Synthesis of all Maximum Length Cellular Automata of Cell Size up to 12

Jaydeb Bhaumik
Haldia Institute of Technology, Haldia-721657, India

Abstract. Maximum length CA has wide range of applications in design of linear block code, cryptographic primitives and VLSI testing particularly in Built-In-Self-Test. In this paper, an algorithm to compute all $n$-cell maximum length CA-rule vectors is proposed. Also rule vectors for each primitive polynomial in $GF(2^n)$ to $GF(2^{12})$ have been computed by simulation and they have been listed. Programmable rule vectors based maximum length CA can be used to design cryptographic primitives.

Keyword Linear hybrid maximum length CA, Rule vectors, primitive polynomial

1 Introduction

A Cellular Automata (CA) consist of a number of cells arranged in a regular manner. Each cell consists of a storage element (D flip-flop) and a combinational logic implementing the next-state function. CA is universally accepted as a very good generator of pseudo random sequences. It is also very well suited for VLSI design due to its regular structure. If the combinational logic of a CA cell only involves XOR logic, then it is called a linear CA. For a three neighborhood one dimensional CA, the combinational logic implementing the next state is $s_i(t + 1) = f(s_{i-1}(t), s_i(t), s_{i+1}(t))$. Where $s_i(t)$ is the output state of the $i$th cell at $t$th time step. $s_{i-1}(t)$ and $s_{i+1}(t)$ are the output states of left and right neighbors of $i$th cell and $f$ denotes the local transition function realized with a combinational logic and is known as a rule of the CA. A CA is said to be hybrid if the rules of different cells vary. An $n$-cell maximum length CA is characterized by the presence of a cycle of length $2^n - 1$ with all non-zero states. In case of a maximum length CA, it has a characteristic polynomial which is primitive. CA-rules 90 and 150 have been considered. The combinational logic for rule 90 and rule 150 are as follows.

Rule 90 : $s_i(t + 1) = s_{i-1}(t) \oplus s_{i+1}(t)$
Rule 150 : $s_i(t + 1) = s_{i-1}(t) \oplus s_i(t) \oplus s_{i+1}(t)$
where $s_i(t)$ is the output state of the $i$th cell at time $t$.

Efficient characterization of 1D CA based on matrix algebra and its application in error correcting codes, cryptography and VLSI testing is available in [3]. The characteristic matrix of a linear CA operating over $GF(2)$ is a matrix
that describes the behavior of the CA. We can calculate the next state of the
CA by multiplying the characteristic matrix by the present state of the CA. A
characteristic matrix is constructed as: $T[i,j] = 1$, if the next state of the
$i_{th}$
cell depends on the $j_{th}$ cell and $T[i,j] = 0$, otherwise.

Only one rule vector for each $n$-length CA has been provided in [3]. A new
architectural design of CA-based codec based on linear maximum length CA
has been proposed in [5]. In [2] authors proposed an algorithm for determining
minimal cost $n$-cell maximum length CA of degree up to 500. Programmable rule
vectors based linear maximum length CA has many applications in the design of
cryptographic primitives. In [4] one such application has been mentioned, where
programmable linear maximum length CA has been used to design an integrated
scheme for both error correction and message authentication. Therefore, designer
needs list of maximum length CA-rule vectors for a particular cell size.

2 Method and Result

The algorithm of determining whether a given $n$- cell CA has a maximum length
cycle is as follows.

1. Take $n \times n$ tridiagonal matrix with all non-zero elements are 1
2. Change main diagonal sequentially by one of the $2^n$ combinations
3. Compute the characteristic polynomial corresponding to the $n \times n$ con-
   structed matrix
4. Calculate the number of non-zero coefficient in the characteristic polynomial
   and if number of coefficients is even then go to step 2
5. Check the coefficients of $x^n$ and $x^0$, if they are zeros then go to step 2.
6. Check if the characteristic polynomial matches with any one of the list of
   primitive polynomials.
7. If matches then corresponding main diagonal of the matrix represents the
   maximum length CA-rule vector

