Transformations of Binary Valued Additive Cellular Automata in One Dimension

Burton Voorhees
Center for Science
Athabasca University

Supported by an NSERC Discovery Grant OGP-OO24817 and by grants from the Athabasca University Research Committee

Acknowledgements

This is part of a joint research project with Valeriy Bulitko, Center for Science, Athabasca University.

V. Bulitko, B. Voorhees, & V. Bulitko (2006) Discrete baker transformation for linear cellular automata analysis. Journal of Cellular Automata 1 41 - 70.

V. Bulitko & B. Voorhees (in preparation) Linear transformations and classes of cellular automata rules with isomorphic state transition diagrams.

V. Bulitko & B. Voorhees (in preparation) Cycle structure of the index baker transformation.

Supported by NSERC Discovery Grant OGP 0024817 and by grants from the Athabasca University Research Committee.

Representation of Additive Rules

Let E_n be the space of all length n binary sequences. An additive rule X: E_n--> E_n with periodic boundary conditions can be represented as a sum of powers of the shift, as a right circulant matrix, and as a polynomial in the n-th root of unity.

$$X = \sum_{i=0}^{n-1} a_i \sigma^i = circ(a_0, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \omega^i$$

The coefficients a_i are called the vector components of X. Note that the vector components are also states in E_n-- the orbit of a state under a rule is also an orbit in rule space.

Representations of Additive Rules

The rule X: $E_n \dashrightarrow E_n$ is also defined by its rule table. For present purposes, the best way of setting up the rule table is to take maximal neighborhoods; i.e., each n-digit binary string defines a neighborhood, so the rule will have 2^n neighborhoods and neighborhood components. These are given in terms of the vector components: Let $i = i_0 \ldots i_{n-1}$ where i is the denary form of the binary string $i_0 \ldots i_{n-1}$ and x_i is the value assigned to the i-th neighborhood by the rule. Then:

$$x_i = \sum_{r=0}^{n-1} i_r a_r$$

The Question

Give a complete characterization of the class of non-singular transformations P such that for any additive rule X defined by $\mathrm{circ}(a_0,\ldots,a_{n-1}) = C(X)$ the matrix $P^{-1}C(X)P$ is also a circulant matrix C(Y) representing an additive rule Y.

If P is a transformation for which this is true, the rules X and Y have isomorphic state transition diagrams.

In the general case, we are considering this question for additive rules with alphabets of cardinality p (prime) defined on d-dimensional tori.

Transformations of Additive Rules

A general, although rather uninformative condition exists for the multidimensional case:

<u>Theorem</u> (Bulitko) A linear non-singular operator P satisfies the condition $P^{-1}C(X)P = C(Y)$ if and only if for any d-tuples $(a_1,\ldots,a_d)$, $(b_1,\ldots,b_d)$

$$\sum_{k_1,\ldots,k_d} \left[P^{-1}\right]^{k_1\ldots k_d}_{i_1\ldots i_d} P^{i_1+b_1,\ldots,i_d+b_d}_{k_1+a_1,\ldots,k_d+a_d} \quad \mathrm{mod}(p)$$

Does not depend on the tuple $(i_1,\ldots,i_d)$

Transformations of Additive Rules

Corollary: For 1-dimensional rules, a linear permutation P satisfies the condition $P^{-1}C(X)P = C(Y)$ if and only if for all a, b

$$\sum_k (-1)^{i+k} M_k^i P_{k+a}^{i+b} \mod(p)$$

is independent of i, where M_i^j is the minor of the element P_i^j.

Transformations of Additive Rules

Consider three transformations that can be carried out on an additive rule:

Shift σ: $X \dashrightarrow \sigma X$ ($a_i \text{ --> } a_{i+1 \bmod(n)}$)

Reflection ρ: $X \dashrightarrow \rho X$ ($a_i \text{ --> } a_{n-i-1}$)

Duality: $X \dashrightarrow \mathbf{1}+X$ ($a_i \text{ --> } 1+a_i \bmod(2)$)

These transformations do not preserve STD isomorphism classes.

Shifts

σX is defined by $a_i \dashrightarrow a_{i+1}$. For $\sigma^k X$, $a_i \dashrightarrow a_{i+k}$.

Theorem (Jen): A state μ is on a cycle of a cylindrical CA rule X if and only if there are integers k and s such that $X^k(\mu) = \sigma^{-s}(\mu)$.

This means that a shift applied to a rule can change cycle periodicities.

$$\left[\sigma^r X\right]^k(\mu) = \sigma^{kr-s}(\mu)$$

Shifts

Example: rule 90 on a cylinder of size 6

Rule	Cycle Equation	Maximum Cycle Periods
$\sigma + \sigma^5$	$(\sigma + \sigma^5)(\mu) = \sigma^{-3}(\mu)$	2
$I + \sigma^2$	$(I+ \sigma^2)(\mu) = \sigma^{-2}(\mu)$	3
$I+ \sigma^4$	$(I+ \sigma^4)(\mu) = \sigma^{--4}(\mu)$	3
$\sigma^2 + \sigma^4$	$(\sigma^2 + \sigma^4)(\mu) = \mu$	Fixed Points
$\sigma + \sigma^3$	$(\sigma + \sigma^3)(\mu) = \sigma^{-1}(\mu)$	6
$\sigma^3 + \sigma^5$	$(\sigma^3 + \sigma^5)(\mu) = \sigma^{-5}(\mu)$	6

