Constructing Orthogonal Latin Squares from Linear Cellular Automata

Luca Mariot[1,2], Enrico Formenti[2], Alberto Leporati[1]

[1] Dipartimento di Informatica, Sistemistica e Comunicazione (DISCo)
Università degli Studi Milano - Bicocca

[2] Laboratoire d'Informatique, Signaux et Systèmes de Sophia Antipolis (I3S)
Université Nice Sophia Antipolis

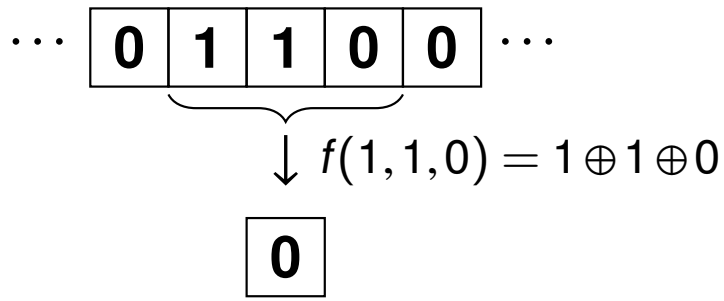
AUTOMATA 2016 – Zurich, June 15–17, 2016

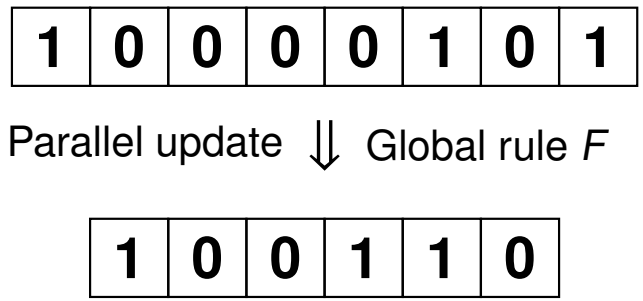
One-Dimensional Cellular Automata (CA)

Definition

One-dimensional CA: quadruple $\langle A, n, r, f \rangle$ where A is the finite set of states, $n \in \mathbb{N}$ is the number of cells on a one-dimensional array, $r \in \mathbb{N}$ is the radius and $f : A^{2r+1} \to A$ is the local rule.

Example: $A = \{0,1\}, n = 8, r = 1, f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)



