*Ergod. Th. & Dynam. Sys.* (2007), **27**, 1965–1990
doi: 10.1017/S0143385707000247 © *2007 Cambridge University Press*
*Printed in the United Kingdom*

# Measure rigidity for algebraic bipermutative cellular automata

MATHIEU SABLIK

*Institut de Mathématiques de Luminy, UMR 6206-Campus de Luminy, Case 907,
13288 Marseille Cedex 09, France
(e-mail: sablik@iml.univ-mrs.fr)*

(*Received* 3 *April* 2005 *and accepted in revised form* 24 *January* 2006)

*Abstract*. Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a bipermutative algebraic cellular automaton. We present conditions that force a probability measure, which is invariant for the $\mathbb{N} \times \mathbb{Z}$-action of $F$ and the shift map $\sigma$, to be the Haar measure on $\Sigma$, a closed shift-invariant subgroup of the abelian compact group $\mathcal{A}^{\mathbb{Z}}$. This generalizes simultaneously results of Host *et al* (B. Host, A. Maass and S. Martínez. Uniform Bernoulli measure in dynamics of permutative cellular automata with algebraic local rules. *Discrete Contin. Dyn. Syst.* **9**(6) (2003), 1423–1446) and Pivato (M. Pivato. Invariant measures for bipermutative cellular automata. *Discrete Contin. Dyn. Syst.* **12**(4) (2005), 723–736). This result is applied to give conditions which also force an $(F, \sigma)$-invariant probability measure to be the uniform Bernoulli measure when $F$ is a particular invertible affine expansive cellular automaton on $\mathcal{A}^{\mathbb{N}}$.

## 1. *Introduction*

Let $F : \mathcal{A}^{\mathbb{M}} \to \mathcal{A}^{\mathbb{M}}$ with $\mathbb{M} = \mathbb{N}$ or $\mathbb{Z}$ be a one-dimensional cellular automaton (CA). The study of invariant measures under the action of $F$ has been addressed from different points of view in the last two decades. As ergodic theory is the study of invariant measures, it is thus natural to characterize them. In addition, since $F$ commutes with the shift map $\sigma$, it is important to describe invariant probability measures for the semi-group action generated by $F$ and $\sigma$. We remark that it easy to prove the existence of such measures by considering a cluster point of the Cesàro mean under iteration of $F$ of a $\sigma$-invariant measure. This problem is related to Furstenberg's conjecture [**Fur67**] that the Lebesgue measure on the torus is the unique invariant measure under multiplication by two relatively prime integers. In the algebraic setting, the study of invariant measures under a group action on a zero-dimensional group, like Ledrappier's example [**Led78**], has been extensively considered in [**Sch95**] and [**Ein05**].

The uniform Bernoulli measure has an important role in the study of $(F, \sigma)$-invariant measures. Hedlund has shown in [**Hed69**] that a CA is surjective if and only if the uniform

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

Bernoulli measure on $\mathcal{A}^{\mathbb{M}}$ is $(F, \sigma)$-invariant. Later, Lind [**Lin84**] has shown for the radius 1 mod 2 automaton that, starting from any Bernoulli measure, the Cesàro mean of the iterates by the CA converges to the uniform measure. This result is generalized for a large class of algebraic CAs and a large class of measures with tools from stochastic processes in [**MM98**] and [**FMMN00**], and with harmonic analysis tools in [**PY02**] and [**PY04**].

However, the uniform Bernoulli measure is not the only $(F, \sigma)$-invariant measure; indeed every uniform measure supported on a $(F, \sigma)$-periodic orbit is $(F, \sigma)$-invariant. We want to obtain additional conditions which allow us to characterize the uniform Bernoulli measure. We limit the study to CAs which have algebraic and strong combinatorial properties: the algebraic bipermutative CAs. Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a bipermutative algebraic CA; we examine the conditions that force an $(F, \sigma)$-invariant measure $\mu$ to be the Haar measure of $\mathcal{A}^{\mathbb{Z}}$, denoted by $\lambda_{\mathcal{A}^{\mathbb{Z}}}$. When $\mathcal{A}^{\mathbb{Z}}$ is an infinite product of the finite group $\mathcal{A}$, the Haar measure is the uniform Bernoulli measure. Host *et al* take this direction in [**HMM03**] and characterize the $(F, \sigma)$-invariant measure of affine bipermutative CAs of radius 1 when the alphabet is $\mathbb{Z}/p\mathbb{Z}$ with $p$ prime. They show two theorems with different assumptions on the measure $\mu$. Pivato gives in [**Piv05**] an extension of the first theorem, considering a larger class of algebraic CAs but with extra conditions on the measure and the kernel of $F$. The main result in the present paper provides a generalization of the second theorem of [**HMM03**], which also generalizes Pivato's result.

To introduce more precisely the previous work and this paper, we need to provide definitions and introduce some classes of CAs. Let $\mathcal{A}$ be a finite set and $\mathbb{M} = \mathbb{N}$ or $\mathbb{Z}$. We consider $\mathcal{A}^{\mathbb{M}}$, the configuration space of $\mathbb{M}$-indexed sequences in $\mathcal{A}$. If $\mathcal{A}$ is endowed with the discrete topology, $\mathcal{A}^{\mathbb{M}}$ is compact and totally disconnected in the product topology. The *shift* map $\sigma : \mathcal{A}^{\mathbb{M}} \to \mathcal{A}^{\mathbb{M}}$ is defined by $\sigma(x)_i = x_{i+1}$ for $x = (x_m)_{m\in\mathbb{M}} \in \mathcal{A}^{\mathbb{M}}$ and $i \in \mathbb{M}$. Denote by $\mathcal{A}^*$ the set of all finite sequences or words $w = w_0 \ldots w_{n-1}$ with letters in $\mathcal{A}$; by $|w|$ we mean the length of $w \in \mathcal{A}^*$. Given $w \in \mathcal{A}^*$ and $i \in \mathbb{M}$, the *cylinder set* starting at coordinate $i$ with the word $w$ is $[w]_i = \{x \in \mathcal{A}^{\mathbb{M}} : x_{i,i+|w|-1} = w\}$, and the cylinder set starting at 0 is simply denoted by $[w]$.

A *cellular automaton* (CA) is a pair $(\mathcal{A}^{\mathbb{M}}, F)$, where $\mathcal{A}^{\mathbb{M}}$ is called the *configuration space* and $F : \mathcal{A}^{\mathbb{M}} \to \mathcal{A}^{\mathbb{M}}$ is a continuous function which commutes with the shift. We can therefore consider $(F, \sigma)$ as a $\mathbb{N} \times \mathbb{M}$-action. By Hedlund's theorem [**Hed69**], this is equivalent to giving a local function which acts uniformly and synchronously on the configuration space, that is to say, there is a finite segment $\mathbb{U} \subset \mathbb{M}$ (called the *neighborhood*) and a *local rule* $\overline{F} : \mathcal{A}^{\mathbb{U}} \to \mathcal{A}$, such that $F(x)_m = \overline{F}((x_{m+u})_{u\in\mathbb{U}})$ for all $x \in \mathcal{A}^{\mathbb{M}}$ and $m \in \mathbb{M}$. The *radius* of $F$ is $r(F) = \max\{|u| : u \in \mathbb{U}\}$; when $\mathbb{U}$ is as small as possible, it is called the *smallest neighborhood*. If the smallest neighborhood is reduced to one point we say that $F$ is *trivial*.

Let $\mathfrak{B}$ be the Borel sigma-algebra of $\mathcal{A}^{\mathbb{M}}$; we denote by $\mathcal{M}(\mathcal{A}^{\mathbb{M}})$ the set of probability measures on $\mathcal{A}^{\mathbb{M}}$ defined on the sigma-algebra $\mathfrak{B}$. As usual, $\sigma\mu$ (respectively $F\mu$) denotes the measure given by $\sigma\mu(B) = \mu(\sigma^{-1}(B))$ (respectively $F\mu(B) = \mu(F^{-1}(B))$) for $B$ a Borel set. This allows us to consider the $(F, \sigma)$-action on $\mathcal{M}(\mathcal{A}^{\mathbb{M}})$. We say that $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{M}})$ is $\sigma$-*invariant* (respectively $F$-*invariant*) if and only if $\sigma\mu = \mu$ (respectively $F\mu = \mu$); obviously, $\mu$ is $(F, \sigma)$-*invariant* if and only if $\mu$ is $\sigma$-invariant and $F$-invariant.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

We denote $\mathcal{I}_\mu(\sigma) = \{B \in \mathfrak{B} : \mu(\sigma^{-1}(B)\triangle B) = 0\}$ to be the algebra of $\sigma$-invariant sets mod $\mu$. If $\mathcal{A}^{\mathbb{M}}$ has a group structure and $\Sigma$ is a closed $\sigma$-invariant subgroup of $\mathcal{A}^{\mathbb{M}}$, the *Haar measure* on $\Sigma$, denoted $\lambda_\Sigma$, is the unique measure in $\mathcal{M}(\mathcal{A}^{\mathbb{M}})$ with $\mathrm{supp}(\mu) \subset \Sigma$ which is invariant by the action of $\Sigma$. We can characterize $\lambda_\Sigma$ using *characters* in $\widehat{\mathcal{A}^{\mathbb{M}}}$, which are continuous morphisms from $\mathcal{A}^{\mathbb{M}}$ to $\mathbb{C}$; indeed, $\mu = \lambda_\Sigma$ if and only if $\mathrm{supp}(\mu) \subset \Sigma$ and $\mu(\chi) = 0$ for all $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$ such that $\chi(\Sigma) \neq \{1\}$, see [**Gui68**] for further details. If $\mathcal{A}$ is a finite group and $\mathcal{A}^{\mathbb{M}}$ is a product group, the Haar measure of $\mathcal{A}^{\mathbb{M}}$ corresponds to the *uniform Bernoulli measure* defined on a cylinder set $[u]_i$ by

$$\lambda_{\mathcal{A}^{\mathbb{M}}}([u]_i) = \frac{1}{|\mathcal{A}|^{|u|}}.$$

Let $(\mathcal{A}^{\mathbb{M}}, F)$ be a CA of smallest neighborhood $\mathbb{U} = [r, s] = \{r, \ldots, s\}$. $F$ is *left-permutative* if and only if, for any $u \in \mathcal{A}^{s-r}$ and $b \in \mathcal{A}$, there is a unique $a \in \mathcal{A}$ such that $\overline{F}(au) = b$; $F$ is *right-permutative* if and only if, for any $u \in \mathcal{A}^{s-r}$ and $b \in \mathcal{A}$, there is a unique $a \in \mathcal{A}$ such that $\overline{F}(ua) = b$. $F$ is *bipermutative* if and only if it is both left and right permutative.

If $\mathcal{A}^{\mathbb{M}}$ has a topological group structure and if $\sigma : \mathcal{A}^{\mathbb{M}} \to \mathcal{A}^{\mathbb{M}}$ is a continuous group endomorphism, $\mathcal{A}^{\mathbb{M}}$ is called a *group shift*. By Hedlund's theorem [**Hed69**], the $\sigma$-commuting multiplication operator is given by a local rule $\overline{*} : \mathcal{A}^{[r,s]} \times \mathcal{A}^{[r,s]} \to \mathcal{A}$. We refer to [**Kit87**] for further details. If $\mathcal{A}^{\mathbb{M}}$ is an abelian group shift and $F : \mathcal{A}^{\mathbb{M}} \to \mathcal{A}^{\mathbb{M}}$ is a group endomorphism which commutes with $\sigma$, then the CA $(\mathcal{A}^{\mathbb{M}}, F)$ is said to be *algebraic*. If $\mathcal{A}$ has an abelian group structure, $\mathcal{A}^{\mathbb{M}}$ is a compact abelian group. We say that $(\mathcal{A}^{\mathbb{M}}, F)$ is a *linear* CA if $F$ is a group endomorphism or equivalently if $\overline{F}$ is a morphism from $\mathcal{A}^{\mathbb{U}}$ to $\mathcal{A}$. In this case $F$, can be written as

$$F = \sum_{u \in \mathbb{U}} f_u \circ \sigma^u$$

where, for all $u \in \mathbb{U}$, $f_u$ is an endomorphism of $\mathcal{A}$ which is extended coordinate by coordinate to $\mathcal{A}^{\mathbb{M}}$. We can write $F$ as a polynomial of $\sigma$, $F = P_F(\sigma)$, where $P_F \in \mathrm{Hom}(\mathcal{A})[X, X^{-1}]$. If $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}$, then an endomorphism of $\mathcal{A}$ is the multiplication by an element of $\mathbb{Z}/n\mathbb{Z}$. We say that $(\mathcal{A}^{\mathbb{M}}, F)$ is an *affine* CA if there exists a linear CA $(\mathcal{A}^{\mathbb{M}}, G)$ and a constant $c \in \mathcal{A}^{\mathbb{M}}$ such that $F = G + c$. The constant must be $\sigma$-invariant.

A linear CA $(\mathcal{A}^{\mathbb{M}}, F)$, where $F = \sum_{u \in [r,s]} f_u \circ \sigma^u$, is left (respectively right) permutative of smallest neighborhood $[r, s]$ if $f_r$ (respectively $f_s$) is a group automorphism. An affine CA $(\mathcal{A}^{\mathbb{M}}, F + c)$, where $(\mathcal{A}^{\mathbb{M}}, F)$ is linear and $c \in \mathcal{A}^{\mathbb{M}}$, is bipermutative if $(\mathcal{A}^{\mathbb{M}}, F)$ is bipermutative. So, if $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$ where $p$ is prime, then any non-trivial affine CA is bipermutative. However, if $p$ is composite, then $F$ is left (right) permutative if and only if the leftmost (rightmost) coefficient of $\overline{F}$ is relatively prime to $p$.

Now we can recall the first theorem of [**HMM03**].

THEOREM 1.1. [**HMM03**] *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an affine bipermutative CA of smallest neighborhood $\mathbb{U} = [0, 1]$ with $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$, where $p$ is prime, and let $\mu$ be an $(F, \sigma)$-invariant probability measure. Assume that:*

(1) *$\mu$ is ergodic for $\sigma$;*

(2) *the measure entropy of $F$ is positive ($h_\mu(F) > 0$).*

*Then $\mu = \lambda_{\mathcal{A}^{\mathbb{Z}}}$.*

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

The second theorem of [**HMM03**] relaxes the $\sigma$-ergodicity into $(F, \sigma)$-ergodicity provided the measure satisfies a technical condition on the sigma-algebra of invariant sets for powers of $\sigma$.

THEOREM 1.2. [**HMM03**] *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an affine bipermutative CA of smallest neighborhood $\mathbb{U} = [0, 1]$ with $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$, where $p$ is prime, and let $\mu$ be an $(F, \sigma)$-invariant probability measure. Assume that:*
(1) *$\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action $(F, \sigma)$;*
(2) $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{p(p-1)}) \mod \mu$;
(3) $h_\mu(F) > 0$.
*Then* $\mu = \lambda_{\mathcal{A}^{\mathbb{Z}}}$.

Pivato gives in [**Piv05**] a result similar to Theorem 1.1, which applies to a larger class of algebraic CAs but with extra conditions on the measure and $\mathrm{Ker}(F)$.

THEOREM 1.3. [**Piv05**] *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an algebraic bipermutative CA of smallest neighborhood $\mathbb{U} = [0, 1]$ and let $\mu$ be an $(F, \sigma)$-invariant probability measure. Assume that:*
(1) *$\mu$ is totally ergodic for $\sigma$;*
(2) $h_\mu(F) > 0$;
(3) $\mathrm{Ker}(F)$ *contains no non-trivial $\sigma$-invariant subgroups.*
*Then* $\mu = \lambda_{\mathcal{A}^{\mathbb{Z}}}$.

It is possible to extend Theorem 1.3 to a non-trivial algebraic bipermutative CA without restriction on the neighborhood. In §2 of this paper, we give entropy formulas for bipermutative CAs without restrictions on the neighborhood. These formulas are the first step to adapt the proof of Theorem 1.2 in §3 in order to obtain our main result.

