting of all invertible CA: we show that its structure is linked with the number of conjugacy classes of subgroups of G, and we give an explicit decomposition in terms of direct and wreath products.

In Section 4, we study generating sets of $\mathrm{CA}(G; A)$. We prove that $\mathrm{CA}(G; A)$ cannot be generated by CA with small memory sets: if T generates $\mathrm{CA}(G; A)$, then T must contain a cellular automaton with minimal memory set equal to G itself. This result provides a striking contrast with CA over infinite groups. Finally, when G is finite abelian, we find the smallest size of a set $U \subseteq \mathrm{CA}(G; A)$ such that $\mathrm{ICA}(G; A) \cup U$ generate $\mathrm{CA}(G; A)$; this number is known in semigroup theory as the *relative rank* of $\mathrm{ICA}(G; A)$ in $\mathrm{CA}(G; A)$, and it turns out to be related with the number of edges of the subgroup lattice of G.

2 Basic Results

For any set X, let $\mathrm{Tran}(X)$ and $\mathrm{Sym}(X)$ be the sets of all functions and bijective functions, respectively, of the form $\tau : X \to X$. Equipped with the composition of functions, $\mathrm{Tran}(X)$ is known as the *full transformation monoid* on X, while $\mathrm{Sym}(X)$ is the *symmetric group* on X. When X is finite and $|X| = q$, we write Tran_q and Sym_q instead of $\mathrm{Tran}(X)$ and $\mathrm{Sym}(X)$, respectively.

A *finite transformation monoid* is simply a submonoid of Tran_q, for some q. This type of monoids has been extensively studied (e.g. see [6] and references therein), and it should be noted its close relation to finite-state machines.

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

If $n = 1$, then $\mathrm{CA}(G; A) = \mathrm{Tran}(A)$, while, if $q \leq 1$, then $\mathrm{CA}(G; A)$ is the trivial monoid with one element; henceforth, we assume $n \geq 2$ and $q \geq 2$. We usually identify A with the set $\{0, 1, \ldots, q-1\}$.

The 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

$$(h)x \cdot g = (hg^{-1})x, \quad \forall h \in G.$$

A transformation $\tau : A^G \to A^G$ is *G-equivariant* if, for all $x \in A^G$, $g \in G$,

$$(x \cdot g)\tau = ((x)\tau) \cdot g.$$

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

$$\mathrm{ICA}(G;A) := \{\tau \in \mathrm{CA}(G;A) : \exists \phi \in \mathrm{CA}(G;A) \text{ such that } \tau\phi = \phi\tau = \mathrm{id}\}.$$

Theorem 1. *Let G be a finite group and A a finite set.*

(i) $\mathrm{CA}(G;A) = \{\tau \in \mathrm{Tran}(A^G) : \tau$ *is G-equivariant*$\}$.

(ii) $\mathrm{ICA}(G;A) = \mathrm{CA}(G;A) \cap \mathrm{Sym}(A^G)$.

Proof. The first part follows by Curtis-Hedlund Theorem (see [4, Theorem 1.8.1]) while the second part follows by [4, Theorem 1.10.2]. □ □

Notation 1. 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 $\mathcal{O}(G;A)$ be the set of all G-orbits on A^G:

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

Clearly, $\mathcal{O}(G;A)$ forms a partition of A^G. In general, when X is a set and $\mathcal{P}$ is a partition of X, we say that a transformation monoid $M \leq \mathrm{Tran}(X)$ *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 $\tau \in \mathrm{CA}(G;A)$,*

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

In particular, $\mathrm{CA}(G;A)$ preserves the partition $\mathcal{O}(G;A)$ of A^G.

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

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 $\mathbf{k} \in A^G$.

Lemma 2. *Let $\tau \in \mathrm{CA}(G;A)$ and let $\mathbf{k} \in A^G$ be a constant configuration. Then, $(\mathbf{k})\tau \in A^G$ 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,

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

Hence, $(\mathbf{k})\tau$ is constant. □ □

For a monoid M and a subset $T \subseteq M$, denote by $C_M(T)$ the *centraliser* of T in M:

$$C_M(T) := \{m \in M : mt = tm, \forall t \in T\}.$$

If G is abelian, the transformation $\sigma_g : A^G \to A^G$, with $g \in G$, defined by

$$(x)\sigma_g := x \cdot g, \quad \forall x \in A^G,$$

is in $\mathrm{CA}(G;A)$. It follows by Theorem 1 that $CA(G;A) = C_{\mathrm{Tran}(A^G)}(T)$, where $T := \{\sigma_g : g \in G\}$.

