Computing Shifts in 90/150 Cellular Automata Sequences

Palash Sarkar
Department of Combinatorics and Optimization
University of Waterloo
200 University Avenue West
Waterloo, Ontario
Canada N2L 3G1
e-mail: psarkar@cacr.math.uwaterloo.ca

Abstract

Sequences produced by cellular automata (CA) are studied algebraically. A suitable k-cell 90/150 CA over $\mathbb{F}_q$ generates a sequence of length $q^k - 1$. The temporal sequence of any cell of such a CA can be obtained by shifting the temporal sequence of any other cell. We obtain a general algorithm to compute these relative shifts. This is achieved by developing the proper algebraic framework for the study of CA sequences.

1 Introduction

Let q be a prime power and $\mathbb{F}_q$ be the finite field of cardinality q. Consider the following $k \times k$ matrix M.

$$
\begin{aligned}
M_{ij} &= 0 && \text{if } |i-j| > 1; \\
&= a_i && \text{if } i = j; \\
&= l_i && \text{if } i = j+1; \\
&= u_i && \text{if } i = j-1,
\end{aligned}
\tag{1}
$$

where the constants $a_1, \ldots, a_k, l_2, \ldots, l_k, u_1, \ldots, u_{k-1}$ belong to $\{0, 1\}$. We consider the entries of M to be elements of $\mathbb{F}_q$. Let $C^0 \in \mathbb{F}_q^k \setminus \{(0, \ldots, 0)\}$ and for $t \geq 1$, define $C^t = MC^{t-1}$. Write $C^t = (C_1^t, \ldots, C_k^t)$. Suppose the sequence of vectors $C^0, C^1, \ldots$ has period $q^k - 1$. We study the following problem.

- Obtain an algorithm that given M will compute integers $j_2, \ldots, j_k$ such that $C_1^t = C_i^{t+j_i}$ for all $t \geq 0$.

The above problem arises naturally in the context of VLSI applications of cellular automata (CA). A cellular automata is an array of cells where each cell can be in a particular state. The set of all possible states is taken to be $\mathbb{F}_q$. The collection of the states of all the cells is said to be the state of the CA. At time $t = 0$, the CA is put into an initial state. For time $t > 0$, the state at time t is determined by the state at time $t-1$ as described below.

Let $\mathcal{C}$ be a k-cell CA and let the state of cell i at time t be denoted by C_i^t, $1 \leq i \leq k$, $t \geq 0$. Then the state of $\mathcal{C}$ at time $t \geq 0$ is $C^t = (C_1^t, \ldots, C_k^t)$. The following determines the next state evolution of $\mathcal{C}$.

$$\begin{array}{rcrcrcrl} C_i^t & = & & & a_1 C_1^{t-1} & + & u_1 C_2^{t-1} & \text{if } i = 1; \\ & = & l_i C_{i-1}^{t-1} & + & a_i C_i^{t-1} & + & u_i C_{i+1}^{t-1} & \text{if } 1 < i < k; \\ & = & l_k C_{k-1}^{t-1} & + & a_k C_k^{t-1} & & & \text{if } i = k. \end{array} \qquad (2)$$

The constants $a_1, \ldots, a_k, u_1, \ldots, u_{k-1}, l_2, \ldots, l_k$ belong to $\{0, 1\}$.

One can define CA such that the constants a_i's, b_j's and c_k's are in $\mathbb{F}_q$. For $q = 2$, this coincides with our definition. The technique that we develop later can also be used to tackle the more general definition. Note that the transition rule can be different for different cells. This is usually required in VLSI applications of CA. The more usual model for CA assumes the same transition rule for all the cells. See [6] for a recent survey of the general theory of CA.

The evolution of the state vector C^t can be described as

$$C^t = MC^{t-1}, \quad t \geq 1, \qquad (3)$$

where M is the matrix defined in Equation (1). The matrix M is called the state transition matrix (STM) of $\mathcal{C}$.

CA over $\mathbb{F}_2$ are used as hardware generators for built-in-self-test (BIST). For this purpose, CA with maximum possible period $2^k - 1$ are used and the state vectors $C^0, C^1, C^2, \ldots$ are used as the test vectors. This motivates the problem of studying the relative shift between the sequences C_i^t and C_j^t for $1 \leq i < j \leq k$. This problem is equivalent to the problem defined before.

