Journal of Statistical Physics, Vol. 110, Nos. 1/2, January 2003 (© 2003)

Multiplicative Cellular Automata on Nilpotent Groups: Structure, Entropy, and Asymptotics

Marcus Pivato[1]

Received November 5, 2001; accepted June 28, 2002

If $\mathbb{M} = \mathbb{Z}^D$, and $\mathscr{B}$ is a finite (nonabelian) group, then $\mathscr{B}^{\mathbb{M}}$ is a compact group; a *multiplicative cellular automaton* (MCA) is a continuous transformation $\mathfrak{G}: \mathscr{B}^{\mathbb{M}} \to \mathscr{B}^{\mathbb{M}}$ which commutes with all shift maps, and where nearby coordinates are combined using the multiplication operation of $\mathscr{B}$. We characterize when MCA are group endomorphisms of $\mathscr{B}^{\mathbb{M}}$, and show that MCA on $\mathscr{B}^{\mathbb{M}}$ inherit a natural structure theory from the structure of $\mathscr{B}$. We apply this structure theory to compute the measurable entropy of MCA, and to study convergence of initial measures to Haar measure.

KEY WORDS: Cellular automata; group; structure; entropy; Haar.

1. INTRODUCTION

If $\mathscr{B}$ is a finite set, and $\mathbb{M}$ is some indexing set, then the *configuration space* $\mathscr{B}^{\mathbb{M}}$ is the set of all $\mathbb{M}$-indexed sequences of elements on $\mathscr{B}$. If $\mathscr{B}$ is discretely topologised, then the Tychonoff product topology on $\mathscr{B}^{\mathbb{M}}$ is compact, totally disconnected, and metrizable. If $\mathbb{M}$ is an abelian monoid (e.g., $\mathbb{M} = \mathbb{Z}^D$, $\mathbb{N}^E$, or $\mathbb{Z}^D \times \mathbb{N}^E$), then the action of $\mathbb{M}$ on itself by translation induces a natural *shift action* of $\mathbb{M}$ on configuration space: for all $\mathsf{v} \in \mathbb{M}$, and $\mathbf{b} = [b_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}] \in \mathscr{B}^{\mathbb{M}}$, define $\boldsymbol{\sigma}^{\mathsf{v}}[\mathbf{b}] = [b'_{\mathsf{m}}|_{\mathsf{m} \in \mathbb{M}}]$ where, $\forall \mathsf{m}$, $b'_{\mathsf{m}} = b_{\mathsf{v}+\mathsf{m}}$.

A *cellular automaton* (CA) is a continuous map $\mathfrak{G}: \mathscr{B}^{\mathbb{M}} \to \mathscr{B}^{\mathbb{M}}$ which commutes with all shifts: for any $\mathsf{m} \in \mathbb{M}$, $\boldsymbol{\sigma}^{\mathsf{m}} \circ \mathfrak{G} = \mathfrak{G} \circ \boldsymbol{\sigma}^{\mathsf{m}}$. A result of Curtis, Hedlund, and Lyndon[(1)] says any CA is determined by a *local map* $\mathfrak{g}: \mathscr{B}^{\mathbb{V}} \to \mathscr{B}$ (where $\mathbb{V} \subset \mathbb{M}$ is some finite subset), so that, for all $\mathsf{m} \in \mathbb{M}$, if we define $\mathsf{m} + \mathbb{V} = \{\mathsf{m} + \mathsf{v}; \mathsf{v} \in \mathbb{V}\}$, and for all $\mathbf{b} \in \mathscr{B}^{\mathbb{M}}$, if we define $\mathbf{b}|_{(\mathsf{m}+\mathbb{V})}$ to be the restriction of $\mathbf{b}$ to an element of $\mathscr{B}^{(\mathsf{m}+\mathbb{V})}$, then $\mathfrak{G}(\mathbf{b})_{\mathsf{m}} = \mathfrak{g}(\mathbf{b}|_{\mathsf{m}+\mathbb{V}})$.

[1] Department of Mathematics, Trent University, Peterborough, Ontario, Canada; e-mail: marcuspivato@trentu.ca

0022-4715/03/0100-0247/0

If $(\mathscr{B}, \cdot)$ is a finite multiplicative group, let $\mathbf{End}[\mathscr{B}]$ be the set of group endomorphisms of $\mathscr{B}$. A *multiplicative cellular automaton* (MCA) is a CA whose local map is a product of affine endomorphisms of separate coordinates. To be precise, let $v: [1 \cdots I] \to \mathbb{V}$ be a (possibly noninjective) map, let $\mathfrak{g}_1, \mathfrak{g}_2, \ldots, \mathfrak{g}_I \in \mathbf{End}[\mathscr{B}]$, and let $g_0, g_1, \ldots, g_I \in \mathscr{B}$ be constants. If $\mathbf{b} = [b_\mathsf{v}|_{\mathsf{v} \in \mathbb{V}}] \in \mathbb{G}^{\mathbb{V}}$, then the local map $\mathfrak{g}$ has the form:

$$\mathfrak{g}(\mathbf{b}) = g_0 \cdot \mathfrak{g}_1(b_{v[1]}) \cdot g_1 \cdot \mathfrak{g}_2(b_{v[2]}) \cdot g_2 \cdot \ldots \cdot g_{I-1} \cdot \mathfrak{g}_I(b_{v[I]}) \cdot g_I \tag{1}$$

The *ordering function* v imposes an order on this product, which is necessary if $\mathscr{B}$ is nonabelian. The endomorphisms $[\mathfrak{g}_i|_{i=1}^I]$ are called the *coefficients* of $\mathfrak{G}$. We can rewrite Eq. (1) as

$$\mathfrak{g}(\mathbf{b}) = g \cdot \mathfrak{g}'_1(b_{v[1]}) \cdot \mathfrak{g}'_2(b_{v[2]}) \cdot \ldots \cdot \mathfrak{g}'_I(b_{v[I]}) = g \cdot \prod_{i=1}^{I} \mathfrak{g}'_i(b_{v[i]}), \tag{2}$$

where $g = g_0 \cdot g_1 \cdot \ldots \cdot g_I$, and, for each $i \in [1 \cdots I]$, $\mathfrak{g}'_i(b) = (g_I g_{I-1} \cdots g_i)^{-1} \cdot \mathfrak{g}_i(b) \cdot (g_I g_{I-1} \cdots g_i)$ is an endomorphism. The product "$\prod_{i=1}^I$" inherits the obvious order from $[1 \cdots I]$. We assume MCAs are written in the form (2), and call g the *bias*. If the bias is trivial ($\mathfrak{G}$ is "unbiased"), then $\mathfrak{g}(\mathbf{b})$ is just a product of endomorphic images of the components $\{b_\mathsf{v}\}_{\mathsf{v} \in \mathbb{V}}$.

$\mathscr{B}^{\mathbb{M}}$ is a compact group under componentwise multiplication; an *endomorphic cellular automaton* (ECA) is a topological group endomorphism $\mathfrak{G}: \mathscr{B}^{\mathbb{M}} \to \mathscr{B}^{\mathbb{M}}$ which commutes with all shift maps. If $\mathscr{B}$ is abelian, then all unbiased MCA are ECA, and vice versa; when $\mathscr{B}$ is nonabelian, however, the ECA form only a small subclass of MCA (see Section 2).

Example 1. Consider the following local maps:

(a) Let $\mathbb{M} = \mathbb{Z}$, $\mathbb{V} = \{0, 1\}$, and let $\mathfrak{g}(b_0, b_1) = b_0 \cdot b_1$.

(b) $\mathbb{M} = \mathbb{N}$, $\mathbb{V} = [0 \cdots 2]$; $\mathfrak{g}(b_0, b_1, b_2) = b_0 \cdot b_1 \cdot b_2$.

(c) $\mathbb{M} = \mathbb{N}$, $\mathbb{V} = [0 \cdots 2]$; $\mathfrak{g}(b_0, b_1, b_2) = b_2^4 \cdot b_1^3 \cdot b_0$.

(d) $\mathbb{M} = \mathbb{Z}^2$, $\mathbb{V} = [-1 \cdots 1]^2$; $\mathfrak{g}(\mathbf{b}) = (g \cdot b_{(-1,0)} \cdot g^{-1}) \cdot b_{(0,-1)} \cdot b_{(0,0)} \cdot b_{(0,1)} \cdot h \cdot b_{(1,0)}^{-1}$, where $g, h \in \mathscr{B}$ are constants.

(e) Suppose $\mathscr{B} = \mathbb{GL}^n(\mathbb{F})$ is the group of invertible $n \times n$ matrices over a finite field $\mathbb{F}$ and let $\mathfrak{g}(\mathbf{B}_{-1}, \mathbf{B}_0, \mathbf{B}_1) = \det[\mathbf{B}_{-1}] \cdot \det[\mathbf{B}_1]^2 \cdot \mathbf{B}_0$.

Example 1a is the *nearest-neighbour multiplication* CA.[2,3] Examples 1a–c are unbiased, and all coefficients are the identity map on $\mathscr{B}$.

In Example 1c, $v\colon [1\cdots 8] \to [0\cdots 2]$ is defined: $v[1] = v[2] = v[3] = v[4] = 2$, $v[5] = v[5] = v[7] = 1$, and $v[8] = 0$; by repeating indices in this way, we can obtain any exponents we want.

In Example 1d, suppose $\mathbf{card}[\mathcal{B}] = B$; then $v\colon [1\cdots 4+B] \to \mathbb{V}$ is defined: $v[1] = (-1, 0)$, $v[2] = (0, -1)$, $v[3] = (0, 0)$, $v[4] = (0, 1)$, and $v[n] = (1, 0)$ for $n \in [5\cdots 4+B]$; in this way, we obtain the exponent $b_{(1,0)}^{B-1} = b_{(1,0)}^{-1}$. All coefficients are the identity map, except for $\mathfrak{g}_1(b) = g \cdot b \cdot g^{-1}$, which is the endomorphism of conjugation-by-g.

In Example 1e, let $\mathbf{I} \in \mathbb{GL}^n(\mathbb{F})$ be the identity matrix. Then $\mathfrak{g}_1(\mathbf{B}) = \det[\mathbf{B}] \cdot \mathbf{I}$ and $\mathfrak{g}_2(\mathbf{B}) = \det[\mathbf{B}]^2 \cdot \mathbf{I}$ are endomorphisms of $\mathbb{GL}^n(\mathbb{F})$, and $\mathfrak{g}_3 = \mathbf{Id}$. In fact, Example 1e is an ECA.

When $\mathcal{B}$ is an additive abelian group (e.g., $\mathcal{B} = (\mathbb{Z}_{/p}, +)$), unbiased MCA are called *linear* CA (or *affine* CA, when biased). Classical modular arithmetic has been applied to study the entropy,(4) and computational complexity(2, 3) of linear CA, while techniques of harmonic analysis yield convergence of initial probability measures on $\mathcal{B}^{\mathbb{M}}$ to the uniformly distributed, or *Haar* measure under iteration by affine CA.(5–9) However, the case when $\mathcal{B}$ is nonabelian is poorly understood; "abelian" techniques usually fail to apply.

In Section 2, we give necessary and sufficient conditions for an MCA to be endomorphic. In Section 3, we use the structure theory of the group $\mathcal{B}$ to develop a corresponding structure theory for MCA over $\mathcal{B}$. We apply this structure theory in Section 4, to compute the measurable entropy of MCA, and in Section 5 to establish sufficient conditions for convergence of initial measures to Haar measure under iteration of MCA. The major results are Theorems 4, 16, and 21.

2. ENDOMORPHIC CELLULAR AUTOMATA

Suppose $\mathfrak{G}\colon \mathcal{B}^{\mathbb{M}} \to \mathcal{B}^{\mathbb{M}}$ is an ECA. Since $\mathfrak{G} \in \mathbf{End}[\mathcal{B}^{\mathbb{M}}]$, the local map $\mathfrak{g}$ must be a group homomorphism from the product group $\mathcal{B}^{\mathbb{V}}$ into $\mathcal{B}$. This constrains the coefficients $\{\mathfrak{g}_{\mathsf{v}}\}_{\mathsf{v}\in\mathbb{V}}$ and their interactions.

Lemma 2. Let $\mathfrak{g}\colon \mathcal{B}^{\mathbb{V}} \to \mathcal{B}$ be a group homomorphism. Then there are endomorphisms $\mathfrak{g}_{\mathsf{v}} \in \mathbf{End}[\mathcal{B}]$ for all $\mathsf{v} \in \mathbb{V}$ so that, for any $\mathbf{b} = [b_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}] \in \mathcal{B}^{\mathbb{V}}$, $\mathfrak{g}(\mathbf{b}) = \prod_{\mathsf{v}\in\mathbb{V}} \mathfrak{g}_{\mathsf{v}}(b_{\mathsf{v}})$, where this product is commutative.

