Algebraic Properties of the Block Transformation on Cellular Automata

Cristopher Moore

SFI WORKING PAPER: 1995-09-080

SFI Working Papers contain accounts of scientific work of the author(s) and do not necessarily represent the views of the Santa Fe Institute. We accept papers intended for publication in peer-reviewed journals or proceedings volumes, but not papers that have already appeared in print. Except for papers by our external faculty, papers must be based on work done at SFI, inspired by an invited visit to or collaboration at SFI, or funded by an SFI grant.

©NOTICE: This working paper is included by permission of the contributing author(s) as a means to ensure timely distribution of the scholarly and technical work on a non-commercial basis. Copyright and all rights therein are maintained by the author(s). It is understood that all persons copying this information will adhere to the terms and constraints invoked by each author's copyright. These works may be reposted only with the explicit permission of the copyright holder.

www.santafe.edu
Algebraic Properties of the Block Transformation on Cellular Automata

Cristopher Moore
Santa Fe Institute moore@santafe.edu
Arthur A. Drisko
University of California, Berkeley drisko@math.berkeley.edu

October 3, 1995

Abstract
By grouping several sites together into one, a cellular automaton can be transformed into another with more states and a smaller neighborhood; if the neighborhood has just two sites, we can think of the resulting CA rule as a binary operation. We show that if the blocked rule satisfies an identity which holds for a broad class of algebras, then the underlying rule must have essentially the same structure, and must depend only on its leftmost and rightmost inputs; roughly speaking, that the block transformation cannot turn a non-linear rule into a linear one.

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

\[ a'_i = f(a_{i-r}, a_{i-r+1}, \ldots, a_{i-1/2}, a_{i+1/2}, \ldots, a_{i+r-1}, a_{i+r}) \]

For instance, if \( r = 1/2 \) each site has just two predecessors,

\[ a'_i = f(a_{i-1/2}, a_{i+1/2}) \]

on a staggered space-time as shown in figure 1. We can then think of the CA rule as a binary operation,

\[ a = b \bullet c \]
This can be a fruitful point of view from which to study CAs; depending on \( \star \)'s algebraic properties, we can make statements about how much parallel or serial computation is needed to predict the CA \([1, 2]\), its reversibility or surjectivity \([3, 4]\), or its periodic behavior \([5]\).

Now suppose that we group \( k \) sites together into a block; we can look at these blocks as single sites of another CA rule, with a larger alphabet \( A^k \) and a smaller radius \( r/k \) (if \( k \) divides \( 2r \)). In particular, by taking \( k = 2r \) we can transform any CA into one with \( r = 1/2 \), as shown in figure 2. Formally, this block transformation is an isomorphism, since it completely preserves the CA's dynamics.

We would like to know, then, to what extent block transformations can simplify the analysis of CAs. For instance, can a block transformation create a more linear CA, with simpler scaling behavior or a principle of superposition, presumably by removing irrelevant microscopic details and revealing deeper, more macroscopic behavior? In particular, can block transformations move CA rules into classes which were shown in \([1, 2]\) to be easily predictable?

We will show that for a large class of algebraic systems, they cannot. More precisely, if a blocked form of a CA is a algebra in which a certain identity holds, then the original, unblocked rule must consist of a similar algebra on its leftmost and rightmost inputs, and that in fact all other inputs have no effect on the output. Thus, the blocked algebra is simply the direct product of \( k \) copies of the unblocked algebra, and is no simpler than the underlying rule.
2 Preliminaries

A binary operation or algebra \((A, \cdot)\) is a function \(f : A \times A \rightarrow A\), written \(f(a, b) = a \cdot b\).

A left (right) identity is an element \(e\) such that \(e \cdot a = a\) \((a \cdot e = a)\). An identity is an element which is both a left and a right identity. Note that if an algebra has both left and right identities, they are unique and identical, since \(e_L = e_L \cdot e_R = e_R\).

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 \(a \cdot c = b\) and \(d \cdot a = b\). 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 cellular automaton 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.

The left, middle and right nuclei of a quasigroup are the elements \(x\) such that, for all \(a, b\), \(x(ab) = (xa)b\), \((ax)b = a(xb)\) and \((ab)x = a(bx)\) respectively. The nucleus is the intersection of these three.