THEOREM 3.3. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a non-trivial algebraic bipermutative CA, let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$, let $k \in \mathbb{N}$ such that every prime factor of $|\mathcal{A}|$ divides $k$ and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$ with* $\mathrm{supp}(\mu) \subset \Sigma$. *Assume that:*
(1) *$\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action $(F, \sigma)$;*
(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_1})$ with $p_1$ the smallest common period of all elements of* $\mathrm{Ker}(F)$;
(3) $h_\mu(F) > 0$;
(4) *every $\sigma$-invariant infinite subgroup of $D^{\Sigma}_{\infty}(F) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ is dense in $\Sigma$.*
*Then* $\mu = \lambda_{\Sigma}$.

Theorem 3.3 is a common generalization of Theorems 1.2 and 1.3 when $\mathcal{A}$ is a cyclic group and $\mathcal{A}^{\mathbb{Z}}$ is the product group. To obtain a generalization of Theorem 1.3 for any abelian group $\mathcal{A}^{\mathbb{Z}}$, we must take a weaker assumption for $D^{\Sigma}_{\infty}$; however, we need a further restriction for the probability measure.

THEOREM 3.4. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a non-trivial algebraic bipermutative CA, let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$, let $k \in \mathbb{N}$ such that every prime factor of $|\mathcal{A}|$ divides $k$ and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$ with* $\mathrm{supp}(\mu) \subset \Sigma$. *Assume that:*

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

(1) *$\mu$ is ergodic for $\sigma$;*
(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_1})$ with $p_1$ the smallest common period of all elements of* $\mathrm{Ker}(F)$*;*
(3) *$h_\mu(F) > 0$;*
(4) *every $(F, \sigma)$-invariant infinite subgroup of $D^\Sigma_\infty(F) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ is dense in $\Sigma$.*

*Then $\mu = \lambda_\Sigma$.*

To do this some technical work is required on each of the assumptions. At present, we do not know how to obtain a common generalization of Theorems 3.3 and 3.4.

In §4, we show how to replace and relax some assumptions of Theorems 3.3 and 3.4, in particular how one obtains Theorems 1.2 and 1.3 as consequences. First, we replace the assumption of positive entropy of $F$ by the positive entropy of $F^n \circ \sigma^m$ for some $(n, m) \in \mathbb{N} \times \mathbb{Z}$. Then we give a necessary and sufficient condition for $D^\Sigma_\infty$ to contain no non-trivial $(F, \sigma)$-invariant infinite subgroups. This condition is implied by the assumption that $\mathrm{Ker}(F)$ contains no non-trivial $\sigma$-invariant subgroups.

In §5, we restrict the study to linear CAs and obtain rigidity results which cannot be deduced from Theorems 1.2 and 1.3. For example, in §5.1, we can see that Theorem 3.3 works for any non-trivial linear CA $F = P_F(\sigma)$ on $(\mathbb{Z}/p\mathbb{Z})^\mathbb{Z}$ with $p$ prime. In this case, Theorem 1.2 works only for CAs of radius 1 and Pivato's result works only if $P_F$ is irreducible on $\mathbb{Z}/p\mathbb{Z}$. In §6, we give an application of this work. We stray from the algebraic bipermutative CA case and show measure rigidity for some affine one-sided invertible expansive CAs (not necessarily bipermutative) with the help of previous results.

## 2. *Entropy formulas for bipermutative CAs*

Let $(\mathcal{A}^\mathbb{Z}, F)$ be a CA, $\mathfrak{B}$ be the Borel sigma-algebra of $\mathcal{A}^\mathbb{Z}$ and $\mu \in \mathcal{M}(\mathcal{A}^\mathbb{Z})$. We put $\mathfrak{B}_n = F^{-n}(\mathfrak{B})$ for $n \in \mathbb{N}$. For $\mathcal{P}$ a finite partition of $\mathcal{A}^\mathbb{Z}$ and for $\mathfrak{B}'$ a sub sigma-algebra of $\mathfrak{B}$ we denote $H_\mu(\mathcal{P}) = -\sum_{A\in\mathcal{P}} \mu(A)\log(\mu(A))$ to be the entropy of $\mathcal{P}$ and $H_\mu(\mathcal{P}|\mathfrak{B}') = -\sum_{A\in\mathcal{P}} \int_A \log(\mathbb{E}_\mu(1_A|\mathfrak{B}'))\,d\mu$ to be the conditional entropy of $\mathcal{P}$ given $\mathfrak{B}'$. Furthermore, $h_\mu(F)$ denotes the entropy of the measure-preserving dynamical system $(\mathcal{A}^\mathbb{M}, \mathfrak{B}, \mu, F)$. We refer to [**Pet89**] or [**Wal82**] for the definition and main properties.

We define the cylinder partitions $\mathcal{P} = \{[a] : a \in \mathcal{A}\}$ and $\mathcal{P}_{[r,s]} = \{[u]_r : u \in \mathcal{A}^{s-r}\}$. The following lemma is a more general version of the entropy formula in Lemma 4.3 of [**HMM03**] (where this lemma is proved for CAs with radius 1).

LEMMA 2.1. *Let $(\mathcal{A}^\mathbb{Z}, F)$ be a bipermutative CA of smallest neighborhood $\mathbb{U} = [r, s]$ with $r \le 0 \le s$ and let $\mu$ be an $F$-invariant probability measure on $\mathcal{A}^\mathbb{Z}$. Then $h_\mu(F) = H_\mu(\mathcal{P}_{[0,s-r-1]}|\mathfrak{B}_1)$.*

*Proof.* We have $h_\mu(F) = \lim_{l\to\infty} h_\mu(F, \mathcal{P}_{[-l,l]})$ with

$$h_\mu(F, \mathcal{P}_{[-l,l]}) = \lim_{T\to\infty} H_\mu\left(\mathcal{P}_{[-l,l]}\middle|\bigvee_{n=1}^{T} F^{-n}(\mathcal{P}_{[-l,l]})\right) = H_\mu\left(\mathcal{P}_{[-l,l]}\middle|\bigvee_{n=1}^{\infty} F^{-n}(\mathcal{P}_{[-l,l]})\right).$$

Let $l \ge s - r$. By bipermutativity of $F$, for $T \ge 1$, knowing $(F^n(x)_{[-l,l]})_{n\in[1,T]}$ and knowing $F(x)_{[Tr-l,Ts+l]}$ is equivalent. This means that $\bigvee_{n=1}^{T} F^{-n}(\mathcal{P}_{[-l,l]}) =$

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

$F^{-1}(\mathcal{P}_{[Tr-l,Ts+l]})$. By taking the limit as $l \to \infty$, we deduce (with the convention $\infty.0 = 0$) that

$$\bigvee_{n=1}^{\infty} F^{-n}(\mathcal{P}_{[-l,l]}) = F^{-1}(\mathcal{P}_{[\infty.r-l,\infty.s+l]}).$$

So we have

$$h_\mu(F, \mathcal{P}_{[-l,l]}) = H_\mu(\mathcal{P}_{[-l,l]}|F^{-1}\mathcal{P}_{[\infty.r-l,\infty.s+l]}).$$

Similarly, by bipermutativity of $F$, the knowledge of $F(x)_{[\infty.r-l,\infty.s+l]}$ and $x_{[0,s-r-1]}$ allows us to know $x_{[-l,l]}$ and *vice versa*. We deduce that

$$\mathcal{P}_{[0,s-r-1]} \vee F^{-1}(\mathcal{P}_{[\infty.r-l,\infty.s+l]}) = \mathcal{P}_{[-l,l]} \vee F^{-1}(\mathcal{P}_{[\infty.r-l,\infty.s+l]}).$$

Therefore,

$$h_\mu(F, \mathcal{P}_{[-l,l]}) = H_\mu(\mathcal{P}_{[0,s-r+1]}|F^{-1}(\mathcal{P}_{[\infty.r-l,\infty.s+l]})).$$

If $r < 0 < s$, then $\mathcal{P}_{[\infty.r-l,\infty.s+l]} = \mathfrak{B}_1$. Otherwise, by taking the limit as $l \to \infty$ and using the martingale convergence theorem, we obtain $h_\mu(F) = H_\mu(\mathcal{P}_{[0,s-r-1]}|\mathfrak{B}_1)$. □

When $\mu$ is an $(F, \sigma)$-invariant probability measure, it is possible to express the entropy of a right-permutative CA according to the entropy of $\sigma$.

PROPOSITION 2.2. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a right-permutative CA of neighborhood $\mathbb{U} = [0, s]$, where $s$ is the smallest possible value, and let $\mu$ be an $(F, \sigma)$-invariant probability measure. Then $h_\mu(F) = s\, h_\mu(\sigma)$.*

*Proof.* Let $N \in \mathbb{N}$ and $l \geq s$. By right-permutativity, since $\mathbb{U} = [0, s]$, for all $x \in \mathcal{A}^{\mathbb{Z}}$ knowing $(F^n(x)_{[-l,l]})_{n\in[0,N]}$ and knowing $x_{[-l,l+Ns]}$ is equivalent; this means that

$$\bigvee_{n=0}^{N} F^{-n}(\mathcal{P}_{[-l,l]}) = \mathcal{P}_{[-l,l+Ns]}.$$

So for $l \geq s$ we have

$$\begin{aligned} h_\mu(F, \mathcal{P}_{[-l,l]}) &= \lim_{N\to\infty} \frac{1}{N} H_\mu\left(\bigvee_{n=0}^{N} F^{-n}(\mathcal{P}_{[-l,l]})\right) \\ &= \lim_{N\to\infty} \frac{1}{N} H_\mu(\mathcal{P}_{[-l,l+Ns]}) \\ &= \lim_{N\to\infty} -\frac{1}{N} \sum_{u\in\mathcal{A}^{Ns+2l}} \mu([u]) \log(\mu[u]) \\ &= \lim_{N\to\infty} -\frac{Ns+2l}{N} \frac{1}{Ns+2l} \sum_{u\in\mathcal{A}^{Ns+2l}} \mu([u]) \log(\mu[u]) \\ &= s\, h_\mu(\sigma). \end{aligned}$$

We deduce that $h_\mu(F) = \lim_{l\to\infty} h_\mu(F, \mathcal{P}_{[-l,l]}) = s\, h_\mu(\sigma)$. □

*Remark 2.1.* We have a similar formula for a left-permutative CA of the neighborhood $\mathbb{U} = [r, 0]$. Moreover, it is easy to see that this proof is true for a right-permutative CA on $\mathcal{A}^{\mathbb{N}}$.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

COROLLARY 2.3. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a bipermutative CA of smallest neighborhood $\mathbb{U} = [r, s]$, and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$. We have*

$$h_\mu(F) = \begin{cases} s\, h_\mu(\sigma) & \text{if } s \geq r \geq 0, \\ (s-r)\, h_\mu(\sigma) & \text{if } s \geq 0 \geq r, \\ -r\, h_\mu(\sigma) & \text{if } 0 \geq s \geq r. \end{cases}$$

*Proof.* Cases where $s \geq r \geq 0$ or $0 \geq s \geq r$ can be directly deduced from Proposition 2.2.

When $s \geq 0 \geq r$, the CA $(\mathcal{A}^{\mathbb{Z}}, \sigma^{-r} \circ F)$ is bipermutative of smallest neighborhood $[0, s-r]$. Since $\sigma$ is bijective, we deduce that $\mathfrak{B}$ is $\sigma$-invariant. Thus, $F^{-1}(\mathfrak{B}) = (\sigma^{-r} \circ F)^{-1}(\mathfrak{B})$. Since $\mu$ is $(F, \sigma)$-invariant, by Lemma 2.1, one has

$$h_\mu(F) = H_\mu(\mathcal{P}_{[0,s-r-1]} | F^{-1}(\mathfrak{B})) = H_\mu(\mathcal{P}_{[0,s-r-1]} | (\sigma^{-r} \circ F)^{-1}(\mathfrak{B})) = h_\mu(\sigma^{-r} \circ F).$$

The result follows from Proposition 2.2. □

*Remark 2.2.* It is not necessary to use Lemma 2.1. Corollary 2.3 can be proved by a similar method to Proposition 2.2.

A bipermutative CA $(\mathcal{A}^{\mathbb{Z}}, F)$ of smallest neighborhood $\mathbb{U}$ is topologically conjugate to $((\mathcal{A}^t)^{\mathbb{N}}, \sigma)$ where $t = \max(\mathbb{U} \cup \{0\}) - \min(\mathbb{U} \cup \{0\})$, via the conjugacy $\varphi : x \in \mathcal{A}^{\mathbb{Z}} \to (F(x)_{[0,t]})_{n\in\mathbb{N}}$. So the uniform Bernoulli measure is a maximal entropy measure. Thus from Corollary 2.3 we deduce an expression of $h_{\text{top}}(F)$. This implies a result of [**War00**], who computes the topological entropy for linear CAs on $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}$ with $p$ prime by algebraic methods. Moreover, this formula gives Lyapunov exponents for permutative CAs according to the definition of [**She92**] or [**Tis00**].

## 3. *Proof of main theorems*

Now we consider $(\mathcal{A}^{\mathbb{Z}}, F)$ to be a bipermutative algebraic CA of smallest neighborhood $\mathbb{U} = [r, s]$. For $y \in \mathcal{A}^{\mathbb{Z}}$ call $T_y$ the translation $x \mapsto x + y$ on $\mathcal{A}^{\mathbb{Z}}$. For every $n \in \mathbb{N}$, we write $D_n(F) = \text{Ker}(F^n)$; if there is no ambiguity we just denote it by $D_n$. Clearly $D_n$ is a subgroup of $D_{n+1}$. Denote $\partial D_{n+1} = D_{n+1} \setminus D_n$ for all $n \in \mathbb{N}$. By bipermutativity we have $|D_n| = |D_1|^n = |\mathcal{A}|^{(s-r)n}$ where $|\cdot|$ denotes the cardinality of the set. We consider the subgroup $D_\infty(F) = \bigcup_{n\in\mathbb{N}} D_n(F)$ of $\mathcal{A}^{\mathbb{Z}}$, and we denote it by $D_\infty$ if there is no ambiguity; it is dense in $\mathcal{A}^{\mathbb{Z}}$ since $F$ is bipermutative. Every $D_n$ is finite and $\sigma$-invariant so every $x \in D_n$ is $\sigma$-periodic. Let $p_n$ be the smallest common period of all elements of $D_n$. Then $p_n$ divides $|D_n|!$.

Let $\mathfrak{B}$ be the Borel sigma-algebra of $\mathcal{A}^{\mathbb{Z}}$ and let $\mu$ be a probability measure on $\mathcal{A}^{\mathbb{Z}}$. Put $\mathfrak{B}_n = F^{-n}(\mathfrak{B})$ for every $n \in \mathbb{N}$, so that it is the sigma-algebra generated by all cosets of $D_n$. For every $n \in \mathbb{N}$ and $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$, the conditional measure $\mu_{n,x}$ is defined for every measurable set $U \subset \mathcal{A}^{\mathbb{Z}}$ by $\mu_{n,x}(U) = \mathbb{E}_\mu(\mathbf{1}_U | \mathfrak{B}_n)(x)$. Its main properties are as follows.

(A) For $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$, $\mu_{n,x}$ is a probability measure on $\mathcal{A}^{\mathbb{Z}}$ and $\text{supp}(\mu_{n,x}) \subset F^{-n}(\{F^n(x)\}) = x + D_n$.

(B) For all measurable sets $U \subset \mathcal{A}^{\mathbb{Z}}$, the function $x \to \mu_{n,x}(U)$ is $\mathfrak{B}_n$-measurable and $\mu_{n,x} = \mu_{n,y}$ for every $y \in F^{-n}(\{F^n(x)\}) = x + D_n$.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

(C) Let $G : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ be a measurable map and let $U$ be a measurable set. For $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$ one has $\mathbb{E}_\mu(\mathbf{1}_{G^{-1}(U)}|G^{-1}(\mathfrak{B}))(x) = \mathbb{E}_\mu(\mathbf{1}_U|\mathfrak{B})(G(x))$. So $\sigma^m \mu_{n,x} = \mu_{n,\sigma^m(x)}$ and $F\mu_{n+1,x} = \mu_{n,F(x)}$ for $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$ and every $n \in \mathbb{N}$.

(D) Since $\mathfrak{B}_n$ is $T_d$-invariant for $d \in D_n$, by (C) one has $\mu_{n,x} = \mu_{n,x+d}$.

