Ergod. Th. & Dynam. Sys. (2012), **32**, 1991–2010 © *Cambridge University Press, 2011*
doi:10.1017/S0143385711000551

Large semigroups of cellular automata

YAIR HARTMAN

Faculty of Mathematics and Computer Science, Weizmann Institute of Science, POB 26, Rehovot, 76100, Israel
(e-mail: yair.hartman@weizmann.ac.il)

(*Received* 12 *November* 2010 *and accepted in revised form* 12 *June* 2011)

Abstract. In this article, we consider semigroups of transformations of cellular automata which act on a fixed shift space. In particular, we are interested in two properties of these semigroups which relate to 'largeness': first, a semigroup has the ID (infinite is dense) property if the only infinite invariant closed set (with respect to the semigroup action) is the entire space; the second property is maximal commutativity (MC). We shall consider two examples of semigroups: one is spanned by cellular automata transformations that represent multiplications by integers on the one-dimensional torus, and the other one consists of all the cellular automata transformations which are linear (when the symbols set is the ring $\mathbb{Z}/s\mathbb{Z}$). It will be shown that these two properties of these semigroups depend on the number of symbols s. The multiplication semigroup is ID and MC if and only if s is not a power of a prime. The linear semigroup over the mentioned ring is always MC but is ID if and only if s is prime. When the symbol set is endowed with a finite field structure (when possible), the linear semigroup is both ID and MC. In addition, we associate with each semigroup which acts on a one-sided shift space a semigroup acting on a two-sided shift space, and vice versa, in a way that preserves the ID and the MC properties.

1. *Introduction*

Consider the one-dimensional torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and the maps $m_u(x) = (ux)_{\mathrm{mod}\ 1}$ for $u \in \mathbb{Z}$. $(\mathbb{T}, m_u)$ is a dynamical system which has many invariant probability measures. The situation seems to be different if one considers the multi-parameter dynamical system $(\mathbb{T}, \Sigma)$, where $\Sigma = \{m_2^r m_3^s\}_{r,s\in\mathbb{N}}$ (the semigroup spanned by both m_2 and m_3). In 1967, Furstenberg asked the following question (Furstenberg's conjecture): is it true that the only non-atomic ergodic $\{m_2^r m_3^s\}$-invariant measure is the Lebesgue measure? This conjecture has been extensively studied, and yet it is still open in the general sense. Rudolph [**16**] proved that any measure which is $\{m_2^r m_3^s\}$-invariant is a linear combination of the Lebesgue measure and measures with zero entropy (with respect to m_2). For more developments around the conjecture, the reader is referred to [**15**] or [**14**].

The topological version of the conjecture was proved by Furstenberg in [**10**].

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

THEOREM†. (Furstenberg) *The only infinite closed subset of* $\mathbb{T}$ *which is* $\{m_2^r m_3^s\}$*-invariant is* $\mathbb{T}$.

This theorem classifies the closed $\{m_2^r m_3^s\}$-invariant subsets of $\mathbb{T}$, or the subsystems of the topological dynamical system $(\mathbb{T}, \{m_2^r, m_3^s\})$. This property of $\{m_2^r m_3^s\}$ acting on $\mathbb{T}$ leads to the following general definition: a semigroup Σ acting on a topological space Ω will be called *ID* (standing for infinite is dense) if the only infinite closed Σ-invariant subset of Ω is Ω itself. In terms of subsystems, an action of an ID semigroup is almost minimal: the only (proper) subsystems are finite.

In [**1**], Berend classified the ID semigroups of endomorphisms of $\mathbb{T}^n$. Later on, in [**2**], he gave a necessary and sufficient condition for a commutative semigroup of endomorphisms of G to be an ID semigroup, where G is a finite-dimensional connected compact abelian group.

Let Ω be a full shift space, i.e. the space of all infinite one- (or two-) sided sequences over some finite symbol set and denote by $\sigma : \Omega \to \Omega$ the left shift. Endomorphisms of the dynamical system (Ω, σ) are continuous transformations $\tau : \Omega \to \Omega$ which satisfy $\tau\sigma = \sigma\tau$. These transformations are called cellular automata transformations. In this article, the term 'transformation' will always refer to a transformation of a cellular automaton. The object studied here is a semigroup which consists of such transformations.

Note that any transformation maps each periodic sequence to a periodic sequence (the period may decrease). Therefore, a semigroup of transformations cannot have minimal action. The ID property is a natural generalization of the minimality concept for symbolic dynamics.

The commutativity property is also of interest. A semigroup is said to be maximal commutative (MC) if it is commutative and it contains all the transformations that commute with all its members.

In §3, we recall the definition of 'multiplication cellular automaton', studied by Blanchard *et al* [**3, 4**], which represents a multiplication by an integer on the one-dimensional torus. We confirm that Furstenberg's result can be applied to semigroups spanned by transformations of multiplication cellular automata when the number of symbols is not a power of a prime. Then, we show that the semigroup of all multiplication transformations is MC if and only if the number of symbols is not a power of a prime.

In §4, another semigroup, consisting of transformations which are all linear, is considered. First, we prove, using 'symbolic tools', that the semigroup which consists of all the transformations over a one-sided shift space is ID, for a symbol set of any size. When s is a power of a prime, and we endow the symbol set with a finite field structure, a generalization of this proof will show that the semigroup of linear transformations is also ID. When considering the symbol set of s symbols as the ring $\mathbb{Z}/s\mathbb{Z}$, the semigroup of linear transformations is ID if and only if s is a prime. However, for any s, when considering the symbol set as a ring or as a field, the semigroup of linear transformations is always MC. Study of transformations which are linear when the symbol set is the ring $\mathbb{Z}/s\mathbb{Z}$ can be found in [**13**]. Transformations which are linear, when the symbol set is a field (in more general settings), were considered in a series of papers of Ceccherini–Silberstein and Coornaert starting from [**6**], and recently appeared in Chapter 8 of their book [**7**].

† The original theorem is more general as it holds for non-lacunary semigroups, as will be discussed later.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

Given a transformation, the question 'which other transformations commute with it?', is known as 'the commuting block maps problem' and was introduced by Coven *et al* [**8**]. They presented a solution for some classes of block maps over the space $\{0, 1\}^{\mathbb{Z}}$. One of the classes is the class of homogeneous block maps, which are called here 'linear cellular automata transformations'. They proved that when the symbol set is $\{0, 1\}$, then the semigroup of all linear cellular automata transformations is MC. The methods used in [**8**] cannot be easily generalized since they use specific properties related to the ring $\mathbb{Z}/2\mathbb{Z}$. The results in §§3 and 4 can be viewed as the solution of the commuting problem for the classes of multiplication transformations and linear transformations.

Sections 3 and 4 treat semigroups acting on a one-sided shift space. Two-sided shift spaces, and semigroups of transformations acting on them, will be introduced in §5. Given a semigroup acting on a one-sided shift space, we construct a semigroup acting on the related two-sided shift space and vice versa. We prove that the MC and the ID properties are preserved under these constructions.

Boyle *et al* [**5**] proved that the automorphism group of a two-sided subshift of finite type is an ID semigroup, for any finite symbol set. In §6, we present a corollary of the theorems proved in §§3 and 5. This corollary yields a stronger version of the Boyle–Lind–Rudolph theorem (only for the full shift space), whenever the number of symbols is not a power of a prime.

Since both properties considered in this article are related to 'largeness', we investigate, in §7, the question how 'small' (in terms of number of generators) a semigroup having these properties can be.

2. *Preliminaries*

Define Λ_s to be a finite set of symbols such that $|\Lambda_s| = s$ for $s \geq 2$ ($s \in \mathbb{N}$). Throughout this article, we will assume that the symbol set is $\Lambda_s = \{0, 1, \ldots, s-1\}$. The one-sided (full) shift space is the topological dynamical system $(\Lambda_s^{\mathbb{N}}, \sigma)$, where σ is the left shift $\sigma(a)_k = a_{k+1}$ and $\Lambda_s^{\mathbb{N}}$ is the metric space of all one-sided sequences over Λ_s, equipped with the metric:

$$d(a, b) = \frac{1}{k+1},$$

where $a_k \neq b_k$ and $a_i = b_i$ for all $i < k$. If one treats Λ_s as a discrete topological space, this metric induces the Tychonoff topology on the product $\Lambda_s^{\mathbb{N}}$. Hence, $\Lambda_s^{\mathbb{N}}$ is a metric compact (Hausdorff) topological space.

A cellular automaton transformation is a continuous function $\tau : \Lambda_s^{\mathbb{N}} \to \Lambda_s^{\mathbb{N}}$ which satisfies $\tau\sigma = \sigma\tau$. As stated before, a 'transformation' in this article will always mean a cellular automaton transformation. Denote the set of all the transformations over $\Lambda_s^{\mathbb{N}}$ by $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$. Note that $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is closed under the composition operation and therefore $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ has the structure of a non-commutative semigroup.

These transformations were characterized in [**11**] as follows.

THEOREM. (Curtis–Hedlund–Lyndon) *Let* $\tau : \Lambda_s^{\mathbb{N}} \to \Lambda_s^{\mathbb{N}}$*; then* $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ *if and only if there exists some* $r \in \mathbb{N}$ *and a function* $f_\tau : \Lambda_s^{r+1} \to \Lambda_s$ *such that*

$$\tau(a)_k = f_\tau(a_k a_{k+1} \ldots a_{k+r})$$

for any $a \in \Lambda_s^{\mathbb{N}}$ *and* $k \in \mathbb{N}$.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

f_τ is called a block map and r is the radius of τ. It is often convenient to use the same notation for the block map f_τ and the transformation τ.

The following two properties will be discussed here.

Definition. A semigroup $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ has the *ID property* if every closed Σ-invariant proper subset of $\Lambda_s^{\mathbb{N}}$ is finite. In this case, we say that Σ is an *ID semigroup*.

