Analysis and computation of the multidimensional linear complexity of periodic arrays

Luis Quiñones, Jaziel Torres, Rafael Arce, José Ortiz, Ivelisse Rubio

University of Puerto Rico at Río Piedras

Table of contents

Preliminaries

Multidimensional array

- Arrays with two or more dimensions with entries in a finite field.
- Sequences are one dimensional arrays.
- We associate the entries with monomials, using coordinates as in the first quadrant of the plane.

$$A = \begin{array}{|c|c|c|c|} \hline & \vdots & & \\ \hline x^0y^2 & x^1y^2 & x^2y^2 & \\ \hline x^0y^1 & x^1y^1 & x^2y^1 & \cdots \\ \hline x^0y^0 & x^1y^0 & x^2y^0 & \\ \hline \end{array}$$

Multidimensional array

- Arrays with two or more dimensions with entries in a finite field.
- Sequences are one dimensional arrays.
- We associate the entries with monomials, using coordinates as in the first quadrant of the plane.

$$A = \begin{array}{|c|c|c|c|} \hline & \vdots & & \\ \hline y^2 & xy^2 & x^2y^2 & \\ \hline y & xy & x^2y & \cdots \\ \hline 1 & x & x & \\ \hline \end{array}$$

Applications

- Multidimensional arrays are used in:
  - Digital watermarking [2]
  - Cryptography
  - Wireless communications
- Depending on the application, we want arrays with *good* properties
  - Correlation
  - **Linear complexity**

Multidimensional periodic arrays: Example

⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋰
D	E	F	D	E	F	D	E	F	⋯
A	B	C	A	B	C	A	B	C	⋯
D	E	F	D	E	F	D	E	F	⋯
A	B	C	A	B	C	A	B	C	⋯
D	E	F	D	E	F	D	E	F	⋯
A	B	C	A	B	C	A	B	C	⋯
D	E	F	D	E	F	D	E	F	⋯
A	B	C	A	B	C	A	B	C	⋯

Two-dimensional periodic array of period $(3, 2)$

Linear complexity

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

0	1	1	0	1

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

0 1 1 0 1 0 0

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

0	1	1	0	1	0	0	0

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

0 1 1 0 1 0 0 0 1 $\cdots$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence **s** of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

0 1 1 0 1 0 0 0 1 $\cdots$

Linear complexity of periodic sequences

- Degree of the minimal polynomial that generates the sequence

Binary sequence $\mathbf{s}$ of period 7:

0	1	1	0	1	0	0	$\cdots$
x^0	x^1	x^2	x^3	x^4	x^5	x^6	

Generator: $1 + x^2 + x^3 + x^4$

$$0\ 1\ 1\ 0 \implies \mathscr{L}(\mathbf{s}) = 4, \quad \mathscr{L}_n(\mathbf{s}) = 4/7$$

Linear complexity of periodic sequences

- $\mathscr{L}(\mathbf{s}) :=$ degree of minimal generating polynomial.
- **Normalized complexity:** $\mathscr{L}_n(\mathbf{s}) := \dfrac{\mathscr{L}(\mathbf{s})}{\text{period}}$
- We use the normalized complexity to compare different arrays.
- The multidimensional complexity is a generalization of the one dimensional case (sequences).
- **Definition:** $Val(A) :=$ set of all polynomials that generate the array.

Linear complexity of periodic sequences

- $\mathscr{L}(\mathbf{s}) :=$ degree of minimal generating polynomial.
- **Normalized complexity:** $\mathscr{L}_n(\mathbf{s}) := \dfrac{\mathscr{L}(\mathbf{s})}{\text{period}}$
- We use the normalized complexity to compare different arrays.
- The multidimensional complexity is a generalization of the one dimensional case (sequences).
- **Definition:** $\mathit{Val}(A) :=$ set of all polynomials that generate the array.
- Beware: The following is true if and only if we have a Gröbner basis for $\mathit{Val}(A)$.

