Finite Field Constructions of Combinatorial Arrays

Lucia Moura
School of Electrical Engineering and Computer Science
University of Ottawa
lucia@eecs.uottawa.ca

XXI Coloquio Latinoamericano de Álgebra, XXI CLA,
Buenos Aires, July 2016

A survey on the general subject

Des. Codes Cryptogr. (2016) 78:197–219
DOI 10.1007/s10623-015-0152-9

CrossMark

Finite field constructions of combinatorial arrays

Lucia Moura[1] · Gary L. Mullen[2] · Daniel Panario[3]

Accepted: 12 October 2015 / Published online: 30 November 2015

Abstract We survey a number of topics and constructions of combinatorial arrays based on finite fields. These combinatorial objects include orthogonal arrays, covering arrays, ordered orthogonal arrays, permutation arrays, frequency permutation arrays, hypercubes and Costas arrays.

Orthogonal arrays

$\mathrm{OA}(N = 3^2,\ k = 4,\ s = 3, t = 2)$ where $\lambda = 1$

0	0	0	0
0	1	2	2
1	2	2	0
2	2	0	2
2	0	2	1
0	2	1	1
2	1	1	0
1	1	0	1
1	0	1	2

Definition

An *orthogonal array* of size N, with k factors, s symbols, strength t and index $\lambda = \frac{N}{s^t}$, denoted by $\mathrm{OA}(N, k, s, t)$, is an $N \times k$ array with $s \geq 2$ symbols such that in every $N \times t$ subarray, every t-tuple of symbols appears the same number λ of times as a row.

OAs with $\lambda = 1$ & $t = 2$ and MOLs

$L_1 =$

0	2	1
1	0	2
2	1	0

$L_2 =$

0	2	1
2	1	0
1	0	2

(0,0)	(2,2)	(1,1)
(1,2)	(0,1)	(2,0)
(2,1)	(1,0)	(0,2)

Definition

A *Latin square of order n* is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs once in each row and each column. Two Latin squares L_1 and L_2 of the same order n are *orthogonal* if, when superimposed, each of the possible n^2 ordered pairs occurs exactly once. A set $\{L_1, L_2, \ldots, L_m\}$ of $m \geq 2$ Latin squares is *mutually orthogonal* (a set of MOLS) if the squares in the set are pairwise orthogonal.

OAs with $\lambda = 1$ & $t = 2$ and MOLs

$L_1 =$

0	2	1
1	0	2
2	1	0

$L_2 =$

0	2	1
2	1	0
1	0	2

OA=

0	0	0	0
0	1	2	2
0	2	1	1
1	0	1	2
1	1	0	1
1	2	2	0
2	0	2	1
2	1	1	0
2	2	0	2

Theorem ($\lambda = 1, t = 2$: OAs equivalent to MOLs)

There exist a set of m MOLS or order s if and only if there exists an $OA(s^2, m+2, s, 2)$. Also, for them to exist $m \leq s-1$.

For $s = q$ a prime power we reach $m = s - 1$:

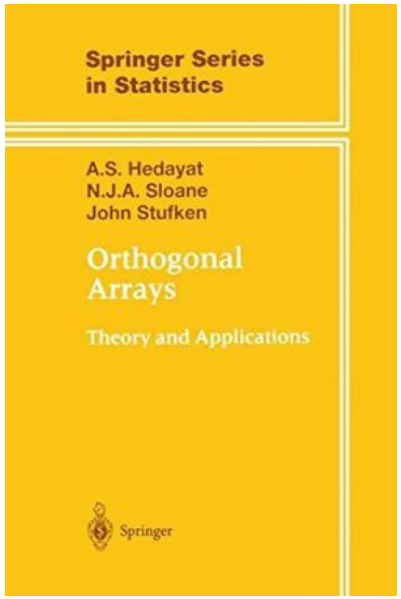
$q - 1$ MOLS of order q; $\quad$ $\mathrm{OA}(q^2, q+1, q, 2)$.

Finite field constructions of OAs

For $q \geq 2$ a prime power the following OAs exist:

1. Bush (1952): $OA(q^t, q+1, q, t)$, where $q \geq t-1 \geq 0$.
2. Bush (1952): $OA(2^{3m}, 2^m+2, 2^m, 3)$, where $m \geq 1$.
3. Addleman and Kempthorne (1961): $OA(2q^n, 2(q^n-1)/(q-1)-1, q, 2)$, where $q > 2$ is an odd prime power and $n \geq 2$.
4. Rao (1947, 1949) and Hamming (1950): $OA(q^n, (q^n-1)/(q-1), q, 2)$, where $n \geq 2$.

reference book on OAs:



LFSR sequences over finite fields

$\mathbb{F}_q$ finite field with q elements; $I = (b_0, \ldots, b_{m-1}) \in \mathbb{F}_{q^m}$;
$f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 \in \mathbb{F}_{q^m}[x]$.

