DISCRETE AND CONTINUOUS
DYNAMICAL SYSTEMS
Volume **12**, Number **4**, April **2005**

Website: http://aimSciences.org

pp. **723–736**

INVARIANT MEASURES FOR BIPERMUTATIVE CELLULAR AUTOMATA

Marcus Pivato

Department of Mathematics
Trent University
Peterborough, Ontario, K9L 1Z8, Canada

(Communicated by Lluís Alsedà)

Abstract. A *right-sided, nearest neighbour cellular automaton* (RNNCA) is a continuous transformation $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ determined by a *local rule* $\phi : \mathcal{A}^{\{0,1\}} \longrightarrow \mathcal{A}$ so that, for any $\mathbf{a} \in \mathcal{A}^{\mathbb{Z}}$ and any $z \in \mathbb{Z}$, $\Phi(\mathbf{a})_z = \phi(a_z, a_{z+1})$. We say that Φ is *bipermutative* if, for any choice of $a \in \mathcal{A}$, the map $\mathcal{A} \ni b \mapsto \phi(a, b) \in \mathcal{A}$ is bijective, and also, for any choice of $b \in \mathcal{A}$, the map $\mathcal{A} \ni a \mapsto \phi(a, b) \in \mathcal{A}$ is bijective.

We characterize the invariant measures of bipermutative RNNCA. First we introduce the equivalent notion of a *quasigroup CA*. Then we characterize Φ-invariant measures when $\mathcal{A}$ is a (nonabelian) group, and $\phi(a, b) = a \cdot b$. Then we show that, if Φ is any bipermutative RNNCA, and μ is Φ-invariant, then Φ must be μ-almost everywhere K-to-1, for some constant K. We then characterize invariant measures when $\mathcal{A}^{\mathbb{Z}}$ is a group shift and Φ is an endomorphic CA.

1. Introduction.

If $\mathcal{A}$ is a (discretely topologized) finite set, then $\mathcal{A}^{\mathbb{Z}}$ is compact in the Tychonoff topology. Let $\sigma : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be the shift map: $\sigma(\mathbf{a}) = \left[b_z|_{z\in\mathbb{Z}}\right]$, where $b_z = a_{z+1}$, for all $z \in \mathbb{Z}$. For any $n, m \in \mathbb{Z}$, let $[n...m] := \{n, n+1, \ldots, m\}$. A *cellular automaton* (CA) is a dynamical system $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ defined by a *local rule* $\phi : \mathcal{A}^{[-\ell...r]} \longrightarrow \mathcal{A}$ (for some $\ell, r \geq 0$) so that, for any $\mathbf{a} \in \mathcal{A}^{\mathbb{Z}}$ and any $z \in \mathbb{Z}$, $\Phi(\mathbf{a})_z = \phi(a_{z-\ell}, \ldots, a_{z+r})$. Equivalently [4], a CA is continuous map $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ which commutes with σ.

Let $[-\ell...r) := [-\ell...r-1]$ and let $(-\ell...r] := [1-\ell...r]$. Then Φ is *right-permutative* if, for any fixed $\mathbf{a} \in \mathcal{A}^{[-\ell...r)}$, the map $\mathcal{A} \ni b \mapsto \phi(\mathbf{a}, b) \in \mathcal{A}$ is bijective. Likewise, Φ is *left-permutative* if, for any fixed $\mathbf{b} \in \mathcal{A}^{(-\ell...r]}$, the map $\mathcal{A} \ni a \mapsto \phi(a, \mathbf{b}) \in \mathcal{A}$ is bijective, and Φ is *bipermutative* if it is both left- and right-permutative.

Example 1.1: (a) If $(\mathcal{A}, +)$ is an abelian group, $\ell = 0$ and $r = 1$, and $\phi(a_0, a_1) = a_0 + a_1$, then Φ is a called a *nearest neighbour addition* CA, and is bipermutative.

(b) If $\mathcal{A} = \mathbb{Z}_{/p}$ (where p is prime), and let $c_0, c_1, d \in \mathbb{Z}_{/p}$ be constants ($c_0 \neq 0 \neq c_1$). If $\phi(a_0, a_1) = c_0 a_0 + c_1 a_1 + d$, then Φ is a called an *affine* CA, and is bipermutative. ♢

We say that Φ is a *right-sided, nearest neighbour* cellular automaton (RNNCA) if $\ell = 0$ and $r = 1$ [as in Examples 1.1(a) and 1.1(b)]. It is easy to show:

2000 *Mathematics Subject Classification.* Primary: 37B15; Secondary: 37A50.

Key words and phrases. Cellular automata, permutative, invariant measure, quasigroup, Latin square, endomorphism, group shift.

Partially supported by NSERC Canada.

Lemma 1.2. *Let $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be a CA and let $\mathcal{B} = \mathcal{A}^{\ell+r}$. There is an RNNCA $\Gamma : \mathcal{B}^{\mathbb{Z}} \longrightarrow \mathcal{B}^{\mathbb{Z}}$ so that the the topological dynamical system $(\mathcal{A}^{\mathbb{Z}}, \Phi)$ is isomorphic to the system $(\mathcal{B}^{\mathbb{Z}}, \Gamma)$.*

Furthermore $\Big(\ \Phi$ *is bipermutative* $\Big) \iff \Big(\ \Gamma$ *is bipermutative* $\Big)$. □

Let λ be the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{Z}}$. Thus, for any $n \leq m$, if $(c_n, \ldots, c_m) \in \mathcal{A}^{[n..m]}$, then $\lambda\{\mathbf{a} \in \mathcal{A}^{\mathbb{Z}} ; (a_n, ..., a_m) = (c_n, ..., c_m)\} = 1/|\mathcal{A}|^{m-n+1}$. Let $\mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma)$ be the set of Φ- and σ-invariant probability measures on $\mathcal{A}^{\mathbb{Z}}$. Let Φ be a permutative CA. Then Φ is surjective, and thus $\lambda \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma)$ [4]. What other measures (if any) lie in $\mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma)$? Let $h_\mu(\Phi)$ denote the *measurable entropy* [10, §5.2] of the measure-preserving dynamical system $(\mathcal{A}^{\mathbb{Z}}, \Phi, \mu)$. Let $\mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-erg})$ be the σ-ergodic measures in $\mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma)$. Host, Maass, and Martínez [1] have shown:

Proposition 1.3. [1, Theorem 12] *Let $\mathcal{A} = \mathbb{Z}_{/p}$, where p is prime. Let $\Phi\colon \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ be an affine CA. If $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-erg})$, and $h_\mu(\Phi) > 0$, then $\mu = \lambda$.* □

This paper generalizes Proposition 1.3 in three ways. In §2, we introduce quasigroups, and reformulate bipermutative RNNCA as *quasigroup CA*. In §3 we characterize invariant measures for *nearest-neighbour multiplication* CA (when $\mathcal{A}$ is a nonabelian group). In §4 we extend the method of [1] to prove: if $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi\text{-erg}; \sigma)$ then there is some $K \leq |\mathcal{A}|$ so that Φ is K-to-1 (μ-æ) (Theorem 4.1). In §5 we generalize Proposition 1.3 to *endomorphic* CA on group shifts (Theorem 5.2).

Notation: If μ is a measure, then '$\forall_\mu\, x$' means 'μ-almost all x', and 'μ-æ' means 'μ-almost everywhere'. If $\mathbf{U}$ and $\mathbf{V}$ are measurable sets, then '$\mathbf{U} \underset{\mu}{\subset} \mathbf{V}$' means $\mu[\mathbf{U} \setminus \mathbf{V}] = 0$, and '$\mathbf{U} \underset{\mu}{=} \mathbf{V}$' means $\mathbf{U} \underset{\mu}{\subset} \mathbf{V}$ and $\mathbf{V} \underset{\mu}{\subset} \mathbf{U}$. If $\mathfrak{S}$ is a sigma algebra and $\mathbf{U}$ is a measurable set, then $\mathbb{E}_\mu[\mathbf{U} \,|\mathfrak{S}]$ is the conditional expectation of $\mathbb{1}_{\mathbf{U}}$ given $\mathfrak{S}$.

2. **Quasigroup Cellular Automata.**

A *quasigroup* [11] is a finite set $\mathcal{A}$ equipped with a binary operation '$*$' which has the left- and right-cancellation properties. In other words, for any $a, b, c \in \mathcal{A}$,

$$\Big(\ a * b = a * c\ \Big) \iff \Big(\ b = c\ \Big) \quad \text{and} \quad \Big(\ b * a = c * a\ \Big) \iff \Big(\ b = c\ \Big).$$

(Note that the operator '$*$' is not necessarily associative. Indeed, it is easy to show: '$*$' is associative if and only if $(\mathcal{A}, *)$ is a group.) Let $A := |\mathcal{A}|$. The 'multiplication table' for $*$ is the $A \times A$ matrix $\mathbf{M}^* = [m_{a,b}]_{a,b \in \mathcal{A}}$, where $m_{a,b} = a * b$. It follows that $(\mathcal{A}, *)$ is a quasigroup if and only $\mathbf{M}^*$ is a *Latin square*, which means that every column and every row of $\mathbf{M}^*$ contains each element of $\mathcal{A}$ exactly once [5]. A *quasigroup cellular automaton* (QGCA) is a RNNCA $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ with local rule $\phi : \mathcal{A}^{\{0,1\}} \longrightarrow \mathcal{A}$ given: $\phi(a_0, a_1) = a_0 * a_1$, where '$*$' is a quasigroup operation. For instance, Example 1.1(a) is a QGCA. It follows:

$$\Big(\ \Phi \text{ is a bipermutative RNNCA}\ \Big) \iff \Big(\ \Phi \text{ is a quasigroup CA}\ \Big).$$

The obvious generalization of Proposition 1.3 fails for arbitrary quasigroup CA. If $\mathcal{B} \subset \mathcal{A}$, then $\mathcal{B}$ is a *subquasigroup* ('$\mathcal{B} \prec \mathcal{A}$') if $\mathcal{B}$ is closed under the '$*$' operation.

Lemma 2.1. *If $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ is a QGCA, and $\mathcal{B} \prec \mathcal{A}$, then $\mathcal{B}^{\mathbb{Z}}$ is a Φ-invariant subshift. If μ is the uniform Bernoulli measure on $\mathcal{B}^{\mathbb{Z}}$, then $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{N}}; \Phi; \sigma\text{-erg})$. If $|\mathcal{B}| = K$, then $h_\mu(\Phi) = \log(K)$ and Φ is K-to-1 (μ-æ).* □

If $\mathcal{B} \prec \mathcal{A}$ and $(\mathcal{A}, *)$ is a finite group, then $\mathcal{B}$ is a subgroup. Thus, if $|\mathcal{A}|$ is prime, then $\mathcal{A}$ cannot have nontrivial subquasigroups. However, other prime cardinality quasigroups can. For example, let $\mathcal{D} := \{a_1, a_2;\ b_1, b_2;\ c_1, c_2, c_3\}$ (so $|\mathcal{D}| = 7$ is prime). Given the multiplication table below, $(\mathcal{D}, *)$ has two subquasigroups: $\mathcal{A} = \{a_1, a_2\}$ and $\mathcal{B} = \{b_1, b_2\}$.

