Two Dimensional Cellular Automata and Pseudorandom Sequence Generation

by

Umer Khayyam Sh
B.S., COMSATS Institute of Information Technology, 2015

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF APPLIED SCIENCE

in the Department of Electrical and Computer Engineering

Two Dimensional Cellular Automata and Pseudorandom Sequence Generation

by

Umer Khayyam Sh
B.S., COMSATS Institute of Information Technology, 2015

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Fayez Gebali, Departmental Member
(Department of Electrical and Computer Engineering)

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Fayez Gebali, Departmental Member
(Department of Electrical and Computer Engineering)

ABSTRACT

Maximum linear feedback shift registers (LFSRs) based on primitive polynomials are commonly used to generate maximum length sequences (m-sequences). An m-sequence is a pseudorandom sequence that exhibits ideal randomness properties like balance, run and autocorrelation but has low linear complexity. One-dimensional Cellular Automata (1D CA) have been used to generate m-sequences and pseudorandom sequences that have high linear complexity and good randomness. This thesis considers the use of two-dimensional Cellular Automata (2D CA) to generate m-sequences and psuedorandom sequences that have high linear complexity and good randomness. The properties of these sequences are compared with those of the corresponding m-sequences and the best sequences generated by 1D CAs.

Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

I am grateful to Allah who is the most merciful and my parents for their continuous support, love, prayers and motivation. I wish to express my sincere gratitude to my supervisor Dr. T. Aaron Gulliver whose guidance, expertise, flexibility and encouragement contributed greatly to my graduate studies. For successful completion of my thesis, his expertise and knowledge were essential. His flexibility allowed me to work remotely on my thesis while working part time in Ottawa at Ciena. I would also like to thank Smarak Acharya for his help during my thesis and my manager Shawn Brady for his support, encouragement and for making it possible for me to work as a part time employee in his team while I worked on my thesis. I am also thankful to the University of Victoria for graduate financial support and Compute Canada for providing computing resources that enabled me to generate the results for my thesis.

DEDICATION

To my parents, for their continuous support, love and prayers.

To my supervisor, Dr. T Aaron Gulliver for his constant support, guidance and flexibility.

Chapter 1

Introduction

Randomness can be defined as a series of events lacking a pattern or predictability and a number generated by such a process is called a random number. It has applications in many fields including gaming, gambling, sports and statistics. In gaming, it is used to fill areas on the screen with objects such as cars, people, and trees. Slot machines in casinos employ randomness to stop randomly when they are played. Random numbers are important in the field of cryptography [1]. An example of generating a random sequence of numbers is rolling a die multiple times. There are only two possible outcomes (heads or tails) if a coin is flipped. One of the outcomes can be considered a 1 and the other a 0 to generate a random binary sequence. Only binary sequences are considered in this thesis.

One way of generating a random sequence (infinite period) is with a hardware random-number generator (HRNG) [2]. They use physical phenomenon such as thermal noise or the photoelectric effect to generate random sequences. Digital circuits are used to produce sequences that appear statistically random [3], and are called pseudorandom sequences (finite period). Pseudorandom sequences are used in cryptographic applications to generate encryption and decryption keys. Pseudorandom sequences repeat after a certain period, but within a period they exhibit properties of statistical randomness similar to those of random sequences. The properties of statistical randomness include balance, run, and autocorrelation [4] which are defined below.

Balance: The balance property of a sequence is a direct implication of the frequency property [3] for statistical randomness of integers. A random binary sequence

should contain an equal number of 0s and 1s [5].

Run: A run is a sequence of identical numbers. For an ideal binary sequence, 1/2 of the runs should have length 1, 1/4 should have length 2, 1/8 should have length 3, and so on [5].

Autocorrelation: The autocorrelation is a measure of how similar a sequence is to a delayed copy of itself [4]. It is given by

$$r(k) = \sum_{m=0}^{N-1} s[m]s[m-k] \tag{1.1}$$

where $s[k]$ is the sequence, N is the length of the sequence and $0 \leq k \leq N-1$. The ratio of the magnitude of the second largest value (N) to the magnitude of the largest value in the autocorrelation is called the maximum sidelobe ratio (MSR). The lower the MSR, the better the autocorrelation of the sequence.

1.1 Maximum Length Sequences

Linear Feedback Shift Registers (LFSR) are commonly used to generate pseudorandom sequences. They are comprised of flip-flops and are synchronized with a clock. An n-bit LFSR consists of n flip flops. Figure 1.1 shows the structure of an n-bit LFSR consisting of n D flip-flops ($D1$ to Dn), n taps (C_1 to C_n) and a feedback circuit comprised of mod-2 adders. The state of an LFSR is the sequence of bits given by the flip-flops ($D1$ to Dn). The output is the contents of flip-flop Dn. The next state is determined by the feedback circuit. The smallest LFSR that produces a sequence is the *linear complexity* of that sequence [1], which is an important property of pseudorandom sequences.

Linear feedback logic based on primitive polynomials generate sequences with a maximum period, called maximum length sequences (m-sequences) [6]. Circuits that generate m-sequences are called maximum length LFSRs. A maximum length LFSR cycles through the $2^n - 1$ non-zero states before returning to the initial state. Hence, the period of an m-sequence is $N = 2^n - 1$. For the all-zero initial state, the next state is independent of the linear feedback logic and is always zero, so this is ignored.

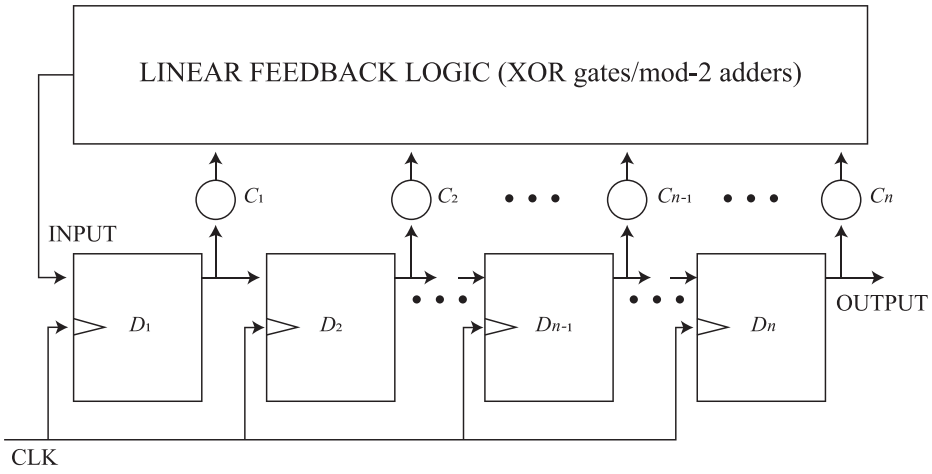


Figure 1.1: The structure of an n-bit LFSR.

An m-sequence is known to have good statistical randomness properties such as balance, run, and autocorrelation but has low linear complexity [5]. The properties of m-sequences are often used as a benchmark for the quality of a pseudorandom sequence. In this thesis, these properties will be used to evaluate the sequences generated. These properties of an m-sequence are as follows [7].

1. **Balance:** In an m-sequence, the number of ones is equal to the number of zeros plus one. It has $0.5(N+1)$ ones and $0.5(N-1)$ zeros within a period (N) [5]. Thus, the balance property of an m-sequence is optimal.

2. **Run:** For an m-sequence

   - there is 1 run of ones of length n,
   - there is 1 run of zeros of length $n-1$,
   - there are 1 run of ones and 1 run of zeros of length $n-2$,
   - there are 2 runs of ones and 2 runs of zeros of length $n-3$,
   - there are 4 runs of ones and 4 runs of zeros of length $n-4$,

   $$\vdots$$

   - there are 2^{n-3} runs of ones and 2^{n-3} runs of zeros of length 1 [5].

3. **Autocorrelation:** The autocorrelation of an m-sequence is given by

$$r(k) = \begin{cases} N, & k = aN \\ -1, & k \neq aN \end{cases} \tag{1.2}$$

where a is an integer.

4. **Linear Complexity:** The linear complexity of an m-sequence is

$$LC = \lceil \log_2 N \rceil = n \tag{1.3}$$

1.2 Cellular Automata

Ulam and von Neumann first conceptualized cellular automata (CA) in 1940, and their scope and applications in computer systems were investigated by Wolfram in 2001 [8]. CAs are structured as an array of cells in one or more dimensions [5]. They produce outputs based on predefined rules [8][9]. The rule used determines the next state of a cell by taking the current states of the cells in the neighbourhood as inputs. This thesis is an extension of [5] which considered binary pseudorandom sequences generated by One-Dimensional Cellular Automata (1D CA). In this thesis, Two-Dimensional Cellular Automata (2D CA) are considered to generate binary pseudorandom sequences.

The neighbourhood of a cell is the cell itself and adjacent cells whose current states are used to determine the next state of the cell. The maximum size of a neighbourhood in a 1D CA is 3, and it comprises the cell itself and the cells to its right and left. The neighbourhood of corner cells in a 1D CA has size 2 (the cell itself and the cell adjacent to it). Figure 1.2 shows a 1D CA of size $n = 5$ and the shaded cells show the neighbourhood of cell 3, where the cells are numbered from left to right.

The state table gives the next state of the cell for each of the possible neighbourhood current states. For a size 3 neighbourhood, there are $2^3 = 8$ states in the state table and $2^8 = 256$ state tables based on different possible next states [5]. The next states generated by the respective state tables are known as rules. These rules are numbered 0 to 255 and are called Wolfram rules [8]. If the state table can be generated by a linear function (mod-2 additions) of the current state of the neighbourhood

the rule is called linear [5]. Of the 256 rules, there are only $2^3 = 8$ linear rules. Not all linear rules give good pseudorandom sequences, but combinations of rules 90 and 150 based on primitive polynomials can be used to generate m-sequences [10][11]. The state table for linear rule 90 is given in Table 1.1. The last column of the table shows the 8 next states for each current state. The next states in vector form (01011010) give the Wolfram rule (rule 90).

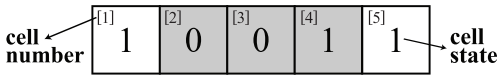


Figure 1.2: A 1D CA of size $n = 5$.

Current State			Next State
$s_{i-1}(k)$	$s_i(k)$	$s_{i+1}(k)$	$s_i(k+1)$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

} 90

Table 1.1: Rule 90 State Table

The two commonly used neighbourhoods for a 2D CA are the von Neumann neighbourhood and the Moore neighbourhood [12] as shown in Figures 1.3 and 1.4, respectively. The maximum size of a von Neumann neighbourhood is 5 and of a Moore neighbourhood is 9. The next state of the center cell depends on the associated rule and the states of the neighbourhood cells. The cells on the corners have a neighbourhood of size 3 and 4 for von Neumann and Moore neighbourhoods, respectively. In this thesis, 2D CAs are considered with the von Neumann neighbourhood, and the Moore neighbourhood can be considered as future work.

For the von Neumann neighbourhood, the function to determine the next state of a cell has 5 inputs and in this thesis is given by the following Boolean function

$$s_{x,y}(k+1) = F(s_{x-1,y}(k), s_{x,y-1}(k), s_{x,y}(k), s_{x,y+1}(k), s_{x+1,y}(k)) \tag{1.4}$$

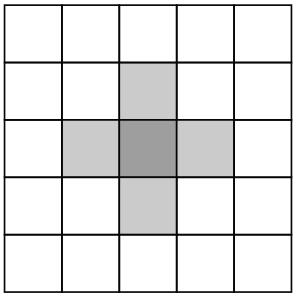


Figure 1.3: The von Neumann neighbourhood of the center cell.

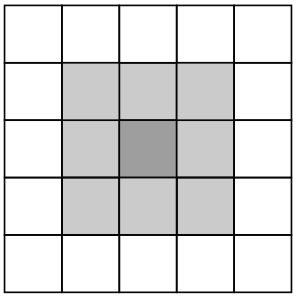


Figure 1.4: The Moore neighbourhood of the center cell.

where
$s_{x,y}(k+1)$ is the next state of a cell,
$s_{x-1,y}(k)$ is the current state of the left cell,
$s_{x,y-1}(k)$ is the current state of the top cell,
$s_{x,y}(k)$ is the current state of a cell,
$s_{x,y+1}(k)$ is the current state of the bottom cell,
$s_{x+1,y}(k)$ is the current state of the right cell, and
$F()$ is the Boolean function or rule.

If an adjacent cell does not exist, its value is set to 0. In Figure 1.5, a 2D CA of size $n = 9$ is shown. The shaded cells show the von Neuman neighbourhood of the center cell (cell 5), and the cell states are also given. The next state of the center cell is found from the state table of the associated rule. For the Boolean function in (1.4), the 5-bit current state is 10100.

For a 5-bit binary sequence, there are a total of $2^5 = 32$ states and the number of possible state tables (rules) is $2^{32} = 4294967296$ [12]. In a state table, the next state is based on a rule in the range 0 to 4294967295. Table 1.2 shows the

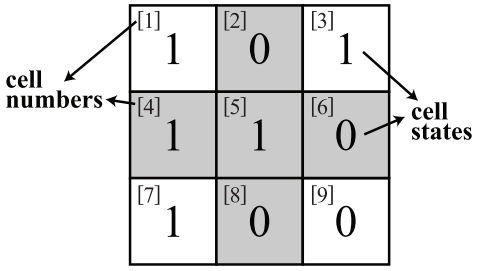


Figure 1.5: A 2D CA of size $n = 9$.

state table for non-linear rule 12586. The 32-bit binary representation of this rule is 00000000000000000011000100101010. State 11111 corresponds to the MSB of the rule and state 00000 corresponds to the LSB. This is an even rule as the next state for state 00000 in the state table is 0. If the next state for state 00000 is 1, the rule is called odd. An example of an odd rule is rule 12587.

There are $2^5 = 32$ linear rules out of the approximately 4.29×10^9 rules. For a linear rule, the Boolean function in (1.4) has only mod-2 additions. In this thesis, L0 to L31 are used to denote the linear rules and the non-linear rules are referred to by their rule numbers. Table 1.3 shows the linear rules L0 to L31 and their respective rule numbers. Note that the linear rules are even. The equations for L1 (00001), L13 (01101) and L31 (11111) using (1.4) are

$$\begin{aligned}
\text{L1} &: s_{x,y}(k+1) = s_{x+1,y}(k), \\
\text{L13} &: s_{x,y}(k+1) = s_{x,y-1}(k) \oplus s_{x,y}(k) \oplus s_{x+1,y}(k), \\
\text{L31} &: s_{x,y}(k+1) = s_{x-1,y}(k) \oplus s_{x,y-1}(k) \oplus s_{x,y}(k) \oplus s_{x,y+1}(k) \oplus s_{x+1,y}(k)
\end{aligned}$$

where $\oplus$ represents mod-2 addition.

Figures 1.6, 1.7 and 1.8 show the structures of the 2D CAs of size $n = 5, 6, 7, \ldots, 16$ used in this thesis.

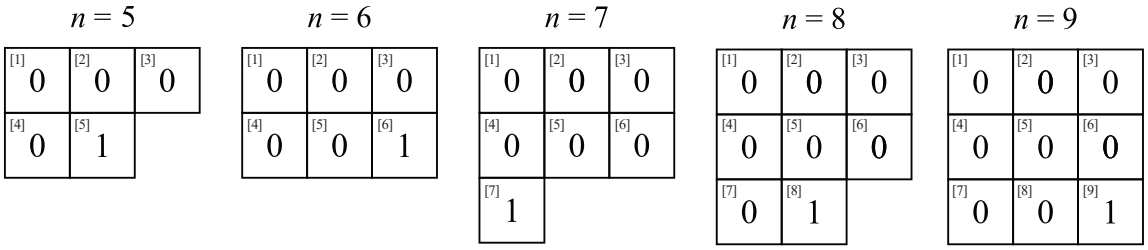


Figure 1.6: The structures of 2D CAs of size n = 5, 6, 7, 8 and 9.

