Complex Systems **7** (1993) 309–325

Commutation of Cellular Automata Rules

Burton Voorhees
Faculty of Science, Athabasca University,
Box 10,000, Athabasca, AB T0G 2R0, Canada

Abstract. This paper addresses the following problem: Given a one-dimensional cellular automata (CA) defined over $\mathbf{Z}_2$ with a rule represented by an operator X, determine all one-dimensional rules over $\mathbf{Z}_2$ which commute with X. It is shown that the set of all such rules is given by the solution set of a system of nonlinear Diophantine equations. This result is generalized to cover cellular automata whose rules obey a relation first studied by Ito, and to the case of idempotent rules. Connections are shown between the results presented in this paper and work on the commuting block map problem [2–4], which is known to have significance for the study of Bernoulli shift systems.

1. Introduction

In several previous papers [5, 6] an operator formalism was introduced to study cellular automata (CA) rules defined over $\mathbf{Z}_p$ where p is prime. Using this formalism, results have been obtained on inversion of certain automata rules [7], on entropic properties of automata rules [8], and on the question of determining fixed points and shift cycles [9].

Recently a division algorithm was discovered and the arithmetic of residues for one-dimensional automata rules studied [10]. In this paper attention is restricted to one-dimensional automata defined over $\mathbf{Z}_2$. For this subset of cellular automata we consider the following problem: Let X be the operator representation of a given CA rule. Find the set $\{A \mid AX = XA\}$. Our goal is to provide a means of computing all rules A that commute with the given rule X. It is shown that the set of all such A is determined by the solution set of a system of nonlinear Diophantine equations, which exhibits an elegant structure.

This result is significant for several reasons. It is of intrinsic interest for the insight it provides in the structure of CA rule space [11], allowing us to study properties of maximal commuting subsets of this space; it generalizes to rules sharing a relation of the form first studied by Ito [1]; and, as will be discussed in section 6, it bears a direct relation to the "commuting block map" problem, and hence to commutation properties of endomorphisms of Bernoulli shift systems [2–4].

In section 2 the operator formalism for CAs is reviewed. In section 3 the division algorithm for CA rules is presented. Section 4 contains the commutation theorems that are our main result, together with examples and analysis of several special cases. Section 5 considers the question of idempotence; and also generalizes the work of Ito [1] by providing a means of computing, for any two given operators X and T, a third operator A such that if A exists $TX = (A + X)T$. In section 6 the present results are compared to work that has been done on the commuting block map problem.

2. Operator formalism

Let E represent the automata state space. Then every CA rule can be naturally represented as an operator $Q : E \to E$. Denote this automaton (Q, E). If a one-dimensional rule is such that the value in cell i at time $t + 1$ is determined only on the basis of the values in cells $i = i - 1$, i, and $i + 1$ at time t, then the automaton follows a nearest-neighbor rule. In general, the same symbol will be used to denote both a rule and the associated operator. For nearest-neighbor rules (and other three-site rules) we define a set of eight nonadditive operators on E that correspond to the automata labeled 128, 64, 32, 16, 8, 4, 2, and 1 in Wolfram's notation [12]. Since a site mapping to 1 under one of these operators also maps to 0 under the remaining seven, there is no interference, and every operator that represents a nearest-neighbor rule over $\mathbf{Z}_2$ can be uniquely expressed as a direct sum of these eight operators. That is, these operators provide a basis for the nonlinear algebra of operators defined by the set of nearest-neighbor rules over $\mathbf{Z}_2$. Expression of an operator Q in terms of these basis operators will be called the canonical representation of Q.

To determine the canonical representation of an operator its numeric label is written in powers of 2 and the appropriate basis operators are substituted. Noting that the set of eight neighborhoods $\{000, 001, 010, 011, 100, 101, 110, 111\}$ are listed in ascending numeric order in Wolfram's labeling scheme, we can represent Q by an eight-digit binary number in which each digit is the coefficient of the corresponding basis operator. That is, the abstract numeric label of a given rule as introduced by Wolfram can also be considered a listing of coefficients for a "vector" representation of the operator defined by this rule.

A canonical representation can be added with coefficients reduced mod(2). Rule 28, for example, is given by (00011100), and rule 172 by (10101100). The sum of these two rules is (10110000), which is rule 176.

This formalism generalizes immediately to arbitrary neighborhood sizes. One writes out the neighborhood list in ascending numeric order and directly obtains the operator representation of any given rule in terms of its decomposition over the canonical set of basis operators.

Suppose that a rule with operator representation Q is defined for neighborhoods containing k cells. The generic k-cell neighborhood can be written as $i_1 \ldots i_k$. Q can be extended to an operator Q^+, defined for neighborhoods

		00	01	10	11		
		x_0	x_1	x_2	x_3		
000	001	010	011	100	101	110	111
q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7

Figure 1: Wolfram labels for two- and three-site rules.

containing $k+m$ cells, by mapping each $i_1 \dots i_k$ to the set $\{y_1 \dots y_r i_1 \dots i_k$ $z_1 \dots z_{m-r} \mid y_1 \dots y_r z_1 \dots z_{m-r} = 0 \dots 0, \dots, 1 \dots 1\}$, reordering so that the $k+m$ neighborhood set so generated is arranged in ascending numeric order. The component representation of Q^+ will have a 1 for every neighborhood $y_1 \dots y_r i_1 \dots i_k z_1 \dots z_{m-r}$, in which the representation of Q has a 1 for $i_1 \dots i_k$, and a 0 otherwise.

With this construction, if i_s is the designated site for which $i_1 \dots i_k$ is the neighborhood, then $y_1 \dots y_r i_1 \dots i_k z_1 \dots z_{m-r}$ will be neighborhoods for i_s as well. If it is required to consider $y_1 \dots y_r i_1 \dots i_k z_1 \dots z_{m-r}$ as the neighborhood of a different site, this can be accomplished by multiplying Q^+ by an appropriate shift operator. A k-site rule Q will have 2^k components. Figure 1 shows the component representation for two- and three-site rules. Note that the base 10 form of the neighborhood, considered as a binary number, provides the index for the corresponding component of the rule.