A group is a quasigroup which is associative, namely \(a \cdot (b \cdot c) = (a \cdot b) \cdot c\), so that all elements are in the nucleus. Then it also follows that an identity exists, and every element \(a\) has an inverse \(a^{-1}\) such that \(a \cdot a^{-1} = a^{-1} \cdot a = e\). For instance, \(Z_p\), 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, i.e., multiplication is not necessarily one-to-one and onto. For instance, \(a \cdot b = \max(a,b)\) is a semigroup.

A subalgebra is a subset \(B \subset A\) which is closed under \(\cdot\); that is, if \(b_1, b_2 \in B\), then \(b_1 \cdot b_2 \in B\) also. Similarly we can speak of subgroups, subquasigroups, subloops, and so on.

Two elements commute if \(a \cdot b = b \cdot a\). An algebra is commutative if all elements commute. Commutative groups are also called Abelian.

A map \(h\) between two algebras \((A, \cdot)\) and \((B, \circ)\) is a homomorphism if \(h(a \cdot b) = h(a) \circ h(b)\). A homomorphism which is one-to-one and onto is an isomorphism, and \(A\) and \(B\) are isomorphic \((A \cong B)\) if one exists.

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: \((a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)\).

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

In our notation, we will refer to blocked states in bold as \(k\)-tuples of unblocked states, e.g. \(s = (s_1, s_2, \ldots, s_k)\).
3 The Theorem

We start with a series of lemmas involving identities of the blocked 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 an algebra $G$.

**Lemma 1.** If $G$ has a left identity $e = (e_1, e_2, \ldots, e_k)$, then $f(e_k, \ldots, a) = a$ regardless of the values of the other sites. Similarly, if $e$ 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 $(a \cdot b)_i$ are $a_i$ and $b_i$; in other words, $(a \cdot b)_i = f(a_i, \ldots, a_k, b_1, \ldots, b_i)$. So if $e$ is a left identity, $f(e_k, a_1, a_2, \ldots, a_k) = (e \cdot a)_k = a_k$, regardless of the values of $a_1, a_2, \ldots, a_k-1$. Similarly, if $e$ 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 $G$ has a left identity $e = (e_1, e_2, \ldots, e_k)$, then $(e_k, e, \ldots, e_k)$ is also a left identity. Similarly, if $e$ is a right identity, then $(e_1, e, \ldots, e_1)$ is also.

**Proof.** This follows immediately from the previous lemma, since (in the left case) $f(e_k, \ldots, e_k, a_1, \ldots, a_i) = a_i$.

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

**Proof.** As stated above, if left and right identities exist, they are identical and unique.

So we have already shown that $f(a, \ldots, b)$ only depends 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 $G$ satisfies certain conditions. The next lemma shows that the block transformation preserves permutivity:

**Lemma 3.** The underlying CA is left (right) permutive if and only if the blocked CA is.

**Proof.** We’ll do the proof for left permutivity. Suppose the blocked CA is not left permutive, so that $a \cdot b = a' \cdot b = c$ for some $a, a'$ and $b$. Let $i$ be the rightmost site at which $a_i \neq a'_i$. Then $c_i = f(a_i, a_{i+1}, \ldots, a_k, b_1, \ldots, b_i) = f(a'_i, a_{i+1}, \ldots, a_k, b_1, \ldots, b_i)$ 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 $a = (a_1, a_2, \ldots, a_k)$ and $a' = (a'_1, a_2, \ldots, a_k)$, $a \cdot b = a' \cdot b$ and $G$ is not left permutive.

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

**Proof.** If $G$ is left permutive, it can only have one left identity; but by Lemma 2 there is an identity whose underlying symbols are all the same.

Next, we show that the existence of an identity implies the existence of $k$ isomorphic commuting subalgebras, exactly what we would see if $G = G^k$ for
some G. Call the support of a blocked state a the set of i such that \(a_i \neq \epsilon\).

Then we have

**Lemma 4.** Suppose G has a left (right) identity \(e = (\epsilon, \epsilon, \ldots, \epsilon)\). 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.** We simply need to note that \(f(\epsilon, a_{i+1}, \ldots, a_i, b_1, \ldots, b_{k-1}, \epsilon) = \epsilon\), so that if \(a_i = b_i = \epsilon\), then \((a \bullet b)_i = \epsilon\) also. Thus the support of \(a \bullet b\) is contained in the union of the supports of a and b, so that if \(a, b \in G_s\), \(a \bullet b \in G_s\) also.

