Low Correlation Zone Sequences over Finite Fields and Rings

Udaya Parampalli

Department of Computer Science and Software Engineering
University of Melbourne

IWSDA 2009, Fukuoka, Japan

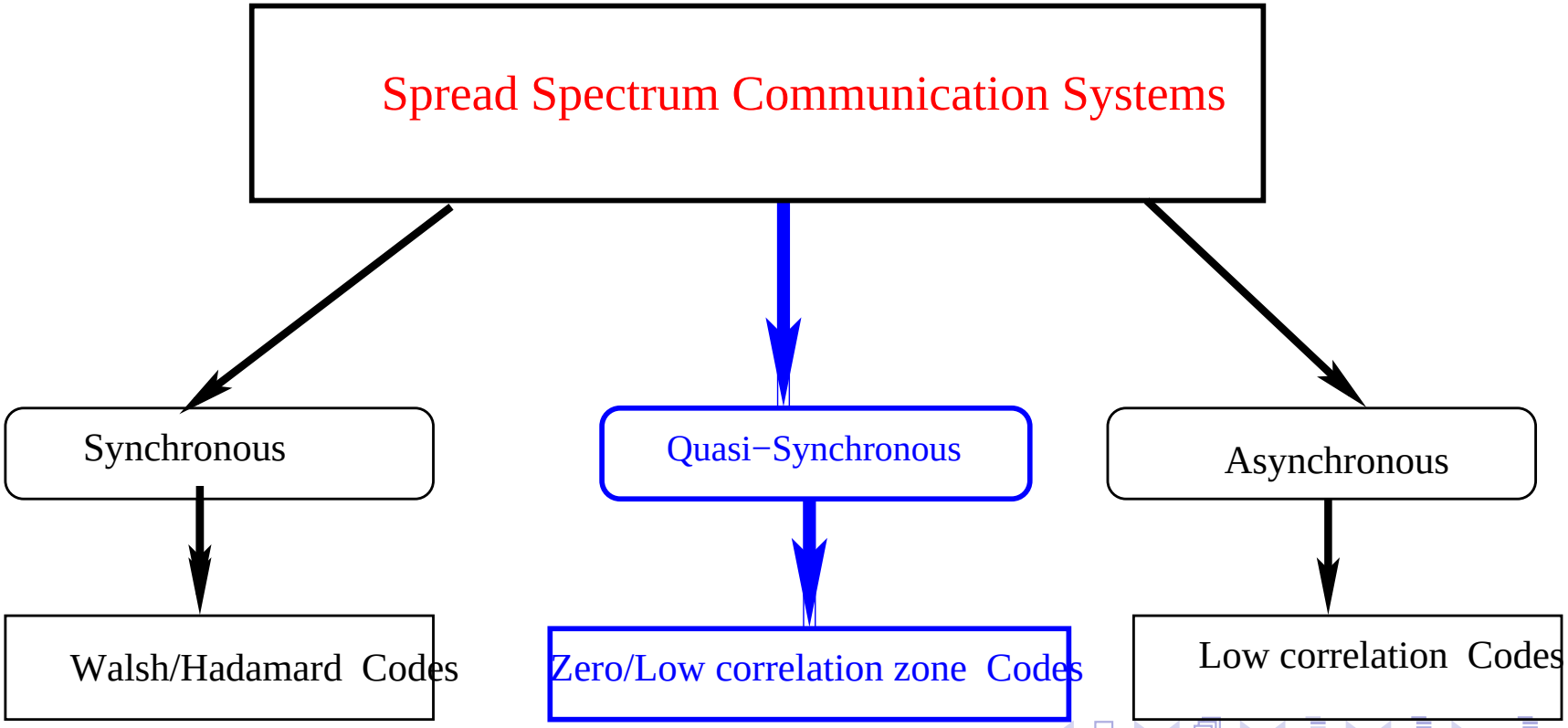
October 20, 2009

Table of Contents

Context

Spread Spectrum Systems

- Sequences with low correlations are used as signature sequences in spread spectrum communication technologies.



Periodic Correlation Function

Definition

Given two complex sequences $a = \{a_0, a_1, \ldots, a_{N-1}\}$ and $b = \{b_0, b_1, \ldots, b_{N-1}\}$ of period N, we define the periodic cross-correlation between a and b as

$$R_{a,b}(\tau) = \sum_{i=0}^{N-1} a_i \, b_{i+\tau}^{\star}, 0 \leq \tau < N,$$

where $\star$ denotes for complex conjugation.

- A key measure to determine similarity between two sequences in the CDMA context.
- Helps in determining optimal sequences for synchronization, code acquisition and channel identification.

Periodic Correlation Function

Definition

Given two complex sequences $a = \{a_0, a_1, \ldots, a_{N-1}\}$ and $b = \{b_0, b_1, \ldots, b_{N-1}\}$ of period N, we define the periodic cross-correlation between a and b as

$$R_{a,b}(\tau) = \sum_{i=0}^{N-1} a_i \, b_{i+\tau}^{\star}, 0 \leq \tau < N,$$

where $\star$ denotes for complex conjugation.

- A key measure to determine similarity between two sequences in the CDMA context.
- Helps in determining optimal sequences for synchronization, code acquisition and channel identification.

Periodic Correlation Function

Definition

Given two complex sequences $a = \{a_0, a_1, \ldots, a_{N-1}\}$ and $b = \{b_0, b_1, \ldots, b_{N-1}\}$ of period N, we define the periodic cross-correlation between a and b as

$$R_{a,b}(\tau) = \sum_{i=0}^{N-1} a_i \, b_{i+\tau}^{\star}, 0 \leq \tau < N,$$

where $\star$ denotes for complex conjugation.

- A key measure to determine similarity between two sequences in the CDMA context.
- Helps in determining optimal sequences for synchronization, code acquisition and channel identification.