The problem was earlier studied by Bardell [1]. In [1], an operational method to compute the shifts for a 6-cell CA was described. However, no algebraic justification or general algorithm was provided in [1]. In this paper, we approach the study of CA sequences algebraically. We first build the proper algebraic framework for the study of such sequences. Then we apply this theory to obtain a general algorithm for computing the shifts in the CA sequences. This completely solves the problem defined before. Apart from the shift computing algorithm our work also throws new light on the understanding of CA sequences.

2 Preliminaries

2.1 Homogenous Linear Recurring Sequences

A sequence s_n is said to be a *k-th order homogenous linear recurring sequence* over $\mathbb{F}_q$ (HLRS(q,k)) if

$$s_{n+k} = c_{k-1} s_{n+k-1} + c_{k-2} s_{n+k-2} + \ldots + c_0 s_n \quad \text{for } n = 0, 1, \ldots \qquad (4)$$

where $c_{k-1}, c_{k-2}, \ldots, c_0$ are elements of $\mathbb{F}_q$. The *characteristic polynomial* for the sequence defined in Equation (4) is defined to be the following polynomial in $\mathbb{F}_q[x]$.

$$f(x) = x^k - c_{k-1}x^{k-1} - c_{k-2}x^{k-2} - \cdots - c_0. \tag{5}$$

The *reciprocal polynomial* $f^*(x) \in \mathbb{F}_q[x]$ of $f(x)$ is defined by $f^*(x) = x^k f(\frac{1}{x})$.

It is known [4, Theorem 6.7, Page 193] that the maximum possible period of an HLRS(q,k) is $q^k - 1$. Sequences achieving this maximum value of period are of fundamental importance in cryptology, computer science, and engineering. The following result is an immediate consequence of [4, Theorem 6.28, Page 203].

Theorem 2.1 *Let s_n be an HLRS(q,k) and $f(x)$ be the characteristic polynomial of s_n. Then s_n has maximum possible period $q^k - 1$ iff $f(x)$ is primitive over $\mathbb{F}_q$.*

The *generating function* $G(x)$ for a sequence s_n is defined to be the following formal power series.

$$G(x) = s_0 + s_1x + s_2x^2 + \cdots + s_nx^n + \cdots = \sum_{n=0}^{\infty} s_nx^n \tag{6}$$

Let s_n be an HLRS(q,k) with characteristic polynomial $f(x)$ and generating function $G(x)$. Then from [4, Theorem 6.40, Page 211] we have

$$G(x) = \frac{g(x)}{f^*(x)}, \quad \text{where } g(x) = -\sum_{j=0}^{k-1}\sum_{i=0}^{j} c_{i+k-j}s_ix^j. \tag{7}$$

The following two results are easy to prove and will be required later.

Proposition 2.1 *Let $s_0, s_1, \ldots$ be an HLRS(q,k) with period $q^k - 1$. For $0 \leq i \leq q^k - 2$, define $W_i = (s_i, s_{i+1}, \ldots, s_{i+k-1})$. Then all the W_i's are distinct and are all the non zero elements of $\mathbb{F}_q^k$.*

Proposition 2.2 *Let $s_0, s_1, \ldots$ be an HLRS(q,k) with primitive characteristic polynomial $f(x)$. Then the characteristic polynomial of the sequence $s_{q^k-1}, \ldots, s_1, s_0, s_{q^k-1}, \ldots, s_1, s_0, \ldots$ is $f^*(x)$.*

2.2 Basic Results

We present some preliminary results which will be required later.

Theorem 2.2 *Let M be a $k \times k$ matrix over $\mathbb{F}_q$ and $\mathbf{v}_0 \in \mathbb{F}_q^k$ be such that $\mathbf{v}_0 \neq (0, \ldots, 0)$. For $i \geq 1$, define $\mathbf{v}_i = M\mathbf{v}_{i-1}$. Then the sequence*

$$\mathbf{s} = \mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \ldots$$

has period $q^k - 1$ iff the characteristic polynomial $f(x)$ of M is primitive over $\mathbb{F}_q$.

