Von Neumann Regular Cellular Automata

Alonso Castillo-Ramirez, Maximilien Gadouleau

Von Neumann Regular Cellular Automata

Alonso Castillo-Ramirez[1] and Maximilien Gadouleau[2]

[1] Departamento de Matemáticas, Centro Universitario de Ciencias Exactas e Ingenierías, Universidad de Guadalajara, Guadalajara, México.
[2] School of Engineering and Computing Sciences, Durham University, South Road, Durham, DH1 3LE, UK

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* (or simply *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 regular if all its elements are regular. We establish that $\mathrm{CA}(G;A)$ is regular if and only if $|G| = 1$ or $|A| = 1$, and we characterise all regular elements in $\mathrm{CA}(G;A)$ when G and A are both finite. Furthermore, we study regular linear CA when $A = V$ is a vector space over a field $\mathbb{F}$; in particular, we show that every regular linear CA is invertible when G is torsion-free (e.g. when $G = \mathbb{Z}^d, d \geq 1$), and that every linear CA is regular when V is finite-dimensional and G is locally finite with $\mathrm{char}(\mathbb{F}) \nmid o(g)$ for all $g \in G$.

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 [12]), 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 this paper we apply functions on the right; hence, for $\tau, \sigma \in \mathrm{CA}(G;A)$, the composition $\tau\circ\sigma$, denoted simply by $\tau\sigma$, means applying first τ and then σ.

In general, $\tau \in \mathrm{CA}(G;A)$ is *invertible*, or *reversible*, or *a unit*, if there exists $\sigma \in \mathrm{CA}(G;A)$ such that $\tau\sigma = \sigma\tau = \mathrm{id}$. 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.

Henceforth, we 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 generalised inverse (which is equivalent of having at least one weak generalised inverse). A 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 [14, 15] using the concept of *Drazin inverse* [8]. However, as Drazin invertible elements 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 in monoids of CA. First, in Section 2 we present some basic results and examples, and we establish that, except for the trivial cases $|G| = 1$ and $|A| = 1$, 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 them and describe a regular submonoid. In Section 4, we study the regular elements of the monoid $\mathrm{LCA}(G;V)$ of linear CA, when V is a vector space over a field $\mathbb{F}$. Specifically, using results on group rings, we show that, when G is torsion-free (e.g., $G = \mathbb{Z}^d$), $\tau \in \mathrm{LCA}(G;V)$ is regular if and only if it is invertible, and that, for finite-dimensional V, $\mathrm{LCA}(G;V)$ itself is regular if and only if G is locally finite and

$\mathrm{char}(\mathbb{F}) \nmid |\langle g \rangle|$, for all $g \in G$. Finally, for the particular case when $G \cong \mathbb{Z}_n$ is a cyclic group, $V := \mathbb{F}$ 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 $\mathrm{Tran}(X)$, $\mathrm{Sym}(X)$, and $\mathrm{Sing}(X)$, be the sets of all functions, all bijective functions, and all non-bijective (or singular) 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, $\mathrm{Sym}(X)$ is the *symmetric group* on X, and $\mathrm{Sing}(X)$ is the *singular transformation semigroup* on X. When X is a finite set of size α, we simply write Tran_α, Sym_α, and Sing_α, in each case.

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 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 G-equivariant, 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, $\tau : A^G \to A^G$ 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 $(g)x = k$, for a fixed $k \in A$, for all $g \in G$. In such case, we denote x by $\mathbf{k} \in A^G$.

Remark 1. It follows by G-equivariance that any $\tau \in \mathrm{CA}(G; A)$ maps constant configurations to constant configurations.

Recall from Section 1 that $\tau \in \mathrm{CA}(G; A)$ is *invertible* if there exists $\sigma \in \mathrm{CA}(G; A)$ such that $\tau\sigma = \sigma\tau = \mathrm{id}$, and that $\tau \in \mathrm{CA}(G; A)$ is *regular* if there exists $\sigma \in \mathrm{CA}(G; A)$ such that $\tau\sigma\tau = \tau$. We now present some examples of CA that are regular but not invertible.

