UNIVERSITY OF TWENTE.

Self-Orthogonal CA

Luca Mariot, Federico Mazzone

l.mariot@utwente.nl

Automata 2025 – Lille, 1 July 2025

Latin Squares

Definition

A *Latin square* of order N is a $N \times N$ matrix L such that every row and every column are permutations of $[N] = \{1, \cdots, N\}$

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

Mutually Orthogonal Latin Squares (MOLS)

Definition

Two Latin squares L_1 and L_2 of order N are *orthogonal* if their superposition yields all the pairs $(x, y) \in [N] \times [N]$.

1	3	4	2
4	2	1	3
2	4	3	1
3	1	2	4

(a) L_1

1	4	2	3
3	2	4	1
4	1	3	2
2	3	4	1

(b) L_2

1 1	3 4	4 2	2 3
4 3	2 2	1 4	3 1
2 4	4 1	3 3	1 2
3 2	1 3	2 1	4 4

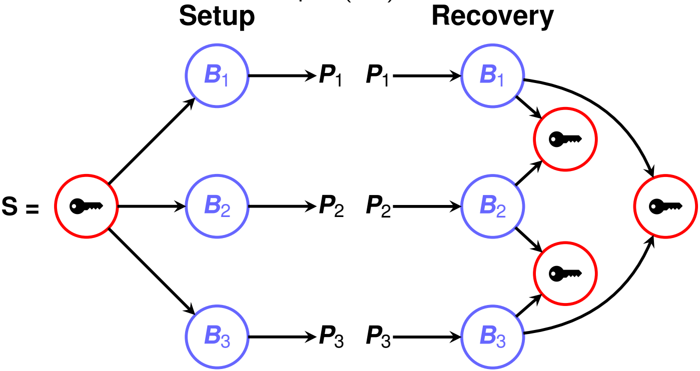
(c) (L_1, L_2)

n pairwise orthogonal Latin squares are denoted as *n*-MOLS
(**Mutually Orthogonal Latin Squares**)

Applications of n-MOLS to Secret Sharing

(k, n) **Threshold Secret Sharing Scheme**: a **dealer** shares a **secret** S among n **players** so that at least k players out of n are required to recover S [S79]

Example: (2,3)–scheme

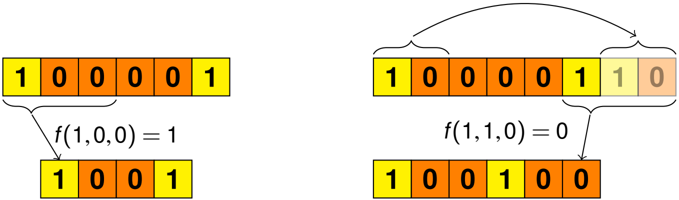


Remark: $(2, n)$–scheme $\Leftrightarrow$ set of n-MOLS [S04]

Cellular Automata

- Vectorial functions $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with *uniform* (shift-invariant) coordinates [MPLJ19]

Example: $q = 2$, $n = 6$, $d = 3$, $f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2}$



No Boundary CA – NBCA

Periodic Boundary CA – PBCA

- Each cell updates its state $s \in \{0,1\}$ by evaluating a local rule $f : \{0,1\}^d \to \{0,1\}$ on itself and the $d-1$ cells on its right

Latin Squares through Bipermutive CA (1/2)

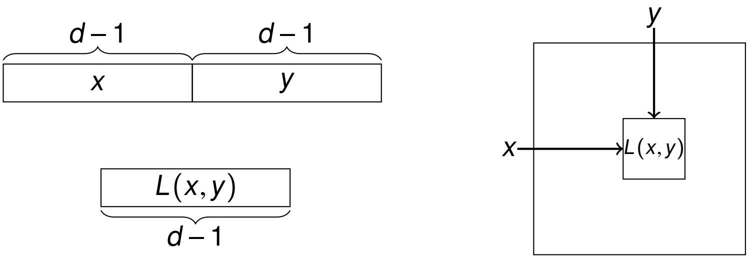
- Bipermutive CA: local rule f is defined as

