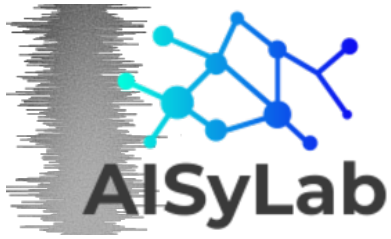


Latin Hypercubes and CA

Max Gadouleau[1], Luca Mariot[2]

[1] Department of Computer Science
Durham University

[2] Cyber Security Research Group
Delft University of Technology

AUTOMATA 2020, 11 August 2020

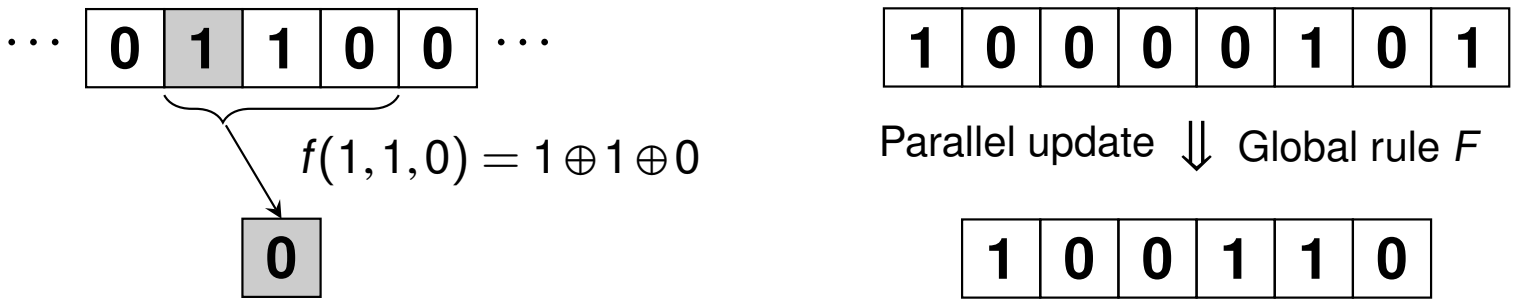
One-Dimensional Cellular Automata (CA)

Definition (One-dimensional CA)

A quadruple $\langle A, n, d, f \rangle$ with A a finite alphabet, $n \in \mathbb{N}$ is the number of cells, $d \in \mathbb{N}$ is the diameter and $f : A^d \to A$ is the local rule.

Remark: we only consider finite fields as alphabets, i.e. $A = \mathbb{F}_q$ for $q = p^a$ with p prime and $a \in \mathbb{N}$

Example: $A = \mathbb{F}_2$, $n = 8$, $d = 3$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)



