A Family of Binary Sequences from Interleaved Construction and their Cryptographic Properties

Jing (Jane) He
Joint work with Daniel Panario and Qiang Wang

Carleton University

Outline

"Criteria of good signal sets"

"Interleaved structure"

"The main results"

"Applications of our results"

Current work

"Future work"

We desire a sequence to possess the following properties:

- Balance property
- Run property
- The ideal two-level autocorrelation property

We desire a signal set containing some sequences of the same period to possess the following properties:

- Good randomness (hard to distinguish from random)
- Low cross correlation
- Large linear complexity (span)

We desire a sequence to possess the following properties:

- Balance property
- Run property
- The ideal two-level autocorrelation property

We desire a signal set containing some sequences of the same period to possess the following properties:

- Good randomness (hard to distinguish from random)
- Low cross correlation
- Large linear complexity (span)

Correlation functions

Definition

Correlation functions: The cross correlation function $C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ of two sequences $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ is defined as

$$C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i - b_{(i+\tau) \pmod N}}, \tau = 0, 1, \ldots.$$

If $\underline{\mathbf{b}} = \underline{\mathbf{a}}$, then denote $C_{\underline{\mathbf{a}}}(\tau) = C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ as the autocorrelation of $\underline{\mathbf{a}}$.

Example

Given two sequences in one period $\underline{a} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ and $\underline{b} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$ and, for example, we set $\tau = 2$. Then the cross correlation of $\underline{a}$ and $\underline{b}$ is

$C_{\underline{a},\underline{b}}(2) = \sum_{i=0}^{6} (-1)^{a_i - b_{(i+2) \pmod 7}} = 5 \times (-1)^0 + 2 \times (-1)^2 = 3$

Correlation functions

Definition

Correlation functions: The cross correlation function $C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ of two sequences **a** and **b** is defined as

$$C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i - b_{(i+\tau)} \pmod N}, \tau = 0, 1, \ldots .$$

If $\underline{\mathbf{b}} = \underline{\mathbf{a}}$, then denote $C_{\underline{\mathbf{a}}}(\tau) = C_{\underline{\mathbf{a}},\underline{\mathbf{b}}}(\tau)$ as the autocorrelation of **a**.

Example

Given two sequences in one period
$\underline{a} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ and $\underline{b} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$
and, for example, we set $\tau = 2$. Then the cross correlation of $\underline{a}$ and $\underline{b}$ is
$C_{\underline{a},\underline{b}}(2) = \sum_{i=0}^{6} (-1)^{a_i - b_{(i+2)} \pmod 7} = 5 \times (-1)^0 + 2 \times (-1)^2 = 3$

Motivation

In 1995 Gong first introduced the interleaved structure and she employed two m-sequences to construct a family of long-period sequences with nice properties.

She also gave the maximal values of correlation function and linear complexity for the sequences constructed from interleaved structure where the two base sequences are of the same period.

Algorithm to construct sequences of period $p \cdot q$

Let s and t be two positive integers. Suppose that $\underline{a} = (a_0, \ldots, a_{s-1})$ and $\underline{b} = (b_0, \ldots, b_{t-1})$ are two ℓ-ary sequences of periods s and t, respectively.

- 1. Choose $\underline{e} = (e_0, \ldots, e_{t-1})$ as the shift sequence for which the first $t-1$ elements are over $\mathbb{Z}_s$ and $e_{t-1} = \infty$. Moreover, if we let $d_{i-1} = e_i - e_{i-1}$, then we choose $\underline{e}$ such that $d_0, d_1 \ldots, d_{t-3}$ is in an arithmetic progression with common distance $d \neq 0$.
- 2. Construct an interleaved sequence $\underline{u} = (u_0, \ldots, u_{st-1})$, whose j^{th} column in the matrix form is given by $L^{e_j}(\underline{a})$.