Definition. A semigroup $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is *maximal commutative (MC)* if:

(1) Σ is commutative; and

(2) for each $\mu \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ such that $\mu\tau = \tau\mu$ (for all $\tau \in \Sigma$), μ necessarily belongs to Σ.

Throughout this article, we denote $a_{[i,j)} = a_i a_{i+1} \dots a_{j-1}$ and $a_{[i,j]} = a_i a_{i+1} \dots a_j$ for $a \in \Lambda_s^{\mathbb{N}}$ or $a \in \Lambda_s^{\mathbb{Z}}$.

Let $\tau_1, \tau_2, \dots, \tau_n$ be transformations. We denote by $\langle \tau_1, \tau_2, \dots, \tau_n \rangle$ the semigroup generated by $\tau_1, \tau_2, \dots, \tau_n$ under the composition operation. If $\Sigma = \{\mu_\alpha\}_{\alpha \in I}$ is a semigroup of transformations (closed under composition) and τ is a transformation, then $\langle \Sigma, \tau \rangle$ is the semigroup generated by τ and μ_α for all $\alpha \in I$.

3. *Multiplication cellular automata transformations*

Let $a \in \Lambda_s^{\mathbb{N}}$. We can think of a as an s-representation of a point in $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ using the evaluation function

$$V : \Lambda_s^{\mathbb{N}} \to \mathbb{T}, \quad V(a) = \sum_{n=0}^{\infty} \frac{a_n}{s^{n+1}}.$$

This function is injective up to the countable set $\{d/(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r})\} \subset \mathbb{T}$, where p_i are primes satisfying $p_i | s$, $e_i \in \mathbb{N}$ and $d \leq p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $(d \in \mathbb{N})$. Each point of this set has a double representation:

$$a_0 a_1 \dots a_k b000 \dots \quad \text{and} \quad a_0 a_1 \dots a_k (b-1)_{\bmod s} (s-1)(s-1)(s-1) \dots .$$

We call these an 'upper representation' and a 'lower representation', respectively.

In order to investigate the relationship between cellular automata transformations and torus functions, we need the following definitions.

Definition. Let $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ and let $f : \mathbb{T} \to \mathbb{T}$ be a torus function; τ *represents* f if the diagram

$$\begin{array}{ccc} \Lambda_s^{\mathbb{N}} & \xrightarrow{\tau} & \Lambda_s^{\mathbb{N}} \\ \downarrow V & & \downarrow V \\ \mathbb{T} & \xrightarrow{f} & \mathbb{T} \end{array}$$

is commutative.

For a prime p satisfying $p|s$, let $\mu_p \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ be the cellular automaton transformation defined by:

$$\mu_p(a)_k = \left(p \cdot a_k + \left\lfloor \frac{p \cdot a_{k+1}}{s} \right\rfloor \right)_{\bmod s}.$$

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

In addition, define the identity map $\mu_1(a)_k = a_k$, the mirror map $\mu_{-1}(a)_k = s - a_k$, and the zero map $\mu_0(a)_k = 0$. For any $u \in \mathbb{Z}$ such that $u = -1^{e_0} p_1{}^{e_1} \cdots p_d{}^{e_d}$, where $p_i | s$ for all $i = 1, \ldots, d$ ($e_0 \in \{0, 1\}$), define $\mu_u = \mu_{-1}{}^{e_0} \circ \mu_{p_1}{}^{e_1} \circ \cdots \circ \mu_{p_d}{}^{e_d}$.

When there is ambiguity regarding the space where the transformation acts, we use the notation $\mu_u^{(s)}$ to emphasize that $\mu_u^{(s)} \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$.

THEOREM 3.1. *Let $s = p_1^{e_1} \cdots p_d^{e_d}$ be the prime decomposition of s; then $\langle \mu_{p_i}, \sigma \rangle \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ (for any i) is ID if and only if s is not a power of a prime.*

THEOREM 3.2. *Let $s = p_1^{e_1} \cdots p_d^{e_d}$ be the prime decomposition of s; then $\langle \mu_{p_1}, \ldots, \mu_{p_d}, \mu_0, \mu_1 \rangle \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is maximal commutative if and only if s is not a power of a prime.*

Denote $m_u : \mathbb{T} \to \mathbb{T}$ by $m_u(x) = (u \cdot x)_{\mathrm{mod}\,1}$, and observe the following relationship.

LEMMA 3.3. *$\mu_p \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ represents m_p (multiplication by p on $\mathbb{T}$).*

Proof. For a 'finite' sequence, i.e. a sequence for which there exists some $k \in \mathbb{N}$ such that $\sigma^k(a) = 000 \ldots$, the commutativity of the diagram follows from the multiplication algorithm of numbers represented by s-expansion. Clearly, the set of all such 'finite' sequences is dense in $\Lambda_s^{\mathbb{N}}$. The proof follows from the continuity of V, m_p, and μ_p. □

This means in particular that when $s = 10$, multiplication by 2 and by 5 on the torus are representable. Note however that m_3 cannot be represented by a cellular automaton transformation in $\mathrm{CAT}(\Lambda_{10}^{\mathbb{N}})$ (see the Blanchard–Host–Maass (BHM) theorem in the following).

Proof of Theorem 3.1. Consider first the case where s is not a power of a prime, and let p be a prime factor of s. The proof simply follows from Furstenberg's theorem, stated in [**10**]. Furstenberg showed that a non-lacunary† semigroup of integers acting on $\mathbb{T}$ by multiplication has the property that the only closed infinite subset of $\mathbb{T}$ which is invariant (with respect to this semigroup action) is $\mathbb{T}$. Note that the semigroup $\{p^{k_1} s^{k_2}\}_{k_1,k_2 \in \mathbb{N}}$ is non-lacunary and therefore has this property.

Let $A \subset \Lambda_s^{\mathbb{N}}$ be a closed $\langle \mu_p, \sigma \rangle$-invariant proper subset of $\Lambda_s^{\mathbb{N}}$. We wish to show that $|A| < \infty$. $\Lambda_s^{\mathbb{N}}$ is a compact space, hence both A and $V(A)$ are compact. In particular, $V(A) \subset \mathbb{T}$ is a closed set. $\mu_p(A) \subset A$, so $V(\mu_p(A)) \subset V(A)$. From $V(\mu_p(A)) = p \cdot V(A)$, it follows that $p \cdot V(A) \subset V(A)$, hence $V(A)$ is m_p-invariant. The same holds for σ and m_s. $V(A)$ is a proper subset of $\mathbb{T}$, thus $V(A)$ is closed and a $\{p^{k_1} s^{k_2}\}$-invariant proper subset of $\mathbb{T}$, hence, by Furstenberg's theorem, it is finite. Although V is not injective, for every $x \in \mathbb{T}$, $|V^{-1}(x)| \leq 2$, therefore A is finite.

In case $s = p^m$ (p prime), $\langle \mu_p, \sigma \rangle = \langle \mu_p \rangle \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is not ID, since $\{p^{k_1}\}_{k_1 \in \mathbb{N}}$ is lacunary and we can use the same example of Furstenberg given in [**10**] as follows. Let $x = \sum_{i=1}^{\infty} p^{-i^2}$, then $\{p^{k_1} x\}_{k_1 \in \mathbb{N}}$ has only the limit points $0, p^{-1}, p^{-2}, \ldots$. The set $\{\mu_p^{k_1}(V^{-1}x)\}_{k_1 \in \mathbb{N}} \subset \mathbb{T}$ is infinite and not dense, therefore $\langle \mu_p \rangle$ is not ID.

† A multiplicative semigroup $\Gamma \subset \mathbb{Z}$ is lacunary if there exists $\gamma \in \mathbb{N}$ such that every member of $\Gamma^+ = \Gamma \cap \mathbb{N}$ is a power of γ. Otherwise, Γ is non-lacunary.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

Alternatively, we give here a symbolic construction: if $s = p^2$, then observe that, by the definition of μ_p,

$$\begin{array}{ll} \mu_p & \mu_p \\ 00 \mapsto 0 & 00 \mapsto 0 \\ 01 \mapsto 0 & 0p \mapsto 1 \\ 10 \mapsto p & p0 \mapsto 0 \\ 11 \mapsto p & pp \mapsto 1. \end{array}$$

Any irrational number $x \in \mathbb{T}$, whose expansion $a \in \Lambda_{p^2}^{\mathbb{N}}$ includes only the digits 0, 1, has an infinite μ_p-orbit (since a represents an irrational number). This means that $\{\mu_p^k(a)\}_{k\in\mathbb{N}}$ is infinite but none of the sequences in it contain digits other than $\{0, 1, p\}$. (Actually, for even ks the sequences will contain only 0 and 1 and for odd ks the only digits that appear are 0 and p.) In particular, the digit $p+1$ does not appear in $\{\mu_p^k(a)\}_{k\in\mathbb{N}}$. Therefore, $\overline{\{\mu_p^k(a)\}_{k\in\mathbb{N}}}$ is an infinite, μ_p-invariant proper subset of $\Lambda_{p^2}^{\mathbb{N}}$, hence $\langle\mu_p\rangle$ is not ID.

For $s = p^n$, observe that

$$\mu_p(0, 0), \mu_p(0, p^k), \mu_p(p^k, 0), \mu_p(p^k, p^k) \in \{0, p^{k+1}\} \quad \text{for } k \in \{0, 1, \ldots, n-2\}$$

and

$$\mu_p(0, 0), \mu_p(0, p^{n-1}), \mu_p(p^{n-1}, 0), \mu_p(p^{n-1}, p^{n-1}) \in \{0, 1\}.$$

The digit $p+1$ cannot appear in the orbit $\{\mu_p^k(a)\}_{k\in\mathbb{N}}$ if $a_n \in \{0, 1\}$ for all n. □

Remark 3.4. The last proof shows a way to construct closed, m_u-invariant subsets of $\mathbb{T}$ (which asserts that m_u is not ID). Take a non-eventually periodic† sequence $a \in \Lambda_{u^2}^{\mathbb{N}}$ composed only of $\{0, 1\}$, consider $\mu_u \in \mathrm{CAT}(\Lambda_{u^2}^{\mathbb{N}})$ and take $V^{-1}(\overline{\{\mu_u^k(a)\}_{k\in\mathbb{N}}}) \subset \mathbb{T}$.

