Complex Systems 4 (1990) 587–597

Division Algorithm for Cellular Automata Rules*

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

Abstract. Given two cellular automata rules represented as operators Q and X, together with certain natural restrictions on their neighborhood structures, an algorithm is provided which yields two other rules, A and R, such that $Q = AX + R$. A generalized arithmetic of residues follows from this.

1. Introduction

Formally, a cellular automata consists of a lattice L containing a finite or infinite set of sites $\{s_i\}$; a subset $N = \{N_i\}$ of the power set $P(\{s_i\})$, called the *neighborhood set*, which is isomorphic to $\{s_i\}$; a finite set K of values that can be assigned to the s_i; and an evolution rule Q that yields a value to each s_i at time $t + 1$ on the basis of values at the sites in the neighborhood N_i at time t.

Assignment of a value from K to each site of L yields a state of the automaton and the state space, denoted E, is the set K^L of all possible states. Thus, the evolution rule Q can be represented as an operator $Q : E \to E$.

This paper presents a division algorithm which, for given rules Q and X, determines rules A and R such that $Q = AX + R$.

For simplicity of presentation, L is taken as one dimensional and K is taken as $\{0, 1\}$. It is also assumed that all neighborhoods have a standard form $\{s_{i-r}, \ldots, s_i, \ldots, s_{i+r}\}$; $\{s_{i-r}, \ldots, s_i, \ldots, s_{i+r-1}\}$; or $\{s_{i-r+1}, \ldots, s_i, \ldots, s_{i+r}\}$, the choice being the same for all i. If k is the number of sites in a neighborhood, the neighborhood radius is defined as $r = (k - 1)/2$. Neighborhoods with an even number of sites will be asymmetric, and this fact plays a role in the division algorithm.

*Supported by NSERC operating grant OGP-0024817 and a grant from Athabasca University Research Fund.

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

Figure 1: Labels for $r = 1/2$ and $r = 1$ rules.

000		x_0x_0
001		x_0x_1
010		x_1x_2
011	X	x_1x_3
100	$\rightarrow$	x_2x_0
101		x_2x_1
110		x_3x_2
111		x_3x_3

Figure 2: $r = 1$ Neighborhood mapping under $X = (x_0x_1x_2x_3)$.

2. Division algorithm

The division algorithm will be illustrated for the simplest case in which Q is an $r = 1$ (nearest-neighbor) rule and X is an $r = 1/2$ rule. Conventionally, the neighborhoods for X will be taken as having the structure $\{s_i, s_{i+1}\}$ although it is equally possible to 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 for this is that an $r = 1$ neighborhood, $\{s_{i-1}, s_i, s_{i+1}\}$, is covered by the two $r = 1/2$ neighborhoods $\{s_{i-1}, s_i\}$ and $\{s_i, s_{i+1}\}$, and is not covered by the neighborhoods $\{s_{i-2}, s_{i-1}\}$ and $\{s_{i-1}, s_i\}$.

Using a labeling scheme first introduced by Wolfram [1], every $r = 1/2$ rule is specified by a four-digit binary number, and every $r = 1$ rule by an eight-digit binary number. These are determined as indicated in figure 1.

Here x_i (or q_i) is 1 if the corresponding neighborhood maps to 1 under the rule, and is 0 otherwise. This labeling scheme will be termed *numeric labeling* since the neighborhoods are listed in ascending numerical order.

Applying the operator designated $X = (x_0x_1x_2x_3)$ to the list of $r = 1$ neighborhoods shows how these neighborhoods map under X. This is indicated in figure 2.

We now look for an $r = 1/2$ rule A with neighborhoods $\{s_{i-1}, s_i\}$ such that $Q = AX + R$, where R is an $r = 1$ rule which is, in some sense, as small as possible. Taking $A = (a_0a_1a_2a_3)$ and $x_i' = 1 - x_i$, figure 3 indicates the action of AX on the set of $r = 1$ neighborhoods.

