

UNIVERSITY
OF TWENTE.



On the transversals of Latin squares generated by
nonlinear bipermutive CA

Alberto Dennunzio, Maximilien Gadouleau, **Luca Mariot**

`l.mariot@utwente.nl`

ACRI 2026

Ghent, July 8, 2026

Orthogonal Latin Squares (MOLS)

Definition

A *Latin square* is a $n \times n$ matrix where all rows and columns are permutations of $[n] = \{1, \dots, n\}$. Two Latin squares 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 |

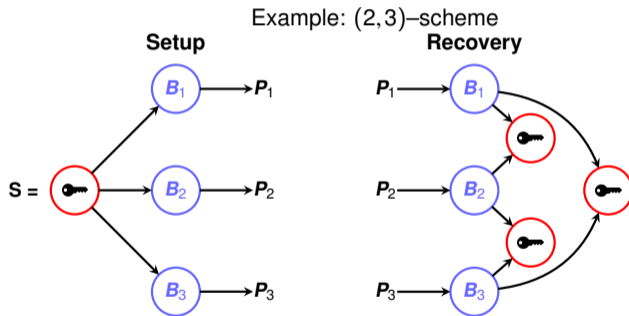
| | | | |
|---|---|---|---|
| 1 | 4 | 2 | 3 |
| 3 | 2 | 4 | 1 |
| 4 | 1 | 3 | 2 |
| 2 | 3 | 1 | 4 |

| | | | |
|---|---|---|---|
| 1 | 3 | 4 | 2 |
| 4 | 2 | 1 | 3 |
| 2 | 4 | 3 | 1 |
| 3 | 1 | 2 | 4 |

- ▶ **n -MOLS**: set of n pairwise orthogonal Latin squares [K15]

Cryptographic Application: Secret Sharing Schemes

(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]



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

Transversals in Latin Squares

- ▶ **Transversal** of an $N \times N$ Latin square: set of N staggered cells where each number from 1 to N appears once

| | | | |
|---|---|---|---|
| 1 | 3 | 4 | 2 |
| 4 | 2 | 1 | 3 |
| 2 | 4 | 3 | 1 |
| 3 | 1 | 2 | 4 |

▶ ○: $T_1 = \{(1,2), (2,3), (3,1), (4,4)\}$

Transversals in Latin Squares

- ▶ **Transversal** of an $N \times N$ Latin square: set of N staggered cells where each number from 1 to N appears once

| | | | |
|---|---|---|---|
| 1 | 3 | 4 | 2 |
| 4 | 2 | 1 | 3 |
| 2 | 4 | 3 | 1 |
| 3 | 1 | 2 | 4 |

▶ ○: $T_1 = \{(1,2), (2,3), (3,1), (4,4)\}$

▶ □: $T_2 = \{(1,3), (2,2), (3,4), (4,1)\}$

Transversals in Latin Squares

- ▶ **Transversal** of an $N \times N$ Latin square: set of N staggered cells where each number from 1 to N appears once

| | | | |
|---|---|---|---|
| 1 | 3 | 4 | 2 |
| 4 | 2 | 1 | 3 |
| 2 | 4 | 3 | 1 |
| 3 | 1 | 2 | 4 |

- ▶ ○: $T_1 = \{(1,2), (2,3), (3,1), (4,4)\}$
- ▶ □: $T_2 = \{(1,3), (2,2), (3,4), (4,1)\}$
- ▶ △: $T_3 = \{(1,1), (2,4), (3,2), (4,3)\}$

Transversals in Latin Squares

- ▶ **Transversal** of an $N \times N$ Latin square L : set of N staggered cells where each number from 1 to N appears once

| | | | |
|---|---|---|---|
| 1 | 3 | 4 | 2 |
| 4 | 2 | 1 | 3 |
| 2 | 4 | 3 | 1 |
| 3 | 1 | 2 | 4 |

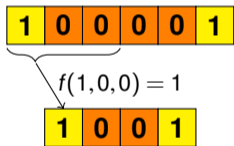
- ▶ ○: $T_1 = \{(1,2), (2,3), (3,1), (4,4)\}$
- ▶ □: $T_2 = \{(1,3), (2,2), (3,4), (4,1)\}$
- ▶ △: $T_3 = \{(1,1), (2,4), (3,2), (4,3)\}$
- ▶ ⬠: $T_4 = \{(4,1), (2,1), (3,3), (4,2)\}$