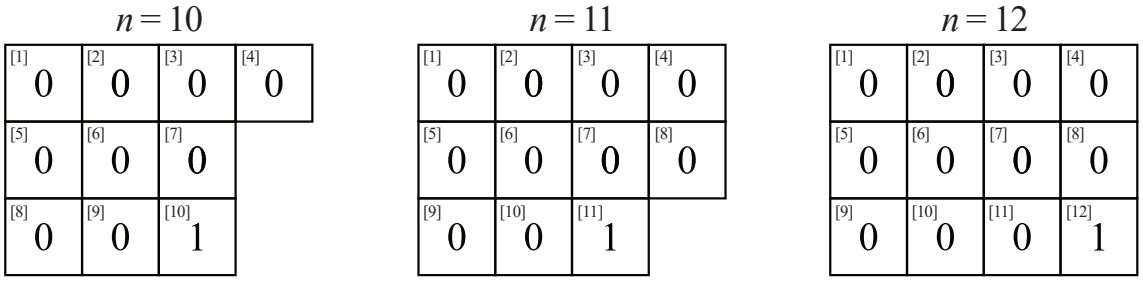


Figure 1.7: The structures of 2D CAs of size n = 10, 11 and 12.

1.3 Thesis Organization

Chapter 2 describes the 2D CA evaluation system and m-sequence generation using linear rules. It further gives a classification of the linear rules. The parameters used to characterize the sequences generated using the evaluation system are also given.

Chapter 3 discusses the results obtained from the 2D CA evaluation system by replacing a linear rule with a non-linear rule for 2D CAs of sizes n = 5 to 14. Filtering criteria are specified and the corresponding results are given for each CA size. The properties of the sequences obtained are compared with those of m-sequences and the sequences obtained using 1D CAs in [5].

Chapter 4 provides some conclusions and suggestions for future work associated with pseudorandom sequence generation using 2D CAs.

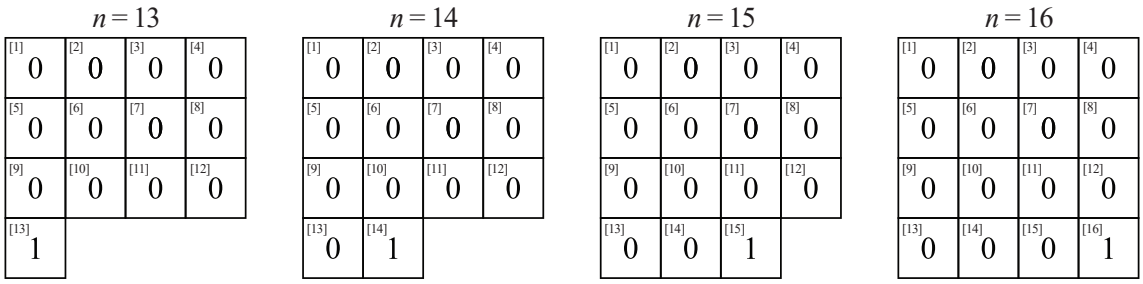


Figure 1.8: The structures of 2D CAs of size $n = 13$, 14, 15 and 16.

Current State					Next State
$s_{x-1,y}(k)$	$s_{x,y-1}(k)$	$s_{x,y}(k)$	$s_{x,y+1}(k)$	$s_{x+1,y}(k)$	$s_{x,y}(k+1)$
1	1	1	1	1	0
1	1	1	1	0	0
1	1	1	0	1	0
1	1	1	0	0	0
1	1	0	1	1	0
1	1	0	1	0	0
1	1	0	0	1	0
1	1	0	0	0	0
1	0	1	1	1	0
1	0	1	1	0	0
1	0	1	0	1	0
1	0	1	0	0	0
1	0	0	1	1	0
1	0	0	1	0	0
1	0	0	0	1	0
1	0	0	0	0	0
0	1	1	1	1	0
0	1	1	1	0	0
0	1	1	0	1	1
0	1	1	0	0	1
0	1	0	1	1	0
0	1	0	1	0	0
0	1	0	0	1	0
0	1	0	0	0	1
0	0	1	1	1	0
0	0	1	1	0	0
0	0	1	0	1	1
0	0	1	0	0	0
0	0	0	1	1	1
0	0	0	1	0	0
0	0	0	0	1	1
0	0	0	0	0	0

} 12586

Table 1.2: Rule 12586 State Table

$F(s_{x-1,y}(k) \oplus s_{x,y-1}(k) \oplus s_{x,y}(k) \oplus s_{x,y+1}(k) \oplus s_{x+1,y}(k))$					Linear Rule	
$s_{x-1,y}(k)$	$s_{x,y-1}(k)$	$s_{x,y}(k)$	$s_{x,y+1}(k)$	$s_{x+1,y}(k)$		Decimal
1	1	1	1	1	L31	2523490710
1	1	1	1	0	L30	1019462460
1	1	1	0	1	L29	1520805210
1	1	1	0	0	L28	4027518960
1	1	0	1	1	L27	1721342310
1	1	0	1	0	L26	3425907660
1	1	0	0	1	L25	2857719210
1	1	0	0	0	L24	16776960
1	0	1	1	1	L23	1768527510
1	0	1	1	0	L22	3284352060
1	0	1	0	1	L21	2779077210
1	0	1	0	0	L20	252702960
1	0	0	1	1	L19	2576967270
1	0	0	1	0	L18	859032780
1	0	0	0	1	L17	1431677610
1	0	0	0	0	L16	4294901760
0	1	1	1	1	L15	1771465110
0	1	1	1	0	L14	3275539260
0	1	1	0	1	L13	2774181210
0	1	1	0	0	L12	267390960
0	1	0	1	1	L11	2573637990
0	1	0	1	0	L10	869020620
0	1	0	0	1	L9	1437226410
0	1	0	0	0	L8	4278255360
0	0	1	1	1	L7	2526451350
0	0	1	1	0	L6	1010580540
0	0	1	0	1	L5	1515870810
0	0	1	0	0	L4	4042322160
0	0	0	1	1	L3	1717986918
0	0	0	1	0	L2	3435973836
0	0	0	0	1	L1	2863311530
0	0	0	0	0	L0	0

Table 1.3: Linear Rules L0 to L31

Chapter 2

2D Cellular Automata and m-sequence Generation

In this chapter, the 2D CA evaluation system and the associated parameters are discussed along with m-sequence generation using linear rules. This system is an extension of the 1D CA evaluation system in [5] and is characterized by the same parameters with the addition of two new parameters (Linear Rules Combination and Class Combination). Combining linear rules (L0 to L31) to generate m-sequences is discussed in this chapter. First, all possible linear rule combinations are used to generate sequences for 2D CAs of size $n = 5, 6, \ldots, 9$. Based on these results, certain combinations are selected and used to generate sequences for 2D CAs of size $n = 10, 11, \ldots, 16$. The following parameters are used to characterize the sequences generated [5].

1. **Size (n):** The number of cells in the 2D CA is the size of the CA. Figure 2.1 shows a 2D CA of size $n = 6$.

2. **Linear Rules Combination (LRC):** Linear rules are assigned to each cell of the 2D CA. This represents the two linear rules that are assigned to the 2D CA. In Figure 2.1, the linear rules combination assigned to the CA is $LRC =$ L28, L27.

3. **Linear Rules (LR):** This is the set of n linear rules based on LRC assigned to the 2D CA. For convenience, the first LRC rule is denoted by 0 in the LR and the second rule is denoted by 1. An n bit vector is formed that represents the CA. LR is also expressed in decimal for convenience. The 6-bit 2D CA in

Figure 2.1 is represented by LR = L27, L28, L28, L27, L28, L27 = 100101 = 37.

4. **Start Value (SV):** Start value is the vector of n bits that is the initial state of the 2D CA. In Figure 2.1, the initial state of the CA is $SV = 000001$. SV is also expressed in decimal for convenience.

5. **Random Rule (RR):** Random rule is the non-linear rule that replaces a linear rule in the 2D CA. In Figure 2.1, $RR = 1264$ replaces L27 in cell number 4.

6. **Random Cell (RC):** Random cell is the cell that is replaced by a RR. In Figure 2.1, $RC = 4$.

7. **Observed Cell (OC):** The cell from which the sequence of bits is obtained is the observed cell. The grey cell in Figure 2.1 corresponds to $OC = 5$.

8. **Sequence (S):** This is the sequence from OC of length $N = 2^n - 1$ which is the period of an m-sequence from an LFSR of the same length as the CA size (n).

9. **Class Combination (CC):** Class combination represents the classes to which the respective LRC rules belong to. Classes for the linear rules are defined in Section 2.2. In Figure 2.1, LRC = L27, L28 so CC = A, E.

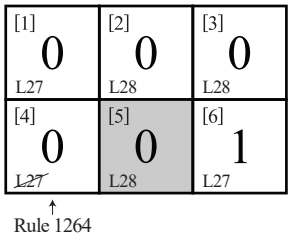
10. **Linear Complexity (LC):** This is the linear complexity of the sequence from OC.

11. **Balance (B):** This is the balance of the sequence from OC and is the number of zeros subtracted from the number of ones in the sequence.

12. **Run (R):** This is the runs of the sequence from OC which is an array of size 16 containing the number of runs of lengths 1, 2, 3, ..., 16.

13. **Autocorrelation (AC) and Max Sidelobe Ratio (MSR):** Autocorrelation is an array containing values of the autocorrelation of the sequence from OC and MSR contains the maximum sidelobe ratio.

Parameters 1 to 7 and 9 are varied in the system while parameters 8 and 10 to 13 are determined. In Section 2.1, a brief description of the framework of the 2D CA evaluation system is provided.



LRC = L28, L27 — *RR*[4] = 1264

CC = Class A, Class E — *OC* = 5

LR = L27(1), L28(0), L28(0), L27(1), L28(0), L27(1) = 100101 = 37 — *SV* = 000001 = 1

Figure 2.1: An example of the rules and parameters in the 2D CA evaluation system.

2.1 The 2D CA Evaluation System

The sytem used for 2D CA evaluation is an extension of the 1D CA evaluation system used in [5], which was developed using the C programming language to analyze 1D CAs containing a non-linear rule for pseudorandom sequence generation. The 2D CA evaluation system was developed using Python scripting and Joblib library was used to employ parallelism. It is first used to analyze sequences generated using linear rules for 2D CAs. In Chapter 3 it is used to analyze 2D CAs containing a non-linear rule for pseudorandom sequence generation. A separate function was developed for each CA size for $n = 5, 6, 7, \ldots, 16$. The operating system used was Linux Ubuntu 14.04. The program is comprised of three (main control, 2D CA and test) modules as shown in Figure 2.2. These modules are described below.

Main Control Module: The control module has inputs n, LRC, LR, SV, OC, RR and RC. An iteration is defined as a sequence generated with one set of input parameters [5]. The number of possible LRC values is $\binom{m}{k} = \frac{m!}{k!(m-k)!}$ where $k = 2$ (maximum number of linear rules in an LRC) and $m = 31$ (all linear rules are considered except L0). The number of balanced RRs out of a total of 4294967296 rules is $\binom{32}{16} - 31$ (minus the linear rules). The number of iterations is determined by the following parameters.

- Maximum value of LRC is $\binom{31}{2} = 465$.
- Maximum value of LR is 2^n.
- Maximum value of SV is 2^n.
- Maximum value of OC is n.

- Number of balanced RRs is $\binom{32}{16} - 31 = 601080359$.
- Maximum value of RC is n.

For one random cell replacement, the maximum number of iterations is

$$465 \times 2^n \times 2^n \times n \times 601080359 \times n, \tag{2.1}$$

which is 7.15×10^{15} for CA size 5. The length of the output sequence generated is twice the period of an m-sequence $(2 \times (2^n - 1))$. Thus, the time taken for each iteration is exponential in n. The first half of the output sequence is discarded and the second half is used as the output sequence S. This approach is used to remove any unwanted effects of the initial conditions [5]. To reduce the complexity and number of iterations, the number of LRC, LR, SV and OC values considered is reduced based on the results in the next section.

CA Module: The CA module consists of different functions for different sizes n. The input n is used to call the function for the respective 2D CA. LRC defines the two linear rules used to configure the n cells using the bit vector LR. RR replaces one linear rule with a non-linear rule at cell position RC. The output sequence S is obtained from cell OC. The state of each cell is updated based on the rule assigned. An output sequence S of length $2^n - 1$ is obtained.

Test Module: The test module takes the sequence S from the CA module as input and calls the following functions.

- **LC Calculator:** The linear complexity of S is calculated and returned by this function. It employs the Berlekamp-Massey algorithm to determine the LC [13] [14].
- **Balance Calculator:** This function calculates and returns the balance B of S by subtracting the number of 0s from the number of 1s.
- **Run Calculator:** This function calculates the runs R of S.
- **AC and MSR Calculator:** This function calculates the AC and MSR of S.

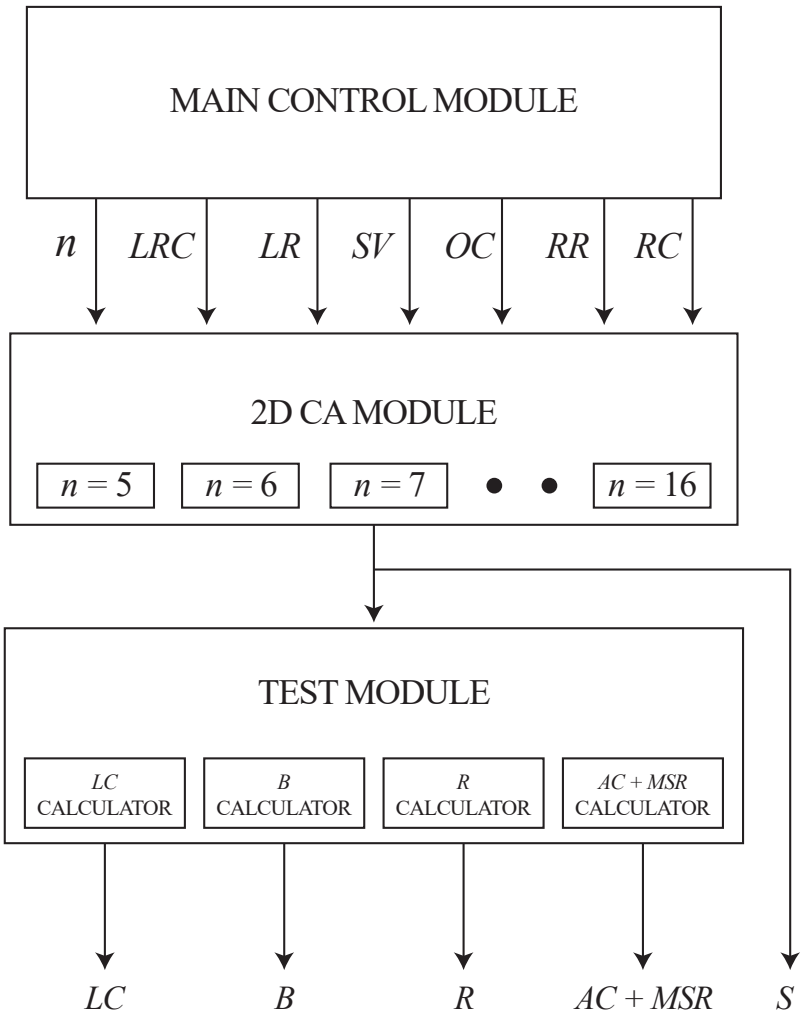


Figure 2.2: Modules of the 2D CA evaluation system.