For all $n \in \mathbb{N}$ define $\zeta_{n,x} = T_{-x}\mu_{n,x}$; this is a probability measure concentrated on $D_n$. The previous four properties of conditional measures can be transposed to $\zeta_{n,x}$.

LEMMA 3.1. *Fix $n \in \mathbb{N}$. For $\mu$-almost all $x \in \mathcal{A}^{\mathbb{Z}}$, the following are true.*

(a) $\zeta_{n,x+d} = T_{-d}\zeta_{n,x}$ *for every* $d \in D_n$.

(b) $\sigma^m \zeta_{n,x} = \zeta_{n,\sigma^m(x)}$ *for every* $m \in \mathbb{Z}$ *and* $F\zeta_{n+1,x} = \zeta_{n,F(x)}$.

(c) *For every $m \in p_n\mathbb{Z}$, we have $\sigma^m \zeta_{n,x} = \zeta_{n,x}$. Hence $x \to \zeta_{n,x}$ is $\sigma^m$-invariant.*

*Proof.* (a) is by Property (D), (b) is by Property (C) and (c) is because $\text{supp}(\zeta_{n,x}) \subset D_n$. □

For $n > 0$ and $d \in D_n$ we define

$$E_{n,d} = \{x \in \mathcal{A}^{\mathbb{Z}} : \zeta_{n,x}(\{d\}) > 0\} \quad \text{and} \quad E_n = \bigcup_{d \in \partial D_n} E_{n,d}.$$

Then $E_{n,d}$ is $\sigma^{p_n}$-invariant by Lemma 3.1(c), and $E_n$ is $\sigma$-invariant because $\partial D_n$ is $\sigma$-invariant. We write $\eta(x) = \zeta_{1,x}(\{0\}) = \mu_{1,x}(\{x\})$. The function $\eta$ is $\sigma$-invariant and $E_1 = \{x \in \mathcal{A}^{\mathbb{Z}} : \eta(x) < 1\}$. Therefore, one has

$$\begin{aligned}\eta(F^{n-1}(x)) &= \mu_{1,F^{n-1}(x)}(\{F^{n-1}(x)\}) = \mu_{1,F^{n-1}(x)}(F^{n-1}(x + D_{n-1})) \\ &\underset{(*)}{=} \mu_{n,x}(x + D_{n-1}) = \zeta_{n,x}(D_{n-1}),\end{aligned}$$

where $(*)$ is by property (C). Thus $E_n = \{x \in \mathcal{A}^{\mathbb{Z}} : \zeta_{n,x}(D_{n-1}) < 1\} = F^{-n+1}(E_1)$.

Let $\Sigma \subset \mathcal{A}^{\mathbb{Z}}$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$. We denote $D_n^\Sigma = D_n \cap \Sigma$ and $\partial D_{n+1}^\Sigma = D_{n+1}^\Sigma \setminus D_n^\Sigma$ for all $n \in \mathbb{N}$ and $D_\infty^\Sigma = D_\infty \cap \Sigma$.

*Remark 3.1.* For $\mu$ an $(F, \sigma)$-invariant probability measure such that $\text{supp}(\mu) \subset \Sigma$, we note that, for every $n \in \mathbb{N}$ and $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$, $\text{supp}(\mu_{n,x}) \subset x + D_n^\Sigma \subset \Sigma$ and $\text{supp}(\zeta_{n,x}) \subset D_n^\Sigma$. So for all $n \in \mathbb{N}$ and $d \in \partial D_n$, if $d \notin \Sigma$ one has $\mu(E_{n,d}) = 0$.

LEMMA 3.2. *Let $\mu$ be a $\sigma$-invariant measure on $\mathcal{A}^{\mathbb{Z}}$. If there exists $k \in \mathbb{N}$ such that $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^k)$, then for all $n \geq 1$ one has $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{k^n})$.*

*Proof.* Applying the ergodic decomposition theorem to $(\mathcal{A}^{\mathbb{Z}}, \mathfrak{B}, \mu, \sigma)$, to prove that $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{k^n})$ is equivalent to proving that almost every $\sigma$-ergodic component $\delta$ of $\mu$ is ergodic for $\sigma^{k^n}$. The proof is done by induction.

The base case $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{k^1})$ is true by hypothesis. Let $n \geq 2$ and assume that this property holds for $n - 1$ and does not hold for $n$. That is to say, we consider a $\sigma$-ergodic component $\delta$ of $\mu$ (by induction it is also $\sigma^{k^{n-1}}$-ergodic) which is not $\sigma^{k^n}$-ergodic. There exists $\lambda \in \mathbb{C}$ such that $\lambda^{k^n} = 1$ and $\lambda^{k^{n-1}} \neq 1$ and a non-constant function $h : \mathcal{A}^{\mathbb{Z}} \to \mathbb{C}$ such that $h(\sigma(x)) = \lambda h(x)$ for $\delta$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$. We deduce that $h^k(\sigma(x)) = \lambda^k h^k(x)$ and $h^k(\sigma^{k^{n-1}}(x)) = \lambda^{k^n} h^k(x) = h^k(x)$ for $\delta$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$. By $\sigma^{k^{n-1}}$-ergodicity of $\delta$, $h^k$ is constant $\delta$-almost everywhere, so $\lambda^k = 1$, which is a contradiction. □

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

*Remark 3.2.* If $k$ divides $k'$ then $\mathcal{I}_\mu(\sigma) \subset \mathcal{I}_\mu(\sigma^k) \subset \mathcal{I}_\mu(\sigma^{k'})$. So if $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{k'})$ one also has $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^k)$.

We recall the main theorem.

THEOREM 3.3. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a non-trivial algebraic bipermutative CA, let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$, let $k \in \mathbb{N}$ such that every prime factor of $|\mathcal{A}|$ divides $k$ and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$ with* $\mathrm{supp}(\mu) \subset \Sigma$. *Assume that:*

(1) *$\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action $(F, \sigma)$;*
(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_1})$ with $p_1$ the smallest common period of all elements of* $\mathrm{Ker}(F)$*;*
(3) *$h_\mu(F) > 0$;*
(4) *every $\sigma$-invariant infinite subgroup of $D_\infty^\Sigma(F) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ is dense in $\Sigma$.*

*Then $\mu = \lambda_\Sigma$.*

*Proof.* For all $n \in \mathbb{Z}$, $F$ is bipermutative if and only if $\sigma^n \circ F$ is bipermutative. Since $F$ is non-trivial, by Corollary 2.3, we deduce that $h_\mu(\sigma^n \circ F) > 0$ for all $n \in \mathbb{Z}$. Moreover, $\mu$ is $\sigma$-invariant. So we can assume that the smallest neighborhood of $F$ is $[0, r]$ with $r \in \mathbb{N}$.

CLAIM 1. *For all $n \in \mathbb{N}$, $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_n})$, where $p_n$ is the smallest common $\sigma$-period of $D_n$.*

*Proof.* Let $n \in \mathbb{N}$. Every $x \in D_n$ is a $\sigma$-periodic point of $\sigma$-period $p_n$, so, by bipermutativity, every $y \in F^{-1}(\{x\})$ is $\sigma$-periodic. Since $\sigma^{p_n}(y) \in F^{-1}(\{x\})$, one has that $p_n$ divides the $\sigma$-period of $y$. We deduce that $p_n$ divides $p_{n+1}$. Moreover, there exists $d \in D_1$ such that $\sigma^{p_n}(y) = y + d$, so $\sigma^{|D_1|p_n}(y) = y + |D_1|d = y$. We deduce that $p_{n+1}$ divides $|\mathcal{A}|^r p_n$, because $|D_1| = |\mathcal{A}|^r$. By induction, $p_n$ divides $|\mathcal{A}|^{r(n-1)} p_1$. If $m$ is large enough, then $|\mathcal{A}|^{r(n-1)}$ divides $k^m$, and hence $p_n$ divides $|\mathcal{A}^{r(n-1)} p_1|$ which divides $(kp_1)^m$. Thus, $\mathcal{I}_\mu(\sigma^{kp_n}) = \mathcal{I}_\mu(\sigma)$ by Remark 3.2, because $\mathcal{I}_\mu(\sigma^{(kp_n)^m}) = \mathcal{I}_\mu(\sigma)$ by Lemma 3.2 and hypothesis (2) of Theorem 3.3. ◇

CLAIM 2. *For $n \in \mathbb{N}$ and $d \in D_n$, the measure $T_d(\mathbf{1}_{E_{n,d}}\mu)$ is absolutely continuous with respect to $\mu$.*

*Proof.* Let $A \in \mathfrak{B}$ be such that $\mu(A) = 0$. Since $\mu(A) = \int_{\mathcal{A}^{\mathbb{Z}}} \mu_{n,x}(A)\, d\mu(x)$, we deduce that $\mu_{n,x}(A) = 0$ for $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$. In particular, $0 = \mu_{n,x}(A) \geq \mu_{n,x}(\{x + d\}) = \zeta_{n,x}(\{d\})$, for $\mu$-almost every $x \in T_{-d}(A)$ because $x + d \in A$. Thus $x \notin E_{n,d}$, so $\mu(T_{-d}(A) \cap E_{n,d}) = 0$. This implies that $T_d(\mathbf{1}_{E_{n,d}}\mu)(A) = 0$, so $T_d(\mathbf{1}_{E_{n,d}}\mu)$ is absolutely continuous with respect to $\mu$. ◇

To prove the theorem, we consider $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ with $\mu(\chi) \neq 0$ and we show that $\chi(x) = 1$ for all $x \in \Sigma$. We consider $\Gamma = \{d \in D_\infty^\Sigma : \chi(d) = \chi(\sigma^m(d)), \forall m \in \mathbb{Z}\}$, a $\sigma$-invariant subgroup of $D_\infty^\Sigma$. We want to show that $\Gamma$ is infinite and, hence, dense in $\Sigma$ by hypothesis (4) of Theorem 3.3. From this we will deduce that $\chi$ must be constant.

CLAIM 3. *There exists $N \subset \mathcal{A}^{\mathbb{Z}}$ with $\mu(N) = 1$ and $F(N) = N$ (up to a set of measure zero), satisfying the following property: for any $n \in \mathbb{N}$ and $d \in \partial D_n^\Sigma$, if there exists $x \in E_{n,d} \cap N$ with $\zeta_{n,x}(\chi) \neq 0$, then $d \in \Gamma$.*

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

*Proof.* For $n \in \mathbb{N}$, the function $x \to \zeta_{n,x}$ is $\sigma^{kp_n}$-invariant by Lemma 3.1(c). Since $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_n})$ by Claim 1, we deduce that $\zeta_{n,x}$ is $\sigma$-invariant. So for $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$ and for any $m \in \mathbb{Z}$, we have $\sigma^m \zeta_{n,x} = \zeta_{n,x}$ (†). Since $T_d(\mathbf{1}_{E_{n,d}}\mu)$ is absolutely continuous with respect to $\mu$ by Claim 2, we have $\sigma^m \zeta_{n,x+d} = \zeta_{n,x+d}$ (‡) too, for $\mu$-almost every $x \in E_{n,d}$, for every $d \in D_n$ and for every $m \in \mathbb{Z}$. We can compute

$$T_{-\sigma^m d}\zeta_{n,x} \underset{(\dagger)}{=} T_{-\sigma^m d}\sigma^m \zeta_{n,x} = \sigma^m T_{-d}\zeta_{n,x} \underset{(*)}{=} \sigma^m \zeta_{n,x+d} \underset{(\ddagger)}{=} \zeta_{n,x+d} \underset{(*)}{=} T_{-d}\zeta_{n,x},$$

where (†) and (‡) are as above, and $(*)$ is by Lemma 3.1(a). So $T_{\sigma^m d - d}\zeta_{n,x} = \zeta_{n,x}$ and by integration $(1 - \chi(\sigma^m d - d))\zeta_{n,x}(\chi) = 0$ for $\mu$-almost every $x \in E_{n,d}$. Thus, there exists $N \subset \mathcal{A}^{\mathbb{Z}}$ with $\mu(N) = 1$, such that for all $d \in D_n$ and $x \in E_{n,d} \cap N$, if $\zeta_{n,x}(\chi) \neq 0$, then $\chi(\sigma^m(d))\chi(d)^{-1} = \chi(\sigma^m(d) - d) = 1$. Hence $\chi(\sigma^m(d)) = \chi(d)$ for all $m \in \mathbb{Z}$, which means $d \in \Gamma$. Moreover, the set $N$ is $F$-invariant up to a set of measure zero, because $\mu$ is $F$-invariant. Thus $\mu(F(N)) = F\mu(F(N)) = \mu(F^{-1}(F(N))) \geq \mu(N) = 1$. ◇

CLAIM 4. *There exists $n_0 \in \mathbb{N}$ such that, if we define $B = \{x \in N : \mathbb{E}_\mu(\chi|\mathfrak{B}_n)(x) \neq 0, \forall n \geq n_0\}$, then $\mu(B) > 0$. Moreover, for all $n \geq n_0$, and any $d \in \partial D_n^\Sigma$, if $E_{n,d} \cap B \neq \emptyset$, then $d \in \Gamma$.*

*Proof.* One has $\lim_{n\to\infty} \mathbb{E}_\mu(\chi|\mathfrak{B}_n) = \mathbb{E}_\mu\big(\chi|\bigcap_{m>1}\mathfrak{B}_m\big)$ by the martingale convergence theorem, and this function is not identically zero because its integral is equal to $\mu(\chi) \neq 0$. Thus we can choose $n_0$ such that $B = \{x \in N : \mathbb{E}_\mu(\chi|\mathfrak{B}_n)(x) \neq 0, \forall n \geq n_0\}$ satisfies $\mu(B) > 0$. Moreover, we have

$$\mathbb{E}_\mu(\chi|\mathfrak{B}_n)(x) = \int_{\mathcal{A}^{\mathbb{Z}}} \chi \, d\mu_{n,x} = \chi(x)\zeta_{n,x}(\chi).$$

By Claim 3, for any $n \geq n_0$ and any $d \in \partial D_n^\Sigma$, if there exists $x \in E_{n,d} \cap B$ then $d \in \Gamma$. ◇

CLAIM 5. $\mu(E_1) > 0$.

*Proof.* Let $A \in \mathcal{P}_{[0,r-1]}$. Let $x \in A$ and $d \in D_1$ such that $x + d \in A$. One has $x_{[0,r-1]} = (x+d)_{[0,r-1]}$ and $F(x) = F(x+d)$. By bipermutativity, one deduces that $x = x + d$, that is to say, $d = 0$. Therefore, for any $x \in A$ and for any $d \in \partial D_1$, we have $x + d \notin A$. Thus, $A \cap F^{-1}(\{F(x)\}) = A \cap (x + D_1) = \{x\}$. Thus, (A) implies that $\mathbb{E}_\mu(\mathbf{1}_A|\mathfrak{B}_1)(x) = \mu_{1,x}(A) = \mu_{1,x}(\{x\}) = \eta(x)$. By Lemma 2.1,

$$\begin{aligned}
h_\mu(F) &= H_\mu(\mathcal{P}_{[0,r-1]}|\mathfrak{B}_1)\\
&= -\sum_{A\in\mathcal{P}_{[0,r-1]}} \int_A \log(\mathbb{E}_\mu(\mathbf{1}_A|\mathfrak{B}_1))\, d\mu\\
&= \int_{\mathcal{A}^{\mathbb{Z}}} -\log(\eta(x))\, d\mu(x)\\
&\underset{(*)}{\leq} \int_{E_1} -\log(\eta(x))\, d\mu(x),
\end{aligned}$$

where $(*)$ is because $E_1 = \{x \in \mathcal{A}^{\mathbb{Z}} : \eta(x) < 1\}$. But $h_\mu(F) > 0$ by hypothesis (3) of Theorem 3.3. This proves Claim 5. ◇

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

CLAIM 6. *$\Gamma$ is infinite.*

*Proof.* For $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$ one has

$$\frac{1}{n}\sum_{j=1}^{n+1}\mathbf{1}_{E_j}(x) \underset{(a)}{=} \frac{1}{n}\sum_{j=1}^{n+1}\mathbf{1}_{F^{-j+1}(E_1)}(x) = \frac{1}{n}\sum_{j=0}^{n}\mathbf{1}_{E_1}(F^j(x))$$
$$\underset{(b)}{=} \frac{1}{n^2}\sum_{j,k=0}^{n}\mathbf{1}_{E_1}(\sigma^k F^j(x)) \underset{(c)}{\longrightarrow} \mu(E_1) \underset{(d)}{>} 0.$$

Here, (a) is because $E_j = F^{-j+1}(E_1)$ for all $j \in \mathbb{N}$, (b) is because $E_1$ is $\sigma$-invariant, (c) is the Ergodic theorem and hypothesis (1) of Theorem 3.3 and (d) is by Claim 5.