Low Correlation Zone Requirement

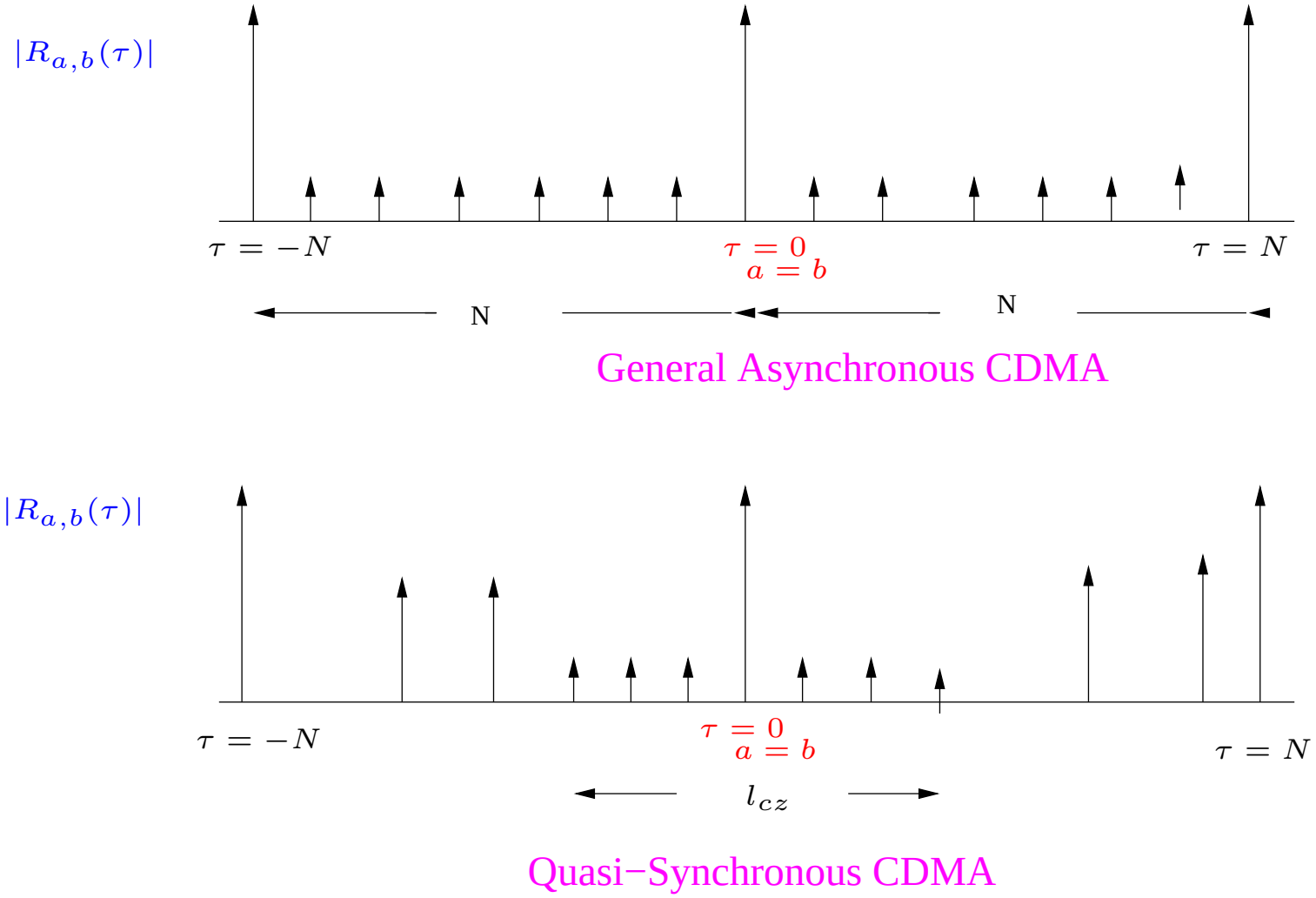


Figure: Correlation Zone

Orthogonality

Consider,

$$\{\mathcal{F} = \{a_0^r, a_1^r, \ldots, a_{N-1}^r\}; r = 1 \cdots M\},$$

a family of M sequences of each length N.
We say the family is **Orthogonal**, if:

$$R_{r,s}(\tau) = \sum_{i=0}^{N-1} a_i^r a_{i+\tau}^{s\star}, \left\{ \begin{array}{l} = N, \text{ for } \tau = 0, r = s \\ = 0, \text{ for } \tau = 0, r \neq s \end{array} \right\}$$

$\star$: Complex Conjugate Note that $R_{r,s}(\tau)$ is zero only for $\tau = 0$.

Walsh sequence set or vectors of Hadamard matrices satisfy the above criterion. They are widely used in synchronous CDMA communication systems.

Orthogonality

Consider,

$$\{\mathcal{F} = \{a_0^r, a_1^r, \ldots, a_{N-1}^r\}; r = 1 \cdots M\},$$

a family of M sequences of each length N.
We say the family is **Orthogonal**, if:

$$R_{r,s}(\tau) = \sum_{i=0}^{N-1} a_i^r a_{i+\tau}^{s\star}, \left\{ \begin{array}{l} = N, \text{ for } \tau = 0, r = s \\ = 0, \text{ for } \tau = 0, r \neq s \end{array} \right\}$$

$\star$: Complex Conjugate Note that $R_{r,s}(\tau)$ is zero only for $\tau = 0$.

Walsh sequence set or vectors of Hadamard matrices satisfy the above criterion. They are widely used in synchronous CDMA communication systems.

Generalized Quasi-Orthogonality

Consider,

$$\{\mathcal{F} = \{a_0^r, a_1^r, \ldots, a_{N-1}^r\}; r = 1 \cdots M\},$$

a family of M sequences of each length N.
For a small number ϵ $(\epsilon < N)$ and a zone l_{cz}, we say the family is **Generalized Quasi-Orthogonal** $(GQO(N, M, \epsilon, l_{cz}))$, if :

$$R_{r,s}(\tau) = \sum_{i=0}^{N-1} a_i^r a_{i+\tau}^{s\star}, \left\{ \begin{array}{l} = N, \text{ for } \tau = 0, r = s \\ = \epsilon, \text{ for } \tau = 0, r \neq s \\ = \epsilon, \text{ for } 0 < |\tau| \leq l_{cz} \end{array} \right\}$$

A requirement is that maximum non-trivial correlation amongst members of a GQO should be a small quantity.

Sequences satisfying this property $l_{cz} = 0$ are studied by [Yang,Kim,Kumar,2000]: Quasi-orthogonal CDMA systems, IEEE-IT, 2000.

Generalized Quasi-Orthogonality

Consider,

$$\{\mathcal{F} = \{a_0^r, a_1^r, \ldots, a_{N-1}^r\}; r = 1 \cdots M\},$$

a family of M sequences of each length N.
For a small number ϵ $(\epsilon < N)$ and a zone l_{cz}, we say the family is **Generalized Quasi-Orthogonal** $(GQO(N, M, \epsilon, l_{cz}))$, if :

$$R_{r,s}(\tau) = \sum_{i=0}^{N-1} a_i^r a_{i+\tau}^{s\star}, \left\{ \begin{array}{l} = N, \text{ for } \tau = 0, r = s \\ = \epsilon, \text{ for } \tau = 0, r \neq s \\ = \epsilon, \text{ for } 0 < |\tau| \leq l_{cz} \end{array} \right\}$$

A requirement is that maximum non-trivial correlation amongst members of a GQO should be a small quantity.