Example 1. Let G be any nontrivial group and A any set with at least two elements. Let $\sigma \in \mathrm{CA}(G; A)$ be a CA with memory set $\{s\} \subseteq G$ and local function $\mu : A \to A$ that is non-bijective. Clearly, σ is not invertible. As $\mathrm{Sing}(A)$ is a regular semigroup (see [11, Theorem II]), there exists $\mu' : A \to A$ such that $\mu\mu'\mu = \mu$. If σ' is the CA with memory set $\{s^{-1}\}$ and local function μ', then $\sigma\sigma'\sigma = \sigma$. Hence σ is regular.

Example 2. Suppose that $A = \{0, 1, \ldots, q-1\}$, with $q \geq 2$. Consider $\tau_1, \tau_2 \in \mathrm{CA}(\mathbb{Z}; A)$ with memory set $S := \{-1, 0, 1\}$ and local functions

$$(x)\mu_1 = \min\{(-1)x, (0)x, (1)x\} \text{ and } (x)\mu_2 = \max\{(-1)x, (0)x, (1)x\},$$

respectively, for all $x \in A^S$. Clearly, τ_1 and τ_2 are not invertible, but we show that they are generalised inverses of each other, i.e. $\tau_1\tau_2\tau_1 = \tau_1$ and $\tau_2\tau_1\tau_2 = \tau_2$, so they are both regular. We prove only the first of the previous identities, as the second one is symmetrical. Let $x \in A^{\mathbb{Z}}$, $y := (x)\tau_1$, $z := (y)\tau_2$, and $a := (z)\tau_1$. We want to show that $y = a$. For all $i \in \mathbb{Z}$ and $\epsilon \in \{-1, 0, 1\}$, we have

$$(i+\epsilon)y = \min\{(i+\epsilon-1)x, (i+\epsilon)x, (i+\epsilon+1)x\} \leq (i)x.$$

Hence,

$$(i)z = \max\{(i-1)y, (i)y, (i+1)y\} \leq (i)x.$$

Similarly $(i-1)z \leq (i-1)x$ and $(i+1)z \leq (i+1)x$, so

$$(i)a = \min\{(i-1)z, (i)z, (i+1)z\} \leq (i)y = \min\{(i-1)x, (i)x, (i+1)x\}.$$

Conversely, we have $(i-1)z, (i)z, (i+1)z \geq (i)y$, so $(i)a \geq (i)y$. In particular, when $q = 2$, τ_1 and τ_2 are the elementary CA known as Rules 128 and 254, respectively.

The following lemma gives an equivalent definition of regular CA. Note that this result still holds if we replace $\mathrm{CA}(G; A)$ with any monoid of transformations.

Lemma 1. *Let G be a group and A a set. Then, $\tau \in \mathrm{CA}(G; A)$ is regular if and only if there exists $\sigma \in \mathrm{CA}(G; A)$ such that for every $y \in (A^G)\tau$ there is $\hat{y} \in A^G$ with $(\hat{y})\tau = y$ and $(y)\sigma = \hat{y}$.*

Proof. If $\tau \in \mathrm{CA}(G; A)$ is regular, there exists $\sigma \in \mathrm{CA}(G; A)$ such that $\tau\sigma\tau = \tau$. Let $x \in A^G$ be such that $(x)\tau = y$ (which exists because $y \in (A^G)\tau$) and define $\hat{y} := (y)\sigma$. Now,

$$(\hat{y})\tau = (y)\sigma\tau = (x)\tau\sigma\tau = (x)\tau = y.$$

Conversely, assume there exists $\sigma \in \mathrm{CA}(G; A)$ satisfying the statement of the lemma. Then, for any $x \in A^G$ with $y := (x)\tau$ we have

$$(x)\tau\sigma\tau = (y)\sigma\tau = (\hat{y})\tau = y = (x)\tau.$$

Therefore, τ is regular. □

Corollary 1. *Let G be a nontrivial group and A a set with at least two elements. Let $\tau \in \mathrm{CA}(G;A)$, and suppose there is a constant configuration $\mathbf{k} \in (A^G)\tau$ such that there is no constant configuration of A^G mapped to $\mathbf{k}$ under τ. Then τ is not regular.*

Proof. The result follows by Remark 1 and Lemma 1. □

In the following examples we see how Corollary 1 may be used to show that some well-known CA are not regular.

Example 3. Let $\phi \in \mathrm{CA}(\mathbb{Z};\{0,1\})$ be the Rule 110 elementary CA, and consider the constant configuration $\mathbf{1}$. Define $x := \ldots 10101010\cdots \in \{0,1\}^{\mathbb{Z}}$, and note that $(x)\phi = \mathbf{1}$. Since $(\mathbf{1})\phi = \mathbf{0}$ and $(\mathbf{0})\phi = \mathbf{0}$, Corollary 1 implies that ϕ is not regular.

