Low Interference of Interleavded Signal Sets

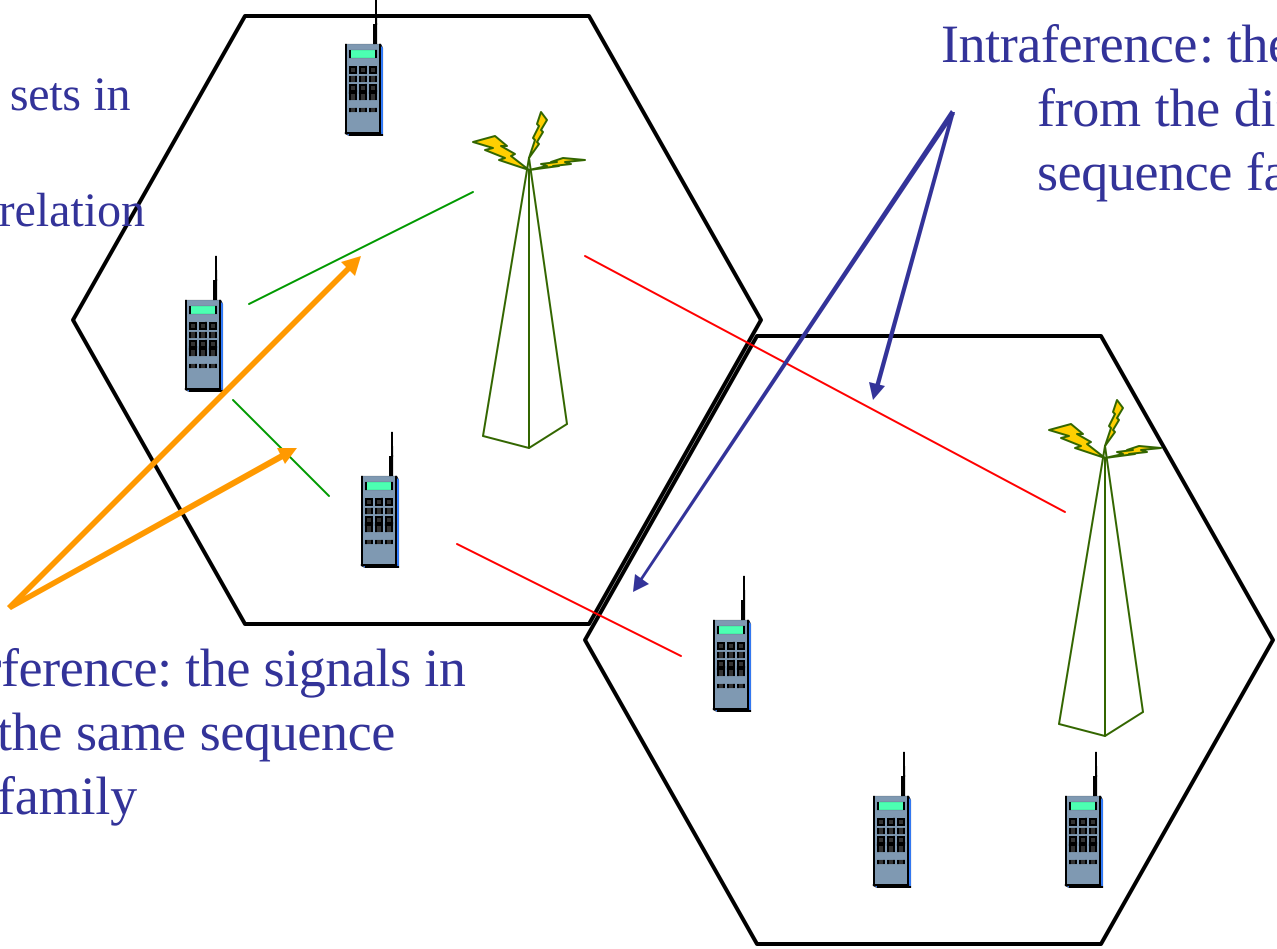
Guang Gong
Department of Electrical & Computer Engineering
University of Waterloo
CANADA
http://comsec.uwaterloo.ca/~ggong

Presentation Outline

- Interference of Signal Sets
- Overview of Known Constructions of Signal Sets with Low Interference in 3GPP
- Interleaved Signal Sets with Low Interference
- Discussions and Open Questions

Design of Signal sets in CDMA:

- Low cross correlation
- Capacity
- Security



Intraference: the signals from the different sequence families

This talk!

