Ordered Orthogonal Array Construction using LFSR Sequences

André Guerino Castoldi
Visiting Researcher at University of Ottawa, Canada
PhD Student at State University of Maringá, Brazil

Join work with **Lucia Moura**, **Daniel Panario** and **Brett Stevens**

Algebraic Combinatorics and Applications, ALCOMA,
March 2015

- (M.Y. Rosenbloom, M.A. Tsfasman, 1997) constructed MDS codes with respect to m-metric (also known as NRT-metric or ρ-metric) called **Reed-Solomon m-codes**.
- Present a new construction to Reed-Solomon m-codes in terms of an equivalent combinatorial object called **Ordered Orthogonal Array** using Linear Feedback Shift Register Sequences (LFSRs).

Orthogonal Arrays

Definition

An **orthogonal array** $OA(t,k,v)$ is a $v^t \times k$ array with each entry from a finite set V (alphabet) of size v and satisfying the following property:

For any subarray $v^t \times t$ each t-tuple of V^t appears **exactly once** as a row.

Example

Strength $t = 3$, $k = 4$ columns, $v = 2$ binary alphabet, 2^3 rows

$$OA(3,4,2) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Ordered Orthogonal Arrays

Let m and s be positive integers and the set $[m \times s] := \{0, \ldots, ms - 1\}$ partitioned into m blocks B_i of cardinality s, where

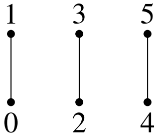
$$B_i = \{is, \ldots, (i + 1)s - 1\}$$

for $i = 0, \ldots, m - 1$. Each block has the total ordering:

$$is \prec is + 1 \prec \ldots \prec (i + 1)s - 1.$$

- The set $[m \times s]$ has the structure of partially ordered set (poset): the union of m totally ordered sets with s elements each.
- An **ideal** is a subset of $[m \times s]$ closed under predecessors.
- An **antiideal** is a subset of $[m \times s]$ closed under followers.

Example: $m = 3$ and $s = 2$



Ideals of size 3	Antiideals of size 3
$\{0,2,4\}$	$\{1,3,5\}$
$\{2,4,5\}$	$\{0,1,3\}$
$\{2,3,4\}$	$\{0,1,5\}$
$\{0,4,5\}$	$\{1,2,3\}$
$\{0,1,4\}$	$\{2,3,5\}$
$\{0,2,3\}$	$\{1,4,5\}$
$\{0,1,2\}$	$\{3,4,5\}$

An antiideal is the complement of an ideal.

Definition

Let t, m, s, v be positive integers such that $2 \leq t \leq ms$. An **ordered orthogonal array** $OOA(t, m, s, v)$ is a $v^t \times ms$ array A with entries from an alphabet V of size v, and satisfying the property:

For each **antiideal** $I \subset [m \times s]$ of cardinality t , in the t columns of A labeled by I each t-tuple of elements in V appears **exactly once** as a row.

