Low Correlation Sequences for CDMA

Gagan Garg

Indian Institute of Science, Bangalore

International Networking and Communications Conference
Lahore University of Management Sciences
Acknowledgement

- Prof. Zartash Afzal Uzmi,
  Lahore University of Management Sciences

- Indian Institute of Science, Bangalore
Outline

- Motivation
- Binary Sequences
- Quaternary Sequences
Motivation

There are a large number of problems in communications that require sets of signals with one or both of the following two properties:

- each signal in the set is easy to distinguish from a time-shifted version of itself
  - ranging systems, radar systems

- each signal in the set is easy to distinguish from (a possibly time-shifted version of) every other signal in the set
  - code-division multiple-access (CDMA) communication systems
Mean-Squared Difference

Assume the signals to be periodic with common time period $T$

We want to distinguish between $a(t)$ and $b(t)$

We also want to distinguish between $-a(t)$ and $b(t)$

Measure of distinguishability is

$$\frac{1}{T} \int_0^T [b(t) \pm a(t)]^2 \, dt$$

$$= \frac{1}{T} \left\{ \int_0^T [b^2(t) + a^2(t)] \, dt \pm 2 \int_0^T a(t)b(t) \, dt \right\}$$

\[ \downarrow \]

energy in $b(t)$ + energy in $a(t)$

\[ \downarrow \]

$r$
Cross-correlation function

\[ r_{a,b}(\tau) := \int_{0}^{T} a(t)b(t + \tau) \, dt \]

If \( a(t) = b(t) \), we want \( r_{a,b}(\tau) \) to be small for \( \tau \in (0, T) \)
If \( a(t) \neq b(t) \), we want \( r_{a,b}(\tau) \) to be small for \( \tau \in [0, T] \)

For complex signals, we replace \( b(t + \tau) \) by its complex conjugate

Assume \( a(t) \) and \( b(t) \) to be periodic signals, which consist of sequences of elemental time-limited pulses.

\[ a(t) := \sum_{n=-\infty}^{\infty} x(n)\varphi(t - nT_c) \]

where \( \varphi(t) \) is the basic pulse waveform and \( T_c \) is the time duration of this pulse and \( T_c | T \Rightarrow \text{sequence } \{x(n)\} \text{ is periodic} \)
Let $N = T/T_c$. Then, period of $\{x(n)\}$ divides $N$.

$$b(t) := \sum_{n=-\infty}^{\infty} y(n) \varphi(t - nT_c)$$

If $\tau = mT_c$

$$r_{a,b}(\tau) = \lambda \sum_{n=0}^{N-1} x(n) y(n + m)$$

where the constant

$$\lambda = \int_{0}^{T_c} \varphi^2(t) \, dt$$
Let \( \{u(t)\} \) and \( \{v(t)\} \) be complex valued sequences of period \( N \).

**Periodic correlation** between them:

\[
\theta_{u,v}(\tau) = \sum_{t=0}^{N-1} u(t + \tau)v^*(t), \quad 0 \leq \tau \leq N - 1
\]

**Aperiodic correlation** between them:

\[
\rho_{u,v}(\tau) = \sum_{t=\max\{0,-\tau\}}^{\min\{N-1,N-1-\tau\}} u(t + \tau)v^*(t), \quad -(N-1) \leq \tau \leq N - 1
\]
An example

Let $N = 3$.

\[
\begin{align*}
\theta_{u,v}(0) &= u(0)v^*(0) + u(1)v^*(1) + u(2)v^*(2) \\
\theta_{u,v}(1) &= u(1)v^*(0) + u(2)v^*(1) + u(0)v^*(2) \\
\theta_{u,v}(2) &= u(2)v^*(0) + u(0)v^*(1) + u(1)v^*(2)
\end{align*}
\]

\[
\begin{align*}
\rho_{u,v}(-2) &= u(0)v^*(2) \\
\rho_{u,v}(-1) &= u(0)v^*(1) + u(1)v^*(2) \\
\rho_{u,v}(0) &= u(0)v^*(0) + u(1)v^*(1) + u(2)v^*(2) \\
\rho_{u,v}(1) &= u(1)v^*(0) + u(2)v^*(1) \\
\rho_{u,v}(2) &= u(2)v^*(0)
\end{align*}
\]
Binary sequences

- Binary $m$-sequences
- Finite Fields
- Gold sequences
Binary $m$-sequence of Period 7