Sequences satisfying this property $l_{cz} = 0$ are studied by [Yang,Kim,Kumar,2000]: Quasi-orthogonal CDMA systems, IEEE-IT, 2000.

Polyphase sequences

- The above definitions are for any complex valued sequences. In practice the signature sequences in CDMA are generally defined over points on unit circle.
- Given two p-ary sequences $a = \{a_0, a_1, \ldots, a_{N-1}\}$ and $b = \{b_0, b_1, \ldots, b_{N-1}\}$ of period N, we define the periodic cross-correlation between a and b as

$$R_{a,b}(\tau) = \sum_{i=0}^{N-1} \omega^{a_i - b_{i+\tau}}, 0 \leq \tau < N,$$

where ω is the pth root of unity given by $\omega = e^{j2\pi/p}, j = \sqrt{-1}$.

Polyphase sequences

- The above definitions are for any complex valued sequences. In practice the signature sequences in CDMA are generally defined over points on unit circle.
- Given two p-ary sequences $a = \{a_0, a_1, \ldots, a_{N-1}\}$ and $b = \{b_0, b_1, \ldots, b_{N-1}\}$ of period N, we define the periodic cross-correlation between a and b as

$$R_{a,b}(\tau) = \sum_{i=0}^{N-1} \omega^{a_i - b_{i+\tau}}, 0 \leq \tau < N,$$

where ω is the pth root of unity given by $\omega = e^{j2\pi/p}, j = \sqrt{-1}$.

Aperiodic Correlation requirements

Consider $GQO(N, M, \epsilon, l_{cz})$. M sequences of length M, with low correlation zone l_{cz} and low correlation value ϵ.
We also sometimes need aperiodic correlations of sequences in ($GQO(N, M, \epsilon, l_{cz})$) satisfy the following property:

$$\delta_{r,s}(\tau) = \sum_{i=0}^{N-\tau} \omega^{a_i^r - a_{i+\tau}^s}, \left\{ \begin{array}{ll} = N, & \text{for } \tau = 0, r = s \\ \leq \epsilon, & \text{for } \tau = 0, r \neq s \\ \leq \epsilon, & \text{for } 0 < |\tau| \leq l_{cz} \end{array} \right\}.$$

In general it is difficult to optimise both aperiodic and periodic correlations.

The usual plan is first construct sequences with optimal periodic properties and then choose appropriate sequences with smaller aperiodic correlations.

Aperiodic Correlation requirements

Consider $GQO(N, M, \epsilon, l_{cz})$. M sequences of length M, with low correlation zone l_{cz} and low correlation value ϵ.
We also sometimes need aperiodic correlations of sequences in ($GQO(N, M, \epsilon, l_{cz})$) satisfy the following property:

$$\delta_{r,s}(\tau) = \sum_{i=0}^{N-\tau} \omega^{a_i^r - a_{i+\tau}^s}, \left\{ \begin{array}{ll} = N, & \text{for } \tau = 0, r = s \\ \leq \epsilon, & \text{for } \tau = 0, r \neq s \\ \leq \epsilon, & \text{for } 0 < |\tau| \leq l_{cz} \end{array} \right\}.$$

In general it is difficult to optimise both aperiodic and periodic correlations.

The usual plan is first construct sequences with optimal periodic properties and then choose appropriate sequences with smaller aperiodic correlations.

Aperiodic Correlation requirements

Consider $GQO(N, M, \epsilon, l_{cz})$. M sequences of length M, with low correlation zone l_{cz} and low correlation value ϵ.
We also sometimes need aperiodic correlations of sequences in ($GQO(N, M, \epsilon, l_{cz})$) satisfy the following property:

$$\delta_{r,s}(\tau) = \sum_{i=0}^{N-\tau} \omega^{a_i^r - a_{i+\tau}^s}, \left\{ \begin{array}{ll} = N, & \text{for } \tau = 0, r = s \\ \leq \epsilon, & \text{for } \tau = 0, r \neq s \\ \leq \epsilon, & \text{for } 0 < |\tau| \leq l_{cz} \end{array} \right\}.$$

In general it is difficult to optimise both aperiodic and periodic correlations.

The usual plan is first construct sequences with optimal periodic properties and then choose appropriate sequences with smaller aperiodic correlations.

Theoretical Limits

Bounds on correlations for Generalized Quasi-Orthogonal sequences

- Welch Bound on Correlations: For a family M periodic complex sequences of length N, the periodic correlations satisfy

$$R(\tau) \geq \sqrt{N}.$$

- Sidelnikov Bound: For the binary case,

$$R(\tau) \geq \sqrt{2N}.$$

- Several variations of the above bounds exist. But they all assume that l_{cz} is equal to length of the sequences. Hence they do not provide sufficient hint for optimal constructions.

Theoretical Limits

Bounds on correlations for Generalized Quasi-Orthogonal sequences

- Welch Bound on Correlations: For a family M periodic complex sequences of length N, the periodic correlations satisfy

$$R(\tau) \geq \sqrt{N}.$$

- Sidelnikov Bound: For the binary case,

$$R(\tau) \geq \sqrt{2N}.$$

- Several variations of the above bounds exist. But they all assume that l_{cz} is equal to length of the sequences. Hence they do not provide sufficient hint for optimal constructions.

Theoretical Limits

Bounds on correlations for Generalized Quasi-Orthogonal sequences

- Welch Bound on Correlations: For a family M periodic complex sequences of length N, the periodic correlations satisfy

$$R(\tau) \geq \sqrt{N}.$$

- Sidelnikov Bound: For the binary case,

$$R(\tau) \geq \sqrt{2N}.$$

- Several variations of the above bounds exist. But they all assume that l_{cz} is equal to length of the sequences. Hence they do not provide sufficient hint for optimal constructions.