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

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

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

3 The Structure of $\mathrm{ICA}(G; A)$

Let G be a finite group of size $n \geq 2$ and A a finite set of size $q \geq 2$. We review few basic concepts about permutation groups (see [5, 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 $x : G \to A$ by

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

Say that two subgroups H_1 and H_2 of G are *conjugate* in G if there exists $g \in G$ such that $g^{-1}H_1g = H_2$. This defines an equivalence relation on the subgroups of G. Denote by $[H]$ the conjugacy class of $H \leq G$.

We say that the actions of G on two sets Ω and Γ are *equivalent* if there is a bijection $\lambda : \Omega \to \Gamma$ such that, for all $x \in \Omega, g \in G$, we have $(x \cdot g)\lambda = (x)\lambda \cdot g$.

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 size $n \geq 2$ and A a finite set of size $q \geq 2$. For any $x, y \in A^G$, there exists $\tau \in \mathrm{ICA}(G; A)$ such that $(xG)\tau = yG$ if and only if $[G_x] = [G_y]$.*

Proof. By [5, Lemma 1.6B], the actions of G on xG and yG are equivalent if and only if G_x and G_y are conjugate in G. We claim that the actions of G on xG and yG are equivalent if and only if there is $\tau \in \mathrm{ICA}(G; A)$ such that $(xG)\tau = yG$. Assume such $\tau \in \mathrm{ICA}(G; A)$ exists. Then, the restriction $\lambda := \tau|_{xG} : xG \to yG$ is the bijection required to show that the actions of G on xG and yG are equivalent. Conversely, suppose there is a bijection $\lambda : xG \to yG$ such that $(z \cdot g)\lambda = (z)\lambda \cdot g$, for all $z \in xG$, $g \in G$. Define $\tau : A^G \to A^G$ by

$$(z)\tau := \begin{cases} (z)\lambda & \text{if } z \in xG, \\ (z)\lambda^{-1} & \text{if } z \in yG, \\ z & \text{otherwise,} \end{cases} \quad \forall z \in A^G.$$

Clearly, τ is G-equivariant and invertible (in fact, $\tau = \tau^{-1}$). Hence $\tau \in \mathrm{ICA}(G; A)$, and it satisfies $(xG)\tau = yG$. □ □

Corollary 1. *Suppose that G is a finite abelian group. For any $x, y \in A^G$, there exists $\tau \in \mathrm{ICA}(G; A)$ such that $(xG)\tau = yG$ if and only if $G_x = G_y$.*

For any integer $\alpha \geq 2$ and any group C, the *wreath product* of C by Sym_α is the set

$$C \wr \mathrm{Sym}_\alpha := \{(v; \phi) : v \in C^\alpha, \phi \in \mathrm{Sym}_\alpha\}$$

equipped with the operation

$$(v; \phi) \cdot (w; \psi) = (vw^\phi; \phi\psi), \text{ for any } v, w \in C^\alpha, \phi, \psi \in \mathrm{Sym}_\alpha$$

where ϕ acts on w by permuting its coordinates:

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

See [5, Sec. 2.6] for a more detailed description of the wreath product.

Notation 2. Let $O \in \mathcal{O}(G;A)$ be a G-orbit on A^G. If $G_{(O)}$ is the pointwise stabiliser of O, i.e. $G_{(O)} := \bigcap_{x\in O} G_x$, then $G^O := G/G_{(O)}$ is a group that is isomorphic to a subgroup of $\mathrm{Sym}(O)$ (see [5, p. 17]). Consider the group

$$C(G^O) := \{\tau|_O : O \to A^G : \tau \in \mathrm{ICA}(G;A) \text{ and } (O)\tau = O\}. \tag{1}$$

By Theorem 1, $C(G^O)$ is isomorphic to the centraliser of G^O in $\mathrm{Sym}(O)$:

$$C(G^O) \cong C_{\mathrm{Sym}(O)}(G^O).$$

Notation 3. Let H be a subgroup of G and $[H]$ its conjugacy class. Define

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

Note that $B_{[H]}$ is a union of G-orbits and, by the Orbit-Stabiliser Theorem (see [5, Theorem 1.4A]), all the G-orbits contained in $B_{[H]}$ have equal sizes. Define

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

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

$$\mathcal{B} := \{B_{[H]} : H \leq G\}$$

is a partition of A^G with r blocks.