Definition (LFSR)

The sequence $S(f, I) = (a_0, a_1, \ldots)$ defined as

$$a_i = \begin{cases} b_i & \text{if } 0 \leq i < m, \\ -c_{m-1}a_{i-1} - c_{m-2}a_{i-2} - \cdots - c_0 a_{i-m} & \text{if } i \geq m, \end{cases} \tag{1}$$

is a **linear feedback shift-register (LFSR) sequence over** $\mathbb{F}_q$ with **characteristic polynomial** f and initial values $b_0, \ldots, b_{m-1}$.

- The sequence is periodic; its least period P divides $q^m - 1$.

M-SEQUENCES

M-SEQUENCE

- Suppose f is irreducible, $\alpha \in \mathbb{F}_{q^m}$ a root that generates the multiplicative group $\mathbb{F}_{q^m} \setminus \{0\}$. Then α is a **primitive element of** $\mathbb{F}_{q^m}$, and f is a **primitive polynomial**.
- When f is primitive the LFSR has maximum period $P = q^m - 1$. This is called an **m-sequence**.

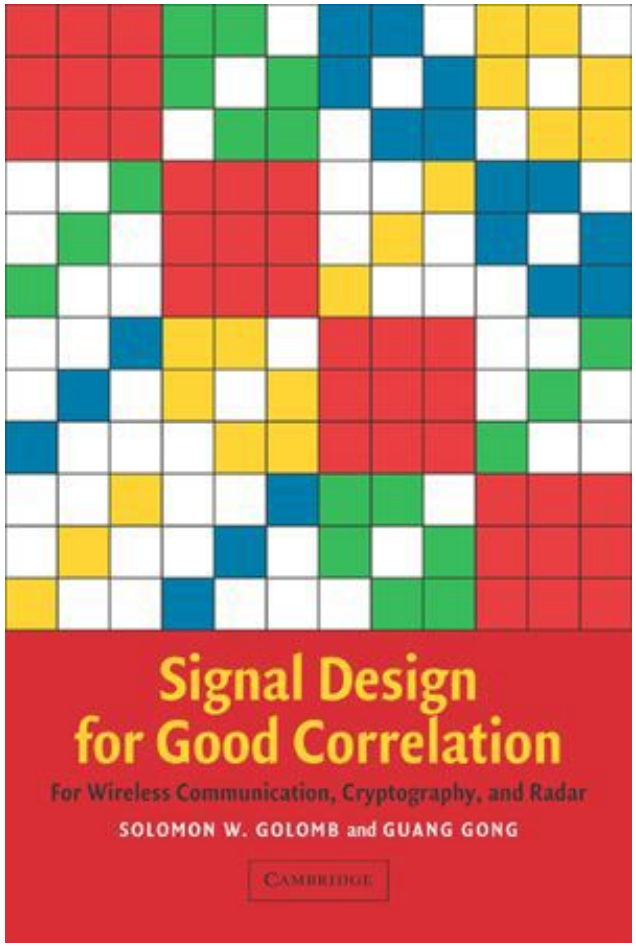
LFSR with $f(x) = x^3 + 0x^2 + 2x + 1$ of degree $m = 3$ over $\mathbb{F}_q$, $q = 3$ is defined by:

- set arbitrary initial values (not all-zero): $a_0 = 0, a_1 = 1, a_2 = 2$
- use f to define: $a_n = 0 \times a_{n-1} - 2 \times a_{n-2} - 1 \times a_{n-3}, \quad n \geq 3$

Because f is **primitive**, the sequence has **maximum period** $q^m - 1 = q^3 - 1 = 26$ (it is an m-sequence).

$$01211201110020212210222001\,01211201110020212210222001\cdots$$

Properties of m-sequences



Properties of m-sequences

- each nonzero m-tuple of $\mathbb{F}_q$ appears once per period, starting at positions $i = 0, \ldots, q^m - 2$

  $01211201110020212210222001 01211201110020212210222001 \cdots$

- the patterns of zeroes is the same at adjacent windows of size $d = q^m - 1/(q-1) = q^{m-1} + \ldots + q + 1$;