Algorithm Cont'd

- 3. For $0 \leq i < st-1$, $0 \leq j \leq t$, define $\underline{s_j} = (s_{j,0}, \ldots, s_{j,st-1})$ as follow:

$$s_{j,i} = \begin{cases} u_i + b_{j+i}, & 0 \leq j \leq t-1, \\ u_i, & j = t. \end{cases}$$

- 4. Define the family of sequences $\mathfrak{S} = \mathfrak{S}(\underline{a}, \underline{b}, \underline{e})$ as $\mathfrak{S} = \{\underline{s_j} \mid j = 0, 1, \ldots, t\}$, where $\underline{a}$ is the *first base sequence*, $\underline{e}$ is the *shift sequence*, and $\underline{b}$ is the *second base sequence*.

Example

The base sequences and the shift sequence

Given sequences $\underline{a} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ and $\underline{b} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. We set the shift sequence be $\underline{e} = (0,1,3,1,0,0,\infty)$.

Generate the interleaved sequence $\underline{u}$

First we get a matrix form for the interleaved sequence $\underline{u}$.

$A_{\underline{u}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$. Concatenate the rows to obtain $\underline{u} = (10101100101000111111010001100111000)$.

Example

The base sequences and the shift sequence

Given sequences $\underline{a} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \end{pmatrix}$ and $\underline{b} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. We set the shift sequence be $\underline{e} = (0,1,3,1,0,0,\infty)$.

Generate the interleaved sequence $\underline{u}$

First we get a matrix form for the interleaved sequence $\underline{u}$.

$$A_{\underline{u}} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

. Concatenate the rows to obtain $\underline{u} = (10101100101000111111010001100111000)$.

Shift $\underline{b}$ and add to $\underline{u}$

Then we shift 1 bit of $\underline{b}$ to the left and write the 5×7 matrix form copying the shifted $\underline{b}$ in each row
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

We get a new constructed sequence $s_1 = (10000010111111101001101000101011\,11)$ from the addition of the above two matrices
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Theorem

Theorem 1: *Let us choose* $\underline{a}$ *as the first base sequence with period* v *and* $\underline{b}$ *as the second base sequence with period* w*. Then using the algorithm we construct a family* $\mathfrak{S}(\underline{a},\underline{b},\underline{e}) = \{\underline{s_j} \mid j = 0,1,\ldots,w\}$ *with the property that the number* $N_0(\underline{s_j})$ *of zeros in one period of each sequence* $\underline{s_j}$ *is:*

- $(w-1)\cdot N_0(\underline{a})+v$, *when j=w;*
- $N_0(\underline{a})\cdot(N_0(\underline{b})-1)+(v-N_0(\underline{a}))\cdot(w-N_0(\underline{b}))+v$, *when* $b_{j+w-1}=0, j\leq w-1$;
- $N_0(\underline{a})\cdot N_0(\underline{b})+(v-N_0(\underline{a}))\cdot(w-N_0(\underline{b})-1)$, *when* $b_{j+w-1}=1, j\leq w-1$.

Theorem

Theorem 2: *Let $\underline{a}$ be a two-level autocorrelation sequence with period v and $\underline{b}$ be a balanced low cross correlation sequence of period w with the maximal absolute value of nontrivial autocorrelation equal to δ_b. The family of sequences $\mathfrak{S}$ generated by the algorithm is a $(vw, w+1, \delta_1)$ signal set, where*

$$\delta_1 = \max\left\{\left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + w, \delta_b v\right\}.$$

Theorem

Theorem 3: *If both $\underline{a}$ and $\underline{b}$ are two-level autocorrelation sequences with periods v and w, respectively, then the family of sequences constructed by the algorithm is a $(vw, w+1, \delta_2)$ signal set with*

$$\delta_2 = \left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + 1.$$

Theorem

Theorem 2: *Let* $\underline{a}$ *be a two-level autocorrelation sequence with period* v *and* $\underline{b}$ *be a balanced low cross correlation sequence of period* w *with the maximal absolute value of nontrivial autocorrelation equal to* δ_b*. The family of sequences* $\mathfrak{S}$ *generated by the algorithm is a* $(vw, w+1, \delta_1)$ *signal set, where*

$$\delta_1 = \max\left\{\left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + w, \delta_b v\right\}.$$

