Complex Systems **10** (1996) 185–194

Algebraic Properties of the Block Transformation on Cellular Automata

Cristopher Moore[*]
Santa Fe Institute

Arthur A. Drisko[†]
University of California, Berkeley

Abstract. By grouping $2r$ sites together into one, a cellular automaton (CA) with radius r can be transformed into one with a two-site neighborhood, which can be thought of as a binary algebra. It is shown that if this *block algebra* is in one of four large classes of algebras (commutative, associative with identity, inverse property loop, or anticommutative with identity) then the underlying rule only depends on its leftmost and rightmost inputs, and the block algebra is simply the direct product of $2r$ copies of the underlying algebra. Therefore, although this algebraic approach to CA has been useful to some extent, complex rules on several-site neighborhoods cannot be expected to be equivalent to binary algebras with these simplifying properties.

1. Introduction

A cellular automaton (CA) is a dynamical system on sequences,

$$a_i' = f(a_{i-r}, \ldots, a_i, \ldots, a_{i+r})$$

where each a_i is a symbol in a finite alphabet A, and r is the *radius* of the rule. We can also consider half-integer r, for which

$$a_i' = f(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1/2}, a_{i+1/2}, \ldots, a_{i+r-1}, a_{i+r})$$

on a staggered space-time. For instance, if $r = 1/2$ each site has just two predecessors,

$$a_i' = f(a_{i-1/2}, a_{i+1/2}),$$

[*] Electronic mail address: `moore@santafe.edu`.
[†] Electronic mail address: `drisko@math.berkeley.edu`.

© 1996 Complex Systems Publications, Inc.

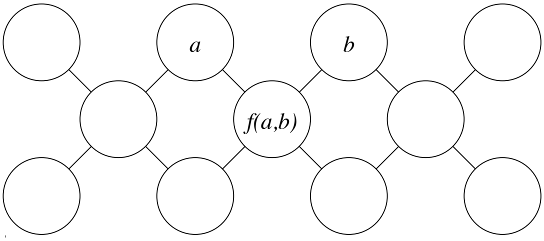

Figure 1: The staggered space-time of an $r = 1/2$ CA.

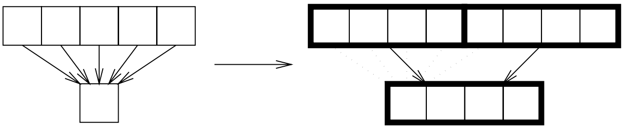

Figure 2: By blocking together $k = 2r$ sites, we can transform any CA into one with $r' = 1/2$. Here $r = 2$ and $k = 4$.

as shown in Figure 1. We can then think of the CA rule as a binary operation or algebra,

$$a = b \bullet c.$$

This can be a fruitful point of view from which to study CAs. Depending on the algebraic properties of $\bullet$, we can make statements about how much parallel or serial computation is needed to predict the CA [4, 5], its reversibility or surjectivity [1, 3], or its periodic behavior [7].

In fact, any CA is equivalent to one with $r = 1/2$ through the following *block transformation.* Treat blocks of k sites as single sites of another CA rule, with a larger alphabet A^k and a smaller radius $r' = r/k$ (if k divides $2r$). Then if $k = 2r$ we get $r' = 1/2$, as shown in Figure 2. We call this blocked rule, seen as a binary operation, the *block algebra* of the original CA.

We would like to know, then, to what extent block transformations can simplify the analysis of CAs. Can nonlinear CA rules on several-site neighborhoods be equivalent to binary algebras with nice algebraic properties, such as those shown in [4, 5] to allow efficient prediction of the CA?

We will show that, under many circumstances, they cannot. More precisely, if the block algebra of a CA is in one of four large classes of algebras (which include groups, monoids, common types of nonassociative algebras, and commutative algebras in general) then the original, unblocked rule must consist of a similar algebra on its leftmost and rightmost inputs, and in fact all other inputs are irrelevant. Thus, the block algebra is simply the direct product of k copies of the original rule; conversely, a CA without this simple structure cannot have a block algebra with any of these simple algebraic properties.