CA Global Rule: $F : \{0,1\}^n \to \{0,1\}^{n-d+1}$ defined as

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

Latin Squares and Quasigroups

Definition

Latin square of order N: 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

Latin square of order N

$\Updownarrow$

Cayley table of quasigroup $(Q, \circ)$ **with** $|Q| = N$

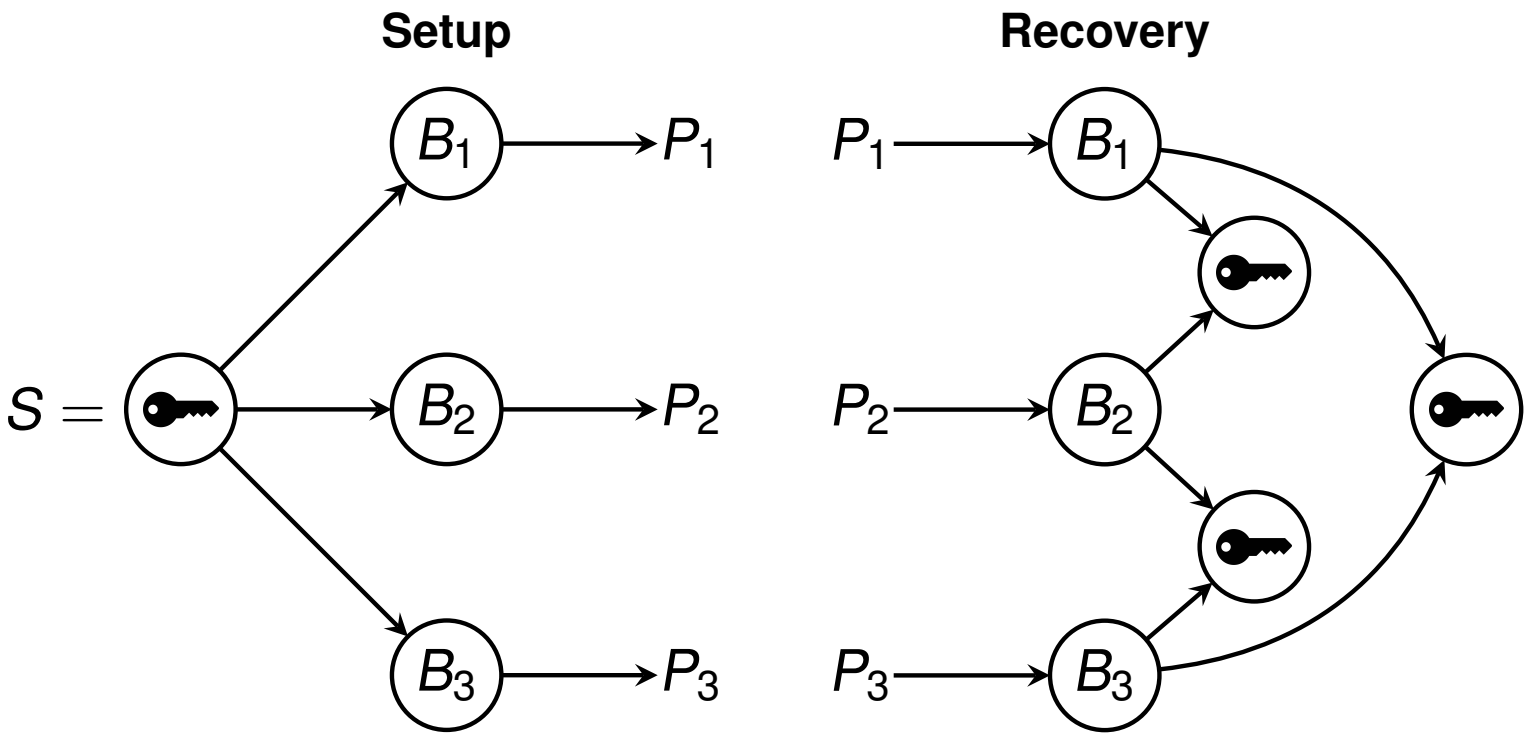
Definition

Quasigroup: algebraic structure $(Q, \circ)$ where for all $x, y \in Q$ the equations $x \circ z = y$ and $z \circ x = y$ have a unique solution for $z \in Q$

Secret Sharing Schemes (SSS)

(k,n) Threshold Secret Sharing Scheme: a procedure enabling a dealer to share a secret S among n players so that at least k players out of n can recover S [Shamir79].

Example: $(2,3)$–scheme



Remark: $(2,2)$–scheme $\Leftrightarrow$ Latin square

Latin Squares through Bipermutive CA (1/2)

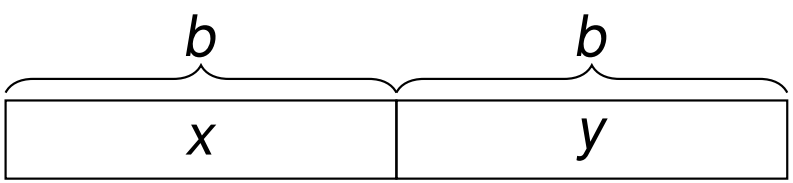
- Bipermutive CA: local rule f is defined as

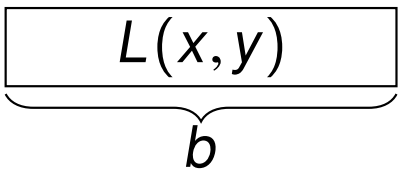
$$f(x_1, \cdots, x_d) = x_1 \oplus \varphi(x_2, \cdots, x_{d-1}) \oplus x_d$$

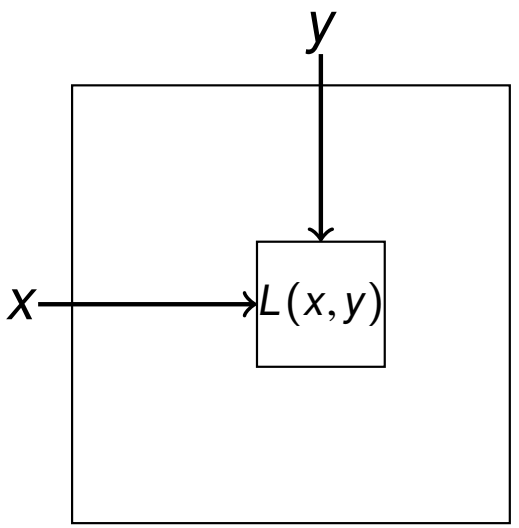
- $\varphi : \mathbb{F}_q^{d-2} \to \mathbb{F}_q$: generating function of f

Lemma ([Eloranta93, Mariot20])

Let $\langle \mathbb{F}_q, 2b, b+1, f \rangle$ be a CA with bipermutive rule f of diameter $d = b+1$. Then, F generates a Latin square of order $N = q^b$