Let $\alpha$ be a root of $x^3 + x + 1 = 0$

Let $\{s(t)\}$ have characteristic polynomial $x^3 + x + 1$, i.e.,

$$s(t + 3) + s(t + 1) + s(t) = 0$$

i.e.,

$$s(t + 3) = s(t + 1) + s(t)$$

Then

$$s(t) = 100101110010\ldots$$ is an $m$-sequence

Periodic autocorrelation

$$\theta_s(\tau) = \sum_{t=0}^{6} (-1)^{s(t+\tau)-s(t)} = \begin{cases} 7 & \tau = 0 \pmod{7} \\ -1 & \text{else} \end{cases}$$
An irreducible binary polynomial $f(x)$ is said to be primitive if the smallest positive exponent $k$ for which $f(x) \mid x^k - 1$ is $k = 2^m - 1$.

Let $f(x)$ be a primitive binary polynomial of degree $m$.

For example, when $m = 3$, the polynomial $f(x) = x^3 + x + 1$ is primitive since $f(x)$ divides $x^7 - 1$ but does not divide $x^k - 1$ for any $1 \leq k \leq 6$.

Let $f(x) = \sum_{i=0}^{m} f_i \cdot x^i$ and let $\{s(t)\}$ be a binary sequence satisfying the recursion

$$\sum_{i=0}^{m} f_i \cdot s(t + i) = 0 \quad \forall \ t$$

$\Rightarrow \{s(t)\}$ can be generated using an $m$-bit linear feedback shift register (LFSR).
Binary $m$-sequences

$f(x)$ is a primitive polynomial $\Rightarrow \{s(t)\}$ has period $2^m - 1$.

Such a sequence is called a maximum-length LFSR sequence, i.e., an $m$-sequence.

For example, when $f(x) = x^3 + x + 1$, $\{s(t)\}$ satisfies the recursion

$$s(t + 3) + s(t + 1) + s(t) = 0$$
Properties of binary $m$-sequences

Periodic autocorrelation function $\theta_s$ of a binary $\{0, 1\}$ sequence $\{s(t)\}$ of period $N$ is defined by

$$\theta_s(\tau) = \sum_{t=0}^{N-1} (-1)^{s(t+\tau)-s(t)} \quad 0 \leq \tau \leq N - 1$$

An $m$-sequence of period $N = 2^m - 1$ has the following properties:

1. Balance property: In each period of the $m$-sequence, there are $2^{m-1}$ ones and $2^{m-1} - 1$ zeroes.
2. Run property: Every nonzero binary $s$-tuple, $s \leq m$ occurs $2^{m-s}$ times and the all-zero tuple occurs $2^{m-s} - 1$ times.
3. Two-level autocorrelation function:

$$\theta_s(\tau) = \begin{cases} N & \tau = 0 \\ -1 & \tau \neq 0 \end{cases}$$
Property 1 and 2 can be proved using the fact that every $m$-sequence occurs precisely once in each period of the $m$-sequence.

For Property 3, when $\tau \neq 0$, consider the difference sequence $\{s(t + \tau) - s(t)\}$.

1. This sequence is not the all zero sequence.

2. It satisfies the same recursion as the sequence $\{s(t)\}$
   \[ \Rightarrow \{s(t + \tau) - s(t)\} \equiv \{s(t + \tau')\} \text{ for some } 0 \leq \tau' \leq N - 1, \]
   i.e., it is a different cyclic shift of the $m$-sequence $\{s(t)\}$.

3. Balance property of $\{s(t + \tau')\}$ proves Property 3.
Field Axioms

Two operations – addition and multiplication – that satisfy

<table>
<thead>
<tr>
<th>Name</th>
<th>Addition</th>
<th>Multiplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commutativity</td>
<td>( a + b = b + a )</td>
<td>( ab = ba )</td>
</tr>
<tr>
<td>Associativity</td>
<td>( (a + b) + c = a + (b + c) )</td>
<td>( (ab)c = a(bc) )</td>
</tr>
<tr>
<td>Distributivity</td>
<td>( a(b + c) = ab + ac )</td>
<td>( (a + b)c = ac + bc )</td>
</tr>
<tr>
<td>Identity</td>
<td>( a + 0 = a = 0 + a )</td>
<td>( a \cdot 1 = a = 1 \cdot a )</td>
</tr>
<tr>
<td>Inverses</td>
<td>( a + (-a) = 0 = (-a) + a )</td>
<td>( aa^{-1} = 1 = a^{-1}a ) if ( a \neq 0 )</td>
</tr>
</tbody>
</table>