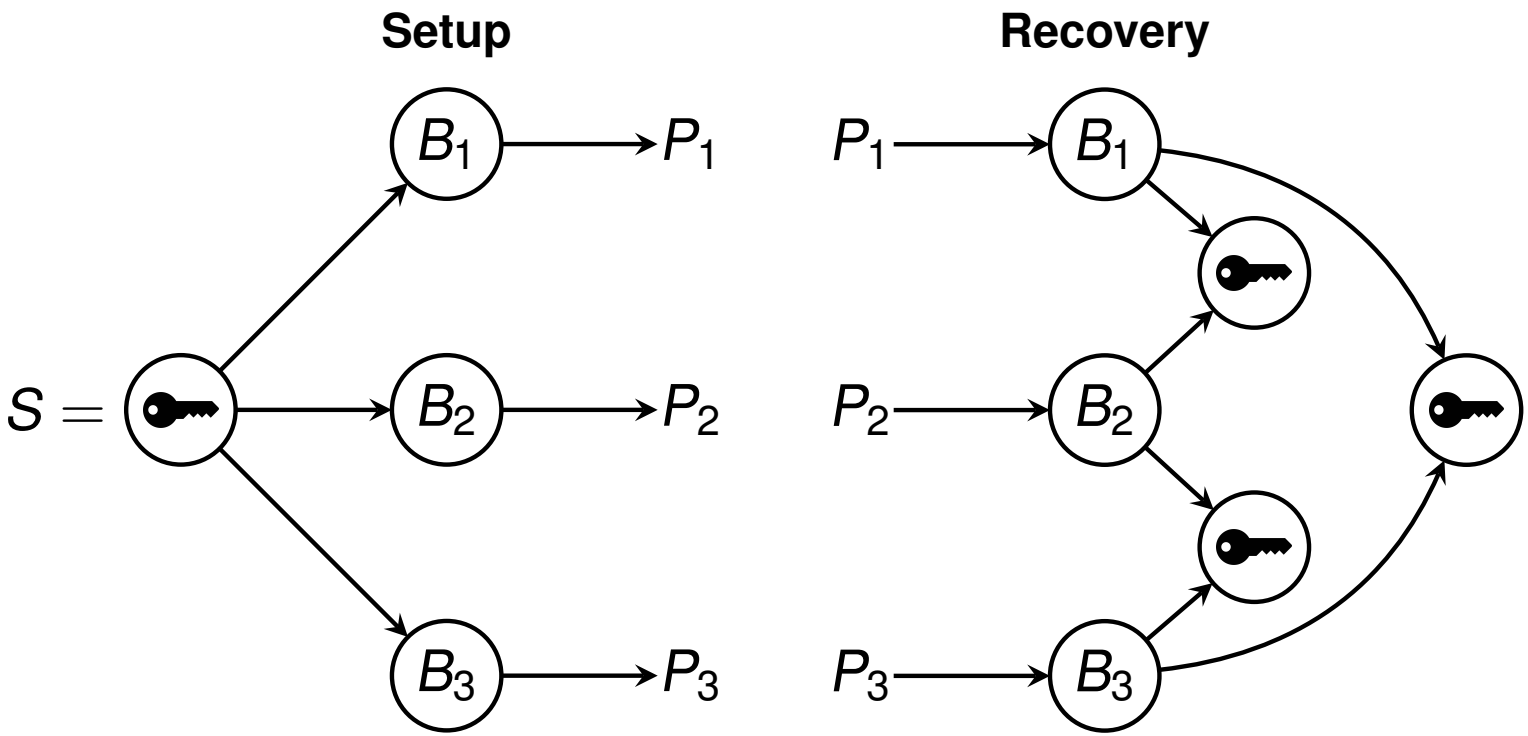


Remark: No boundary conditions ⇒ The array "shrinks"

Secret Sharing Schemes (SSS)

- Secret sharing scheme: a procedure enabling a dealer to share a secret S among a set $\mathcal{P}$ of n players
- (k, n) threshold schemes: at least k players out of n are required to recover S [Shamir79].

Example: $(2,3)$–scheme



SSS based on Cellular Automata: Why?

Twofold motivation:

- Theoretical: access structures arising from SSS where CA are used in a "natural" and simple way
- Practical: CA-based threshold schemes $\Rightarrow$ Efficient (parallel) implementation of threshold schemes

Remark: All the published CA-based SSS [Mariot14, DelRey05] provide a sequential threshold access structure (the shares need to be adjacent)

Question: Can (k, n)–schemes be realised through CA?

A Combinatorial Perspective: 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

Orthogonal Latin Squares

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)