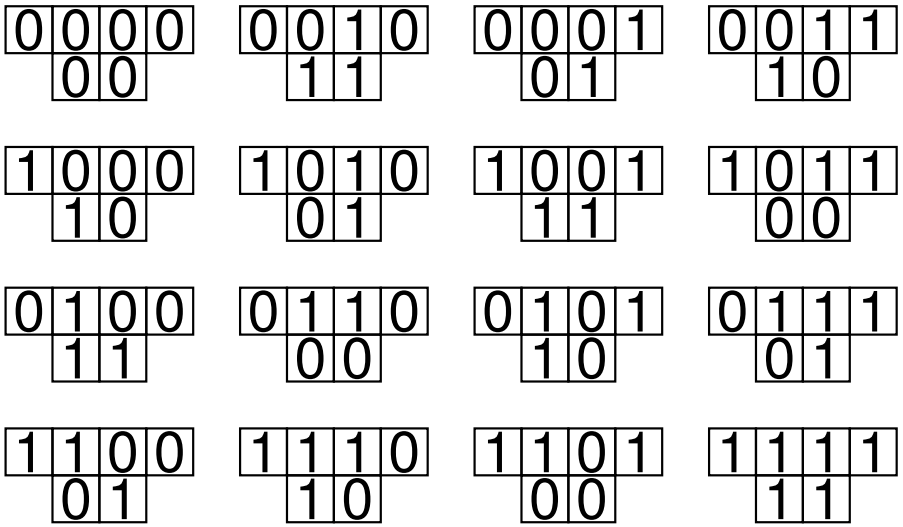






Latin Squares through Bipermutive CA (2/2)

- 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

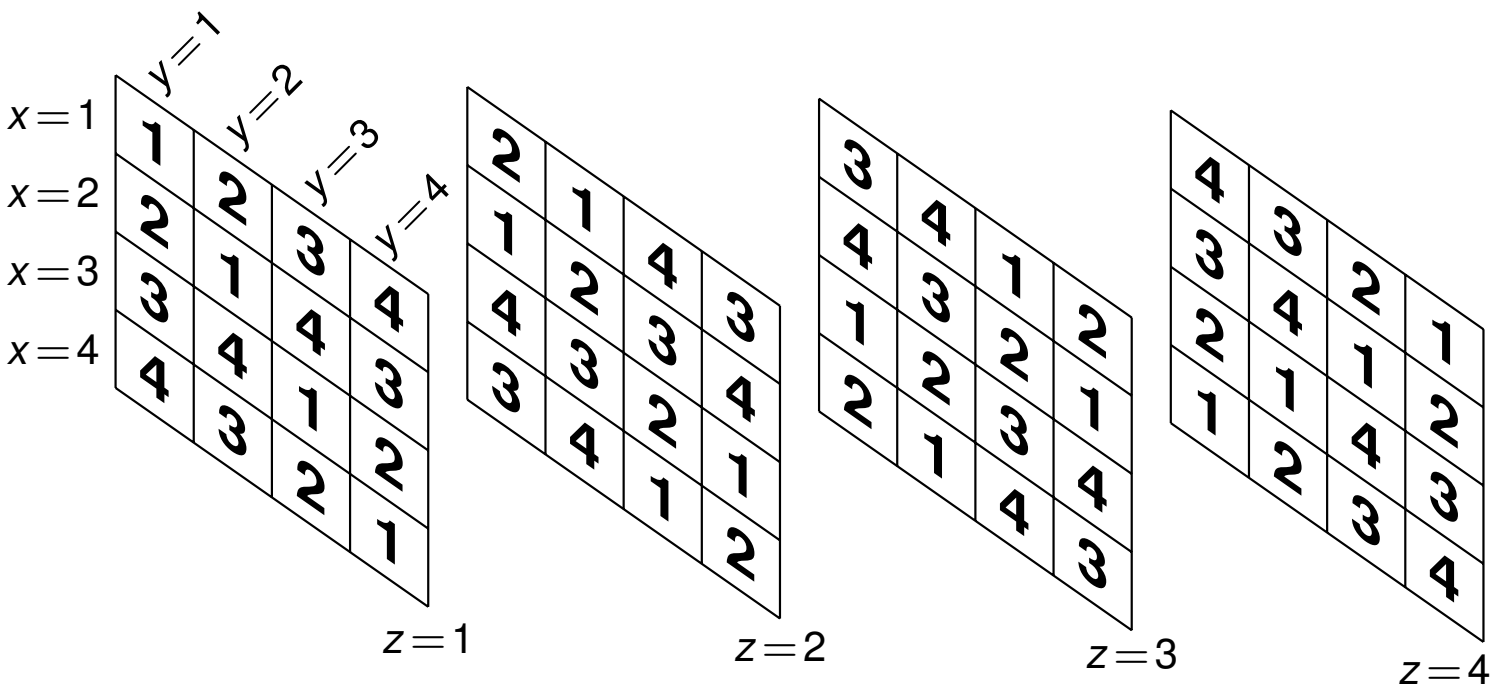
(b) Latin square L_{150}

Latin Hypercubes

Definition (Latin hypercube of dimension k and order N)