Theorem

Theorem 3: *If both* $\underline{a}$ *and* $\underline{b}$ *are two-level autocorrelation sequences with periods* v *and* w*, respectively, then the family of sequences constructed by the algorithm is a* $(vw, w+1, \delta_2)$ *signal set with*

$$\delta_2 = \left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + 1.$$

Theorem

Theorem 2: *Let* $\underline{a}$ *be a two-level autocorrelation sequence with period* v *and* $\underline{b}$ *be a balanced low cross correlation sequence of period* w *with the maximal absolute value of nontrivial autocorrelation equal to* δ_b*. The family of sequences* $\mathfrak{S}$ *generated by the algorithm is a* $(vw, w+1, \delta_1)$ *signal set, where*

$$\delta_1 = \max\left\{\left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + w, \delta_b v\right\}.$$

Theorem

Theorem 3: *If both* $\underline{a}$ *and* $\underline{b}$ *are two-level autocorrelation sequences with periods* v *and* w*, respectively, then the family of sequences constructed by the algorithm is a* $(vw, w+1, \delta_2)$ *signal set with*

$$\delta_2 = \left(\left\lfloor \frac{w}{v} \right\rfloor + 1\right)(v+1) + 1.$$

Corollary

Corollary 1: *When v and w are equal, the family of sequences generated by the algorithm is a $(v^2, v+1, 2v+3)$ signal set.*

Corollary

Corollary 2: *Fix a prime number $p \equiv 3 \pmod 4$ and any other prime $q \geq p$. The family of sequences $\mathfrak{S}$ generated by the algorithm from two Legendre sequences of periods p and q is a $(pq, q+1, \delta)$ signal set, where*

$$\delta = \delta_1 = \left(\left\lfloor \frac{q}{p} \right\rfloor + 1 \right) \cdot (p+1) + q.$$

Furthermore, when both p and q are congruent to $3 \pmod 4$ we obtain

$$\delta = \delta_2 = \left(\left\lfloor \frac{q}{p} \right\rfloor + 1 \right) \cdot (p+1) + 1.$$

Legendre Sequence

Definition

Let p be an odd prime. The Legendre sequence $\underline{\mathbf{s}} = \{s_i \mid i \geq 0\}$ of period p is defined as

$$s_i = \begin{cases} 1, & \text{if } i \equiv 0 \mod p; \\ 0, & \text{if } i \text{ is a quadratic residue modulo } p; \\ 1, & \text{if } i \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Correlation function of Legendre sequence

Let $\underline{\mathbf{s}}$ be a Legendre sequence of period p as above. Then If $p \equiv 3 \pmod 4$, $C_{\underline{\mathbf{s}}}(\tau) = \{-1, p\}$. This is called the ideal two-level autocorrelation function.
If $p \equiv 1 \pmod 4$, $C_{\underline{\mathbf{s}}}(\tau) = \{1, -3, p\}$.

Legendre Sequence

Definition

Let p be an odd prime. The Legendre sequence $\underline{\mathbf{s}} = \{s_i \mid i \geq 0\}$ of period p is defined as

$$s_i = \begin{cases} 1, & \text{if } i \equiv 0 \mod p; \\ 0, & \text{if } i \text{ is a quadratic residue modulo } p; \\ 1, & \text{if } i \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Correlation function of Legendre sequence

Let $\underline{\mathbf{s}}$ be a Legendre sequence of period p as above. Then
If $p \equiv 3 \pmod 4$, $C_{\underline{\mathbf{s}}}(\tau) = \{-1, p\}$. This is called the ideal two-level autocorrelation function.
If $p \equiv 1 \pmod 4$, $C_{\underline{\mathbf{s}}}(\tau) = \{1, -3, p\}$.

