# New covering arrays of strength 4 and $q$ symbols from three truncated Möbius planes in $PG(3, q)$

**Lucia Moura**
University of Ottawa
lmoura@uottawa.ca

Joint work with Kianoosh Shokri and Brett Stevens


5th Pythagorean Conference, Kalamata, Greece, June 1-6, 2025

1. Intro, OAs, CAs

2. CAs of strength 3 from LFSR & geometry

3. new CAs of strength 4 from LFRS & geometry

1. Intro, OAs, CAs
2. CAs of strength 3 from LFSR & geometry
3. new CAs of strength 4 from LFRS & geometry

# Orthogonal arrays

$OA_{\lambda=1}(N = 3^2, t = 2, k = 4, v = 3)$

| | | | |
|---|---|---|---|
| 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 $N$, $k$ columns, $v$ symbols, strength $t$ and index $\lambda$ denoted by $\mathrm{OA}_\lambda(N; t, k, v)$, is an $N \times k$ array with $v$ symbols such that in every $N \times t$ subarray, every $t$-tuple of symbols appears **exactly** $\lambda$ times as a row. $(\exists ?;\ N = \lambda v^t)$

# Covering arrays

$$CA_{\lambda=1}(N = 3^2; t = 2, k = 4, v = 3)$$

| | | | |
|---|---|---|---|
| 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

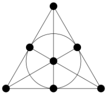
A **covering array** of size $N$, $k$ columns, $v$ symbols, strength $t$ and index $\lambda$, denoted by $\mathrm{CA}_\lambda(N; t, k, v)$, is an $N \times k$ array with $v$ symbols such that in every $N \times t$ subarray, every $t$-tuple of symbols appears **at least** $\lambda$ of times as a row. $(\min N \geq \lambda v^t)$

# OAs of strength 2 having almost strength 3

Munemasa (1998): $OA_{\lambda=2}(N = 8; t = 2, k = 7, v = 2)$
**almost** an $OA_{\lambda=1}(N = 8; t = 3, k = 7, v = 2)$

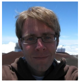
LFSR sequence: **0100111**0100111···

| 0123456 | uncovered triples of columns:[1] |
|---|---|
| 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 | $\{1, 3, 4\}$ |
| 0000000 | |



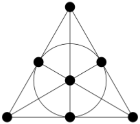
[1] 28/35 covered; 7/35 uncovered.

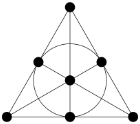
# 3-CAs out of two almost 3-OAs

Raaphorst, M., Stevens (2014):  

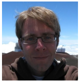
$$CA_1(N = 15; t = 3, k = 7, v = 2)$$

| 0123456 | uncovered triples of columns: |
|---|---|
| 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} |
| 0000000 | |
| 1110010 | {3, 4, 6} |
| 1100101 | {2, 3, 5} |
| 1001011 | {1, 2, 4} |
| 0010111 | {0, 1, 3} |
| 0101110 | {6, 0, 2} |
| 1011100 | {5, 6, 1} |
| 0111001 | {4, 5, 0} |
| 0000000 | |





# Two 2-OAs of strength almost 3 = 3-CA

Raaphorst, M., Stevens (2014):  

$$CA(2q^3-1; 3, \frac{q^3-1}{q-1}, q),\ q \text{ prime power}$$

| 0123456 | uncovered triples of columns: |
|---|---|
| 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 | $\{1,3,4\}$ |
| 0000000 | |
| 1110010 | $\{3,4,6\}$ |
| 1100101 | $\{2,3,5\}$ |
| 1001011 | $\{1,2,4\}$ |
| 0010111 | $\{0,1,3\}$ |
| 0101110 | $\{6,0,2\}$ |
| 1011100 | $\{5,6,1\}$ |
| 0111001 | $\{4,5,0\}$ |
| 0000000 | |

2 $\times$ 2-OAs (almost 3-OAs) = 3-CA

2 PG(2,q), $|\text{line in P1} \cap \text{line in P2}| \leq 2$

# Some 3-OAs of strength almost 4 = 4-CAs?

## Some 3-OAs of strength almost 4 = 4-CAs?

- **Tzanakis, M., Stevens and Panario, Discrete Math (2016)**

for $q = 4$, 2 ovoids in $\mathrm{PG}(3, 4)$ do the trick:
$2 \times$ 3-OAs (almost 4-OAs) give a 4-CA: $\exists$ $\mathrm{CA}(511; 4, 17, 4)$.

# Some 3-OAs of strength almost 4 = 4-CAs?

- **Tzanakis, M., Stevens and Panario, Discrete Math (2016)**



for $q = 4$, 2 ovoids in $\mathrm{PG}(3,4)$ do the trick:
$2 \times$ 3-OAs (almost 4-OAs) give a 4-CA: $\exists$ $\mathrm{CA}(511; 4, 17, 4)$.