Preliminary versions of these results appeared in [6], where Theorem 1 was proved for a much smaller class of algebras called "special medial."

2. Preliminaries

A *binary operation* or *algebra* $(A, \bullet)$ is a function $f : A \times A \to A$, written $f(a, b) = a \bullet b$ or simply ab. Its *order* is the number of elements in A.

A *left (right) identity* is an element e such that $e \bullet a = a$ $(a \bullet e = a)$. An *identity* is an element which is both a left and a right identity.

A *quasigroup* is a binary operation in which the left and right division properties hold: for any a and b, there exist (possibly different) c and d such that $a \bullet c = b$ and $d \bullet a = b$. Equivalently, the multiplication table is a *Latin square*, where every symbol occurs exactly once in each row and each column, so that multiplication on the left or right by any element is a permutation (one-to-one and onto function) of all the elements. A *loop* is a quasigroup with an identity.

A CA is *left (right) permutive* if it is a one-to-one function on its leftmost (rightmost) input when all other elements are fixed. An $r = 1/2$ CA is left and right permutive if and only if it is a quasigroup.

A *group* is a quasigroup which is associative, namely $a \bullet (b \bullet c) = (a \bullet b) \bullet c$. Then it follows that an identity exists, and every element a has an *inverse* a^{-1} such that $a \bullet a^{-1} = a^{-1} \bullet a = e$. For instance, $\mathbb{Z}_p$, addition on the integers mod p, is the *cyclic group* of order p.

A *semigroup* is an associative algebra which is not necessarily a quasigroup, that is, multiplication is not necessarily one-to-one and onto. For instance, $a \bullet b = \max(a, b)$ is a semigroup. A *monoid* is a semigroup with an identity.

A *subalgebra* is a subset $B \subset A$ which is closed under $\bullet$; that is, if $b_1, b_2 \in B$, then $b_1 \bullet b_2 \in B$ also. Similarly we can speak of subgroups, subquasigroups, subloops, and so on. If S is a subset of A, then $\langle S \rangle$ is the subalgebra generated from the elements of S by all possible products; equivalently, $\langle S \rangle$ is the smallest subalgebra containing S. For instance, if $S = \{x\}$, then $\langle S \rangle = \{x, xx, x(xx), (xx)x, \ldots\}$.

Two elements *commute* if $a \bullet b = b \bullet a$. An algebra is *commutative* if all elements commute. Commutative groups are also called *abelian*.

A map h between two algebras $(A, \bullet)$ and $(B, \circ)$ is a *homomorphism* if $h(a \bullet b) = h(a) \circ h(b)$. A homomorphism which is one-to-one and onto is an *isomorphism*, and A and B are *isomorphic* $(A \cong B)$ if one exists. An isomorphism from a group onto itself is an *automorphism*.

The *direct product* $A \times B$ of two algebras is the set of pairs (a, b) with $a \in A$ and $b \in B$, with multiplication defined componentwise: $(a_1, b_1) \bullet (a_2, b_2) = (a_1 \bullet a_2, b_1 \bullet b_2)$.

For any algebra G, $G^k = \overbrace{G \times G \times \cdots \times G}^{k \text{ times}}$ is the algebra of k-tuples whose components are in G.

In our notation, we refer to blocked states in bold as k-tuples of unblocked states, for example, $\mathbf{s} = (s_1, s_2, \ldots, s_k)$.

3. The theorem

We start with a series of lemmas involving identities of the block algebra. Throughout, we assume that we have blocked together $k = 2r$ sites of the underlying CA, whose rule is f, to produce an $r = 1/2$ blocked CA, whose rule is the block algebra $\mathbf{G}$.