Proof : If M is non singular, then $ord(M)$, the order of M in the general linear group $GL(k,q)$ is finite. For $\mathbf{v}$ a non zero vector of $\mathbb{F}_q^k$, define the order of $\mathbf{v}$ with respect to M to be the least positive integer $i_{\mathbf{v}}$ such that $M^{i_{\mathbf{v}}}\mathbf{v} = \mathbf{v}$. If M has finite order, then each non zero vector $\mathbf{v}$ also has a finite order. Further, the orders $i_{\mathbf{v}}$ divide $ord(M)$. In fact, $ord(M) = \mathrm{lcm}(i_{\mathbf{v}_1}, \ldots, i_{\mathbf{v}_{q^k-1}})$, where $\mathbf{v}_1, \ldots, \mathbf{v}_{q^k-1}$ are all the non zero vectors of $\mathbb{F}_q^k$. To see this, let $l = \mathrm{lcm}(i_{\mathbf{v}_1}, \ldots, i_{\mathbf{v}_{q^k-1}})$. Then for each $\mathbf{v} \in \mathbb{F}_q^k$, we have $(M^l - I_k)\mathbf{v} = 0$, where I_k is the identity matrix of order k. Thus the operator $M^l - I_k$ annihilates the whole of $\mathbb{F}_q^k$ and hence $M^l - I_k = 0$. Further, for any $i < l$, there will be a $\mathbf{v}$, such that $M^i\mathbf{v} \neq \mathbf{v}$ and so $M^i \neq I_k$. Thus l is the order of M.

only if : Suppose $\mathbf{s}$ has period $q^k - 1$. Since $\mathbf{v}_0$ is a non zero vector, the sequence $\mathbf{s}$ contains all the non zero elements of $\mathbb{F}_q^k$. Thus the order of any non zero $\mathbf{v} \in \mathbb{F}_q^k$ is $q^k - 1$. Hence the order of M is also $q^k - 1$. Let i be the least positive integer such that $f(x)$ divides $x^i - 1$. Since $f(M) = 0$ (by Cayley-Hamilton theorem), this means $M^i - I_k = 0$. Since $ord(M) = q^k - 1$, we have $i = q^k - 1$. Hence $f(x)$ is primitive.

if : (This proof has been conveyed to the author by Rana Barua [2].) For any non zero $\mathbf{v} \in \mathbb{F}_q^k$, define $f_{\mathbf{v}}(x)$, the minimal polynomial for $\mathbf{v}$, to be the least degree monic polynomial such that $f_{\mathbf{v}}(M)\mathbf{v} = 0$. An easy application of the division algorithm shows that $f_{\mathbf{v}}(x)$ must in fact divide $f(x)$. Since $f(x)$ is primitive, this implies, $f_{\mathbf{v}}(x) = f(x)$ for all non zero $\mathbf{v} \in \mathbb{F}_q^k$. Let r be the period of $\mathbf{s}$. Then $M^r\mathbf{v}_0 = \mathbf{v}_0$. But this means the minimal polynomial for the $\mathbf{v}_0$ divides $x^r - 1$. Since we have already shown that the minimum polynomial for $\mathbf{v}_0$ is $f(x)$ which by hypothesis is primitive, it follows that $r = q^k - 1$. ■

Theorem 2.3 *Let M be a $k \times k$ matrix over $\mathbb{F}_q$ and let $\mathbf{v}_0 \in \mathbb{F}_q^k$, $\mathbf{v}_0 \neq (0, \ldots, 0)$. For $i \geq 1$, define $\mathbf{v}_i = M\mathbf{v}_{i-1}$. Then the sequence $\mathbf{v}_0, \mathbf{v}_1, \ldots$ satisfies the recurrence*

$$\mathbf{v}_{n+l} = c_{l-1}\mathbf{v}_{n+l-1} + c_{l-2}\mathbf{v}_{n+l-2} + \cdots + c_0\mathbf{v}_n$$

for all $n = 0, 1, \ldots$, where $f(x) = x^l - c_{l-1}x^{l-1} - c_{l-2}x^{l-2} - \cdots - c_0$ is the minimal polynomial for $\mathbf{v}_0$.

Proof : Since $f(x)$ is the minimal polynomial for $\mathbf{v}_0$, we have $f(M)\mathbf{v}_0 = 0$. Thus

$$\begin{aligned}
\mathbf{v}_{n+l} - (c_{l-1}\mathbf{v}_{n+l-1} + \cdots + c_0\mathbf{v}_n) &= M^{n+l}\mathbf{v}_0 - \left(c_{l-1}M^{n+l-1}\mathbf{v}_0 + \cdots + c_0M^n\mathbf{v}_0\right) \\
&= M^n\left(M^l - \left(c_{l-1}M^{l-1} + \cdots + c_0I_k\right)\right)\mathbf{v}_0 \\
&= M^n f(M)\mathbf{v}_0 \\
&= 0
\end{aligned}$$

■

3 Cellular Automata

There are two ways of looking at the evolution of a CA over time $t \geq 0$. One can study the evolution of the state vector C^t or the evolution of the individual cells C_i^t. The two evolutions are connected.