These \(G_s\) are isomorphic to each other if we just shift s:

**Lemma 5.** If \(s' = s + j\) for some \(1 \leq j \leq k\), then \(G_s\) and \(G_{s'}\) are isomorphic.

**Proof.** If \(k \neq s\), then \(\sigma: G_s \rightarrow G_{s'}\) where \(\sigma((a_1, \ldots, a_{k-1}, \epsilon)) = (\epsilon, a_1, \ldots, a_{k-1})\) is an isomorphism between \(G_s\) and \(G_{s'}\), since the CA map is symmetric with respect to the shift on sequences.

So, for instance, if the underlying CA has \(n\) states and G is a loop, G will have \(k\) isomorphic subloops \(G_{s_i}\) of size \(n\); \(k - 1\) families \(F_i\) each containing \(k - j\) isomorphic subloops \(G_{s_i}^{(i)}\) of size \(n^j\); and so on.

Moreover, with a two-sided identity the \(G_s\) commute with each other if their \(s'\)s are disjoint:

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

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

In particular, G has \(k\) commuting, isomorphic subalgebras \(G_{s_i}\) (that is, \(G_{s_i}\)) whose only non-identity component is at the \(i\)th site. If we define a binary operation \(a \cdot b = f(a, \epsilon, \ldots, \epsilon, b)\), then \((a \bullet b)_i = a_i \cdot b_i\) if \(a, b \in G_i\). This is very close to G = \(G_1 \times G_2 \times \cdots \times G_k \cong G_k^1\); we need one more condition on G for this to be true.

An algebra is medial [6] (or entropic in [7]) if \((ab)(cd) = (ac)(bd)\). For instance, quasigroups of the form \(a \bullet b = f(a) + g(b) + h\) where \(\pm\) is an Abelian group and \(f\) and \(g\) are commuting homomorphisms are medial. In [1] the medial identity turns out to be closely related to scaling properties and principles of superposition in CAs. We need a somewhat weaker property, namely

**Definition.** A special medial algebra is one in which the medial identity \((ab)(cd) = (ac)(bd)\) holds whenever \(a\) and \(c\) commute with \(b\) and \(d\).

The following lemma makes the relevance of this definition clear:

**Lemma 7.** If G is a special medial algebra with two commuting subalgebras \(G_1\) and \(G_2\) such that every element in G can be uniquely written as a product \(g_1g_2\) where \(g_1 \in G_1\) and \(g_2 \in G_2\), then \(G \cong G_1 \times G_2\).

**Proof.** Let \(g, g' \in G\). Then \(gg' = (g_1g_2)(g'_1g'_2) = (g_1g'_1)(g_2g'_2)\) since \(g_2\) and \(g'_2\) commute, and the isomorphism \(h : G \rightarrow G_1 \times G_2\) such that \(h(g_1g_2) = (g_1, g_2)\) completes the proof.

Then we finally have
Theorem. If blocking \( k \) sites together of a CA gives a special medial algebra \( \mathcal{G} \) which has a two-sided identity, then the original rule must be of the form \( f(a, \ldots, b) = a \cdot b \) depending only on the leftmost and rightmost sites. Moreover, \( \mathcal{G} = \mathcal{G}^k \) where \( \mathcal{G} = (A, \cdot) \).

Proof. To show that \( f \) only depends on the leftmost and rightmost sites, consider \( a \cdot b \) where \( a = (a_1, a_2, \ldots, a_k) \) and \( b = (b_1, \ldots, e) \). Then \( a = c \cdot d \) where \( c = (a_1, e, \ldots, e) \) and \( d = (e, a_2, \ldots, a_k) \), and \( d \) commutes with \( b \) and \( c \). So \( a \cdot b = (c \cdot d) \cdot (b \cdot e) = (c \cdot b) \cdot (d \cdot e) = (a_1 \cdot b_1, a_2, \ldots, a_k) \), and the first component is \( f(a_1, a_2, \ldots, a_k, b_1) = a_1 \cdot b_1 \) regardless of \( a_2, \ldots, a_k \).

Finally, for any \( b \), \( (a \cdot b)_1 = f(a_1, \ldots, b_1) = a_1 \cdot b_1 \), so \( a \cdot b = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_k \cdot b_k) \) and \( \mathcal{G} = \mathcal{G}^k \).

So what algebras are special medial? An example of a loop which is not is 

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

with identity 1. Although 4 commutes with 2 and 3, \((42)(43) = 65 = 3 \) while \((44)(23) = 11 = 1 \). Alternately, note that \( \{1, 2, 3\} \cong Z_3 \) and \( \{1, 4\} \cong Z_2 \) are two commuting subloops which fulfill the conditions of lemma 7, but this loop is not isomorphic to \( Z_3 \times Z_2 \cong Z_6 \).

