Topic 3. Design of Sequences with Low Correlation

1. M-sequences and Quadratic Residue Sequences
2. Multiple Trace Term Sequences and WG Sequences
3. Gold-pair, Kasami Sequences, and Interleaved Sequences
4. Case Study: Examples of Orthogonal Codes
5. Applications in CDMA Systems
1 M-sequences and Quadratic Residue Sequences

A. M-sequence Generator:

Input: - A finite field $F = GF(q)$;
- $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1x - c_0, c_i \in F$, a primitive polynomial over $F$.

Output: $a = a_0, a_1, a_2, \cdots$ an $m$-sequence over $F$ of period $q^n-1$.

Procedure $(F, f(x), a)$:

Compute: $a_{i+n} = \sum_{j=0}^{n-1} c_j a_{j+i}, \quad i = 0, 1, \cdots$

quit
B. Profile of Randomness of Binary M-sequences of Degree $n$

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Period</strong></td>
<td>$2^n - 1$</td>
</tr>
<tr>
<td><strong>Balance</strong></td>
<td>$2^{n-1}$ 1’s and $2^{n-1} - 1$ 0’s</td>
</tr>
</tbody>
</table>
| **Run property**         | (1) For $1 \leq k \leq n-2$ runs of 0’s (1’s) of length $k$ occurs $2^{n-2-k}$ times  
(2) Zero run of length $n-1$ occurs once; no runs of 1’s of length $n-1$  
(3) Runs of 1’s of length $n$ occurs once |
| **Span $n$ property or ideal $n$-tuple distribution** | Each nonzero $n$-tuple occurs once |
| **Autocorrelation**      | 2-level                           |
| **Linear span and $\rho$** | $n$, the normalized linear span $\rho = \frac{n}{2^n - 1}$ |

As good as it could be!

Only need to know $2n$ bits to reconstruct the entire sequence!
Property 1 (Binary $m$-sequences). Let an LFSR have a primitive characteristic polynomial $f(x)$. Then there exists an initial state for the LFSR such that the corresponding output sequence $a = \{a_i\}$, i.e., an $m$-sequence, satisfies

$$a_i = a_{2i}, \quad i = 0, 1, \ldots .$$

In other words, there exists an initial state of the LFSR such that the output sequence is identical to its 2-decimation sequence.
C. Quadratic Residue (or Legendre) Sequences

Note. Starting from now, we only consider binary sequences.

Some concepts in number theory:

**Quadratic Residue:** Let \( p \) be an odd prime number. A number \( i: 1 < i < p \) is called a quadratic residue modulo \( p \) if there is an integer \( x \) for which \( x^2 \equiv i \mod p \).

**Fact.** A set defined by
\[
QR = \{i^2 \mod p \mid 0 < i \leq (p-1)/2\}
\]
contains all quadratic residue modulo \( p \).

**The Legendre symbol:** The Legendre symbol \((i/p)\) is defined as follows:
\[
\left( \frac{i}{p} \right) = \begin{cases} 
1 & \text{if } i \text{ is a quadratic residue modulo } p \\
-1 & \text{Otherwise}
\end{cases}
\]
Quadratic Sequence Generator:

Input: A prime number \( p \) with \( p \equiv 3 \mod 4 \)
Output: \( a = a_0, a_1, \ldots \) a binary sequence of period \( p \)

Procedure\((p, a)\):
Compute: \( \left( \frac{i}{p} \right) \) and set \( a_0 = 1 \) and set
\[
\begin{cases} 
0 \Leftrightarrow \left( \frac{i}{p} \right) = 1 \\
1 \Leftrightarrow \left( \frac{i}{p} \right) = -1 
\end{cases}
\]

Return: \( a \)
Quit
Example 8. Let $p = 11$. Then

\[
\begin{align*}
\left(\frac{0}{p}\right) &= 1, \\
\left(\frac{1}{p}\right) &= 1, \\
\left(\frac{2}{p}\right) &= -1 \\
\left(\frac{3}{p}\right) &= 1, \\
\left(\frac{4}{p}\right) &= 1, \\
\left(\frac{5}{p}\right) &= 1 \\
\left(\frac{6}{p}\right) &= -1, \\
\left(\frac{7}{p}\right) &= -1, \\
\left(\frac{8}{p}\right) &= -1 \\
\left(\frac{9}{p}\right) &= 1, \\
\left(\frac{10}{p}\right) &= -1
\end{align*}
\]

So, $a$ has period 11 and $a = (10100011101)$.