- ▶ **Remark:** if L has N disjoint transversal $\Rightarrow L$ has an *orthogonal mate* [K15]

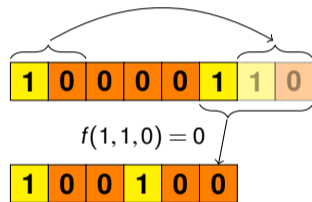
Cellular Automata

- ▶ One-dimensional **Cellular Automaton** (CA): a discrete parallel computation model composed of a finite array of n **cells**

Example: $n = 6$, $d = 3$, $f(s_i, s_{i+1}, s_{i+2}) = s_i \oplus s_{i+1} \oplus s_{i+2}$ (rule 150)



No Boundary CA – NBCA



Periodic Boundary CA – PBCA

- ▶ Each cell updates its **state** $s \in \mathbb{F}_2 = \{0, 1\}$ by applying a **local rule** $f : \mathbb{F}_2^d \rightarrow \mathbb{F}_2$ to itself and the $d - 1$ cells on its right [M19, M26]

Latin Squares through Bipermutive CA (1/2)

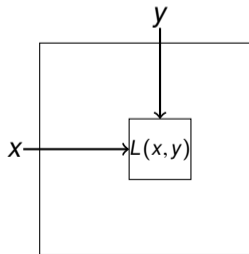
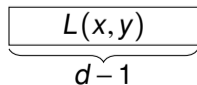
- ▶ **Bipermutive CA**: local rule f is defined as

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

- ▶ $g : \mathbb{F}_2^{d-2} \rightarrow \mathbb{F}_2$: **generating function** of f [L13]

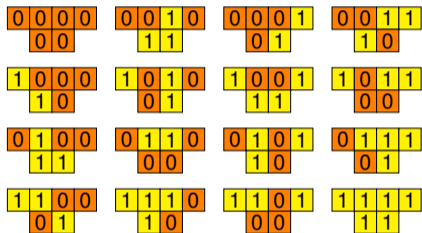
Lemma ([M16])

A (no-boundary) CA $F : \mathbb{F}_2^{2(d-1)} \rightarrow \mathbb{F}_2^d$ with bipermutive rule $f : \mathbb{F}_2^d \rightarrow \mathbb{F}_2$ generates a Latin square of order $N = 2^{d-1}$



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}

Problem: characterize the transversals of Latin squares generated by bipermutive CA

Transversals on the Main Diagonal

Question: which bipermutive CA have a transversal on the main diagonal?

| | | | |
|---|---|---|---|
| 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

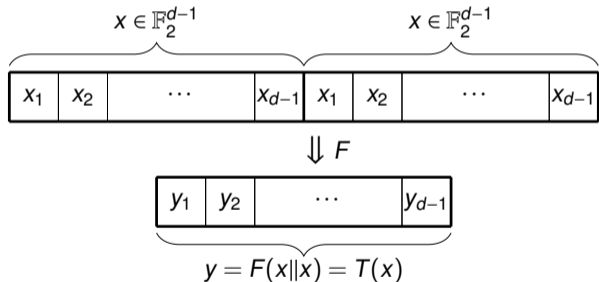
Idea: study the structure of the input configuration on the diagonal

Global Rule Restriction to Main Diagonal

Input configuration form: $(x, x) \in \mathbb{F}_2^{2(d-1)}$ (left and right block coincide)

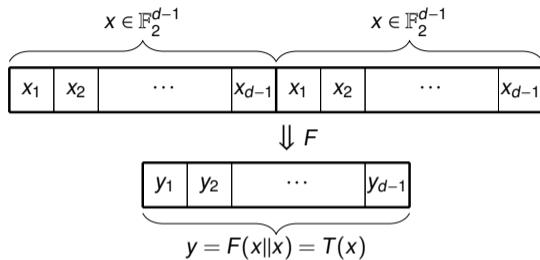
| | 00 | 10 | 01 | 11 |
|----|----|----|----|----|
| 00 | 1 | 4 | 3 | 2 |
| 10 | 2 | 3 | 4 | 1 |
| 01 | 4 | 1 | 2 | 3 |
| 11 | 3 | 2 | 1 | 4 |

(a) Rule 150



What is the mathematical form of the global rule?