A Finite and an Infinite Field

- The set $\mathbb{R}$ of all real numbers
- The set $\mathbb{F}_2 = \{0, 1\}$

We shall call this the **binary field**.

$$1 \oplus 1 = 0$$
$$1 \cdot 1 = 1$$

Check that all the field axioms are satisfied.
The Field of Complex Numbers

Introduce an imaginary element $\mathbb{i}$ such that $\mathbb{i}^2 = -1$

$$\mathbb{C} = \{a + \mathbb{i}b \mid a, b \in \mathbb{R}\}$$

$$(a + \mathbb{i}b)(c + \mathbb{i}d) = (ac + \mathbb{i}(ad + bc) + \mathbb{i}^2 bd)$$
$$= (ac - bd) + \mathbb{i}(ad + bc)$$

Check that all the field axioms are satisfied.
The Finite Field of 4 Elements – $\mathbb{F}_4$

Introduce an imaginary element $\alpha$ such that $\alpha^2 = \alpha \oplus 1$

$$\mathbb{F}_4 = \{ a \oplus \alpha b \mid a, b \in \mathbb{F}_2 \}$$

$$= \{ 0, 1, \alpha, 1 + \alpha \}$$

$$(a \oplus \alpha b)(c \oplus \alpha d) = ac \oplus \alpha(ad \oplus bc) \oplus \alpha^2(bd)$$

$$= (ac \oplus bd) \oplus \alpha(ad \oplus bc \oplus bd)$$

$$(1 \oplus \alpha)(1 \oplus \alpha) = (1 \oplus 1) \oplus \alpha(1 \oplus 1 \oplus 1)$$

$$= \alpha$$

$$(1 \oplus \alpha) \oplus \alpha = 1 \oplus \alpha(1 \oplus 1)$$

$$= 1$$
Learn your Tables!

### Addition Table

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>$\alpha$</th>
<th>$1 + \alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$1 + \alpha$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$1 + \alpha$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>1 + $\alpha$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$1 + \alpha$</td>
<td>$1 + \alpha$</td>
<td>$\alpha$</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

### Multiplication Table

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>$\alpha$</th>
<th>$1 + \alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$1 + \alpha$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>0</td>
<td>$\alpha$</td>
<td>1 + $\alpha$</td>
<td>1</td>
</tr>
<tr>
<td>$1 + \alpha$</td>
<td>0</td>
<td>$1 + \alpha$</td>
<td>1</td>
<td>$\alpha$</td>
</tr>
</tbody>
</table>
Representation as powers

Since $\alpha^2 = 1 + \alpha$, we replace $(1 + \alpha)$ by $\alpha^2$

<table>
<thead>
<tr>
<th>addition</th>
<th>$0$</th>
<th>$1$</th>
<th>$\alpha$</th>
<th>$\alpha^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0$</td>
<td>$0$</td>
<td>$1$</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
</tr>
<tr>
<td>$1$</td>
<td>$1$</td>
<td>$0$</td>
<td>$\alpha^2$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
<td>$0$</td>
<td>$1$</td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>$\alpha^2$</td>
<td>$\alpha$</td>
<td>$1$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>multiplication</th>
<th>$0$</th>
<th>$1$</th>
<th>$\alpha$</th>
<th>$\alpha^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0$</td>
<td>$0$</td>
<td>$0$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$1$</td>
<td>$0$</td>
<td>$1$</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$0$</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
<td>$1$</td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>$0$</td>
<td>$\alpha^2$</td>
<td>$1$</td>
<td>$\alpha$</td>
</tr>
</tbody>
</table>
**Best of both**

Addition table in terms of $1 + \alpha$

<table>
<thead>
<tr>
<th>addition</th>
<th>0</th>
<th>1</th>
<th>$\alpha$</th>
<th>$1 + \alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$1 + \alpha$</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$1 + \alpha$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>$1 + \alpha$</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$1 + \alpha$</td>
<td>$1 + \alpha$</td>
<td>$\alpha$</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Multiplication table in terms of $\alpha^2$