For $p = 31$, then $a = (10010010000111010100011110110111)$ which has period 31. Verify it for the autocorrelation!
Profile of Quadratic Residue (or Legendre) Sequences:

1. Period: \( p \)
2. Balance: \( (p+1)/2 \) 1's and \( (p-1)/2 \) 0's
3. 2-level autocorrelation
4. Linear span: \( (p-1)/2 \)
5. \( N(QR,p) \), the number of shift distinct quadratic sequences modulo \( p \), \( N(QR,p) = 2 \).

Sound randomness! However, it cannot be implemented efficiently!

Compare it with m-sequences?
A. Three-Term Sequences

**Construction A:** For odd \( n \geq 5, \) and \( n = 2m+1 \) with period \( N = 2^n - 1, \) let \( b = \{b_i\} \) be an \( m \)-sequence of period \( N \) with the constant-on-coset property. Assume

\[
q_1 = 2^m + 1 \quad \text{and} \quad q_2 = 2^m + 2^{m-1} + 1.
\]

Define

\[
a_i = b_i + b_{q_1i} + b_{q_2i}, \quad i = 0, 1, \ldots
\]

Then \( a = \{a_i\} \) is a binary sequence with 2-level autocorrelation.
Architecture for Implementation of the 3-Term Sequences
Profile of 3-term sequences

1. Period: $2^n - 1$

2. Balance: $2^{n-1}$ 1's and $2^{n-1} - 1$ 0's

3. 2-level autocorrelation

4. Linear span: $3n$

5. $N(T3, n)$, the number of shift distinct 3-term sequences,
   
   $$N(T3, n) = \phi(2^n - 1) / n$$
Implementation of 3-term sequences of \( n = 5 \): (1, 5, 7)
Implementation of 3-term sequences of $n = 7$: (1, 9, 13)
5-Term Sequences and WG Transformation Sequences

Some property of finite fields

Some property of finite fields:
Some property of finite fields

• Trace Functions

**Definition.** A trace function $Tr(x)$ of $GF(p^n)$ is a function from $GF(p^n)$ to $GF(p)$ defined as follows

$$Tr(x) = x + x^p + \cdots + x^{p^{n-1}}$$

$$Tr(x): GF(p^n) \rightarrow GF(p)$$

**Property 1.**
(a) The trace function is a linear function.
(b) $(x + y)^p = x^p + y^p$, $\forall x, y \in GF(p^n)$.

• Primitive Elements of Finite Fields

Let the finite field $GF(p^n)$ be defined by a primitive polynomial over $GF(p)$ with degree $n$. Then the defining element is called a **primitive element** in $GF(p^n)$.
5-Term Sequences and WG Transformation Sequences

**Construction B:** Let \( n \not\equiv 0 \mod 3 \), \( \alpha \) a primitive element of \( \mathbb{F}_{2^n} \), and \( t(x) = x + x^3 + x^{2^2} + x^{2^3}, x \in \mathbb{F}_{2^n} \), where the \( q_i \)'s are given by

<table>
<thead>
<tr>
<th>( n = 3k - 1 )</th>
<th>( q_1 = 2^{2k} + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( q_2 = 2^{2k-1} + 2^{k-1} + 1 )</td>
</tr>
<tr>
<td></td>
<td>( q_3 = 2^{2k-1} - 2^{k-1} + 1 )</td>
</tr>
<tr>
<td></td>
<td>( q_4 = 2^{2k-1} + 2^k - 1 )</td>
</tr>
<tr>
<td>( n = 3k - 2 )</td>
<td>( q_1 = 2^{k-1} + 1 )</td>
</tr>
<tr>
<td></td>
<td>( q_2 = 2^{2k-2} + 2^{k-1} + 1 )</td>
</tr>
<tr>
<td></td>
<td>( q_3 = 2^{2k-2} - 2^{k-1} + 1 )</td>
</tr>
<tr>
<td></td>
<td>( q_4 = 2^{2k-1} - 2^{k-1} + 1 )</td>
</tr>
</tbody>
</table>