Interference: the signals in the same sequence family

CDMA (Code Division Multiple Access): A type of communications that all users share a common channel. The detector can distinguish the transmitted signals from the received signal with interference from the other signals by computing the cross correlation of the received signal and locally generated signals. The performance of the CDMA depends on the maximum cross correlation of the sequences employed by users.

Mathematical Formalization of Interferences of Signal Sets

- Notation:
  - α a primitive element of a finite field F_{2^n};
  - Let $\mathbf{a} = \{a_i\}$ be a binary sequence of period N;

    r-decimation of **a**: $\mathbf{b} = \{b_i\}$ where $b_i = a_{ri}$;

    Left-shift operator: $L\mathbf{a} = a_1, a_2, \cdots$, and $L^i\mathbf{a} = a_i, a_{i+1}, \cdots$.

- Crosscorrelation of two sequences
- Signal sets

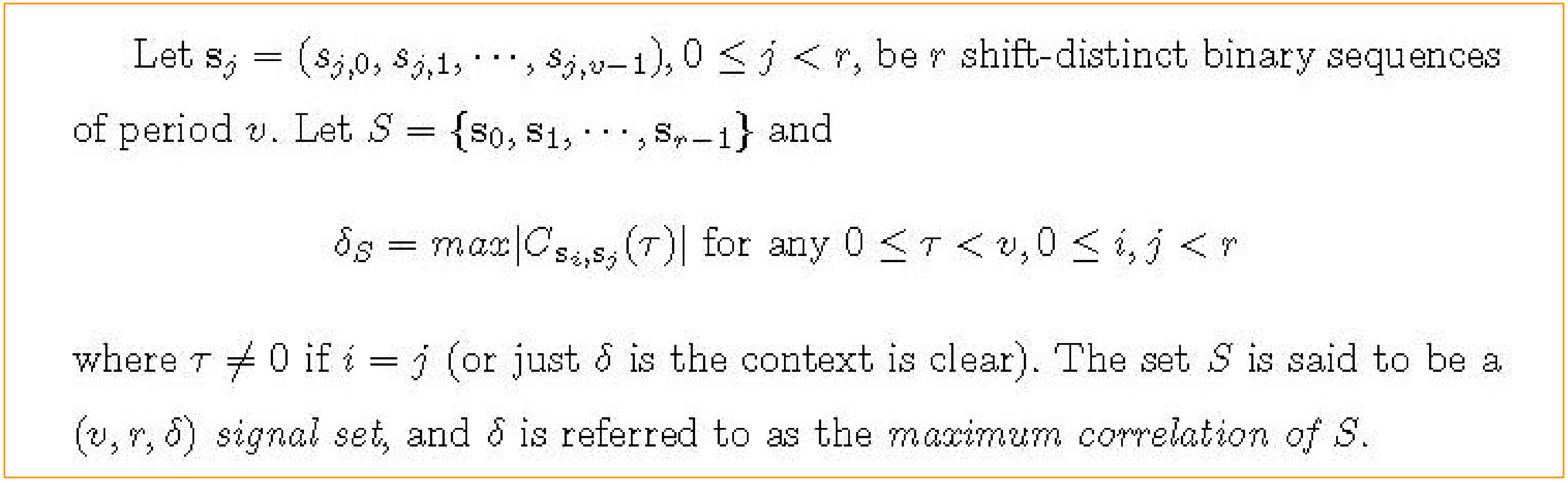
Crosscorrelation

A *crosscorrelation function* between two periodic binary sequences $\mathbf{a} = \{a_i\}$, of period v, and $\mathbf{b} = \{b_i\}$, of period u, over $\mathbb{F}_2$ is defined by

$$C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_{i+\tau}+b_i}, \tau = 0, 1, \cdots$$

where $N = gcd(v, u)$, the greatest common factor of v and u.