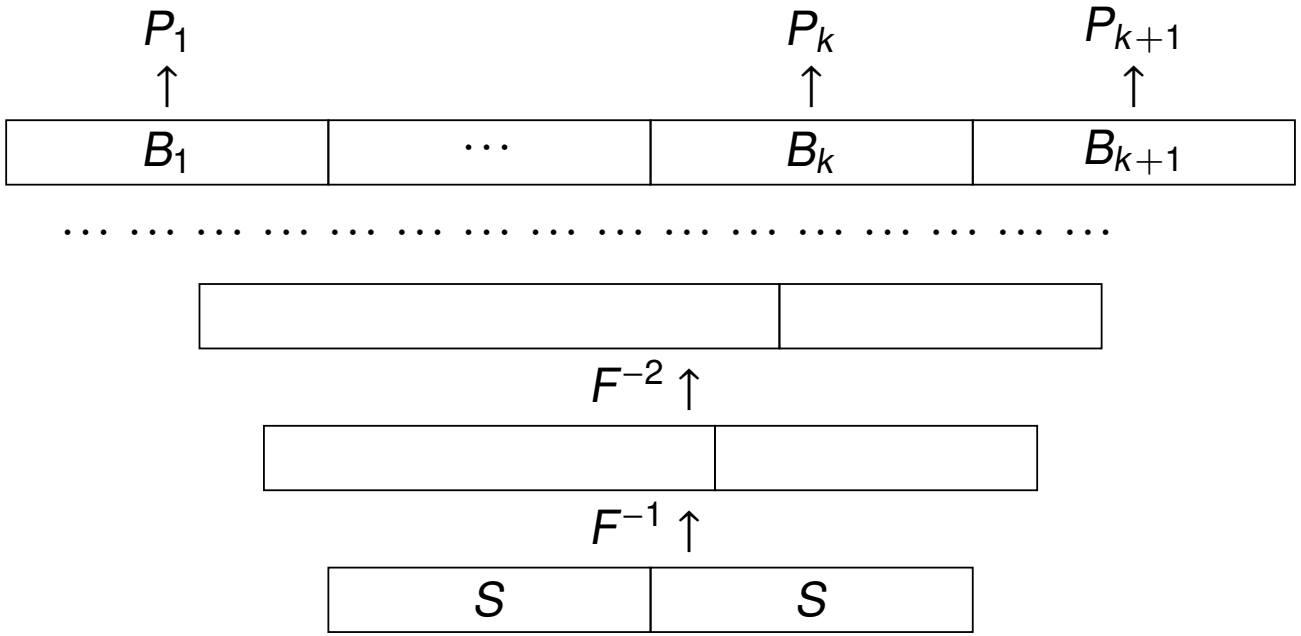
A k-dimensional array of side N such that fixing any $k-1$ coordinates $i_1, \cdots, i_{k-1}$ permutes $[N]$ on the remaining coordinate i_k

Example: $k = 3$, $N = 4 \Leftrightarrow$ Each number from 1 to 4 occurs once in each row, column, and file



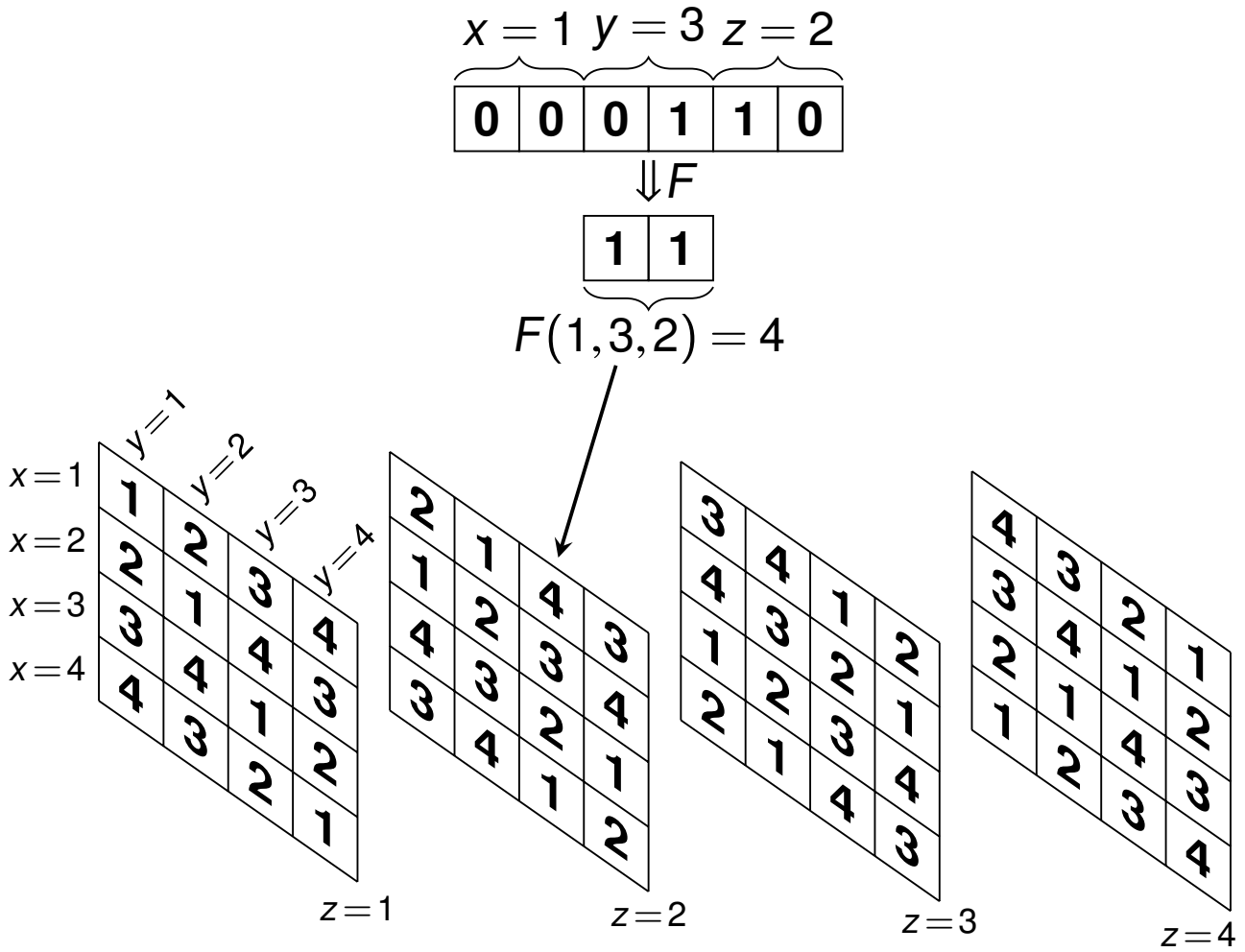
Motivation: CA-based Secret Sharing Schemes

