

Latin Hypercubes based on Linear Cellular Automata

Luca Mariot¹, Max Gadouleau²

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

² Department of Computer Science
Durham University

Nice, September 26, 2019

One-Dimensional Cellular Automata (CA)

Definition

One-dimensional CA: triple $\langle n, d, f \rangle$ where $n \in \mathbb{N}$ is the number of cells in a one-dimensional array, $d \in \mathbb{N}$ is the diameter and $f : \{0, 1\}^d \rightarrow \{0, 1\}$ is the local rule.

Example: $n = 8$, $d = 3$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)

...

0	1	1	0	0
---	---	---	---	---

 ...

$f(1, 1, 0) = 1 \oplus 1 \oplus 0$

0

1	0	0	0	0	1	0	1
---	---	---	---	---	---	---	---

Parallel update \Downarrow Global rule F

1	0	0	1	1	0
---	---	---	---	---	---

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

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

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 $[N] = \{1, \dots, N\}$

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

Latin square of order N



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

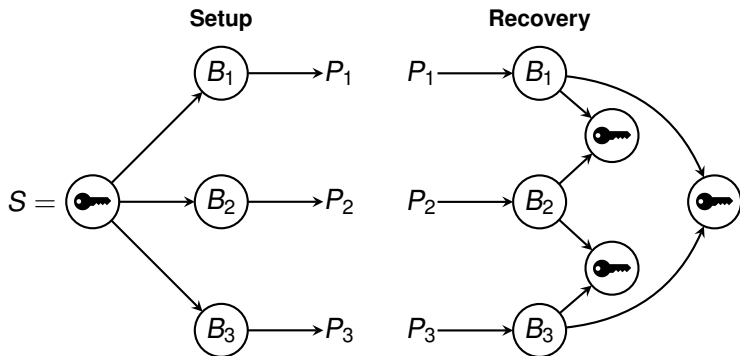
Definition

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)

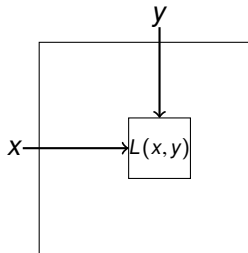
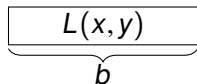
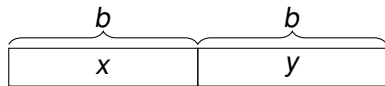
- ▶ **Bipermutive CA**: local rule f is defined as

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

- ▶ $\varphi : \{0, 1\}^{d-2} \rightarrow \{0, 1\}$: **generating function** of f

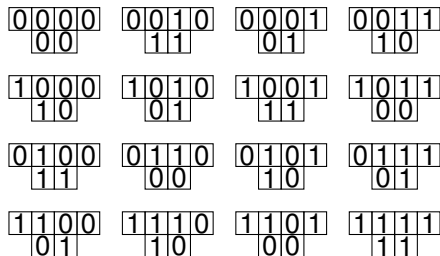
Lemma ([Eloranta93, Mariot16])

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



Latin Squares through Bipermutive CA (2/2)

- ▶ **Example:** CA $\langle 4, 1, f \rangle$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (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

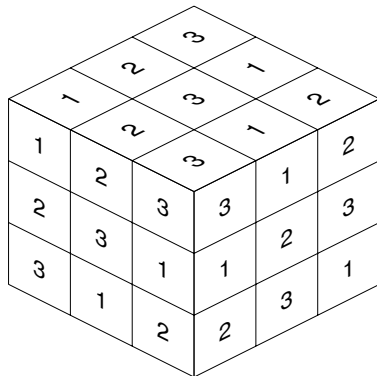
Definition

Latin hypercube of dimension k and order N : a k -dimensional array of side N such that fixing any $k - 1$ coordinates i_1, \dots, i_{k-1} gives a permutation of $[N]$ on the remaining coordinate i_k

Example: $k = 3, N = 3$

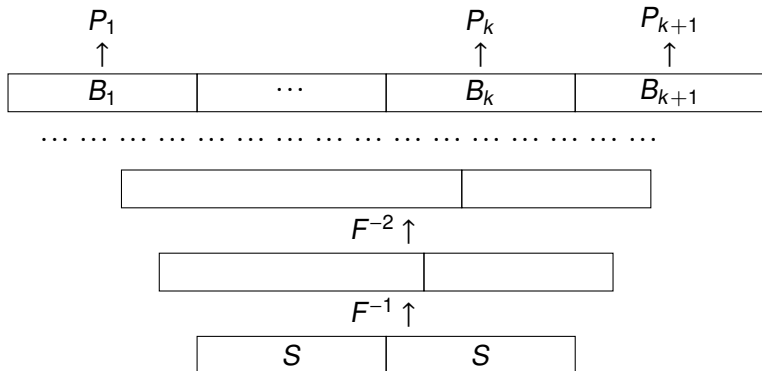


Each number from 1 to 3 occurs once in each row, column, and file



Motivation: CA-based Secret Sharing Schemes

Latin hypercubes based on CA can be used to design secret sharing schemes with **consecutive access structure** [Mariot14]



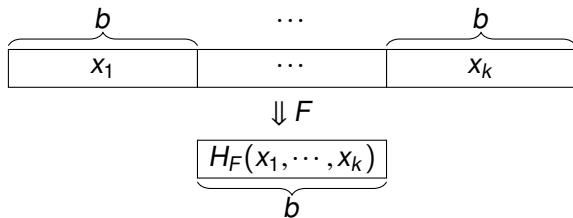
Problems Statement

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

Problem

Let $b, k \in \mathbb{N}$, $N = 2^b$ and $d = b(k - 1) + 1$.