- **Present work:**

$q$ odd prime power, take 1/2 the points of 3 ovoids in $\mathrm{PG}(3,q)$;
$3 \times$ 3-OAs (almost 4-OAs) give a 4-CA:

# Some 3-OAs of strength almost 4 = 4-CAs?

- **Tzanakis, M., Stevens and Panario, Discrete Math (2016)**



for $q = 4$, 2 ovoids in $\mathrm{PG}(3,4)$ do the trick:
$2 \times$ 3-OAs (almost 4-OAs) give a 4-CA: $\exists$ $\mathrm{CA}(511; 4, 17, 4)$.

- **Present work:**

$q$ odd prime power, take $1/2$ the points of 3 ovoids in $\mathrm{PG}(3,q)$;
$3 \times$ 3-OAs (almost 4-OAs) give a 4-CA:


**Theorem (Shokri, M., Stevens (2025+))**

*For any odd prime power $q$, there exists a $CA(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$.*

1. Intro, OAs, CAs
2. CAs of strength 3 from LFSR & geometry
3. new CAs of strength 4 from LFRS & geometry

# LFSR sequences over $\mathbb{F}_q$, 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 $\alpha$ is a **primitive element of** $\mathbb{F}_{q^m}$, and $f$ is a **primitive polynomial**.
- When $f$ is primitive the LFSR has maximum period $P = q^m - 1$, and it 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** $q^t - 1 = q^3 - 1 = 26$ (it is an M-sequence).

$01211201110020212210222001012112011100202122102220 01 \cdots$

# Properties of m-sequences

- each nonzero $m$-tuple of $\mathbb{F}_q$ appears once per period as windows of size $m$ starting at positions $i = 0, \ldots, q^m - 2$
  01211201110020212210222001012112011100202122102220 01 $\cdots$
- the patterns of zeroes is the same at adjacent windows of size $k = (q^m - 1)/(q - 1) = q^{m-1} + \ldots + q + 1$;

  0121120111002 0212210222001 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 $(a, b) = (0, 0)$
- $a_i = Tr_{q^m/q}(\alpha^i)$, $i = 0, 1, 2, \ldots$
  where $Tr_{q^m/q}(\beta) = \beta + \beta^q + \beta^{q^2} + \ldots + \beta^{q^{m-1}}$

# Subinterval array $A^k(f)$, $f$ with degree $m$

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 $f$.
Consider the following $q^m \times k = (q^m - 1)/(q - 1)$ array:

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

Every $m$ consecutive columns have their $q^m$ tuples covered.
This is an $OA_{q^{m-2}}(q^m, 2, k, q)$, where $k = (q^m - 1)/(q - 1)$.

# 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 | 000000000000000000000000000000000000000 · · · |
| 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 |

$$= OA_{q^{m-2}}(q^m; 2, (q^m - 1)/(q - 1), q) = OA_3(27; 2, 13, 3)$$

# 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 |
| | 0123456789$abc$ |

$\{0, 6, a, b\} + i \pmod{13} = \mathsf{BIBD}(13, 4, 1) = \mathsf{PG}(2, 3) = \mathsf{PG}(m-1, q)$

miss being an OA of strength $m$ because of $m$-sets of columns in blue lines

# Subinterval array: 2 compact representations

| | |
|---|---|
| 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 |
| | 0123456789*abc* |

| | |
|---|---|
| 1 | 0121120111002 |
| 2 | 1211201110020 |
| 3 | 2112011100202 |

$$\left| \alpha^0 \alpha^1 \alpha^2 \alpha^3 \alpha^4 \alpha^5 \alpha^6 \cdots \alpha^{12} \right|$$

| | |
|---|---|
| 10 | 1002021221022 |
| 25 | 0101211201110 |
| 24 | 0010121120111 |

# Strength-3 CAs using subinterval arrays

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

| | |
|---|---|
| 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 |

# 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 | | ~~0000000000000~~ |
| 1 | 0121120111002 | 27 | 2001110211210 |
| 2 | 1211201110020 | 28 | 0200111021121 |
| 3 | 2112011100202 | 29 | 2020011102112 |
| 4 | 1120111002021 | 30 | 1202001110211 |
| 5 | 1201110020212 | 31 | 2120200111021 |
| 6 | 2011100202122 | 32 | 2212020011102 |
| 7 | 0111002021221 | 33 | 1221202001110 |
| 8 | 1110020212210 | 34 | 0122120200111 |
| 9 | 1100202122102 | 35 | 2012212020011 |
| 10 | 1002021221022 | 36 | 2201221202001 |
| 11 | 0020212210222 | 37 | 2220122120200 |
| 12 | 0202122102220 | 38 | 0222012212020 |
| 13 | 2021221022200 | 39 | 0022201221202 |
| 14 | 0212210222001 | 40 | 1002220122120 |
| 15 | 2122102220010 | 41 | 0100222012212 |
| 16 | 1221022200101 | 42 | 1010022201221 |
| 17 | 2210222001012 | 43 | 2101002220122 |
| 18 | 2102220010121 | 44 | 1210100222012 |
| 19 | 1022200101211 | 45 | 1121010022201 |
| 20 | 0222001012112 | 46 | 2112101002220 |
| 21 | 2220010121120 | 47 | 0211210100222 |
| 22 | 2200101211201 | 48 | 1021121010022 |
| 23 | 2001012112011 | 49 | 1102112101002 |
| 24 | 0010121120111 | 50 | 1110211210100 |
| 25 | 0101211201110 | 51 | 0111021121010 |
| 26 | 1012112011100 | 52 | 0011102112101 |

