

General Features of W-Rule Cellular Automata

Olu Lafe

lafe@quikcat.com

Lafe Technologies

28001 Chagrin Blvd., Suite 305

Beachwood, Ohio 44122

Acknowledgments

- **Brian Blackmore** (Mathematical proofs and conjectures on periodicity and invertibility, encryption coding)
- **Dr. Eric Graham** (Symbolic programming, exact parameter determination)
- **Dr. Doug Danforth** (Generalized polynomial representation, L matrix, exact and approximate parameter determination)

Cellular Automata

- A cellular automaton (CA) is a collection of cells that have discrete states which change with time
- The cells have neighbors
- The neighborhood size is the same for all cells
- The neighborhood includes the cell itself

Notation

- K = Maximum state of the CA
- m = Size of the neighborhood
- N = Number of cells in the lattice
- \mathbf{x} = Vector representing the neighborhood cell states x_i ($i=0,1,2,\dots,m-1$)
- r = the rule that changes the state of a cell as a function of \mathbf{x}
- W = Vector representing the weights W_j ($j=0,1,2,\dots,2^{m-1}$) describing the rule

Definition of W-Rule

$$r(x) = W_{\mu} x^{\mu} \bmod K$$

$$x^{\mu} = \prod_i x_i^{\mu_i}$$

$$0 \leq i < m, 0 \leq x_i < K, 0 \leq \mu < 2^m, \mu = \mu_i 2^i$$

$$\mu_i \in [0,1]$$

Observe that the number (2^m) of weights is independent of the maximum state K

W-Rule for $m=2$

$$r(x) = (W_0 + x_0W_1 + x_1W_2 + x_0x_1W_3) \bmod K$$

W-Rule ($K=2, m=3$) Parameters for Wolfram's Rule

<i>Wolfram Rule</i>	W_0	W_1	W_2	W_3	W_4	W_5	W_6	W_7
252	1	1	0	1	0	0	0	0
195	0	1	1	0	0	0	0	1
127	0	0	0	0	0	0	1	1
16	1	0	1	1	1	0	0	0

General Polynomial Representation of the Local Rule

$$\xi = x.K = x_0 K^0 + x_1 K^1 + \dots + x_{m-1} K^{m-1}$$

$$x_i = (\xi \text{ DIV } K^i) \text{ mod } K$$

$$r(\xi) = \left(\sum_{j=0}^{2^{m-1}} c_j \xi^j \right) \text{ mod } K$$

The W-Rule is a special case of the general polynomial representation with $W=W(c)$

Special Features of W-Rule

- Matrix Representation
- Periodicity
- Invertibility
- Encryption
- Compression

Global Properties of W-Rule

- Let X represent the *global* state of the lattice of all N cells. $R(X)$ is the *global* rule formed by applying the CA *local* rule $r(\mathbf{x})$ to all cell neighborhoods.
- R^n implies the application of the global rule n times.

Periodic W-Rule

The periodic W-Rule transforms global values X

$$X = R^{\tau}(X)$$

$$R^n(\alpha) = R(R^{n-1}(\alpha))$$

$$R^1(\alpha) = R(\alpha)$$

Hence

$$R^2(\alpha) = R(R^1(\alpha)), \text{ and so forth}$$

τ = Period of the W - Rule

Example of Periodic W-Rule for $m=3, K=16, N=8$

W: 6 15 10 10 6 10 4 10

t=0

a

t=1 Number of terms=8

$$6+6h+15b+10bh+10a+4ah+10ab+10abh$$

t=2 Number of terms=59

$$\begin{aligned} &4ab^2+4a^2+8h+8ab^2h+8a^2gh+12g+8ab^2g+8gh+8a^2g+8ab^2gh+8a^3b^2ch \\ &+c+8a^3b^2c+8ab^2ch+8ch^2+12cg+8ab^2cgh+8a^2bh+4a^2b+12bh+8a^2bgh \\ &+8bg+8a^2bg+4a^2bch+12bc+8a^2bcgh^2+4a^2bc+8bch+8bch^2+4bcg \\ &+8a^2bcg+8a^2bch^2+4b^2+8a^2b^2h+4a+8a^3+12ah+12ag+8b^2g+4agh \\ &+4b^2c+8acgh^2+8a^3c+4a^2b^2c+4acg+8b^2cg+8ach^2+8a^2b^2cgh+12acgh \\ &+8a^2b^2cg+8a^2bh+12abh+8a^3b+8abgh+8abcgh^2+8a^3bch+4abch \\ &+4abcg+12abcgh \end{aligned}$$