Welch Boound on Periodic Sequences

Consider set of M vectors of length N.

$$\{(a_1^s, a_2^s, \cdots a_N^s), 0 \leq s < M\}, \text{ each of unit norm}$$

$$R_{s,s}(0) = \sum_{i=0}^{N-1} |a_i^s|^2 = 1.$$

Let δ be the non-trivial value of inner product between any two vectors in the matrix:

$$\text{Inner Product } \delta(r,s) = R_{r,s}(0) = \sum_{i=0}^{N-1} a_i^r (a_i^s)^\star.$$

$$\delta^{2k} = R_{s,t}(0)^{2k} \geq \frac{1}{(M-1)} \left[\frac{M}{\binom{N+k-1}{k}} - 1 \right]$$

Welch Boound on Periodic Sequences

Consider set of M vectors of length N.

$$\{(a_1^s, a_2^s, \cdots a_N^s), 0 \leq s < M\}, \text{ each of unit norm}$$

$$R_{s,s}(0) = \sum_{i=0}^{N-1} |a_i^s|^2 = 1.$$

Let δ be the non-trivial value of inner product between any two vectors in the matrix:

$$\text{Inner Product } \delta(r,s) = R_{r,s}(0) = \sum_{i=0}^{N-1} a_i^r (a_i^s)^\star.$$

$$\delta^{2k} = R_{s,t}(0)^{2k} \geq \frac{1}{(M-1)} \left[\frac{M}{\binom{N+k-1}{k}} - 1 \right]$$

Bound for Generalized Quasi-Orthogonal Sequences

Construct a new matrix H from M vectors of the previous slide: Include all vectors as rows of H and further add $1, \cdots l_{cz}$ shifts of these vectors to H.

$$H(iN + j, t] := a^i_{t+j},$$

where $0 \leq i \leq M - 1$, $0 \leq j \leq l_{cz} - 1$ and $0 \leq t < N$.
Clearly there are Ml_{cz} vectors in H; Using Inner-product theorem

$$\delta^{2k} \geq \frac{1}{(Ml_{cz} - 1)} \Big[\frac{Ml_{cz}}{\binom{N+k-1}{k}} - 1 \Big].$$

Because of $R_{s,t}(\tau) = R_{t,s}(-\tau)^\star$,

$$R_{s,t}(\tau) \geq \frac{1}{(Ml_{cz} - 1)} \Big[\frac{Ml_{cz}}{\binom{N+k-1}{k}} - 1 \Big], 0 \leq |\tau| \leq l_{cz}.$$

Bound for Generalized Quasi-Orthogonal Sequences

Construct a new matrix H from M vectors of the previous slide: Include all vectors as rows of H and further add $1, \cdots l_{cz}$ shifts of these vectors to H.

$$H(iN + j, t] := a^i_{t+j},$$

where $0 \leq i \leq M - 1$, $0 \leq j \leq l_{cz} - 1$ and $0 \leq t < N$.
Clearly there are Ml_{cz} vectors in H; Using Inner-product theorem

$$\delta^{2k} \geq \frac{1}{(Ml_{cz} - 1)} \Big[\frac{Ml_{cz}}{\binom{N+k-1}{k}} - 1 \Big].$$

Because of $R_{s,t}(\tau) = R_{t,s}(-\tau)^\star$,

$$R_{s,t}(\tau) \geq \frac{1}{(Ml_{cz} - 1)} \Big[\frac{Ml_{cz}}{\binom{N+k-1}{k}} - 1 \Big], 0 \leq |\tau| \leq l_{cz}.$$

Special Cases

- Welch's result assumes that norm of the vectors is unity, i.e, $R_{r,r}(0) = \sum_{i=0}^{N-1} |a_i^r|^2 = 1, 0 \leq r < M$.
- δ^2 is the value of non-trivial correlation between any two sequences with shifts in the range $0 \leq \tau < l_{cz}$.
  In practice, the sequences are over unit circle (polyphase or biphase), then $R_{r,r}(0) = N$.
- Choose $k = 1$ in the previous result and apply the previous theorem by normalizing sequences, we get

$$\delta^2 \geq N \frac{(Ml_{cz} - N)}{Ml_{cz} - 1}.$$

- Rearranging, we get

$$(Ml_{cz} - 1)(1 - \delta^2/N) \leq N - 1.$$

Special Cases

- Welch's result assumes that norm of the vectors is unity, i.e, $R_{r,r}(0) = \sum_{i=0}^{N-1} |a_i^r|^2 = 1, 0 \leq r < M$.
- δ^2 is the value of non-trivial correlation between any two sequences with shifts in the range $0 \leq \tau < l_{cz}$.
  In practice, the sequences are over unit circle (polyphase or biphase), then $R_{r,r}(0) = N$.
- Choose $k = 1$ in the previous result and apply the previous theorem by normalizing sequences, we get

$$\delta^2 \geq N \, \frac{(Ml_{cz} - N)}{Ml_{cz} - 1}.$$

- Rearranging, we get

$$(Ml_{cz} - 1)(1 - \delta^2/N) \leq N - 1.$$

Special Cases

- Welch's result assumes that norm of the vectors is unity, i.e, $R_{r,r}(0) = \sum_{i=0}^{N-1} |a_i^r|^2 = 1, 0 \leq r < M$.
- δ^2 is the value of non-trivial correlation between any two sequences with shifts in the range $0 \leq \tau < l_{cz}$.
  In practice, the sequences are over unit circle (polyphase or biphase), then $R_{r,r}(0) = N$.
- Choose $k = 1$ in the previous result and apply the previous theorem by normalizing sequences, we get

$$\delta^2 \geq N \, \frac{(Ml_{cz} - N)}{Ml_{cz} - 1}.$$

- Rearranging, we get

$$(Ml_{cz} - 1)(1 - \delta^2/N) \leq N - 1.$$

Zero/low correlation zone constraints

Zero Correlation Zone If $\delta^2/N = 0$, then we have,

$$Ml_{cz} \leq N.$$

If $l_{cz} = 1$, that is zone size is 1 and we want correlation to be zero, then Walsh or Hadamard sequence sets satisfy the bound with equality.

Low Correlation Zone If $\delta = 1$, then it is a case of low correlation zone, hence we have

$$Ml_{cz} \leq N + 1.$$

When $M = 1$, m-sequences meet this bound. So, from the above results it is clear that product of zone size and number of sequences should match the period.

Zero/low correlation zone constraints

Zero Correlation Zone If $\delta^2/N = 0$, then we have,

$$Ml_{cz} \leq N.$$

If $l_{cz} = 1$, that is zone size is 1 and we want correlation to be zero, then Walsh or Hadamard sequence sets satisfy the bound with equality.

Low Correlation Zone If $\delta = 1$, then it is a case of low correlation zone, hence we have

$$Ml_{cz} \leq N + 1.$$

When $M = 1$, m-sequences meet this bound. So, from the above results it is clear that product of zone size and number of sequences should match the period.

Early Constructions

- The first Construction: Binary sequences using PN and GMW constructions: [Lin,Chang,1997], [Long,Zhang,Hu 1998], [TangFan2000].
- Use d-form Functions: [Kim, Jang, No,Chung], 2005, Quaternary Constructions.
- Interleaved constructions (Optimal and nearly Optimal): [Tang,Udaya 2005] Using Hadamard Matrices.
- p-ary sequences making making is m-sequences: [Jang, No, Chung, Tang 2007].
- Construction via Sub-field Reduction: [Gong,Golomb,Song, 2007].