If the STM M is non singular then it is not difficult to see that the sequence of vectors $C^0, C^1, \ldots$ is periodic. Since each C_i is in $\mathbb{F}_q^k$ and M is a linear transformation of $\mathbb{F}_q^k$ into itself, the maximum possible period is $q^k - 1$. The actual length of the period depends upon the initial vector C^0. For example, if $C^0 = (0, \ldots, 0)$, then the period of the sequence $C^0, C^1, \ldots$ is 0. On the other hand, different non zero values for C^0 may lead to different values of the period. By the period of a CA $\mathcal{C}$ we mean the maximum possible period for the sequence $C^0, C^1, \ldots$ where the maximum is taken over all possible values of C^0.

Theorem 3.1 *If a k-cell CA $\mathcal{C}$ over $\mathbb{F}_q$ has period $q^k - 1$, then the constants l_i and u_j defined in Equation (2) must all be non zero.*

Proof : Suppose the l_i's and u_j's are not all non zero. Then either some l_i is zero or some u_j is zero. We consider only the first case, the other being similar. Let r be such that $2 \leq r \leq k$ and $l_r = 0$. Write $C = (C_1, \ldots, C_{r-1}, C_r, \ldots, C_k)$ and consider the cells $(C_1, \ldots, C_{r-1})$ to be $\mathcal{C}_1$ and the cells $(C_r, \ldots, C_k)$ to be $\mathcal{C}_2$. Since $l_r = 0$, the evolution of $\mathcal{C}_1$ has no effect on the evolution of $\mathcal{C}_2$. This implies that the maximum possible period for $\mathcal{C}_2$ is $q^{k-r+1} - 1$. On the other hand, the evolution of $\mathcal{C}_2$ can possibly influence $\mathcal{C}_1$. Hence the maximum possible period for $\mathcal{C}_1$ is q^{r-1}. Thus the maximum possible period for $\mathcal{C}$ is $q^{r-1}(q^{k-r+1} - 1) = q^k - q^{r-1} \leq q^k - q < q^k - 1$. This contradicts the fact that the period of $\mathcal{C}$ is $q^k - 1$. ∎

We will be interested in CA with maximum period and hence in light of Theorem 3.1, we will henceforth assume $l_i = u_j = 1$ for all $2 \leq i \leq n$ and $1 \leq j \leq n - 1$. Then the matrix M becomes a tridiagonal matrix with both the lower and upper sub diagonal equal to 1. If $q = 2$, such a CA is called a 90/150 CA [9]. Following this convention we will call such a CA a 90/150 CA, even if $q > 2$. Interestingly, for 90/150 CA and $q = 2$, the set of strings $a_1 \ldots a_n$ which makes the matrix M non singular turns out to be a regular set. See [7] for a proof of this fact and also an exact enumeration of the set of such "reversible" strings.

Theorem 3.2 *Let $\mathcal{C}$ be a k-cell 90/150 CA over $\mathbb{F}_q$ having STM M. Then the minimal polynomial of M is equal to the characteristic polynomial of M.*

Proof : Let $f(x)$ be the characteristic polynomial of M. From the Cayley-Hamilton theorem we know that the matrix M satisfies $f(x)$. We show that M cannot satisfy any polynomial of lesser degree. Let M^r_{ij} be the i,jth entry of the matrix M^r. Then it is easy to prove by induction that $M^r_{1,r+1} = 1$ for $1 \leq r \leq k - 1$ and $M^r_{1,j} = 0$ for $j > r + 1$. Let $p(x)$ be a polynomial of degree $l < k$. By the observation above, $M^l_{1,l+1} = 1$ and $M^j_{1,l+1} = 0$ for $j < l$. But then the $(1, l + 1)$th entry of $p(M)$ is non zero and hence $p(M) \neq 0$. ∎

If $f(x)$ is the characteristic (resp. minimal) polynomial of the STM M of a CA $\mathcal{C}$, then we will simply say that $\mathcal{C}$ has characteristic (resp. minimal) polynomial $f(x)$. From Theorem 2.2 we obtain the following result.

Theorem 3.3 *Let $\mathcal{C}$ be a k-cell CA over $\mathbb{F}_q$. Then $\mathcal{C}$ has period $q^k - 1$ iff the characteristic polynomial $f(x)$ of $\mathcal{C}$ is primitive.*

4 Cellular Automata Sequences

In this section we concentrate on the study of the sequence C_i^t of a particular cell of a CA. The first result establishes the connection between C^t and C_i^t.

