The Algebraic Structure of Cellular Automata

Anthony D. Rhodes, Portland State University, 2013

"One must [first] have chaos to give birth to a dancing star."

– Friedrich Nietzsche, *Thus Spake Zarathustra*

0.Introduction

The effort to effectively model and better understand *complexity* in all of its varied phenomenal permutations is one of the foremost goals of modern science. Recently, cellular automata and related computational models have been used to successfully explore the complexity of general abstract systems. Contemporary research suggests that there are universal principles – *a fortiori*, simple atomic "programs" – that apply operationally to systems throughout the natural world.[9] This paper is a modest attempt to taxonomize a small subset of these abstract systems using algebraic techniques. The results that follow are based primarily on John Pedersen's paper "Cellular Automata as Algebraic Systems" and Stephen Wolfram's related work with Cellular Automata.

I.Preliminaries

<u>Definition 1</u>. A one-dimensional *cellular automaton* (*CA*) is a 4-tuple: $\mathrm{A}=(S,l,r,\sigma)$, where $S\subset\mathbb{R}$ is a finite set of states, *l* and *r* are natural numbers, and σ is a function $\sigma:S^{r+l+1}\to S$, where we will require 0 to be an element of A (henceforth known as the *quiescent state*) and $\sigma(0,0,...,0)=0$. A configuration is a function $s:\mathbb{Z}\to S,$ which may be thought of as a doubly-infinite, one-dimensional array of cells – or place-holders, where each cell contains a single element from the set S. This doubly-infinite array is accordingly indexed by $\mathbb{Z}$, where, for instance, cell "0" resides to the left of cell "1" and to the right of cell "-1" and so forth.

The automaton is "dynamic" insofar as its cell configuration changes through a sequence of discrete time steps. At time $t=0$ the automaton is in its *initial configuration*; thereafter the states evolve in discrete time steps corresponding with $t=1,2,3...,$ etc. If $s:\mathbb{Z}\to S$ is a configuration, $s(i)$ denotes the state of cell *i*, for each $i \in \mathbb{Z}$. Hereafter s will specifically refer to the initial configuration of an automaton. We will denote the state of cell *n* at time $t \geq 0$ of the automaton A with initial configuration s by $\mathrm{A}_{t,n}(s)$. Cell states are defined in a recursive fashion, so that the state of a particular cell at time $t+1$ depends on the states of its *l* left neighbors and its *r* right neighbors at time t, as determined by σ. Hence,

$$\mathrm{A}_{t+1,n}(s) = \sigma\left(\mathrm{A}_{t,n-l}(s), \mathrm{A}_{t,n-l+1}(s), ..., \mathrm{A}_{t,n+r}(s)\right).$$

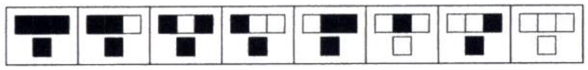
The *(global) configuration* of $A(s)$ (so it has initial configuration *s*) at a *fixed time* t can be thought of as the collection $\{A_{t,i}(s)\}$ over all cells, $i \in \mathbb{Z}$; we denote this configuration as $\mathrm{A}_t(s)$. The evolution of a particular *CA* with initial configuration *s* is therefore written as follows: $s = \mathrm{A}_0(s), \mathrm{A}_1(s), \mathrm{A}_2(s), ...$ Oftentimes it is useful for the purpose of further study to consider a global "snapshot" of the evolution of a particular *CA*, where the sequence $\mathrm{A}_0(s), \mathrm{A}_1(s), \mathrm{A}_2(s), ...$ is realized pictorially, read top-to-bottom, beginning with $\mathrm{A}_0(s)$.

We now develop several examples of simple cellular automata (*CA*s) in order to help facilitate the reader's understanding and to demonstrate some of the remarkable behavior exhibited by *CA*s.

Let the cells of our *CA* be binary, so that: $S = \{0 \sim \mathit{white},\ 1 \sim \text{black}\}$. Furthermore, we consider the simple case where $l = r = 1$. Thus $\sigma : S^3 \to S$ and each state transition is determined by a triplet. In following the ordering conventions developed by S. Wolfram [9], we consider the automaton "Rule 250" where the "rule", i.e. the definition of σ over each element of S^3 (note that there are 2^3 such elements), is defined as follows:

$$\sigma : S^3 \to S \begin{cases} \sigma(1,1,1) = 1 \\ \sigma(1,1,0) = 1 \\ \sigma(1,0,1) = 1 \\ \sigma(1,0,0) = 1 \\ \sigma(0,1,1) = 1 \\ \sigma(0,1,0) = 0 \\ \sigma(0,0,1) = 1 \\ \sigma(0,0,0) = 0 \end{cases}$$

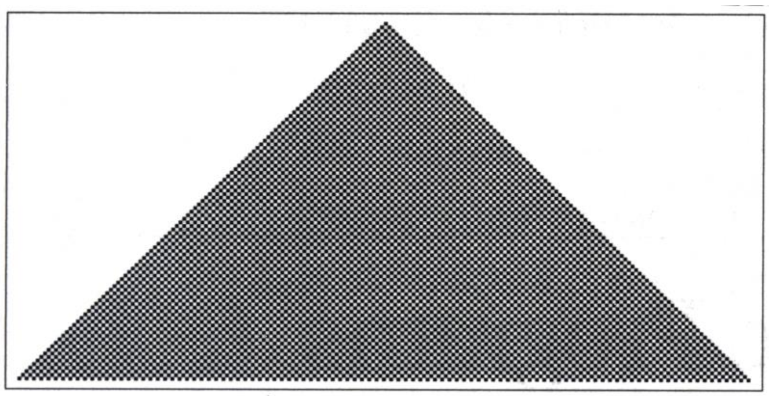
As the reader may check, this assignment is realized pictorially by the rule scheme shown below.



rule 250

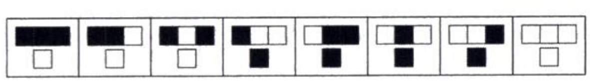
We can see that the sequence of global configurations for this *CA* is very well-behaved; iterations beginning with the *elementary initial configuration* $\bar{1}$ (*cf.* p.12), are depicted below, where:

$$\bar{1}(i)=\begin{cases}1 & \text{if } i=0\\ 0 & \text{else}\end{cases}$$

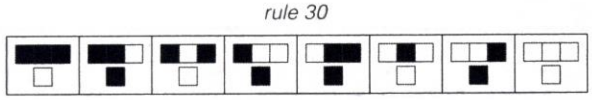


repetition (rule 250)

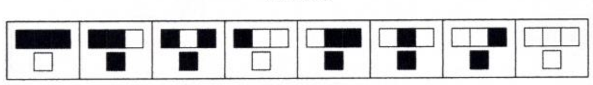
However, as the next examples illustrate, many "simple" automata give rise to complex and even seemingly random behavior. Let us consider, to this end, rules "30", "90" and "110". In each case the respective rule scheme is listed below (here the explicit definition of σ has been suppressed for simplification).