Signal Sets



Let $\mathbf{s}_j = (s_{j,0}, s_{j,1}, \cdots, s_{j,v-1}), 0 \le j < r$, be r shift-distinct binary sequences of period v. Let $S = \{\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{r-1}\}$ and

$$\delta_S = max|C_{\mathbf{s}_i,\mathbf{s}_j}(\tau)| \text{ for any } 0 \le \tau < v, 0 \le i, j < r$$

where $\tau \neq 0$ if $i = j$ (or just δ is the context is clear). The set S is said to be a (v, r, δ) *signal set*, and δ is referred to as the *maximum correlation of* S.

Known signal set with low cross correlation

- Gold-pair construction
- Kasami (small) set construction
- Bent function signal set construction
- Interleaved construction (today’s talk))
- Z_4 construction

Signal Sets in Practice

- Orthogonal code (or Walsh code or Hadamard code) in IS-95 CDMA
- Gold-pair construction (for large capacity, 3GPP)
- Kasami (small) set construction (for large capacity, 3GPP)
- Z_4 construction (3GPP, sacrificed correlation for large capacity)

Interleaved Sequences

A design for large linear span (certain) security at price of sacrificed cross correlation!

- Definition of Interleaved Sequences
- Constructions of Signal Sets from Interleaved Sequences
- Profiles of the Interleaved Signal Sets
- Implementation

Definition of Interleaved Sequences

Let $\underline{\mathbf{u}} = (u_0, u_1, \cdots, u_{st-1})$ be a binary sequence of period *st*. We can write the elements of the sequence *A* into a *s* by *t* array as follows:

$$\begin{pmatrix} u_0 & u_1 & \cdots & u_{t-1} \\ u_t & u_{t+1} & \cdots & u_{t+t-1} \\ u_{2t} & u_{2t+1} & \cdots & u_{2t+t-1} \\ \vdots & & & \\ u_{(s-1)t} & u_{(s-1)t+1} & \cdots & u_{(s-1)t+t-1} \end{pmatrix}$$

If all these column sequences are phase shifts of a binary sequence, say $\underline{\mathbf{a}}$, of period *s*, then we say that $\underline{\mathbf{u}}$ is a (*s*, *t*)-*interleaved sequence*.

Let $\underline{\mathbf{u}}_j$ denote the *jth* column of the above array. Then we have

$$\underline{\mathbf{u}}_j = L^{e_i}(\underline{\mathbf{a}}),\ 0 \le j < t$$

where *L* is the left shift operator and the e_j are nonnegative integers with $0 \le e_j < s$.

Example 1.

Let **e** = (3, 6, 5, 5, 2, 3, 5) and **a** = (1, 1, 1, 0, 1, 0, 0), a binary *m*-sequence of period 7. Then a (7, 7) array is as follows:

$$\begin{matrix}
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1
\end{matrix}$$

A (7, 7) interleaved sequence

u = 0 0 0 0 1 0 0 1 1 0 0 0 1 0
0 1 1 1 1 0 1 0 1 1 1 0 0 1
1 0 1 1 0 1 1 1 1 0 0 1 1 0
1 0 1 1 1 1 1

Constructions of (v^2, v+1, 2v+3) signal sets

Procedure 1:

1. Choose **a** = (a_0, a_1, ..., a_{v-1}) and **b** = (b_0, b_1, ..., b_{v-1}), two binary sequence of period v with 2-level auto-correlation.

2. Choose **e** =(e_0, e_1, ..., e_{v-1}), an integer sequence whose elements taken from $\boldsymbol{Z}_v$, a set consisting of integers modulo v.

3. Construct $\underline{\mathbf{u}} = (u_0, u_1, \cdots, u_{v^2-1})$, a (v, v) interleaved sequence whose *jth* column sequence is given $L^{e_j}(\underline{a})$.