The idea is to choose the a_i so as to fit the third column of figure 3 as closely as possible to the expression $Q = (q_0q_1q_2q_3q_4q_5q_6q_7)$. To do this we

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

Figure 3: Mapping of $r = 1$ neighborhoods under AX.

note that the third column in figure 3 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 $(q_0q_1q_2q_3q_4 q_5q_6q_7)$, we now consider the equation $\mathbf{XA} = \mathbf{Q}$. By construction, each row of X contains only a single 1. Therefore, if $\mathbf{c}_i$ is the ith column vector of $\mathbf{X}$ and $\mathbf{c}_i^T$ is its transpose, then $\mathbf{c}_i^T * \mathbf{c}_j = n_j\delta_{ij}$ where δ_{ij} is the Kronecker symbol and n_j is the number of 1s contained in c_j. Thus, multiplying the matrix equation $\mathbf{XA} = \mathbf{Q}$ on both sides by $\mathbf{X}^T$ yields the set of equations

$$n_iq_i = Q_i \tag{2.1}$$

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

The algorithm for 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 $a_i = 1$.

This algorithm minimizes R in the sense that the label for R contains the fewest possible number of ones.

3. Examples

The nearest-neighbor rule (01011010) (rule 90) has been studied extensively [2]. We will divide this rule by the $r = 1/2$ rules (0110) and (0010). For $X = (0110)$ the X matrix becomes

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{3.1}$$

Now (2.1) yields the set of equations

$$\begin{aligned} 2a_0 &= 0 \\ 2a_1 &= 2 \\ 2a_2 &= 2 \\ 2a_3 &= 0 \end{aligned} \tag{3.2}$$

This indicates that $A = (0110)$ as well. We note, however, that the neighborhoods for X are $\{s_i, s_{i+1}\}$, while for A they are $\{s_{i-1}, s_i\}$. This is an important point since, for example, (0011) is the identity operator for the $\{s_i, s_{i+1}\}$ neighborhoods while (0101) is the identity for the $\{s_{i-1}, s_i\}$ neighborhoods. Thus, the $r = 1$ identity, (00110011), is (0101)(0011) rather than (0011)(0011). (However, if the radii of the X and A rules are whole numbers, there are an odd number of sites and no problem of neighborhood asymmetry arises.) With this caveat we can say that (0110) is the "square root" of rule 90.

In general, the neighborhoods for the operator A will need to be determined from the known neighborhoods of X and Q in such a way that the composition of X and A neighborhoods exactly covers the Q neighborhoods.

If $X = (0010)$ the $\mathbf{X}$ matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{3.3}$$

Now (2.1) yields the set of equations

$$\begin{aligned} 4a_0 &= 2 \\ 2a_1 &= 1 \\ 2a_2 &= 1 \end{aligned} \tag{3.4}$$

The algorithm now determines that $A = (1110)$. However, computation of AX yields (11111111), so there is a remainder $R = 10100101$. This second example illustrates a significant point. In the division algorithm as taken a_i is set to 1 if $Q_i = n_i/2$. We could equally well set a_i to 0 in this case and the remainder computed would contain the same number of 1s. When this situation occurs we will term it a case of *equivocation*. The choice made will be called positive equivocation. If $a_i = 0$ when $Q_i = n_i/2$ this will be said to be negative equivocation. It turns out that this is important in the arithmetic of residue classes, as will be seen in the next section.

4. Residue arithmetic

A natural question to ask is whether there is an arithmetic of residue classes similar to that for integers. There is, but the possibility of equivocation makes it more complicated. Following modular arithmetic, if $Q = AX + R$ we will say that $Q \equiv R \bmod (X)$, read Q is congruent to R modulo X.

Lemma 1. *Congruence modulo X satisfies*

1. $Q \equiv Q \bmod (X)$
2. $Q \equiv R \bmod (X) \Leftrightarrow R \equiv Q \bmod (X)$

Thus congruence modulo X has the reflexive and symmetric properties, but transitivity may not hold. To see this consider $Q \equiv R \bmod (X)$ and $R \equiv S \bmod (X)$. Then there are rules A and B such that $Q = AX + R$ and $R = BX + S$. This allows us to write $Q = AX + BX + S \bmod (X) = (A+B)X + S \bmod (X)$. Formally this looks as if $Q \equiv S \bmod (X)$. Suppose, however, that $Q = (00101110)$ and $X = (0110)$. Then by equation (3.1) and the division algorithm $Q = (0111)(0110) + (01010000)$ so the remainder is (01010000). The remainder R can be written $01010000 = (0110)(0110) + (00001010)$. Thus we can write $Q = [(0111) + (0110)](0110) + (00001010) = (0001)(0110) + (00001010)$. This equation is true, but it does not follow from the division algorithm unless we choose the $a_i = 0$ for $Q_i = n_i/2$. If equivalence classes of equivocation are defined by saying that the equivocation class of a rule Q is the set of all rules congruent to Q under all possible combinations of positive and negative equivocation, then congruence modulo X is transitive across equivocation classes, but not across residue classes alone.