$*$	a_1	a_2	b_1	b_2	c_1	c_2	c_3
a_1	a_1	a_2	c_1	c_2	b_2	b_1	c_3
a_2	a_2	a_1	c_2	c_1	b_1	c_3	b_2
b_1	c_1	c_3	b_1	b_2	c_2	a_1	a_2
b_2	c_3	c_1	b_2	b_1	a_1	a_2	c_2
c_1	b_1	b_2	c_3	a_1	a_2	c_2	c_1
c_2	b_2	c_2	a_1	a_2	c_3	c_1	b_1
c_3	c_2	b_1	a_2	c_3	c_1	b_2	a_1

Note: If $\Phi\colon \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ is a QGCA, and $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-erg}\right)$, and $h_\mu(\Phi) > 0$, then μ is *not* necessarily the uniform measure on $\mathcal{B}^{\mathbb{Z}}$ for some $\mathcal{B} \prec \mathcal{A}$; see Examples 3.2(b,c). $\diamondsuit$

Let $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$. Any right-sided CA $\Phi\colon \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ induces a *unilateral* CA $\widetilde{\Phi}\colon \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ with the same local rule. Any $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\right)$ projects to a measure $\widetilde{\mu} \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi; \sigma\right)$, and any $\widetilde{\mu} \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi; \sigma\right)$ extends to a unique $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\right)$. In what follows, we will abuse notation and write $\widetilde{\Phi}$ as Φ.

Lemma 2.2. [3, Prop.2.3] *If $\Phi\colon \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ is right-permutative, then $(\mathcal{A}^{\mathbb{N}}, \Phi)$ is conjugate to a full shift. To be precise, define $\Xi : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ by*

$$\Xi(\mathbf{a}) := \left[a_0,\ \Phi(\mathbf{a})_0,\ \Phi^2(\mathbf{a})_0,\ \Phi^3(\mathbf{a})_0,\ \ldots\right].$$

Then Ξ is a conjugacy from $(\mathcal{A}^{\mathbb{N}}, \Phi)$ to $(\mathcal{A}^{\mathbb{N}}, \sigma)$ (ie. Ξ is a homeomorphism and $\Xi \circ \Phi = \sigma \circ \Xi$). $\square$

Let $(\mathcal{A}, *)$ be a quasigroup. The *dual* quasigroup is the set $\mathcal{A}$ equipped with binary operator $\widehat{*}$ defined: $a \mathbin{\widehat{*}} b = c$, where c is the unique element in $\mathcal{A}$ such that $a * c = b$. If $(\mathcal{A}, *)$ is a group, then $a \mathbin{\widehat{*}} b = a^{-1} * b$. If $\Phi\colon \mathcal{A}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$ is a QGCA (with local map $\phi(a, b) = a * b$), then the *dual* of Φ is the right-permutative RNNCA $\widehat{\Phi}\colon \mathcal{A}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$ with local map $\widehat{\phi}(a, b) := a \mathbin{\widehat{*}} b$ (see Figure 1).

Lemma 2.3. *Let $(\mathcal{A}, *)$ be a quasigroup. Let $\Phi\colon \mathcal{A}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$ be the corresponding QGCA.*

(a) *$(\mathcal{A}, \widehat{*})$ is a quasigroup, and $\widehat{\Phi}\colon \mathcal{A}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$ is a QGCA. The dual of $\widehat{*}$ is $*$, and the dual of $\widehat{\Phi}$ is Φ.*

(b) *Ξ is a topological conjugacy from the dynamical system $(\mathcal{A}^{\mathbb{N}}, \sigma)$ to $(\mathcal{A}^{\mathbb{N}}, \widehat{\Phi})$.*

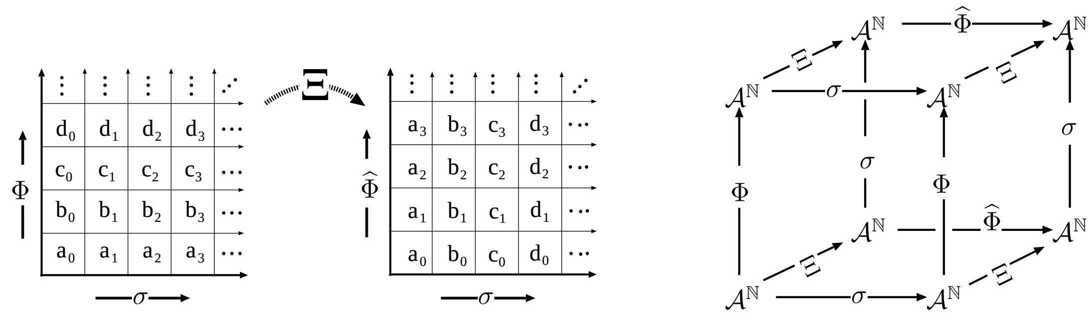
(c) *If $\mathcal{B} \subset \mathcal{A}$, then $\Big((\mathcal{B}, *) \prec (\mathcal{A}, *) \Big) \iff \Big((\mathcal{B}, \widehat{*}) \prec (\mathcal{A}, \widehat{*}) \Big)$.*

Let μ be a measure on $\mathcal{A}^{\mathbb{N}}$, and let $\widehat{\mu} := \Xi(\mu)$. Then:

(d) *$\Big(\mu$ is Φ-invariant $\Big) \iff \Big(\widehat{\mu}$ is σ-invariant $\Big)$.*

(e) *$\Big(\mu$ is σ-ergodic $\Big) \iff \Big(\widehat{\mu}$ is $\widehat{\Phi}$-ergodic $\Big)$.*

(f) *If $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi; \sigma\right)$, then $h(\Phi, \mu) = h(\widehat{\Phi}, \widehat{\mu}) = h(\sigma, \mu) = h(\sigma, \widehat{\mu})$.* $\square$



(A) The space-time diagrams of Φ and $\widehat{\Phi}$. **(B)** Ξ induces a commuting cube.

FIGURE 1.

3. **Multiplication CA on Nonabelian Groups .** Throughout this section, let $\mathcal{A}$ be a finite (possibly nonabelian) group with identity e, and let $\Phi : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ be the *nearest neighbour multiplication* CA (NNMCA), with local map $\phi(a_0, a_1) = a_0 \cdot a_1$. This type of CA was previously studied in [9, 12]. Let $\widetilde{\mathbb{N}} := \{1, 2, 3, \ldots\}$. Let $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}\right)$. For any $\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, let $\mu_{\mathbf{a}}$ be the conditional measure induced by $\mathbf{a}$ on the zeroth coordinate. That is:

$$\forall\ b \in \mathcal{A}, \quad \mu_{\mathbf{a}}(b) \quad := \quad \mu\left[x_0 = b \mid \mathbf{x}\big|_{\widetilde{\mathbb{N}}} \ = \ \mathbf{a}\right],$$

(where $\mathbf{x} \in \mathcal{A}^{\mathbb{N}}$ is a μ-random sequence). Let $\widetilde{\mu}$ be the projection of μ onto $\mathcal{A}^{\widetilde{\mathbb{N}}}$. Then we have the following disintegration [13]:

$$\mu \quad = \quad \int_{\mathcal{A}^{\widetilde{\mathbb{N}}}} (\mu_{\mathbf{a}} \otimes \delta_{\mathbf{a}})\ d\widetilde{\mu}[\mathbf{a}]. \tag{1}$$

Let $\mathcal{C} \prec \mathcal{A}$ be a subgroup. Say μ is a $\mathcal{C}$*-measure* if, for $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, $\mathsf{supp}\,(\mu_{\mathbf{a}})$ is a right coset of $\mathcal{C}$, and $\mu_{\mathbf{a}}$ is uniformly distributed on this coset. Our main result in this section is:

Theorem 3.1. *If $\Phi\colon \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ is an NNMCA, and $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi\text{-erg}; \sigma\right)$, then μ is a $\mathcal{C}$-measure for some $\mathcal{C} \prec \mathcal{A}$.* □

Example 3.2: (a) Let $\mathcal{C} \prec \mathcal{A}$ be any subgroup, and let μ be the uniform measure on $\mathcal{C}^{\mathbb{N}}$. Then μ is a $\mathcal{C}$-measure (for any $\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, $\mu_{\mathbf{a}}$ is uniform on $\mathcal{C}$), and $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi\text{-erg}; \sigma\right)$

(b) Let $\mathcal{Q} = \{\pm 1,\ \pm\mathbf{i},\ \pm\mathbf{j},\ \pm\mathbf{k}\}$ be the Quaternion group [2, §1.5], and let $\Phi_{\mathcal{Q}} : \mathcal{Q}^{\mathbb{N}} \longrightarrow \mathcal{Q}^{\mathbb{N}}$ be the NNMCA. If $\mathbf{p} := [\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \ldots]$, then $\Phi_{\mathcal{Q}}(\mathbf{p}) = [\mathbf{k}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}, \mathbf{j}, \ldots]$, so $\Phi^2_{\mathcal{Q}}(\mathbf{p}) = [\mathbf{j}, \mathbf{k}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}, \ldots]$ so $\Phi^3_{\mathcal{Q}}(\mathbf{p}) = [\mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \ldots] = \mathbf{p}$. Let $\mu_{\mathcal{Q}}$ be the measure on $\mathcal{Q}^{\mathbb{N}}$ assigning probability 1/3 to each of $\mathbf{p}$, $\Phi_{\mathcal{Q}}(\mathbf{p})$ and $\Phi^2_{\mathcal{Q}}(\mathbf{p})$. Then $\mu_{\mathcal{Q}} \in \mathcal{M}\left(\mathcal{Q}^{\mathbb{N}}; \Phi_{\mathcal{Q}}\text{-erg}; \sigma\right)$.

Now, let $\mathcal{C}$ be any other group, and let $\mathcal{A} = \mathcal{C} \times \mathcal{Q}$. Identify $\mathcal{C}$ with $\mathcal{C} \times \{1\} \prec \mathcal{A}$; then $\mathcal{C}$ is a normal subgroup of $\mathcal{A}$, and $\mathcal{Q} = \mathcal{A}/\mathcal{C}$. The cosets of $\mathcal{C}$ all have the form $\mathcal{C} \times \{q\}$ for some $q \in \mathcal{Q}$. There is a natural identification $\mathcal{A}^{\mathbb{N}} \cong \mathcal{C}^{\mathbb{N}} \times \mathcal{Q}^{\mathbb{N}}$, given: $\left[\binom{c_0}{q_0}, \binom{c_1}{q_1}, \binom{c_2}{q_2}, \ldots\right] \longleftrightarrow \left([c_0, c_1, c_2, \ldots];\ \ [q_0, q_1, q_2, \ldots]\right)$. Let $\mu_{\mathcal{C}}$ be the uniform Bernoulli measure on $\mathcal{C}^{\mathbb{N}}$, and let $\mu = \mu_{\mathcal{C}} \otimes \mu_{\mathcal{Q}}$.