Example 4. Let $\tau \in \mathrm{CA}(\mathbb{Z}^2;\{0,1\})$ be Conway's Game of Life, and consider the constant configuration $\mathbf{1}$ (all cells alive). By [5, Exercise 1.7.], $\mathbf{1}$ is in the image of τ; since $(\mathbf{1})\tau = \mathbf{0}$ (all cells die from overpopulation) and $(\mathbf{0})\tau = \mathbf{0}$, Corollary 1 implies that τ is not regular.

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

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 $|A| = 1$.*

Proof. If $|G| = 1$ or $|A| = 1$, 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 regular.

Consider the constant configurations $\mathbf{0}, \mathbf{1} \in A^G$. Let $z \in A^G$ be defined by

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

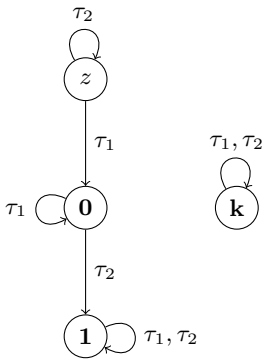

Fig. 1. Images of τ_1 and τ_2.

Figure 1 illustrates the images z, $\mathbf{0}$, $\mathbf{1}$, and $\mathbf{k} \neq \mathbf{0}, \mathbf{1}$ (in case it exists) under τ_1 and τ_2. Clearly,

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

In fact,

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

Furthermore,

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

Hence, $\mathbf{0}$ is a constant configuration in the image of τ but with no preimage among the constant configurations. By Corollary 1, τ is not regular. □

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 automata

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 [2–4].

Definition 2. *The following definitions apply for an arbitrary group G and an arbitrary set A:*

1. *For any $x \in A^G$, the* G-orbit *of x in A^G is $xG := \{x \cdot g : g \in G\}$.*
2. *For any $x \in A^G$, the* stabiliser *of x in G is $G_x := \{g \in G : x \cdot g = x\}$.*
3. *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.*

4. The group of invertible cellular automata *over G and A is*

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

In the case when G and A are both finite, every subset of A^G is closed in the prodiscrete topology, so the subshifts of A^G are simply unions of G-orbits. Moreover, as every map $\tau : A^G \to A^G$ is continuous in this case, $\mathrm{CA}(G;A)$ consists of all the G-equivariant maps of A^G. Theorem 2 is easily deduced from Lemmas 3, 9 and 10 in [4].

If M is a group, or a monoid, write $K \leq M$ if K is a subgroup, or a submonoid, of M, respectively.

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 $(x)\tau = y$ if and only if $G_x = G_y$.*
(iii) *There exists $\tau \in \mathrm{CA}(G;A)$ such that $(x)\tau = y$ 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 $x \in A^G$ such that $(x)\tau = y$ and $G_x = G_y$.*

Proof. First, suppose that τ is regular. By Lemma 1, there exists $\phi \in \mathrm{CA}(G;A)$ such that for every $y \in (A^G)\tau$ there is $\hat{y} \in A^G$ with $(\hat{y})\tau = y$ and $(y)\phi = \hat{y}$. Take $x := \hat{y}$. By Theorem 2, $G_x \leq G_y$ and $G_y \leq G_x$. Therefore, $G_x = G_y$.

Conversely, suppose that for every $y \in (A^G)\tau$ there is $x \in A^G$ such that $(x)\tau = y$ and $G_x = G_y$. Choose pairwise distinct G-orbits $y_1G, \ldots, y_\ell G$ such that

$$(A^G)\tau = \bigcup_{i=1}^{\ell} y_i G.$$

For each i, fix $y_i' \in A^G$ such that $(y_i')\tau = y_i$ and $G_{y_i} = G_{y_i'}$. We define $\phi : A^G \to A^G$ as follows: for any $z \in A^G$,

$$(z)\phi := \begin{cases} z & \text{if } z \notin (A^G)\tau, \\ y_i' \cdot g & \text{if } z = y_i \cdot g \in y_i G. \end{cases}$$

The map ϕ is well-defined because

$$y_i \cdot g = y_i \cdot h \iff hg^{-1} \in G_{y_i} = G_{y_i'} \iff y_i' \cdot g = y_i' \cdot h.$$

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. □

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

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 $H \leq G$. Define the *box* in A^G corresponding to $[H]$, where $H \leq G$, 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 (because $G_{(x\cdot g)} = g^{-1}G_xg$) and, by the Orbit-Stabiliser Theorem, all the G-orbits contained in $B_{[H]}(G;A)$ have equal sizes. When G and A are clear from the context, we write simply $B_{[H]}$ instead of $B_{[H]}(G;A)$.