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \begin{array}{c} \begin{array}{cc|cc|cc} 0 & 1 & 2 & 3 & 4 & 5 \end{array} \\ \left[\begin{array}{cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \end{array}$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \left[\begin{array}{cc|cc|cc} 0 & \mathbf{1} & 2 & \mathbf{3} & 4 & \mathbf{5} \\ \hline 1 & \mathbf{0} & 1 & \mathbf{0} & 1 & \mathbf{1} \\ 0 & \mathbf{0} & 0 & \mathbf{1} & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 1 & \mathbf{0} & 1 & \mathbf{0} \\ 1 & \mathbf{0} & 1 & \mathbf{1} & 1 & \mathbf{0} \\ 0 & \mathbf{1} & 1 & \mathbf{1} & 1 & \mathbf{1} \\ 1 & \mathbf{1} & 0 & \mathbf{1} & 0 & \mathbf{0} \\ 1 & \mathbf{1} & 0 & \mathbf{0} & 0 & \mathbf{1} \\ 0 & \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} \end{array}\right]$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \begin{array}{c} \begin{array}{cc|cc|cc} \mathbf{0} & \mathbf{1} & 2 & \mathbf{3} & 4 & 5 \end{array} \\ \left[\begin{array}{cc|cc|cc} \mathbf{1} & \mathbf{0} & 1 & \mathbf{0} & 1 & 1 \\ \mathbf{0} & \mathbf{0} & 0 & \mathbf{1} & 0 & 1 \\ \mathbf{0} & \mathbf{1} & 1 & \mathbf{0} & 1 & 0 \\ \mathbf{1} & \mathbf{0} & 1 & \mathbf{1} & 1 & 0 \\ \mathbf{0} & \mathbf{1} & 1 & \mathbf{1} & 1 & 1 \\ \mathbf{1} & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & \mathbf{1} & 0 & \mathbf{0} & 0 & 1 \\ \mathbf{0} & \mathbf{0} & 0 & \mathbf{0} & 0 & 0 \end{array}\right] \end{array}$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \begin{array}{c} \begin{array}{cc|cc|cc} \mathbf{0} & \mathbf{1} & 2 & 3 & 4 & \mathbf{5} \end{array} \\ \left[\begin{array}{cc|cc|cc} \mathbf{1} & \mathbf{0} & 1 & 0 & 1 & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & 0 & 1 & 0 & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & 1 & 0 & 1 & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & 1 & 1 & 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & 1 & 1 & 1 & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & 0 & 1 & 0 & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & \mathbf{0} \end{array}\right] \end{array}$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \begin{array}{c} \begin{array}{cc|cc|cc} 0 & \mathbf{1} & \mathbf{2} & \mathbf{3} & 4 & 5 \end{array} \\ \left[\begin{array}{cc|cc|cc} 1 & \mathbf{0} & \mathbf{1} & \mathbf{0} & 1 & 1 \\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 1 \\ 0 & \mathbf{1} & \mathbf{1} & \mathbf{0} & 1 & 0 \\ 1 & \mathbf{0} & \mathbf{1} & \mathbf{1} & 1 & 0 \\ 0 & \mathbf{1} & \mathbf{1} & \mathbf{1} & 1 & 1 \\ 1 & \mathbf{1} & \mathbf{0} & \mathbf{1} & 0 & 0 \\ 1 & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 & 1 \\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 \end{array}\right] \end{array}$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \begin{array}{c} \begin{array}{cc|cc|cc} 0 & 1 & \mathbf{2} & \mathbf{3} & 4 & \mathbf{5} \end{array} \\ \left[\begin{array}{cc|cc|cc} 1 & 0 & \mathbf{1} & \mathbf{0} & 1 & \mathbf{1} \\ 0 & 0 & \mathbf{0} & \mathbf{1} & 0 & \mathbf{1} \\ 0 & 1 & \mathbf{1} & \mathbf{0} & 1 & \mathbf{0} \\ 1 & 0 & \mathbf{1} & \mathbf{1} & 1 & \mathbf{0} \\ 0 & 1 & \mathbf{1} & \mathbf{1} & 1 & \mathbf{1} \\ 1 & 1 & \mathbf{0} & \mathbf{1} & 0 & \mathbf{0} \\ 1 & 1 & \mathbf{0} & \mathbf{0} & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{0} & \mathbf{0} & 0 & \mathbf{0} \end{array}\right] \end{array}$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \begin{array}{c} \begin{array}{cc|cc|cc} 0 & \mathbf{1} & 2 & 3 & \mathbf{4} & \mathbf{5} \end{array} \\ \left[\begin{array}{cc|cc|cc} 1 & \mathbf{0} & 1 & 0 & \mathbf{1} & \mathbf{1} \\ 0 & \mathbf{0} & 0 & 1 & \mathbf{0} & \mathbf{1} \\ 0 & \mathbf{1} & 1 & 0 & \mathbf{1} & \mathbf{0} \\ 1 & \mathbf{0} & 1 & 1 & \mathbf{1} & \mathbf{0} \\ 0 & \mathbf{1} & 1 & 1 & \mathbf{1} & \mathbf{1} \\ 1 & \mathbf{1} & 0 & 1 & \mathbf{0} & \mathbf{0} \\ 1 & \mathbf{1} & 0 & 0 & \mathbf{0} & \mathbf{1} \\ 0 & \mathbf{0} & 0 & 0 & \mathbf{0} & \mathbf{0} \end{array}\right] \end{array}$$

Example

Strength $t = 3$, $m = 3$, $s = 2$, $v = 2$ binary alphabet, 2^3 rows

$$OOA(3,3,2,2) = \left[\begin{array}{cc|cc|cc} 0 & 1 & 2 & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \hline 1 & 0 & 1 & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ 0 & 1 & 1 & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 1 & 0 & 1 & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ 0 & 1 & 1 & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ 1 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 1 & 1 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array}\right]$$

Theorem

For q a prime power and $t \geq 2$, there exists an $OOA(t, q+1, t-1, q)$.