1. **(Characterization):** When does a CA $F : \mathbb{F}_2^{bk} \rightarrow \mathbb{F}_2^b$ with rule $f : \mathbb{F}_2^d \rightarrow \mathbb{F}_2$ give a k -dimensional Latin hypercube of order N ?
2. **(Counting):** How many local rules $f : \mathbb{F}_2^d \rightarrow \mathbb{F}_2$ generate k -dimensional hypercubes of order N ?



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 $F : \mathbb{F}_2^6 \rightarrow \mathbb{F}_2$ defined by the local rule

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

1	0	0	0	1	0
---	---	---	---	---	---

0	0
---	---

1	0	0	1	1	0
---	---	---	---	---	---

0	0
---	---

1	0	1	0	1	0
---	---	---	---	---	---

0	0
---	---

1	0	1	1	1	0
---	---	---	---	---	---

0	0
---	---

- ▶ 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) :

Linear Bipermutive CA (LBCA)

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

$$f(x_1, \dots, x_d) = a_1 x_1 \oplus \dots \oplus a_d x_d, \quad a_i \in \mathbb{F}_2$$

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

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

$$x = (x_1, \dots, x_n) \mapsto M_F x^T$$

Linear System for LBCA cubes

- ▶ Let $k = 3$, $b \in \mathbb{N}$ and let $F : \mathbb{F}_2^{3b} \rightarrow \mathbb{F}_2^b$ be a LBCA defined by a rule $f : \mathbb{F}_2^{2b+1} \rightarrow \mathbb{F}_2$.
- ▶ 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 $F : \mathbb{F}_2^{3b} \rightarrow \mathbb{F}_2^b$ be a LBCA defined by

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

Then, F generates a Latin cube of order $N = 2^b$ if and only if the Toeplitz matrix M_F defined by $a_2, \dots, a_{2b} \in \mathbb{F}_2$ is invertible.

Theorem ([Price18])

Let $b \in \mathbb{N}$. Then, the number of invertible $b \times b$ Toeplitz matrices over \mathbb{F}_2 is $2^{2(b-1)}$.

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}_2 , we have:

Corollary

Let $b \in \mathbb{N}$. Then, the number of linear bipermutive CA $F : \mathbb{F}_2^{3b} \rightarrow \mathbb{F}_2^b$ whose associated hypercube H_F is a Latin cube is $2^{2(b-1)}$.

Generalizing to Hypercubes

- ▶ When $k > 3$, the LBCA $F : \mathbb{F}_2^{bk} \rightarrow \mathbb{F}_2^b$ is defined by a local rule $f : \mathbb{F}_2^{b(k-1)+1} \rightarrow \mathbb{F}_2$ of the form:

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

- ▶ the values of $y = F(x) \in \mathbb{F}_2^b$ are determined by a linear system in b equations and bk variables:

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

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 $F : \mathbb{F}_2^{bk} \rightarrow \mathbb{F}_2^b$ with rule $f : \mathbb{F}_2^{b(k-1)+1} \rightarrow \mathbb{F}_2$ is a k -dimensional Latin hypercube of order $N = 2^b$ if and only if 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 $\det(a_2, \dots, a_{2b})$ be the **Boolean function** associating to each $b \times b$ Toeplitz matrix its determinant, 0 or 1

Example: $b = 2$

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

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

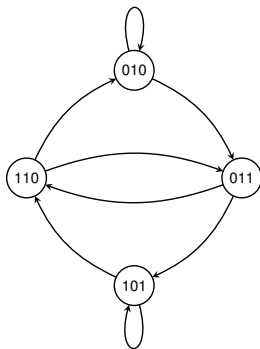
a_2	a_3	a_4	$\det(a_2, a_3, a_4)$
0	0	0	0
1	0	0	0
0	1	0	1
1	1	0	1
0	0	1	0
1	0	1	1
0	1	1	1
1	1	1	0

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

De Bruijn Graph of Determinant

Latin hypercubes of dimension k corresponds to paths of length $k - 3$ on the **De Bruijn Graph** G_{det} associated to 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

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

Counting Latin Hypercubes

Lemma

The De Bruijn graph G_{det} of the determinant function det is 2^{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 2^b generated by LBCA $F : \mathbb{F}_2^{bk} \rightarrow \mathbb{F}_2^b$ with rule $f : \mathbb{F}_2^{b(k-1)+1} \rightarrow \mathbb{F}_2$ is






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

Recap of the main results:

- ▶ We generalized the construction of Latin squares based on Bipermutive CA in [Mariot16] 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

Several interesting problems remain to be explored, such as:

- ▶ Design of an algorithm for constructing sequences of invertible Toeplitz matrices with overlapping coefficients
- ▶ Generalize these results to LBCA over larger finite fields \mathbb{F}_q
- ▶ Characterize sets of **Mutually Orthogonal** Latin hypercubes defined by LBCA

-  [Eloranta93] Eloranta, K.: Partially Permutive Cellular Automata. *Nonlinearity* 6(6), 1009–1023 (1993)
-  [Mariot16] Mariot, L., Formenti, E., Leporati, A.: Constructing Orthogonal Latin Squares from Linear Cellular Automata. In: *Exploratory papers of AUTOMATA 2016*. CoRR abs/1610.00139 (2016)
-  [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.
-  [Shamir79] Shamir, A.: How to share a secret. *Commun. ACM* 22(11):612–613 (1979)