Let $\tau : \Lambda_s^{\mathbb{N}} \to \Lambda_s^{\mathbb{N}}$ be a cellular automaton transformation. We would like to determine under which conditions τ represents a continuous torus function. In other words, when can $\tilde{\tau} : \mathbb{T} \to \mathbb{T}$ be constructed using the diagram

$$\begin{array}{ccc} \Lambda_s^{\mathbb{N}} & \xrightarrow{\tau} & \Lambda_s^{\mathbb{N}} \\ \downarrow V & & \downarrow V \\ \mathbb{T} & \overset{\tilde{\tau}}{\dashrightarrow} & \mathbb{T} \end{array}$$

where V is the evaluation function.

For $\tilde{\tau}$ to be well defined, we must confirm that if $a, b \in V^{-1}(x)$, then $V\tau(a) = V\tau(b)$.

LEMMA 3.5. *Let $p|s$ and $s \neq p^m$. If $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ commutes with μ_p, then $\tilde{\tau}$ is a well-defined continuous torus function.*

Proof. For concreteness, we will focus on the case $s = 10$, $p = 2$. The general case easily follows. Let τ be a transformation that commutes with μ_2. Denote $A = \{d/2^a5^b\} \subset \mathbb{T}$, the set of all the points of the torus with two decimal expansions. For each $x \in A$, define $x^u, x^l \in \Lambda_{10}^{\mathbb{N}}$ to be the upper and lower decimal representations of x, respectively. In other

† Definitions and details are provided in the next section.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

words, $x^u \neq x^l$ but $V(x^u) = V(x^l)$. We need to show that $V\tau(x^u) = V\tau(x^l)$ for all $x \in A$. For $x \in \mathbb{T}\backslash A$, $x^u = x^l$ is the unique decimal expansion of x.

Define

$$\Delta = \{\delta \in \mathbb{T} \mid \exists x \in A, |V\tau(x^u) - V\tau(x^l)| = \delta\}.$$

Note that $0 \in \Delta$ since one can check that, for example, $V\tau(000\ldots) = V\tau(999\ldots)$. For each $\delta \in \Delta$, $x \in \mathbb{T}$ will be called *a witness of* δ if $|V\tau(x^u) - V\tau(x^l)| = \delta$. It will be sufficient to prove that $\Delta = \{0\}$. We claim that $\Delta \subset \mathbb{T}$ satisfies the conditions of Furstenberg's theorem.

Let $\{\delta_n\} \subset \Delta$ such that $\delta_n \to \delta \in \mathbb{T}$. For each δ_n, denote its witness by $x^n \in A$. Denote $x^{n,u}$ and $x^{n,l}$, the two decimal expansions of x^n, i.e. $|V\tau(x^{n,u}) - V\tau(x^{n,l})| = \delta_n$. Since $(x^{n,u}, x^{n,l}) \subset (\Lambda_{10}^{\mathbb{N}})^2$ and as a result of the compactness of $\Lambda_{10}^{\mathbb{N}}$, we can assume, without loss of generality, that $(x^{n,u}, x^{n,l}) \to (y, z)$. V is continuous and $V(x^{n,u}) = V(x^{n,l})$ for all n, thus $V(y) = V(z)$. This means that y and z are two representations of the same element of the torus. The continuity of $V\tau$ implies $|V\tau(y) - V\tau(z)| = \delta$, so $V(y) = V(z)$ is a witness of δ. Therefore, $\delta \in \Delta$ and Δ is a closed set.

Next, we show that $\Delta \subset \mathbb{T}$ is $\{2^{k_1}10^{k_2}\}_{k_1,k_2\in\mathbb{N}}$-invariant. Let $\delta \in \Delta$ and let $x \in A$ be one of its witnesses. Define $y = 2x \in \mathbb{T}$. Obviously, $y \in A$. For the two decimal expansions of y,

$$\begin{aligned} |V\tau(y^u) - V\tau(y^l)| = |V\tau\mu_2(x^u) - V\tau\mu_2(x^l)| &= |V\mu_2\tau(x^u) - V\mu_2\tau(x^l)| \\ &= |2 \cdot V\tau(x^u) - 2 \cdot V\tau(x^l)| \\ &= 2\delta \in \mathbb{T}. \end{aligned}$$

This means that $y \in A$ is in fact a witness for $2\delta = m_2(\delta)$, hence $m_2(\Delta) \subset \Delta$. The same is valid for multiplication by 10 (note that in this case it is not necessary for τ to commute with μ_2, but only to be a cellular automaton transformation, so by definition it commutes with $\sigma = \mu_{10}$).

To conclude, $\Delta \subset \mathbb{T}$ is closed and invariant under the action of the non-lacunary semigroup $\{2^{k_1}10^{k_2}\}$. By Furstenberg's theorem, Δ must be either $\mathbb{T}$ or finite. Recall that we need to show that $\Delta = \{0\}$.

Assume by contradiction that there exists $\delta \in \Delta$ such that $\delta \neq 0$ and let x be a witness of δ. Denote

$$x^l = a_0a_1\ldots a_kb999\ldots, \quad x^u = a_0a_1\ldots a_k(b-1)_{\mathrm{mod}\ 10}000\ldots.$$

Then

$$\left(\frac{x}{10}\right)^l = 0a_0a_1\ldots a_kb999\ldots, \quad \left(\frac{x}{10}\right)^u = 0a_0a_1\ldots a_k(b-1)_{\mathrm{mod}\ 10}000\ldots.$$

If $r \leq k+1$ (r is the radius of τ), then

$$\left|V\tau\left(\left(\frac{x}{10}\right)^u\right) - V\tau\left(\left(\frac{x}{10}\right)^l\right)\right| = \frac{\delta}{10} \in \Delta.$$

The same argument for $x/10^2$ implies that $\delta/10^2 \in \Delta$; similarly, $x/10^j$ implies that $\delta/10^j \in \Delta$ for all $j \in \mathbb{N}$, hence Δ is infinite.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

If $r \geq k+2$, note that for every $c \in \mathbb{N}$, $|V\tau((x/10^c)^u) - V\tau((x/10^c)^l)| \neq 0$, so we can use the same procedure for $x/10^c$ with a sufficiently large c, concluding again that Δ is infinite. (In this case, the decimal expansions are

$$\left(\frac{x}{10^c}\right)^u = 0\ldots 0a_1\ldots a_k b000$$

and

$$\left(\frac{x}{10^c}\right)^l = 0\ldots 0a_1\ldots a_k(b-1)_{\mathrm{mod}\ 10}999\ldots,$$

where the number of 0s at the beginning of each expansion is c. Choosing c such that $r \leq c+k+1$ reduces the case to the preceding one.)

We have shown that if there exists $\delta \in \Delta$, $\delta \neq 0$, then Δ contains infinitely many elements, which implies $\Delta = \mathbb{T}$. But this is a contradiction since Δ is a countable set. Thus, $\Delta = \{0\}$ and $\tilde{\tau}$ is well defined. A standard compactness argument shows that $\tilde{\tau}$ is continuous. □

Until now, we have shown that every transformation that commutes with μ_p represents some continuous torus function. The next theorem, due to Blanchard *et al* [**3**], classifies the continuous torus functions that can be represented by a cellular automaton transformation, for general s. Although our definition for 'representing a torus function' is somewhat different from that of [**3**], the same arguments and constructions which appear in [**3**] can be applied here. They proved the following theorem.

THEOREM. (Blanchard–Host–Maass) *If $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ represents a continuous torus function $\tilde{\tau}: \mathbb{T} \to \mathbb{T}$, then $\tilde{\tau}$ is of the form $\tilde{\tau}(x) = ux$, where $u \in \mathbb{Z}$ divides some positive power of s, or $\tilde{\tau}$ is a constant function $\tilde{\tau}(x) \equiv t/(s-1)$, where $t \in \{0, 1, \ldots, s-2\}$.*

Combining Lemma 3.5 and the BHM theorem completes the proof of Theorem 3.2.

Proof of Theorem 3.2. Where s is not a power of a prime, clearly, $\langle \mu_{p_1}, \ldots, \mu_{p_d}, \mu_0 \rangle$ is commutative since the multiplications on the torus, $m_{p_1}, \ldots, m_{p_d}$ and m_0 commute.

If $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ commutes with this semigroup, in particular it commutes with μ_{p_1}, and by Lemma 3.5, τ represents a continuous torus function $\tilde{\tau}$. By the BHM theorem, $\tilde{\tau} = m_u$, where each prime $p|u$ is one of $p_1, \ldots, p_d$ or $\tilde{\tau}$ is a constant map $\tilde{\tau} \equiv t/(s-1)$ for some $t \in \{0, 1, \ldots, s-2\}$. Consider the latter case where $\tilde{\tau} \equiv t/(s-1)$. Note that a constant map commutes with another map if and only if the image of the constant map is a fixed point of the other. Thus, in order to commute with all μ_{p_i}, $t/(s-1)$ must be a fixed point of m_{p_i} for all i. Clearly, 0 is a fixed point of all m_{p_i}, so we add μ_0 to the semigroup in order to get maximality†.

We conclude that when s is not a power of a prime, $\tau \in \langle \mu_{p_1}, \ldots, \mu_{p_d}, \mu_0 \rangle$, and hence the semigroup is MC.