Multidimensional linear complexity

Period (6,7)

$$A = \begin{array}{c|c|c|c|c|c|c} y^6 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline y^5 & 1 & 1 & 0 & 0 & 1 & 0 \\ \hline y^4 & 0 & 1 & 1 & 0 & 0 & 0 \\ \hline y^3 & 1 & 0 & 1 & 1 & 0 & 0 \\ \hline y^2 & 1 & 0 & 0 & 0 & 0 & 1 \\ \hline y & 0 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline\hline & 1 & x & x^2 & x^3 & x^4 & x^5 \end{array}$$

$$\mathit{Val}(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$$A = \begin{array}{c|ccccccc} y^6 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ y^5 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ y^4 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ y^3 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ y^2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ y & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{array}$$

$$Val(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$$A = \begin{array}{c|ccccccc} y^6 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ y^5 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ y^4 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ y^3 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ y^2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ y & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{array}$$

$$\mathit{Val}(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$$A = \begin{array}{c|ccccccc} y^6 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ y^5 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ y^4 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ y^3 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ y^2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ y & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{array}$$

$$Val(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$$A = \begin{array}{c|c|ccccccc} y^6 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ y^5 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ y^4 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ y^3 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ y^2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ y & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{array}$$

$$\mathit{Val}(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$A =$

y^6	0	0	1	0	1	1	0
y^5	1	1	0	0	1	0	1
y^4	0	1	1	0	0	0	0
y^3	1	0	1	1	0	0	1
y^2	1	0	0	0	0	1	1
y	0	0	0	1	1	0	0
1	0	1	0	1	0	1	0
	1	x	x^2	x^3	x^4	x^5	x^6

$$\mathit{Val}(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$A =$

y^6	0	0	1	0	1	1	0
y^5	1	1	0	0	1	0	1
y^4	0	1	1	0	0	0	0
y^3	1	0	1	1	0	0	1
y^2	1	0	0	0	0	1	1
y	0	0	0	1	1	0	0
1	0	1	0	1	0	1	0
	1	x	x^2	x^3	x^4	x^5	x^6

$$\mathit{Val}(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$$A = \begin{array}{c|ccccccc} y^6 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ y^5 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ y^4 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ y^3 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ y^2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ y & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ \hline & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{array}$$

$$\mathit{Val}(A) = \left\langle \begin{array}{c} X^6 + 1, \\ XY^3 + Y^3 + XY + X + Y + 1, \\ Y^4 + Y^3 + Y^2 + 1 \end{array} \right\rangle$$

Multidimensional linear complexity

Period (6,7)

$A =$

y^6	0	0	1	0	1	1	0
y^5	1	1	0	0	1	0	1
y^4	0	1	1	0	0	0	0
y^3	1	0	1	1	0	0	1
y^2	1	0	0	0	0	1	1
y	0	0	0	1	1	0	0
1	0	1	0	1	0	1	0
	1	x	x^2	x^3	x^4	x^5	x^6

$$\mathscr{L}(A) = 19 \qquad \mathscr{L}_n(A) = \frac{19}{42} \approx 0.45$$

Array construction: composition method

Composition method

- Used by Tirkel, Osborne and Hall [5]; generalized by Moreno and Tirkel [2].
- Two ingredients:
  - Shift sequence $\mathbf{t}$ of period n_1.
  - Column sequence $\mathbf{s}$ of period n_2.

Composition method

- Used by Tirkel, Osborne and Hall [5]; generalized by Moreno and Tirkel [2].
- Two ingredients:
  - Shift sequence $\mathbf{t}$ of period n_1.
  - Column sequence $\mathbf{s}$ of period n_2.

Sequences with good properties $\xRightarrow{\text{seems}}$ Arrays with good properties

Composition method

- Used by Tirkel, Osborne and Hall [5]; generalized by Moreno and Tirkel [2].
- Two ingredients:
  - Shift sequence $\mathbf{t}$ of period n_1.
  - Column sequence $\mathbf{s}$ of period n_2.