Remark 2. $B_{[G]} = \{x \in A^G : x \text{ is constant}\}$ and $\alpha_{[G]}(G;A) = q$.

Example 1. 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

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

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 2×2 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

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

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

$$O_6 := \left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right\},$$

$$O_7 := \left\{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right\}.$$

Hence,

$$B_{[H_1]} := O_1 \cup O_2,\ B_{[H_2]} := O_3,\ B_{[H_3]} := O_4,\ B_{[H_4]} := O_5,\ B_{[H_5]} := O_6 \cup O_7;$$
$$\alpha_{[H_i]}(G;A) = 2,\ \text{for } i \in \{1,5\},\ \text{and } \alpha_{[H_i]}(G;A) = 1,\ \text{for } i \in \{2,3,4\}.$$

Remark 3. By Lemma 3, the $\mathrm{ICA}(G;A)$-orbits on A^G coincide with the blocks in $\mathcal{B}$, while the $\mathrm{ICA}(G;A)$-blocks of imprimitivity on each $B_{[H]}$ are the G-orbits contained in $B_{[H]}$.

The following result is a refinement of [12, Theorem 9] and [3, Lemma 4].

Theorem 2. *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 different conjugacy classes of subgroups of G. For each $1 \leq i \leq r$, fix a G-orbit $O_i \subseteq B_{[H_i]}$. Then,*

$$\mathrm{ICA}(G; A) \cong \prod_{i=1}^{r} \left(C_i \wr \mathrm{Sym}_{\alpha_i} \right),$$

where $C_i := C(G^{O_i}) \cong C_{\mathrm{Sym}(O_i)}(G^{O_i})$ and $\alpha_i := \alpha_{[H_i]}(G; A)$.

Proof. Let $B_i := B_{[H_i]}$. By Lemma 3, $\mathrm{ICA}(G; A)$ is contained in the group

$$\prod_{i=1}^{r} \mathrm{Sym}(B_i) = \mathrm{Sym}(B_1) \times \mathrm{Sym}(B_2) \times \cdots \times \mathrm{Sym}(B_r).$$

For each $1 \leq i \leq r$, let $\mathcal{O}_i$ be the set of G-orbits contained in B_i (so $O_i \in \mathcal{O}_i$). Note that $\mathcal{O}_i$ is a uniform partition of B_i. For any $\tau \in \mathrm{ICA}(G; A)$, Lemma 1 implies that the projection of τ to $\mathrm{Sym}(B_i)$ is contained in

$$S(B_i, \mathcal{O}_i) := \{\phi \in \mathrm{Sym}(B_i) : \forall P \in \mathcal{O}_i,\ (P)\phi \in \mathcal{O}_i\}.$$

By [2, Lemma 2.1(iv)],

$$S(B_i, \mathcal{O}_i) \cong \mathrm{Sym}(O_i) \wr \mathrm{Sym}_{\alpha_i}.$$

It is well-known that Sym_{α_i} is generated by its transpositions. As the invertible cellular automaton constructed in the proof of Lemma 3 induces a transposition $(xG, yG) \in \mathrm{Sym}_{\alpha_i}$, with $xG, yG \in \mathcal{O}_i$, we deduce that $\mathrm{Sym}_{\alpha_i} \leq \mathrm{ICA}(G; A)$. The result follows by the construction of $C_i \cong C_{\mathrm{Sym}(O_i)}(G^{O_i})$ and Theorem 1. □ □

Corollary 2. *Let G be a finite abelian 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,*

$$\mathrm{ICA}(G; A) \cong \prod_{i=1}^{r} \left((G/H_i) \wr \mathrm{Sym}_{\alpha_i} \right),$$

and $|G|\alpha_i = |H_i| \cdot |\{x \in A^G : G_x = H_i\}|$, where $\alpha_i := \alpha_{[H_i]}(G; A)$.