For example, if $k = 2$, the neighborhood list is 00, 01, 10, 11. Suppose that these are considered neighborhoods of the first site. This will be denoted by underlining the designated site: $\underline{0}0, \underline{0}1, \underline{1}0, \underline{1}1$. The rule defined in component form by $Q = (0110)$ extends to a rule Q^+ on the three-site neighborhoods given by $\underline{0}0 \to \underline{0}00, \underline{0}01$; $\underline{0}1 \to \underline{0}10, \underline{0}11$; $\underline{1}0 \to \underline{1}00, \underline{1}01$; $\underline{1}1 \to \underline{1}10, \underline{1}11$. Thus $Q^+ = (00111100)$. Note, however, that although Q^+ is defined on three-site neighborhoods, it is a left-justified rule rather than a nearest-neighbor rule. The nearest-neighbor rule corresponding to Q^+ is σQ^+, where σ is the left shift operator. Since all CA rules commute with shifts this is a technical point only.

Lemma 1. *Let A and B be m-site rules and let X be a k-site rule, $k > m$. Then*

1. $(A+B)^+ = A^+ + B^+$, *where extension is to $m+r$ sites.*
2. $A^+X = (AX)^+$ *and* $XA^+ = (XA)^+$, *where extension of A is to $m+r$ sites and extensions of AX and XA are to $(k+m-1)+r$ sites.*

3. Division of CA rules

If Q and X and given CA rules a simple procedure allows determination of rules A and R such that $Q = AX + R$ [10]. This division algorithm will be illustrated for the simplest case in which Q is a three-site nearest-neighbor rule and X is a two-site rule. The neighborhoods for X will be taken as having the structure $\{s_i s_{i+1}\}$, although it is equally possible to

$$
\begin{array}{lcll}
000 & & x_0x_0 & a_0x_0' + a_3x_0 \\
001 & & x_0x_1 & a_0x_0'x_1' + a_1x_0'x_1 + a_2x_0x_1' + a_3x_0x_1 \\
010 & & x_1x_2 & a_0x_1'x_2' + a_1x_1'x_2 + a_2x_1x_2' + a_3x_1x_2 \\
011 & & x_1x_3 & a_0x_1'x_3' + a_1x_1'x_3 + a_2x_1x_3' + a_3x_1x_3 \\
100 & \xrightarrow{X} & x_2x_0 & \xrightarrow{A} \; a_0x_2'x_0' + a_1x_2'x_0 + a_2x_2x_0' + a_3x_2x_0 \\
101 & & x_2x_1 & a_0x_2'x_1' + a_1x_2'x_1 + a_2x_2x_1' + a_3x_2x_1 \\
110 & & x_3x_2 & a_0x_3'x_2' + a_1x_3'x_2 + a_2x_3x_2' + a_3x_3x_2 \\
111 & & x_3x_3 & a_0x_3' + a_3x_3
\end{array}
$$

Figure 2: Mapping of three-site neighborhoods under AX.

consider $\{s_{i-1}, s_i\}$ neighborhoods and the operator A will, in fact, need to be a rule with this neighborhood structure. (The reason is that a three-site neighborhood $\{s_{i-1}, s_i s_{i+1}\}$ is covered by $\{s_{i-1}, s_i\}$ and $\{s_i, s_{i+1}\}$.)

Applying the operator designated $X = (x_0x_1x_2x_3)$ to the list of three-site neighborhoods shows how these neighborhoods map under X. This is indicated in the first two columns of Figure 2.

We now look for a two-site rule A with neighborhoods $\{s_{i-1}, s_i\}$ such that $Q = AX + R$, where R is a nearest-neighbor rule that is, in some sense, as small as possible. Taking $A = (a_0a_1a_2a_3)$ and setting $x_i' = 1 - x_i$, the third column of Figure 2 indicates the action of AX on the set of three-site neighborhoods. The expressions in this column are the simplest algebraic combinations of the coefficients of A and X that yield the value of AX acting on each of the three-site neighborhoods.

The idea is to choose the a_i so the third column of Figure 2 fits as closely as possible to $Q = (q_0q_1q_2q_3q_4q_5q_6q_7)$. To do this note that the third column in Figure 2 can be written as a matrix product $\mathbf{XA}$, where

$$
\mathbf{A} = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} \qquad \mathbf{X} = \begin{pmatrix}
x_0' & 0 & 0 & x_0 \\
x_0'x_1' & x_0'x_1 & x_0x_1' & x_0x_1 \\
x_1'x_2' & x_1'x_2 & x_1x_2' & x_1x_2 \\
x_1'x_3' & x_1'x_3 & x_1x_3' & x_1x_3 \\
x_2'x_0' & x_2'x_0 & x_2x_0' & x_2x_0 \\
x_2'x_1' & x_2'x_1 & x_2x_1' & x_2x_1 \\
x_3'x_2' & x_3'x_2 & x_3x_2' & x_3x_2 \\
x_3' & 0 & 0 & x_3
\end{pmatrix}
$$

Taking $\mathbf{Q}$ as the column vector with components given by $(q_0q_1q_2q_3q_4$ $q_5q_6q_7)$, consider the equation $\mathbf{XA} = \mathbf{Q}$. By construction each row of $\mathbf{X}$ contains only a single 1. Therefore, if $\mathbf{c}_i$ is the ith column vector of $\mathbf{X}$ and $\mathbf{c}_i^{\mathrm{T}}$ is its transpose, then $\mathbf{c}_i^{\mathrm{T}} * \mathbf{c}_j = n_j\delta_{ij}$, where δ_{ij} is the Kronecker delta and n_j is the number of 1s contained in $\mathbf{c}_j$. Multiplying $\mathbf{XA} = \mathbf{Q}$ on both sides by $\mathbf{X}^{\mathrm{T}}$ yields the set of equations

$$n_ia_i = Q_i \tag{3.1}$$

where $Q_i = \mathbf{c}_i^{\mathrm{T}} \cdot \mathbf{Q}$ is the number of 1s that $\mathbf{c}_i$ and $\mathbf{Q}$ have in common.