A set of n pairwise orthogonal Latin squares is denoted as n-MOLS

$(2, n)$-Schemes through n-MOLS

Setup Phase

1. The dealer D chooses a row $S \in \{1, \cdots, N\}$ as the secret

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

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

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

$(2, n)$-Schemes through n-MOLS

Setup Phase

1. The dealer D chooses a row $S \in \{1, \cdots, N\}$ as the secret

$\rightarrow$

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

$\rightarrow$

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

$\rightarrow$

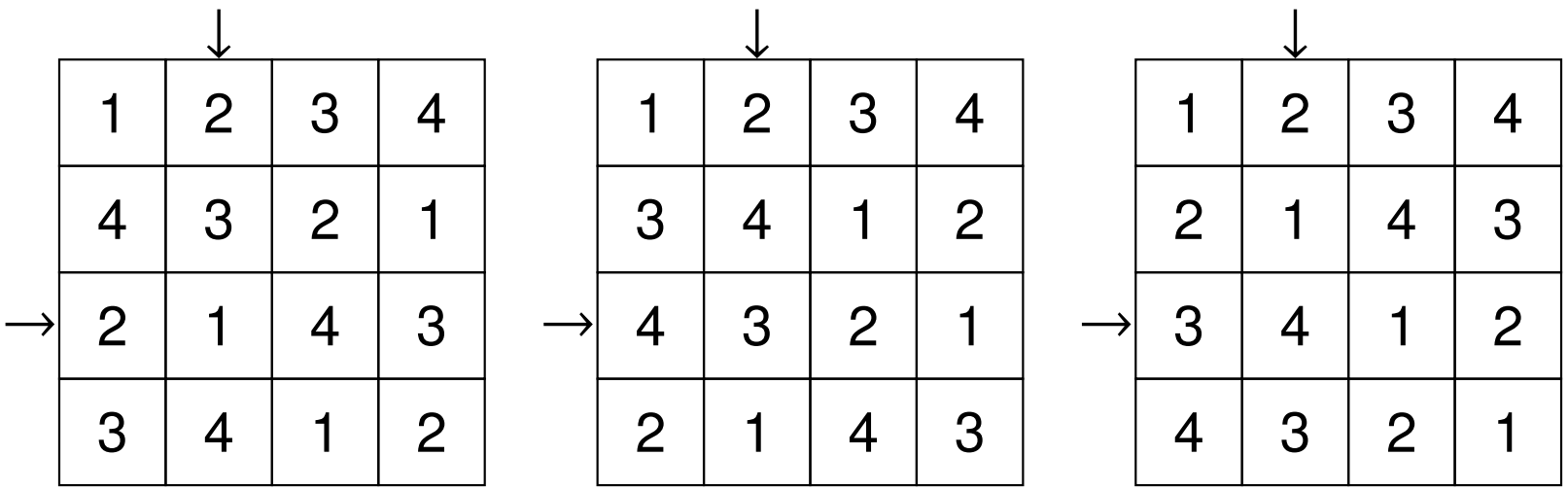
1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Example: $(2, 3)$-scheme, $S = 3$