† Note that sometimes 0 can be replaced by other digits that have this property: $1/2$ is a fixed point of both m_3 and m_5. In $\Lambda_{15}^{\mathbb{N}}$, $\frac{1}{2}$ is represented by the constant sequence $77\ldots$. Denoting $\tau(a) = 77\ldots$, we get that $\langle \mu_3, \mu_5, \tau \rangle \subset \mathrm{CAT}(\Lambda_{15}^{\mathbb{N}})$ is MC as well as $\langle \mu_3, \mu_5, \mu_0 \rangle \subset \mathrm{CAT}(\Lambda_{15}^{\mathbb{N}})$. However, a commutative semigroup can have at most one constant map and for the general statement we choose μ_0.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

Note that when $s = p^m$, the proof above does not hold, since if we define $\Delta \subset \mathbb{T}$ as in the proof of Lemma 3.5, then Δ is $\{p^{k_1}s^{k_2}\}$-invariant. $\{p^{k_1}s^{k_2}\} = \{p^{k_1}\} \subset \mathbb{N}$ is lacunary and, therefore, we cannot apply Furstenberg's theorem to conclude that $\Delta = \{0\}$.

We will show now that when $s = p^m$, the semigroup is actually not MC. Assume $s = p^m$. Define the block map $f : \Lambda_p^m \to \Lambda_{p^m}$ by

$$f(a_0a_1 \dots a_{m-1}) = p^{m-1}a_0 + p^{m-2}a_1 + \cdots + pa_{m-2} + a_{m-1}.$$

f defines a function $\phi : \Lambda_p^{\mathbb{N}} \to \Lambda_{p^m}^{\mathbb{N}}$ by $\phi(a)_k = f(a_{[mk,m(k+1))})$. ϕ interprets the first m-word as a p-expansion of an element in p^m, and assigns it as the first coordinate. The second m-word (the symbols $a_m a_{m+1} \dots a_{2m-1}$) is interpreted in the same way and the result is assigned to the second coordinate, and so on.

This gives a topological conjugacy $\phi : (\Lambda_p^{\mathbb{N}}, \langle \mu_p^{(p)}, \mu_0^{(p)} \rangle) \to (\Lambda_{p^m}^{\mathbb{N}}, \langle \mu_p^{(p^m)}, \mu_0^{(p^m)} \rangle)$, which means that ϕ forms a homeomorphism between $\Lambda_p^{\mathbb{N}}$ and $\Lambda_{p^m}^{\mathbb{N}}$, and that there exists a bijection $\tau \mapsto \tilde{\tau}$ from $\langle \mu_p^{(p)}, \mu_0^{(p)} \rangle$ to $\langle \mu_p^{(p^m)}, \mu_0^{(p^m)} \rangle$ such that, for any $\tau \in \langle \mu_p^{(p)}, \mu_0^{(p)} \rangle$, $\phi(\tau) = \tilde{\tau}(\phi)$. Explicitly, if $\tau = (\mu_p^{(p)})^{k_1}(\mu_0^{(p)})^{k_2}$, then $\tilde{\tau} = (\mu_p^{(p^m)})^{k_1}(\mu_0^{(p^m)})^{k_2}$. Any $\nu \in \mathrm{CAT}(\Lambda_p^{\mathbb{N}})$ that commutes with $\langle \mu_p^{(p)}, \mu_0^{(p)} \rangle$ defines $\bar{\nu} \in \mathrm{CAT}(\Lambda_{p^m}^{\mathbb{N}})$ by $\bar{\nu} = \phi(\nu(\phi^{-1}))$. The topological conjugacy asserts that $\bar{\nu}$ commutes with $\langle \mu_p^{(p^m)}, \mu_0^{(p^m)} \rangle$. Hence, in order to show that $\langle \mu_p^{(p^m)}, \mu_0^{(p^m)} \rangle \subset \mathrm{CAT}(\Lambda_{p^m}^{\mathbb{N}})$ is not MC, it is enough to show that $\langle \mu_p^{(p)}, \mu_0^{(p)} \rangle = \langle \sigma, \mu_0 \rangle \subset \mathrm{CAT}(\Lambda_p^{\mathbb{N}})$ is not MC.

Now, any transformation in $\mathrm{CAT}(\Lambda_p^{\mathbb{N}})$ with $00 \dots \in \Lambda_p^{\mathbb{N}}$ as a fixed point commutes with $\langle \sigma, \mu_0 \rangle$, or, equivalently, any block map that sends the word $00 \dots 0 \mapsto 0$ commutes with both σ and μ_0, and this completes the proof. □

Remark 3.6. From the BHM theorem, we have that a non-constant transformation that represents a continuous torus function must be of the form μ_u, where $u \in \mathbb{Z}$. In the case $s = 10$, for example, μ_{-1} also commutes with both μ_2 and μ_5. Note that for positive u, μ_u keeps the same representations: if $a \in \Lambda_{10}^{\mathbb{N}}$ is the upper representation of $x \in \mathbb{T}$, then $\mu_u(a)$ is the upper representation of $ux \in \mathbb{T}$, while μ_u for $u < 0$ flips between the representations. Thus, although m_{-1} and m_0 commute, μ_{-1} and μ_0 do not commute.

To summarize, we have shown a way to construct semigroups which are both MC and ID whenever $s \neq p^m$ for a prime p. The same construction, when $s = p^m$, is neither MC nor ID.

Semigroups of $\mathrm{CAT}(\Lambda_{p^m}^{\mathbb{N}})$ which are both MC and ID are described in the next section.

4. *Linear cellular automata transformations*

In this section, we consider Λ_s as the ring $\mathbb{Z}/s\mathbb{Z}$. Note that the ring's structure depends on the interpretation of each symbol in Λ_s; every bijection between the symbol set Λ_s and the elements of $\mathbb{Z}/s\mathbb{Z}$ defines a different ring structure on Λ_s. For simplicity, choose the identity permutation and treat Λ_s as $\mathbb{Z}/s\mathbb{Z}$. Thus, $\Lambda_s^{\mathbb{N}}$ is endowed with the structure of a Λ_s-module.

When $s = p^m$ is a power of a prime, one can give the symbol set a field structure (again, the interpretation of the symbols affects the field structure). We will distinguish between

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

these objects by the following notations: Λ_s is the ring $\mathbb{Z}/s\mathbb{Z}$ (either when $s = p^m$ or not) and $\mathbb{F}_{p^m}$ is the field of p^m elements. Thus, $\mathbb{F}_{p^m}^{\mathbb{N}}$ is endowed with the structure of an infinite-dimensional vector space over $\mathbb{F}_{p^m}$.

Define $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ to be the subset of $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$, which consists of all the cellular automata transformations which are linear, i.e. $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}}) = \mathrm{CAT}(\Lambda_s^{\mathbb{N}}) \cap \mathrm{Hom}_{\Lambda_s}(\Lambda_s^{\mathbb{N}}, \Lambda_s^{\mathbb{N}})$. Clearly, $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ is a semigroup since both $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ and $\mathrm{Hom}_{\Lambda_s}(\Lambda_s^{\mathbb{N}}, \Lambda_s^{\mathbb{N}})$ are closed under composition.

In the same manner, define $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ to be all the transformations which are linear.

In this section, we will prove the following theorems.

THEOREM 4.1. *The semigroup* $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ *is an ID for any finite field* $\mathbb{F}_{p^m}$.

THEOREM 4.2. *The semigroup* $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ *is an ID semigroup if and only if* s *is prime.*

THEOREM 4.3. *The semigroup* $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ *is maximal commutative for any finite field* $\mathbb{F}_{p^m}$.

THEOREM 4.4. *The semigroup* $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ *is maximal commutative for any* $s \geq 2$.

In order to prove that $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ is an ID semigroup, we first prove that $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is an ID semigroup for any s†. Then we show the property for $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$.

Note that for $s \neq p^m$, this claim results from §3 as follows: if $s = p_1^{e_1} \cdots p_d^{e_d}$ $(d > 1)$, then $\langle \mu_{p_i}, \sigma \rangle$ is an ID semigroup (for $i = 1, 2, \ldots, d$). In particular, $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is also an ID semigroup, as it contains a sub-semigroup which is ID.

To prove that $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is ID for any s, we will use the following definitions.

Definition. A sequence $a \in \Lambda_s^{\mathbb{N}}$ is a *rich sequence* if there exists $\{n_m\} \subset \mathbb{N}$ with $n_m \to \infty$ such that for each $m \in \mathbb{N}$, there exists $k(m) \in \mathbb{N}$ with the property $a_{[i,i+k)} \neq a_{[j,j+k)}$ for all $i \neq j < n_m$.

Definition. A sequence $a \in \Lambda_s^{\mathbb{N}}$ is a *periodic sequence* if for some $c > 0$, $a_n = a_{n+c}$ for all $n \in \mathbb{N}$. $a \in \Lambda_s^{\mathbb{N}}$ is *c-periodic* if c is the minimal integer for which this holds. c is called *the period of* a.

Definition. A sequence $a \in \Lambda_s^{\mathbb{N}}$ is a *b, c-eventually periodic sequence* if $\sigma^b(a)$ is c-periodic, but $\sigma^{b-1}(a)$ is not periodic. For simplicity, the parameters b, c will be omitted when possible.

LEMMA 4.5. *A sequence* $a \in \Lambda_s^{\mathbb{N}}$ *is eventually periodic if and only if it is not rich.*

One can give a purely symbolic proof for this lemma. However, consider the evaluation function $V : \Lambda_s^{\mathbb{N}} \to \mathbb{T}$, mentioned in §3; the eventually periodic sequences are mapped to rational numbers while rich sequences are s-expansions of irrational numbers (for any s).

It follows from the definition that a rich sequence has an ample supply of words ($a_{[i,j]}$ is a word appearing in a). This will enable, in Theorem 4.9, a construction of specific transformations showing that the image of the action of $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ on any rich sequence is dense. On the other hand, by definition, eventually periodic sequences lack this property.

† Note that when considering $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$, the symbol set Λ_s carries no structure.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

However, the maximal amount of different words that can be found in an eventually periodic sequence, is described in the next lemma.