Lemma 1. *If* $\mathbf{G}$ *has a left identity* $\mathbf{e} = (e_1, e_2, \ldots, e_k)$*, then* $f(e_k, \ldots, a) = a$ *regardless of the values of the other sites. Similarly, if* $\mathbf{e}$ *is a right identity, then* $f(a, \ldots, e_1) = a$*.*

Proof. Note that the neighborhood of the underlying rule has $2r + 1 = k + 1$ sites in it, so that the leftmost and rightmost predecessors of $(\mathbf{a} \bullet \mathbf{b})_i$ are a_i and b_i; in other words, $(\mathbf{a} \bullet \mathbf{b})_i = f(a_i, \ldots, a_k, b_1, \ldots, b_i)$. So if $\mathbf{e}$ is a left identity, $f(e_k, a_1, a_2, \ldots, a_k) = (\mathbf{e} \bullet \mathbf{a})_k = a_k$, regardless of the values of $a_1, a_2, \ldots, a_{k-1}$. Similarly, if $\mathbf{e}$ is a right identity, $f(a_1, a_2, \ldots, a_k, e_1) = a_1$ regardless of $a_2, \ldots, a_k$. ■

Lemma 2. *If* $\mathbf{G}$ *has a left identity* $\mathbf{e} = (e_1, e_2, \ldots, e_k)$*, then* $(e_k, e_k, \ldots, e_k)$ *is also a left identity. Similarly, if* $\mathbf{e}$ *is a right identity, then* $(e_1, e_1, \ldots, e_1)$ *is also.*

Proof. This follows immediately from Lemma 1, since (in the left case) $f(e_k, \ldots, e_k, a_1, \ldots, a_i) = a_i$. ■

Corollary. *If* $\mathbf{G}$ *has both a left and a right identity, they are identical and* $\mathbf{e} = (e, e, \ldots, e)$ *consists of* k *sites with the same state* e*.*

Proof. We have shown that $(e, \ldots, e)$ is a left (right) identity where $e = e_k$ $(e = e_1)$. But if left and right identities exist, $e_L = e_L \bullet e_R = e_R$ and they are identical and unique. ■

So we have already shown that $f(a, \ldots, b)$ depends only on a and b if one of them is e. We will go on from here to show that this is true even if neither is, if $\mathbf{G}$ satisfies certain conditions.

Lemma 3 is rather well known, but is included for completeness.

Lemma 3. *The underlying CA is left (right) permutive if and only if the blocked CA is, that is, if* $\mathbf{G}$ *is a quasigroup.*

Proof. We do the proof for left permutivity. Suppose the blocked CA is not left permutive, so that $\mathbf{a} \bullet \mathbf{b} = \mathbf{a}' \bullet \mathbf{b} = \mathbf{c}$ for some $\mathbf{a}$, $\mathbf{a}'$, and $\mathbf{b}$. Let i be the rightmost site at which $a_i \neq a'_i$. Then $c_i = f(a_i, \ldots, a_k, b_1, \ldots, b_i) = f(a'_i, \ldots, a_k, b_1, \ldots, b_i)$ and f is not left permutive.

Conversely, suppose f is not left permutive, so that $f(a_1, a_2, \ldots, a_k, b_1) = f(a'_1, a_2, \ldots, a_k, b_1)$. Then taking $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{a}' = (a'_1, a_2, \ldots, a_k)$, $\mathbf{a} \bullet \mathbf{b} = \mathbf{a}' \bullet \mathbf{b}$ and $\mathbf{G}$ is not left permutive. ■

Corollary. *If* $\mathbf{G}$ *has a left (right) identity and is left (right) permutive (in particular, if* $\mathbf{G}$ *is a loop) then* $\mathbf{e} = (e, e, \ldots, e)$ *is the unique left (right) identity.*

Proof. If $\mathbf{G}$ is left permutive, it can only have one left identity, which by Lemma 2 is of the form $(e, \ldots, e)$. ■

Next, we show that the existence of an identity implies the existence of k isomorphic commuting subalgebras, exactly what would be seen if $\mathbf{G} = G^k$ for some G. Call the *support* of a blocked state $\mathbf{a}$ the set of i such that $a_i \neq e$, then we have Lemma 4.

