Von Neumann Regular Cellular Automata

Alonso Castillo-Ramirez and Maximilien Gadouleau

January 11, 2017

Abstract

For any group G and any set A, a cellular automaton (CA) is a transformation of the configuration space A^G defined via a finite memory set and a local function. Let $\mathrm{CA}(G; A)$ be the monoid of all CA over A^G. In this paper, we investigate a generalisation of the inverse of a CA from the semigroup-theoretic perspective. An element $\tau \in \mathrm{CA}(G; A)$ is *von Neumann regular* if there exists $\sigma \in \mathrm{CA}(G; A)$ such that $\tau \circ \sigma \circ \tau = \tau$ and $\sigma \circ \tau \circ \sigma = \sigma$, where $\circ$ is the composition of functions. Such an element σ is called a *generalised inverse* of τ. The monoid $\mathrm{CA}(G; A)$ itself is von Neumann regular if all its elements are von Neumann regular. We establish that $\mathrm{CA}(G; A)$ is von Neumann regular if and only if $|G| = 1$ or $|A| \leq 1$, and we characterise all von Neumann regular elements in $\mathrm{CA}(G; A)$ when G and A are both finite. Furthermore, we study von Neumann regular linear CA when G is an abelian group and $A = \mathbb{F}$ is a field; in particular, we characterise them when G is torsion-free abelian or finite abelian with $\mathrm{char}(\mathbb{F}) \nmid |G|$.

Keywords: Cellular automata, linear cellular automata, monoids, von Neumann regular elements, generalised inverses.

1 Introduction

Cellular automata (CA), introduced by John von Neumann and Stanislaw Ulam in the 1940s, are models of computation with important applications to computer science, physics, and theoretical biology. We follow the modern general setting for CA presented in [5]. For any group G and any set A, a CA over G and A is a transformation of the configuration space A^G defined via a finite memory set and a local function. Most of the classical literature on CA focus on the case when $G = \mathbb{Z}^d$, for $d \geq 1$, and A is a finite set (see [10]), but important results have been obtained for larger classes of groups (e.g., see [5] and references therein).

Recall that a *semigroup* is a set equipped with an associative binary operation, and that a *monoid* is a semigroup with an identity element. Let $\mathrm{CA}(G; A)$ be the set of all CA over G and A. It turns out that, equipped with the composition of functions, $\mathrm{CA}(G; A)$ is a monoid.

In general, $\tau \in \mathrm{CA}(G; A)$ is called *invertible*, or *reversible*, or *a unit*, if there exists $\sigma \in \mathrm{CA}(G; A)$ such that $\tau\sigma = \sigma\tau = \mathrm{id}$ (here $\tau\sigma$ represents the function composition obtained by applying τ first, and then σ). In such case, σ is called *the inverse* of τ and denoted by $\sigma = \tau^{-1}$. When A is finite, it may be shown that $\tau \in \mathrm{CA}(G; A)$ is invertible if and only if it is a bijective function (see [5, Theorem 1.10.2]).

We shall consider the notion of *regularity* which, coincidentally, was introduced by John von Neumann in the context of rings, and has been widely studied in semigroup theory (recall that the multiplicative structure of a ring is precisely a semigroup). Intuitively, cellular automaton $\tau \in \mathrm{CA}(G; A)$ is *von Neumann regular* if there exists $\sigma \in \mathrm{CA}(G; A)$ mapping any configuration in the image of τ to one of its preimages under τ. Clearly, this generalises the notion of reversibility.

From now on, we simply use the term 'regular' to mean 'von Neumann regular'. Let S be any semigroup. For $a, b \in S$, we say that b is *a weak generalised inverse* of a if

$$aba = a.$$

We say that b is *a generalised inverse* (often just called *an inverse*) of a if

$$aba = a \text{ and } bab = b.$$

An element $a \in S$ may have none, one, or more (weak) generalised inverses. It is clear that any generalised inverse of a is also a weak generalised inverse; not so obvious is that, given the set $W(a)$ of weak generalised inverses of a we may obtain the set $V(a)$ of generalised inverses of a as follows (see [6, Exercise 1.9.7]):

$$V(a) = \{bab' : b, b' \in W(a)\}.$$

An element $a \in S$ is *regular* if it has at least one (weak) generalised inverse. The semigroup S itself is called *regular* if all its elements are regular. Many of the well-known types of semigroups are regular, such as idempotent semigroups (or *bands*), full transformation semigroups, and Rees matrix semigroups. Among various advantages, regular semigroups have a particularly manageable structure which may be studied using the so-called Green's relations. For further basic results on regular semigroups see [6, Section 1.9].