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

- $\varphi : \mathbb{F}_q^{d-2} \to \mathbb{F}_q$: generating function of f [LM13]

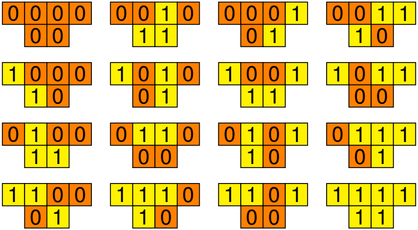
Lemma ([MFL16])

A (no-boundary) CA $F : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^d$ with bipermutive rule $f : \mathbb{F}_q^d \to \mathbb{F}_q$ generates a Latin square of order $N = q^{d-1}$



Latin Squares through Bipermutive CA (2/2)

- 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

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(b) Latin square L_{150}

Linear CA

- Local rule: *linear combination* of the neighborhood cells

$$f(x_1, \cdots, x_d) = a_1 x_1 + \cdots + a_d x_d \ , \ a_i \in \mathbb{F}_q$$

- Associated polynomial:

$$f \mapsto p_f(X) = a_1 + a_2 X + \cdots + a_d X^{d-1}$$

- $(n-d+1) \times n$ transition matrix [ML18]:

$$M_F = \begin{pmatrix} a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_d \end{pmatrix}, \quad x \mapsto M_F x^\top$$

- **Remark:** a linear rule is bipermutive iff $a_1, a_d \neq 0$

Sylvester Matrices

- Two linear bipermutive CA with rules $f, g : \mathbb{F}_q^d \to \mathbb{F}_q$ generate orthogonal Latin squares iff the following matrix is invertible:

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

- ... but this is the **Sylvester matrix** of the two polynomials p_f, p_g, and $det(M_{F,G} \neq 0 \Leftrightarrow \gcd(p_f, p_g) = 1$ [GKZ08]

MOLS from Linear Bipermutive CA (LBCA)

Theorem ([MGLF20])

A set of t linear bipermutive CA $F_1, \ldots F_t : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ generates a family of t-MOLS of order $N = q^{d-1}$ if and only if their associated polynomials are pairwise coprime

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

(a) Rule 150

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

(b) Rule 90

1 1	4 2	3 3	2 4
2 2	3 1	4 4	1 3
4 3	1 4	2 1	3 2
3 4	2 3	1 2	4 1

(c) Superposition

Figure: $P_{150}(X) = 1 + X + X^2$, $P_{90}(X) = 1 + X^2$ (coprime)

$(2,n)$-Secret Sharing from CA MOLS

L_{90} $(1+X^2)$

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

L_{150} $(1+X+X^2)$

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

$\Rightarrow$

x	y	L_{90}	L_{150}
1	1	1	1
1	2	2	4
1	3	3	3
1	4	4	2
2	1	2	2
2	2	1	3
2	3	4	4
2	4	3	1
3	1	3	4
3	2	4	1
3	3	1	2
3	4	2	3
4	1	4	3
4	2	3	2
4	3	2	1
4	4	1	4

Construction:

1. First two columns: all pairs (x,y) in lexicographic order
2. List the i-th Latin square in the $(i+2)$-th column

Dealing phase:

1. Use column 1 for the secret S and randomly sample a row R where $A(R,1)=S$
2. The share for P_i is $A(R,i+1)$ for $i \in [n]$

Recovery phase:

- Any subset of two players can uniquely identify the row

Self-Orthogonal CA

Definition

A bipermutive CA $F : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ is *self-orthogonal* if its Latin square L_F is orthogonal to its transpose $L_F^\top$.