Claim 1: *μ is a $\mathcal{C}$-measure.*

Proof: Let $\mathbf{a} \in \mathcal{A}^{\mathbb{N}}$ be a μ-random sequence. Then $\mathbf{a} = (\mathbf{c}, \mathbf{q})$, where $\mathbf{q} \in \{\mathbf{p},\ \Phi_{\mathcal{Q}}(\mathbf{p}),\ \Phi_{\mathcal{Q}}^2(\mathbf{p})\}$, (with probability 1/3 each), and $\mathbf{c} = (c_0, c_1, c_2, \ldots)$ is a sequence of independent, uniformly distributed random elements of $\mathcal{C}$. The coordinates $[a_1, a_2, a_3, \ldots] = \left[\binom{c_1}{q_1}, \binom{c_2}{q_2}, \binom{c_2}{q_2}, \ldots\right]$ determine $\mathbf{q}$, and thus, determine q_0. Thus, $\mu_{[a_1,a_2,a_3,\ldots]}$ is uniformly distributed on the coset $\mathcal{C} \times \{q_0\}$. ◇ `Claim 1`

Claim 2: *Let $\Phi : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ be the NNMCA. Then $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi\text{-erg}; \sigma\right)$.*

Proof: μ is clearly σ-invariant.

μ is Φ-invariant: Let $\Phi_c : \mathcal{C}^{\mathbb{N}} \longrightarrow \mathcal{C}^{\mathbb{N}}$ be the NNMCA on $\mathcal{C}^{\mathbb{N}}$. Then $\Phi = \Phi_c \times \Phi_{\mathcal{Q}}$. Thus, $\Phi(\mu) = \Phi_c(\mu_c) \otimes \Phi_{\mathcal{Q}}(\mu_{\mathcal{Q}}) = \mu_c \otimes \mu_{\mathcal{Q}} = \mu$.

μ is Φ-ergodic: The system $(\mathcal{C}^{\mathbb{N}}, \Phi_c, \mu_c)$ is mixing [7, Thm 6.3], thus weakly mixing. The system $(\mathcal{Q}^{\mathbb{N}}, \Phi_{\mathcal{Q}}, \mu_{\mathcal{Q}})$ is ergodic. Thus, the product system $(\mathcal{A}^{\mathbb{N}}, \Phi, \mu) \cong \left(\mathcal{C}^{\mathbb{N}} \times \mathcal{Q}^{\mathbb{N}},\ \Phi_c \times \Phi_{\mathcal{Q}},\ \mu_c \otimes \mu_{\mathcal{Q}}\right)$ is also ergodic [10, Thm. 2.6.1]. ◇ `Claim 2`

Note that $h(\mu, \sigma) = h(\mu_c, \sigma) = \log_2 |\mathcal{C}| > 0$, but $\mathsf{supp}(\mu) \neq \mathcal{B}^{\mathbb{N}}$ for any subgroup $\mathcal{B} \prec \mathcal{A}$.

(c) Let $(\mathcal{A}, +)$ be an abelian group, and let $\mathfrak{G} \subset \mathcal{A}^{\mathbb{Z}}$ be a ***subgroup shift*** (a closed, σ-invariant subgroup). If Φ is as in 1.1(a), then $\Phi(\mathfrak{G}) = \mathfrak{G}$. If η is the Haar measure on $\mathfrak{G}$, then $\eta \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-erg}\right)$. Note that there may be no $\mathcal{B} \prec \mathcal{A}$ so that $\mathfrak{G} = \mathcal{B}^{\mathbb{Z}}$; see [6, Example 4]. Invariant measures of additive CA on subgroup shifts are investigated in [8]. ◇

Lemma 3.3. **(a)** *If μ is a $\mathcal{C}$-measure, then $h(\mu, \sigma) = \log_2 |\mathcal{C}|$.*

(b) $\Big($ *μ is an $\mathcal{A}$-measure* $\Big) \iff \Big($ *μ is the uniform measure on $\mathcal{A}^{\mathbb{N}}$* $\Big)$.

(c) *Let $\{e\}$ be the identity subgroup. Then the following are equivalent:*

[i] *μ is an $\{e\}$-measure;* [ii] $|\mathsf{supp}(\mu_{\mathbf{a}})| = 1$, *for $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$;* [iii] $h(\mu, \sigma) = 0$.

Proof: **(a)** and **(b)** are obvious, and in **(c)**, it is clear that [i] $\iff$ [ii]. To see that [ii] $\iff$ [iii], let $\widetilde{\mathbf{F}} := \left\{\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}\ ;\ |\mathsf{supp}(\mu_{\mathbf{a}})| \geq 2\right\}$. If ρ is a measure on $\mathcal{A}$, define $H(\rho) := -\sum_{b \in \mathcal{A}} \rho\{b\} \log_2(\rho\{b\})$. Then $\Big(\ H(\rho) > 0\ \Big) \iff \Big(\ |\mathsf{supp}(\rho)| \geq 2\ \Big)$. Thus,

$$h(\mu, \sigma) \underset{(*)}{=\!=} \int_{\mathcal{A}^{\widetilde{\mathbb{N}}}} H(\mu_{\mathbf{a}})\ d\widetilde{\mu}[\mathbf{a}] \underset{(\dagger)}{=\!=} \int_{\widetilde{\mathbf{F}}} H(\mu_{\mathbf{a}})\ d\widetilde{\mu}[\mathbf{a}] \underset{(\ddagger)}{>} 0,$$

For $(*)$ see [10, Prop. 5.2.12]. $(\dagger)$ and $(\ddagger)$ are because $(H(\mu_{\mathbf{a}}) > 0) \iff \left(\mathbf{a} \in \widetilde{\mathbf{F}}\right)$, and $(\ddagger)$ holds only if $\widetilde{\mu}[\widetilde{\mathbf{F}}] > 0$. Thus, [ii] $\iff \Big(\ \widetilde{\mu}[\widetilde{\mathbf{F}}] = 0\ \Big) \iff \Big(\ h(\mu, \sigma) = 0\ \Big)$. □

Corollary 3.4. *Let $h_{\max} := \max\{\log_2 |\mathcal{C}|\ ;\ \mathcal{C}$ a proper subgroup of $\mathcal{A}\}$. If $\Phi : \mathcal{A}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$ is a NNMCA, and $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi\text{-erg}; \sigma\right)$ and $h(\mu, \sigma) > h_{\max}$, then $\mu = \lambda$.*

Proof: Theorem 3.1 says μ must be a $\mathcal{C}$-measure for some subgroup $\mathcal{C} \prec \mathcal{A}$. But if $\mathcal{B}$ is any proper subgroup, then $h(\mu, \sigma) > h_{\max} \geq \log_2 |\mathcal{B}|$, so Lemma 3.3**(a)** says $\mathcal{C}$ can't be $\mathcal{B}$. Thus, $\mathcal{C} = \mathcal{A}$. Then Lemma 3.3**(b)** says that μ is the uniform measure. □

Example 3.5: (a) If p is prime, then $\mathbb{Z}_{/p}$ has no nontrivial proper subgroups, so $h_{\max} = 0$. In this case, Corollary 3.4 becomes a special case of Proposition 1.3.

(b) If p and q are prime and p divides $q-1$, then there is a unique nonabelian group of order pq [2, §5.5]. For example, let $p=3$ and $q=7$ and let $\mathcal{A}$ be the unique nonabelian group of order 21. Then $h_{\max} = \log_2(7) \approx 2.807 < 4.392 \approx \log_2(21)$. Hence, if $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi\text{-erg}; \sigma\right)$ and $h(\mu,\sigma) \geq 2.81$, then $\mu = \lambda$. $\diamondsuit$

If $b \in \mathcal{A}$, then we define *(left) scalar multiplication* by b upon $\mathcal{A}^{\mathbb{N}}$ in the obvious way: if $\mathbf{c} = [c_0, c_1, c_2, \ldots] \in \mathcal{A}^{\mathbb{N}}$, then $b \cdot \mathbf{c} = [bc_0,\ bc_1,\ bc_2, \ldots]$. For any sequence $\mathbf{a} = [a_1, a_2, a_3, \ldots]$ in $\mathcal{A}^{\widetilde{\mathbb{N}}}$ and any $b \in \mathcal{A}$, let $[b, \mathbf{a}]$ denote the sequence $[b, a_1, a_2, a_3, \ldots]$ in $\mathcal{A}^{\mathbb{N}}$. Recall the conjugacy $\Xi : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ and the dual cellular automaton $\widehat{\Phi} : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ introduced in §2.

Lemma 3.6. *Let* $\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$*, and suppose* $\Xi(\mathbf{a}) = [b_0, b_1, b_2, \ldots]$*. Then:*

(a) $\Xi[e, \mathbf{a}] = [e,\ b_0,\ b_0 b_1,\ b_0 b_1 b_2,\ b_0 b_1 b_2 b_3, \ldots]$.

(b) *If* $b \in \mathcal{A}$*, then* $\Xi[b, \mathbf{a}] = b \cdot \Xi[e, \mathbf{a}]$*. If* $c \in \mathcal{A}$ *then* $\Xi[cb, \mathbf{a}] = c \cdot \Xi[b, \mathbf{a}]$. □

A point $\mathbf{g} \in \mathcal{A}^{\mathbb{N}}$ is (Φ, μ)-*generic* if $\mu[\mathbf{U}] = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\mathbf{U}}\left(\Phi^n(\mathbf{g})\right)$ for any cylinder set $\mathbf{U} \subset \mathcal{A}^{\mathbb{N}}$. Let $\mathcal{G}(\Phi, \mu)$ be the set of (Φ, μ)-generic points in $\mathcal{A}^{\mathbb{N}}$.

Lemma 3.7. **(a)** *If* $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi\text{-erg}\right)$*, then* $\mu[\mathcal{G}(\Phi, \mu)] = 1$.

(b) *If* $\widehat{\mu} = \Xi(\mu)$*, then* $\left(\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi\text{-erg}; \sigma\right)\right) \iff \left(\widehat{\mu} \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \widehat{\Phi}; \sigma\text{-erg}\right)\right)$.

(c) *Let* $\mathbf{g} \in \mathcal{A}^{\mathbb{N}}$*. Then* $\left(\mathbf{g} \in \mathcal{G}(\Phi, \mu)\right) \iff \left(\Xi(\mathbf{g}) \in \mathcal{G}(\sigma, \widehat{\mu})\right)$.

(d) *Let* $\widetilde{\mathbf{G}} := \left\{\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}\ ;\ [b, \mathbf{a}] \in \mathcal{G}(\Phi, \mu)\ \text{for all}\ b \in \mathsf{supp}(\mu_{\mathbf{a}})\right\}$*. Then* $\widetilde{\mu}[\widetilde{\mathbf{G}}] = 1$.

Proof: **(a)** For each cylinder set $\mathbf{C} \subset \mathcal{A}^{\mathbb{N}}$, let $\mathcal{G}_{\mathbf{C}} \subset \mathcal{A}^{\mathbb{N}}$ be the set of points which are (Φ, μ)-generic for $\mathbf{C}$; then $\mu[\mathcal{G}_{\mathbf{C}}] = 1$ by the Birkhoff Ergodic Theorem. If $\mathfrak{C}$ is the set of all cylinder sets, then $\mathfrak{C}$ is countable, and $\mathcal{G}(\Phi, \mu) = \bigcap_{\mathbf{C} \in \mathfrak{C}} \mathcal{G}_{\mathbf{C}}$.

(b) follows from Lemma 2.3(d,e). **(c)** follows from Lemma 2.2.