Theorem 4.1 *Let $\mathcal{C}$ be a k-cell CA over $\mathbb{F}_q$ and $C^0 \neq (0, \ldots, 0)$ be the initial configuration of $\mathcal{C}$. Let the minimal polynomial of C_0 be $f(x)$. Then for all $1 \leq i \leq k$, the sequence C_i^t is a HLRS(q, k) whose characteristic polynomial is $f(x)$.*

Proof : Using Theorem 2.3 we obtain the fact that the sequence C^t satisfies a linear recurrence whose characteristic polynomial is $f(x)$. Since $C^t = (C_1^t, \ldots, C_k^t)$, this implies that each of the sequences C_i^t also satisfies the same recurrence. ∎

We now concentrate on 90/150 k-cell CA $\mathcal{C}$ over $\mathbb{F}_q$ having period $q^k - 1$. Theorems 3.2 and 3.3 imply that

- the minimal polynomial of $\mathcal{C}$ is equal to the characteristic polynomial $f(x)$ of $\mathcal{C}$ and
- $f(x)$ is primitive.

Further, Theorem 4.1 shows that the sequence of values of any cell of $\mathcal{C}$ is a HLRS(q, k) with characteristic polynomial $f(x)$.

Theorem 4.2 *Let $\mathcal{C}$ be a k-cell 90/150 CA over $\mathbb{F}_q$ with primitive characteristic polynomial and $C^0 \neq (0, \ldots, 0)$. Then for any $1 \leq i < j \leq k$, there exists an integer r such that $C_j^{t+r} = C_i^t$ for all $t \geq 0$.*

Proof : Let $f(x)$ be the characteristic polynomial of $\mathcal{C}$. Since $f(x)$ is primitive, the minimal polynomial of C^0 is also $f(x)$. Hence by Theorem 4.1, both the sequences C_i^t and C_j^t are HLRS(q, k) with characteristic polynomial $f(x)$. Using Theorem 2.1, we obtain that the periods of C_i^t and C_j^t are $q^k - 1$. Let $W = (C_i^0, \ldots, C_i^{k-1})$. Using Proposition 2.1 we get that there exists a minimum r such that $W = (C_j^r, \ldots, C_j^{r+k-1})$. Since both C_i^t and C_j^t satisfy the same kth order recurrence this immediately implies that $C_j^{r+t} = C_i^t$ for all $t \geq 0$. ∎

Remark : Note that if the characteristic polynomial of $\mathcal{C}$ is not primitive, then it is not clear that in general C_j^t can be obtained by shifting C_i^t.

Thus when $f(x)$ is primitive, for any $1 \leq i < j \leq k$, the sequence C_j^t can be obtained from the sequence C_i^t by shifting the sequence C_i^t a certain number of places to the right. We are interested in the shifts between C_i^t and C_j^t. For that it is sufficient to consider the shifts of C_i^t, $2 \leq i \leq k$ with respect to C_1^t.

Let $G(x)$ be the generating function for the sequence C_1^t. From Equation (7) we get

$$G(x) = \frac{g(x)}{f^*(x)} \tag{8}$$

where $f^*(x)$ is the reciprocal polynomial of $f(x)$. For $1 \leq i \leq k$, define

$$P_i(x) = C_i^0 + C_i^1 x + C_i^2 x^2 + \cdots + C_i^{q^k-2} x^{q^k-2}. \tag{9}$$

Let $P(x) = P_1(x)$. We first relate the polynomial $P(x)$ to $G(x)$.

$$\begin{aligned} G(x) &= C_1^0 + C_1^1 x + C_1^2 x^2 + \ldots + C_1^{q^k-2} x^{q^k-2} + C_1^{q^k-1} x^{q^k-1} + C_1^{q^k} x^{q^k} + \ldots \\ &= P_1(x) + x^{q^k-1} P_1(x) + x^{2(q^k-1)} P_1(x) + \ldots \\ &= P(x)(1 + x^{q^k-1} + x^{2(q^k-1)} + x^{3(q^k-1)} + \cdots) \\ &= \frac{P(x)}{1 - x^{q^k-1}}. \end{aligned} \tag{10}$$

Here we use the fact that the period of C_1^t is $q^k - 1$ and hence $C_1^t = C_1^{q^k-1+t}$ for all $t \geq 0$. Combining Equations (8) and (10) we get

$$\frac{P(x)}{1 - x^{q^k-1}} = \frac{g(x)}{f^*(x)}. \tag{11}$$

Using Theorem 4.2, we can define integers $j_1 = 0, j_2, \ldots, j_k$ such that

$$P_i(x) = x^{j_i} P(x) \pmod{1 - x^{q^k-1}} \tag{12}$$

The integers $j_2, \ldots, j_k$ are the relative shifts of $C_2^t, \ldots, C_k^t$ with respect to C_1^t. The following result is important in obtaining an algorithm to compute $j_2, \ldots, j_k$.