Another generalisation of reversible CA has appeared in the literature before [12, 13] using the concept of *Drazin inverse* [8]. However, as Drazin inverible elements in a semigroup are a special kind of regular elements, our approach turns out to be more general and natural.

In the following sections we study the regular elements of various monoids of CA. First of all, in Section 2 we present some preliminary results and establish that, except for the trivial cases $|G| = 1$ and $|A| \leq 1$, the monoid $\mathrm{CA}(G; A)$ is not regular. In Section 3, we study the regular elements of $\mathrm{CA}(G; A)$ when G and A are both finite; in particular, we characterise all of them and describe a maximal regular submonoid (i.e. a regular submonoid that is not properly contained in any other regular submonoid). In Section 4, we study the regular elements of the monoid $\mathrm{LCA}(G; \mathbb{F})$ of linear CA, with G an abelian group and $\mathbb{F}$ a field. Specifically, when G is a torsion-free abelian group (such as $\mathbb{Z}^d$, $d \in \mathbb{N}$), we characterise all regular elements of $\mathrm{LCA}(G; \mathbb{F})$; when G is finite abelian, we prove that $\mathrm{LCA}(G; \mathbb{F})$ is regular if and only if the characteristic of $\mathbb{F}$ does not divide the order of G; and, finally, when $G \cong \mathbb{Z}_n$ is a cyclic group, $\mathbb{F}$ is a finite field, and $\mathrm{char}(\mathbb{F}) \mid n$, we count the total number of regular elements in $\mathrm{LCA}(\mathbb{Z}_n; \mathbb{F})$.

2 Regular cellular automata

For any set X, let $\mathrm{Tran}(X)$ and $\mathrm{Sym}(X)$ be the sets of all functions and bijective functions of the form $\tau : X \to X$, respectively. 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 a finite set of size α, we write Tran_α and Sym_α instead of $\mathrm{Tran}(X)$ and $\mathrm{Sym}(X)$, respectively.

We shall review the broad definition of CA that appears in [5, 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 $g \in G$, denote by $R_g : G \to G$ the right multiplication function, i.e. $(h)R_g := hg$ for any $h \in G$. We shall emphasise that we apply functions on the right, while [5] applies functions on the left.

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

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

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

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 $x \in A^G$, $g \in G$,

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

Any cellular automaton is a G-equivariant transformation, but the converse is not true in general. A generalisation of Curtis-Hedlund Theorem (see [5, Theorem 1.8.1]) establishes that, when A is finite, a function $\tau : A^G \to A^G$ is a CA if and only if τ is G-equivariant and continuous in the prodiscrete topology of A^G; in particular, when G and A are both finite, G-equivariance completely characterises CA over G and 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 denote x by $\mathbf{k} \in A^G$. It follows by G-equivariance that any $\tau \in \mathrm{CA}(G; A)$ maps constant configurations to constant configurations.

The following theorem applies to CA over an arbitrary group and an arbitrary set, and it shows that, except for the trivial cases, $\mathrm{CA}(G; A)$ always contains non-regular elements.
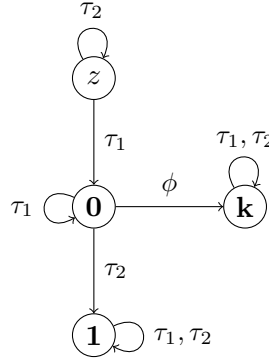

Figure 1: Images of τ_1, τ_2 and ϕ.

Theorem 1. *Let G be a group and A a set. The semigroup $\mathrm{CA}(G; A)$ is regular if and only if $|G| = 1$ or $|A| \leq 1$.*

Proof. If $|G| = 1$ or $|A| \leq 1$, then $\mathrm{CA}(G; A) = \mathrm{Tran}(A)$ or $\mathrm{CA}(G; A)$ is the trivial semigroup with one element, respectively. In both cases, $\mathrm{CA}(G; A)$ is regular (see [6, Exercise 1.9.1]).