Lemma 4. *Suppose* $\mathbf{G}$ *has a left (right) identity* $\mathbf{e} = (e, \ldots, e)$*. Then for any subset* s *of* $\{1, 2, \ldots, k\}$*, let* G_s *be the set of blocked states whose support is contained in* s*. Then* G_s *is closed under* $\bullet$*, and so is a subalgebra of* G*.*

Proof. If $a_i = b_i = e$, then $(\mathbf{a} \bullet \mathbf{b})_i = f(e, a_{i+1}, \ldots, a_k, b_1, \ldots, b_{i-1}, e) = e$. Thus the support of $\mathbf{a} \bullet \mathbf{b}$ is contained in the union of the supports of $\mathbf{a}$ and $\mathbf{b}$, and if $\mathbf{a}, \mathbf{b} \in G_s$, then $\mathbf{a} \bullet \mathbf{b} \in G_s$ also. ■

These G_s are isomorphic to each other if we just shift s. If $x \leq k - j$ for all $x \in s$, define $s + j$ as the set $\{j < x \leq k \,|\, x - j \in s\}$. Then we have Lemma 5.

Lemma 5. G_s *and* G_{s+j} *are isomorphic.*

Proof. It is sufficient to show this for $j = 1$; then the rest follows by induction. If $k \notin s$, then $\sigma : G_s \to G_{s+1}$ where $\sigma((a_1, \ldots, a_{k-1}, e)) = (e, a_1, \ldots, a_{k-1})$ is an isomorphism between G_s and G_{s+1}, since the CA map is symmetric with respect to the shift on sequences. ■

So, for instance, if the underlying CA has n states, $\mathbf{G}$ will have k isomorphic subalgebras $G_{\{i\}}$ of order n; a family for each j, $1 \leq j < k$, each containing $k - j$ isomorphic subalgebras $G_{\{i,i+j\}}$ of order n^2; and so on.

Moreover, with a two-sided identity the G_s commute with each other if their s are disjoint.

Lemma 6. *If* G *has a two-sided identity* $\mathbf{e}$*, then* G_s *commutes with* $G_{s'}$ *if* s *and* s' *are disjoint.*

Proof. Suppose $\mathbf{a} \in G_s$ and $\mathbf{b} \in G_{s'}$ where s and s' are disjoint. Then for each i, either $a_i = e$ or $b_i = e$, so $(\mathbf{a} \bullet \mathbf{b})_i$ is either $f(e, \ldots, b_i) = b_i$ or $f(a_i, \ldots, e) = a_i$, which in either case is the same as $(\mathbf{b} \bullet \mathbf{a})_i$. So $\mathbf{a}$ and $\mathbf{b}$ commute. ■

In particular, $\mathbf{G}$ has k commuting, isomorphic subalgebras G_i (i.e., $G_{\{i\}}$) whose only nonidentity component is at the ith site. If we define a binary operation $a \cdot b = f(a, e, \ldots, e, b)$, then $(\mathbf{a} \bullet \mathbf{b})_i = a_i \cdot b_i$ if $\mathbf{a}, \mathbf{b} \in G_i$. This is just one step away from $\mathbf{G} = G_1 \times G_2 \times \cdots \times G_k \cong G_1^k$; we now show several cases in which this follows.

Definition 1. Let G be an algebra and $H \subset G$ a subalgebra. Then define the following three sets related to H:

$$\begin{aligned} Z^\lambda(H) &= \{y \,|\, w(ab) = (wa)b \text{ and } aw = wa \text{ for all } a, b \in H, w \in \langle y \rangle\} \\ Z^\rho(H) &= \{y \,|\, (ab)w = a(bw) \text{ and } aw = wa \text{ for all } a, b \in H, w \in \langle y \rangle\} \\ Z^\mu(H) &= \{y \,|\, a(wb) = (aw)b \text{ and } aw = wa \text{ for all } a, b \in H, w \in \langle y \rangle\}. \end{aligned}$$

In other words, $Z^\lambda(H)$ is the set of elements y such that they, and all their powers w, commute with the elements of H and associate from the left with pairs of elements in H. $Z^\rho(H)$ is similarly defined with association from the right, and $Z^\mu(H)$ with association with w in the middle.

As shorthand for what we wish to prove, we provide Definition 2.