Theorem 4.3 *Let $\mathcal{C}$ be a 90/150 k-cell CA over $\mathbb{F}_q$ with characteristic i polynomial $f(x)$ which is primitive over $\mathbb{F}_q$. Then*

$$\begin{array}{rcccll} & & x^{j_i}(xa_i - 1) + x^{j_{i+1}+1} & \equiv & 0 \bmod f^*(x) & \text{if } i = 1; \\ x^{j_{i-1}+1} & + & x^{j_i}(xa_i - 1) + x^{j_{i+1}+1} & \equiv & 0 \bmod f^*(x) & \text{if } 1 < i < k; \\ x^{j_{i-1}+1} & + & x^{j_i}(xa_i - 1) & \equiv & 0 \bmod f^*(x) & \text{if } i = k. \end{array} \tag{13}$$

Proof : From Equation (2) we obtain

$$\begin{array}{lcll} P_1(x) & \equiv & x\left(a_1 P_1(x) + P_2(x)\right) & \bmod(1 - x^{q^k-1}) \\ P_2(x) & \equiv & x\left(P_1(x) + a_2 P_2(x) + P_3(x)\right) & \bmod(1 - x^{q^k-1}) \\ \cdots & \cdots & \cdots & \cdots \\ P_{k-1}(x) & \equiv & x\left(P_{k-2}(x) + a_{k-1} P_{k-2}(x) + P_k(x)\right) & \bmod(1 - x^{q^k-1}) \\ P_k(x) & \equiv & x\left(P_{k-1}(x) + a_k P_k(x)\right) & \bmod(1 - x^{q^k-1}) \end{array}$$

Let $P = (P_1(x), \ldots, P_k(x))$. Then the above equations can be represented as

$$xMP^T \equiv P^T \bmod (1 - x^{q^k-1})$$

where P^T is the transpose of P and M is the STM of $\mathcal{C}$. This gives

$$(xM - I_k)\, P^T \equiv 0 \bmod (1 - x^{q^k-1}).$$

Now $P = (P_1(x), \ldots, P_k(x)) = (x^{j_1}P(x), \ldots, x^{j_k}P(x)) = (x^{j_1}, \ldots, x^{j_k})P(x)$. Thus we can write

$$(xM - I_k)\,(x^{j_1}, \ldots, x^{j_k})^T P(x) \equiv 0 \bmod (1 - x^{q^k-1}).$$

Thus there exists polynomials $p_1(x), \ldots, p_k(x)$ such that

$$(xM - I_k)\,(x^{j_1}, \ldots, x^{j_k})^T P(x) = (p_1(x), \ldots, p_k(x))^T (1 - x^{q^k-1}).$$

This gives

$$(xM - I_k)\,(x^{j_1}, \ldots, x^{j_k})^T \frac{P(x)}{(1 - x^{q^k-1})} = (p_1(x), \ldots, p_k(x))^T.$$

Using Equation (11), we get

$$(xM - I_k)\,(x^{j_1}, \ldots, x^{j_k})^T \frac{g(x)}{f^*(x)} = (p_1(x), \ldots, p_k(x))^t.$$

From this we obtain

$$(xM - I_k)\,(x^{j_1}, \ldots, x^{j_k})^T g(x) \equiv 0 \bmod f^*(x).$$

Since $f(x)$ is primitive, so is $f^*(x)$. The degree of $g(x)$ is less than k and hence $g(x)$ has a unique inverse $e(x)$ modulo $f^*(x)$. Multiplying both sides by $e(x)$ we obtain