2.2 m-sequence Generation using Linear Rules

To generate m-sequences using linear rules in a 2D CA, only rules which take inputs from at least 3 neighbours to determine the next state of the respective cell are considered. This approach is used because 1D CAs have a maximum of 3 neighbours and to ensure that there is sufficient interaction between the neighbourhood cells in determining the next state of each cell. Table 2.1 shows the resulting linear rules that are considered for generating m-sequences. It should be noted that some of these rules are just rotations of each other. Figure 2.3 shows the clockwise rotations of L28. If we rotate L28 clockwise, we get L13 and then rotating L13 gives L7 and then L22. Similarly, Figures 2.4, 2.5 and 2.6 show the rotations of linear rules L21,

L25 and L30, respectively. Rotations of rule L27 and rule L31 yield the same rules because L27 takes inputs from all four adjacent neighbours of the center cell and rule L31 takes inputs from all 5 neighbours (including the center cell). Thus, these linear rules can be classified into six different classes based on the rules that are rotations of each other as shown in Table 2.2. Rules in classes A, B and C take inputs from 3 cells, rules in Class D and Class E take inputs from 4 cells and the rule in Class F takes inputs from all 5 cells in the neighbourhood.

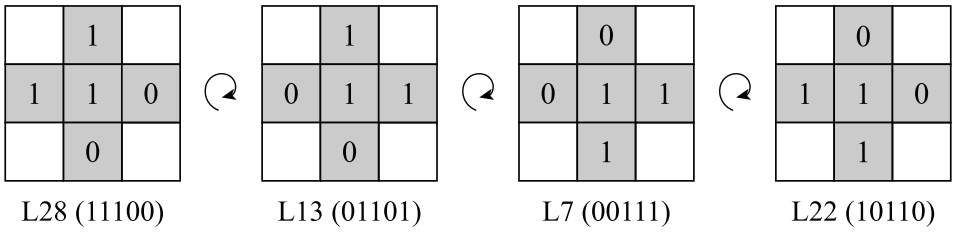


Figure 2.3: The clockwise rotations of L28.

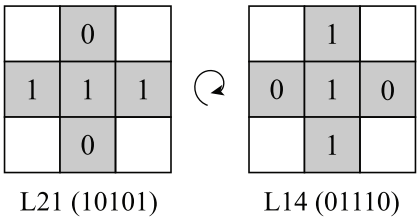


Figure 2.4: The clockwise rotations of L21.

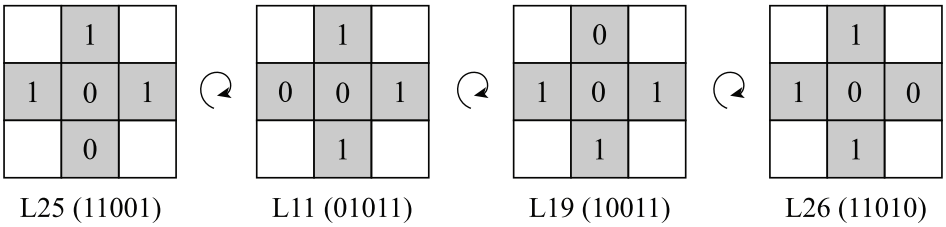


Figure 2.5: The clockwise rotations of L25.

Using the linear rules in Table 2.1, the number of linear rules considered is reduced from 32 to 16. The corresponding maximum number of LRC values is $\binom{16}{2} = 120$ which is less than the 465 given in Section 2.1. In order to determine the linear rule combinations that generate m-sequences, all possible values of LR for each of the 120

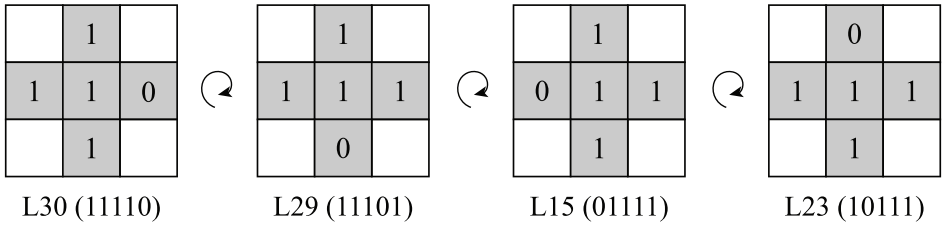


Figure 2.6: The clockwise rotations of L30.

$F(s_{x-1,y}(k) \oplus s_{x,y-1}(k) \oplus s_{x,y}(k) \oplus s_{x,y+1}(k) \oplus s_{x+1,y}(k))$					Linear Rule	
$s_{x-1,y}(k)$	$s_{x,y-1}(k)$	$s_{x,y}(k)$	$s_{x,y+1}(k)$	$s_{x+1,y}(k)$		Decimal
1	1	1	1	1	L31	2523490710
1	1	1	1	0	L30	1019462460
1	1	1	0	1	L29	1520805210
1	1	1	0	0	L28	4027518960
1	1	0	1	1	L27	1721342310
1	1	0	1	0	L26	3425907660
1	1	0	0	1	L25	2857719210
1	0	1	1	1	L23	1768527510
1	0	1	1	0	L22	3284352060
1	0	1	0	1	L21	2779077210
1	0	0	1	1	L19	2576967270
0	1	1	1	1	L15	1771465110
0	1	1	1	0	L14	3275539260
0	1	1	0	1	L13	2774181210
0	1	0	1	1	L11	2573637990
0	0	1	1	1	L7	2526451350

Table 2.1: Linear Rules With at Least Three Inputs

LRC were checked for 2D CA sizes n = 5, 6, 7, 8 and 9. The maximum number of LR values for any LRC that includes two rules is $2n$ – 2 because the all zeros and all ones LR values include only one rule from the LRC. Table 2.3 shows the possible values of LR for a 2D CA size n = 4 and LRC = L7, L25. There are $16 - 2 = 14$ unique LR values.

2.2.1 Initial Observations

The 2D CA evaluation system was first used to analyze all possible combinations of the linear rules in CAs of size n = 5, 6, 7, 8 and 9. The outputs were stored in Excel files and then filtered to obtain those combinations that generate m-sequences. The following observations can be made.

Class	Linear Rules
A	L28, L13, L7, L22
B	L30, L29, L15, L23
C	L25, L11, L19, L26
D	L21, L14
E	L27
F	L31

Table 2.2: Classification of Linear Rules

LRC	LR
L7, L25	1110
L7, L25	1101
L7, L25	1100
L7, L25	1011
L7, L25	1010
L7, L25	1001
L7, L25	1000
L7, L25	0111
L7, L25	0110
L7, L25	0101
L7, L25	0100
L7, L25	0011
L7, L25	0010
L7, L25	0001

Table 2.3: All Possible Values of LR That Include Both LRC Rules

1. Many different combinations (LRC and respective LR) of the linear rules in Table 2.1 generate m-sequences. These combinations gave m-sequences for all possible initial states except $SV = 0$. For $SV = 0$, the sequence generated is all zeros. This is because all the linear rules (L0 to L31) of 2D CA are even rules as discussed in Section 1.2. For even rules the LSB bit is 0 and for $SV = 0$, all the neighbourhood cell states are 0, so the next state of all cells is always 0. Hence, $SV = 1$ was fixed for further analysis.

2. For the values of LRC and LR that generated m-sequences, all values of $OC = 1, 2, \ldots, n$ generated m-sequences. Hence, $OC = 4$ was fixed for further analysis.

3. None of the LRC having both rules from the same class generated m-sequences. For example, if L28 is considered from Class A, no combinations with an-

other rule from the same class (L13, L7 or L22) generated an m-sequence. m-sequences are only generated by combinations of rules from different classes.

4. For CA size $n = 9$, if a combination of a rule from a certain class generated an m-sequence with a rule from another class, then the combination of rules obtained by rotating these rules in the same direction also generated an m-sequence. For example, combinations of L30 from Class B with L11 from Class C generated m-sequences, and combinations of the rotations of these rules, i.e. L23 from Class B and L25 from Class C, also generated m-sequences.

2.2.2 Results for 2D CA sizes $n = 5$, 6, 7, 8 and 9

Using the linear rules in Table 2.1, all possible values of LR for all possible LRC of these rules were first tested for $n = 5$. The results obtained show that different linear rule combinations for a 2D CA system can generate m-sequences. Table 2.4 shows the unique LRC that generated m-sequences for $n = 5$. The first column shows the LRC which generated m-sequences. The second column shows the respective classes that the rules in LRC belong to. The third column shows one of the multiple LR values of the respective LRC in the first column, that generated m-sequences. Results for all the LR of LRC = L21, L27 that generated m-sequences are shown in Table 2.5. Tables 2.6, 2.7, 2.8 and 2.9 show all unique LRC and respective LR (one of the multiple values) that generated m-sequences for 2D CAs of sizes $n = 6$, 7, 8 and 9, respectively.

From the results in Table 2.4, 2.7, 2.8 and 2.9, it can be seen that seven unique CC generate m-sequences for 2D CAs of sizes $n = 5$, 7, 8 and 9, respectively. For $n = 6$, six unique CC generated m-sequences which can be seen in Table 2.6. For further analysis, the best LRC is selected from each unique CC as a representative of that CC. In Table 2.10, all the unique CC are shown. The criteria for the selection of the best LRC from each of the respective CC is the total number of appearances of the respective LRC in Tables 2.4 and 2.6 to 2.9. The LRC that appeared the greatest number of times from a respective CC was selected as the representative of that CC. For example, from CC = Class A, Class C, LRC = L7, L25 appears 4 times in Tables 2.4, 2.7, 2.6 and 2.9 (for 2D CA size $n = 5$, 7, 8 and 9) whereas LRC = L13, L26 from the same CC appears twice and only in Tables 2.6 and 2.9. Therefore, from these LRC, LRC = L7, L25 is chosen. Table 2.11 shows the seven LRC that were selected as representative of the respective CC in Table 2.10 based on the criteria discussed

LRC	*CC*	*LR*	*LC*	*B*	*R*	*AC*
L7, L25	A, C	00111	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L28, L27	A, E	11010	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L13, L27	A, E	01111	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L7, L27	A, E	01111	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L22, L27	A, E	11010	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L30, L11	B, C	11010	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L29, L19	B, C	01110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L15, L26	B, C	00101	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L23, L25	B, C	10001	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L30, L27	B, E	01011	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L23, L27	B, E	11010	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L15, L27	B, E	11110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L29, L27	B, E	01111	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L26, L21	C, D	01110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L25, L14	C, D	10000	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L25, L31	C, F	11110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L11, L31	C, F	11110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L19, L31	C, F	11010	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L26, L31	C, F	11110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L21, L27	D, E	11010	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .
L14, L27	D, E	11110	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .

Table 2.4: m-sequences for the Unique LRC for CA Size $n = 5$

OC	*LRC*	*LR*	*SV*	*LC*	*B*	*R*	*AC*	*S*
4	L21, L27	11010	1	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .	010010. . .
4	L21, L27	10010	1	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .	000101. . .
4	L21, L27	01111	1	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .	110000. . .
4	L21, L27	01101	1	5	1	8, 4, 2, 1, 1, 0, 0, . . .	31, -1, -1, -1, . . .	011000. . .

Table 2.5: m-sequences for the LR Values for LRC = L21, L27

above. For $n = 5$, 7, 8 and 9, all seven CC representatives generated m-sequences. For 2D CA of size $n = 6$, LRC = L7, L25 and L21, L27 did not generate m-sequences as can be determined from Table 2.6. These seven representatives are used for further analysis in this thesis.

2.2.3 Results for 2D CA size $n = 10, 11, 12, \ldots, 16$

Sequences for 2D CAs of size $n = 10, 11, 12, \ldots, 16$ were generated using the CC representatives given in Table 2.11. The objective was to ensure that the selected CC

LRC	CC	LR	LC	B	R	AC
L13, L26	A, C	101011	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L22, L11	A, C	111100	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L28, L27	A, E	110011	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L13, L27	A, E	111001	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L7, L27	A, E	110011	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L22, L27	A, E	100111	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L30, L11	B, C	010101	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L15, L26	B, C	101010	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L30, L27	B, E	010101	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L23, L27	B, E	110100	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L15, L27	B, E	111001	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L29, L27	B, E	001011	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L26, L21	C, D	001110	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L25, L14	C, D	011100	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L25, L31	C, F	100110	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L11, L31	C, F	110101	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L19, L31	C, F	110100	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .
L26, L31	C, F	101011	6	1	16, 8, 4, 2, 1, 1, 0, 0, . . .	63, -1, -1, -1, . . .

Table 2.6: m-sequences for the Unique LRC for CA Size $n = 6$

representatives generate m-sequences for 2D CAs of size $n > 9$. Tables 2.12, 2.13 and 2.14 show the results for $n = 10$, 11 and 12, respectively. For $n = 10$, two CC representatives (LRC = L7, L25 and L30, L11) did not generate m-sequences, whereas for $n = 11$ and 12, m-sequences were generated for all seven CC representatives. In the tables, only one value of the LR is shown for the respective LRC (CC representatives) that generated m-sequences. Tables 2.14, 2.15, 2.16 and 2.17 show the results obtained for m-sequence generation using the selected CC representatives for $n =$ 13, 14, 15 and 16, respectively. For $n = 14$, 15 and 16, all seven CC representatives generated m-sequences. For $n = 13$, LRC = L7, L25 did not generate an m-sequence.

LRC	CC	LR	LC	B	R	AC
L7, L25	A, C	0110111	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L28, L27	A, E	1001101	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L13, L27	A, E	1111011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L7, L27	A, E	1110011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L22, L27	A, E	1101011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L30, L11	B, C	0101011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L29, L19	B, C	1001010	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L15, L26	B, C	1010100	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L23, L25	B, C	0110111	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L30, L27	B, E	0111001	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L23, L27	B, E	1101101	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L15, L27	B, E	1111011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L29, L27	B, E	0011000	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L26, L21	C, D	1100000	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L25, L14	C, D	0011001	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L25, L31	C, F	1111011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L11, L31	C, F	1111011	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L19, L31	C, F	1101101	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L26, L31	C, F	1111001	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L21, L27	D, E	1101101	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .
L14, L27	D, E	1100111	7	1	32, 16, 8, 4, 2, 1, 1, 0, 0, . . .	127, -1, -1, -1, . . .

Table 2.7: m-sequences for the Unique LRC for CA Size $n = 7$

LRC	CC	LR	LC	B	R	AC
L7, L25	A, C	11001111	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L28, L27	A, E	10011111	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L13, L27	A, E	01111001	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L7, L27	A, E	11100111	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L22, L27	A, E	11010010	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L30, L11	B, C	10101011	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L29, L19	B, C	00111001	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L23, L25	B, C	11000110	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L30, L27	B, E	01000011	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L23, L27	B, E	10010010	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L15, L27	B, E	11011110	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L29, L27	B, E	00110101	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L25, L14	C, D	01110000	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L25, L31	C, F	00111001	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L11, L31	C, F	11010110	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L19, L31	C, F	11110011	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L26, L31	C, F	10111011	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L21, L27	D, E	00111111	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .
L14, L27	D, E	11011110	8	1	64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	255, -1, -1, -1, . . .

Table 2.8: m-sequences for the Unique LRC for CA Size $n = 8$

LRC	CC	LR	LC	B	R	AC
L28, L19	A, C	100110110	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L13, L26	A, C	111110000	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L7, L25	A, C	011011001	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L22, L11	A, C	000011111	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L28, L27	A, E	101111010	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L13, L27	A, E	101111010	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L7, L27	A, E	011110011	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L22, L27	A, E	110011110	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L30, L11	B, C	000111110	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L29, L19	B, C	011011010	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L15, L26	B, C	111000001	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L23, L25	B, C	100100101	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L30, L27	B, E	001001111	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L23, L27	B, E	111100100	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L15, L27	B, E	111100001	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L29, L27	B, E	001001101	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L26, L21	C, D	001110110	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L25, L14	C, D	001101110	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L25, L31	C, F	110100101	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L11, L31	C, F	111100100	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L19, L31	C, F	111100100	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L26, L31	C, F	111100001	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L21, L27	D, E	110101001	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .
L14, L27	D, E	110100011	9	1	128, 64, 32, 16, 8, 4, 2, 1, 1, 0, . . .	511, -1, -1, . . .

