Hip to Be (Latin) Square: Maximal Period Sequences from Orthogonal CA

Luca Mariot

L.Mariot@tudelft.nl

CANDAR 2021 – November 26, 2021
One-dimensional **Cellular Automaton** (CA): a discrete parallel computation model composed of a finite array of \( n \) cells

Example: \( n = 8, \, d = 3, \, f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+2} \) (rule 90)

![Cellular Automaton](image)

No Boundary CA – NBCA

Truth table – Rule 90

Each cell updates its state \( s \in \{0, 1\} \) by applying a local rule \( f : \{0, 1\}^d \rightarrow \{0, 1\} \) to itself and the \( d - 1 \) cells on its right
CA-based Crypto History: Wolfram’s PRNG

- CA-based Pseudorandom Generator (PRG) [W86]: central cell of rule 30 CA used as a stream cipher keystream

This CA-based PRNG was later shown to be vulnerable [MS91]

- More recent works [LM13, FIMY14, LM4] tried to fix it using larger rules with better crypto properties
Bipermutive CA: local rule $f$ defined as

$$f(x_1, \cdots, x_d) = x_1 \oplus \varphi(x_2, \cdots, x_{d-1}) \oplus x_d$$

Example: CA $F : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^2$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)

Encoding: $00 \mapsto 1, 10 \mapsto 2, 01 \mapsto 3, 11 \mapsto 4$

(a) Rule 150 on 4 bits

(b) Latin square $L_{150}$

Orthogonal Cellular Automata (OCA): pair of bipermutive CA generating two orthogonal Latin squares
**OCA by Linear CA**

- **Bipermutive Linear rule:** \( f(x) = x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{d-1} x_{d-1} \oplus x_d \)
- **Polynomial rule:** \( P_f(X) = 1 + a_2 X + \cdots + a_{d-1} X^{d-2} + X^{d-1} \)

**Theorem ([MGFL20])**

*Two linear bipermutive CA \( F, G \) are OCA if and only if their associated polynomials \( P_f(X), P_g(X) \) are relatively prime.*

| Rule | Associated Polynomial |
|------|-----------------------|
| 150  | \( P_{150}(X) = 1 + X + X^2 \) |
| 90   | \( P_{90}(X) = 1 + X^2 \) (coprime) |

**Figure:**

- (a) Rule 150
- (b) Rule 90
- (c) Superposition

Luca Mariot  
*Hip to Be (Latin) Square: Maximal Period Sequences from Orthogonal CA*
Pseudorandom Generator based on OCA

Basic Idea:

▶ Start from random \((x(0), y(0))\) and evaluate two OCA \(F, G\) over it
▶ Use the outputs \(F(x(0), y(0))\) and \(G(x(0), y(0))\) as new OCA inputs
▶ Continue to iterate the system

Motivation:

▶ The system is always reversible (because of orthogonality)
▶ Orthogonality ensure a minimum degree of diffusion
Research Question: How do we choose $F$ and $G$ to get a maximum period length of $2^{2(d-1)}$?

Example: $d = 3$, rules 90 and 150
Distribution of Maximum Periods for $d = 4, 5$

Main Remark: Best upper bound reached is $2^{2(d-1)} - 1$
The Case of Linear OCA

For linear OCA $F, G$, finding an upper bound boils down to determine the order of the Sylvester Matrix:

$$M_{F,G} = \begin{pmatrix} a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & 0 \\
0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_d \\
b_1 & \cdots & b_d & 0 & \cdots & \cdots & \cdots & 0 \\
0 & b_1 & \cdots & b_d & 0 & \cdots & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & \cdots & \cdots & \cdots & 0 & b_1 & \cdots & b_d \end{pmatrix}.$$  

We devised a combinatorial algorithm to efficiently enumerate all such matrices of maximum order.
Table: Number of maximal period linear OCA pairs of diameter $d \leq 11$.

| $d$ | $n$ | $2^{2n} - 1$ | $\#LOCA_d$ | $\#mLOCA_d$ | Time     |
|-----|-----|--------------|-------------|-------------|----------|
| 2   | 1   | 3            | 0           | –           | –        |
| 3   | 2   | 15           | 1           | 1           | < 1s     |
| 4   | 3   | 63           | 5           | 1           | < 1s     |
| 5   | 4   | 255          | 21          | 3           | < 1s     |
| 6   | 5   | 1023         | 85          | 15          | < 1s     |
| 7   | 6   | 4095         | 341         | 42          | 3.967s   |
| 8   | 7   | 16383        | 1365        | 181         | 59.162s  |
| 9   | 8   | 65535        | 5461        | 572         | 18m59.302s |
| 10  | 9   | 262143       | 21845       | 1872        | 5h56m10.208s |
| 11  | 10  | 1048575      | 87381       | 5899        | 4d16h27m22.126s |
Conclusions

Recap of main findings:

- Orthogonal CA seems to represent an interesting way to generate pseudorandom sequences with long periods
- The longest periods seem to occur in the case of linear OCA
- Upper bounding the periods of linear OCA is equivalent to finding the order of a Sylvester matrix

Open problems:

- Study the number of maximum order Sylvester matrices (new sequence added in the OEIS [O21])
- Characterize which pairs of polynomials induce maximum order Sylvester matrices
- Study the periods of nonlinear OCA, possibly using an evolutionary approach [MPJL17, MPJL18]
- Generalize to CA-based Latin hypercubes [GM20]
References

[O21] OEIS Sequence A346142. URL: https://oeis.org/A346142

[E93] Eloranta, K.: Partially Permutive Cellular Automata. Nonlinearity 6(6), 1009–1023 (1993)

[FIMY14] Formenti, E., Imai, K., Martin, B., Yunès, J.-B.: Advances on Random Sequence Generation by Uniform Cellular Automata. In: Computing with New Resources 2014: 56-70 (2014)

[GM20] Gadouleau, M., Mariot, L.: Latin Hypercubes and Cellular Automata. In: Proceedings of AUTOMATA 2020: 139-151 (2020)

[LM14] Leporati, A., Mariot, L.: Cryptographic properties of bipermutive cellular automata rules. J. Cell. Autom. 9(5-6):437–475 (2014)

[LM13] Leporati, A., Mariot, L.: 1-Resiliency of Bipermutive Cellular Automata Rules. In: Proceedings of AUTOMATA 2013: 110-123 (2013)

[MGFL20] Mariot, L., Gadouleau, M., Formenti, E., Leporati A.: Mutually orthogonal latin squares based on cellular automata. Des. Codes Cryptogr. 88(2):391–411 (2020)

[MPJL18] Mariot, L., Picek, S., Jakobovic, D., Leporati, A.: Evolutionary Search of Binary Orthogonal Arrays. In: Proceedings of PPSN 2018 (I): 121-133 (2018)

[MPJL17] Mariot, L., Picek, S., Jakobovic, D., Leporati, A.: Evolutionary Algorithms for the Design of Orthogonal Latin Squares based on Cellular Automata. In: Proceedings of GECCO’17 (2017)

[MFL16] Mariot, L., Formenti, E., Leporati, A.: Constructing Orthogonal Latin Squares from Linear Cellular Automata. In: Exploratory papers of AUTOMATA 2016 (2016)

[MS91] Meier, W., Staffelbach, O.: Analysis of Pseudo Random Sequence Generated by Cellular Automata. In EUROCRYPT, Vol. 91, pp. 186-200 (1991)

[W86] Wolfram, S.: Random Sequence Generation by Cellular Automata. Adv. Appl. Math. 7(2), 123–169 (1986)