In Table under the caption 'CA-rule vector', ‘0’ and ‘1’ correspond to rule
90 and 150 respectively. Under caption 'Primitive poly.' the entries represent
primitive polynomial in binary format. It has been observed that mirror image
each rule vector corresponds to same primitive polynomial. For example in
8-cell CA, 00000110 and 01100000 are two rule vectors for primitive polynomial
$x^8 + x^4 + x^3 + x^2 + 1$ (100011101), where rule vectors are mirror image of each
other.
| # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|
| 2       | 111            | 10             |
| 3       | 1011, 110      | 100            |
| 4       | 10011, 1010    |                |
| 5       | 100101, 11100  | 10000          |
| 6       | 1000011, 000110| 101111         |
| 7       | 10000011, 1011001| 01110110     |
|         | 10001001, 0111010| 0011011110   |
|         | 10001111, 1110001| 0001101111   |
|         | 10010001, 1110100| 0101000111   |
|         | 10010111, 1110000| 0010011111   |
|         | 11000001, 0010000| 1110111111   |
|         | 11001011, 1011011| 0101111110   |
|         | 11010011, 1111101| 0000111110   |
|         | 11100001, 1001101| 1010111111   |
|         | 11110111, 0011110| 1011001111   |
|         | 11111101, 0100110| 0110101111   |

| # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|
| 8       | 100011101, 0000110|           |
|         | 100101011, 0101111|           |
|         | 100101101, 0111011|           |
|         | 101001101, 0110110|           |
|         | 101011111, 1001001|           |
|         | 101000111, 0101110|           |
|         | 110101101, 0111001|           |
|         | 110100101, 1111001|           |
|         | 110101011, 1111001|           |
|         | 11100011, 1001011|           |
|         | 11111011, 0011110|           |
|         | 11111101, 0100111|           |
| # cells | Primitive Poly. | CA-rule vector | # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|---------|----------------|----------------|
| 9       | 1011010001     | 0100000001     | 10      | 10001101111    | 0001000010     |
|         | 1011011101     | 1010111110     |         | 10010000001    | 0001111111     |
|         | 1011110101     | 0011110011     |         | 10010001011    | 0111010001     |
|         | 1100010011     | 0110000110     |         | 10011000101    | 0001111101     |
|         | 1100010101     | 1000110011     |         | 10011101011    | 0011011111     |
|         | 1100011111     | 1000101111     |         | 10011110011    | 0100011111     |
|         | 1100100011     | 1100101011     |         | 10011110011    | 0100011111     |
|         | 1100110011     | 0111010001     |         | 10100001101    | 0101100001     |
|         | 1100111111     | 0101111001     |         | 10100011001    | 0101000110     |
|         | 1101001101     | 0110100011     |         | 10100100011    | 0010100110     |
|         | 1101100011     | 0001011111     |         | 10100110011    | 0011010110     |
|         | 1101110011     | 0000101111     |         | 10100111111    | 1111111101     |
|         | 1110001011     | 0000001111     |         | 10100111111    | 1111111101     |
|         | 1110011101     | 0001000110     |         | 10111000111    | 1000010110     |
|         | 1110100011     | 0000101110     |         | 10111011011    | 1000010110     |
|         | 1110110011     | 0100001001     |         | 10111010111    | 1000010110     |
|         | 1111000101     | 0010011010     |         | 10111100111    | 1100000001     |
|         | 1111010011     | 1001111111     |         | 1100000001     | 0001010110     |
|         | 1111100011     | 0000100010     |         | 11000001011    | 0001010110     |
|         | 1111110011     | 0000011110     |         | 11000010101    | 0001010110     |
|         | 1111111011     | 1001101111     |         | 11000101011    | 1100000001     |
|         | 1111111111     | 1001000001     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
|         | 1111111111     | 0000100010     |         | 11001001011    | 0001010110     |
| # cells | Primitive Poly | CA-rule vector |
|---------|----------------|----------------|
| 10      | 11010110101    | 10111011110    |
|         | 11011000010    | 10000101100    |
|         | 11011010011    | 00110111111    |
|         | 11011011111    | 01100100010    |
|         | 11011111101    | 01111100111    |
|         | 11100011011    | 00110001111    |
|         | 11100011101    | 00111000111    |
|         | 11101000001    | 11010010110    |
|         | 11100110001    | 01100001111    |
|         | 11101000111    | 11000101100    |
|         | 11101010011    | 00011011011    |
|         | 11101010101    | 00110110001    |
|         | 11101011001    | 01010001111    |
|         | 11101100011    | 11000111001    |
|         | 11101110011    | 00111000111    |
|         | 11101110111    | 01001001111    |
|         | 11101111001    | 01100010111    |
|         | 11101111101    | 01100010111    |
|         | 11101111111    | 01100010111    |
|         | 11101111111    | 01100010111    |
|         | 11101111111    | 01100010111    |
|         | 11101111111    | 01100010111    |
|         | 11101111111    | 01100010111    |
| 11      | 10001000011    | 10111001111    |
|         | 10001000101    | 10010101101    |
|         | 10001000111    | 10111001111    |
|         | 10001010011    | 01100010101    |
|         | 10001010101    | 01100010101    |
|         | 10001011001    | 00110100010    |
|         | 10001011011    | 01001001111    |
|         | 10001011101    | 01100010111    |
|         | 10001011111    | 01100010111    |
|         | 10001011111    | 01100010111    |
|         | 10001011111    | 01100010111    |
|         | 10001011111    | 01100010111    |
|         | 10001011111    | 01100010111    |
|         | 10001011111    | 01100010111    |
|         | 10001011111    | 01100010111    |
| # cells | Primitive Poly. | CA-rule vector | # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|---------|----------------|----------------|
| 11      | 101001101101   | 00110101110    | 11      | 1011110011101  | 00110101111    |
|         | 101011111111   | 00110111100    |         | 101111101101   | 00110111111    |
|         | 101110001101   | 00110111100    |         | 101111101101   | 00110111111    |
|         | 101010010001   | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
|         | 10110101101    | 01101101100    |         | 101111101101   | 00110111111    |
| # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|---------------|
| 11      | 110101011001   | 01001011001   |
|         | 110101100011   | 001010011011 |
|         | 110101101111   | 011110010011 |
|         | 110101110001   | 101110100010 |
|         | 110110100011   | 000011010110 |
|         | 110110101111   | 000010110111 |
|         | 110110110011   | 001011001011 |
|         | 110110111011   | 001000110111 |
|         | 110110111111   | 000010101111 |
|         | 110111001001   | 001011100110 |
|         | 110111010111   | 011110100011 |
|         | 110111101101   | 011110011111 |
|         | 110111100001   | 011110011011 |
|         | 110111110111   | 011110011011 |
|         | 111000000010   | 100001000010 |
|         | 111000011101   | 001100111111 |
|         | 111001000001   | 011011001011 |
|         | 111001001001   | 001111011011 |
|         | 111001101011   | 001111011111 |
|         | 111001101101   | 001111011111 |
|         | 111001101111   | 001111011111 |
|         | 111010010001   | 111000000011 |
|         | 111010100010   | 101110011011 |
|         | 111010101001   | 111000000011 |
|         | 111010110101   | 111000000011 |
|         | 111010111001   | 111000000011 |
|         | 111010111101   | 111000000011 |
|         | 111011001001   | 111000000011 |
|         | 111011010001   | 111000000011 |
|         | 111011011001   | 111000000011 |
|         | 111011011101   | 111000000011 |
|         | 111011100001   | 111000000011 |
|         | 111011101001   | 111000000011 |
|         | 111011110001   | 111000000011 |
|         | 1111000010001  | 111000000011 |
|         | 111100010001   | 111000000011 |
|         | 111100011001   | 111000000011 |
|         | 111100011101   | 111000000011 |
|         | 111100100001   | 111000000011 |
|         | 111100101001   | 111000000011 |
|         | 111100110001   | 111000000011 |
|         | 111100111001   | 111000000011 |
|         | 111100111101   | 111000000011 |
|         | 111101000001   | 111000000011 |
|         | 111101001001   | 111000000011 |
|         | 111101010001   | 111000000011 |
|         | 111101011001   | 111000000011 |
|         | 111101100001   | 111000000011 |
|         | 111101101001   | 111000000011 |
|         | 111101110001   | 111000000011 |
|         | 111101111001   | 111000000011 |
|         | 111110000001   | 111000000011 |
|         | 111110001001   | 111000000011 |
|         | 111110010001   | 111000000011 |
|         | 111110011001   | 111000000011 |
|         | 111110100001   | 111000000011 |
|         | 111110101001   | 111000000011 |
|         | 111110110001   | 111000000011 |
|         | 111110111001   | 111000000011 |
|         | 111111000001   | 111000000011 |
|         | 111111001001   | 111000000011 |
|         | 111111010001   | 111000000011 |
|         | 111111100001   | 111000000011 |
|         | 111111101001   | 111000000011 |
|         | 111111110001   | 111000000011 |
| # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|
| 12      | 10000011010011 | 011011000110   |
|         | 10000011010011 | 10011100100101 |
|         | 10000011110111 | 01101001101001 |
|         | 10000011010011 | 00000110001001 |
|         | 10000110100011 | 01010010100101 |
|         | 10000110100011 | 00110100100110 |
|         | 10000111010111 | 00111010100110 |
|         | 10000111010111 | 11010110100110 |
|         | 10000111110111 | 11101010100110 |
|         | 10000111110111 | 11110100100110 |
|         | 10001000001111 | 10101010100110 |
|         | 10001001110011 | 10011001100110 |
|         | 10001010011111 | 00010110100110 |
|         | 10001010110111 | 11011010100110 |
|         | 10001011010111 | 01101001100110 |
|         | 10001011110111 | 00110110100110 |
|         | 10001100001111 | 11011010100110 |
|         | 10001101110011 | 10011001100110 |
|         | 10001110110111 | 00010110100110 |
|         | 10001110110111 | 11011010100110 |
|         | 10001111110111 | 11101010100110 |
|         | 10010000001111 | 10101010100110 |
|         | 10010010011011 | 00010110100110 |
|         | 10010011110111 | 00110110100110 |
|         | 10010100001111 | 11011010100110 |
|         | 10010110110111 | 01101001100110 |
|         | 10010111010111 | 00110110100110 |
|         | 10010111110111 | 11101010100110 |
|         | 10011000110111 | 00010110100110 |
|         | 10011010011011 | 00010110100110 |
|         | 10011011110111 | 00110110100110 |
|         | 10011100011011 | 11011010100110 |
|         | 10011110110111 | 00010110100110 |
|         | 10011111110111 | 11101010100110 |

| # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|
| 12      | 10011001000101 | 001000111101   |
|         | 10011001000101 | 10011001100110 |
|         | 10011001100110 | 00010110100110 |
|         | 10011001100110 | 11101010100110 |
|         | 10011001111010 | 01110110100110 |
|         | 10011001111010 | 10011001100110 |
|         | 10011010000110 | 00100011110110 |
|         | 10011010000110 | 10011001100110 |
|         | 10011010100110 | 00010110100110 |
|         | 10011010100110 | 11101010100110 |
|         | 10011010110110 | 00010110100110 |
|         | 10011010110110 | 11101010100110 |
|         | 10011010110110 | 00010110100110 |
|         | 10011010110110 | 11101010100110 |
|         | 10011011000110 | 00010110100110 |
|         | 10011011000110 | 11101010100110 |
|         | 10011011000110 | 00010110100110 |
|         | 10011011000110 | 11101010100110 |
|         | 10011011010110 | 00010110100110 |
|         | 10011011010110 | 11101010100110 |
|         | 10011011010110 | 00010110100110 |
|         | 10011011010110 | 11101010100110 |
| # cells | Primitive Poly. | CA-rule vector | # cells | Primitive Poly. | CA-rule vector |
|---------|----------------|----------------|---------|----------------|----------------|
| 12      | 1011101111111 | 010010010001   | 12      | 1101110101011 | 010110101011   |
|         | 1011110000001 | 011100000001   |         | 1110000000101 | 000000111111   |
|         | 1100001011011 | 1001110010101  |         | 1110000010001 | 001100010111   |
|         | 1100001111011 | 1110101010011  |         | 1110000101111 | 001111111111   |
|         | 1100001010001 | 000101000010   |         | 1110000100111 | 010101100011   |
|         | 1100001011011 | 000100010101   |         | 1110000101011 | 010101001011   |
|         | 1100001110001 | 001100000101   |         | 1110010000111 | 001110010011   |
|         | 1100001110111 | 100000111111   |         | 1110010011111 | 000011111111   |
|         | 1100010011011 | 110001111001   |         | 1110010101011 | 001101001011   |
|         | 1100010011101 | 001111110101   |         | 1110010111101 | 000011111101   |
|         | 1100010100001 | 000000100110   |         | 1110010110101 | 001101000101   |
|         | 1100010101011 | 101111111111   |         | 1110010110011 | 001101100011   |
|         | 1100010110111 | 110100101111   |         | 1110010110111 | 001101100101   |
|         | 1100010111011 | 011010101111   |         | 1110010111001 | 001101101011   |
|         | 1100010111111 | 011011001011   |         | 1110010111111 | 001101101101   |
|         | 1100100011111 | 000011111111   |         | 1110011000111 | 001100011101   |
|         | 1100100110011 | 010111001001   |         | 1110011001001 | 110000001011   |
|         | 1100100110111 | 101010101101   |         | 1110011001101 | 001101001011   |
|         | 1100100111011 | 110010101111   |         | 1110011001111 | 001101001101   |
|         | 1100100111111 | 110100111111   |         | 1110011001001 | 001101001111   |
|         | 1100101010001 | 001111111010   |         | 1110011001111 | 001101001110   |
|         | 1100101011011 | 011001001111   |         | 1110011010001 | 001101001110   |
|         | 1100101011111 | 111010001111   |         | 1110011010101 | 001101010101   |
|         | 1100101110001 | 101011001011   |         | 1110011010111 | 001101010100   |
|         | 1100101110111 | 111010101111   |         | 1110011011001 | 001101010100   |
|         | 1100101111011 | 111010101111   |         | 1110011011101 | 001101010100   |
|         | 1100101111111 | 111010101111   |         | 1110011011111 | 001101010100   |