The function defined by

\[
 f(x) = Tr(t(x+1) + 1), \ x \in \mathbb{F}_{2^n} \quad (9.1)
\]
is called the Welch-Gong transformation of \( Tr(t(x)) \), or the WG transformation for short. Note that \( f(x) \) is a function from \( \mathbb{F}_{2^n} \) to \( \mathbb{F}_2 \). Let \( a = \{a_i\} \) and \( b = \{b_i\} \) whose elements are given by

\[
 a_i = Tr(t(\alpha^i)) , i = 0, 1, \cdots \quad (9.2)
\]
\[
 b_i = f(\alpha^i) = Tr(t(\alpha^i + 1) + 1) , i = 0, 1, \cdots \quad (9.3)
\]

Then both \( a \) and \( b \) have 2-level autocorrelation, and \( b \) is called a Welch-Gong transformation sequence of \( a \), or a WG sequence for short.
Figure 9.4: LFSR implementation of 5 term sequences
Remark. The initial states of the LFSRs should satisfy the constan-on-coset property.

Figure 9.6: LFSR implementation of 5-term sequences of period 127

Example 9.2 A 5-term sequence of period 127: For \( n = 5 \), a 5-term sequence \( a \) degenerates to a quadratic sequence, and a WG sequence \( b \) to an \( m \)-sequence. For \( n \geq 7 \), Construction B produces new sequences. Let \( n = 7 = 3 \times 3 - 2 \Rightarrow k = 3 \); let \( f(x) = x^7 + x + 1 \); and let \( \alpha \) be a root of \( f(x) \) in \( \mathbb{F}_{2^7} \). Then

\[
q_1 = 2^2 + 1 = 5, \quad q_2 = 2^4 + 2^2 + 1 = 21, \\
q_3 = 2^4 - 2^2 + 1 = 13, \quad \text{and} \quad q_4 = 2^5 - 2^2 + 1 = 29.
\]

We compute the minimal polynomials \( f_{\alpha^i}(x) \) of \( \alpha^i, i \in \{5, 21, 13, 29\} \) (or by look-up table in Appendix C of Chapter 3) as follows:

\[
f_2(x) = f_{\alpha^8}(x) = x^7 + x^3 + x^2 + x + 1 \\
f_3(x) = f_{\alpha^{21}}(x) = x^7 + x^6 + x^3 + x + 1 \\
f_5(x) = f_{\alpha^{13}}(x) = x^7 + x^6 + x^5 + x^2 + 1 \\
f_{\alpha^{29}}(x) = x^7 + x^4 + 1.
\]
There are two methods to implement a WG sequence. For small $n$, a WG sequence can be implemented by Method 1, as shown below.

**Method 1: Trinomial Decimation.** For small $n$, the WG sequence $b$ can be implemented using the following result. Let $\alpha$ be a primitive element of $\mathbb{F}_{2^n}$ and $b$ the WG sequence from $a$. Then the elements of $b$ can be obtained by performing an irregular decimation on $a$ as follows

$$b_0 = a_0, \text{ and } b_i = \begin{cases} a_{\tau(i)} & \iff n \text{ even} \\ a_{\tau(i)} + 1 & \iff n \text{ odd,} \end{cases}$$

or equivalently, $b_i \equiv a_{\tau(i)} + n \pmod{2}$, for $i > 0$, where $\tau(i)$ is determined by

$$\alpha^{\tau(i)} = \alpha^i + 1. \quad (9.4)$$

**Method 2: Finite Field Configuration.** In general, WG sequences can be implemented by a finite field configuration (see Figure 9.5). From

![Diagram](image)

Figure 9.5: Galois Field Configuration of WG Generators
Table 9.3: Profile of 5-term sequences and WG sequences

<table>
<thead>
<tr>
<th>Period</th>
<th>$2^n - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balance</td>
<td>$2^{n-1}$ 1’s and $2^n - 1$ 0’s</td>
</tr>
<tr>
<td>Autocorrelation</td>
<td>(ideal) 2-level</td>
</tr>
<tr>
<td>$N(T5, n)$ or $N(WG, n)$</td>
<td>$\phi(2^n - 1)/n$</td>
</tr>
</tbody>
</table>

| Linear span | $LS(a) = 5n$; $LS(b) = n(2^{[n/3]} - 3)$ |
| Trace representation | $a \leftrightarrow g(x) = Tr(t(x))$  
$b \leftrightarrow f(x) = \sum_{i \in I} Tr(x^i)$ where 
$I = I_1 \cup I_2$ for $n = 3k - 1$ where 
$I_1 = \{2^{2k-1} + 2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\}$  
$I_2 = \{2^{2k} + 2i | 0 \leq i \leq 2^{k-1} - 2\}$  
and where $I = \{1\} \cup I_3 \cup I_4$ for $n = 3k - 2$ where 
$I_3 = \{2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\}$  
$I_4 = \{2^{2k-1} + 2^{k-1} + 2 + i | 0 \leq i \leq 2^{k-1} - 3\}$ |

