

Correlation Among Signal Sets



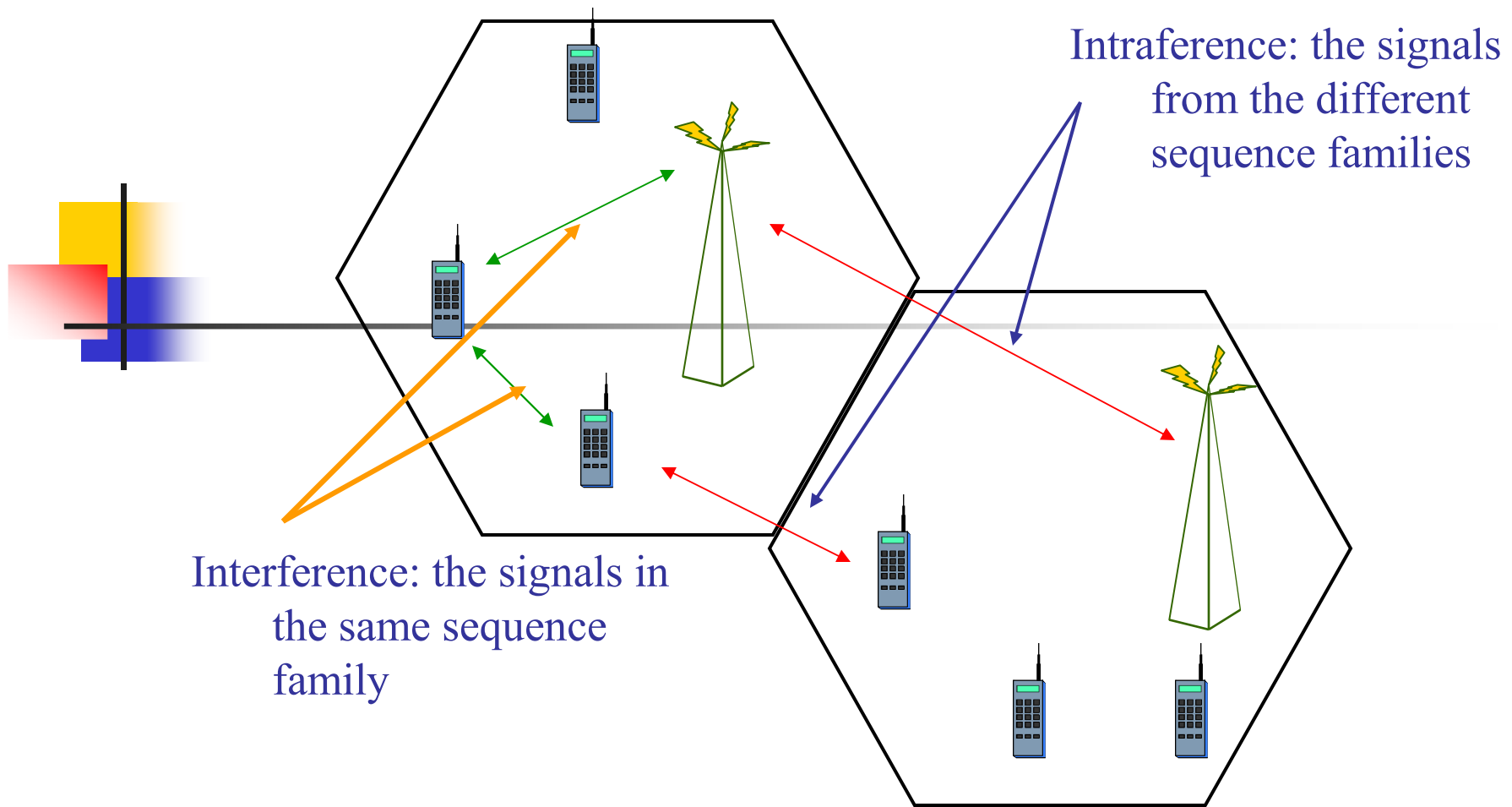
Guang Gong

Department of Electrical & Computer
Engineering
University of Waterloo
CANADA



Presentation Outline

- Intraference Among Signal Sets
- Construction of Kasami (Small) Signal Sets with Low Intraference
- Construction of Generalized Kasami (Small) Signal Sets with Low Intraference
- Construction of Interleaved Signal Sets with Low Intraference
- Cryptographical Properties of the Corresponding Boolean Functions
- Discussions and Open Questions