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

compact form:

$$\left|\begin{array}{ccccccc} \alpha^0 & \alpha^1 & \alpha^2 & \cdots & \alpha^{10} & \alpha^{11} & \alpha^{12} \\ \hline \alpha^0 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-10} & \alpha^{-11} & \alpha^{-12} \end{array}\right|$$

| | |
|---|---|
| 1 | 0121120111002 |
| 2 | 1211201110020 |
| 3 | 2112011100202 |
| 27 | 2001110211210 |
| 28 | 0200111021121 |
| 29 | 2020011102112 |

# Strength-3 CAs using subinterval arrays

**Theorem (Raaphorst, M., Stevens (2014))**

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

# Strength-3 CAs using subinterval arrays

**Theorem (Raaphorst, M., Stevens (2014))**

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


- Ten years later, $R_q$ still gives the best-known upper bound in Colbourn's covering array tables for all prime powers $q \neq 2, 3$ .

# Strength-3 CAs using subinterval arrays

**Theorem (Raaphorst, M., Stevens (2014))**

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


• Ten years later, $R_q$ still gives the best-known upper bound in Colbourn's covering array tables for all prime powers $q \neq 2, 3$ .

• Colbourn, Ingals, Jedwab, Saalting, Smith, Stevens, **Sets of mutually orthogoval projective and affine planes**, 2024.
define: two planes are orthogoval if each line of a plane intersects each line of the other plane in at most 2 points.

# Strength-3 CAs using subinterval arrays

**Theorem (Raaphorst, M., Stevens (2014))**

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

- Ten years later, $R_q$ still gives the best-known upper bound in Colbourn's covering array tables for all prime powers $q \neq 2, 3$ .

- Colbourn, Ingals, Jedwab, Saalting, Smith, Stevens, **Sets of mutually orthogoval projective and affine planes**, 2024.
define: two planes are orthogoval if each line of a plane intersects each line of the other plane in at most 2 points.

- $R_q$ is constructed using 2 orthogoval projective planes.

1. Intro, OAs, CAs
2. CAs of strength 3 from LFSR & geometry
3. new CAs of strength 4 from LFRS & geometry

# Generalization from 3-CAs to 4-CAs

For the 3-CA construction $R_q$:

- we use the whole PG$(2, q)$: $k = \frac{q^3-1}{q-1}$ columns; each column is generated by a vector in $\mathbb{F}_q^3$.
- 2 subinterval arrays constructed using LFSR sequences from primitive $\alpha \in \mathbb{F}_{q^3}$:
  $\alpha^i$ and $\alpha^{-i}$, for $0 \le i < q^2 + q + 1$
- Each array is a 2-OA that is almost a 3-OA, the missing triples are 3 colinear points on a projective plane $P(2, q)$.
- The 2 arrays together form a 3-CA (3 colinear points in one plane are not colinear in the other)

# Generalization from 3-CAs to 4-CAs

For the 3-CA construction $R_q$:

- we use the **whole PG**$(2, q)$: $k = \frac{q^3-1}{q-1}$ columns; each column is generated by a vector in $\mathbb{F}_q^3$.
- 2 subinterval arrays constructed using LFSR sequences from primitive $\alpha \in \mathbb{F}_{q^3}$:
  $\alpha^i$ and $\alpha^{-i}$, for $0 \leq i < q^2 + q + 1$
- Each array is a 2-OA that is almost a 3-OA, the missing triples are 3 colinear points on a projective plane $P(2, q)$.
- The 2 arrays together form a 3-CA (3 colinear points in one plane are not colinear in the other)

# Generalization from 3-CAs to 4-CAs

For the 3-CA construction $R_q$:

- we use the **whole PG**$(2,q)$: $k = \frac{q^3-1}{q-1}$ columns; each column is generated by a vector in $\mathbb{F}_q^3$.
- 2 subinterval arrays constructed using LFSR sequences from primitive $\alpha \in \mathbb{F}_{q^3}$:
  $\alpha^i$ and $\alpha^{-i}$, for $0 \le i < q^2+q+1$
- Each array is a 2-OA that is almost a 3-OA, the missing triples are 3 colinear points on a projective plane $P(2,q)$.
- The 2 arrays together form a 3-CA (3 colinear points in one plane are not colinear in the other)