Theorem: Reed-Solomon m-codes

Let q be a prime power and $s \leq t$. There exists an MDS code with respect to m-metric whose the parameters are $[q+1, s, t, (q+1)s-(t-1)]_q$.

M.Y. Rosenbloom, M.A. Tsfasman, *Codes for m-metric*, Probl. Inf. Transm. (1997)

M.M. Skriganov, *Coding theory and uniform distributions*, St. Petersburg Math. J. (2002)

S. Raaphorst, L. Moura, B. Stevens, *A Construction for Strength-3 Covering Arrays from Linear Feedback Shift Register Sequences*. Designs, Codes and Cryptography (2014).

- Let $f(x) = c_0 + c_1 x + \ldots + c_{t-1}x^{t-1} + x^t$ be a primitive polynomial over $\mathbb{F}_q$ of degree t and $\alpha \in \mathbb{F}_{q^t}$ a root of f. A **linear feed back shift register** with primitive polynomial f and initial values $T = (b_0, \ldots, b_{t-1}) \in \mathbb{F}_q^t$ is a sequence $S(f, T) = (a_i)_{i \geq 0}$ over $\mathbb{F}_q$ defined as

$$a_i = \begin{cases} b_i & \text{if } 0 \leq i < t \\ -\sum_{j=0}^{t-1} c_j a_{i-t+j} & \text{if } i \geq t. \end{cases}$$

- There exists an unique nonzero initial values $T \in \mathbb{F}_q^t$ such that the trace representation of the LFSR generated by f and T is given by $S(f, T) = (a_i)_{i \geq 0} = (Tr(\alpha^i))_{i \geq 0}$.
- The sequence $S(f, T)$ has maximum period $q^t - 1$.

- Define $k = \dfrac{q^t - 1}{q - 1}$.
- $C_i^k(S(f,T)) = (a_i, \ldots, a_{i+k-1})$ is the subinterval of $S(f,T)$ of length k beginning in position i.
- For any $i > 0, j > 0$ the positions of zeroes in $C_i^k(S(f,T))$ and $C_{i+jk}^k(S(f,T))$ are identical.
- Consider the following $q^t \times k$ array:

$$M = \begin{bmatrix} C_0^k(S(f,T)) \\ C_1^k(S(f,T)) \\ \vdots \\ C_{q^t-2}^k(S(f,T)) \\ 0, 0, \ldots, 0 \end{bmatrix}$$

The array M is called **subinterval array of f**.

Let $f(x) = x^3 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. The sequence is defined by $a_i = a_{i-2} + a_{i-3}$ for $i \geq 3$. A period of the LFSR generated by f and (100) is

$$1001011.$$

The **subinterval array of f** is:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

- Each nonzero t-tuple of $\mathbb{F}_q$ appears **once** per period of an LFSR.
- Each set of t **consecutive columns** of the subinterval array M of f has the coverage property.

Theorem (S. Raaphorst, L. Moura, B. Stevens, 2014)

Let f be a primitive polynomial over $\mathbb{F}_q$ of degree t and $\alpha \in \mathbb{F}_{q^t}$ a root of f. Define $k = \frac{q^t-1}{q-1}$. Let M be the subinterval array of f. The following are equivalent:

1. A set of t columns $\{i_1, \ldots, i_t\}$ is **covered** in M.
2. There is **no row** r other than the all-zero row of M such that $r_{i_1} = \ldots = r_{i_t} = 0$.
3. The set $\{\alpha^{i_1}, \ldots, \alpha^{i_t}\}$ is **linearly independent** over $\mathbb{F}_q$.

- Each nonzero t-tuple of $\mathbb{F}_q$ appears **once** per period of an LFSR.
- Each set of t **consecutive columns** of the subinterval array M of f has the coverage property.

Theorem (S. Raaphorst, L. Moura, B. Stevens, 2014)

Let f be a primitive polynomial over $\mathbb{F}_q$ of degree t and $\alpha \in \mathbb{F}_{q^t}$ a root of f. Define $k = \frac{q^t-1}{q-1}$. Let M be the subinterval array of f. The following are equivalent:

1. A set of t columns $\{i_1, \ldots, i_t\}$ is **covered** in M.
2. There is **no row** r other than the all-zero row of M such that $r_{i_1} = \ldots = r_{i_t} = 0$.
3. The set $\{\alpha^{i_1}, \ldots, \alpha^{i_t}\}$ is **linearly independent** over $\mathbb{F}_q$.