4. Set $\underline{s}_j = (s_{j,0}, s_{j,1}, \cdots, s_{j,v^2-1}), 0 \le j < v$ whose elements are defined by

$$s_{j,i} = u_i + b_{j+i}, \text{ or } \underline{\mathbf{s}} = \underline{\mathbf{u}} + L^j(\underline{\mathbf{b}}), \quad 0 \le j < v$$

5. A signal set S is defined by

$$S = \{\underline{\mathbf{u}}, \underline{\mathbf{s}}_j\text{:} \ \ j = 0, 1, \text{....}, v\text{-}1\}.$$

Example 2. Let $v = 7$.

1. Choose $\underline{\mathbf{a}} = (1\ 1\ 1\ 0\ 1\ 0\ 0)$ and $\mathbf{b} = (1\ 0\ 0\ 1\ 0\ 1\ 1)$, m-sequences of period 7.
2. Choose $\underline{\mathbf{e}} = (3, 6, 5, 5, 2, 3, 5)$.
3. Construct the interleaved sequence $\underline{\mathbf{u}}$:
4. Construct $\underline{\mathbf{s}}_j$: j =0, 1, ..., 6.

The column sequences of $\underline{\mathbf{s}}_0$ can be obtained from the sequence $\underline{\mathbf{u}}$ by complement of columns of $\underline{\mathbf{u}}$ whose indexes correspond to 1's in the sequence $\underline{\mathbf{b}}$; the column sequences of $\underline{\mathbf{s}}_1$ obtained from $\underline{\mathbf{u}}$ by complement of those in the sequence $\underline{\mathbf{b}}$ with a phase shift 1, and so on.

$$\begin{array}{rccccccc}
\underline{\mathbf{b}} = & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
 & \downarrow & & & \downarrow & & \downarrow & \downarrow \\
 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
\underline{\mathbf{u}} = & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
 & 1 & 0 & 1 & 1 & 1 & 1 & 1
\end{array}$$

$\underline{\mathbf{s}}_0 = \underline{\mathbf{u}} + \underline{\mathbf{b}}$:

$$\begin{matrix}
1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0
\end{matrix}$$

$\underline{\mathbf{s}}_1 = \underline{\mathbf{u}} + L\underline{\mathbf{b}}$:

$$\begin{matrix}
0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0
\end{matrix}$$

$\underline{\mathbf{s}}_0 = \underline{\mathbf{u}} + \underline{\mathbf{b}} =$ 1 0 0 1 1 1 1 0 1 0 10 0 1 1 1 1 0 1 1 0 1 1 1 0 0 1 0 0
0 1 0 0 0 0 0 1 0 1 1 0 1 0 0 1 0 1 0 0

$\underline{\mathbf{s}}_1 = \underline{\mathbf{u}} + \underline{\mathbf{b}} =$0 0 1 0 0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 1 1 0 1 0 0 1 1 0 0 1
1 1 0 0 0 1 1 0 0 1 0 0 0

$\underline{\mathbf{s}}_2 = \underline{\mathbf{u}} + L^2\underline{\mathbf{b}} =$ 0 1 0 1 0 1 0 1 0 0 1 1 0 0 0 0 1 0 0 1 1 0 0 1 0 1 1 1 1 1 1 0 1 0 1
1 0 0 1 0 0 0 1 1 1 0 0 0 1

$\underline{\mathbf{s}}_3 = \underline{\mathbf{u}} + L^3\underline{\mathbf{b}} =$ 1 0 1 1 0 0 0 0 1 1 1 1 1 0 1 1 0 0 0 0 1 1 1 0 0 1 0 1 0 0 0 0 1 1 1 0
1 1 1 0 1 0 0 0 0 0 0 1 1

$\underline{\mathbf{s}}_4 = \underline{\mathbf{u}} + L^4\underline{\mathbf{b}} =$ 0 1 1 1 1 0 1 1 0 1 1 0 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 1 0
1 1 1 1 1 1 1 0 0 1 1 0

$\underline{\mathbf{s}}_5 = \underline{\mathbf{u}} + L^5\underline{\mathbf{b}} =$1 1 1 0 1 1 0 0 0 1 0 0 0 0 1 0 0 1 1 1 1 1 0 0 1 0 1 1 0 1 0 1 0 0 1 0 0 1
0 1 0 0 0 1 0 1 1 0 1

$\underline{\mathbf{s}}_6 = \underline{\mathbf{u}} + L^6\underline{\mathbf{b}} =$ 1 1 0 0 0 0 1 0 0 0 0 1 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 0 1 1 1 1 1 0 0 0 0
0 0 1 1 0 1 1 1 0 1 0

5. Set $S = \{\underline{\mathbf{u}}, \underline{\mathbf{s}}_0, \underline{\mathbf{s}}_1, \ldots, \underline{\mathbf{s}}_6\}$.