Proof. For each $\mathsf{v} \in \mathbb{V}$, let $\mathfrak{i}_{\mathsf{v}}\colon \mathcal{B} \to \mathcal{B}^{\mathbb{V}}$ be the embedding into the vth coordinate: for any $b \in \mathcal{B}$, $(\mathfrak{i}_{\mathsf{v}}(b))_{\mathsf{v}} = b$, and $(\mathfrak{i}_{\mathsf{v}}(b))_{\mathsf{w}} = e$ for all $\mathsf{w} \neq \mathsf{v}$ in $\mathbb{V}$, where $e \in \mathcal{B}$ is the identity element. Then define $\mathfrak{g}_{\mathsf{v}} = \mathfrak{g} \circ \mathfrak{i}_{\mathsf{v}}$. If $\mathbf{b} = [b_{\mathsf{v}}|_{\mathsf{v}\in\mathbb{V}}]$, then clearly, $\mathbf{b} = \prod_{\mathsf{v}\in\mathbb{V}} \mathfrak{i}_{\mathsf{v}}(b_{\mathsf{v}})$, where the factors all commute, and thus, $\mathfrak{g}(\mathbf{b}) = \mathfrak{g}(\prod_{\mathsf{v}\in\mathbb{V}} \mathfrak{i}_{\mathsf{v}}(b_{\mathsf{v}})) = \prod_{\mathsf{v}\in\mathbb{V}} \mathfrak{g}(\mathfrak{i}_{\mathsf{v}}(b_{\mathsf{v}})) = \prod_{\mathsf{v}\in\mathbb{V}} \mathfrak{g}_{\mathsf{v}}(b_{\mathsf{v}})$, where, again, the factors all commute. ∎

We say two endomorphisms $\mathfrak{g}_\mathsf{w}$ and $\mathfrak{g}_\mathsf{v}$ have *commuting images* if, for any $b_\mathsf{w}, b_\mathsf{v} \in \mathscr{B}$, $\mathfrak{g}_\mathsf{v}(b_\mathsf{v}) \cdot \mathfrak{g}_\mathsf{w}(b_\mathsf{w}) = \mathfrak{g}_\mathsf{w}(b_\mathsf{w}) \cdot \mathfrak{g}_\mathsf{v}(b_\mathsf{v})$. Thus, the coefficients of any ECA $\mathfrak{G}$ must all have commuting images; this restricts the structure of $\mathfrak{G}$, and the more noncommutative $\mathscr{B}$ itself is, the more severe the restriction becomes. The noncommutativity of $\mathscr{B}$ is measured by two subgroups: the *centre*, $Z(\mathscr{B}) = \{z \in \mathscr{B}; \forall b \in \mathscr{B}, b \cdot z = z \cdot b\}$, and the *commutator subgroup*, $[\mathscr{B}, \mathscr{B}] = \langle b \cdot h \cdot b^{-1} \cdot h^{-1}; b, h \in \mathscr{B} \rangle$. If $\phi: \mathscr{B} \to \mathscr{A}$ is any homomorphism from $\mathscr{B}$ into an abelian group $\mathscr{A}$, then $[\mathscr{B}, \mathscr{B}] \subset \ker[\phi]$.

Corollary 3. Contining with the previous notation,

1. If $\exists \mathsf{v} \in \mathbb{V}$ so that $\mathfrak{g}_\mathsf{v}$ is surjective, then, for all other $\mathsf{w} \in \mathbb{V}$, $\mathsf{image}[\mathfrak{g}_\mathsf{w}] \subset Z(\mathscr{B})$. If $Z(\mathscr{B}) = \{e\}$, then all other coefficients of $\mathfrak{g}$ are trivial.

2. Suppose $\mathsf{v} \neq \mathsf{w} \in \mathbb{V}$ are such that $\mathfrak{g}_\mathsf{v} = \mathfrak{g}_\mathsf{w}$. Then $\mathsf{image}[\mathfrak{g}_\mathsf{v}]$ is an abelian subgroup of $\mathscr{B}$, and thus, $[\mathscr{B}, \mathscr{B}] \subset \ker[\mathfrak{g}_\mathsf{v}]$. Thus, if $[\mathscr{B}, \mathscr{B}] = \mathscr{B}$, then $\mathfrak{g}_\mathsf{v}$ and $\mathfrak{g}_\mathsf{w}$ are trivial.

3. If $\mathscr{B}$ is simple but nonabelian, then only one coefficient of $\mathfrak{G}$ can be nontrivial; this coefficient is an automorphism.

Proof. Parts 1 and 2 are straightforward. To see Part 3, note that $Z(\mathscr{B})$ is a normal subgroup, so if $\mathscr{B}$ is simple nonabelian, then $Z(\mathscr{B}) = \{e\}$. On the other hand, any endomorphism of $\mathscr{B}$ is either trivial or an automorphism. Hence, if $\mathfrak{G}$ is nontrivial, it must have one automorphic coefficient, and then, by Part 1 all other coefficients must be trivial. ▮

3. STRUCTURE THEORY

We now relate the structure of the group $\mathscr{B}$ to the structure of MCA on $\mathscr{B}^\mathbb{M}$. We review the structure theory of dynamical systems in Section 3.1 and group structure theory in Section 3.2. In Section 3.3, we show that, if $\mathscr{A}$ is a fully characteristic subgroup of $\mathscr{B}$, and $\mathscr{C} = \mathscr{B}/\mathscr{A}$, then the decomposition of $\mathscr{B}$ into $\mathscr{A}$ and $\mathscr{C}$ yields a corresponding decomposition of MCA on $\mathscr{B}^\mathbb{M}$.

Notation. We will often decompose objects (e.g., groups, spaces, measures, functions) into factor and cofactor components. We will use three lexicographically consecutive letters to indicate, respectively, the cofactor, product, and factor (e.g., for groups: $\mathscr{A} \hookrightarrow \mathscr{B} \twoheadrightarrow \mathscr{C}$; for measure spaces: $(\mathbf{Y}, \mathscr{Y}, \mu) = (\mathbf{X} \times \mathbf{Z}, , \mathscr{X} \otimes \mathscr{Z}, \lambda \otimes \nu)$; for dynamical systems, $\mathsf{G} = \mathsf{F} \star \mathsf{H}$; for cellular automata, $\mathfrak{G} = \mathfrak{F} \star \mathfrak{H}$, and for their local maps, $\mathfrak{g} = \mathfrak{f} \star \mathfrak{h}$, etc.).

3.1. Relative and Nonhomogeneous CA

Let $\mathbf{X}$ and $\mathbf{Z}$ be a topological spaces. A topological $\mathbf{Z}$-*relative dynamical system*[10, 11] on $\mathbf{X}$ is a continuous map $\mathsf{F}: \mathbf{X} \times \mathbf{Z} \to \mathbf{X}$. We write the second argument of F as a subscript: for $(x, z) \in \mathbf{X} \times \mathbf{Z}$, $\mathsf{F}(x, z)$ is written as "$\mathsf{F}_z(x)$." Thus, F is treated as a $\mathbf{Z}$-parameterized family of *fibre maps* $\{\mathsf{F}_z: \mathbf{X} \to \mathbf{X}\}_{z \in \mathbf{Z}}$. Let $\mathscr{M}[\mathbf{X}]$ be the set of Borel probability measures on $\mathbf{X}$; if $\lambda \in \mathscr{M}[\mathbf{X}]$, then F is λ-*preserving* if $\mathsf{F}_z(\lambda) = \lambda$ for all $z \in \mathbf{Z}$.

If $\mathsf{H}: \mathbf{Z} \to \mathbf{Z}$ is a topological dynamical system, then the *skew product* of F and H is the topological dynamical system $\mathsf{G} = \mathsf{F} \star \mathsf{H}$ on $\mathbf{Y} = \mathbf{X} \times \mathbf{Z}$ defined: $\mathsf{G}(x, z) = (\mathsf{F}_z(x), \mathsf{H}(z))$. Now, suppose $\mathbf{X} = \mathscr{A}^{\mathbb{M}}$ and $\mathbf{Z} = \mathscr{C}^{\mathbb{M}}$, where $\mathscr{A}$ and $\mathscr{C}$ are finite sets. If $\mathscr{B} = \mathscr{A} \times \mathscr{C}$, then there is a natural bijection $\mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \cong \mathscr{B}^{\mathbb{M}}$. A $\mathscr{C}$-*relative cellular automaton* (RCA) on $\mathscr{A}^{\mathbb{M}}$ is a continuous map $\mathfrak{F}: \mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ which commutes with all shift maps: $\boldsymbol{\sigma}^{\mathsf{m}} \circ \mathfrak{F} = \mathfrak{F} \circ \boldsymbol{\sigma}^{\mathsf{m}}$, for all $\mathsf{m} \in \mathbb{M}$. Like an ordinary CA, $\mathfrak{F}$ is determined by a *local map* $\mathfrak{f}: \mathscr{A}^{\mathbb{V}} \times \mathscr{C}^{\mathbb{V}} \to \mathscr{A}$, where $\mathbb{V} \subset \mathbb{M}$ is finite, so that, for all $(\mathbf{a}, \mathbf{c}) \in \mathscr{B}^{\mathbb{M}}$, and $\mathsf{m} \in \mathbb{M}$, $\mathfrak{F}(\mathbf{a}, \mathbf{c})_{\mathsf{m}} = \mathfrak{f}(\mathbf{a}|_{\mathsf{m}+\mathbb{V}}, \mathbf{c}|_{\mathsf{m}+\mathbb{V}})$. For any $\mathbf{c} \in \mathscr{C}^{\mathbb{V}}$, the *local fibre map* $\mathfrak{f}_{\mathbf{c}}: \mathscr{A}^{\mathbb{V}} \to \mathscr{A}$ is defined by $\mathfrak{f}_{\mathbf{c}}(\mathbf{a}) = \mathfrak{f}(\mathbf{c}, \mathbf{a})$. If $\mathscr{A}$ is a group and $\mathfrak{f}_{\mathbf{c}}$ is a product of affine endomorphisms for every $\mathbf{c} \in \mathscr{C}^{\mathbb{V}}$, then $\mathfrak{F}$ is called a *multiplicative* relative cellular automaton (MRCA).

If $\mathfrak{H}: \mathscr{C}^{\mathbb{M}} \to \mathscr{C}^{\mathbb{M}}$ is a CA with local map $\mathfrak{h}: \mathscr{C}^{\mathbb{V}} \to \mathscr{C}$, then the *skew product* $\mathfrak{F} \star \mathfrak{H}$ is a CA on $\mathscr{B}^{\mathbb{M}}$, with local map $\mathfrak{g}: \mathscr{B}^{\mathbb{V}} \cong \mathscr{A}^{\mathbb{V}} \times \mathscr{C}^{\mathbb{V}} \to \mathscr{B}$ defined: $\mathfrak{g}(\mathbf{a}, \mathbf{c}) = (\mathfrak{f}_{\mathbf{c}}(\mathbf{a}), \mathfrak{h}(\mathbf{c}))$.

A *nonhomogeneous cellular automaton* (NHCA) is a continuous map $\mathfrak{G}: \mathscr{B}^{\mathbb{M}} \to \mathscr{B}^{\mathbb{M}}$ which does *not* necessarily commute with shift maps, but where there is some finite $\mathbb{V} \subset \mathbb{M}$, so that, for all $\mathsf{m} \in \mathbb{M}$, there is a local map $\mathfrak{g}_{\mathsf{m}}: \mathscr{B}^{(\mathsf{m}+\mathbb{V})} \to \mathscr{B}$ so that, $\forall \mathbf{b} \in \mathscr{B}^{\mathbb{M}}$, $\mathfrak{G}(\mathbf{b})_{\mathsf{m}} = \mathfrak{g}_{\mathsf{m}}(\mathbf{b}|_{(\mathsf{m}+\mathbb{V})})$. Thus, for example, any CA is an NHCA. If $\mathfrak{F}: \mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is an RCA, then, for any $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$, the fibre map $\mathfrak{F}_{\mathbf{c}}: \mathscr{A}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is an NHCA.

3.2. Group Structure Theory

Let $\mathscr{B}$ be a group. A subgroup $\mathscr{A} \subset \mathscr{B}$ is called *fully characteristic*[12] if, for every $\phi \in \mathbf{End}[\mathscr{B}]$, we have $\phi(\mathscr{A}) \subset \mathscr{A}$. We indicate this: "$\mathscr{A} \prec \mathscr{B}$." For example, if $Z(\mathscr{B})$ is the center of $\mathscr{B}$, then $Z(\mathscr{B}) \prec \mathscr{B}$. Observe that any fully characteristic subgroup is normal.

The main result of this section is:

Theorem 4. Suppose that $\mathscr{A} \prec \mathscr{B}$, and $\mathscr{B}/\mathscr{A} = \mathscr{C}$. If $\mathfrak{G}: \mathscr{B}^{\mathbb{M}} \to \mathscr{B}^{\mathbb{M}}$ is an MCA, then there is an MCA $\mathfrak{H}: \mathscr{C}^{\mathbb{M}} \to \mathscr{C}^{\mathbb{M}}$ and an MRCA $\mathfrak{F}: \mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ so that $\mathfrak{G} = \mathfrak{F} \star \mathfrak{H}$.

We will prove this result in Section 3.3, and also describes the structure of the local maps of $\mathfrak{H}$ and $\mathfrak{F}$ (see Proposition 8). First we introduce the relevant algebraic machinery.

Semidirect Products and Pseudoproducts. Suppose $\mathscr{A} \subset \mathscr{B}$ is a normal subgroup, and $\mathscr{C} = \mathscr{B}/\mathscr{A}$, and let $\pi\colon \mathscr{B} \twoheadrightarrow \mathscr{C}$ be the quotient map. Let $\varsigma\colon \mathscr{C} \rightarrowtail \mathscr{B}$ be a section of π —that is, for all $c \in \mathscr{C}$, $\pi(\varsigma(c)) = c$. For any $a \in \mathscr{A}$ and $c \in \mathscr{C}$, we define $a \star c := a \cdot \varsigma(c)$. For every $b \in \mathscr{B}$, there are unique $a \in \mathscr{A}$ and $c \in \mathscr{C}$ so that $b = a \star c$. Thus, the map $\mathscr{A} \times \mathscr{C} \ni (a, c) \mapsto a \star c \in \mathscr{B}$ is a bijection.[2] We call $\mathscr{B}$ a *pseudoproduct* of $\mathscr{A}$ and $\mathscr{C}$, and write: "$\mathscr{B} = \mathscr{A} \star \mathscr{C}$."

If $c \in \mathscr{C}$, the *conjugation automorphism* $c^* \in \mathbf{Aut}[\mathscr{A}]$ is defined:

$$c^*a = \varsigma(c) \cdot a \cdot \varsigma(c)^{-1}.$$

Thus, multiplication using pseudoproduct notation satisfies the equation:

$$(a_1 \star c_1) \cdot (a_2 \star c_2) = (a_1 \cdot \varsigma(c_1)) \cdot (a_2 \cdot \varsigma(c_2)) = a_1 \cdot (c_1^* a_2) \cdot (\varsigma(c_1) \cdot \varsigma(c_2)). \tag{3}$$

In general, $\varsigma(c_1) \cdot \varsigma(c_2)$ does not equal $\varsigma(c_1 \cdot c_2)$; *this* is true only $\mathscr{B}$ is a *semidirect product* of $\mathscr{A}$ and $\mathscr{C}$. In this case, ς is an isomorphism from $\mathscr{C}$ into an embedded subgroup $\varsigma(\mathscr{C}) \subset \mathscr{B}$, and (3) becomes:

$$(a_1 \star c_1) \cdot (a_2 \star c_2) = (a_1 \cdot (c_1^* a_2)) \star (c_1 \cdot c_2). \tag{4}$$

In this case, we write: "$\mathscr{B} = \mathscr{A} \rtimes \mathscr{C}$." We can treat $\mathscr{C}$ as embedded in $\mathscr{B}$, so ς is just the identity, and $a \star c = a \cdot c$.