- Latin hypercube of dimension $k \Leftrightarrow (k,k)$-SSS
- Latin hypercubes based on CA can be used to design secret sharing schemes with consecutive access structure [Mariot14]



- Useful in distributed cryptographic protocols, with applications e.g. to automatized control [Herranz18]

CA-Based Latin Hypercubes

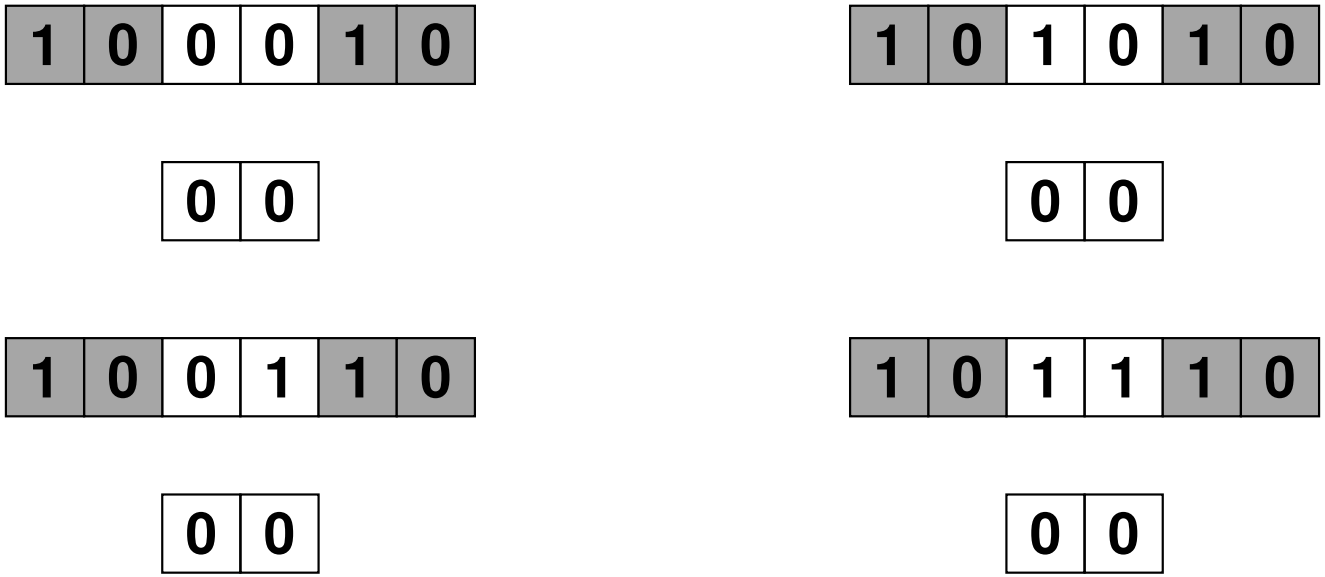


Example: Latin cube of order 4 generated by a CA $F : \mathbb{F}_2^6 \to \mathbb{F}_2^2$ defined by local rule $f(x_1, \cdots, x_5) = x_1 \oplus x_3 \oplus x_5$.

Latin Cubes: Bipermutivity is not Enough!