Reflection

This is the transformation $(a_0, a_1, ..., a_{n-2}, a_{n-1}) \rightarrow (a_{n-1}, a_{n-2}, ..., a_1, a_0)$

Or, in matrix form with I* the anti-identity:

$$I^* \vec{a} = \overleftarrow{a} \qquad I^* = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ & & & \iddots & & \\ & & \iddots & & & \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Reflection & Shift

Reflection does not commute with the shift: if ρ(X) is the reflection of X then,

$$[\rho,\sigma](\vec{a}) = \rho\sigma(\vec{a}) - \sigma\rho(\vec{a}) = \left(\sigma+\sigma^{-1}\right)\rho(\vec{a}) = \left(\sigma+\sigma^{-1}\right)(\overleftarrow{a})$$

That is, the commutator of the shift and reflection acting on a rule, mod(2) acts as rule 90 acting on the reflection of the rule.

Reflection

Reflection of a rule is not the same as multiplying the circulant matrix representing the rule by the anti-identity (if nothing else, multiplication by I^* gives a left-circulant while the rule is represented by a right circulant).

$$C(X)=\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-3} & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \cdots & a_{n-4} & a_{n-3} \\ & & & \vdots & & \\ a_2 & a_3 & a_4 & \cdots & a_0 & a_1 \\ a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_0 \end{pmatrix} \qquad C(\rho(X))=\begin{pmatrix} a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \\ a_0 & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_3 & a_2 \\ & & & \vdots & & \\ a_{n-3} & a_{n-4} & a_{n-5} & \cdots & a_{n-1} & a_{n-2} \\ a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_0 & a_{n-1} \end{pmatrix}$$

$$I^*C(X)=\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_0 \\ a_2 & a_3 & a_4 & \cdots & a_0 & a_1 \\ a_3 & a_4 & a_5 & \cdots & a_1 & a_2 \\ & & & \vdots & & \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-3} & a_{n-2} \\ a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix} \qquad C(X)I^*=\begin{pmatrix} a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0 \\ a_{n-2} & a_{n-3} & a_{n-4} & \cdots & a_0 & a_{n-1} \\ a_{n-3} & a_{n-4} & a_{n-5} & \cdots & a_{n-1} & a_{n-2} \\ & & & \vdots & & \\ a_1 & a_0 & a_{n-1} & \cdots & a_3 & a_2 \\ a_0 & a_{n-1} & a_{n-2} & \cdots & a_2 & a_1 \end{pmatrix}$$

Duality

$X \to 1+X = \underline{X}$, defined by ($a_i \to 1+a_i \mod(2)$). For a rule represented in the form

$$X = \sum_{i=0}^{n-1} a_i \sigma^i = circ(a_0, \ldots, a_{n-1})$$

Define the parity of the rule as

$$\pi(X) = \sum_{i=0}^{n-1} a_i \mod(2)$$

The parity of a state μ is defined similarly.

$$\pi(\mu) = \sum_{i=0}^{n-1} \mu_i \mod(2)$$

Duality

<u>Lemma</u> Let $\mathsf{E}(n)$ be the set of all length n binary strings and let $\mathsf{E}^{(e)}(n)$ and $\mathsf{E}^{(o)}(n)$ be respectively the subsets of $\mathsf{E}(n)$ having even and odd numbers of ones respectively. For any additive rule X: $\mathsf{E}(n) \text{-->} \mathsf{E}(n)$:

If $\pi(X) = 0$ X maps all of $\mathsf{E}(n)$ to $\mathsf{E}^{(e)}(n)$ in one iteration.

If $\pi(X) = 1$ X maps $\mathsf{E}^{(o)}(n)$ to $\mathsf{E}^{(o)}(n)$ and $\mathsf{E}^{(e)}(n)$ to $\mathsf{E}^{(e)}(n)$.

Duality

<u>Lemma</u>: All rules in an STD equivalence class have the same parity.

<u>Theorem</u>: (1) If n is even then:

$$\pi\left(X\right)=0 \Rightarrow \underline{X}^k(\mu)=X^k(\mu)\ \forall\mu,k>1$$

$$\pi\left(X\right)=1 \Rightarrow \begin{cases} \underline{X}^k(\mu)=X^k(\mu) & k\ even \\ \underline{X}^k(\mu)=\pi(\mu)\mathbf{1}+X^k(\mu) & k\ odd \end{cases}$$

(2) If n is odd then for all k

$$\pi(\mu)=0 \Rightarrow \underline{X}^k(\mu)=X^k(\mu)$$

$$\pi(\mu)=1 \Rightarrow \underline{X}^k(\mu)=\mathbf{1}+X^k(\mu)$$

Duality

If n is even and $\pi(X) = 0$ then $\pi(\underline{X}) = 0$ and all states on cycles of both X and $\underline{X}$ have even parity ($\pi(\mu)=0$). Thus, the cycles of X and $\underline{X}$ are identical, but the tree structure differs.

Duality

If n is even and $\pi(X) = 1$ then $\pi(\underline{X}) = 1$.