Example of Periodic W-Rule for m=3, K=16, N=8

W: 6 15 10 10 6 10 4 10

t=3 Number of terms=126

$$\begin{aligned}
 &6+8a^2h+4bc^2+12h+8bc^2h+8g+8h^2+8gh+8f+8fh+8fgh+15d+8a^2dh \\
 &+8ab^2d+8a^2d+12dh+8dg+8dh^2+8dgh+8df+8dfh+8dfgh+10c+8ab^2c \\
 &+8cg+4ab^2cd+14cd+8bc^2d+8a^2cdh+8ab^2cdh+12cdh+8ab^2cdg \\
 &+8cdg+8cdh^2+8ab^2cdgh+8cdgh+8cdf+8cdfh+8cdfgh+2b+12c^2 \\
 &+8c^2h+4bh+8a^2bh^2+8bf+8bfh+8bfg+8ab^3d+4c^2d+10bd+8a^2bdh \\
 &+12bdh+8bdg+8a^2bdh^2+8bdf+8bdfh+8bdfgh+8c^3+8ab^3c+8a^2bch \\
 &+4bc+8a^2bc+8bcg+8c^3d+10bcd+4bcdh+8a^2bcdh^2+8bcdh+8bcdh \\
 &+8bcdh+12b^2+8b^3c^2+8abc^2+8abc^2h+8ah^2+8ad+8b^2d+8b^3c^2d \\
 &+8a^2b^2d+8adh+8adh^2+4b^2c+4ac+8a^2b^2c+8acg+8acgh+12b^2cd \\
 &+8b^3c^2d+8acd+8b^2cdh+8a^2b^2cd+8b^2cdg+8acd^2+8ac^2+8abgh^2 \\
 &+12ab+4abh+8abh^2+8abgh+8abf+8abfh+8abfgh+4b^2c^2d+8abdgh^2 \\
 &+4abd^2+8abd^2+8abd^2+8abd^2+8abd^2+8abd^2+8b^2c^3+8b^3c \\
 &+4abc+8abch+8abcg+8abcgh+8b^2c^3d+8abcdgh^2+4abcd+8a^2b^3cd \\
 &+4abcdh+8abcdh^2+8abcdgh+8abcdh+8abcdh+8abcdh+8abcdh
 \end{aligned}$$

t=4 Number of terms=24

$$\begin{aligned}
 &8cd^2+e+8de+8bc^2de+8d^2+8c+8d^2e+8c^2+8c^2d+8bd+8c^2de+8bc \\
 &+8c^2d^2e+8bcd+8bcde+8a+8ae+8ade+8ac+8ace+8acde+8abc+8abce \\
 &+8abcde
 \end{aligned}$$

Example of Periodic W-Rule for $m=3, K=16, N=8$

W: 6 15 10 10 6 10 4 10

t=5 Number of terms=29

$8de^2+6+15f+10e+2ef+8cd^2ef+8e^2+14d+10df+8e^2f+4de+10def$
 $+8d^2+8d^2e+8ce+8d^2ef+8cd+8d^2e^2f+8cde+8cdef+8b+8bf+8bef$
 $+8bd+8bdf+8bdef+8bcd+8bcd^2+8bcdf+8bcdef$

t=6 Number of terms=59

$12ef^2+8def^2g+g+8de^2f+12de^2fg+4fg+12e+8de^2f^2+12f^2+8cd^2eg$
 $+12f^2g+8de^3f+8cd^2efg+8de^3fg+8def^2+8d+12e^2+8def^2g+8e^3f^2g$
 $+12e^2f+4df+8cd^2e^2fg+8dfg+12e^2fg+8e^3+4de+8e^3g+12e^2f^2g$
 $+8e^3f+4def+12defg+8cde^2+8cef^2+4c+8d^2g+4cg+8cde^2f+8cf$
 $+8d^2fg+12cfg+8cf^2+4ce+8cde^2f^2g+8d^2eg+8cf^2g+12ceg+12cefg$
 $+8cd+8ce^2+8cdef^2+8cdef^2g+8ce^2f+8ce^2fg+8d^2e^2fg+12cde$
 $+8ce^2f^2g+4cdeg+8cdef+4cdefg$