Sequences with good properties $\xRightarrow{\text{seems}}$ Arrays with good properties

$$\mathscr{L}_n(A) \approx \mathscr{L}_n(\mathbf{s})$$

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

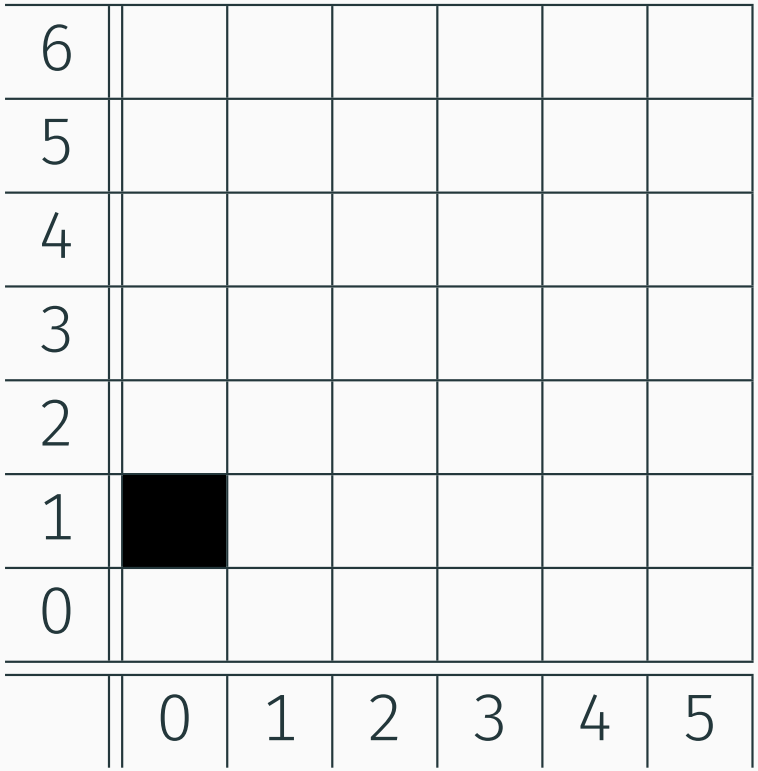
Column sequence: 0 1 1 0 1 0 0 ...

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

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

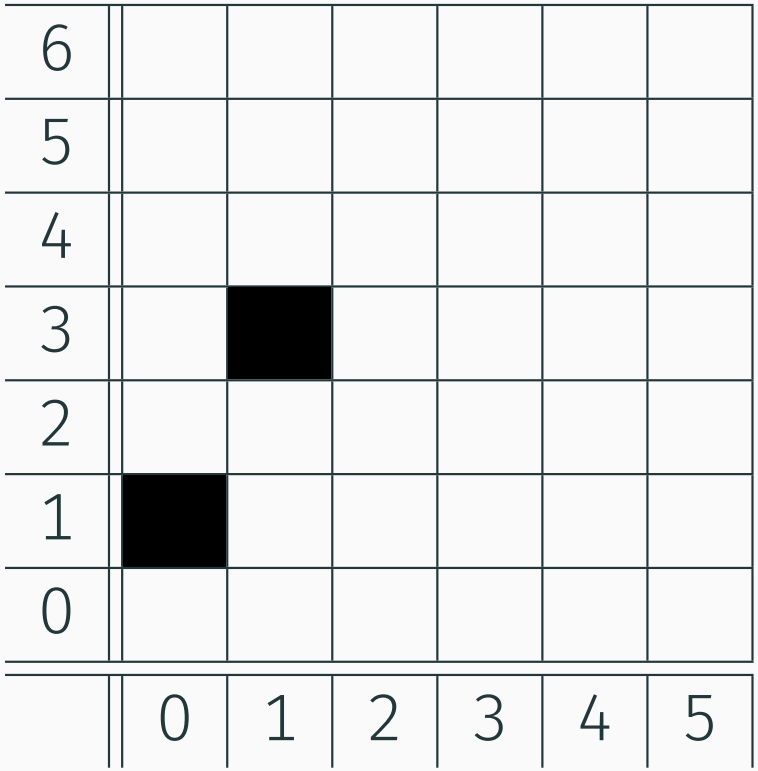
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