Example 5. For any finite group G and finite set A of size q, we have

$$B_{[G]} = \{\mathbf{k} \in A^G : \mathbf{k} \text{ is constant}\}.$$

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,

$$\mathrm{CA}(C) = \{\tau|_C : \tau \in \mathrm{CA}(G;A), \tau(C) \subseteq C\}.$$

A submonoid $R \leq M$ is called *maximal regular* if there is no regular monoid K such that $R < K < M$.

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

$$R := \left\{\sigma \in \mathrm{CA}(G;A) : G_x = G_{(x)\sigma} \text{ for all } x \in A^G\right\}.$$

(i) $\mathrm{ICA}(G;A) \leq R$.
(ii) *R is a regular monoid.*
(iii) $R \cong \prod_{H\leq G} \mathrm{CA}(B_{[H]})$.
(iv) *R is not a maximal regular submonoid of* $\mathrm{CA}(G;A)$.

Proof. Part **(i)** and **(iii)** are trivial while part **(ii)** follows by Theorem 3.

For part **(iv)**, let $x, y \in A^G$ be such that $G_x < G_y$, so x and y are in different boxes. Define $\tau \in \mathrm{CA}(G;A)$ such that $(x)\tau = y$, $(B_{[G_y]})\tau = yG$, and τ fixes any other configuration in $A^G \setminus (B_{[G_y]} \cup \{xG\})$. It is clear by Theorem 3 that τ is regular. We will show that $K := \langle R, \tau\rangle$ is a regular submonoid of $\mathrm{CA}(G;A)$. Let $\sigma \in K$ and $z \in (A^G)\sigma$. If $\sigma \in R$, then it is obviously regular, so assume that $\sigma = \rho_1\tau\rho_2$ with $\rho_1 \in K$ and $\rho_2 \in R$. If $z \in A^G \setminus (B_{[G_y]})$, it is clear that z has a preimage in its own box; otherwise $(B_{[G_y]})\sigma = (yG)\rho_2 = zG$ and z has a preimage in $B_{[G_y]}$. Hence σ is regular and so is K. □

4 Regular linear cellular automata

Let V a vector space over a field $\mathbb{F}$. 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 $\tau : V^G \to V^G$. 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.

As in the case of semigroups, von Neumann regular rings have been widely studied and many important results have been obtained. In this chapter, we study the regular elements of $\mathrm{LCA}(G; V)$ under some natural assumptions on the group G.

First, we introduce some preliminary results and notation. The *group ring* $R[G]$ is the set of all functions $f : G \to R$ with finite support (i.e. the set $\{g \in G : (g)f \neq 0\}$ is finite). 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 $a_g \in R$. The multiplication in $R[G]$ is defined naturally using the multiplications of G and R:

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

If we let $R := \mathrm{End}_{\mathbb{F}}(V)$, it turns out that $\mathrm{End}_{\mathbb{F}}(V)[G]$ is isomorphic to $\mathrm{LCA}(G; V)$ as $\mathbb{F}$-algebras (see [5, Theorem 8.5.2]).

Define the *order* of $g \in G$ by $o(g) := |\langle g \rangle|$ (i.e. the size of the subgroup generated by g). The group G is *torsion-free* if the identity is the only element of finite order; for instance, the groups $\mathbb{Z}^d$, for $d \in \mathbb{N}$, are torsion-free groups.

In the following theorem we characterise the regular linear cellular automata over torsion-free groups.