- **Question**: does any bipermutive rule generate a Latin cube?
- Unfortunately, no! Let $b = 2$, $k = 3$, and consider the CA $F : \mathbb{F}_2^6 \to \mathbb{F}_2$ defined by the local rule

$$f(x_1, x_2, x_3, x_4, x_5) = x_1 \oplus x_5$$



- Fixing (x_1, x_2) and (x_5, x_6) to $(1, 0)$, the CA F will always give $(0, 0)$ as a result, *independently* of (x_3, x_4):

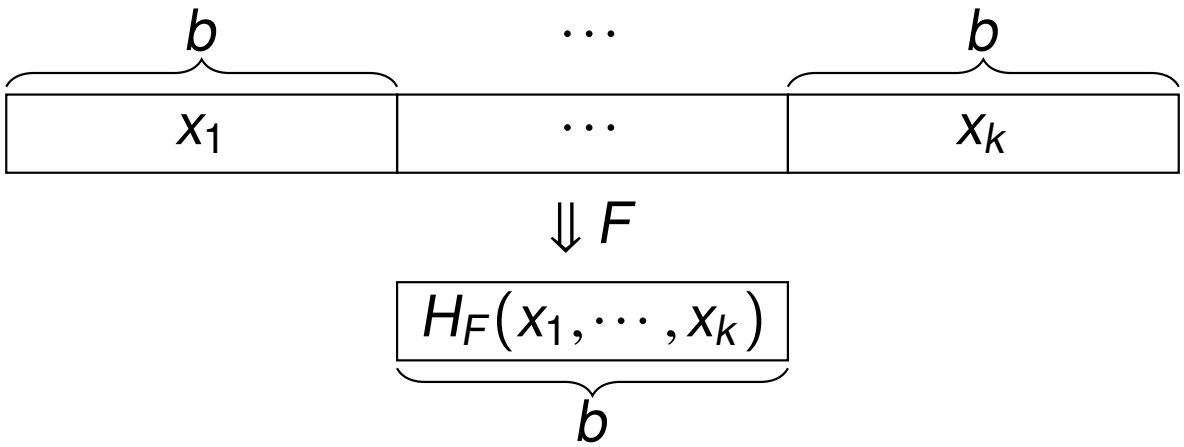
Problem Statement

Idea: Generalize the square construction to CA acting on k blocks of length b that represent the k dimensions of the hypercube

Problem

Let $b, k \in \mathbb{N}$, $N = q^b$ and $d = b(k-1)+1$.

1. ***(Characterization)**: When does a CA $F : \mathbb{F}_q^{bk} \to \mathbb{F}_q^b$ with rule $f : \mathbb{F}_q^d \to \mathbb{F}_q$ give a k-dimensional Latin hypercube of order N?*
2. ***(Counting)**: How many local rules $f : \mathbb{F}_q^d \to \mathbb{F}_q$ generate k-dimensional hypercubes of order N?*



Linear Bipermutive CA (LBCA)

- Local rule: linear combination of the neighborhood cells

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

- A linear local rule f is bipermutive iff $a_1 \neq 0$, $a_d \neq 0$
- Global rule: $n \times (n+d-1)$ $(d-1)$-diagonal transition matrix

$$M_F = \begin{pmatrix} a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_1 & \cdots & a_d & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_1 & \cdots & a_d \end{pmatrix}$$

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

Linear System for LBCA cubes

- Let $k = 3$, $b \in \mathbb{N}$ and let $F : \mathbb{F}_q^{3b} \to \mathbb{F}_q^b$ be a LBCA defined by a rule $f : \mathbb{F}_q^{2b+1} \to \mathbb{F}_q$.
- Since f is linear, $y = F(x)$ can be expressed as a system of b linear equations and $3b$ variables:

$$\begin{cases} y_1 &= x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{2b} x_{2b} \oplus x_{2b+1} \\ y_2 &= x_2 \oplus a_2 x_3 \oplus \cdots \oplus a_{2b} x_{2b+1} \oplus x_{2b+2} \\ &\vdots \\ y_b &= x_b \oplus a_2 x_{b+1} \oplus \cdots \oplus a_{2b} x_{3b-1} \oplus x_{3b} \end{cases}$$

- Fixing the $2b$ leftmost and rightmost variables reduces this to a linear system in b equations and b variables

Toeplitz Matrix Characterization

Matrix associated to the reduced linear system:

$$M_f = \begin{pmatrix} a_{b+1} & a_{b+2} & \cdots & a_{2b} \\ a_b & a_{b+1} & \cdots & a_{2b-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_{b+1} \end{pmatrix}$$

Remark: the above matrix is a Toeplitz matrix, thus we have:

Lemma

Let $F : \mathbb{F}_q^{3b} \to \mathbb{F}_q^b$ *be a LBCA defined by*

$$f(x_1, \cdots, x_{2b+1}) = x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{2b} x_{2b} \oplus x_{2b+1} \ .$$

Then, F generates a Latin cube of order $N = q^b$ *if and only if the Toeplitz matrix* M_F *defined by* $a_2, \cdots, a_{2b} \in \mathbb{F}_q$ *is invertible.*

Counting LBCA Latin Cubes

Theorem ([Price18])

Let $b \in \mathbb{N}$. Then, the number of invertible $b \times b$ Toeplitz matrices over $\mathbb{F}_q$ is $q^{q^{b-1}}$.