**Remark:** WG sequences have important applications in generating key streams in stream ciphers because their good randomness properties.

@ G. Gong
3. Gold-pair, Kasami Sequences, and Interleaved Sequences

Signal Set

Let

$$S_j = (s_{j,0}, s_{j,1}, \cdots, s_{j,v-1}), 0 \leq j < r$$

be \( r \) shift-distinct \( p \)-ary sequences of period \( v \),

$$S = \{S_0, S_1, \cdots, S_{r-1}\}$$

Let

$$\delta = \max |C_{S_i, S_j}(\tau)| \text{ for any } 0 \leq \tau < v, 0 \leq i, j < r,$$

where \( \tau \neq 0 \) if \( i = j \). If \( \delta \leq c\sqrt{v} \) where \( c > 0 \) is a constant, then we say that the set \( S \) has low cross-correlation. In this case, we call \( S \) a \((v, r, \delta)\) signal set. When we consider the cross correlation of two sequences \( S_i, S_j \) in \( S \), we simply write \( C_{i, j}(\tau) \) for \( C_{S_i, S_j}(\tau) \).
A. Gold-pair Sequences

Construction: Let \( a = \{a_i\} \) be an \( m \)-sequence of degree \( n \) odd. Select \( d \) as one of the following values:

- \( d = 2^k + 1 \) (Gold exponents), \( (k, \ n) = 1, \ k < (n + 1)/2 \).
- \( d = 2^{2k} - 2^k + 1 \) (Kasami Large Set Exponents), \( (k, \ n) = 1, \ k < (n + 1)/2 \).
- \( d = 2^{\frac{n-1}{2}} + 3 \) (the Welch Conjecture Exponent)

For \( 0 \leq j < 2^n - 1 \), let \( s_j = \{s_{j,i}\} \) be a binary sequence whose elements are given by

\[
s_{j,i} = a_i + a_{j+di}, \quad i = 0, 1, \ldots, 2^n - 2
\]

Then \( s_j \) is called a Gold-pair sequence.

Let \( s_{2^n-1} = a \) and \( s_{2^n} = a^{(d)} \).

Set

\[
S = \{s_j \mid 0 \leq j \leq 2^n\}.
\]

Then \( S \) is called a Gold-pair (signal) set.
Note that we can also write $s_j$ as a sum of a shift of $a$ and $b = a^{(d)}$, i.e.,

$$s_j = L^j a + b, \quad 0 \leq j < 2^n - 1.$$  

**Remark.** A useful formula for the relationship between the cross correlation and the Hamming weight.

Let $a$ and $b$ be two binary sequences with period $2^n - 1$, then the cross correlation between these two sequences can be determined by the Hamming weight of $a + L^\tau b$ as follows:

$$C_{a,b}(\tau) = 2^n - 1 - 2w(a + L^\tau (b))$$

where $w(.)$ denotes the Hamming weight of the vector.
Profile of the Gold-pair Signal Set:

1. $S$ is a $(2^n - 1, 2^n + 1, \pm 2^{(n+1)/2})$-signal set.

2. The cross correlation $C_{i,j}(\tau)$ of any two sequences $s_i$ and $s_j$ in $S$ is three-valued and it takes values: $-1, \pm 2^{(n+1)/2}$.

3. In $S$, there are $2^{n-1} + 2$ sequences are balanced, i.e., each has $2^{n-1}$ 1's. Moreover, each sequence in $S$ has its Hamming weight taking one of the three values: $2^{n-1}, 2^{n-1} \pm 2^{(n-1)/2}$.

4. $b$ is also an $m$-sequence, i.e., $(d, 2^n - 1) = 1$.