For the 4-CA construction, $q$ odd prime power:

- we used use half the points of an ovoid in PG$(3,q)$, which is a set of $q^2+1$ points no 3 of which colinear: $k = \frac{q^2+1}{2}$ columns.
- 3 subinterval arrays constructed using LFSR sequences from primitive $\alpha \in \mathbb{F}_{q^4}$, but only take indices multiple of $q+1$:
  $\alpha^{i(q+1)}$, $\alpha^{2i(q+1)}$, $\alpha^{4i(q+1)}$, for $0 \le i < \frac{q^2+1}{2}$
- Each array is a 3-OA that is almost a 4-OA, the missing quadruples are 4 coplanar points on an ovoid in $P(3,q)$.
- We investigate this structure more carefully to show that these 3 arrays together form a 4-CA.

# OVOID IN PG(3, $q$) (EXAMPLE FOR $q = 7$)

- each column corresponds to $\alpha^{i(q+1)}$, where $\alpha$ is primitive in $\mathbb{F}_{q^4}$

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6 3 6 1 4 1 2 1 0 4 3 1 5 2 1 5 2 3 6 5 0 4 1 6 5
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4 6 4 6 2 6 3 0 0 3 6 5 4 6 0 0 1 6 6 5 3 3 6 3 4
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6 5 4 5 3 2 6 0 1 2 6 0 5 4 5 1 1 3 3 3 6 0 6 6 2
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0 2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5

---

0 0 5 1 5 6 6 2 4 5 2 4 4 0 0 5 5 0 5 0 5 3 3 4 2 1 3 3 1 5 4 2 1 6 1 2 4 1 3 3 4 3 5 1 5 0 3 0 6 4
0 6 5 1 0 2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5 3 5 4 1 0 6 0 2 3 6 1 5 5 0 3 6 2 6 5 1 3
0 0 6 2 5 0 6 3 6 0 0 3 0 2 2 1 6 5 4 3 2 6 2 2 5 3 5 1 3 6 0 3 1 1 1 6 2 1 3 6 6 6 3 6 2 1 6 4 0 5
0 1 0 3 3 5 2 4 6 1 3 2 3 3 4 1 4 5 1 2 0 1 5 5 5 2 3 5 1 2 2 2 1 2 3 5 2 6 0 4 0 0 6 2 5 0 6 3 6 0
0 2 1 4 1 3 5 5 6 2 6 1 6 4 6 1 2 5 5 1 5 3 1 1 5 1 1 2 6 5 4 1 1 3 5 4 2 4 4 2 1 1 2 5 1 6 6 2 5 2
0 3 2 5 6 1 1 6 6 3 2 0 2 5 1 1 0 5 2 0 3 5 4 4 5 0 6 6 4 1 6 0 1 4 0 3 2 2 1 0 2 2 5 1 4 5 6 1 4 4
0 4 3 6 4 6 4 0 6 4 5 6 5 6 3 1 5 5 6 6 1 0 0 0 5 6 4 3 2 4 1 6 1 5 2 2 2 0 5 5 3 3 1 4 0 4 6 0 3 6
0 5 4 0 2 4 0 1 6 5 1 5 1 0 5 1 3 5 3 5 6 2 3 3 5 5 2 0 0 0 3 5 1 6 4 1 2 5 2 3 4 4 4 0 3 3 6 6 2 1
0 4 4 0 4 0 4 1 1 6 3 5 1 1 5 4 6 3 5 2 5 3 6 5 1 1 6 1 4 5 4 0 1 0 2 6 0 0 5 1 5 6 6 2 4 5 2 4 4 0

$\vdots$

# Ovoid in PG$(3, q)$ (example for $q = 7$)

- each column corresponds to $\alpha^{i(q+1)}$, where $\alpha$ is primitive in $\mathbb{F}_{q^4}$

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6 ~~3 6 1 4 1 2 1 0 4 3 1 5 2 1 5 2 3 6 5 0 4 1 6 5~~
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4 ~~6 4 6 2 6 3 0 0 3 6 5 4 6 0 0 1 6 6 5 3 3 6 3 4~~
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6 ~~5 4 5 3 2 6 0 1 2 6 0 5 4 5 1 1 3 3 3 6 0 6 6 2~~
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0 ~~2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5~~

---

1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 ×
1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 ×
× × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × ×

# Ovoid in PG(3, $q$) (example for $q = 7$)

- each column corresponds to $\alpha^{i(q+1)}$, where $\alpha$ is primitive in $\mathbb{F}_{q^4}$

