# Construction of covering arrays from m-sequences

Georgios Tzanakis [1]

Joint work with L. Moura [2] and D. Panario [1]

Carleton University [1]

University of Ottawa [2]

December 5, 2013

WORK IN PROGRESS

# Outline of talk

# Outline of talk

# Definition of covering arrays

A covering array $CA(N; t, k, v)$ is a $N \times k$ array with entries from an alphabet of size $v$, with the property that any $N \times t$ sub-array has at least one row equal to every possible $t$-tuple.

# Definition of covering arrays

A covering array $CA(N; t, k, v)$ is a $N \times k$ array with entries from an alphabet of size $v$, with the property that any $N \times t$ sub-array has at least one row equal to every possible $t$-tuple.

## Example

A covering array $CA(13; 3, 10, 2)$

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 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 of covering arrays

A covering array $CA(N; t, k, v)$ is a $N \times k$ array with entries from an alphabet of size $v$, with the property that any $N \times t$ sub-array has at least one row equal to every possible $t$-tuple.

**Example**

A covering array $CA(13; 3, 10, 2)$

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 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 of covering arrays

A covering array $CA(N; t, k, v)$ is a $N \times k$ array with entries from an alphabet of size $v$, with the property that any $N \times t$ sub-array has at least one row equal to every possible $t$-tuple.

**Example**

A covering array $CA(9; 2, 4, 3)$

| | | | |
|---|---|---|---|
| 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 of covering arrays

A covering array $CA(N; t, k, v)$ is a $N \times k$ array with entries from an alphabet of size $v$, with the property that any $N \times t$ sub-array has at least one row equal to every possible $t$-tuple.

**Example**

A covering array $CA(9; 2, 4, 3)$

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

# Outline of talk

# Research on covering arrays

1. Bounds on number of rows
2. Combinatorial and algebraic constructions
3. Computer-generated constructions
4. Recursive constructions

# Research on covering arrays

1. Bounds on number of rows
2. Combinatorial and algebraic constructions
3. Computer-generated constructions
4. Recursive constructions

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Colbourn, '04

*"Lower bounds are in general not well explored..."*

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Elementary counting arguments

- $v^t \leq CAN(t, k, v) \leq v^k$
- $CAN(t-1, k-1, v) \leq \frac{1}{v} CAN(t, k, v)$
- If $k_1 < k_2$ then $CAN(t, k_1, v) < CAN(t, k_2, v)$
- ...

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Case $t = 2, v = 2$

- Kleitman and Spencer '73; Katona '73

$$CAN(2, k, 2) = \min\left\{N \in \mathbb{N};\ k \leq \binom{N-1}{\lceil \frac{N}{2} \rceil}\right\}$$

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Case $t = 2, v > 2$

- Gargano, Körner, Vacarro '90

$$CAN(2, k, v) = \frac{v}{2} \log K(1 + o(1))$$

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Recursive results

- $CAN(2, kq + 1, q) \leq CAN(2, k, q) + q^2 - q$
- $CAN(2, k(q + 1), q) \leq CAN(2, k, q) + q^2 - 1$
- $CAN(3, 2k, v) \leq CAN(3, k, v) + (v - 1)CAN(2, k, v)$
- ...

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Asymptotic results

- $CAN \leq \frac{(t-1)\log k}{\log\left(\frac{v^t}{v^t-1}\right)}(1 + O(1))$
- $CAN(t, k, 2) \leq 2^t t^{O(\log t)} \log k$
- $\frac{CAN(2,k,v)}{\log k} \longrightarrow \frac{1}{2}v$
- ...

# Research on covering arrays

## 1. Bounds on number of rows

### Definition

The covering array number $CAN(t, k, v)$ is the smallest possible $N$ such that a $CA(N; t, k, v)$ exists

### Online repositories

- Colbourn
- NIST
- Torres-Jimenez
- Sherwood

# Research on covering arrays

1. Bounds on number of rows
2. Combinatorial and algebraic constructions
3. Computer-generated constructions
4. Recursive constructions