Trace Sequences

Let p be an odd prime, and $n = em$, e, m are integers. Let $q = p^e$, For simplicity denote $\mathbf{GF}(p^e)$ as $\mathbf{GF}(q)$ and $\mathbf{GF}(p^n)$ as $\mathbf{GF}(q^m)$.
Let $Tr_e^n(x)$ (and respectively

$$Tr_1^e(x) : \mathbf{GF}(q^m) \to \mathbf{GF}(q).$$

The trace map is given by:

$$Tr_e^n(x) = \sum_{i=0}^{m-1} x^{p^{ei}}, \quad Tr_1^e(x) = \sum_{i=0}^{e-1} x^{p^i}.$$

- Linear function.
- Random Function.
- Almost equal number of solutions: $Tr_e^n(x) = c$, for any $c \in \mathbf{GF}(q)$.

Interleaved Sequences

Left shift operator L on a is defined as
$L(a) = (a_1, \ldots, a_{N-1}, a_0)$.

- A component sequence: $\underline{a} = (a_i,\ i = 0, 1, \ldots, N-1)$ over p-ary symbols.
- A shift Sequence: $\underline{e} = (e_j,\ j = 0, 1, \ldots, T-1)$, where e_j is an integer or ∞.
- The Interleaved Sequence: N by T matrix A formed out of a using the shift sequence $\underline{e}$,

$$A = \begin{pmatrix} a_{0+e_0} & a_{0+e_1} & \cdots & a_{0+e_{T-1}} \\ a_{1+e_0} & a_{1+e_1} & \cdots & a_{1+e_{T-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-1+e_0} & a_{N-1+e_1} & \cdots & a_{N-1+e_{T-1}} \end{pmatrix},$$

where the subscript addition is performed modulo N and $a_{i+\infty} = 0$ for arbitrary i.

Interleaved Sequences

Left shift operator L on a is defined as
$L(a) = (a_1, \ldots, a_{N-1}, a_0)$.

- A component sequence: $\underline{a} = (a_i,\ i = 0, 1, \ldots, N-1)$ over p-ary symbols.
- A shift Sequence: $\underline{e} = (e_j,\ j = 0, 1, \ldots, T-1)$, where e_j is an integer or ∞.
- The Interleaved Sequence: N by T matrix A formed out of a using the shift sequence $\underline{e}$,

$$A = \begin{pmatrix} a_{0+e_0} & a_{0+e_1} & \cdots & a_{0+e_{T-1}} \\ a_{1+e_0} & a_{1+e_1} & \cdots & a_{1+e_{T-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-1+e_0} & a_{N-1+e_1} & \cdots & a_{N-1+e_{T-1}} \end{pmatrix},$$

where the subscript addition is performed modulo N and $a_{i+\infty} = 0$ for arbitrary i.

Interleaved Sequences

Left shift operator L on a is defined as
$L(a) = (a_1, \ldots, a_{N-1}, a_0)$.

- A component sequence: $\underline{a} = (a_i,\ i = 0, 1, \ldots, N-1)$ over p-ary symbols.
- A shift Sequence: $\underline{e} = (e_j,\ j = 0, 1, \ldots, T-1)$, where e_j is an integer or ∞.
- The Interleaved Sequence: N by T matrix A formed out of a using the shift sequence $\underline{e}$,

$$A = \begin{pmatrix} a_{0+e_0} & a_{0+e_1} & \cdots & a_{0+e_{T-1}} \\ a_{1+e_0} & a_{1+e_1} & \cdots & a_{1+e_{T-1}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-1+e_0} & a_{N-1+e_1} & \cdots & a_{N-1+e_{T-1}} \end{pmatrix},$$

where the subscript addition is performed modulo N and $a_{i+\infty} = 0$ for arbitrary i.

Interleaved Sequences

- The jth column sequence $\{A\}_j$ of the matrix A is

$$\{A\}_j = \begin{cases} 0, & \text{if } e_j = \infty \\ L^{e_j}(\underline{a}), & \text{else} \end{cases},$$

- By concatenating the successive rows of matrix A, an interleaved sequence $\underline{u}$ of period NT can be obtained as

$$u_{iT+j} = A_{i,j},\ 0 \leq i < N,\ 0 \leq j < T.$$

Interleaved Sequences

- The jth column sequence $\{A\}_j$ of the matrix A is

$$\{A\}_j = \begin{cases} 0, & \text{if } e_j = \infty \\ L^{e_j}(\underline{a}), & \text{else} \end{cases},$$

- By concatenating the successive rows of matrix A, an interleaved sequence $\underline{u}$ of period NT can be obtained as

$$u_{iT+j} = A_{i,j},\ 0 \leq i < N,\ 0 \leq j < T.$$

Cross Correlation

- Let $\underline{v}$ be a sequence interleaved by the p-ary component sequence $\underline{b} = (b_i,\, i = 0, 1, \ldots, N-1)$ and a shift sequence $\underline{f} = (f_j,\, j = 0, 1, \ldots, T-1)$

$$B = \begin{pmatrix} b_{0+f_0} & b_{0+f_1} & \cdots & b_{0+f_{T-1}} \\ b_{1+f_0} & b_{1+f_1} & \cdots & b_{1+f_{T-1}} \\ \vdots & \vdots & \ddots & \vdots \\ b_{N-1+f_0} & b_{N-1+f_1} & \cdots & b_{N-1+f_{T-1}} \end{pmatrix}.$$

$$R_{\underline{u},\underline{v}}(\tau) = \sum_{k=0}^{N\cdot T-1} \omega^{u_k - v_{k+\tau}}, \omega = e^{j2\pi/p}.$$

$$= \sum_{j=0}^{T-1} R_{\underline{a},\underline{b}}(f_{j+\tau} - e_j).$$

Cross Correlation

- Let $\underline{v}$ be a sequence interleaved by the p-ary component sequence $\underline{b} = (b_i,\, i = 0, 1, \ldots, N-1)$ and a shift sequence $\underline{f} = (f_j,\, j = 0, 1, \ldots, T-1)$

$$B = \begin{pmatrix} b_{0+f_0} & b_{0+f_1} & \cdots & b_{0+f_{T-1}} \\ b_{1+f_0} & b_{1+f_1} & \cdots & b_{1+f_{T-1}} \\ \vdots & \vdots & \ddots & \vdots \\ b_{N-1+f_0} & b_{N-1+f_1} & \cdots & b_{N-1+f_{T-1}} \end{pmatrix}.$$

$$R_{\underline{u},\underline{v}}(\tau) = \sum_{k=0}^{N \cdot T-1} \omega^{u_k - v_{k+\tau}}, \omega = e^{j2\pi/p}.$$