<table>
<thead>
<tr>
<th>multiplication</th>
<th>0</th>
<th>1</th>
<th>$\alpha$</th>
<th>$\alpha^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>0</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
<td>1</td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>0</td>
<td>$\alpha^2$</td>
<td>1</td>
<td>$\alpha$</td>
</tr>
</tbody>
</table>
The Finite Field of 8 Elements \(- \mathbb{F}_8\)

\[
\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}
\]

**binary addition**

\[
1 + 1 = 0 \quad \alpha^i + \alpha^i = 0
\]

**\(\alpha\) satisfies**

\[
\alpha^3 + \alpha + 1 = 0
\]

**We also have**

\[
\alpha^7 = 1
\]

**Multiplication**

\[
\alpha^3 \cdot \alpha^6 = \alpha^9 = \alpha^2
\]

**Addition**

\[
\alpha^3 + \alpha^6 = (\alpha + 1) + (\alpha^2 + 1)
\]

\[
= \alpha^2 + \alpha = \alpha(\alpha + 1) = \alpha^{1+3} = \alpha^4
\]
The Finite Field of $2^m$ Elements – $\mathbb{F}_{2^m}$

Let $f(x)$ be a binary primitive polynomial of degree $m$ and let $\alpha$ satisfy $f(\alpha) = 0$.

$$\mathbb{F}_{2^m} = \left\{ \sum_{i=0}^{m-1} c_i \alpha^i \mid c_i \in \{0, 1\} \right\}$$

$$= \{0\} \cup \{\alpha^i \mid 0 \leq i \leq 2^m - 2\}$$

In $\mathbb{F}_{2^m}$, $f(x)$ has one zero, viz. $\alpha$.

$\mathbb{F}_{2^m}$ has the remaining $m - 1$ zeroes of $f(x)$ as well.

$$\left\{ \alpha^{2^j} \mid j = 1, 2, \ldots, m - 1 \right\}$$
Binary $m$-sequence in terms of the trace function

Power series expansion gives us that the $m$-sequence $\{s(t)\}$ has a unique expression of the form

$$s(t) = \sum_{i=0}^{m-1} c_i \alpha^{2^i t} = \sum_{i=0}^{m-1} (c_0 \alpha^t)^{2^i} = tr(c_0 \alpha^t)$$

where $tr(\cdot) : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ is the trace function given by

$$tr(x) = \sum_{i=0}^{m-1} x^{2^i}$$

It turns out that every $m$-sequence $\{b(t)\}$ of period $2^m - 1$ can be expressed in the form

$$b(t) = tr(a \alpha^{d t})$$

where $a \in \mathbb{F}_{2^m}$ and $1 \leq d \leq 2^m - 2$ is an integer such that $(d, 2^m - 1) = 1$. 

Gagan Garg

Low Correlation Sequences for CDMA
Trace Function over $\mathbb{F}_8$

maps from $\mathbb{F}_8 \rightarrow \{0, 1\}$

$$tr(x) = x + x^2 + x^4$$

$$tr(\alpha) = \alpha + \alpha^2 + \alpha^4 = (\alpha + \alpha^2) + \alpha(1 + \alpha) = (\alpha + \alpha^2) + (\alpha + \alpha^2) = 0$$

$$\{tr(\alpha^t)\}_{t=0}^{6} = 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1$$ is $m$-sequence $s(t)$

$$\{tr(\alpha^{3t})\}_{t=0}^{6} = 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0$$ is another $m$-sequence $u(t)$

Periodic crosscorrelation

$$\theta_{s,u}(\tau) = \sum_{t=0}^{6} (-1)^{s(t+\tau)-u(t)} \in \{-5, -1, 3\}$$
Family of Gold Sequences

Contains the 9 sequences

\[ \mathcal{F} = \{s(t)\} \cup \{u(t)\} \cup \{u(t + \tau) + s(t) \mid 0 \leq \tau \leq 6\} \]

\[ \theta_{\text{max}} = \max \{ |\theta_{a,b}(\tau)| \mid a, b \in \mathcal{F} \text{ either } a \neq b \text{ or } \tau \neq 0 \} \]

\[ = 5 \]

General parameters

<table>
<thead>
<tr>
<th>Family</th>
<th>Period</th>
<th>Size</th>
<th>( \theta_{\text{max}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>( 2^n - 1, \ n \text{ odd} )</td>
<td>( 2^n + 1 )</td>
<td>( \approx \sqrt{2^{n+1}} )</td>
</tr>
</tbody>
</table>

Gold sequences have been employed in GPS satellites
General case

Let \( \{u(t)\} \) be an \( m \)-sequence of period \( 2^m - 1 \), \( m \) odd.