The algorithm for the choice of the a_i and the remainder R is as follows:

1. If $Q_i = 0$, set $a_i = 0$.
2. If $n_i = Q_i \neq 0$, set $a_i = 1$.
3. If $n_i \neq Q_i \neq 0$, then
   (a) If $Q_i < n_i/2$, set $a_i = 0$.
   (b) If $Q_i \geq n_i/2$, set $a_i = 1$.
4. Determine the rule R from the labeling by $R = Q + AX \bmod (2)$.

This algorithm minimizes R in the sense that the binary label for R contains the smallest possible number of 1s.

Extension to the case in which Q is defined for k-site neighborhoods and X for m-site neighborhoods is simply a matter of defining the appropriate $\mathbf{X}$ matrix. In this case $\mathbf{X}$ will have 2^k rows and 2^{k-m+1} columns. The rows will be labeled by Q-neighborhoods, listed in ascending numeric order, and columns by A-neighborhoods similarly listed. For $0 \leq i < 2^k$, $0 \leq j < 2^{k-m+1}$, the generic term of $\mathbf{X}$ is

$$\mathbf{X}_{ij} = x^*_{i_0} \cdots x^*_{i_{k-m}} \tag{3.2}$$

Taking the binary expression of the index j as $j_0 \ldots j_{k-m}$, we set $x^*_{i_s} = x_{i_s}$ if j_s is 1 and equal to x'_{i_s} if j_s is 0.

For $0 \leq s \leq k - m$, the i_s's are given by

$$i_s = \left[i/2^{k-s-m}\right] \bmod (2^m) \tag{3.3}$$

where $[z]$ denotes the largest integer less than or equal to z.

4. Commutation of CA rules

Derivation of the commutation equations requires extensive use of both the base 10 and binary forms of rule components and indices. Our general notation will be that a single symbol—for example, i, j, x, a, and so forth—will denote that the term represented is taken in base 10. The binary form will be shown by indication of each digit. For example, if an index is written j, it is understood to be in base 10. But $j = j_0 \ldots j_k$ is in base 2 with j_s indicating the coefficient of 2^{k-s-1}.

Let A and X be two k-site rules with X given. The commutator $AX + XA$ is denoted $[A, X]$. (Note that a plus sign is used here since these rules are defined over $\mathbf{Z}_2$.) The condition $[A, X] = \mathbf{0}$ can be expressed in terms of the matrices $\mathbf{X}$ and $\mathbf{A}$ as defined in the previous section by $\mathbf{X}A = \mathbf{A}X$. This yields a set of 2^{2k-1} equations for components $(a_0 \ldots a_{2^k-1})$ of A. For $i = i_0 i_1 \ldots i_{k-1}$ the ith equation in this set will have the form

$$x'_{i_0} x'_{i_1} \ldots x'_{i_{k-2}} x'_{i_{k-1}} a_0 + x'_{i_0} x'_{i_1} \ldots x'_{i_{k-2}} x_{i_{k-1}} a_1 + \cdots$$
$$+ x_{i_0} x_{i_1} \ldots x_{i_{k-2}} x_{i_{k-1}} a_{2^k-1} = (\text{same, } x \text{ and } a \text{ exchanged})$$

Now consider the coefficient of a_r in the term on the left. This coefficient comes from the rth column of the $\mathbf{X}$ matrix, and the component x_{i_s} in this term will be prime or unprime as r_s (the coefficient of 2^{k-s-1} in the binary form of r) is 0 (primed) or 1 (unprimed).

This observation allows the equation to be written as

$$\sum_{r=0\ldots0}^{1\ldots1} a_r \prod_{s=0}^{k-1}(1 + r_s + x_{i_s}) = \sum_{r=0\ldots0}^{1\ldots1} x_r \prod_{s=0}^{k-1}(1 + r_s + a_{i_s}) \tag{4.1}$$

where the binary form of r is $r_0 r_1 \ldots r_{k-1}$, the sum under the product is taken mod(2), and each i_s is

$$i_s = \left[\frac{i}{2^{k-s-1}}\right] \bmod (2^k) \tag{4.2}$$

We now prove a result that allows Equation (4.1) to be transformed into a more useful form.

Theorem 1.

$$\begin{aligned} &\sum_{r=0\ldots0}^{1\ldots1} a_r \prod_{s=0}^{k-1}(1 + r_x + x_{i_0}) \\ &\quad = \sum_{n=0\ldots0}^{1\ldots1} x_{i_0}^{1-n_0} \cdots x_{i_{k-1}}^{1-n_{k-1}} \sum_{r=0}^{2^k-n-1} \binom{2^k - n - 1}{r} a_r \end{aligned} \tag{4.3}$$

in which n has binary form $n_0 \ldots n_{k-1}$ and $\binom{n}{m}$ indicates the $(m+1)$st entry in the nth row of the mod(2) *Pascal triangle.*

Proof. We prove this result by showing that for all $0 \le r \le 2^k - 1$ the coefficients of a_r are the same on both sides of this equation. For a given value of r define two subsets of $0, \ldots, k-1$ by $R_0 = \{s \mid r_s = 0\}$ and $R_1 = \{s \mid r_s = 1\}$. Then the left side of Equation (4.3) has the form

$$a_r \prod_{s \in R_1} x_{i_s} \prod_{s \in R_0} (1 + x_{i_s})$$

Thus the coefficient of a_r consists of a sum over all products of the x_{i_s}'s containing the product over R_1 as a factor.