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 Intraferences Among 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 \mathbf{a} : $\mathbf{b} = \{b_i\}$ where $b_i = a_{ri}$;
 - Left-shift operator: $L\mathbf{a} = a_1, a_2, \dots$, and $L^i\mathbf{a} = a_i, a_{i+1}, \dots$.
- Crosscorrelation of two sequences
- Signal sets
- Intraference between any two signal sets
- Intraference among a family of 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

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

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

Signal Sets

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

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

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
- \mathbb{Z}_4 construction

Intraference between two signal sets

Definition 1. Let S and T be two shift distinct signal sets with parameters (v, r, δ_S) and (u, s, δ_T) respectively. Let

$$\delta_{S,T} = \max |C_{s,t}(\tau)|, \text{ for } 0 \leq \tau < v, s \in S, t \in T.$$

Then

$$\Delta = \max\{\delta_{S,T}, \delta_S, \delta_T\}$$

is said to be the maximum correlation between S and T .

Intraference among a family of signal sets

Definition 2. Let $\{S_1, S_2, \dots, S_k\}$ be k shift distinct signal sets with parameters (v_i, r_i, δ_i) , $i = 1, \dots, k$. We denote δ_{S_i, S_j} and δ_{S_i} by $\delta_{i,j}$ and δ_i for convenience. By this notation, we have $\delta_i = \delta_{i,i}$. The maximum correlation among the signal sets S_1, \dots, S_k is defined as

$$\Delta = \max\{\delta_{i,j}, 1 \leq i, j \leq k\}.$$

Construction of Kasami (Small) Signal Sets

Construction of Kasami (Small) Signal Sets: Let $\mathbf{s}_\lambda = \{s_{\lambda,i}\}$ be a binary sequence whose elements are given by

$$s_{\lambda,i} = f_\lambda(\alpha^i), i = 0, 1, \dots, \text{ where} \quad (1)$$

$$f_\lambda(x) = \text{Tr}_1^m (\text{Tr}_m^n(x^2) + \lambda x^d), \lambda \in \mathbb{F}_{2^m}, x \in \mathbb{F}_{2^n}. \quad (2)$$

A signal set S consists of \mathbf{s}_λ for all $\lambda \in \mathbb{F}_{2^m}$, i.e.,

$$S = \{\mathbf{s}_\lambda | \lambda \in \mathbb{F}_{2^m}\}. \quad (3)$$

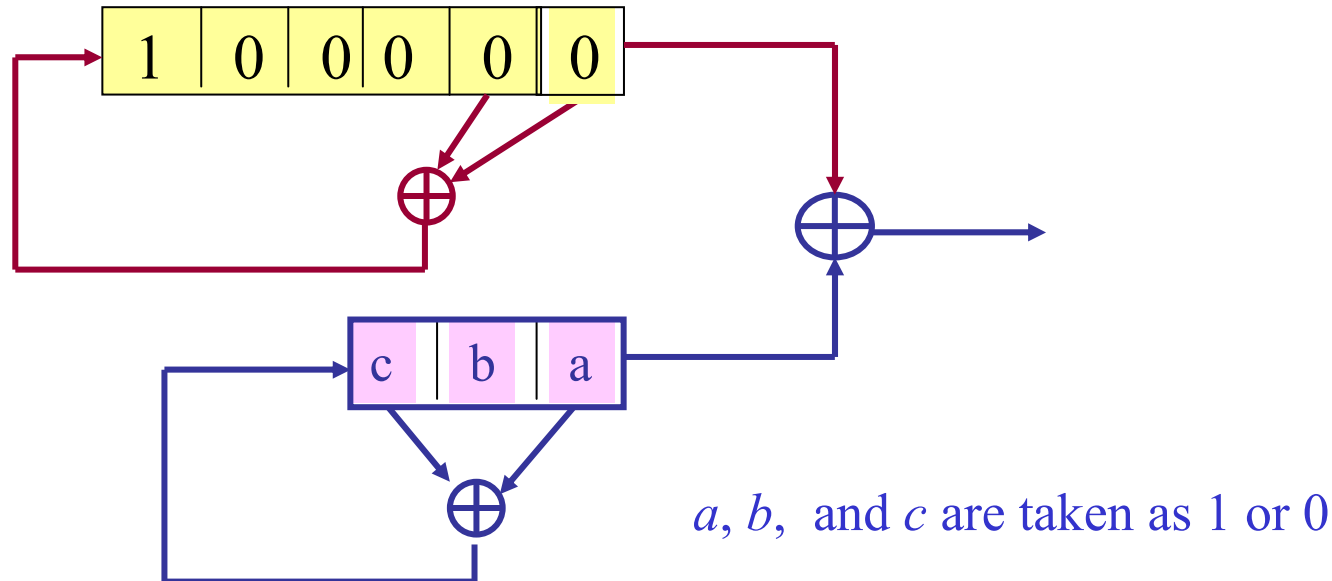
\mathbf{s}_λ is said to be a *Kasami (small set) sequence* and S a *Kasami (small) signal set*. Note that $f_\lambda(x)$ is the trace representation of \mathbf{s}_λ .