We call $\mathscr{B}$ a *polymorph* of $\mathscr{A}$ if: (1) $\mathscr{B} = \mathscr{A} \rtimes \mathscr{C}$; (2) $\mathscr{A}$ and $\varsigma(\mathscr{C})$ are both fully characteristic in $\mathscr{B}$; and (3) $c^* \in Z(\mathbf{Aut}[\mathscr{A}])$, for every $c \in \mathscr{C}$.

Example 5.

(a) Let $\mathscr{B} = \mathbf{Q}_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ be the *Quaternion Group*, defined by: $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, and $q_1 \cdot q_2 = q_3 = -q_2 \cdot q_1$ for $(q_1, q_2, q_3) = (\mathbf{i}, \mathbf{j}, \mathbf{k})$ or any cyclic permutation thereof. Let $\mathscr{A} = Z(\mathbf{Q}_8) = \{\pm 1\}$; then $\mathscr{C} = \mathbf{Q}_8/\mathscr{A} \cong \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$. Define homomorphism $\pi\colon \mathbf{Q}_8 \to \mathscr{C}$ by $\pi(\pm 1) = \mathbf{O} := (0, 0)$, $\pi(\pm \mathbf{i}) = \mathbf{I} := (1, 0)$, $\pi(\pm \mathbf{j}) = \mathbf{J} := (0, 1)$, $\pi(\pm \mathbf{k}) = \mathbf{K} := (1, 1)$, with $\ker[\pi] = \{\pm 1\} = \mathscr{A}$. If $\varsigma\colon \mathscr{C} \to \mathscr{B}$ is defined: $\varsigma(\mathbf{O}) = 1$, $\varsigma(\mathbf{I}) = \mathbf{i}$, $\varsigma(\mathbf{J}) = \mathbf{j}$, $\varsigma(\mathbf{K}) = \mathbf{k}$, then ς induces a (non-semidirect) pseudoproduct structure $\mathbf{Q}_8 = \mathscr{A} \star \mathscr{C}$. In this case, $\mathscr{A} = Z(\mathscr{B})$, and multiplication satisfies the formula:

[2] ... but generally not a homomorphism.

$$\begin{aligned}(a_1 \star c_1)\cdot(a_2 \star c_2)\\ = (a_1 \cdot a_2 \cdot \zeta(c_1, c_2)) \star (c_1 \cdot c_2) \qquad \text{for all} \quad a_1, a_2 \in \mathscr{A}, \quad c_1, c_2 \in \mathscr{C}.\end{aligned}$$

Here, $\zeta(c_1, c_2) = \varsigma(c_1 \cdot c_2)^{-1} \cdot \varsigma(c_1) \cdot \varsigma(c_2) = \mathsf{sign}[\varsigma(c_1) \cdot \varsigma(c_2)]$. For example, $\zeta(\mathbf{I}, \mathbf{J}) = \mathsf{sign}[\mathbf{k}] = +1$, while $\zeta(\mathbf{J}, \mathbf{I}) = \mathsf{sign}[-\mathbf{k}] = -1$, and $\zeta(\mathbf{O}, c) = 1$ for any $c \in \mathscr{C}$.

(b) If p is prime and $\mathscr{A} = (\mathbb{Z}_{/p}, +)$ is the (additive) cyclic group of order p, then $\mathbf{Aut}[\mathscr{A}]$ is the (multiplicative) group $(\mathbb{Z}_{/p}{}^{\times}, \cdot)$ of nonzero elements of the field $\mathbb{Z}_{/p}$, acting on $\mathbb{Z}_{/p}$ by multiplication, mod p. The group $(\mathbb{Z}_{/p}{}^{\times}, \cdot)$ is isomorphic to $(\mathbb{Z}_{/p-1}, +)$; thus, $\mathscr{B} = \mathbb{Z}_{/p} \rtimes \mathbb{Z}_{/p}{}^{\times} \cong \mathbb{Z}_{/p} \rtimes \mathbb{Z}_{/p-1}$ is a group of order $p \cdot (p-1)$, and $\mathbb{Z}_{/p}$ is a characteristic subgroup. Since $\mathbb{Z}_{/p}{}^{\times}$ is itself abelian, $\mathscr{B}$ is a polymorph of $\mathbb{Z}_{/p}$.

If q divides $p-1$, then there is a cyclic multiplicative subgroup $\mathbf{C}_q \subset \mathbb{Z}_{/p}{}^{\times}$ of order q. The semidirect product $\mathbf{D}_{p;\,q} = \mathbb{Z}_{/p} \rtimes \mathbf{C}_q$, is also a polymorph of $\mathbb{Z}_{/p}$. For example, if $p = 7$, then $\mathbf{C}_3 = \{1, 2, 4\}$, and $\mathbf{D}_{7;\,3} = \mathbb{Z}_{/7} \rtimes \mathbf{C}_3$ has cardinality 21.

3.3. The Induced Decomposition

If $\mathscr{B} = \mathscr{A} \star \mathscr{C}$, then for any $\mathbf{a} \in \mathscr{A}^{\mathbb{M}}$ and $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$, define $\mathbf{b} = \mathbf{a} \star \mathbf{c} \in \mathscr{B}^{\mathbb{M}}$ by $b_{\mathsf{m}} = a_{\mathsf{m}} \star c_{\mathsf{m}}$ for all $\mathsf{m} \in \mathbb{M}$; we will thus identify $\mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}}$ with $\mathscr{B}^{\mathbb{M}}$.

Suppose $\mathscr{B} = \mathscr{A} \rtimes \mathscr{C}$, and let $\mathfrak{G}\colon \mathscr{B}^{\mathbb{Z}} \to \mathscr{B}^{\mathbb{Z}}$ be the *nearest neighbour multiplication* CA, Example 1a. If $\mathbf{b} = \mathbf{a} \star \mathbf{c}$, then Moore[3] noted that

$$\mathfrak{g}(b_0, b_1) = (a_0 \star c_0) \cdot (a_1 \star c_1) = (a_0 \cdot c_0^{*} a_1) \star (c_0 \cdot c_1) = \mathfrak{f}_{\mathsf{c}}(a_0, a_1) \star \mathfrak{h}(c_0, c_1)$$

where $\mathfrak{h}\colon \mathscr{C}^{\{0,1\}} \to \mathscr{C}$ is defined $\mathfrak{h}(c_0, c_1) = c_0 \cdot c_1$, and $\mathfrak{f}\colon \mathscr{A}^{\{0,1\}} \times \mathscr{C}^{\{0,1\}} \to \mathscr{A}$ is defined $\mathfrak{f}_{\mathsf{c}}(a_0, a_1) = a_0 \cdot c_0^{*} a_1$. Thus, $\mathfrak{G} = \mathfrak{F} \star \mathfrak{H}$, where $\mathfrak{H}\colon \mathscr{C}^{\mathbb{M}} \to \mathscr{C}^{\mathbb{M}}$ is the CA with local map $\mathfrak{h}$, and $\mathfrak{F}\colon \mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is the RCA with local map $\mathfrak{f}$. In other words, the decomposition of $\mathscr{B} = \mathscr{A} \rtimes \mathscr{C}$ induces a decomposition of $\mathfrak{G}$. We now generalize this idea to arbitrary MCA.

Lemma 6. Suppose $\mathscr{A} \prec \mathscr{B}$, $\mathscr{C} = \mathscr{B}/\mathscr{A}$, and $\mathscr{B} = \mathscr{A} \star \mathscr{C}$. Let $\mathfrak{g} \in \mathbf{End}[\mathscr{B}]$.

1. There exist $\mathfrak{f} \in \mathbf{End}[\mathscr{A}]$ and $\mathfrak{h} \in \mathbf{End}[\mathscr{C}]$ so that the following diagram commutes:

$$\begin{array}{ccccc} \mathscr{A} & \hookrightarrow & \mathscr{B} & \twoheadrightarrow & \mathscr{C} \\ \downarrow{\scriptstyle \mathfrak{f}} & & \downarrow{\scriptstyle \mathfrak{g}} & & \downarrow{\scriptstyle \mathfrak{h}} \\ \mathscr{A} & \hookrightarrow & \mathscr{B} & \twoheadrightarrow & \mathscr{C} \end{array}$$

We indicate this: "$\mathfrak{g} = \mathfrak{f} \star \mathfrak{h}$."

2. Define $\mathfrak{g}': \mathscr{C} \to \mathscr{A}$ by $\mathfrak{g}'(c) = \mathfrak{g}(\varsigma(c)) \cdot \varsigma(\mathfrak{h}(c))^{-1}$. If $a \in \mathscr{A}$ and $c \in \mathscr{C}$, then $\mathfrak{g}(a \star c) = (\mathfrak{f}(a) \cdot \mathfrak{g}'(c)) \star \mathfrak{h}(c)$.

3. If $\mathscr{B}$ is a polymorph of $\mathscr{A}$, then $\mathfrak{g}'$ is trivial, so $\mathfrak{g}(b) = \mathfrak{f}(a) \star \mathfrak{h}(c)$.

4. If $\mathscr{B}$ is a polymorph of $\mathscr{A}$ and $\mathfrak{f} \in \mathbf{Aut}[\mathscr{A}]$, then $\mathfrak{g}|_{\varsigma(\mathscr{C})} = \mathbf{Id}$ and $\mathfrak{h} = \mathbf{Id}_{\mathscr{C}}$.

Proof. Part 1: Define $\mathfrak{f} = \mathfrak{g}|_{\mathscr{A}}$. Then $\mathfrak{f} \in \mathbf{End}[\mathscr{A}]$ because $\mathscr{A} \prec \mathscr{B}$. Define $\mathfrak{h}$ by: $\mathfrak{h}(b \cdot \mathscr{A}) = \mathfrak{g}(b) \cdot \mathscr{A}$ for any coset $(b \cdot \mathscr{A}) \in \mathscr{C}$. Then, for any $(b_1 \cdot \mathscr{A})$ and $(b_2 \cdot \mathscr{A})$ in $\mathscr{C}$, we have $\mathfrak{h}(b_1\mathscr{A} \cdot b_2\mathscr{A}) = \mathfrak{h}((b_1 \cdot b_2) \cdot \mathscr{A}) = \mathfrak{g}(b_1 \cdot b_2) \cdot \mathscr{A} = \mathfrak{g}(b_1) \cdot \mathfrak{g}(b_2) \cdot \mathscr{A} = \mathfrak{g}(b_1)\, \mathscr{A} \cdot \mathfrak{g}(b_2)\, \mathscr{A} = \mathfrak{h}(b_1\mathscr{A}) \cdot \mathfrak{h}(b_2\mathscr{A})$, so $\mathfrak{H}$ is a endomorphism of $\mathscr{C}$. Clearly, $\mathfrak{h} \circ \pi = \pi \circ \mathfrak{g}$.

Part 4: If $a_1, a_2 \in \mathscr{A}$ and $d_1, d_2 \in \mathscr{D} = \varsigma(\mathscr{C})$, then by (4),

$$\mathfrak{f}(a_1) \cdot (\mathfrak{g}(d_1)^* \circ \mathfrak{f})(a_2) \cdot (\mathfrak{g}(d_1) \cdot \mathfrak{g}(d_2))$$

$$= (\mathfrak{g}(a_1) \cdot \mathfrak{g}(d_1)) \cdot (\mathfrak{g}(a_2) \cdot \mathfrak{g}(d_2)) = \mathfrak{g}((a_1 \cdot d_1) \cdot (a_2 \cdot d_2))$$

$$= \mathfrak{g}((a_1 \cdot d_1^*(a_2)) \cdot (d_1 \cdot d_2)) = \mathfrak{f}(a_1) \cdot (\mathfrak{f} \circ d_1^*)(a_2) \cdot \mathfrak{g}(d_1) \cdot \mathfrak{g}(d_2).$$

Cancel $\mathfrak{f}(a_1)$ and $\mathfrak{g}(d_1)\,\mathfrak{g}(d_2)$, and note that a_2 is arbitrary to conclude: $\mathfrak{g}(d_1)^* \circ \mathfrak{f} = \mathfrak{f} \circ d_1^*$. Since $d_1^* \in Z(\mathbf{Aut}[\mathscr{A}])$, commute these terms to get $\mathfrak{g}(d_1)^* \circ \mathfrak{f} = d_1^* \circ \mathfrak{f}$; cancel $\mathfrak{f} \in \mathbf{Aut}[\mathscr{A}]$ to conclude that $\mathfrak{g}(d_1)^* = d_1^*$. Now, $\mathscr{D}$ is fully characteristic, so $\mathfrak{g}(d_1) \in \mathscr{D}$. But the map $\mathscr{D} \ni d \mapsto d^* \in \mathbf{Aut}[\mathscr{A}]$ is really just the inclusion map $\mathscr{D} \cong \mathscr{C} \hookrightarrow \mathbf{Aut}[\mathscr{A}]$, and therefore injective, so we conclude $\mathfrak{g}(d_1) = d_1$.

Thus, $\mathfrak{g}|_{\mathscr{D}} = \mathbf{Id}_{\mathscr{D}}$, so $\mathfrak{g} \circ \varsigma = \varsigma$. Since $\pi \circ \varsigma = \mathbf{Id}_{\mathscr{C}}$, we conclude: $\mathfrak{h} = \mathfrak{h} \circ \mathbf{Id}_{\mathscr{C}} = \mathfrak{h} \circ \pi \circ \varsigma = \pi \circ \mathfrak{g} \circ \varsigma = \pi \circ \varsigma = \mathbf{Id}_{\mathscr{C}}$.

Parts 2 and 3 are straightforward. ▮

Example 7. Recall $\mathbf{Q}_8 = \mathscr{A} \star \mathscr{C}$ from Example 5a. Define $\mathfrak{g}_1, \mathfrak{g}_2 \in \mathbf{Aut}[\mathbf{Q}_8]$ by Table I. Then $\mathfrak{f}_1 = \mathfrak{f}_2 = \mathbf{Id}_{\mathscr{A}}$, while $\mathfrak{h}_1$, $\mathfrak{h}_2$, $\mathfrak{g}'_1$, and $\mathfrak{g}'_2$ are defined by Table II.