Assume that $|G| \geq 2$ and $|A| \geq 2$. Suppose that $\{0, 1\} \subseteq A$. Let $S := \{e, g, g^{-1}\} \subseteq G$, where e is the identity of G and $e \neq g \in G$ (we do not require $g \neq g^{-1}$). For $i = 1, 2$, let $\tau_i \in \mathrm{CA}(G; A)$ be the cellular automaton defined by the local function $\mu_i : A^S \to A$, where, for any $x \in A^S$,

$$(x)\mu_1 := \begin{cases} (e)x & \text{if } (e)x = (g)x = (g^{-1})x, \\ 0 & \text{otherwise}; \end{cases}$$

$$(x)\mu_2 := \begin{cases} 1 & \text{if } (e)x = (g)x = (g^{-1})x = 0, \\ (e)x & \text{otherwise}; \end{cases}$$

We shall show that $\tau := \tau_2 \tau_1 \in \mathrm{CA}(G; A)$ is not a regular element. Suppose there exists $\phi \in \mathrm{CA}(G; A)$ such that $\tau = \tau \phi \tau$. Consider the constant configurations $\mathbf{0}, \mathbf{1} \in A^G$ defined by $(h)\mathbf{0} = 0$ and $(h)\mathbf{1} = 1$, for all $h \in G$. Clearly,

$$(\mathbf{0})\tau = (\mathbf{0})\tau_2 \tau_1 = (\mathbf{1})\tau_1 = \mathbf{1}.$$

Let $z \in A^G$ be defined by

$$(h)z := \begin{cases} m \mod (2) & \text{if } h = g^m, m \in \mathbb{N} \text{ minimal}, \\ 0 & \text{otherwise}. \end{cases}$$

Observe that

$$(z)\tau = (z)\tau_2\tau_1 = (z)\tau_1 = \mathbf{0}.$$

By evaluating $\tau = \tau\phi\tau$ on both sides at z we obtain $\mathbf{0} = (\mathbf{0})\phi\tau$. Note that $(\mathbf{0})\phi = \mathbf{k}$ for some constant configuration $\mathbf{k} \in A^G$ (as any CA maps constant configurations to constant configurations). Figure 1 illustrates some of the images of the set $\{z, \mathbf{0}, \mathbf{1}, \mathbf{k}\}$ under τ_1, τ_2 and ϕ. However,

$$(\mathbf{k})\tau = \begin{cases} \mathbf{1} & \text{if } \mathbf{k} = \mathbf{0}, \\ \mathbf{k} & \text{otherwise}. \end{cases}$$

Therefore, $(z)\tau = \mathbf{0} \neq (\mathbf{k})\tau = (z)\tau\phi\tau$, which is a contradiction. $\qquad\square$

Now that we know that $\mathrm{CA}(G; A)$ always contains both regular and non-regular elements (when $|G| \geq 2$ and $|A| \geq 2$), an interesting problem is to find a criterion that describes all regular CA. In the following sections, we solve this problem by adding some extra assumptions, such as finiteness and linearity.

3 Regular finite cellular autotama

In this section we characterise the regular elements in the monoid $\mathrm{CA}(G; A)$ when G and A are both finite (Theorem 3). In order to achieve this, we summarise some of the notation and results obtained in [2, 3, 4].

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

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

For any $x \in A^G$, denote by G_x the *stabiliser* of x in G:

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

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.

Let $\mathrm{ICA}(G; A)$ be the group of all invertible cellular automata over G and A:

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

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 $H \leq G$. For any pair of conjugacy classes $[H_1]$ and $[H_2]$ write $[H_1] \leq [H_2]$ if $H_1 \leq g^{-1}H_2g$, for some $g \in G$. When G is finite, this is a well-defined partial order on the set of conjugacy classes of subgroups of G.

Theorem 2 corresponds to Lemmas 3, 9 and 6 in [4].

Theorem 2. *Let G be a finite group of size $n \geq 2$ and A a finite set of size $q \geq 2$. Let $x, y \in A^G$.*

(i) *Let $\tau \in \mathrm{CA}(G; A)$. If $(x)\tau \in (xG)$, then $\tau|_{xG} \in \mathrm{Sym}(xG)$.*

(ii) *There exists $\tau \in \mathrm{ICA}(G; A)$ such that $(xG)\tau = yG$ if and only if $[G_x] = [G_y]$.*

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

Theorem 3. *Let G be a finite group and A a finite set of size $q \geq 2$. Let $\tau \in \mathrm{CA}(G; A)$. Then, τ is regular if and only if for every $y \in (A^G)\tau$ there is $x \in (y)\tau^{-1}$ such that $[G_x] = [G_y]$.*

Proof. Suppose there exists $y \in (A^G)\tau$ such that for all $x \in (y)\tau^{-1}$ we have $[G_x] < [G_y]$. Suppose that τ is regular, so there exists $\phi \in \mathrm{CA}(G; A)$ such that $\tau = \tau\phi\tau$. Fix $x \in (y)\tau^{-1}$. Then,
$$(x)\tau = (x)\tau\phi\tau \implies y = (y)\phi\tau.$$
This means that $(y)\phi \in (y)\tau^{-1}$, so $[G_{(y)\phi}] < [G_y]$ by hypothesis. However, by Theorem 2,
$$[G_y] \leq [G_{(y)\phi}] < [G_y],$$
which is a contradiction. Therefore, τ is not regular.