1,1	2,2	3,3	4,4
2,2	1,1	4,4	3,3
3,3	4,4	1,1	2,2
4,4	3,3	2,2	1,1

(a) L_{90}

1,1	4,3	2,4	3,2
3,4	2,2	4,1	1,3
4,2	1,4	3,3	2,1
2,3	3,1	1,2	4,4

(b) L_{150}

- **Applications:** *anonymous* secret sharing, quantum error correcting codes [BS98, KM22]
- **Question:** give a characterization of self-orthogonal CA

Computer Search

- Performed exhaustive search up to $d = 6$

d	#BCA	#SOCA	#LIN/AFF	Polynomials
3	4	2	2	$1+X+X^2$
4	16	4	4	$1+X+X^3$, $1+X^2+X^3$
5	256	8	8	$1+X+X^4$, $1+X^2+X^4$ $1+X^3+X^4$, $1+X+X^2+X^3+X^4$
6	65 336	16	16	$1+X+X^5$, $1+X^2+X^5$ $1+X^3+X^5$, $1+X^4+X^5$ $1+X+X^2+X^3+X^5$ $1+X+X^2+X^4+X^5$ $1+X+X^3+X^4+X^5$ $1+X^2+X^3+X^4+X^5$

Empirical Findings:

- Only some *linear* BCA are SO
- All linear BCA described by irreducible polynomials are SO

Characterization of the Linear Case

- The transpose CA $F^\top : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ is defined as:

$$F^\top(x||y) = F(y||x)$$

- **Idea:** compose the matrix M_F with the *permutation matrix*

$$M_s = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 & 0 \end{pmatrix} .$$

Transition Matrix of Transpose CA

- the transition matrix for $F^\top$ is thus:

$$M_{F^\top} = M_F \cdot M_s = \begin{pmatrix} a_d & 0 & \dots & \dots & 0 & a_1 & \dots & \dots & a_{d-1} \\ a_{d-1} & a_d & \dots & \dots & 0 & 0 & a_1 & \dots & a_{d-2} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \dots & \dots & a_d & 0 & 0 & \dots & a_1 \end{pmatrix} .$$

- **Next step:** check the *superposed matrix* $M_{F,F^\top} = \begin{pmatrix} M_F \\ M_{F^\top} \end{pmatrix}$
- We are interested in understanding when $M_{F,F^\top}$ is invertible

Superposed matrix

- Form of $M_{F,F^\top}$:

$$M_{F,F^\top} = \begin{pmatrix} M_F \\ M_{F^\top} \end{pmatrix} = \begin{pmatrix} a_1 & \dots & \dots & a_d & 0 & 0 & \dots & \dots & 0 \\ 0 & a_1 & \dots & \dots & a_d & 0 & \dots & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \dots & a_1 & \dots & \dots & \dots & a_d \\ a_d & 0 & \dots & \dots & 0 & a_1 & \dots & \dots & a_{d-1} \\ a_{d-1} & a_d & \dots & \dots & 0 & 0 & a_1 & \dots & a_{d-2} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & a_3 & \dots & \dots & a_d & 0 & 0 & \dots & a_1 \end{pmatrix}$$

- Necessary and sufficient condition:

Lemma

The LBCA $F : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ is self-orthogonal if and only if the matrix $M_{F,F^\top}$ is invertible.

Characterization with polynomials

- $M_{F,F^\top}$ is no longer a Sylvester matrix, but a **circulant** matrix

Theorem ([LN94])

The map $\Phi : (c_1, \ldots, c_n) \mapsto c(X) = c_1 + \ldots + c_n X^{n-1} \mod X^n - 1$ *is an isomorphism between the ring of* $n \times n$ *circulant matrices on* $\mathbb{F}_q$ *and the quotient polynomial ring* $R_P = \mathbb{F}_q[X]/(X^n - 1)$.

- So, we can check self-orthogonality by checking that $p_f(X)$ is a *unit* of the quotient ring R_P:

Theorem

The LBCA $F : \mathbb{F}_q^{2(d-1)} \to \mathbb{F}_q^{d-1}$ *with rule* $f : \mathbb{F}_q^d \to \mathbb{F}_q$ *and associated polynomial* $p_f(X) \in \mathbb{F}_q[X]$ *is self-orthogonal if and only if* $\gcd(p_f(X), X^n - 1) = 1$, *where* $n = 2(d-1)$.