  $0121120111002\ 021221022200 1\ 01211201110020212210222001 \cdots$

  0121120111002
  0212210222001

- 2-tuple balance property implies for $1 \leq \tau \leq d$: the pairs $(a_i, a_{i+\tau}) = (a, b)$ occurs in a period:
  - q^{m-2} times, if $(a, b) \neq (0, 0)$
  - $q^{m-2} - 1$ times, if $(a, b) = (0, 0)$

Subinterval array $A^k(f)$

Let f be a degree-m **primitive polynomial** over $\mathbb{F}_q$ with root $\alpha \in \mathbb{F}_{q^m}$. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ is a basis for $\mathbb{F}_{q^m}$.
Consider the **LFSR seq.** with initial values $T = (a_0, \ldots, a_{m-1})$ not all zero and characteristic polynomial f.
Let k be a positive integer. Consider the following $q^m \times k$ array:

$$A^k(f, T) \sim A^k(f) = \begin{bmatrix} 0 & 0 & \ldots & 0 \\ a_0 & a_1 & \ldots & a_{k-1} \\ a_1 & a_2 & \ldots & a_k \\ \vdots & \vdots & & \vdots \\ a_{q^m-2} & a_{q^t-1} & \ldots & a_{q^m-2+k-1} \end{bmatrix}$$

Every m consecutive columns have their q^m tuples covered.
This is an OA$(q^m, k, q, 2)$ with $\lambda = q^{m-2}$, for $k \leq (q^m - 1)/(q - 1)$.

Subinterval array $A^k(f)$

0	0000000000000000000000000000000000000000000000000000 · · ·
1	0121120111002021221022200101211201110020212210222001 · · ·
2	1211201110020212210222001012112011100202122102220010 · · ·
3	2112011100202122102220010121120111002021221022200101 · · ·
4	1120111002021221022200101211201110020212210222001012 · · ·
5	1201110020212210222001012112011100202122102220010121 · · ·
6	2011100202122102220010121120111002021221022200101211 · · ·
7	0111002021221022200101211201110020212210222001012112 · · ·
8	1110020212210222001012112011100202122102220010121120 · · ·
9	1100202122102220010121120111002021221022200101211201 · · ·
10	1002021221022200101211201110020212210222001012112011 · · ·
11	0020212210222001012112011100202122102220010121120111 · · ·
12	0202122102220010121120111002021221022200101211201110 · · ·
13	2021221022200101211201110020212210222001012112011100 · · ·
14	0212210222001012112011100202122102220010121120111002 · · ·
15	2122102220010121120111002021221022200101211201110020 · · ·
16	1221022200101211201110020212210222001012112011100202 · · ·
17	2210222001012112011100202122102220010121120111002021 · · ·
18	2102220010121120111002021221022200101211201110020212 · · ·
19	1022200101211201110020212210222001012112011100202122 · · ·
20	0222001012112011100202122102220010121120111002021221 · · ·
21	2220010121120111002021221022200101211201110020212210 · · ·
22	2200101211201110020212210222001012112011100202122102 · · ·
23	2001012112011100202122102220010121120111002021221022 · · ·
24	0010121120111002021221022200101211201110020212210222 · · ·
25	0101211201110020212210222001012112011100202122102220 · · ·
26	1012112011100202122102220010121120111002021221022200 · · ·
27	0121120111002021221022200101211201110020212210222001 · · ·