Conversely, suppose that for every $y \in (A^G)\tau$ there is $x \in (y)\tau^{-1}$ such that $[G_x] = [G_y]$. Choose pairwise distinct G-orbits $y_1 G, \ldots, y_\ell G$ such that
$$(A^G)\tau = \bigcup_{i=1}^{\ell} y_i G.$$
For each i, fix $y_i' \in A^G$ such that $y_i' \in (y_i)\tau^{-1}$ and $[G_{y_i}] = [G_{y_i'}]$. We define $\phi : A^G \to A^G$ as follows: for any $z \in A^G$,
$$(z)\phi := \begin{cases} z & \text{if } z \notin (A^G)\tau, \\ y_i' \cdot g & \text{if } z = y_i \cdot g \in y_i G. \end{cases}$$
Clearly, ϕ is G-equivariant, so $\phi \in \mathrm{CA}(G; A)$. Now, for any $x \in A^G$ with $(x)\tau = y_i \cdot g$,
$$(x)\tau\phi\tau = (y_i \cdot g)\phi\tau = (y_i' \cdot g)\tau = (y_i')\tau \cdot g = y_i \cdot g = (x)\tau.$$
This proves that $\tau\phi\tau = \tau$, so τ is regular. $\qquad\square$

Our goal now is to find a maximal regular submonoid of $\mathrm{CA}(G; A)$ (Theorem 4). In order to achieve this, we need some further terminology and basic results.

Let H be a subgroup of G and $[H]$ its conjugacy class. Define the *box* in A^G corresponding to $[H]$ by
$$B_{[H]}(G; A) := \{x \in A^G : [G_x] = [H]\}.$$
As any subgroup of G is the stabiliser of some configuration in A^G, the set $\{B_{[H]}(G; A) : H \leq G\}$ is a partition of A^G. Note that $B_{[H]}(G; A)$ is a subshift of A^G (i.e. a union of G-orbits) and, by the Orbit-Sabiliser Theorem, all the G-orbits contained in $B_{[H]}(G; A)$ have equal sizes. Define
$$\alpha_{[H]}(G; A) := \left|\left\{xG : x \in A^G, \ xG \subseteq B_{[H]}(G; A)\right\}\right|;$$
in other words, $\alpha_{[H]}(G; A)$ is the number of distinct G-orbits contained in the box $B_{[H]}(G; A)$. 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.

Example 1. For any finite group G and finite set A of size q, we have
$$B_{[G]} = \{\mathbf{k} \in A^G : \mathbf{k} \text{ is constant}\} \text{ and } \alpha_{[G]}(G; A) = q.$$

In general, for a subgroup $H \leq G$, the integer $\alpha_{[H]}$ may be calculated using the techniques described in [4, Section 4].

For any subshift $C \subseteq A^G$, define
$$\mathrm{CA}(C) := \{\tau \in \mathrm{Tran}(C) : \tau \text{ is } G\text{-equivariant}\}.$$
In particular, $\mathrm{CA}(A^G) = \mathrm{CA}(G; A)$. Clearly,
$$\mathrm{CA}(C) = \{\tau|_C : \tau \in \mathrm{CA}(G; A), \tau(C) \subseteq C\}.$$

Lemma 1. *Let $H \leq G$. Then,*

$$\mathrm{CA}(B_{[H]}) \cong \mathrm{CA}(xG) \wr \mathrm{Tran}_{\alpha_{[H]}}$$

where $x \in B_{[H]}$, and $\wr$ denotes the wreath product *of transformation semigroups (see [1, Section 2]).*

Proof. First note that $\mathrm{CA}(xG) \cong \mathrm{CA}(yG)$, for any $x, y \in B_{[H]}$, as the cellular automaton $\tau \in \mathrm{ICA}(G; A)$ guaranteed by Theorem 2 (ii) induces an isomorphism by conjugation. Since $\{xG : x \in B_{[H]}\}$ is a uniform partition of $B_{[H]}$, the result follows by [1, Lemma 2.1(iv)]. $\square$

Theorem 4. *Let G be a finite group and A a finite set of size $q \geq 2$. Let*

$$R := \left\{ \sigma \in \mathrm{CA}(G; A) : [G_x] = [G_{(x)\sigma}] \text{ for all } x \in A^G \right\} \cong \prod_{H \leq G} \mathrm{CA}(B_{[H]}).$$

(i) $\mathrm{ICA}(G; A) \leq R$.