Let \( \{v(t)\} = \{u(dt)\} \), where \( d = 2^k + 1 \) for some \( k \) such that \((k, m) = 1\).

Then \( \mathcal{G} \) is a family of \( 2^m + 1 \) cyclically distinct sequences \( \{g_i(t)\}, \ 0 \leq i \leq 2^m \) given by

\[
\begin{align*}
g_i(t) &= tr(\alpha^t + \alpha^i \alpha^{dt}), \quad 0 \leq i \leq 2^m - 2, \\
g_{2^m-1}(t) &= tr(\alpha^t), \\
g_{2^m}(t) &= tr(\alpha^{dt}).
\end{align*}
\]
The cross correlation of sequences in $\mathcal{G}$ assumes values from the set

$$\left\{-1, -1 \pm \sqrt{2^{m+1}}\right\}$$

It can be shown that the Gold family $\mathcal{G}$ is optimal in the sense of having the lowest value of $\theta_{\text{max}}$ possible for a family of binary sequences for the given length $N = 2^m - 1$ and family size $M = 2^m + 1$. 

Gagan Garg

Low Correlation Sequences for CDMA
Quaternary Sequences

Galois Rings

Family $\mathcal{A}$
A Polynomial with $\mathbb{Z}_4$ coefficients

$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\} = \text{integers (modulo 4)}$

Let

$$f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$$

$$g(x^2) = (-1)f(x)f(-x) \pmod{4}$$

$$= (-1)(x^3 + x + 1)(-x^3 - x + 1)$$

$$= x^6 + 2x^4 + x^2 + 3$$

$$\Rightarrow g(x) = x^3 + 2x^2 + x + 3$$

$$g(x) = x^3 + x + 1 = f(x) \pmod{2}$$

So $g(x)$ is irreducible $\pmod{2}$ and therefore irreducible $\pmod{4}$.
Let $\mathcal{A}$ be the family of all nonzero sequences having characteristic polynomial $g(x) = x^3 + 2x^2 + x + 3$, i.e.,

\[ \mathcal{A} = \{ s(t) \mid s(t + 3) + 2s(t + 2) + s(t + 1) + 3s(t) = 0 \pmod{4} \} \]

Turns out $\mathcal{A}$ contains 9 sequences of period 7:
Better than Gold!

Periodic (quaternary) correlations of family $\mathcal{A}$ defined by

$$\theta_{s,u}(\tau) = \sum_{t=0}^{6} (i)^{s(t+\tau)} u(t), \quad i = \sqrt{-1}. $$

are better than those of Gold sequences!

<table>
<thead>
<tr>
<th>Family</th>
<th>Period</th>
<th>Size</th>
<th>$\theta_{\text{max}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>$2^n - 1$</td>
<td>$2^n + 1$</td>
<td>$\approx \sqrt{2^{n+1}}$</td>
</tr>
<tr>
<td></td>
<td>$n$ odd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\mathbb{Z}_4$ Family $\mathcal{A}$</td>
<td>$2^n - 1$</td>
<td>$2^n + 1$</td>
<td>$\approx \sqrt{2^n}$</td>
</tr>
<tr>
<td></td>
<td>any $n$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Of course, $\mathcal{A}$ uses a larger alphabet)
Let $\beta$ be a root of $g(x)$, i.e.,

$$\beta^3 + 2\beta^2 + \beta + 3 = 0 \pmod{4}$$

$\beta$ has multiplicative order 7 since $g(x^2) = (-1)f(x)f(-x)$.

$$GR(4, 3) = \left\{ \sum_{i=0}^{2} c_i \beta^i \mid c_i \in \mathbb{Z}_4 \right\}$$

An alternate description:

$$GR(4, 3) = \left\{ x + 2y \mid x, y \in T \right\}$$

where

$$T = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^6\}$$

is the set of Teichmuller representatives.

$$T \equiv \mathbb{F}_8 \quad \text{under} \quad (\text{mod} \ 2) \ \text{arithmetic}$$
Addition in the Galois Ring

\[ GR(4, 3) = \{ x + 2y \mid x, y \in \mathcal{T} = \{0, 1, \beta, \ldots, \beta^6\} \} \]