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

$$000100110101111 \quad 0001001101\mathbf{01}1110$$

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

$$00010011010111\textcolor{red}{\mathbf{1}} \quad 0001001101\textcolor{blue}{\mathbf{01}}1110$$

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

$$000100110101111 \quad \textcolor{red}{\mathbf{0}}0010011010\textcolor{blue}{\mathbf{11}}110$$

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

000100110101111 000100110101111 0

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

$$000100110101111 \quad 00\textcolor{red}{\mathbf{0}}1001101011\textcolor{blue}{\mathbf{11}}0$$

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

$$000100110101111 \quad 000\mathbf{1}00110101111\mathbf{10}$$

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

00010011010111**1** **0001**001101**011110**

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

000**1001**1010111**1** **0001**001101011110

Let $f(x) = x^4 + x + 1$ be a primitive polynomial over $\mathbb{F}_2$. A period of the LFSR generated by f and 0001 is

$$000100110101111.$$

Let $\mathbf{k_1} = \mathbf{11} \in \mathbb{Z}_{15}$ such that $\alpha^{11}(\alpha - 1) = 1$.

0001001**10**101111   000**1001**101011110

Theorem

Let f be a primitive polynomial over $\mathbb{F}_q = \{0, \beta_1, \ldots, \beta_{q-1}\}$ of degree t with $\alpha \in \mathbb{F}_{q^t}$ a root of f. For $j = 1, \ldots, q-1$, let $k_j \in \mathbb{Z}_{q^t-1}$ such that $\alpha^{k_j}(\alpha - \beta_j) = 1$. Then

$$Tr(\alpha^{i+1}) - \beta_j Tr(\alpha^i) = Tr(\alpha^{i-k_j})$$

for all $i \geq 0$.

Let $f(x) = x^4 + 2x + 2$ be a primitive polynomial over $\mathbb{F}_3$ and $\alpha \in \mathbb{F}_{81}$ be a root of f.

- $S(f, 1000) = (Tr(\alpha^i))_{i \geq 0}$.
- $\alpha^{27}(\alpha - 1) = 1$, $\mathbf{k_1 = 27}$
- $\alpha^{76}(\alpha - 2) = 1$, $\mathbf{k_2 = 76}$

1000100110121100210201221010111122201121

2000200220212200120102112020222211102212.

Let $f(x) = x^4 + 2x + 2$ be a primitive polynomial over $\mathbb{F}_3$ and $\alpha \in \mathbb{F}_{81}$ be a root of f.

- $S(f, 1000) = (Tr(\alpha^i))_{i \geq 0}$.
- $\alpha^{27}(\alpha - 1) = 1$, $\mathbf{k_1 = 27}$
- $\alpha^{76}(\alpha - 2) = 1$, $\mathbf{k_2 = 76}$

100010011012110021020122101**011112**2201121

200020022021220012010211202022221102212.

Let $f(x) = x^4 + 2x + 2$ be a primitive polynomial over $\mathbb{F}_3$ and $\alpha \in \mathbb{F}_{81}$ be a root of f.

- $S(f, 1000) = (Tr(\alpha^i))_{i \geq 0}$.
- $\alpha^{27}(\alpha - 1) = 1$, $\mathbf{k_1 = 27}$
- $\alpha^{76}(\alpha - 2) = 1$, $\mathbf{k_2 = 76}$

100010011012110021020122101**011112**2201121

2000200220212**2001**2010211202022221102212.

Let $f(x) = x^4 + 2x + 2$ be a primitive polynomial over $\mathbb{F}_3$ and $\alpha \in \mathbb{F}_{81}$ be a root of f.

- $S(f, 1000) = (Tr(\alpha^i))_{i \geq 0}$.
- $\alpha^{27}(\alpha - 1) = 1$, $\mathbf{k_1 = 27}$
- $\alpha^{76}(\alpha - 2) = 1$, $\mathbf{k_2 = 76}$

1000100110121100210201221 0**101**11122201121

2000200220212**2001**20102112020222211102212.

Let $f(x) = x^4 + 2x + 2$ be a primitive polynomial over $\mathbb{F}_3$ and $\alpha \in \mathbb{F}_{81}$ be a root of f.