LEMMA 4.6. *Let $a \in \Lambda_s^{\mathbb{N}}$ be b, c-eventually periodic; then there exists $k \in \mathbb{N}$ such that $a_{[i,i+k)} \neq a_{[j,j+k)}$ for all $i \neq j < b + c - 1$.*

Denote

$$B_{b,c} = \{a_0 \dots a_{b-1}\overline{a_b \dots a_{b+c-1}}\} = \{a_0 \dots a_{b-1}a_b \dots a_{b+c-1}a_b \dots a_{b+c-1} \dots\} \subset \Lambda_s^{\mathbb{N}}.$$

Note that the parameters b, c are not minimal as they are in the definition of a b, c-eventually periodic sequence. $B_{b,c}$ can be defined alternatively by the subset of $\Lambda_s^{\mathbb{N}}$ consisting of all b', c'-eventually periodic sequences with $c'|c$, $b' \leq b$.

LEMMA 4.7. *For any b, c, $B_{b,c}$ is closed and $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$-invariant.*

Proof. Since $|B_{b,c}| < \infty$, $B_{b,c}$ is a closed set. Obviously, if a is b, c-eventually periodic, then for any $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$, $\tau(a)$ is b', c'-eventually periodic with $c'|c$, $b' \leq b$, thus $\tau(a) \in B_{b,c}$, which shows the invariance. □

LEMMA 4.8. *Let $A \subset \Lambda_s^{\mathbb{N}}$ be a $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$-invariant subset. If A contains a b, c-eventually periodic sequence, then $B_{b,c} \subset A$.*

Proof. Let $a \in A$ be b, c-eventually periodic and let $x \in B_{b,c}$. We will define a transformation $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ such that $\tau(a) = x$. From Lemma 4.6, there exists $k \in \mathbb{N}$ such that $a_{[i,i+k)} \neq a_{[j,j+k)}$ for all $i, j < b + c - 1$. Thus, the following block map is well defined:

$$f(y_0 y_1 \dots y_{k-1}) = \begin{cases} x_i & \text{if } y_0 y_1 \dots y_{k-1} = a_{[i,i+k)}, \\ 0 & \text{otherwise.} \end{cases}$$

If τ is the transformation associated with f, then $\tau(a) = x$. This can be done for any $x \in B_{b,c}$, thus $B_{b,c} \subset A$. □

THEOREM 4.9. *The semigroup $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is an ID semigroup for any $s \geq 2$.*

Proof. Let A be a $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$-invariant subset of $\Lambda_s^{\mathbb{N}}$.

Distinguish between two cases.

(1) If A contains a rich sequence, we claim that $\overline{A} = \Lambda_s^{\mathbb{N}}$. Let $a \in A$ be a rich sequence, $x \in \Lambda_s^{\mathbb{N}}$ and let $\epsilon > 0$. Choose $n_0 > 1/\epsilon$. By the definition of a rich sequence, it is possible to find a $k \in \mathbb{N}$ such that $a_{[i,i+k)} \neq a_{[j,j+k)}$ for any $i \neq j < n_0$. Define a block map as follows:

$$f(y_0 y_1 \dots y_{k-1}) = \begin{cases} x_i & \text{if } y_0 y_1 \dots y_{k-1} = a_{[i,i+k)}, \\ 0 & \text{otherwise.} \end{cases}$$

Note that for a transformation τ defined by this block map, $\tau(a)_{[0,n_0)} = x_{[0,n_0)}$ and thus $d(\tau(a), x) < \epsilon$. This holds for any $x \in \Lambda_s^{\mathbb{N}}$ and arbitrary ϵ, therefore $\overline{A} = \Lambda_s^{\mathbb{N}}$.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

(2) Otherwise, A contains only eventually periodic sequences. Assume that A is infinite; we need to show that $\overline{A} = \Lambda_s^{\mathbb{N}}$. From Lemma 4.8, A is a union of $B_{b,c}$ sets. Since $|B_{b,c}| < \infty$, A is a union of infinitely many $B_{b,c}$ sets. Thus, A contains $B_{b,c}$ with arbitrarily large $b + c$.

Let $x \in \Lambda_s^{\mathbb{N}}$ and $\epsilon > 0$. There exists $B_{b,c} \subset A$ with $b + c > 1/\epsilon$. By definition, $B_{b,c}$ contains all the $b + c$ prefixes, in particular, it contains a sequence a which coincides with x on the first $b + c$ coordinates: $a_{[0,b+c)} = x_{[0,b+c)}$. Since this can be done for any $\epsilon > 0$, we conclude that $\overline{A} = \Lambda_s^{\mathbb{N}}$. □

Recall that the goal was to prove that $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ is an ID semigroup. The method used in the preceding proof was building specific block maps. This was possible because of the variety of different words appearing in a rich sequence, or, in infinitely many eventually periodic sequences. To be able to build such a block map for a transformation in $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$, we must ensure that there are enough words which are not only different but also linearly independent.

LEMMA 4.10. *Let $a \in \mathbb{F}_{p^m}^{\mathbb{N}}$ be a rich sequence; then for any $n \in \mathbb{N}$, there exists a $k(n)$ such that the set of vectors $\{a_{[i,i+k)}\}_{i=0}^{n-1} \subset \mathbb{F}_{p^m}^k$ is linearly independent.*

Proof. Assume by contradiction that there exists an $n_0 \in \mathbb{N}$ such that for any k, $\{a_{[i,i+k)}\}_{i=0}^{n_0-1}$ is linearly dependent. For any $k \in \mathbb{N}$, define $r(k)$ as the minimal integer such that $a_{[r,r+k)}$ is linearly dependent on its predecessors ($\{a_{[i,i+k)}\}_{i=0}^{r-1}$ are linearly independent). For any k, $r(k) \le n_0 - 1$, and thus there exists a sequence $k_l \to \infty$ such that $r(k_l) = r_0$ is fixed.

Since the field $\mathbb{F}_{p^m}$ is finite, there is a finite number of linear dependences for n_0 vectors. Assume, without loss of generality, that for any k_l, the r_0th vector depends on its predecessors by the same linear combination, $a_{[r_0,r_0+k_l)} = \sum_{i=0}^{r_0-1} \beta_i a_{[i,i+k_l)}$, for all $l \in \mathbb{N}$.

In particular, for each $j > r_0$, find $k_l > j$ and conclude that the jth coordinate satisfies $a_j = \sum_{i=j-r_0}^{j-1} \beta_i a_i$. Therefore, for any l such that $k_l > s^{r_0}$, we can find i, $j < k_l$ such that $a_{[i,i+r_0)} = a_{[j,j+r_0)}$, and thus $a_{i+r_0} = a_{j+r_0}$. By induction, a is eventually periodic, which is a contradiction. □

LEMMA 4.11. *Let $a \in \mathbb{F}_{p^m}^{\mathbb{N}}$ be a b, c-eventually periodic sequence; then there exists some $k \in \mathbb{N}$ such that the set of vectors $\{a_{[i,i+k)}\}_{i=0}^{b-1} \subset \mathbb{F}_{p^m}^k$ is linearly independent.*

Proof. From Lemma 4.6, there exists a k_0 such that all the words $\{a_{[i,i+k_0)}\}_{i=0}^{b-1}$ are different†. Clearly, this holds for any $k > k_0$. If for some $k > k_0$ these vectors are linearly independent, then we are done.

Otherwise, enlarge $k_l \to \infty$ and repeat the argument used in the previous lemma to get $r_0 \le b - 1$ such that $a_{[r_0,r_0+k_l)} = \sum_{i=0}^{r_0-1} \beta_i a_{[i,i+k_l)}$. But then $\sigma^{r_0}(a)$ is periodic, in contradiction to the minimality of b. □

Now we can prove Theorem 4.1.

† We can assure that all the first $b + c - 1$ k_0-words in n are different. Here we need only the first $b - 1$ words to be different.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

Proof of Theorem 4.1. Let $A \subset \mathbb{F}_{p^m}^{\mathbb{N}}$ be an infinite LCAT($\mathbb{F}_{p^m}^{\mathbb{N}}$)-invariant set. We need to show that A is dense. Let $\epsilon > 0$.

If A contains a rich sequence a, by Lemma 4.10, for any n_0, there exists a k such that the first n_0 k-words of a are linearly independent. Choose $n_0 > 1/\epsilon$ and denote $k = k(n_0)$. Given $x \in \mathbb{F}_{p^m}^{\mathbb{N}}$, consider a block map that assigns to the block $a_{[i,i+k)}$ the value x_i for each $i = 0, \ldots, r-1$. Note that as a result of the independence of $\{a_{[i,i+k)}\}_{i=0}^{n_0-1}$, such block maps exist and they are linear functionals on $\mathbb{F}_{p^m}^{k}$. Hence, a transformation defined by such a block map is indeed linear and thus is a member of LCAT($\mathbb{F}_{p^m}^{\mathbb{N}}$). Obviously, $d(\tau(a), x) < \epsilon$, and hence $\overline{A} = \mathbb{F}_{p^m}^{\mathbb{N}}$.

Otherwise, A is an infinite set of eventually periodic sequences. Using Lemma 4.11 and a similar argument, we get the following. Let $x \in \mathbb{F}_{p^m}^{\mathbb{N}}$ and let $a \in A$ be a b, c-eventually periodic sequence. We can construct a block map that is associated with $\tau \in \mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ such that $d(\tau(a), x) < 1/b$. Thus, if A contains b, c-eventually periodic sequences with arbitrarily large b, then $\overline{A} = \mathbb{F}_{p^m}^{\mathbb{N}}$.