However, we have 

Lemma 8. All groups and semigroups are special medial.

Proof. Since they’re associative, \( abc = acbd \) if \( b \) and \( c \) commute. ■

Lemma 9. In a special medial algebra with identity, any element that commutes with all elements is in the nucleus.

Proof. Suppose \( x \) commutes with all elements. Then \( (ax)b = (xa)(eb) = (xe)(ab) = x(ab) \), and similarly with \( x \) on the right; so \( x \) is in the left and right nuclei. Then \( (ax)b = (xa)b = x(ab) = (ab)x = a(bx) = a(xb) \), so it’s in the middle nucleus as well. ■

Corollary. If a special medial algebra with identity is commutative, then it is associative; in particular, if a special medial loop is commutative, it is an Abelian group.

Proof. Since all elements commute, they’re all in the nucleus. ■

However, there are non-commutative, non-associative special medial loops, such as the Octonians \( \{\pm 1, \pm i, \pm j, \pm k, \pm E, \pm I, \pm J, \pm K\} \) with the following multiplication table:
with the understanding that \((-a)b = a(-b) = -(ab)\). The reader can easily confirm that the special medial identity holds, since \(a = \pm b\) if \(a, b \neq 1\) commute.

We also have

**Lemma 10.** If \(G\) is a special medial loop and \(S\) is a set of pairwise commuting elements of \(G\) containing the identity, then the set \(\langle S \rangle\) generated by \(S\) under \(\cdot\) is a commutative semigroup, or an Abelian group if it is finite.

**Proof.** Let \(S^k\) be the set of all products of \(k\) or fewer elements of \(S\), parenthesized in any manner. Elements in \(S^1 = S\) commute; now proceed by induction.

Assume that all elements in \(S^k\) commute. Any \(x, y \in S^{k+1}\) can be written \(x = ab, y = cd\) with \(a, b, c, d \in S^k\); but \(xy = (ab)(cd) = (ac)(bd) = (ca)(db) = (cd)(ab) = yx\). So all elements in \(S^{k+1}\) commute as well, and by induction all elements in \(\langle S \rangle\) commute.

So \(\langle S \rangle\) is commutative and special medial, and by Lemma 9 associative as well; so it’s a commutative semigroup. Multiplication is one-to-one since it’s a subalgebra of a loop; if it’s finite, multiplication must be onto as well, making it a quasigroup and hence an Abelian group. \(\square\)

We also have

**Definition.** An algebra is power associative if any single element \(a\) generates a commutative semigroup \(\langle a \rangle = \{a^n\}\), so that every way of writing \(a^n\) gives the same result (for instance, \(a^2a = a da = d^2\)) and \(a^m a^n = a^{m+n}\).

**Corollary.** Special medial algebras are power associative, and any single element \(a\) of a finite special medial loop generates a cyclic group.

**Proof.** Simply take \(S = \{a\}\) in lemma 10. \(\square\)

Special medial loops share power associativity with Moufang loops, which satisfy the identity \((ab)(ca) = (a(bc))a\), and Bol loops, which satisfy the weaker identity \(((ab)c)b = a((bc)b)\) [7]. However, non-associative commutative Moufang loops (which are also Bol) are not special medial by the corollary to Lemma 9, and the following loop is special medial but not Moufang or Bol:

\[
\begin{array}{cccccccc}
1 & i & j & k & E & I & J & K \\
1 & 1 & i & j & k & E & I & J & K \\
i & i & -1 & k & -j & I & -E & -K & J \\
j & j & -k & -1 & i & J & K & -E & -I \\
k & k & j & -i & -1 & K & -J & I & -E \\
E & E & -I & -J & -K & -1 & i & j & k \\
l & l & E & -K & J & -i & -1 & -k & j \\
J & J & k & E & -I & -j & K & -1 & -i \\
K & K & -J & I & E & -k & -j & i & -1 \\
\end{array}
\]
Lemma 11. Any algebra with identity in which no two distinct non-identity elements commute, and in which \( a^2 = a \) or \( a^2 = e \) for all \( a \), is special medial.