(ii) *R is a regular monoid.*

(iii) *R is a maximal regular submonoid of $\mathrm{CA}(G; A)$ if and only if $q \geq 3$ or G has no subgroup of index 2.*

Proof. Part **(i)** follows by Theorem 2. As the CA ϕ constructed in the proof of Theorem 3 is in R, part **(ii)** follows.

By [4, Lemma 4], we know that $\alpha_{[H]}(G; A) = 1$ if and only if $[G : H] = q = 2$, where $[G : H]$ denotes the index of H in G. Hence, part **(iii)** is equivalent to the following statement: R is a maximal regular subsemigroup of $\mathrm{CA}(G; A)$ if and only if $\alpha_{[H]}(G; A) \geq 2$ for all $H \leq G$.

Suppose first that $\alpha_{[H]}(G; A) \geq 2$ for all $H \leq G$, and that there is a regular submonoid $M \leq \mathrm{CA}(G; A)$ such that $R \subsetneq M$. Let $\tau \in M \setminus R$. By definition of R, there must be $x \in A^G$ such that $[G_x] < [G_{(x)\tau}]$. Let $y := (x)\tau$. If $(B_{[G_y]})\tau = B_{[G_y]}$, we may compose τ with a non-invertible transformation in R to obtain a non-invertible transformation of $B_{[G_y]}$ (provided that $\alpha_{[G_y]}(G; A) \geq 2$, as otherwise, all transformations of $B_{[G_y]}$ are invertible by Theorem 2 (i)). Hence, we may assume there exists $y' \in B_{[G_y]} \setminus (B_{[G_y]})\tau$. As $yG \neq y'G$, we may conjugate τ by an element of $\mathrm{ICA}(G; A)$ that swaps y and y', so we may assume that $y \in B_{[G_y]} \setminus (B_{[G_y]})\tau$. As M is regular, there is $\sigma \in M$ such that $\tau = \tau\sigma\tau$. Now, $(x)\tau = y = (x)\tau\sigma\tau = (y)\sigma\tau$. Since $y \in B_{[G_y]} \setminus (B_{[G_y]})\tau$, we have $(y)\sigma \notin B_{[G_y]}$. Thus, by Theorem 2, we must have $[G_x] < [G_y] < [G_{(y)\sigma}]$, which makes impossible that $(y)\sigma\tau \in B_{[G_y]}$.

Conversely, suppose that there exists $H \leq G$ such that $\alpha_{[H]}(G; A) = 1$. Clearly, H is non-trivial because $\alpha_{[\{e\}]}(G; A) = q \geq 2$, where e is the identity of G. Hence, there exists an idempotent $\epsilon \in \mathrm{CA}(G; A)$ collapsing an orbit $xG \subseteq B_{[\{e\}]}$ to the orbit $yG = B_{[H]}$. We may assume that

$$(z)\epsilon = \begin{cases} y \cdot g & \text{if } z = x \cdot g; \\ z & \text{otherwise.} \end{cases}$$

We claim that $M := \langle R \cup \{\epsilon\} \rangle$ is a regular submonoid that strictly contains R. Observe that any $\tau \in M$ satisfies $(yG)\tau = yG$ because yG is the unique orbit in $B_{[H]}$. Hence, every element in the image of $\tau \in M$ has a preimage in the same box. Indeed, by the construction of M, the only configurations of $(A^G)\tau$ that might not have a preimage in the same box are the elements of yG: however, they all do because $(yG)\tau = yG$. Thus, the CA $\phi \in R \subseteq M$ defined in the proof of Theorem 3 satisfies $\tau\phi\tau = \tau$. $\square$

4 Regular linear cellular automata

Let V a vector space over a field $\mathbb{F}$. Clearly, for any group G, the configuration space V^G is also a vector space over $\mathbb{F}$ equipped with the pointwise addition and scalar multiplication. Denote by $\mathrm{End}_{\mathbb{F}}(V^G)$ the set of all $\mathbb{F}$-linear transformations of the form $\tau : V^G \to V^G$. For any group G define

$$\mathrm{LCA}(G;V) := \mathrm{CA}(G;V) \cap \mathrm{End}_{\mathbb{F}}(V^G).$$

Note that $\mathrm{LCA}(G;V)$ is not only a monoid, but also an $\mathbb{F}$-algebra (i.e. a vector space over $\mathbb{F}$ equipped with a bilinear binary product), because, again, we may equip $\mathrm{LCA}(G;V)$ with the pointwise addition and scalar multiplication. In particular, $\mathrm{LCA}(G;V)$ is also a ring.