Table I

	1	−1	**i**	−**i**	**j**	−**j**	**k**	−**k**
$\mathfrak{g}_1$	1	−1	**j**	−**j**	**k**	−**k**	**i**	−**i**
$\mathfrak{g}_2$	1	−1	−**i**	**i**	**k**	−**k**	**j**	−**j**

Table II

	O	I	J	K
$\mathfrak{h}_1$	O	J	K	I
$\mathfrak{h}_2$	O	I	K	J
$\mathfrak{g}'_1$	1	1	1	1
$\mathfrak{g}'_2$	1	-1	1	1

Proposition 8. The statement of Theorem 4 is true. To be specific, if $\mathfrak{G}$ has local map

$$\mathfrak{g}: \mathscr{B}^{\mathbb{V}} \ni \mathbf{b} \mapsto \left(g \cdot \prod_{i=1}^{I} \mathfrak{g}_i(b_{v[i]}) \right) \in \mathscr{B},$$

$$\text{(where } b \in \mathscr{B} \text{ and } \mathfrak{g}_i \in \mathbf{End}[\mathscr{B}], \text{ for all } i \in [0 \cdots I])$$

then the local maps $\mathfrak{h}: \mathscr{C}^{\mathbb{V}} \to \mathscr{C}$ and and $\mathfrak{f}: \mathscr{A}^{\mathbb{V}} \times \mathscr{C}^{\mathbb{V}} \to \mathscr{A}$ are defined as follows. Fix a pseudoproduct representation $\mathscr{B} = \mathscr{A} \star \mathscr{C}$. Let $g = f \star h$ for some $f \in \mathscr{A}$ and $h \in \mathscr{C}$. For all $i \in [0 \cdots I]$, let $\mathfrak{g}_i = \mathfrak{f}_i \star \mathfrak{h}_i$, where $\mathfrak{f}_i \in \mathbf{End}[\mathscr{A}]$ and $\mathfrak{h}_i \in \mathbf{End}[\mathscr{C}]$, as in Lemma 6. Then:

1. $\mathfrak{h}(\mathbf{c}) = h \cdot \prod_{i=1}^{I} \mathfrak{h}_i(c_{v[i]})$, and $\mathfrak{f}$ is defined by expression (8) later.

In particular:

2. Suppose $\mathscr{B}$ is a polymorph of $\mathscr{A}$, and $\mathfrak{f}_i \in \mathbf{Aut}[\mathscr{B}]$, $\forall i \in [0 \cdots I]$. Then $\mathfrak{h}(\mathbf{c}) = \prod_{i=0}^{I} c_{v[i]}$ and $\mathfrak{f}_{\mathbf{c}}(\mathbf{a}) = f \cdot \prod_{i=0}^{I} \mathfrak{f}^i_{\mathbf{c}}(a_{v[i]})$, where, $\forall i \geqslant 0$, $\forall a \in \mathscr{A}$, $\mathfrak{f}^i_{\mathbf{c}}(a) = h^* c^*_{v[0]}\, c^*_{v[1]} \cdots c^*_{v[i-1]}\, \mathfrak{f}_i(a)$.

3. Suppose $\mathscr{A} \subset Z(\mathscr{B})$. Treat $\mathscr{A}$ as an additive group $(\mathscr{A}, +)$. Then $\mathfrak{F}_{\mathbf{c}}(\mathbf{a}) = \mathfrak{L}(\mathbf{a}) + \mathfrak{P}(\mathbf{c})$, where $\mathfrak{L}: \mathscr{A}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is a linear cellular automaton with local map

$$\mathfrak{l}: \mathscr{A}^{\mathbb{V}} \ni \mathbf{a} \mapsto \left(\sum_{i=0}^{I} \mathfrak{f}_i(a_{v[i]}) \right) \in \mathscr{A} \tag{5}$$

and $\mathfrak{P}: \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is a block map with local map $\mathfrak{p}: \mathscr{C}^{\mathbb{V}} \to \mathscr{A}$ given by (9) later.

Example 9.

(a) Suppose $\mathscr{A} \subset Z(\mathscr{B})$, as in Part 3 of Proposition 8. If $\mathfrak{g}(\mathbf{b}) = b_{\mathsf{v}_1}^{n_1} b_{\mathsf{v}_2}^{n_2} \cdots b_{\mathsf{v}_J}^{n_J}$, then $\mathfrak{l}(\mathbf{a}) = \sum_{\mathsf{v} \in \mathbb{V}} \ell_{\mathsf{v}} \cdot a_{\mathsf{v}}$, where $\ell_{\mathsf{v}} = \sum_{\mathsf{v}_j = \mathsf{v}} n_j$ for each $\mathsf{v} \in \mathbb{V}$. Meanwhile, $\mathfrak{h}(\mathbf{c}) = c_{\mathsf{v}_1}^{n_1} c_{\mathsf{v}_2}^{n_2} \cdots c_{\mathsf{v}_J}^{n_J}$.

(b) Consider Example 1b, with $\mathscr{B} = \mathbb{Z}_{/5} \rtimes \mathbb{Z}_{/4}$. In this case, $\mathfrak{h}_i = \mathbf{Id}_{\mathscr{C}}$ and $\mathfrak{f}_i = \mathbf{Id}_{\mathscr{A}}$ for all i. Thus, $\mathfrak{H}\colon (\mathbb{Z}_{/4})^{\mathbb{Z}} \to (\mathbb{Z}_{/4})^{\mathbb{Z}}$ is the linear CA with local map: $\mathfrak{h}(c_0, c_1, c_2) = c_0 + c_1 + c_2$. For any $a \in \mathbb{Z}_{/5}$ and $c \in \mathbb{Z}_{/4}$, $c^* a = 2^c \cdot a$; thus, Part 2 of Proposition 8 implies that $\mathfrak{f}\colon (\mathbb{Z}_{/5})^{[0\cdots 2]} \times (\mathbb{Z}_{/4})^{[0\cdots 2]} \to \mathbb{Z}_{/5}$ is defined for all $(a_0, a_1, a_2) \in (\mathbb{Z}_{/5})^{[0\cdots 2]}$ and $(c_0, c_1, c_2) \in (\mathbb{Z}_{/4})^{[0\cdots 2]}$, by: $\mathfrak{f}_{(c_0, c_1, c_2)}(a_0, a_1, a_2) = a_0 + 2^{c_0} a_1 + 2^{c_0 + c_1} a_2$.

(c) Consider Example 1c, with $\mathscr{B} = \mathbb{Z}_{/5} \rtimes \mathbb{Z}_{/4}$. Now $\mathfrak{H}\colon (\mathbb{Z}_{/4})^{\mathbb{Z}} \to (\mathbb{Z}_{/4})^{\mathbb{Z}}$ has local map $\mathfrak{h}(c_0, c_1, c_2) = c_0 + 3c_1 + 4c_2 \equiv c_0 - c_1 \pmod 4$. Meanwhile, Part 2 of Proposition 8 implies that

$$\begin{aligned}
&\mathfrak{f}_{(c_0, c_1, c_2)}(a_0, a_1, a_2)\\
&\quad = a_2 + 2^{c_2} a_2 + 2^{2c_2} a_2 + 2^{3c_2} a_2 + 2^{4c_2} a_1 + 2^{4c_2 + c_1} a_1 + 2^{4c_2 + 2c_1} a_1 + 2^{4c_2 + 3c_1} a_0\\
&\quad = (1 + 2^{c_2} + 2^{2c_2} + 2^{3c_2})\, a_2 + (2^{4c_2} + 2^{4c_2 + c_1} + 2^{4c_2 + 2c_1})\, a_1 + 2^{4c_2 + 3c_1} a_0.
\end{aligned}$$

(d) Recall $\mathfrak{g}_1, \mathfrak{g}_2 \in \mathbf{Aut}[\mathbf{Q}_8]$ from Example 7, and define $\mathfrak{g}\colon \mathbf{Q}_8^{[0\cdots 2]} \to \mathbf{Q}_8$ by $\mathfrak{g}(q_0, q_1, q_2) = q_0 \cdot \mathfrak{g}_1(q_1) \cdot \mathfrak{g}_2(q_2)$. Identify $\{\pm 1\} = \mathscr{A}$ with $(\mathbb{Z}_{/2}, +)$, and identify $\mathscr{C}$ with $\mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$ as described in Example 5a. Then by Part 3 of Proposition 8,

$$\mathfrak{l}(a_0, a_1, a_2) = a_0 + \mathfrak{f}_1(a_1) + \mathfrak{f}_2(a_2) = a_0 + a_1 + a_2;$$

$$\mathfrak{h}(c_0, c_1, c_2) = c_0 + \mathfrak{h}_1(c_1) + \mathfrak{h}_2(c_2) = \begin{bmatrix} c_{0,1} \\ c_{0,2} \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} c_{1,1} \\ c_{1,2} \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} c_{2,1} \\ c_{2,2} \end{bmatrix}.$$

(where $c_i = \left[\begin{smallmatrix} c_{i,1} \\ c_{i,2} \end{smallmatrix}\right] \in \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$, for $i = 0, 1, 2$). Also, applying (9) later,

$$\mathfrak{p}(c_0, c_1, c_2) = \mathfrak{e}(c_0, c_1, c_2) + \mathbf{Id}'(c_0) + \mathfrak{g}_1'(c_1) + \mathfrak{g}_2'(c_2) = \mathfrak{e}(c_0, c_1, c_2) + \mathfrak{g}_2'(c_2),$$

where

$$\mathfrak{e}(c_0, c_1, c_2) = \begin{cases} 0 & \text{if } \varsigma(c_0) \cdot \varsigma(c_1) \cdot \varsigma(\mathfrak{h}_2(c_2)) = \varsigma[c_0 \cdot c_1 \cdot \mathfrak{h}_2(c_2)] \\ 1 & \text{if } \varsigma(c_0) \cdot \varsigma(c_1) \cdot \varsigma(\mathfrak{h}_2(c_2)) = -\varsigma[c_0 \cdot c_1 \cdot \mathfrak{h}_2(c_2)] \end{cases}.$$

(e) $\mathfrak{g}\colon \mathbf{Q}_8^{[0\cdots 3]} \to \mathbf{Q}_8$ by $\mathfrak{g}(q_0, q_1, q_2, q_3) = q_3 \cdot q_0^3 \cdot q_2^5 \cdot q_1^{-1}$. Then, in additive notation, $\mathfrak{l}(a_0, a_1, a_2, a_3) = a_0 + a_1 + a_2 + a_3$ and $\mathfrak{h}(c_0, c_1, c_2, c_3) = c_0 + c_1 + c_2 + c_3 \pmod 2$.

Proof of Proposition 8. For $i \in [0 \cdots I]$, define $\mathfrak{f}^i\colon \mathscr{C}^{\mathbb{V}} \times \mathscr{A} \to \mathscr{A}$ by

$$\mathfrak{f}^i_{\mathfrak{c}}(a) = \left(h \cdot \prod_{j=0}^{i-1} \mathfrak{h}_j(c_{v[j]}) \right)^* (\mathfrak{f}_i(a) \cdot \mathfrak{g}_i'(c_{v[i]})); \tag{6}$$

for example, $\mathfrak{f}_{\mathbf{c}}^0(a) = h^*(\mathfrak{f}_0(a) \cdot \mathfrak{g}_0'(c_{v[0]}))$. Next, define $\mathfrak{e}: \mathscr{C}^{\mathbb{V}} \to \mathscr{A}$ by:

$$\mathfrak{e}(\mathbf{c}) = \left(\varsigma(h) \cdot \prod_{i=0}^{I} \varsigma(\mathfrak{h}_i(c_{v[i]})) \right) \cdot \varsigma\left(h \cdot \prod_{i=0}^{I} \mathfrak{h}_i(c_{v[i]}) \right)^{-1}, \tag{7}$$

and define $\mathfrak{f}: \mathscr{A}^{\mathbb{V}} \times \mathscr{C}^{\mathbb{V}} \to \mathscr{A}$ by:

$$\mathfrak{f}_{\mathbf{c}}(\mathbf{a}) = f \cdot \left(\prod_{i=0}^{I} \mathfrak{f}_{\mathbf{c}}^i(a_{v[i]}) \right) \cdot \mathfrak{e}(\mathbf{c}). \tag{8}$$

To prove Part 1, we must show, for any $\mathbf{a} \in \mathscr{A}^{\mathbb{V}}$ and $\mathbf{c} \in \mathscr{C}^{\mathbb{V}}$, that $\mathfrak{g}(\mathbf{a} \star \mathbf{c}) = \mathfrak{f}_{\mathbf{c}}(\mathbf{a}) \star \mathfrak{h}(\mathbf{c})$.