Let $k(X)$ be the number of columns of the $\mathbf{X}$ matrix that do not contain all zeros. Let $e(Q, X)$ be the number of columns that are equivocal for an operator $Q = AX + R$.

Lemma 2. *Let X be given as a rule of radius r. The number of rules of radius $s > r$ that are congruent to 0 modulo X is given by $2^{k(X)}$ with $1 \leq k(X) \leq 2^{2(s-r)+1}$. The set of all Q congruent to 0 mod (X), denoted $\{0_i\}$, is a group with respect to component-wise addition.*

Proof. If Q is congruent to 0 mod (X) then there is an A such that $Q = AX$. That is, the binary label of Q decomposes exactly into a sum of columns of the $\mathbf{X}$ matrix. Since $k(X)$ is the number of nonzero columns of this matrix there are $2^{k(X)}$ possible combinations of columns. The total number of columns in the matrix is $2^{2(s-r)+1}$.

To see that $\{0_i\}$ is a group note that $0_i = A_iX$ and there is no equivocation in these products. Thus $0_i + 0_j = (A_i + A_j)X$ simply corresponds to another combination of columns of the $\mathbf{X}$ matrix, hence is also in $\{0_i\}$. Each element is its own inverse, and the zero element is 0_0, which is rule 0 in Wolfram's labeling scheme. ∎

Lemma 3. *Let X be given. The number of residue classes modulo X in the equivocation class of an operator Q is $2^{e(Q,X)}$. There will be $2^{k(X)-e(Q,X)}$ distinct values of A for this class.*

Proof. If the equivocation of an operator Q when divided by X is $e(Q,X)$, this means there are $e(Q,X)$ columns of the $\mathbf{X}$ matrix that are equivocal. For each of these columns it is possible to choose $a_i = 0$ or $a_i = 1$ without changing the number of 1s in the remainder. On the other hand, each such choice determines a distinct rule A and a distinct remainder. Thus the equivocation class of Q will contain $2^{e(Q,X)}$ different residue classes and the number of distinct rules A will be given by $2^{k(X)-e(Q,X)}$. ∎

Theorem 1. *Let $\{0_i | 0 \leq i < 2^{k(X)}\}$ be the set of rules of given radius that are congruent to 0 modulo X. Let Q be a given rule of the same radius. Then the full equivocation class of Q is the set $eq(Q) = \{S | S = Q + 0_i$ for some $i\}$.*

Proof. $Q = A_QX + R$ and $0_i = A_iX$. Hence $Q + 0_i = (A_Q + A_i)X + R$. Write A_Q as $U_Q + E_Q$ where U_Q is the part of A_Q for which Q is unequivocal and E_Q is that part that is equivocal. Note that the remainder R comes entirely from the E_QX contribution: there will be a 1 in a given position of R either to compensate for an extra 1 in E_QX, or to include a 1 that is contained in Q but not in E_QX. We also note that A_i is completely unequivocal. Thus, if addition of A_i to A_Q changes only U_Q there will be no change in the remainder R. If it causes a change in E_Q, however, this corresponds to a change in equivocation. Since the set of 0_i contains all possible combinations of columns of the $\mathbf{X}$ matrix, they will also exhaust the possible combinations of equivocation that can occur for Q. ∎

As an example of theorem 1 consider the 2-site rule $X = (0010)$. The matrix for this rule is given by equation (3.3). $k(X) = 3$ so the set $\{0_i\}$ has eight members. Listing these together with the corresponding A_i gives

A_i	0_i
(0000)	(00000000)
(0010)	(00001100)
(0100)	(00100010)
(0110)	(00101110)
(1000)	(11010001)
(1010)	(11011101)
(1100)	(11110011)
(1110)	(11111111)

There are 31 additional equivocation classes. These are listed, in terms of their component residue classes and the associated A matrices, in table 1.