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6 ~~3 6 1 4 1 2 1 0 4 3 1 5 2 1 5 2 3 6 5 0 4 1 6 5~~
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4 ~~6 4 6 2 6 3 0 0 3 6 5 4 6 0 0 1 6 6 5 3 3 6 3 4~~
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6 ~~5 4 5 3 2 6 0 1 2 6 0 5 4 5 1 1 3 3 3 6 0 6 6 2~~
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0 ~~2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5~~

1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 ×
1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 ×
× × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × ×

- now use $\alpha^2$: $(\alpha^2)^{i(q+1)}$. (25 points out of 400 points)

0 1 2 0 0 0 6 6 0 6 1 6 3 3 1 1 1 4 1 2 5 3 5 4 6
0 6 4 1 2 6 4 5 5 5 1 0 3 6 6 6 0 3 5 6 0 6 5 3 3
0 1 5 3 0 3 3 2 5 4 5 3 0 5 5 2 0 2 0 4 1 3 3 0 6
1 6 0 0 1 5 4 1 3 4 1 6 1 2 2 6 4 1 1 5 4 4 6 4 4

# Ovoid in PG(3, $q$) (example for $q = 7$)

- each column corresponds to $\alpha^{i(q+1)}$, where $\alpha$ is primitive in $\mathbb{F}_{q^4}$

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6 ~~3 6 1 4 1 2 1 0 4 3 1 5 2 1 5 2 3 6 5 0 4 1 6 5~~
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4 ~~6 4 6 2 6 3 0 0 3 6 5 4 6 0 0 1 6 6 5 3 3 6 3 4~~
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6 ~~5 4 5 3 2 6 0 1 2 6 0 5 4 5 1 1 3 3 3 6 0 6 6 2~~
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0 ~~2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5~~

1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 × 1 ×
1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 ×
× × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × × 1 × × ×

- now use $\alpha^2$: $(\alpha^2)^{i(q+1)}$. (25 points out of 400 points)

0 1 2 0 0 0 6 6 0 6 1 6 3 3 1 1 1 4 1 2 5 3 5 4 6
0 6 4 1 2 6 4 5 5 5 1 0 3 6 6 6 0 3 5 6 0 6 5 3 3
0 1 5 3 0 3 3 2 5 4 5 3 0 5 5 2 0 2 0 4 1 3 3 0 6
1 6 0 0 1 5 4 1 3 4 1 6 1 2 2 6 4 1 1 5 4 4 6 4 4

- now use $\alpha^4$: $(\alpha^4)^{i(q+1)}$. (25 points out of 400 points)

0 2 0 6 0 1 3 1 1 1 5 5 6 1 0 0 6 6 6 3 1 4 2 3 4
0 4 2 4 5 1 3 6 0 5 0 5 3 6 1 6 5 5 0 6 6 3 6 6 3
0 5 0 3 5 5 0 5 0 0 1 3 6 1 3 3 2 4 3 5 2 2 4 3 0
1 0 1 4 3 1 1 2 4 1 4 6 4 6 0 5 1 4 6 2 6 1 5 4 4

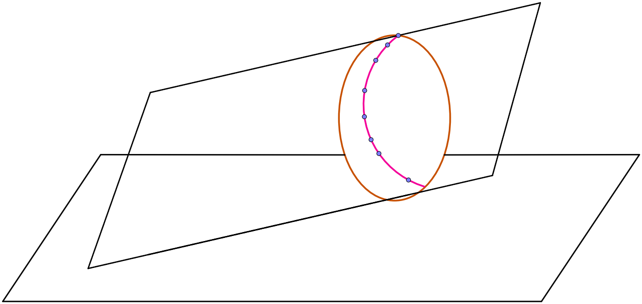
# Ovoid in PG(3, $q$) (example for $q = 7$)

```
0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6 3 6 1 4 1 2 1 0 4 3 1 5 2 1 5 2 3 6 5 0 4 1 6 5
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4 6 4 6 2 6 3 0 0 3 6 5 4 6 0 0 1 6 6 5 3 3 6 3 4
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6 5 4 5 3 2 6 0 1 2 6 0 5 4 5 1 1 3 3 3 6 0 6 6 2
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0 2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5
-------------------------------------------------------------------------------------------------------
0 0 5 1 5 6 6 2 4 5 2 4 4 0 0 5 5 0 5 0 5 3 3 4 2 1 3 3 1 5 4 2 1 6 1 2 4 1 3 3 4 3 5 1 5 0 3 0 6 4
0 6 5 1 0 2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5 3 5 4 1 0 6 0 2 3 6 1 5 5 0 3 6 2 6 5 1 3
0 0 6 2 5 0 6 3 6 0 0 3 0 2 2 1 6 5 4 3 2 6 2 2 5 3 5 1 3 6 0 3 1 1 1 6 2 1 3 6 6 6 3 6 2 1 6 4 0 5
0 1 0 3 3 5 2 4 6 1 3 2 3 3 4 1 4 5 1 2 0 1 5 5 5 2 3 5 1 2 2 2 1 2 3 5 2 6 0 4 0 0 6 2 5 0 6 3 6 0
0 2 1 4 1 3 5 5 6 2 6 1 6 4 6 1 2 5 5 1 5 3 1 1 5 1 1 2 6 5 4 1 1 3 5 4 2 4 4 2 1 1 2 5 1 6 6 2 5 2
0 3 2 5 6 1 1 6 6 3 2 0 2 5 1 1 0 5 2 0 3 5 4 4 5 0 6 6 4 1 6 0 1 4 0 3 2 2 1 0 2 2 5 1 4 5 6 1 4 4
0 4 3 6 4 6 4 0 6 4 5 6 5 6 3 1 5 5 6 6 1 0 0 0 5 6 4 3 2 4 1 6 1 5 2 2 2 0 5 5 3 3 1 4 0 4 6 0 3 6
0 5 4 0 2 4 0 1 6 5 1 5 1 0 5 1 3 5 3 5 6 2 3 3 5 5 2 0 0 0 3 5 1 6 4 1 2 5 2 3 4 4 4 0 3 3 6 6 2 1
0 4 4 0 4 0 4 1 1 6 3 5 1 1 5 4 6 3 5 2 5 3 6 5 1 1 6 1 4 5 4 0 1 0 2 6 0 0 5 1 5 6 6 2 4 5 2 4 4 0

                                                 ⋮
```