Proof. By [5, Theorem 4.2A (v)], $C_{\mathrm{Sym}(O_i)}(G^{O_i}) \cong G^{O_i} \cong G/G_{x_i}$, where $x_i \in O_i$. By Remark 1, the list of pointwise stabilisers coincide with the list of subgroups of G, and, as G is abelian, $[H_i] = \{H_i\}$ for all i. Finally, by the Orbit-Stabiliser theorem, every orbit contained in $B_i = \{x \in A^G : G_x = H_i\}$ has size $\frac{|G|}{|H_i|}$; as these orbits form a partition of B_i, we have $|B_i| = \alpha_i \frac{|G|}{|H_i|}$. □ □

Example 2. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $A = \{0, 1\}$. By Example 1,

$$\mathrm{ICA}(G, A) \cong (\mathbb{Z}_2)^4 \times (G \wr \mathrm{Sym}_2).$$

4 Generating Sets of of $\mathrm{CA}(G; A)$

For a monoid M and a subset $T \subseteq M$, denote by $\langle T \rangle$ the submonoid *generated* by T, i.e. 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).

Define the *kernel* of a transformation $\tau : X \to X$, denoted by $\ker(\tau)$, as the partition of X induced by the equivalence relation $\{(x, y) \in X^2 : (x)\tau = (y)\tau\}$. For example, $\ker(\phi) = \{\{x\} : x \in X\}$, for any $\phi \in \mathrm{Sym}(X)$, while $\ker(y \to z) = \{\{y, z\}, \{x\} : x \in X \setminus \{y, z\}\}$, for $y, z \in X$, $y \neq z$.

A large part of the classical research on CA has been 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 $\mathrm{CA}(G;A)$.

Theorem 3. *Let G be a finite group of size $n \geq 2$ and A a finite set of size $q \geq 2$. Let T be a generating set of $\mathrm{CA}(G;A)$. Then, there exists $\tau \in T$ with minimal memory set $S = G$.*

Proof. Suppose that T is a generating set of $\mathrm{CA}(G,A)$ such that each of its elements has minimal memory set of size at most $n-1$. Consider the idempotent $\sigma := (\mathbf{0} \to \mathbf{1}) \in \mathrm{CA}(G,A)$, where $\mathbf{0}, \mathbf{1} \in A^G$ are different constant configurations. Then, $\sigma = \tau_1\tau_2 \dots \tau_\ell$, for some $\tau_i \in T$. By the definition of σ, there must be $1 \leq j \leq \ell$ such that $\ker(\tau_j) = \{\{\mathbf{0},\mathbf{1}\}, \{x\} : x \in A^G \setminus \{\mathbf{0},\mathbf{1}\}\}$. By Lemma 2, $(A^G_{\mathrm{c}})\tau_j \subseteq A^G_{\mathrm{c}}$ and $(A^G_{\mathrm{nc}})\tau_j = A^G_{\mathrm{nc}}$, where

$$A^G_{\mathrm{c}} := \{\mathbf{k} \in A^G : \mathbf{k} \text{ is constant}\} \text{ and } A^G_{\mathrm{nc}} := \{x \in A^G : x \text{ is non-constant}\}.$$

Let $S \subseteq G$ and $\mu : A^S \to A$ be the minimal memory set and local function of $\tau := \tau_j$, respectively. By hypothesis, $s := |S| < n$. Since the restriction of τ to A^G_{c} is not a bijection, there exists $\mathbf{k} \in A^G_{\mathrm{c}}$ (defined by $(g)\mathbf{k} := k \in A$, $\forall g \in G$) such that $\mathbf{k} \notin (A^G_{\mathrm{c}})\tau$.

For any $x \in A^G$, define the *k-weight* of x by

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

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

$$w := \sum_{x \in A^G_{\mathrm{nc}}} |x|_k = n(q-1)q^{n-1} - n(q-1) = n(q-1)(q^{n-1}-1).$$

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

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

$$\mathrm{Sub}(y,x) := |\{g \in G : y = x|_{Sg}\}|.$$

Then, for any $y \in A^S$,

$$N_y := \sum_{x \in A^G_{\mathrm{nc}}} \mathrm{Sub}(y,x) = \begin{cases} nq^{n-s} & \text{if } y \in A^S_{\mathrm{nc}}, \\ n(q^{n-s}-1) & \text{if } y \in A^S_{\mathrm{c}}. \end{cases}$$