Definition 2. An algebra $\mathbf{G}$ is *cellular* if, whenever it can be written as the block algebra obtained from a CA rule f by blocking k sites together, then f depends only on its leftmost and rightmost inputs, and so $\mathbf{G} = G^k$ where the operation of G is defined as $a \cdot b = f(a, \ldots, b)$.

Then we have Theorem 1.

Theorem 1. *An algebra* $\mathbf{G}$ *with a two-sided identity for which* $Z^\lambda(H) = Z^\rho(H)$ *for all subalgebras* $H \subset \mathbf{G}$ *is cellular.*

Proof. Let $\mathbf{a} = (a_1, e, \ldots, e)$, $\mathbf{b} = (b_1, e, \ldots, e)$, and $\mathbf{y} = (e, y_2, \ldots, y_k)$. Then the reader can easily check that

$$\begin{aligned} \mathbf{y} \bullet (\mathbf{a} \bullet \mathbf{b}) &= (\mathbf{a} \bullet \mathbf{b}) \bullet \mathbf{y} = \mathbf{a} \bullet (\mathbf{b} \bullet \mathbf{y}) = \mathbf{a} \bullet (\mathbf{y} \bullet \mathbf{b}) \\ &= (f(a_1, e, \ldots, e, b_1), y_2, \ldots, y_k). \end{aligned}$$

That is, $\mathbf{y}$ commutes with $\mathbf{a}$ and $\mathbf{b}$ and their product, and associates with them from the right. However,

$$(\mathbf{y} \bullet \mathbf{a}) \bullet \mathbf{b} = (\mathbf{a} \bullet \mathbf{y}) \bullet \mathbf{b} = (f(a_1, y_2, \ldots, y_k, b_1), y_2, \ldots, y_k).$$

So if $\mathbf{y}$ also associates with $\mathbf{a}$ and $\mathbf{b}$ from the left or the middle, $f(a_1, y_2, \ldots, y_k, b_1) = f(a_1, e, \ldots, e, b_1) = a_1 \cdot b_1$ for arbitrary $y_2, \ldots, y_k$; that is, f depends only on its leftmost and rightmost inputs and $\mathbf{G}$ is cellular.

But any elements generated by $\mathbf{a}$ and $\mathbf{b}$ are in G_1, that is, all their components are e except for the first; and any element $\mathbf{w}$ generated by $\mathbf{y}$ is in $G_{\{2,\ldots,k\}}$, that is, its first component is e. So $\mathbf{y}$ is in $Z^\rho(\langle \mathbf{a}, \mathbf{b} \rangle)$, and if $Z^\rho(H) = Z^\lambda(H)$ for any subalgebra H (in which case both are equal to $Z^\mu(H)$) then $\mathbf{y}$ also associates with $\mathbf{a}$ and $\mathbf{b}$ from the left and middle and the theorem is proved. ■

This applies to several large classes of algebras with identity, as we now show.

Corollary 1. *Monoids are cellular.*

Proof. If an algebra is associative, then $Z^\rho(H) = Z^\lambda(H) = Z(H)$ where $Z(H)$, the *centralizer* of H, is the submonoid consisting of all elements that commute with the elements of H. ■

Monoids include groups, of course. A large class of loops containing groups as a subclass is also cellular.

Definition 3. [8] A loop has the *left (right) inverse property* if for every a there is an element a^λ (resp. a^ρ) such that $a^\lambda(ab) = b$ (resp. $(ba)a^\rho = b$) for all b. An *inverse property loop* is one with both the left and right inverse properties; then it follows that $a^\lambda = a^\rho = a^{-1}$ where $aa^{-1} = a^{-1}a = e$ and $(ab)^{-1} = b^{-1}a^{-1}$.