rule 30

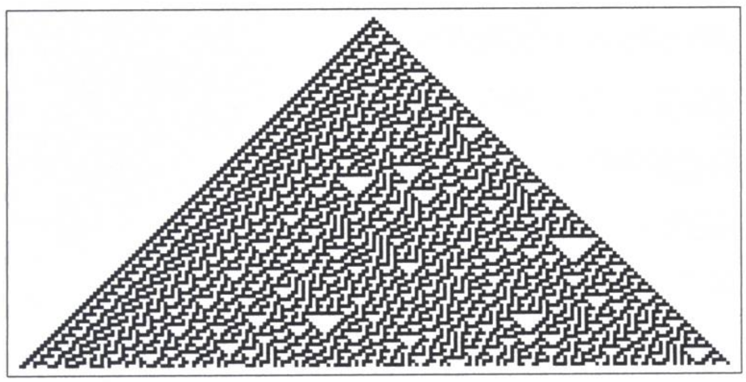


rule 90

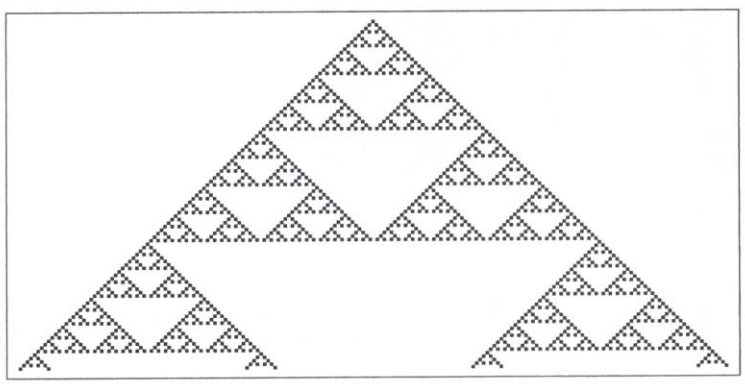


rule 110

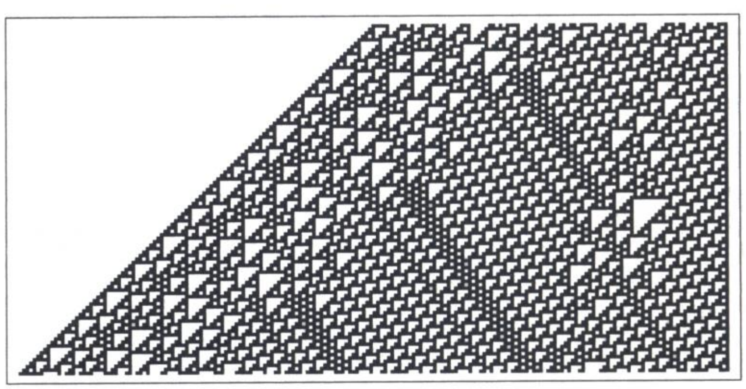
And now we consider the global evolutionary behavior of these *CA*s, again with respect to the initial configuration $\overline{1}$.



randomness (rule 30)



nesting (rule 90)



localized structures (rule 110)

As the previous examples show, different *CA*s evolve to one of a combination of either constant or locally organized behavior or even apparently random, fractal-like behavior; in many cases these global structures are consistent for a particular *CA* across nearly all initial configurations.[9] As I have indicated, these and other corroborating results reveal a surprising propinquity between so-called "ordered" or deterministic systems and chaotic systems. The discovery of this unexpected coupling appears gravid with all sorts of important consequences for an array of fields as far-flung as computational complexity, biology, artificial life and philosophy.

For the remainder of this paper we address the question of determining the evolutionary behavior of general *CA*s using concepts from *universal algebras*.

Definition 2. (Universal Algebra) For S a nonempty set and *n* a nonnegative integer we define $S^0 = \{\varnothing\}$, and for *n* > 0, S^n is the set of n-tuples of elements from S. An *n-ary* operation on S is any function from S^n to S (consider σ from above); *n* is said to be the *arity* of σ. The image of $\langle a_1, a_2, ..., a_n \rangle$ under an *n-ary* operation σ is written $\sigma(a_1, a_2, ..., a_n)$, as before.

II.Cellular Automata as Groupoids

In what follows we are primarily interested in approaching *CA*s in terms of a minimally-restrictive algebraic structure known as a *groupoid*. A groupoid is a set with a *binary* operation σ; that is, $\sigma(a_1, a_2) \in S \quad \forall a_1, a_2 \in S$. Many familiar algebraic features such as associativity, commutativity and the presence of identities and inverse elements (requirements that define, for instance, a common *group* structure) are not requisite for groupoids.

We now define two essential *operations on groupoids*; note that these operations are defined in an analogous way for groups, rings, fields and so forth.

Cartesian Product of (Two) Groupoids If $(A,\cdot_A)$ and $(B,\cdot_B)$ are each groupoids with binary operations as indicated, then $(A\times B,\cdot)$ is also a groupoid defined on the set $\mathrm{A}\times\mathrm{B}$, where $(a_1,b_1)\cdot(a_2,b_2)=(a_1\cdot_A a_2, b_1\cdot_B b_2)$.

Homomorphisms and Quotients on Groupoids A mapping $\theta:\mathrm{A}\to\mathrm{B}$ is a groupoid *homomorphism* if $\theta(a_1\cdot_A a_2)=\theta(a_1)\cdot_B\theta(a_2)\ \ \forall a_1,a_2\in A$. Such a θ is an *isomorphism* if it is bijective, and an *endomorphism* if it maps A into itself. A groupoid B is a *quotient* of groupoid A if there is a surjective homomorphism from A to B. Isomorphisms between groupoids define an equivalence relation in the usual way.

Although *CA*s may in general exhibit unpredictable evolutionary behavior, one nice fundamental result is that the class of *CA*s with fixed parameters *l* = 1 and *r* = 0 are sufficient to simulate *all* other *CA*s – irrespective of the initial state.[7] That is to say, for any arbitrary *CA*, $\mathrm{A}=(S,l,r,\sigma)$, there exists a *CA* $\mathrm{B}=(S,1,0,\tau)$ and integers *k* and *c* ("scale" and "shift" factors, respectively) where $\mathrm{B}_{kt,n+ct}(s)=\mathrm{A}_{t,n}(s)$ for all $s\in S^{\mathbb{Z}}$. This means that with the evolutionary diagram of B in hand, it is possible to "read" from it the output of automaton A. Note that with *l* and *r* fixed as indicated, the induced automaton is arity-2 – which is to say that it is a groupoid. The reduction of all *CA*s to this particular special case is, nevertheless, somewhat intuitive; it is commonly known, for instance, that all Turing machines (*TM*s) can be simulated by some binary TM.

We will denote the operation of the groupoid A defining a cellular automaton using juxtaposition notation. Accordingly, for *s*, some initial configuration of A, the state of cell *n* after one computational iteration is expressed:

$$A_{2,\mathrm{n}}(s)=A_{1,\mathrm{n-1}}A_{1,\mathrm{n}}(s)\quad\forall n\in\mathbb{Z}$$

Where multiplication here occurs according to the definition of the state mapping σ defined for A. More generally, for any finite number of discrete time steps, we have:

$$A_{t+1,n}(s)=A_{t,n-1}(s)A_{t,n}(s)\quad\forall n\in\mathbb{Z},\ t\in\mathbb{N}.$$

We would now like to develop a way to algebraically relate two or more automata – perhaps with different initial states. Consider then a "global" multiplication between two configurations, *s* and *t* of A, denoted: $s \cdot_A t$, so that $(s \cdot_A t)(n) = s(n) \cdot_A t(n)$. Hence, the product configuration is rendered by inducing the binary operation from A at each "pair" $s(n)$ and $t(n)$ over all n. For example, if $s(100) = 1$, $t(100) = 7$ for two configurations of automaton A (note that $|\mathrm{S}| > 2$ here) and $\sigma(1,7) = 6$, then it follows that $(s \cdot_A t)(100) = s(100) \cdot_A t(100) = 6$. Notice that multiplication between configurations is non-commutative, i.e. $s \cdot_A t \neq t \cdot_A s$ in general. Even so, it is possible to coax a "structurally-preserving" property from out of the shadows by way of the use of a *shift operator*. Define $\Xi(s)$ on the configuration *s* by $(\Xi(s))(n) = s(n-1)$. Now if we combine together the global multiplication and shift operators, we see that the result is a homomorphism between configurations:

$$\Xi(s \cdot_A t) = \Xi(s) \cdot_A \Xi(t).$$

This is straightforward to verify:

$$(\Xi(s \cdot_A t))(n) = (s \cdot_A t)(n-1) = s(n-1) \cdot_A t(n-1) = (\Xi(s))(n) \cdot_A (\Xi(t))(n) \square$$

Finally, it is possible to combine notations from above, whereby:

$$\mathrm{A}_{t+1}(s) = \mathrm{A}_t(s)\,\Xi(\mathrm{A}_t(s)).$$

In continuing the theme of exploring operations between automata, we consider the following definitions.