It follows that, for $\mu$-almost every $x \in \mathcal{A}^{\mathbb{Z}}$, there are infinitely many values of $n > 0$ such that $x \in E_n$. Thus $\mu\big(\bigcap_{m\in\mathbb{N}}\bigcup_{n\geq m} E_n\big) = 1$. Since $\mu(B) > 0$, we deduce that $\mu\big(\bigcap_{m\in\mathbb{N}}\bigcup_{n\geq m} E_n \cap B\big) > 0$. For all $n \in \mathbb{N}$, if $d \notin \mathrm{supp}(\mu) \subset \Sigma$, then Remark 3.1 implies that $\mu(E_{n,d}) = 0$. We can conclude that $\{d \in D_\infty^\Sigma : \exists n \in \mathbb{N}$ such that $d \in \partial D_n$ and $E_{n,d} \cap B \neq \emptyset\}$ is infinite and, by Claim 4, it is a subset of $\Gamma$. Therefore, $\Gamma$ is infinite. ◇

If we consider $\Gamma' = (\mathrm{Id}_{\mathcal{A}^{\mathbb{Z}}} - \sigma)\Gamma$, we have an infinite $\sigma$-invariant subgroup of $D_\infty^\Sigma$ because $\mathrm{Ker}(\mathrm{Id}_{\mathcal{A}^{\mathbb{Z}}} - \sigma)$ is finite. Hypothesis (4) of Theorem 3.3 then implies that $\Gamma'$ is dense in $\Sigma$, but, by construction, $\chi(\Gamma') = \{1\}$, so, by continuity of $\chi$, $\chi(x) = 1$ for all $x \in \Sigma$. Contrapositively, we must have $\mu(\chi) = 0$ for all $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ such that $\chi(\Sigma) \neq \{1\}$. Since $\mathrm{supp}(\mu) \subset \Sigma$, we conclude that $\mu = \lambda_\Sigma$. □

*Remark 3.3.* The proof of Theorem 3.3 works if $(\mathcal{A}^{\mathbb{N}}, F)$ is a right-permutative algebraic CA where all $x \in D_1 = \mathrm{Ker}(F)$ are $\sigma$-periodic, but this last assumption is possible only if $F$ is also left-permutative; therefore, it is a false generalization.

*Remark 3.4.* Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a non-trivial algebraic bipermutative CA and let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$ which verifies hypothesis (4) of Theorem 3.3. Let $c \in \Sigma$ be a $\sigma$-invariant configuration. We define the CA $G = F + c$. Let $\mu$ be a $(G, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$. If $\mu$ verifies the assumptions of Theorem 3.3 for the $\mathbb{N} \times \mathbb{Z}$-action induced by $(G, \sigma)$, then $\mu = \lambda_\Sigma$.

Assumption (4) of Theorem 3.3 becomes more natural when it is replaced by "every $(F, \sigma)$-invariant infinite subgroup of $D_\infty^\Sigma(F) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ is dense in $\Sigma$". It is not clear that this condition is implied by the assumptions of Theorem 3.3. However, if we consider a $\sigma$-ergodic measure we can prove the following theorem.

THEOREM 3.4. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a non-trivial algebraic bipermutative CA, let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$, let $k \in \mathbb{N}$ such that every prime factor of $|\mathcal{A}|$ divides $k$ and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$ with* $\mathrm{supp}(\mu) \subset \Sigma$. *Assume that:*

(1) *$\mu$ is ergodic for $\sigma$;*

(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_1})$ with $p_1$ the smallest common period of all elements of* $\mathrm{Ker}(F)$*;*

(3) *$h_\mu(F) > 0$;*

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

(4) *every $(F,\sigma)$-invariant infinite subgroup of $D^{\Sigma}_{\infty}(F) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ is dense in $\Sigma$.*

*Then $\mu = \lambda_\Sigma$.*

*Proof.* A $\sigma$-ergodic measure is $(F,\sigma)$-ergodic so results from Claim 1 to Claim 6 hold.

CLAIM 7. *Let $B' = \bigcup_{j\in\mathbb{Z}} \sigma^j(\{x \in N : \mathbb{E}_\mu(\chi|\mathfrak{B}_n)(x) \neq 0, \forall n \in \mathbb{N}\})$. Then $\mu(B') = 1$.*

*Proof.* By Claim 4, $\mu(B) > 0$ where $B = \{x \in N : \mathbb{E}_\mu(\chi|\mathfrak{B}_n)(x) \neq 0, \forall n \geq n_0\}$. Thus there exists $k \in [0, 3]$ such that $B_{n_0} = \{x \in N : \Re(\mathbf{i}^k\mathbb{E}_\mu(\chi|\mathfrak{B}_{n_0})) > 0, \forall n \geq n_0\}$ verifies $\mu(B_{n_0}) > 0$, where $\mathbf{i}^2 = -1$. Since $B_{n_0} \in \mathfrak{B}_{n_0} \subset \mathfrak{B}_{n_0-1}$, one has

$$\int_{B_{n_0}} \Re(\mathbf{i}^k\mathbb{E}_\mu(\chi|\mathfrak{B}_{n_0-1}))(x)\, d\mu = \int_{B_{n_0}} \Re(\mathbf{i}^k\mathbb{E}_\mu(\chi|\mathfrak{B}_{n_0})(x))\, d\mu > 0.$$

So $B_{n_0-1} = \{x \in B_{n_0} : \Re(\mathbf{i}^k\mathbb{E}_\mu(\chi|\mathfrak{B}_{n_0-1})(x)) > 0\} = \{x \in N : \Re(\mathbf{i}^k\mathbb{E}_\mu(\chi|\mathfrak{B}_n)(x)) > 0, \forall n \geq n_0 - 1\}$ verifies $\mu(B_{n_0-1}) > 0$. By induction, $\mu(B_0) > 0$, so $\mu(B') > 0$. Since $B'$ is $\sigma$-invariant, $\mu(B') = 1$ by $\sigma$-ergodicity from hypothesis (1) of Theorem 3.4 . ◇

CLAIM 8. *Let $n \in \mathbb{N}$ and let $d \in \partial D^{\Sigma}_n$. If $E_{n,d} \cap B'$ is non-empty then $d \in \Gamma = \{d' \in D^{\Sigma}_{\infty} : \chi(d') = \chi(\sigma^m(d')), \forall m \in \mathbb{Z}\}$.*

*Proof.* Let $d \in \partial D^{\Sigma}_n$ and let $x \in E_{n,d} \cap B'$. There exists $j \in \mathbb{Z}$ such that

$$0 \neq \mathbb{E}_\mu(\chi|\mathfrak{B}_n)(\sigma^j(x)) = \int_{\mathcal{A}^{\mathbb{Z}}} \chi\, d\mu_{n,\sigma^j(x)} = \chi(\sigma^j(x))\zeta_{n,\sigma^j(x)}(\chi) \underset{(*)}{=} \chi(\sigma^j(x))\zeta_{n,x}(\chi).$$

Here $(*)$ is because $x \to \zeta_{n,x}$ is $\sigma^{kp_n}$-invariant by Lemma 3.1(c) and $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_n})$ by Claim 1, so $x \to \zeta_{n,x}$ is $\sigma$-invariant. One deduces that $\zeta_{n,x}(\chi) \neq 0$. But $x \in E_{n,d} \cap N$, so $d \in \Gamma$ by Claim 3. ◇

CLAIM 9. *Let $n \geq 1$ and let $d \in \partial D^{\Sigma}_n$. For $\mu$-almost all $x \in E_{n,d} \cap B'$ one has $F(x) \in E_{n-1,F(d)} \cap B'$.*

*Proof.* Let $d \in \partial D^{\Sigma}_n$ and $x \in E_{n,d} \cap B'$. One has

$$\zeta_{n-1,F(x)}(\{F(d)\}) \underset{(a)}{=} \zeta_{n,x}(F^{-1}(\{F(d)\})) \geq \zeta_{n,x}(\{d\}) \underset{(b)}{>} 0.$$

Here (a) is by Lemma 3.1(b) and (b) is because $x \in E_{n,d}$. We deduce that $F(x) \in E_{n-1,F(d)}$. Since $\mu(B') = 1$ by Claim 7 and $\mu$ is $F$-invariant, one has $\mu\big(\bigcap_{n\in\mathbb{N}} F^{-n}(B')\big) = 1$ so $F(x) \in E_{n-1,F(d)} \cap B'$ for $\mu$-almost all $x \in E_{n,d} \cap B'$. ◇

CLAIM 10. *$\bigcap_{n\in\mathbb{N}} F^{-n}\Gamma$ is infinite.*

*Proof.* Let $n \geq 0$. The set $E_n = F^{-n+1}(E_1)$ is $\sigma$-invariant since $E_1$ is $\sigma$-invariant and $F$ commutes with $\sigma$. Moreover, $\mu(E_n) = \mu(E_1) > 0$ by Claim 5. By $\sigma$-ergodicity (hypothesis (1) of Theorem 3.4), $\mu(E_n) = 1$ so $\mu(E_n \cap B') = 1$ by Claim 7. For all $n \geq 1$, there exists $d_n \in \partial D^{\Sigma}_n$ such that $\mu(E_{n,d_n} \cap B') > 0$, and thus, by Claim 9, $\mu(E_{n-k,F^k(d_n)} \cap B') > 0$ for all $k \in [0, n]$. That is to say, $F^k(d_n) \in \Gamma$ for $k \in [0, n]$ by Claim 8. One deduces that $\bigcap_{n\in\mathbb{N}} F^{-n}\Gamma$ is infinite since it contains $d_n$ for all $n \in \mathbb{N}$. ◇

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

If we consider $\Gamma'' = (\mathrm{Id}_{\mathcal{A}^{\mathbb{Z}}} - \sigma)\big(\bigcap_{n\in\mathbb{N}} F^{-n}\Gamma\big)$, we have an infinite $(F, \sigma)$-invariant subgroup of $D_\infty^\Sigma$ because $\mathrm{Ker}(\mathrm{Id}_{\mathcal{A}^{\mathbb{Z}}} - \sigma)$ is finite. We deduce that $\Gamma''$ is dense in $\Sigma$ by condition (4) of Theorem 3.4, but $\chi(\Gamma'') = \{1\}$ by construction, so, by continuity of $\chi$, $\chi(x) = 1$ for all $x \in \Sigma$. Contrapositively, we must have $\mu(\chi) = 0$ for all $\chi \in \widehat{\mathcal{A}^{\mathbb{Z}}}$ such that $\chi(\Sigma) \neq \{1\}$. Since $\mathrm{supp}(\mu) \subset \Sigma$, we conclude that $\mu = \lambda_\Sigma$. □

COROLLARY 3.5. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an algebraic bipermutative CA. Let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$ such that there exists $\pi : \mathcal{A}^{\mathbb{Z}} \to \Sigma$, a surjective continuous morphism which commutes with $F$ and $\sigma$ ($(\Sigma, \sigma, F)$ is a dynamical and algebraic factor of $(\mathcal{A}^{\mathbb{Z}}, \sigma, F)$). Let $k \in \mathbb{N}$ be such that every prime factor of $|\mathcal{A}|$ divides $k$. Let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$. Assume that:*

(1) *$\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action $(F, \sigma)$;*
(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{kp_1})$ with $p_1$ the smallest common period of all elements of* $\mathrm{Ker}(F)$*;*
(3) *$h_{\pi\mu}(F) > 0$;*
(4) *every $\sigma$-invariant infinite subgroup of $D_\infty^\Sigma = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ is dense in $\Sigma$.*

*Then $\pi\mu = \lambda_\Sigma$.*

## 4. *A discussion about the assumptions*

Comparing the assumptions of Theorems 3.3 and 3.4 with those of Theorems 1.1, 1.2 and 1.3 is not completely obvious. Already Theorems 3.3 and 3.4 consider bipermutative algebraic CAs without restriction on the neighborhood. In this section, we discuss the assumptions of these theorems and show that Theorems 3.3 and 3.4 generalize Theorems 1.2 and 1.3 but the ergodic assumptions cannot be compared with those of Theorem 1.1.

### 4.1. *Class of CAs considered.*

Theorems 3.3 and 3.4 consider algebraic bipermutative CAs without restriction on the neighborhood. The bipermutativity is principally used to prove the entropy formula of Lemma 2.1. We can hope that such a formula exists for expansive CAs . Section 4.3 gives a result in this direction. The next proposition shows that considering algebraic CAs or the restriction of a linear CA is equivalent.

PROPOSITION 4.1. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift and let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an algebraic CA. There exist a linear CA, $(\mathcal{B}^{\mathbb{Z}}, G)$, and a $\sigma_{\mathcal{B}^{\mathbb{Z}}}$-invariant subgroup of $\mathcal{B}^{\mathbb{Z}}$, $\Gamma$, such that $(\mathcal{A}^{\mathbb{Z}}, \sigma, F)$ is isomorphic to $(\Gamma, \sigma_{\mathcal{B}^{\mathbb{Z}}}, G)$ in both the dynamical and algebraical sense.*

*Proof.* Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an algebraic CA. By Kitchens [**Kit87**, Proposition 2], there exists a finite abelian group, $\mathcal{B}'$, a Markov subgroup of $\mathcal{B}'^{\mathbb{Z}}$, $\Gamma$, and a continuous group isomorphism, $\varphi$, such that $\varphi \circ \sigma = \sigma_{\mathcal{B}'^{\mathbb{Z}}} \circ \varphi$. Define $G' = \varphi \circ F \circ \varphi^{-1}$. One has the following commutative diagram:

$$\begin{array}{ccc} \mathcal{A}^{\mathbb{Z}} & \xrightarrow{\sigma, F} & \mathcal{A}^{\mathbb{Z}} \\ \downarrow \varphi & & \downarrow \varphi \\ \Gamma & \xrightarrow{\sigma_{\mathcal{B}'^{\mathbb{Z}}}, G'} & \Gamma \end{array} \qquad \begin{array}{c} \varphi \circ \sigma = \sigma_{\mathcal{B}'^{\mathbb{Z}}} \circ \varphi \\ \varphi \circ F = G' \circ \varphi \end{array}$$

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

$G'$ is continuous and commutes with $\sigma_{\mathcal{B}'^{\mathbb{Z}}}$, so it is a CA on $\Gamma'$. We want to extend $G'$ to obtain a linear CA. By Hedlund [**Hed69**], there exist a neighborhood $\mathbb{U}$, a subgroup of $\mathcal{B}'^{\mathbb{U}}$, $H$, and a local function $\overline{G'} : H \to \mathcal{B}'$ which define $G'$. Moreover, by linearity, $\overline{G'}$ is a group morphism. If we could extend $\overline{G'}$ to a morphism from $\mathcal{B}^{\mathbb{U}}$ to $\mathcal{B}$ (where $\mathcal{B}'$ is a subgroup of $\mathcal{B}$), we would obtain the local rule of a linear CA.

There exist $d, k \in \mathbb{N}$ such that $\mathcal{B}'$ can be viewed as a subgroup of $(\mathbb{Z}/d\mathbb{Z})^k$. If $\mathcal{B} = (\mathbb{Z}/d\mathbb{Z})^k$, then $H$ can be viewed as a subgroup of $\mathcal{B}^{\mathbb{U}}$. By the fundamental theorem of finitely generated abelian groups [**Lan02**, Theorem 7.8], there exist $e_1, \ldots, e_{k|\mathbb{U}|}$, a basis of $\mathcal{B}^{\mathbb{U}}$, and $a_1, \ldots, a_{k|\mathbb{U}|} \in \mathbb{N}$ such that $\mathcal{B}^{\mathbb{U}} = \bigoplus_i \langle e_i \rangle$ and $H = \bigoplus_i \langle a_i e_i \rangle$. For all $i \in [1, k|\mathbb{U}|]$, there exist $f_i \in \mathcal{B}$ such that $\overline{G'}(a_i e_i) = a_i f_i$ because the order of $\overline{G'}(a_i e_i)$ is at most $d/a_i$. We define the morphism $\overline{G} : \mathcal{B}^{\mathbb{U}} \to \mathcal{B}$ by $\overline{G}(e_i) = f_i$ for all $i \in [1, k|\mathbb{U}|]$. $\overline{G}$ defines a linear CA on $\mathcal{B}^{\mathbb{Z}}$ denoted $G$ whose restriction is $(\Gamma, G')$. □

*Remark 4.1.* The study of algebraic CAs can be restricted to the study of the restriction of linear CAs to Markov subgroups.