We remark that Wang and Qi's result is the case when taking two Legendre sequences $\underline{a}$ and $\underline{b}$ with twin prime periods $p \equiv 3 \pmod 4$ and $q = p+2$, respectively.

Corollary

Corollary 3: *Let two Legendre sequences of twin prime periods p and $p+2$, where $p \equiv 3 \pmod 4$ be the base sequences under the construction of the algorithm. The maximum magnitude of nontrivial cross correlation values of this constructed family is $3p+4$.*

Theorem

Theorem 4: *Fix a prime number* $p \equiv 1 \pmod 4$ *and any other prime* $q \geq p$. *The family of sequences* $\mathfrak{S}$ *generated by the algorithm from two Legendre sequences of periods* p *and* q *is a* $(pq, q+1, \delta_3)$ *family, where* $\delta_3 = \left(\left\lfloor \frac{q}{p} \right\rfloor + 1\right) \cdot (p+1) + 3q - 2$.

Current Work

We have partially done with the linear complexities of interleaved sequences constructed from Legendre sequences with period p and q.

Please see the data.

When $p \equiv 3 \pmod 8$, that is the feedback polynomial of $\underline{a}$ is $g_{\underline{a}} = \phi_p$ and $\deg(g_{\underline{a}}) = p-1$. We give the linear complexity values and the feedback polynomials below.

$q \equiv 7 \pmod 8$	$q \equiv 1 \pmod 8$	$q \equiv 3 \pmod 8$	$q \equiv 5 \pmod 8$
$LC_{3\cdot 7} = (q-1)\deg g_{\underline{a}}$ $\frac{\phi_p(x^q)}{\phi_p(x)} = \phi_{pq}$		$LC_{3\cdot 11} = (q-1)\deg g_{\underline{a}}$ $\frac{\phi_p(x^q)}{\phi_p(x)} = \phi_{pq}$	$LC_{3\cdot 13} = (q-1)\deg g_{\underline{a}}$ $\frac{\phi_p(x^q)}{\phi_p(x)} = \phi_{pq}(x)$
$LC_{11\cdot 23} = (q-1)\deg g_{\underline{a}}$ $\frac{\phi_p(x^q)}{\phi_p(x)} = \phi_{pq}$	$LC_{11\cdot 17} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{11\cdot 19} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{11\cdot 13} = (q-1)\deg g_{\underline{a}}$ $\frac{\phi_p(x^q)}{\phi_p(x)} = \phi_{pq}(x)$
$LC_{19\cdot 23} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{19\cdot 41} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{19\cdot 43} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{19\cdot 29} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$
$LC_{43\cdot 47} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{43\cdot 73} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{43\cdot 59} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$	$LC_{43\cdot 53} = q\deg g_{\underline{a}}$ $\phi_p(x^q)$

When $p \equiv 5 \pmod 8$, that is the feedback polynomial of $\underline{a}$ is $g_{\underline{a}} = x^p + 1$ and $\deg(g_{\underline{a}}) = p$. We give the linear complexity values and the feedback polynomials below.

$q \equiv 7 \pmod 8$	$q \equiv 1 \pmod 8$	$q \equiv 3 \pmod 8$	$q \equiv 5 \pmod 8$
$LC_{5\cdot 7} = (q-1)p$ $\frac{x^{pq}+1}{x^p+1}$	$LC_{5\cdot 17} = (q-1)p$ $\frac{x^{pq}+1}{x^p+1}$	$LC_{5\cdot 11} = (q-1)p$ $\frac{x^{pq}+1}{x^p+1}$	$LC_{5\cdot 13} = pq-1$ $\frac{x^{pq}+1}{x+1}$
$LC_{13\cdot 23} = pq-1$ $\frac{x^{pq}+1}{x+1}$	$LC_{13\cdot 17} = pq-1$ $\frac{x^{pq}+1}{x+1}$	$LC_{13\cdot 19} = pq-1$ $\frac{x^{pq}+1}{x+1}$	$LC_{13\cdot 29} = pq-1$ $\frac{x^{pq}+1}{x+1}$