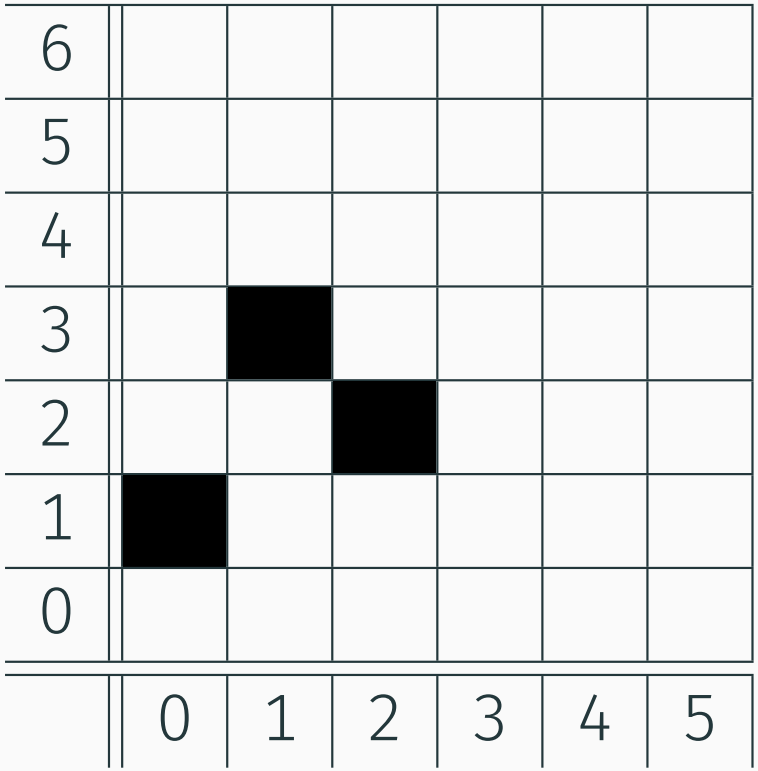
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

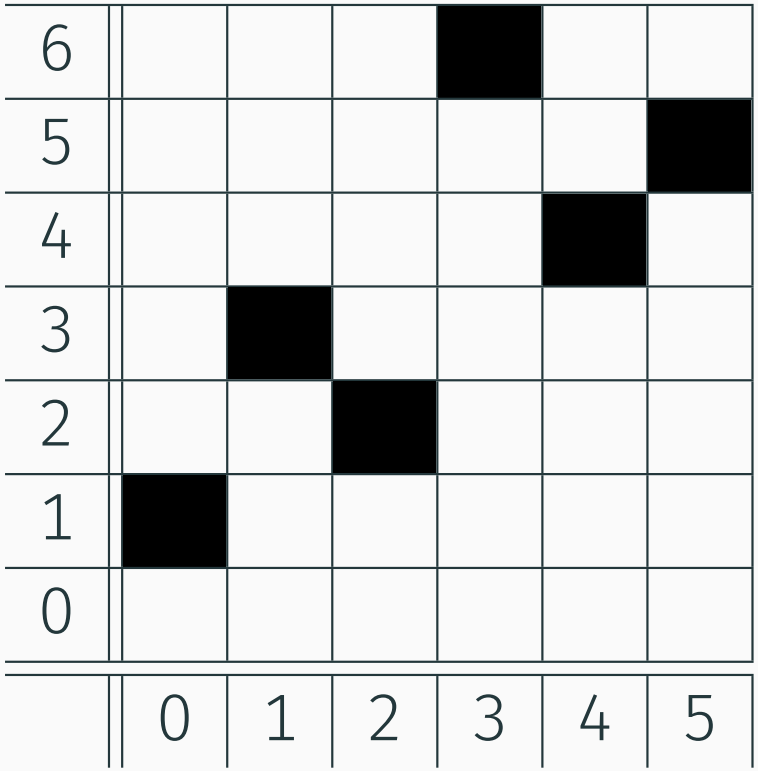
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