Constructions for (v^2, v+1, 2v+3) signal sets (Cont.)

Theorem 1. If the shift sequence e satisfies the following condition,

$$(*)\begin{cases} e_j \neq 0, 0 \leq j < v \\ \left|\{e_j - e_{j+s} \mid 0 \leq j < v - s\}\right| = v - s, \text{for all } 1 \leq s < v \end{cases}$$

then S is a (v^2, v+1, 2v+3) signal set. Moreover, the cross-correlation and out of phase auto-correlation values of any two sequences in S belong to the set {1, -v, v+2, 2v+3, -2v-1}.

* Gong (1995) introduced the idea of Procedure 1 for constructing ($(2^n-1)^2$, 2^n, $1+2^n$) signal sets where $v = 2^n-1$ and both **a** and **b** are m-sequences of period 2^n-1, and proved Theorem 1.

We can verify that the exponent sequence in Example 4 satisfies (*). From Theorem 1, it is a (49, 8, 17) signal set.

Shortened M-sequence Construction

Procedures for constructing the exponent sequence **e** which satisfies the condition (*).

Construction A (Shortened M-sequence Construction)

$((2^n\text{-}1)^2, 2^n, 1+2^{n+1})$ signal set:

1. Choose a primitive polynomial $f(x)$ over $GF(2)$ of degree $2n$ as the characteristic polynomial of a LFSR and generate $GF(2^{2n})$ by $f(\alpha)=0$.

2. Set the initial state of the LFSR as follows

$$d_0 = Tr(1) = 0, d_1 = Tr(a), \cdots, d_{2n-1} = Tr(a^{2n-1})$$

and generate a m-sequence $\{d_i\}$ of period 2^{2n}-1.

3. Arrange $\{d_i\}$ into a (r, v) array where $s = 2^n+1$ and $v = 2^n$-1:

$$D = \begin{pmatrix} 0 & d_1 & d_2 & \cdots & d_{s-2} & d_{s-1} \\ 0 & d_{s+1} & d_{s+2} & \cdots & d_{s+s-2} & d_{2s-1} \\ \vdots & & & & & \\ 0 & d_{(v-1)s+1} & d_{(v-1)s+2} & \cdots & d_{(v-1)s+s-2} & d_{vs-1} \end{pmatrix}$$

Let U be a matrix obtained from D by deleting the first and the last columns, then U gives an interleaved sequence **u** of period $(2^n\text{-}1)^2$ which has column sequence **a** given by $\{Tr(\alpha^i)\}$ where $\beta = \alpha^s$ and the exponent sequence satisfied (*).

4. Select **b** a binary 2-level sequence of period 2^n - 1. Continue the Procedure 1, we get the signal set S.

Example 3. Interleaved Generator (49, 8, 17):

1. Choose a primitive polynomial $f(x) = x^6+x+1$ for generating m-sequence $\{d_i\}$ with the initial state $(Tr(1), Tr(\alpha), \ldots, Tr(\alpha^5)) = (0, 0, 0, 0, 0, 1)$ and arrange it into a 9 by 7 array D:

$$
\begin{array}{ccccccccc}
\text{Cut} & & & & & & & & \text{Cut} \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}
$$

→

2. By deleting the first and the last columns of D, we have

$$
\begin{array}{ccccccc}
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1
\end{array}
$$

which is the sequence $\underline{\mathbf{u}}$ given in Example 4.

