#CatedrasCiber

On the combinatorial properties of shrinking sequences

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Notation

We fix the following notation:

- $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and $\mathbb{F}_2 = \{0, 1\}$
- A *binary sequence* (s_i) is a mapping from $\mathbb{N}_0$ to $\mathbb{F}_2$
- A sequence is periodic if $s_{i+T} = s_i$, for all $i \in \mathbb{N}_0$.

Cyclic Linear Code

Definition

A linear code $\mathbf{C}$ of length $\mathbf{T}$ over $\mathbb{F}_2$ is called a **cyclic code** if for every codeword $(s_0, \ldots, s_{T-1})$, the word obtained by a cyclic shift to the right, $(s_{T-1}, s_0, \ldots, s_{T-2})$, is also a codeword in $\mathbf{C}$.

- Cyclic codes can be defined with a single generator vector $(s_0, \ldots, s_{T-1})$
- The main parameter that we investigate is *dimension*

Let L be a positive integer and $c_0, c_1, \ldots, c_{L-1} \in \mathbb{F}_2$. A binary sequence $s = (s_i)$ satisfying

$$s_{i+L} = \sum_{j=0}^{L-1} c_j s_{i+j}, \qquad (1)$$

for all $i \in \mathbb{N}_0$ is called an (L-th order) *linear recurring sequence (LRS)* and the monic polynomial

$$C(x) = x^L + \sum_{j=0}^{L-1} c_j x^j \in \mathbb{F}_2[x]$$

is the *characteristic polynomial* of the recurrence and we say that the sequence is generated by $C(x)$.

Correspondance between codes and sequences

- period $\iff$ length
- linear complexity $\iff$ dimension
- lattice structure $\iff$ minimum distance
- m-sequences $\iff$ $[2^n - 1, n]$ cyclic codes

Shrunken sequence

Given two m-sequences (a_i) and (b_i) with characteristic polynomials $p_1(x), p_2(x) \in \mathbb{F}_2[x]$ of degrees L_1 and L_2, with $\gcd(L_1, L_2) = 1$. The *shrinking generator* is the decimation of (b_i) by (a_i).

Example

$p_1(x) = x^2 + x + 1,\ p_2(x) = x^3 + x + 1$

1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
1	1	~~1~~	0	1	~~0~~	0	1	~~1~~	1	0	~~1~~	0	0	~~1~~	1	1	~~0~~	1
1	1		0	1		0	1		1	0		0	0		1	1		1

Facts about shrunken sequences

Theorem (Coppersmith et al., 93)

Given $p_1(x), p_2(x)$ *of degrees* L_1, L_2*, the corresponding shrunken sequence* $\mathbf{s}$ *has period* $(2^{L_2} - 1)2^{L_1 - 1}$*. Moreover, the linear complexity satisfies* $L_2 2^{L_1 - 2} < L(\mathbf{s}) \leqslant L_2 2^{L_1 - 1}$*.*

Some Computational Results regarding Linear Complexity

decimator/sequence	$x^3 + x + 1$
$x^5 + x^3 + 1$	80
$x^5 + x^3 + x^2 + x + 1$	80
$x^5 + x^4 + x^3 + x + 1$	80
$x^5 + x^4 + x^3 + x^2 + 1$	75
$x^5 + x^4 + x^3 + x + 1$	80
$x^5 + x^4 + x^2 + x + 1$	80
$x^5 + x^4 + x^2 + x + 1$	80

Interleave structure

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} \longrightarrow 11010110001110$$

Composition structure

Folded array

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} \longrightarrow$$

Unfolded sequence

11010110001110

Structure of shrunken sequence

Theorem (Gomez et al. 2021, Cardell et al. 2019)

Let L_1, L_2 *be coprime positive integers with* $\gcd(L_1, L_2) = 1$ *and let* $(a_i), (b_i)$ *be m-sequences with (coprime) periods* $T_1 = 2^{L_1} - 1$ *and* $T_2 = 2^{L_2} - 1$. *Let* $\delta \in \{1, \dots, T_2 - 1\}$ *such that* $T_1 \cdot \delta = 2^{L_1 - 1} \mathbf{mod} T_2$. *Denote by* (i_j) *the sequence of indices belonging to the set* I *defined previously, i.e.* $a_{i_j} = 1$ *and define the* $(2^{L_1 - 1})$*-periodic sequence*

$$t_j = \delta \cdot i_j - j \quad \text{mód } T_2.$$

Then, the shrunken sequence is the result of unfolding the array given by the composition of (b_i) *and* (t_j).