(d) Suppose not. For every $\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, let $\mathcal{B}_{\mathbf{a}} := \{b \in \mathsf{supp}(\mu_{\mathbf{a}})\ ;\ [b, \mathbf{a}] \notin \mathcal{G}(\Phi, \mu)\}$. Let $\widetilde{\mathbf{H}} := \mathcal{A}^{\widetilde{\mathbb{N}}} \setminus \widetilde{\mathbf{G}} = \left\{\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}\ ;\ \mathcal{B}_{\mathbf{a}} \neq \emptyset\right\}$, and let $\mathbf{H} := \left\{[b, \mathbf{h}]\ ;\ \mathbf{h} \in \widetilde{\mathbf{H}},\ b \in \mathcal{B}_{\mathbf{h}}\right\}$. If $\widetilde{\mu}[\widetilde{\mathbf{G}}] < 1$, then $\widetilde{\mu}[\widetilde{\mathbf{H}}] > 0$. Thus, $\mu[\mathbf{H}] \underset{(\dagger)}{=} \int_{\widetilde{\mathbf{H}}} \mu_{\mathbf{h}}[\mathcal{B}_{\mathbf{h}}]\ d\widetilde{\mu}[\mathbf{h}] \underset{(*)}{>} 0$, where $(\dagger)$ is by eqn.(1), and $(*)$ is because $\mu_{\mathbf{h}}[\mathcal{B}_{\mathbf{h}}] > 0$, for all $\mathbf{h} \in \widetilde{\mathbf{H}}$.
But $\mathcal{G}(\Phi, \mu) \subset \mathcal{A}^{\mathbb{N}} \setminus \mathbf{H}$, so if $\mu[\mathbf{H}] > 0$, then $\mu[\mathcal{G}(\Phi, \mu)] < 1$, contradicting (a). □

Lemma 3.8. *Let* $\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$*, and let* $b, b' \in \mathcal{A}$*. Suppose both* $[b, \mathbf{a}]$ *and* $[b', \mathbf{a}]$ *are in* $\mathcal{G}(\Phi, \mu)$.

If $c = b' \cdot b^{-1}$*, then* $\widehat{\mu}$ *is invariant under (left) scalar multiplication by* c*. In other words, for any measurable subset* $\mathbf{U} \subset \mathcal{A}^{\mathbb{N}}$*,* $\widehat{\mu}[c \cdot \mathbf{U}] = \widehat{\mu}[\mathbf{U}]$.

Proof: It suffices to check invariance for cylinder sets (they generate the Borel sigma algebra of $\mathcal{A}^{\mathbb{N}}$). Let $\mathbf{U} \subset \mathcal{A}^{\mathbb{N}}$ be a cylinder set. Let $\mathbf{g} := \Xi[b, \mathbf{a}]$ and $\mathbf{g}' := \Xi[b', \mathbf{a}]$. Then

$$\widehat{\mu}[\mathbf{U}] \underset{(\mathrm{g1})}{=} \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\mathbf{U}}\left(\sigma^n(\mathbf{g})\right) \underset{(*)}{=} \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{\mathbf{U}}\left(\sigma^n(c^{-1} \cdot \mathbf{g}')\right)$$

$$= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{(c\cdot\mathbf{U})}\left(\sigma^n(\mathbf{g}')\right) \underset{(\mathrm{g2})}{=} \widehat{\mu}[c \cdot \mathbf{U}].$$

(g1) is because $\mathbf{g} \in \mathcal{G}(\sigma, \widehat{\mu})$ and **(g2)** is because $\mathbf{g}' \in \mathcal{G}(\sigma, \widehat{\mu})$ [both by Lemma 3.7(c)]. $(*)$ is because $\mathbf{g}' = \Xi[b', \mathbf{a}] \underset{(\dagger)}{=} c \cdot \Xi[b, \mathbf{a}] = c \cdot \mathbf{g}$, where $(\dagger)$ is Lemma 3.6(b). □

Let $\widetilde{\mathbf{I}} := \left\{ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}} \,;\, \exists \text{ distinct } b, b' \in \mathcal{A} \text{ so that } [b, \mathbf{a}] \text{ and } [b', \mathbf{a}] \text{ are } (\Phi, \mu)\text{-generic} \right\}$.

Lemma 3.9. *If* $h(\mu, \sigma) > 0$*, then* $\widetilde{\mu}[\widetilde{\mathbf{I}}] > 0$ (so the hypothesis of Lemma 3.8 is nonvacuous).

Proof: Let $\widetilde{\mathbf{F}} := \left\{ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}} \,;\, |\mathsf{supp}\,(\mu_{\mathbf{a}})| \geq 2 \right\}$. Then Lemma 3.3(c) says $\widetilde{\mu}[\widetilde{\mathbf{F}}] > 0$, because $h(\mu, \sigma) > 0$. Thus, $\mu[\widetilde{\mathbf{F}} \cap \widetilde{\mathbf{G}}] > 0$, by Lemma 3.7(d). But $\widetilde{\mathbf{I}} \supseteq \widetilde{\mathbf{F}} \cap \widetilde{\mathbf{G}}$. □

Lemma 3.10. *Let* $c \in \mathcal{A}$*, and define* $\Gamma : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ *by* $\Gamma[\mathbf{a}] = c \cdot \mathbf{a}$*. If* $\widehat{\mu} = \Xi[\mu]$ *is* Γ*-invariant, then for* $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$*,* $\mu_{\mathbf{a}}$ *is invariant under left multiplication by* c*.*

Proof: Let $b \in \mathcal{A}$. Let $b' := c \cdot b$. Define measurable functions $\beta, \beta' : \mathcal{A}^{\widetilde{\mathbb{N}}} \longrightarrow \mathbb{R}$ by $\beta(\mathbf{a}) := \mu_{\mathbf{a}}(b)$ and $\beta'(\mathbf{a}) := \mu_{\mathbf{a}}(b')$. We must show that $\beta = \beta'$, $\widetilde{\mu}$-æ.

Claim 1: *Define* $\gamma : \mathcal{A}^{\mathbb{N}} \longrightarrow \mathcal{A}^{\mathbb{N}}$ *by* $\gamma[a_0, a_1, a_2, \ldots] := [c \cdot a_0,\ a_1,\ a_2, \ldots]$*. Then* μ *is* γ*-invariant.*

Proof: For any measurable subset $\mathbf{U} \subset \mathcal{A}^{\mathbb{N}}$,

$$\mu\left[\gamma(\mathbf{U})\right] \underset{(D)}{=} \widehat{\mu}\left[\Xi \circ \gamma(\mathbf{U})\right] \underset{(*)}{=} \widehat{\mu}\left[\Gamma \circ \Xi(\mathbf{U})\right] \underset{(I)}{=} \widehat{\mu}\left[\Xi(\mathbf{U})\right] \underset{(D)}{=} \mu\left[\mathbf{U}\right].$$

(D) is by definition of $\widehat{\mu}$. $(*)$ is because Lemma 3.6(b) implies $\Xi \circ \gamma = \Gamma \circ \Xi$. **(I)** is because $\widehat{\mu}$ is Γ-invariant. ◇ Claim 1

Claim 2: *For any measurable* $\widetilde{\mathbf{W}} \subset \mathcal{A}^{\widetilde{\mathbb{N}}}$, $\displaystyle\int_{\widetilde{\mathbf{W}}} \beta(\mathbf{w})\, d\widetilde{\mu}[\mathbf{w}] = \int_{\widetilde{\mathbf{W}}} \beta'(\mathbf{w})\, d\widetilde{\mu}[\mathbf{w}]$.

Proof: Let $\mathbf{U} = [b] \times \widetilde{\mathbf{W}}$, and let $\mathbf{U}' = \gamma(\mathbf{U}) = [cb] \times \widetilde{\mathbf{W}} = [b'] \times \widetilde{\mathbf{W}}$. Then:

$$\int_{\widetilde{\mathbf{W}}} \beta(\mathbf{w})\, d\widetilde{\mu}[\mathbf{w}] \underset{(*)}{=} \mu[\mathbf{U}] \underset{(\dagger)}{=} \mu[\mathbf{U}'] \underset{(*)}{=} \int_{\widetilde{\mathbf{W}}} \beta'(\mathbf{w})\, d\widetilde{\mu}[\mathbf{w}],$$

where $(*)$ is by equation (1), and $(\dagger)$ is by Claim 1. ◇ Claim 2

Claim 2 implies $\beta = \beta'$ ($\widetilde{\mu}$-æ). In other words, for $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, $\mu_{\mathbf{a}}[b] = \mu_{\mathbf{a}}[cb]$. □

Proof of Theorem 3.1: If $h(\mu, \sigma) = 0$, then μ is an $\{e\}$-measure by Lemma 3.3(c). So assume $h(\mu, \sigma) \neq 0$. Let $\mathcal{C}$ be the set of all $c \in \mathcal{A}$ so that there is some $\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$ and $b \in \mathcal{A}$ with both $[b, \mathbf{a}]$ and $[(cb), \mathbf{a}]$ in $\mathcal{G}(\Phi, \mu)$. Lemma 3.9 says $\mathcal{C} \neq \emptyset$, because $h(\mu, \sigma) \neq 0$.

Claim 1: $\mathcal{C}$ *is a group, and* $\mu_{\mathbf{a}}$ *is invariant under (left)* $\mathcal{C}$*-multiplication for* $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$.

Proof: Lemma 3.8 says that $\widehat{\mu}$ is invariant under $\mathcal{C}$-scalar multiplication. Let $\mathcal{D}$ be the group generated by $\mathcal{C}$. Then $\mathcal{C} \subseteq \mathcal{D}$, and $\widehat{\mu}$ is also invariant under $\mathcal{D}$-scalar multiplication. Lemma 3.10 implies that $\mu_{\mathbf{a}}$ is invariant under (left) $\mathcal{D}$-multiplication for $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$. It follows from Lemma 3.7(d) that $\mathcal{D} \subseteq \mathcal{C}$, and hence, $\mathcal{C} = \mathcal{D}$. ◇ Claim 1

Claim 2: *For* $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, $\mathsf{supp}(\mu_{\mathbf{a}})$ *is a (right) coset of* $\mathcal{C}$.