1. If $\pi(\mu) = 0$ then $\underline{X}(\mu) = X(\mu)$.
2. If $\pi(\mu) = 1$ then basins of X and $\underline{X}$ appear in pairs related by duality, and the $\underline{X}$ states inter-twine with the X states:

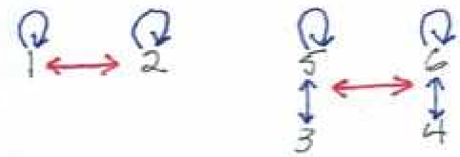
μà $X(\mu)$à $X^2(\mu)$à $X^3(\mu)$à $X^4(\mu)$à …

$1+\mu$à $1+X(\mu)$à $1+X^2(\mu)$à $1+X^3(\mu)$à $1+X^4(\mu)$à …

STD Isomorphism Classes

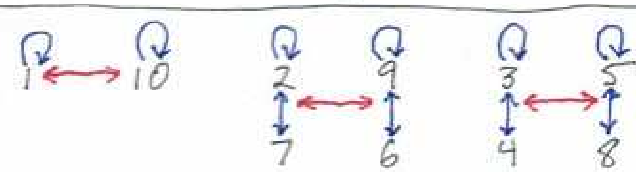
Bulitko has developed a program to compute all additive rules with isomorphic state transition diagrams for any cylinder size. These have been computed up to n = 12. The relations between classes generated by reflection and duality transformations shows some interesting structure.