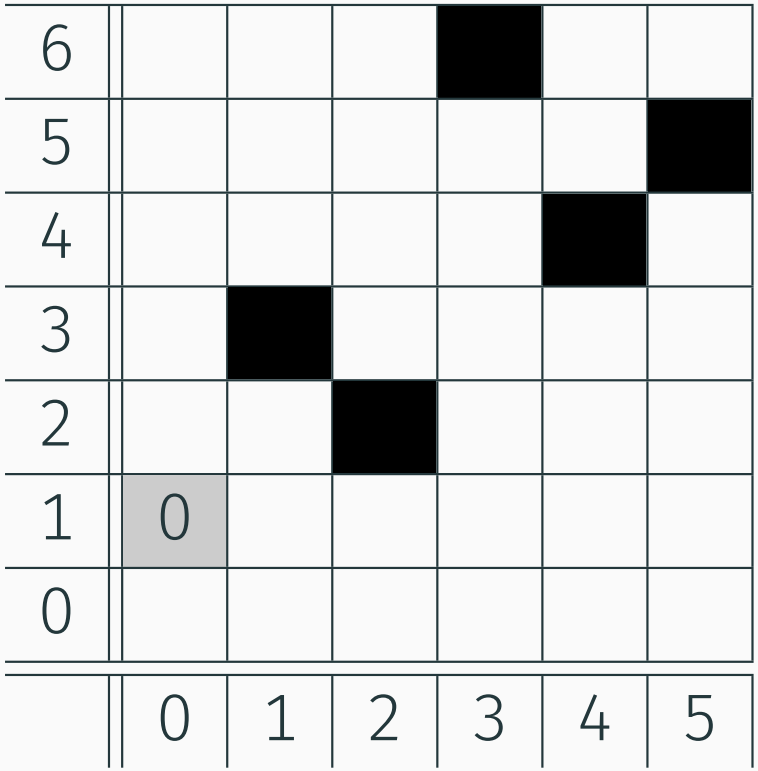
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

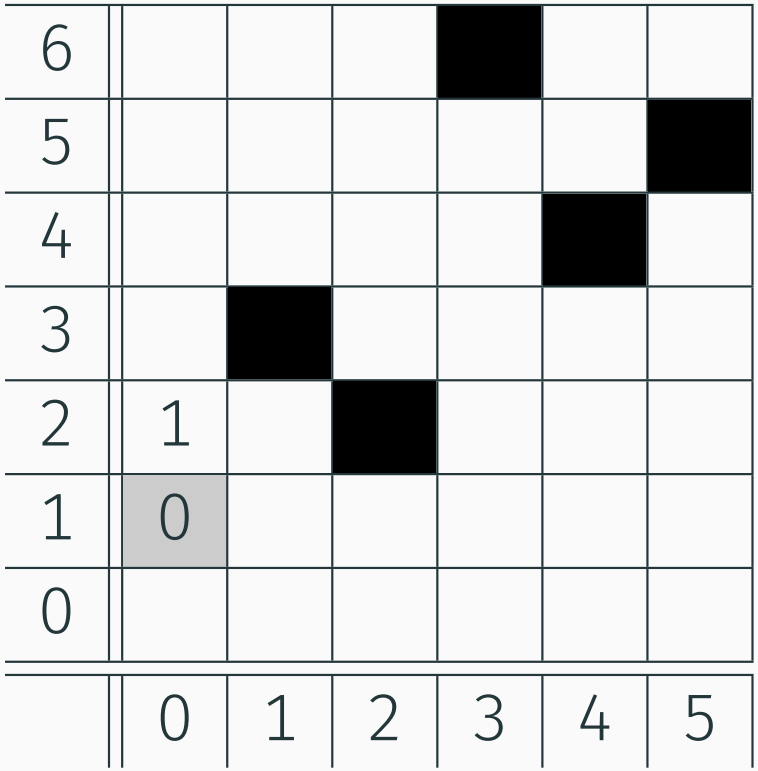
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

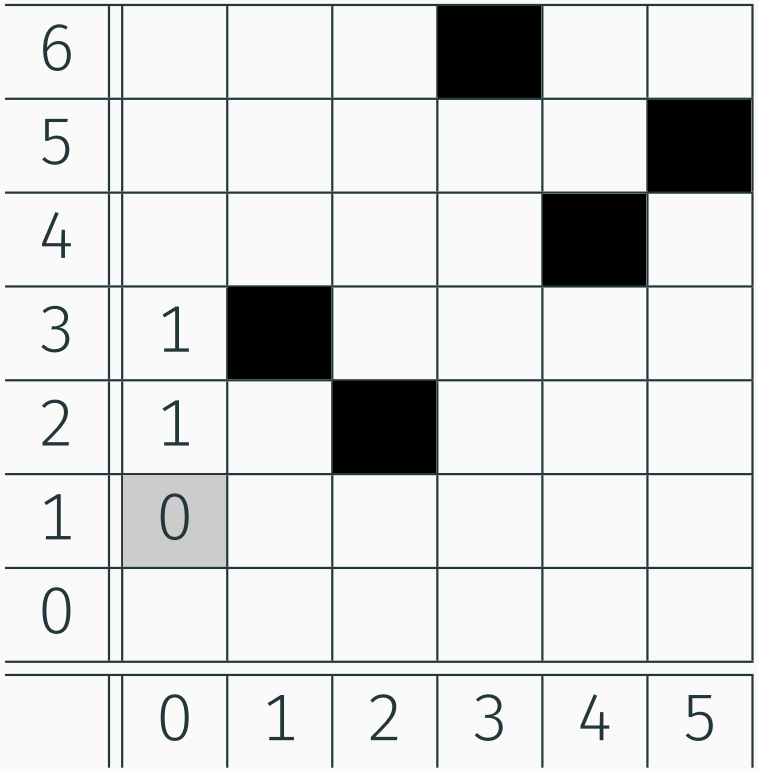
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

