Enumerating Orthogonal Latin Squares Generated by Bipermutive CA

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 Côte d'Azur

AUTOMATA 2017 – Milan, June 7–9, 2017

One-Dimensional Cellular Automata (CA)

Definition

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

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

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

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

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 $z \in Q$

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

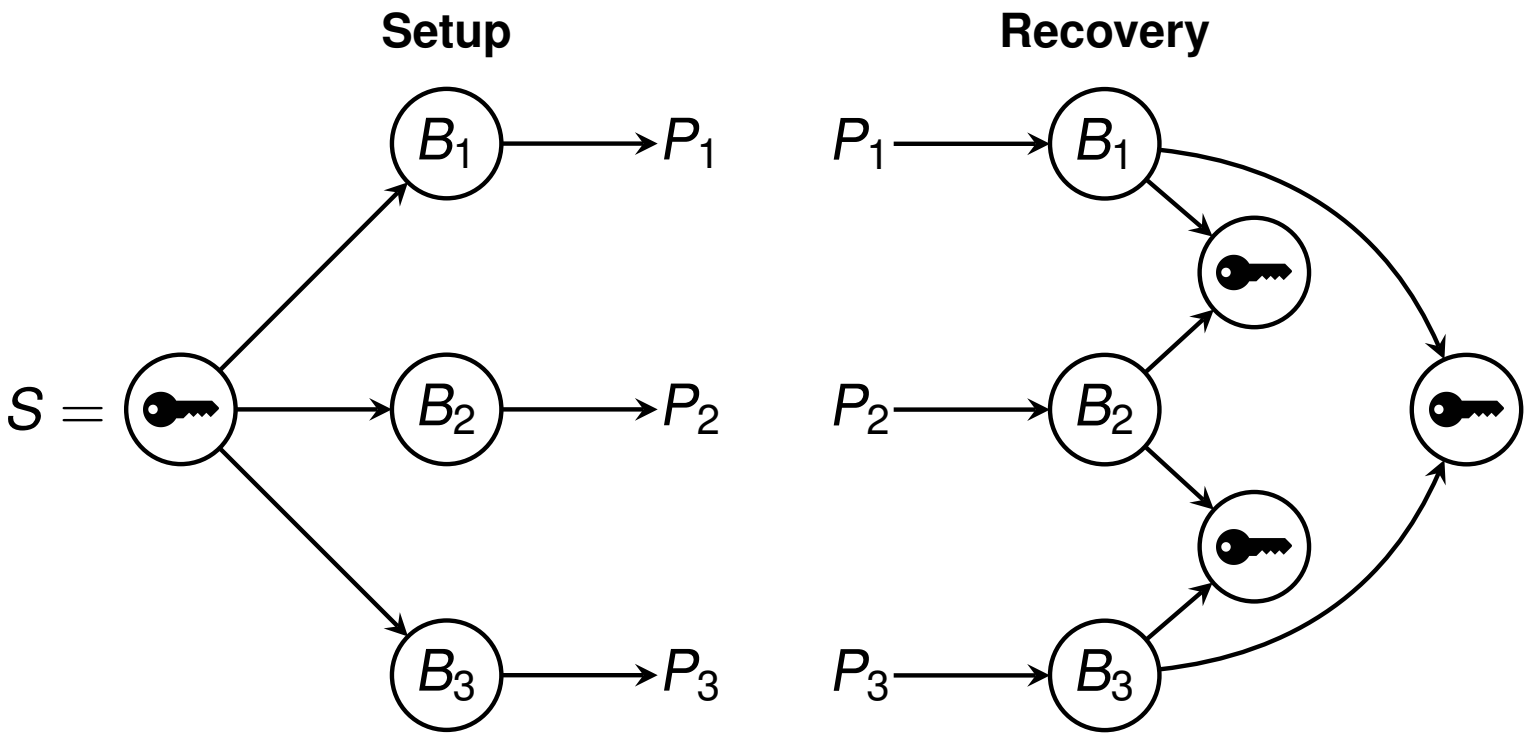
(c) (L_1, L_2)

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

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: $(2,n)$–scheme $\Leftrightarrow$ set of n-MOLS

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)

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

Latin Squares through Bipermutive CA (1/2)

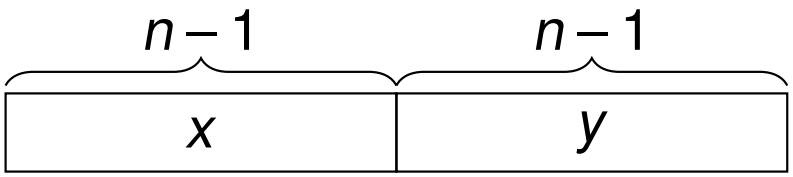
- Idea: determine which CA induce orthogonal Latin squares
- Bipermutive CA: local rule f is defined as