Table 2.9: m-sequences for the Unique LRC for CA Size $n = 9$

CC
A, C
A, E
B, C
B, E
C, D
C, F
D, E

Table 2.10: All Unique CC That Generate m-sequences

CC	LRC
A, C	L7, L25
A, E	L28, L27
B, C	L30, L11
B, E	L30, L27
C, D	L25, L14
C, F	L25, L31
D, E	L21, L27

Table 2.11: Representative LRC of Respective CC

LRC	LR	LC	B	R	AC
L28, L27	1111101101	10	1	256, 128, 64, 32, 16, 8, 4, 2, 1, 1, . . .	1023, -1, -1, . . .
L30, L27	1111001011	10	1	256, 128, 64, 32, 16, 8, 4, 2, 1, 1, . . .	1023, -1, -1, . . .
L25, L14	0100111100	10	1	256, 128, 64, 32, 16, 8, 4, 2, 1, 1, . . .	1023, -1, -1, . . .
L25, L31	1100110010	10	1	256, 128, 64, 32, 16, 8, 4, 2, 1, 1, . . .	1023, -1, -1, . . .
L21, L27	1111001111	10	1	256, 128, 64, 32, 16, 8, 4, 2, 1, 1, . . .	1023, -1, -1, . . .

Table 2.12: m-sequences Using CC Representatives for $n = 10$

LRC	LR	LC	B	R	AC
L7, L25	11100111011	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .
L28, L27	11111010111	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .
L30, L11	11101111000	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .
L30, L27	11111011101	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .
L25, L14	00011100101	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .
L25, L31	11111101110	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .
L21, L27	11111111110	11	1	512, 256, 128, 64, 32, 16, 8, 4, 2, . . .	2047, -1, -1, . . .

Table 2.13: m-sequences Using CC Representatives for $n = 11$

LRC	LR	LC	B	R	AC
L7, L25	110101101011	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .
L28, L27	111111110011	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .
L30, L11	111111101000	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .
L30, L27	111111110011	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .
L25, L14	000110011100	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .
L25, L31	111011111000	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .
L21, L27	111111011001	12	1	1024, 512, 256, 128, 64, 32, 16, 8, . . .	4095, -1, -1, . . .

Table 2.14: m-sequences Using CC Representatives for $n = 12$

LRC	LR	LC	B	R	AC
L28, L27	1111111110111	13	1	2048, 1024, 512, 256, 128, 64, 32, . . .	8191, -1, -1, . . .
L30, L11	1111111110001	13	1	2048, 1024, 512, 256, 128, 64, 32, . . .	8191, -1, -1, . . .
L30, L27	1111111110111	13	1	2048, 1024, 512, 256, 128, 64, 32, . . .	8191, -1, -1, . . .
L25, L14	0001001110001	13	1	2048, 1024, 512, 256, 128, 64, 32, . . .	8191, -1, -1, . . .
L25, L31	1111111110111	13	1	2048, 1024, 512, 256, 128, 64, 32, . . .	8191, -1, -1, . . .
L21, L27	1111101010111	13	1	2048, 1024, 512, 256, 128, 64, 32, . . .	8191, -1, -1, . . .

Table 2.15: m-sequences Using CC Representatives for $n = 13$

LRC	LR	LC	B	R	AC
L7, L25	11100111100111	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .
L28, L27	11111111111100	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .
L30, L11	11111110010010	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .
L30, L27	11111111111100	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .
L25, L14	00011010100001	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .
L25, L31	11111110101111	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .
L21, L27	11111110100011	14	1	4096, 2048, 1024, 512, 256, 128, . . .	16383, -1, -1, . . .

Table 2.16: m-sequences Using CC Representatives for $n = 14$

LRC	LR	LC	B	R	AC
L7, L25	111001101101111	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .
L28, L27	111111111111000	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .
L30, L11	111111111110100	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .
L30, L27	111111111110001	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .
L25, L14	00011010100001	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .
L25, L31	111111111110001	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .
L21, L27	111111111001100	15	1	8192, 4096, 2048, 1024, 512, 256, . . .	32767, -1, -1, . . .

Table 2.17: m-sequences Using CC Representatives for $n = 15$

LRC	LR	LC	B	R	AC
L7, L25	1011110111100111	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .
L28, L27	1111111101110000	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .
L30, L11	1111101110000000	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .
L30, L27	1111110101010101	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .
L25, L14	0001001110010000	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .
L25, L31	1111110111011100	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .
L21, L27	1111110110111000	16	1	16384, 8192, 4096, 2048, 1024, 512, . . .	65535, -1, -1, . . .

Table 2.18: m-sequences Using CC Representatives for $n = 16$

Chapter 3

Pseudorandom Sequence Generation

In this chapter, psuedorandom sequences are generated and analyzed using the seven LRC chosen as CC representatives given in Table 2.11. The LR values for the respective LRC in Tables 2.4 and 2.6 to 2.9 for 2D CAs of sizes $n = 5$ to 9, respectively, are used and a single cell is replaced with all balanced RR in the range 0 to 4294967296. Multi stage filtering is then done to obtain RRs for each CC representative that generate sequences with high linear complexity and good randomness properties. The properties of the sequences obtained are then compared to those of m-sequences. The filtering criteria used are discussed in the next section.

3.1 Filtering Criteria

The filtering criteria employed are similar to those used in [5] to filter the sequences generated using 1D CAs, but are more strict to obtain sequences with better randomness properties and to reduce the computational complexity. The two filtering stages described below are used to filter sequences to obtain RRs that provide good sequences.

First Stage: The first stage of filtering is based on LC, MSR and the randomness tests (frequency test for balance and run test) defined in [15].

- **LC:** The generated sequences are initially filtered based on the LC. Only

those RRs are considered which generate sequences having

$$LC \geq 2^n/2$$

- **Frequency Test for Balance:** In this test, each bit of a sequence is assigned a value -1 or +1 (0 = -1 and 1 = +1) and the sum of the values is calculated

$$X_N = \sum_{m=0}^{N-1} 2s(m) - 1$$

where $s(m)$ is the mth bit of S and $N = 2^n - 1$ is the length of S [5][15].This is used to calculate the complementary error function

$$P_B = \text{erfc}(|X_N|/(\sqrt{2N}))$$

A balance threshold of $P_{BTh} = 0.9$ is used to filter the sequences, so the RR is kept if the generated sequence has

$$P_B \geq 0.9$$

- **Run Test:** In this test the ratio of the number of 1s to the length of S is calculated as

$$\pi = \sum_{m=0}^{N-1} s(m)/N$$

where $s(m)$ is the mth bit of S. If the condition $|\pi - 1/2| < X_N/\sqrt{N}$ is not satisfied, then the test fails. Then the test statistic

$$V_N(obs) = \sum_{m=0}^{N-2} v(m) + 1$$

is calculated where $v(m) = 0$ if the $(m+1)$th bit is the same as the mth bit and $v(m) = 1$ otherwise. The corresponding complementary error function

$$P_R = \text{erfc}\left(\frac{|V_N(obs) - 2N\pi(1-\pi)|}{2\sqrt{2N}\pi(1-\pi)}\right)$$

is calculated [5][15]. A run threshold of $P_{RTh} = 0.9$ is used to filter the

sequences, so the RR is kept if the sequence has

$$P_R \geq 0.9$$

- **MSR:** MSR is considered to evaluate the AC of the sequences. An MSR threshold of $MSR_{Th} = 0.2$ is used to filter the sequences, so the RR is kept if the sequence has

$$MSR < 0.2$$

Second Stage: To reduce the computational complexity, all sequences are first generated with fixed $SV = 1$. The RRs obtained after first stage of filtering are then used to generate sequences for all 2^n SV. They are further filtered based on the rules which maintain a relatively unchanged LC of no more than $\pm 10\%$ for all 2^n SVs [5] and pass the criteria

$$P_B \geq 0.5$$
$$P_R \geq 0.5$$
$$MSR < 0.2$$

for all SVs. The objective here is to obtain good sequences irrespective of the initial state of the CA, which is similar to m-sequences.

3.2 Initial Observations

The sequences generated after a single cell replacement with all balanced RRs in the range 0 to 4294967295 for 2D CAs of sizes $n = 5$, 6, 7, 8 and 9 were filtered based on the criteria above. After the first stage of filtering, the following observations were made.

1. The value of OC has a negligible affect on LC if all other inputs are fixed. Examples of this behavior for 2D CAs of sizes $n = 7$, 8 and 9 are shown in Tables 3.1, 3.2 and 3.3, respectively. In these tables, LRC, LR, RR, RC and SV are constant and only OC is varied. Note that the value of LC is close to $2^n/2$ for all the values of OC. Hence, $OC = 4$ was fixed to reduce computational complexity.

2. For each CC representative for the same size 2D CA, different RRs generated sequences that passed the filtering criteria. For 2D CAs of size $n = 9$, no overlap

was found between the RRs of the respective CC representatives obtained after the first stage of filtering. The first stage filtering criteria were then relaxed to

$$P_B \geq 0.8$$
$$P_R \geq 0.8$$
$$MSR < 0.2$$

which resulted in

970 filtered RRs for LRC = L7, L25,
1042 filtered RRs for LRC = L28, L27,
1066 filtered RRs for LRC = L30, L11,
976 filtered RRs for LRC = L30, L27,
1137 filtered RRs for LRC = L25, L14,
1130 filtered RRs for LRC = L25, L31 and
1337 filtered RRs for LRC = L21, L27.

An overlap of only 8 RRs was found between two of the seven CC representatives.

3. For different size 2D CAs with fixed values of SV, RC, OC and LRC, different RRs generated sequences that passed the first stage of filtering criteria. Table 3.4 shows the sequences generated by RR = 361019349 for 2D CAs of sizes n = 5, 6, 7, 8 and 9 for LRC = L28, L27. RR = 361019349 is one of the 225 RRs that generated sequences which passed the first stage of filtering criteria for 2D CA size n = 9 with LRC = L28, L27. Note that the sequences generated by RR = 361019349 for n = 5, 6, 7 and 8 fail the filtering criteria but pass for n = 9.

4. The maximum linear complexity obtained for different sizes of 2D CAs for each CC representative is close to $2^n/2$. Table 3.5 shows the maximum LC obtained for each of the seven CC representatives for 2D CAs of size n = 9 with SV = 1, RC = 5 and OC = 4. Figure 3.1 shows a plot of the maximum LC obtained for 2D CAs of sizes n = 5 to 9. Note that the maximum LC approximately doubles with an increase of n by 1.

5. Odd RRs generated all non-zero sequences for $SV = 0$, as their LSB bit is 1 and for the neighborhood state 00000, the next state is 1. Even RRs generated all zero sequences for $SV = 0$, since all the linear rules for 2D CA are also even as discussed in Section 2.2.1 (initial observation 1). For even RRs, $SV = 0$ was ignored during the second stage of filtering.

The results obtained from the first stage of filtering were then considered in the second stage of filtering discussed in Section 3.1 to obtain the final results.

OC	RC	RR	LRC	LR	SV	LC	B	AC	MSR	S
1	5	554823149	L7, L25	0110111	1	63	-9	127,-9,3,-5,3,-37, ...	0.37	1010101...
2	5	554823149	L7, L25	0110111	1	64	-5	127,3,11,3,7,7, ...	0.18	0100010...
3	5	554823149	L7, L25	0110111	1	63	-5	127,3,11,3,7,7, ...	0.18	0010001...
4	5	554823149	L7, L25	0110111	1	65	1	127,3,7,-5,-1,-1, ...	0.12	1011101...
5	5	554823149	L7, L25	0110111	1	64	-7	127,-5,-5,7,-1,-9, ...	0.21	1001001...
6	5	554823149	L7, L25	0110111	1	63	-3	127,-1,-37,11,3,-5, ...	0.25	1101100...
7	5	554823149	L7, L25	0110111	1	65	-1	127,-1,11,-5,-1,-1, ...	0.15	0101101...

Table 3.1: LC Versus OC for $n = 7$, $RR = 554823149$ and $RC = 5$

OC	RC	RR	LRC	LR	SV	LC	B	AC	MSR	S
1	5	52621007	L7, L25	11001111	1	128	-1	255,-1,-1,-1,-1,-1, ...	0.17	0011010...
2	5	52621007	L7, L25	11001111	1	128	-1	255,-1,-1,-1,-1,-1, ...	0.17	0110101...
3	5	52621007	L7, L25	11001111	1	128	1	255,-1,-1,-129,-1,-1, ...	0.31	1110001...
4	5	52621007	L7, L25	11001111	1	128	1	255,-1,-1,-1,-1,-1, ...	0.09	0110111...
5	5	52621007	L7, L25	11001111	1	128	1	255,-129,63,-33,-17,23, ...	0.25	10101101...
6	5	52621007	L7, L25	11001111	1	128	1	255,-1,-1,63,-33,15, ...	0.25	0000011...
7	5	52621007	L7, L25	11001111	1	128	1	255,-1,-1,-1,-1,-1, ...	0.09	0001101...
8	5	52621007	L7, L25	11001111	1	128	1	255,-1,-1,-1,-1,-1, ...	0.14	0101100...

Table 3.2: LC Versus OC for $n = 8$, $RR = 52621007$ and $RC = 5$

OC	RC	RR	LRC	LR	SV	LC	B	AC	MSR	S
1	5	99790800	L7, L25	011011001	1	256	1	511,-1,-1,-1,-1,-21, ...	0.18	0100000...
2	5	99790800	L7, L25	011011001	1	255	1	511,-1,-1,-1,-1,-1, ...	0.13	0010011...
3	5	99790800	L7, L25	011011001	1	256	1	511,-1,-1,-1,-1,-1, ...	0.13	0001010...
4	5	99790800	L7, L25	011011001	1	257	1	511,-1,-65,-9,11,15, ...	0.1	1110101...
5	5	99790800	L7, L25	011011001	1	255	1	511,63,7,-21,-5,-13, ...	0.13	0001100...
6	5	99790800	L7, L25	011011001	1	256	1	511,-1,-1,-1,-1,3, ...	0.1	0000011...
7	5	99790800	L7, L25	011011001	1	256	1	511,-1,-1,-1,-1,-1, ...	0.12	0010010...
8	5	99790800	L7, L25	011011001	1	255	1	511,-1,-1,-1,-1,-1, ...	0.12	0110110...
9	5	99790800	L7, L25	011011001	1	255	1	511,-1,-1,-1,-1,-1, ...	0.11	1011010...

Table 3.3: LC Versus OC for $n = 9$, $RR = 99790800$ and $RC = 5$

n	OC	RC	RR	LRC	LR	SV	LC	B	AC	MSR	S
5	4	5	361019349	L28, L27	11010	1	1	31	31,31,31,31, ...	1	1111111...
6	4	5	361019349	L28, L27	110011	1	22	-11	63,3,-1,-1, ...	0.68	1110110...
7	4	5	361019349	L28, L27	1001101	1	0	-127	127,127,127,127, ...	1	000000...
8	4	5	361019349	L28, L27	10011111	1	6	-141	255,27,27,143, ...	0.98	1000001...
9	4	5	361019349	L28, L27	101111010	1	256	1	511,3,-1,7, ...	0.15	0110011...