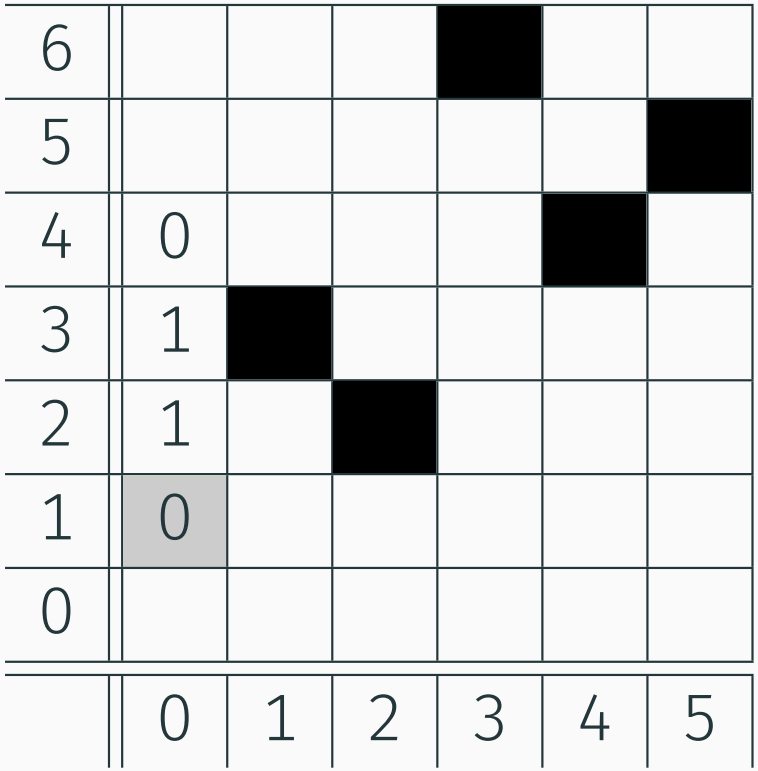
Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...



Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

Composition method: Example

Shift sequence: 1 3 2 6 4 5 ...

Column sequence: 0 1 1 0 1 0 0 ...

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

Main question

What is the multidimensional linear complexity of an array constructed by the method of composition?

Results from [1], generalized

Let A be an array constructed using the composition method with

- Shift sequence $\mathbf{t}$ over $\mathbb{Z}_d$ of period n_1.
- Column sequence $\mathbf{s}$ over $\mathbb{F}_q$ of period n_2 and minimal polynomial $\mu(y)$.

Theorem 1. $\mathscr{L}_n(A) \leqslant \mathscr{L}_n(\mathbf{s})$.

Theorem 2. If $\mu(y)$ is divisible by $y - 1$, then

$$\mathscr{L}_n(A) \leqslant \mathscr{L}_n(\mathbf{s}) - \frac{n_1 - 1}{n_1 n_2}.$$

Main question narrowed

What is the multidimensional linear complexity of an array constructed by the method of composition?

... with the Legendre sequence as column?

Thus, we study different shift sequences.