5. Linear span is either $2n$ or $n$. 

@ G. Gong
LFSR Implementation:

1. Select $n$ odd, $f(x)$, a primitive polynomial of degree $n$ over $GF(2)$, as a characteristic polynomial of LFSR1.

2. Select $d$ and compute the characteristic polynomial of the LFSR2, which is the minimal polynomial of $d$-decimation of a sequence generated by LFSR1.

3. We obtain all sequences in $S$ by varying different initial states of the LFSR1.

LFSR implementation of Gold pair generators
Example 1. Design of a (31, 33, 9) Gold-pair signal set.

Method 1: LFSR Implementation:

1. Select $f(x) = x^5 + x^3 + 1$, a primitive polynomial over $GF(2)$ of degree 5 as the characteristic polynomial of LFSR1.

2. Select $d = 1 + 2^2 = 5$ and compute the minimal polynomial of $\alpha^5$ in $GF(2^5)$, defined by $f(\alpha) = 0$. This gives

   $g(x) = x^5 + x^4 + x^3 + x + 1$

   Use $g(x)$ as the characteristic polynomial of LFSR2.

3. Fixing an initial state of one these two LFSRs and varying another, we get all 33 shift distinct sequences in $S$. 
Method 2: Software Implementation

1. Select $f(x) = x^5 + x^3 + 1$, a primitive polynomial over $GF(2)$ of degree 5 to generate a sequence $a$:

   $1 0 0 0 0 1 0 1 0 1 1 1 0 1 1 0 0 0 1 1 1 1 1 1 0 0 1 0 1 0 0$

2. Select $d = 1 + 2^2 = 5$ and perform 5-desimation on $a$, we obtain

   $b = a^{(5)}, b_i = a_{5i}, i = 0, 1, \ldots$

   $1 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 1 0 1$

3. Generate

   $L^i(a) + b, \quad 0 \leq i < 31$

   Together with $a$ and $b$, this gives all 33 sequences in $S$. 

@ G. Gong
Profile of $S$

- Period 31.
- There are 33 shift distinct sequences in $S$.
- The cross correlation of any two sequences in $S$ only takes three values: -1, -9, 7.
- $S$ is a (31, 33, 9)-signal set.
- There 18 sequences in $S$ are balanced, i.e. each has weight 16. The rest 15 has their weights either 12 or 20.
- Linear span 10 or 5.
B. Kasami Sequences

Construction: Let \( n = 2^m \) and and \( \mathbf{a} = \{a_i\} \) be an \( m \)-sequence of degree \( n \). Let \( s_j = \{s_{j,i}\} \) be a binary sequence whose elements are given by

\[
s_{j,i} = a_i + a_{j + di}, \quad i = 0, 1, \ldots
\]

where \( d = 2^m + 1 \).

Let \( s_{2^m - 1} = \mathbf{a} \) and

\[
S = \{s_j | 0 \leq j \leq 2^m - 1\}.
\]

Then \( S \) is called a Kasami small signal set. In other words, if we write \( \mathbf{b} = \mathbf{a}^{(d)} \) then

\[
s_j = \mathbf{a} + L^j \mathbf{b}, \quad 0 \leq j < 2^m - 1
\]
Profile of the Kasami small signal set

1. The Kasami small signal set $S$ is a signal set.

2. The cross correlation $C_{i,j}(\tau)$ of any two sequences $s_i$ and $s_j$ in $S$ is three-valued and it takes values:
   $$-1, -1 \pm 2^{n/2}$$

3. $b$ is an $m$-sequence of period $2^{n/2}-1$.

4. Linear span: $3n/2$ or $n$. 
Example 2. Design a (63, 8, 9) Kasami signal set.

LFSR Implementation:
- Select $n = 6$ and $f(x) = x^6 + x + 1$; set $\alpha$ be a root of $f(x)$ in $GF(2^6)$.
- Compute the minimal polynomial of $\alpha^9$ 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:

\[ s_1 = 111011011110001011101000000100110110001000001001101010001011
\]

Complement the columns corresponding to 1’s in \( b \):

\[
\begin{array}{ccccccccccc}
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]
C. Interleaved Sequences