To see this, let $\mathbf{c} = [c_{\mathsf{v}}|_{\mathsf{v} \in \mathbb{V}}] \in \mathscr{C}^{\mathbb{V}}$ and $\mathbf{a} = [a_{\mathsf{v}}|_{\mathsf{v} \in \mathbb{V}}] \in \mathscr{A}^{\mathbb{V}}$. Then

$$\mathfrak{g}(\mathbf{a} \star \mathbf{c}) = g \cdot \prod_{i=0}^{I} \mathfrak{g}_i(a_{v[i]} \cdot \varsigma(c_{v[i]})) = f \cdot \varsigma(h) \cdot \prod_{i=0}^{I} \mathfrak{g}_i(a_{v[i]}) \cdot \mathfrak{g}_i(\varsigma(c_{v[i]})).$$

In the case $I = 1$, this becomes:

$$\begin{aligned}
\mathfrak{g}(\mathbf{a} \star \mathbf{c}) &= f \cdot \varsigma(h) \cdot \mathfrak{g}_0(a_{v[0]}) \cdot \mathfrak{g}_0(\varsigma(c_{v[0]})) \cdot \mathfrak{g}_1(a_{v[1]}) \cdot \mathfrak{g}_1(\varsigma(c_{v[1]})) \\
&= f \cdot \varsigma(h) \cdot \mathfrak{f}_0(a_{v[0]}) \cdot \mathfrak{g}_0'(c_{v[0]}) \cdot \varsigma(\mathfrak{h}_0(c_{v[0]})) \cdot \mathfrak{f}_1(a_{v[1]}) \\
&\quad \cdot \mathfrak{g}_1'(c_{v[1]}) \cdot \varsigma(\mathfrak{h}_1(c_{v[1]})) \\
&= f \cdot \varsigma(h) \cdot \mathfrak{f}_0(a_{v[0]}) \cdot \mathfrak{g}_0'(c_{v[0]}) \cdot \mathfrak{h}_0(c_{v[0]})^* \, (\mathfrak{f}_1(a_{v[1]}) \, \mathfrak{g}_1'(c_{v[1]})) \\
&\quad \cdot \varsigma(\mathfrak{h}_0(c_{v[0]})) \cdot \varsigma(\mathfrak{h}_1(c_{v[1]})) \\
&= f \cdot h^*(\mathfrak{f}_0(a_{v[0]}) \cdot \mathfrak{g}_0'(c_{v[0]})) \cdot (h \cdot \mathfrak{h}_0(c_{v[0]}))^* \, (\mathfrak{f}_1(a_{v[1]}) \cdot \mathfrak{g}_1'(c_{v[1]})) \\
&\quad \cdot \varsigma(h) \cdot \varsigma(\mathfrak{h}_0(c_{v[0]})) \cdot \varsigma(\mathfrak{h}_1(c_{v[1]})) \\
&= f \cdot \mathfrak{f}_{\mathbf{c}}^0(a_{v[0]}) \cdot \mathfrak{f}_{\mathbf{c}}^1(a_{v[1]}) \cdot \mathfrak{e}(\mathbf{c}) \cdot \varsigma(h \cdot \mathfrak{h}_0(c_{v[0]}) \cdot \mathfrak{h}_1(c_{v[1]})) \\
&= \mathfrak{f}_{\mathbf{c}}(\mathbf{a}) \cdot \varsigma(\mathfrak{h}(\mathbf{c})) = \mathfrak{f}_{\mathbf{c}}(\mathbf{a}) \star \mathfrak{h}(\mathbf{c}).
\end{aligned}$$

A similar argument clearly works for $I \geqslant 2$.

It remains to show that $\mathfrak{e}(\mathbf{c}) \in \mathscr{A}$, which is equivalent to showing that $\pi(\mathfrak{e}(\mathbf{c})) = e_{\mathscr{C}}$, where $\pi: \mathscr{B} \twoheadrightarrow \mathscr{C}$ is the quotient map and $e_{\mathscr{C}} \in \mathscr{C}$ is the identity. But

$$\begin{aligned}
\pi(\mathfrak{e}(\mathbf{c})) &= \pi\left[\left(\varsigma(h) \cdot \prod_{i=0}^{I} \varsigma(\mathfrak{h}_i(c_{v[i]})) \right) \cdot \varsigma\left(h \cdot \prod_{i=0}^{I} \mathfrak{h}_i(c_{v[i]}) \right)^{-1} \right] \\
&= \pi(\varsigma(h)) \cdot \prod_{i=0}^{I} \pi(\varsigma(\mathfrak{h}_i(c_{v[i]}))) \cdot \pi\left(\varsigma\left(h \cdot \prod_{i=0}^{I} \mathfrak{h}_i(c_{v[i]}) \right) \right)^{-1} \\
&= h \cdot \prod_{i=0}^{I} \mathfrak{h}_i(c_{v[i]}) \cdot \left(h \cdot \prod_{i=0}^{I} \mathfrak{h}_i(c_{v[i]}) \right)^{-1} = e_{\mathscr{C}}.
\end{aligned}$$

Part 2: $\mathfrak{g}'_i$ and $\mathfrak{e}$ are trivial, and Part 4 of Lemma 6 implies that $\mathfrak{h}_i = \mathbf{Id}_{\mathscr{C}}$, $\forall i \in [0 \cdots I]$.

Part 3: All the conjugation automorphisms are trivial, so expression (6) (written additively) simplifies to $\mathfrak{f}^i_{\mathbf{c}}(a) = \mathfrak{f}_i(a) + \mathfrak{g}'_i(\mathbf{c})$, for all $i \in [0 \cdots I]$. Substitute this into (8), to get

$$\mathfrak{f}_{\mathbf{c}}(\mathbf{a}) = f + \sum_{i=0}^{I} (\mathfrak{f}_i(a) + \mathfrak{g}'_i(\mathbf{c})) + \mathfrak{e}(\mathbf{c}) = \mathfrak{l}(\mathbf{a}) + \mathfrak{p}(\mathbf{c}),$$

where

$$\mathfrak{p}(\mathbf{c}) = f + \mathfrak{e}(\mathbf{c}) + \sum_{i=0}^{I} \mathfrak{g}'_i(\mathbf{b}_{v[i]}), \tag{9}$$

and $\mathfrak{l}(\mathbf{a})$ is as in (5). ▮

Application to Nilpotent Groups. A *fully characteristic series* is an ascending chain of subgroups:

$$\{e\} = \mathscr{Z}_0 \prec \mathscr{Z}_1 \prec \cdots \prec \mathscr{Z}_K = \mathscr{B}. \tag{10}$$

where each is fully characteristic in the next. For example, the *upper central series* of $\mathscr{B}$ is the series (10), where $\mathscr{Z}_1 = Z(\mathscr{B})$, and for each $k \geqslant 1$, $\mathscr{Z}_{k+1}$ is the complete preimage in $\mathscr{B}$ of $Z(\mathscr{C}_k)$ under the quotient map $\mathscr{B} \twoheadrightarrow \mathscr{C}_k := \mathscr{B}/\mathscr{Z}_k$, until we reach $K > 0$ so that $\mathscr{Z}_K = \mathscr{Z}_{K+1} = \mathscr{Z}_{K+2} = \cdots$. Thus, for all $k \in [1 \cdots K]$, the factor groups $\mathscr{Q}_k = \mathscr{Z}_k/\mathscr{Z}_{k-1} \cong Z(\mathscr{B}/\mathscr{Z}_{k-1})$ are abelian (but $\mathscr{C}_K = \mathscr{B}/\mathscr{Z}_K$ is not). In general, $\mathscr{Z}_K \neq \mathscr{B}$; if they are equal, then $\mathscr{B}$ is called *nilpotent*, and $\mathscr{C}$ is trivial.

Example 10. Let $\mathscr{B} = \mathbf{Q}_8$ from Example 5a. Then $\mathscr{Z}_1 = Z(\mathbf{Q}_8) = \{\pm 1\}$, and $\mathbf{Q}_8/\mathscr{Z}_1 \cong \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$ is abelian, so that $\mathscr{Z}_2 = \mathbf{Q}_8$. Thus, $\mathbf{Q}_8$ is nilpotent, with upper central series: $\{1\} \prec \{\pm 1\} \prec \mathbf{Q}_8$.

We can apply Theorem 4 recursively to a totally characteristic series like (10). Let $\mathscr{A}_1 = \mathscr{Z}_1$, and $\mathscr{C}_1 = \mathscr{B}/\mathscr{A}_1$, and write $\mathscr{B} = \mathscr{A}_1 \star \mathscr{C}_1$, so that $\mathfrak{G} = \mathfrak{F}_1 \star \mathfrak{H}_1$, where $\mathfrak{H}_1 \colon \mathscr{C}_1^{\mathbb{M}} \to \mathscr{C}_1^{\mathbb{M}}$ and $\mathfrak{F}_1 \colon \mathscr{A}_1^{\mathbb{M}} \times \mathscr{C}_1^{\mathbb{M}} \to \mathscr{A}_1^{\mathbb{M}}$ are multiplicative. The series (10) induces a fully characteristic series

$$\{e\} = \mathscr{Z}_{1/1} \prec \mathscr{Z}_{2/1} \prec \cdots \prec \mathscr{Z}_{K/1} = \mathscr{C}_1, \tag{11}$$

where for each $k \in [1 \cdots K]$, we let $\mathscr{Z}_{k/1} = \mathscr{Z}_k/\mathscr{A}_1 \subset \mathscr{C}_1$. Now let $\mathscr{A}_2 = \mathscr{Z}_{2/1}$ and $\mathscr{C}_2 = \mathscr{C}_1/\mathscr{A}_2 \cong \mathscr{B}/\mathscr{Z}_2$, and write $\mathscr{C}_1 = \mathscr{A}_2 \star \mathscr{C}_2$, so that $\mathfrak{H}_1 = \mathfrak{F}_2 \star \mathfrak{H}_2$, where $\mathfrak{F}_2 \colon \mathscr{A}_2^{\mathbb{M}} \times \mathscr{C}_2^{\mathbb{M}} \to \mathscr{A}_2^{\mathbb{M}}$ and $\mathfrak{H}_2 \colon \mathscr{C}_2^{\mathbb{M}} \to \mathscr{C}_2^{\mathbb{M}}$. Proceed inductively. In particular, if $\mathscr{B}$ is nilpotent, apply this to the upper central series to obtain a decomposition: $\mathfrak{G} = \mathfrak{F}_1 \star (\mathfrak{F}_2 \star [\cdots \star (\mathfrak{F}_{K-1} \star \mathfrak{H}) \cdots])$, where, for all $k \in [1 \cdots K)$, $\mathfrak{F}_k: \mathscr{A}_k^{\mathbb{M}} \times \mathscr{C}_k^{\mathbb{M}} \to \mathscr{A}_k^{\mathbb{M}}$ is an affine RCA, while $\mathfrak{H}: \mathscr{A}_K^{\mathbb{M}} \to \mathscr{A}_K^{\mathbb{M}}$ is an affine CA on the final abelian factor $\mathscr{A}_K = \mathscr{B}/\mathscr{Z}_{K-1}$.

4. ENTROPY

Throughout this section, $\mathbb{M} = \mathbb{Z}$ or $\mathbb{N}$, and $\mathbb{V} = [V_0 \cdots V_1] \subset \mathbb{M}$. Let $L = -\min\{V_0, 0\}$ and $R = \max\{0, V_1\}$, and let $V = R + L$. Let $\mathscr{B}$ be a finite set, with $B = \mathsf{card}[\mathscr{B}]$. If $\mathbf{c} \in \mathscr{B}^{[J \cdots K)}$ and $\langle \mathbf{c} \rangle = \{\mathbf{b} \in \mathscr{B}^{\mathbb{Z}};\ \mathbf{b}|_{[J \cdots K)} = \mathbf{c}\}$ is the corresponding *cylinder set*, we say $\langle \mathbf{c} \rangle$ is a cylinder set of *length* $\ell = K - J$. Let $\eta_{\mathscr{B}}$ be the uniformly distributed Bernoulli measure on $\mathscr{B}^{\mathbb{Z}}$, which assigns probability $B^{-\ell}$ to all cylinder sets of length ℓ. If $\mathbb{Y}_1, \mathbb{Y}_2 \subset \mathbb{Z}$ are disjoint, and $\mathbf{b}_k \in \mathscr{B}^{\mathbb{Y}_k}$, then we define $\mathbf{b}_1\_\mathbf{b}_2 \in \mathscr{B}^{\mathbb{Y}_1 \sqcup \mathbb{Y}_2}$ by: $(\mathbf{b}_1\_\mathbf{b}_2)|_{\mathbb{Y}_k} = \mathbf{b}_k$, for $k = 1, 2$. Thus, $\langle \mathbf{b}_1\_\mathbf{b}_2 \rangle = \langle \mathbf{b}_1 \rangle \cap \langle \mathbf{b}_2 \rangle$. Also, if $\mathbb{Y} \subset \mathbb{Z}$ and $\mathbb{X} = \mathbb{Y} + \mathbb{V}$, then we abuse notation by letting $\mathfrak{G}: \mathscr{B}^{\mathbb{X}} \to \mathscr{B}^{\mathbb{Y}}$ be the "local map" induced by $\mathfrak{G}$.

4.1. Permutativity and Relative Permutativity

A local map $\mathfrak{g}: \mathscr{B}^{\mathbb{V}} \to \mathscr{B}$ is *left permutative* if $L > 0$ and, for every $\mathbf{b} \in \mathscr{B}^{(-L \cdots R]}$ the map $\mathscr{B} \ni a \mapsto \mathfrak{g}(a\_\mathbf{b}) \in \mathscr{B}$ is a bijection; $\mathfrak{g}$ is *right permutative* if $R > 0$ and, for every $\mathbf{b} \in \mathscr{B}^{[-L \cdots R)}$ the map $\mathscr{B} \ni c \mapsto \mathfrak{g}(\mathbf{b}\_c) \in \mathscr{B}$ is a bijection. $\mathfrak{g}$ is *permutative* if it is either left- or right-permutative. A CA on $\mathscr{B}^{\mathbb{Z}}$ is *bipermutative* if it is permutative on both sides; a CA on $\mathscr{B}^{\mathbb{N}}$ is called *bipermutative* if it is right-permutative. If $V = R + L$ then we say $\mathfrak{g}$ is *V-bipermutative*. A nonhomogeneous CA $\mathfrak{G}$ is *V-bipermutative* if $\mathfrak{g}_{\mathsf{m}}$ is V-bipermutative for every $\mathsf{m} \in \mathbb{M}$. A relative CA $\mathfrak{F}: \mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is *V-bipermutative* if the NHCA $\mathfrak{F}_{\mathbf{c}}$ is V-bipermutative for every $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$.

Example 11.

(a) If $\mathscr{B} = (\mathbb{Z}_{/n}, +)$ and $V_0 < 0 < V_1$, then a linear CA with local map $\mathfrak{g}(\mathbf{b}) = \sum_{v=V_0}^{V_1} g_v \cdot b_v$ is left- (resp. right-) permutative iff g_{V_0} (resp. g_{V_1}) is relatively prime to n.

(b) In Example 9b, $\mathfrak{H}$ is a 3-bipermutative CA, while $\mathfrak{F}$ is a 3-bipermutative RCA.