On the right, for the same fixed value of r, we have a_r appearing for each n value such that $r \le 2^k - n - 1$. This condition selects n values that satisfy $n \le 2^k - r - 1$. If $n = 0 \ldots 0$ we have a single term $x_{i_0} \ldots x_{i_{k-1}}$, while $n = 2^k - r - 1$ gives the term $\prod_{s \in R_1} x_{i_s}$. This last term follows because the binary expression of $2^k - 1$ consists entirely of 1s so that the binary form of $2^k - r - 1$ has 0s where the binary form of r has 1s, and 1s at all other positions.

Now suppose that $n = 2^k - 1 - (r + b)$ for $0 < b < 2^k - r - 1$. Then we are considering the binary coefficients $\binom{r+b}{r}$, and these satisfy the

condition that they are 0 if the binary forms of r and b have a 1 in the same position, and are 1 otherwise. This is a consequence of a theorem due to Kummer [13], which states that the exponent of 2 in the prime factorization of $\binom{n}{m}^*$ (asterisk denotes coefficients taken mod(10)) is equal to the number of borrows required in the *binary* subtraction $n - m$. Application of this result to $\binom{r+b}{r}^*$ indicates that this exponent is the number of borrows in the binary subtraction of $(r+b)-r$, which is 0 (yielding an odd coefficient, hence equal to 1 mod (2)) if and only if the binary form of $r+b$ has a 1 in each position in which the binary form of r has a 1. Equivalently, the binary forms of r and b do not have a 1 in the same positions. This means that the binary form of $n = 2^k - 1 - (r+b)$ has 0s in all places where r has 1s. Then, as b ranges over its set of possible values, we find 0s in all possible combinations of the remaining digits of n. Thus the coefficient of a_r on the right of Equation (4.2) consists of all possible products of the x_{i_s}'s that contain $\prod_{s\in R_1} x_{i_s}$ as a factor, and that is the same as the coefficient of a_r that appears on the left of Equation (4.3). Since this is true for all r, the claimed result follows. ∎

Application of Equation (4.3) allows Equation (4.1) to be rewritten as

$$\begin{aligned}\sum_{n=0\ldots0}^{1\ldots1} x_{i_0}^{1-n_0}\ldots x_{i_{k-1}}^{1-n_{k-1}} \sum_{r=0}^{2^k-n-1}\binom{2^k-n-1}{r} a_r \\ = \sum_{n=0\ldots0}^{1\ldots1} a_{i_0}^{1-n_0}\ldots a_{i_{k-1}}^{1-n_{k-1}} \sum_{r=0}^{2^k-n-1}\binom{2^k-n-1}{r} x_r\end{aligned} \tag{4.4}$$

From the symmetries of the Pascal triangle [14] we know that

$$\binom{2^k-n-1}{r} = \binom{2k-n-1}{2^k-n-r-1}$$

and with this substitution, and an interchange of summations, the left side of Equation (4.4) may be written as

$$\sum_{n=0}^{2^k-1} a_n \sum_{r=0}^{2^k-n-1}\binom{2^k-n-1}{2^k-n-r-1} x_{i_0}^{1-r_0}\ldots x_{i_{k-1}}^{1-r_{k-1}} \tag{4.5}$$

For fixed n we now consider the coefficient of a_n in this summation. Note that the summation is along the $(n+1)$st diagonal of the mod(2) Pascal triangle, beginning at the (2^k-1)st row. Note also that it is a property of the mod (2) Pascal triangle that this segment of the $(n+1)$st diagonal equals the (2^k-n-1)st row [14], and thus has the same symmetry properties as this row. In particular, it contains an even number of 1s unless $n = 2^k - 1$, in which case it consists of a single 1.

Let $x(i)$ be the base 10 form of the binary number for which the x_{i_s} are components, and suppose that elements of a fixed subset W of $\{x_{i_0},\ldots,x_{i_{k-1}}\}$

are equal to 1 and those not in W are equal to 0. Taking r in the second sum of Equation (4.5) equal to $2^k - n - 1$ yields a product term that contains the fewest number of x_{i_s}'s for a given value of n. All other product terms will contain this minimum term as a factor. Therefore if this term contains any x_{i_s}'s not in W, the entire coefficient of a_n is automatically zero. Thus we need only consider values of n for which all of the x_{i_s}'s contained in the minimum product term are in W. If this minimum term is a product of all members of W then all other terms in the r sum will contain an x_{i_s} not in W and hence will be 0. Therefore the coefficient of a_n for this case will be 1. Because $n = x(i)$, it follows that for this maximal minimum product term $r = 2^k - n - 1$ or $n = 2^k - r - 1$; furthermore, the assumption that this term exhausts W implies that in binary form r has a 1 entry for each x_{i_s} not contained in the minimum product and a 0 entry for each x_{i_s} contained in the minimum product, while the binary form of $2^k - 1$ is all 1s. Thus the binary form of n in this case has a 1 in the sth position if and only if x_{i_s} is contained in W.

Finally, if the minimum product term consists of a product $\prod(U)$ over a proper subset U of W, then the coefficient of a_n has the form

$$\prod(U) = \sum_{t_0 \ldots t_1 = 0 \ldots 0}^{1 \ldots 1} x_{i_{b0}}^{t_0} \ldots x_{i_{bq}}^{t_1}$$

where the x_{i_b}'s are drawn from $W - U$. But this sum is always over an even number of terms, hence is 0 modulo 2. Combination of these results with Equation (4.4) proves the following theorem.

Theorem 2. *Let $X = (x_0 \ldots x_{2^k-1})$ be a given k-site rule over $\mathbf{Z}_2$. The set of all k-site rules $A = (a_0 \ldots a_{2^k-1})$ that commute with X is obtained by solving the set of Diophantine equations*

$$a_{x(i)} = \sum_{n=0 \ldots 0}^{1 \ldots 1} a_{i_0}^{1-n_0} \ldots a_{i_{k-1}}^{1-n_{k-1}} \sum_{r=0}^{2^k-n-1} \binom{2^k - n - 1}{r} x_r \tag{4.6}$$

for $0 \leq i < 2^{2k-1}$ with i_s defined in terms of i as before and $x(i)$ the base 10 form of $x_{i_0} x_{i_1} \ldots x_{i_{k-1}}$.