Definition 3. A cellular automaton $\mathrm{B} = (\mathrm{B}, \tau)$ is a *subautomaton* of a *CA* $\mathrm{A} = (\mathrm{A}, \sigma)$ if and only if $B \subseteq \mathrm{A}$ and for all $b \in B^{\mathbb{Z}}$ and for all $t \in \mathbb{N}$ and $n \in \mathbb{Z}$, $\mathrm{A}_{t,n}(b) = \mathrm{B}_{t,n}(b)$. That is, the evolution of A is identical with that of B for all initial configurations containing only states in B.

Definition 4. A cellular automaton $\mathrm{B} = (\mathrm{B}, \tau)$ is a *quotient automaton* of a *CA* $\mathrm{A} = (\mathrm{A}, \sigma)$ if and only if there is a surjective mapping $\theta : \mathrm{A} \to \mathrm{B}$ such that for all $t \in \mathbb{N}$, $n \in \mathbb{Z}$ and $s \in A^{\mathbb{Z}}$,

$$\theta\left(\mathrm{A}_{t,n}(s)\right) = \mathrm{B}_{t,n}\left(\theta(s)\right)$$

where $\theta(s)$ denotes the vector obtained from *s* by applying θ to each component of *s*. If θ is injective then the automata are isomorphic.

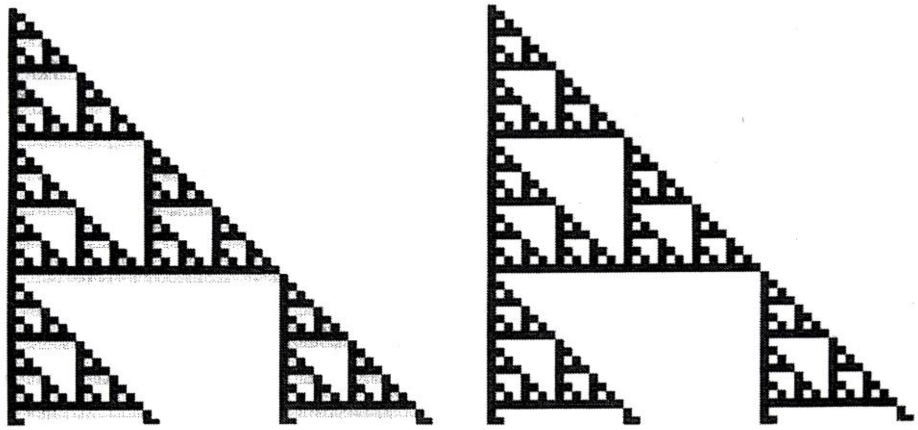
Thus the presence of a quotient automaton with respect to automaton A implies that the global evolution of some $\mathrm{B}(s)$ can be rendered from $\mathrm{A}(s)$ by making the replacement $\theta(s)$ for each state *s* in $\mathrm{A}(s)$. We consider the following algebraic example to help illustrate this idea.

Let $\mathrm{A}(S,1,0,\sigma)$ be defined so that $S = \{0,1,2,3\}$ and $\sigma : S^2 \to S$ where $\sigma(a_1, a_2) = a_1 + a_2 \pmod 4$. Consider now the automaton $B(S',1,0,\tau)$ where $S' = \{0,1\}$ and $\tau(a_1, a_2) = a_1 + a_2 \pmod 2$. Then the surjective mapping $\theta : \mathrm{A} \to \mathrm{B}$ defined by $\theta(a) = a \pmod 2$ defines a quotient automaton of A. To see this explicitly, note that:

$$\theta\left(\mathrm{A}_{t,n}(s)\right) = \theta\left(\sigma(a_1, a_2)\right) = \theta\left(a_1 + a_2 \pmod 4\right) = a_1 + a_2 (\mathrm{mod}\, 2) =$$

$$\theta(a_1 + a_2) = \tau\left(\left(\theta(a_1), \theta(a_2)\right)\right) = \mathrm{B}_{t,n}\left(\theta(s)\right).$$

The figure below offers a pictorial interpretation of an analogous quotient between 'mod 3' and 'mod 2' *CA*s. Note the degree to which the evolutionary diagram – though it obscures the underlying algebraic details – nonetheless enhances our ability to easily identify a quotient automaton.



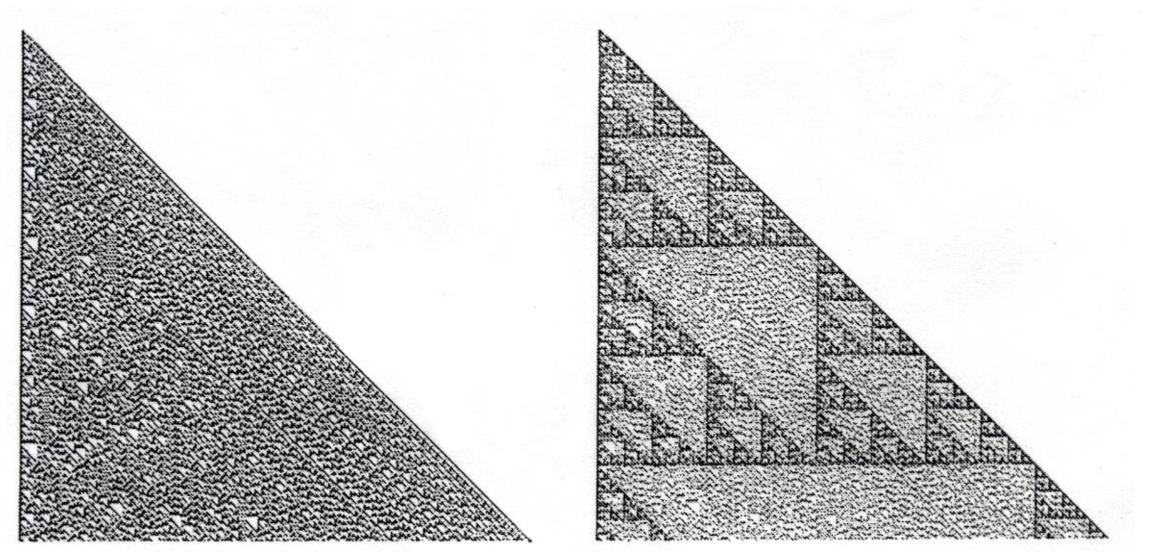
(a) (b)

Figure1: (a) Evolution of a three-state *CA* from an initial configuration of one cell in state 1 for 50 generations. (b) Evolution of a two-state quotient CA of the automaton in (a) under the mapping grey $\to$ white, black $\to$ black, white $\to$white. The rule for this *CA* is $\sigma(x,y) = x + y \pmod 2$.

Definition 5. A cellular automaton $\mathrm{A} = (\mathrm{A}, \sigma)$is a product automaton of the *CA*s B and $\tilde{\mathrm{B}}$ if $\mathrm{A} = \mathrm{B} \times \tilde{\mathrm{B}}$, and for all $t, n \in \mathbb{N}$ and all $s \in A^{\mathbb{Z}}$,

$$\mathrm{A}_{t,n}(s) = \left(\mathrm{B}_{t,n}(\pi_1(s)), \tilde{\mathrm{B}}_{t,n}(\pi_2(s))\right)$$

where π_1 and π_2 are projection maps so that $\pi_1(a_1, a_2) = a_1$ and $\pi_2(a_1, a_2) = a_2$, for all tuples in S^2 induced by A. If A is isomorphic to $\mathrm{B} \times \tilde{\mathrm{B}}$ (*i.e.* $A \simeq B \times \tilde{B}$) then A may be considered to be a "global amalgamation" of the product $\mathrm{B} \times \tilde{\mathrm{B}}$. In terms of the corresponding evolutionary behavior diagram, the superposition of the diagrams for B and $\tilde{\mathrm{B}}$ engenders the diagram for A. We portray this phenomenon in the figure below.