When $p \equiv 7 \pmod 8$, that is the feedback polynomial of $\underline{a}$ is $g_{\underline{a}} = n(x)$ and $\deg(g_{\underline{a}}) = \frac{p-1}{2}$. We give the linear complexity values and the feedback polynomials in the table below.

	$q \equiv 1 \pmod 8$	$q \equiv 7 \pmod 8$	$q \equiv 3 \pmod 8$	$q \equiv 5 \pmod 8$
p, q $LC\ value$ $LC =$ $pol. =$	$7, 73$ 219 $q \cdot \deg(n(x))$ $n(x^q)$	$7, 71$ 210 $(q-1) \cdot \deg(n(x))$ $\frac{n(x^q)}{n(x)}$	$7, 67$ 201 $q \cdot \deg(n(x))$ $n(x^q)$	$7, 61$ 183 $q \cdot \deg(n(x))$ $n(x^q)$
p, q $LC\ value$ $LC =$ $pol. =$	$7, 41$ 120 $(q-1) \cdot \deg n(x)$ $\frac{n(x^q)}{n(x)}$	$7, 47$ 141 $q \cdot \deg(n(x))$ $n(x^q)$	$7, 59$ 177 $q \cdot \deg(n(x))$ $n(x^q)$	$7, 53$ 159 $q \cdot \deg n(x)$ $n(x^q)$
p, q $LC\ value$ $LC =$ $pol. =$	$7, 17$ 51 $q \cdot \deg n(x)$ $n(x^q)$	$7, 31$ 93 $q \cdot \deg n(x)$ $n(x^q)$	$7, 43$ 126 $(q-1) \cdot \deg n(x)$ $\frac{n(x^q)}{n(x)}$	$7, 37$ 108 $(q-1) \cdot \deg n(x)$ $\frac{n(x^q)}{n(x)}$
p, q $LC\ value$ $LC =$ $pol. =$	N/A N/A N/A N/A	$7, 23$ 66 $(q-1) \cdot \deg n(x)$ $\frac{n(x^q)}{n(x)}$	$7, 19$ 57 $q \deg n(x)$ $n(x^q)$	$7, 29$ 84 $(q-1) \cdot \deg n(x)$ $\frac{n(x^q)}{n(x)}$
p, q $LC\ value$ $LC =$ $pol. =$	N/A N/A N/A N/A	N/A N/A N/A N/A	$7, 11$ 33 $q \cdot \deg n(x)$ $n(x^q)$	$7, 13$ 36 $(q-1) \cdot \deg n(x)$ $\frac{n(x^q)}{n(x)}$
p, q $LC\ value$ $LC =$ $pol. =$	$23, 97$ 1067 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 89$ 979 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 83$ 913 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 61$ 671 $q \cdot \deg(n(x))$ $n(x^q)$
p, q $LC\ value$ $LC =$ $pol. =$	$23, 41$ 451 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 79$ 869 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 67$ 737 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 53$ 583 $q \cdot \deg(n(x))$ $n(x^q)$
p, q $LC\ value$ $LC =$ $pol. =$	N/A N/A N/A N/A	$23, 71$ 770 $(q-1) \cdot \deg(n(x))$ $\frac{n(x^q)}{n(x)}$	$23, 59$ 649 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 37$ 407 $q \cdot \deg(n(x))$ $n(x^q)$
p, q $LC\ value$ $LC =$ $pol. =$	N/A N/A N/A N/A	$23, 47$ 506 $(q-1) \cdot \deg(n(x))$ $\frac{n(x^q)}{n(x)}$	$23, 43$ 473 $q \cdot \deg(n(x))$ $n(x^q)$	$23, 29$ 319 $q \cdot \deg(n(x))$ $n(x^q)$
p, q $LC\ value$ $LC =$ $pol. =$	N/A N/A N/A N/A	$23, 31$ 341 $q \cdot \deg(n(x))$ $n(x^q)$	N/A N/A N/A N/A	N/A N/A N/A N/A