• Definition of Interleaved Sequences

• Constructions of Signal Sets from Interleaved Sequences

• Profiles of the Interleaved Signal Sets

• Implementation
**Definition of Interleaved Sequences**

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

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

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

Let \( \mathbf{u}_j \) denote the \( j \)th column of the above array. Then we have

\[
\mathbf{u}_j = L_{e_j}(\mathbf{a}), \ 0 \leq j < t
\]

where \( L \) is the left shift operator and the \( e_j \) are nonnegative integers with \( 0 \leq e_j < s \).
Example 3.
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:

\[
\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

A (7, 7) interleaved sequence

\[
u = \begin{array}{cccccccc}
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
\end{array}
\]
Constructions of \((v^2, v+1, 2v+3)\) signal sets

Procedure 1:

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

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

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

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

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

5. A signal set \(S\) is defined by

\[
S = \{\mathbf{u}, \mathbf{s}_j : j = 0, 1, \ldots, v-1\}.
\]
Example 4. Let \( \nu = 7 \).

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

The column sequences of \( \mathbf{s}_0 \) can be obtained from the sequence \( \mathbf{u} \) 
by complement of columns of \( \mathbf{u} \) 
whose indexes correspond to 1's in the sequence \( \mathbf{b} \); the column 
sequences of \( \mathbf{s}_1 \) obtained from \( \mathbf{u} \) 
by complement of those in the 
sequence \( \mathbf{b} \) with a phase shift 1, and so on.
\[ s_0 = u + b = 1 0 0 1 1 1 1 0 1 0 1 0 0 1 1 1 1 0 1 1 0 1 1 0 0 1 0 0 \\
0 1 0 0 0 0 0 1 0 1 1 0 1 0 0 1 0 1 0 0 0 \]

\[ s_1 = u + b = 0 0 1 0 0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0 1 0 1 1 1 0 1 0 0 1 1 0 0 1 \]

\[ s_2 = u + L^2 b = 0 1 0 1 0 1 0 1 0 0 1 1 0 0 0 0 1 0 0 1 1 0 0 1 0 1 1 1 1 1 1 0 1 0 1 \\
1 0 0 1 0 0 0 1 1 1 0 0 0 1 \]

\[ s_3 = u + L^3 b = 1 0 1 1 0 0 0 0 1 1 1 1 1 0 1 1 0 0 0 0 1 1 1 0 0 1 0 1 0 0 0 0 1 1 1 0 1 0 0 0 0 0 0 0 1 1 \]

\[ s_4 = u + L^4 b = 0 1 1 1 1 1 0 1 1 0 1 1 0 1 1 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 1 0 1 1 \]

\[ s_5 = u + L^5 b = 1 1 1 0 1 1 0 0 0 1 0 0 0 0 1 0 0 1 1 1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 0 1 \]

\[ s_6 = u + L^6 b = 1 1 0 0 0 0 1 0 0 0 0 1 1 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 0 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 0 1 0 \]

5. Set \( S = \{ u, s_0, s_1, \ldots, s_6 \} \).
Constructions for \((\nu^2, \nu+1, 2\nu+3)\) signal sets (Cont.)

**Theorem 1.** If the shift sequence \(e\) satisfies the following condition,

\[
(*) \quad |\{e_j - e_{j+s} | 0 \leq j < \nu - s\}| = \nu - s, \text{ for all } 1 \leq s < \nu
\]

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

* Gong (1995) introduced the idea of Procedure 1 for constructing \(((2^n-1)^2, 2^n, 1+2^n)\) signal sets where \(\nu = 2^n-1\) 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** (Shortened M-sequence Construction)

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

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

2. Generate an $m$-sequence $\{w_i\}$ of period $2^{2n}-1$ by the LFSR which satisfies the constant-on-coset property.

3. Arrange $\{w_i\}$ into an $(r, \nu)$ array where $r = 2^n+1$ and $\nu = 2^n-1$:

$$W = \begin{pmatrix}
0 & w_1 & w_2 & \cdots & w_{s-2} & w_{s-1} \\
0 & w_{s+1} & w_{s+2} & \cdots & w_{s+s-2} & w_{2s-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & w_{(\nu-1)s+1} & w_{(\nu-1)s+2} & \cdots & w_{(\nu-1)s+s-2} & w_{\nu s-1}
\end{pmatrix}$$
Let $U$ be a matrix obtained from $W$ by deleting the first and the last columns, then $U$ gives an interleaved sequence $u$ of period $(2^n-1)^2$ which has the base sequence $a$ which is $r$-decimation of $b$ 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 5. Interleaved Generator (49, 8, 17):