Note that the symmetry between the left and right sides of Equation (4.4) means that Equation (4.6) can also be written in the form

$$a_{x(i)} = x_{a(i)} \tag{4.7}$$

However this form, although formally elegant, is computationally unhelpful since if A is not given, there is no way to determine the values of $a(i)$.

The result of Theorem 2 easily generalizes to include cases in which X and A are defined over neighborhoods having different numbers of sites. All that is required is to extend the rule defined for fewer sites until the number of sites is equal.

Theorem 3. *Suppose that X is a k-site rule and A is an m-site rule, with $m < k$. Let A^+ be the extension of A to a k-site rule. Then $[A, X] = 0$ if and only if $[A^+, X] = 0$.*

As an example of how commutator sets are computed, consider the two-site rule (0010). The possible values of i are given by 0, 1, 2, 3, 4, 5, 6, and 7, which, from Equation (4.2), give the possible combinations for $x(i)$ as x_0x_0, x_0x_1, x_1x_2, x_1x_3, x_2x_0, x_2x_1, x_3x_2, and x_3x_3. For $X = (0010)$ these yield $x(i)$ values 0, 0, 1, 0, 2, 2, 1, and 0, and substitution into Equation (4.6) produces the set of equations

$$
\begin{aligned}
a_0 &= a_0a_0(x_0 + x_1 + x_2 + x_3) + a_0(x_0 + x_2) + a_0(x_0 + x_1) + x_0 \\
a_0 &= a_0a_1(x_0 + x_1 + x_2 + x_3) + a_0(x_0 + x_2) + a_1(x_0 + x_1) + x_0 \\
a_1 &= a_1a_2(x_0 + x_1 + x_2 + x_3) + a_1(x_0 + x_2) + a_2(x_0 + x_1) + x_0 \\
a_0 &= a_1a_3(x_0 + x_1 + x_2 + x_3) + a_1(x_0 + x_2) + a_3(x_0 + x_1) + x_0 \\
a_2 &= a_2a_0(x_0 + x_1 + x_2 + x_3) + a_2(x_0 + x_2) + a_1(x_0 + x_1) + x_0 \\
a_2 &= a_2a_1(x_0 + x_1 + x_2 + x_3) + a_2(x_0 + x_2) + a_1(x_0 + x_1) + x_0 \\
a_1 &= a_3a_2(x_0 + x_1 + x_2 + x_3) + a_3(x_0 + x_2) + a_2(x_0 + x_1) + x_0 \\
a_0 &= a_3a_3(x_0 + x_1 + x_2 + x_3) + a_3(x_0 + x_2) + a_3(x_0 + x_1) + x_0
\end{aligned}
$$

which, on substitution of the X values, simplify to

$$
\begin{aligned}
a_0 &= 0 \\
a_1a_2 &= 0 \\
a_1(1 + a_3) &= 0 \\
a_1 &= a_3(1 + a_2)
\end{aligned}
$$

It is easy to determine that the solution set of these equations is $\{(0000), (0010), (0101), (0011)\}$. Thus these are the only rules that commute with (0010). By extending to three-site neighborhoods we obtain $(0010)_r^+ = (00001100)$ and $(0010)_l^+ = (00100010)$ where in the first case, as indicated by subscripts, the two-site neighborhoods have been extended on the right and in the second case they have been extended on the left. For both of these extensions Equations (4.6) are the same. It turns out that these equations divide naturally into two sets. The first defines values of some of the a_i, while the second are constraints:

1. $a_0 = 0$
   $a_1 = a_3(1 + a_6) = a_7(1 + a_6)$
   $a_2 = a_6(1 + a_4) = a_6(1 + a_5)$
   $a_4 = a_5(1 + a_3)$
2. $a_1a_2 = a_1a_4 = a_2a_4 = a_2a_5 = 0$
   $a_1(1 + a_3) = 0$
   $a_3(1 + a_7) = 0$

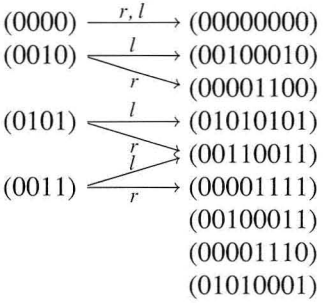

Figure 3: Two- and three-site commutators of (0010).

It is not particularly difficult to compute the solution set for these equations, or to see that all but the last of the equations in the second set are automatically satisfied as a result of the first set.

The full solution set contains right and left extensions of all two-site rules that commute with (0010) as well as three additional members. It must be the case that the full set contains contains both right and left shifts, the identity, and both right and left extensions of (0010). This is indicated in Figure 3 with labeled arrows indicating right and left extensions. Note that $(0101)_r^+ = (0011)_l^+$.

There are several special cases of Equation (4.6) that merit consideration.

Definitions

1. If the components of an operator X satisfy $x_{i+2^{k-r}} = x_i$, then X is said to be 2^{k-r} periodic.

2. If the components of X satisfy $x_{i+2^{k-r}} = 1 + x_i$, then X is said to be 2^{k-r} antiperiodic.

Lemma 2. *If X is 2^{k-r} antiperiodic for $r > 1$, then X is 2^{k-r+1} periodic.*

Theorem 4. *For $-r \leq s \leq k - r - 1$ the shift σ^s is $2^{k-r-s-1}$ antiperiodic.*