Table 3.4: Sequences Generated for $n = 5$ to 9, $RR = 361019349$ and $LRC =$ L28, L27

OC	RC	RR	LRC	LR	SV	LC	B	MSR
4	5	290319915	L7, L25	011011001	1	261	3	0.12
4	5	1620744815	L28, L27	101111010	1	262	3	0.13
4	5	3051654437	L30, L11	000111110	1	262	3	0.14
4	5	2614969442	L30, L27	001001111	1	263	3	0.14
4	5	2948091975	L25, L14	001101110	1	261	3	0.1
4	5	397071510	L25, L31	110100101	1	262	3	0.29
4	5	2983375986	L21, L27	110101001	1	261	1	0.09

Table 3.5: Maximum LC Obtained for all Seven CC Representatives for $n = 9$, $RC = 5$, $OC = 4$ and $SV = 1$

3.3 Filter Results for $n = 9$

Results were first generated for 2D CAs of size $n = 9$ by replacing the center cell ($RC = 5$) with all balanced non-linear rules. $RC = 5$ (center cell) was selected so that the neighborhood size of the cell to which the RR is assigned is maximum (5). $RC = 5$ was fixed for other sizes as well to reduce the computational complexity as many sequences generated with $RC = 5$ passed the filtering criteria. Sequences were generated for the seven CC representatives (LRC) given in Table 2.11 and the LR values for the respective LRC given in Table 2.9 were used. $SV = 1$ and $OC = 4$ were also fixed to obtain the initial results as discussed in Sections 3.1 and 3.2, respectively. By fixing the values of SV, OC, RC and LR, and reducing the LRC values to seven, the number of iterations using (2.1) was reduced to

$$7 \times 2^1 \times 2^1 \times 1 \times 601080359 \times 1 = 4207562513.$$

Sequences generated by 2139 RRs passed the first stage of filtering and they were then used to generate sequences for all 2^n SVs resulting in $2139 \times 2^9 = 1095168$ additional iterations.

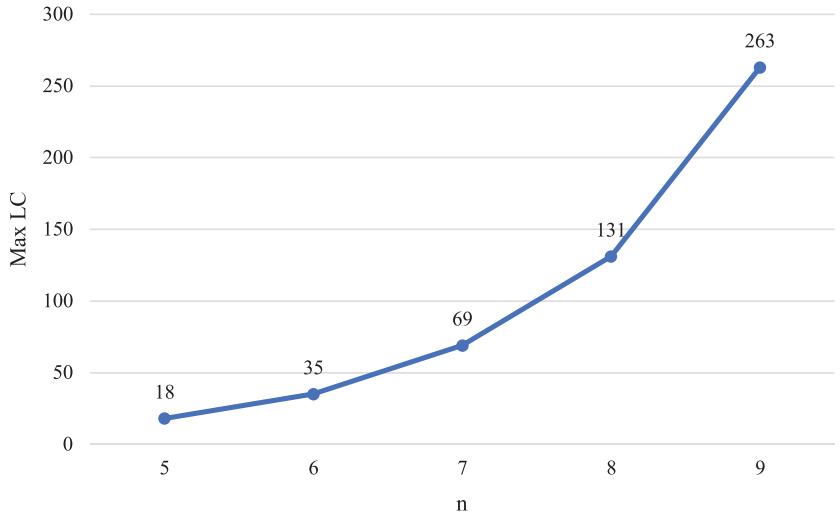


Figure 3.1: Maximum LC obtained after single cell replacement with a balanced non-linear rule for 2D CAs of sizes $n = 5$ to 9.

It was observed that both even and odd non-linear rules (RRs) passed the first stage of filtering but only even RRs passed the second stage of filtering. Column two of Table 3.6 shows the numbers of RRs that passed the first stage of filtering for each of the seven LRC. Some of these RRs are given in column three. It can be seen that both even and odd RRs are present in Table 3.6. Tables 3.7 and 3.8 show the numbers of RRs that passed the second stage of filtering for each of the seven LRC along with the RRs for the respective LRCs.

The best filtered results obtained for each CC representative are discussed below.

1. For LRC = L7, L25, RR = 1725929730 gave the best results. The sequences generated with RR = 1725929730 for the non-zero SVs have $MSR = 0.08$, $P_B = 0.96$, and $P_R = 0.89$ for the odd SVs and $P_R = 0.96$ for the even SVs. The results are shown in Table 3.9. The minimum LC is 253 and the maximum is 258.

2. For LRC = L28, L27, RR = 1398495324, 1521459290, 1528288344, 1941406796, 3404668986, 3537245726, 4214735880 and 4216804360 gave the best results. The sequences generated for the non-zero SVs with these rules have $MSR = 0.1$, $P_B = 0.96$ and $P_R = 0.96$ or 0.89. The minimum LC is 251 and the maximum

LRC	No.	*RR*s
L7, L25	317	16711440, 32894880, 35381070, 38657835, 66244560, 81182610, 72990570, 87011085, 99790800, 99987360, 100249440, 100380480, 108109800, 115121970, 115121970
L28, L27	225	323059164, 361019349, 418324699, 445168602, 459565016, 472899795, 484315859, 537590511, 651762150, 665690596, 716670186, 720831722, 839709646, 846221262
L30, L11	314	28093687, 38785275, 40672507, 42329595, 56989171, 59369203, 60925939, 65572595, 72637949, 78227197, 85816565, 92923637, 95266037, 97307893, 100990457
L30, L27	453	12766207, 37806075, 39607547, 39345915, 4624075, 46320635, 47860475, 50072827, 67761917, 73571325, 74981117, 74650621, 75372797, 76574717, 78655458
L25, L14	121	26476140, 37027275, 45284685, 78904140, 105970095, 146732865, 165475875, 186381540, 195884115, 244445550, 279965520, 336129015, 345566055, 372566475
L25, L31	301	252679850, 253169612, 254482289, 255020458, 255022506, 255053012, 255052970, 255054891, 257255850, 257265322, 257283250, 258545586, 258566570, 259116264
L21, L27	409	4015103, 3843071, 8323583, 7244287, 41763263, 35301311, 37282751, 45150911, 45671103, 47502527, 102061983, 110450335, 157604207, 193257007, 272565239

Table 3.6: Number Of *RR*s That Passed the First Stage of Filtering for the Respective *LRC*s for $n = 9$, $OC = 4$, $SV = 1$ and $RC = 5$

is 260.

3. For LRC = L30, L11, RR = 2307253734 and 3114903078, gave the best results. The sequences generated for the non-zero SVs with both these rules have MSR = 0.08, P_B = 0.96 and P_R = 0.96 or 0.89. The minimum LC is 253 and the maximum is 259.

4. For LRC = L30, L27, RR = 1840917140, 2902001324, 3917026950 and 3987876740 gave the best results. The sequences generated for the non-zero SVs with these rules have MSR = 0.08, P_B = 0.96 and P_R = 0.96 or 0.89. The minimum LC is 251 and the maximum is 261.

5. For LRC = L25, L14, none of the RRs passed the second stage of filtering.

6. For LRC = L25, L31, RR = 1767184360 gave the best results. The sequences generated with RR = 1767184360 for the non-zero SVs have MSR = 0.08, P_B

= 0.96 and P_R = 0.96 or 0.89. The minimum LC is 252 and the maximum is 260.

7. For LRC = L21, L27, RR = 2518583190, 4094226384, 4271314560 and 4272249472 gave the best results. The sequences generated for the non-zero SVs with these rules have MSR = 0.09, P_B = 0.96 and P_R = 0.96 or 0.89. The minimum LC is 250 and the maximum is 261.

From these results it can be seen that the sequences generated by each of the RRs discussed above for the respective LRCs exhibit excellent randomness properties and high linear complexity. The sequence generated with RR = 1725929730, for LRC = L28, L27 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size n = 9 after single cell replacement with a non-linear rule.

Comparison with an m-sequence: Table 3.10 compares the 2D CA of size n = 9 sequence generated using LRC = L7, L25, LR = 011011001 = 217, RR = 1725929730, RC = 5, OC = 4 and SV = 1 with the m-sequence given in Table 2.9 for n = 9 and LRC = L7, L25. The linear complexity of the 2D CA sequences is 256 and is much higher than that of the m-sequence which is 9. The balance is 1 and P_R is 0.96 which are excellent and equal to those of the m-sequence. The MSR is 0.08, which is very good, but not as good as that of the m-sequence (0).

Comparison with a 1D CA sequence: Table 3.11 compares the sequence generated using LRC = L7, L25, LR = 011011001, RR = 1725929730, RC = 5, OC = 4 and SV = 1 with the filtered sequence obtained in [5] for a 1D CA of size n = 9 using linear rules 90 and 150, LR = 100110001 (where rule 90 = 0 and rule 150 = 1), OC = 2, RR = 163, RC = 8 and SV = 1. LC of the 2D CA sequence is 256 and that of the 1D CA sequence is 253. The P_B and P_R for the 2D CA sequence are 0.96 as compared to 0.76 and 0.51 for the 1D CA sequence. The MSR of the 2D CA sequence is 0.08 and is lower than that of the 1D CA sequence which is 0.12. Thus, the 2D CA sequence has better randomness properties.

3.4 Filter Results for $n = 8$

Results for 2D CAs of size $n = 8$ were obtained with $RC = 5$ using all balanced non-linear rules. Sequences were generated for all seven CC representatives (LRC) given in Table 2.11 and the LR values for the respective LRC given in Table 2.8 were used. $SV = 1$ and $OC = 4$ were used as discussed in Sections 3.1 and 3.2. For $n = 8$, values of all the parameters in (2.1) are same as with $n = 9$ so the number of iterations for $n = 8$ is the same as with $n = 9$. Many different RRs passed the first stage of filtering for each of the respective LRCs except for LRC = L30, L27. Column two of Table 3.12 shows the numbers of RRs that passed the first stage of filtering for each of the seven LRCs. Some of the corresponding RRs are given in column three. It was observed that both even and odd non-linear rules (RRs) passed the first stage of filtering but none of the odd RRs passed the second stage of filtering which is similar to the results for $n = 9$.

The best filtered results obtained for each CC representative are discussed below.

1. For LRC = L7, L25, only odd RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

2. For LRC = L28, L27, all 12870 RRs that passed the first stage of filtering criteria generated the same output sequences and passed the second stage of filtering. All of these RRs are even. The sequences generated for the non-zero SVs by these rules have $MSR = 0.18$, $P_B = 0.95$ and the values of $P_R = 0.85$ or 0.95. The minimum LC is 123 and the maximum is 133.

3. For LRC = L30, L11, only odd RRs generated sequences that passed the first stage of filtering and none of these passed the second stage of filtering.

4. For LRC = L30, L27, none of the RRs passed the first stage of filtering.

5. For LRC = L25, L14, both even and odd RRs generated sequences that passed the first stage of filtering. All the even RRs generated the same output sequence and all the odd RRs generated the same output sequence. None of these sequences passed the second stage of filtering.

6. For LRC = L25, L31, all 60056 RRs that passed the first stage of filtering criteria passed the second stage of filtering. Examples of the RRs that generated

the best sequences are RR = 303295980, 303525356, 303541740, 303556076 and 303558116. The sequences obtained for non-zero SVs using these rules have $MSR = 0.12$, $P_B = 0.95$ and $P_R = 0.85$ or 0.95. The minimum LC is 124 and the maximum is 131.

7. For LRC = L21, L27, all 102960 RRs that passed the first stage of filtering passed the second stage of filtering. Examples of the RRs that generated the best sequences are RR = 36830670, 37076430, 37092686 and 37060046. The sequences obtained for non-zero SVs using these rules have $MSR = 0.11$, $P_B = 0.95$ and $P_R = 0.85$ or 0.95. The minimum LC is 124 and the maximum is 131. The results for RR = 36830670 for all SVs are given in Table 3.9.

The sequence generated with RR = 36830670, for LRC = L21, L27 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 8$ after single cell replacement with a non-linear rule.

Comparison with an m-sequence: Table 3.14 compares the 2D CA of size $n = 8$ sequence generated using LRC = L21, L27, LR = 00111111 = 63, RR = 36830670, $RC = 5$, $OC = 4$ and $SV = 1$ with the m-sequence given in Table 2.8 for $n = 8$ and LRC = L21, L27. The linear complexity of the 2D CA sequences is 130 and is much higher than that of the m-sequence which is 8. The balance is 1 and P_R is 0.95 which are excellent and equal to those of the m-sequence. The MSR is 0.11, which is good, but not as good as that of the m-sequence (0).

Comparison with a 1D CA sequence: Table 3.15 compares the sequence generated using LRC = L21, L27, LR = 00111111, RR = 36830670, $RC = 5$, $OC = 4$ and $SV = 1$ with the filtered sequence obtained in [5] for a 1D CA of size $n = 8$ using linear rules 90 and 150, LR = 01011101 (where rule 90 = 0 and rule 150 = 1), $OC = 2$, $RR = 225$, $RC = 4$ and $SV = 1$. The linear complexity is 130 for both the 1D CA and 2D CA sequences. The P_B and P_R for the 2D CA sequence are 0.95 as compared to 0.49 and 0.43 for the 1D CA sequence. The MSR of the 2D CA sequence is 0.11 and is significantly lower than that of the 1D CA sequence which is 0.22. Thus, the 2D CA sequence has better randomness properties.

3.5 Filter Results for $n = 7$

Results for 2D CAs of size $n = 7$ were obtained with $RC = 5$ using all balanced non-linear rules. Sequences were generated for all seven CC representatives (LRC) given in Table 2.11 and the LR values for the respective LRC given in Table 2.7 were used. $SV = 1$ and $OC = 4$ were used. For $n = 7$, values of all the parameters in (2.1) are same as with $n = 9$ so the number of iterations for $n = 7$ is the same as with $n = 9$. Many RRs passed the first stage of filtering for each of the respective LRCs and some of the corresponding RRs are given in Table 3.16. Column two of Table 3.16 shows the numbers of RRs that passed the first stage of filtering for each of the seven LRCs. It was observed that both even and odd non-linear rules (RRs) passed the first stage of filtering but none of the odd RRs passed the second stage of filtering which is a similar to the results for $n = 8$ and 9.

The best filtered results obtained for each CC representative are discussed below.

1. For LRC = L7, L25, both even and odd RRs generated sequences that passed the first stage of filtering but sequences generated with only even RRs passed the second stage of filtering. Examples of the RRs that generated the best sequences for $n = 7$ are RR = 554884830, 555114206 and 555130590. The sequences obtained for the non-zero SVs with these rules have $MSR = 0.12$, $P_B = 0.93$ and $P_R = 0.79$ or 0.93. The minimum LC is 62 and the maximum is 66. The results for RR = 554884830 for all SVs are shown in Table 3.17.

2. For LRC = L28, L27, of the 38610 RRs that passed the first stage of filtering, only the sequences generated by even rules passed the second stage of filtering. The sequences generated for non-zero SVs with these rules have $MSR = 0.18$, $P_B = 0.93$ and $P_R = 0.79$ or 0.93. The minimum LC is 62 and the maximum is 67.

3. For LRC = L30, L11, only odd RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

4. For LRC = L30, L27, only odd RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

5. For LRC = L25, L14, only even RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

6. For LRC = L25, L31, all 25740 RRs that passed the first stage of filtering also passed the second stage of filtering. These rules generated sequences with the similar randomness properties. For non-zero SVs, the sequences generated by these rules have $MSR = 0.15$, $P_B = 0.93$ and $P_R = 0.79$ or 0.93 (depending upon the SV for each of these sequences). The minimum LC is 62 and the maximum is 65.

7. For LRC = L21, L27, only odd RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

The sequence generated with $RR = 554884830$ for LRC = L7, L25 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 7$ after single cell replacement with a non-linear rule.

Comparison with an m-sequence: Table 3.18 compares the 2D CA of size n= 7 sequence generated using LRC = L7, L25, LR = 0110111 = 55, RR = 554884830, $RC = 5$, $OC = 4$ and $SV = 1$ with the m-sequence given in Table 2.7 for $n = 7$ and LRC = L7, L25. The linear complexity of the 2D CA sequences is 64 and is much higher than that of the m-sequence which is 7. The balance is 1 and P_R is 0.93 which are excellent and equal to those of the m-sequence. The MSR is 0.12, which is good, but not as good as that of the m-sequence (0.01).