(a) (b)

Figure 2: (a) Evolution of the three-state automaton whose rule is given by $\sigma(x,y) = x^2 + y \pmod{3}$. (b) Evolution of the product automaton of the CAs in figure 1(b) and figure 2(a). At this resolution, all non-zero values appear black.

Under specific conditions, the isomorphism of *CA*s with the product of automata yields propitious algebraic results.

<u>Lemma 1</u>. If we impose the requirement that automaton $\mathrm{A} = (\mathrm{A}, \sigma)$ contains a "zero point" so that $\sigma(0, a_1) = \sigma(a_1, 0) = 0 \quad \forall a_1 \in A$, then it follows that $\dot{0} \times \mathrm{A} \simeq \mathrm{A} \times \dot{0} \simeq \dot{0}$, where $\dot{0}$ here represents the zero or "blank" automaton. Similarly, if the *CA* A contains a "left-right identity" so that $\sigma(1, \mathrm{a}_1) = \sigma(a_1, 1) = a_1 \quad \forall a_1 \in \mathrm{A}$, then it follows that $\mathrm{A} \simeq \dot{1} \times \mathrm{A} \simeq \mathrm{A} \times \dot{1}$, where $\dot{1}$ here represents the identity or "full" automaton.

<u>Proof</u>. Define the canonical homomorphism $\theta_0 : \dot{0} \times \mathrm{A} \to \dot{0}$ by $\theta_0\left(\sigma\left(0, \pi_2(s)\right)\right) = 0$; this gives the desired isomorphism. Likewise, consider the canonical identity homomorphism, $\theta_1 : \dot{1} \times \mathrm{A} \to \mathrm{A}$ where $\theta_1\left(\sigma\left(0, \pi_2(s)\right)\right) = a_2$, where., once again, $\pi_2(s) = \pi_2(a_1, a_2) = a_2$ – without loss of generality; this provides the necessary bijection. $\square$

Theorem 1. Let A, B and $\tilde{\mathrm{B}}$ be cellular automata corresponding to groupoids A, B and $\tilde{B}$ respectively. Then A is isomorphic to (a subautomaton of/a quotient automaton of) B if and only if A is isomorphic to (a subgroupoid of/a quotient groupoid of) B.

Proof. The subgroupoid case is trivial and we therefore omit it. For the quotient case, let A be a quotient automaton of B and $\theta : A \to B$ the associated quotient map. Without loss of generality, let *s* by some initial configuration with $s(0) = \delta_0$ and $s(1) = \delta_1$. It follows then that $\theta\left(\mathrm{A}_{1,1}(s)\right) = \mathrm{B}_{1,1}\left(\theta(s)\right)$ which implies $\theta(\delta_0\delta_1) = \theta(\delta_0)\theta(\delta_1)$, so θ is a groupoid homomorphism, as required.

Conversely, suppose that $\theta : A \to B$ is a groupoid homomorphism onto B, and let *s* be any configuration of A. Then for all integers *n*, we have that $\theta\left(s(n-1)s(n)\right) =$ $\theta\left(s(n-1)\right)\theta\left(s(n)\right)$; whereupon:

$$\theta\left(s(n-1)s(n)\right) = \theta\left(\mathrm{A}_{1,n}(s)\right) = \mathrm{B}_{0,n-1}\left(\theta(s)\right)\mathrm{B}_{0,n}\left(\theta(s)\right) = \mathrm{B}_{1,n}\left(\theta(s)\right)$$

This result holds for all integers *n* and all $t \geq 0$ (recall that s is an arbitrary configuration, making the value of *t* arbitrary), thus establishing the quotient automaton condition.

Corollary 1. A is the product of automaton of B and $\tilde{\mathrm{B}}$ if and only if A is the groupoid product of B and $\tilde{B}$.

Proof. Suppose A is the product automaton of B and $\tilde{\mathrm{B}}$. Then for all $t, n \in \mathbb{N}$ and all $s \in A^{\mathbb{Z}}$, $\mathrm{A}_{t,n}(s) = \left(\mathrm{B}_{t,n}\left(\pi_1(s)\right), \tilde{\mathrm{B}}_{t,n}\left(\pi_2(s)\right)\right)$. If we fix values for *t* and *n* and let $s = (a,b)$ over all values $(a,b) \in A^2$, then $A = B \times \tilde{\mathrm{B}}$, where the groupoid operation on the product is imparted from A. The logical converse follows naturally.▯

The main purpose in these latter results is to highlight both the degree to which the properties of *CA*s are in large part determined by the algebraic structure of their underlying group(oids) and to also draw attention to the potential decomposition properties of *CA*s. As we have shown by example the in Figure 2, the product of *CA*s can be realized pictorially as the superimposition of their respective evolutionary diagrams. It therefore stands to reason that if it is possible to decompose the groupoid substrate of a given *CA* into a coherent set of elemental types, then a general taxonomy of *CA*s is within reach. Unfortunately, however, there is no finite set of finite groupoids that generate all others by way of basic algebraic operations.[7] In his article, Pederson verifies that every finite groupoid is a subdirect product of finitely-many subdirectly irreducible groupoids; and, since there are an infinite number of such irreducible groupoids, it follows that the complexity of their classification is not conducive to a reductive organization of *CA*s.

In order to obtain reasonable decomposition results, we accordingly restrict the class of groupoids under consideration to those which are amenable to decomposition themselves. To this end, we now regard *CA* $\mathrm{A} = (\mathrm{A}, \sigma)$, where A is a finite abelian group. By the fundamental theorem of abelian groups, it is known that: $A \simeq \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{k_i}}$, where $\{p_i\}$ is a set of primes and $\{k_i\}$ is a set of positive integers. Together, we use this result combined with previous remarks to achieve a concise classification of the evolution of any *CA* with an underlying finite abelian group structure.

In the usual way, denote the elements of $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$, where $\langle 1 \rangle = \mathbb{Z}_n$. We now proceed to show that the evolutionary behavior of *CA* $\mathrm{A} = (\mathrm{A}, \sigma)$, with finite abelian group A, for *any* initial configuration, is entirely determined by its behavior for the *elementary initial configuration* consisting of a single instance of the generator of the group (recall that the group is cyclic here) followed by a doubly-infinite array of zeros. More formally, recall that the configuration $\overline{1}$ was defined:

$$\overline{1}(i) = \begin{cases} 1 & if\ i = 0 \\ 0 & else \end{cases}$$

Next we demonstrate that the abelian nature of the underlying group for A extends as an "additive" property to the sum of configurations. To wit, for any configurations $s, t \in A^{\mathbb{Z}}$ and any $t_0 \geq 0$, where + denotes the binary operation for A, we have:

$$A_{t_0}(s+t)=(s+t)+((s-1)+(t-1))=(s+t)+\Xi(s+t)$$

$$= s+t+\Xi(s)+\Xi(t) \qquad \text{(by the additivity of the shift operator)}$$

$$= s+\Xi(s)+t+\Xi(t) \qquad \text{(by commutativity)}$$

$$= A_{t_0}(s)+A_{t_0}(t).$$

Next we prove a result by induction which will lead to a general theorem for *CA*s defined for finite abelian groups.

<u>Lemma</u>. $A_{t,k}(\overline{1})=\binom{t}{k}\bmod n$ where the $\binom{t}{k}$ coefficient is defined in the usual way to be zero whenever $k>t$ or $k<0$.

<u>Proof</u>. Using induction on k and t, where $k \geq 0$: if $k=0$ then $A_{t,0}(\overline{1})=0=\binom{t}{0}\bmod n$, irrespective of *t*. Now suppose that $A_{t,k}(\overline{1})=\binom{t}{k}\bmod n\ \forall k \leq k^* \in \mathbb{N},\ t \leq t^*-1$. We consider the case:

$$A_{t^*,k^*+1}(\overline{1})=A_{t^*-1,k^*}(\overline{1})+A_{t^*-1,k^*+1}(\overline{1}) \quad \text{(by definition of the evolution of a 2-ary } CA\text{)}$$

$$=\binom{t^*-1}{k^*}+\binom{t^*-1}{k^*+1}\bmod n \qquad \text{(by the inductive hypothesis)}$$

$$=\ldots=\frac{t^*!}{(k^*+1)!(t-(k^*+1))}\bmod n=\binom{t^*}{k^*+1}\bmod n,$$

which proves the desired result.

