Commuting Cellular Automata

Cristopher Moore*

Santa Fe Institute,
1399 Hyde Park Road,
Santa Fe, NM 87501

Timothy Boykett†

Uni Linz,
A-4040 Linz, Austria
and
Time's Up,
Industriezeile 33B A-4020 Linz, Austria

The algebraic conditions under which two one-dimensional cellular automata can commute is studied. It is shown that if either rule is permutive, that is, one-to-one in its leftmost and rightmost inputs, then the other rule can be written in terms of it; if either rule is a group, then the other is linear in it; and if either is permutive and *affine*, that is, linear up to a constant, then the other must also be affine. We also prove some simple results regarding the existence of identities, idempotents (quiescent states), and zeroes (absorbing states).

1. Introduction

When do two cellular automata (CA) commute? This question has been studied under several names, including the "commuting block maps problem" [3, 12] and the "commuting endomorphisms problem" since a CA can also be thought of as an endomorphism on the set of sequences. In [13] the special case of two-state CAs is also studied. In this paper, we extend these results using an algebraic approach to CAs that has been succesful in a number of other areas.

Given a finite alphabet A, consider the set $\Sigma = A^{\mathbb{Z}}$ of biinfinite sequences (a_i) in which $a_i \in A$ for all $i \in \mathbb{Z}$. A CA is a dynamical system on Σ of the form

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

where r is the *radius* of the rule.

*Electronic mail address: moore@santafe.edu.
†Electronic mail address: tim@bruckner.stoch.uni-linz.ac.at.

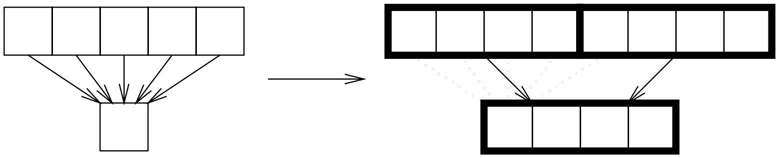

Figure 1. By combining blocks of $2r$ sites, we can transform any CA into one with $r = 1/2$. Here $r = 2$.

Consider a CA with radius 1/2, taking place on a staggered space-time. Then each site has just two predecessors,

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

and we can think of the CA rule as a binary algebra,

$$a = f(b, c) = b \cdot c.$$

In fact, any CA can be rewritten in this form, by lumping blocks of $2r$ sites together as shown in Figure 1. A number of authors [1, 2, 5, 7–10] enjoy looking at CAs in this way, and have studied properties such as reversibility, permutivity, periodicity, and the computational complexity of predicting CA behavior, depending on what algebraic identities $\cdot$ satisfies.

Suppose two CAs, represented by binary algebras $\cdot$ and $\star$, commute as mappings on Σ. Then the two space-time diagrams

$$\begin{array}{ccccc} a & & b & & c \\ & a \cdot b & & b \cdot c & \\ & & (a \cdot b) \star (b \cdot c) & & \end{array} \qquad \begin{array}{ccccc} a & & b & & c \\ & a \star b & & b \star c & \\ & & (a \star b) \cdot (b \star c) & & \end{array}$$

must evaluate to the same state, and we have the identity

$$(a \cdot b) \star (b \cdot c) = (a \star b) \cdot (b \star c). \tag{1}$$

The rest of this paper will consist of looking at the consequences of equation (1) under various assumptions about the two CA rules.

We show that if $\cdot$ is permutive, that is, one-to-one in its left and right inputs (or leftmost and rightmost for CAs with larger radius) then $\star$ is *isotopic* to it, $a \star b = f(a) \cdot g(b)$ for some functions f and g. Moreover, if $\cdot$ is a group, then f and g are homomorphisms so that $\star$ is linear with respect to $\cdot$. Finally, if $\cdot$ is permutive and affine, that is, linear up to a constant, then $\star$ is also affine. We prove a number of lesser results as well.

An extensive study of the special case

$$(a \cdot b) \star (b \cdot c) = (a \star b) \cdot (b \star c) = b$$

where $\cdot$ and $\star$ represent reversible CAs which are each others' inverses, is carried out in [1, 2].

2. Preliminaries

A *binary algebra* $\cdot$ is a function $f : A \times A \to A$, written $f(a, b) = a \cdot b$.

A *left (right) identity* is an element 1 such that $1 \cdot a = a$ (resp. $a \cdot 1 = a$) for all a. A *left (right) zero* is an element z such that $z \cdot a = z$ (resp. $a \cdot z = z$) for all a. An *identity (zero)* is both a left and a right identity (zero).