$n = 3$



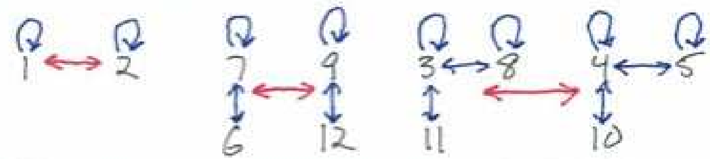
1 2
5 6
3 4

$n = 5$



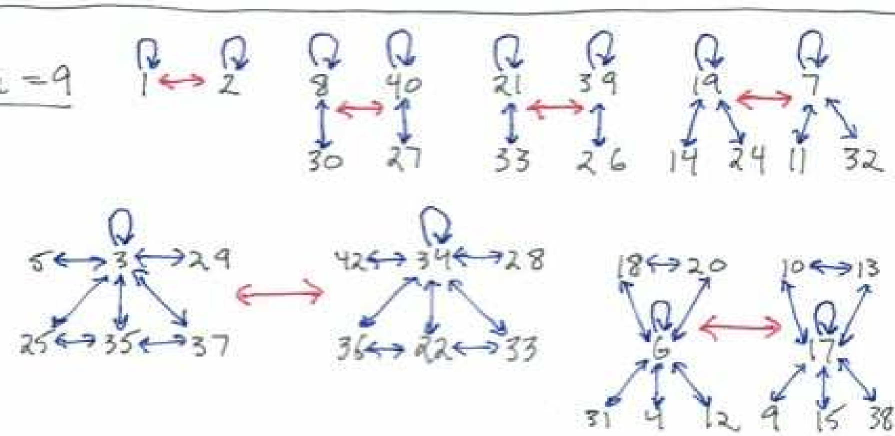
1 10
2 9
7 6
3 5
4 8

$n = 7$

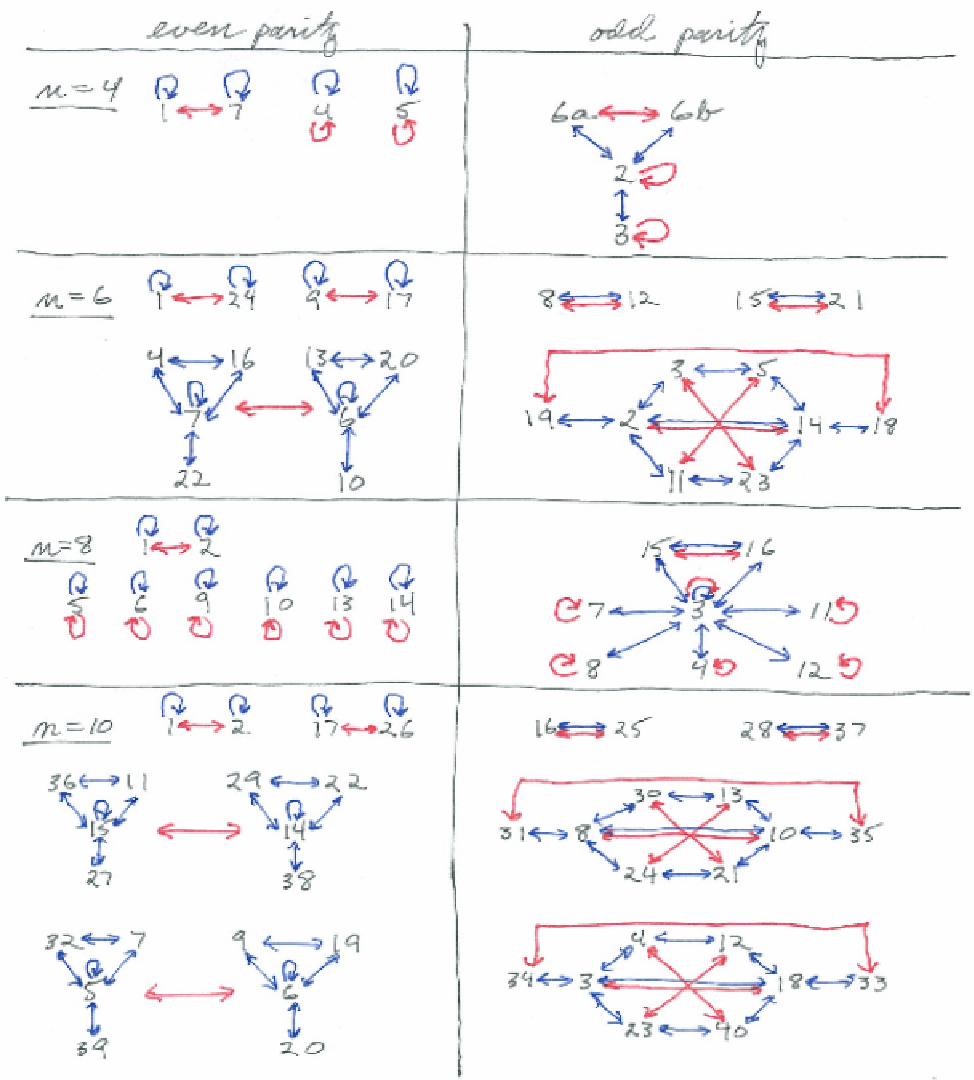


1 2
7 9
6 12
3 8
11
4 5
10

$n = 9$



1 2
8 40
30 27
21 39
33 26
19 7
14 24 11 32
5 3 29
25 35 37
42 34 28
36 22 33
18 20
6
31 4 12
10 13
17
9 15 38



even parity
odd parity
n = 4
n = 6
n = 8
n = 10

STD Isomorphism Classes for n = 6

1. 000000	2. 000001. 011010, 010000, 101100, 001011, 100110
3. 000010, 001000	4. 000011, 011000, 101110
5. 000100, 101001, 110010	6. 000101, 001111, 010100, 011110, 110011, 111001
7. 000110, 001100, 100001, 101011, 110000, 111010	8. 000111, 011100, 110001
9. 001001, 010010, 100100	10. 001010
11. 001101, 010110, 111011	12. 001110, 100011, 111000
13. 010001, 100111, 111100	14. 010011, 011001, 100101, 101111, 110100, 111110
15. 010101	16. 010111, 011101
17. 011011, 101101, 110110	18. 011111
19. 100000	20. 100010, 101000
21. 101010	22. 110101
23. 110111, 111101	24. 111111

QuickTime™ and a
Graphics decompressor
are needed to see this picture.

	1	24	9	17	8	12	15	21	22	7	4	16	10	6	13	20	19	18	2	14	3	5	11	23
1	1																							
24		1																						
9			1																					
17				1																				
8					0	1																		
12					1	0																		
15							0	1																
21							1	0																
22									0	1	0	0												
7									1/6	1/3	1/3	1/6												
4									0	2/3	0	1/3												
16									0	1/2	1/2	0												
10													0	1	0	0								
6													1/6	1/3	1/3	1/6								
13													0	2/3	0	1/3								
20													0	1/2	1/2	0								
19																	0	0	1	0	0	0	0	0
18																	0	0	0	1	0	0	0	0
2																	1/6	0	0	1/3	1/6	0	1/3	0
14																	0	1/6	1/3	0	0	1/3	0	1/6
3																	0	0	1/2	0	0	1/2	0	0
5																	0	0	0	2/3	1/3	0	0	0
11																	0	0	2/3	0	0	0	0	1/3
23																	0	0	0	1/2	0	0	1/2	0

Discrete Baker Transformation

For binary valued additive rules in one dimension the discrete baker transformation is defined by

$$a_i \to \sum_{j:i=2j \bmod(n)} a_j \mod(2)$$

In terms of vector components and neighborhood components

$$\vec{a} \to b \cdot \vec{a} \qquad b_{ij} = \begin{cases} 1 & 2j = i \bmod(n) \\ 0 & otherwise \end{cases}$$

$$\vec{x} \to B \cdot \vec{x} \qquad x_i \to x_{i \cdot b} \qquad B_{ij} = \begin{cases} 1 & j = i \cdot b \\ 0 & otherwise \end{cases}$$

Discrete Baker Transformation

Lemma:

$$\left[\sum_{i=0}^{n-1} a_i \sigma^i\right]^2 = \sum_{i=0}^{n-1} a_i \sigma^{2i \bmod (n)}$$

As a result, for additive rules

$$b(X) = X^2, \quad b^k(X) = X^{2^k}$$

Examples:

n=5: (a_0,a_1,a_2,a_3,a_4)--> (a_0,a_3,a_1,a_4,a_2)

n=6: $(a_0,a_1,a_2,a_3,a_4,a_5)$--> $(a_0+a_3,0,a_1+ a_4,0,a_2+ a_5,0)$

Discrete Baker Transformation

Since each n-digit binary string defines an additive rule, the baker transformation acts both on rule space and the rule state space. The orbits of this transformation acting on all additive rules on cylinders of size n define the Baker Diagram for n.

Some examples of orbits:

n = 5: $I+\sigma \dashrightarrow I+\sigma^2 \dashrightarrow I+\sigma^4 \dashrightarrow I+\sigma^3$

n = 6: $I+\sigma \dashrightarrow I+\sigma^2 \;\text{<-->}\; I+\sigma^4 \;\text{<--}\; I+\sigma^5$ and $I+\sigma^3 \dashrightarrow \underline{0}$

n = 7: $I+\sigma \dashrightarrow I+\sigma^2 \dashrightarrow I+\sigma^4$ and $I+\sigma^3 \dashrightarrow I+\sigma^6 \dashrightarrow I+\sigma^5$

If n is odd and A(X) is the adjacency matrix for STD(X) then $A(BX) = BA(X)B^{-1}$.