- $S(f, 1000) = (Tr(\alpha^i))_{i \geq 0}$.
- $\alpha^{27}(\alpha - 1) = 1$, $\mathbf{k_1 = 27}$
- $\alpha^{76}(\alpha - 2) = 1$, $\mathbf{k_2 = 76}$

1000100110121100210201221010111122201121

20002002202122001201021120202222111**02212**

- Let $f(x) = x^4 + 2x + 2$ be a primitive polynomial over $\mathbb{F}_3$ and α a root of f.
- Label the columns of the subinterval array M of f by $\mathbb{Z}_{40} = \{0, 1, \ldots, 39\}$.
- Let $k_1 = 27 \in \mathbb{Z}_{40}$ such that $\alpha^{27}(\alpha - 1) = 1$.
- Let $k_2 = 36 \in \mathbb{Z}_{40}$ such that $2\alpha^{36}(\alpha - 1) = 1$.

2	3	$3 + k_1 = 30$	$3 + k_2 = 39$
1	4	$3 + 2k_1 = 17$	$3 + 2k_2 = 35$
0	5	$3 + 3k_1 = 4$	$3 + 3k_2 = 31$

$$OOA(4,4,3,3) = [0\ 1\ 2 \mid 5\ 4\ 3 \mid 4\ 17\ 30 \mid 31\ 35\ 39]$$

Antiideal $\{3, 30, 17, 39\}$

$\mathbf{k_1 = 27}$

$$021 \; \overset{\mathbf{3}}{\downarrow}\!\!\!\!\!\!\;\; \color{blue}{\mathbf{0}} \; 20122101011112220112120002 \; \overset{\mathbf{30}}{\color{blue}{\mathbf{0}}} \; 022021220$$

$\mathbf{k_2 = 36}$

Antiideal $\{3, 30, 17, 39\}$
$\mathbf{k_1 = 27}$

$$021\ \overset{\mathbf{3}}{\underset{}{\mathbf{0}}}\ 2012210101111\ \overset{\mathbf{17}}{\mathbf{2}}\ 220112120002\ \overset{\mathbf{30}}{\mathbf{0}}\ 022021220$$

$\mathbf{k_2 = 36}$

Antiideal $\{3, 30, 17, 39\}$

$\mathbf{k_1 = 27}$

$\mathbf{k_2 = 36}$

$$021 \; \overset{\mathbf{3}}{\overset{\downarrow}{\color{blue}\mathbf{0}}} \; 20122101011112220112120002002202122 \; \overset{\mathbf{39}}{\overset{\downarrow}{\color{blue}\mathbf{0}}}$$

Antiideal $\{3, 30, 17, 39\}$

$\mathbf{k_1 = 27}$

$\mathbf{k_2 = 36}$

$$021\ \overset{3}{\downarrow}\!\!\!\!\!\!\quad \mathbf{0}\ 2012210101111222011212000200220\ \overset{35}{\downarrow}\!\!\!\!\!\!\quad \mathbf{2}\ 122\ \overset{39}{\downarrow}\!\!\!\!\!\!\quad \mathbf{0}$$

Antiideal $\{3, 30, 17, 39\}$

$\mathbf{k_1 = 27}$

$\mathbf{k_2 = 36}$

$$021\ \overset{\mathbf{3}}{\underset{\displaystyle\mathbf{0}}{\downarrow}}\ 2012210101111\ \overset{\mathbf{17}}{\underset{\displaystyle\mathbf{2}}{\downarrow}}\ 220112120002\ \overset{\mathbf{30}}{\underset{\displaystyle\mathbf{0}}{\downarrow}}\ 022021220$$

$$021\ \overset{\mathbf{3}}{\underset{\displaystyle\mathbf{0}}{\downarrow}}\ 2012210101111222011212000200220\ \overset{\mathbf{35}}{\underset{\displaystyle\mathbf{2}}{\downarrow}}\ 122\ \overset{\mathbf{39}}{\underset{\displaystyle\mathbf{0}}{\downarrow}}$$

Theorem

For q a prime power and $t \geq 2$, there exists an $OOA(t, q+1, t-1, q)$.

Sketch of the proof:

- Let $f(x) = \sum_{i=0}^{t} c_i x^i$ be a primitive polynomial over $\mathbb{F}_q = \{0, \beta_1, \ldots, \beta_{q-1}\}$ and α a root of f.
- Label the columns of the subinterval array M of f by $\mathbb{Z}_k = \{0, 1, \ldots, k-1\}$, where $k = \frac{q^t - 1}{q-1}$.
- For each $j = 1, \ldots, q-1$, let $k_j \in \mathbb{Z}_k$ such that $\tau_j \alpha^{k_j}(\alpha - \beta_j) = 1$, $\tau_j \in \mathbb{F}_q$.