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

## 2. Algebraic and combinatorial constructions

- Results on orthogonal arrays (using MOLS, Hadamard matrices, finite fields . . . )
- Optimal $CA(N; 2, k, 2)$'s for all $k$ (Kleitman, Spencer '73; Katona '73)
- Using group divisible designs (Stevens, Ling, Mendelsohn '02)
- Using group actions
  - strength 3 (Chateauneuf, Colbourn, Kreher '02)
  - strength 2 (Meagher, Stevens '05)
- Using trinomial coefficients (Martinez-Pena, Torres-Jimenez '10)
- Using m-sequences (Raaphorst, Moura, Stevens '13)
- Survey: Colbourn '04

# Research on covering arrays

1. Bounds on number of rows
2. Combinatorial and algebraic constructions
3. Computer-generated constructions
4. Recursive constructions

# Research on covering arrays

1. Bounds on number of rows
2. Combinatorial and algebraic constructions
3. Computer-generated constructions
    - Greedy algorithms
    - Metaheurstic algorithms
4. Recursive constructions

# Research on covering arrays

1. Bounds on number of rows
2. Combinatorial and algebraic constructions
3. Computer-generated constructions
4. Recursive constructions

# Outline of talk

# Motivation

- Elegant combinatorial object
- Software testing
- Hardware testing
- Biology
- Industrial processes

# Outline of talk

# Definition of linear recurrence sequences

## Definition

A sequence $a_i$, $i = 0, 1, 2, \ldots$ is a linear recurrence sequence of order $n$ over $\mathbb{F}_q$ if it satisfies

$$a_{i+n} = \sum_{j=0}^{n-1} c_j a_{i+j}, \; i \geq 0$$

for some $c_j \in \mathbb{F}_q$ and initial values $a_0, \ldots, a_{n-1}$

## Example

00101211201110020212210222 0010121 $\ldots$ over $\mathbb{F}_3$ is produced by

$$a_{i+3} = a_{i+1} + 2a_i$$

and initial conditions $a_0 = 0, a_1 = 0, a_2 = 1$

# Definition of linear recurrence sequences

## Definition

A sequence $a_i,\ i = 0, 1, 2, \ldots$ is a linear recurrence sequence of order $n$ over $\mathbb{F}_q$ if it satisfies

$$a_{i+n} = \sum_{j=0}^{n-1} c_j a_{i+j},\ \ i \geq 0$$

for some $c_j \in \mathbb{F}_q$ and initial values $a_0, \ldots, a_{n-1}$

## Example

00101211201110020212210222 0010121 ... over $\mathbb{F}_3$ is produced by

$$a_{i+3} = a_{i+1} + 2a_i$$

and initial conditions $a_0 = 0, a_1 = 0, a_2 = 1$

# Outline of talk

# m-sequences and primitive elements

## Definition

A linear recurrence sequence of order $n$ over $\mathbb{F}_q$ and period $q^n - 1$ is called an m-sequence

m-sequences correspond to primitive polynomials

$$a_{i+n} = \sum_{j=0}^{n-1} c_i a_{i+j}, \; i \geq 0$$

$$x^n - \sum_{j=0}^{n-1} c_j x^j \longleftrightarrow \alpha^k, (k, q^n - 1) = 1$$

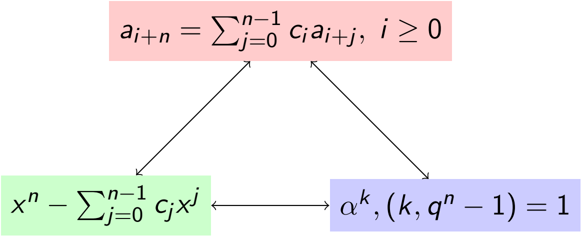
where $\alpha$ is a fixed primitive element of $\mathbb{F}_{q^n}$

# m-sequences and primitive elements

## Definition

A linear recurrence sequence of order $n$ over $\mathbb{F}_q$ and period $q^n - 1$ is called an m-sequence

## m-sequences correspond to primitive polynomials




where $\alpha$ is a fixed primitive element of $\mathbb{F}_{q^n}$

# Outline of talk

# Our work in a nutshell

- Long term goal: give an algebraic construction for covering arrays $CA(N; t, k, q)$ for general strength $t$ and prime powers $q$
- Short term goal: give an algebraic construction when
  - strength $t = 4$
  - rows $N = 2(q^n - 1) + 1$
  - any $q$
- What we have:
  - A method and a backtracking algorithm in SAGE
  - Hints about an algebraic construction