$(2, n)$-Schemes through n-MOLS

Setup Phase

2. D randomly selects a column $j \in \{1, \cdots, N\}$

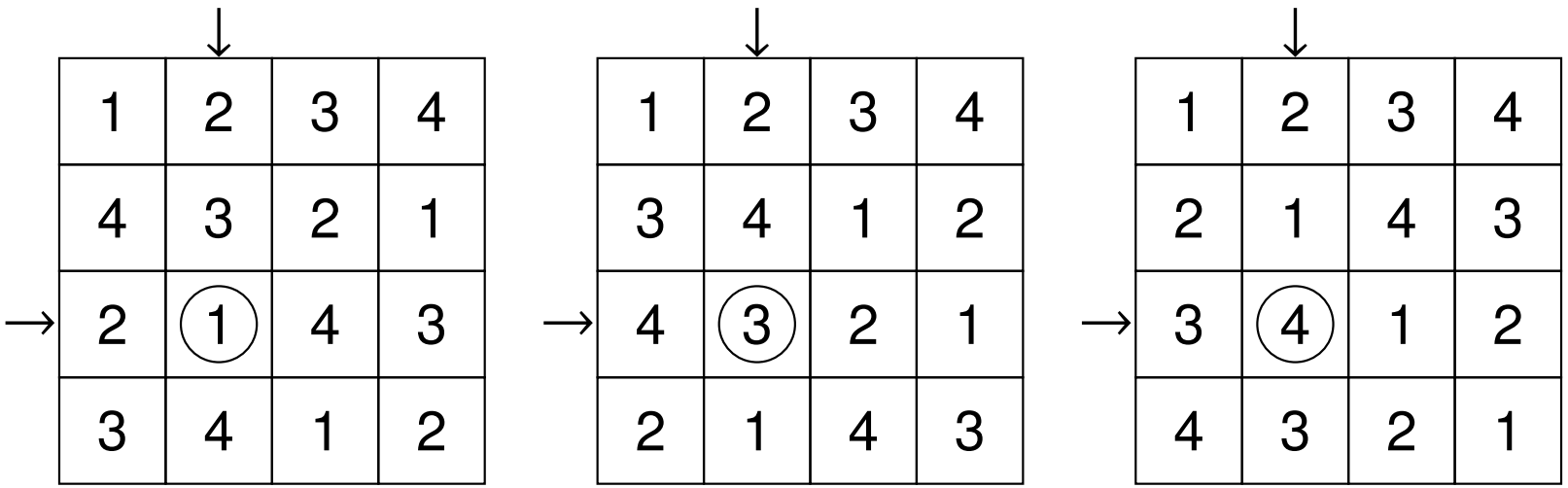


Example: $S = 3$, $j \leftarrow 2$

$(2,n)$-Schemes through n-MOLS

Setup Phase

3. The value of $L_i(S,j)$ for $i \in [N]$ is the share of P_i

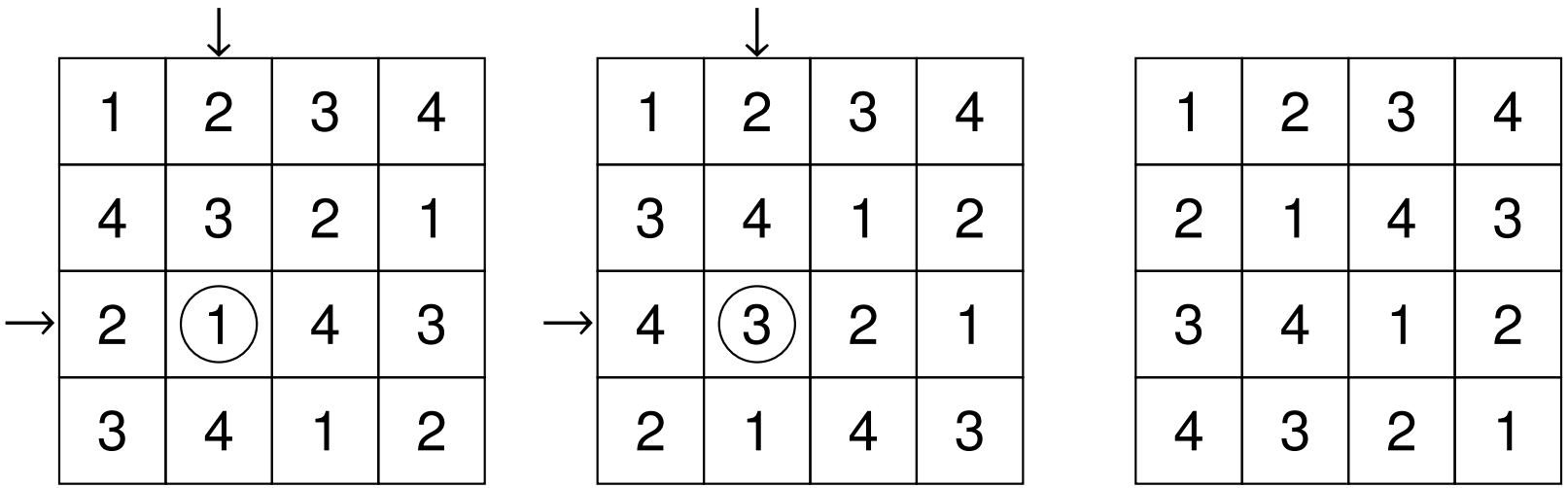


Example: $(2,3)$-scheme, $S = 3$, $j \leftarrow 2$, $B_1 = 1$, $B_2 = 3$, $B_3 = 4$

$(2,n)$-Schemes through n-MOLS

Recovery Phase

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)