Fact 1 (Kasami, 1969) S is a $(2^n, 2^m, 2^m + 1)(n = 2m)$ signal set. Moreover, crosscorrelation of any pair of sequences in S or out-of-phase autocorrelation of any sequence in S is 3-valued and belongs to $\{-1, -1 \pm 2^m\}$.

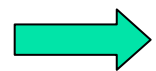
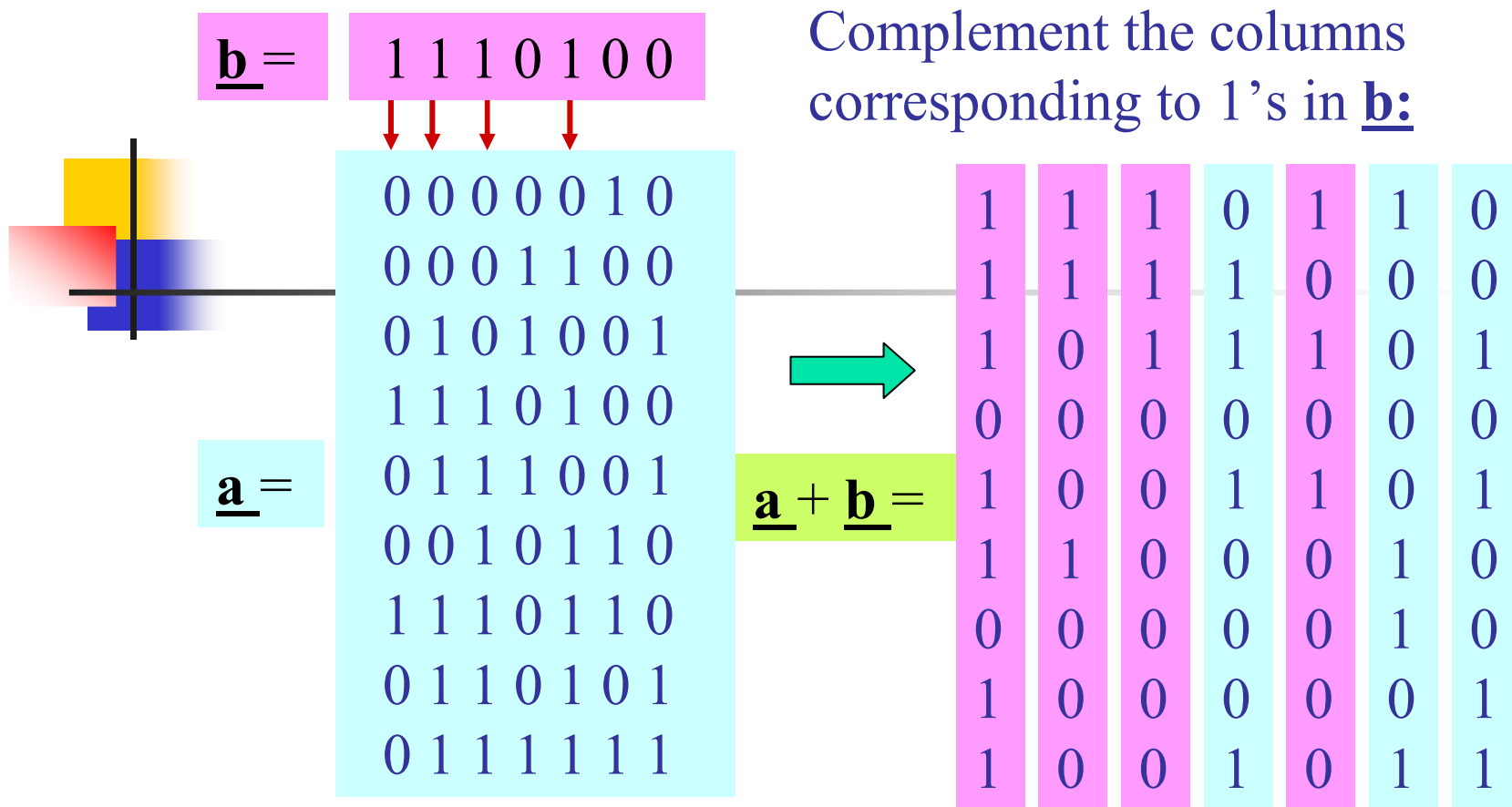
Example 1. Design a (63, 8, 9) Kasami signal set.