Global Rule Form on the Main Diagonal

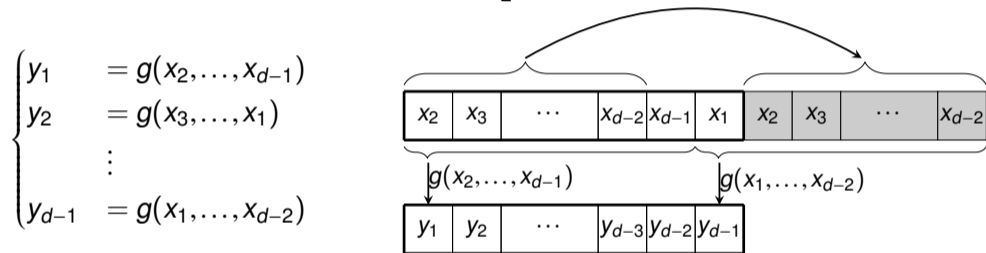


$$\begin{cases}
 y_1 & = f(x_1, x_2, \dots, x_{d-1}, x_1) = \cancel{x_1} \oplus g(x_2, \dots, x_{d-1}) \oplus \cancel{x_1} = g(x_2, \dots, x_{d-1}) \\
 y_2 & = f(x_2, x_3, \dots, x_1, x_2) = \cancel{x_2} \oplus g(x_3, \dots, x_1) \oplus \cancel{x_2} = g(x_3, \dots, x_1) \\
 & \vdots \\
 y_{d-1} & = f(x_{d-1}, x_1, \dots, x_{d-2}, x_{d-1}) = \cancel{x_{d-1}} \oplus g(x_1, \dots, x_{d-2}) \oplus \cancel{x_{d-1}} = g(x_1, \dots, x_{d-2})
 \end{cases}$$

Remark 1: on the diagonal, the local rule depends only on the central $d - 2$ cells

PBCA Mapping of the Diagonal Transversal

Remark 2: the transversal map $T : \mathbb{F}_2^{d-1} \rightarrow \mathbb{F}_2^{d-1}$ is defined by a PBCA with $d-1$ cells, equipped with $g : \mathbb{F}_2^{d-2} \rightarrow \mathbb{F}_2$ as a local rule.



Theorem

The Latin square of the NBCA F has a transversal on the main diagonal if and only if the generating function g induces an invertible PBCA $T : \mathbb{F}_2^{d-1} \rightarrow \mathbb{F}_2^{d-1}$.

Computational Search Experiments (Bonus)

| Intercalates | Nonlinearity | Rules |
|---------------------|--------------|-------|
| 2816 | 4 | 8 |
| 2944 | 4 | 8 |
| 3072 | 4 | 24 |
| 3200 | 4 | 16 |
| 3328 | 4 | 16 |
| 3520 | 4 | 16 |
| 3584 | 4 | 8 |
| 3648 | 4 | 52 |
| 3680 | 4 | 8 |
| 3712 | 4 | 16 |
| 3744 | 4 | 8 |
| 3776 | 4 | 8 |
| 3840 | 4 | 8 |
| 3904 | 4 | 20 |
| 3936 | 4 | 16 |
| 3968 | 4 | 8 |
| 4032 | 2 | 8 |
| 4032 | 4 | 32 |
| 4096 | 4 | 24 |
| 4160 | 2 | 16 |
| 4160 | 4 | 24 |
| 4288 | 2 | 40 |
| 4352 | 4 | 16 |
| 4864 | 4 | 8 |
| 5376 | 2 | 32 |
| 5888 | 4 | 16 |
| 7936 ^(†) | 0 | 16 |

- ▶ Exhaustive search of bijective rules up to $d = 6$
- ▶ Only **linear** rules have a transversal on the main diagonal up to $d = 5$
- ▶ $d = 6$: 472 rules found, out of which **456 are nonlinear**
- ▶ ≥ 28 isotopy classes, linear rules form a single class

| | | | |
|---|---|---|---|
| ① | ④ | 3 | 2 |
| 2 | 3 | 4 | 1 |
| ④ | ① | 2 | 3 |
| 3 | 2 | 1 | 4 |