Let $\delta : A^2 \to \{0,1\}$ be the Kronecker's delta function. Since $(A^G_{\mathrm{nc}})\tau = A^G_{\mathrm{nc}}$, we have

$$\begin{aligned} w &= \sum_{x \in A^G_{\mathrm{nc}}} |(x)\tau|_k = \sum_{y \in A^S} N_y(1 - \delta((y)\mu, k)) \\ &= nq^{n-s} \sum_{y \in A^S_{\mathrm{nc}}} (1 - \delta((y)\mu,k)) + n(q^{n-s}-1) \sum_{y \in A^S_{\mathrm{c}}} (1 - \delta((y)\mu,k)). \end{aligned}$$

Because $\mathbf{k} \notin (A^G_{\mathrm{c}})\tau$, we know that $(y)\mu \neq k$ for all $y \in A^S_{\mathrm{c}}$. Therefore,

$$\frac{w}{n} = q^{n-s} \sum_{y \in A^S_{\mathrm{nc}}} (1 - \delta_{(y)\mu,k}) + (q^{n-s}-1)q.$$

As $s < n$, this implies that $\frac{w}{n}$ is an integer divisible by q, which is a contradiction. □ □

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 $\mathrm{Rank}(M)$:

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

It is well-known that, if X is any finite set, the rank of the full transformation monoid $\mathrm{Tran}(X)$ is 3, while the rank of the symmetric group $\mathrm{Sym}(X)$ is 2 (see [6, Ch. 3]). Ranks of various finite monoids have been determined in the literature before (e.g. see [1, 2, 7, 8, 10]).

In [3], the rank of $\mathrm{CA}(\mathbb{Z}_n, A)$, where $\mathbb{Z}_n$ is the cyclic group of order n, was studied and determined when $n \in \{p, 2^k, 2^k p : k \geq 1,\ p \text{ odd prime}\}$. Moreover, the following problem was proposed:

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

For any finite monoid M and $U \subseteq M$, the *relative rank* of U in M, denoted by $\mathrm{Rank}(M : U)$, 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,

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

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

Lemma 4. *Let G be a finite group and A a finite set. Then,*

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

We shall determine the relative rank of $\mathrm{ICA}(G; A)$ in $\mathrm{CA}(G; A)$ 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 5. *Let G be a finite group and A a finite set of size $q \geq 2$. Let $x \in A^G$. If $(xG)\tau = xG$, then $\tau|_{xG} \in \mathrm{Sym}(xG)$.*

Proof. It is enough to show that $\tau|_{xG} : xG \to xG$ is surjective because xG is finite. Let $y \in xG$. Since $(x)\tau \in xG$, there is $g \in G$ such that $y = (x)\tau \cdot g$. By G-equivariance, $y = (x \cdot g)\tau \in (xG)\tau$, and the result follows. □ □

Notation 4. 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 $H_1 \leq g^{-1}H_2 g$, 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, $H_1 \leq g^{-1}H_2 g$ and $H_2 \leq f^{-1}H_2 f$, 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 $H_1 = g^{-1}H_2 g$. This shows that $[H_1] = [H_2]$.

Lemma 6. *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 $\tau \in \mathrm{CA}(G; A)$ such that $(xG)\tau = yG$ if and only if $[G_x] \leq [G_y]$.*

Proof. Suppose that $[G_x] \leq [G_y]$. Then, $G_x \leq g^{-1}G_y g$, for some $g \in G$. We define an idempotent $\tau_{x,y} : A^G \to A^G$ that maps xG to yG:

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

We verify that $\tau_{x,y}$ is well-defined. If $x \cdot h_1 = x \cdot h_2$, for $h_i \in G$, then $h_1 h_2^{-1} \in G_x$. As $G_x \leq g^{-1} G_y g$, for some $s \in G_y$, we have $h_1 h_2^{-1} = g^{-1} s g$. Thus, $g h_1 = s g h_2$ implies that $y \cdot g h_1 = y \cdot g h_2$, and $(x \cdot h_1)\tau = (x \cdot h_2)\tau$. Clearly, $\tau_{x,y}$ is non-invertible and G-equivariant, so $\tau_{x,y} \in \mathrm{CA}(G; A)$.