LFSR Implementation:

- Select $n = 6$ and $f(x) = x^6 + x + 1$; set α be a root of $f(x)$ in $GF(2^6)$.
- Compute the minimal polynomial of α^9 which gives $g(x) = x^3 + x^2 + 1$.



The correlation values are: -1, 7, - 9.



Write it row by row from the most left upper corner:

$\underline{s}_1 = 1110110111100010111010000001001101$
 $1100010000001010001011001011$

Kasami Signal Sets with Low Intraference



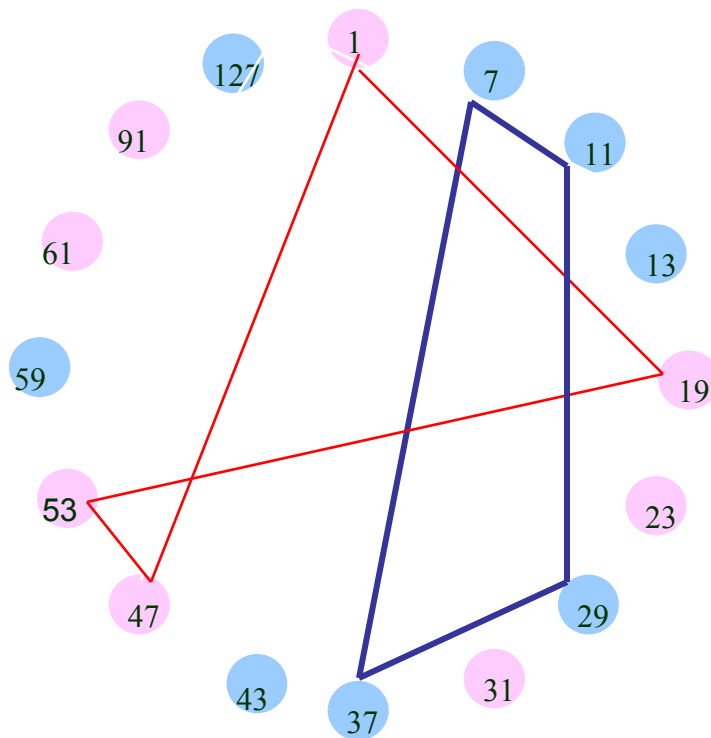
Let $S^{(r)} = \{s^{(r)} \mid s \in S\}$ where $r = 2^m + 3$.

Theorem 1. *The maximum cross correlation between any of two sequences in $S \cup S^{(r)}$, denoted by Δ , is given by*

$$\Delta = 2^{m+1} + 2^m - 1.$$

Moreover, crosscorrelation of any pair of sequences in $S \cup S^{(r)}$ or out-of-phase autocorrelation of any sequence in $S \cup S^{(r)}$ is five-valued and belongs to $\{-1 - 2^m, -1, -1 + 2^m, -1 + 2^{m+1}, -1 + 2^{m+1} + 2^m\}$.