An element e is *idempotent* if $e \cdot e = e$, and an algebra is idempotent if all its elements are. Dynamically, an idempotent is a *quiescent* state, since rows of it remain constant; it often appears as a downward-pointing triangle in space-time diagrams. A zero is an *absorbing* state, which spreads outward at the speed of light and eats everything in its path.

The *right (left) shift operation* is simply $a \cdot b = a$ (resp. $a \cdot b = b$). It is equivalent to the $r = 1$ CA rule $f(a, b, c) = a$ (resp. $f(a, b, c) = c$) when pairs of sites are combined to produce an $r = 1/2$ CA.

We sometimes write left and right multiplication as functions, $L^{\cdot}_a(b) = a \cdot b$ and $R^{\cdot}_a(b) = b \cdot a$. A CA is *left (right) permutive* if L_a (resp. R_a) is one-to-one for all a. When we combine sites to produce an $r = 1/2$ CA, this corresponds exactly with the usual definition of permutivity for CAs of arbitrary radius, namely that f is one-to-one in its leftmost (rightmost) input when all other inputs are held constant [9].

A *quasigroup* is an algebra which is both left and right permutive. Then for any a and b, there exist (possibly different) elements $a/b = R_b^{-1}(a)$ and $b\backslash a = L_b^{-1}(a)$ such that $(a/b) \cdot b = a$ and $b \cdot (b\backslash a) = a$. A *loop* is a quasigroup with an identity.

A *group* is a quasigroup which is *associative*, so that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Then it follows that an identity exists, and every element a has an *inverse* a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Two elements *commute* if $a \cdot b = b \cdot a$. An algebra is *commutative* if all elements commute. Commutative groups are also called *abelian*. We will use + and 0, instead of $\cdot$ and 1, when discussing an abelian group.

Two quasigroups $\star$ and $\cdot$ are *isotopic* if $a \star b = f(a) \cdot g(b)$ for some functions f and g. We call $\star$ an *isotope* of $\cdot$ in the more general case where f and g are not necessarily one-to-one, in which case $\star$ may not be a quasigroup. Typically there are many pairs of functions f, g that define the same isotope.

A function h on A is a *homomorphism* with respect to $\cdot$ if it is linear, that is, if $h(a \cdot b) = h(a) \cdot h(b)$. Homomorphisms of abelian groups can be represented as matrices. An *automorphism* is a one-to-one homomorphism.

We recommend [4, 11] as introductions to the theory of quasigroups and loops.

3. Identities, idempotents, and zeroes

First, we note that equation (1) is a rather weak constraint, since every CA rule commutes with the shift operation and with itself, as shown in Propositions 1 and 2.

Proposition 1. If $\cdot$ is the right (left) shift $a \cdot b = a$ (resp. $a \cdot b = b$), then equation (1) holds for any algebra $\star$.

Proof. Both sides of equation (1) evaluate to $a \star b$ (resp. $b \star c$). ■

Proposition 2. If $\cdot$ and $\star$ are identical then equation (1) holds.

Proof. Obvious. ■

Thus without further assumptions, equation (1) places very little constraint on the structure of $\cdot$ and $\star$. Nor will associativity or the existence of one-sided identities or zeroes improve matters much, since for the right shift $a \cdot (b \cdot c) = (a \cdot b) \cdot c = a$, and every element is a left zero and a right identity.

We prove a number of trivial results based on the existence of identities, idempotents, or zeroes in Propositions 3 through 8.

Proposition 3. If $\cdot$ has a left identity 1, and if $L_1^\star$ is one-to-one, then $1 \star 1$ is also a left identity of $\cdot$.

Proof. Writing $L_{1^\star}^{-1}(a)$ as $1\backslash a$, we have $(1 \star 1) \cdot a = (1 \star 1) \cdot (1 \star (1\backslash a)) = (1 \cdot 1) \star (1 \cdot (1\backslash a)) = 1 \star (1\backslash a) = a$. ■

Proposition 4. If $\cdot$ and $\star$ have identities $1_\cdot$ and $1_\star$, then they are equal and $\cdot$ and $\star$ are identical.

Proof. First we show that $1_\cdot = 1_\star$:

$$1_\cdot = 1_\cdot \cdot 1_\cdot = (1_\star \star 1_\cdot) \cdot (1_\cdot \star 1_\star) = (1_\star \cdot 1_\cdot) \star (1_\cdot \cdot 1_\star) = 1_\star \star 1_\star = 1_\star .$$

Writing $1_\cdot = 1_\star = 1$, then

$$a \star b = (a \cdot 1) \star (1 \cdot b) = (a \star 1) \cdot (1 \star b) = a \cdot b$$

and the two operations are identical. ■

Proposition 5. If an element e is idempotent with respect to $\cdot$, then $e \star e$ is also. Thus, if e is the only idempotent of $\cdot$, it is also idempotent with respect to $\star$.

