Simplicity conditions for binary orthogonal arrays

Gábor P. Nagy
Joint work with Claude Carlet (Paris/Bergen) and Rebeka Kiss (Szeged)

COMBINATORICS 2022
Mantova, May 30 - June 3, 2022

Budapest University of Technology and Economics (Hungary)
University of Szeged (Hungary)

Outline

Correlation-immune Boolean functions and orthogonal arrays

Parameters and bounds for orthogonal arrays

Simpilicity results

Outline

Cryptographically secure pseudo-random sequences

(Pseudo-)random sequences

- good statistical properties *("balanced")*
- example: LFSR (linear recurrence)

Cryptographically secure pseudo-random sequences

- it is hard to compute x_n from $x_0, \ldots, x_{n-1}$
- non-example: LFSR

Applications

- stream ciphers: $c_i = p_i + x_i$
- masking: counter-measure against side-channel attacks

Cryptographically secure pseudo-random sequences

(Pseudo-)random sequences

- good statistical properties *("balanced")*
- example: LFSR (linear recurrence)

Cryptographically secure pseudo-random sequences

- it is hard to compute x_n from $x_0, \ldots, x_{n-1}$
- non-example: LFSR

Applications

- stream ciphers: $c_i = p_i + x_i$
- masking: counter-measure against side-channel attacks

Siegenthaler correlation attack (1985)

Combination generators

- Given $x_t^{(1)}, \ldots, x_t^{(k)}$ binary LFSRs.
- Given Boolean function $f : \mathbb{F}_2^k \to \mathbb{F}_2$.
- The keystream is the output $s_t = f(x_t^{(1)}, \ldots, x_t^{(k)})$.
- The secret key is the set of initial states $\boldsymbol{x}_0^{(1)}, \ldots, \boldsymbol{x}_0^{(k)}$.

The combiner function f must be **correlation immune of order** t:

- its output value distribution should not change
- when at most t components of its input are fixed to arbitrary values.

Correlation attack

- Otherwise the key space can be reduced significantly
- by a divide-and-conquer technique.

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Orthogonal arrays

- Introduced by C.R. Rao in 1947.

Definition: $OA(N, k, s, t)$

An $N \times k$ array A with entries from $S = \{0, \ldots, s-1\}$ is said to be an **orthogonal array with s symbols, strength t, and index λ**, if every $N \times t$ subarray of A contains each t-tuple based on S exactly $\lambda = N/s^t$ times as a row.

- An orthogonal array is *simple*, if there is no repetition among its rows.
- Permutations of the rows, columns and symbols give *isomorphic* orthogonal arrays.

An $OA(8, 4, 2, 2)$:

1	0	0	0
1	1	0	0
0	0	1	0
0	1	1	0
0	0	0	1
0	1	0	1
1	0	1	1
1	1	1	1

Hamming weight of Boolean functions

Theorem (folklore)

The following are *essentially* equivalent:

1. order t correlation immune Boolean functions in k variables,
2. simple binary orthogonal arrays with k columns and strength t.

"Essentially" means:

- the rows of the array consist of the **support** of f,
- that is,
- the vectors $\boldsymbol{x} = (x_1, \ldots, x_k) \in \mathbb{F}_2^k$ such that $f(x_1, \ldots, x_k) = 1$.
- The **Hamming weight** of f is the size of the support.

Remark. $f(x_1, x_2, x_3, x_4) = x_1 + x_3 + x_4$ gives the previous $OA(8, 4, 2, 2)$.

Hamming weight of Boolean functions

Theorem (folklore)

The following are *essentially* equivalent:

1. order t correlation immune Boolean functions in k variables,
2. simple binary orthogonal arrays with k columns and strength t.

"Essentially" means:

- the rows of the array consist of the **support** of f,
- that is,
- the vectors $\boldsymbol{x} = (x_1, \ldots, x_k) \in \mathbb{F}_2^k$ such that $f(x_1, \ldots, x_k) = 1$.
- The **Hamming weight** of f is the size of the support.

Remark. $f(x_1, x_2, x_3, x_4) = x_1 + x_3 + x_4$ gives the previous $OA(8, 4, 2, 2)$.