Comparison with a 1D CA sequence: Table 3.15 compares the sequence generated using LRC = L7, L25, LR = 0110111, $RR = 554884830$, $RC = 5$, OC = 4 and $SV = 1$ with the filtered sequence obtained in [5] for a 1D CA of size n = 7 using linear rules 90 and 150, LR = 0101011 (where rule 90 = 0 and rule 150 = 1), $OC = 2$, $RR = 18$, $RC = 6$ and $SV = 1$. Both the 1D and 2D sequences have $LC = 64$ and $PB = 0.93$. P_R for the 2D CA sequence is 0.93 as compared to 0.66 for the 1D CA sequence. The MSR of the 2D CA sequence is 0.11 and is significantly lower than that of the 1D CA sequence which is 0.29. Thus, the 2D CA sequence has better randomness properties.

3.6 Filter Results for $n = 6$

For 2D CAs of size $n = 6$, two of the seven CC representatives (LRC = L7, L25 and L21, L27) did not generate m-sequences as discussed in Section 2.2.2. The results here

for $n = 6$ were obtained for the five CC representatives that generated m-sequences. The LR values of those LRCs are given in Table 2.6. $RC = 5$, $OC = 4$ and $SV = 1$ were used. As the number of LRC is 5, the number of iterations for $n = 6$ using (2.1) is reduced to

$$5 \times 2^1 \times 2^1 \times 1 \times 601080359 \times 1 = 3005401795.$$

Similar to 2D CAs of sizes $n = 7$, 8 and 9, many different RRs passed the first stage of filtering for each of the five LRCs. These RRs included both even and odd RRs but unlike for $n = 7$, 8 and 9, only odd RRs passed the second stage of filtering.

The results obtained for each CC representative are discussed below.

1. For LRC = L28, L27, only even RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

2. For LRC = L30, L11, both even and odd RRs generated sequences that passed the first stage of filtering but sequences generated with only odd RRs passed the second stage of filtering. Examples of the RRs that generated the best sequences for $n = 6$ are RR = 319880399, 320109775 and 320126159. The sequences obtained for all 2^n SVs (including $SV = 0$) using these rules have $MSR = 0.17$, $P_B = 0.9$ and $P_R = 0.7$ or 0.9. The minimum LC is 30 and the maximum is 33. The results for $RR = 319880399$ for all SVs are given in Table 3.20.

3. For LRC = L30, L27, both even and odd RRs generated sequences that passed the first stage of filtering but only the sequences generated by odd RRs passed the second stage of filtering. Sequences generated using RR = 589364431, 589593807 and 589610191 for all 2^n SVs (including $SV = 0$) have $MSR = 0.17$, $P_B = 0.9$ and $P_R = 0.7$ or 0.9. The minimum LC is 29 and the maximum is 33. .

4. For LRC = L25, L14, only odd RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

5. For LRC = L25, L31, only even RRs generated sequences that passed the first stage of filtering. None of these sequences passed the second stage of filtering.

The sequence generated with $RR = 319880399$ for LRC = L30, L11 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 6$ after single cell replacement with a non-linear rule.

Comparison with an m-sequence: Table 3.18 compares the 2D CA of size $n = 6$ sequence generated using LRC = L30, L11, $LR = 010101 = 21$, $RR = 319880399$, $RC = 5$, $OC = 4$ and $SV = 1$ with the m-sequence given in Table 2.6 for $n = 6$ and LRC = L30, L11. The linear complexity of the 2D CA sequences is 32 and is much higher than that of the m-sequence which is 6. The balance is 1 and P_R is 0.9 which are excellent and equal to those of the m-sequence. The MSR is 0.17, which is good, but not as good as that of the m-sequence (0.02).

Comparison with a 1D CA sequence: Table 3.15 compares the sequence generated using LRC = L30, L11, $LR = 010101$, $RR = 319880399$, $RC = 5$, $OC = 4$ and $SV = 1$ with the filtered sequence obtained in [5] for a 1D CA of size $n = 6$ using linear rules 90 and 150, $LR = 101110$ (where rule 90 = 0 and rule 150 = 1), $OC = 2$, $RR = 86$, $RC = 2$ and $SV = 1$. Both the 1D and 2D CA sequences have $P_B = 0.9$ and $MSR = 0.17$. P_R for the 2D CA sequence is 0.9 as compared to 0.7 for the 1D CA sequence. Thus, the 2D CA sequence is slightly better than the 1D CA sequence.

3.7 Filter Results for $n = 5$

For 2D CAs of size $n = 5$, results were obtained with $RC = 5$ using all balanced non-linear rules. Sequences were generated for all seven CC representatives given in Table 2.11 and the LR values for the respective LRCs given in Table 2.6. $SV = 1$ and $OC = 4$ were used. For $n = 5$, values of all the parameters in (2.1) are same as with $n = 9$ so the number of iterations for $n = 5$ is the same as with $n = 9$. None of the sequences generated passed the first stage of filtering.

LRC = L25, L14 gave the best results with some RRs before the first stage of filtering. Examples of these RRs are $RR = 285339375$, 285437679, 285454063 and 285462255. Sequences were generated using these rules for all 2^n SVs. An all-zero sequence was obtained for $SV = 12$ for all rules. The sequences obtained for the

$2^n - 1$ SVs (excluding $SV = 12$) using these rules have $MSR = 0.23$, $P_B = 0.86$ and $P_R = 0.85$ or 0.59. The minimuim LC is 15 and the maximum is 17. The results for $RR = 285339375$ are given in Table 3.23.

The sequence generated with $RR = 285339375$ for LRC = L25, L14 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 5$ after single cell replacement with a non-linear rule.

Comparison with an m-sequence: Table 3.24 compares the 2D CA of size $n = 5$ sequence generated using LRC = L25, L14, $LR = 10000 = 16$, $RR = 285339375$, $RC = 5$, $OC = 4$ and $SV = 1$ with the m-sequence given in Table 2.4 for $n = 5$ and LRC = L25, L14. The linear complexity of the 2D CA sequences is 16 and is much higher than that of the m-sequence which is 5. The balance is 1 which is excellent and equal to that of the m-sequence. P_R is 0.59 which is less than that of the m-sequence which is 0.85. The MSR is 0.23, which is good, but not as good as that of the m-sequence (0.03).

Comparison with a 1D CA sequence: Table 3.25 compares the sequence generated using LRC = L25, L14, $LR = 10000$, $RR = 285339375$, $RC = 5$, $OC = 4$ and $SV = 1$ with the filtered sequence obtained in [5] for a 1D CA of size $n = 5$ using linear rules 90 and 150, $LR = 00111$ (where rule 90 = 0 and rule 150 = 1), $OC = 2$, $RR = 107$, $RC = 4$ and $SV = 1$. Both the 1D and 2D sequences have $LC = 16$ and $P_R = 0.59$. P_B for the 2D CA sequence is 0.86 as compared to 0.79 for the 1D CA sequence. MSR of the 2D CA sequence is 0.23 and is lower than that of the 1D CA sequence which is 0.29. Thus, the 2D CA sequence has better randomness properties.

3.8 Filter Results for $n = 10$, 11 and 12

For 2D CAs of sizes $n = 10$, 11 and 12 results were obtained with $RC = 6$, $OC = 5$ and $SV = 1$ using all balanced even non-linear rules. Sequences were generated for LRC = L28, L27 only and the LR values for the respective n and LRCs given in Tables 2.12, 2.13 and 2.14 were used. Many different RRs passed the first stage of filtering for each 2D CA size. These rules were then used to generate sequences for all non-zero SVs for the second stage of filtering. Filtered results obtained for each

n are discussed below.

2D CA size $n = 10$: RR = 2312541294, 2457129398 and 2467649334 gave the best results for $n = 10$. The sequences generated for the non-zero SVs with these rules have $MSR = 0.08$, $P_B = 0.98$ and $P_R = 0.98$ or 0.93. The minimum LC is 506 and the maximum is 517. The results for RR = 2312541294 for all SVs are given in Table 3.26. The sequence generated with $SV = 1$ and RR = 2312541294 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 10$ after single cell replacement with a non-linear rule.

- **Comparison with an m-sequence:** Table 3.27 compares the 2D CA of size $n = 10$ sequence generated using LRC = L28, L27, LR = 1111101101 = 1005, RR = 2312541294, $RC = 6$, $OC = 5$ and $SV = 1$ with the m-sequence given in Table 2.12 for $n = 10$ and LRC = L28, L27. The linear complexity of the 2D CA sequences is 512 and is much higher than that of the m-sequence which is 10. The balance is 1 and P_R is 0.98 which are excellent and equal to those of the m-sequence. The MSR is 0.08, which is very good, but not as good as that of the m-sequence (0).
- **Comparison with a 1D CA sequence:** Table 3.28 compares the sequence generated using LRC = L28, L27, LR = 1111101101, RR = 2312541294, $RC = 6$, $OC = 5$ and $SV = 1$ with the filtered sequence obtained in [5] for a 1D CA of size $n = 10$ using linear rules 90 and 150, LR = 1111110000 (where rule 90 = 0 and rule 150 = 1), $OC = 2$, RR = 154, $RC = 4$ and $SV = 1$. The linear complexity is 512 for the 2D CA sequence as compared to 513 for the 1D CA sequence. The P_B and P_R values for the 2D CA sequence are 0.98 as compared to 0.33 and 0.53 for the 1D CA sequence. The MSR of the 2D CA sequence is 0.08 and is lower than that of the 1D CA sequence which is 0.10. Thus, the 2D CA sequence has better randomness properties.

2D CA size $n = 11$: RR = 509237910, 1269124080, 1272103830, 2526451380 and 2528382900 gave the best results for $n = 11$. The sequences generated for the non-zero SVs with these rules have $MSR = 0.06$, $P_B = 0.98$ and $P_R = 0.98$ or 0.95. The minimum LC is 1017 and the maximum is 1030. The results for

RR = 509237910 for all SVs are given in Table 3.29. The sequence generated with $SV = 1$ and RR = 509237910 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 11$ after single cell replacement with a non-linear rule.

- **Comparison with an m-sequence:** Table 3.30 compares the 2D CA of size $n = 11$ sequence generated using LRC = L28, L27, LR = 11111010111 = 2007, RR = 509237910, $RC = 6$, $OC = 5$ and $SV = 1$ with the m-sequence given in Table 2.13 for $n = 11$ and LRC = L28, L27. The linear complexity of the 2D CA sequences is 1024 and is much higher than that of the m-sequence which is 11. The balance is 1 and P_R is 0.98 which are excellent and equal to those of the m-sequence. The MSR is 0.06, which is excellent, but not as good as that of the m-sequence (0).
- **Comparison with a 1D CA sequence:** Table 3.31 compares the sequence generated using LRC = L28, L27, LR = 11111010111, RR = 509237910, $RC = 6$, $OC = 5$ and $SV = 1$ with the filtered sequence obtained in [5] for a 1D CA of size $n = 11$ using linear rules 90 and 150, LR = 01011000010 (where rule 90 = 0 and rule 150 = 1), $OC = 2$, $RR = 86$, $RC = 10$ and $SV = 1$. The linear complexity is 1024 and the MSR is 0.06 for both the 1D CA and 2D CA sequences. The P_B and P_R values for the 2D CA sequence are 0.98 as compared to 0.98 and 0.95 for the 1D CA sequence. Thus, the 2D CA sequence has slightly better randomness properties.

2D CA size $n = 12$: RR = 2809934922 gave the best results for $n = 12$. The sequences generated for the non-zero SVs with this rule have $MSR = 0.05$, P_B = 0.99 and P_R = 0.99 or 0.96. The minimum LC is 2043 and the maximum is 2053. The results for RR = 2809934922 for all SVs are given in Table 3.32. The sequence generated with $SV = 1$ and RR = 2809934922 is now compared with an m-sequence and the filtered sequence obtained in [5] for a 1D CA of size $n = 12$ after single cell replacement with a non-linear rule.

- **Comparison with an m-sequence:** Table 3.34 compares the 2D CA of size $n = 12$ sequence generated using LRC = L28, L27, LR = 111111110011 = 4083, RR = 2809934922, $RC = 6$, $OC = 5$ and $SV = 1$ with the m-sequence given in Table 2.14 for $n = 12$ and LRC = L28, L27. The linear

complexity of the 2D CA sequences is 2048 and is much higher than that of the m-sequence which is 12. The balance is 1 and P_R is 0.99 which are excellent and equal to those of the m-sequence. The MSR is 0.05, which is excellent, but not as good as that of the m-sequence (0).

- **Comparison with a 1D CA sequence:** Table 3.35 compares the sequence generated using LRC = L28, L27, LR = 111111110011, RR = 2809934922, RC = 6, OC = 5 and SV = 1 with the filtered sequence obtained in [5] for a 1D CA of size n = 12 using linear rules 90 and 150, LR = 001001111010 (where rule 90 = 0 and rule 150 = 1), OC = 2, RR = 99, RC = 3 and SV = 1. The linear complexity is 2048 for the 2D CA sequence as compared to 2049 for the 1D CA sequence. The P_B and P_R values for the 2D CA sequence are 0.99 as compared to 0.98 and 0.92 for the 1D CA sequence. The MSR of the 2D CA sequence is 0.05 and is significantly lower than that of the 1D CA sequence which is 0.23. Thus, the 2D CA sequence has better randomness properties.

3.9 Filter Results for n = 13 and 14

For 2D CAs of sizes n = 13 and 14 results were obtained with RC = 6, OC = 5 and SV = 1 using all balanced even non-linear rules. Sequences were generated for LRC = L28, L27 only and the LR values for the respective n and LRCs given in Tables 2.15 and 2.16 were used. Many different RRs passed the first stage of filtering for each 2D CA size. Filtered results obtained after the first stage of filtering for each n are discussed below.

2D CA size n = 13: RR = 370400470, 711419114 and 2810623652 gave the best results for n = 13. The sequences generated for SV = 1 with these rules have MSR = 0.04, P_B = 0.99 and P_R = 0.99. The minimum LC is 4096 and the maximum is 4099.

2D CA size n = 14: RR = 1001200268 gave the best results for n = 14. The sequence generated for SV = 1 with this rule has MSR = 0.03, P_B = 0.99 and P_R = 0.99. The LC is 8192.

3.10 Execution Time

Computing resources from Compute Canada were used to run the 2D CA evaluation system and obtain results for 2D CAs of sizes $n = 5$ to 14. Because of the high computational complexity, multiple instances of the evaluation system were executed on the Compute Canada nodes where each instance was assigned a different subset of the balanced non-linear rules in the range 0 to 4294967295. Each instance of the evaluation system utilized 20 CPU cores using the Python Joblib library. All results were obtained after a linear rule replacement with all balanced non-linear rules. The time taken for a given CA size was dependent on the number of iterations and the time taken for each iteration. After fixing and reducing the number of input parameters, the number of iterations for $n = 5$, 7, 8 and 9 was reduced to 4207562513 as discussed in Sections 3.7, 3.5, 3.4 and 3.3, respectively. For 2D CAs of size $n = 6$, the number of iterations was reduced to 3005401795 as discussed in Section 3.6. Table 3.35 shows the time taken to obtain the results for $n = 5$ to 9 in CPU hours. Column two shows the number of iterations for each value of n and column three shows the corresponding time in CPU hours. The time taken for each iteration is exponential in n as discussed in Section 2.1. Table 3.36 gives the time taken for one iteration for each value of n in milliseconds. For $n = 5$, 6, 7, 8 and 9, one iteration took 5.03, 10.42, 17.24, 33.06 and 66.12 milliseconds, respectively. Thus, with an increase in value of n by one, the time taken for an iteration approximately doubled.