Corollary 2. *Inverse property loops are cellular.*

Proof. Suppose $y \in Z^\rho(H)$. Then y^{-1} is in $Z^\rho(H)$ also, since $\langle y^{-1}\rangle = \langle y\rangle$; and for any $a, b \in H$ their inverses a^{-1}, b^{-1} are in H also. So $(b^{-1}a^{-1})y^{-1} = b^{-1}(a^{-1}y^{-1})$, and taking the inverse of both sides gives $y(ab) = (ya)b$. Thus y also associates with a and b from the left, and $Z^\rho(H) = Z^\lambda(H)$. ■

This includes several large classes of loops, including groups, Moufang loops such as the octonions, totally symmetric loops, and diassociative loops (see [8] for definitions of these).

Definition 4. An algebra is *anticommutative* if no two distinct elements commute, unless there is an identity and one of them is equal to it.

Corollary 3. *Anticommutative algebras with identity are cellular.*

Proof. If a subalgebra H contains two nonidentity elements, then $Z^\rho(H) = Z^\lambda(H) = \{e\}$ since e associates with everything and is the only element that commutes with both of them. If H has only one nonidentity element c (in which case c^2 is c or e) then $Z^\rho(H) = Z^\lambda(H) = \{e, c\}$ since these are the only two elements that commute with c, and they associate with any pair $a, b \in \{e, c\}$. Of course, if H has no nonidentity elements then Z^ρ and Z^λ are the entire algebra G. ■

Theorem 1 fails if either of its conditions is relaxed. For instance, consider the two-state, nearest-neighbor CA rule $f(a_{i-1}, a_i, a_{i+1}) = a_{i-1}+a_i+a_{i+1}$ mod 2, called rule 150 in [9]. Its block algebra **G** is

•	00	01	10	11
00	00	01	11	10
01	11	10	00	01
10	10	11	01	00
11	01	00	10	11

Distinct elements never commute, so $Z^\lambda(H) = Z^\rho(H)$ for any subalgebra H by the argument of Corollary 3 ($\{00\}$ and $\{11\}$ are the only proper subalgebras). But there is no identity, and $\mathbf{G}$ is clearly not cellular since f depends on its middle input.

Conversely, we can construct noncellular block algebras that have identities, but for which $Z^\lambda(H) \neq Z^\rho(H)$ for some H. A nonpermutive example is elementary rule 218 [9], whose rule table is

111	110	101	100	011	010	001	000
1	1	0	1	1	0	1	0

which can also be written

$$f(a_{i-1}, a_i, a_{i+1}) = \begin{cases} (a_{i-1} + a_{i+1}) \bmod 2 & \text{if } a_i = 0 \\ \max(a_{i-1}, a_{i+1}) & \text{if } a_i = 1. \end{cases}$$

Its block algebra $\mathbf{G}$ is

•	00	01	10	11
00	00	01	10	11
01	01	00	11	11
10	10	11	00	01
11	11	10	11	11

with the identity $\mathbf{e} = 00$. If $H = \{00, 01\}$, then $Z^\lambda(H) = \{00, 01, 10\}$ while $Z^\rho(H) = \{00, 01\}$, and again $\mathbf{G}$ is not cellular since f depends on a_i.

This example works in a simple way. For each choice of the middle inputs of a CA, we can define an algebra on the leftmost and rightmost inputs; by Lemma 1, all these algebras must have identity e if the block algebra has an identity $\mathbf{e} = (e, \ldots, e)$, but $\mathbf{G}$ is only cellular if all these algebras are the same. In this case, the value of a_i selects between two different algebras $(a_{i-1} + a_{i+1}) \bmod 2$ and $\max(a, b)$.

To get a permutive example in which $\mathbf{G}$ is a quasigroup, we need four states. This is because there is only one loop of order 3 with a given identity, namely

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \cong \mathbb{Z}_3$$

while for order 4 there are four:

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \cong \mathbb{Z}_2^2, \quad \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{array}, \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{array}, \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \\ 2 & 0 & 3 & 1 \\ 3 & 2 & 1 & 0 \end{array} \cong \mathbb{Z}_4.$$

Then we can construct an $r = 1$, four-state CA where we use a_i to choose which of these four we apply to a_{i-1} and a_{i+1}. Again, we will get a $\mathbf{G}$ with identity $\mathbf{e} = 00$ for which $Z^\lambda(H) \neq Z^\rho(H)$ for some subalgebra H.