Theorem 5. *Let X be 2^{k-m} periodic. Then in Equation (4.6)*

$$n_0 = n_1 = \cdots = n_{m-1} = 1$$

Proof. The x_s's satisfy $x_{s+2^{k-m}} = x_s$ and the sum over s in Equation (4.6) has coefficients drawn from the $(2^k - r - 1)$st row of the mod(2) Pascal triangle. The self-similar structure of this triangle is well known (e.g., see [14]). By the symmetry of this figure, so long as $2^k - r - 1 > 2^{k-m} - 1$, each component x_s of X with a nonzero coefficient in Equation (4.6) will be matched with a set of components $\{x_{s+d2^{k-m}}\}$, also with nonzero coefficients,

where d is even. Therefore the only terms contributing to the right-hand side of (4.6) will be those that have $2^k - r - 1 \leq 2^{k-m} - 1$. But

$$2^k - 2^{k-m} = \sum_{s=k-m}^{k-1} 2^s$$

so that

$$n = \sum_{s=0}^{k-1} n_s 2^{k-s-1} \geq \sum_{s=k-m}^{k-1} 2^s$$

meaning that $n_0 = n_1 = \cdots = n_{m-1} = 1$, at least. ∎

Theorem 6. *If X is 2^{k-1} antiperiodic then Equations (4.6) become*

$$a_{x(i)} = a_{i_0} + \sum_{n=0}^{2^k-1} a_{i_1}^{1-n_1} \ldots a_{i_{k-1}}^{1-n_{k-1}} \binom{2^k - n - 1}{r} x_r \tag{4.8}$$

Proof. The proof is similar to that of Theorem 5. If $r < 2^{k-1}$, every contribution to the sum over x_r in Equation (4.6) will be of the form $x_r + (1 + x_r) = 1$; and, with a single exception, there will be an even number of 1s by the 2^{k-1} antiperiodic condition.

The only exception to this is the term $a_{i_0}(x_0 + x_{2^{k-1}}) = a_{i_0}$. Therefore the sum over the x_r can give no contribution except for a_{i_0} unless $r \geq 2^{k-1}$; but this means that $n_0 = 1$. ∎

5. Ito relations and idempotence

In a very nice paper Ito [1] carried out a study of the three-site rules 18 and 126. He was attracted to this study because the state transition diagrams of these two rules are remarkably similar. In the present formalism this similarity is expressed in terms of the existence of a third rule, rule 252. If X, Y, and T are taken as the operator representations of rules 18, 126, and 252, respectively, then these operators satisfy the equation $TX = YT$ [6]. More generally, rules X and Y will be said to be Ito related via T if there is a T such that this equation holds.

Theorem 7. *For given X and T there exists a Y such that X and Y are Ito related via T if and only if $T \mid [X, T]$, that is, T must divide the commutator of X and T.*

Proof. If there is a Y such that $TX = YT$, then $XT + [X, T] = YT$, hence $[X, T] = (X + Y)T$. On the other hand, if $T \mid [X, T]$, then there is an A such that $[X, T] = AT$. Thus $XT + TX = AT$ or $TX = (X + A)T$, and we take $Y = X + A$. ∎

The equation $[X, T] = AT$ can be written in a form similar to Equation (4.4). Since T and X are given, however, it is easier to use the compact form of Equation (4.7). The same arguments that led to Equation (4.6) then yield the following theorem.

Theorem 8. *Let X and T be given k-site rules. Then there exists an A such that X and $Y = A + X$ are Ito related via T if and only if a solution exists for the set of equations*

$$a_{t(i)} = x_{t(i)} + t_{x(i)} \tag{5.1}$$

As an example, let $X = (01001000)$ (rule 18) and $T = (00111111)$ (rule 252). Then, recalling that the addition in Equation (5.1) is mod(2), we obtain the set of equations

$$\begin{aligned}
a_0 &= x_0 + t_0 = x_0 + t_1 = 0 \\
a_1 &= x_1 + t_2 = 0 \\
a_3 &= x_3 + t_5 = x_3 + t_2 = x_3 + t_4 = 1 \\
a_4 &= x_4 + t_4 = x_4 + t_5 = 0 \\
a_5 &= x_5 + t_6 = 1 \\
a_6 &= x_6 + t_2 = x_6 + t_3 = 1 \\
a_7 &= a_7 + t_0 = x_7 + t_1 = 0
\end{aligned} \tag{5.2}$$

Hence $A = (00a_2 10110)$. If $a_2 = 1$ this gives $X + A = (01111110)$, which is rule 126, the case studied by Ito. If $a_2 = 0$ then $X + A = (01011110)$, indicating that rule 122 is also Ito related to rule 18 via rule 252.

Another question of some interest is whether k-site operators are idempotent. In the formalism of this paper this reduces to determining solutions to the equation $X^2 = X^+$, where the term on the right is appropriately extended. A technicality is involved, however, since it is necessary to specify which site of a neighborhood the rule maps the neighborhood to. This can be illustrated by the following example. For a two-site rule with neighborhoods $\underline{0}0$, $\underline{0}1$, $\underline{1}0$, and $\underline{1}1$ the identity operator is (0011). On the other hand, if the neighborhoods are $0\underline{0}$, $0\underline{1}$, $1\underline{0}$, and $1\underline{1}$ the identity is (0101). In order to consider for these operators the equation $X^2 = X^+$, we first extend them on the right to three-site neighborhoods $(0011)^+ = (00001111)$ and $(0101)^+ = (01010101)$. The first of these is the identity with respect to the neighborhoods $\underline{x}yz$ and the second with respect to the neighborhoods $xy\underline{z}$. The nearest-neighborhood identity is given by $(0011)(0101) = (00110011)$. This indicates that it is important to keep track of the designated site to which neighborhoods map.

Let X be a k-site operator such that $\mu_i(t+1) = X(\mu_{i-r}, \ldots, \mu_{i+k-r-1})$. Then X^2 will be a $(2k-1)$-site operator defined by $\mu_i(t+1) = X^2(\mu_{i-2r}, \ldots, \mu_{i+2(k-r-1)})$. Therefore X^+ must also be a $2k-1$ site operator defined by $\mu_i(t+1) = X^+(\mu_{i-2r}, \ldots, \mu_{i+2(k-r-1)})$. If the neighborhood listing for X^+ is to be maintained in ascending numeric order then the X neighborhoods must be extended as $x_1 \ldots x_r y_1 \ldots y_k z_1 \ldots z_{k-r-1}$, where $y_1 \ldots y_k$ indicates the original X neighborhood. The idempotence condition is then given by the following theorem.