Since we consider $\sigma$-invariant measures, we can assume that the neighborhood of the CA is $\mathbb{U} = [0, r]$. Moreover, it is easy to show the next proposition and consider CAs of the neighborhood $\mathbb{U} = [0, 1]$.

PROPOSITION 4.2. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a CA of neighborhood $\mathbb{U} = [0, r]$. There is a CA $((\mathcal{A}^r)^{\mathbb{Z}}, G)$ of the neighborhood $\mathbb{U} = [0, 1]$ so that the topological system $(\mathcal{A}^{\mathbb{Z}}, F)$ is isomorphic to the system $((\mathcal{A}^r)^{\mathbb{Z}}, G)$ via the conjugacy*

$$\phi_r : (x_i)_{i\in\mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}} \to ((x_{[ri,ri+r-1]})_{i\in\mathbb{Z}}) \in (\mathcal{A}^r)^{\mathbb{Z}}.$$

*Furthermore, one has*

$$(\mathcal{A}^{\mathbb{Z}}, F) \text{ is bipermutative} \iff ((\mathcal{A}^r)^{\mathbb{Z}}, G) \text{ is bipermutative},$$
$$(\mathcal{A}^{\mathbb{Z}}, F) \text{ is algebraic} \iff ((\mathcal{A}^r)^{\mathbb{Z}}, G) \text{ is algebraic},$$
$$(\mathcal{A}^{\mathbb{Z}}, F) \text{ is linear} \iff ((\mathcal{A}^r)^{\mathbb{Z}}, G) \text{ is linear}.$$

If $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ is $\sigma$-totally ergodic then $\phi_r\mu \in \mathcal{M}((\mathcal{A}^r)^{\mathbb{Z}})$ is $\sigma_{(\mathcal{A}^r)^{\mathbb{Z}}}$-totally ergodic. Moreover, by conjugacy, $h_\mu(F) > 0$ is equivalent to $h_{\phi_r\mu}(G) > 0$. So, as suggested in [**Piv05**], Theorem 1.3 holds for algebraic bipermutative CAs without any restriction on the neighborhood.

COROLLARY 4.3. *Let $\mathcal{A}^{\mathbb{Z}}$ be any abelian group shift, let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an algebraic bipermutative CA (without restriction on the neighborhood) and let $\mu$ be an $(F, \sigma)$-invariant probability measure. Assume that:*

(1) *$\mu$ is totally ergodic for $\sigma$;*
(2) *$h_\mu(F) > 0$;*
(3) *$\mathrm{Ker}(F)$ contains no non-trivial $\sigma$-invariant subgroups.*

*Then $\mu = \lambda_{\mathcal{A}^{\mathbb{Z}}}$.*

*Remark 4.2.* The correspondence holds only if $\mu$ is supposed to be $\sigma$-totally ergodic. Indeed if $\mu$ is $\sigma$-ergodic, $\phi_r\mu$ is not necessarily $\sigma_{(\mathcal{A}^r)^{\mathbb{Z}}}$-ergodic.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

4.2. *Ergodicity of action.* Assumption (1) of Theorem 3.3 characterizes the ergodicity of the action $(F, \sigma)$ on the measure space $(\mathcal{A}^{\mathbb{Z}}, \mathfrak{B}, \mu)$. Since we want to characterize $(F, \sigma)$-invariant measures, it is natural to assume that $\mu$ is $(F, \sigma)$-ergodic because every $(F, \sigma)$-invariant measure can be decomposed into $(F, \sigma)$-ergodic components. The following relations are easy to check for an $(F, \sigma)$-invariant probability measure $\mu$:

$$\mu \text{ is } (F, \sigma)\text{-totally ergodic} \Rightarrow \mu \text{ is } \sigma\text{-totally ergodic}$$
$$\Rightarrow \mu \text{ is } \sigma\text{-ergodic} \Rightarrow \mu \text{ is } (F, \sigma)\text{-ergodic;}$$
$$\mu \text{ is } \sigma\text{-totally ergodic} \Rightarrow \mu \text{ is } (F, \sigma)\text{-ergodic} \quad \text{and} \quad \mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^k) \text{ for every } k \geq 1.$$

Thus, hypothesis (1) of Theorem 1.3 implies hypothesis (1) and (2) of Theorem 3.4 which imply hypothesis (1) and (2) of Theorem 3.3. However, we note that the ergodicity assumption (1) of Theorem 1.1 cannot be compared with hypotheses (1) and (2) of Theorem 3.3. Indeed, there are probability measures which are $(F, \sigma)$-ergodic with $\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^k)$ for some $k \geq 1$ which are not $\sigma$-ergodic. Conversely, there exist probability measures which are $\sigma$-ergodic with $\mathcal{I}_\mu(\sigma) \neq \mathcal{I}_\mu(\sigma^k)$ for some $k \geq 1$.

Moreover, if $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$ and $F = a\,\mathrm{Id} + b\,\sigma$ on $\mathcal{A}^{\mathbb{Z}}$ then $p - 1$ is a multiple of the common period of every element of $\mathrm{Ker}(F)$. So the spectrum assumption (2) of Theorem 1.2 implies hypothesis (2) of Theorems 3.3 and 3.4. For Theorem 1.3 the total ergodicity of $\mu$ under $\sigma$ is required. This property does not seem to be very far from hypothesis (2) of Theorems 3.3 and 3.4. But condition (2) of Theorems 3.3 and 3.4 (concerning the $\sigma$-invariant set) shows the importance of the algebraic characteristic of the system. The property of $(F, \sigma)$-total ergodicity of $\mu$ is more restrictive. With such an assumption, Einsiedler [**Ein05**] has proven rigidity results for a class of algebraic actions that are not necessarily CAs. To finish, the next example shows that assumption (2) of Theorems 3.3 and 3.4 is necessary to obtain the characterization of the uniform Bernoulli measure.

*Example 4.3.* Let $\mathcal{A} = \mathbb{Z}/2\mathbb{Z}$ and $F = \mathrm{Id} + \sigma$ on $\mathcal{A}^{\mathbb{Z}}$. We consider the subgroup $X_1 = \{x \in \mathcal{A}^{\mathbb{Z}} : x_{2n} = x_{2n+1}, \forall n \in \mathbb{Z}\}$, which is neither $\sigma$-invariant nor $F$-invariant. Let $X_2 = \sigma(X_1) = \{x \in \mathcal{A}^{\mathbb{Z}} : x_{2n} = x_{2n-1}, \forall n \in \mathbb{Z}\}$, $X_3 = F(X_1) = \{x \in \mathcal{A}^{\mathbb{Z}} : x_{2n} = 0, \forall n \in \mathbb{Z}\}$ and $X_4 = F(X_2) = \{x \in \mathcal{A}^{\mathbb{Z}} : x_{2n+1} = 0, \forall n \in \mathbb{Z}\}$. The set $X = X_1 \cup X_2 \cup X_3 \cup X_4$ is $(F, \sigma)$-invariant. Let $\nu$ be the Haar measure on $X_1$. We consider $\mu = \frac{1}{4}(\nu + \sigma\nu + F\nu + F\sigma\nu)$. It is easy to verify that $\mu$ is an $(F, \sigma)$-ergodic measure such that $h_\mu(\sigma) > 0$. However, $X_i \in \mathcal{I}_\mu(\sigma^2) \setminus \mathcal{I}_\mu(\sigma)$ for all $i \in [1, 4]$, and hence hypothesis (2) of Theorem 3.3 is false, so we cannot apply Theorem 3.3 and $\mu$ it is not the uniform Bernoulli measure. Silberger proposes similar constructions in [**Sil05**].

4.3. *Positive entropy.* Corollary 2.3 shows that for a non-trivial bipermutative CA, $(\mathcal{A}^{\mathbb{Z}}, F)$, the assumption of positive entropy of $F$ can be replaced by the positive entropy of $F^n \circ \sigma^m$ for some $(n, m) \in \mathbb{N} \times \mathbb{Z}$. Therefore, the positive entropy hypothesis (3) of Theorems 3.3 and 3.4 can be replaced by the positive entropy of the action $(F, \sigma)$ in some given direction. We can find this type of assumption in [**Ein05**].

We can also expect a similar formula for an expansive CA $F$ but in this case we have the inequality $h_\mu(F) > 0$ if and only if $h_\mu(\sigma) > 0$. To begin, we show an inequality for a general CA.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

PROPOSITION 4.4. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a CA of the neighborhood $\mathbb{U} = [r, s] \ni 0$ (not necessarily the smallest possible one) and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$. Then $h_\mu(F) \le (r - s)\, h_\mu(\sigma)$.*

*Proof.* By definition, for $N \in \mathbb{N}$, $l \in \mathbb{N}$ and $x \in \mathcal{A}^{\mathbb{Z}}$, the knowledge of $x_{[rN-l,sN+l]}$ determines $(F^n(x)_{[-l,l]})_{n\in[0,N]}$. This means that $\mathcal{P}_{[rN-l,sN+l]}$ is a refinement of $\bigvee_{n=0}^{N} F^{-n}(\mathcal{P}_{[-l,l]})$. So for $l \ge \max(s, -r)$ we have

$$\begin{aligned} h_\mu(F, \mathcal{P}_{[-l,l]}) &= \lim_{N\to\infty} \frac{1}{N} H_\mu\left(\bigvee_{n=0}^{N} F^{-n}(\mathcal{P}_{[-l,l]})\right) \\ &\le \lim_{N\to\infty} \frac{1}{N} H_\mu(\mathcal{P}_{[rN-l,Ns+l]}) \\ &= \lim_{N\to\infty} -\frac{N(s-r)+2l}{N} \frac{1}{N(s-r)+2l} \sum_{u\in\mathcal{A}^{N(s-r)+2l}} \mu([u]) \log(\mu[u]) \\ &= (s-r)\, h_\mu(\sigma). \end{aligned}$$

We deduce that $h_\mu(F) = \lim_{l\to\infty} h_\mu(F, \mathcal{P}_{[-l,l]}) \le (s - r)\, h_\mu(\sigma)$. □

Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a positively expansive CA. There exists $r_e$, the *constant of expansivity*, such that, for all $x, y \in \mathcal{A}^{\mathbb{Z}}$, if $x \ne y$ there exists $n \in \mathbb{N}$ which verifies $F^n(x)_{[-r_e,r_e]} \ne F^n(y)_{[-r_e,r_e]}$. Then $(\mathcal{A}^{\mathbb{Z}}, F)$ is topologically conjugate to the one-sided subshift $(S_F, \sigma)$, where $S_F \subset \mathcal{B}^{\mathbb{N}}$, with $\mathcal{B} = \mathcal{A}^{2r_e+1}$, and where $S_F = \{(F^i(x)_{[-r_e,r_e]})_{i\in\mathbb{N}} : x \in \mathcal{A}^{\mathbb{Z}}\}$, via the conjugacy $\phi_F : x \in \mathcal{A}^{\mathbb{Z}} \to (F^i(x)_{[-r_e,r_e]})_{i\in\mathbb{N}} \in S_F$. Define $F_T : S_F \to S_F$ by $F_T \circ \phi_F(x) = \phi_F \circ \sigma^{r_e}(x)$ for every $x \in \mathcal{A}^{\mathbb{Z}}$. $(S_F, F_T)$ is an invertible one-sided CA. Define the *radius of expansivity* $r_T = \max\{r(F_T), r(F_T^{-1})\}$.

PROPOSITION 4.5. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a positively expansive CA and $\mu$ an $(F, \sigma)$-invariant probability measure, then $h_\mu(F) \ge (1/r_T) h_\mu(\sigma)$.*

*Proof.* By definition of $r_T$, for $N \in \mathbb{N}$, $l \ge r_e$ and $x \in \mathcal{A}^{\mathbb{Z}}$, the knowledge of $(F^n(x)_{[-l,l]})_{n\in[0,r_T N]}$ implies the knowledge of $x_{[-N-l,N+l]}$. This means that $\bigvee_{n=0}^{r_T N} F^{-n}(\mathcal{P}_{[-l,l]})$ is a refinement of $\mathcal{P}_{[-N-l,N+l]}$. A computation similar to that in the previous proof shows that $r_T\, h_\mu(F) \ge h_\mu(\sigma)$. □

This result can be viewed as a rigidity result. Indeed, for an expansive CA $(\mathcal{A}^{\mathbb{Z}}, F)$, the measure entropy of $F$ and $\sigma$ are linked for an $(F, \sigma)$-invariant measure. This is a first step in the research of Lyapunov exponents for expansive CAs [**Tis00**].

4.4. *$(F, \sigma)$-invariant subgroups of $D_\infty$.* Now let us discuss assumption (4) of Theorems 3.3 and 3.4 which is an algebraic condition on the CAs. We can remark that Theorems 1.1 and 1.2 have no such assumption because they concern a particular class of CAs which verifies this assumption: $F = a\,\mathrm{Id} + b\,\sigma$ on $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}$ with $p$ prime. By Proposition 4.2 it is easy to modify the proof of Theorem 1.3 to consider non-trivial algebraic bipermutative CAs without restriction on the neighborhood (Corollary 4.3). However, it is necessary to compare the assumption "Ker$(F)$ contains no non-trivial $\sigma$-invariant subgroups" with "every $\sigma$-invariant infinite subgroup of $D_\infty$ is dense in $\mathcal{A}^{\mathbb{Z}}$".

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

We show that the second property is more general and give in §5.1 a general class of examples where it is the case.

If $H \subset \mathcal{A}^{\mathbb{Z}}$, denote by $\langle H \rangle$ the subgroup generated by $H$, by $\langle H \rangle_\sigma$ the smallest $\sigma$-invariant subgroup which contains $H$ and by $\langle H \rangle_{F,\sigma}$ the smallest $(F, \sigma)$-invariant subgroup which contains $H$. Let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup. If $H \subset \Sigma$, then we note that $\langle H \rangle$, $\langle H \rangle_\sigma$ and $\langle H \rangle_{F,\sigma}$ are subgroups of $\Sigma$.

PROPOSITION 4.6. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be an algebraic CA and let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$. The following propositions are equivalent.*

(1) *$D_\infty^\Sigma$ contains no non-trivial $(F, \sigma)$-invariant infinite subgroups.*

(2) *There exist $m \in \mathbb{N}$ and $n_0 \geq 0$ such that $D_{n_0}^\Sigma \subset \langle d \rangle_{F,\sigma}$ for all $d \in \partial D_{n_0+m}^\Sigma$.*

(3) *There exists $m \in \mathbb{N}$ such that $D_{n_0}^\Sigma \subset \langle d \rangle_{F,\sigma}$ for all $n_0 \in \mathbb{N}^*$ and $d \in \partial D_{n_0+m}^\Sigma$.*

(4) *There exists $m \in \mathbb{N}$ such that $D_1^\Sigma \subset \langle d \rangle_{F,\sigma}$ for all $d \in \partial D_{m+1}^\Sigma$.*

*Proof.* (2) $\Rightarrow$ (1) Let $\Gamma$ be an $(F, \sigma)$-invariant infinite subgroup of $D_\infty^\Sigma$. We prove by induction that $D_n^\Sigma \subset \Gamma$ for all $n \geq n_0$. Since $\Gamma$ is infinite and $D_n^\Sigma$ is finite for all $n \in \mathbb{N}$, we deduce that there exists $n' \geq 0$ such that there exists $d \in \Gamma \cap \partial D_{n'+n_0+m}^\Sigma$. By $F$-invariance of $\Gamma$ we have $F^{n'}(d) \in \Gamma \cap \partial D_{n_0+m}^\Sigma$, and thus $D_{n_0}^\Sigma \subset \langle F^{n'}(d) \rangle_{F,\sigma} \subset \Gamma$.

