A new construction of strength-3 covering arrays using linear feedback shift register (LFSR) sequences

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

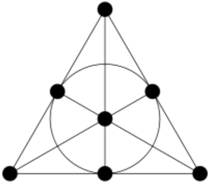
joint work with **Sebastian Raaphorst** and **Brett Stevens**

Special Days on combinatorial constructions using finite fields,
RICAM, Linz, December 2013

What are combinatorial designs?

Combinatorial designs are combinatorial objects such as arrays or set systems with some type of **“balance property”**.

- The construction in this talk relates many interesting combinatorial designs:
  block designs, Steiner triple systems, projective planes, orthogonal arrays, covering arrays.
- The construction uses LFSR sequences in finite fields to build **partial orthogonal arrays** that we transform into (complete) **covering arrays**.

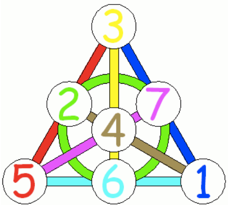


Steiner triple systems

Definition

A Steiner triple system of order n, $STS(n)$, is a set of 3-subsets (triples) of $X = \{1, 2, \ldots, n\}$ such that each unordered pair of elements of X appears in exactly 1 triple.

$STS(7)$:



$\{1,2,4\}, \{1,3,7\}, \{1,5,6\}, \{2,3,5\}, \{2,6,7\}, \{3,4,6\}, \{4,5,7\}$

Balanced incomplete block designs

A *balanced in complete block design*,

$\text{BIBD}(n, k, \lambda)$, λ k

Definition

A ~~Steiner triple system of order n~~, $STS(n)$, is a set of 3-subsets (~~triples~~) of $X = \{1, 2, \ldots, n\}$ such that each unordered pair of elements of X appears in exactly 1 triple.

~~$STS(7)$~~:

$\{1,2,4\}, \{1,3,7\}, \{1,5,6\}, \{2,3,5\}, \{2,6,7\}, \{3,4,6\}, \{4,5,7\}$

$$BIBD(n, 3, 1) = STS(n)$$

Ex: BIBD(13,4,1) =BIBD$(n^2+n+1, n+1, 1)$ for $n=3$

$\{\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{9}\}$ ← difference set
$\{1,2,4,10\}$
$\{2,3,5,11\}$
$\{3,4,6,12\}$
$\{4,5,7,0\}$
$\{5,6,8,1\}$
$\{6,7,9,2\}$
$\{7,8,10,3\}$
$\{8,9,11,4\}$
$\{9,10,12,5\}$
$\{10,11,0,6\}$
$\{11,12,1,7\}$
$\{12,0,2,8\}$

all possible distances mod 13 appear exactly once as difference of two elements in $\{0,1,3,9\}$

Orthogonal arrays

Strength $t = 2$; $v = 3$ symbols; $k = 4$ columns; 2^3 rows

$$\begin{bmatrix} 0000 \\ 0122 \\ 1220 \\ 2202 \\ 2021 \\ 0211 \\ 2110 \\ 1101 \\ 1012 \end{bmatrix}$$

Definition: Orthogonal Array

An *orthogonal array* of strength t, k columns, v symbols and index λ denoted by $OA_\lambda(t, k, v)$, is an $\lambda v^t \times k$ array with symbols from $\{0, 1, \ldots, v-1\}$ such that in every $t \times N$ subarray, every t-tuple of $\{0, 1, \ldots, v-1\}^t$ appears in exactly λ rows.

Covering arrays

Strength $t = 3$; $v = 2$ 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 $CA(N; t, k, v)$, is an $N \times k$ array with symbols from $\{0, 1, \ldots, v-1\}$ such that in every $t \times N$ subarray, every t-tuple of $\{0, 1, \ldots, v-1\}^t$ is covered at least once.

Covering arrays

Strength $t = 3$; $v = 2$ 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 $CA(N; t, k, v)$, is an $N \times k$ array with symbols from $\{0, 1, \ldots, v-1\}$ such that in every $t \times N$ subarray, every t-tuple of $\{0, 1, \ldots, v-1\}^t$ is covered at least once.