Legendre sequence

- Balanced binary sequence of period p with *good* correlation and complexity properties.

$$s_j = \begin{cases} 1 & j \text{ is a quadratic residue mod } p \\ 0 & j \text{ is a quadratic non-residue mod } p \\ 0 & j = 0 \end{cases}$$

Upper bound from Arce et al. [1]

Proposition

Let A be the array constructed by composition with the Legendre sequence with respect to p as the column sequence and a shift sequence $\mathbf{t}$ over $\mathbb{Z}_d$ with period n_1. Then, the normalized complexity of A, $\mathscr{L}_n(A)$ is:

$$\mathscr{L}_n(A) \leqslant \begin{cases} \mathscr{L}_n(\mathbf{s}) & p \equiv 1 \mod 4 \\ \mathscr{L}_n(\mathbf{s}) - \frac{n_1 - 1}{n_1 p} & p \equiv 3 \mod 4 \end{cases}.$$

In the case of equality, we say that A has **maximal complexity**.

The motivation

- Moreno et al. [1, 3] computed the linear complexity for some constructions, and all attained the bound.

The motivation

- Moreno et al. [1, 3] computed the linear complexity for some constructions, and all attained the bound.

Conjecture. For **any** shift sequence, A has maximal complexity. That is

$$\mathscr{L}_n(A) = \begin{cases} \mathscr{L}_n(\mathbf{s}) & p \equiv 1 \mod 4 \\ \mathscr{L}_n(\mathbf{s}) - \frac{n_1 - 1}{n_1 p} & p \equiv 3 \mod 4 \end{cases}.$$

The motivation

- Moreno et al. [1, 3] computed the linear complexity for some constructions, and all attained the bound.

Conjecture. For **any** shift sequence, A has maximal complexity. That is

$$\mathscr{L}_n(A) = \begin{cases} \mathscr{L}_n(\mathbf{s}) & p \equiv 1 \mod 4 \\ \mathscr{L}_n(\mathbf{s}) - \frac{n_1 - 1}{n_1 p} & p \equiv 3 \mod 4 \end{cases}.$$

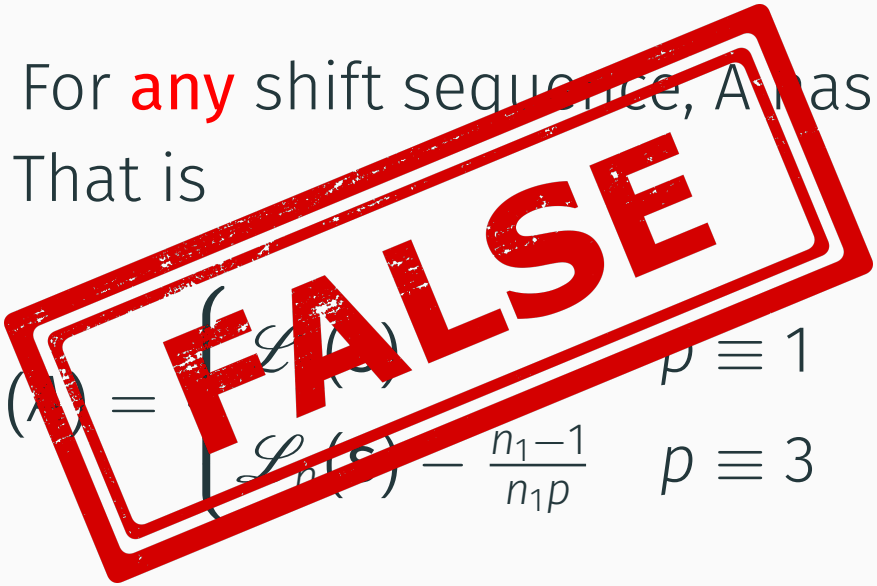
We have a short and dramatic answer...

The motivation

- ✳ Moreno et al. [1, 3] computed the linear complexity for some constructions, and all attained the bound.

Conjecture. For any shift sequence, A has maximal complexity. That is

$$\mathscr{L}_n(A) = \begin{cases} \mathscr{L}_n(S) & p \equiv 1 \mod 4 \\ \mathscr{L}_n(S) - \frac{n_1 - 1}{n_1 p} & p \equiv 3 \mod 4 \end{cases}.$$



We have a short and dramatic answer...

Results and conjectures by shift sequences

Shift sequence $t_i = i \mod q - 1$

- Legendre with respect to p.
- **Shift sequence:** $t_i = \log(\alpha^i) = i \mod q - 1$ over $\mathbb{F}_q$. Period $q - 1$.

