Orthogonal labelings in de Bruijn graphs

Luca Mariot

L.Mariot@tudelft.nl

IWOCA 2020 – Open Problems Session
Definition

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

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

\[
\begin{array}{ccc}
(v_1,v_2) \to (u_1,u_2) & l \\
00 \to 00 & 0 \\
10 \to 00 & 1 \\
01 \to 10 & 0 \\
11 \to 10 & 1 \\
00 \to 01 & 1 \\
10 \to 01 & 0 \\
01 \to 11 & 1 \\
11 \to 11 & 0 \\
\end{array}
\]
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 $l_1 \cdot l_2$.

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

<table>
<thead>
<tr>
<th>$(v_1, v_2)$ $\rightarrow$ $(u_1, u_2)$</th>
<th>$l_1$</th>
<th>$l_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 $\rightarrow$ 00</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10 $\rightarrow$ 00</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>01 $\rightarrow$ 10</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>11 $\rightarrow$ 10</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>00 $\rightarrow$ 01</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10 $\rightarrow$ 01</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>01 $\rightarrow$ 11</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>11 $\rightarrow$ 11</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
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 $G_{m,n}$.
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 $f : \{0, 1\}^d \rightarrow \{0, 1\}$ 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]
Definition

A Latin square of order $N$ is a $N \times N$ matrix $L$ such that every row and every column are permutations of $[N] = \{1, \ldots, N\}$.
Definition

Two Latin squares $L_1$ and $L_2$ of order $N$ are orthogonal if their superposition yields all the pairs $(x, y) \in [N] \times [N]$.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>4</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>4</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

(a) $L_1$  \hspace{1cm} (b) $L_2$  \hspace{1cm} (c) $(L_1, L_2)$

Sets of $k$ pairwise OLS $\Leftrightarrow$ Threshold Secret Sharing Schemes $(2, k)$ [Shamir79]
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 $2^{d-1}$
Bipermutative CA ⇔ bipermutative labeling on $G_{m,n}$
OLS from bipermutative CA ⇔ 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]