More results in the case $q = 2$

- Irreducibility is indeed a sufficient condition:

Lemma

A binary LBCA $F : \mathbb{F}_2^{2(d-1)} \to \mathbb{F}_2^{d-1}$ defined by $f : \mathbb{F}_2^d \to \mathbb{F}_2$ such that $p_f(X)$ is irreducible is self-orthogonal.

- Further, for some diameters d there is a simpler condition:

Lemma

Let $d = 2^t + 1$ for $t \in \mathbb{N}$. Then, a LBCA $F : \mathbb{F}_2^{2(d-1)} \to \mathbb{F}_2^{d-1}$ defined by $f : \mathbb{F}_2^d \to \mathbb{F}_2$ is self-orthogonal if and only if $p_f(1) \neq 0$.

- **In practice:** if $d = 2^t + 1$, just check the *parity* of the coefficients $c_1, \cdots c_d$ of the polynomial

Conclusions and Future Works

Upon a closer look:

- Circulant matrices are actually periodic linear CA! [BCMM98, ION83]
- **Thus:** checking self-orthogonality of a linear NBCA is equivalent to checking *invertibility* of the corresponding PBCA

Future directions:

- Do there exist *nonlinear* self-orthogonal CA?
- Investigate applications to anonymous secret sharing and quantum ECC [BS98, KM22]
- Study the dynamics of iterated self-orthogonal maps and the construction of bent functions [M23, GMP23]

References

- [BCMM98] D. Bini, G.M.D. Corso, G. Manzini, L. Margara: Inversion of Circulant Matrices over Zm. In: Proceedings of ICALP'98, pp. 719-730. Springer (1998)
- [BCMM98] C. Blundo, D.R. Stinson: Anonymous secret sharing schemes. Discret. Appl. Math. 77(1):13-28 (1997)
- [GMP23] M. Gadouleau, L. Mariot, S. Picek. Bent functions in the partial spread class generated by linear recurring sequences. Des. Codes Cryptogr. 91(1):63–82 (2023)
- [GKZ08] I.M. Gelfand, M. Kapranov, A. Zelevinsky: Discriminants, resultants, and multidimensional determinants. Springer Science & Business Media (2008)
- [KM22] A. Kumar, S. Maitra: Resolvable block designs in construction of approximate real MUBs that are sparse. Cryptogr. Commun. 14(3):527–549 (2022)
- [ION83] M. Ito, N. Osato, M. Nasu: Linear cellular automata over Zm. J. Comput. Syst. Sci. 27(1):125–140 (1983)
- [LM13] A. Leporati, L. Mariot: 1-Resiliency of Bipermutive Cellular Automata Rules. In: Proceedings of AUTOMATA 2013: 110-123 (2013)
- [LN94] R. Lidl, H. Niederreiter: Introduction to finite fields and their applications. Cambridge University Press (1994)
- [M23] L. Mariot: Enumeration of maximal cycles generated by orthogonal cellular automata. Nat. Comput. 22(3):477-491 (2023)
- [MGLF20] L. Mariot, M. Gadouleau, E. Formenti, and A. Leporati. Mutually orthogonal latin squares based on cellular automata. Des. Codes Cryptogr. 88(2):391–411 (2020)
- [MPLJ9] L. Mariot, S. Picek, A. Leporati, and D. Jakobovic. Cellular automata based S-boxes. Cryptography and Communications 11(1): 41-62 (2019)
- [ML18] L. Mariot, A. Leporati: A cryptographic and coding-theoretic perspective on the global rules of cellular automata. Nat. Comput. 17(3):487-498 (2018)
- [MFL16] L. Mariot, E. Formenti, A. Leporati: Constructing Orthogonal Latin Squares from Linear Cellular Automata. In: Exploratory papers of AUTOMATA 2016 (2016)
- [S79] A. Shamir: How to share a secret. Commun. ACM 22(11):612–613 (1979)
- [S04] D.R. Stinson: Combinatorial designs. Springer (2004)