Let $n \geq n_0$ and assume that $D_n^\Sigma \subset \Gamma$. We want to show that $D_{n+1}^\Sigma \subset \Gamma$. As before, since $\Gamma$ is infinite and $F$-invariant we can find $d \in \Gamma \cap \partial D_{n+1+m}^\Sigma$. From $F^{n+1-n_0}(d) \in \Gamma \cap \partial D_{n_0+m}^\Sigma$, we deduce $D_{n_0}^\Sigma \subset \langle F^{n+1-n_0}(d) \rangle_{F,\sigma}$. Let $d' \in D_{n+1}^\Sigma$. Then $F^{n+1-n_0}(d') \in D_{n_0}^\Sigma \subset \langle F^{n+1-n_0}(d) \rangle_{F,\sigma}$ and consequently there exists a finite subset $\mathbb{V} \subset \mathbb{Z} \times \mathbb{N}$ such that $F^{n+1-n_0}(d') = \sum_{(u,m') \in \mathbb{V}} c_{u,m'} \sigma^u \circ F^{m'+n+1-n_0}(d)$ where $c_{u,m'} \in \mathbb{Z}$. We deduce that $d' - \sum_{(u,m') \in \mathbb{V}} c_{u,m'} \sigma^u \circ F^{m'}(d) \in D_{n+1-n_0}^\Sigma \subset D_n^\Sigma \subset \Gamma$. But $d \in \Gamma$, so $\sigma^n \circ F^{m'} \in \Gamma$ for all $(n, m') \in \mathbb{V}$. Thus, $d' \in \Gamma$. This holds for any $d' \in D_{n+1}^\Sigma$. Thus, $D_{n+1}^\Sigma \subset \Gamma$. By induction, $D_k^\Sigma \subset \Gamma$ for all $k \in \mathbb{N}$. Finally, $D_\infty^\Sigma = \bigcup_{n \in \mathbb{N}} D_n^\Sigma \subset \Gamma$.

(1) $\Rightarrow$ (4) By contradiction, we assume that for all $m \in \mathbb{N}$ there exists $d \in \partial D_{m+1}^\Sigma$ such that $\langle d \rangle_{F,\sigma} \cap D_1^\Sigma \neq D_1^\Sigma$. Since $D_1^\Sigma$ is a finite group there exists a strict subgroup $H$ of $D_1^\Sigma$ such that $\Delta = \{d \in D_\infty^\Sigma | \langle d \rangle_{F,\sigma} \cap D_1^\Sigma \subset H\}$ is infinite. Observe that $F(\Delta) \subset \Delta$. For all $d' \in \Delta$ we denote $\Delta_{d'} = \{d \in \Delta | d' \in \langle d \rangle_{F,\sigma}\}$. Let $(n_i)_{i \in \mathbb{N}}$ be an increasing sequence such that $\Delta \cap \partial D_{n_i}^\Sigma \neq \emptyset$. If $d \in \Delta \cap \partial D_{n_{i+1}}^\Sigma$, we have $d' = F^{n_{i+1}-n_i}(d) \in \langle d \rangle_{F,\sigma}$, so that $d \in \Delta_{d'}$, and also $d' \in \Delta \cap \partial D_{n_i}^\Sigma$. So we can construct by induction an infinite sequence $(d_i)_{i \in \mathbb{N}}$ of $D_\infty^\Sigma$ such that $d_i \in \Delta \cap \partial D_{n_i}^\Sigma$ and $d_{i+1} \in \Delta_{d_i}$ for all $i \in \mathbb{N}$. Thus $\Gamma = \bigcup_{i \in \mathbb{N}} \langle d_i \rangle_{F,\sigma}$ is an infinite $(F, \sigma)$-invariant subgroup of $D_\infty^\Sigma$ such that $\Gamma \cap D_1^\Sigma \subset H$, which contradicts (1).

(4) $\Rightarrow$ (3) Let $m \in \mathbb{N}$ such that $D_1^\Sigma \subset \langle d \rangle_{F,\sigma}$ for all $d \in \partial D_{m+1}^\Sigma$. We prove by induction that for all $n \geq 1$ and $d \in \partial D_{n+m}^\Sigma$ one has $D_n^\Sigma \subset \langle d \rangle_{F,\sigma}$. For $n = 1$ it is the assumption. Assume that the property is true for $n \in \mathbb{N}^*$. Let $d \in \partial D_{n+1+m}^\Sigma$; since $F^n(d) \in \partial D_{m+1}^\Sigma$, one has $D_1^\Sigma \subset \langle F^n(d) \rangle_{F,\sigma}$. If $d' \in D_{n+1}^\Sigma$, then $F^n(d') \in D_1^\Sigma$ and we deduce the existence of $\mathbb{V} \subset \mathbb{Z} \times \mathbb{N}$ such that $F^n(d') = \sum_{(u,m') \in \mathbb{V}} c_{u,m'} \sigma^u \circ F^{m'+n}(d)$ where $c_{u,m'} \in \mathbb{Z}$. From $d' - \sum_{(u,m') \in \mathbb{V}} c_{u,m'} \sigma^u \circ F^{m'}(d) \in D_n^\Sigma$ and from the fact that $D_n^\Sigma \subset \langle F(d) \rangle_{F,\sigma}$ because $F(d) \in \partial D_{n+m}^\Sigma$, we deduce that $d' - \sum_{(u,m') \in \mathbb{V}} c_{u,m'} \sigma^u \circ F^{m'}(d) \in \langle F(d) \rangle_{F,\sigma} \subset \langle d \rangle_{F,\sigma}$. Thus, $d' \in \langle d \rangle_{F,\sigma}$. One can then deduce that $D_{n+1}^\Sigma \subset \langle d \rangle_{F,\sigma}$.

(3) $\Rightarrow$ (2) is trivial. □

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

COROLLARY 4.7. *If $D_1^\Sigma = \mathrm{Ker}(F) \cap \Sigma$ contains no non-trivial $\sigma$-invariant subgroups then $D_\infty^\Sigma$ contains no non-trivial $(F, \sigma)$-invariant infinite subgroups.*

*Proof.* If $D_1^\Sigma = \mathrm{Ker}(F) \cap \Sigma$ contains no non-trivial $\sigma$-invariant subgroups, for all $d \in \partial D_1^\Sigma$, the subgroup $\langle d\rangle_{F,\sigma}$ must be equal to $D_1^\Sigma$. By Proposition 4.6, one can deduce that $D_\infty^\Sigma$ contains no non-trivial $(F, \sigma)$-invariant infinite subgroups. □

For a linear CA $(\mathcal{A}^\mathbb{Z}, F)$ where $\mathcal{A} = \mathbb{Z}/n\mathbb{Z}$, the $\sigma$-invariant subgroups coincide with the $(F, \sigma)$-invariant subgroups. From Corollary 4.7 we get directly that Theorem 3.3 is stronger than Theorem 1.3 in this case. Moreover, if we consider the case of Theorem 1.2, that is to say, that $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$ with $p$ prime and $F = a\,\mathrm{Id} + b\,\sigma$ with $a \neq 0$ and $b \neq 0$, then $\mathrm{Ker}(F) \simeq \mathbb{Z}/p\mathbb{Z}$ does not contain non-trivial $\sigma$-invariant subgroups. So Theorem 3.3 also generalizes Theorem 1.2.

When $\mathcal{A}$ is not cyclic, the $\sigma$-invariant subgroups do not necessarily coincide with the $(F, \sigma)$-invariant subgroups. In this case we do not know if Theorem 3.3 implies Theorem 1.3. However, Corollary 4.7 implies that Theorem 3.4 is stronger than Theorem 1.3 for every algebraic bipermutative CA.

## 5. *Extensions to some linear CAs*

5.1. *The case $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$.* Theorem 1.2 concerns linear CAs on $(\mathbb{Z}/p\mathbb{Z})^\mathbb{Z}$ of smallest neighborhood $\mathbb{U} = [0, 1]$. We will show that this implies the fourth assumption of Theorem 3.3. In fact, we can show that the fourth assumption is directly implied when we consider a non-trivial linear CA on $(\mathbb{Z}/p\mathbb{Z})^\mathbb{Z}$. This allows us to prove the following result.

PROPOSITION 5.1. *Let $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$, let $(\mathcal{A}^\mathbb{Z}, F)$ be a non-trivial linear CA with $p$ prime and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^\mathbb{Z}$. Assume that:*

(1) *$\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action $(F, \sigma)$;*

(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{p\,p_1})$ with $k \in \mathbb{N}^*$ and $p_1$ the smallest common period of all elements of* $\mathrm{Ker}(F)$*;*

(3) $h_\mu(F) > 0$.

*Then:*

(a) $\mu = \lambda_{\mathcal{A}^\mathbb{Z}}$*;*

(b) *moreover, $p_1$ divides $\prod_{i=0}^{r-1}(p^r - p^i)$ where $r = \max\{\mathbb{U}, 0\} - \min\{\mathbb{U}, 0\}$ and $\mathbb{U}$ is the smallest neighborhood of $F$.*

*Proof.* Proof of (a): By $(F, \sigma)$-invariance of $\mu$, we can compose $F$ with $\sigma$ and assume that the smallest neighborhood of $F$ is $[0, r]$ with $r \in \mathbb{N} \setminus \{0\}$. So $F = \sum_{u\in[0,r]} f_u \circ \sigma^u = P_F(\sigma)$ where $P_F$ is a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ with $f_0 \neq 0$ and $f_r \neq 0$. We remark that $F$ is bipermutative.

Case 1: First we assume that $P_F$ is irreducible on $\mathbb{Z}/p\mathbb{Z}$. We can view $D_1(F)$ as a $\mathbb{Z}/p\mathbb{Z}$ vector space and consider the isomorphism $\sigma_1 : D_1(F) \to D_1(F)$, the restriction of $\sigma$ at the subgroup $D_1(F)$. By bipermutativity of $F$, $D_1 \simeq (\mathbb{Z}/p\mathbb{Z})^r$. Moreover, $P_F(\sigma_1) = 0$; since $P_F$ is irreducible and its degree is equal to the dimension of $D_1$, we deduce that $P_F$ is the characteristic polynomial of $\sigma_1$. Since $P_F$ is irreducible, $D_1(F)$ is $\sigma_1$-simple, so $D_1(F)$ contains no non-trivial $\sigma$-invariant subgroups, see [**AB93**, §VI.8] for further details.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

By Corollary 4.7, $D_\infty(F)$ also contains no non-trivial $(F, \sigma)$-invariant infinite subgroup, so hypothesis (4) of Theorem 3.3 is verified.

Case 2: Now we assume that $P_F = P^\alpha$ where $P$ is irreducible on $\mathbb{Z}/p\mathbb{Z}$ and $\alpha \in \mathbb{N}$. We have $D_n(P_F(\sigma)) = \mathrm{Ker}(P^{\alpha n}(\sigma)) = D_{\alpha n}(P(\sigma))$ for all $n \in \mathbb{N}$. So $D_\infty(P_F(\sigma)) = D_\infty(P(\sigma))$. Now we are in the previous case and the fourth condition of Theorem 3.3 is verified.

Case 3: In the general case, $P_F = P_1^{\alpha_1} \ldots P_l^{\alpha_l}$ where $P_i$ is irreducible and $\alpha_i \in \mathbb{N}$ for all $i \in [1, l]$. Let $\Gamma$ be an $(F, \sigma)$-invariant infinite subgroup of $D_\infty(P_F(\sigma))$. By the kernel decomposition Lemma [**AB93**, §VI.4], we have $D_n(P_F(\sigma)) = D_n(P_1^{\alpha_1}(\sigma)) \oplus \cdots \oplus D_n(P_l^{\alpha_l}(\sigma))$ for every $n \in \mathbb{N}$. Moreover, $D_n(P_F(\sigma)) \cap \Gamma$ is a $\sigma$-invariant subspace of $D_n(P_F(\sigma))$ considered as a $\mathbb{Z}/p\mathbb{Z}$-vector space and $D_n(P_F(\sigma)) \cap \Gamma = (D_n(P_1^{\alpha_1}(\sigma)) \cap \Gamma) \oplus \cdots \oplus (D_n(P_l^{\alpha_l}(\sigma)) \cap \Gamma)$. We deduce that

$$D_\infty(P_F(\sigma)) \cap \Gamma = \bigoplus_{i \in [1,l]} (D_\infty(P_i^{\alpha_1}(\sigma)) \cap \Gamma) \underset{(*)}{=} \bigoplus_{i \in [1,l]} (D_\infty(P_i(\sigma)) \cap \Gamma),$$

where $(*)$ follows as in Case 2. There exists $i \in [1, l]$ such that $\Gamma \cap D_\infty(P_i(\sigma))$ is an infinite subgroup. By Case 1, one has $\Gamma \cap D_\infty(P_i(\sigma)) = D_\infty(P_i(\sigma))$, so $D_\infty(P_i(\sigma)) \subset \Gamma$. We deduce that $\Gamma$ is dense, because $D_\infty(P_i(\sigma))$ is dense, because $P_i(\sigma)$ is bipermutative. Thus the fourth condition of Theorem 3.3 is verified and part (a) of the proposition follows.

Proof of (b): If $x \in \mathrm{Ker}(F)$, then the coordinates of $x$ verify $x_{n+r} = -f_r^{-1} \sum_{i=0}^{r-1} f_i x_{n+i}$ for all $n \in \mathbb{Z}$. This recurrence relation can be expressed with a matrix. For all $n \in \mathbb{Z}$ one has $X_{n+1} = AX_n$ where

$$X_n = \begin{pmatrix} x_{n+r-1} \\ \vdots \\ x_n \end{pmatrix} \quad \text{and} \quad A = \begin{bmatrix} -f_{r-1}f_r^{-1} & \cdots & \cdots & \cdots & -f_0 f_r^{-1} \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}.$$

$A$ is invertible because $f_0 \neq 0 \neq f_r$, and for all $n \in \mathbb{Z}$ one has $X_n = A^n X_0$. Thus the period of $X_n$ divides the period of $A$, which divides the cardinality of the set of invertible matrices on $\mathbb{Z}/p\mathbb{Z}$ of size $r$, that is to say, the number of bases of $(\mathbb{Z}/p\mathbb{Z})^r$, which is $\prod_{i=0}^{r-1}(p^r - p^i)$. □

*Remark 5.1.* Proposition 5.1 still holds if $((\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}, F)$ is an affine CA.

*Remark 5.2.* Proposition 5.1 extends to the case when $\mathcal{A}$ is a finite field and $F = \sum_{u \in \mathbb{U}} f_u \sigma^u$ is a linear CA where each coefficient $f_u$ is the multiplication by an element of the field.

Let $((\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}, F)$ be a non-trivial linear CA where $P_F(\sigma) = \sum_{u \in [0,r]} f_u \circ \sigma^u$ is a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ with $f_0 \neq 0$ and $f_r \neq 0$. In this case, Theorem 1.3, generalized to non-trivial algebraic bipermutative CAs without restriction on the neighborhood, holds only if $\mathrm{Ker}(F)$ contains no non-trivial $\sigma$-invariant subgroups, which is equivalent to the irreducibility of $P_F$. Proposition 5.1 holds for every linear CA on $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}$.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

5.2. *The case $\mathcal{A} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.* Now we consider $\mathcal{A} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ with $p$ and $q$ distinct primes and $(\mathcal{A}^{\mathbb{Z}}, F)$ a linear bipermutative CA. In this case $D_\infty$ contains infinite $\sigma$-invariant subgroups which are not dense in $\mathcal{A}^{\mathbb{Z}}$. For example, $D_\infty^{\Gamma_1}$ and $D_\infty^{\Gamma_2}$ where $\Gamma_1 = (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}} \times \{0_{(\mathbb{Z}/q\mathbb{Z})^{\mathbb{Z}}}\}$ and $\Gamma_2 = \{0_{(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}}}\} \times (\mathbb{Z}/q\mathbb{Z})^{\mathbb{Z}}$. The measures $\lambda_{\Gamma_1}$ and $\lambda_{\Gamma_2}$ are $(F, \sigma)$-totally ergodic with positive entropy for $\sigma$. If $\mu$ is an $(F, \sigma)$-invariant measure which verifies the conditions of Theorem 3.3, we cannot conclude that $\mu = \lambda_{\mathcal{A}^{\mathbb{Z}}}$. However, if we consider the natural factor $\pi_1 : \mathcal{A}^{\mathbb{Z}} \to \Gamma_1$ and $\pi_2 : \mathcal{A}^{\mathbb{Z}} \to \Gamma_2$, then, by Corollary 3.5, one has $\pi_1\mu = \lambda_{\Gamma_1}$ or $\pi_2\mu = \lambda_{\Gamma_2}$. A natural conjecture is this: if every cellular automaton factor of $F$ has positive entropy, then $\mu = \lambda_{\mathcal{A}^{\mathbb{Z}}}$. The problem is to rebuild the measure starting from $\pi_1\mu$ and $\pi_2\mu$.