# Our work in a nutshell

- Long term goal: give an algebraic construction for covering arrays $CA(N; t, k, q)$ for general strength $t$ and prime powers $q$
- Short term goal: give an algebraic construction when
  - strength $t = 4$
  - rows $N = 2(q^n - 1) + 1$
  - any $q$
- What we have:
  - A method and a backtracking algorithm in SAGE
  - Hints about an algebraic construction

# Our work in a nutshell

- Long term goal: give an algebraic construction for covering arrays $CA(N; t, k, q)$ for general strength $t$ and prime powers $q$
- Short term goal: give an algebraic construction when
  - strength $t = 4$
  - rows $N = 2(q^n - 1) + 1$
  - any $q$
- What we have:
  - A method and a backtracking algorithm in SAGE
  - Hints about an algebraic construction

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

$q = 3,\ t = 3,\ f(x) = x^3 + 2x + 1$

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 |
| 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 |
| 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 |
| 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 |
| 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 |
| 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 |
| 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 |
| 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 |
| 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 |
| 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 |
| 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 |
| 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 |
| 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 |
| 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 |
| 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 |
| 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 |
| 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 |
| 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 |
| 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 |
| 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 |
| 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 |
| 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 |
| 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 |

$q = 3,\ t = 3,\ f(x) = x^3 + 2x + 1$

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 |
| 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 |
| 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 |
| 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 |
| 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 |
| 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 |
| 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 |
| 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 |
| 2 | 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 |
| 1 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 |
| 0 | 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 |
| 0 | 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 |
| 2 | 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 |
| 0 | 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 |
| 2 | 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 |
| 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 |
| 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 |
| 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 |

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

$q = 3, \ t = 3, \ g(x) = x^3 + x^2 + 2x + 1$

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 |
| 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 |
| 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 |
| 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 |
| 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 |
| 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 |
| 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 |
| 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 |
| 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 |
| 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 |
| 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 |
| 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 |
| 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 |
| 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 |
| 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 |
| 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 |
| 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 |
| 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 |
| 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 |
| 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 |
| 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 |
| 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 |
| 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 |
| 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 |

$$q = 3,\ t = 3,\ g(x) = x^3 + x^2 + 2x + 1$$

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 |
| 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 |
| 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 |
| 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 |
| 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 |
| 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 |
| 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 |
| 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 |
| 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 |
| 1 | 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 |
| 0 | 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 |
| 0 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 |
| 2 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 |
| 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 |
| 2 | 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 |
| 0 | 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 |
| 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 |
| 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 |
| 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 |
| 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 |
| 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 |
| 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 |
| 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 |

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 |
| 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 |
| 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 |
| 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 |
| 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 |
| 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 |
| 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 |
| 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 |
| 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 |
| 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 |
| 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 |
| 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 |
| 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 |
| 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 |
| 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 |
| 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 |
| 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 |
| 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 |
| 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 |
| 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 |
| 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 |
| 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 |
| 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 |
| 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 |
| 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 |
| 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 |
| 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 |
| 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 |
| 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 |
| 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 |
| 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 |
| 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 |
| 1 | 0 | 2 | 1 | 2 | 2 | 2 | 1 | 0 | 0 | 2 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 0 | 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 |
| 1 | 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 |
| 1 | 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 |
| 1 | 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 |
| 2 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 2 | 1 | 2 | 2 | 2 |
| 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 |
| 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 |
| 0 | 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 |
| 2 | 1 | 1 | 2 | 1 | 0 | 1 | 0 | 0 | 2 | 2 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 1 | 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 |
| 2 | 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 |
| 2 | 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 |
| 1 | 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 |
| 2 | 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 |
| 0 | 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 |
| 2 | 0 | 0 | 1 | 1 | 1 | 0 | 2 | 1 | 1 | 2 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 2 | 1 | 2 | 1 |
| 0 | 1 | 1 | 1 | 2 | 2 | 0 |
| 1 | 0 | 0 | 2 | 2 | 2 | 0 |
| 1 | 1 | 2 | 2 | 2 | 1 | 2 |
| 0 | 0 | 1 | 2 | 1 | 0 | 2 |
| 1 | 2 | 2 | 1 | 0 | 0 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 0 | 2 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 2 | 1 | 2 | 1 | 1 | 0 | 2 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 1 | 2 | 0 | 0 | 1 | 0 | 2 |
| 1 | 0 | 1 | 1 | 0 | 2 | 2 |
| 2 | 0 | 1 | 0 | 2 | 1 | 2 |
| 0 | 1 | 1 | 1 | 1 | 2 | 1 |
| 0 | 1 | 0 | 1 | 2 | 1 | 0 |
| 1 | 1 | 2 | 2 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 | 2 |
| 1 | 2 | 1 | 0 | 1 | 0 | 2 |
| 0 | 1 | 2 | 1 | 0 | 0 | 2 |
| 2 | 1 | 1 | 0 | 0 | 2 | 0 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 1 | 2 | 2 | 0 | 0 | 1 | 0 |
| 2 | 1 | 0 | 0 | 1 | 1 | 2 |
| 2 | 2 | 2 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 2 | 2 | 0 | 1 | 0 | 2 | 2 |
| 0 | 0 | 1 | 0 | 2 | 1 | 1 |
| 2 | 0 | 1 | 2 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros.
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