- ▶ **Intercalate**: 2×2 Latin subsquare
- ▶ # of intercalates: **invariant** for isotopy [K15]

Example with $d = 6$, $g(x_1, x_2, x_3, x_4) = x_1 \oplus x_3 \oplus x_1 x_4$

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 22 | 11 | 32 | 21 | 2 | 31 | 12 | 9 | 14 | 3 | 8 | 29 | 26 | 23 | 20 | 17 | 6 | 27 | 16 | 5 | 18 | 15 | 28 | 25 | 30 | 19 | 24 | 13 | 10 | 7 | 4 |
| 2 | 21 | 12 | 31 | 22 | 1 | 32 | 11 | 10 | 13 | 4 | 7 | 30 | 25 | 24 | 19 | 18 | 5 | 28 | 15 | 6 | 17 | 16 | 27 | 26 | 29 | 20 | 23 | 14 | 9 | 8 | 3 |
| 4 | 23 | 16 | 29 | 24 | 3 | 30 | 9 | 12 | 15 | 2 | 5 | 32 | 27 | 22 | 17 | 20 | 7 | 26 | 13 | 8 | 19 | 14 | 25 | 28 | 31 | 18 | 21 | 16 | 11 | 6 | 1 |
| 3 | 24 | 9 | 30 | 23 | 4 | 29 | 10 | 11 | 16 | 1 | 6 | 31 | 28 | 21 | 18 | 19 | 8 | 25 | 14 | 7 | 20 | 13 | 26 | 27 | 32 | 17 | 22 | 15 | 12 | 5 | 2 |
| 7 | 18 | 13 | 28 | 19 | 6 | 25 | 16 | 15 | 10 | 5 | 4 | 27 | 30 | 17 | 24 | 23 | 2 | 29 | 12 | 3 | 22 | 9 | 32 | 31 | 26 | 21 | 20 | 11 | 14 | 1 | 8 |
| 8 | 17 | 14 | 27 | 20 | 5 | 26 | 15 | 16 | 9 | 6 | 3 | 28 | 29 | 18 | 23 | 24 | 1 | 30 | 11 | 4 | 21 | 10 | 31 | 32 | 25 | 22 | 19 | 12 | 13 | 2 | 7 |
| 6 | 19 | 16 | 25 | 18 | 7 | 28 | 13 | 14 | 11 | 8 | 1 | 26 | 31 | 20 | 21 | 22 | 3 | 32 | 9 | 2 | 23 | 12 | 29 | 30 | 27 | 24 | 17 | 10 | 15 | 4 | 5 |
| 5 | 20 | 15 | 26 | 17 | 8 | 27 | 14 | 13 | 12 | 7 | 2 | 25 | 32 | 19 | 22 | 21 | 4 | 31 | 10 | 1 | 24 | 11 | 30 | 29 | 28 | 23 | 18 | 9 | 16 | 3 | 6 |
| 14 | 25 | 4 | 23 | 26 | 13 | 24 | 3 | 6 | 1 | 12 | 15 | 18 | 21 | 32 | 27 | 30 | 9 | 20 | 7 | 10 | 29 | 8 | 19 | 22 | 17 | 28 | 31 | 2 | 5 | 16 | 11 |
| 13 | 26 | 3 | 24 | 25 | 14 | 23 | 4 | 5 | 2 | 11 | 16 | 17 | 22 | 31 | 28 | 29 | 10 | 19 | 8 | 9 | 30 | 7 | 20 | 21 | 18 | 27 | 32 | 1 | 6 | 15 | 12 |
| 15 | 28 | 1 | 22 | 27 | 16 | 21 | 2 | 7 | 4 | 9 | 14 | 19 | 24 | 29 | 26 | 31 | 12 | 17 | 6 | 11 | 32 | 5 | 18 | 23 | 20 | 25 | 30 | 3 | 8 | 13 | 10 |
| 16 | 27 | 2 | 21 | 28 | 15 | 22 | 1 | 8 | 3 | 10 | 13 | 20 | 23 | 30 | 25 | 32 | 11 | 18 | 5 | 12 | 31 | 6 | 17 | 24 | 19 | 26 | 29 | 4 | 7 | 14 | 9 |
| 12 | 29 | 6 | 19 | 32 | 9 | 18 | 7 | 4 | 5 | 14 | 11 | 24 | 17 | 26 | 31 | 28 | 13 | 22 | 3 | 16 | 25 | 2 | 23 | 20 | 21 | 30 | 27 | 8 | 1 | 10 | 15 |
| 11 | 30 | 5 | 20 | 31 | 10 | 17 | 8 | 3 | 6 | 13 | 12 | 23 | 18 | 25 | 32 | 27 | 14 | 21 | 4 | 15 | 26 | 1 | 24 | 19 | 22 | 29 | 28 | 7 | 2 | 9 | 16 |
| 9 | 32 | 7 | 18 | 29 | 12 | 19 | 6 | 1 | 8 | 15 | 10 | 21 | 29 | 27 | 30 | 25 | 16 | 23 | 2 | 13 | 28 | 3 | 22 | 17 | 24 | 31 | 26 | 5 | 4 | 11 | 14 |