Linear complexity of a two-dimensional array

A polynomial $C = \sum_{(\alpha_1,\alpha_2)\in S\subset\mathbb{N}_0^2} c_{\alpha_1,\alpha_2} x^{\alpha_1} y^{\alpha_2} \in \mathbb{F}_2[x,y]$ is *valid* for the two-dimensional array $\mathbf{A}$ when the equation

$$\sum_S c_{\alpha_1,\alpha_2} \mathbf{A}(\alpha_1+\beta_1, \alpha_2+\beta_2) = 0$$

for all α_1, α_2. The set of all valid polynomials for $\mathbf{A}$ forms an ideal, and its degree is *the linear complexity*.

Relation between arrays and sequences

Theorem (Arce-Nazario et al. 2020)

The linear complexity of any unfolded sequence $\mathbf{s}$ *and its folded array* $\mathbf{A}$ *are equal. Evenmore, the set of connection polynomials of* $\mathbf{s}$ *can be calculated from the ideal of valid polynomials of* $\mathbf{A}$*.*

Facts about $\mathbf{A}$

- If a polynomial in $\mathbb{F}_2[x]$ is valid for $\mathbf{A}$, it is a multiple of the minimal polynomial of (b_i).
- If a polynomial in $\mathbb{F}_2[y]$ is valid for $\mathbf{A}$, it is a multiple of $(y+1)^\tau$.

First result

Theorem

The linear complexity of a shrunken sequence $\mathbf{s}$ *is*

$$L(\mathbf{s}) = L_2 \cdot 2^{L_1 - 1}, \quad \textit{when } 2^{L_1} \cdot (2^{L_1} - 1) < L_2.$$

Idea of the proof

The number of columns of $\mathbf{A}$ is $\tau = 2^{L_1 - 1}$, so a valid polynomial is

$$y^\tau + 1 = (y+1)^\tau = y^\tau - 1 \qquad \text{and} \qquad (y+1)^{\tau-1} = 1 + y + y^2 + \cdots + y^{\tau-1}.$$

Idea of the proof

The number of columns of $\mathbf{A}$ is $\tau = 2^{L_1-1}$, so a valid polynomial is

$$y^{\tau}+1 = (y+1)^{\tau} = y^{\tau}-1 \qquad \text{and} \qquad (y+1)^{\tau-1} = 1+y+y^2+\cdots+y^{\tau-1}.$$

Our aim is to prove that $(y+1)^{\tau-1}$ is not valid.

Idea of the proof

The number of columns of $\mathbf{A}$ is $\tau = 2^{L_1-1}$, so a valid polynomial is

$$y^\tau + 1 = (y+1)^\tau = y^\tau - 1 \qquad \text{and} \qquad (y+1)^{\tau-1} = 1 + y + y^2 + \cdots + y^{\tau-1}.$$

Our aim is to prove that $(y+1)^{\tau-1}$ is not valid. After some computations, this fact is equivalent to

$$p_2(\alpha) = 0 = \sum_{j=0}^{\tau-1} \alpha^{j-\delta \cdot i_j} = \sum_{j=0}^{\tau-1} (\alpha')^{(2\cdot\tau-1)\cdot j - \tau \cdot i_j},$$

where $(\alpha')^{2\tau-1} = \alpha$. If the degree of the minimal polynomial $p_2(x)$ is bigger than the right hand, this is a contradiction.

Idea of the proof

For a general polynomial valid polynomial

$$C(x,y) = \sum_{i=0}^{\tau-1} C_i(x)(y+1)^i \qquad (\deg C_i(x) < \deg p_2(x),\ \forall i),$$

which gives another valid polynomial

$$(y+1)^{\tau-1-n}\, C(x,y) = C_n(x)(y+1)^{\tau-1} + D(x,y)(y+1)^{\tau},$$

which implies that $(y+1)^{\tau-1}$ is valid.

Conclusions and Open Problems

Our contribution is, for some set of parameters:

- the value of the linear complexity
- conditions on when the linear complexity is maximal
- the value of the linear complexity profile

We are working on determining

- The linear complexity and when it is maximal
- The linear complexity profile
- The k-error linear complexity
- Studying other pseudorandom tests using the composition structure