Example 2. Let $n = 8$, so $m = 4$. There are 16 shift-distinct Kasami signal sets with parameters $(255, 16, 17)$. In this case, $r = 19$. Thus, the result in Theorem 1 partitions 16 shift-distinct Kasami signal sets into four groups. In each group, any neighboring nodes (see below) has the minimum maximum cross correlation value 47 (compared it with the maximum correlation value 17 in each individual Kasami signal set).



Note that for $n = 10$, the minimum maximum intraference is 95 between two shift-distinct Kasami sets, arranged according to Theorem 1, and 33 for each Kasami signal set with period 1023.

Construction of Generalized Kasami Signal Sets: Let $g(x) : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2$ be an orthogonal function (i.e., the evaluation of $g(x)$ is a 2-level autocorrelation sequence of period $2^m - 1$), and let $\mathbf{s}_\lambda = \{s_{\lambda,i}\}_{i \geq 0}$ whose elements are given by

$$s_{\lambda,i} = f_\lambda(\alpha^i), i = 0, 1, \dots, \text{ where} \quad (15)$$

$$f_\lambda(x) = g(Tr_m^n(x^2) + \lambda x^d), \lambda \in \mathbb{F}_{2^m}, x \in \mathbb{F}_{2^n}. \quad (16)$$

So, $f_\lambda(x)$ is the trace representation of \mathbf{s}_λ . A signal set $S(g)$ consists of \mathbf{s}_λ for all $\lambda \in \mathbb{F}_{2^m}$, i.e.,

$$S(g) = \{\mathbf{s}_\lambda | \lambda \in \mathbb{F}_{2^m}\}. \quad (17)$$

$S(g)$ is said to be a *generalized Kasami (small) signal set*.

Fact 2 $S(g)$ is a $(2^n, 2^m, 2^m + 1)$ ($n = 2m$) signal set for any orthogonal function g . Furthermore, the crosscorrelation of any pair of sequences in $S(g)$ or out-of-phase autocorrelation of a sequence in $S(g)$ is 3-valued and belongs to $\{-1, -1 \pm 2^m\}$.

Generalized Kasami with Low Intraference

Let $T = \{s^{(r)} \mid s \in S(g)\}$ where $r = 2^m + 3$.

Theorem 2. *The maximum cross correlation between $S(g)$ and T , say Δ , is given by*

$$\Delta = 2^{m+1} + 2^m - 1.$$

More precisely, crosscorrelation of any pair of sequences in $S(g) \cup T$ or out-of-phase autocorrelation of any sequence in $S(g) \cup T$ is five-valued and belongs to $\{-1 - 2^m, -1, -1 + 2^m, -1 + 2^{m+1}, -1 + 2^{m+1} + 2^m\}$.

Interleaved Signal Sets

1. Choose $\mathbf{a} = (a_0, a_1, \dots, a_{v-1})$ and $\mathbf{b} = (b_0, b_1, \dots, b_{v-1})$, two binary sequences of period v with 2-level autocorrelation.
2. Pick $\mathbf{e} = (e_0, e_1, \dots, e_{v-1})$, an integer sequence whose elements are taken from \mathbf{Z}_v , which satisfies the difference condition:

$$\text{for each } 1 \leq s < v, \text{ the differences } e_j - e_{j+s}, 0 \leq j < v - s \text{ are all distinct}$$

3. Construct $\mathbf{u} = (u_0, u_1, \dots, u_{v^2-1})$, a (v, v) interleaved sequence whose j th column sequence is given by $L^{e_j}(\mathbf{a})$, i.e., $u_{iv+j} = a_{i+e_j}$.
4. Set

$$\mathbf{s}_j = (s_{j,0}, s_{j,1}, \dots, s_{j,v^2-1}), 0 \leq j < v$$

whose elements are defined by

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

5. A signal set $S(\mathbf{b})$ is defined as

$$S(\mathbf{b}) = \{\mathbf{s}_j \mid j = 0, 1, \dots, v-1\} \cup \{\mathbf{u}\}.$$



Interleaved Signal Sets (Cont.)