Subinterval array $A^k(f), k = (q^m - 1)/(q - 1)$

0	0000000000000	0000000000000000000000000000000000000000 · · ·
1	0121120111002	021221022200101211201110020212210222001 · · ·
2	1211201110020	212210222001012112011100202122102220010 · · ·
3	2112011100202	122102220010121120111002021221022200101 · · ·
4	1120111002021	221022200101211201110020212210222001012 · · ·
5	1201110020212	210222001012112011100202122102220010121 · · ·
6	2011100202122	102220010121120111002021221022200101211 · · ·
7	0111002021221	022200101211201110020212210222001012112 · · ·
8	1110020212210	222001012112011100202122102220010121120 · · ·
9	1100202122102	220010121120111002021221022200101211201 · · ·
10	1002021221022	200101211201110020212210222001012112011 · · ·
11	0020212210222	001012112011100202122102220010121120111 · · ·
12	0202122102220	010121120111002021221022200101211201110 · · ·
13	2021221022200	101211201110020212210222001012112011100 · · ·
14	0212210222001	012112011100202122102220010121120111002 · · ·
15	2122102220010	121120111002021221022200101211201110020 · · ·
16	1221022200101	211201110020212210222001012112011100202 · · ·
17	2210222001012	112011100202122102220010121120111002021 · · ·
18	2102220010121	120111002021221022200101211201110020212 · · ·
19	1022200101211	201110020212210222001012112011100202122 · · ·
20	0222001012112	011100202122102220010121120111002021221 · · ·
21	2220010121120	111002021221022200101211201110020212210 · · ·
22	2200101211201	110020212210222001012112011100202122102 · · ·
23	2001012112011	100202122102220010121120111002021221022 · · ·
24	0010121120111	002021221022200101211201110020212210222 · · ·
25	0101211201110	020212210222001012112011100202122102220 · · ·
26	1012112011100	202122102220010121120111002021221022200 · · ·
27	0121120111002	021221022200101211201110020212210222001 · · ·

Subinterval array $A^k(f), k = (q^m - 1)/(q - 1)$

0	0000000000000
1	0121120111002
2	1211201110020
3	2112011100202
4	1120111002021
5	1201110020212
6	2011100202122
7	0111002021221
8	1110020212210
9	1100202122102
10	1002021221022
11	0020212210222
12	0202122102220
13	2021221022200
14	0212210222001
15	2122102220010
16	1221022200101
17	2210222001012
18	2102220010121
19	1022200101211
20	0222001012112
21	2220010121120
22	2200101211201
23	2001012112011
24	0010121120111
25	0101211201110
26	1012112011100

$= \mathrm{OA}(q^m, (q^m - 1)/(q - 1), q, 2) = \mathrm{OA}(27, 13, 3, 2); \quad \lambda = q^{m-2} = 3$

Subinterval array $A^k(f), k = (q^m - 1)/(q - 1)$

0	0000000000000
1	0121120111002
2	1211201110020
3	2112011100202
4	1120111002021
5	1201110020212
6	2011100202122
7	0111002021221
8	1110020212210
9	1100202122102
10	1002021221022
11	0020212210222
12	0202122102220
13	2021221022200
14	0212210222001
15	2122102220010
16	1221022200101
17	2210222001012
18	2102220010121
19	1022200101211
20	0222001012112
21	2220010121120
22	2200101211201
23	2001012112011
24	0010121120111
25	0101211201110
26	1012112011100
	0123456789abc

$\{1, 7, b, c\} + i \pmod{13} = \mathrm{BIBD}(13, 4, 1) = \mathrm{PG}(2, 3) = \mathrm{PG}(m - 1, q)$

OAs of strength 2 close to having strength 3

Theorem (Munemasa (1998))

Let $f(x) = 1 + x^l + x^m$ be a primitive trinomial of degree m over $\mathbb{F}_2$, let k be a positive integer where $m < k \leq 2m+1$ and let $A^k(f)$ be the subinterval array of f of length k. Define

$$T_k = \begin{cases} \{\{i, i+l, i+m\} : 1 \leq i \leq k-m\}, \text{if } k \leq 2m, \\ \{\{i, i+l, i+m\} : 1 \leq i \leq k-m\} \cup \\ \quad \{\{1, 2l+1, 2m+1\}\}, \text{ if } k = 2m+1. \end{cases}$$

Then $A^k(f)$ is an orthogonal array of strength 2. Moreover, a 3-set T of columns of $A^k(f)$ is balanced-covered (i.e. each triple in $\mathbb{F}_2$ appears $\lambda_3 = 2^{m-3}$ times in T) if and only if $T \notin T_k$; when $T \in T_k$, the coverage of tuple (b_1, b_2, b_3) for column indices in T is precisely $\delta_{b_1+b_2+b_3,0} 2^{m-2}$, where $\delta_{i,0} = 1$ if $i = 0$ and $\delta_{i,0} = 0$, otherwise.

OAs of strength 2 close to having strength 3

column indexes: 0123456	uncovered triple of columns
0000000	
0100111	$\{0,2,3\}$
1001110	$\{6,1,2\}$
0011101	$\{5,0,1\}$
0111010	$\{4,6,0\}$
1110100	$\{3,5,6\}$
1101001	$\{2,4,5\}$
1010011	$\{1,3,4\}$

This is an OA$(8,7,2,2)$. This is "almost" an OA$(8,7,2,3)$: 28/35 triples of columns ok; 7/35 of them uncovered.
In general: OA$(2^m, 2m+1, 2, 2)$ almost OA$(2^m, 2m+1, 2, 3)$

Extensions of the work in Munemasa (1998)

- M. Dewar, L. Moura, D. Panario, B. Stevens, Q. Wang (2007) produce complete OA$(2^m, 2m, 2, 3)$ using primitive pentanomial sover $\mathbb{F}_2$ (except for a list of 22 exceptional pentanomials).