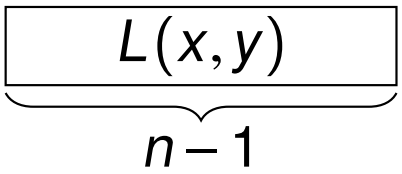
$$f(x_1, \cdots, x_n) = x_1 \oplus \varphi(x_2, \cdots, x_{2r}) \oplus x_n$$

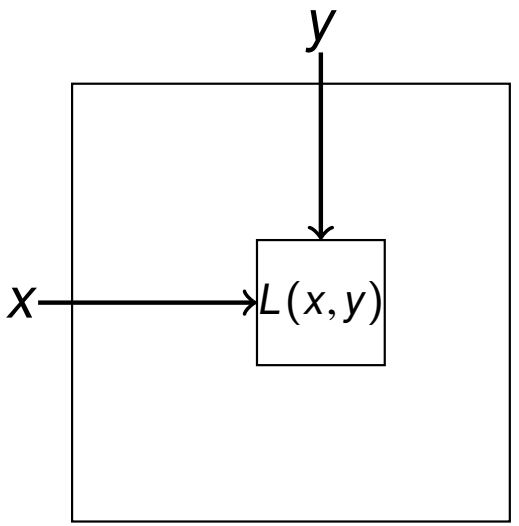
- $\varphi : \{0,1\}^{n-2} \to \{0,1\}$: generating function of f

Lemma ([Eloranta93, Mariot16])

Let $\langle 2(n-1), n, f \rangle$ be a CA with bipermutive rule. Then, the global rule F generates a Latin square of order $N = 2^{n-1}$

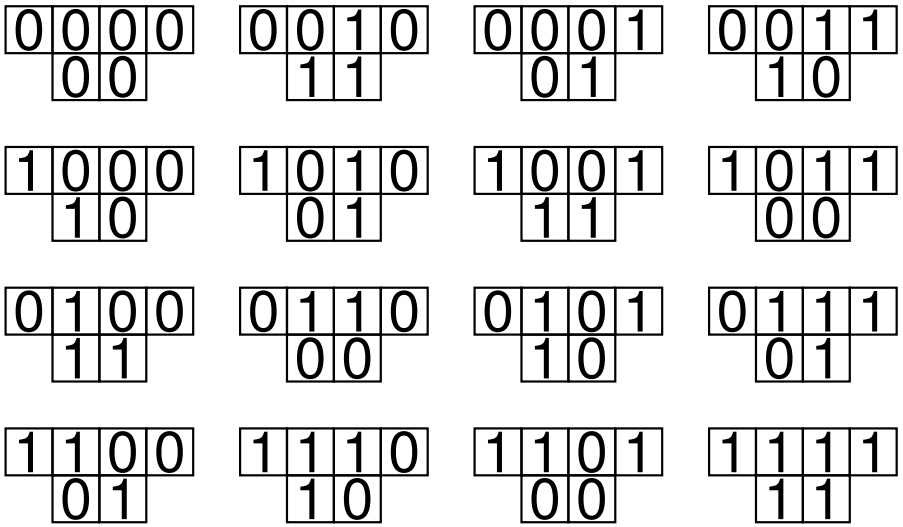






Latin Squares through Bipermutive CA (2/2)

- 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}

Orthogonal Latin Squares by Linear CA

- Bipermutive Linear rule: $f(x) = x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_{n-1} x_{n-1} \oplus x_n$
- Associated polynomial: $f \mapsto P_f(X) = a_1 + a_2 X + \cdots + a_n X^{n-1}$

Theorem ([Mariot16])

Bipermutive linear rules $f, g : \{0,1\}^n \to \{0,1\}$ generate orthogonal Latin squares 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)

Enumerating CA-based OLS

- Enumeration of OLS in the linear case $\Leftrightarrow$ Enumeration of pairs of coprime polynomials (But that's another story...)
- ... What about the nonlinear case?
- MOLS arising from nonlinear constructions have relevance in cheater-immune Secret Sharing Schemes [Tompa88]

Goal: Exhaustive enumeration of pairs of bipermutive rules of size n generating orthogonal Latin squares, classified by nonlinearity

Nonlinearity

- Affine function: $l(x_1, \cdots, x_n) = a \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n$, $a, a_i \in \{0,1\}$
- Nonlinearity of f: Hamming distance of the truth table of f from the set of all affine functions
- Walsh transform of f: given $\omega \in \{0,1\}^n$,

$$W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus \omega \cdot x} \text{ , where } \omega \cdot x = \bigoplus_{i=1}^{n} \omega_i \cdot x_i$$

Definition

Let $f : \{0,1\}^n \to \{0,1\}$. The *nonlinearity* of f is defined as

$$Nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \{0,1\}^n} \{|W_f(\omega)|\}$$

Search Space Size

- Number of Boolean functions of n variables: $\mathcal{F}_n = 2^{2^n}$
- Bipermutive rules of size $n \Leftrightarrow$ Generating functions of size $n-2$ (which are $\mathcal{F}_{n-2} = 2^{2^{n-2}}$)
- Pairs of bipermutive rules of size n: $\mathcal{B}_n = 2^{2^{n-1}} = \mathcal{F}_{n-1}$

n	3	4	5	6	7
$\mathcal{B}_n$	16	256	65536	4294967296	$\approx 1.84 \cdot 10^{19}$

- **Remark:** Exhaustive enumeration possible up to $n = 6$
- How can we further prune the search space?