Example of Periodic W-Rule for m=3, K=16, N=8

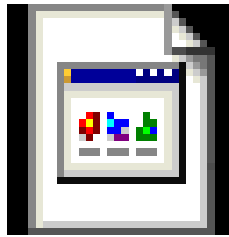
W: 6 15 10 10 6 10 4 10

t=7 Number of terms=126

$$\begin{aligned}
 &12fg^2+6+8de^2+8ef^2h+15h+8de^2h+10g+8ef^2g+8fg^2h+12ef^2gh \\
 &+6gh+8de^2gh+4g^2+10f+8ef^2h+12g^2h+10fh+8de^2fh+8g^2+8ef^2g \\
 &+8de^2fg+4fg+8g^2h+10fgh+4f^2+8f^2g^2+8efg^2+8eh+8f^2h+8f^2g^2h \\
 &+12f^2g+12eg+4f^2gh+8f^2g^2h+8egh+8eg^2+8cd^2ef+4ef+12f^2g^2h \\
 &+8cd^2efh+8f^2g^2+8f^2g+12efg+8f^2g^2h+8cd^2efgh+12efgh+4d \\
 &+8dfg^2+8e^2h+4dh+4dgh+8def^2gh+8dg^2+12df+4dfh+8e^2fg+12dfgh \\
 &+8defg^2+8e^2f^2h+8deh+8e^2f^2g+8df^2gh+8e^2f^2gh+12def+12defh \\
 &+8defg+8e^2f^2gh+12defgh+8c+8d^2+8ch+8d^2h+8cg+8cef^2gh+8cgh \\
 &+8d^2gh+8cfh+8cfg+8d^2e+8d^2eh+8ceg+8cf^2gh+8d^2egh+8d^2ef \\
 &+8d^2efh+8cefh+8cefg+8d^2efgh+8cd+8cdh+8cdef^2gh+8cdgh \\
 &+8d^2e^2f+8d^2e^2fh+8d^2e^2fgh+8cdeg+8cdef+8cdefg+8cdefgh \\
 &+8b+8bh+8bgh+8bf+8bfh+8bfgh+8bef+8befh+8befgh+8bd+8bdh \\
 &+8bdgh+8bdf+8bdfh+8bdfgh+8bdef+8bdefh+8bdefgh+8bcd+8bcdh \\
 &+8bcdgh+8bcdh+8bcdh+8bcdh+8bcdh+8bcdh+8bcdh+8bcdh+8bcdh+8bcdh
 \end{aligned}$$

t=8 Number of terms=1

a



W-Rule-Demo.htm

Invertible W-Rule

$$X(t) = R(X(t-1))$$

$$X(t-1) = R^{-1}(X(t))$$

Example of Invertible W-Rule for $m=3, K=16$

- **W-Rule**

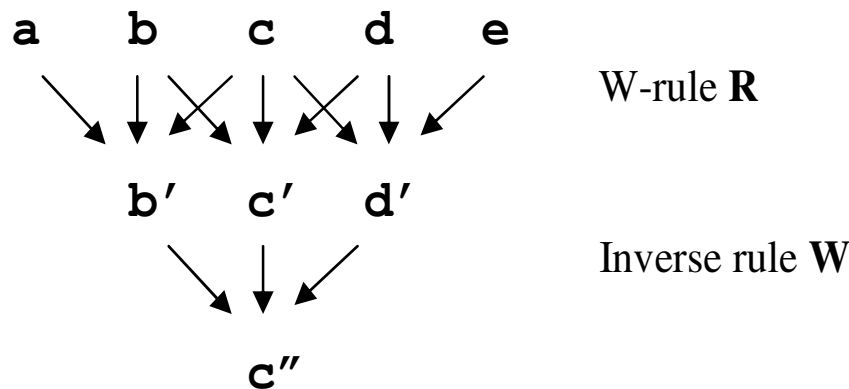
$$W_0=7 \quad W_1=12 \quad W_2=13 \quad W_3=0 \quad W_4=4 \quad W_5=12 \\ W_6=12 \quad W_7=8$$