Even in the absence of an identity, at least one large class of algebras is cellular.

Theorem 2. *Commutative algebras are cellular.*

Proof. Let $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{b} = (b_1, e, \ldots, e)$. Then $(\mathbf{a} \bullet \mathbf{b})_1 = f(a_1, a_2, \ldots, a_k, b_1)$ and $(\mathbf{b} \bullet \mathbf{a})_1 = f(b_1, e, \ldots, e, a_1)$. If $\mathbf{a}$ and $\mathbf{b}$ commute, these are equal and for arbitrary $a_2, \ldots, a_k$ we have $f(a_1, a_2, \ldots, a_k, b_1) = b_1 \cdot a_1 = a_1 \cdot b_1$. ■

This makes a pleasant pair with Corollary 3 of Theorem 1, that completely noncommutative algebras with identity are also cellular.

4. Conclusion

By blocking sites together to produce a two-site neighborhood, a CA rule can be thought of as a binary algebra. The properties of this block algebra can be related to the dynamical properties of the CAs in various ways [1, 3, 4, 5, 7].

However, we have shown that if this algebra is associative with identity, an inverse property loop, anticommutative with identity, or commutative, then the original CA rule depends only on its leftmost and rightmost inputs, and the block algebra is simply the direct product of $2r$ copies of the underlying one. Therefore, CAs that depend in a nontrivial way on several sites in their neighborhood cannot be expected to have nice algebraic properties under the block transformation.

This includes most of the types of $r = 1/2$ CAs shown in [4, 5] to be efficiently predictable, except for quasigroups separably isotopic to abelian groups (such as $\mathbf{G}$ for rule 150 above).

The four classes of algebra we have shown to be cellular are incomparable to each other. For instance, there are anti-commutative loops of order 5 that lack both the left and right inverse properties; commutative loops of order 6 without the inverse property; monoids that are not loops; and so on. It is tempting to think that a single, larger class containing all of these, obeying a weaker identity, can be shown to be cellular. We also conjecture that loops with the *weak inverse property* [8], in which $(ab)c = 1$ if and only if $a(bc) = 1$, are cellular.

Acknowledgements

A.D. is grateful to Jonathan Farley and Gerhard Paseman for helpful conversations, and to the Santa Fe Institute for a visit at which the conditions of Theorem 1 were improved. C.M. is grateful to Mats Nordahl for helpful discussions, to De Danske Statsbaner (DSB) for a pleasant train ride on which a preliminary version of Theorem 1 was written, and to Elizabeth Hunke and Spootie the Cat for companionship. C.M. still believes that $Z^\lambda(H)$ and $Z^\rho(H)$ should be called the *left and right Spootifiers* of H.

References

[1] T. Boykett, "Combinatorial Construction of One-dimensional Reversible Cellular Automata," *Contributions to General Algebra*, **9** (1995) 81–90.

[2] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications* (Academic Press, New York, 1974).

[3] K. Eloranta, "Partially Permutive Cellular Automata," *Nonlinearity*, **6** (1993) 1009.

[4] C. Moore, "Quasi-linear Cellular Automata," *Physica D*, **103** (1997) 100–132, *Proceedings of the International Workshop on Lattice Dynamics.*

[5] C. Moore, "Predicting Non-linear Cellular Automata Quickly by Decomposing them into Linear Ones," To appear in *Physica D*, *Proceedings of the International Workshop on Lattice Dynamics.*

[6] C. Moore and A. Drisko, "Algebraic Properties of the Block Transformation on Cellular Automata," Santa Fe Institute Working Paper 95-09-080.

[7] J. Pedersen, "Cellular Automata as Algebraic Systems," *Complex Systems*, **6** (1992) 237–250.

[8] H. O. Pflugfelder, *Quasigroups and Loops: An Introduction* (Heldermann Verlag, Berlin, 1990).

[9] S. Wolfram, "Statistical Mechanics of Cellular Automata," *Reviews of Modern Physics*, **55** (1983) 601–644.