Covering arrays generalize orthogonal arrays

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

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

An orthogonal array with index $\lambda = 1$: every every t-tuple of $\{0,1,\ldots,v-1\}^t$ appears exactly once in any t columns.
So, an $OA(t,k,v)$ is a $CA(v^t;t,k,v)$ that meets this lower bound.

For $t = 2$ and q a prime power, $\exists OA(2, k = q+1, q)$; $q-1$ MOLS.

For $t = 3$, the following orthogonal arrays exist:
$\exists OA(3,4,2), OA(3,4,3), OA(3,6,4), OA(3,6,5), OA(3,8,7)$, etc.
giving $CAN(3,4,2) = 2^3 = 8, \cdots, CAN(3,8,7) = 7^3 = 343$, etc.

Bose-Bush bound: $k \leq v+2$ is necessary for an $OA(3,k,v)$.

A Construction for Strength-3 Covering Arrays from Linear Feedback Shift Register Sequences

Work with Raaphorst, Stevens
Designs, Codes and Cryptography (September 2013).

- Use finite fields and linear feedback shift register sequences to build OA of strength 2 "almost" OA of strength 3.
- Build a CA of strength $t = 3$ by combining two of these "almost" OA of strength 3.
- We get a $CA(2q^3 - 1; 3, q^2 + q + 1; q)$.
- This improves upper bound for 512 parameter sets in Colbourn's covering array tables.

Our new construction of strength-3 covering arrays

The best CAs we can get from OAs are $CA(q^3; 3, q+2, q)$.
Our construction works for larger k up to $q^2 + q + 1$, guaranteeing an upper bound under a factor of 2 from the trivial lower bound.

Theorem (Construction for $t = 3$)

If q is a prime power then there exists a $CA(N = 2q^3 - 1; t = 3, k = q^2 + q + 1; v = q)$.

We will use liner feedback shift register sequences LFSR to build "partial" OAs (variable strength OA) that are concatenated vertically to create the CAs.

Example: our construction for $q = 2$

We get a $CA(2q^3 - 1; 3, q^2 + q + 1; q) = CA(15; 3, 7, 2)$

LFSR sequences of maximal period:

$$\underline{0011101}00111010011101\cdots$$

	0123456			
r_0:	0000000	uncovered triples		concatenate with reversals
r_1:	0011101	015	r_8:	1011100
r_2:	0111010	046	r_0:	0101110
r_3:	1110100	356	r_{10}:	0010111
r_4:	1101001	245	r_{11}:	1001011
r_5:	1010011	134	r_{12}:	1100101
r_6:	0100111	023	r_{13}:	1110010
r_7:	1001110	126	r_{14}:	0111001
		$BIBD(7, 3, 1)$		

Example: our construction for $q = 3$

We get a $CA(2q^3 - 1; 3, q^2 + q + 1; q) = CA(53; 3, 13, 3)$

$\underline{0121120111002}02122102220010121120111002021221022200 1\cdots$

	0123456789abc	$BIBD(q^2+q+1, 3, q-1)$		
r_0:	0000000000000	uncovered triples		conc. reversals
r_1:	0121120111002	3-sets of 06ab	r_{27} :	2001110211210
r_2:	1211201110020	3-sets of 59ac	r_{28} :	0200111021121
	$\cdots$	$\cdots$		$\cdots$
r_{12}:	0202122102220	3-sets of 028c	r_{38} :	0222012212020
r_{13}:	2021221022200	3-sets of 17bc	r_{39} :	0022201221202
r_{14}:	0212210222001	3-sets of 06ab	r_{40} :	1002220122120
r_{15}:	2122102220010	3-sets of 59ac	r_{41} :	0100222012212
	$\cdots$	$\cdots$		$\cdots$
r_{25}:	0101211201110	3-sets of 028c	r_{51} :	0111021121010
r_{26}:	1012112011100	3-sets of 17bc	r_{52} :	0011102112101
	matrix M	$BIBD(13, 3, 2)$		reversed M