- Ovoid in PG$(3, q)$ - largest set of points no tree of which are colinear, $|O| = q^2 + 1$.
- Its plane sections (circles) are a $3 - (q^2 + 1, q + 1, 1)$ design, called a Möbius plane of order $q$.

# Ovoid and one circle of a Möbius plane



# Build 4-CA - from 3 truncated Möbius planes

$\alpha$

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6 ~~3 6 1 4 1 2 1 0 4 3 1 5 2 1 5 2 3 6 5 0 4 1 6 5~~
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4 ~~6 4 6 2 6 3 0 0 3 6 5 4 6 0 0 1 6 6 5 3 3 6 3 4~~
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6 ~~5 4 5 3 2 6 0 1 2 6 0 5 4 5 1 1 3 3 3 6 0 6 6 2~~
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0 ~~2 3 2 6 6 4 4 4 1 0 1 1 5 0 4 4 4 6 6 5 4 0 4 5~~

# Build 4-CA - from 3 truncated Möbius planes

$\alpha$ (truncated Möbius plane)

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0

# Build 4-CA - from 3 truncated Möbius planes

$\alpha$ (truncated Möbius plane)

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 5 | 1 | 4 | 2 | 1 | 0 | 5 | 0 | 6 | 0 | 1 | 6 | 1 | 6 | 6 | 0 | 4 | 6 | 3 | 1 | 0 | 6 | 2 | 3 | 6 |
| 0 | 5 | 6 | 6 | 4 | 5 | 1 | 6 | 2 | 0 | 6 | 1 | 4 | 0 | 5 | 3 | 5 | 5 | 5 | 5 | 1 | 6 | 0 | 6 | 3 | 4 |
| 0 | 1 | 1 | 1 | 5 | 5 | 3 | 1 | 0 | 1 | 3 | 6 | 3 | 1 | 2 | 0 | 5 | 0 | 4 | 6 | 5 | 2 | 3 | 3 | 0 | 6 |
| 1 | 4 | 6 | 5 | 0 | 2 | 0 | 3 | 1 | 2 | 5 | 4 | 4 | 0 | 1 | 2 | 3 | 2 | 4 | 5 | 1 | 0 | 6 | 5 | 1 | 0 |

$\alpha^2$ (truncated Möbius plane)

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 0 | 0 | 0 | 6 | 6 | 0 | 6 | 1 | 6 | 3 | 3 | 1 | 1 | 1 | 4 | 1 | 2 | 5 | 3 | 5 | 4 | 6 |
| 0 | 6 | 4 | 1 | 2 | 6 | 4 | 5 | 5 | 5 | 1 | 0 | 3 | 6 | 6 | 6 | 0 | 3 | 5 | 6 | 0 | 6 | 5 | 3 | 3 |
| 0 | 1 | 5 | 3 | 0 | 3 | 3 | 2 | 5 | 4 | 5 | 3 | 0 | 5 | 5 | 2 | 0 | 2 | 0 | 4 | 1 | 3 | 3 | 0 | 6 |
| 1 | 6 | 0 | 0 | 1 | 5 | 4 | 1 | 3 | 4 | 1 | 6 | 1 | 2 | 2 | 6 | 4 | 1 | 1 | 5 | 4 | 4 | 6 | 4 | 4 |