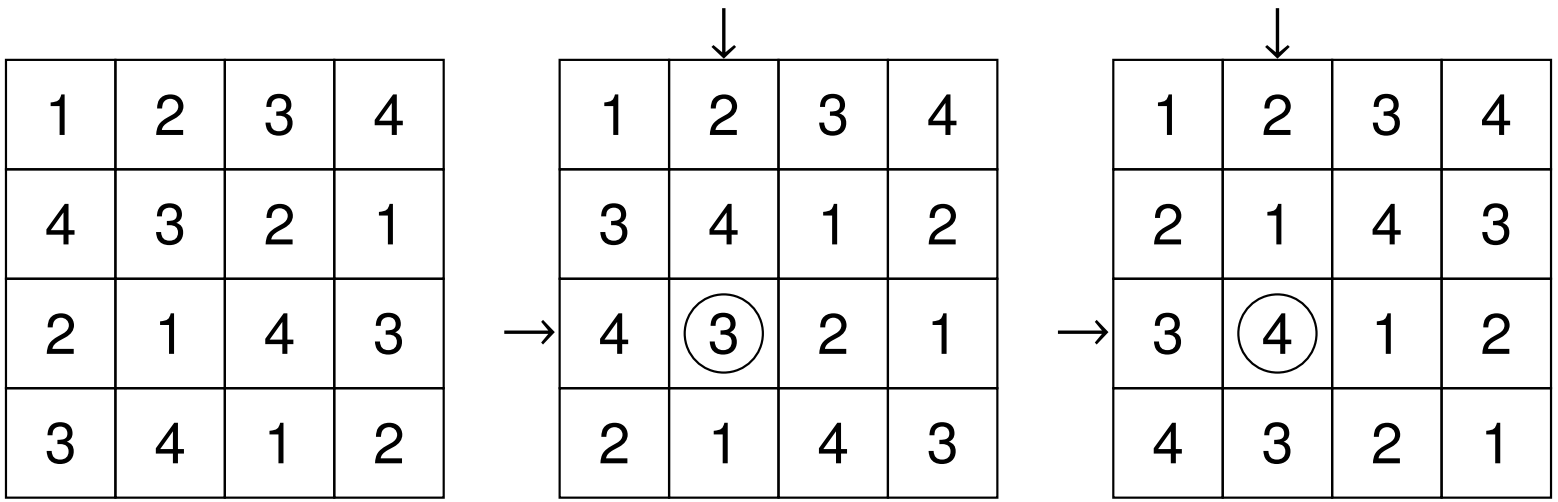


Example: $(2,3)$-scheme, $B_1 = 1$, $B_2 = 3 \Rightarrow (3,2)$

$(2,n)$-Schemes through n-MOLS

Recovery Phase

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)