5.3. *The case $\mathcal{A} = \mathbb{Z}/p^k\mathbb{Z}$.* In this case, we do not know under what extra conditions an $(F, \sigma)$-invariant measure is the Haar measure. Moreover, some linear CAs are not bipermutative. The next lemma shows how to remove this condition when you consider a power of the CA.

LEMMA 5.2. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a linear CA with $\mathcal{A} = \mathbb{Z}/p^k\mathbb{Z}$, where $p$ is prime, $k \geq 1$ and $F = \sum_{i \in [r,s]} f_i\, \sigma^i$, with $f_i \in \mathbb{Z}/p^k\mathbb{Z}$. Let $\widehat{\mathbb{U}} = \{i \in [r, s] : f_i$ coprime with $p\}$, $\hat{r} = \min \widehat{\mathbb{U}}$ and $\hat{s} = \max \widehat{\mathbb{U}}$. Assume $\widehat{\mathbb{U}}$ is not empty and $\hat{r} < \hat{s}$.*

*Then $F^{p^{k-1}}$ is bipermutative of smallest neighborhood $\mathbb{U}' = [p^{k-1}\hat{r}, p^{k-1}\hat{s}]$.*

*Proof.* We can write $F = P_F(\sigma)$ with $P_F \in \mathbb{Z}/p^k\mathbb{Z}[X, X^{-1}]$. We decompose $P_F = P_1 + pP_2$ where $P_1 = \sum_{i \in \widehat{\mathbb{U}}} f_i\, X^i$. By Fermat's little theorem and induction on $j \geq 1$, we can easily prove that

$$(P_1 + pP_2)^{p^j} = (P_1)^{p^j} \mod p^{j+1}.$$

So we have $P_F^{p^{k-1}} = P_1^{p^{k-1}} = \sum_{i \in [p^{k-1}\hat{r}, p^{k-1}\hat{s}]} g_i X^i$ where $g_i \in \mathbb{Z}/p^k\mathbb{Z}$. Moreover, $g_{p^{k-1}\hat{r}} = f_{\hat{r}}^{p^{k-1}}$ and $g_{p^{k-1}\hat{s}} = f_{\hat{s}}^{p^{k-1}}$ are relatively prime to $p$. We deduce that $F^{p^{k-1}} = P_F^{p^{k-1}}(\sigma)$ is bipermutative of smallest neighborhood $\mathbb{U}' = [p^{k-1}\hat{r}, p^{k-1}\hat{s}]$. □

Now from Corollary 2.3 we can deduce an entropy formula for general linear CAs on $(\mathbb{Z}/p^k\mathbb{Z})^{\mathbb{Z}}$.

COROLLARY 5.3. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a linear CA with $\mathcal{A} = \mathbb{Z}/p^k\mathbb{Z}$, where $p$ is prime, $k \geq 1$ and $F = \sum_{i \in [s,r]} f_i\, \sigma^i$ with $f_i \in \mathbb{Z}/p^k\mathbb{Z}$. Let $\hat{r} < \hat{s}$ be as in Lemma 5.2. Let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$. Then $h_\mu(F) = (\max(\hat{r}, 0) - \min(\hat{s}, 0))h_\mu(\sigma)$.*

COROLLARY 5.4. *Let $(\mathcal{A}^{\mathbb{Z}}, F)$ be a linear CA with $\mathcal{A} = \mathbb{Z}/p^k\mathbb{Z}$, where $p$ is prime, $k \geq 1$ and $F = \sum_{i \in [s,r]} f_i\, \sigma^i$ with $f_i \in \mathbb{Z}/p^k\mathbb{Z}$. Assume that, for at least two $i \in [s, r]$, $f_i$ is relatively prime with $p$. Let $\Sigma$ be a closed $(F, \sigma)$-invariant subgroup of $\mathcal{A}^{\mathbb{Z}}$ and let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{Z}}$ with $\mathrm{supp}(\mu) \subset \Sigma$. Assume that:*

(1) *$\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action induced by $(F, \sigma)$;*
(2) *$\mathcal{I}_\mu(\sigma) = \mathcal{I}_\mu(\sigma^{pp_1})$ with $p_1$ the smallest common period of all elements of $\mathrm{Ker}(F)$;*
(3) *$h_\mu(\sigma) > 0$;*

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

(4) *every* $\sigma$*-invariant infinite subgroup of* $D_\infty^\Sigma(F) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(F^n) \cap \Sigma$ *is dense in* $\Sigma$.
*Then* $\mu = \lambda_\Sigma$.

*Example 5.3.* Let $\mathcal{A} = \mathbb{Z}/4\mathbb{Z}$, we consider the CA $(\mathcal{A}^\mathbb{Z}, F)$ defined by $F = \mathrm{Id} + \sigma + 2\sigma^2$. Then $\Sigma = \{0, 2\}^\mathbb{Z}$ satisfies the conditions of Corollary 5.4. In this case, the only $(F, \sigma)$-invariant probability measures of positive entropy known are $\lambda_{\mathcal{A}^\mathbb{Z}}$ and $\lambda_\Sigma$.

## 6. *Measure rigidity for some affine one-sided expansive CAs*

An invertible one-sided CA $(\mathcal{A}^\mathbb{N}, F)$ is said to be expansive if there exists a constant $r_e \in \mathbb{N}$ such that, for all $x, y \in \mathcal{A}^\mathbb{N}$, if $x \neq y$ there exists $n \in \mathbb{Z}$ which verifies $F^n(x)_{[0,r_e]} \neq F^n(y)_{[0,r_e]}$. Expansive CAs are different from positively expansive CAs because we also look at the past of the orbit. Boyle and Maass introduced in [**BM00**] a class of one-sided invertible expansive CAs which have remarkable combinatorial properties. Further properties were obtained in [**DMS03**]. We study this class of examples from the point of view of measure rigidity. This class of CAs is not bipermutative so we cannot apply Theorem 3.3 directly. However, in some cases, it is possible to associate a 'dual' CA which corresponds to the assumptions of Theorem 3.3. This is a first step to study measure rigidity for expansive CAs.

We are going to recall some properties obtained in [**BM00**]. Let $F : \mathcal{A}^\mathbb{N} \to \mathcal{A}^\mathbb{N}$ be a CA such that $r(F) = 1$. Associate to $F$ the equivalence relation $\mathcal{R}_F$ over $\mathcal{A}$ defined by: $a\mathcal{R}_F b$ if and only if $\overline{F}(ca) = \overline{F}(cb)$ for all $c \in \mathcal{A}$. Write $\mathcal{P}_{\mathcal{R}_F}$ to be the partition induced by $\mathcal{R}_F$ and $C_{\mathcal{R}_F}(a)$ to be the class associated to $a$. Also define $\pi_F : \mathcal{A} \to \mathcal{A}$ by $\pi_F(a) = \overline{F}(aa)$ for any $a \in \mathcal{A}$.

PROPOSITION 6.1. [**BM00**] *A one-sided CA* $F : \mathcal{A}^\mathbb{N} \to \mathcal{A}^\mathbb{N}$ *with* $r(F) = 1$ *is invertible with* $r(F^{-1}) = 1$ *if and only if the following conditions hold:*

(1) $\pi_F$ *is a permutation;*
(2) $F$ *is left-permutative;*
(3) *for all* $a \in A$, $\mathrm{Succ}_F(a) := \mathrm{Im}(\overline{F}(a\,\cdot)) \subset \pi_F(C_{\mathcal{R}_F}(a))$.

If $F$ is an expansive invertible CA with $r(F) = r(F^{-1}) = 1$, then $(\mathcal{A}^\mathbb{N}, F)$ is topologically conjugate to the bilateral subshift $(S_F, \sigma)$ where $S_F = \{(F^i(x)_0)_{i\in\mathbb{Z}} : x \in \mathcal{A}^\mathbb{N}\}$ via the conjugacy $\phi_F : x \in \mathcal{A}^\mathbb{N} \to (F^i(x)_0)_{i\in\mathbb{N}} \in S_F$. Define $F_T : S_F \to S_F$ by $F_T(\phi_F(x)) = \phi_F(\sigma(x))$ for every $x \in \mathcal{A}^\mathbb{N}$. If $F$ is expansive then $(S_F, F_T)$ is a CA (defined on $S_F$ instead of a fullshift). Invertible expansive CAs with $r(F) = r(F^{-1}) = r(F_T) = 1$ can be characterized as follows.

PROPOSITION 6.2. [**BM00**] *A one-sided invertible CA* $F : \mathcal{A}^\mathbb{N} \to \mathcal{A}^\mathbb{N}$ *with* $r(F) = r(F^{-1}) = 1$ *is expansive with* $r(F_T) = 1$ *if and only if the following conditions are verified:*

(1) $|C \cap \pi_F(C')| \leq 1$ *for any* $C, C' \in \mathcal{P}_{\mathcal{R}_F}$*;*
(2) *for all* $a \in \mathcal{A}$, $\mathrm{Succ}_F(a) := \mathrm{Im}(\overline{F}(a\,\cdot)) = \pi_F(C_{\mathcal{R}_F}(a))$.

Such a CA is said to be in Class (A). The alphabet $\mathcal{A}$ of a CA in Class (A) has cardinality $n^2$ for some $n \in \mathbb{N}$.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

Write $\mathcal{B} = \mathcal{P}_{\mathcal{R}_F}$. In [**BM00**], the authors show that $(S_F, \sigma)$ is conjugate to the fullshift $(\mathcal{B}^{\mathbb{Z}}, \sigma)$ by $\varphi : S_F \to \mathcal{B}^{\mathbb{Z}}$ such that $\varphi((a_i)_{i\in\mathbb{Z}}) = (C_{\mathcal{R}_F}(a_i))_{i\in\mathbb{Z}}$. The CA $(S_F, F_T)$ determines by $\varphi$ a CA $(\mathcal{B}^{\mathbb{Z}}, \widetilde{F_T})$ on $\mathcal{B}^{\mathbb{Z}}$ and $(S_F, F_T)$ is conjugate to $(\mathcal{B}^{\mathbb{Z}}, \widetilde{F_T})$. To sum up, we have

$$(\mathcal{A}^{\mathbb{N}}, \sigma) \equiv (S_F, F_T) \equiv (\mathcal{B}^{\mathbb{Z}}, \widetilde{F_T}),$$
$$(\mathcal{A}^{\mathbb{N}}, F) \equiv (S_F, \sigma) \equiv (\mathcal{B}^{\mathbb{Z}}, \sigma),$$

(where $\equiv$ means topologically conjugate).

PROPOSITION 6.3. *If $F$ is in Class (A) then $\widetilde{F_T}$ is bipermutative.*

*Proof.* Let $(\mathcal{A}^{\mathbb{N}}, F)$ be a CA in Class (A) and let $\alpha, \alpha', \beta, \gamma, \delta \in \mathcal{B}$ such that $\widetilde{F_T}(\alpha, \beta, \gamma) = \widetilde{F_T}(\alpha', \beta, \gamma) = \delta$. Suppose $\beta = \varphi(b)$, for some $b \in S_F$. Then $b \in \pi_F(\gamma)$ by condition (2) of Proposition 6.2, so $b \in \beta \cap \pi_F(\gamma)$, which is a singleton set by condition (1). Hence $\beta$ and $\gamma$ uniquely determine $b$. Likewise, if $\alpha = \varphi(a)$ and $\alpha' = \varphi(a')$ for some $a, a' \in S_F$, then we must have $a, a' \in \overline{F}(b, \delta)$. But $\overline{F}(b, .) : \mathcal{A} \to \mathcal{A}$ is constant on $\delta$ by definition of the partition $\mathcal{P}_{\mathcal{R}_F}$, so $a = a'$ so $\alpha = \alpha'$. We deduce that the function $\widetilde{F_T}(\cdot, \beta, \gamma) : \mathcal{B} \to \mathcal{B}$ is injective. So it is bijective because $\mathcal{B}$ is finite. Thus, $(\mathcal{B}, \widetilde{F_T})$ is left-permutative.

In the same way we can prove that $(\mathcal{B}, \widetilde{F_T})$ is right-permutative by applying Propositions 6.1 and 6.2 to $F^{-1}$ instead. The result follows. □

After this proposition, with a view to applying Theorems 3.3 and 3.4, we want to characterize the CA $F$ in Class (A) such that $\widetilde{F_T}$ is algebraic. We have only the next sufficient condition.

PROPOSITION 6.4. *Let $(\mathcal{A}^{\mathbb{N}}, F)$ be a linear CA, with $F = f_0\,\mathrm{Id} + f_1\sigma$ where $f_0$ and $f_1$ are endomorphisms of $\mathcal{A}$ extended coordinate by coordinate to $\mathcal{A}^{\mathbb{N}}$.*

(a) *$F$ is invertible with $r(F^{-1}) = 1$ if and only if $f_0$ is an automorphism and $f_1 \circ f_0^{-1} \circ f_1 = 0$.*

(b) *$F$ is in Class (A) if and only if $f_0$ is an automorphism, $\mathrm{Im}\, f_1 = f_0(\mathrm{Ker}\, f_1)$ and $\mathrm{Im}\, f_1 \cap \mathrm{Ker}\, f_1 = \{0\}$.*

(c) *When $(\mathcal{A}^{\mathbb{Z}}, F)$ is in Class (A), the CA $(\mathcal{P}^{\mathbb{Z}}_{\mathcal{R}_F}, \widetilde{F_T})$ is linear.*

*Proof.* First we note that $b \in C_{\mathcal{R}_F}(b')$ if and only if $f_0(a) + f_1(b) = f_0(a) + f_1(b')$ for all $a \in \mathcal{A}$; this is equivalent to $b \in b' + \mathrm{Ker}\, f_1$. So $C_{\mathcal{R}_F}(b) = b + \mathrm{Ker}\, f_1$ for all $b \in \mathcal{A}$. Thus, $\mathcal{P}_{\mathcal{R}_F} \cong \mathcal{A}/\mathrm{Ker}\, f_1$. Moreover, $\mathrm{Succ}_F(a) = \mathrm{Im}(\overline{F}(a\,\cdot)) = f_0(a) + \mathrm{Im}\, f_1$ for all $a \in \mathcal{A}$, and $\pi_F = f_0 + f_1$.

Proof of (a): Assuming $f_0$ is an automorphism and $f_1 \circ f_0^{-1} \circ f_1 = 0$, it is possible to express $F^{-1}$ as $F^{-1} = f_0^{-1}\mathrm{Id} - f_0^{-1} \circ f_1 \circ f_0^{-1}\sigma$. Conversely, if $F$ is invertible with $r(F^{-1}) = 1$, by Proposition 6.1, $f_0$ is an automorphism because $F$ is left-permutative and $f_1 \circ f_0^{-1} \circ f_1 = 0$ because for some $a \in \mathcal{A}$ one has

$$f_0(a) + \mathrm{Im}(f_1) = \mathrm{Succ}_F(a) \subset \pi_F(C_{\mathcal{R}_F}(a)) = f_0(a) + f_1(a) + f_0(\mathrm{Ker}\, f_1),$$

that is to say, $\mathrm{Im}\, f_1 \subset f_0(\mathrm{Ker}\, f_1)$.