Conversely, suppose there exists $\tau \in \mathrm{CA}(G; A)$ such that $(xG)\tau = yG$. Then, $(x)\tau = y \cdot h$, for some $h \in G$. Let $s \in G_x$. By G-equivariance,

$$y \cdot h = (x)\tau = (x \cdot s)\tau = (x)\tau \cdot s = y \cdot hs.$$

Thus $hsh^{-1} \in G_y$ and $s \in h^{-1} G_y h$. This shows that $[G_x] \leq [G_y]$. □ □

Corollary 3. *Suppose that G is finite abelian. Let $x, y \in A^G$ be such that $xG \neq yG$. There exists $\tau_{x,y} \in \mathrm{CA}(G; A)$ such that $(x)\tau_{x,y} = y$ and $(z)\tau_{x,y} = z$ for all $z \in A^G \setminus xG$ if and only if $G_x \leq G_y$.*

Notation 5. Consider the directed graph $(\mathcal{C}_G, \mathcal{E}_G)$ with vertex set $\mathcal{C}_G$ and edge set

$$\mathcal{E}_G := \left\{ ([H_i], [H_j]) \in \mathcal{C}_G^2 : [H_i] \leq [H_j] \right\}.$$

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

Remark 5. Lemma 6 may be restated in terms of $\mathcal{E}_G$. By Lemma 5, loops $([H_i], [H_i])$ do not have corresponding non-invertible CA when $\alpha_{[H_i]}(G; A) = 1$.

Theorem 4. *Let G be a finite abelian group and A a finite set of size $q \geq 2$. 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 $\alpha_i := \alpha_{[H_i]}(G; A)$. Then,*

$$\mathrm{Rank}(\mathrm{CA}(G; A) : \mathrm{ICA}(G; A)) = |\mathcal{E}_G| - \sum_{i=2}^{r} \delta(\alpha_i, 1),$$

where $\delta : \mathbb{N}^2 \to \{0, 1\}$ is Kronecker's delta function.

Proof. For all $1 \leq i \leq r$, let $B_i := B_{[H_i]}$. Fix orbits $x_i G \subseteq B_i$, so $H_i = G_{x_i}$. Assume that the list of subgroups of G is ordered such that

$$|x_1 G| \leq \cdots \leq |x_r G|, \text{ or, equivalently, } |G_{x_1}| \geq \cdots \geq |G_{x_r}|.$$

For every $\alpha_i \geq 2$, fix orbits $y_i G \subseteq B_i$ such that $x_i G \neq y_i G$. We claim that $\mathrm{CA}(G, A) = M := \langle \mathrm{ICA}(G; A) \cup U \rangle$, where

$$U := \left\{ \tau_{x_i, x_j} : [G_{x_i}] < [G_{x_j}] \right\} \cup \left\{ \tau_{x_i, y_i} : \alpha_i \geq 2 \right\},$$

and $\tau_{x_i,x_j}, \tau_{x_i,y_i}$ are the idempotents defined in Corollary 3. For any $\tau \in \mathrm{CA}(G; A)$, consider $\tau_i \in \mathrm{CA}(G; A)$, $1 \leq i \leq r$, defined by

$$(x)\tau_i = \begin{cases} (x)\tau & \text{if } x \in B_i \\ x & \text{otheriwse.} \end{cases}$$

By Lemmas 3 and 6, $(B_i)\tau \subseteq \bigcup_{j \leq i} B_j$ for all i. Hence, we have the decomposition

$$\tau = \tau_1 \tau_2 \ldots \tau_r.$$

For each i, decompose τ_i further as $\tau_i = \tau_i' \tau_i''$, where $(B_i)\tau_i' \subseteq \bigcup_{j<i} B_j$ and $(B_i)\tau_i'' \subseteq B_i$. We shall prove that $\tau_i' \in M$ and $\tau_i'' \in M$.

1. We show that $\tau_i' \in M$. If $B_i = \cup_{s=1}^{\alpha_i} P_s$ is the decomposition of B_i into its G-orbits, we may write $\tau_i' = \tau_i'|_{P_1} \dots \tau_i'|_{P_{\alpha_i}}$, where $\tau_i'|_{P_s}$ acts as τ_i' on P_s and fixes everything else. Note that $Q_s = (P_s)\tau_i'|_{P_s}$ is a G-orbit in B_j for some $j < i$. By Theorem 2, there exist