Then $S(\mathbf{b})$ is a $(v^2, v + 1, 2v + 3)$ signal set. Moreover, the crosscorrelation of any two sequences in S or the out-of-phase auto-correlation of any sequence in S belongs to the set $\{1, -v, v + 2, 2v + 3, -2v - 1\}$.

Example 3. Construct an interleaved signal set with parameters (49, 8, 17). Let $v = 7$.

1. Choose $\underline{\mathbf{a}} = (1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0)$ and $\underline{\mathbf{b}} = (1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1)$, 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 $\underline{\mathbf{s}}_j$: $j = 0, 1, \dots, 6$.

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.

$\underline{\mathbf{b}} = 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1$

↓ ↓ ↓ ↓

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 |

Interleaved Signal Sets with Low Intraference

Let $\mathbf{b} = \{b_i\}$ be an m -sequence of degree m , and $\mathbf{c} = \{c_i\}$ be a d -decimation of \mathbf{b} , i.e., $c_i = b_{id}, i = 0, 1, \dots$. We assume that d is taken from the set of the exponents which give the Gold-pair sequences with three valued cross correlation with \mathbf{b} . We denote

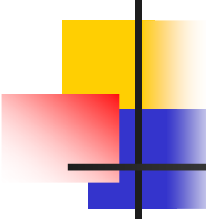
$$\mathbf{b}_{i+1} = \mathbf{b} + L^i(\mathbf{c}), i = 0, 1, \dots, 2^m - 2, \mathbf{b}_0 = \mathbf{b}, \text{ and } \mathbf{b}_{2^m} = \mathbf{c}$$

Theorem 3. Let $\mathcal{S} = \{S(\mathbf{b}_i) \mid 0 \leq i \leq 2^m\}$. For any pair of sequences $\mathbf{s} \in S(\mathbf{b}_i)$ and $\mathbf{t} \in S(\mathbf{b}_j)$, the cross correlation between \mathbf{s} and \mathbf{t} is bounded by

$$|C_{\mathbf{s}, \mathbf{t}}(\tau)| \leq 2^{m+1} + 2^{\lceil m/2 \rceil} + 1, 0 \leq \tau < v^2 - 1, \tau \neq 0 \text{ if } \mathbf{s} \neq \mathbf{t}.$$

Therefore, Δ , the maximum cross correlation of \mathcal{S} , is given by

$$\Delta = 2^{m+1} + 2^{\lceil m/2 \rceil} + 1.$$



Example 4. Let $v = 31 = 2^5 - 1$. Let \mathbf{b} be an m-sequence with period 31, and $\mathbf{c} = \mathbf{b}^{(5)}$. We have a Gold-pair set of period 31:

$$\mathbf{b}_{i+1} = \mathbf{b} + L^i(\mathbf{c}), i = 0, 1, \dots, 30, \mathbf{b}_0 = \mathbf{b}, \text{ and } \mathbf{b}_{32} = \mathbf{c}$$

So, there are 33 interleaved signal sets with parameters (961, 32, 65). Theorem 3 states that the cross correlation of any pair of sequences in the following set:

$$\Gamma = \bigcup_{i=0}^{32} \mathcal{S}(\mathbf{b}_i)$$

is upper bounded by 73.

Remark: Compare with the maximum correlation 65 in each interleaved signal sets. So, the intraferences among these signal sets do not degrade much, since it only slightly increases from 65 to 73.

Cryptographical Properties of the Corresponding Boolean Functions

The functions, defined below,

$$f(x) = \text{Tr}_1^m(\text{Tr}_m^n(ax + bx^r) + cx^{r-2}), \quad a, b \in F_{2^n}, c \in F_{2^m}$$

are functions from F_{2^n} to F_2 , which correspond to the trace representations of the sequences in the union of the Kasami signal set and its r decimation together with their shifted sequences.

Theorem 1 establishes that $f(x)$, for any a , b , and c , has nonlinearity

$$N_f = 2^{m+1} + 2^m - 1$$



Discussions and Open Questions

- How does one prove the intraference of the Kasami signals in Theorems 1 and 2 are minimum? The experimental results confirm that.
- It is unknown how to construct Gold-pair signal sets with low intraference. The experimental results show that they have a similar result as Kasami case. But no proof has been found.
- How to construct bent function signal sets and Z_4 signal sets with low intraference?