Discrete Baker Transformation

Rules belonging to the same basin in a baker diagram have the same parity.

Theorem [Bulitko, Voorhees, Bulitko, 2006]

Let X and Y be rules belonging to the same cycle of a baker diagram with cycle length r and let $\{c_1,\ldots,c_m\}$ be the set of cycle lengths appearing in STD(X). Then:

1. STD(X) and STD(Y) are isomorphic as graphs.
2. The tree heights in STD(X) do not exceed 1. If n is odd, this height is 1+det(C(X)) mod(2).
3. For all i, c_i divides $2^r - 1$ and $r = lcm\left(ord_{c_1} 2, \ldots, ord_{c_m} 2\right)$

Index Permutations

A transformation T on rule space is an index permutation if there is a permutation τ:(0,1,…,n-1) such that for any rule $X = (a_0, a_1, \ldots, a_{n-1})$, $TX = (a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{t(n-1)})$.

Shifts, reflections, and the baker transformation are index permutations; duality is not.

Index Permutations

Theorem (Bulitko):

Let T be an index permutation acting on rules in one dimension. The condition that X and TX have isomorphic STDs is that $\tau(k-j) = \tau(k) - \tau(j)$ for all k,j in (0,…,n-1).

Index permutations satisfying this condition are called functional index permutations.

Index Permutations

The shift and reflection transformations are not functional index permutations but for odd n the baker transformation is.

<u>Example</u>: n = 5 (permutations for shift, reflections, baker)

σ	ρ	B
0 1 2 3 4	0 1 2 3 4	0 1 2 3 4
1 2 3 4 0	4 3 2 1 0	0 3 1 4 2

Index Permutations

k \ j	0	4	3	2	1
0	(1,0) (4,0) (0,0)				
1	(2,1) (3,4) (3,3)	(1,0) (4,0) (0,0)			
2	(3,2) (2,3) (1,1)	(4,3) (1,2) (4,4)	(1,0) (4,0) (0,0)		
3	(4,3) (1,2) (4,4)	(0,4) (0,1) (2,2)	(1,0) (4,0) (0,0)	(1,0) (4,0) (0,0)	
4	(0,4) (0,1) (2,2)	(1,0) (4,0) (0,0)	(2,1) (3,4) (3,3)	(3,2) (2,3) (1,1)	(1,0) (4,0) (0,0)

First number is $\tau(k-j)$, second is $\tau(k) - \tau(j)$

(k,m)-Circulants

Functional index permutations preserve STD structure. There is only one other class of transformations that does this.

Define: A (k,m)-circulant is a matrix with $T_{i+m,j} = T_{i,j-k \bmod(n)}$

Representing With Roots of Unity

This begins with the representation of rules and states

$$X = \sum_{i=0}^{n-1} a_i \omega^i, \qquad \mu = \sum_{i=0}^{n-1} \mu_i \omega^i$$

This is similarity to representation as dipolynomials, as used by Martin, Odlyzko, & Wolfram in their classic study of rule 90. It is more useful, however, since there is no need to reduce produces of polynomials--the reduction is automatic since $\omega^n = 1$. In addition, it takes advantage of properties of circulant matrices.

Representing With Roots of Unity

An $n\times n$ matrix $\mathbf{A}$ is circulant if and only if $\mathbf{A} = P_A(\sigma)$ for some polynomial P_A of degree less than or equal to n. Further, if $\mathbf{A} = \mathrm{circ}(a_0,\ldots,a_{n-1})$ then

$$P_A(\sigma) = \sum_{s=0}^{n-1} a_s \sigma^s$$

Representing With Roots of Unity

All n×n circulant matrices are diagonalized by the Fourier matrices:

$$F_n C(X) F_n^* = \Lambda(X) = diag(\lambda_0, \ldots, \lambda_{n-1})$$

$$F_n = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \omega^{n-1} & \omega^{n-2} & \cdots & \omega^2 & \omega \\ 1 & \omega^{n-2} & \omega^{n-4} & \cdots & \omega^4 & \omega^2 \\ & & & \vdots & & \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{n-4} & \omega^{n-2} \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-2} & \omega^{n-1} \end{pmatrix}$$

Representing With Roots of Unity

$$\lambda_s = \sum_{i=0}^{n-1} a_i \omega^{si}$$

$$\lambda_{\mathrm{s}} = \mathrm{P}_{\mathrm{X}}(\omega^{\mathrm{s}})$$

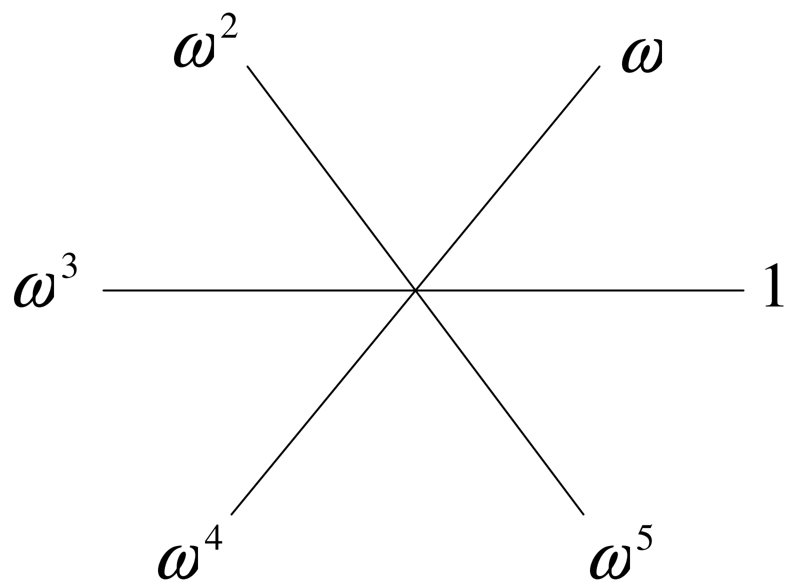
$$\lambda_0 = \pi(X)$$

$$\lambda_1 = X$$

$$\lambda_{2^k} = X^{2^k}$$

Representing With Roots of Unity

An interesting factor enters when this is combined with mod(2) arithmetic. For example, with n = 6