- **Inverse W-Rule**

$$W'_0=13 \quad W'_1=0 \quad W'_2=1 \quad W'_3=8 \quad W'_4=12 \quad W'_5=12 \\ W'_6=12 \quad W'_7=8$$

Symbolic Calculation of W

Calculating the inverse of an arbitrary W-rule **R** is simple in principle:



From 5 cell values a, b, c, d, e apply **R** to calculate evolved cell value polynomials b', c' and d' . Then apply the unknown rule **W** to calculate the cell value c'' , which is a polynomial in a, b, c, d, e and the 8 w terms in **W**. Since $p=c''-c$ must be zero for all values of a, b, c, d, e a sufficient condition for an inverse is that each factor of p must be zero, resulting a set of approximately 100 linear equations for the eight w terms. A solution of the set of linear equations will result in an inverse of the rule **R**.

Finding the Weights for the Inverse W Rule via Symbolic Algebra

The problem is to find solutions for W_0 to W_7 that satisfy all values of a,b,c,d,e in range 0 to 15 for the following equation (modulo 16):

$$\begin{aligned}
 &13bW_4+4dW_6+12bc2eW_7+12eW_7+4ceW_5+4bc2W_7+7W_7+W_6+8bc2deW_7 \\
 &+8cdeW_5+12bc2dW_7+9dW_7+15c+W_5+4eW_5+13cW_7+4d2W_7+11dW_5 \\
 &+15cW_6+8cdeW_7+15cdW_7+7W_4+4bcW_5+4beW_7+4c2eW_7+12bceW_5 \\
 &+8bcd2W_7+bW_7+12bcdW_5+7bW_6+12c2W_6+8c2deW_7+8bcdeW_5+11bdW_7 \\
 &+12cW_4+11bW_5+8bcdW_6+12beW_5+7bcW_7+9bdW_5+13bcW_6+8bcdeW_7 \\
 &+5bcdW_7+12abW_4+4acW_5+12b2dW_6+W_3+8b2cd2W_7+8abc2W_7+4aW_7 \\
 &+12b2W_7+4eW_3+12acdW_5+8abc2W_6+12aW_6+4b2W_6+15dW_3+8b2dW_7 \\
 &+8abc2dW_7+12adW_7+8abcW_4+12aW_5+8b2cdW_6+7cW_3+12d2W_3+8acW_7 \\
 &+4b2cW_7+12b2d2W_7+4adW_5+8acW_6+12b2cW_6+13cdW_3+4b2cdW_7 \\
 &+8acdW_7+8cdeW_3+4aW_4+8abcW_5+8bcd2W_3+12bW_3+4c2W_3+12abW_7 \\
 &+4ac2W_7+12c2eW_3+8abcdW_5+4abW_6+12ac2W_6+8bdW_3+12c2dW_3 \\
 &+4abdW_7+12ac2dW_7+8c2deW_3+12acW_4+4abW_5+4bcW_3+12bd2W_3 \\
 &+12abcW_7+12abdW_5+4abcW_6+4bcdW_3+4abcdW_7+7W_2+12dW_2+13cW_2 \\
 &+4bW_2+12bdW_2+12bcW_2+8bcdW_2+7W_1+12eW_1+13dW_1+4cW_1+12ceW_1 \\
 &+12cdW_1+8cdeW_1+W_0 = 0
 \end{aligned}$$

Sufficient Conditions for W-Rule Reversibility

- i.* $W_0=0$
- ii.* W_1 has a multiplicative inverse modulo K
- iii.* For all $i, j > 1$, $W_i W_j=0$ modulo K

Unique W-Rule Inverse if above conditions hold

i) $W'_0 = 0$

ii) $W'_1 = W_1^{-1}$

iii) for all $\nu > 1$, $W'_\nu = -(W_1^{-1})^{H(\nu)+1} W_\nu$

where the inverse W coefficients are indicated by a prime and $H(\nu)$ is the Hamming weight of the number ν or the count of 1s in the binary representation of ν