LRC	No.	*RR*s
L7, L25	100	16711440, 32894880, 66244560, 81182610, 99790800, 99987360, 100249440, 100380480, 115121970, 117415680, 132026130, 148602690, 166883280, 200626080, 201150240, 234172320, 267653040, 687570240, 703950240, 718429650, 735268290, 735071730, 752303490, 754138560, 770846160, 785522130, 803081490, 803015970, 1173728160, 1190239200, 1190697840, 1341721440, 1643571600, 1675151730, 1677117840, 1710926160, 1725274530, 1725929730, 1727437200, 1759148370, 1792760130, 1809664290, 1808878050, 1811171760, 1843341570, 1859787090, 1878264240, 1876101570, 2245437330, 2248058640, 2278983570, 2281080720, 2281408320, 2281604880, 2329302930, 2345945010, 2348173200, 2345682930, 2362587090, 2362652610, 2365011840, 2415134640, 2723796330, 2858243370, 2865845730, 2874623370, 2875016490, 2883143010, 2901620160, 2926646760, 2951808480, 3321864960, 3355345680, 3404747760, 3455591280, 3455656800, 3805598130, 3805663650, 3814310250, 3839275410, 3841962240, 3855720930, 3856114050, 3891691920, 3892216080, 3931197930, 3940372770, 3940045170, 3947905530, 3950002680, 3957145890, 3958653360, 3982041450, 3990495570, 3992134080, 3999076650, 4007399730, 4023910770, 4023976290, 4026007920
L28, L27	105	1378085982, 1380546910, 1386458206, 1388984926, 1390554718, 1393939804, 1394202972, 1398495324, 1395515740, 1400325212, 1406604380, 1408437340, 1404144988, 1520871002, 1521003354, 1521459290 , 1523462746, 1528288344, 1524966746, 1657289582, 1658394990, 1667589484, 1671205740, 1671800172, 1673103724, 1677460332, 1677525356, 1787082602, 1787147626, 1789046378, 1791507306, 1793860458, 1810179432, 1914556750, 1915740238, 1917548622, 1922276430, 1926765390, 1927685710, 1936024908, 1939248716, 1941406796, 1944726092, 2048251210, 3267070014, 3270386238, 3262859326, 3263477566, 3279113276, 3390042170, 3398414394, 3398931514, 3398998842, 3400699450, 3401156922, 3403885626, 3403093050, 3404668986, 3417219640, 3417869112, 3416630584, 3419870264, 3420662840, 3537508894, 3537245726, 3553762844, 3554351132, 3663156250, 3662508314, 3663288602, 3663419418, 3664601370, 3680196632, 3689556504, 3690922008, 3803481902, 3933684778, 3937313322, 3939250986, 3939381802, 3942255146, 3954740008, 4063740942, 4068719630, 4073468686, 4075234318, 4080387340, 4082455820, 4084031756, 4087060492, 4198351114, 4204435978, 4203524874, 4204305162, 4203329802, 4206658314, 4208334346, 4214735880, 4216673544, 4216804360, 4217196808, 4220884232, 4222652168, 4226621704, 4227662088
L30, L11	77	2307253734, 2310218726, 2368712932, 2366502116, 2367517924, 2372507364, 2376835812, 2380696036, 2414774496, 2576704870, 2582085990, 2611260770, 2640942692, 2646722404, 2649131364, 2650147172, 2680103008, 2683011680, 2843415206, 2846073766, 2844648614, 2848509606, 2848573094, 2872259490, 2879889826, 2881037986, 2905192100, 2909245860, 2909378212, 2911233444, 2918845092, 2939074720, 2938484128, 2939368352, 3116484390, 3114379046, 3114903078, 3118893350, 3118956838, 3152643618, 3172498980, 3172038436, 3174579748, 3177551140, 3178075172, 3179668772, 3182440228, 3211105568, 3216712224, 3216648736, 3378336966, 3378746310, 3383730374, 3409262018, 3420685250, 3420555202, 3446510788, 3446740932, 3454239684, 3454895300, 3455911108, 3475485120, 3484001984, 3488055744, 3488188096, 3648265542, 3651578182, 3651641670, 3656351814, 3689514562, 3718687044, 3715306308, 3715700292, 3722936644, 3722675012, 3752304960, 3756623424
L30, L27	166	706510010, 706640058, 708459194, 712382906, 739802812, 740473788, 744529852, 746647484, 747663292, 749382332, 751849404, 775044024, 777804984, 781609400, 788138680, 943665214, 945052990, 946443838, 974614842, 978345786, 977984058, 977917498, 978670906, 979194938, 989726778, 1010947900, 1015800380, 1044438840, 1044568888, 1045518136, 1046108728, 1046240312, 1046649656, 1047665464, 1054754872, 1746565790, 1750621854, 1753280414, 1754820254, 1761673110, 1759610782, 1771859094,

Table 3.7: Number Of *RR*s That Passed the First Stage of Filtering for the Respective *LRC*s for $n = 9$, $OC = 4$, $SV = 1$ and $RC = 5$ (Part 1)

LRC	No.	*RR*s
L30, L27	166	1775651222, 1792428442, 1786518682, 1798715794, 1798454162, 1794509210, 1805281938, 1799109778, 1809205650, 1799173266, 1820005020, 1814609564, 1811286418, 1819742620, 1820073116, 1824575388, 1830059412, 1834245524, 1835766420, 1840917140, 1842760084, 1849047448, 1843284116, 1861750424, 1865563024, 1869682576, 1874341520, 1874603152, 1874733200, 1875561104, 2018794782, 2022433310, 2025791518, 2050373914, 2047079194, 2054298394, 2065396242, 2071599634, 2071861266, 2081157660, 2080047634, 2082371612, 2086427676, 2095745564, 2097347348, 2100705556, 2103484180, 2100967956, 2112586260, 2111868692, 2113538580, 2114124568, 2114518552, 2121407256, 2121668888, 2121732376, 2122192920, 2135481872, 2136497680, 2140172048, 2145012240, 2147354640, 2820045230, 2824231342, 2857785770, 2860192426, 2887154092, 2902001324, 2901607340, 2901477292, 2920708520, 2924011176, 2928764840, 2931697832, 2931871656, 2933673128, 2935555752, 3121904938, 3134999594, 3154181932, 3160972844, 3161102892, 3189537832, 3198052392, 3201024552, 3201846824, 3204121128, 3910302598, 3917026950, 3930707594, 3935789450, 3931265930, 3938330762, 3950909570, 3954583938, 3956752770, 3960895884, 3965081996, 3971818636, 3971885196, 3977673092, 3976395652, 3983120004, 3987876740, 3988899716, 3988836228, 3998768776, 3998962312, 3988595844, 4009035144, 4005613448, 4011684992, 4014006144, 4017232768, 4017494400, 4026074752, 4023536512, 4164366606, 4208934922, 4229069580, 4229331212, 4244506636, 4243292684, 4273744904
L25, L14	0	
L25, L31	69	255020458, 255022506, 255052970, 257255850, 257265322, 258545586, 258566570, 259116264, 263327666, 263383272, 266906282, 267390898, 267406824, 267406770, 724784562, 724801202, 727017898, 731270632, 731303152, 733122218, 735317992, 1293359026, 1293366186, 1296897970, 1296905138, 1296935656, 1298740146, 1301728434, 1303554730, 1305267378, 1305775794, 1307610794, 1763136938, 1763153578, 1764478122, 1764971946, 1766667178, 1767184360, 1771474664, 2389257138, 2389291690, 2389783466, 2393516970, 2855475114, 2855490994, 2857227434, 2865507250, 2865523122, 2865539762, 3424065450, 3424072618, 3424095914, 3425389994, 3425914282, 3428128682, 3428159146, 3429446570, 3429469866, 3429968818, 3429977514, 3429970858, 3429984682, 3433720234, 3434244530, 3437800106, 3895152042, 3897895850, 3897930410, 3897944234
L21, L27	116	2486383574, 2487840214, 2502335318, 2500644694, 2511655510, 2511770198, 2512739414, 2518583190, 2520077206, 2524873110, 2533572374, 2535807766, 2540001558, 3020517330, 3023774674, 3026401746, 3028189650, 3033961682, 3035943122, 3041709394, 3042903378, 3044225362, 3046430290, 3048526418, 3049876562, 3058601362, 3057999250, 3059680658, 3070697234, 3078185234, 3075937554, 3081034258, 3083025426, 3082910738, 3086794770, 3557122004, 3560231892, 3578473812, 3580981588, 3581350228, 3585397332, 3589623892, 3587494996, 3591690132, 3594698132, 3591956372, 3592887188, 3603119252, 3604419732, 3607314196, 3611475220, 3609930516, 3611647252, 3620035604, 3620150292, 3691454404, 3691974596, 3692734404, 3708604228, 3709130564, 3713738052, 3713590596, 3718601284, 3718683204, 3722623044, 3725653892, 3726288772, 3728302980, 3728524164, 3722909764, 3730482564, 3738637444, 3742684932, 3743767300, 3747928324, 3757477892, 4094226384, 4100364752, 4096609232, 4102495952, 4101411280, 4106435792, 4111257424, 4124632144, 4126050384, 4130278288, 4130435984, 4132343184, 4137892496, 4139078288, 4140731536, 4146420496, 4140510352, 4148866320, 4155042320, 4158830608, 4159383568, 4234615232, 4232891840, 4235547072, 4237878976, 4239215296, 4239329984, 4240620736, 4243491008, 4245475136, 4255439424, 4259493952, 4257651776, 4259747904, 4262113152, 4266593664, 4271314560, 4272249472, 4274314368, 4280720128

Table 3.8: Number Of *RR*s That Passed the First Stage of Filtering for the Respective *LRC*s for $n = 9$, $OC = 4$, $SV = 1$ and $RC = 5$ (Part 2)

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
4	5	1725929730	L7, L25	011011001	1	256	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	2	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	3	254	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	4	257	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	5	253	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	6	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	7	256	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	8	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	9	255	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	10	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	11	257	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	12	257	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	13	256	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	14	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	15	255	1	0.96	0.96	0.08
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4	5	1725929730	L7, L25	011011001	497	256	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	498	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	499	255	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	500	258	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	501	255	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	502	255	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	503	255	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	504	257	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	505	256	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	506	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	507	257	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	508	255	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	509	256	1	0.96	0.96	0.08
4	5	1725929730	L7, L25	011011001	510	256	1	0.96	0.89	0.08
4	5	1725929730	L7, L25	011011001	511	255	1	0.96	0.96	0.08

Table 3.9: Results for LRC = L7, L25, RR = 1725929730 and $RC = 5$ for $n = 9$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
4	NA	NA	217	1	9	1	128,64,32,16,8,4, ...	0.96	511,-1,-1,-1, ...	0
4	5	1725929730	217	1	256	1	112,78,37,18,7,3, ...	0.96	511,-1,-65,-25, ...	0.08

Table 3.10: Comparison of an m-sequence With a 2D CA of size $n = 9$ Sequence Obtained for LRC = L7, L25

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
4	8	163	90, 150	100110001	1	253	0.76	0.51	0.12
4	5	1725929730	L7, L25	011011001	1	256	0.96	0.96	0.08

Table 3.11: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 9$

LRC	No.	RRs
L7, L25	25740	288419549, 288648925, 288665309, 288680669, 288681685, 288681689, 288679645, 288681565, 288681629, 288911069, 288927453, 288943773, 288941789, 288943829, 288943833
L28, L27	12870	554888942, 555118318, 555134702, 555149038, 555150062, 555150958, 555151022, 555151078, 555151082, 555380462, 555396846, 555412206, 555413102, 555413166, 555411182
L30, L11	12870	33619965, 33849341, 33865725, 33880061, 33881085, 33881981, 33882045, 33882101, 33882105, 34111485, 34127869, 34144249, 34142205, 34143229, 34144125
L30, L27	0	
L25, L14	38610	2359260, 2588636, 2605020, 2621276, 2619356, 2620380, 2621340, 2621396, 2621400, 2850780, 2883540, 2883544, 2867164, 2881500, 2882524
L25, L31	60056	303295980, 303525356, 303541740, 303556076, 303558116, 303558120, 303557996, 303557100, 303558060, 303787500, 303803884, 303818220, 303818220, 303820140, 303819244
L21, L27	102960	2228190, 2457566, 2473950, 2489310, 2490206, 2488286, 2490270, 2490326, 2490330, 2719710, 2736094, 2752470, 2752470, 2752474, 2751454

Table 3.12: Number Of RRs That Passed the First Stage of Filtering for the Respective LRCs For $n = 8$, $OC = 4$, $SV = 1$ and $RC = 5$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
4	5	36830670	L21, L27	00111111	1	130	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	2	130	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	3	128	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	4	126	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	5	128	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	6	127	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	7	126	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	8	130	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	9	129	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	10	127	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	11	128	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	12	129	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	13	128	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	14	128	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	15	128	1	0.95	0.85	0.11
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4	5	36830670	L21, L27	00111111	241	127	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	242	126	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	243	127	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	244	127	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	245	129	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	246	127	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	247	128	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	248	129	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	249	128	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	250	127	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	251	129	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	252	128	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	253	130	1	0.95	0.85	0.11
4	5	36830670	L21, L27	00111111	254	128	1	0.95	0.95	0.11
4	5	36830670	L21, L27	00111111	255	130	1	0.95	0.85	0.11

Table 3.13: Results for LRC = L21, L27, RR = 36830670 and $RC = 5$ for $n = 8$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
4	NA	NA	63	1	8	1	64,32,16,8,4,2, ...	0.95	255,-1,-1,-1, ...	0
4	5	36830670	63	1	130	1	64,32,18,4,8,0, ...	0.95	255,-1,-1,-1, ...	0.11

Table 3.14: Comparison of an m-sequence With a 2D CA of size $n = 8$ Sequence Obtained for LRC = L21, L27

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	4	225	90, 150	01011101	1	130	0.49	0.43	0.22
4	5	36830670	L21, L27	00111111	1	130	0.95	0.95	0.11

Table 3.15: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 8$

LRC	No.	RRs
L7, L25	51480	286387693, 286617069, 286647789, 286633453, 286649709, 286648813, 286649773, 286649829, 286649833, 286879213, 286895597, 286909933, 286911853, 286910957, 286911917
L28, L27	38610	50592989, 50822365, 50838749, 50853085, 50854109, 50855005, 50855069, 50855125, 50855129, 51084509, 51100893, 51116253, 51115229, 51117149, 51117213
L30, L11	12870	572718287, 572947663, 572964047, 572980303, 572980367, 572978383, 572980423, 572980427, 572979407, 573209807, 573226191, 573240527, 573241551, 573242447, 573242511
L30, L27	12870	805563855, 805793231, 805809615, 805825871, 805823951, 805824975, 805825935, 805825991, 805825995, 806055375, 806071759, 806086095, 806087119, 806088015, 806088079
L25, L14	12870	20053710, 20299470, 20283086, 20315726, 20315790, 20315846, 20315850, 20314830, 20313806, 20575950, 20561614, 20545230, 20577870, 20577934, 20577990
L25, L31	25740	555933422, 556162798, 556179182, 556193518, 556195438, 556194542, 556195502, 556195558, 556195562, 556424942, 556441326, 556456686, 556457646, 556457702, 556457706
L21, L27	37884	285470429, 285699805, 285716189, 285730525, 285731549, 285732445, 285732509, 285732565, 285732569, 285961949, 285978333, 285994709, 285994713, 285992669, 285993693

Table 3.16: Number of RRs That Passed the First Stage of Filtering for the Respective LRCs for $n = 7$, $OC = 4$, $SV = 1$ and $RC = 5$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
4	5	554884830	L7, L25	0110111	1	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	2	65	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	3	62	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	4	65	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	5	63	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	6	64	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	7	65	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	8	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	9	63	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	10	64	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	11	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	12	65	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	13	62	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	14	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	15	63	1	0.93	0.79	0.12
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4	5	554884830	L7, L25	0110111	113	64	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	114	63	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	115	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	116	65	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	117	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	118	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	119	62	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	120	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	121	64	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	122	64	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	123	66	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	124	64	1	0.93	0.79	0.12
4	5	554884830	L7, L25	0110111	125	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	126	64	1	0.93	0.93	0.12
4	5	554884830	L7, L25	0110111	127	64	1	0.93	0.79	0.12