# Build 4-CA - from 3 truncated Möbius planes

$\alpha$ (truncated Möbius plane)

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 5 | 1 | 4 | 2 | 1 | 0 | 5 | 0 | 6 | 0 | 1 | 6 | 1 | 6 | 6 | 0 | 4 | 6 | 3 | 1 | 0 | 6 | 2 | 3 | 6 |
| 0 | 5 | 6 | 6 | 4 | 5 | 1 | 6 | 2 | 0 | 6 | 1 | 4 | 0 | 5 | 3 | 5 | 5 | 5 | 5 | 1 | 6 | 0 | 6 | 3 | 4 |
| 0 | 1 | 1 | 1 | 5 | 5 | 3 | 1 | 0 | 1 | 3 | 6 | 3 | 1 | 2 | 0 | 5 | 0 | 4 | 6 | 5 | 2 | 3 | 3 | 0 | 6 |
| 1 | 4 | 6 | 5 | 0 | 2 | 0 | 3 | 1 | 2 | 5 | 4 | 4 | 0 | 1 | 2 | 3 | 2 | 4 | 5 | 1 | 0 | 6 | 5 | 1 | 0 |

$\alpha^2$ (truncated Möbius plane)

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 0 | 0 | 0 | 6 | 6 | 0 | 6 | 1 | 6 | 3 | 3 | 1 | 1 | 1 | 4 | 1 | 2 | 5 | 3 | 5 | 4 | 6 |
| 0 | 6 | 4 | 1 | 2 | 6 | 4 | 5 | 5 | 5 | 1 | 0 | 3 | 6 | 6 | 6 | 0 | 3 | 5 | 6 | 0 | 6 | 5 | 3 | 3 |
| 0 | 1 | 5 | 3 | 0 | 3 | 3 | 2 | 5 | 4 | 5 | 3 | 0 | 5 | 5 | 2 | 0 | 2 | 0 | 4 | 1 | 3 | 3 | 0 | 6 |
| 1 | 6 | 0 | 0 | 1 | 5 | 4 | 1 | 3 | 4 | 1 | 6 | 1 | 2 | 2 | 6 | 4 | 1 | 1 | 5 | 4 | 4 | 6 | 4 | 4 |

$\alpha^4$ (truncated Möbius plane)

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 2 | 0 | 6 | 0 | 1 | 3 | 1 | 1 | 1 | 5 | 5 | 6 | 1 | 0 | 0 | 6 | 6 | 6 | 3 | 1 | 4 | 2 | 3 | 4 |
| 0 | 4 | 2 | 4 | 5 | 1 | 3 | 6 | 0 | 5 | 0 | 5 | 3 | 6 | 1 | 6 | 5 | 5 | 0 | 6 | 6 | 3 | 6 | 6 | 3 |
| 0 | 5 | 0 | 3 | 5 | 5 | 0 | 5 | 0 | 0 | 1 | 3 | 6 | 1 | 3 | 3 | 2 | 4 | 3 | 5 | 2 | 2 | 4 | 3 | 0 |
| 1 | 0 | 1 | 4 | 3 | 1 | 1 | 2 | 4 | 1 | 4 | 6 | 4 | 6 | 0 | 5 | 1 | 4 | 6 | 2 | 6 | 1 | 5 | 4 | 4 |

# Build 4-CA - from 3 truncated Möbius planes

$\alpha$ (truncated Möbius plane)

0 5 1 4 2 1 0 5 0 6 0 1 6 1 6 6 0 4 6 3 1 0 6 2 3 6
0 5 6 6 4 5 1 6 2 0 6 1 4 0 5 3 5 5 5 5 1 6 0 6 3 4
0 1 1 1 5 5 3 1 0 1 3 6 3 1 2 0 5 0 4 6 5 2 3 3 0 6
1 4 6 5 0 2 0 3 1 2 5 4 4 0 1 2 3 2 4 5 1 0 6 5 1 0

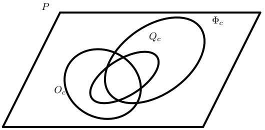
$\alpha^2$ (truncated Möbius plane)

0 1 2 0 0 0 6 6 0 6 1 6 3 3 1 1 1 4 1 2 5 3 5 4 6
0 6 4 1 2 6 4 5 5 5 1 0 3 6 6 6 0 3 5 6 0 6 5 3 3
0 1 5 3 0 3 3 2 5 4 5 3 0 5 5 2 0 2 0 4 1 3 3 0 6
1 6 0 0 1 5 4 1 3 4 1 6 1 2 2 6 4 1 1 5 4 4 6 4 4

$\alpha^4$ (truncated Möbius plane)

0 2 0 6 0 1 3 1 1 1 5 5 6 1 0 0 6 6 6 3 1 4 2 3 4
0 4 2 4 5 1 3 6 0 5 0 5 3 6 1 6 5 5 0 6 6 3 6 6 3
0 5 0 3 5 5 0 5 0 0 1 3 6 1 3 3 2 4 3 5 2 2 4 3 0
1 0 1 4 3 1 1 2 4 1 4 6 4 6 0 5 1 4 6 2 6 1 5 4 4

The intersection of one circle from each truncated Möbius plane has at most 3 points.