$\omega^3 = -1$, $\omega^4 = -\omega$, $\omega^5 = -\omega^2$ but -1 = 1 mod(2)

Representing With Roots of Unity

Thus, for n = 6:

$$\lambda_0 = \pi(X) = \lambda_3$$

$$\lambda_1 = (a_0 + a_3) + (a_1 + a_4)\omega + (a_2 + a_5)\omega^2 = \lambda_4$$

$$\lambda_2 = (a_0 + a_3) + (a_2 + a_5)\omega + (a_1 + a_4)\omega^2 = \lambda_5$$

Representing With Roots of Unity

Example: A (2,2) circulant P with n = 6.

$$X = circ(a_0, a_1, a_2, a_3, a_4, a_5), \qquad Y = circ(b_0, b_1, b_2, b_3, b_4, b_5)$$

$$C(Y) = PC(X)P^{-1}$$

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\left(\lambda_0^Y, \lambda_1^Y, \lambda_2^Y, \lambda_3^Y, \lambda_4^Y, \lambda_5^Y\right) = \left(\lambda_3^X, \lambda_4^X, \lambda_5^X, \lambda_0^X, \lambda_1^X, \lambda_2^X\right)$$

Representing With Roots of Unity

Equating eigenvalues and using the mod(2) conditions $\omega^3 = 1$, $\omega^4 = \omega$, $\omega^5 = \omega^2$, gives

$$\vec{b} = \left(b_0, b_1, b_2, b_0 + a_0 + a_3, b_1 + a_1 + a_4, b_2 + a_2 + a_5\right)$$

$$PC(X + \underline{X})P^{-1} = PC(X)P^{-1} + PC(\underline{X})P^{-1} = J$$

$$PC(\underline{X})P^{-1} = J + PC(X)P^{-1}$$

$$P^3\left(\vec{b}\right) = \vec{b}$$

J is the matrix consisting of all ones. STDs of X and <u>X</u> are related by duality; P has two period 3 cycles and two fixed points.

Representing With Roots of Unity

For each set of 8 rules determined by b_0, b_1, b_2 the diagram of mappings under P are:

$$
\begin{tikzcd}
 & & & X_0 & & & \\
 & X_1 \arrow[dl] & & & & \underline{X}_1 \arrow[dl] & \\
X_2 \arrow[rr] & & X_3 \arrow[ul] & & \underline{X}_2 \arrow[rr] & & \underline{X}_3 \arrow[ul] \\
 & & & \underline{X}_0 & & &
\end{tikzcd}
$$

Representing With Roots of Unity

A second (2,2)-circulant Q has a similar structure to P. Both have 16 fixed points and 16 period 3 cycles. In addition:

$$P\left[PC(X)P^{-1}\right]P^{-1} = QC(X)Q^{-1}$$

$$P^2 = Q$$

$$a_0+a_3,\ a_1+a_4,\ a_2+a_5$$

b_0 b_1 b_2

	000	001	010	011	100	101	110	111
000	0	σ^5	σ^4	$\sigma^4+\sigma^5$	σ^3	$\sigma^3+\sigma^5$	$\sigma^3+\sigma^4$	$\sigma^3+\sigma^4+\sigma^5$
001	$\sigma^2+\sigma^5$	σ^2	$\sigma^2+\sigma^4+\sigma^5$	$\sigma^2+\sigma^4$	$\sigma^2+\sigma^3+\sigma^5$	$\sigma^2+\sigma^3$	$\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$\sigma^2+\sigma^3+\sigma^4$
010	$\sigma+\sigma^4$	$\sigma+\sigma^4+\sigma^5$	σ	$\sigma+\sigma^5$	$\sigma+\sigma^3+\sigma^4$	$\sigma+\sigma^3+\sigma^4+\sigma^5$	$\sigma+\sigma^3$	$\sigma+\sigma^3+\sigma^5$
011	$\sigma+\sigma^2+\sigma^4+\sigma^5$	$\sigma+\sigma^2+\sigma^4$	$\sigma+\sigma^2+\sigma^5$	$\sigma+\sigma^2$	$\sigma+\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$\sigma+\sigma^2+\sigma^3+\sigma^4$	$\sigma+\sigma^2+\sigma^3+\sigma^5$	$\sigma+\sigma^2+\sigma^3$
100	$I+\sigma^3$	$I+\sigma^3+\sigma^5$	$I+\sigma^3+\sigma^4$	$I+\sigma^3+\sigma^4+\sigma^5$	I	$I+\sigma^5$	$I+\sigma^4$	$I+\sigma^4+\sigma^5$
101	$I+\sigma^2+\sigma^3+\sigma^5$	$I+\sigma^2+\sigma^3$	$I+\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$I+\sigma^2+\sigma^3+\sigma^4$	$I+\sigma^2+\sigma^5$	$I+\sigma^2$	$I+\sigma^2+\sigma^4+\sigma^5$	$I+\sigma^2+\sigma^4$
110	$I+\sigma+\sigma^3+\sigma^4$	$I+\sigma+\sigma^3+\sigma^4+\sigma^5$	$I+\sigma+\sigma^3$	$I+\sigma+\sigma^3+\sigma^5$	$I+\sigma+\sigma^4$	$I+\sigma+\sigma^4+\sigma^5$	$I+\sigma$	$I+\sigma+\sigma^5$
111	$I+\sigma+\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$I+\sigma+\sigma^2+\sigma^3+\sigma^4$	$I+\sigma+\sigma^2+\sigma^3+\sigma^5$	$I+\sigma+\sigma^2+\sigma^3$	$I+\sigma+\sigma^2+\sigma^4+\sigma^5$	$I+\sigma+\sigma^2+\sigma^4$	$I+\sigma+\sigma^2+\sigma^5$	$I+\sigma+\sigma^2$