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

such that ϕ_s acts as the double transposition $(x_iG, P_s)(x_jG, Q_s)$. Since G/G_{x_i} and G/G_{x_j} are transitive on their respective orbits, we may take ϕ_s such that $(x_i)\phi_s\tau_i'|_{P_s}\phi_s^{-1} = x_j$. Then,

$$\tau_i'|_{P_s} = \phi_s^{-1}\tau_{x_i,x_j}\phi_s \in M.$$

2. We show $\tau_i'' \in M$. In this case, $\tau_i'' \in \mathrm{Tran}(B_i)$. In fact, as τ_i'' preserves the partition of B_i into G-orbits, Lemma 5 implies that $\tau_i'' \in (G/G_{x_i}) \wr \mathrm{Tran}_{\alpha_i}$. If $\alpha_i \geq 2$, the semigroup Tran_{α_i} is generated by $\mathrm{Sym}_{\alpha_i} \leq \mathrm{ICA}(G, A)$ togerher with the idempotent τ_{x_i,y_i}. Hence, $\tau_i'' \in M$.

Therefore, we have established that $\mathrm{CA}(G; A) = \langle \mathrm{ICA}(G; A) \cup U \rangle$.

Suppose now that there exists $V \subseteq \mathrm{CA}(G; A)$ such that $|V| < |U|$ and

$$\langle \mathrm{ICA}(G; A) \cup V \rangle = \mathrm{CA}(G; A).$$

Hence, for some $\tau \in U$, we must have

$$V \cap \langle \mathrm{ICA}(G; A), \tau \rangle = \emptyset.$$

If $\tau = \tau_{x_i,y_i}$, for some i with $\alpha_i \geq 2$, this implies that there is no $\xi \in V$ with

$$\ker(\xi) = \left\{\{a, b\}, \{c\} : a \in x_iG,\ b \in y_iG,\ c \in A^G \setminus (x_iG \cup y_iG)\right\}.$$

Hence, there is no $\xi \in \langle \mathrm{ICA}(G; A) \cup V \rangle = \mathrm{CA}(G; A)$ with kernel of this form, which is a contradiction because τ_{x_i,y_i} itself has kernel of this form. We obtain a similar contradiction if $\tau = \tau_{x_i,x_j}$ with $[G_{x_i}] < [G_{x_j}]$. □ □

Corollary 4. *Let G be a finite abelian group with $\mathrm{Rank}(G) = m$ and A a finite set of size $q \geq 2$. With the notation of Theorem 4,*

$$\begin{aligned}\mathrm{Rank}(\mathrm{CA}(G; A)) &\leq \sum_{i=2}^{r} m\alpha_i + 2r + |\mathcal{E}_G| - \delta(q, 2) - \sum_{i=2}^{r}(3\delta(\alpha_i, 1) + \delta(\alpha_i, 2)) \\ &\leq \sum_{i=2}^{r} m\alpha_i + 2r + r^2.\end{aligned}$$

Proof. Using the fact $\mathrm{Rank}((G/H_i) \wr \mathrm{Sym}_{\alpha_i}) \leq m\alpha_i + 2 - 2\delta(\alpha_i, 1) - \delta(\alpha_i, 2)$ and $\mathrm{Rank}((G/H_1) \wr \mathrm{Sym}_q) = 2 - \delta(q, 2)$, the result follows by Theorem 4, Corollary 2 and Lemma 4. □ □

The bound of Corollary 4 may become tighter if we actually know $\mathrm{Rank}(G/H_i)$, for all $H_i \leq G$, as in Example 2.

Example 3. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ be the Klein-four group and $A = \{0, 1\}$. With the notation of Example 1, 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 4 and Example 2,

$$\begin{aligned}&\mathrm{Rank}(\mathrm{CA}(G; A) : \mathrm{ICA}(G; A)) = |\mathcal{E}_G| - 3 = 12 - 3 = 9, \\ &\mathrm{Rank}(\mathrm{CA}(G; A)) \leq 9 + 9 = 18, \text{ as } \mathrm{Rank}(\mathrm{ICA}(G; A)) \leq 9.\end{aligned}$$

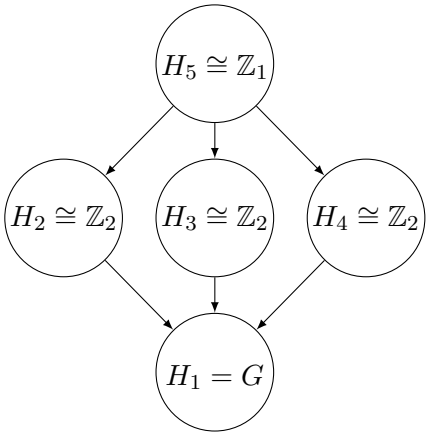

Figure 1: Lattice of subgroups of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Because of Theorem 4, it is particularly relevant to determine in which situations $\alpha_{[H]}(G; A) = 1$. We finish this paper with some partial results in this direction that hold for arbitrary finite groups.