$$= \sum_{j=0}^{T-1} R_{\underline{a},\underline{b}}(f_{j+\tau} - e_j).$$

Cross Correlation

- Let $\underline{v}$ be a sequence interleaved by the p-ary component sequence $\underline{b} = (b_i,\, i = 0, 1, \ldots, N-1)$ and a shift sequence $\underline{f} = (f_j,\, j = 0, 1, \ldots, T-1)$

$$B = \begin{pmatrix} b_{0+f_0} & b_{0+f_1} & \cdots & b_{0+f_{T-1}} \\ b_{1+f_0} & b_{1+f_1} & \cdots & b_{1+f_{T-1}} \\ \vdots & \vdots & \ddots & \vdots \\ b_{N-1+f_0} & b_{N-1+f_1} & \cdots & b_{N-1+f_{T-1}} \end{pmatrix}.$$

$$R_{\underline{u},\underline{v}}(\tau) = \sum_{k=0}^{N\cdot T-1} \omega^{u_k - v_{k+\tau}}, \omega = e^{j2\pi/p}.$$

$$= \sum_{j=0}^{T-1} R_{\underline{a},\underline{b}}(f_{j+\tau} - e_j).$$

We introduce two variables ∞_1 and ∞_2 and define $\infty - \infty = \infty$, $k - \infty = \infty_1$ and $\infty - k = \infty_2$ for any finite integer k.

Let $C_k(\tau)$ denote the cardinality of the set

$\{j | k = f_{j+\tau} - e_j \pmod N,\ 0 \leq j < T\}$

for arbitrary $0 \leq k < N$ or $k = \infty$, ∞_1, or ∞_2, and

$$I(\underline{a}) = \sum_{i=0}^{N-1} \omega^{a_i} \text{ and } I(\underline{b}) = \sum_{i=0}^{N-1} \omega^{b_i},$$

where $I(\underline{a})$ ($I(\underline{b})$ resp.) is called the imbalance of $\underline{a}$ ($\underline{b}$ resp.).

We introduce two variables ∞_1 and ∞_2 and define $\infty - \infty = \infty$, $k - \infty = \infty_1$ and $\infty - k = \infty_2$ for any finite integer k.
Let $C_k(\tau)$ denote the cardinality of the set
$\{j | k = f_{j+\tau} - e_j \pmod N,\ 0 \leq j < T\}$
for arbitrary $0 \leq k < N$ or $k = \infty$, ∞_1, or ∞_2, and

$$I(\underline{a}) = \sum_{i=0}^{N-1} \omega^{a_i} \text{ and } I(\underline{b}) = \sum_{i=0}^{N-1} \omega^{b_i},$$

where $I(\underline{a})$ ($I(\underline{b})$ resp.) is called the imbalance of $\underline{a}$ ($\underline{b}$ resp.).

m-sequence based Shift Sequence

- Let α be a primitive element over $\mathbf{GF}(p^n)$, and let $T = (p^n - 1)/(p^m - 1)$. We consider a shift sequence $\underline{e} = (e_0, e_1, \ldots, e_{T-1})$ determined by

$$\alpha^{Te_t} = Tr_m^n(\alpha^t), 0 \leq t < T.$$

- Let $\underline{f} = \underline{e}$.
-

$$R_{\underline{u},\underline{v}}(\tau) = \begin{cases} p^{n-2m}(I(\underline{a}) + 1)(I^*(\underline{b}) + 1) - 1, \\ \text{if } \tau \not\equiv 0 (\bmod T) \\ \\ p^{n-m} R_{\underline{a},\underline{b}}(d) + p^{n-m} - 1, \\ \text{if } \tau = d \cdot T \end{cases}.$$

A Construction with Balanced Sequences

If sequence $\underline{a}$ or $\underline{b}$ is balanced, i.e., $(I(\underline{a})+1)=0$ or $(I(\underline{b})+1)=0$, and $R_{\underline{a},\underline{b}}(0)=0$, then

$$R_{\underline{u},\underline{v}}(\tau)=\begin{cases} p^{n-m}R_{\underline{a},\underline{b}}(d)+p^{n-m}-1, & \text{if } \tau=d\cdot T \text{ and } d\neq 0 \\ -1, & \text{Otherwise} \end{cases}.$$

1. Let U be a set of balance sequences of length p^m-1 with the property that $R_{\underline{a},\underline{b}}(0)=-1$ for any $a\neq b\in U$.
2. Now apply interleaved construction to all the sequences in U based on the shift sequence $\underline{e}$ resulting in a family $\mathcal{S}$ of p^m-1 sequences each of period p^n-1.

A Construction with Balanced Sequences

If sequence $\underline{a}$ or $\underline{b}$ is balanced, i.e., $(I(\underline{a})+1)=0$ or $(I(\underline{b})+1)=0$, and $R_{\underline{a},\underline{b}}(0)=0$, then

$$R_{\underline{u},\underline{v}}(\tau)=\begin{cases} p^{n-m}R_{\underline{a},\underline{b}}(d)+p^{n-m}-1, & \text{if } \tau=d\cdot T \text{ and } d\neq 0 \\ -1, & \text{Otherwise} \end{cases}.$$

1. Let U be a set of balance sequences of length p^m-1 with the property that $R_{\underline{a},\underline{b}}(0)=-1$ for any $a\neq b\in U$.
2. Now apply interleaved construction to all the sequences in U based on the shift sequence $\underline{e}$ resulting in a family $\mathcal{S}$ of p^m-1 sequences each of period p^n-1.

An upper bound

The following upper bound follows from combinatorics of balanced p-ary sequences.

$$
\begin{aligned}
|U| &\leq \min\left\{ \frac{\binom{p^m-1}{p^{m-1}}\binom{(p-1)p^{m-1}-1}{p^{m-1}}\cdots\binom{2p^{m-1}-1}{p^{m-1}}}{p^m-1}, \right. \\
&\qquad \left. p^m-1 \right\} \\
&= \begin{cases} 1, & m=1 \\ 1, & p=2, m=2 \\ 5, & p=2, m=3 \\ p^m-1, & \text{else} \end{cases}.
\end{aligned}
$$

Connection to Hadamard Matrices

- A Butson Hadamard Matrix H_N of size N over the set of complex p^{th} roots of unity satisfying:

$$H_N H_N^T = N I_N,$$

  where T denotes conjugate transpose.
- $p = 2$: Binary Hadamard matrices.
- It is clear that, if you delete the first column of a Hadamard matrix, the rows satisfy the requirement for U.