Proof of (b): As in the proof of (a), one has $\mathrm{Succ}_F(a) = \pi_F(C_{\mathcal{R}_F}(a))$ for any $a \in \mathcal{A}$ if and only if $\mathrm{Im}\, f_1 = f_0(\mathrm{Ker}\, f_1)$. Moreover, if $|C \cap \pi_F(C')| \leq 1$ for any $C, C' \in \mathcal{P}_{\mathcal{R}_F}$, then $0 + \mathrm{Ker}\, f_1 \cap \pi_F(0 + \mathrm{Ker}\, f_1) = \mathrm{Ker}\, f_1 \cap f_0(\mathrm{Ker}\, f_1) = \mathrm{Ker}\, f_1 \cap \mathrm{Im}\, f_1 = \{0\}$.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

Conversely, for any $b, b' \in \mathcal{A}$ one has $C_{\mathcal{R}_F}(b) \cap \pi_F(C_{\mathcal{R}_F}(b)) = b + \mathrm{Ker} f_1 \cap \pi_F(b') + \mathrm{Im} f_1$, so if $\mathrm{Ker} f_1 \cap \mathrm{Im} f_1 = \{0\}$ then $C_{\mathcal{R}_F}(b) \cap \pi_F(C_{\mathcal{R}_F}(b))$ contains at most one element. Characterization of linear CAs in Class (A) follows from Proposition 6.2.

Proof of (c): Let $(\mathcal{A}^{\mathbb{N}}, F)$ be a CA in Class (A). We will show that $(\mathcal{P}_{\mathcal{R}_F}^{\mathbb{Z}}, \widetilde{F_T})$ is linear. Since $\mathcal{A}$ is finite abelian and $\mathrm{Im} f_1 \cap \mathrm{Ker} f_1 = \{0\}$ by (b), one has $\mathrm{Im} f_1 \oplus \mathrm{Ker} f_1 = \mathcal{A}$. Moreover, $\mathrm{Im} f_1$ and $\mathrm{Ker} f_1$ are isomorphic to the same group, denoted $\mathcal{B}$, because $f_0$ is an automorphism and $\mathrm{Im} f_1 = f_0(\mathrm{Ker} f_1)$ by (b). An element $a \in \mathcal{A}$ is written $\binom{x}{y}$ where $x \in \mathrm{Im} f_1 \simeq \mathcal{B}$ and $y \in \mathrm{Ker} f_1 \simeq \mathcal{B}$. One has $\mathcal{P}_{\mathcal{R}_F} \simeq \mathcal{A}/\mathrm{Ker} f_1 \simeq \mathrm{Im} f_1 \simeq \mathcal{B}$. We want to show that $(\mathcal{B}^{\mathbb{Z}}, \widetilde{F_T})$ is linear. We can write $f_0$ and $f_1$ as $2 \times 2$-matrices with coefficients in $\mathrm{Hom}(\mathcal{B})$:

$$f_0 = \begin{bmatrix} f_{0,11} & f_{0,12} \\ f_{0,21} & f_{0,22} \end{bmatrix} \quad \text{and} \quad f_1 = \begin{bmatrix} f_{1,11} & f_{1,12} \\ f_{1,21} & f_{1,22} \end{bmatrix}.$$

Since $\mathrm{Im} f_1 = f_0(\mathrm{Ker} f_1)$, one has $f_{0,22} = 0$ and since $f_0$ is an automorphism, we deduce that $f_{0,12}$ and $f_{0,21}$ are automorphisms of $\mathcal{B}$. Since the second coordinate corresponds to the kernel of $f_1$, one has $f_{12}^1 = f_{22}^1 = 0$ and since $\mathrm{Im} f_1 \cap \mathrm{Ker} f_1 = \{0\}$, one has $f_{1,21} = 0$. Moreover, $f_{1,11}$ is an automorphism of $\mathcal{B}$ since it is the restriction of $f_1$ at $\mathrm{Im} f_1$. So we have

$$f_0 = \begin{bmatrix} f_{0,11} & f_{0,12} \\ f_{0,21} & 0 \end{bmatrix}, \quad f_0^{-1} = \begin{bmatrix} 0 & f_{0,21}^{-1} \\ f_{0,12}^{-1} & -f_{0,12}^{-1} \circ f_{0,11} \circ f_{0,21}^{-1} \end{bmatrix} \text{ and } f_1 = \begin{bmatrix} f_{1,11} & 0 \\ 0 & 0 \end{bmatrix}.$$

These formulas are illustrated by the next diagram which represents the action of $\overline{F}$ and $\overline{F^{-1}}$ on a neighborhood:

$$\vdots$$

$$\begin{pmatrix} f_{0,11}(x_0) + f_{0,12}(y_0) + f_{1,11}(x_1) \\ f_{0,21}(x_0) \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \qquad\qquad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \quad \cdots$$

$$\begin{pmatrix} f_{0,21}^{-1}(y_0) \\ f_{0,12}^{-1}(x_0) - f_{0,12}^{-1} \circ f_{0,11} \circ f_{0,21}^{-1}(y_0) + f_{0,12}^{-1} \circ f_{1,11} \circ f_{0,21}^{-1}(y_1) \end{pmatrix}$$

$$\vdots$$

We deduce that $\widetilde{F_T} = f_{1,11}^{-1} \circ \sigma - f_{1,11}^{-1} \circ f_{0,11} \circ \mathrm{Id} - f_{1,11}^{-1} \circ f_{0,12} \circ f_{0,21} \circ \sigma^{-1}$, so $(\mathcal{B}^{\mathbb{Z}}, \widetilde{F_T})$ is linear. □

With Proposition 5.1 and the conjugacy relations it is possible to characterize the uniform Bernoulli measure of some linear CAs in Class (A).

PROPOSITION 6.5. *Let $(\mathcal{A}^{\mathbb{N}}, F)$ be an affine invertible CA in Class (A) with $|\mathcal{A}| = p^2$ with $p$ prime. Let $\mu$ be an $(F, \sigma)$-invariant probability measure on $\mathcal{A}^{\mathbb{N}}$. Assume that:*

(1) *$\mu$ is ergodic for the $\mathbb{Z} \times \mathbb{N}$-action $(F, \sigma)$;*

(2) *$\mathcal{I}_\mu(F) = \mathcal{I}_\mu(F^{p(p-1)(p^2-1)})$;*

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

(3) $h_\mu(\sigma) > 0$.
*Then* $\mu = \lambda_{\mathcal{A}^\mathbb{N}}$.

*Proof.* By Proposition 6.4, $\widetilde{F_T}$ is a linear bipermutative CA of the neighborhood $[-1, 1]$ on $\mathcal{B}^\mathbb{Z}$, where $\mathcal{B} = \mathbb{Z}/p\mathbb{Z}$ . There exists $\phi : \mathcal{A}^\mathbb{N} \to \mathcal{B}^\mathbb{Z}$ such that $(\mathcal{A}^\mathbb{N}, F, \sigma)$ and $(\mathcal{B}^\mathbb{Z}, \sigma, \widetilde{F_T})$ are conjugate via $\phi$, so:

(1) $\phi\mu$ is ergodic for the $\mathbb{N} \times \mathbb{Z}$-action $(\widetilde{F_T}, \sigma)$;
(2) $\mathcal{I}_{\phi\mu}(\sigma) = \mathcal{I}_{\phi\mu}(\sigma^{p(p-1)(p^2-1)}) \underset{(*)}{=} \mathcal{I}_{\phi\mu}(\sigma^{p(p-1)})$, where $(*)$ is by Remark 3.2;
(3) $h_{\phi\mu}(\widetilde{F_T}) > 0$.

By Proposition 5.1(a) we deduce that $\phi\mu = \lambda_{\mathcal{B}^\mathbb{Z}}$ so $\mu = \lambda_{\mathcal{A}^\mathbb{N}}$. □

The next example shows two CAs of Class (A) with $|\mathcal{A}| = 2^2$.

*Example 6.1.* Let $\mathcal{A} = \mathbb{Z}/2Z \times \mathbb{Z}/2\mathbb{Z}$. We define two CAs $(\mathcal{A}^\mathbb{N}, F_1)$ and $(\mathcal{A}^\mathbb{N}, F_2)$ in Class (A) by

$$\overline{F_1}\left(\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

and

$$\overline{F_2}\left(\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}\right) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}.$$

The first coordinate corresponds to the class of $\mathcal{P}_{\mathcal{R}_{F_i}}$ and the second coordinate corresponds to the class of $\mathcal{P}_{\mathcal{R}_{F_i^{-1}}}$. For $i \in \{1, 2\}$, let $\mu_i$ be such that:

(1) $\mu_i$ is $(F_i, \sigma)$-ergodic and $\mathcal{I}_{\mu_i}(F) = \mathcal{I}_{\mu_i}(F^6)$;
(2) there exists $(n, m) \in \mathbb{N} \times \mathbb{Z}$ such that $h_{\mu_i}(\sigma^n \circ F_i^m) > 0$.

All the hypotheses of Proposition 6.5 are satisfied, so that we can conclude that $\mu_i = \lambda_{\mathcal{A}^\mathbb{N}}$ for all $i \in \{1, 2\}$. To see where Theorem 1.3 does not hold when we assume $\mu$ $\sigma$-totally ergodic, we are going to calculate $\mathrm{Ker}(\widetilde{F_i^T})$ for $i \in \{1, 2\}$.

For $F_1$ one has

$$\overline{\widetilde{F_1^T}}(\alpha, \beta, \gamma) = \alpha + \beta + \gamma.$$

This formula is illustrated by the following diagram, which represents the action of $\overline{F_1}$ and $\overline{F_1^{-1}}$ on a neighborhood:

$$\begin{array}{ccc} & \vdots & \\ & \begin{pmatrix} x_0 + x_1 + y_0 \\ x_0 \end{pmatrix} & \\ \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} & & \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \quad \cdots \\ & \begin{pmatrix} y_0 \\ y_0 + y_1 + x_0 \end{pmatrix} & \\ & \vdots & \end{array}$$

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

So we have

$$D_1(\widetilde{F_1^T}) = \mathrm{Ker}(\widetilde{F_1^T}) = \{^\infty 000^\infty, ^\infty 011^\infty, ^\infty 110^\infty, ^\infty 101^\infty\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

$\mathrm{Ker}(F_1^T)$ contains no non-trivial $\sigma$-invariant subgroups. Then $\mu_1 = \lambda_{\mathcal{A}^{\mathbb{N}}}$ by Theorem 3.3 and Corollary 4.7. In this case, if $\mu$ were $\sigma$-totally ergodic, then we could also have applied Theorem 1.3 to conclude that $\mu = \lambda_{\mathcal{A}^{\mathbb{N}}}$.

For $F_2$ one has

$$\overline{\widetilde{F_2^T}}(\alpha, \beta, \gamma) = \alpha + \gamma.$$

This formula is illustrated by the following diagram which represents the action of $\overline{F_2}$ and $\overline{F_2^{-1}}$ on a neighborhood:

$$\begin{array}{ccc} \vdots & & \\ \begin{pmatrix} x_1 + y_0 \\ x_0 \end{pmatrix} & & \\ \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} & \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} & \cdots \\ \begin{pmatrix} y_0 \\ y_1 + x_0 \end{pmatrix} & & \\ \vdots & & \end{array}$$

One obtains

$$D_1(\widetilde{F_2^T}) = \mathrm{Ker}(\widetilde{F_2^T}) = \{^\infty 00^\infty, ^\infty 11^\infty, ^\infty 01^\infty, ^\infty 10^\infty\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$D_2(\widetilde{F_2^T}) = \langle D_1 \cup \{^\infty 0001^\infty, ^\infty 0111^\infty, ^\infty 0011^\infty\}\rangle_\sigma.$$

We note that for all $d \in \partial D_2$ one has $D_1 \subset \langle d\rangle_\sigma$, so $\mu_2 = \lambda_{\mathcal{A}^{\mathbb{N}}}$ by Theorem 3.3 and Proposition 4.6. We also note that in this case $\{^\infty 00^\infty, ^\infty 11^\infty\}$ is a non-trivial $\sigma$-invariant subgroup of $\mathrm{Ker}(F)$ so Theorem 1.3 would not apply, even if we assumed that $\mu$ was $\sigma$-totally ergodic.

*Acknowledgements.* I would like to thank Alejandro Maass and Francois Blanchard for many stimulating conversations during the process of writing this paper. I thank also the referee, as the final version of this paper owes much to his numerous suggestions. I thank Nucleus Millennium P01-005 and Ecos-Conicyt C03E03 for financial support. Last but not least, a special acknowledgment goes to Wen Huang for his attentive reading and his relevant remarks.

## References

**[AB93]** J.-M. Arnaudiès and J. Bertin. *Groupes, Algèbres et Géométrie, Tome 1*. Ellipses, Paris, 1993.

**[BM00]** M. Boyle and A. Maass. Expansive invertible onesided cellular automata. *J. Math. Soc. Japan* **52**(4) (2000), 725–740.

https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press

**[DMS03]** P. Dartnell, A. Maass and F. Schwartz. Combinatorial constructions associated to the dynamics of one-sided cellular automata. *Theoret. Comput. Sci.* **304**(1–3) (2003), 485–497.

**[Ein05]** M. Einsiedler. Isomorphism and measure rigidity for algebraic actions on zero-dimensional groups. *Monatsh. Math.* **144**(1) (2005), 39–69.

**[FMMN00]** P. A. Ferrari, A. Maass, S. Martínez and P. Ney. Cesàro mean distribution of group automata starting from measures with summable decay. *Ergod. Th. & Dynam. Sys.* **20**(6) (2000), 1657–1670.

**[Fur67]** H. Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Systems Theory* **1** (1967), 1–49.

**[Gui68]** A. Guichardet. *Analyse Harmonique Commutative (Monographies Universitaires de Mathématiques, 26)*. Dunod, Paris, 1968.

**[Hed69]** G. A. Hedlund. Endormorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory* **3** (1969), 320–375.

**[HMM03]** B. Host, A. Maass and S. Martínez. Uniform Bernoulli measure in dynamics of permutative cellular automata with algebraic local rules. *Discrete Contin. Dyn. Syst.* **9**(6) (2003), 1423–1446.

**[Kit87]** B. P. Kitchens. Expansive dynamics on zero-dimensional groups. *Ergod. Th. & Dynam. Sys.* **7**(2) (1987), 249–261.

**[Lan02]** S. Lang. *Algebra*, 3rd edn. *(Graduate Texts in Mathematics, 211)*. Springer, New York, 2002.

**[Led78]** F. Ledrappier. Un champ markovien peut être d'entropie nulle et mélangeant. *C. R. Acad. Sci. Paris Sér.* A–B **287**(7) (1978), A561–A563.

**[Lin84]** D. A. Lind. Applications of ergodic theory and sofic systems to cellular automata. *Phys.* D **10**(1–2) (1984), 36–44.

**[MM98]** A. Maass and S. Martínez. On Cesàro limit distribution of a class of permutative cellular automata. *J. Stat. Phys.* **90**(1–2) (1998), 435–452.

**[Pet89]** K. Petersen. *Ergodic Theory (Cambridge Studies in Advanced Mathematics, 2)*. Cambridge University Press, Cambridge, 1989. Corrected reprint of the 1983 original.

**[Piv05]** M. Pivato. Invariant measures for bipermutative cellular automata. *Discrete Contin. Dyn. Syst.* **12**(4) (2005), 723–736.

**[PY02]** M. Pivato and R. Yassawi. Limit measures for affine cellular automata. *Ergod. Th. & Dynam. Sys.* **22**(4) (2002), 1269–1287.

**[PY04]** M. Pivato and R. Yassawi. Limit measures for affine cellular automata. II. *Ergod. Th. & Dynam. Sys.* **24**(6) (2004), 1961–1980.

**[Sch95]** K. Schmidt. *Dynamical Systems of Algebraic Origin (Progress in Mathematics, 128)*. Birkhäuser, Basel, 1995.

**[She92]** M. A. Shereshevsky. Lyapunov exponents for one-dimensional cellular automata. *J. Nonlinear Sci.* **2**(1) (1992), 1–8.

**[Sil05]** S. Silberger. Subshifts of the three dot system. *Ergod. Th. & Dynam. Sys.* **25**(5) (2005), 1673–1687.

**[Tis00]** P. Tisseur. Cellular automata and Lyapunov exponents. *Nonlinearity* **13**(5) (2000), 1547–1560.

**[Wal82]** P. Walters. *An Introduction to Ergodic Theory (Graduate Texts in Mathematics, 79)*. Springer, New York, 1982.

**[War00]** T. B. Ward. Additive cellular automata and volume growth. *Entropy* **2**(3) (2000), 142–167 (electronic).


https://doi.org/10.1017/S0143385707000247 Published online by Cambridge University Press