In this chapter, we study the regular elements of $\mathrm{LCA}(G;V)$, when G is an abelian group. As in the case of semigroups, von Neumann regular rings have been widely studied (e.g., see [9]).

For any ring R and any group G, define the *support* of a function $f : G \to R$ as the set $\mathrm{Supp}(f) := \{g \in G : (g)f \neq 0_R\}$. The *group ring* $R[G]$ is the set of all functions $f : G \to R$ with finite support. If we let $R := \mathrm{End}_{\mathbb{F}}(V)$, then $\mathrm{End}_{\mathbb{F}}(V)[G]$ is an $\mathbb{F}$-algebra isomorphic to $\mathrm{LCA}(G;V)$ (see [5, Theorem 8.5.2]).

Equivalently, the group ring $R[G]$ may be defined as the set of all formal finite sums $\sum_{g \in G} a_g g$ with $a_g \in R$ (see [11, Section 3.2]). The multiplication in $R[G]$ is defined naturally using the multiplications of G and R:

$$\sum_{g \in G} a_g g \sum_{h \in G} a_h h = \sum_{g,h \in G} a_g a_h gh.$$

Henceforth, we focus on the regular elements of $\mathrm{LCA}(G;V)$ when V is a one-dimensional vector space (i.e. V is just the field $\mathbb{F}$). In this case, $\mathrm{End}_{\mathbb{F}}(\mathbb{F}) \cong \mathbb{F}$, so $\mathrm{LCA}(G;\mathbb{F})$ and $\mathbb{F}[G]$ are ring-isomorphic.

An abelian group G is called *torsion-free* if the identity is the only element of finite order (i.e. if $g^n = e$, for some $n \in \mathbb{N}$, then $g = e$). For instance, the groups $\mathbb{Z}^d$, for $d \in \mathbb{N}$, are torsion-free abelian groups.

In order to characterise regular linear cellular automata over torsion-free abelian groups, we need the following result, which is a special case of [7, Theorem 2].

Theorem 5. *Let G be an torsion-free abelian group. For $1 \leq r, s \leq |G|$, define*

$$\mu_G(r,s) := \min \{|AB| : A, B \subseteq G, |A| = r, |B| = s\}.$$

Then,

$$\mu_G(r,s) = r + s - 1.$$

The *minimal memory set* of a CA τ is the memory set of τ with minimal cardinality. This always exists and is unique for any CA.

Theorem 6. *Let G be a torsion-free abelian group and let $\mathbb{F}$ be any field. A non-zero element $\tau \in \mathrm{LCA}(G;\mathbb{F})$ is regular if and only if its minimal memory set is a singleton.*

Proof. The minimal memory set $T \subset G$ of $\tau \in \mathrm{LCA}(G;\mathbb{F})$ is the support of τ seen as an element of $\mathbb{F}[G]$ (see [5, Proposition 8.5.1. (iii)]). Suppose that τ is non-zero regular and let $\sigma \in \mathrm{LCA}(G;\mathbb{F})$ be such that $\tau\sigma\tau = \tau$. Observe that the support of a product of elements of $\mathbb{F}[G]$ is equal to the product of the supports (this is not true if we replace $\mathbb{F}$ for a ring with zero divisors). Hence, $T = TST$, where $S \subset G$ is the support of σ. By Theorem 5,

$$|TST| \geq |TS| + |T| - 1 \geq |S| + 2|T| - 2 \geq 2|T| - 1.$$

Since $|T| \geq 2|T| - 1$ if and only if $1 \geq |T|$, and $T \neq \emptyset$ because τ is non-zero, it follows that T is a singleton.

Conversely, suppose that $\tau \in \mathrm{LCA}(G; \mathbb{F})$ has memory set $\{t\} \subseteq G$. Then, seen as an element of $\mathbb{F}[G]$, τ must have the form αt, for $\alpha \in \mathbb{F}$, $\alpha \neq 0$. Then, $\sigma = \alpha^{-1} t^{-1} \in \mathbb{F}[G]$ satisfies

$$\tau \sigma \tau = (\alpha t)(\alpha^{-1} t^{-1})(\alpha t) = \tau.$$

$\square$

Corollary 1. *Let G be a torsion-free abelian group and let $\mathbb{F}$ be any field. A non-zero element $\tau \in \mathrm{LCA}(G; \mathbb{F})$ is regular if and only if it is invertible.*

A non-zero element a of a ring R is called *nilpotent* if there exists $n > 0$ such that $a^n = 0$. The following basic result will be quite useful in the rest of this section.