(c) In Example 9c, $\mathfrak{h}(c_0, c_1, c_2) = \mathfrak{h}(c_0, c_1) = c_0 - c_1$ is right-permutative, with $\mathbb{V} = \{0, 1\}$, so $\mathfrak{H}$ is 2-bipermutative as a map on $\mathscr{C}^{\mathbb{N}}$. However, $\mathfrak{F}$ is *not* right-permutative. To see this, write:

$$\mathfrak{f}_{(c_0, c_1, c_2)}(a_0, a_1, a_2) = \mathfrak{f}^0_{(c_0, c_1, c_2)}(a_0) + \mathfrak{f}^1_{(c_0, c_1, c_2)}(a_1) + \mathfrak{f}^2_{(c_0, c_1, c_2)}(a_2).$$

Then:

$$\mathfrak{f}^2_{(c_0,c_1,c_2)} = 1+2^{c_2}+2^{2c_2}+2^{3c_2} = \begin{cases} 4 \pmod 5 & \text{if } \quad c_2=0 \quad \text{or} \quad 4; \\ 0 \pmod 5 & \text{if } \quad c_2=1,2 \quad \text{or} \quad 3; \end{cases}$$

Thus, $\mathfrak{f}_{(c_0,c_1,c_2)}$ is right-permutative if and only if $c_2=0$ or 4.

The following results extend well-known properties of permutative cellular automata[(1)] to the nonhomogeneous case; the proofs are similar, and are left to the reader.

Lemma 12. Let $J<K$, and $\ell=K-J$. Let $\mathfrak{G}$ be an NHCA, and let $\mathbf{d}\in\mathscr{B}^{[J\cdots K)}$.

1. If $\mathfrak{G}$ is right-permutative, then for all $\mathbf{b}\in\mathscr{B}^{[J-L\cdots J+R)}$, there is a unique $\mathbf{c}\in\mathscr{B}^{[J+R\cdots K+R)}$ so that $\mathfrak{G}(\mathbf{b\_c})=\mathbf{d}$.

2. If $\mathfrak{G}$ is left-permutative, then for all $\mathbf{b}\in\mathscr{B}^{[K-L\cdots K+R)}$, there is a unique $\mathbf{a}\in\mathscr{B}^{[J-L\cdots K-L)}$ so that $\mathfrak{G}(\mathbf{a\_b})=\mathbf{d}$.

3. If $\mathfrak{G}$ is bipermutative, then for any $j\in[J\cdots K)$ and $\mathbf{b}\in\mathscr{B}^{[j-L\cdots j+R)}$, there are unique $\mathbf{a}\in\mathscr{B}^{[J-L\cdots j-L)}$ and $\mathbf{c}\in\mathscr{B}^{[j+R\cdots K+R)}$ so that $\mathfrak{G}(\mathbf{a\_b\_c})=\mathbf{d}$.

Corollary 13. If $\mathfrak{G}$ is permutative, then $\eta_{\mathscr{B}}$ is $\mathfrak{G}$-invariant.

4.2. Measurable Entropy

Suppose $(\mathbf{Y},\mathscr{Y},\mu)$ is a probability space, $\mathscr{Q}$ is a finite set, and $\mathbf{Q}\colon\mathbf{Y}\to\mathscr{Q}$ is measurable; we say $\mathbf{Q}$ is a *partition* of $\mathbf{Y}$, indexed by $\mathscr{Q}$. If $\rho=\mathbf{Q}(\mu)\in\mathscr{M}[\mathscr{Q}]$, then let $h(\mathbf{Q};\mu)=-\sum_{q\in\mathscr{Q}}\rho[q]\cdot\log(\rho[q])$. If $\mathbf{Q}_k\colon\mathbf{Y}\to\mathscr{Q}_k$ for $k=1,2$, then let $\mathbf{Q}_1\vee\mathbf{Q}_2\colon\mathbf{Y}\to\mathscr{Q}_1\times\mathscr{Q}_2$ be the partition mapping $y\in\mathbf{Y}$ to $(\mathbf{Q}_1(y),\mathbf{Q}_2(y))$. If $\mathsf{G}\colon\mathbf{Y}\to\mathbf{Y}$ is μ-preserving, then define $\mathsf{G}\mathbf{Q}=\mathbf{Q}\circ\mathsf{G}$. If G is invertible (respectively noninvertible), let $\mathbb{T}=\mathbb{Z}$ (respectively $\mathbb{T}=\mathbb{N}$); for any $\mathbb{I}\subset\mathbb{T}$, define $\mathsf{G}^{\mathbb{I}}\mathbf{Q}=\bigvee_{i\in\mathbb{I}}\mathsf{G}^i\mathbf{Q}\colon\mathbf{Y}\to\mathscr{Q}^{\mathbb{I}}$. The G-*entropy* of $\mathbf{Q}$ is the limit: $h(\mathbf{Q},\mathsf{G},\mu)=\lim_{N\to\infty}\frac{1}{N}h(\mathsf{G}^{[0\cdots N)}\mathbf{Q};\mu)$.

Let $\Sigma(\mathsf{G}^{\mathbb{T}}\mathbf{Q})$ be the smallest σ-algebra for which the function $\mathsf{G}^{\mathbb{T}}\mathbf{Q}$ is measurable. $\mathbf{Q}$ is a *generator* for G if $\Sigma(\mathsf{G}^{\mathbb{T}}\mathbf{Q})$ is μ-*dense* in $\mathscr{Y}$, meaning that, for all $\mathbf{V}\in\mathscr{Y}$, there is $\mathbf{W}\in\Sigma(\mathsf{G}^{\mathbb{T}}\mathbf{Q})$ so that $\mu(\mathbf{V}\Delta\mathbf{W})=0$; the (measurable) *entropy* of the system $(\mathbf{Y},\mathscr{Y},\mu;\mathsf{G})$ is then defined: $h(\mathbf{Y},\mathscr{Y},\mu;\mathsf{G})=h(\mathbf{Q},\mathsf{G},\mu)$ (independent of the choice of generator).

Suppose that $\{\mathfrak{R}_n\}_{n=0}^{\infty}$ is a collection of NHCA on $\mathscr{B}^{\mathbb{M}}$. For any $n\in\mathbb{N}$, define $\mathfrak{R}^{(n)}=\mathfrak{R}_{n-1}\circ\mathfrak{R}_{n-2}\circ\cdots\circ\mathfrak{R}_0$. If $\mathbf{Q}$ is a partition, then, for all $N\in\mathbb{N}$, define $\mathfrak{R}^{[0\cdots N)}\mathbf{Q} = \bigvee_{n=0}^{N-1} \mathfrak{R}^{(n)}\mathbf{Q}$. Thus, if $\mathfrak{R}_n = \mathfrak{G}$ for all $n \in \mathbb{N}$, then $\mathfrak{R}^{(n)} = \mathfrak{G}^n$, and $\mathfrak{R}^{[0\cdots N)}\mathbf{Q} = \mathfrak{G}^{[0\cdots N)}\mathbf{Q}$.

Say that $\mathbf{Q}_k\colon \mathbf{Y} \to \mathscr{Q}_k$ $(k = 1, 2)$ are *equivalent* if each is measurable with respect to the other. Then, for any $\mu \in \mathscr{M}[\mathbf{Y}]$, $h(\mathbf{Q}_1; \mu) = h(\mathbf{Q}_2; \mu)$.

Proposition 14. Let $\mathfrak{R}_n$ be V-bipermutative, for all $n \in \mathbb{N}$. Let $\mu \in \mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ and let $\mathbf{Q} = \mathbf{pr}_{[-L\cdots R)}\colon \mathscr{B}^{\mathbb{M}} \to \mathscr{B}^{[-L\cdots R)}$. Then:

1. $\mathfrak{R}^{[0\cdots N)}\mathbf{Q}$ and $\mathbf{pr}_{[-NL\cdots NR)}$ are equivalent. Thus, $h(\mathfrak{R}^{[0\cdots N)}\mathbf{Q}; \mu) = h(\mathbf{pr}_{[-NL\cdots NR)}; \mu)$.
2. $\Sigma(\mathfrak{R}^{\mathbb{N}}\mathbf{Q})$ is the Borel sigma-algebra of $\mathscr{B}^{\mathbb{M}}$.

In particular, suppose $\mathfrak{R}_n = \mathfrak{G}$, for all $n \in \mathbb{N}$. Then:

3. $\mathbf{Q}$ is a $(\mathfrak{G}, \mu)$-generator.
4. If μ is $\boldsymbol{\sigma}$-invariant and $\mathfrak{G}$-invariant, then $h(\mathfrak{G}; \mu) = V \cdot h(\boldsymbol{\sigma}; \mu)$.

In particular, $h(\mathfrak{G}; \eta_{\mathscr{B}}) = V \cdot \log(B)$.

Proof. Part 1 is proved by repeated application of Part 3 from Lemma 12. The other statements then follow. ▮

Remark. By combining Part 4 with Example 11a, we recover the previously computed[4] entropy of linear CA on $((\mathbb{Z}_{/p})^{\mathbb{Z}}, \eta_{\mathscr{B}})$.

4.3. Relative Entropy

Let $\mathbf{Y} = \mathbf{X} \times \mathbf{Z}$, $\mathsf{G} = \mathsf{F} \star \mathsf{H}$, and $\lambda \in \mathscr{M}[\mathbf{X}]$ be as in Section 3.1. If $\nu \in \mathscr{M}[\mathbf{Z}]$ is H-invariant, then $\mu = \lambda \otimes \nu$ is G-invariant. For any $z \in \mathbf{Z}$ and $n \in \mathbb{N}$, define $\mathsf{F}_z^{(n)} = \mathsf{F}_{\mathsf{H}^{n-1}(z)} \circ \cdots \circ \mathsf{F}_{\mathsf{H}^2(z)} \circ \mathsf{F}_{\mathsf{H}(z)} \circ \mathsf{F}_z$. If $\mathbf{P}\colon \mathbf{X} \to \mathscr{P}$ is a partition, then for all $z \in \mathbf{Z}$, let $\mathsf{G}_z^{[0\cdots N)}\mathbf{P}\colon \mathbf{X} \to \mathscr{P}^N$ be the partition: $\mathsf{G}_z^{[0\cdots N)}\mathbf{P} = \bigvee_{n=0}^{N-1} \mathsf{F}_z^{(n)}\mathbf{P}$, and define $h(\mathbf{P}; \mathsf{F}, \lambda/\mathsf{H}, \nu) = \lim_{N\to\infty} \frac{1}{N} \int_{\mathbf{Z}} h(\mathsf{G}_z^{[0\cdots N)}\mathbf{P}, \lambda)\, d\nu[z]$. The *relative entropy* of F over H is defined: $h(\mathsf{F}, \lambda/\mathsf{H}, \nu) = \sup_{\mathbf{P}} h(\mathbf{P}; \mathsf{F}, \lambda/\mathsf{H}, \nu)$, where the supremum is taken over all measurable partitions $\mathbf{P}$ of $\mathbf{X}$.

Theorem 15. $h(\mathsf{G}, \lambda \times \nu) = h(\mathsf{H}, \nu) + h(\mathsf{F}, \lambda/\mathsf{H}, \nu)$. (Abramov and Rokhlin).[11, 13]

Theorem 16. Let $\mathscr{B} = \mathscr{A} \times \mathscr{C}$. Let $\lambda \in \mathscr{M}[\mathscr{A}^{\mathbb{M}}]$, $\nu \in \mathscr{M}[\mathscr{C}^{\mathbb{M}}]$, and $\mu = \lambda \otimes \nu \in \mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ be $\boldsymbol{\sigma}$-invariant. Suppose $\mathfrak{G} = \mathfrak{F} \star \mathfrak{H}$, where $\mathfrak{F}\colon \mathscr{A}^{\mathbb{M}} \times \mathscr{C}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ is λ-preserving and V-bipermutative, while $\mathfrak{H}\colon \mathscr{C}^{\mathbb{M}} \to \mathscr{C}^{\mathbb{M}}$ is ν-preserving and W-bipermutative. Then:

(1) $h(\mathfrak{F}, \lambda/\mathfrak{H}, \nu) = V \cdot h(\lambda, \boldsymbol{\sigma})$;

(2) $h(\mathfrak{H}, \nu) = W \cdot h(\nu, \boldsymbol{\sigma})$;

(3) $h(\mathfrak{G}, \mu) = V \cdot h(\lambda, \boldsymbol{\sigma}) + W \cdot h(\nu, \boldsymbol{\sigma})$.

Proof. To see (1), let $\mathbf{Q} = \mathbf{pr}_{[-L\cdots R)}: \mathscr{A}^{\mathbb{M}} \to \mathscr{A}^{[-L\cdots R)}$. Fix $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$, and, for all $n \in \mathbb{N}$, let $\mathfrak{R}_n = \mathfrak{F}_{\mathfrak{H}^n(\mathbf{c})}$. Then $\mathfrak{R}^{(n)} = \mathfrak{F}_{\mathbf{c}}^{(n)}$, and $\mathfrak{R}^{[0\cdots N)}\mathbf{Q} = \mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{Q}$, so Part 1 of Proposition 14 says: $h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{Q}; \lambda) = h(\mathbf{pr}_{[-NL\cdots NR)}; \lambda)$.

Let $\mathbf{P}: \mathscr{A}^{\mathbb{M}} \to \mathscr{P}$ be any other partition of $\mathscr{A}^{\mathbb{M}}$, and fix $\epsilon > 0$. Then, by Part 2 of Proposition 14, there is some $M = M(\mathbf{c}) > 0$ so that, for all $N \in \mathbb{N}$, $h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{P}; \lambda) < N\epsilon + h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N+M)}\mathbf{Q}; \lambda)$. If $\mathsf{card}[\mathscr{P}] = P$, then also, $h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{P}; \lambda) < N\log(P)$. Find M so that $\mu[\mathscr{D}] < \epsilon/\log(P)$, where $\mathscr{D} = \{\mathbf{c} \in \mathscr{C}^{\mathbb{M}}; M(\mathbf{c}) > M\}$. Then

$$\int_{\mathscr{C}^{\mathbb{M}}} h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{P}; \lambda)\, d\nu[\mathbf{c}]$$

$$= \int_{\mathscr{D}} h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{P}; \lambda)\, d\nu[\mathbf{c}] + \int_{\mathscr{C}^{\mathbb{M}}\setminus\mathscr{D}} h(\mathfrak{G}_{\mathbf{c}}^{[0\cdots N)}\mathbf{P}; \lambda)\, d\nu[\mathbf{c}]$$

$$< \left(N\log(P)\,\frac{\epsilon}{\log(P)} \right) + N\epsilon + h(\mathbf{pr}_{[-(N+M)\,L\cdots(N+M)\,R)}; \lambda).$$

Thus, $h(\mathbf{P}; \mathfrak{F}, \lambda/\mathfrak{H}, \nu) < 2\epsilon + \lim_{N\to\infty} \frac{1}{N} h(\mathbf{pr}_{[-NL\cdots NR)}; \lambda) = 2\epsilon + V \cdot h(\boldsymbol{\sigma}; \lambda)$. Take the supremum over all $\mathbf{P}$ to conclude: $h(\mathfrak{F}, \lambda/\mathfrak{H}, \nu) < 2\epsilon + V \cdot h(\boldsymbol{\sigma}; \lambda)$. Now let $\epsilon \to 0$.