| 10 | 31 | 8 | 17 | 30 | 11 | 20 | 5 | 2 | 7 | 16 | 9 | 22 | 19 | 28 | 29 | 26 | 15 | 24 | 1 | 14 | 27 | 4 | 21 | 18 | 23 | 32 | 25 | 6 | 3 | 12 | 13 |
| 27 | 16 | 17 | 6 | 7 | 20 | 13 | 26 | 19 | 24 | 25 | 30 | 15 | 12 | 5 | 2 | 11 | 32 | 1 | 22 | 23 | 4 | 29 | 10 | 3 | 8 | 9 | 14 | 31 | 28 | 21 | 18 |
| 28 | 15 | 18 | 5 | 8 | 19 | 14 | 25 | 20 | 23 | 26 | 29 | 16 | 11 | 6 | 1 | 12 | 31 | 2 | 21 | 24 | 3 | 30 | 9 | 4 | 7 | 10 | 13 | 32 | 27 | 22 | 17 |
| 25 | 14 | 19 | 8 | 5 | 18 | 15 | 28 | 17 | 22 | 27 | 32 | 13 | 10 | 7 | 4 | 9 | 30 | 3 | 24 | 21 | 2 | 31 | 12 | 1 | 6 | 11 | 16 | 29 | 26 | 23 | 20 |
| 26 | 13 | 20 | 7 | 6 | 17 | 16 | 27 | 18 | 21 | 28 | 31 | 14 | 9 | 8 | 3 | 10 | 29 | 4 | 23 | 22 | 1 | 32 | 11 | 2 | 5 | 12 | 15 | 30 | 25 | 24 | 19 |
| 29 | 12 | 23 | 2 | 1 | 24 | 11 | 30 | 21 | 20 | 31 | 26 | 9 | 16 | 3 | 6 | 13 | 28 | 7 | 18 | 17 | 8 | 27 | 14 | 5 | 4 | 15 | 10 | 25 | 32 | 19 | 22 |
| 30 | 11 | 24 | 1 | 2 | 23 | 12 | 29 | 22 | 19 | 32 | 25 | 10 | 15 | 4 | 5 | 14 | 27 | 8 | 17 | 18 | 7 | 28 | 13 | 6 | 3 | 16 | 9 | 26 | 31 | 20 | 21 |
| 31 | 10 | 21 | 4 | 3 | 22 | 9 | 32 | 23 | 18 | 29 | 28 | 11 | 14 | 1 | 8 | 15 | 26 | 5 | 20 | 19 | 6 | 25 | 16 | 7 | 2 | 13 | 12 | 27 | 30 | 17 | 24 |
| 32 | 9 | 22 | 3 | 4 | 21 | 10 | 31 | 24 | 17 | 30 | 27 | 12 | 13 | 2 | 7 | 16 | 25 | 6 | 19 | 20 | 5 | 26 | 15 | 8 | 1 | 14 | 11 | 28 | 29 | 18 | 23 |
| 24 | 3 | 26 | 13 | 12 | 31 | 6 | 17 | 32 | 27 | 18 | 21 | 4 | 7 | 14 | 9 | 8 | 19 | 10 | 29 | 28 | 15 | 22 | 1 | 16 | 11 | 2 | 5 | 20 | 23 | 30 | 25 |
| 23 | 4 | 25 | 14 | 11 | 32 | 5 | 18 | 31 | 28 | 17 | 22 | 3 | 8 | 13 | 10 | 7 | 20 | 9 | 30 | 27 | 16 | 21 | 2 | 15 | 12 | 1 | 6 | 19 | 24 | 29 | 26 |
| 22 | 1 | 28 | 15 | 10 | 29 | 8 | 19 | 30 | 25 | 20 | 23 | 2 | 5 | 16 | 11 | 6 | 17 | 12 | 31 | 26 | 13 | 24 | 3 | 14 | 9 | 4 | 7 | 18 | 21 | 32 | 27 |
| 21 | 2 | 27 | 16 | 9 | 30 | 7 | 20 | 29 | 26 | 19 | 24 | 1 | 6 | 15 | 12 | 5 | 18 | 11 | 32 | 25 | 14 | 23 | 4 | 13 | 10 | 3 | 8 | 17 | 22 | 31 | 28 |
| 18 | 7 | 32 | 9 | 14 | 27 | 4 | 21 | 26 | 31 | 24 | 17 | 6 | 3 | 12 | 13 | 2 | 23 | 16 | 25 | 30 | 11 | 20 | 5 | 10 | 15 | 8 | 1 | 22 | 19 | 28 | 29 |
| 17 | 8 | 31 | 10 | 13 | 28 | 3 | 22 | 25 | 32 | 23 | 18 | 5 | 4 | 11 | 14 | 1 | 24 | 15 | 26 | 29 | 12 | 19 | 6 | 9 | 16 | 7 | 2 | 21 | 20 | 27 | 30 |
| 20 | 5 | 30 | 11 | 16 | 25 | 2 | 23 | 28 | 29 | 22 | 19 | 8 | 1 | 10 | 15 | 4 | 21 | 14 | 27 | 32 | 9 | 18 | 7 | 12 | 13 | 6 | 3 | 24 | 17 | 26 | 31 |
| 19 | 6 | 29 | 12 | 15 | 26 | 1 | 24 | 27 | 30 | 21 | 20 | 7 | 2 | 9 | 16 | 3 | 22 | 13 | 28 | 31 | 10 | 17 | 8 | 11 | 14 | 5 | 4 | 23 | 18 | 25 | 32 |