Proof: For $\forall_{\widetilde{\mu}}\ \mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}$, Claim 1 implies that $\mathsf{supp}(\mu_{\mathbf{a}})$ is a disjoint union of cosets of $\mathcal{C}$, and that $\mu_{\mathbf{a}}$ is uniformly distributed on each of these cosets. Let

$$\widetilde{\mathbf{M}} \quad := \quad \left\{\mathbf{a} \in \mathcal{A}^{\widetilde{\mathbb{N}}}\ ;\ \mathsf{supp}(\mu_{\mathbf{a}}) \text{ contains more than one coset of } \mathcal{C}\right\}.$$

We claim that $\widetilde{\mu}[\widetilde{\mathbf{M}}] = 0$. Suppose not. Then Lemma 3.7(d) implies that $\widetilde{\mu}[\widetilde{\mathbf{M}} \cap \widetilde{\mathbf{G}}] > 0$. So let $\mathbf{m} \in \widetilde{\mathbf{M}} \cap \widetilde{\mathbf{G}}$, and find elements $b, b' \in \mathsf{supp}(\mu_{\mathbf{m}})$ living in *different* cosets, such that $[b, \mathbf{m}]$ and $[b', \mathbf{m}]$ are both in $\mathcal{G}(\Phi, \mu)$. If $c = b^{-1}b'$, then $b' = cb$, so $c \in \mathcal{C}$. But b and b' are in different cosets of $\mathcal{C}$; hence, $c \notin \mathcal{C}$. Contradiction. ◇ `Claim 2` □

4. **Degree of QGCA relative to invariant measures.** If μ is a Φ-invariant measure, then Φ is *K-to-1 (μ-æ)* if there is a measurable subset $\mathcal{U} \subseteq \mathcal{A}^{\mathbb{Z}}$ such that: **[i]** $\mu[\mathcal{U}] = 1$; **[ii]** $\Phi^{-1}(\mathcal{U}) \underset{\mu}{=} \mathcal{U}$; and **[iii]** Every $\mathbf{u} \in \mathcal{U}$ has exactly K preimages in $\mathcal{U}$ —ie. $\left|\mathcal{U} \cap \Phi^{-1}\{\mathbf{u}\}\right| = K$. We will generalize the methods of [1] to prove:

Theorem 4.1. *Let* $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ *be a QGCA, and let* $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-erg}\right)$. *Let* $N := |\mathcal{A}|$. *Then* $\exists\ K \in [1...N]$ *so that* $h_\mu(\Phi) = \log_2(K)$, *and* Φ *is* K*-to-1 (μ-æ).* □

Example: Let λ be the uniform Bernoulli measure on $\mathcal{A}^{\mathbb{Z}}$. Then λ is invariant for any QGCA, $h_\lambda(\Phi) = \log_2(N)$, and Φ is N-to-1 (λ-æ) (set $\mathcal{U} := \mathcal{A}^{\mathbb{Z}}$ above). Indeed, λ is the only (Φ, σ)-invariant measure with entropy $\log_2(N)$. Proposition 1.3 is proved in [1] by first proving a special case of Theorem 4.1 (when Φ is an affine CA) and then showing that $K = N$. ◇

Let $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}})$. If $\mathfrak{q}$ is any partition of $\mathcal{A}^{\mathbb{Z}}$, and $\mathfrak{S}$ is any sigma-algebra, define

$$H_\mu(\mathfrak{q}\,|\mathfrak{S}) \quad := \quad \sum_{\mathbf{Q} \in \mathfrak{q}} \int_{\mathbf{Q}} \log_2\left(\mathbb{E}_\mu[\mathbf{Q}\,|\mathfrak{S}]\right)(\mathbf{x})\ d\mu[\mathbf{x}]. \tag{2}$$

If $\Psi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ is a continuous transformation (eg. either Φ or σ), and $\mathfrak{q}$ is a partition of $\mathcal{A}^{\mathbb{Z}}$, and $\infty \leq \ell \leq n \leq \infty$, define $\Psi^{[\ell,m]}(\mathfrak{q}) := \bigvee_{m=\ell}^{n} \Psi^{-m}(\mathfrak{q})$. In particular, let $\mathfrak{p}_0$ be the partition of $\mathcal{A}^{\mathbb{Z}}$ generated by zero-coordinate cylinder sets, and let $\mathfrak{p}_{[\ell,n]} := \sigma^{[\ell,n]}(\mathfrak{p}_0)$. Thus, $\mathfrak{B} := \mathfrak{p}_{[-\infty,\infty]}$ is the Borel sigma-algebra of $\mathcal{A}^{\mathbb{Z}}$. Let $\mathfrak{B}^1 := \Phi^{-1}(\mathfrak{B})$. If $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi\right)$, then $h_\mu(\Phi) = \lim_{r\to\infty} h_\mu\left(\Phi, \mathfrak{p}_{[-r,r]}\right)$, where $h_\mu\left(\Phi, \mathfrak{p}_{[-r,r]}\right) := H_\mu\left(\mathfrak{p}_{[-r,r]}\,\middle|\,\Phi^{[1,\infty]}\left(\mathfrak{p}_{[-r,r]}\right)\right)$.

Lemma 4.2. *If* $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ *is a QGCA, and* $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\right)$, *then* $h_\mu(\Phi) = H_\mu\left(\mathfrak{p}_0\,|\mathfrak{B}^1\right)$.

Proof: Let $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$ be an unknown sequence. Φ is bipermutative, so knowledge of $(\Phi^t(\mathbf{x}))_{[-r,r]}$ (for $t \in [0..T]$) determines $\mathbf{x}_{[-T-r,T+r]}$, and vice versa. Thus we get an equality of partitions: $\Phi^{[0,T]}\left(\mathfrak{p}_{[-r,r]}\right) = \mathfrak{p}_{[-T-r,T+r]}$. Letting $T\to\infty$ yields an equality of σ-algebras: $\Phi^{[0,\infty]}\left(\mathfrak{p}_{[-r,r]}\right) = \mathfrak{p}_{[-\infty,\infty]} = \mathfrak{B}$. Applying Φ^{-1} to everything yields: $\Phi^{[1,\infty]}\left(\mathfrak{p}_{[-r,r]}\right) = \Phi^{-1}(\mathfrak{B}) = \mathfrak{B}^1$. Thus,

$$\begin{aligned} h_\mu\left(\Phi, \mathfrak{p}_{[-r,r]}\right) \quad &:= \quad H_\mu\left(\mathfrak{p}_{[-r,r]}\,\middle|\,\Phi^{[1,\infty]}\left(\mathfrak{p}_{[-r,r]}\right)\right) \quad = \quad H_\mu\left(\mathfrak{p}_{[-r,r]}\,|\mathfrak{B}^1\right) \\ &\underset{(*)}{=} \quad H_\mu\left(\mathfrak{p}_0\,|\mathfrak{B}^1\right). \end{aligned}$$

$(*)$ is because Φ is bipermutative, so knowledge of $\Phi(\mathbf{x})$ and x_0 determines $\mathbf{x}$.

Thus, $h_\mu(\Phi) = \lim_{r\to\infty} h_\mu\left(\Phi, \mathfrak{p}_{[-r,r]}\right) = \lim_{r\to\infty} H_\mu\left(\mathfrak{p}_0 \,\middle|\, \mathfrak{B}^1\right) = H_\mu\left(\mathfrak{p}_0 \,\middle|\, \mathfrak{B}^1\right)$. □

For any $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, let $\mathcal{F}(\mathbf{x}) := \Phi^{-1}\{\Phi(\mathbf{x})\} = \left\{\mathbf{y} \in \mathcal{A}^{\mathbb{Z}}\ ;\ \Phi(\mathbf{y}) = \Phi(\mathbf{x})\right\}$. Hence, the sets $\mathcal{F}(\mathbf{x})$ (for $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$) are the 'minimal elements' of sigma algebra $\mathcal{B}^1$. The conditional expectation operator $\mathbb{E}_\mu\left[\bullet \,\middle|\, \mathfrak{B}^1\right]$ defines *fibre measures* $\mu_{\mathbf{x}}$ (for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$) with three properties:

(F1) For any measurable $\mathbf{U} \subset \mathcal{A}^{\mathbb{Z}}$ and for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mu_{\mathbf{x}}(\mathbf{U}) = \mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right](\mathbf{x})$.

(F2) For any fixed $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mu_{\mathbf{x}}$ is a probability measure on $\mathcal{A}^{\mathbb{Z}}$, and $\mathsf{supp}(\mu_{\mathbf{x}}) = \mathcal{F}(\mathbf{x})$.

(F3) For any fixed measurable $\mathbf{U} \subset \mathcal{A}^{\mathbb{Z}}$, the function $\mathcal{A}^{\mathbb{Z}} \ni \mathbf{x} \mapsto \mu_{\mathbf{x}}(\mathbf{U}) \in \mathbb{R}$ is $\mathfrak{B}^1$-measurable. Hence, $\mu_{\mathbf{x}} = \mu_{\mathbf{y}}$ for any $\mathbf{y} \in \mathcal{F}(\mathbf{x})$.

Our goal is to show that there is some constant K and, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, there is a subset $\mathcal{E} \subset \mathcal{F}(\mathbf{x})$ of cardinality K so that $\mu_{\mathbf{x}}$ is uniformly distributed on $\mathcal{E}$.

Lemma 4.3. *For any measurable* $\mathbf{U} \subset \mathcal{A}^{\mathbb{Z}}$ *and for* $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mu_{\mathbf{x}}\left(\sigma^{-1}(\mathbf{U})\right) = \mu_{\sigma(\mathbf{x})}(\mathbf{U})$.

Proof: For $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, **(F1)** says $\mu_{\mathbf{x}}\left(\sigma^{-1}(\mathbf{U})\right) = \mathbb{E}_\mu\left[\sigma^{-1}(\mathbf{U}) \,\middle|\, \mathfrak{B}^1\right](\mathbf{x})$ and $\mu_{\sigma(\mathbf{x})}(\mathbf{U}) = \mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right](\sigma(\mathbf{x}))$. We must show that $\mathbb{E}_\mu\left[\sigma^{-1}(\mathbf{U}) \,\middle|\, \mathfrak{B}^1\right](\mathbf{x}) = \mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right](\sigma(\mathbf{x}))$, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$. Now, $\mathbb{E}_\mu\left[\sigma^{-1}(\mathbf{U}) \,\middle|\, \mathfrak{B}^1\right]$ and $\mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right]$ are $\mathfrak{B}^1$-measurable functions, so it suffices to show that, for any $\mathbf{B} \in \mathfrak{B}^1$,

$$\int_{\mathbf{B}} \mathbb{E}_\mu\left[\sigma^{-1}(\mathbf{U}) \,\middle|\, \mathfrak{B}^1\right](\mathbf{x})\ d\mu[\mathbf{x}] \quad = \quad \int_{\mathbf{B}} \mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right](\sigma(\mathbf{x}))\ d\mu[\mathbf{x}].$$

But
$$\int_{\mathbf{B}} \mathbb{E}_\mu\left[\sigma^{-1}(\mathbf{U}) \,\middle|\, \mathfrak{B}^1\right](\mathbf{x})\ d\mu[\mathbf{x}] \underset{\text{(E)}}{=\!=} \int_{\mathbf{B}} \mathbb{1}_{\sigma^{-1}(\mathbf{U})}(\mathbf{x})\ d\mu[\mathbf{x}]$$
$$= \mu\left[\mathbf{B} \cap \sigma^{-1}(\mathbf{U})\right] \underset{\text{(I)}}{=\!=} \mu\left[\sigma(\mathbf{B}) \cap \mathbf{U}\right] = \int_{\sigma(\mathbf{B})} \mathbb{1}_{\mathbf{U}}(\mathbf{x}')\ d\mu[\mathbf{x}']$$
$$\underset{\text{(E)}}{=\!=} \int_{\sigma(\mathbf{B})} \mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right](\mathbf{x}')\ d\mu[\mathbf{x}'] \underset{\text{(S)}}{=\!=} \int_{\mathbf{B}} \mathbb{E}_\mu\left[\mathbf{U} \,\middle|\, \mathfrak{B}^1\right](\sigma(\mathbf{x}))\ d\mu[\mathbf{x}],$$

as desired. Here **(E)** is the definition of conditional expectation, **(I)** is because μ is σ-invariant, and **(S)** is the substitution $\mathbf{x}' = \sigma(\mathbf{x})$ (because μ is σ-invariant). □

For any $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, let $\eta(\mathbf{x}) := \mu_{\mathbf{x}}\{\mathbf{x}\}$. Thus, if $\mathbf{y} \in \mathcal{A}^{\mathbb{Z}}$ is an unknown, μ-random sequence, then $\eta(\mathbf{x})$ is the conditional probability that $\mathbf{y} = \mathbf{x}$, given that $\Phi(\mathbf{y}) = \Phi(\mathbf{x})$.