- D. Panario, O. Sosnovski, B. Stevens, Q. Wang (2012) remove the requirement that f be primitive; they also produce OAs over $\mathbb{F}_3$.

Covering arrays

Strength $t = 3$; $s = 2$ symbols; $k = 10$ columns; $N = 13$ rows

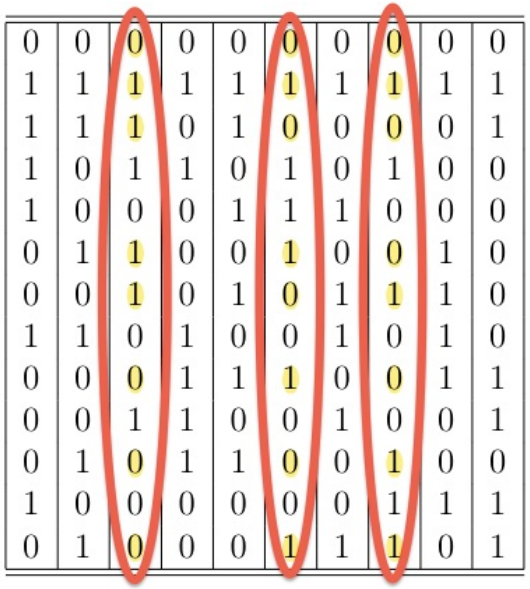
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
1	1	1	0	1	0	0	0	0	1
1	0	1	1	0	1	0	1	0	0
1	0	0	0	1	1	1	0	0	0
0	1	1	0	0	1	0	0	1	0
0	0	1	0	1	0	1	1	1	0
1	1	0	1	0	0	1	0	1	0
0	0	0	1	1	1	0	0	1	1
0	0	1	1	0	0	1	0	0	1
0	1	0	1	1	0	0	1	0	0
1	0	0	0	0	0	0	1	1	1
0	1	0	0	0	1	1	1	0	1

Definition: Covering Array

A *covering array* of strength t, k factors, v symbols and size N, denoted by $CA(N; t, k, s)$, is an $N \times k$ array with symbols from $\{0, 1, \ldots, s-1\}$ such that in every $t \times N$ subarray, every t-tuple of $\{0, 1, \ldots, s-1\}^t$ is covered at least once.

Covering arrays

Strength $t = 3$; $s = 2$ symbols; $k = 10$ columns; $N = 13$ rows



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

Definition: Covering Array

A *covering array* of strength t, k factors, v symbols and size N, denoted by $CA(N; t, k, s)$, is an $N \times k$ array with symbols from $\{0, 1, \ldots, s-1\}$ such that in every $t \times N$ subarray, every t-tuple of $\{0, 1, \ldots, s-1\}^t$ is covered at least once.

Covering arrays generalize OAs

$CAN(t, k, s) = \min\{N : \text{a } CA(N; t, k, s) \text{ exists}\}$

An obvious lower bound: $CAN(t, k, s) \geq s^t$

An orthogonal array with index $\lambda = 1$: every every t-tuple of $\{0, 1, \ldots, s-1\}^t$ appears exactly once in any t columns.

So, an $OA(s^t, t, k, s)$ is a $CA(s^t; t, k, s)$ that meets this lower bound.

Strength-3 CAs using subinterval arrays

Take f a primitive polynomial of degree 3 over $\mathbb{F}_q$. This gives an $\mathrm{OA}(q^3, q^2+q+1, 3, 2)$ that is almost $\mathrm{OA}(q^3, q^2+q+1, 3, 3)$.