# Our main theorem


**Theorem (Shokri, M., Stevens (2025+))**

*For any odd prime power $q$, there exists a $CA(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$.*

# Our main theorem

**Theorem (Shokri, M., Stevens (2025+))**

*For any odd prime power $q$, there exists a* $CA(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$.

This improves best bounds in CA tables by 25% for all odd prime powers $q \geq 11$.

| $q$ | CAs from our construction | The best-known CAs | | | |
|---|---|---|---|---|---|
| | $CA(N_s = 3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ | $CA(N_c; 4, k_c, q)$ | Method | $N_c - N_s$ | $(N_c - N_s)/N_c$ |
| 3 | $CA(241; 4, 5, 3)$ | $CA(81; 4, 5, 3)$ | Derive from strength 5 | 160 | 1.975 |
| 5 | $CA(1873; 4, 13, 5)$ | $CA(1225; 4, 14, 5)$ | 2-Restricted SCPHF RE (CL) | 648 | 0.528 |
| 7 | $CA(7201; 4, 25, 7)$ | $CA(6853; 4, 30, 7)$ | 3-Restricted SCPHF RE (CL) | 348 | 0.05 |
| 9 | $CA(19681; 4, 41, 9)$ | $CA(19593; 4, 41, 9)$ | 2-Restricted SCPHF RE (CL) | 88 | 0.004 |
| 11 | $CA(\mathbf{43921}; 4, 61, 11)$ | $CA(55891; 4, 80, 11)$ | 3,3-Restricted SCPHF RE (CL) | −11970 | −0.214 |
| 13 | $CA(\mathbf{85681}; 4, 85, 13)$ | $CA(109837; 4, 94, 13)$ | 3,3-Restricted SCPHF RE (CL) | −24156 | −0.219 |
| 17 | $CA(\mathbf{250561}; 4, 145, 17)$ | $CA(329137; 4, 152, 17)$ | 3-Restricted SCPHF RE (CL) | −78576 | −0.238 |
| 19 | $CA(\mathbf{390961}; 4, 181, 19)$ | $CA(520543; 4, 191, 19)$ | 2,2-Restricted SCPHF RE (CL) | −129582 | −0.248 |
| 23 | $CA(\mathbf{839521}; 4, 265, 23)$ | $CA(1119361; 4, 302, 23)$ | CPHF IPO 4 (WCS) | −279840 | −0.249 |
| 25 | $CA(\mathbf{1171873}; 4, 313, 25)$ | $CA(1562497; 4, 344, 25)$ | CPHF IPO 4 (WCS) | −390606 | −0.249 |

# Conclusions and Future work

| $m$ | OA from LFSR. | CA construction | |
|---|---|---|---|
| 2 | $OA_1(q^2, 2, q+1, q)$ | OA: $CA(q^2; 2, q+1, q)$ | Bush (1952) |
| 3 | $OA_q(q^3, 2, \frac{q^3-1}{q-1}, q)$ almost strength 3 | $CA(2q^3-1; 3, \frac{q^3-1}{q-1}, q)$ | Raaphorst et al. (2014) |
| 4 | $OA_q(q^4; 3, q^2+1, q)$ almost strength 4 | $CA(2q^4-1; 4, q^2+1, 4)$ | Tzanakis et al. (2016) |
| | | $CA(3q^4-1; 4, \frac{q^2+1}{2}, q)$, $q$ odd prime power | Shokri et al. (2025+) |

# Conclusions and Future work

| $m$ | OA from LFSR. | CA construction | |
|---|---|---|---|
| 2 | $OA_1(q^2, 2, q+1, q)$ | OA: $CA(q^2; 2, q+1, q)$ | Bush (1952) |
| 3 | $OA_q(q^3, 2, \frac{q^3-1}{q-1}, q)$ almost strength 3 | $CA(2q^3-1; 3, \frac{q^3-1}{q-1}, q)$ | Raaphorst et al. (2014) |
| 4 | $OA_q(q^4; 3, q^2+1, q)$ almost strength 4 | $CA(2q^4-1; 4, q^2+1, 4)$ | Tzanakis et al. (2016) |
| | | $CA(3q^4-1; 4, \frac{q^2+1}{2}, q)$, $q$ odd prime power | Shokri et al. (2025+) |

Future work:

- what about strength 4 and $q$ even?
- what about $q$ odd and $k = q^2+1$?
- how would this generalize to strength 5?