Lemma 4.4. **(a)** *η is σ-invariant (μ-æ).*

(b) *If $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \sigma\text{-erg}\right)$, then $\exists\ H \in \mathbb{R}$ so that $\eta(\mathbf{x}) = H$, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$.*

(c) *If $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-erg}\right)$, then:*
[i] *η is Φ-invariant (μ-æ); and* [ii] $h_\mu(\Phi) = -\log_2(H)$.

Proof: **(a)** $\eta(\sigma(\mathbf{x})) = \mu_{\sigma(\mathbf{x})}\{\sigma(\mathbf{x})\} \underset{(*)}{=\!=} \mu_{\mathbf{x}}\left(\sigma^{-1}\{\sigma(\mathbf{x})\}\right) \underset{(\dagger)}{=\!=} \mu_{\mathbf{x}}\{\mathbf{x}\} = \eta(\mathbf{x})$. $(*)$ is Lemma 4.3. $(\dagger)$ is because σ is invertible on $\mathcal{A}^{\mathbb{Z}}$. Parts **(b)** and **(c)**[i] follow.

(c)[ii]: **Claim 1:** *For all $\mathbf{P} \in \mathfrak{p}_0$, and for $\forall_\mu\ \mathbf{x} \in \mathbf{P}$,* $\mathbb{E}_\mu\left[\mathbf{P} \,\middle|\, \mathfrak{B}^1\right](\mathbf{x}) = H$.

Proof: $\mathbb{E}_\mu\left[\mathbf{P} \,\middle|\, \mathfrak{B}^1\right](\mathbf{x}) \underset{\text{(F1)}}{=\!=} \mu_{\mathbf{x}}(\mathbf{P}) \underset{\text{(F2)}}{=\!=} \mu_{\mathbf{x}}\Big(\mathbf{P} \cap \mathcal{F}(\mathbf{x})\Big) \underset{(\dagger)}{=\!=} \mu_{\mathbf{x}}\{\mathbf{x}\} = \eta(\mathbf{x}) \underset{(\flat)}{=\!=} H$. $(\flat)$ is by part **(b)**. $(\dagger)$ is because, if $\mathbf{x} \in \mathbf{P} \in \mathfrak{p}_0$, then $\mathbf{P} \cap \mathcal{F}(\mathbf{x}) = \{\mathbf{x}\}$ (because Φ is bipermutative, so any $\mathbf{y} \in \mathcal{F}(\mathbf{x})$ is determined by y_0. But if $\mathbf{y} \in \mathbf{P}$, then $y_0 = x_0$, so $\mathbf{y} = \mathbf{x}$). ◇ Claim 1

$$\text{Thus,}\quad h_\mu(\Phi) \underset{(*)}{=\!=} -\sum_{\mathbf{P}\in\mathfrak{p}_0}\int_{\mathbf{P}} \log_2\left(\mathbb{E}_\mu\left[\mathbf{P}\,\middle|\,\mathfrak{B}^1\right]\right)(\mathbf{x})\ d\mu[\mathbf{x}]$$

$$\underset{(\dagger)}{=\!=} -\sum_{\mathbf{P}\in\mathfrak{p}_0}\int_{\mathbf{P}} \log_2(H)\ d\mu \quad = \quad -\log_2(H).$$

$(*)$ is by Lemma 4.2 and eqn.(2). $(\dagger)$ is by Claim 1. □

We must now show that $H = \frac{1}{K}$ for some K. Let $N := |\mathcal{A}|$, and identify $\mathcal{A}$ with the group $\mathbb{Z}_{/N}$ in an arbitrary way. Define $\tau : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ as follows. For any $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\tau(\mathbf{x}) = \mathbf{y}$, where $\mathbf{y}$ is the unique element in $\mathcal{F}(\mathbf{x})$ such that $y_0 = x_0 + 1$ (mod N). Existence/uniqueness of $\mathbf{y}$ follows from bipermutativity.

Note that $\tau(\mu) \neq \mu$, so a statement which is true μ-æ may *not* be true $\tau(\mu)$-æ. For example, Lemma 4.4**(c)**[i] does *not* imply $\eta\left(\Phi\left[\tau(\mathbf{x})\right]\right) = \eta\left(\tau(\mathbf{x})\right)$ for $\forall_\mu\ \mathbf{x}$.

For any $n \in \mathbb{Z}_{/N}$, let $\mathbf{E}_n := \left\{\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}\ ;\ \eta\left(\tau^n(\mathbf{x})\right) > 0\right\}$. Let $\mu_n := \tau^n\left(\mathbb{1}_{\mathbf{E}_n} \cdot \mu\right)$.

Lemma 4.5. *Let $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi; \sigma\text{-erg}\right)$. Then for any $n \in \mathbb{Z}_{/N}$, the following hold:*
- **(a)** *μ_n is absolutely continuous relative to μ.*
- **(b)** *η is Φ-invariant (μ_n-æ).*
- **(c)** *For $\forall_\mu\ \mathbf{x} \in \mathbf{E}_n$, $\quad \eta(\mathbf{x}) \ = \ \eta\left(\tau^n(\mathbf{x})\right)$.*

Proof: **(a)** Let $\mathbf{Z} \subset \mathcal{A}^{\mathbb{Z}}$ be Borel-measurable. If $\mu[\mathbf{Z}] = 0$, we must show $\mu_n[\mathbf{Z}] = 0$.

Claim 1: *For $\forall_\mu\ \mathbf{z} \in \tau^{-n}(\mathbf{Z})$, $\quad \eta\left(\tau^n(\mathbf{z})\right) = 0$; hence $\mathbf{z} \notin \mathbf{E}_n$.*

Proof: $\eta\left(\tau^n(\mathbf{z})\right) := \mu_{\tau^n(\mathbf{z})}\{\tau^n(\mathbf{z})\} \underset{(F3)}{=\!=} \mu_{\mathbf{z}}\{\tau^n(\mathbf{z})\} \underset{(*)}{\leq} \mu_{\mathbf{z}}[\mathbf{Z}] \underset{(\dagger)}{=\!=} 0.$

$(*)$ is because $\mathbf{z} \in \tau^{-n}(\mathbf{Z})$, so $\tau^n(\mathbf{z}) \in \mathbf{Z}$. $(\dagger)$ is because $\int_{\mathcal{A}^{\mathbb{Z}}} \mu_{\mathbf{x}}[\mathbf{Z}]\ d\mu[\mathbf{x}] = \mu[\mathbf{Z}] = 0$, hence $\mu_{\mathbf{x}}[\mathbf{Z}] = 0$, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$. ◇ `Claim 1`

Hence $\mu_n[\mathbf{Z}] \ = \ \left(\mathbb{1}_{\mathbf{E}_n} \cdot \mu\right)\left[\tau^{-n}(\mathbf{Z})\right] \ = \ \mu\left[\tau^{-n}(\mathbf{Z}) \cap \mathbf{E}_n\right] \underset{(*)}{=\!=} 0$, where $(*)$ is Claim 1.

(b) Part **(a)** means that "μ-æ" implies "μ_n-æ". Now invoke Lemma 4.4**(c)**[i].

(c) $\eta(\mathbf{x}) \underset{(\dagger)}{=\!=} \eta\left(\Phi[\mathbf{x}]\right) \underset{(*)}{=\!=} \eta\left(\Phi\left[\tau^n(\mathbf{x})\right]\right) \underset{(\flat)}{=\!=} \eta\left(\tau^n(\mathbf{x})\right)$. Here, $(\dagger)$ is Lemma 4.4**(c)**[i], $(*)$ is because $\tau^n(\mathbf{x}) \in \mathcal{F}(\mathbf{x})$, and $(\flat)$ is by part **(b)**. □

Now, let $\mathcal{E}(\mathbf{x}) := \{\mathbf{y} \in \mathcal{F}(\mathbf{x})\ ;\ \eta(\mathbf{y}) > 0\}$.

Corollary 4.6. *For $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\quad \mu_{\mathbf{x}}$ is equidistributed on $\mathcal{E}(\mathbf{x})$. If $|\mathcal{E}(\mathbf{x})| = K$, then $\mu_{\mathbf{x}}\{\mathbf{y}\} = \frac{1}{K}$ for all $\mathbf{y} \in \mathcal{E}(\mathbf{x})$. Hence, $\eta(\mathbf{x}) \ = \ \frac{1}{K}$.*

Proof: $1 \underset{(F2)}{=\!=} \mu_{\mathbf{x}}\left(\mathcal{F}(\mathbf{x})\right) = \sum_{\mathbf{y}\in\mathcal{F}(\mathbf{x})} \mu_{\mathbf{x}}\{\mathbf{y}\} \underset{(*)}{=\!=} \sum_{\mathbf{y}\in\mathcal{E}(\mathbf{x})} \eta(\mathbf{x}) = K \cdot \eta(\mathbf{x})$, so $\eta(\mathbf{x}) = \frac{1}{K}$.

To see $(*)$, let $\mathbf{y} \in \mathcal{F}(\mathbf{x})$. Then $\mu_{\mathbf{x}}\{\mathbf{y}\} \underset{(F3)}{=\!=} \mu_{\mathbf{y}}\{\mathbf{y}\} = \eta(\mathbf{y})$. If $\mathbf{y} \notin \mathcal{E}(\mathbf{x})$, then $\eta(\mathbf{y}) = 0$. If $\mathbf{y} \in \mathcal{E}(\mathbf{x})$, let $\mathbf{y} = \tau^n(\mathbf{x})$ for $n \in \mathbb{Z}_{/N}$. Then $\mathbf{x} \in \mathbf{E}_n$, so $\eta(\mathbf{y}) = \eta(\mathbf{x})$ by Lemma 4.5(c). □

Corollary 4.7. *There exists $K \in [1..N]$ so that, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\quad |\mathcal{E}(\mathbf{x})| = K$, and so that $\mu_{\mathbf{x}}\{\mathbf{y}\} = \frac{1}{K}$ for all $\mathbf{y} \in \mathcal{E}(\mathbf{x})$. Thus, $h_\mu(\Phi) = \log_2(K)$.*

Proof: Corollary 4.6 implies that $H = \frac{1}{K}$ in Lemma 4.4**(b)**. Now apply Lemma 4.4**(c)**[ii]. □

Proof of Theorem 4.1: Let $\mathcal{U} := \{\mathbf{x} \in \mathcal{A}^{\mathbb{Z}} ; |\mathcal{E}(\mathbf{x})| = K\}$. Then Corollary 4.7 says $\mu(\mathcal{U}) = 1$. Since μ is Φ-invariant, it follows that $\mu(\Phi^{-1}(\mathcal{U})) = 1$ also; hence $\Phi^{-1}(\mathcal{U}) \underset{\mu}{=} \mathcal{U}$.