0	0000000000000
1	0121120111002
2	1211201110020
3	2112011100202
4	1120111002021
5	1201110020212
6	2011100202122
7	0111002021221
8	1110020212210
9	1100202122102
10	1002021221022
11	0020212210222
12	0202122102220
13	2021221022200
14	0212210222001
15	2122102220010
16	1221022200101
17	2210222001012
18	2102220010121
19	1022200101211
20	0222001012112
21	2220010121120
22	2200101211201
23	2001012112011
24	0010121120111
25	0101211201110
26	1012112011100

Theorem (S. Raaphorst, L. Moura, B. Stevens (2014))
a triple of columns $\{x, y, z\}$ is uncovered $\iff$
columns $\{x, y, z\}$ are linearly dependent $\iff$
there exist a row (in addition to row 0) with 0 in columns x, y and z $\iff$
$\{x, y, z\}$ is a triple inside a $\mathrm{BIBD}(q^2+q+1, q+1, 1) = \mathrm{PG}(2, q)$

Strength-3 CAs using subinterval arrays

Let $k = (q^3 - 1)/(q - 1)$.

Use $A^k(f)$. Append below $A^k(f(1/x))$.

0	0000000000000
1	0121120111002
2	1211201110020
3	2112011100202
4	1120111002021
5	1201110020212
6	2011100202122
7	0111002021221
8	1110020212210
9	1100202122102
10	1002021221022
11	0020212210222
12	0202122102220
13	2021221022200
14	0212210222001
15	2122102220010
16	1221022200101
17	2210222001012
18	2102220010121
19	1022200101211
20	0222001012112
21	2220010121120
22	2200101211201
23	2001012112011
24	0010121120111
25	0101211201110
26	1012112011100

	~~0000000000000~~
27	2001110211210
28	0200111021121
29	2020011102112
30	1202001110211
31	2120200111021
32	2212020011102
33	1221202001110
34	0122120200111
35	2012212020011
36	2201221202001
37	2220122120200
38	0222012212020
39	0022201221202
40	1002220122120
41	0100222012212
42	1010022201221
43	2101002220122
44	1210100222012
45	1121010022201
46	2112101002220
47	0211210100222
48	1021121010022
49	1102112101002
50	1110211210100
51	0111021121010
52	0011102112101

$$\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$$

Strength-3 CAs using subinterval arrays

Theorem (Raaphorst, Moura, Stevens (2014))

Let q be a prime power.
Then, there exists a $CA(N = 2q^3 - 1; t = 3, k = q^2 + q + 1; s = q)$

This improves upper bound for 512 parameter sets in Colbourn's covering array tables.

Improved CA bounds: $q \leq 25$, prime powers

q	k	new N	old N
2	7	15	12
3	13	53	50
4	21	**127**	152
5	31	**249**	365
7	57	**685**	1015
8	73	**1023**	1492
9	91	**1457**	2169
11	133	**2661**	3971
13	183	**4393**	6565
16	273	**8191**	12226
17	307	**9825**	15874
19	381	**13717**	24158
23	553	**24333**	38590
25	651	**31249**	49346

$\leftarrow$ improved upper bounds in Colbourn's CAs table for all $q \neq 2, 3$, $q \leq 25$

Improved bounds for $v \leq 25$, non prime powers

Non-prime-powers: "drop the symbols+fusion" for the next prime power.

$s \leq q$	k	new N	old N
6	57	683	624
10	133	**2659**	3794
12	183	**4391**	6350
14	273	**8187**	11996
15	273	**8189**	11998
18	381	**13715**	20191
20	553	**24327**	35941
21	553	**24329**	35943
22	553	**24331**	35945
24	651	**31247**	46196

$\leftarrow$ improved upper bounds in Colbourn's CAs table for all $v \neq 2, 3, 6$, $v \leq 25$

`www.public.asu.edu/~ccolbou/src/tabby/catable.html`

Strength-4 CAs using subinterval arrays

G. Tzanakis, L. Moura, D. Panario and B. Stevens (2016)

Construction using 2 or 3 stacked interval arrays + backtracking.

1. Stack interval arrays $A^k(f_1)$, $A^k(f_2)$ (sometimes $A^k(f_3)$) with f_i primitive of degree $m = 4$.
2. Backtracking: find maximum number of columns that together form a CA of strength 4.
   Algorithm uses binary necklaces to reject isomorphic branches in the search tree.