When $p \equiv 1 \pmod 8$, that is the feedback polynomial of $\underline{a}$ is $g_{\underline{a}}(x) = (1+x) \cdot n(x)$ and $\deg(g_{\underline{a}}) = \frac{p+1}{2}$.

	$q \equiv 1 \pmod 8$	$q \equiv 7 \pmod 8$	$q \equiv 3 \pmod 8$	$q \equiv 5 \pmod 8$
p, q	$17, 97$	$17, 89$	$17, 83$	$17, 61$
LC value	872	800	746	548
$LC =$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$
$pol. =$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$
p, q	$17, 73$	$17, 79$	$17, 67$	$17, 53$
LC value	656	710	594	468
$LC =$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$(q-1) \cdot \deg(g_{\underline{a}}(x))$	$(q-1) \cdot \deg(g_{\underline{a}}(x))$
$pol. =$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{(1+x)n(x)}$	$\frac{(1+x^q)n(x^q)}{(1+x)n(x)}$
p, q	$17, 41$	$17, 71$	$17, 59$	$17, 37$
LC value	368	638	530	332
$LC =$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$
$pol. =$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$
p, q	N/A	$17, 47$	$17, 43$	$17, 29$
LC value	N/A	422	386	260
$LC =$	N/A	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$
$pol. =$	N/A	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$
p, q	N/A	$17, 31$	$17, 19$	N/A
LC value	N/A	278	162	N/A
$LC =$	N/A	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$(q-1) \cdot \deg(g_{\underline{a}}(x))$	N/A
$pol. =$	N/A	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{(1+x)n(x)}$	N/A
p, q	N/A	$17, 23$	N/A	N/A
LC value	N/A	206	N/A	N/A
$LC =$	N/A	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	N/A	N/A
$pol. =$	N/A	$\frac{(1+x^q)n(x^q)}{1+x}$	N/A	N/A
p, q	$41, 97$	$41, 89$	$41, 83$	$41, 61$
LC value	2036	1868	1722	1280
$LC =$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$(q-1) \cdot \deg(g_{\underline{a}}(x))$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$
$pol. =$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{(1+x)n(x)}$	$\frac{(1+x^q)n(x^q)}{1+x}$
p, q	$41, 73$	$41, 79$	$41, 67$	$41, 53$
LC value	1532	1658	1406	1112
$LC =$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$
$pol. =$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$
p, q	N/A	$41, 71$	$41, 59$	N/A
LC value	N/A	1490	1238	N/A
$LC =$	N/A	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	N/A
$pol. =$	N/A	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	N/A
p, q	$41, 73$	$41, 79$	$41, 67$	$41, 53$
LC value	1532	1658	1406	1112
$LC =$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	$q \cdot \deg(g_{\underline{a}}(x)) - 1$
$pol. =$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$	$\frac{(1+x^q)n(x^q)}{1+x}$
p, q	N/A	$41, 47$	N/A	N/A
LC value	N/A	986	N/A	N/A
$LC =$	N/A	$q \cdot \deg(g_{\underline{a}}(x)) - 1$	N/A	N/A
$pol. =$	N/A	$\frac{(1+x^q)n(x^q)}{1+x}$	N/A	N/A

Future work

1. Linear complexities of the families of interleaved sequences with period p and q.
2. Apply the techniques of interleaved construction to aperiodic sequences and compute the merit factor.