A closer look at LFSRs

a linear feedback shift register sequence with primitive characteristic polynomial $f(x) = x^3 + 0x^2 + 2x + 1$ of degree $t = 3$ over $GF(q)$, $q = 3$ is defined by:
set arbitrary initial conditions (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** $q^t - 1 = q^3 - 1 = 26$

$$\underline{0121120111002}02122102220010121120111002021221022200 1\cdots$$

properties:

- each nonzero 3-tuple of GF(q) appears once per period, starting at positions $i = 0, \ldots, q^3 - 2$
- the patterns of zeroes is the same at adjacent windows of size $q^3 - 1/(q-1) = q^2 + q + 1$
- there are exactly $q + 1$ such zeroes.

Variable strength orthogonal arrays (VOA)

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

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

Every t consecutive columns have their q^t tuples covered.
Usually, M is not $OA(t,k,q)$: not all triples of columns **covered**.
Call Λ the hypergraph with hyper-edges the t-tuples of columns that are covered. We call M a $VOA(q^t; \Lambda, q)$.

For $t = 2$, M is the old construction for $OA(2, q+1, q)$

$t = 2$, $q = 3$, $k = \frac{q^2-1}{q-1} = q + 1$.
$T = (0, 1)$; $f(x) = x^2 + x + 2$, degree$(f) = t = 2$
LFSR: $01220211012202110122021 1 \cdots$

$$M = M(f,T) = \left[\begin{array}{c} 0000 \\ \hline 0122 \\ 1220 \\ 2202 \\ 2021 \\ 0211 \\ 2110 \\ 1101 \\ 1012 \end{array}\right]$$

is an orthogonal array of strength $t = 2$!!!

Our construction focus on $M = M(T, f)$ for $t = 3$

M is a $VOA(3, \Lambda, q)$ for $\Lambda = BIBD(q^2 + q + 1, 3, q^2)$

0121120111002021221022200101211201110020212210222001 $\cdots$

	0123456789abc	$BIBD(q^2 + q + 1, 3, q - 1)$
r_0:	0000000000000	uncovered triples
r_1:	0121120111002	3-sets of 06ab
r_2:	1211201110020	3-sets of 59ac
	$\cdots$	$\cdots$
r_{12}:	0202122102220	3-sets of 028c
r_{13}:	2021221022200	3-sets of 17bc
r_{14}:	0212210222001	3-sets of 06ab
r_{15}:	2122102220010	3-sets of 59ac
	$\cdots$	$\cdots$
r_{25}:	0101211201110	3-sets of 028c
r_{26}:	1012112011100	3-sets of 17bc

Triples of zeroes in rows of M relate to coverage

Theorem

Let q be a prime power, f be a primitive polynomial of degree 3 over $GF(q)$ with root $\alpha \in GF(q^3)$, and let $k = \frac{q^3-1}{q-1} = q^2 + q + 1$. Consider the $q^3 \times k$ array $M = M(f)$, the subinterval array of f. Then M is a $VOA(q^3; \Lambda, q)$, and for a set $\{i_0, i_1, i_2\}$, $0 \leq i_0 < i_1 < i_2 < q^2 + q + 1$, the following are equivalent:

1. $\{i_0, i_1, i_2\} \in \Lambda$ *(i.e. $\{i_0, i_1, i_2\}$ is "covered" in M).*
2. *There is no row r in M, $0 \leq r < q^3$, other than the all-zero row such that $M_{r,i_0} = M_{r,i_1} = M_{r,i_2} = 0$.*
3. $\{\alpha^{i_0}, \alpha^{i_1}, \alpha^{i_2}\}$ *is linearly independent over $GF(q)$.*

The structure of zeroes in rows of M

Theorem

Let f be a primitive polynomial f of degree 3 over $GF(q)$.