Case when W_0 is not Zero: Conjecture

$$\text{i) } W_0' = -\sum_{Y>0} W_0^{H(Y)} W_Y'$$

$$\text{ii) } W_1' = W_1^{-1} - \sum_{Y \in \{y | H(y) > 1, y.1=1\}} W_0^{H(Y)-1} W_Y'$$

$$\text{iii) } \text{for all } \nu > 1, W_\nu' = -(W_1^{-1})^{H(\nu)+1} W_\nu - \sum_{Y \in \{y | H(y) > H(\nu), y.\nu=H(\nu)\}} W_0^{H(Y)-H(\nu)} W_Y'$$

where the inverse W coefficients are indicated by a prime and $H(\nu)$ is the Hamming weight of the number ν or the count of 1 s in the binary representation of ν

Matrix Representation of W-Rule

- Apply the local rule $r(x)$ to all K^m possible CA neighborhood patterns to obtain

$$y(x) = \left(\sum_{\mu=0}^{2^m-1} W_{\mu} \left(\prod_{i=0}^{m-1} x^{\mu_i} \right) \right) \text{mod } K$$

or

$$\{y\} = [L]\{W\}$$

where

$\{y\}$ is a column vector with K^m elements

$\{W\}$ has 2^m elements

$[L]$ is a matrix of size $K^m \times 2^m$

Immediate Consequence of Matrix Representation

- All of the highly complex nonlinearity of the CA is compressed into the matrix $[L]$.
- The relationship between the output $\{y\}$ and the weights $\{W\}$ is linear.
- Finding an inverse of matrix $[L]$ allows a direct computation of the W coefficients.
- For dual state CA ($K=2$), $[L]$ is its own inverse thus allowing $\{W\}$ to be determined from:

W Determination for Dual State CA

$$\{w\} = [L]\{y\}$$

since

$$L^2 = [L][L] = I \text{ (the identity matrix)}$$

W Determination for $K > 2$ CA

$$\{W\} = [A]\{y\}$$

where

$$A_{x\mu} = \prod_{i=0}^{m-1} \left(\delta_{\mu_i, x_i} - \delta_{\mu_i, 1} \delta_{x_i, 0} \right) \quad 0 \leq x_i < K$$

and δ is the Kroeneker delta function

Least Squares Estimation of W-Rule Weights

$$L^+ = (L^T L)^{-1} L^T \text{ (PseudoInverse)}$$

$$W = L^+ (x) y(x) \text{ (sum over } x)$$

$$(L^T L)_{\mu}^{\nu} = K^{\mu.\nu} (K(K+1)/2)^{(\mu.\nu+\nu.\mu)} (K(K+1)(2K+1)/6)^{\mu.\nu}$$