Theorem 9. *Let q, $0 \le q \le 2k-1$ indicate the designated site to which an operator X^2 maps, where X is a k-site operator. Then X is idempotent if and only if*

$$x_{i_q} = \sum_{n=0\ldots0}^{1\ldots1} x_{i_0}^{1-n_0} \ldots x_{i_{k-1}}^{1-n_{k-1}} \sum_{r=0}^{2^k-n-1} \binom{2^k-n-1}{r} x_r \tag{5.3}$$

As an example consider the $k = 2$ case with left-justified neighborhoods $\underline{x}z$ extending to neighborhoods $\underline{x}zy$. Equation (5.3) then becomes

$$\begin{aligned}
x_0 &= x_0 x_3 \\
x_0 &= x_1 + x_0(x_1 + x_2) + x_0 x_1 (x_2 + x_3) \\
x_1 &= x_0(1 + x_1)(1 + x_2) + x_1 x_2 x_3 \\
x_1 &= x_0(1 + x_1)(1 + x_3) + x_1(x_2 + x_3) + x_1 x_2 x_3 \\
0 &= x_0(x_1 + x_2 + x_1 x_2 + x_2 x_3) \\
0 &= x_0(1 + x_1)(1 + x_2) + x_1 + x_1 x_2 x_3 \\
x_3 &= x_0(1 + x_2)(1 + x_3) + x_2(x_1 + x_3) + x_1 x_2 x_3 \\
0 &= x_0(1 + x_3)
\end{aligned} \tag{5.4}$$

After some computation the complete set of two-site idempotent operators with neighborhoods $\underline{x}z$ is determined to be $\{(0000), (0010), (0011), (1011), (1111)\}$. Similarly, the set of two-site idempotent operators with neighborhoods $x\underline{z}$ is $\{(0000), (0100), (0101), (1101), (1111)\}$.

6. The commuting block map problem

A length-n string of numbers taken from $\mathbf{Z}_2$ is called an n-block. If E_n is the set of all n-blocks then an n-block map is a function $f : E_n \to \mathbf{Z}_2$. Block maps are of interest in the study of Bernoulli shift systems as a result of a theorem due to Curtis, Hedlund, and Lyndon [15], which asserts that every endomorphism of such a system is shift equivalent to a block map. In paticular, the problem of finding commuting endomorphisms of Bernoulli systems reduces to the problem of finding commuting block maps. Thus there has been considerable work toward solution of the following question. Let f be a given block map. What is the set $C(f)$ of all block maps that commute with f? This is termed the commuting block map problem [2–4]. Because every k-site CA rule is shift equivalent to a k-block map (indeed, a k-block map is just a left-justified k-site CA) our Equation (4.6) provides a computational means of addressing this problem. That is, given f we find an associated CA rule X_f and solve Equation (4.6).

Block maps have a naturally defined multinomial expression $f(z_1, \ldots, z_k)$. The next theorem relates this expression to the component form of the corresponding CA rule.

Theorem 10. *Let $f(z_1, \ldots, z_k)$ be a k-block map, and let z be the base-10 form of $z_1 \ldots z_k$. The corresponding CA rule X is given by designating the*

site to which neighborhoods map, and setting $x_z = f(z_1, \ldots, z_k)$. *On the other hand, if* $X = (x_0, \ldots, x_{2^k-1})$ *in component form, then it defines the block map* $f(z_1, \ldots, z_k)$ *by*

$$f(z_1 \ldots z_k) = \sum_{r=0\ldots0}^{1\ldots1} z_1^{1-r_0} \ldots z_k^{1-r_{k-1}} \sum_{s=0}^{2^k-r-1} \binom{2^k - r - 1}{s} x_s \tag{6.1}$$

In references [2–4] two subsets of the set of all block maps are defined: those that are linear and those that are linear in the first variable. In addition, reference [2] considers cases in which a block map has the form

$$f(z_1, \ldots, z_k) = z_0 + \prod_{i=1}^{k} (\delta_i - z_i) \qquad \delta_i \in \mathbf{Z}_2 \tag{6.2}$$

while references [3, 4] generalize this to block maps of the form

$$f(z_1, \ldots, z_{mk}) = z_0 + \prod_{i=1}^{k} (\delta_i - z_{mi}) \qquad \delta_i \in \mathbf{Z}_2 \tag{6.3}$$

The following definitions are taken from reference [2].

Definitions

3. A k-block map f is linear if its multinomial expression has the form

$$f(z_1, \ldots, z_k) = a_0 + \sum_{i=1}^{k} a_i z_i. \tag{6.4}$$

   If $a_0 = 0$, f is homogeneous, and if $a_0 = 1$, f is inhomogeneous.

4. A k-block map f is linear in the first variable if there is a g such that $f(z_1, \ldots, z_k) = z_1 + g(z_2, \ldots, z_k)$.

5. A linear k-block map f is even or odd accordingly as an even or odd number of the a_i in Equation (6.4) are equal to 1.

Theorem 11. *(Reference [2]) For* $k \geq 2$, *a* k*-block* f *is linear in the first variable if and only if* $f(0B) \neq f(1B)$ *for all* $(k-1)$*-blocks* B.

Comparison with definition 2 immediately yields the following corollary.

Corollary. A k-block map is linear in the first variable if and only if the associated CA operator X is 2^{k-1} antiperiodic.

Theorem 12. *A* k*-block map is linear if and only if there is a non-negative integer* $s < k$ *such that the associated CA rule has the form*

$$X_f = a_0 1 + \sum_{r=1}^{k} a_r \sigma^{k-s-r}$$

Remark. The number s is introduced to compensate for the location of the designated CA mapping site that appears in the sth position from the left in the k-block. If X_f is left-justified then $s = 0$.