Strength-4 CAs using subinterval arrays

q	l	$CA(N; 4, k, q)$	PrevN	q	l	$CA(N; 4, k, q)$	PrevN
2	2	$CA(31; 4, 6, 2)$*	21	9	2	$CA(13121; 4, 18, 9)$	13113
3	2	$CA(161; 4, 10, 3)$*	159	9	3	$CA(\mathbf{19681}; 4, 42, 9)$	**30537**
3	3	$CA(241; 4, 12, 3)$*	189	9	4	$CA(\mathbf{26241}; 4, 50, 9)$	**30537**
3	4	$CA(321; 4, 12, 3)$*	189	9	5	$CA(\mathbf{32801}; 4, 82, 9)$	**33129**
4	2	$CA(\mathbf{511}; 4, 17, 4)$*	**760**	11	2	$CA(29281; 4, 21, 11)$	29271
4	3	$CA(766; 4, 20, 4)$	760	11	3	$CA(\mathbf{43921}; 4, 37, 11)$	**69091**
4	4	$CA(1021; 4, 20, 4)$	760	11	4	$CA(\mathbf{58561}; 4, 77, 11)$	**69091**
5	2	$CA(\mathbf{1249}; 4, 16, 5)$	**1865**	11	5	$CA(\mathbf{73201}; 4, 125, 11)$	**73931**
5	3	$CA(\mathbf{1873}; 4, 25, 5)$	**2845**	13	2	$CA(57121; 4, 24, 13)$	57109
5	4	$CA(2497; 4, 23, 5)$	1865	13	3	$CA(\mathbf{85681}; 4, 45, 13)$	**136045**
7	2	$CA(4801; 4, 15, 7)$	4795	13	4	$CA(\mathbf{114241}; 4, 98, 13)$	**136045**
7	3	$CA(7201; 4, 26, 7)$	7189	13	5	$CA(\mathbf{142801}; 4, 170, 13)$	**146185**
7	4	$CA(9601; 4, 43, 7)$	9583	16	2	$CA(\mathbf{131071}; 4, 28, 16)$	**188401**
7	5	$CA(12001; 4, 47, 7)$	9583	16	3	$CA(\mathbf{196606}; 4, 55, 16)$	**315136**
8	2	$CA(8191; 4, 17, 8)$	8184	16	4	$CA(\mathbf{262141}; 4, 129, 16)$	**315136**
8	3	$CA(12286; 4, 30, 8)$	12272	17	2	$CA(\mathbf{167041}; 4, 29, 17)$	**240721**
8	4	$CA(\mathbf{16381}; 4, 48, 8)$	**18880**	17	3	$CA(\mathbf{250561}; 4, 61, 17)$	**402577**
8	5	$CA(20476; 4, 65, 8)$	19776	17	4	$CA(\mathbf{334081}; 4, 141, 17)$	**402577**
8	6	$CA(24571; 4, 67, 8)$	19776	19	2	$CA(\mathbf{260641}; 4, 30, 19)$	**377227**
				23	2	$CA(\mathbf{781249}; 4, 35, 23)$	**815167**

Ordered Orthogonal Arrays

Definition

An *ordered orthogonal array* $\mathrm{OOA}(N, m, n, s, t)$ is a $N \times mn$ array with the columns indexed by ordered pairs (i, j), $1 \leq i \leq m, 1 \leq j \leq n$, with s symbols, strength t and index $\lambda = N/s^t$, if every left-justified t-set T of columns has the OA property: in the $N \times t$ subarray indexed by the columns in T each t-tuple of symbols appears the same number λ of times as rows.

transposed OOA:

0:	01211201110020212210222001 0				
1:	12112011100202122102220010 0				•
2:	21120111002021221022200101 0		•		•
5:	20111002021221022200101211 0			•	
4:	12011100202122102220010121 0			•	
3:	11201110020212210222001012 0		•	•	
7:	11100202122102220010121120 0				
10:	00202122102220010121120111 0				
0:	01211201110020212210222001 0	•			•
2:	21120111002021221022200101 0				
11:	02021221022200101211201110 0	•			
7:	11100202122102220010121120 0	•	•		

Ordered Orthogonal Arrays

Theorem (Castoldi, Moura, Panario, Stevens (2015))