Alternatively, note that the evolution of automaton $A_{t,k+1}(\overline{1})$ yields a familiar result in the form of Pascal's triangle (mod n) embedded in a doubly-infinite array of zero values:

	0	0	1	0	0	0	0	0		$t=0$
	0	0	1	1	0	0	0	0		$t=1$
…	0	0	1	2	1	0	0	0	…	$t=2$
	0	0	1	3	3	1	0	0		$t=3$
	0	0	1	4	6	4	1	0		$t=4$

Thus the result of the lemma likewise follows from elementary identities involving binomial coefficients. □

If we combine this outcome with the aforementioned additive property of *CA* evolutionary behavior, one can prove, in a manner similar to the preceding proof, that for any initial configuration s, any $t \geq 1$ and any $i \in \mathbb{Z}$,

$$A_{t,i}(s) = \sum_{k=0}^{i} s(k) A_{t,i}(\overline{1}). \qquad (1)$$

The reader will note that this result importantly relates the computation of any finite abelian *CA* with arbitrary initial configuration to the evolutionary status of the *elementary initial configuration* (i.e. the embedded form of Pascal's triangle) "operated" together with the given arbitrary initial configuration. In short, this result yields an efficient way to articulate the evolutionary behavior of such finite abelian *CA*s using minimal computation.

We better illustrate this property with a concrete example. Consider the initial configuration $s = \langle \ldots, 0, 0, 1, 2, 3, 4, 5, 0, 0, \ldots \rangle$, (with $s(0) = 1$) for $A = \mathbb{Z}_{10}$.

Then the evolution of A is given as:

	0	0	1	2	3	4	5	0		$t=0$
	0	0	1	3	5	7	9	5		$t=1$
…	0	0	1	4	8	2	6	4	…	$t=2$
	0	0	1	5	2	0	8	0		$t=3$
	0	0	1	6	7	2	8	8		$t=4$

with all computations executed mod 10.

As the reader may check, for instance,

$$A_{4,2}(s) = 7 = \sum_{k=0}^{2} s(k) A_{4,\mathrm{i-k}}(\bar{1}) = (1+6)+(2+4)+(3+1).$$

If we combine (1) with the preceding lemma, the result is a useful characterization of the evolution of all *CA*s with arbitrary initial configuration over finite cyclic groups.

<u>Theorem 2(A)</u>. Let *A* be the *CA* over $\mathbb{Z}_n$. Then for any initial configuration s and any $t \geq 1$,

$$A_{\mathrm{t,i}}(s) = \sum_{k=0}^{i} s(k) \binom{t}{i-k} \bmod n.$$

More generally still, if we wish to apply this result to *all CA*s with an underlying finite abelian group structure, we can employ the fundamental theorem of finite abelian groups to Theorem 2(A). The theorem that follows is even broader in scope. [7, p. 243]

<u>Theorem 2(B)</u>. Let *A* be a *CA* over any finite abelian group, whereupon $A \simeq \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{k_i}}$ for a set of primes $\{p_i\}$ with positive integer exponents. Then for any initial configuration s and any $t \geq 1$,

$$A_{\mathrm{t,i}}(s) = \sum_{j=0}^{n} \sum_{k=0}^{i} s(k) \binom{t}{i-k} \left(\bmod \prod p^k\right).$$

This theorem gives a general classification of the evolutionary behavior of *any* finite abelian *CA*. However, because no such analogue to the fundamental theorem of finite abelian groups exists for groupoids in general (see the discussion above), decomposition results for nonabelian *CA*s is much less tractable.

Next we consider algebraic properties of *CA*s that harness one of the key features of many “well-behaved” automata – periodicity.

III. Algebraic Varieties and Periodic Behavior

Having exhausted our effort to codify *CA*s through a decomposition technique which relies heavily on a simple, underlying abelian algebraic structure, we now follow a more general approach using a *variety of algebras*. Informally, a *variety* is class of algebras (with a fixed *signature* – see the subsequent comments) that is closed under the formation of homomorphic copies of quotients, subalgebras and direct products.[7] Nevertheless, for the purposes of this paper and the proofs that follow, we will use an alternative – yet equivalent – characterization of a variety expressed by the "HSP"/Birkhoff Theorem.

Birkhoff's Theorem. A class of algebraic structures with a fixed signature is a variety if and only if the class satisfies a given set of identities.[3]

Accordingly, a variety is an algebraic class that can be defined *equationally* (a more formal rendering of what is meant by an "equation" follows). Below we consider varieties that capture the periodicity of *CA*s via a set of equations.

Definition 6. The *signature* of an algebra is a list of operations (typically this is expressed as a list of the respective "arity" of each operation) defined for the given algebra. For instance, a groupoid has signature (2) – for its lone binary operation; a group, on the other hand, has signature (2, 1, 0) – for the binary operation of the group, inversion and identity, respectively.

In this way, the class of all semi-groups (*i.e.* an algebraic structure with an associative binary operation) forms a variety of algebras of signature (2); the class of semi-groups is, naturally, closed under homomorphisms, "subalgebras" – namely, the operation of generating subalgebras of semi-groups – and direct products. Conversely, using Birkhoff's Theorem directly, the class of all semi-groups can be defined equationally: $a(bc)=(ab)c$, which is to say the class of all *associative* algebraic structures with a binary operation is a variety. Similarly, the class of all groups forms a variety of algebras of signature (2, 1, 0) since the class of groups is "H-S-P" closed; and by the same token, the following collection of identities is sufficient to demonstrate that groups form a variety.

$$a(bc) = (ab)c$$
$$a = 1a = a1$$
$$1 = aa^{-1} = a^{-1}a$$

We say that a groupoid A satisfies the identity $x = y$ where x and y are groupoid terms, where a "term" may be thought of as a concatenation of elements of A under the groupoid operation in the variables $x_1, x_2, ..., x_n$, if for every n-tuple $(a_1, a_2, ..., a_n)$ of elements from A, the expressions $x[x_1 / a_1, ..., x_n / a_n]$ and $y[x_1 / a_1, ..., x_n / a_n]$ evaluate to the same element of A; here x_i / a_i denotes the replacement of x_i by a_i for all occurrences of x_i. For clarification, the equations preceding this paragraph specify three *identities* over elements in a groupoid that give rise, collectively, to an algebraic group structure.

Next we offer an alternative definition of an identity which is equivalent to the preceding discussion by way of the extension of a groupoid mapping. The *free groupoid* $F(X)$ on the set X is defined as the set of all groupoid terms. $F(X)$ has the property that any mapping from X into any other groupoid G can be extended uniquely to a homomorphism from $F(X)$ to G. In this manner, we will say that a groupoid G satisfies the identity $x = y$ for variables in X if and only if, for any mapping of X into G, the unique extension $\phi : F(X) \to G$ of the mapping fulfills the condition $\phi(x) = \phi(y)$.

Definition 7. A cellular automaton A is *k-periodic* (starting at generation *g*) if there exists $g \in \mathbb{N}$ such that for all initial configurations $s \in A^{\mathbb{Z}}$ and all $t \geq g$,

$$A_{t+k,n}(s) = A_{t,n}(s).$$

In other words, A is *periodic* if, for all initial configurations, its evolutionary behavior repeats uniformly after a finite number of generations. Note that the period *k* above is defined in such a way so as to include *CA*s with period less than *k*; this precaution is necessary so that the groupoids corresponding to all *k*-periodic *CA*s will form a variety.

Theorem 3. For each $g,k \in \mathbb{N}$, the groupoids defining *k*-periodic cellular automata after *g* generations form a variety: $V_{g,k}$. If $g \le h$ then $V_{g,k} \subseteq V_{\mathrm{h},k}$, and if *k* divides *p* then $V_{g,k} \subseteq V_{\mathrm{g,p}}$ [7, p. 244].