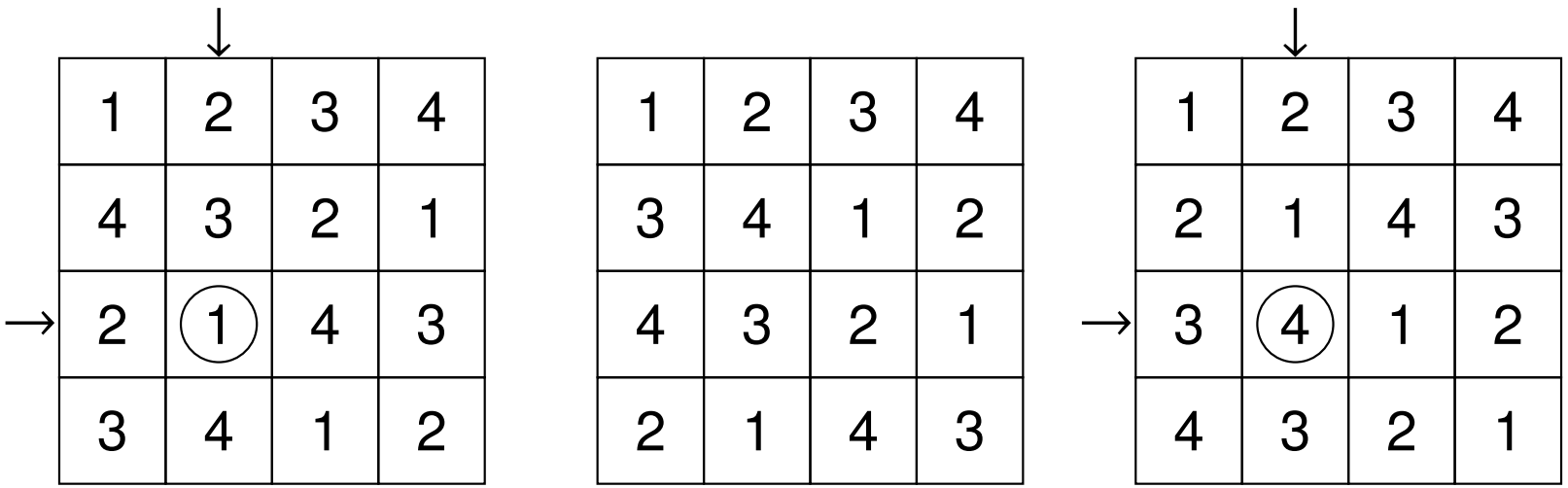


Example: $(2,3)$-scheme, $B_2 = 3$, $B_3 = 4 \Rightarrow (3,2)$

$(2,n)$-Schemes through n-MOLS

Recovery Phase

4. Since L_i, L_k are orthogonal, (B_i, B_k) uniquely identify (S, j)



Example: $(2,3)$-scheme, $B_1 = 1$, $B_3 = 4 \Rightarrow (3,2)$

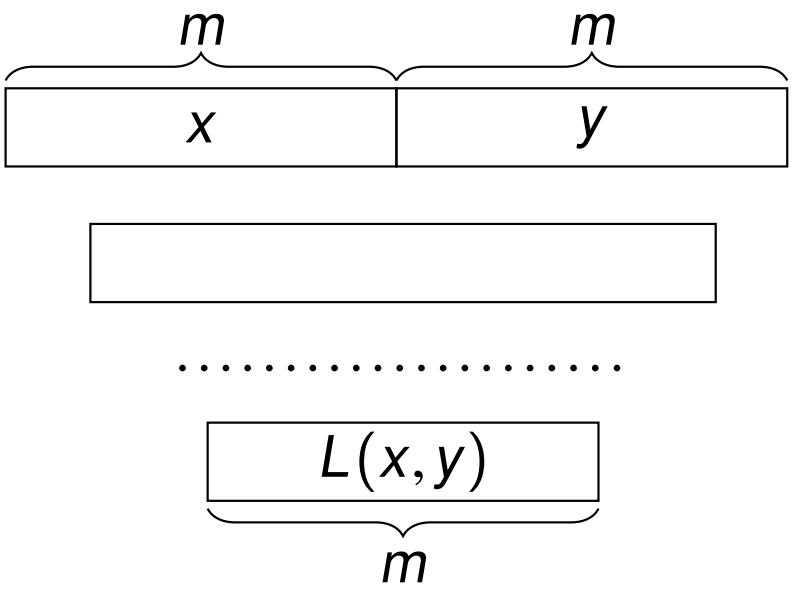
Latin Squares through Bipermutive CA (1/2)

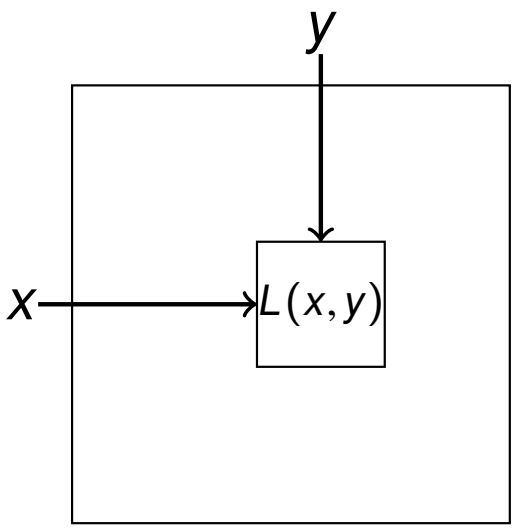
- Idea: determine which CA induce orthogonal Latin squares
- Bipermutive CA: local rule f is defined as