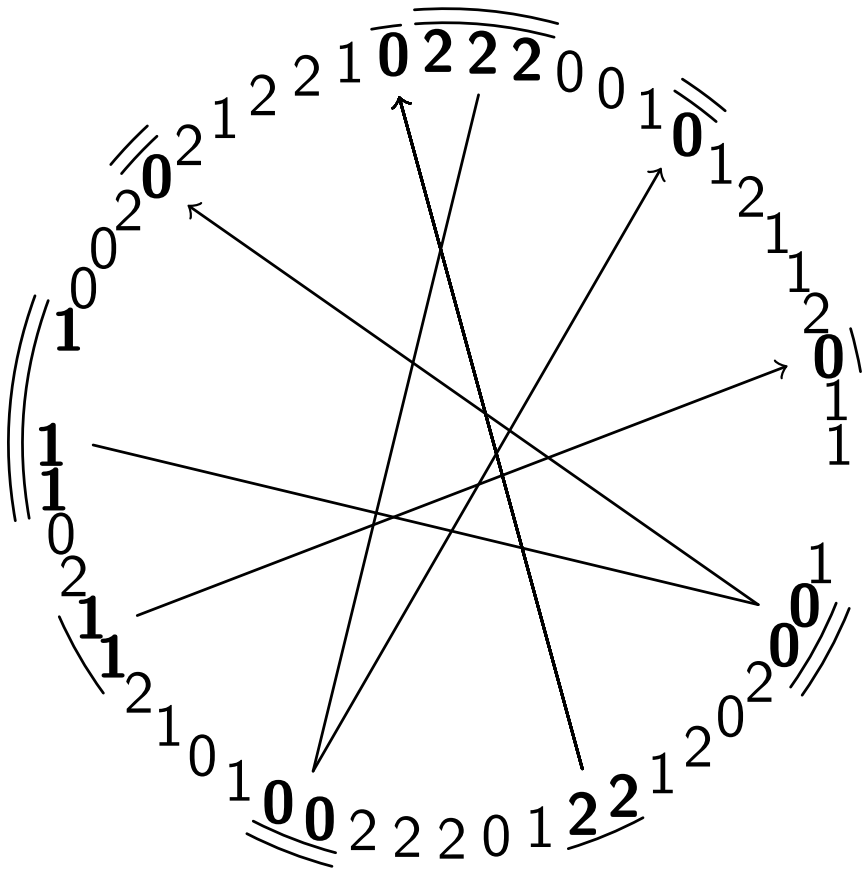
Let f be a primitive polynomial over a finite field $\mathbb{F}_q$ of degree $t \geq 3$ and $\alpha \in \mathbb{F}_{q^t}$ be a root of f. For each $\beta \in \mathbb{F}_q^\times$, let $k_\beta \in \mathbb{Z}_{q^t-1}$ such that $\alpha^{k_\beta}(\alpha - \beta) = 1$. Consider matrix $A^k(f)$ with $k = (q^t - 1)/(q - 1)$. Take blocks of columns $(0, \ldots, t-1)$, $(2t-1, \ldots, t)$, and $(t + tk_\beta, t + (t-1)k_\beta, \ldots, t + k_\beta)$ for each $\beta \in \mathbb{F}_q^\times$. Then, the array A formed by the columns of $A^k(f)$ labeled by these blocks is an $OOA(t, q+1, t, q)$.

OOA(27,3,4,3,3):

0:	012112011100202122102220010 0				•
1:	121120111002021221022200101 0		•		•
2:	211201110020212210222001012 0				
5:	201110020212210222001012110			•	
4:	120111002021221022200101210			•	
3:	112011100202122102220010121 0		•	•	
7:	111002021221022200101211200				
10:	002021221022200101211201110				
0:	012112011100202122102220010 0	•			•
2:	211201110020212210222001012 0				
11:	020212210222001012112011100	•			
7:	111002021221022200101211200	•	•		

OOA construction: studying runs of zeroes

Consider the primitive polynomial $f(x) = 1 + 2x^2 + x^3$ over $\mathbb{F}_3$.
Sequence: 10020212210222001012112011.
Then $k_1 = 23$ satisfies $\alpha^{23}(\alpha - 1) = 1$, where α is a root of f.



Conclusion

- Subinterval arrays $A = A^{(q^m-1)/(q-1)}(f)$ of m-sequences give "partial" orthogonal arrays of strength m.
- Coverage is missing in columns that correspond to points of $\mathrm{PG}(m-1,q)$ incident to $(m-2)-$ *dimensional* subspaces of $\mathrm{PG}(m-1,q)$.
- For $m=2$ the array A is an $\mathrm{OA}(q^2, q+1, q, 2)$ (like in classical OA constructions for strength 2).
- For $m=3$, we stack two such arrays to get $\mathrm{CA}(2q^3-1; t=3, q^2+q+1, 1)$. These are the best known for $t=3$, k=q^2+q+1, where $q \neq 2,3$.
- For $m=4$ we stack two or three of them, and select columns to obtain new CAs of strength 4.
- For all $m=t$, we build $\mathrm{OOA}(t, q+1, t, q)$ by minding the locations of runs of zeroes in the m-sequence.