# Our method

1. Choose a prime power $q$ for the alphabet
2. Choose a strength $t$ and pick two primitive polynomials $f, g$ over $\mathbb{F}_q$ of degree $t$
3. Form an array by taking all the shifts of the m-sequence associated to $f$ as rows and then only consider the first $\frac{q^n-1}{q-1}$ columns
4. Form the same kind of array using $g$
5. Concatenate vertically the two arrays and a row of zeros.
6. Choose appropriate columns from the resulting array so that the subarray they form is a covering array

# Outline of talk

# Some obtained covering arrays

## and interesting points

$CA(161; 4, 10, 3)$

- Comparison with Colbourn's tables:

| | $N$ | $t$ | $k$ | $v$ |
|---|---|---|---|---|
| Best known | 159 | 4 | 10 | 3 |
| Us | 161 | 4 | 10 | 3 |
| Best known | 183 | 4 | 11 | 3 |

- Choice of columns: [0,8,16,24,32] along with [1,9,17,25,33] or [3,11,19,27,35]
- Columns are the multiples of $2(q+1)$ and shifts

# Some obtained covering arrays

## and interesting points

$CA(511; 4, 17, 4)$

- Comparison with Colbourn's tables:

| | $N$ | $t$ | $k$ | $v$ |
|---|---|---|---|---|
| Best known | 508 | 4 | 13 | 4 |
| Us | 511 | 4 | 17 | 4 |
| Best known | 760 | 4 | 20 | 4 |

- Has a place in Colbourn's tables
- Choice of columns: [0,5,10,15,20,25,. . . ,70,75,80]
- Columns are the multiples of $q + 1$

# Some obtained covering arrays

## and interesting points

$CA(1249; 4, 15, 5)$

- Comparison with Colbourn's tables:

| | $N$ | $t$ | $k$ | $v$ |
|---|---|---|---|---|
| Best known | 1245 | 4 | 15 | 5 |
| Us | 1249 | 4 | 15 | 5 |
| Best known | 1865 | 4 | 24 | 5 |

- Search not complete
- Choice of columns: $[0,12,24,36,\ldots,132,144] + 2$ other
- Most columns are the multiples of $2(q+1)$

# Some obtained covering arrays

## and interesting points

### Choice of columns

Connection with multiples of $q+1$

### Pairs $f, g$ of primitive polynomials for $q = 4$

- Fix primitive $\alpha \in \mathbb{F}_{q^n}$.
- Find $k, m$ such that $f(\alpha^k) = 0$, $g(\alpha^m) = 0$
- Let $H = Z_{255}^{*} / < 4 >$
- $f, g$ work in our construction iff $\mathrm{ord}_H(k) = 8$ and $\mathrm{ord}_H(m) \neq 8$.

# Outline of talk

# Future work

## Ongoing

- Improve our backtracking algorithm
- Characterize the choices for the pairs of primitive polynomials
- Understand the choice of columns

## Long term

- Generalize the construction as much as possible