Lemma 2. *Let R be a commutative ring. If $a \in R$ is nilpotent, then a is not a regular element.*

Proof. Let R be a commutative ring and $a \in R$ a nilpotent element. Let $n > 0$ be the smallest integer such that $a^n = 0$. Suppose a is a regular element, so there is $x \in R$ such that $axa = a$. By commutativity, we have $a^2 x = a$. Multiplying both sides of this equation by a^{n-2} we obtain $0 = a^n x = a^{n-1}$, which contradicts the minimality of n. $\square$

The *characteristic* of a field $\mathbb{F}$, denoted by $\mathrm{char}(\mathbb{F})$, is the smallest $k \in \mathbb{N}$ such that

$$\underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} = 0,$$

where 1 is the multiplicative identity of $\mathbb{F}$. If no such k exists we say that $\mathbb{F}$ has characteristic 0.

Theorem 7. *Let G be a finite abelian group and let $\mathbb{F}$ be any field. Then, $\mathrm{LCA}(G; \mathbb{F})$ is regular if and only if $\mathrm{char}(\mathbb{F}) \nmid |G|$.*

Proof. We shall use the fact $\mathrm{LCA}(G; \mathbb{F})$ and $\mathbb{F}[G]$ are ring-isomorphic. Suppose first that $\mathrm{char}(\mathbb{F}) \nmid |G|$. It follows by Maschke's Theorem that $\mathbb{F}[G]$ is ring-isomorphic to a direct sum of fields $\bigoplus_{i=1}^{r} \mathbb{K}_i$ (see [11, Exercise 3.4.3]). We claim this ring is regular. Indeed, for any $a = (a_1, \ldots, a_r) \in \bigoplus_{i=1}^{r} \mathbb{K}_i$, let $b = (b_1, \ldots, b_r) \in \bigoplus_{i=1}^{r} \mathbb{K}_i$ be defined as follows: for each $i = 1, \ldots r$,

$$b_i := \begin{cases} 0 & \text{if } a_i = 0 \\ (a_i)^{-1} & \text{otherwise.} \end{cases}$$

Hence, the equation $aba = a$ is satisfied.

Conversely, suppose that $\mathrm{char}(\mathbb{F}) \mid |G|$. Let $s := \sum_{g \in G} g \in \mathbb{F}[G]$. As $sg = s$, for all $g \in G$, and $\mathrm{char}(\mathbb{F}) \mid |G|$, we have $s^2 = |G|s = 0$. Clearly, $\mathbb{F}[G]$ is commutative because G is abelian, so, by Lemma 2, s is not a regular element. $\square$

Corollary 2. *For any finite abelian group G and any field $\mathbb{F}$ of characteristic 0, the ring $\mathrm{LCA}(G; \mathbb{F})$ is regular.*

We finish this section with the special case when G is the cyclic group $\mathbb{Z}_n$ and $\mathbb{F}$ is a finite field with $\mathrm{char}(\mathbb{F}) \mid n$. By Theorem 7, not all the elements of $\mathrm{LCA}(\mathbb{Z}_n; \mathbb{F})$ are regular, so how many of them are there? In order to count them we need a few technical results about commutative rings.

An *ideal* I of a commutative ring R is a subring such that $rb \in I$ for all $r \in R$, $b \in I$. For any $a \in R$, the *principal ideal* generated by a is the ideal

$$\langle a \rangle := \{ra : r \in R\}.$$

A ring is called *local* if it has a unique maximal ideal.

Denote by $\mathbb{F}[x]$ the ring of polynomials with coefficients in $\mathbb{F}$. When $G \cong \mathbb{Z}_n$, we have the following ring-isomorphisms:

$$\mathrm{LCA}(\mathbb{Z}_n; \mathbb{F}) \cong \mathbb{F}[\mathbb{Z}_n] \cong \mathbb{F}[x]/\langle x^n - 1 \rangle,$$

where $\langle x^n - 1 \rangle$ is a principal ideal in $\mathbb{F}[x]$.