Thus, for $\forall_\mu\, \mathbf{u} \in \mathcal{U}$, there is some $\mathbf{x} \in \mathcal{U}$ so that $\Phi(\mathbf{x}) = \mathbf{u}$. But then $\Phi^{-1}(\mathbf{u}) = \mathcal{F}(\mathbf{x})$, so $\Phi^{-1}(\mathbf{u}) \cap \mathcal{U} = \mathcal{F}(\mathbf{x}) \cap \mathcal{U} = \mathcal{E}(\mathbf{x})$ is a set of cardinality K, by definition of $\mathcal{U}$. □

5. **Endomorphic Cellular Automata.** A *group shift* is a sequence space $\mathcal{A}^{\mathbb{Z}}$ equipped with a topological group structure such that σ is a group automorphism. Equivalently, the multiplication operation $\bullet$ on $\mathcal{A}^{\mathbb{Z}}$ is defined by some *local multiplication map* $\psi : \mathcal{A}^{[-\ell..r]} \times \mathcal{A}^{[-\ell..r]} \longrightarrow \mathcal{A}$ so that, if $\mathbf{a}, \mathbf{b} \in \mathcal{A}^{\mathbb{Z}}$ and $\mathbf{c} = \mathbf{a} \bullet \mathbf{b}$, then $c_0 = \psi(a_{-\ell}, \ldots, a_r;\ b_{-\ell}, \ldots, b_r)$. The most obvious group shift is a *product group*, where $\mathcal{A}$ is a finite group and multiplication on $\mathcal{A}^{\mathbb{Z}}$ is defined componentwise. However, this is not the only group shift [6].

An *endomorphic cellular automaton* (ECA) is a cellular automaton $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ which is also a group endomorphism of $\mathcal{A}^{\mathbb{Z}}$. For example, it is easy to verify:

Proposition 5.1. *Let $(\mathcal{A}, +)$ be an additive abelian group. Let $\mathcal{A}^{\mathbb{Z}}$ be the product group. Let $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be a RNNCA, with local map $\phi : \mathcal{A}^{\{0,1\}} \longrightarrow \mathcal{A}$. Then:*

(a) *Φ is an ECA if and only if $\phi(a_0, a_1) = \phi_0(a_0) + \phi_1(a_1)$, where ϕ_0, ϕ_1 are endomorphisms of $\mathcal{A}$.*

(b) *Φ is bipermutative if and only if ϕ_0 and ϕ_1 are automorphisms of $\mathcal{A}$.* □

A *beca* is a bipermutative, right-sided, nearest-neighbour endomorphic cellular automaton. Let $\mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma^{\text{-tot}})$ be the set of Φ-invariant and totally σ-ergodic measures on $\mathcal{A}^{\mathbb{Z}}$. If $\mathcal{G}$ is a group, let $\mathsf{Aut}(\mathcal{G})$ be the automorphism group of $\mathcal{G}$. If $\psi \in \mathsf{Aut}(\mathcal{G})$ (eg. $\mathcal{G} = \mathcal{A}^{\mathbb{Z}}$ and $\phi = \sigma$) then "$\mathcal{H} \underset{\phi}{\prec} \mathcal{G}$" means $\mathcal{H} \subset \mathcal{G}$ is a ϕ-invariant subgroup of $\mathcal{G}$. Say $\mathcal{G}$ is *ϕ-primitive* if there are no proper nontrivial $\mathcal{H} \underset{\phi}{\prec} \mathcal{G}$. The main result of this section is:

Theorem 5.2. *Let $\mathcal{A}^{\mathbb{Z}}$ be a group shift and let $\Phi \colon \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be a beca such that $\ker(\Phi)$ is σ-primitive. If $\mu \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma^{\text{-tot}})$, and $h_\mu(\Phi) > 0$, then $\mu = \lambda$.* □

Recall from §4 that if $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, then $\mathcal{F}(\mathbf{x}) := \Phi^{-1}\{\Phi(\mathbf{x})\}$.

Lemma 5.3. *Let $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be a beca on a group shift. Let $\mathcal{K} := \ker(\Phi)$.*

(a) *For any $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mathcal{F}(\mathbf{x}) = \mathbf{x} \bullet \mathcal{K}$.*

(b) *Let $\mathbf{e} \in \mathcal{A}^{\mathbb{Z}}$ be the identity element. Then $\mathbf{e}$ is a constant sequence —ie. there is some $e \in \mathcal{A}$ so that $\mathbf{e} = (\ldots., e, e, e, \ldots.)$.*

(c) *$\mathcal{K} \underset{\sigma}{\prec} \mathcal{A}^{\mathbb{Z}}$. Also, if $\mathbf{k} \in \mathcal{K}$, then $\mathbf{k}$ is entirely determined by k_0.*

(d) *There is a natural bijection $\zeta : \mathcal{A} \longrightarrow \mathcal{K}$, where $\zeta[a]$ is the unique $\mathbf{k} \in \mathcal{K}$ with $k_0 = a$. In particular, $\zeta[e] = \mathbf{e}$.*

(e) *There is a permutation $\rho : \mathcal{A} \longrightarrow \mathcal{A}$ so that $\sigma \circ \zeta = \zeta \circ \rho$. In particular, $\rho(e) = e$.*

Hence, every element of $\mathcal{K}$ is P-periodic, for some $P < |\mathcal{A}|$.

(f) *Any $\mathcal{J} \underset{\sigma}{\prec} \mathcal{K}$ is thus a disjoint union of periodic σ-orbits.*

(g) $\Big(\ \mathcal{A} \setminus \{e\}$ *consists of a single ρ-orbit* $\Big) \iff \Big(\ \mathcal{K}$ *is σ-primitive* $\Big)$.

Proof: **(a)** is a basic property of group homomorphisms. For **(b)** recall that $\sigma \in \mathsf{Aut}(\mathcal{A}^{\mathbb{Z}})$, so $\sigma(\mathbf{e}) = \mathbf{e}$, so $\mathbf{e}$ must be constant. **(c)** follows from **(b)** because Φ is bipermutative. Then **(c)** $\Longrightarrow$ **(d)** $\Longrightarrow$ **(e)** $\Longrightarrow$ **(f)** $\Longrightarrow$ **(g)**. □

If $(\mathcal{A},+)$ is abelian and $\mathcal{A}^{\mathbb{Z}}$ is the product group, then Lemma 5.3 takes the form:

Lemma 5.4. *Let $(\mathcal{A},+)$ be an abelian group. Let $\mathcal{A}^{\mathbb{Z}}$ be the product group. Let $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be a beca and let $\mathcal{K} := \ker(\Phi)$.*

(a) *For any $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mathcal{F}(\mathbf{x}) = \mathbf{x} + \mathcal{K}$.*

(b) *The map $\zeta : \mathcal{A} \longrightarrow \mathcal{K}$ in* Lemma 5.3**(d)** *is a group isomorphism.*

(c) *$\rho \in \mathsf{Aut}(\mathcal{A})$, in* Lemma 5.3**(e)**. *To be precise, suppose Φ has local map $\phi(a_0, a_1) = \phi_0(a_0) + \phi_1(a_1)$, where $\phi_0, \phi_1 \in \mathsf{Aut}(\mathcal{A})$, as in* Proposition 5.1**(b)**. *Then $\rho = -\phi_1^{-1} \circ \phi_0$.*

(d) *If $\mathcal{J} \underset{\sigma}{\prec} \mathcal{K}$, then $\mathcal{J} = \zeta(\mathcal{B})$, for some $\mathcal{B} \underset{\rho}{\prec} \mathcal{A}$.*

(e) $\Big($ *$\mathcal{A}$ is ρ-primitive* $\Big) \iff \Big($ *$\mathcal{K}$ is σ-primitive* $\Big)$.

Proof: **(b)** To see that ζ is a group homomorphism, suppose $\mathbf{k} = \zeta(a)$ and $\mathbf{k}' = \zeta(a')$. Let $\mathbf{j} = \mathbf{k} + \mathbf{k}'$ and let $\mathbf{i} = \zeta(a + a')$; we must show $\mathbf{j} = \mathbf{i}$. The operation on $\mathcal{K}$ is componentwise addition, so $j_0 = k_0 + k_0' = a + a' = i_0$. Then Lemma 5.3**(c)** implies $\mathbf{i} = \mathbf{j}$. Hence, ζ is a homomorphism, and thus, an isomorphism (it is bijective). All other claims follow. □

Let η be as in §4, and for any $\mathbf{k} \in \mathcal{K}$, let $\mathbf{E_k} := \left\{\mathbf{x} \in \mathcal{A}^{\mathbb{Z}} \ ; \ \eta(\mathbf{x} \bullet \mathbf{k}) > 0\right\}$.

Lemma 5.5. *Suppose $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{N}}; \Phi; \sigma\text{-erg}\right)$. For any $\mathbf{k} \in \mathcal{K}$, the following hold:*

(a) $\sigma(\mathbf{E_k}) \underset{\mu}{=} \mathbf{E}_{\sigma(\mathbf{k})}$. **(b)** *Thus, if $\sigma^P(\mathbf{k}) = \mathbf{k}$, then $\sigma^P(\mathbf{E_k}) \underset{\mu}{=} \mathbf{E_k}$.*

Proof: **(a)** For $\forall_\mu\ \mathbf{x} \in \mathbf{E_k}$, $0 < \eta(\mathbf{x} \bullet \mathbf{k}) \underset{(*)}{=} \eta\Big(\sigma(\mathbf{x} \bullet \mathbf{k})\Big) = \eta\Big(\sigma(\mathbf{x}) \bullet \sigma(\mathbf{k})\Big)$, and thus, $\sigma(\mathbf{x}) \in \mathbf{E}_{\sigma(\mathbf{k})}$. Hence $\sigma(\mathbf{E_k}) \underset{\mu}{\subseteq} \mathbf{E}_{\sigma(\mathbf{k})}$. By symmetric reasoning, $\mathbf{E}_{\sigma(\mathbf{k})} \underset{\mu}{\subseteq} \sigma(\mathbf{E_k})$.

To see $(*)$, define $\mu_{\mathbf{k}} \in \mathcal{M}(\mathcal{A}^{\mathbb{Z}})$ by $\mu_{\mathbf{k}}[\mathbf{U}] := \mu\left[\mathbf{E_k} \cap (\mathbf{U} \bullet \mathbf{k}^{-1})\right]$. Then $\mu_{\mathbf{k}}$ is absolutely continuous with respect to μ, by reasoning similar to Lemma 4.5(a); hence η is σ-invariant ($\mu_{\mathbf{k}}$-æ), by reasoning similar to Lemma 4.5(b). □

Corollary 5.6. *For any $\mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, let $\mathcal{E}(\mathbf{x}) := \{\mathbf{y} \in \mathcal{F}(\mathbf{x}) \ ; \ \eta(\mathbf{y}) > 0\}$ as in §4. If $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma\text{-tot}\right)$, then there exists $\mathcal{J} \underset{\sigma}{\prec} \mathcal{K}$ so that, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mathcal{E}(\mathbf{x}) = \mathbf{x} \bullet \mathcal{J}$.*

Proof: Define $\mathcal{J} := \{\mathbf{k} \in \mathcal{K} \ ; \ \mu(\mathbf{E_k}) > 0\}$.