In table 1 an X in a given A column indicates that the value of A is a coefficient in the equation $Q = AX + R$. The residue classes in each equivocation class are listed under $Eq(Q)$, together with a label for each class. Thus, for example, class $D_3 = (20, 24)$ indicates that residue classes $R = 20$ and $R = 24$ (in Wolfram's notation) are contained in the same equivocation class. The total number of rules in each equivocation class is eight since there are eight elements in $\{0_i\}$. Thus there are four rules in each of the residue classes 20 and 24.

The most transparent listing of equivocation classes in a group table is given by taking the ordering $(A, C), (E, G), (B, F), (D, H)$. Each of the pairs contained in parentheses contains eight equivocation classes, hence 64 rules. The sets $C = (C_1, C_2, C_3)$, $(A, C) = (A_0, A_1, A_2, A_3, A_4, C_1, C_2, C_3)$, and $(A, C, E, G) = (A_0, A_1, A_2, A_3, A_4, C_1, C_2, C_3, E_1, E_2, E_3, E_4, E_5, G_1, G_2, G_3)$ are subgroups under component-wise binary addition. If (A, C) is taken as the identity element then the sets (A, C), (E, G), (B, F), and (D, H) form a four-element group with group table isomorphic to the group table of $\{00, 01, 10, 11\}$, while the sets (A, C, E, G) and (B, F, D, H) form a two element group with table isomorphic to $\{0, 1\}$.

If rules Q and Q' are in the same equivocation class we will say that $Q \equiv Q' \operatorname{emod}(X)$. This is the relation that is analogous to congruence in the case of integers.

Theorem 2. *If* $Q \equiv R \operatorname{emod}(X)$ *and* $Q' \equiv S \operatorname{emod}(X)$ *then* $Q + Q' \equiv R + S \operatorname{emod}(X)$. *Also, if* $Q \equiv R \operatorname{emod}(X)$ *and* $R \equiv S \operatorname{emod}(X)$ *then* $Q \equiv S \operatorname{emod}(X)$.

5. Generalizations

It should be clear that this division algorithm can be applied for any pair of automata rules Q, X so long as the neighborhood structure of X is such that a table like that of figure 2 can be constructed. For example, if Q is a rule

	$Eq(Q)$	0000	0010	0100	0110	1000	1010	1100	1110
A_0	0	X	X	X	X	X	X	X	X
A_1	1	X	X	X	X	X	X	X	X
A_2	16	X	X	X	X	X	X	X	X
A_3	128	X	X	X	X	X	X	X	X
D_1	(4,8)		X		X		X		X
D_2	(5,9)		X		X		X		X
D_3	(20,24)		X		X		X		X
D_4	(68,72)		X		X		X		X
D_5	(132,136)		X		X		X		X
B_1	(2,32)			X	X			X	X
B_2	(3,33)			X	X			X	X
B_3	(18,48)			X	X			X	X
B_4	(66,96)			X	X			X	X
B_5	(130,160)			X	X			X	X
E_1	(6,10,36,40)				X				X
E_2	(7,11,37,41)				X				X
E_3	(22,26,52,56)				X				X
E_4	(70,74,100,104)				X				X
E_5	(134,138,164,168)				X				X
C_1	(17,192)					X	X	X	X
C_2	(65,144)					X	X	X	X
C_3	(80,129)					X	X	X	X
H_1	(21,25,196,200)						X		X
H_2	(69,73,148,152)						X		X
H_3	(84,88,133,137)						X		X
F_1	(19,49,194,224)							X	X
F_2	(67,97,146,176)							X	X
F_3	(82,112,131,161)							X	X
G_1	(23,27,53,57 198,202,228,232)								X
G_2	(71,75,101,105 150,154,180,184)								X
G_3	(86,90,116,120 135,139,165,169)								X

Table 1: Equivocation classes for three-cite rules divided by (0010).