Theorem 8. *Let $n \geq 2$ be an integer, and let $\mathbb{F}$ be a finite field of size q such that $\mathrm{char}(\mathbb{F}) \mid n$. Consider the following factorization of $x^n - 1$ into irreducible elements of $\mathbb{F}[x]$:*

$$x^n - 1 = p_1(x)^{m_1} p_2(x)^{m_2} \ldots p_r(x)^{m_r}.$$

For each $i = 1, \ldots r$, let $d_i := \deg(p_i(x))$. Then, the number of regular elements in $\mathrm{LCA}(\mathbb{Z}_n; \mathbb{F})$ is exactly

$$\prod_{i=1}^{r} \left((q^{d_i} - 1) q^{d_i(m_i - 1)} + 1 \right).$$

Proof. Recall that

$$\mathrm{LCA}(\mathbb{Z}_n; \mathbb{F}) \cong \mathbb{F}[x]/\langle x^n - 1 \rangle.$$

By the Chinese Remainder Theorem,

$$\mathbb{F}[x]/\langle x^n - 1 \rangle \cong \mathbb{F}[x]/\langle p_1(x)^{m_1} \rangle \times \mathbb{F}[x]/\langle p_2(x)^{m_2} \rangle \times \cdots \times \mathbb{F}[x]/\langle p_r(x)^{m_r} \rangle.$$

An element $a = (a_1, \ldots, a_r)$ in the right-hand side of the above isomorphism is a regular element if and only if a_i is a regular element in $\mathbb{F}[x]/\langle p_i(x)^{m_i} \rangle$ for all $i = 1, \ldots, r$.

Fix $m := m_i$, $p(x) = p_i(x)$, and $d := d_i$. Consider the principal ideals $A := \langle p(x) \rangle$ and $B := \langle p(x)^m \rangle$ in $\mathbb{F}[x]$. Then, $\mathbb{F}[x]/B$ is a local ring with unique maximal ideal A/B, and each of its nonzero elements is either nilpotent or a unit (i.e. invertible): in particular, the set of units of $\mathbb{F}[x]/B$ is precisely $(\mathbb{F}[x]/B) - (A/B)$. By the Third Isomorphism Theorem, $(\mathbb{F}[x]/B)/(A/B) \cong (\mathbb{F}[x]/A)$, so

$$|A/B| = \frac{|\mathbb{F}[x]/B|}{|\mathbb{F}[x]/A|} = \frac{q^{dm}}{q^d} = q^{d(m-1)}.$$

Thus, the number of units in $\mathbb{F}[x]/B$ is

$$|(\mathbb{F}[x]/B) - (A/B)| = q^{dm} - q^{d(m-1)} = (q^d - 1) q^{d(m-1)}.$$

As nilpotent elements are not regular by Lemma 2, every regular element of $\mathbb{F}[x]/\langle p_i(x)^{m_i} \rangle$ is zero or a unit. Thus, the number of regular elements in $\mathbb{F}[x]/\langle p_i(x)^{m_i} \rangle$ is $(q^{d_i} - 1) q^{d_i(m_i - 1)} + 1$. $\square$

References

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

[2] Castillo-Ramirez, A., Gadouleau, M.: Ranks of finite semigroups of one-dimensional cellular automata. Semigroup Forum **93**, 347–362 (2016).

[3] 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**, pp. 90–104, Springer International Publishing Switzerland (2016).

[4] Castillo-Ramirez, A., Gadouleau, M.: Cellular Automata and Finite Groups. Preprint: arXiv:1610.00532 (2016).

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

[6] Clifford, A.H., Preston, G. B.: The Algebraic Theory of Semigroups, Volume 1. Mathematical Surveys of the American Mathematical Society **7**, Providence, R.I. (1961).

[7] Eliahou, S., Kervaire, M.: Minimal sumsets in infinite abelian groups. J. Algebra **287**, 449–457 (2005).

[8] Drazin, M.P.: Pseudo-Inverses in Associative Rings and Semigroups. Amer. Math. Mon. **65**, 506–514 (1958).

[9] Goodearl, K. R.: Von Neumann Regular Rings. Monographs and Studies in Mathematics **4**. Pitman Publishing Ltd. (1979).

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

[11] Milies, C.P., Sehgal, S.K.: An Introduction to Group Rings. Kluwer Academic Publishers (2002).

[12] Zhang, K., Zhang, L.: Generalized Reversibility of Cellular Automata with Boundaries. Proceedings of the 10th World Congress on Intelligent Control and Automation, Beijing, China (2012).

[13] Zhang, K., Zhang, L.: Generalized Reversibility of Topological Dynamical Systems and Cellular Automata. J. Cellular Automata **10**, 425–434 (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