Connection to Hadamard Matrices

- A Butson Hadamard Matrix H_N of size N over the set of complex p^{th} roots of unity satisfying:

$$H_N H_N^T = N I_N,$$

  where T denotes conjugate transpose.
- $p = 2$: Binary Hadamard matrices.
- It is clear that, if you delete the first column of a Hadamard matrix, the rows satisfy the requirement for U.

Connection to Hadamard Matrices

- A Butson Hadamard Matrix H_N of size N over the set of complex p^{th} roots of unity satisfying:

$$H_N H_N^T = N I_N,$$

  where T denotes conjugate transpose.
- $p = 2$: Binary Hadamard matrices.
- It is clear that, if you delete the first column of a Hadamard matrix, the rows satisfy the requirement for U.

Non-Cyclic Hadamard Matrices

Let H'_N be the punctured matrix of H_N without the first column. A Hadmard matrix H_N is said to be completely noncyclic if all the row vectors of the punctured matrix H'_N are shift distinct.

- In Small lengths: Binary Case:

length	Class	No. shift distinct row vectors in H'_M	Perm. which turns H'_N to completely noncyclic
4	$Class\ 1$	2	$None$
8	$Class\ 1$	6	$None$
12	$Class\ 1$	11	$(2,3)$
16	$Class\ 1$	15	$(2,3)$
16	$Class\ 2$	15	$(2,3)$
16	$Class\ 3$	15	$(2,3)$

Table 1. Number of shift distinct vectors of known classes of $H'_N, N \leq 28$.

Other works

- A construction K and a Mass Formula[Gong,Golomb,Song 2007]. A generalized sequence construction. A computational procedure which requires certain set of permutation functions.
- Paley Hadamard matrices: $q+1$, $q=3(\bmod 4)$, or $2(q+1)$, $q=1(\bmod 4)$, for any odd prime power q.
- Williamson Hadamard Construction: Powerful "plug-in" method to construct Hadamard matrices of order $4w$.

Other works

- A construction K and a Mass Formula[Gong,Golomb,Song 2007]. A generalized sequence construction. A computational procedure which requires certain set of permutation functions.
- Paley Hadamard matrices: $q+1$, $q=3(\mathrm{mod}\,4)$, or $2(q+1)$, $q=1(\mathrm{mod}\,4)$, for any odd prime power q.
- Williamson Hadamard Construction: Powerful “plug-in” method to construct Hadamard matrices of order $4w$.

Simplex Code

- A recursive infinite construction.
  $1 \rightarrow 0$ and $-1 \rightarrow 1$.
- Let, $\mathbf{0}_{2^m-1}$: All zero vector of length $2^m - 1$;
  and $\mathbf{1}_{2^m-1}$: All one vector of length $2^m - 1$.
  $\mathbf{\Gamma}_{2^m-1}$: Vector with alternating 0 and 1ús of length $2^m - 1$.
  Let $\overline{a}$ be the binary complement of a. Let $\mathcal{S}_m$ be a $(2^m - 1, 2^m)$ binary code consisting of $2^m - 1$ nonzero codewords of length $2^m - 1$ and $\mathbf{0}_{2^m-1}$, which is recursively defined by

$$\mathcal{S}_m = \begin{pmatrix} \mathcal{S}_{m-1} & \mathbf{0}^T_{2^{m-1}} & \mathcal{S}_{m-1} \\ \mathcal{S}_{m-1} & \mathbf{1}^T_{2^{m-1}} & \overline{\mathcal{S}_{m-1}} \end{pmatrix}, \; m = 2, 3, \cdots . \tag{1}$$

  where $\overline{\mathcal{S}_{m-1}}$ denotes the code whose i^{th} codeword is the complement of ith one of $\mathcal{S}_{m-1}$.

Simplex Code

- A recursive infinite construction.
  $1 \rightarrow 0$ and $-1 \rightarrow 1$.
- Let, $\mathbf{0}_{2^m-1}$: All zero vector of length $2^m - 1$;
  and $\mathbf{1}_{2^m-1}$: All one vector of length $2^m - 1$.
  $\mathbf{\Gamma}_{2^m-1}$: Vector with alternating 0 and 1ús of length $2^m - 1$.
  Let $\overline{a}$ be the binary complement of a. Let $\mathcal{S}_m$ be a $(2^m - 1, 2^m)$ binary code consisting of $2^m - 1$ nonzero codewords of length $2^m - 1$ and $\mathbf{0}_{2^m-1}$, which is recursively defined by

$$\mathcal{S}_m = \begin{pmatrix} \mathcal{S}_{m-1} & \mathbf{0}_{2^{m-1}}^T & \mathcal{S}_{m-1} \\ \mathcal{S}_{m-1} & \mathbf{1}_{2^{m-1}}^T & \overline{\mathcal{S}_{m-1}} \end{pmatrix}, \; m = 2, 3, \cdots . \tag{1}$$

  where $\overline{\mathcal{S}_{m-1}}$ denotes the code whose i^{th} codeword is the complement of ith one of $\mathcal{S}_{m-1}$.

Example

- $\mathcal{S}_1 = [0, 1]^T$.
-

Index	Codewords
1	000
2	101
3	011
4	110

Table: Code words of $\mathcal{S}_2$

- $(2^2 - 2 = 2)$ shift distinct codewords.

Example

- $\mathcal{S}_1 = [0, 1]^T$.
-

Index	Codewords
1	000
2	101
3	011
4	110

Table: Code words of $\mathcal{S}_2$

- $(2^2 - 2 = 2)$ shift distinct codewords.

Example Continued

Index	Codewords
1	$000\mathbf{0}000$
2	$011\mathbf{0}011$
3	$101\mathbf{0}101$
4	$110\mathbf{0}110$
5	$000\mathbf{1}111$
6	$011\mathbf{1}100$
7	$101\mathbf{1}010$
8	$110\mathbf{1}001$

Table: Code words of $\mathcal{S}_3$

- Note that $(2, 4)$, $(3, 7)$, and $5, 6)$, are shift equivalent codeword pairs. Thus we have five $(2^3 - 3 = 5)$ shift distinct codewords in $\mathcal{S}_3$.
  In general we show [Udaya-Tang05] $2^m \times (2^m - 1)$ punctured Sylvester Hadamard matrix has $2^m - m$ shift distinct row vectors.

Example Continued

Index	Codewords
1	$000\mathbf{0}000$
2	$011\mathbf{0}011$
3	$101\mathbf{0}101$
4	$110\mathbf{0}110$
5	$000\mathbf{1}111$
6	$011\mathbf{1}100$
7	$101\mathbf{1}010$
8	$110\mathbf{1}001$

Table: Code words of $\mathcal{S}_3$

- Note that $(2, 4)$, $(3, 7)$, and $5, 6)$, are shift equivalent codeword pairs. Thus we have five $(2^3 - 3 = 5)$ shift distinct codewords in $\mathcal{S}_3$. In general we show [Udaya-Tang05] $2^m \times (2^m - 1)$ punctured Sylvester Hadamard matrix has $2^m - m$ shift distinct row vectors.