We still need to consider the case where A is an infinite set of eventually periodic sequences with bounded parameter b. In this case, the parameter c of the sequences in A in unbounded. The shift σ is in LCAT($\mathbb{F}_{p^m}^{\mathbb{N}}$) and A is LCAT($\mathbb{F}_{p^m}^{\mathbb{N}}$)-invariant, therefore A contains infinitely many periodic sequences with arbitrarily large period c. Let $x \in \mathbb{F}_{p^m}^{\mathbb{N}}$ and let $a \in A$ be a c-periodic sequence. Repeating the argument in Lemma 4.11, we can find a $k \in \mathbb{N}$ such that all the first $c-1$ k-words in a are linearly independent (using the minimality of c). Thus, it is possible to construct in the same way a $\tau \in \mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$ such that $d(\tau(a), x) < 1/c$. Since A contains sequences with arbitrarily large c, $\overline{A} = \mathbb{F}_{p^m}^{\mathbb{N}}$. □

Proof of Theorem 4.2. Clearly, if s is prime, then LCAT($\Lambda_s^{\mathbb{N}}$) = LCAT($\mathbb{F}_s^{\mathbb{N}}$), and hence, by Theorem 4.1, LCAT($\Lambda_s^{\mathbb{N}}$) is ID.

Assume that $s = pq$ ($p, q \neq 1$, they may be equal). Let $A = p\Lambda_s^{\mathbb{N}}$ be the set of all sequences $a \in \Lambda_s^{\mathbb{N}}$ such that $p | a_n$ for all n. $A \neq \Lambda_s^{\mathbb{N}}$ since p is not invertible in Λ_s. Note that A is LCAT($\Lambda_s^{\mathbb{N}}$)-invariant since each coordinate of $\tau(a)$ (for $a \in A$, $\tau \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$) is a linear combination of numbers that are divided by p. Hence, A is an infinite non-dense LCAT($\Lambda_s^{\mathbb{N}}$)-invariant subset of $\Lambda_s^{\mathbb{N}}$, which implies that LCAT($\Lambda_s^{\mathbb{N}}$) is not ID when s is not a prime. □

Given $\tau \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$, denote its block map by $f_\tau : \Lambda_s^{r+1} \to \Lambda_s$. The linearity of τ imposes the following condition on f_τ:

$$\alpha f_\tau(a_{[0,r]}) + \beta f_\tau(b_{[0,r]}) = f_\tau(\alpha a_{[0,r]} + \beta b_{[0,r]})$$

for any $\alpha, \beta \in \Lambda_s$ and $a_{[0,r]}, b_{[0,r]} \in \Lambda_s^{r+1}$.

This means that $\tau \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ if and only if its block map is a Λ_s-linear functional on Λ_s^{r+1}. We can describe the action of $\tau \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ by a 'shift-polynomial' in the manner described below.

Consider the standard basis $\{e^i\}_{i=0}^{r}$ of Λ_s^{r+1} and let $c_i = f_\tau(e^i)$. Let $a_0 \ldots a_r \in \Lambda_s^{r+1}$; then $f_\tau(a_0 \ldots a_r) = c_0 \cdot a_0 + c_1 \cdot a_1 + \cdots + c_r \cdot a_r$. Now associate with τ the polynomial $p_\tau(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_r x^r$, $p_\tau \in \Lambda_s[x]$. Observe that substituting

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

a cellular automaton transformation in some polynomial $p \in \Lambda_s[x]$ yields a cellular automaton transformation. In particular, substituting the shift σ in p_τ yields τ.

One can check that the ring $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ with composition as multiplication and pointwise addition, is isomorphic to $\Lambda_s[x]$ by $\tau \mapsto p_\tau$. This was shown in [**9**] and discussed in [**8**] for the case $s = 2$. In particular, $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ is a commutative semigroup since the polynomial ring is commutative.

The same isomorphism to the polynomial ring holds for $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$, and hence the commutativity property follows.

Proof of Theorems 4.3 and 4.4. We prove the maximal commutativity for $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$. For the proof of Theorem 4.3, replace $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ in the following by $\mathrm{LCAT}(\mathbb{F}_{p^m}^{\mathbb{N}})$.

$\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ is commutative since it is isomorphic, as a ring, to the commutative ring of polynomials over Λ_s. Thus, all we have to show is maximality. Let $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ be a transformation such that $\tau\mu = \mu\tau$ for every $\mu \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$. Given $\mu \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$, let $p_\mu(x) = \sum_{i=0}^{r} c_i x^i$ be the polynomial associated with it. Without loss of generality, assume that both μ and τ are of the same radius r, hence $\tau\mu$ and $\mu\tau$ are of radius $\leq 2r$ and we may consider the radius to be exactly $2r$ (the radius in our definition is not necessarily minimal). For any block $a_{[0,2r]} \in \Lambda_s^{2r+1}$,

$$\begin{aligned}\tau\mu(a_{[0,2r]}) &= \tau(\mu(a_{[0,r]})\mu(a_{[1,r+1]}) \ldots \mu(a_{[r,2r]})) \\ &= \tau\left(\left(\sum_{i=0}^{r} c_i a_i\right)\left(\sum_{i=0}^{r} c_i a_{i+1}\right) \ldots \left(\sum_{i=0}^{r} c_i a_{i+r}\right)\right)\end{aligned}$$

and

$$\begin{aligned}\mu\tau(a_{[0,2r]}) &= \mu(\tau(a_{[0,r]})\tau(a_{[1,r+1]}) \ldots \tau(a_{[r,2r]})) \\ &= \sum_{i=0}^{r} c_i \tau(a_{[i,i+r]}).\end{aligned}$$

From commutativity,

$$\sum_{i=0}^{r} c_i \tau(a_{[i,i+r]}) = \tau\left(\left(\sum_{i=0}^{r} c_i a_i\right)\left(\sum_{i=0}^{r} c_i a_{i+1}\right) \ldots \left(\sum_{i=0}^{r} c_i a_{i+r}\right)\right) \tag{1}$$

for any choice of $c_i \in \Lambda_s$ (for $i = 0, \ldots, r$) and for all $a_{[0,2r]} \in \Lambda_s^{2r+1}$. Let $c \in \Lambda_s$. Substituting

$$c_i = \begin{cases} c, & i = 0, \\ 0, & i > 0, \end{cases}$$

in (1) yields

$$c\tau(a_{[0,r]}) = \tau((ca_0)(ca_1) \ldots (ca_r)) = \tau(ca_{[0,r]})$$

for all $a_{[0,r]} \in \Lambda_s^{r+1}$, which asserts that τ is homogeneous. To show that τ is additive, we need to verify that, for any $x_0 \ldots x_r$,

$$\tau(x_0 x_1 \ldots x_r) = \sum_{i=0}^{r} x_i \tau(e^i),$$

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

where $\{e^i\}_{i=0}^r$ is the standard basis of Λ_s^{r+1}. Fix $x_{[0,r]} \in \Lambda_s^{r+1}$. Substituting $c_i = x_{r-i}$ and

$$a_i = \begin{cases} 0, & i \neq r, \\ 1, & i = r, \end{cases}$$

in (1) yields

$$x_r\tau(0\ldots1) + x_{r-1}\tau(0\ldots10) + \cdots + x_0\tau(1\ldots0) = \tau(x_0x_1\ldots x_r).$$

Note that the left-hand side is equal to $\sum_{i=0}^r x_i\tau(e^i)$, therefore τ is additive, which proves that τ is linear, namely $\tau \in \mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$. □

5. *Semigroups over one-sided and two-sided shift spaces*

So far we have dealt only with one-sided shift spaces, $\Lambda_s^{\mathbb{N}}$. A cellular automaton transformation over a two-sided shift space $\Lambda_s^{\mathbb{Z}}$ is a continuous function $\Lambda_s^{\mathbb{Z}} \to \Lambda_s^{\mathbb{Z}}$ which commutes with the left shift σ. Similar to the description of a transformation over $\Lambda_s^{\mathbb{N}}$ by a block map, there exists a two-sided version of the Curtis–Hedlund–Lyndon theorem.

THEOREM. (Curtis–Hedlund–Lyndon) *Let $\tau : \Lambda_s^{\mathbb{Z}} \to \Lambda_s^{\mathbb{Z}}$; then $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ if and only if there exists some $r \in \mathbb{N}$ and a function $f_\tau : \Lambda_s^{2r+1} \to \Lambda_s$ such that*

$$\tau(a)_k = f(a_{k-r}\ldots a_{k-1}a_ka_{k+1}\ldots a_{k+r})$$

for any $a \in \Lambda_s^{\mathbb{Z}}$ and $k \in \mathbb{N}$.

f_τ is called a block map and r is the radius of τ. As in the one-sided case, it is often convenient to use the same notation for the block map f_τ and the transformation τ.

Every block map of $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is a valid block map for a transformation in $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$. Under this correspondence, we may regard τ as being contained in $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$, and we may say that $\mathrm{CAT}(\Lambda_s^{\mathbb{N}}) \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$. In particular, any semigroup $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ can also be considered as a semigroup $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$.

For $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ such that $\sigma \in \Sigma$, denote $\Sigma_+ = \Sigma \cap \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$. Σ_+ contains all the transformations in Σ which can also act on $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$. Observe that for each $\tau \in \Sigma\backslash\Sigma_+$, if we compose it with σ^r, where r is the radius of τ, we get an element in Σ_+. Note that Σ_+ is a sub-semigroup of $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ (when it is non-empty).

One may think of a cellular automaton as an action of a machine that reads the first $r+1$ symbols $(a_0\ldots a_r)$, assigns to them an output according to its block map, and inserts it in the first coordinate. Then, the machine moves to the next $r+1$ symbols $(a_1\ldots a_{r+1})$ and inserts the corresponding output in the second coordinate and so on. The machines τ and $\sigma^z\tau$ $(z \in \mathbb{Z})$ use the same block map and differ in the location where they insert the output. This perspective suggests that we could view a cellular automaton transformation as being determined by its block map rather than where the precise location of the output is. This motivates the following theorems.

THEOREM 5.1. *Let $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ be an ID semigroup; then $\langle\Sigma, \sigma^{-1}\rangle \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ is an ID semigroup.*

THEOREM 5.2. *Let $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ be a maximal commutative semigroup; then $\langle\Sigma, \sigma^{-1}\rangle$ is maximal commutative in $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$.*

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

THEOREM 5.3. *Let* $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ *be an ID semigroup; then* $\langle \Sigma, \sigma \rangle_+ \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ *is an ID semigroup.*

THEOREM 5.4. *Let* $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ *be a maximal commutative semigroup; then* Σ_+ *is maximal commutative in* $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$.