$$(xM - I_k)\,(x^{j_1}, \ldots, x^{j_k})^T \equiv 0 \bmod f^*(x).$$

Expanding the matrix congruence we obtain the required result. ■

5 Algorithm to Compute Shifts

Based on Theorem 4.3 we now develop an algorithm to compute the shifts in a given CA. We will be working over $\mathbb{F}_q$ and modulo $f^*(x)$, which is primitive of degree k over $\mathbb{F}_q$. The Equations in (13) have to be solved for $j_2, \ldots, j_k$. Since $f^*(x)$ is primitive, the polynomials $x^i \bmod f^*(x)$ are all distinct for $0 \le i \le q^k - 2$. In fact these polynomials form the multiplicative group of the finite field $\mathbb{F}_{q^k}$. Thus given any non zero polynomial $p(x)$ of degree at most $k-1$, there is a unique i (modulo $q^k - 1$) such that $p(x) \equiv x^i \bmod f^*(x)$. A close inspection of the Equations in (13) reveal that we will have to repeatedly solve equations of this kind. For this we need an explicit representation of the finite field $\mathbb{F}_{q^k}$ modulo $f^*(x)$. In fact, we will use two representations of this field as we explain below.

Let $pow[0, \ldots, q^k - 2]$ be an array of length $q^k - 1$ such that $pow[i] \equiv x^i \bmod f^*(x)$. Given i, this will allow us to retrieve the polynomial $x^i \bmod f^*(x)$ in constant time. However, we also want to do the converse, i.e., given a non zero polynomial $p(x)$ of degree at most $k-1$, we want to find the unique integer i (modulo $q^k - 1$) such that $p(x) \equiv x^i \bmod f^*(x)$. Let $\sigma : \mathbb{F}_q \to \{0, \ldots, q-1\}$ be a bijection. Then given any polynomial $p(x)$ of degree at most $k-1$, it can be uniquely coded by an integer in the set $\{0, \ldots, q^k - 1\}$ as follows. Let $p(x) = c_{k-1}x^{k-1} + \ldots + c_1 x + c_0$. Then $\sigma(p(x)) = \sigma(c_{k-1})q^{k-1} + \ldots + \sigma(c_1)q + \sigma(c_0)$. Conversely, given any integer i in the set $\{0, \ldots, q^k - 1\}$, there is a unique polynomial $p(x)$, denoted by $\sigma^{-1}(i)$ such that $\sigma(p(x)) = i$. We define an array $rev[1, \ldots, q^k - 1]$, where $\sigma^{-1}(i) \equiv x^{rev[i]} \bmod f^*(x)$, $1 \le i \le q^k - 1$. The arrays $pow[]$ and $rev[]$ can be constructed simultaneously as follows.

1. $temp = 1$, $pow[0] = 1$, $rev[\sigma(1)] = 0$.
2. for $i = 1$ to $q^k - 2$ do
   - $temp = x * temp \pmod{f^*(x)}$.
   - $pow[i] = temp$.
   - $rev[\sigma(temp)] = i$.
3. end do

The time taken to prepare the arrays is $O(kq^k)$. This is the most time consuming part of the entire algorithm. We now present the algorithm to compute the numbers $j_2, \ldots, j_k$.

1. input: (1) the string $(a_1, \ldots, a_k)$ and (2) the polynomial $f^*(x)$.
2. $j_1 = 0$, $j_2 = rev[\sigma(xa_1 - 1)] - 1$.
3. for $i = 2$ to $k - 1$ do
   - $t_1(x) = pow[j_{i-1} + 1]$, $t_2(x) = (xa_i - 1) * pow[j_i] \pmod{f^*(x)}$.
   - $t(x) = t_1(x) + t_2(x) \pmod{f^*(x)}$.
   - $j_{i+1} = rev[\sigma(t(x))] - 1$.
4. end do

The correctness of the algorithm follows from Theorem 4.3 and the time taken by the algorithm is $O(k^2)$. Thus the total time taken to prepare the arrays and find all the shifts is $O(kq^k + k^2)$. The total storage space required is $O(kq^k)$.

6 Concluding Remarks

When $q = 2$, it is possible to obtain the string $a_1 \ldots a_k$ from the polynomial $f(x)$. An algorithm to do this was described by Tezuka and Fushimi [8] based on a result by Mesirov and Sweet [5]. Given a degree k irreducible polynomial $f(x)$ over $\mathbb{F}_2$, there are at most 2 distinct k-cell CA whose characteristic polynomial is $f(x)$. The two CA are described by either the string $a_1 \ldots a_k$ or the string $a_k \ldots a_1$.

We have implemented the algorithm by Tezuka and Fushimi [8] and the algorithm in Section 4. Thus given a primitive polynomial $f(x)$ of degree k over $\mathbb{F}_2$, we obtain the k-cell CA and then compute the shifts of the output sequences of the cells. We provide an example of a 16 degree primitive polynomial over $\mathbb{F}_2$.