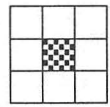
00	01	02	10	11	12	20	21	22
p'_0	0	0	0	p_0	0	0	0	p''_0
$p'_0p'_1$	p'_0p_1	$p'_0p''_1$	$p_0p'_1$	p_0p_1	$p_0p''_1$	$p''_0p'_1$	p''_0p_1	$p''_0p''_1$
$p'_0p'_2$	p'_0p_2	$p'_0p''_2$	$p_0p'_2$	p_0p_2	$p_0p''_2$	$p''_0p'_2$	p''_0p_2	$p''_0p''_2$
$p'_1p'_3$	p'_1p_3	$p'_1p''_3$	$p_1p'_3$	p_1p_3	$p_1p''_3$	$p''_1p'_3$	p''_1p_3	$p''_1p''_3$
$p'_1p'_4$	p'_1p_4	$p'_1p''_4$	$p_1p'_4$	p_1p_4	$p_1p''_4$	$p''_1p'_4$	p''_1p_4	$p''_1p''_4$
$p'_1p'_5$	p'_1p_5	$p'_1p''_5$	$p_1p'_5$	p_1p_5	$p_1p''_5$	$p''_1p'_5$	p''_1p_5	$p''_1p''_5$
$p'_2p'_6$	p'_2p_6	$p'_2p''_6$	$p_2p'_6$	p_2p_6	$p_2p''_6$	$p''_2p'_6$	p''_2p_6	$p''_2p''_6$
$p'_2p'_7$	p'_2p_7	$p'_2p''_7$	$p_2p'_7$	p_2p_7	$p_2p''_7$	$p''_2p'_7$	p''_2p_7	$p''_2p''_7$
$p'_2p'_8$	p'_2p_8	$p'_2p''_8$	$p_2p'_8$	p_2p_8	$p_2p''_8$	$p''_2p'_8$	p''_2p_8	$p''_2p''_8$
$p'_3p'_0$	p'_3p_0	$p'_3p''_0$	$p_3p'_0$	p_3p_0	$p_3p''_0$	$p''_3p'_0$	p''_3p_0	$p''_3p''_0$
$p'_3p'_1$	p'_3p_1	$p'_3p''_1$	$p_3p'_1$	p_3p_1	$p_3p''_1$	$p''_3p'_1$	p''_3p_1	$p''_3p''_1$
$p'_3p'_2$	p'_3p_2	$p'_3p''_2$	$p_3p'_2$	p_3p_2	$p_3p''_2$	$p''_3p'_2$	p''_3p_2	$p''_3p''_2$
$p'_4p'_3$	p'_4p_3	$p'_4p''_3$	$p_4p'_3$	p_4p_3	$p_4p''_3$	$p''_4p'_3$	p''_4p_3	$p''_4p''_3$
p'_4	0	0	0	p_4	0	0	0	p''_4
$p'_4p'_5$	p'_4p_5	$p'_4p''_5$	$p_4p'_5$	p_4p_5	$p_4p''_5$	$p''_4p'_5$	p''_4p_5	$p''_4p''_5$
$p'_5p'_6$	p'_5p_6	$p'_5p''_6$	$p_5p'_6$	p_5p_6	$p_5p''_6$	$p''_5p'_6$	p''_5p_6	$p''_5p''_6$
$p'_5p'_7$	p'_5p_7	$p'_5p''_7$	$p_5p'_7$	p_5p_7	$p_5p''_7$	$p''_5p'_7$	p''_5p_7	$p''_5p''_7$
$p'_5p'_8$	p'_5p_8	$p'_5p''_8$	$p_5p'_8$	p_5p_8	$p_5p''_8$	$p''_5p'_8$	p''_5p_8	$p''_5p''_8$
$p'_6p'_0$	p'_6p_0	$p'_6p''_0$	$p_6p'_0$	p_6p_0	$p_6p''_0$	$p''_6p'_0$	p''_6p_0	$p''_6p''_0$
$p'_6p'_1$	p'_6p_1	$p'_6p''_1$	$p_6p'_1$	p_6p_1	$p_6p''_1$	$p''_6p'_1$	p''_6p_1	$p''_6p''_1$
$p'_6p'_2$	p'_6p_2	$p'_6p''_2$	$p_6p'_2$	p_6p_2	$p_6p''_2$	$p''_6p'_2$	p''_6p_2	$p''_6p''_2$
$p'_7p'_3$	p'_7p_3	$p'_7p''_3$	$p_7p'_3$	p_7p_3	$p_7p''_3$	$p''_7p'_3$	p''_7p_3	$p''_7p''_3$
$p'_7p'_4$	p'_7p_4	$p'_7p''_4$	$p_7p'_4$	p_7p_4	$p_7p''_4$	$p''_7p'_4$	p''_7p_4	$p''_7p''_4$
$p'_7p'_5$	p'_7p_5	$p'_7p''_5$	$p_7p'_5$	p_7p_5	$p_7p''_5$	$p''_7p'_5$	p''_7p_5	$p''_7p''_5$
$p'_8p'_6$	p'_8p_6	$p'_8p''_6$	$p_8p'_6$	p_8p_6	$p_8p''_6$	$p''_8p'_6$	p''_8p_6	$p''_8p''_6$
$p'_8p'_7$	p'_8p_7	$p'_8p''_7$	$p_8p'_7$	p_8p_7	$p_8p''_7$	$p''_8p'_7$	p''_8p_7	$p''_8p''_7$
p'_8	0	0	0	p_8	0	0	0	p''_8