Let \[ z_1 + 2z_2 = (x_1 + 2y_1) + (x_2 + 2y_2) \]
\[ \Rightarrow z_1 = x_1 + x_2 \pmod{2} \text{ and } z_2 = y_1 + y_2 + \sqrt{x_1x_2} \pmod{2} \]

Eg. \[ z_1 + 2z_2 = (\beta^3 + 2\beta^2) + (\beta^6 + 2\beta^5) \]
\[ z_1 = \beta^3 + \beta^6 \pmod{2} = \alpha^3 + \alpha^6 \pmod{2} = \alpha^4 \Rightarrow z_1 = \beta^4 \]
\[ z_2 = \beta^2 + \beta^5 + \sqrt{\beta^9} \pmod{2} = \alpha^2 + \alpha^5 + \alpha \pmod{2} \]
\[ = 1 \pmod{2} \Rightarrow z_2 = 1 \]

Thus, \[ (\beta^3 + 2\beta^2) + (\beta^6 + 2\beta^5) = \beta^4 + 2 \cdot 1 \]

(Multiplication \((x_1 + 2y_1) \cdot (x_2 + 2y_2)\) is now straightforward)
Family $\mathcal{A}$ and the Trace Function

The trace function on $GR(4, 3)$ maps $GR(4, 3) \rightarrow \mathbb{Z}_4$

\[ T(x + 2y) = (x + x^2 + x^4) + 2(y + y^2 + y^4) \]

\[
\begin{array}{c|c}
   x & T(x) \\
   \hline
   0 & 0 \\
   1 & 3 \\
   \beta^4 & \beta^2 \beta \\
   \beta^5 & \beta^6 \beta^3 \\
\end{array}
\]

\[ t \rightarrow 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 0 \ 1 \ 2 \ldots \]

\[ T(\beta^t) \rightarrow 3 \ 2 \ 2 \ 1 \ 2 \ 1 \ 1 \ 3 \ 2 \ 2 \ldots \]

Trace description of Family $\mathcal{A}$:

\[ \mathcal{A} = \{ T(\beta^t) \} \cup \{ T([1 + 2\delta]\beta^t) \mid \delta \in \mathcal{T} \} \]
Let $f(x)$ be a primitive polynomial over $\mathbb{F}_2$ of degree $m$.

Let

$$g(x^2) = (-1)^m f(x) f(-x)$$

$$GR(4, m) = \mathbb{Z}_4[x] / (f(x))$$

$$\Rightarrow GR(4, m) \cong \mathbb{Z}_4[\zeta]$$

where $\zeta$ belongs to some extension ring of $\mathbb{Z}_4$ and satisfies

$$f(\zeta) = 0$$
Set

\[ \mathcal{T} = \{0\} \cup \{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\} \]

where \( N = 2^m - 1 \) is the order of \( \zeta \) in \( GR(4, m) \).

The trace function \( T(\cdot) : GR(4, m) \to \mathbb{Z}_4 \) is defined by

\[ T(x + 2y) = \sum_{i=0}^{m-1} \left(x^{2^i} + 2y^{2^i}\right), \quad x, y \in \mathcal{T} \]
Let
\[ T = \{ \gamma_i \mid i = 1, 2, \ldots, 2^m \} \]
be a labeling of the elements in \( T \).

Let
\[
\begin{align*}
s_i(t) &= T([1 + 2\gamma_i]\zeta^t), \quad 1 \leq i \leq 2^m, \\
s_{2^m+1}(t) &= 2T(\zeta^t).
\end{align*}
\]

Then the sequences \( \{s_i(t)\} \) are a set of cyclically distinct representatives for Family \( \mathcal{A} \).
If \( i \neq j \) or \( \tau \neq 0 \), the correlation values of sequences in Family \( \mathcal{A} \) belong to the set

\[
\theta_{ij}(\tau) \in \left\{ -1, -1 \pm \frac{m-1}{2}, \pm \sqrt{2} \frac{m-1}{2} \right\}, \quad m \text{ odd}
\]
or

\[
\theta_{ij}(\tau) \in \left\{ -1, -1 \pm \frac{m}{2}, -1 \pm \sqrt{2} \frac{m}{2} \right\}, \quad m \text{ even}
\]

\[
\Rightarrow \quad \theta_{\text{max}} \leq 1 + \sqrt{2^m}
\]

As compared to the binary family of Gold sequences, Family \( \mathcal{A} \) offers a lower value of \( \theta_{\text{max}} \) for the same period and family size.
Further Reading