Denote by $[G : H]$ the index of $H \leq G$ (i.e. the number of cosets of H in G).

Lemma 7. *Let G be a finite group and A a finite set of size $q \geq 2$. Assume there is $H \leq G$ with $[G : H] = 2$. Then, $\alpha_{[H]}(G; A) = 1$ if and only if $q = 2$.*

Proof. As $H \leq G$ has index 2, it is normal. Fix $s \in G \setminus H$. 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 $x \in B_{[H]}$.

Suppose first that $A = \{0, 1\}$. Let $y \in B_{[H]}$. As H is normal, $[H] = \{H\}$, so $G_y = H$. For any $h \in H$,

$$(h)y = (e)y \cdot h^{-1} = (e)y \text{ and } (sh)y = (s)y \cdot h^{-1} = (s)y,$$

so y is constant on the cosets H and $sH = Hs$. 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 $\alpha_{[H]}(G; A) = 1$.

If $|A| \geq 3$, we may use a similar argument as above, except that now $y \in B_{[H]}$ may satisfy $(g)y \in A \setminus \{0, 1\}$ for all $g \in H$, so $y \notin xG$ and $\alpha_{[H]}(G; A) \geq 2$. □ □

Lemma 8. *Let G be a finite group and A a finite set of size $q \geq 2$. Suppose there is $H \leq G$ such that $\alpha_{[H]}(G; A) = 1$. Then, $q \mid [G : H] = \frac{|G|}{|H|}$.*

Proof. Let $x \in B_{[H]}$ be such that $G_x = H$. As $\alpha_{[H]}(G; A) = 1$, $B_{[H]} = xG$. First we show that $x : G \to A$ is surjective. If $(G)x \subset A$, let $a \in (G)x$ and $b \in A \setminus (G)x$. Define $y \in A^G$ by

$$(g)y := \begin{cases} b & \text{if } (g)x = a \\ (g)x & \text{otherwise.} \end{cases}$$

Then $y \in B_{[H]}$, as $G_y = G_x$, but $y \notin xG$, which is a contradiction. For $a \in A$, let $(a)x^{-1} := \{g \in G : (g)x = a\}$. Now we show that, for any $a, b \in A$,

$$|(a)x^{-1}| = |(b)x^{-1}|.$$

Suppose that $|(a)x^{-1}| < |(b)x^{-1}|$. Define $z \in A^G$ by

$$(g)z := \begin{cases} b & \text{if } (g)x = a \\ a & \text{if } (g)x = b \\ (g)x & \text{otherwise.} \end{cases}$$

Again, $z \in B_{[H]}$, as $G_z = G_x$, but $z \notin xG$, which is a contradiction. As x is constant on the left cosets of H in G, for each $a \in A$, $(a)x^{-1}$ is a union of left cosets. All cosets have the same size, so $(a)x^{-1}$ and $(b)x^{-1}$ contain the same number of them, for any $a, b \in A$. Therefore, $q \mid [G : H]$. □ □

Corollary 5. *Let G be a finite abelian group and A a finite set of size $q \geq 2$ such that $q \nmid |G|$. With the notation of Theorem 4,*

$$\mathrm{Rank}(\mathrm{CA}(G; A) : \mathrm{ICA}(G; A)) = |\mathcal{E}_G|.$$

Acknowledgments.

This work was supported by the EPSRC grant EP/K033956/1.

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] Castillo-Ramirez, A., Gadouleau, M.: Ranks of finite semigroups of one-dimensional cellular automata, `http://arxiv.org/abs/1510.00197` (2015).

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

[5] Dixon, J.D., Mortimer, B.: Permutation Groups. Graduate Texts in Mathematics **163**, Springer-Verlag, New York (1996).

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

[7] 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).

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

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

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

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

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