1. Case $p \mid q - 1$:
   A **never has** maximal complexity.
2. Case $p \nmid q - 1$:
   A **has** maximal complexity.

Shift sequence $t_i = i \mod q - 1$

Theorem

Let A be the array constructed by composition with the Legendre sequence with respect to p as the column sequence and shift sequence $t_i = i \mod q - 1$ with period $n_1 = q - 1$, where q is a power of prime.

(1) If $p \nmid n_1$, then the normalized complexity of A, $\mathscr{L}_n(A)$ is:

$$\mathscr{L}_n(A) = \begin{cases} \mathscr{L}_n(\mathbf{s}) & p \equiv 1 \mod 4 \\ \mathscr{L}_n(\mathbf{s}) - \frac{n_1 - 1}{n_1 p} & p \equiv 3 \mod 4 \end{cases}.$$

(2) If $p \mid n_1$ then $\mathscr{L}_n(A) = \mathscr{L}_n(\mathbf{s})/n_1$.

Shift sequence $t_i = \alpha^i$

Shift sequence: $t_i = \alpha^i$, where α is a primitive element of $\mathbb{Z}_q$, q prime. Period $q - 1$.

1. Case $p \mid q - 1$:

   Conjecture: A **never has** maximal complexity.

2. Case $p \nmid q - 1$:

   2.1 $p = q$

   Conjecture: A **has** maximal complexity.

   2.2 $p \neq q$

   For some values of p and q, A has maximal complexity.

Shift sequence $t_i = A\alpha^{2i} + B\alpha^i + C$

Shift sequence (Exponential quadratic) **:**
$t_i = A\alpha^{2i} + B\alpha^i + C$, with $\alpha, A, B, C \in \mathbb{Z}_q$, q prime, and α primitive. Period $q - 1$.

1. Case $p \mid q - 1$:

   For some values of p and q, A has maximal complexity
2. Case $p \nmid q - 1$:

   2.1 $p = q$

   Conjecture: A **has** maximal complexity.

   2.2 $p \neq q$

   For some values of p and q, A has maximal complexity.

Summary of results

Case		Shift Sequence		
		$t_i = i \mod q-1$	$t_i = \alpha^i$	$t_i = \lambda\alpha^{2i} + \alpha^i$
$p \mid q-1$		Not maximal	*Not maximal?*	Inconsistent
$p \nmid q-1$	$p = q$	Maximal	*Maximal?*	*Maximal?*
	$p \neq q$	Maximal	Inconsistent	Inconsistent

** Conjectures in italics*

Ongoing and future work

Ongoing and future work

Ongoing:

- Prove all conjectures (trying).
- Study the other two shift sequences presented by Moreno and Trikel [3]:
  - Rational function characteristic p.
  - Rational function characteristic 2.
- Study all permutations of length $p-1$, p, and $p+1$ as shift sequence, composed with Legendre with respect to p.

Ongoing and future work

Future:

- Arrays in 3 or more dimensions.
- Study arrays composed with other column sequences:
  - Sidelnikov sequences [4], ternary Legendre sequences, m-sequences, and others.

References

[1] Rafael Arce-Nazario, Francis Castro, Domingo Gomez-Perez, Oscar Moreno, José Ortiz-Ubarri, Ivelisse Rubio, and Andrew Tirkel. Multidimensional linear complexity analysis of periodic arrays. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–21, 2019.

[2] Oscar Moreno and Andrew Tirkel. Multi-dimensional arrays for watermarking. In *2011 IEEE International Symposium on Information Theory Proceedings*, pages 2691–2695. IEEE, 2011.

[3] Oscar Moreno and Andrew Tirkel. New optimal low correlation sequences for wireless communications. In *International Conference on Sequences and Their Applications*, pages 212–223. Springer, 2012.

[4] V.M. Sidelnikov. Some k-valued pseudo-random sequences and nearly equidistant codes. *Probl. Inf. Transm.*, 5(1):12–16, 1969.

[5] Andrew Z Tirkel, Charles F Osborne, and Tom E Hall. Steganography-applications of coding theory. In *IEEE Information Theory Workshop, Svalbard, Norway*, pages 57–59, 1997.

Acknowledgements

Department of Computer Sciences, UPR-RP

PR Louis Stokes Alliance for Minority Participation

Questions are welcomed!

Thanks for your attention.

University of Puerto Rico, Río Piedras Campus

Picture from www.uprrp.edu