Representing With Roots of Unity

There are only two distinct (2,2)-circulant patterns that appear and these cases are inverses. Their action on powers of the shift is:

A Case	B Case
$\sigma \longrightarrow \sigma^2+\sigma^4+\sigma^5$ $\sigma^2 \longrightarrow \sigma^2$ $\sigma^3 \longrightarrow I+\sigma+\sigma^4$ $\sigma^4 \longrightarrow \sigma^4$ $\sigma^5 \longrightarrow I+\sigma^2+\sigma^3$ $I \longrightarrow I$	$\sigma \longrightarrow I+\sigma^3+\sigma^4$ $\sigma^2 \longrightarrow \sigma^2$ $\sigma^3 \longrightarrow I+\sigma^2+\sigma^5$ $\sigma^4 \longrightarrow \sigma^4$ $\sigma^5 \longrightarrow \sigma+\sigma^2+\sigma^4$ $I \longrightarrow I$

Representing With Roots of Unity

Similar analysis for (2,4)-circulants gives

$$\left(\lambda_0^Y,\lambda_1^Y,\lambda_2^Y,\lambda_3^Y,\lambda_4^Y,\lambda_5^Y\right)=\left(\lambda_3^X,\lambda_2^X,\lambda_1^X,\lambda_0^X,\lambda_5^X,\lambda_4^X\right)$$

$$\vec{b}=\left(b_0,b_1,b_2,b_0+a_0+a_3,b_1+a_2+a_5,b_2+a_1+a_4\right)$$

In this case two patterns of transitions show up:

(1) Four fixed points and two period 2 cycles (a_0+a_3, a_0+a_3, a_0+a_3 = 000, 011, 100, 111);

(2) Eight period 2 cycles (a_0+a_3, a_0+a_3, a_0+a_3 = 001, 010, 101, 110);

	000	001	010	011	100	101	110	111
000	0	σ^4	σ^5	$\sigma^4+\sigma^5$	σ^3	$\sigma^3+\sigma^4$	$\sigma^3+\sigma^5$	$\sigma^3+\sigma^4+\sigma^5$
001	$\sigma^2+\sigma^5$	$\sigma^2+\sigma^4+\sigma^5$	σ^2	$\sigma^2+\sigma^4$	$\sigma^2+\sigma^3+\sigma^5$	$\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$\sigma^2+\sigma^3$	$\sigma^2+\sigma^3+\sigma^4$
010	$\sigma+\sigma^4$	σ	$\sigma+\sigma^4+\sigma^5$	$\sigma+\sigma^5$	$\sigma+\sigma^3+\sigma^4$	$\sigma+\sigma^3$	$\sigma+\sigma^3+\sigma^4+\sigma^5$	$\sigma+\sigma^3+\sigma^5$
011	$\sigma+\sigma^2+\sigma^4+\sigma^5$	$\sigma+\sigma^2+\sigma^5$	$\sigma+\sigma^2+\sigma^4$	$\sigma+\sigma^2$	$\sigma+\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$\sigma+\sigma^2+\sigma^3+\sigma^5$	$\sigma+\sigma^2+\sigma^3+\sigma^4$	$\sigma+\sigma^2+\sigma^3$
100	$I+\sigma^3$	$I+\sigma^3+\sigma^4$	$I+\sigma^3+\sigma^5$	$I+\sigma^3+\sigma^4+\sigma^5$	I	$I+\sigma^4$	$I+\sigma^5$	$I+\sigma^4+\sigma^5$
101	$I+\sigma^2+\sigma^3+\sigma^5$	$I+\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$I+\sigma^2+\sigma^3$	$I+\sigma^2+\sigma^3+\sigma^4$	$I+\sigma^2+\sigma^5$	$\sigma+\sigma^2+\sigma^4+\sigma^5$	$I+\sigma^2$	$I+\sigma^2+\sigma^4$
110	$I+\sigma+\sigma^3+\sigma^4$	$I+\sigma+\sigma^3$	$I+\sigma+\sigma^3+\sigma^4+\sigma^5$	$I+\sigma+\sigma^3+\sigma^5$	$I+\sigma+\sigma^4$	$I+\sigma$	$I+\sigma+\sigma^4+\sigma^5$	$I+\sigma+\sigma^5$
111	$I+\sigma+\sigma^2+\sigma^3+\sigma^4+\sigma^5$	$I+\sigma+\sigma^2+\sigma^3+\sigma^5$	$I+\sigma+\sigma^2+\sigma^3+\sigma^4$	$I+\sigma+\sigma^2+\sigma^3$	$I+\sigma+\sigma^2+\sigma^4+\sigma^5$	$I+\sigma+\sigma^2+\sigma^5$	$I+\sigma+\sigma^2+\sigma^4$	$I+\sigma+\sigma^2$