Profile of Randomness of (49, 8, 17)

1. Period: 49
2. 8 shift distinct sequences
3. The maximal magnitude of the cross correlation: 17
4. The cross correlation takes five values:

   {1, -7, 9, 17, -15}
5. Balance: 25 0's and 24 1's
6. Linear span: 24 except for **u** where **u** has linear span 21.

Compare it with the Kasami set with parameters (63, 8, 9)!
(An example of scarified the correlation for linear span!)

Construction B: $(p^2, p+1, 2p+3)$ signal set (p prime).

1. Choose **a** and **b**, two quadratic residue sequences modulo p.

2. Choose a, a primitive element of $GF(p)$.

3. Compute: $e_j = \alpha^j, 0 \leq j < p$.

Example 4. Let $p = 11$.

a = (1 1 0 1 1 1 0 0 0 1 0) and **b** = (1 0 1 0 0 0 1 1 1 0 1)
which are shift-distinct quadratic sequences of period 11.

Since 2 is a primitive element of $GF(11)$, then we compute that $e_j = 2^j$ mod 11, $0 \leq j < 11$. So

e = (1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1).

Construct the interleaved sequence $\underline{\mathbf{u}}$:

$\underline{\mathbf{a}}$ = (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)

$\underline{\mathbf{e}}$ = (1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1)

$\underline{\mathbf{u}}$=

*	-	*	-	-	-	*	*	*	-	*
1	0	1	0	1	0	1	0	1	0	1
0	1	1	1	0	1	0	0	1	0	0
1	1	0	0	0	1	1	1	1	0	1
1	1	0	1	0	0	1	0	0	1	1
1	0	0	1	1	1	0	1	0	0	1
0	0	1	0	0	1	1	1	0	1	0
0	0	0	1	1	1	1	0	1	1	0
0	1	1	1	1	0	1	1	0	0	0
1	0	1	1	0	0	0	1	1	1	1
0	1	0	0	1	0	0	1	1	1	0
1	1	1	0	1	1	0	0	0	1	1

Construct S, a (121, 12, 25) signal set:

$\underline{\mathbf{s}}_0 = \underline{\mathbf{u}} + \underline{\mathbf{b}}$

0	0	0	0	1	0	0	1	0	0	0
1	1	0	1	0	1	1	1	0	0	1
0	1	1	0	0	1	0	0	0	0	0
0	1	1	1	0	0	0	1	1	1	0
0	0	1	1	1	1	1	0	1	0	0
1	0	0	0	0	1	0	0	1	1	1
1	0	1	1	1	1	0	1	0	1	1
1	1	0	1	1	0	0	0	1	0	1
0	0	0	1	0	0	1	0	0	1	0
1	1	1	0	1	0	1	0	0	1	1
0	1	0	0	1	1	1	1	1	1	0

$S = \{\underline{\mathbf{s}} = \underline{\mathbf{u}} + L^i\underline{\mathbf{b}}, 0 \leq i < 11, \underline{\mathbf{u}}\}$.

Profile of *S*

1. Period: 121
2. 12 shift distinct sequences
3. The minimal maximal magnitude of the cross correlation: 25
4. The cross correlation takes five values:

   {1, -11, 13, 25, -23}
5. Balance: 61 0's and 60 1's
6. Linear span: 55

Profile of Interleaved Constructions A and B

1. S is a $((2^n-1)^2, 2^n, 1+2^{n+1})$-signal set and $(p^2, p+1, 2p+3)$-signal set from Constructions A and B respectively.

2. The cross correlation takes five values:

$$\{1, -v, v+2, 2v+3, -2v-1\}$$

where $v = 2^n-1$ or $v = p$ in Constructions A and B respectively.

3. Each signal in S except for $\underline{\mathbf{u}}$ has $(v^2+1)/2$ zeros and $(v^2-1)/2$ ones. In other words, all signals in S except for $\underline{\mathbf{u}}$ satisfy the balance property.