Table 3.17: Results for LRC = L7, L25, RR = 554884830 and $RC = 5$ for $n = 7$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
4	NA	NA	55	1	7	1	32,16,8,4,2,1...	0.93	127,-1,-1,-1, ...	0
4	5	554884830	55	1	64	1	32,16,8,4,2,1 ...	0.93	127,-1,-1,-1, ...	0.11

Table 3.18: Comparison of an m-sequence With a 2D CA of size $n = 7$ Sequence Obtained for LRC = L7, L25

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	6	18	90, 150	0101011	1	64	0.93	0.66	0.29
4	5	554884830	L7, L25	0110111	1	64	0.93	0.93	0.11

Table 3.19: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 7$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
4	5	319880399	L30, L11	010101	0	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	1	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	2	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	3	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	4	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	5	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	6	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	7	32	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	8	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	9	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	10	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	11	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	12	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	13	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	14	33	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	15	33	1	0.9	0.9	0.17
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
4	5	319880399	L30, L11	010101	49	31	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	50	31	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	51	31	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	52	31	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	53	31	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	54	31	1	0.9	0.9	0.17
4	5	319880399	L30, L11	010101	55	31	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	56	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	57	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	58	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	59	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	60	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	61	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	62	30	1	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	63	30	1	0.9	0.7	0.17

Table 3.20: Results for LRC = L30, L11, RR = 319880399 and $RC = 5$ for $n = 6$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
4	NA	NA	21	1	6	1	16,8,4,2,1,1 ...	0.9	63,-1,-1,-1, ...	0.02
4	5	319880399	21	1	32	1	16,8,4,2,1,1 ...	0.9	63,-1,-1,-1, ...	0.17

Table 3.21: Comparison of an m-sequence With a 2D CA of size $n = 6$ Sequence Obtained for LRC = L30, L11

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	2	86	90, 150	101110	1	32	0.9	0.7	0.17
4	5	319880399	L30, L11	010101	1	32	0.9	0.9	0.17

Table 3.22: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 6$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
4	5	285339375	L25, L14	10000	0	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	1	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	2	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	3	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	4	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	5	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	6	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	7	15	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	8	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	9	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	10	15	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	11	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	12	0	-31	0	0	1
4	5	285339375	L25, L14	10000	13	15	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	14	17	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	15	15	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	16	17	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	17	15	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	18	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	19	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	20	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	21	17	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	22	17	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	23	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	24	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	25	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	26	16	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	27	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	28	15	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	29	16	1	0.86	0.59	0.23
4	5	285339375	L25, L14	10000	30	15	1	0.86	0.85	0.23
4	5	285339375	L25, L14	10000	31	17	1	0.86	0.59	0.23

Table 3.23: Results for LRC = L25, L14, RR = 285339375 and $RC = 5$ for $n = 5$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
4	NA	NA	16	1	5	1	8,4,2,1,1, ...	0.85	31,-1,-1,-1, ...	0.03
4	5	285339375	16	1	16	1	10,4,1,0,2, ...	0.59	31,-1,-1,-7, ...	0.23

Table 3.24: Comparison of an m-sequence With a 2D CA of size $n = 5$ Sequence Obtained for LRC = L25, L14

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	4	107	90, 150	00111	1	16	0.79	0.59	0.29
4	5	285339375	L25, L14	10000	1	16	0.86	0.59	0.23

Table 3.25: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 5$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
5	6	2312541294	L28, L27	1111101101	1	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	2	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	3	511	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	4	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	5	512	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	6	513	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	7	509	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	8	511	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	9	512	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	10	512	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	11	511	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	12	509	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	13	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	14	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	15	512	1	0.98	0.93	0.08
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
5	6	2312541294	L28, L27	1111101101	1009	511	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	1010	511	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	1011	511	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1012	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1013	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1014	511	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1015	512	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	1016	511	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1017	515	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	1018	512	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	1019	510	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1020	512	1	0.98	0.93	0.08
5	6	2312541294	L28, L27	1111101101	1021	511	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1022	512	1	0.98	0.98	0.08
5	6	2312541294	L28, L27	1111101101	1023	513	1	0.98	0.93	0.08

Table 3.26: Results for LRC = L28, L27, RR = 2312541294 and RC = 6 for $n = 10$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
5	NA	NA	1005	1	10	1	256,128,64,32,16, ...	0.98	1023,-1,-1,-1, ...	0
5	6	2312541294	1005	1	512	1	256,128,64,31,19, ...	0.98	1023,-1,-1,-1, ...	0.08

Table 3.27: Comparison of an m-sequence With a 2D CA of size $n = 10$ Sequence Obtained for LRC = L28, L27

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	4	154	90, 150	1111110000	1	513	0.33	0.53	0.10
5	6	2312541294	L28, L27	1111101101	1	512	0.98	0.98	0.08

Table 3.28: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 10$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
5	6	509237910	L28, L27	11111010111	1	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	3	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	4	1022	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	5	1023	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	6	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	7	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	8	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	9	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	10	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	11	1023	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	12	1022	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	13	1023	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	14	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	15	1025	1	0.98	0.95	0.06
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
5	6	509237910	L28, L27	11111010111	2033	1023	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2034	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2035	1023	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2036	1025	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2037	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2038	1019	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2039	1023	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2040	1026	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2041	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2042	1025	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2043	1023	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2044	1024	1	0.98	0.98	0.06
5	6	509237910	L28, L27	11111010111	2045	1024	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2046	1025	1	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	2047	1023	1	0.98	0.98	0.06

Table 3.29: Results for LRC = L28, L27, $RR = 509237910$ and $RC = 6$ for $n = 11$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
5	NA	NA	2007	1	11	1	512,256,128,64,32, ...	0.98	2047,-1,-1,-1, ...	0
5	6	509237910	2007	1	1024	1	512,256,108,86,36, ...	0.98	2047,-1,-1,-1, ...	0.06

Table 3.30: Comparison of an m-sequence With a 2D CA of size $n = 11$ Sequence Obtained for LRC = L28, L27

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	10	86	90, 150	01011000010	1	1024	0.98	0.95	0.06
5	6	509237910	L28, L27	11111010111	1	1024	0.98	0.98	0.06

Table 3.31: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 11$

OC	RC	RR	LRC	LR	SV	LC	B	P_B	P_R	MSR
5	6	2809934922	L28, L27	111111110011	1	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	2	2047	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	3	2047	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4	2049	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	5	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	6	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	7	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	8	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	9	2049	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	10	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	11	2047	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	12	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	13	2046	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	14	2047	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	15	2048	1	0.99	0.96	0.05
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
5	6	2809934922	L28, L27	111111110011	4081	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4082	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4083	2052	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4084	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4085	2046	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4086	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4087	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4088	2053	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4089	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4090	2045	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4091	2048	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4092	2046	1	0.99	0.99	0.05
5	6	2809934922	L28, L27	111111110011	4093	2043	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4094	2048	1	0.99	0.96	0.05
5	6	2809934922	L28, L27	111111110011	4095	2048	1	0.99	0.99	0.05

Table 3.32: Results for LRC = L28, L27, RR = 2809934922 and RC = 6 for $n = 12$

OC	RC	RR	LR	SV	LC	B	R	P_R	AC	MSR
5	NA	NA	4083	1	12	1	1024,512,256,128,64, ...	0.99	4095,-1,-1,-1, ...	0
5	6	2809934922	4083	1	2048	1	1024,512,252,144,49, ...	0.99	4095,-1,-1,-1, ...	0.05

Table 3.33: Comparison of an m-sequence With a 2D CA of size $n = 12$ Sequence Obtained for LRC = L28, L27

OC	RC	RR	LRC	LR	SV	LC	P_B	P_R	MSR
2	3	99	90, 150	001001111010	1	2049	0.98	0.92	0.23
5	6	2809934922	L28, L27	111111110011	1	2048	0.99	0.99	0.05

Table 3.34: Comparison of a Filtered 1D CA Sequence With a Filtered 2D CA Sequence for $n = 12$

n	Iterations	Time (h)
5	4207562513	5880
6	3005401795	8700
7	4207562513	20160
8	4207562513	38640
9	4207562513	77280

Table 3.35: Execution Times for $n = 5$, 6, 7, 8 and 9

n	Time (ms)
5	5.03
6	10.42
7	17.24
8	33.06
9	66.12

Table 3.36: Execution Time of One Iteration for $n = 5$, 6, 7, 8 and 9

Chapter 4

Conclusion

The first objective of this thesis was to determine if two-dimensional cellular automata (2D CA) can be used to generate maximum length sequences (m-sequences). The linear rules (L0 to L31) were defined for 2D CAs and they were considered for m-sequence generation. The subset of linear rules for which the next state of the cell is based on the current states of at least 3 neighbors was selected. These rules were classified into six classes (A to F) based on the rules that were rotations of each other. An evaluation system was designed to check all possible combinations of these linear rules (LR) for m-sequence generation. Two unique linear rules were used in each LR and the parameter linear rule combination (LRC) was used indicate these rules in the CA. Many different combinations of linear rules generated m-sequences for 2D CAs of sizes $n = 5$ to 9. It was observed that the linear rules from seven unique class combinations (CCs) generated m-sequences and an LRC was selected from each as a representative of that CC. The criteria for the selection of CC representatives (LRC) was the number of appearances of the respective LRC in the results obtained for 2D CAs of sizes $n = 5$ to 9. The seven selected LRCs were then used to generate m-sequences for 2D CAs of sizes $n = 10$ to 16 to ensure that they can generate m-sequences for 2D CAs of size $n > 9$. The results obtained showed that all seven CC representatives generated m-sequences for 2D CAs of sizes $n = 11$, 12, 14, 15 and 16. For $n = 10$, two CC representatives did not generate m-sequences and for $n = 13$, one CC representative did not generate m-sequences.

The second objective of this thesis was to use 2D CAs to generate pseudorandom sequences with high linear complexity and good randomness. The same evaluation system was used to generate sequences for 2D CAs of sizes $n = 5$ to 14. For $n = 5$ to

9, sequences were generated using all seven CC representatives after a single cell replacement with all balanced non-linear rules (RR) in the range 0 to 4294967295. For $n = 10$, 11 and 12, the sequences were generated using only one CC representative (LRC = L28, L27) after a single cell replacement with all balanced even non-linear rules. The results were first examined for initial state $SV = 1$. Two stage filtering was implemented to filter sequences generated by these CAs considering the linear complexity (LC), complementary error functions for balance and run [15] (P_B and P_R) and maximum sidelobe ratio (MSR) for the autocorrelation. The calculations of P_B and P_R were adopted from [15]. MSR is the ratio of the largest sidelobe of the autocorrelation to the mainlobe. The first stage involved filtering sequences that had linear complexity $LC \geq 2^n/2$, $P_B \geq 0.9$, $P_R \geq 0.9$ and $MSR < 0.2$. Using the RRs that generated the sequences which passed the first stage of filtering, the sequences for all SV values were generated. The second stage filtered the sequences which maintained $LC = 2^{n-1} \pm 10\%$ for all 2^n SVs and had $P_B \geq 0.5$, $P_R \geq 0.5$ and $MSR < 0.2$. The results obtained after the second stage of filtering showed that for 2D CAs of size $n = 7$ to 12, many different even RRs can be combined with linear rules based on m-sequences to generate sequences that satisfy all the filtering criteria. For $n = 6$, only odd RRs generated sequences that passed both stages of filtering. For $n = 5$, none of the sequences passed the filtering criteria.

The best 2D CA sequences obtained for $n = 5$ to 12 were compared with m-sequences and the 1D CA sequences filtered in [5] for the respective 1D CA sizes. The comparison with m-sequences showed that the 2D CA sequences had much higher linear complexity ($2^n/2$ versus n) and the same values for balance and P_R. The 2D CA sequences had good autocorrelation but not as good as the m-sequences. The MSR value decreased with increasing n and for 2D CAs of size $n = 12$, the MSR value was 0.05 for the sequence generated by $RR = 2809934922$ (for all non-zero SVs). The comparison with 1D CA sequences showed that both had similar LC ($2^{n-1} \pm 10\%$) but the 2D CA sequences had better randomness properties. The values of P_B and P_R were significantly higher for the 2D CA sequences and the MSR was lower. In conclusion, 2D CAs can be used to generate m-sequences and pseudorandom sequences with high linear complexity and better randomness than sequences generated using 1D CAs. It is conjectured that if the Moore neighbourhood is used, the increased interaction between cells may not improve the performance so the sequences obtained may not be as good as the sequences obtained using the von Neuman neighbourhood.

4.1 Future Work

In this thesis, a 2D CA evaluation system was developed to generate psuedorandom sequences using the von Neumann neighborhood. The Moore nighborhood can be considered in future to generate these sequences. With the Moore neighborhood, the number of rules will increase to 2^{512} and there will be 2^9 linear rules since the neighborhood size is 9. The sequences generated can also be tested for other properties of randomness such as closure, recurrence, window and shift [4][5]. With sufficient computing resources, multiple linear rule replacements with non-linear rules can also be considered.

Bibliography

[1] A.J. Menezes *et al.*, Handbook of Applied Cryptography, CRC Press, pp. 39-40, Boca Raton, FL, 2001.

[2] T.E. Tkacik, "A Hardware Random Number Generator," *International Workshop on Cryptographic Hardware and Embedded Systems*, LNCS, vol. 2523, pp. 450-453. Springer, Berlin, 2002.

[3] M.G. Kendall and B.B. Smith, "Randomness and Random Sampling Numbers," *Journal of the Royal Statistical Society*, vol. 101, no. 1, pp. 147-160, 1938.

[4] A. Mitra, "On the Properties of Pseudo Noise Sequences with a Simple Proposal of Randomness Test," *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 2, no. 9, pp. 1997-2002, 2008.

[5] S. Acharya, "Cellular Automata Pseudorandom Sequence Generation," M.A.Sc. Thesis, University of Victoria, Victoria, BC, Canada, 2017.

[6] S. Mishra, R.R. Tripathi and D.K. Tripathi, "Implementation of Configurable Linear Feedback Shift Register in VHDL," *International Conference on Emerging Trends in Electrical Electronics and Sustainable Energy Systems*, pp. 342-346, 2016.

[7] R.E. Ziemer and R.L. Peterson, Digital Communications and Spread Spectrum Systems, Macmillan, pp. 385-386, New York, NY, 1985.

[8] S. Wolfram, Cellular Automata and Complexity: Collected Papers, Westview Press, Boulder, CO, 1st Edition, 1994.

[9] S. Wolfram, A New Kind of Science, Wolfram Media, Champaign, IL, 2002.

[10] S. Wolfram, "Random Sequence Generation by Cellular Automata," *Advances in Applied Mathematics*, vol. 7, no. 2, pp. 123-169, 1986.

[11] K. Cattell and J.C. Muzio, "Synthesis of One Dimensional Linear Hybrid Cellular Automata," *IEEE Transactions on Computer Aided Design*, vol. 15, no. 3, pp. 325-335, 1996.

[12] N.H. Packard and S. Wolfram, "Two-dimensional Cellular Automata," *Journal of Statistical Physics*, vol. 38, no. 5-6, pp. 901-946, 1985.

[13] R. Scurr, "Sequences and Cellular Automata," ENEL 427 Final Report, University of Canterbury, Christchurch, New Zealand, 1998.

[14] E. Casey, "Berlekamp-Massey Algorithm," REU Summer Report, University of Minnesota, Minneapolis, MN, 2000.

[15] A. Rukhin *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," rev. 1a, cert. by National Institute of Standards and Technology (NIST) and U.S. Department of Commerce, 2010.