Representing With Roots of Unity

For (2,4)-circulants the action on powers of the shift are:

A Case	B Case
$\sigma \longrightarrow I+\sigma^2+\sigma^3$ $\sigma^2 \longrightarrow \sigma^4$ $\sigma^3 \longrightarrow I+\sigma+\sigma^4$ $\sigma^4 \longrightarrow \sigma^2$ $\sigma^5 \longrightarrow \sigma^2+\sigma^4+\sigma^5$ $I \longrightarrow I$	$\sigma \longrightarrow \sigma+\sigma^2+\sigma^4$ $\sigma^2 \longrightarrow \sigma^4$ $\sigma^3 \longrightarrow I+\sigma^2+\sigma^5$ $\sigma^4 \longrightarrow \sigma^2$ $\sigma^5 \longrightarrow I+\sigma^3+\sigma^4$ $I \longrightarrow I$

Representing With Roots of Unity

The same procedure can be carried out for other n values:

4	$\vec{b} = (b_0, b_1, a_0 + a_2 + b_0, a_1 + a_3 + b_1)$
5	$\vec{b} = (a_0, a_1, a_2, a_3, a_4)$ $\vec{b} = (a_0, a_3, a_1, a_4, a_2)$ Baker transformation $\vec{b} = (a_0, a_2, a_4, a_1, a_3)$ Inverse baker transformation $\vec{b} = (a_0, a_4, a_3, a_2, a_1)$ Baker squared
6	(2,2) $\vec{b} = (b_0, b_1, b_2, a_0 + a_3 + b_0, a_1 + a_4 + b_1, a_2 + a_5 + b_2)$ (2,4) $\vec{b} = (b_0, b_1, b_2, a_0 + a_3 + b_0, a_2 + a_5 + b_1, a_1 + a_4 + b_2)$

For odd n there is also the dual rule.

Representing With Roots of Unity

7	$\vec{b}=(a_0,a_1,a_2,a_3,a_4,a_5,a_6)$
	$\vec{b}=(a_0,a_4,a_1,a_5,a_2,a_6,a_3)$ Baker transformation
	$\vec{b}=(a_0,a_2,a_4,a_6,a_1,a_3,a_5)$ Baker squared
	$\vec{b}=(a_0,a_5,a_3,a_1,a_6,a_4,a_2)$ Square root of baker
	$\vec{b}=(a_0,a_3,a_6,a_2,a_5,a_1,a_4)$ Inverse of square root of baker
	$\vec{b}=(a_0,a_6,a_5,a_4,a_3,a_2,a_1)$ Cube of square root of baker
8	$\vec{b}=(b_0,b_1,b_2,b_3,a_0+a_4+b_0,a_1+a_5+b_1,a_2+a_6+b_2,a_3+a_7+b_3)$
	$\vec{b}=(b_0,b_1,b_2,b_3,a_0+a_4+b_0,a_3+a_7+b_1,a_2+a_6+b_2,a_1+a_5+b_3)$

Representing With Roots of Unity

N = 9

$$\vec{b}=\left(b_0,b_1,b_2,a_0+a_3+b_0,a_1+a_4+b_1,a_2+a_5+b_2,a_0+a_6+b_0,a_1+a_7+b_1,a_2+a_8+b_2\right)$$

$$\vec{b}=\left(b_0,b_1,b_2,a_0+a_6+b_0,a_2+a_5+b_1,a_1+a_7+b_2,a_0+a_3+b_0,a_5+a_8+b_1,a_1+a_4+b_2\right)$$

$$\vec{b}=\left(b_0,b_1,b_2,a_0+a_3+b_0,a_1+a_7+b_1,a_5+a_8+b_2,a_0+a_6+b_0,a_4+a_7+b_1,a_2+a_5+b_2\right)$$

$$\vec{b}=\left(b_0,b_1,b_2,a_0+a_6+b_0,a_5+a_8+b_1,a_4+a_7+b_2,a_0+a_3+b_0,a_2+a_8+b_1,a_1+a_7+b_2\right)$$

$$\vec{b}=\left(b_0,b_1,b_2,a_0+a_3+b_0,a_4+a_7+b_1,a_2+a_8+b_2,a_0+a_6+b_0,a_1+a_4+b_1,a_5+a_8+b_2\right)$$

$$\vec{b}=\left(b_0,b_1,b_2,a_0+a_6+b_0,a_2+a_8+b_1,a_1+a_4+b_2,a_0+a_3+b_0,a_2+a_5+b_1,a_4+a_7+b_2\right)$$

Iteration of the first of these yields a fixed point. The remaining yield cycles of periods 6, 3, 2, 3, and 6 respectively.

Technical Question

For p prime let ω be the first p-th root of unity. Let S be the set of all p-th roots of unity: $S = \{\omega^k | 0 \leq k \leq p-1\}$. Then

$$\sum_{k=0}^{p-1} \omega^k = 0$$

Question: Is there any proper subset of S whose sum is 0?