Artificial Intelligence and Security Lab
Cyber Security Research Group
Delft University of Technology

Orthogonal labelings in de Bruijn graphs

Luca Mariot

L.Mariot@tudelft.nl

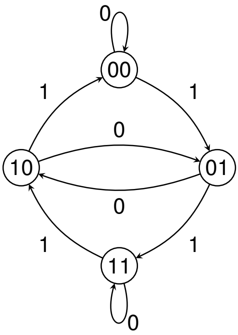
IWOCA 2020 – Open Problems Session

De Bruijn graphs and bipermutative labelings

Definition

A labeling $l : E \to S$ for the de Bruijn graph $G_{m,n} = (V, E)$ over the set S is *bipermutative* if, for any vertex $v \in V$, the labels on the ingoing and outgoing edges of v form a permutation of S.

Example: $S = \{0, 1\}$, $m = n = 2$, $l_1((v_1, v_2), (u_1, u_2)) = v_1 \oplus u_2$



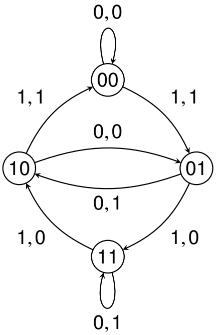
$(v_1, v_2) \to (u_1, u_2)$	l
$00 \to 00$	0
$10 \to 00$	1
$01 \to 10$	0
$11 \to 10$	1
$00 \to 01$	1
$10 \to 01$	0
$01 \to 11$	1
$11 \to 11$	0

Orthogonal labelings

Definition

Two bipermutative labelings l_1, l_2 are *orthogonal* for $G_{m,n}$ over S if, for each pair $(x,y) \in S^n \times S^n$, there is *exactly one* path in $G_{m,n}$ of length n labelled by (x,y) under the superposed labeling $l_1.l_2$.

Example: $S = \{0,1\}$, $m = n = 2$, $l_1 = v_1 \oplus u_2$, $l_2 = v_1 \oplus u_1 \oplus u_2$



$(v_1, v_2) \to (u_1, u_2)$	l_1	l_2
$00 \to 00$	0	0
$10 \to 00$	1	1
$01 \to 10$	0	1
$11 \to 10$	1	0
$00 \to 01$	1	1
$10 \to 01$	0	0
$01 \to 11$	1	0
$11 \to 11$	0	1

Open Problems

Problem (Counting)

Given $m, n \in \mathbb{N}$*, what is the number* $N(m, n)$ *of orthogonal pairs of bipermutative labelings for* $G_{m,n}$*?*

Problem (Enumeration)

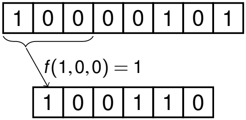
Find an algorithm that enumerates only $N(m, n)$ *of orthogonal pairs of bipermutative labelings for* $G_{m,n}$*.*

Context – Cellular Automata (CA)

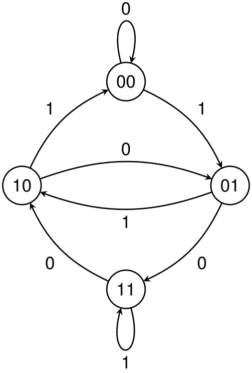
Definition

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

Example: $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ (Rule 150)



- CA input vector $\Leftrightarrow$ path on the (overlapped) *vertices*
- CA output vector $\Leftrightarrow$ path on the edges [Sutner91]



Context – 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

Context – Orthogonal Latin Squares (OLS)

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	2,4	4,1

(c) (L_1, L_2)

Sets of k *pairwise* OLS $\Leftrightarrow$ *Threshold Secret Sharing Schemes* $(2, k)$ [Shamir79]

Latin Squares through Bipermutative CA (1/2)

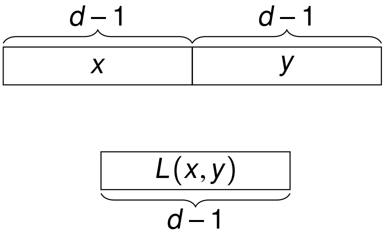
- Bipermutative CA: local rule f is defined as

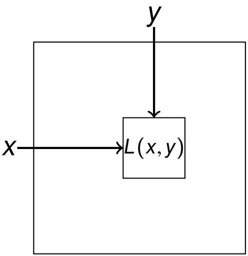
$$f(x_1, \cdots, x_d) = x_1 \oplus \varphi(x_2, \cdots, x_{d-1}) \oplus x_d$$

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

Lemma ([Eloranta93, Mariot19])

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





OLS from CA and Orthogonal Labelings

- Bipermutative CA $\Leftrightarrow$ bipermutative labeling on $G_{m,n}$
- OLS from bipermutative CA $\Leftrightarrow$ orthogonal labelings on $G_{m,n}$

What do we know so far?

- **Counting**: solved for *linear* CA – when $S = \{0, 1\}$, $N(2, n)$ corresponds to OEIS sequence A002450 [Mariot19]
- **Enumeration/Construction**: baseline algorithm [Mariot17a] to enumerate a superset of orthogonal labelings (without visiting all pairs), evolutionary algorithms to construct single pairs [Mariot17b]

References

- [Eloranta93] Eloranta, K.: Partially Permutive Cellular Automata. Nonlinearity 6(6), 1009–1023 (1993)
- [Mariot19] 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., Formenti, E., Leporati, A.: Enumerating Orthogonal Latin Squares Generated by Bipermutive Cellular Automata. In: Dennunzio, A., Formenti, E., Manzoni, L., Porreca, A. E. (eds.): AUTOMATA 2017. LNCS vol. 10248, pp. 151–164. Springer (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)
- [Shamir79] Shamir, A.: How to share a secret. Commun. ACM 22(11):612–613 (1979)
- [Sutner91] Sutner, K.: De Bruijn Graphs and Linear Cellular Automata. Complex Systems 5(1) (1991)