Wrapping up:

- ▶ Characterized subclass of (nonlinear) BCA whose Latin squares have a transversal on the main diagonal
- ▶ The generating function must induce an invertible PBCA of size $d - 1$ [D95, M21]
- ▶ Linear rules of this subclass seem to form an isotopy class on their own

Future Directions:

- ▶ Characterize other transversals (**idea**: Eulerian cycles on de Bruijn graph [M17])
- ▶ Investigate disjointness properties of CA transversals

References

- [D95] J. Daemen: Cipher and hash function design strategies based on linear and differential cryptanalysis. Ph.D. thesis, KU Leuven (1995)
- [K15] A.D. Keedwell, J. Dénes: Latin squares and their applications. Elsevier (2015)
- [L13] A. Leporati and L. Mariot: 1-Resiliency of bipermutive cellular automata rules. In: Proceedings of AUTOMATA 2013, pp. 110–123 (2013)
- [M26] L. Manzoni, L. Mariot, G. Menara: Combinatorial designs and cellular automata: A survey. Discret. Appl. Math. 379:656–674 (2026)
- [M21] L. Mariot, S. Picek, D. Jakobovic, A. Leporati: Evolutionary algorithms for designing reversible cellular automata. Genet. Prog. Evolvable Mach. 22(4):429–461 (2021)
- [M19] L. Mariot, S. Picek, A. Leporati, and D. Jakobovic. Cellular automata based S-boxes. Cryptography and Communications 11(1):41–62 (2019)
- [M17] L. Mariot, A. Leporati, A. Dennunzio, E. Formenti: Computing the periods of preimages in surjective cellular automata. Nat. Comput. 16(3):367–381 (2017)
- [M16] 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 - constructions and analysis. Springer (2004)