Claim 1: *For any $\mathbf{j} \in \mathcal{J}$, $\mu(\mathbf{E_j}) = 1$.*

Proof: Lemma 5.3**(e)** yields $P \in \mathbb{N}$ so that $\sigma^P(\mathbf{j}) = \mathbf{j}$. Then Lemma 5.5**(b)** says that $\sigma^P(\mathbf{E_j}) = \mathbf{E_j}$. But μ is σ^P-ergodic; hence $\mu(\mathbf{E_j}) = 1$. ◇ `Claim 1`

Claim 2: *For $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, $\mathcal{E}(\mathbf{x}) = \mathbf{x} \bullet \mathcal{J}$.*

Proof: $\mathcal{E}(\mathbf{x}) = \{\mathbf{x} \bullet \mathbf{k} \ ; \ \mathbf{k} \in \mathcal{K},\ \mathbf{x} \in \mathbf{E_k}\}$, so we must show: for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, and all $\mathbf{k} \in \mathcal{K}$, $\Big(\mathbf{x} \in \mathbf{E_k} \Big) \iff \Big(\mathbf{k} \in \mathcal{J} \Big)$. Now, $\mu\left[\bigcup_{\mathbf{k} \in \mathcal{K} \setminus \mathcal{J}} \mathbf{E_k}\right] = 0$, by definition of $\mathcal{J}$, and $\mu\left[\bigcap_{\mathbf{j} \in \mathcal{J}} \mathbf{E_j}\right] = 1$, by Claim 1. Thus, for $\forall_\mu\ \mathbf{x} \in \mathcal{A}^{\mathbb{Z}}$, we have $\mathbf{x} \in \bigcap_{\mathbf{j} \in \mathcal{J}} \mathbf{E_j} \ \setminus \bigcup_{\mathbf{k} \in \mathcal{K} \setminus \mathcal{J}} \mathbf{E_k}$. ◇ `Claim 2`

Let $\mathcal{U} := \mathbf{E_e} = \left\{\mathbf{x} \in \mathcal{A}^{\mathbb{Z}} \ ; \ \eta(\mathbf{x}) > 0\right\}$.

Claim 3: *If $\mathbf{k} \in \mathcal{K}$, then* $\Big(\mathbf{k} \in \mathcal{J} \Big) \iff \Big(\mathcal{U} \bullet \mathbf{k} \underset{\mu}{\subseteq} \mathcal{U} \Big)$.

Proof: $\Big(\mathbf{k} \in \mathcal{J} \Big) \overset{\dagger *}{\iff} \Big(\mu\left[\mathbf{E_k}\right] = 1 \Big) \overset{*\diamond}{\iff} \Big(\mu\left[\mathcal{U} \cap \mathbf{E_k}\right] = 1 \Big) \overset{\ddagger}{\iff}$

$\Big($ For $\forall_\mu$ $\mathbf{u} \in \mathcal{U}$, $\eta(\mathbf{u} \bullet \mathbf{k}) > 0 \Big)$ $\overset{\diamond}{\iff}$ $\Big($ For $\forall_\mu$ $\mathbf{u} \in \mathcal{U}$, $\mathbf{u} \bullet \mathbf{k} \in \mathcal{U} \Big)$ $\iff$ $\Big(\mathcal{U} \bullet \mathbf{k} \underset{\mu}{\subset} \mathcal{U} \Big)$. Here $(*)$ is by Claim 1, $(\dagger)$ is by definition of $\mathcal{J}$, $(\ddagger)$ is by definition of $\mathbf{E_k}$, and $(\diamond)$ is by definition of $\mathcal{U}$. ◇ Claim 3

Claim 4: *$\mathcal{J}$ is a subgroup of $\mathcal{K}$.*

Proof: Let $\mathbf{j}_1, \mathbf{j}_2 \in \mathcal{J}$, and $\mathbf{j} := \mathbf{j}_1 \bullet \mathbf{j}_2$. Claim 3 says $\mathcal{U} \bullet \mathbf{j} = (\mathcal{U} \bullet \mathbf{j}_1) \bullet \mathbf{j}_2 \underset{\mu}{\subset} \mathcal{U} \bullet \mathbf{j}_2 \underset{\mu}{\subset} \mathcal{U}$. Claim 3 then says $\mathbf{j} \in \mathcal{J}$. Thus $\mathcal{J}$ is closed under '$\bullet$'; being finite, $\mathcal{J}$ is a subgroup. ◇ Claim 4

To see that $\sigma^{-1}(\mathcal{J}) = \mathcal{J}$, let $\mathbf{k} \in \mathcal{K}$. Then $\Big(\mathbf{k} \in \mathcal{J} \Big)$ $\overset{\dagger}{\iff}$ $\Big(\mu[\mathbf{E_k}] = 1 \Big)$ $\overset{*}{\iff}$ $\Big(\mu\left[\sigma(\mathbf{E_k})\right] = 1 \Big)$ $\overset{\ddagger}{\iff}$ $\Big(\mu\left[\mathbf{E}_{\sigma(\mathbf{k})}\right] = 1 \Big)$ $\overset{*}{\iff}$ $\Big(\sigma(\mathbf{k}) \in \mathcal{J} \Big)$ $\iff$ $\Big(\mathbf{k} \in \sigma^{-1}(\mathcal{J}) \Big)$. Here, $(\dagger)$ is by Claim 1, $(*)$ is because μ is σ-invariant, and $(\ddagger)$ is by Lemma 5.5(a). □

Corollary 5.7. *Let $J := |\mathcal{J}|$. Then $h_\mu(\Phi) = \log(J)$, and Φ is J-to-1 (μ-æ).*

Proof: Combine Corollary 5.6 with Corollary 4.7. □

Proof of Theorem 5.2: If $h_\mu(\Phi) > 0$, then Corollary 5.7 says $|\mathcal{J}| > 1$. But $\mathcal{J} \underset{\sigma}{\prec} \mathcal{K}$, and $\mathcal{K}$ is σ-primitive, so $\mathcal{J} = \mathcal{K}$. Thus, $|\mathcal{J}| = |\mathcal{K}| \underset{(*)}{=} |\mathcal{A}|$, where $(*)$ is by Lemma 5.3**(d)**. Thus, $h_\mu(\sigma) \underset{(*)}{=} h_\mu(\Phi) \underset{(\dagger)}{=} \log|\mathcal{A}|$, which means $\mu = \lambda$. Here $(*)$ is by Lemma 2.3(f) and $(\dagger)$ is by Corollary 5.7. □

Lemmas 5.3**(g)** and 5.4**(e)** characterize when $\mathcal{K}$ is σ-primitive. For example, let $p \in \mathbb{N}$ be prime, and $\mathcal{A} := (\mathbb{Z}_{/p})^N$ for some $N > 0$. Then $\mathcal{A}$ is a vector space over the field $\mathbb{Z}_{/p}$, and $\rho : \mathcal{A} \longrightarrow \mathcal{A}$ is a group automorphism iff ρ is a $\mathbb{Z}_{/p}$-linear automorphism. Thus, ρ can be described by an $N \times N$ matrix $\mathbf{M}$ of coefficients in $\mathbb{Z}_{/p}$. Furthermore, $\mathcal{B} \subset \mathcal{A}$ is a (ρ-invariant) subgroup iff $\mathcal{B}$ is a (ρ-invariant) subspace. The ρ-invariant subspaces in $\mathcal{A}$ are described by the *rational canonical form* [2, §12.2] of ρ, which is a matrix $\widetilde{\mathbf{M}}$, similar to $\mathbf{M}$, of the form

$$\widetilde{\mathbf{M}} = \begin{bmatrix} \mathbf{M}_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \mathbf{M}_L \end{bmatrix}, \text{ where, for all } \ell \in [1..L],\ \mathbf{M}_\ell = \left[\begin{array}{c|c} 0 \dots 0 & m_{\ell 1} \\ \hline \mathbf{Id} & \vdots \\ & m_{\ell r_\ell} \end{array}\right],$$

(for some $r_\ell > 0$ and $m_{\ell 1}, \ldots, m_{\ell r_\ell} \in \mathbb{Z}_{/p}$, and where $\mathbf{Id}$ is an identity matrix). Each *component matrix* $\mathbf{M}_\ell$ corresponds to a ρ-invariant subspace of $\mathcal{A}$. We say $\rho \in \mathsf{Aut}(\mathcal{A})$ is *simple* if its rational canonical form has only one component.

Lemma 5.8. $\Big($ *ρ is simple* $\Big) \iff \Big($ *$\mathcal{A}$ is ρ-primitive.* $\Big)$. □

Corollary 5.9. *Let $\mathcal{A} = (\mathbb{Z}_{/p})^N$. Let $\mathcal{A}^{\mathbb{Z}}$ be the product group. Let $\Phi : \mathcal{A}^{\mathbb{Z}} \longrightarrow \mathcal{A}^{\mathbb{Z}}$ be a beca with local map $\phi(a_0, a_1) = \phi_0(a_0) + \phi_1(a_1)$. If $\rho = -\phi_1^{-1} \circ \phi_0$ is simple, then the conclusion of* Theorem 5.2 *holds.*

Proof: Combine Lemma 5.8 with parts **(c)** and **(e)** of Lemma 5.4. □

Example 5.10: Let $\mathcal{A} = (\mathbb{Z}_{/7})^4$, and let $\phi(a_0, a_1) = \phi_0(a_0) + a_1$, where ϕ_0 has matrix

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Thus, $\rho = -\phi_0$ is simple. Hence, if $\mu \in \mathcal{M}\left(\mathcal{A}^{\mathbb{Z}}; \Phi; \sigma^{\text{-tot}}\right)$ and $h_\mu(\Phi) > 0$, then $\mu = \lambda$. ♢

REFERENCES

[1] Bernard Host, Alejandro Maass and Servet Martínez. Uniform Bernoulli measure in dynamics of permutative cellular automata with algebraic local rules. *Discrete & Continuous Dynamical Systems*, 9(6):1423–1446, 2003.

[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Prentice-Hall, Englewood Cliffs, NJ, 1991.

[3] F. Blanchard and A. Maass. Dynamical properties of expansive one-sided cellular automata. *Isreal J. Math.*, 99:149–174, 1997.

[4] G. Hedlund. Endomorphisms and automorphisms of the shift dynamical systems. *Mathematical System Theory*, 3:320–375, 1969.

[5] J. Dénes and A.D. Keedwell. *Latin squares and their applications*. Academic Press, New York, 1974.

[6] Bruce Kitchens. Expansive dynamics in zero-dimensional groups. *Ergodic Theory & Dynamical Systems*, 7:249–261, 1987.

[7] Rune Kleveland. Mixing properties of one-dimensional cellular automata. *Proceedings of the AMS*, 125(6):1755–1766, June 1997.

[8] A. Maass, S. Martínez, M. Pivato, and R. Yassawi. Asymptotic randomization of subgroup shifts by linear cellular automata. (submitted), 2004.

[9] Cris Moore. Quasi-linear cellular automata. *Physica D*, 103:100–132, 1997.

[10] Karl Petersen. *Ergodic Theory*. Cambridge University Press, New York, 1989.

[11] Hala O. Pflugfelder. *Quasigroups and Loops: Introduction*, volume 7 of *Sigma Series in Pure Math B*. Heldermann Verlag, Berlin, 1990.

[12] M. Pivato. Multiplicative cellular automata on nilpotent groups: Structure, entropy, and asymptotics. *Journal of Statistical Physics*, 110(1/2):247–267, January 2003.

[13] Laurent Schwartz. *Lectures on disintegration of measures*. Tata Institute of Fundamental Research, Bombay, 1975.

Received September 2003; first revision April 2004; second revision December 2004.

E-mail address: pivato@xaravve.trentu.ca