Outline

Parameters of orthogonal arrays

Problems

- For which parameters N, k, s, t does an orthogonal array $OA(N, k, s, t)$ exist?
- For fixed integers k, s, t, find the minimum value of N such that an $OA(N, k, s, t)$ exists.
- What about *simple* orthogonal arrays? ($\rightsquigarrow$ minimum cost masking)

Notation:
$$\begin{cases} F(k,s,t) &= \min\{N \mid \text{an } OA(N,k,s,t) \text{ exists}\}, \\ F^*(k,s,t) &= \min\{N \mid \text{a simple } OA(N,k,s,t) \text{ exists}\}. \end{cases}$$

Facts

- $F(k, s, t) \leq F^*(k, s, t)$.
- For fixed s, t, $F(k, s, t)$ is a monotone non-decreasing function in k.
- For binary orthogonal arrays, it suffices to deal with even strength.

Bounds by Rao and Delsarte

Notation:
$$\begin{cases} F(k,s,t) &= \min\{N \mid \text{an } OA(N,k,s,t) \text{ exists}\}, \\ F^*(k,s,t) &= \min\{N \mid \text{a simple } OA(N,k,s,t) \text{ exists}\}. \end{cases}$$

Rao's Bound

$$F(k,s,2u) \geq \sum_{j=0}^{u} \binom{k}{j} (s-1)^j.$$

Delsarte's LP Bound

A linear programming bound that is better than Rao's Bound. However, no explicit formula in general.

1. For $s = t = 2$, Rao's Bound means $F(k,2,2) \geq k+1$.
2. $F(k,2,2)$ is divisible by 4.
3. The **Hadamard conjecture** is equivalent with $F(k,2,2) = k+1$ for $k+1 \equiv 0 \pmod 4$.

The number $F^*(k, 2, t)$ of rows in minimal simple binary orthogonal arrays

Table by Carlet and Chen (2018)

$k \backslash t$	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2												
2	2	4											
3	2	4	8										
4	2	8	8	16									
5	2	8	16	16	32								
6	2	8	16	32	32	64							
7	2	8	16	64	64	64	128						
8	2	12	16	64	128	128	128	256					
9	2	12	24	128	128	256	256	256	512				
10	2	12	24	128	256	512	512	512	512	1 024			
11	2	12	24	**A**	**A'**	512	1 024	1 024	1 024	1 024	2 048		
12	2	16	24	**A**	**A'**	**B**	1 024	2 048	2 048	2 048	2 048	4 096	
13	2	16	32	**A**	**A'**	**C**	**B'**	4 096	4 096	4 096	4 096	4 096	8 192

The Carlet-Guilley Problem

General question

For which parameters k, s, t does

$$F(k, s, t) = F^*(k, s, t)$$

hold?

Carlet-Guilley Problem (2014)

Is $F^*(k, 2, t)$ a monotone non-decreasing function when k grows and t remains fixed?

Carlet-Chen-Wang result (2018/2019)

The Hadamard conjecture is equivalent with

$$F^*(k, 2, 3) = 8 \left\lceil \frac{k}{4} \right\rceil .$$

The Carlet-Guilley Problem

General question

For which parameters k, s, t does

$$F(k,s,t) = F^*(k,s,t)$$

hold?

Carlet-Guilley Problem (2014)

Is $F^*(k,2,t)$ a monotone non-decreasing function when k grows and t remains fixed?

Carlet-Chen-Wang result (2018/2019)

The Hadamard conjecture is equivalent with

$$F^*(k,2,3) = 8\left\lceil \frac{k}{4} \right\rceil .$$

Outline

Main theoretical result

Theorem (Carlet, Kiss, N 2022)

Let A be an $OA(N, k, s, 2u)$. Define the integer

$$M(k, s, 2u) = \sum_{j=0}^{u} \binom{k}{j} (s-1)^j.$$

(i) If $N < 2\,M(k, s, 2u)$, then A is simple.

(ii) If $N = 2\,M(k, s, 2u)$, then each row of A has multiplicity at most 2.

(iii) If $k \geq 5$, $s = 2$, $u = 2$ and $N = 2\,M(k, 2, 4)$, then either A is simple, or $k = 5$.

Corollary

If t is even and $F(k, s, t) < 2\,M(k, s, t)$, then

$$F(k, s, t) = F^*(k, s, t).$$

Main theoretical result

Theorem (Carlet, Kiss, N 2022)

Let A be an $OA(N, k, s, 2u)$. Define the integer

$$M(k, s, 2u) = \sum_{j=0}^{u} \binom{k}{j} (s-1)^j.$$

(i) If $N < 2\,M(k, s, 2u)$, then A is simple.