Figure 4: X-matrix for division of three-site rule by two-site rule over Z_3.

of radius r and X is a rule of radius $m < r$ then A will be a rule of radius $r - m$. Even if $m \geq r$ division is possible by first extending Q to a rule of radius $r' > m$. Extension is carried out by mapping neighborhoods of radius r to neighborhoods of radius r' by adjoining neighborhoods of radius $r' - r$, in ascending numerical order, to the right side of the radius-r neighborhoods. The division algorithm can also be extended to more general sets K, and to higher-dimensional lattices.

In figure 4 we show the $\mathbf{X}$ matrix for division of nearest-neighbor one-dimensional rules defined over $\mathbf{Z_3}$. The rule X is now a two-site rule defined by the table

00	01	02	10	11	12	20	21	22
x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8



Q Neighborhood

Possible X and A Neighborhoods

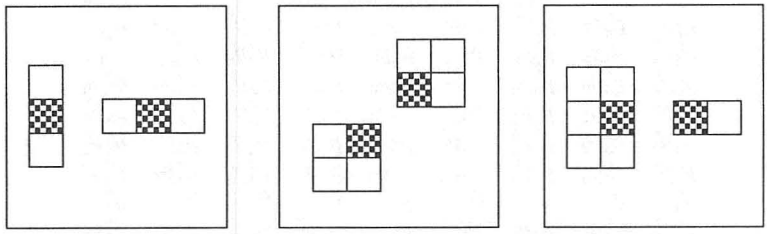


Figure 5: Some two-dimensional neighborhoods compatible with a Moore neighborhood.

The notation used is $p_i' = (1 + x_i)(2 + x_i)/2$; $p_i = x_i(1 + x_i)/2$; and $p_i'' = x_i(2 + x_i)/2$. The $p_i(a)$ are the simplest polynomials in the x_i having the property that $p_i(a)$ is one if $x_i = a$ and zero otherwise.

Figure 5 shows examples of compatible neighborhood structures for two-dimensional lattices.

We will say that a rule Q is prime if it is congruent to 0 only modulo itself and the identity. For cellular automata rules, however, there is a difference from integers: almost all rules are prime.

A rough estimate of the percentage of composite rules can be gained for one-dimensional cellular automata. If a one-dimensional rule has radius r then it can be divided by any rule of radius s such that $1/2 \leq s < r$. There are 2_{r-1} such possible radii, each having 2^{2^s+2} rules. Each rule of radius s will multiply with a rule of radius $r - s$ to give a rule of radius r. Ignoring cases in which rules commute, or in which two different factors yield the same product, there are

$$\sum_{s=1/2}^{r-1/2} 2^{2^{2s+1}+2^{2(r-s)+1}} \tag{5.1}$$

possible combinations. On the other hand for radius r there are a total of $2^{2^{2r+1}}$ rules. Dividing this into the sum of (4.1) gives an upper bound of

$$\sum_{s=1/2}^{r-1/2} 2^{-2^{2r+1}\left[1-2^{-2s}-2^{-2(r-s)}\right]} \tag{5.2}$$

for the fraction of composed rules. The actual number of composite rules will be less than this. For example, for $s = 1/2$, $r = 1$ (4.2) equals 1 but

in fact only 61 of the 256 $r = 1$ rules are composite. Further, as r increases this number decreases dramatically. For example, for $r = 3/2$ it is $1/8$ and for $r = 2$ it is $2^{-11} + 2^{-16}$. Thus it is not surprising that the rule for the well known Game of Life turns out to be prime.

References

[1] S. Wolfram, *Rev. Mod. Phys.*, **55** (1983) 601–644.

[2] O. Martin, A.M. Odlyzko, and S. Wolfram, *Commun. Math. Phys.*, **93** (1984) 219–258.