Proof. $(e \star e) \cdot (e \star e) = (e \cdot e) \star (e \cdot e) = e \star e$. ■

Corollary 1. If $\cdot$ is a loop, its identity 1 is idempotent with respect to $\star$.

Proof. In a loop, the identity is the only idempotent. ■

Proposition 6. If $\cdot$ and $\star$ are commutative and idempotent, they are identical.

Proof. $a \star b = (a \star b) \cdot (b \star a) = (a \cdot b) \star (b \cdot a) = a \cdot b$. ■

Proposition 7. If $\cdot$ has a left zero z, and if $L_z^\star$ is one-to-one, then $z \star z$ is also a left zero of $\cdot$.

Proof. Writing $L_z^{\star -1}(a)$ as $z\backslash a$, we have $(z \star z) \cdot a = (z \star z) \cdot (z \star (z\backslash a)) = (z \cdot z) \star (z \cdot (z\backslash a)) = z \star z$. ■

Proposition 8. If $\cdot$ has a two-sided zero z, then $L_z^\star$ and $R_z^\star$ cannot be one-to-one unless $z \star z = z$ and $\cdot$ is the constant algebra $a \cdot b = z$ for all a and b.

Proof. $a \cdot b = ((a/z) \star z) \cdot (z \star (z\backslash b)) = ((a/z) \cdot z) \star (z \cdot (z\backslash b)) = z \star z$ for any a and b, but $a \cdot z = z$ so $z \star z = z$. ■

4. Isotopy, linearity, and affinity

In this section we give several classes of commuting CAs that are isotopic.

Proposition 9. If f is a homomorphism on $\cdot$, then the isotope $a \star b = f(a \cdot b) = f(a) \cdot f(b)$ commutes with $\cdot$.

Proof. Both sides of equation (1) become $(f(a) \cdot f(b)) \cdot (f(b) \cdot f(c))$. ■

An algebra is *medial* if $(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$. Then we have Proposition 10.

Proposition 10. If $\cdot$ is medial and f and g are homomorphisms on $\cdot$, then $a \star b = f(a) \cdot g(b)$ commutes with $\cdot$.

Proof. Equation (1) becomes $(f(a) \cdot f(b)) \cdot (g(b) \cdot g(c)) = (f(a) \cdot g(b)) \cdot (f(b) \cdot g(c))$. ■

Conversely, isotopy is implied by equation (1) if $\cdot$ fulfills certain conditions given in Theorem 1.

Theorem 1. If $\star$ and $\cdot$ commute, and if there is an element b such that $L_b^{\cdot}$ and $R_b^{\cdot}$ are one-to-one, then $\star$ is an isotope of $\cdot$.

Proof. Writing $b\backslash a$ and a/b for $L_b^{\cdot -1}(a)$ and $R_b^{\cdot -1}(a)$ respectively, we have

$$a \star c = ((a/b) \cdot b) \star (b \cdot (b\backslash c)) = ((a/b) \star b) \cdot (b \star (b\backslash c)) = f(a) \cdot g(c)$$

where $f = R_b^\star R_b^{\cdot -1}$ and $g = L_b^\star L_b^{\cdot -1}$. ■

Corollary 2. If $\cdot$ is a quasigroup or has an identity, then $\star$ is an isotope of $\cdot$.

Proof. Multiplication by 1, or by any element in a quasigroup, is one-to-one. ■

Furthermore, if b plays the same role in both algebras, then one is permutive if and only if the other is, as stated in Proposition 11.

Proposition 11. If an element b exists such that $L^{\cdot}_b$, $R^{\cdot}_b$, $L^{\star}_b$, and $R^{\star}_b$ are all one-to-one, then $\star$ is an isotope of $\cdot$ with one-to-one functions f and g, and is left (right) permutive, or a quasigroup, if and only if $\cdot$ is.

Proof. If $L^{\star}_b$ and $R^{\star}_b$ are one-to-one, then f and g in Theorem 1 are one-to-one. Then $L^{\star}_a = L^{\cdot}_{f(a)}g$ is one-to-one if and only if $L^{\cdot}_{f(a)}$ is, and similarly on the right. ■

If $\cdot$ is a loop, we can strengthen Theorem 1 further, as stated in Proposition 12.