Denote by $\pi_+ : \Lambda_s^{\mathbb{Z}} \to \Lambda_s^{\mathbb{N}}$ the projection on the positive coordinates: $\pi_+(a_{(-\infty,\infty)}) = a_{[0,\infty)}$.

Note that these statements are sharp in the following sense: in Theorem 5.1, if we delete σ^{-1}, then $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ is not an ID semigroup (the set of all sequences such that $\pi_+(a)$ is 1-periodic is invariant). Clearly, it is necessary to add σ^{-1} in Theorem 5.2. The statement of Theorem 5.3 is meaningless without adding σ since Σ_+ may be empty.

Definition. A sequence $a \in \Lambda_s^{\mathbb{Z}}$ is *c-periodic* if for any $z \in \mathbb{Z}$, $a_z = a_{z+c}$, where c is minimal with this property.

Proof of Theorem 5.1. Let $Y \subset \Lambda_s^{\mathbb{Z}}$ be an infinite set, and let $w_{-n} \dots w_0 \dots w_n$ be some finite word of length $2n+1$. Define $X = \{\sigma^{-k}(y) \mid y \in Y, k > n\}$ and note that $\pi_+(X)$ is an infinite subset of $\Lambda_s^{\mathbb{N}}$. By the fact that Σ is ID, there exist $\tilde{x} \in \pi_+(X)$ and $\tau \in \Sigma$ such that $\tau(\tilde{x})_{[0,2n]} = w_{-n} \dots w_0 \dots w_n$ and $\tilde{x} = \sigma^{-k}(y)$, where $k > n$ and $y \in Y$, that is $\tau\sigma^{-k+n}(y)_{[-n,n]} = w_{-n} \dots w_0 \dots w_n$. Since $\tau\sigma^{-k+n} \in \langle \Sigma, \sigma^{-1} \rangle$ and $w_{-n} \dots w_0 \dots w_n$ is an arbitrary word, we conclude that $\langle \Sigma, \sigma^{-1} \rangle$ is ID. □

Proof of Theorem 5.2. Let $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ with radius r and consider $\tau\sigma^r$. Note that for every $k \in \mathbb{Z}$, the kth coordinate $\tau\sigma^r(a)_k$ is dependent only on $a_{[k,k+2r+1]}$. Thus, $\tau\sigma^r$ can also act on the one-sided shift space, hence $\tau\sigma^r \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ (with radius $\leq 2r$).

Assume that τ commutes with all $\Sigma' = \langle \Sigma, \sigma^{-1} \rangle$; we need to show that $\tau \in \Sigma'$. In particular, τ commutes with Σ. Let $\mu \in \Sigma$; then $\tau\mu = \mu\tau$ and hence $\sigma^r\tau\mu = \mu\sigma^r\tau$. Since $\sigma^r\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ and Σ is MC, $\sigma^r\tau \in \Sigma$, which implies that $\tau \in \Sigma'$. □

Proof of Theorem 5.3. Let $X \subset \Lambda_s^{\mathbb{N}}$ be an infinite set, and let $Y \subset \Lambda_s^{\mathbb{Z}}$ be the set

$$Y = \{y \mid \forall n \in \mathbb{N}, \exists x \in X, m \in \mathbb{N}, y_{[-n,n]} = x_{[m,m+2n]}\},$$

that is every symmetric word in an element of Y appears as a word in some element of X.

First, we show that $Y \neq \emptyset$. Given $x \in X$, we construct $y \in Y$: there exists a symbol η that appears infinitely many times in x. Define $y_0 = \eta$. There exist two symbols ζ and θ such that the word $\zeta\eta\theta$ appears infinitely many times in x. Choose $y_{[-1,1]} = \zeta\eta\theta$. Continue with this process to get that $y \in Y$. In particular, $Y \neq \emptyset$ and for every $x \in X$ and for arbitrarily large length m, there exists this y that shares a word of length m with x.

Assume that $|Y| = \infty$. Since Σ is ID, $\Sigma(Y) = \{\tau(y)\}_{\tau \in \Sigma, y \in Y}$ is dense, that is any arbitrarily large symmetric word appears in some element of $\Sigma(Y)$. Let $w_0 \dots w_k \in \Lambda_s^{k+1}$ be a word. Find τ and y such that $\tau(y)_{[0,k]} = w_0 \dots w_k$, and denote by r the radius of τ. By the definition of Y, there exist $x \in X$ and a length $m > 0$ such that $y_{[r,k+3r]} = x_{[m,m+k+2r]}$. Note that $\tau \in \Sigma$ implies that $\tau\sigma^r \in \langle \Sigma, \sigma \rangle_+$, and $\tau\sigma^r(x)_{[m,m+k]} = \tau\sigma^r(y)_{[r,k+r]} = \tau(y)_{[0,k]}$. Hence, $\tau\sigma^{r+m}(x)_{[0,k]} = w_0 \dots w_k$. Since $\tau\sigma^{r+m} \in \langle \Sigma, \sigma \rangle_+$ and the word $w_0 \dots w_k$ is arbitrary, we conclude that $\langle \Sigma, \sigma \rangle_+$ is ID.

Therefore, it is enough to show that $|Y| = \infty$. Assume by contradiction that $|Y| < \infty$. Since by definition Y is σ-invariant, it consists only of periodic sequences.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

Suppose that there exists $y \in Y$ such that for arbitrarily large k, there exists $x^{(k)} \in X$ and $n > k$ with $y_{[-k,-1]} = x^{(k)}_{[-k+n,n-1]}$ but $y_0 \neq x^{(k)}_n$. We can assume, without loss of generality, that $x^{(k)}_n$ is the same symbol for all k. Thus, there exists $y' \in Y$ such that $y'_{(\infty,-1]} = y_{(\infty,-1]}$ but $y'_0 \neq y_0$. Now, either y or y' is non-periodic, which is contradiction.

Hence, for every $y \in Y$ there exists a length $M(y)$ such that if $y_{[-k,-1]} = x_{[-k+n,n-1]}$ (for $x \in X$, $k > M(y)$, $n > k$), then $y_0 = x_n$. Denote $M = \max_{y \in Y}\{M(y)\}$. If $x \in X$ shares a word of length M with some element in Y, then they are right asymptotic (there exists $n \in \mathbb{N}$, $z \in \mathbb{Z}$ such that $x_{[n,\infty)} = y_{[z,\infty)}$). But we saw that every $x \in X$ shares arbitrarily long words with some $y \in Y$, so every $x \in X$ is right asymptotic to some $y \in Y$.

Now, since Y contains only periodic sequences, there are infinitely many sequences $\{x^{(n)}\} \subset X$ that are eventually periodic with the same period. Moreover, we can assume that they are all right asymptotic. $x^{(n)}$ is $b^{(n)}$, c-eventually periodic, where $b^{(n)} \to \infty$. By the minimality of the parameters, the sequence $x^{(n)}_{[b(n)-1,\infty)}$ is not periodic (while $x^{(n)}_{[b(n),\infty)}$ is periodic). Define $y \in \Lambda_s^{\mathbb{Z}}$ by $y_{[0,\infty)} = x^{(n)}_{[b(n),\infty)}$. Consider the symbols appearing in $\{x^{(n)}_{b(n)-1}\}$ (where $b(n) > 0$). Without loss of generality, all of these are the same symbol η and define $y_{-1} = \eta$. Consider the symbols appearing in $\{x^{(n)}_{b(n)-2}\}$ for such $x^{(n)}$, where $b(n) > 1$. One of the symbols appears infinitely many times; set y_{-2} to be that symbol. Continue with this process to get $y \in \Lambda_s^{\mathbb{Z}}$. By the construction, $y \in Y$ and it is non-periodic, which is a contradiction. We conclude that Y is infinite and the proof is completed. □

Proof of Theorem 5.4. Let $\tau \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ such that τ commutes with all Σ_+.

First, we show that τ, as a transformation in $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$, commutes with all Σ. Let $\mu \in \Sigma$ be a transformation with radius r. Since Σ is MC, it must contain σ and thus $\mu\sigma^r \in \Sigma_+$. τ commutes with all the elements of Σ_+; in particular $\mu\sigma^r\tau = \tau\mu\sigma^r$. σ^r commutes with both τ, μ, and σ^r is invertible, hence $\mu\tau = \tau\mu$. The MC of Σ implies that $\tau \in \Sigma$. Thus, $\tau \in \Sigma \cap \mathrm{CAT}(\Lambda_s^{\mathbb{N}}) = \Sigma_+$. □

6. *The action of the automorphism group*

Denote the group of all the automorphisms of the dynamical system $(\Lambda_s^{\mathbb{Z}}, \sigma)$ by $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$. $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$ consists of all the cellular automata transformations which are bijective functions.

The automorphism group is 'large' in the algebraic sense. Hedlund [**11**] showed that $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$ contains a copy of every finite group, and Boyle *et al* [**5**] showed that it contains free groups. Recently, $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$ has been extensively studied and a rich algebraic theory has been developed. The automorphism group is studied usually for automorphisms of subshift of finite type, as well as for automorphism groups of multidimensional shifts of finite type (see [**12**]).

The automorphism group is 'large' in the dynamical sense as well. Boyle *et al* [**3**] showed that $\Lambda_s^{\mathbb{Z}}$ does not contain a proper infinite closed set which is $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$-invariant. This means in our terms that $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$ is an ID semigroup. Their theorem is more general and holds for an automorphism group of any mixing shift of finite type (see [**3**]). A stronger version of this theorem can be derived from previous results in this article for the particular case of the full shift $\Lambda_s^{\mathbb{N}}$ when s is not a power of a prime.