Theorem 5. *Let G be a torsion-free group and let V be any vector space. A non-zero element $\tau \in \mathrm{LCA}(G; V)$ is regular if and only if it is invertible.*

Proof. It is clear that any invertible element is regular. Let $\tau \in \mathrm{LCA}(G; V) \cong \mathrm{End}(V)[G]$ be non-zero regular. By definition, there exists $\sigma \in \mathrm{LCA}(G; V)$ such that $\tau\sigma\tau = \tau$. As $\mathrm{LCA}(G; V)$ is a ring, the previous is equivalent to

$$\tau(\sigma\tau - 1) = 0,$$

where $1 = 1e$ and $0 = 0e$ are the identity and zero endomorphisms, respectively. Since $\tau \neq 0$, either $\sigma\tau - 1 = 0$, in which case τ is invertible, or $\sigma\tau - 1$ is a zero-divisor. In the latter case, [7, Proposition 6] implies that $\sigma\tau$ has finite order; since G is torsion-free, we must have $\sigma\tau = 1$, so τ is invertible. □

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.

A group G is *locally finite* if every finitely generated subgroup of G is finite; in particular, the order of every element of G is finite. Examples of such groups are finite groups and infinite direct sums of finite groups.

Theorem 6. *Let G be a group and let V be a finite-dimensional vector space over $\mathbb{F}$. Then, $\mathrm{LCA}(G;V)$ is regular if and only if G is locally finite and $\mathrm{char}(\mathbb{F}) \nmid o(g)$, for all $g \in G$.*

Proof. By [7, Theorem 3] (see also [1, 13]), we have that a group ring $R[G]$ is regular if and only if R is regular, G is locally finite and $o(g)$ is a unit in R for all $g \in G$. In the case of $\mathrm{LCA}(G;V) \cong \mathrm{End}(V)[G]$, since $\dim(V) := n < \infty$, the ring $R := \mathrm{End}(V) \cong M_{n\times n}(\mathbb{F})$ is regular (see [10, Theorem 1.7]. The condition that $o(g)$, seen as the matrix $o(g)I_n$, is a unit in $M_{n\times n}(\mathbb{F})$ is satisfied if and only if $o(g)$ is nonzero in $\mathbb{F}$, which is equivalent to $\mathrm{char}(\mathbb{F}) \nmid o(g)$, for all $g \in G$. □

Corollary 2. *Let G be a group and let V be a finite-dimensional vector space over a field $\mathbb{F}$ of characteristic 0. Then, $\mathrm{LCA}(G;V)$ is regular if and only if G is locally finite.*

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 isomorphic as $\mathbb{F}$-algebras.

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 $a^2x = a$. 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. □

Example 6. Suppose that G is a finite abelian group and let $\mathbb{F}$ be a field such that $\mathrm{char}(\mathbb{F}) \mid |G|$. By Theorem 6, $\mathrm{LCA}(G;\mathbb{F})$ must have elements that are not regular. For example, 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.

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 6, 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 isomorphisms as $\mathbb{F}$-algebras:

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

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

Theorem 7. *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 $\mathbb{F}[x]$:*

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

For each $i = 1, \dots r$, 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 $a = (a_1, \dots, a_r)$ 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 $i = 1, \dots, r$.

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 $(q^{d_i} - 1)q^{d_i(m_i-1)} + 1$. □

Acknowledgments. We thank the referees of this paper for their insightful suggestions and corrections. In particular, we thank the first referee for suggesting the references [1, 7, 13], which greatly improved the results of Section 4.

References

1. Auslander, M.: On regular group rings. Proc. Amer. Math. Soc. **8**, 658 – 664 (1957).
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. Connell, I.G.: On the Group Ring. Canad. J. Math. **15**, 650 – 685 (1963).
8. Drazin, M.P.: Pseudo-Inverses in Associative Rings and Semigroups. Amer. Math. Mon. **65**, 506–514 (1958).
9. Eliahou, S., Kervaire, M.: Minimal sumsets in infinite abelian groups. J. Algebra **287**, 449–457 (2005).
10. Goodearl, K. R.: Von Neumann Regular Rings. Monographs and Studies in Mathematics **4**. Pitman Publishing Ltd. (1979).
11. Howie, J. M.: The Subsemigroup Generated by the Idempotents of a Full Transformation Semigroup. J. London Math. Soc. **s1-41**, 707–716 (1966).
12. Kari, J.: Theory of cellular automata: A Survey. Theoret. Comput. Sci. **334**, 3–33 (2005).
13. McLaughlin, J.E.: A note on regular group rings. Michigan Math. J. **5**, 127–128 (1958).
14. 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).
15. Zhang, K., Zhang, L.: Generalized Reversibility of Topological Dynamical Systems and Cellular Automata. J. Cellular Automata **10**, 425–434 (2015).