Proposition 12. If $\cdot$ is a loop, then $\star$ is an isotope of $\cdot$ with functions f and g such that $f(1) = g(1) = 1$ and $f(b)$ and $g(b)$ commute in $\cdot$ for all b.

Proof. If $a \star b = f(a) \cdot g(b)$, then equation (1) becomes

$$f(a \cdot b) \cdot g(b \cdot c) = (f(a) \cdot g(b)) \cdot (f(b) \cdot g(c)). \tag{2}$$

Letting $a = b = c = 1$ gives

$$f(1) \cdot g(1) = (f(1) \cdot g(1)) \cdot (f(1) \cdot g(1)).$$

Since 1 is the only idempotent, $f(1) \cdot g(1) = 1$. Letting $b = 1$ in equation (2) gives

$$a \star c = f(a) \cdot g(c) = (f(a) \cdot g(1)) \cdot (f(1) \cdot g(c)) = f'(a) \cdot g'(c)$$

where $f'(a) = f(a) \cdot g(1)$ and $g'(c) = f(1) \cdot g(c)$.

Since f' and g' also work as a pair of functions to define the isotopy of $\star$, and since $f'(1) = g'(1) = f(1) \cdot g(1) = 1$, we can assume without loss of generality $f(1) = g(1) = 1$. Then letting $a = c = 1$ in equation (2) gives

$$f(b) \cdot g(b) = g(b) \cdot f(b)$$

so $f(b)$ and $g(b)$ commute for all b. ■

Adding associativity makes $\star$ linear, as stated in Theorem 2.

Theorem 2. If $\cdot$ is a group, then $\star$ is an isotope of $\cdot$ where f and g are homomorphisms with respect to $\cdot$.

Proof. If $\cdot$ is associative, equation (2) now reads

$$f(a \cdot b) \cdot g(b \cdot c) = f(a) \cdot g(b) \cdot f(b) \cdot g(c).$$

Letting $c = 1$, commuting $f(b)$ with $g(b)$, and dividing by $g(b)$ on the right gives

$$f(a \cdot b) = f(a) \cdot f(b)$$

and similarly for g. ■

We call this "linearity" not just because f and g are homomorphisms, but because the evolution of the CA of $\star$ obeys a principle of superposition in the case where $\cdot$ is abelian. Call $\star$ *linear with respect to* $+$ (some authors prefer "additive") if space-time diagrams of the CA of $\star$ can be combined with $+$:

$$\begin{array}{ccc} a & & b \\ & a \star b & \end{array} \quad + \quad \begin{array}{ccc} c & & d \\ & c \star d & \end{array} \quad = \quad \begin{array}{ccc} a + c & & b + d \\ & (a+c) \star (b+d) & \end{array}$$

or in other words

$$(a + c) \star (b + d) = (a \star b) + (c \star d). \tag{3}$$

Such principles of superposition are studied in [7]. Equation (3) is a kind of *generalized medial identity* [4]; it is also the *interchange rule* of horizontal and vertical composition of natural transformations in category theory [6], a fact that may or may not have anything to do with CA.

Then we have Theorem 3.

Theorem 3. If $+$ is an abelian group, then $\star$ commutes with $+$ if and only if $\star$ is linear with respect to $+$.

Proof. If $\star$ commutes with $+$, then $a \star b = f(a) + g(b)$ where f and g are homomorphisms on $+$ by Theorem 2, and then both sides of equation (3) evaluate to $f(a) + g(b) + f(c) + g(d)$. Conversely, equation (3) clearly contains equation (1) as a special case when $b = c$. ■

This includes rules such as elementary rule 150 (numbered according to [14]), $f(x, y, z) = x + y + z \bmod 2$; which, when pairs of sites are combined, becomes the linear quasigroup

$$\begin{pmatrix} x \\ y \end{pmatrix} \cdot \begin{pmatrix} w \\ z \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w \\ z \end{pmatrix}.$$

More generally, say that $\cdot$ is *affine* with respect to an abelian group $+$ if it is of the form

$$a \cdot b = f(a) + g(b) + h$$

where f and g are homomorphisms on $+$. The behavior of such rules is easily predictable [7], even if the fs, gs, and hs vary in space-time [8].

Theorem 4. Two affine CAs, $a{\cdot}b = f(a)+g(b)+h$ and $a{\star}b = j(a)+k(b)+l$, commute if and only if the following relations hold:

$$jf = fj, \qquad (jg + kf) = (fk + gj), \qquad \text{and} \qquad kg = gk \tag{4}$$

$$(j + k)(h) + l = (f + g)(l) + h. \tag{5}$$

Proof. Equation (1) becomes

$$\begin{aligned} &jf(a) + (jg + kf)(b) + kg(c) + (j + k)(h) + l = \\ &\qquad fj(a) + (fk + gj)(b) + gk(c) + (f + g)(l) + h \end{aligned}$$

which yields equations (4) and (5) if we variously set a, b, and c to zero. ■

Conversely, if $\cdot$ is permutive, then $\star$ must be of this form, as stated in Theorem 5.