1. *Define $M = M(f)$ as before, the set $\mathcal{B} = \{\{a_1, \ldots, a_{q+1}\} : M_{i,a_1} = \ldots = M_{i,a_{q+1}} = 0$ for some $0 \leq i < q^3 - 1\}$ is the set of blocks of a projective plane of order q.*
2. *Consider Λ associated with $M = M(f)$. Then, $\binom{V}{3} \setminus \Lambda$ is a simple $BIBD(q^2 + q + 1, 3, q - 1)$, and Λ is a simple $BIBD(q^2 + q + 1, 3, q^2)$.*

Key properties: completing coverage with "reversal" of M

- Let $H = \{0 \leq i < k : a_i = 0\}$ (pos of 0's in 1st row of M).
  H is a $(q^2 + q + 1, q + 1, 1)$-difference set.
  Its translates are the blocks of the projective plane $\mathcal{B}$.
- If $\{a, b, c\} \subset H$ with $a < b < c$, then,
  $b - c + a \bmod q^2 + q + 1 \notin H$.
- Let $D = \{a, b, c\}$ with $0 \leq a < b < c < q^2 + q + 1$. If triple of columns D is uncovered in $M(f)$, then $D' = \{a, b, b - c + a\}$ is covered in $M(f)$.
- Let $\hat{f} = f(1/x)x^{\deg(f)}$, the reciprocal polynomial of f.
  If $D = \{a, b, c\}$ is not covered in $M(f)$, then D is covered in $M(\hat{f})$.
- $M(\hat{f})$ is obtained by reversal (mirror image) of $M(f)$.

For $t = 3$, there exists a $CA(2q^3 - 1; 3, q^2 + q + 1; q)$

$01211201110020212210222001\,01211201110020212210222001 \cdots$

	$M(f)$	$BIBD(q^2 + q + 1, 3, q - 1)$		$M(\hat{f})$
r_0:	0000000000000	uncovered triples		~~0000000000000~~
r_1:	0121120111002	3-sets of 06ab	r_{27} :	2001110211210
r_2:	1211201110020	3-sets of 59ac	r_{28} :	0200111021121
	...	...		...
r_{12}:	0202122102220	3-sets of 028c	r_{38} :	0222012212020
r_{13}:	2021221022200	3-sets of 17bc	r_{39} :	0022201221202
r_{14}:	0212210222001	3-sets of 06ab	r_{40} :	1002220122120
r_{15}:	2122102220010	3-sets of 59ac	r_{41} :	0100222012212
	...	...		...
r_{25}:	0101211201110	3-sets of 028c	r_{51} :	0111021121010
r_{26}:	1012112011100	3-sets of 17bc	r_{52} :	0011102112101
		$BIBD(13, 3, 2)$		

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

← 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.

$v \leq q$	k	new N	old N
6	57	684	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

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

Improving upper bounds for higher k

- Using constructed CAs as ingredients in recursive constructions we improve many upper bounds.
- Before-and-after run of Colbourn tables of best bounds, gives upper bound improvements for 512 (ranges of) parameter sets. `http://www.public.asu.edu/~ccolbou/src/tabby/catable.html`

Open Problem: How this extends to $t \geq 4$?

For general t, q, $M(f)$ is a $q^t \times \frac{q^t-1}{q-1}$ array which is a $VOA(q^t, \Lambda, q)$ for some hypergraph Λ on $\frac{q^t-1}{q-1}$ vertices.

- Find s permutations of the columns of $M(f)$ such that the vertical concatenation of the s permuted $M(f)$ is a $CA(s(q^t - 1) + 1; t, \frac{q^t-1}{q-1}, q)$.
- Determine $s(t, q)$ the smallest such s.
  From our constructions, we know $s(2, q) = 1$, $s(3, q) = 2$.
  We experimentally determined $s(4, 2) \leq 4$, $s(4, 3) \leq 6$, $s(5, 2) \leq 9$; none of these cases improved best bounds.
- Determine a largest subset of the $\frac{q^t-1}{q-1}$ columns where it is enough to paste $s = 2$ matrices. For $t = 4$, this would lead to $CA(N = 2q^4 - 1; t = 4, k, q)$ where $k \leq \frac{q^t-1}{q-1}$.
- Study the structure of Λ (covered t-tuples) for $t \geq 4$, to get insight on constructions.