Example : Let $f(x) = x^{16} + x^5 + x^3 + x^2 + 1$. The algorithm of Tezuka and Fushimi [8] determines the values of $a_1 \ldots a_{16}$ to be either 0001001001111000 or 0001111001001000. The values of the shifts (i.e. $j_1, \ldots, j_{16}$) in the first case are the following. (In the second case, the shifts are simply obtained by reading the values in the opposite direction.)

0,65534,8108,65532,3385,48804,56397,3945,43509,63038,208,4960, 1572,9683,1574,1575.

Note that the shifts appear to be quite random which is considered to be good for BIST applications. The period of all the sequences $C^t_1, \ldots, C^t_{16}$ is $2^{16} - 1 = 65535$. Hence a shift of 65532 can be thought of as a shift of 3 in the reverse direction. Thus shifts with values near the middle are actually exponential sized shifts. For example the shift of size 43509 is an exponential sized shift. ■

In an earlier work, Bardell [1] had provided an example of computing shifts in 90/150 CA sequences over $\mathbb{F}_2$. In Bardell's example a 6-cell 90/150 CA with $a_1 \ldots a_6 = 100000$ was considered. The characteristic polynomial is $f(x) = x^6+x^5+x^4+x+1$ which is primitive over $\mathbb{F}_2$. The shifts were computed to be $0, 39, 35, 47, 33, 32$. On the other hand, the values of the shifts computed for Bardell's example by our algorithm is $0, 24, 28, 16, 30, 31$. Note that from the second shift onward the sum of Bardell's shift and our shift is equal to $63 = 2^6 - 1$, which is equal to the period of the sequences. Thus Bardell's shifts and our shifts are actually obtained in opposite directions. The reason for this is the following. In the computation, Bardell works modulo $f(x)$, whereas we work modulo $f^*(x)$. From Proposition 2.2, we know that if $f(x)$ is the characteristic polynomial of $s_0, s_1, \ldots, s_{2^k-1}, \ldots$, then the characteristic polynomial of the sequence $s_{2^k-1}, \ldots, s_1, s_0, s_{2^k-1}, \ldots, s_1, s_0, \ldots$ is $f^*(x)$. This explains why Bardell obtained the reverse shifts. The difference is minor, but the use of reciprocal polynomial comes out very naturally from the algebraic theory that we have developed. We note that no such theory was provided in [1].

To the best of our knowledge, no CA design algorithm is known for $q > 2$. This question is connected to the orthogonal multiplicity of polynomials in fields $\mathbb{F}_q$ with $q \neq 2$ (see [3]). Computational results from [3] suggest that for each degree k primitive polynomial $f(x)$ over $\mathbb{F}_q$ it is possible to construct a CA whose characteristic polynomial is $f(x)$. It is not clear that such a CA will necessarily be a 90/150 CA as we have defined. However, the u_i's and the l_j's in Equation (2) must necessarily be non zero (see Theorem 3.1). We conjecture that for given a primitive polynomial $f(x)$ over $\mathbb{F}_q$, it is in fact possible to construct a 90/150 CA having $f(x)$ as its characteristic polynomial.

Acknowledgement : The author wishes to thank Kishan Chand Gupta for carefully reading an initial draft of the paper and pointing out several typos.

References

[1] P. H. Bardell. Analysis of cellular automata used as pesudorandom pattern generators. *Proceedings of International Test Conference*, 1990, 762-768.

[2] R. Barua, personal communication.

[3] S. R. Blackburn. Orthogonal sequences of polynomials over arbitrary fields. *Journal of Number Theory*, 68, 99-111 (1998).

[4] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, revised edition, 1994.

[5] J. P. Mesirov and M. M. Sweet. Continued fraction expansions of rational expressions for built-in self-test. *Journal of Number Theory*, 27, 144-148 (1987).

[6] P. Sarkar. A brief history of cellular automata. *ACM Computing Surveys*, 32(1), 80-107, (2000).

[7] P. Sarkar and R. Barua. The set of reversible 90/150 cellular automata is regular. *Discrete Applied Mathematics*, 84 (1-3), 199-213 (1998).

[8] S. Tezuka and M. Fushimi. A method of designing cellular automata as pseudo random number generators for built-in self-test for VLSI. In *Finite Fields: Theory, Applications and Algorithms*, Contemporary Mathematics, AMS, pages 363–367, 1994.

[9] S. Wolfram. Statistical Mechanics of cellular automata. Rev. Modern Physics 55, 601-644 (1983).