Proof. Let A be a *CA* and s some initial configuration of A. Define, inductively

$$s_i^0 = s(i) \qquad s_i^{k+1} = s_{i-1}^k s_i^k.$$

It then follows from the previous 2-ary configuration of *CA*s, that $A_{t,i}(s) = s_i^t$ $\forall i \in \mathbb{Z},\ t \in \mathbb{N}$. To see this more directly refer to the diagram below.

	c_{-2}	c_{-1}	c_0	c_1	c_2	
…	$c_{-3}c_{-2}$	$c_{-2}c_{-1}$	$c_{-1}c_0$	c_0c_1	c_1c_2	…
	$(c_{-4}c_{-3})(c_{-3}c_{-2})$	$(c_{-3}c_{-2})(c_{-2}c_{-1})$	$(c_{-2}c_{-1})(c_{-1}c_0)$	$(c_{-1}c_0)(c_0c_1)$	$(c_0c_1)(c_1c_2)$	

Here the c_i denotation is used to reference "cell *i*" of the initial configuration. It follows then that A is *k*-periodic beginning at generation *g* if and only if

$$s_i^{t+k} = s_i^t \quad \forall i \in \mathbb{Z}, t \ge g. \qquad (2)$$

Thus a period 1 *CA* beginning, say, with generation 0 would exhibit identical rows at all discrete time stages; moreover, this *CA* would satisfy the identity $c_{i-1}c_i = c_i$ (which we may extend inductively) for all integer values of *i*. In the same way, a period 2 *CA* beginning with generation 0 would exhibit two sets of identical rows for even and odd indices respectively; furthermore, this *CA* would comply with $(c_{i-2}c_{i-1})(c_{i-1}c_i) = c_i$ – which requires the satisfaction of the equivalent groupoid identity $(xy)(yz) = z$ over all elements of the groupoid for A.

More generally, we now explore an inductive description of periodicity by way of the satisfaction of identities on the variables $X = \{x_0, x_1, x_2, \ldots\}$. For ease of notation, we introduce a "left shift" operator (Λ) on *strings*, which is to say a concatenation of elements from the set X . If we let $\Lambda_0 : X \to X : x_i \to x_{i+1}$ be the left shift operator on a single string from X , then we define Λ as the natural, operation-preserving (i.e. $\Lambda(x \cdot y) = \Lambda(x) \cdot \Lambda(y)$) extension of Λ_0 over the free groupoid $F(X)$. The reader will observe that Λ is the unique extension of Λ_0 defining an endomorphism.

Using the left shift operator, groupoid *terms* may be generated sequentially using the following recursive construction:

$$\alpha_0 = x_0 \quad \alpha_{i+1} = \Lambda(\alpha_i) \cdot \alpha_i \quad \forall i \in \mathbb{N}$$

In this fashion, $\alpha_1 = x_1 x_0, \alpha_2 = (x_2 x_1)(x_1 x_0)$, and so forth. Using this convention and the results of the preceding discussion, note that the variety $V_{g,k}$ of cellular automata with period *k* after generation *g* is defined by

$$\alpha_{g+k} = \alpha_g . \qquad (3)$$

<u>Example</u>. For a *CA* with period 2 beginning at generation 0,

$$\alpha_0 = \alpha_2 = \Lambda(\alpha_1) \cdot \alpha_1 = \Lambda(\alpha_1) \cdot \Lambda(\alpha_0)\alpha_0$$

$\overset{iff}{\leftrightarrow} x_0 = x_2 x_1 x_1 x_0$ (now replace variable x_i with re-indexed

$c_i = a_i \in A$, in reverse, for $0 \le i \le 2$)

$\overset{iff}{\leftrightarrow} (c_{i-2} c_{i-1})(c_{i-1} c_i) = c_i$.

As the reader may verify, this last condition is identical to the requirement stipulated for a *CA* with period 2 beginning with generation 0 using definition (2), which indicates that definition (3) implies (2). More rigorously, suppose that the groupoid A meets the periodicity condition (3); we show that (2) is also satisfied; thus we show, finally: (2) iff (3).

Fix values $i \in \mathbb{Z}$ and $t \in \mathbb{N}$. Let $f_0 : X \to A$ be the map defined by $f_0(x_j) = s_{i-j}^t$, and let f be the natural extension of this map to a homomorphism from $F(X)$ to A. Then we have that for any *m*, the following holds

$$f(\alpha_m) = f(\Lambda(\alpha_{m-1}) \cdot \alpha_{m-1})$$

$$= f(\Lambda(\alpha_{m-1})) \cdot f(\alpha_{m-1}) = f(\Lambda(\Lambda(\alpha_{m-2}) \cdot \alpha_{m-2})) \cdot f(\Lambda(\alpha_{m-2}) \cdot \alpha_{m-2})$$

$$= \ldots = s_{i-1}^{m+t-1} s_i^{m+t-1} = s_i^{m+t}. \quad \text{(by induction and the construction given in (2)).}$$

Because (3) holds without loss of generality for any periodic A, this indicates

$$f(\alpha_{g+k}) = f(\alpha_g) \overset{iff}{\leftrightarrow} s_i^{(g+k)+t} = s_i^{g+t}.$$

Since this latter condition defines a periodic *CA* with configuration *s*, we have shown that the requirement for a periodic variety implies that of a periodic *CA*. Now we demonstrate the converse implication.

Suppose then that A has period *k* after *g* generations, so condition (2) is met. Let $a_0, a_1, \ldots, a_{g+k} \in A$ and $h_0 : X \to A$ by the injective map where $h_0(x_i) = a_i$ for $0 \le i \le g+k$. As in the previous cases, we define the extension of this map naturally as the homomorphism over the free groupoid $h : F(X) \to A$. In order to establish the desired identity condition for the groupoid (outlined on p. 16), it remains to show that $h(\alpha_{g+k}) = h(\alpha_g)$. Allow that *s*, an initial configuration is defined without loss of generality as $s(i) = a_{g+k-i}$ for $i = 0,1,\ldots,g+k$. More explicitly, the cells of *s* are given as

a_{g+k}	a_{g+k-1}	a_{g+k-2}	...	a_1	a_0

If we define s_i^t in the usual inductive way for this initial configuration, then using an argument analogous to that of the preceding paragraph, one can establish that $h(\alpha_t) = s_{g+k}^t \; \forall t \ge 1$. Now the presumed *k*-periodic nature of A yields $s_{g+k}^{g+k} = s_{g+k}^{g}$, whereby $h(\alpha_{g+k}) = h(\alpha_g)$, as needed. ▯

In summary, we have established that a cellular automata is *k*-periodic beginning with generation *g* (*viz.*, it satisfies (2)) if and only if it satisfies the identity given by (3) over the variables $x_0, x_1, x_2, \ldots$; by Birkhoff's Theorem, this equivalence is sufficient to show that the class of the groupoids underlying such *CA*s forms a variety: $V_{g,k}$.

Lastly, if $g \le h$, it follows that $V_{g,k} \subseteq V_{\mathrm{h},k}$ since a *k*-periodic *CA* after *g* generations is still *k*-periodic for any time-lapse exceeding *g* generations. In addition, if $\mathrm{k} \mid p$, then $kn = p$, so a *k*-periodic *CA* is automatically *p*-periodic for a common, fixed number of generations; ergo, $V_{g,k} \subseteq V_{\mathrm{g,p}}$. □

Corollary 2. A product automaton of periodic automata is periodic. In addition, if $A \in V_{g,k}$ and $B \in V_{\mathrm{h,p}}$, then $A \times B \in V_{m,c}$ where $m = \max\{g,h\}$ and $c = lcm\{k, p\}$.