(ii) If $N = 2\,M(k, s, 2u)$, then each row of A has multiplicity at most 2.

(iii) If $k \geq 5$, $s = 2$, $u = 2$ and $N = 2\,M(k, 2, 4)$, then either A is simple, or $k = 5$.

Corollary

If t is even and $F(k, s, t) < 2\,M(k, s, t)$, then

$$F(k, s, t) = F^*(k, s, t).$$

Orthogonal arrays and linear codes

- Let C be a $\mathbb{F}_q$-linear code of length k and dimension h.
- Let A be the $q^h \times k$ matrix whose rows are the elements of C.
- Then A is an $OA(q^h, k, q, d^\perp - 1)$, where
- $d^\perp$ is the minimum distance of the dual code $C^\perp$.

- For all integer m, duals of certain double-error-correcting BCH codes provide arrays $OA(2^{2m+1}, 2^m + 1, 2, 5)$,
- and $OA(2^{2m}, 2^m, 2, 4)$ by shortening.
- Hence, for all k,

$$F(k, 2, 4) < 8M(k, 2, 4) \approx 4k^2.$$

Lower bounds on N: Nonlinear contructions

Kerdock-Preparata type constructions

- For any even integer $m \geq 4$, Kerdock constructed a binary, non-linear code of length 2^m, cardinality 4^m, minimum distance $2^{m-1} - 2^{(m-2)/2}$ and dual distance 6.
- This code can be interpreted as a simple $OA(4^m, 2^m, 2, 5)$.
- In the usual way, by shortening we obtain a simple $OA(2^{2m-1}, 2^m - 1, 2, 4)$.

Proposition (Carlet, Kiss, N 2022)

Let k, m be integers, $m \geq 4$ even, with

$$2^{m-1/2} \leq k \leq 2^m - 1.$$

Then $F^*(k, 2, 4) = F(k, 2, 4)$.

Corollary

The set of integers k confirming the Carlet-Guilley Problem have density at least 0.39.

Lower bounds on N: Nonlinear contructions

Kerdock-Preparata type constructions

- For any even integer $m \geq 4$, Kerdock constructed a binary, non-linear code of length 2^m, cardinality 4^m, minimum distance $2^{m-1} - 2^{(m-2)/2}$ and dual distance 6.
- This code can be interpreted as a simple $OA(4^m, 2^m, 2, 5)$.
- In the usual way, by shortening we obtain a simple $OA(2^{2m-1}, 2^m - 1, 2, 4)$.

Proposition (Carlet, Kiss, N 2022)

Let k, m be integers, $m \geq 4$ even, with

$$2^{m-1/2} \leq k \leq 2^m - 1.$$

Then $F^*(k, 2, 4) = F(k, 2, 4)$.

Corollary

The set of integers k confirming the Carlet-Guilley Problem have density at least 0.39.

Minimal simple binary orthogonal arrays

$k \backslash t$	1	2	3	4	5	6	7	8	9	10	11	12	13
10	2	12	24	128	256	512	512	512	512	1 024			
11	2	12	24	**A**	**A'**	512	1 024	1 024	1 024	1 024	2 048		
12	2	16	24	**A**	**A'**	**B**	1 024	2 048	2 048	2 048	2 048	4 096	
13	2	16	32	**A**	**A'**	**C**	**B'**	4 096	4 096	4 096	4 096	4 096	8 192

$A = 128$ **and** $A' = 256$ Constructions from the Nordstrom-Robinson (self-dual Kerdock) code of length 16. (Continues for two more lines.) Computer result for $F^*(10, 2, 4) = 128$.

$B = 768$ **and** $B' = 1\,536$ The values equal to Delsarte's LP Bound. The existence and uniqueness of an $OA(1\,536, 13, 2, 7)$ has been shown recently by A. Krotov. Independent construction by computer.

$C = 1\,024$ The value equals to Delsarte's LP Bound. The OA is the dual of a binary linear $[13, 3, 7]$-code. (Wang 2019)

Grazie per l'attenzione!

Acknowledgement

The presented work was carried out within the project **"Security Enhancing Technologies for the Internet of Things"** 2018-1.2.1-NKP-2018-00004, supported by the National Research, Development and Innovation Fund of Hungary.