Choose the columns of M labeled by

$$
\begin{array}{lll}
t-2 & t-1 & (t-1)+k_j \\
t-3 & t & (t-1)+2k_j \\
\vdots & \vdots & \vdots \\
1 & 2t-4 & (t-1)+(t-2)k_j \\
0 & 2t-3 & (t-1)+(t-1)k_j
\end{array}
$$

where $j = 1, \ldots, q-1$.

Let $k_i \in \mathbb{Z}_{q^t-1}$ such that $\alpha^{k_i}(\alpha - \beta_i) = 1$. For $0 \leq l \leq t-2$, suppose that

$$z\underbrace{0\ldots0}_{l}z_0z_1\ldots z_{t-l-2} \quad \longrightarrow^{k_i} \quad \overbrace{w\underbrace{0\ldots0}_{l+1}z_0w_1\ldots w_{t-l-3}}^{t}w_{t-l-2}$$

$$p(x) = -c_0z + \sum_{r=0}^{t-l-3}\Big(z_{t-l-2-r} + \sum_{j=l+2+r}^{t-1} c_jz_{j-l-2-r}\Big)x^{r+1} + z_0x^{t-l-1}$$

Given a run of zeroes of length l, a run of zeroes of length $l+1$ is reached by counting ahead k_i positions if and only if β_i is a root of p.

Let $k_i \in \mathbb{Z}_{q^t-1}$ such that $\alpha^{k_i}(\alpha - \beta_i) = 1$. For $0 \leq l \leq t-2$, suppose that

$$z\underbrace{0\ldots0}_{l}z_0 z_1 \ldots z_{t-l-2} \quad \longrightarrow^{k_i} \quad \overbrace{w\underbrace{0\ldots0}_{l+1}z_0 w_1 \ldots w_{t-l-3}\,w_{t-l-2}}^{t}$$

$$p(x) = -c_0 z + \sum_{r=0}^{t-l-3}\Big(z_{t-l-2-r} + \sum_{j=l+2+r}^{t-1} c_j z_{j-l-2-r}\Big)x^{r+1} + z_0 x^{t-l-1}$$

Given a run of zeroes of length l, a run of zeroes of length $l+1$ is reached by counting ahead k_i positions if and only if β_i is a root of p.

Let $k_i \in \mathbb{Z}_{q^t-1}$ such that $\alpha^{k_i}(\alpha - \beta_i) = 1$. For $0 \leq l \leq t-3$, suppose that

$$z\underbrace{0\ldots0}_{l}z_0z_1\ldots z_{t-l-2} \quad \xrightarrow{k_i} \quad \overbrace{w\underbrace{0\ldots0}_{l+1}z_0w_1\ldots w_{t-l-3}}^{t}w_{t-l-2}$$

$$\xrightarrow{k_i} \quad \overbrace{y\underbrace{0\ldots0}_{l+2}z_0y_1\ldots y_{t-l-4}}^{t}y_{t-l-3}$$

$$p_1(x) = -c_0w + \sum_{r=0}^{t-l-4}\Big(w_{t-l-3-r} + \sum_{j=l+3+r}^{t-1} c_jw_{j-l-3-r}\Big)x^{r+1} + z_0x^{t-l-2}$$

Therefore $p(x) = (x - \beta_i)p_1(x)$.
The number of runs of zeroes that is reached by counting ahead k_i positions from a fixed run of zeroes is equal to the multiplicity of β_i as a root of $p(x)$.

Let $k_i \in \mathbb{Z}_{q^t-1}$ such that $\alpha^{k_i}(\alpha - \beta_i) = 1$. For $0 \leq l \leq t-3$, suppose that

$$z\underbrace{0\ldots0}_{l}z_0z_1\ldots z_{t-l-2} \quad \xrightarrow{}^{k_i} \quad \overbrace{w\underbrace{0\ldots0}_{l+1}z_0w_1\ldots w_{t-l-3}}^{t}w_{t-l-2}$$

$$\xrightarrow{}^{k_i} \quad \overbrace{y\underbrace{0\ldots0}_{l+2}z_0y_1\ldots y_{t-l-4}}^{t}y_{t-l-3}$$

$$p_1(x) = -c_0w + \sum_{r=0}^{t-l-4}\left(w_{t-l-3-r} + \sum_{j=l+3+r}^{t-1} c_jw_{j-l-3-r}\right)x^{r+1} + z_0x^{t-l-2}$$

Therefore $p(x) = (x-\beta_i)p_1(x)$.
The number of runs of zeroes that is reached by counting ahead k_i positions from a fixed run of zeroes is equal to the multiplicity of β_i as a root of $p(x)$.

Thank you!