Proof. By Theorem 3 and the fact that *c* is divisible by both *k* and *p*, and that a periodic *CA* beginning with generation *g* is also periodic for any time-lapse after *g*, we have:

$$V_{g,k} \subseteq V_{m,k} \subseteq V_{m,c} \text{ and } V_{\mathrm{h,p}} \subseteq V_{\mathrm{m,p}} \subseteq V_{m,c}.$$

Since varieties are closed under products, it follows that if $A \in V_{m,c}, \mathrm{B} \in V_{m,c}$ then $A \times B \in V_{m,c}$. □

Corollary 3. For all $n, k \in \mathbb{N}$, there exists a natural number $\mu_k(n)$ such that if a *CA* with at most *n* states is *k*-periodic, then it is *k*-periodic after $\mu_k(n)$ generations. In this way, every *CA* with period *k* and at most *n* states is an element of the variety $V_{\mu_k(n),\mathrm{k}}$. Furthermore, for every *n* there exist a natural number $\pi(n)$ such that if a CA on *n* states is periodic, then it has period at most $\pi(n)$.

Proof. Note that there exists only a finite number of *CA*s for a finite state set (recall that a periodic *CA* is periodic irrespective of its initial configuration); thus there is such a finite value $\mu_k(n)$. As with the previous corollary, if a *k*-periodic *CA* is periodic after $g < \mu_k(n)$ generations, then we have $A \in V_{g,k} \subseteq V_{\mu_k(n),\mathrm{k}}$, as required. Finally, the finitude of all *CA*s with a finite state set guarantees the existence of the number $\pi(n)$. □

We now endeavor to classify periodic *CA*s with a reasonably small state set. Using the *pseudo-identity* restriction, $0 \cdot 0 = 0$ for groupoids, it can be shown computationally that of the total $3^8 = 6,561$ such 3-state groupoids, 2,352 are non-isomorphic. Intuitively, one would expect that a small fraction of these corresponding *CA*s are periodic, and indeed, exhaustive computations show that only 191 of these are 1-periodic, while 256 are 2-periodic (recall that 1-periodic *CA*s over a fixed state set are a subset of 2-periodic *CA*s).[7] Despite, however, the paucity of periodic *CA*s even over small state sets, these *CA*s nevertheless all stabilize extremely quickly. In this way, it might be said more broadly that while "order" (here we consider order *qua* a reduction to periodicity) in an arbitrary, deterministic computational model is largely uncommon, when present, order rapidly suffuses each and every aspect of the governing system. To this point, computer enumeration has shown that $\mu_1(3) = 4$, $\mu_2(3) = 5$ (for a 4-state *CA* the bound is however at least 6) and $\pi(3) = 2$. This last result yields the remarkable conclusion that there exist only 256 periodic *CA*s with 3-state sets, up to isomorphism. Again, we emphasize the fact that without some of the results annunciated here, classification of all periodic *CA*s with 3-state sets would seem, *prima facie*, possibly intractable.

For illustrative purposes, note that the 3-state *CA*, with $A = \{0,1,2\}$ is 1-periodic beginning with generation 3, in line with the foregoing comments. To see that this cellular automaton is 1-periodic for all initial configurations, notice the inherent hierarchy of elements with respect to the groupoid operation: $1 \to 2 \to 0$. The *CA* tableau for A is listed at the right.

	0	1	1	2	2	1	1	0	
	0	0	1	2	0	2	1	0	
…	0	0	0	2	0	0	2	0	…
	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	0	

$0 \cdot 0 = 0$
$0 \cdot 1 = 0$
$0 \cdot 2 = 0$
$1 \cdot 0 = 0$
$2 \cdot 0 = 0$
$1 \cdot 1 = 1$
$1 \cdot 2 = 2$
$2 \cdot 1 = 2$
$2 \cdot 2 = 0$

Another notable result, summarized in the following theorem, employs again the strategy of building a general result pertaining to *CA* periodicity by considering the domain of small state sets.

<u>Theorem 4</u>. For all positive integers *k* and *g*, $C_3 \cap V_{g,2k+1} = C_3 \cap V_{g,1}$ and $C_3 \cap V_{g,2k} = C_3 \cap V_{g,2} \;\; \forall g \geq 0$ (where C_3 denotes the set of all 3-element groupoids).

Put concisely, Theorem 4 states that *any* 3-state *CA* with odd period beginning at (fixed) generation *g* is 1-periodic; similarly, any *CA* with even period is 2-periodic. [7, p.245]

<u>Proof</u>. Computer enumeration shows that $C_3 \cap V_{g,2k+1} = C_3 \cap V_{g,1} \;\; \forall g \leq 4$, and because $\mu_1(3) = 4$, it follows that this result holds for all values of *g*. Analogously, enumeration gives $C_3 \cap V_{g,2k} = C_3 \cap V_{g,2} \; \forall g \leq 5$, and as $\mu_2(3) = 5$, equality holds for all *g*. Recalling that $\pi(3) = 2$, the theorem follows. $\square$

From the preceding characterization of 3-state *CA*s with the pseudo-identity restriction, we can now develop an equational construction for all such 3-state *CA*s.

<u>Theorem 5</u>. A 3-state cellular automata A with $0 \cdot 0 = 0$ is periodic if and only if its groupoid satisfies the recursive identity $\alpha_7 = \alpha_5$; when this identity is expanded over arbitrary elements $s,t,u,v,w,x,y,z \in A$ (where some of these elements are necessarily identical) we have:

$$
\begin{aligned}
&(\{[((st \cdot tu)(tu \cdot uv)(uv \cdot vw))] \\
&\cdot[((tu \cdot uv)(uv \cdot vw))((uv \cdot vw)(vw \cdot wx))]\} \\
&\cdot\{[((tu \cdot uv)(uv \cdot vw))((uv \cdot vw)(vw \cdot wx))] \\
&\cdot[((uv \cdot vw)(vw \cdot wx))((vw \cdot wx)(wx \cdot xy))]\}) \\
&\cdot(\{[tu \cdot uv)(uv \cdot vw))((uv \cdot vw)(vw \cdot wx))] \\
&\cdot[((uv \cdot vw)(vw \cdot wx))((vw \cdot wx)(wx \cdot xy))]\} \\
&\cdot\{[((uv \cdot vw)(vw \cdot wx))((vw \cdot wx)(wx \cdot xy))]
\end{aligned}
$$

$$\cdot [((vw \cdot wx)(wx \cdot xy))((wx \cdot xy)(xy \cdot yz))]\})$$
$$= [((uv \cdot vw)(vw \cdot wx))((vw \cdot wx)(wx \cdot xy))]$$
$$\cdot [((vw \cdot wx)(wx \cdot xy))((wx \cdot xy)(xy \cdot yz))].$$

Proof. Together, from Theorem 4 we know that $\pi(3) = 2$ and $\mu_2(3) = 5$, which indicates that every 3-state *CA* satisfying the pseudo-identity condition has period ≤ 2 beginning at generation 5. From the recursive construction defined on p.18, $\alpha_{g+k} = \alpha_g$, whence $\alpha_7 = \alpha_5$. The explicit expansion given above follows from the aforementioned recursion [7, p. 246]. □

IV. Shift-Periodic Cellular Automata

So far we have only directly considered *CA*s with an underlying binary operational structure (*i.e.* where $l = 1, r = 0$ *à la* definition 1). With the shift operations introduced previously, it is possible to generalize the 2-ary groupoids *CA*s to settings which encompass larger definitional "neighborhoods." To this end, we introduce a slight modification to our earlier characterization of periodicity so as to allow for the implementation of the shift operator in some of our earlier theorems.

Definition 7. A ($l = 1, r = 0$) cellular automaton A is *shift-periodic* of period *k* and *shift factor c*, starting at generation *g*, if, for all initial configurations *s* of A,

$$A_{t+k,n+c}(s) = A_{t,n}(s) \quad \forall t \geq g, n \in \mathbb{Z}.$$

To ensure clarity, an example of a CA $A = \{1, 2, 3, 4\}$ with period 2 (for the specific initial configuration given), shift factor 4 and starting generation 0 is provided below.