(2) follows from Part 4 of Proposition 14 and (3) follows from Theorem 15. ▮

Note that, in Theorem 16, $\mathscr{B}$ need not be a group, nor $\mathfrak{G}$ a multiplicative cellular automaton. However, Theorem 4 provides a natural skew product decomposition in this case.

Example 17. In Example 11b, $V = W = 2$, $\mathsf{card}[\mathscr{A}] = 5$ and $\mathsf{card}[\mathscr{C}] = 4$; thus $h(\mathfrak{G}, \eta_{\mathscr{B}}) = 2 \cdot \log_2(5) + 2 \cdot \log_2(4) = 2\log_2(5) + 4$.

5. CONVERGENCE OF MEASURES

Endow $\mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ with the weak* topology induced by $\mathbf{C}(\mathscr{B}^{\mathbb{M}}; \mathbb{C})$, the space of continuous, complex-valued functions. The uniformly distributed Bernoulli measure $\eta_{\mathscr{B}} \in \mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ is the Haar measure on $\mathscr{B}^{\mathbb{M}}$ as a compact group, and is invariant under the action of any left- or right-permutative MCA (Lemma 13). Thus, if $\mu \in \mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ is some initial measure, then $\eta_{\mathscr{B}}$ is a natural candidate for the (Cesàro) limit of $\mathfrak{G}^n\mu$ as $n \to \infty$. Since $\eta_{\mathcal{B}}$ is the measure of maximal entropy on $\mathcal{B}^{\mathbb{M}}$, such limiting behaviour is a sort of "asymptotic randomization" of $\mathcal{B}^{\mathbb{M}}$. When $\mathcal{B}$ is abelian, and $\mathfrak{G}$ is an affine CA, the Cesàro convergence of measures to $\eta_{\mathcal{B}}$ is somewhat understood;[5–9] we now extend these results to nonabelian MCA.

Harmonic Mixing and Diffusion. The *characters* of an abelian group $(\mathcal{A}, +)$ are the continuous homomorphisms from $\mathcal{A}$ into the unit circle group $(\mathbb{T}^1, \cdot) \subset \mathbb{C}$. The set of characters forms a group, denoted $\widehat{\mathcal{A}}$. For example, if $\mathcal{A} = \mathbb{Z}_{/n}$, then every $\chi \in \widehat{\mathcal{A}}$ has the form $\chi(a) = \exp(\frac{2\pi \mathbf{i}}{n} c \cdot a)$, where $c \in \mathbb{Z}_{/n}$ is a constant coefficient, and the product $c \cdot a$ is computed mod n.

For any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ there is some finite $\mathbb{K} \subset \mathbb{M}$ and, for each $\mathsf{k} \in \mathbb{K}$, a nontrivial $\chi_{\mathsf{k}} \in \widehat{\mathcal{A}}$, so that, if $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, then $\boldsymbol{\chi}(\mathbf{a}) = \prod_{\mathsf{k} \in \mathbb{K}} \chi_{\mathsf{k}}(a_{\mathsf{k}})$; we indicate this: "$\boldsymbol{\chi} = \bigotimes_{\mathsf{k} \in \mathbb{K}} \chi_{\mathsf{k}}$." For example, if $\mathcal{A} = \mathbb{Z}_{/n}$, this means there is a collection of nonzero coefficients $[c_{\mathsf{k}}|_{\mathsf{k} \in \mathbb{K}}]$ so that if $\mathbf{a} \in \mathcal{A}^{\mathbb{M}}$, then $\boldsymbol{\chi}(\mathbf{a}) = \exp(\frac{2\pi \mathbf{i}}{n} \sum_{\mathsf{k} \in \mathbb{K}} c_{\mathsf{k}} \cdot a_{\mathsf{k}})$.

The *rank* of $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$ is the cardinality of $\mathbb{K}$. Let $\mu \in \mathcal{M}[\mathcal{A}^{\mathbb{M}}]$; we will use the notation $\langle \boldsymbol{\chi}, \mu \rangle = \int_{\mathcal{A}^{\mathbb{M}}} \boldsymbol{\chi}\, d\mu$. We call μ *harmonically mixing* (and write "$\mu \in \mathcal{HM}[\mathcal{A}^{\mathbb{M}}]$") if, for all $\epsilon > 0$, there is $r \in \mathbb{N}$ so that, if $\chi \in \widehat{\mathcal{A}^{\mathbb{M}}}$ and $\mathsf{rank}[\chi] > r$, then $|\langle \mu, \chi \rangle| < \epsilon$. For example, most Bernoulli measures[7] and Markov random fields[8] on $\mathcal{A}^{(\mathbb{Z}^D)}$ are harmonically mixing.

If $\mathfrak{G} \in \mathbf{End}[\mathcal{A}^{\mathbb{M}}]$, then for any $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, the map $\boldsymbol{\chi} \circ \mathfrak{G}$ is also a character. If $\mathbb{J} \subset \mathbb{N}$, then $\mathfrak{G}$ is $\mathbb{J}$-*diffusive* if, for every $\boldsymbol{\chi} \in \widehat{\mathcal{A}^{\mathbb{M}}}$, $\lim_{j \to \infty, j \in \mathbb{J}} \mathsf{rank}[\boldsymbol{\chi} \circ \mathfrak{G}^j] = \infty$. If $\mathbb{J} = \mathbb{Z}$, then we just say $\mathfrak{G}$ is *diffusive*; if $\mathbb{J} \subset \mathbb{N}$ is a subset of Cesàro density 1, then $\mathfrak{G}$ is *diffusive in density*.

Example 18. Let $(\mathcal{A}, +)$ be a finite abelian group, $\mathbb{M} = \mathbb{Z}^D$, and let $\mathfrak{L}$ be a linear CA with local map $\mathfrak{l}(\mathbf{a}) = \sum_{\mathsf{v} \in \mathbb{V}} \ell_{\mathsf{v}} a_{\mathsf{v}}$, where $\ell_{\mathsf{v}} \in \mathbb{Z}$ is relatively prime to $\mathsf{card}[\mathcal{A}]$ for all $\mathsf{v} \in \mathbb{V}$. Then $\mathfrak{L}$ is diffusive in density.[8]

If $\mathfrak{G}$ is $\mathbb{J}$-diffusive and $\mu \in \mathcal{HM}[\mathcal{A}^{\mathbb{M}}]$, then Theorem 12 of ref. 7 says $\text{wk*}\lim_{\mathbb{J} \ni j \to \infty} \mathfrak{G}^n\mu = \eta_{\mathcal{B}}$. In particular, if $\mathfrak{G}$ is diffusive in density, then the Cesàro average weak*-converges to Haar measure:

$$\text{wk*}\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \mathfrak{G}^n\mu = \eta_{\mathcal{B}}. \tag{12}$$

To extend these results to multiplicative cellular automata, we need a version of diffusion applicable to affine relative cellular automata. An *affine endomorphism* of $\mathscr{A}^{\mathbb{M}}$ is a self-map $\mathfrak{G}: \mathscr{A}^{\mathbb{M}} \to \mathscr{A}^{\mathbb{M}}$ of the form $\mathfrak{G}(\mathbf{a}) = \mathbf{c} + \mathfrak{L}(\mathbf{a})$, where $\mathfrak{L} \in \mathbf{End}[\mathscr{A}^{\mathbb{M}}]$ and $\mathbf{c} \in \mathscr{A}^{\mathbb{M}}$ is constant. The set of affine endomorphisms is denoted $\widetilde{\mathbf{End}}[\mathscr{A}^{\mathbb{M}}]$.

An *affine character* is a function $\boldsymbol{\alpha}: \mathscr{A}^{\mathbb{M}} \to \mathbb{T}^1$ of the form $\boldsymbol{\alpha}(\mathbf{a}) = c \cdot \boldsymbol{\chi}(\mathbf{a})$, where $c \in \mathbb{T}^1$ is a constant, and $\boldsymbol{\chi} \in \widehat{\mathscr{A}^{\mathbb{M}}}$. The set of affine characters of $\mathscr{A}^{\mathbb{M}}$ is denoted $\widetilde{\mathscr{A}^{\mathbb{M}}}$. For example, if $\zeta \in \widehat{\mathscr{A}^{\mathbb{M}}}$, and $\mathfrak{G} \in \widetilde{\mathbf{End}}[\mathscr{A}^{\mathbb{M}}]$, then $\zeta \circ \mathfrak{G} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$. The *rank* of $\boldsymbol{\alpha} = c \cdot \boldsymbol{\chi}$ is the rank of $\boldsymbol{\chi}$. If $\mu \in \mathscr{M}[\mathscr{A}^{\mathbb{M}}]$ is harmonically mixing, with ϵ and r as before, then it follows that $|\langle \mu, \boldsymbol{\alpha} \rangle| < \epsilon$ for any $\boldsymbol{\alpha} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$ with $\mathsf{rank}[\boldsymbol{\alpha}] > r$.

Relative Diffusion. Suppose $\mathscr{B} = \mathscr{A} \star \mathscr{C}$, where $\mathscr{A}$ is abelian, and let $\mathfrak{G} = \mathfrak{F} \star \mathfrak{H}$ be as in Theorem 4. For any $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$, the fibre map $\mathfrak{F}_{\mathbf{c}}$ is an affine endomorphism; we say that $\mathfrak{F}$ is an *affine relative cellular automaton* (ARCA). For any $j \in \mathbb{N}$, $\mathfrak{G}^j = \mathfrak{F}^{(j)} \star \mathfrak{H}^j$, where $\mathfrak{F}^{(j)}$ is another ARCA, so $\boldsymbol{\alpha} \circ \mathfrak{F}^{(j)}_{\mathbf{c}} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$ for any $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$ and $\boldsymbol{\alpha} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$. We say $\mathfrak{G}$ is *relatively* $\mathbb{J}$-*diffusive* if $\lim_{\mathbb{J} \ni j \to \infty} \mathsf{rank}[\boldsymbol{\alpha} \circ \mathfrak{F}^{(j)}_{\mathbf{c}}] = \infty$ for every $\mathbf{c} \in \mathscr{C}^{\mathbb{M}}$ and $\boldsymbol{\alpha} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$. If $\nu \in \mathscr{M}[\mathscr{C}^{\mathbb{M}}]$, and $\mathbb{J} \subset \mathbb{N}$, then $\mathfrak{G}$ is ν-*relatively* $\mathbb{J}$-*diffusive* if,

$$\forall \boldsymbol{\alpha} \in \widetilde{\mathscr{A}^{\mathbb{M}}}, \quad \forall r > 0, \quad \lim_{\mathbb{J} \ni j \to \infty} \nu\{\mathbf{c} \in \mathscr{C}^{\mathbb{M}}; \mathsf{rank}[\boldsymbol{\alpha} \circ \mathfrak{F}^{(j)}_{\mathbf{c}}] \leqslant r\} = 0. \tag{13}$$

Clearly, relative diffusion implies ν-relative diffusion for any $\nu \in \mathscr{M}[\mathscr{C}^{\mathbb{M}}]$.

Proposition 19. If $\mathscr{A} \subset Z(\mathscr{B})$ as in Part 3 of Proposition 8, then $\mathfrak{F}$ is relatively $\mathbb{J}$-diffusive if and only if $\mathfrak{L}$ is $\mathbb{J}$-diffusive as a linear cellular automaton.

Proof. For any $N \in \mathbb{N}$, define $\mathfrak{P}^{(N)} = \sum_{n=0}^{N-1} \mathfrak{L}^n \circ \mathfrak{P} \circ \mathfrak{H}^{N-n-1}$. If $j \in \mathbb{J}$, then $\mathfrak{F}^{(j)}_{\mathbf{c}} = \mathfrak{L}^j + \mathfrak{P}^{(j)}(\mathbf{c})$. Thus, for any $\boldsymbol{\alpha} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$, $\mathsf{rank}[\boldsymbol{\alpha} \circ \mathfrak{F}^j_{\mathbf{c}}] = \mathsf{rank}[\boldsymbol{\alpha} \circ \mathfrak{L}^j]$. ▮

Proposition 20. Let $\lambda \in \mathscr{H}\mathscr{M}[\mathscr{A}^{\mathbb{M}}]$, $\nu \in \mathscr{M}[\mathscr{C}^{\mathbb{M}}]$, and $\mu = \lambda \otimes \nu \in \mathscr{M}[\mathscr{B}^{\mathbb{M}}]$. Let $\bar{\nu} = \text{wk}^*\lim_{\mathbb{J} \ni j \to \infty} \mathfrak{H}^j \nu$, and let $\eta_{\mathscr{A}}$ be the Haar measure on $\mathscr{A}^{\mathbb{M}}$. If $\mathfrak{G}$ is ν-relatively $\mathbb{J}$-diffusive, then $\text{wk}^*\lim_{\mathbb{J} \ni j \to \infty} \mathfrak{G}^j \mu = \eta_{\mathscr{A}} \otimes \bar{\nu}$.