Since the number of LBCA with rules of diameter $d = 2b + 1$ generating Latin cubes corresponds to the number of invertible $b \times b$ Toeplitz matrices over $\mathbb{F}_q$, we have:

Corollary

Let $b \in \mathbb{N}$. Then, the number of linear bipermutive CA $F : \mathbb{F}_q^{3b} \to \mathbb{F}_q^b$ whose associated hypercube H_F is a Latin cube is $q^{q^{b-1}}$.

Generalizing to Hypercubes

- When $k > 3$, the LBCA $F : \mathbb{F}_q^{bk} \to \mathbb{F}_q^b$ is defined by a local rule $f : \mathbb{F}_q^{b(k-1)+1} \to \mathbb{F}_q$ of the form:

$$f(x_1, \cdots, x_{b(k-1)+1}) = x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{b(k-1)} x_{b(k-1)} \oplus x_{b(k-1)+1}$$

- the values of $y = F(x) \in \mathbb{F}_q^b$ are determined by a linear system in b equations and bk variables:

$$\begin{cases} y_1 & = x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{b(k-1)} x_{b(k-1)} \oplus x_{b(k-1)+1} \\ y_2 & = x_2 \oplus a_2 x_3 \oplus \cdots \oplus a_{b(k-1)} x_{b(k-1)+1} \oplus x_{b(k-1)+2} \\ & \vdots \\ y_b & = x_b \oplus a_2 x_{b+1} \oplus \cdots \oplus a_{b(k-1)} x_{bk-1} \oplus x_{bk} \end{cases}$$

Characterization of LBCA Latin Hypercubes

Matrix associated to the reduced system obtained by leaving free only the variables of the $(i+1)$-th block, $1 \leq i \leq k-2$:

$$M_{F,i} = \begin{pmatrix} a_{bi+1} & a_{bi+2} & \cdots & a_{b(i+1)-1} \\ a_{bi} & a_{bi+1} & \cdots & a_{b(i+1)-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{b(i-1)+2} & a_{b(i-1)+3} & \cdots & a_{bi+1} \end{pmatrix}$$

Theorem

The hypercube generated by a LBCA $F : \mathbb{F}_q^{bk} \to \mathbb{F}_q^b$ with rule $f : \mathbb{F}_q^{b(k-1)+1} \to \mathbb{F}_q$ is a k-dimensional Latin hypercube of order $N = q^b$ if and only all Toeplitz matrices $M_{F,i}$ are invertible.

Adjacent Matrices Coefficients

Remark: the matrices $M_{F,i}, M_{F,i+1}$ share the coefficients respectively on the upper and lower triangular parts:

$$M_{F,i} = \begin{pmatrix} a_{bi+1} & \mathbf{a_{bi+2}} & \cdots & \mathbf{a_{b(i+1)}} \\ a_{bi} & a_{bi+1} & \cdots & \mathbf{a_{b(i+1)-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{b(i-1)+2} & a_{b(i-1)+3} & \cdots & a_{bi+1} \end{pmatrix}$$

$$M_{F,i+1} = \begin{pmatrix} a_{b(i+1)+1} & a_{b(i+1)+2} & \cdots & a_{b(i+2)} \\ \mathbf{a_{b(i+1)}} & a_{b(i+1)+1} & \cdots & a_{b(i+2)-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a_{bi+2}} & \mathbf{a_{bi+3}} & \cdots & a_{b(i+1)+1} \end{pmatrix}$$

Determinant Boolean Function

- Let $det(a_2, \cdots, a_{2b})$ be the Boolean function associating to each $b \times b$ Toepliz matrix its determinant, 0 or 1