Proof. If no two non-identity elements commute, the requirement that \( a \) and \( c \) each commute with \( b \) and \( d \) leaves just a few cases: either all four are equal, or some are equal and others are the identity, or \( a, c \neq e \) and \( b, d \neq e \) and all distinct while \( b = d = e \) or \( a = c = e \). The only one of these cases in which the special medial identity is not trivial is \( a = b = d \) and \( c = e \) (or \( a = c = d \) and \( b = e \)), in which case it states that \( a^2 a = a a^2 \). The additional requirement that \( a^2 = a \) or \( a^2 = e \) makes this true.

We next show some examples of \( r = 1 \) CAs whose blocked forms have two-sided identities, but which are not special medial; so in fact the underlying rule depends on all its inputs and \( G \neq G^b \). A non-permutive example is elementary rule 218 [8], whose rule table is

\[
\begin{array}{cccccc}
00 & 01 & 010 & 011 & 100 & 101 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1
\end{array}
\]

which can also be written

\[
f(a_{i-1}, a_i, a_{i+1}) = \begin{cases} 
(a_{i-1} + a_{i+1}) \mod 2 & \text{if } a_i = 0 \\
\max(a_{i-1}, a_{i+1}) & \text{if } a_i = 1
\end{cases}
\]

After blocking to \( r = 1/2 \), \( G \) is

\[
\begin{array}{cccc}
00 & 01 & 10 & 11 \\
00 & 00 & 01 & 10 & 11 \\
01 & 01 & 00 & 11 & 11 \\
10 & 10 & 11 & 00 & 01 \\
11 & 11 & 10 & 11 & 11
\end{array}
\]

with \( e = (0, 0) \).

This example works in a simple way. When the middle inputs of a CA are fixed, we can define an algebra on the leftmost and rightmost inputs; by lemma 1, this algebra must have an identity. In this case, the algebra is \((a + b) \mod 2 \) or \(\max(a, b) \), both of which have identity 0, depending on \( a_i \). (If we switch these two so that \( f(1, 0, 1) = 1 \) and \( f(1, 1, 1) = 0 \), we get rule 122 [8].)
To get a permutive example (in which $G$ is a quasigroup) we need four states. This is because there is only one loop of size 3 with a given identity, namely

\[
\begin{array}{ccc}
0 & 1 & 2 \\
1 & 2 & 0 \cong Z_3 \\
2 & 0 & 1 \\
\end{array}
\]

while for $n = 4$ there are four:

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
1 & 2 & 3 & 0 \\
2 & 3 & 0 & 1 \\
3 & 2 & 1 & 0 \\
\end{array} \cong Z_2^2
\]

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
1 & 0 & 3 & 2 \\
2 & 3 & 1 & 0 \\
3 & 2 & 0 & 1 \\
\end{array} \cong Z_4
\]

Then we can construct an $r = 1$, $n = 4$ CA where we use $a_i$ to choose which of these four we apply to $a_{i-1}$ and $a_{i+1}$. Again, we’ll get a $G$ with identity $e = (0, 0)$ which is not special medial.

We end with a result similar to theorem 1 regarding commutativity:

**Theorem 2.** If a blocked algebra $G$ with $k > 1$ is commutative, then the underlying rule must be of the form $f(a, \ldots, b) = a \cdot b$, depending only on the leftmost and rightmost sites, with $\cdot$ commutative; so that $G = G^k$ where $G = (A, \cdot)$.

**Proof.** Suppose $a \cdot b = b \cdot a$. Then their first components are $f(a_1, a_2, \ldots, a_k, b_1) = f(b_1, b_2, \ldots, b_k, a_1)$, so $f = a_1 \cdot b_1$ and $\cdot$ is commutative. Then $G = G^k$ follows as in theorem 1.

Of course, if the underlying rule is reflection symmetric so that $f(a_{i-r}, \ldots, a_{i+r}) = f(a_{i+r}, \ldots, a_{i-r})$, then $r(a \cdot b) = r(b) \cdot r(a)$ where $r((a_1, \ldots, a_k)) = (a_k, \ldots, a_1)$.

### 4 Conclusion

We have shown that if a blocked CA is a group, semigroup, or special medial algebra with identity, then its underlying rule must depend only on its leftmost and rightmost inputs, and that the blocked algebra is simply a power of the underlying one. Therefore, the block transformation cannot create these types of algebraic behavior unless they are already present in the underlying rule.

This includes most of the types of $r = 1/2$ CAs shown in [2] to be efficiently predictable, except for quasigroups separably isotopic to Abelian groups.

**Acknowledgements.** C.M. is grateful to Mats Nordahl for helpful discussions, and to De Danske Statsbaner (DSB) for a pleasant train ride on which Theorem 1 was written.

**References**


9