Proof. We want $\lim_{\mathbb{J} \ni j \to \infty} \langle \boldsymbol{\beta}, \mathfrak{G}^j \mu \rangle = \langle \boldsymbol{\beta}, \eta_{\mathscr{A}} \otimes \bar{\nu} \rangle$, for every $\boldsymbol{\beta} \in \mathbf{C}(\mathscr{B}^{\mathbb{M}}; \mathbb{C})$. It suffices to assume $\boldsymbol{\beta} = \boldsymbol{\alpha} \otimes \boldsymbol{\phi}$, where $\boldsymbol{\alpha} \in \mathbf{C}(\mathscr{A}^{\mathbb{M}}; \mathbb{C})$ and $\boldsymbol{\phi} \in \mathbf{C}(\mathscr{C}^{\mathbb{M}}; \mathbb{C})$. Since the characters of $\mathscr{A}^{\mathbb{M}}$ form a basis for the Banach space $\mathbf{C}(\mathscr{A}^{\mathbb{M}}; \mathbb{C})$, it suffices to assume $\boldsymbol{\alpha} \in \widehat{\mathscr{A}^{\mathbb{M}}}$, and $\|\boldsymbol{\phi}\|_\infty = 1$.

$$\text{Then: } \langle \boldsymbol{\beta}, \eta_{\mathscr{A}} \otimes \bar{\nu} \rangle = \langle \boldsymbol{\alpha}, \eta_{\mathscr{A}} \rangle \cdot \langle \boldsymbol{\phi}, \bar{\nu} \rangle = \begin{cases} \langle \boldsymbol{\phi}, \bar{\nu} \rangle & \text{if } \boldsymbol{\alpha} = \mathbb{1} \\ 0 & \text{if } \boldsymbol{\alpha} \neq \mathbb{1} \end{cases}$$

Now, for all $\mathbf{a} \star \mathbf{c} \in \mathscr{B}^{\mathbb{M}}$, $\boldsymbol{\beta} \circ \mathfrak{G}^j(\mathbf{a} \star \mathbf{c}) = (\boldsymbol{\alpha} \otimes \boldsymbol{\phi})(\mathfrak{F}_{\mathbf{c}}^{(j)}(\mathbf{a}) \star \mathfrak{H}^j(\mathbf{c})) = (\boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}(\mathbf{a})) \cdot (\boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c}))$. Thus, $\langle \boldsymbol{\beta}, \mathfrak{G}^j \mu \rangle = \langle \boldsymbol{\beta} \circ \mathfrak{G}^j, \mu \rangle = \int_{\mathscr{C}^{\mathbb{M}}} (\boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c})) \cdot \langle \boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}, \lambda \rangle \, d\nu[\mathbf{c}]$.

If $\boldsymbol{\alpha} = \mathbb{1}$, then this integral is just equal to $\int_{\mathscr{C}^{\mathbb{M}}} \boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c}) \, d\nu[\mathbf{c}]$, which converges to $\langle \boldsymbol{\phi}, \bar{\nu} \rangle$ by hypothesis. Hence, assume $\boldsymbol{\alpha} \neq \mathbb{1}$; we then want to show that $\lim_{\mathbb{J} \ni j \to \infty} \langle \boldsymbol{\beta}, \mathfrak{G}^j \mu \rangle = 0$.

Fix $\epsilon > 0$. Since $\lambda \in \mathscr{H}\mathscr{M}[\mathscr{A}^{\mathbb{M}}]$, find $r > 0$ so that, if $\boldsymbol{\alpha} \in \widetilde{\mathscr{A}^{\mathbb{M}}}$ and $\mathsf{rank}[\boldsymbol{\alpha}] > r$, then $|\langle \boldsymbol{\alpha}, \lambda \rangle| < \frac{\epsilon}{2}$. Let $\mathbf{D}_j = \{\mathbf{c} \in \mathscr{C}^{\mathbb{M}}; \mathsf{rank}[\boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}] > r\}$, for every $j \in \mathbb{J}$. By Eq. (13), find $J \in \mathbb{N}$ so that, $\forall j \in \mathbb{J}$ with $j > J$, $\nu[\mathbf{D}_j] > 1 - \frac{\epsilon}{2}$. Then

$$
\begin{aligned}
|\langle \boldsymbol{\beta}, \mathfrak{G}^j \mu \rangle| &= \left| \int_{\mathscr{C}^{\mathbb{M}}} \boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c}) \cdot \langle \boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}, \lambda \rangle \, d\nu[\mathbf{c}] \right| \\
&\leqslant \left| \int_{\mathbf{D}_j} \boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c}) \cdot \langle \boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}, \lambda \rangle \, d\nu[\mathbf{c}] \right| \\
&\quad + \left| \int_{\mathscr{C}^{\mathbb{M}} \setminus \mathbf{D}_j} \boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c}) \cdot \langle \boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}, \lambda \rangle \, d\nu[\mathbf{c}] \right| \\
&\leqslant \int_{\mathbf{D}_j} |\boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c})| \cdot |\langle \boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}, \lambda \rangle| \, d\nu[\mathbf{c}] \\
&\quad + \int_{\mathscr{C}^{\mathbb{M}} \setminus \mathbf{D}_j} |\boldsymbol{\phi} \circ \mathfrak{H}^j(\mathbf{c}) \cdot \langle \boldsymbol{\alpha} \circ \mathfrak{F}_{\mathbf{c}}^{(j)}, \lambda \rangle| \, d\nu[\mathbf{c}] \\
&\leqslant \int_{\mathbf{D}_j} 1 \cdot \frac{\epsilon}{2} \, d\nu[\mathbf{c}] + \int_{\mathscr{C}^{\mathbb{M}} \setminus \mathbf{D}_j} 1 \, d\nu[\mathbf{c}] < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon. \quad \blacksquare
\end{aligned}
$$

Suppose $\mathscr{B}$ is nilpotent, with upper central series (10). If $k \in [1 \cdots K]$, then $\mathscr{Q}_k = \mathscr{Z}_k / \mathscr{Z}_{k-1}$ is abelian, and the decomposition $\mathscr{B} = \mathscr{Q}_1 \star (\mathscr{Q}_2 \star [\cdots (\mathscr{Q}_{K-1} \star \mathscr{Q}_K) \cdots])$ induces a natural identification $\mathscr{B}^{\mathbb{M}} \cong \mathscr{Q}_1^{\mathbb{M}} \times \mathscr{Q}_2^{\mathbb{M}} \times \cdots \times \mathscr{Q}_K^{\mathbb{M}}$. If $\lambda_k \in \mathscr{M}[\mathscr{Q}_k^{\mathbb{M}}]$ for all k, then $\lambda_1 \otimes \cdots \otimes \lambda_K \in \mathscr{M}[\mathscr{B}^{\mathbb{M}}]$. Let $\mathscr{H}\mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ denote the convex, weak*-closure in $\mathscr{M}[\mathscr{B}^{\mathbb{M}}]$ of the set

$$\{\lambda_1 \otimes \cdots \otimes \lambda_K; \lambda_k \in \mathscr{H}\mathscr{M}[\mathscr{Q}_k^{\mathbb{M}}] \text{ for all } k\}.$$

Theorem 21. Suppose $\mathscr{B}$ is nilpotent, and $\mathfrak{G}$ has a local map of the form $\mathfrak{g}(\mathbf{b}) = b_{\mathsf{v}_1}^{n_1} b_{\mathsf{v}_2}^{n_2} \cdots b_{\mathsf{v}_J}^{n_J}$. For every $\mathsf{v} \in \mathbb{V}$, suppose $\ell_{\mathsf{v}} = \sum_{\mathsf{v}_j = \mathsf{v}} n_j$ is relatively prime to $\mathsf{card}[\mathscr{B}]$.

If $\mu \in \mathcal{HM}[\mathcal{B}^{\mathbb{M}}]$, then $\text{wk}^*\lim_{\mathbb{J}\ni j\to\infty} \mathfrak{G}^j(\mu) = \eta_{\mathcal{B}}$ along a set $\mathbb{J} \subset \mathbb{N}$ of density one. Thus, Eq. (12) holds.

Proof. We'll prove this by induction on K, the length of the series (10). If $K = 1$, then $\mathcal{B}$ is abelian; then $\mathfrak{G}$ is diffusive in density by Example 18, and the result follows from Theorem 12 of ref. 7.

If $K > 1$, then let $\mathcal{A} = \mathcal{Q}_1 = Z(\mathcal{B})$, and $\mathcal{C} = \mathcal{B}/\mathcal{A}$. Thus $\mathcal{HM}[\mathcal{B}^{\mathbb{M}}]$ is the convex weak* closure of $\mathcal{S} = \{\lambda \otimes \nu;\ \lambda \in \mathcal{HM}[\mathcal{A}^{\mathbb{M}}]\ \text{and} \nu \in \mathcal{HM}[\mathcal{C}^{\mathbb{M}}]\}$, so it suffices to prove the theorem for $\mu = \lambda \otimes \nu \in \mathcal{S}$. Let $\mathfrak{G} = \mathfrak{F} \star \mathfrak{H}$. Then $\mathfrak{H}$ has local map $\mathfrak{h}(\mathbf{c}) = c_{\mathsf{v}_1}^{n_1} c_{\mathsf{v}_2}^{n_2} \cdots c_{\mathsf{v}_J}^{n_J}$, and, by hypothesis, all ℓ_{v} are all relatively prime to $\mathsf{card}[\mathcal{C}]$. But $\mathcal{C}$ has an upper central series like (11) of length $K-1$, so by induction hypothesis, there is a set $\mathbb{K} \subset \mathbb{N}$ of density one so that $\text{wk}^*\lim_{\mathbb{K}\ni k\to\infty} \mathfrak{H}^k(\nu) = \eta_{\mathcal{C}}$.

Since $\mathcal{A} = Z(\mathcal{B})$, let $\mathfrak{L}$ be as in Part 3 of Proposition 8. As in Example 9a, $\mathfrak{l}(\mathbf{a}) = \sum_{\mathsf{v}\in\mathbb{V}} \ell_{\mathsf{v}} \cdot a_{\mathsf{v}}$, and, by hypothesis, ℓ_{v} are all relatively prime to $\mathsf{card}[\mathcal{A}]$, so, as in Example 18, $\mathfrak{L}$ is $\mathbb{I}$-diffusive for some subset $\mathbb{I} \subset \mathbb{N}$ of density one. Proposition 19 then implies that $\mathfrak{F}$ is relatively $\mathbb{I}$-diffusive. Let $\mathbb{J} = \mathbb{I} \cap \mathbb{K}$, also a set of density one. Then apply Proposition 20 to conclude that $\text{wk}^*\lim_{\mathbb{J}\ni j\to\infty} \mathfrak{G}^j\mu = \eta_{\mathcal{A}} \otimes \eta_{\mathcal{C}} = \eta_{\mathcal{B}}$. ∎

Example 22. Recall $\mathfrak{G}\colon \mathbf{Q}_8^{\mathbb{Z}} \to \mathbf{Q}_8^{\mathbb{Z}}$ from Example 9e. In this case, $\mathcal{A} \cong \mathbb{Z}_{/2}$, and $\mathfrak{L}$, having local map $\mathfrak{l}(a_0, a_1, a_2, a_3) = a_0 + a_1 + a_2 + a_3$, is diffusive in density, so $\mathfrak{F}$ is relatively diffusive in density. Meanwhile, $\mathcal{C} = \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$ and $\mathfrak{H}$, with local map $\mathfrak{h}(c_0, c_1, c_2, c_3) = c_0 + c_1 + c_2 + c_3$, is also diffusive in density. Hence, Eq. (12) holds for any $\mu \in \mathcal{HM}[\mathbf{Q}_8^{\mathbb{Z}}]$.

6. CONCLUSION

Multiplicative cellular automata over a group $\mathcal{B}$ inherit a natural structural decomposition from $\mathcal{B}$. Using this decomposition, we can compute the measurable entropy of MCA, and show that a broad class of initial measures converge to the Haar measure in Cesàro average. However, many questions remain. For example, it is unclear how to show relative diffusion when $\mathcal{A}$ is not central in $\mathcal{B}$. Indeed, even non-relative diffusion is mysterious for noncyclic abelian groups.[8] Also, computation of relative entropy will be much more complicated in the case of "variably permutative" relative CA, such as Example 11c; perhaps this requires some "relative" version of Lyapunov exponents.[14,15]

Permutative MCA are a considerable generalization of the linear cellular automata previously studied, but they are still only a very special class of permutative cellular automata. The asymptotics of measures for general permutative CA[16] is still poorly understood.

REFERENCES

1. G. Hedlund, Endomorphisms and automorphisms of the shift dynamical systems, *Math. Syst. Theory* **3**:320–375 (1969).
2. C. Moore, Quasi-linear cellular automata, *Physica D* **103**:100–132 (1997).
3. C. Moore, Predicting non-linear cellular automata quickly by decomposing them into linear ones, *Physica D* **111**:27–41 (1998).
4. G. Manzini, Michele D'amico, and Luciano Margara, On computing the entropy of cellular automata, in *25th International Colloquium on Automata, Languages, and Programming (ICALP '98)*, G. Winskel, K. G. Larsen, and S. Skyum, eds., Lecture Notes in Computer Science, No. 1443, pp. 470–481 (Springer-Verlag, Heidelberg, 1998).
5. A. Maass and S. Martínez, Time averages for some classes of expansive one-dimensional cellular automata, in *Cellular Automata and Complex Systems*, E. Goles and S. Martinez, eds. (Kluwer Academic Publishers, Dordrecht, 1999), pp. 37–54.
6. D. Lind, Applications of ergodic theory and sofic systems to cellular automata, *Physica D* **10**:36–44 (1984).
7. M. Pivato and R. Yassawi, Limit measures for affine cellular automata, *Ergodic Theory Dyn. Syst.* **22**:1269–1287 (2002).
8. M. Pivato and R. Yassawi, Limit measures for affine cellular automata II, submitted to *Ergodic Theory and Dynamical Systems*; preprint available at: http://arXiv.org/abs/math.DS/0108083, 2001.
9. S. Martínez, P. Ferrari, A. Maass, and P. Ney, Cesàro mean distribution of group automata starting from measures with summable decay, *Ergodic Theory Dynam. Systems* **20**(6):1657–1670 (2000).
10. H. Furstenberg, *Ergodic Theory and Combinatorial Number Theory* (Princeton University Press, Princeton, New Jersey, 1981).
11. K. Petersen, *Ergodic Theory* (Cambridge University Press, New York, 1989).
12. W. R. Scott, *Group Theory* (Dover, 1987).
13. L. M. Abramov and V. A. Rokhlin, The entropy of a skew product of measure-preserving transformations, *Amer. Math. Soc. Transl. Ser. 2* **48**:225–265, 1965.
14. M. A. Shereshevsky, Lyapunov exponents for one-dimensional cellular automata, *J. Nonlinear Sci.* **2**:1–8 (1992).
15. P. Tisseur, Cellular automata and Lyapunov exponents, *Nonlinearity* **13**:1547–1569 (2000).
16. A. Maass and S. Martínez, On Cesàro limit distribution of a class of permutative cellular automata, *J. Statist. Phys.* **90**:435–452 (1998).