4. For $v = 2^n-1$ in Construction A, the linear span of any sequence in S is given by $(2^n-1)LS(\underline{\mathbf{a}}) + LS(\underline{\mathbf{b}})$ except for $\underline{\mathbf{u}}$ where $\underline{\mathbf{u}}$ has linear span

$$(2^n-1)LS(\underline{\mathbf{a}}).$$

For $v = p$, each sequence in S, except for $\underline{\mathbf{u}}$, has linear span

$$(p-1)p/2.$$

Implementations

Construction A, which generates $((2^n-1)^2, 2^n, 1+2^{n+1})$-signal sets, can be implemented by using two binary sequence generators with 2-level auto-correlation of period $2^{2n}-1$ and 2^n-1 respectively together a shrinking operation: deleting 2 consecutive bits for every 2^n+1 consecutive bits from the 2-level binary sequence of period $2^{2n}-1$.

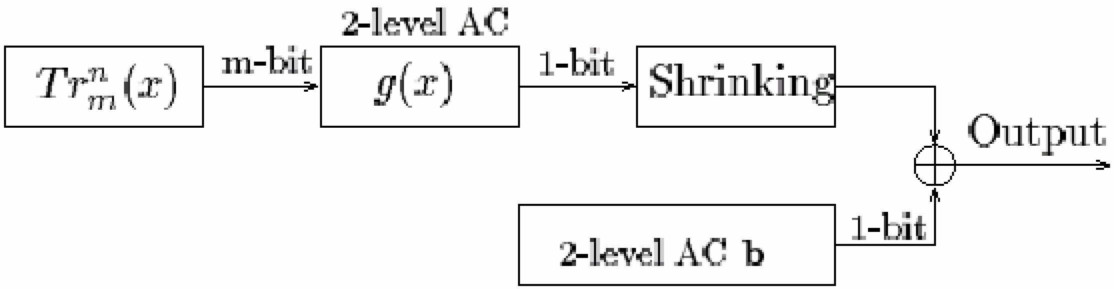
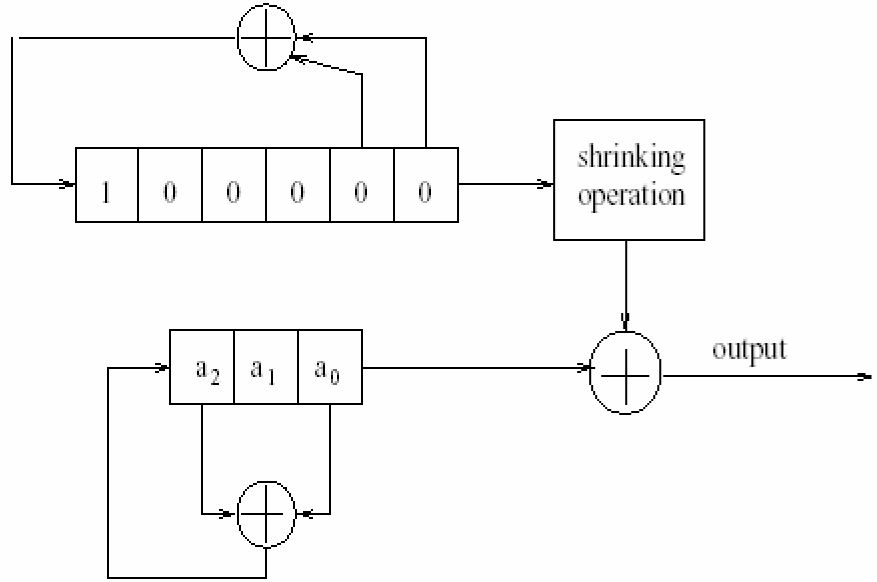


Figure 10.9: Galois configuration of $((2^m-1)^2, 2^m+1, 1+2^{m+1})$ signal sets.



Implementation of Interleaved Signal Set in Example 3

Implementations (Cont.)

For Construction B, it can be implemented by means of pre-storage of the exponent sequence **e** and the quadratic sequence **a** (here we choose **b** = **a**) for small p (for example, $p < 2^{30}$).

References

- G. Gong, New Designs for signal sets with low cross-correlation, balance property and large linear span: $GF(p)$ Case, *IEEE Trans. on Inform. Theory*, vol.48, No.11, November 2002, pp.2847-2867.
- G. Gong, Correlation among signal sets, Invited talk, at AMS, May 13-16, 2004, Houston.