Preliminary Results

- Reversal of f: $f_R(x_1, \cdots, x_n) = f(x_n, \cdots, x_1)$
- Complement of f: $f_C(x_1, \cdots, x_n) = 1 \oplus f(x_1, \cdots, x_n)$

Lemma

Let $(f, g) : \{0,1\}^n \to \{0,1\}$ be bipermutive rules generating orthogonal Latin squares. Then, the Latin squares respectively induced by (f_R, g_R) and (f_C, g_C) are orthogonal as well

- Clearly, the swapped pair (g, f) generates the orthogonal Latin squares in swapped order
- Hence, the search space can be divided by 8

Pairwise Balancedness (PWB)

Definition

$f, g : \{0,1\}^n \to \{0,1\}$ are pairwise balanced (PWB) if

$$\left|(f,g)^{-1}(0,0)\right| = \left|(f,g)^{-1}(1,0)\right| =$$
$$= \left|(f,g)^{-1}(0,1)\right| = \left|(f,g)^{-1}(1,1)\right| = 2^{n-2}$$

Example:

- $f(x_1, x_2, x_3) = x_1 \oplus x_3$ (Rule 90)
- $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)

$$\Omega(f) = (0,1,0,1,1,0,1,0) \ ,$$
$$\Omega(g) = (0,1,1,0,1,0,0,1) \ .$$

Each of the pairs $(0,0),(1,0),(0,1),(1,1)$ occurs $2^{3-2} = 2$ times

Main Results

Lemma

Let $f, g : \{0,1\}^n \to \{0,1\}$ be bipermutive rules generating orthogonal Latin squares. Then, f and g are PWB

Lemma

Let $f, g : \{0,1\}^n \to \{0,1\}$ be bipermutive rules with generating functions $\varphi, \gamma : \{0,1\}^{n-2} \to \{0,1\}$. If φ and γ are PWB, then f and g are PWB as well

- **Remark**: φ, γ PWB: sufficient but not necessary condition for f, g to be PWB!
- Counterexamples already available for $n = 4$

Enumeration of PWB Generating Functions

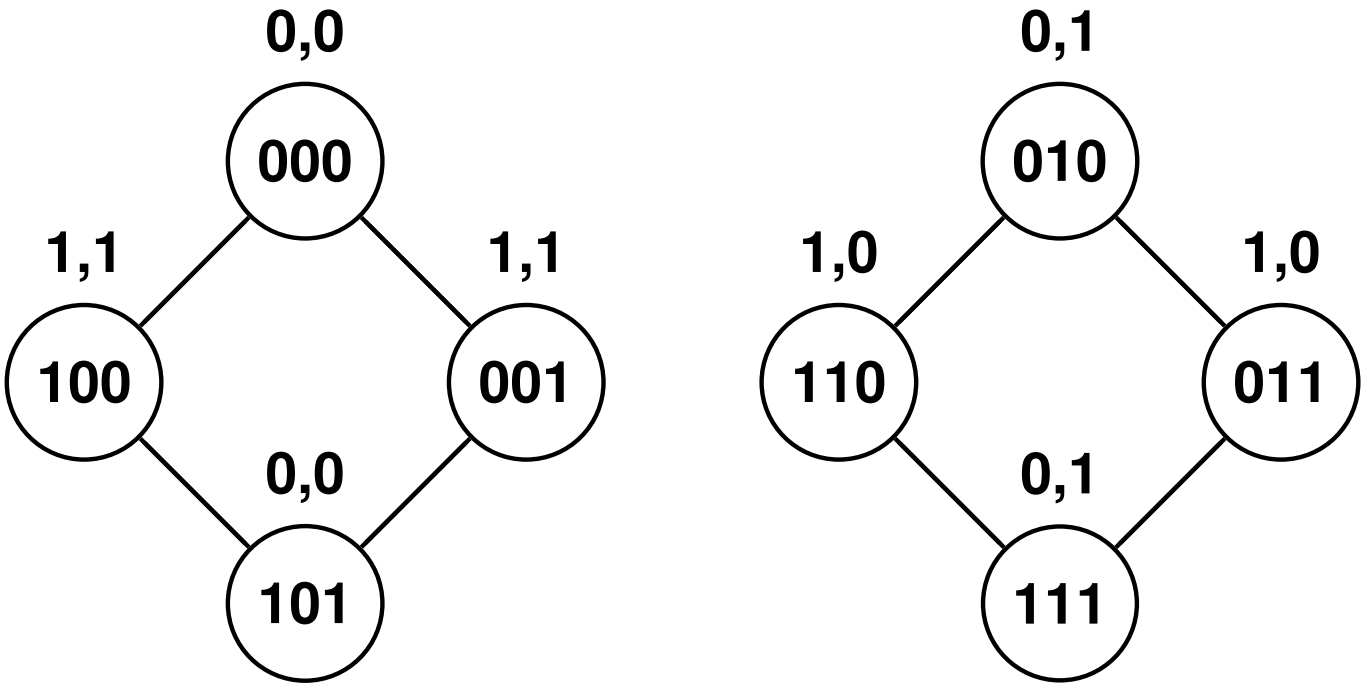
- PWB generating functions of size $n-2 \Leftrightarrow$ balanced quaternary strings of size 2^{n-2}
- Example: $n = 5$, $00 \mapsto 1, 10 \mapsto 2, 01 \mapsto 3, 11 \mapsto 4$