Theorem 5. If $\cdot$ and $\star$ commute, and if $\cdot$ is a quasigroup and affine with respect to an abelian group $+$, then $\star$ is also affine with respect to $+$ and equations (4) and (5) hold.

Proof. By Theorem 1, $\star$ is an isotope of $\cdot$, and therefore also of $+$:

$$a \star b = p(a) \cdot q(b) = fp(a) + gq(b) + h$$

which we can write in the form

$$\begin{aligned} a \star b &= fp(a) - fp(0) + gq(b) - gq(0) + h + (fp + gq)(0) \\ &= j(a) + k(b) + l \end{aligned}$$

where $j(a) = fp(a) - fp(0)$, $k(b) = gq(b) - gq(0)$, and $l = h + (fp + gq)(0)$. Moreover, $j(0) = k(0) = 0$. We will now show that j and k are homomorphisms.

With this form for $\star$, equation (1) becomes

$$\begin{aligned} &j(f(a) + g(b) + h) + k(f(b) + g(c) + h) + l = \\ &\qquad fj(a) + (fk + gj)(b) + gk(c) + (f + g)(l) + h. \end{aligned} \tag{6}$$

Letting $a = b = c = 0$ gives equation (5), which subtracted from equation (6) leaves

$$\begin{aligned} &j(f(a) + g(b) + h) + k(f(b) + g(c) + h) - (j + k)(h) = \\ &\qquad fj(a) + (fk + gj)(b) + gk(c) \end{aligned} \tag{7}$$

Letting a, b, and c in turn be the only nonzero variables gives the relations

$$j(f(a) + h) - j(h) = fj(a) \tag{8}$$

$$j(g(b) + h) + k(f(b) + h) - (j + k)(h) = (fk + gj)(b) \tag{9}$$

$$k(g(c) + h) - k(h) = gk(c). \tag{10}$$

Letting $c = 0$ in equation (7), and subtracting equations (8) and (9), yields

$$j(f(a) + g(b) + h) = j(f(a) + h) + j(g(b) + h) - j(h).$$

Since $\star$ is permutive, f and g are one-to-one, and we can replace $f(a)$ and $g(b) + h$ with arbitrary elements a' and b' respectively, giving:

$$j(a' + b') = j(a' + h) + j(b') - j(h).$$

Letting $b' = 0$ gives

$$j(a' + h) = j(a') + j(h)$$

so

$$j(a' + b') = j(a') + j(b').$$

Thus j is a homomorphism, and similarly for k. Equations (8), (9), and (10) reduce to equation (4), and the theorem is proved. ■

Roughly speaking, we can rephrase this as follows: CAs that are both permutive and linear (up to a constant) cannot commute with nonlinear ones. A similar result is proved for CAs on a two-state alphabet in [3]. However, their methods do not generalize easily to CAs with more than two states, since they use the multiplicative, as well as additive, properties of $\mathbb{Z}_2$.

Further work should include extending these methods to two and higher dimensions. We strongly believe that Theorem 5 holds in all dimensions, where permutive then means one-to-one in inputs on the convex hull of the neighborhood of the CA.

Acknowledgements

This work was supported in part by NSF grant ASC-9503162.

References

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

[2] T. Boykett, *Algebraic Aspects of Reversible Computation,* Ph.D. thesis, Mathematics, University of Western Australia (1996).

[3] E. Coven, G. Hedlund, and F. Rhodes, "The Commuting Block Maps Problem," *Transactions of the American Mathematical Society*, **249** (1979) 113–138.

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

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

[6] S. MacLane, *Categories for the Working Mathematician* (Springer-Verlag, 1971).

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

[8] C. Moore, "Predicting Non-linear Cellular Automata Quickly by Decomposing Them into Linear Ones," *Physica D*, **111** (1998) 27–41.

[9] C. Moore and A. Drisko, "Algebraic Properties of the Block Transformation on Cellular Automata," *Complex Systems*, **10** (1996) 185–194.

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

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

[12] F. Rhodes, "The Sums of Powers Theorem for Commuting Block Maps," *Transactions of the American Mathematical Society*, **271** (1982) 225–236.

[13] B. Voorhees, "Commutation of Cellular Automata Rules," *Complex Systems*, **7** (1993) 309–325.

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