Modified Simplex Code Construction

$$R(a) = (\overline{a_0}, a_1, \cdots, a_{2^m-2}).$$

Further let ψ_m be a code consisting of the zero codeword $\mathbf{0}_{2^m-1}$ and $2^m - 1$ nonzero codewords. We also use the operator R in straightforward manner to ψ_m, i.e.,

$$R(\psi_m) = \{R(a), a \in \psi_m\}.$$

Then, the modified recursion is defined as

$$\psi_{m+1} = \begin{pmatrix} \psi_m & \mathbf{0}^T_{2^{m-1}} & \psi_m \\ R(\psi_m) & \mathbf{1}^T_{2^{m-1}} & \overline{R(\psi_m)} \end{pmatrix}. \tag{2}$$

Starter matrix

Example

Let ψ_4 denote the code consisting of the bellowing 16 codewords of length 15. It is easily checked that ψ_4 is corresponding to a punctured 16×15 Hadamard matrix.

Index	Codewords
1	$0,0,0,0,0,0,0,0,0,0,0,0,0,0,0$
2	$0,0,0,0,0,0,0,1,1,1,1,1,1,1,1$
3	$0,0,0,1,1,1,1,0,0,0,0,1,1,1,1$
4	$0,0,1,0,1,1,1,0,1,1,1,0,0,0,1$
5	$0,1,0,1,0,1,1,1,0,1,1,0,0,1,0$
6	$0,1,1,0,0,1,1,1,1,0,0,1,1,0,0$
7	$0,1,1,1,1,0,0,0,1,0,1,0,1,1,0$
8	$0,1,1,1,1,0,0,1,0,1,0,1,0,0,1$
9	$1,0,0,1,1,0,1,1,1,0,1,1,0,0,0$
10	$1,0,1,0,1,0,1,1,0,1,0,0,1,1,0$
11	$1,0,1,1,0,1,0,0,0,1,1,1,1,0,0$
12	$1,0,1,1,0,1,0,1,1,0,0,0,0,1,1$
13	$1,1,0,0,1,1,0,0,1,1,0,1,0,1,0$
14	$1,1,0,0,1,1,0,1,0,0,1,0,1,0,1$
15	$1,1,0,1,0,0,1,0,1,1,0,0,1,0,1$
16	$1,1,1,0,0,0,1,0,0,0,1,1,0,1,1$

Generalized Hadamard matrices

- We introduced a general construction of infinite classes Generalized Hadamard matrices through Cocycles [Horadam, Udaya,2002,2003] .
- Let G be a group under addition. A *cocycle* on G is a function $\psi : G \times G \rightarrow G$ satisfying $\psi(0,0) = 0$ and

$$\psi(g,h) + \psi(g+h,k) = \psi(g,h+k) + \psi(h,k), \ \forall \ g,h,k \in G.$$

- A useful tool in projective representation theory, cohomology of groups.
- We take G to be the additive group of the finite field.

Multiplication Cocycles

The finite field multiplication function can be used to define cocycles leading to Hadamard matrix.
A cocyclic generalized Hadamard matrix looks as follows. Here α is a primiive element in $GF(p^m)$ and $N = p^m - 1$.

$$G = \begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 0 & \alpha & \alpha^2 & \alpha^3 & \cdots & 1 \\ . & . & . & . & \cdots & . \\ 0 & \alpha^{N-1} & 1 & \alpha & \cdots & \alpha^{N-2} \end{pmatrix},$$

Applying trace function to the above matrix leads to Binary Hadamad matrices.

Presemifield Multiple Cocycles

- The multiplication function of the above construction can be generalized to any pre-semifield. They lead to rich classes of Generalized Hadamard matrices.
- Recall that $(F, +, *)$ is a *presemifield* if $(F, +)$ is an abelian group (with additive identity 0), $(F \backslash \{0\}, *)$ is a quasigroup (that is, for any non-zero $g, h \in F$ there are unique solutions in F to $g * x = h$ and to $y * g = h$), and both distributive laws hold.
- A *semifield* is a presemifield with a multiplicative identity.
- If $(F, +, *)$ is a finite presemifield it has order $q = p^a$ for some prime p, its additive group $G = (F, +)$ is the same as that of the finite field $\mathrm{GF}(q)$ of the same order.

Z_4 construction

[Elliot, Rao, 1982] give a general construction of fast transforms in the context of signal processing. We use one such construction to produce to new non-cyclic 4-ary Hadamard matrices.

$$C_1 = \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}, C_2 = \begin{bmatrix} S_1 & S_1 \\ C_1 & -C_1 \end{bmatrix},$$

$$C_t = \begin{bmatrix} C_{t-1} & C_{t-1} \\ C_1 \otimes S_{t-2} & -C_1 \otimes S_{t-2} \end{bmatrix}, t \geq 3,$$

where S_t is a Sylvester Hadmard matrix of order 2^t.

$$S_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, C_2 = \begin{bmatrix} S_1 & S_1 \\ S_1 & -S_1 \end{bmatrix},$$

Example

$$C_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & 1 & -i & -i & -1 & -1 & i & i \\ 1 & -1 & -i & i & -1 & 1 & i & -i \\ 1 & 1 & i & i & -1 & -1 & -i & -i \\ 1 & -1 & i & -i & -1 & 1 & -i & i \end{bmatrix},$$

$$C_3 C_3^T = 8 I_8$$

.

Other Constructions

- Using two m-sequences and combining them in a relation similar to the recursion defined before [Jang,No,Chung,Tang07].
- The same method generalization to q-ary context.
- Quaternary matrix [Kim,No,Chung5].

Constructions with Flexible zone size

- New design of low-correlation zone sequence sets [Kim,Jang,No,Chung 2006], $\epsilon = 2$.
- Interleaved Sequence of Period $2N$ [Zhou,Tang,Gong,2008],$\epsilon = 2$
- Quaternary low correlation through Inverse Gray map, [Chung,Yang2008].
- Some new designs in this workshop.

Frequency Hopping

- The above discussion can be extended to the case Frequency hopping CDMA communication systems.
- Hamming Correlation as opposed to inner-product correlation defined above.
- What does low correlation means in this context?

Conclusions

- Sequence design for Quasi-Synchronous Communication Systems.
- Interleaved Construction and connection to Non-cyclic Hadamard matrices.
- New designs with more choice of zone lengths and longer periods.