**Conclusion** In this paper a simple algorithm to compute rule vectors for \( n \)-cell maximum length CA has been introduced. Also, all maximum length CA rule vectors for cell size 2 to 12 have been computed by employing proposed algorithm and they have been tabulated. Programmable rule vectors based maximum length CA can be used to design cryptographic primitives. Since the list of all rule vectors are available so it will certainly reduce design cycle time.
References

1. B. Kar, S. Nandi, and P. P. Chaudhury, “Theory and application of cellular automata based cryptography,” *IEEE Transactions on Computers*, vol. 43, no. 12, pp. 1346-1357, Dec. 1994.

2. K. Cattell, S. Zhang, “Minimal Cost One-Dimensional Linear Hybrid Cellular Automata of Degree Through 500,” *Journal of electronic Testing: Theory and Application*, vol. 6, pp. 255-258, 1995.

3. P. P. Chaudhuri, D. Roy Chowdhury, S. Nandi and S. Chattopadhyay, Additive Cellular Automata: Theory and Applications, *IEEE Computer Society press*, California, USA, 1997.

4. J. Bhaumik and D. Roy Chowdhury, “An Integrated ECC-MAC Based on RS Code,” *Transactions on Computational Science*, vol. IV, LNCS 5430, pp. 117-135, Apr. 2009.

5. J. Bhaumik and D. Roy Chowdhury, “New Architectural Design of CA-Based Codec,” *IEEE Transactions on Very Large Scale Integration Systems*, vol. 18, no. 7, pp. 1139-1144, July 2010.