$$f(x_1, \cdots, x_{2r+1}) = x_1 \oplus g(x_2, \cdots, x_{2r}) \oplus x_{2r+1}$$

Lemma

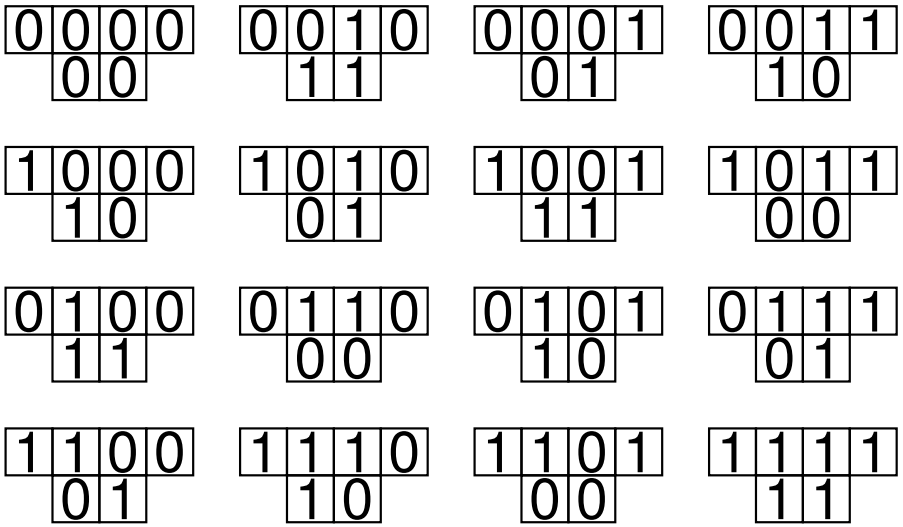
Let $\langle \mathbb{F}_2, 2m, r, f \rangle$ be a bipermutive CA with $2r|m$. Then, the CA generates a Latin square of order $N = 2^m$





Latin Squares through Bipermutive CA (2/2)

- Example: CA $\langle \mathbb{F}_2, 4, 1, f \rangle$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (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

$$f(x_1, \cdots, x_{2r+1}) = a_1 x_1 \oplus \cdots \oplus a_{2r+1} x_{2r+1} \ , \ a_i \in \mathbb{F}_2$$

- Associated polynomial:

$$f \mapsto \varphi(X) = a_1 + a_2 X + \cdots + a_{2r+1} X^{2r}$$

- Global rule: $m \times (m+2r)$ $2r$-diagonal transition matrix

$$M_F = \begin{pmatrix} a_1 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_{2r} \end{pmatrix}$$

$$x = (x_1, \cdots, x_n) \mapsto M_F x^\top$$

Orthogonal Latin Squares by Linear CA

Theorem

Let $F = \langle \mathbb{F}_2, 2m, r, f \rangle$ and $G = \langle \mathbb{F}_2, 2m, r, g \rangle$, be linear CA. The Latin squares induced by F and G are orthogonal if and only if $P_f(X)$ and $P_g(X)$ are 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)

Conclusions and Future Developments

Summing up:

- A $(2, n)$-scheme can be realised by n linear CA whose associated polynomials are pairwise coprime
- Setup: evolution of the n CA starting from a configuration whose left half is the secret, while right half are random bits
- Recovery: inversion of a Sylvester matrix

Future directions:

- Count (and build!) pairs of coprime polynomials
- Generalise to higher thresholds (via orthogonal hypercubes)

References

- [delRey05] del Rey, Á.M., Mateus, J.P., Sánchez, G.R.: A secret sharing scheme based on cellular automata. Appl. Math. Comput. 170(2), 1356–1364 (2005)
- [Mariot14] Mariot, L., Leporati, A.: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Proceedings of ACRI 2014. LNCS vol. 8751, pp. 417–426. Springer (2014)
- [Shamir79] Shamir, A.: How to share a secret. Commun. ACM 22(11):612–613 (1979)
- [Stinson04] Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer (2004)