In reference [2] a complete characterization is given for $C(f)$ in the case of linear f. Using the formalism of this paper it is a simple matter to reprove this theorem in terms of linear CA rules (see Theorem 13).

Theorem 13. *Let W, X, Y, and Z be CA rules generated by linear k-block maps. Let W and X be homogeneous, and let Y and Z be inhomogeneous. Then*

1. $[W, X] = 0$,
2. $[X, Y] = 0$ *if and only if X is odd, and*
3. $[Y, Z] = 0$ *if and only if Y and Z are both even or both odd.*

Proof. By Theorem 11 we can write

$$W = \sum w_i \sigma^i \qquad X = \sum x_i \sigma^i$$
$$Y = \mathbf{1} + \sum y_i \sigma^i \qquad Z = \mathbf{1} + \sum z_i \sigma^i$$

Direct computation now shows that $[W, X] = 0$, and that

$$[X, Y] = (1 + \sum x_i)\mathbf{1}$$
$$[Y, Z] = (1 + \sum y_i)\mathbf{1} + (1 + \sum z_i)\mathbf{1}$$

The theorem follows immediately. ∎

Theorem 14. *Let f be a k-block map of the form of Equation (6.2) with $\delta_1 \ldots \delta_k$ fixed, and let X_f be the CA operator associated with f.*

1. *If $z_0 = 0$, the operator X_f is the canonical basis operator that maps the k-site neighborhood $1 \ldots 1 + \delta_1 \ldots \delta_k$ to 1 and all other neighborhoods to 0.*
2. *If $z_0 = 1$, then X_f is 1 plus the basis operator of part (1).*

Proof. If $z_0 = 0$, the product in Equation (6.2) is also 0 unless $x_i + \delta_i = 1$ for all i. Hence the only neighborhood that maps to 1 is that for which $x_i = 1 + \delta_i$.

If $z_0 = 1$, then X_f maps every neighborhood to 1 except those defined by $x_i = 1 + \delta_i$. ∎

There is a similar result for the more general case in which f is an mk-block map as defined in Equation (6.2).

Theorem 15. *Let f be the mk-block map defined by Equation (6.3) with $\delta_1 \ldots \delta_k$ fixed. If $z_0 = 0$ the operator X_f is a sum of $2^{k(m-1)}$ of the canonical basis operators. If $z_0 = 1$, then X_f will be* **1** *plus this sum. In addition, if $z_0 = 0$, then the numerical label for X_f is given by*

$$2^{\phi(\delta)} \prod_{r=0}^{k-1} \sum_{s=0}^{2^m-1} 2^{2^{rm+1}s}$$

where

$$\phi(\delta) = \sum_{i=1}^{k} (1 + \delta_i) 2^{(k-i)m}$$

Proof. If $z_0 = 0$, then X_f will map 2^k of the possible 2^{mk} neighborhoods to 1 and the remainder to 0. Hence X_f will be a sum of 2^{mk-k} basis operators. If $x_0 = 1$, X_f will be **1** plus this sum. Further, the neighborhoods that map to 1 will be of the form

$$x_1 \ldots x_{m-1}(1 + \delta_1)x_{m+1} \ldots x_{2m-1}(1 + \delta_2)x_{2m+1} \ldots x_{km-1}(1 + \delta_k)$$

But the neighborhoods are listed in ascending numerical order so the number of the basis operator corresponding to the numerical label of a neighborhood $z_1 \ldots z_{mk}$ is just 2^z. Thus the number that labels X_f is

$$\sum 2^{n(x_1 \ldots x_{m-1}(1+\delta_1)x_{m+1} \ldots x_{km-1}(1+\delta_k))}$$

where $n(x_1 \ldots x_{m-1}(1+\delta_1)x_{m+1} \ldots x_{km-1}(1+\delta_k))$ is the base-10 value of the argument, and the sum is over

$$0 \ldots 0 \leq x_1 \ldots x_{m-1}x_{m+1} \ldots x_{2m-1}x_{2m+1} \ldots x_{km-1} \leq 1 \ldots 1$$

Evaluation of this sum yields the expression for the numerical label of X_f. ∎

Acknowledgments

The author wishes to thank an anonymous referee whose careful reading of an earlier manuscript resulted in elimination of a number of notational inconsistencies. This work was supported by NSERC operating grant OGP 0024817.

References

[1] H. Ito, *Physica D*, **31** (1988) 318–338.

[2] E. M. Coven, G. A. Hedlund, and F. Rhodes, *Transactions of the American Mathematical Society*, **249**(1) (1979) 113–138.

[3] F. Rhodes, *Transactions of the American Mathematical Society*, **271**(1) (1982) 225–236.

[4] F. Rhodes, Journal of Combinatorial Theory, Series A, **33**(1) (1982) 48–64.

[5] B. Voorhees, *Physica D*, **31** (1988) 135–140.

[6] B. Voorhees, *Physica D*, **45** (1990) 26–35.

[7] B. Voorhees, *Communications in Mathematical Physics*, **117** (1988) 431–439.

[8] B. Voorhees, *International Journal of Theoretical Physics*, **26**(11) (1989) 1387–1396.

[9] B. Voorhees, *Journal of Statistical Physics*, **66**(5/6) (1992) 1397–1414.

[10] B. Voorhees, *Complex Systems*, **4** (1990) 587–597.

[11] W. Li and N. Packard, "The Structure of the Elementary Cellular Automata Rule Space," CCSR reprint, University of Illinois (1989).

[12] S. Wolfram, *Reviews of Modern Physics*, **55** (1983) 601–644.

[13] E. Kummer, *Journal für die Reine und Angewandte Mathematik*, **44** (1852) 93–146.

[14] C. T. Long, *Fibonacci Quarterly*, **19** (1981) 458–463.

[15] G. A. Hedlund, *Mathematical Systems Theory*, **3** (1969) 320–375.