L Matrix for $K=2$, $m=1$

1 0

1 1

L Matrix for $K=3, m=1$

1 0

1 1

1 2

L Matrix for $K=2, m=2$

1 0 0 0

1 1 0 0

1 0 1 0

1 1 1 1

L Matrix for $K=3, m=2$

1	0	0	0
1	1	0	0
1	2	0	0
1	0	1	1
1	1	1	1
1	2	1	2
1	0	2	0
1	1	2	2
1	2	2	1

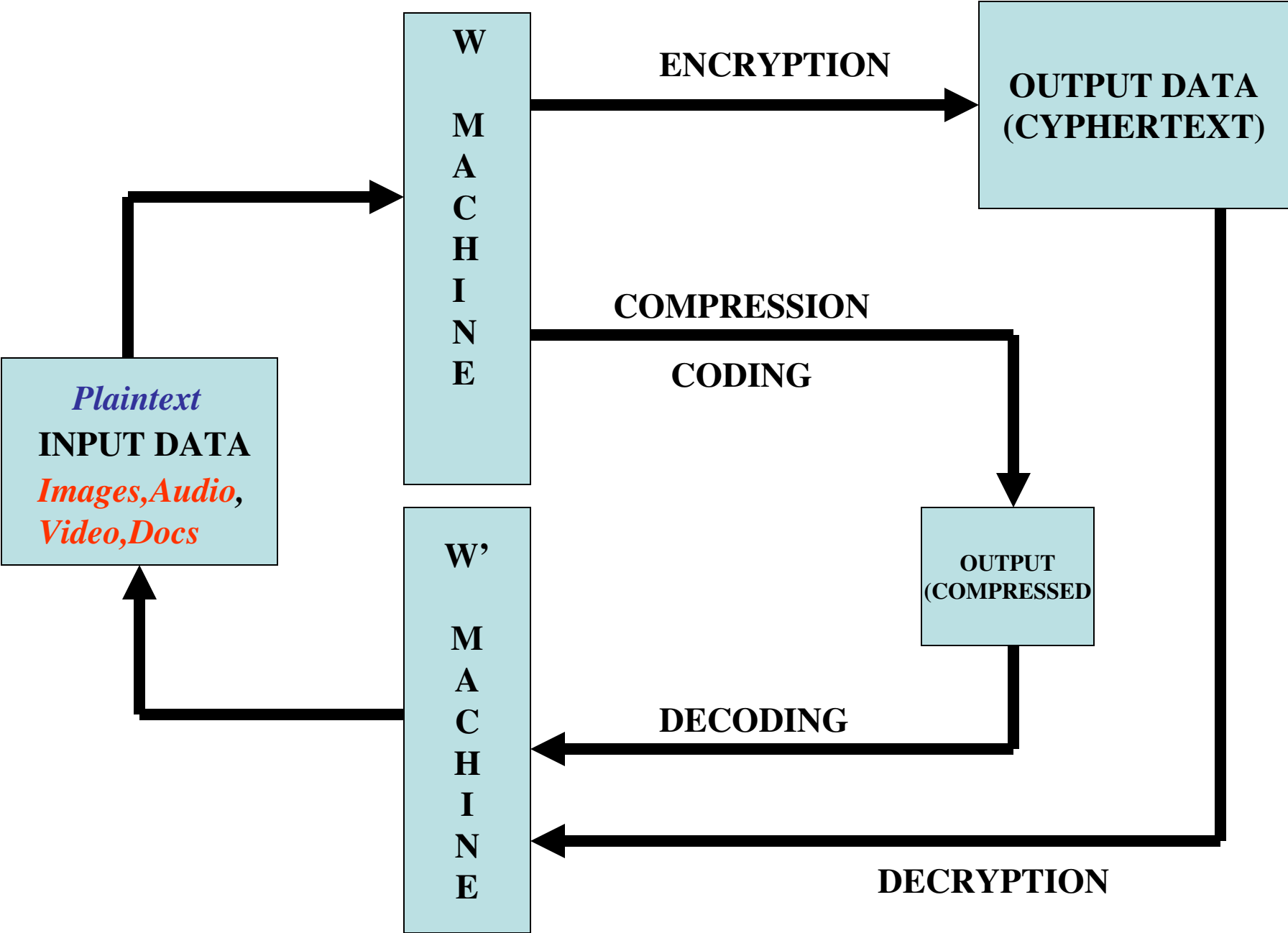
L Matrix for $K=2, m=3$

1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	1	1	0	0	0	0
1	0	0	0	1	0	0	0
1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1

L Matrix for $K=3, m=3$

1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0
1	2	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	2	1	2	0	0	0	0
1	0	2	0	0	0	0	0
1	1	2	2	0	0	0	0
1	2	2	1	0	0	0	1
1	0	0	0	1	0	0	0
1	1	0	0	1	1	0	0
1	2	0	0	1	2	0	0
1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1
1	2	1	2	1	2	1	2
1	0	2	0	1	0	2	0
1	1	2	2	1	1	2	2
1	2	2	1	1	2	2	1
1	0	0	0	2	0	0	0
1	1	0	0	2	2	0	0
1	2	0	0	2	1	0	0
1	0	1	0	2	0	2	0
1	1	1	1	2	2	2	2
1	2	1	2	2	1	2	1
1	0	2	0	2	0	1	0
1	1	2	2	2	2	1	1
1	2	2	1	2	1	1	2

Applications



Secret Key Encryption Application

- Select m, K, N
- Encryption key length is 2^m characters - each of maximum magnitude $K-1$
- Choose weights W of
 - A. Periodic Rule (period T)
OR
 - B. Invertible Pair (W, W')
- Use Plaintext as initial configuration of CA

Encryption Application (Cont'd)

- Evolve CA for $T-1$ time steps in Case A OR
- Evolve CA for 1 time step in Case B
- New Evolved State is the Cyphertext.
- To recover Plaintext – Use Cyphertext as initial configuration.
- Evolve CA for 1 time step using W (in Case A) OR W' (in Case B)

Generation of Basis Functions for Signal/Image Compression