Example: $b = 2$

$$M_F = \begin{pmatrix} a_3 & a_4 \\ a_2 & a_3 \end{pmatrix}$$

$$det(a_2, a_3, a_4) = a_3 \oplus a_2 a_4$$

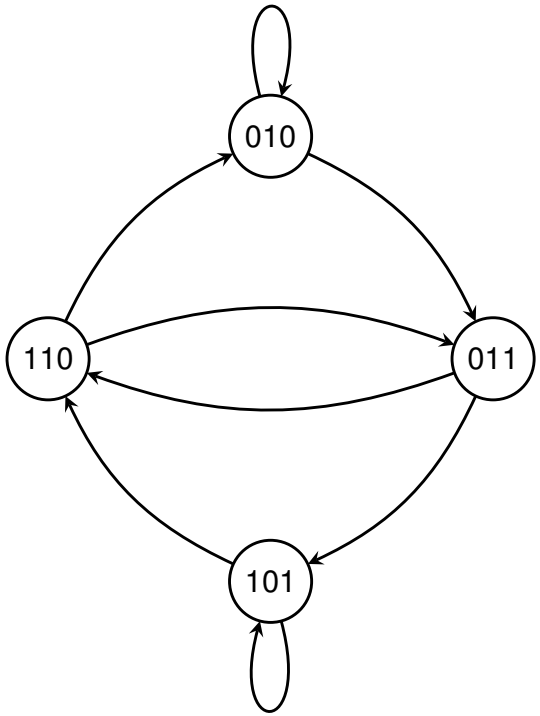
a_2	a_3	a_4	$det(a_2, a_3, a_4)$
0	0	0	0
1	0	0	0
0	**1**	**0**	**1**
1	**1**	**0**	**1**
0	0	1	0
1	**0**	**1**	**1**
0	**1**	**1**	**1**
1	1	1	0

- The **support** of $det(\cdot)$ defines the invertible matrices
- $det(\cdot)$ is always balanced

De Bruijn Graph of Determinant

Latin hypercubes of dimension k correspond to paths of length $k-3$ on the De Bruijn Graph G_{det} of the support of $det(\cdot)$:

a_2	a_3	a_4	$det(a_2,a_3,a_4)$
0	0	0	0
1	0	0	0
0	**1**	**0**	**1**
1	**1**	**0**	**1**
0	0	1	0
1	**0**	**1**	**1**
0	**1**	**1**	**1**
1	1	1	0



Example: the path $(0,1,0)-(0,1,1)-(1,0,1)$ gives rise to the $k=5$ dimensional Latin hypercube of order 2^2 defined by

$$f(x_1,\cdots,x_9) = x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_8 \oplus x_9$$

Counting Latin Hypercubes

Lemma

The De Bruijn graph G_{det} of the determinant function det is $(q-1)q^{b-1}$-regular for all $b \in \mathbb{N}$

Since the number of Latin hypercubes corresponds to the number of paths of length $k-3$ on G_{det}, we obtain

Theorem

The number of k-dimensional Latin hypercubes of order q^b generated by LBCA $F : \mathbb{F}_q^{bk} \to \mathbb{F}_q^b$ with rule $f : \mathbb{F}_q^{b(k-1)+1} \to \mathbb{F}_q$ is

$$L_{b,k,q} = (q-1)^{k-2} q^{(k-1)(b-1)} \quad .$$

Conclusions

Recap of the main results:

- We generalized the construction of Latin squares based on Bipermutive CA in [Mariot20] to Latin hypercubes of any dimensions
- For dimension $k = 3$, any LBCA whose central coefficients define an invertible Toeplitz matrix generates a Latin cube
- Latin hypercubes of dimension $k > 3$ induced by LBCA can be characterized by paths over the de Bruijn graph of the determinant function

Open Problems

Several interesting problems remain to be explored, such as:

- Design of an algorithm for constructing sequences of invertible Toeplitz matrices with overlapping coefficients
- Characterize sets of Mutually Orthogonal Latin hypercubes defined by LBCA, using e.g. the generalized resultant in [Deissler18]
- Analyze the cycle structure of the preimages of LBCA generating hypercubes [Mariot17a]
- Employ heuristic techniques to explore hypercubes based on *nonlinear CA* (e.g. Genetic Programming [Mariot17b])

References

- [Deissler18] Deissler, J.: A resultant for Hensel's Lemma. arXiv preprint arXiv:1301.4073 (2018)
- [Eloranta93] Eloranta, K.: Partially Permutive Cellular Automata. Nonlinearity 6(6), 1009–1023 (1993)
- [Herranz18] Herranz, J., Sáez, G.: Secret sharing schemes for (k,n)-consecutive access structures. In: CANS 2018. LNCS vol. 11124, pp. 463–480. Springer (2018)
- [Mariot20] Mariot, L., Gadouleau, M., Formenti, E., Leporati, A.: Mutually orthogonal latin squares based on cellular automata. Designs, Codes and Cryptography 88(2):391–411 (2020)
- [Mariot17a] Mariot, L., Leporati, A., Dennunzio, A., Formenti, E.: Computing the periods of preimages in surjective cellular automata. Natural Computing 16(3):367–381 (2017).
- [Mariot17b] Mariot, L., Picek, S., Jakobovic, D., Leporati, A.: Evolutionary algorithms for the design of orthogonal latin squares based oncellular automata. In: Proceedings of the Genetic and Evolutionary Computation Conference, GECCO 2017, Berlin, Germany, July 15-19, 2017, pages 306–313 (2017)
- [Mariot14] Mariot, L., Leporati, A.: Sharing Secrets by Computing Preimages of Bipermutive Cellular Automata. In: Was, J., Sirakoulis, G.Ch., Bandini, S. (eds.): ACRI 2014. LNCS vol. 8751, pp. 417–426. Springer, Heidelberg (2014)
- [Price18] Price, G., Wortham, M.: On Toeplitz matrices over $GF(2)$. arXiv preprint arXiv:1804.00983, 2018.