In §3, we defined $\mu_u \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ ($u|s^n$ for some n). As already mentioned (§5), μ_u can be viewed as a transformation in $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$. As such, $\mu_u \in \mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$ is both onto

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

and injective (note that $(\mu_u)^{-1} = \sigma^{-1}(\mu_{s/u})$). Clearly, as a transformation acting on a one-sided shift space, $\mu_p \in \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ is onto but not injective.

THEOREM 6.1. *$\langle \mu_p, \sigma, \sigma^{-1} \rangle$ is an ID semigroup of $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$, where $p|s$ is prime and s is not a power p.*

In particular, $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$ is an ID semigroup, where s is not a power of a prime.

Proof. Let $s = pq$, where p is a prime that does not divide q. From Theorem 3.1, $\langle \mu_p, \sigma \rangle$ is an ID semigroup of $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$. Hence, by Theorem 5.1, $\langle \mu_p, \sigma, \sigma^{-1} \rangle$ is an ID semigroup of $\mathrm{CAT}(\Lambda_s^{\mathbb{Z}})$. $\mu_p \in \mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$, and clearly $\sigma, \sigma^{-1} \in \mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$, thus $\mathrm{Aut}(\Lambda_s^{\mathbb{Z}})$ is an ID semigroup as it contains the ID sub-semigroup $\langle \mu_p, \sigma, \sigma^{-1} \rangle$. □

7. *ID and maximal commutativity*

Let Ω be a shift space, $\Sigma \subset \mathrm{CAT}(\Omega)$ a semigroup, and let Σ' be a sub-semigroup of Σ. Clearly, any Σ-invariant subset of Ω is in particular Σ'-invariant. Therefore, any semigroup which contains an ID semigroup is also ID.

On the other hand, the MC property in not preserved under inclusion (adding new elements will break down the commutativity) or by moving to smaller semigroups (removing elements will break the maximality down).

A semigroup which is ID is 'large' in a dynamical sense, while the MC property indicates 'largeness' in an algebraic sense.

However, neither of the properties implies the other: the semigroup $\langle \mu_2, \sigma \rangle \subset \mathrm{CAT}(\Lambda_{10}^{\mathbb{N}})$ (§3) is ID but not MC. Although $\mathrm{LCAT}(\Lambda_s^{\mathbb{N}})$ is not ID when s is not prime, it is MC for any s.

Although ID and MC are properties that indicate 'largeness', we saw a semigroup generated by only two transformations which is ID. In the following, we construct a semigroup generated by two transformations which is MC (and not ID).

Consider the case $s = 2$. As in §4, one can treat Λ_2 as the ring $\mathbb{Z}/2\mathbb{Z}$. Let $\tau \in \mathrm{CAT}(\Lambda_2^{\mathbb{Z}})$ be defined by

$$\tau(a)_k = a_k + \prod_{i=1}^{r} (a_{k+i} + \delta_i),$$

where addition and multiplication are defined in $\mathbb{Z}/2\mathbb{Z}$, $\delta_i \in \mathbb{Z}/2\mathbb{Z}$ $(i = 1, \ldots, r)$ and the radius $r \geq 2$.

Define the *least period of* τ by the minimal integer m such that $\delta_i = \delta_{i+m}$ for $i = 1, 2, \ldots, r - m$.

Coven *et al* [**8**] solved the 'commuting block maps problem' for several classes of block maps, in particular for the block maps of the form that defines τ above. They showed that the set of transformations commuting with τ depends on whether $m \leq r/2$ or not. We rephrase their solution for transformations of the form of τ with $m \leq r/2$ using the terminology of the present article.

The small period theorem. (Coven–Hedlund–Rhodes) Let $\tau \in \mathrm{CAT}(\Lambda_2^{\mathbb{Z}})$ be defined by

$$\tau(a)_k = a_k + \prod_{i=1}^{r} (a_{k+i} + \delta_i),$$

where the least period of $\tau \leq r/2$. Then $\langle \tau, \sigma, \sigma^{-1}, \mathrm{Id} \rangle \subset \mathrm{CAT}(\Lambda_2^{\mathbb{Z}})$ is MC.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

Consider τ with the following parameters: $r = 2$ and $\delta_1 = \delta_2 = 0$. The resulting transformation is $\tau(a)_k = a_k + a_{k+1}a_{k+2}$.

τ 'changes' the kth coordinate if and only if $a_{k+1} = a_{k+2} = 1$. For each $i \in \mathbb{Z}$, define $e^i \in \Lambda_2^{\mathbb{Z}}$ to be the sequence with 1 in the ith coordinate and 0 elsewhere. The consecutive pair 11 does not appear in e^i, and therefore $\tau(e^i) = e^i$ for all $i \in \mathbb{Z}$. Define $A = \overline{\{e^i\}_{i\in\mathbb{Z}}} = \{e^i\}_{i\in\mathbb{Z}} \cup \{0\}$ (where $\{0\} = 000\ldots$). $A \subset \Lambda_2^{\mathbb{Z}}$ is an infinite closed $\langle\tau, \sigma\rangle$-invariant proper subset of $\Lambda_2^{\mathbb{Z}}$, which asserts that $\langle\tau, \sigma\rangle$ is not an ID semigroup.

By Theorem 5.4 and the Small Period theorem we have that $\langle\tau, \sigma, \mathrm{Id}\rangle$ is MC in $\mathrm{CAT}(\Lambda_2^{\mathbb{N}})$. This is an example of an MC semigroup over the one-sided shift space which is generated by 3 elements only. Clearly, since every transformation commutes with σ and Id, $\langle\tau, \sigma, \mathrm{Id}\rangle \subset \mathrm{CAT}(\Lambda_2^{\mathbb{N}})$ is of minimal number of generators for a semigroup having the MC property over $\Lambda_2^{\mathbb{N}}$.

Let $\Sigma \subset \mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ be an MC semigroup. For any s, the minimal number of generators of Σ is at least 3. For $s = 2$, we saw that this number is actually 3.

Problem. What is the minimal number of generators for a semigroup having the MC property for any s?

For s which is not a power of a prime, we constructed a semigroup in $\mathrm{CAT}(\Lambda_s^{\mathbb{N}})$ generated by two elements which is ID. A semigroup Σ is called cyclic if $\Sigma = \langle\tau\rangle$ for some τ.

Problem. Is it true that a cyclic semigroup over $\Lambda_s^{\mathbb{N}}$ ($s \geq 2$) cannot have the ID property?

What is the minimal number of generators for an ID semigroup over $\Lambda_s^{\mathbb{N}}$ for general s?

By the theorems in §5, one can see that the questions above do not change significantly, when asking these questions about a semigroup over a two-sided shift space.

Although the ID property does not always follow from MC, it may be so for certain MC semigroups. Therefore, we pose the following interesting question.

Problem. Let Ω be a shift space and $\Sigma \subset \mathrm{CAT}(\Omega)$ a maximal commutative semigroup of cellular automata transformations. Are there any conditions on Σ which imply that Σ has the ID property?

Acknowledgements. This article is based on an MSc Thesis submitted to the Hebrew University, Jerusalem. I would like to thank my advisor, Professor Hillel Furstenberg, for introducing me to the area and for sharing with me the joy of doing mathematics. I would like also to thank Dr Uri Shapira and Dr Jehuda Hartman for their help. Special thanks are due to the referee for his helpful suggestions and improvements in several proofs.

References

[1] D. Berend. Multi-invariant sets on tori. *Trans. Amer. Math. Soc.* **280**(2) (1983), 509–532.

[2] D. Berend. Multi-invariant sets on compact abelian groups. *Trans. Amer. Math. Soc.* **286**(2) (1984), 505–535.

[3] F. Blanchard, B. Host and A. Maass. Représentation par automate de fonctions continues de tore. *J. Théor. Nombres Bordeaux* **5**(2) (1993), 303–321.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press

[4] F. Blanchard and A. Maass. Dynamical properties of expansive one-sided cellular automata. *Israel J. Math.* **99**(1) (1997), 149–174.
[5] M. Boyle, D. Lind and D. Rudolph. The automorphism group of a shift of finite type. *Trans. Amer. Math. Soc.* **306**(1) (1988), 71–114.
[6] T. Ceccherini-Silberstein and M. Coornaert. The garden of eden theorem for linear cellular automata. *Ergod. Th. & Dynam. Sys.* **26**(01) (2006), 53–68.
[7] T. G. Ceccherini-Silberstein and M. Coornaert. *Cellular Automata and Groups (Springer Monographs in Mathematics)*. Springer, Berlin, 2010.
[8] E. M. Coven, G. A. Hedlund and F. Rhodes. The commuting block maps problem. *Trans. Amer. Math. Soc.* **249**(1) (1979), 113–138.
[9] J. D. Ferguson. Some properties of mappings on sequence spaces. *Dissertation*, Yale University, 1962.
[10] H. Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Theory Comput. Syst.* **1**(1) (1967), 1–49.
[11] G. A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Theory Comput. Syst.* **3**(4) (1969), 320–375.
[12] M. Hochman. On the automorphism groups of multidimensional shifts of finite type. *Ergod. Th. & Dynam. Sys.* **30**(03) (2010), 809–840.
[13] M. Ito, N. Osato and M. Nasu. Linear cellular automata over zm. *J. Comput. System Sci.* **27**(1) (1983), 125–140.
[14] A. Katok and R. J. Spatzier. Invariant measures for higher-rank hyperbolic abelian actions. *Ergod. Th. & Dynam. Sys.* **16**(04) (1996), 751–778.
[15] E. Lindenstrauss. Invariant measures for multiparameter diagonalizable algebraic actions—a short survey. *European Congress of Mathematics (Stockholm, 27 June–2 July 2004)*. ASM International, 2005, p. 247.
[16] D. J. Rudolph. x2 and x3 invariant measures and entropy. *Ergod. Th. & Dynam. Sys.* **10** (1990), 395–406.

https://doi.org/10.1017/S0143385711000551 Published online by Cambridge University Press