$$\Omega(\varphi) = (0,1,0,1,1,0,1,0)$$
$$\Omega(\gamma) = (0,1,1,0,1,0,0,1)$$
$$S_{\varphi,\gamma} = (1,4,3,2,4,1,2,3)$$

- Each number from 1 to 4 appears $2^{5-4} = 2$ times
- The number of balanced quaternary strings of length 2^{n-2} is

$$\#BalG_n = \binom{2^{n-2}}{2^{n-4}} \cdot \binom{3 \cdot 2^{n-4}}{2^{n-4}} \cdot \binom{2^{n-3}}{2^{n-4}}$$

Enumeration of PWB Bipermutive Functions



- Bipermutivity: each c.c. has either $(0,0)/(1,1)$ or $(1,0)/(0,1)$ labels, oriented north-south or east-west
- PWB: number of $(0,0)/(1,1)$ and $(1,0)/(0,1)$ c.c. are equal
- Number of PWB pairs of bipermutive rules of size n:

$$\#Bal\mathcal{B}_n = \binom{2^{n-2}}{2^{n-3}} \cdot 2^{2^{n-2}}$$

Search Spaces Sizes

n	$\#\mathcal{B}_n$	$\#Bal\mathcal{G}_n$	$\#Bal\mathcal{B}_n$
3	16	0	8
4	256	24	96
5	65536	2520	17920
6	4294967296	63006300	843448320
7	$\approx 1.84 \cdot 10^{19}$	$\approx 9.96 \cdot 10^{15}$	$\approx 2.58 \cdot 10^{18}$

- Our results do not still allow to exhaustively search beyond $n = 6$, even by focusing on $Bal\mathcal{B}_n$
- We used a 40-core machine to span $Bal\mathcal{B}_n$, which took 22 hours to complete

Classification Results

n	LS_size	#total	#linear	#nonlinear	$(Nl(f), Nl(g), \#pairs)$
3	4×4	1	1	0	–
4	8×8	9	5	4	$(4,4,4)$
5	16×16	213	21	192	$(4,4,96)$, $(8,8,96)$
6	32×32	66685	85	66600	$(4,4,512)$, $(12,12,17992)$, $(8,8,4020)$, $(16,16,28388)$, $(20,20,14384)$, $(4,12,8)$, $(8,16,160)$, $(12,20,128)$, $(16,24,88)$

Conclusions and Future Directions

Summing up:

- We considered the problem of exhaustively enumerating pairs of bipermutive CA generating orthogonal Latin squares, and classify them wrt nonlinearity
- We proved that pairwise balancedness is a necessary condition for two rules to generate OLS
- We used this condition to enumerate pairs up to size $n = 6$

Future directions:

- Find sufficient conditions for two rules to generate OLS
- Combinatorial encoding to evolve pairs of PWB bipermutive rules through Genetic Algorithms (preliminary results available in [Mariot17])

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)
- [Eloranta93] Eloranta, K.: Partially Permutive Cellular Automata. Nonlinearity 6(6), 1009–1023 (1993)
- [Mariot17] Mariot, L., Picek, S., Jakobovic, D., Leporati, A.: Evolutionary Algorithms for the Design of Orthogonal Latin Squares based on Cellular Automata. In: Proceedings of GECCO'17 (2017)
- [Mariot16] Mariot, L., Formenti, E., Leporati, A.: Construting Orthogonal Latin Squares from Linear Cellular Automata. In: Exploratory papers of AUTOMATA 2016 (2016)
- [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)
- [Tompa88] Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptology 1(2), 133–138 (1988)