										$1 \cdot 2 = 2$
	1	2	3	4	1	2	3	4		$4 \cdot 1 = 1$
	1	2	1	2	1	2	1	2		$2 \cdot 3 = 1$
…	1	2	3	4	1	2	3	4	…	$3 \cdot 4 = 2$
	1	2	1	2	1	2	1	2		$2 \cdot 1 = 3$
	1	2	3	4	1	2	3	4		$3 \cdot 2 = 2$
										$else: a \cdot b = 1$

Theorem 6. For each $g, k, c \in \mathbb{N}$, the groupoids defining *CA*s of period *k* with shift factor *c* starting in generation *g* form a variety $V_{g,k,c}$ defined by the identity

$$\alpha_{g+k} = \Lambda^c\left(\alpha_g\right).$$

Here α_i follows the inductive definition given in Theorem 3 and Λ^c is the c-fold composition of the shift operator. [7, p. 248]

Proof. The proof here is nearly identical to that of the proof for Theorem 3. Simply replace (3) with the condition $\alpha_{g+k} = \Lambda^c\left(\alpha_g\right)$ and the result follows, *mutatis mutandis*.

Using the shift operator, we now develop analogues to Corollaries 2 and 3 for varieties based upon shift-periodic *CA*s. □

Theorem 7(1). If $g \le h$ then $V_{g,k,c} \subseteq V_{h,k,c}$. In this way, for each $k, c, n \in \mathbb{N}$ there exists a number $\mu_{k,c}(n)$ such that if a cellular automaton with *n* states is shift-periodic with period *k* and shift factor *c*, then this recurrence starts at generation $\mu_{k,c}(n)$.

Proof. Suppose that $A \in V_{g,k,c}$ with $g \le h$. Then A is shift periodic beginning with generation *g*, period *k* and shift factor *c*; but if the recurrence of A occurs by generation *g*, then it continues through generation $h \ge g$; thus $A \in V_{h,k,c}$. Once again, the finitude of possible *CA*s over *n* states guarantees the existence of the value $\mu_{k,c}(n)$. □

Theorem 7(2). If $a = \gcd\{k, c\}$ and there exists *m* such that $pa = mk$ and $da = mc$ then $V_{g,k,c} \subseteq V_{\mathrm{g,p,d}}$.

Proof. Suppose the preceding conditions hold for some $A \in V_{\mathrm{g},k,c}$. The existence of the integer *m* above shows us that the period of A can be made, in essence, to "sync up" with a period of duration *p* through *m* computational cycles of A (since $pa = mk$); likewise, the shift factor of A can be coordinated with a shift factor of length *d* through *m* computations of A (as $da = mc$); together, this implies $\in V_{\mathrm{g,p,d}}$. □

Through exhaustive enumeration it can be shown that $\mu_{1,1}(3) = 4$, $\mu_{2,1}(3) = 6$ and $\mu_{\mathrm{k},1}(3) = 4$ when $k \geq 3$.[7]

The computational results for all 3-state binary CAs with the pseudo-identity property are listed in the table below. Values in the table represent the total number of non-isomorphic *CA*s of the specified type, with period *k* and generation *g* for the various shift factors.

Table 1

Shift factor 0:

g/k	1	2	3	4
0	1	4	1	4
1	35	47	35	47
2	143	178	143	178
3	182	236	182	236
4	191	255	191	255
5	191	256	191	256
6	191	256	191	256

Shift factor 1:

g/k	1	2	3	4
0	1	0	0	0
1	35	11	1	1
2	143	52	34	34
3	182	81	54	54
4	191	94	60	60
5	191	96	60	60
6	191	97	60	60
7	191	97	60	60

Shift factor 2:

g/k	1	2	3	4	5	6
0	0	1	0	0	0	0
1	1	35	1	11	1	1
2	34	178	34	52	34	34
3	54	236	54	81	54	54
4	60	255	60	94	60	60
5	60	256	60	96	60	60
6	60	256	60	97	60	60
7	60	256	60	97	60	60

V. Conclusion

Enumeration for larger shift factors indicates that the presence of such shift-periodic *CA*s is scarce to non-existent; [7] this result is reasonable if we consider the restrictiveness of shift-periodicity over *all* initial configurations. If this conclusion is indeed valid it would indicate that there are only 293 3-state binary *CA*s that exhibit "order" *qua* shift-periodicity; where here the value 293 is from a total of 2,352 *CA*s, up to isomorphism, with 256 groupoids of period 2 (for even shift factor; where we note that $\mu_{k,1}(3)=4$) and 37 of the 97 occurring with period 2 and an odd shift factor (these were groupoids distinct from the previous set).

Current research for *CA*s with four or more states is still incomplete, as, for instance, the number of non-isomorphic 4-state *CA*s with period 1 is well over 500,000. Despite these computational obstacles, the instance of "ordered," i.e. periodic, *CA*s appears unsurprisingly to vanish asymptotically as the state size grows – however, a comprehensive proof of this supposition is still needed. The salient point, adumbrated previously, is that under arbitrary conditions, structural cohesion for even simple dynamic processes is exceptionally unusual; this paper provides irrefragable evidence of this phenomenon.

The opportunities for extended, fruitful research in this topic are legion. Much of the work in the present paper relies heavily upon two elementary notions of observable order: (1) periodicity and (2) shift-periodicity. These ideas may, however, be more finely-tuned with future explorations. For instance, since many *CA*s appear to exhibit systemic order that is localized – and would therefore elude consideration by the strict definitions of periodicity used here – future researchers might do well to utilize broader definitions like "cluster-periodicity" or "quasi-periodicity" in order to capture this cohesive, localized behavior. More generally still, it may be useful to consider the evolution in outputs of a given *CA* in terms of their tendency to increase or decrease in *complexity* over time as an alternative measure of order in an abstract "system" (here it would be possible to use a Kolmogorov criterion to compare the relative algorithmic "compressibility" of subsequent outputs). Conversely, in applications to fields such as Cryptography, the absence of order as a means to encrypt sensitive data is highly desirable; thus in this case the classification of non-periodic, pseudo-random generating *CA*s would potentially yield a wealth of intellectual capital.

Finally – although it may only be of purely speculative interest at the present time, Stephen Wolfram has recently suggested.[9] that the taxonomy of dynamical abstract systems (*via CA*s, among other models) is ripe with high-level, meta-scientific potential. In this regard, some of his latest research has begun to attempt to answer one of the great, perennial questions in all of philosophy and science: *why is there any order at all in our universe*? The answer to this question – if such a question elicits an answer, even – would seem to go a long way toward elucidating the long-standing efficacy of the scientific method as the greatest explanatory tool in all of human creation. Under this paradigm, the elements of the underlying groupoid of a given *CA* represent the *sine qua nons* of theoretical cosmological configurations – features such as the fundamental physical forces (e.g. gravitation, electro-magnetism) operational in a potential universe, its inherent dimension(s) and so forth. Incredibly then, the class of *CA*s could be considered as a computational model capable of mapping out, in some sense, the tapestry of a vast, formerly unknowable *multiverse*, comprised of a staggering number of possible – yet non-existent – chaotic and formless worlds, in addition to a vanishingly small number of "ordered" worlds – like our own.

Sources

[1] Aarson, Scott. *Quantum Computing Since Democritus*. Cambridge: Cambridge University Press, 2013.

[2] Boolos, George. *Computability and Logic*. Cambridge: Cambridge University Press, 2007.

[3] Burris, Stanley and H. P. Sankappanavar. *A Course in Universal Algebra*. New York: Springer, 1981.

[4] Dummit, David and Richard Foote. *Abstract Algebra*. Hoboken: Wiley, 2003.

[5] Hungerford, Thomas. *Algebra*. New York: Springer, 1996.

[6] Mitchell, Melanie. *Complexity: A Guided Tour*. New York: Oxford Press, 2011.

[7] Pedersen, John. "Cellular Automata as Algebraic Systems." Complex Systems 6 (1992): 237-250.

[8] Sipser, Michael. *Introduction to the Theory of Computation*. Boston: PWS Publishing, 2012.

[9] Wolfram, Stephen. *A New Kind of Science*. Champaign: Wolfram Media, 2002.

[10] Wolfram, Stephen. *Cellular Automata and Complexity*. Boston: Addison-Wesley, 1994.