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

2. By deleting the first and the last columns of \( W \), we have

   \[
   \begin{array}{ccccccc}
   0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
   0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
   0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
   0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
   0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
   0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
   0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
   \end{array}
   \]

   which is the sequence \( u \) 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!)
4. Case Study: Examples of Orthogonal Code Design

- Review for Inner Product
- Hadamard Matrices
- Orthogonal Code Design from 2-Level Autocorrelation Sequences
- Examples
Review for Inner Product: let

- \( \mathbb{C} \) be the complex field;
- \( F = \mathbb{C}^r \), contains vectors of dimension \( r \) whose elements are taken from \( \mathbb{C} \).

The inner product of any two vectors in \( F \), say \( \mathbf{b} \) and \( \mathbf{c} \), is defined by

\[
\mathbf{b} \cdot \mathbf{c} = b_0c_0 + b_1c_1 + \cdots + b_{r-1}c_{r-1}
\]

If \( \mathbf{b} \cdot \mathbf{c} = 0 \), then \( \mathbf{b} \) and \( \mathbf{c} \) are said to be orthogonal.

Example.
Let
\[
\mathbf{b} = (1, -1, -1, 1) \quad \text{and} \quad \mathbf{c} = (-1, -1, 1, 1).
\]
Since
\[
\mathbf{b} \cdot \mathbf{c} = 1(-1) + (-1)(-1) + (-1) \cdot 1 + 1 \cdot 1 = 0
\]
then \( \mathbf{b} \) and \( \mathbf{c} \) are orthogonal.

Definition. A finite subset \( M \) of \( F \) is said to be an **orthogonal code** if any two vectors in \( M \), called codewords, are orthogonal.

How to construct a binary orthogonal code?
A set consisting of row vectors of a Hadamard matrix constitutes an orthogonal code, i.e.,

orthogonal code ↔ Hadamard matrix

(it is also called a Walsh code in communications).

**Hadamard Matrices:** Let $H$ be a $m$ by $m$ matrix whose elements are taken from \{1, -1\}. If

$$HH^T = mI_m$$

where $I_m$ is the $m$ by $m$ identity matrix, then $H$ is called a Hadamard matrix.

**Existence of Hadamard matrices:**

$m$ is a multiple of 4

The following matrix is a Hadamard matrix:

$$H = \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1
\end{pmatrix}$$
Orthogonal Code Design from 2-Level Autocorrelation Sequences

**Construction:** Let \( a = \{a_i\} \) be a binary 2-level autocorrelation sequence of period \( m = 2^n - 1 \) and

\[ b_i = (-1)^{a_i}, i = 0, 1, \ldots, m-1 \]

Then

\[
H = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & b_0 & b_1 & \cdots & b_{m-1} \\
1 & b_1 & b_2 & \cdots & b_0 \\
& \vdots & & & \\
1 & b_{m-1} & b_0 & \cdots & b_{m-2}
\end{bmatrix}
\]

is a Hadamard matrix.

**Example.** Let \( a = (1001011) \), an m-sequence of period 7. Then the following matrix is a Hadamard matrix, so we obtain an orthogonal code from the m-sequence of degree 3.

**Question:** Which construction of 2-level autocorrelation sequence has a simple implementation?
5 Applications to DS-CDMA System

- System Basics
- Physical Layer of Forward and Reverse Links
- Use of Hadamard matrices for orthogonality
  - Forward: Orthogonal CDMA Channels
  - Reverse: Orthogonal Coding
- Use of cyclic Hadamard matrices for 2-level auto-correlation function property
  - PN Long Code and Short Code
  - Unique Identification
  - Data Scrambling and Authentication
  - Spectrum Spreading
The CDMA Cocktail Party

This is great stuff

Where is she

You know that

Where is the meeting

Who called

How can I get there

How long will this take

Who knows

Where is the office

Can I go home?
Multiple Access Methods
CDMA System Design

Voice Coding

Forward Link Generation

Reverse Link Generation

Power Control
The CDMA Rate Families

- IS-95 defines the 9600 bps family of rates (Rate Set 1)
  - 9600, 4800, 2400, and 1200 bps
  - Can select one of the four rates every 20 ms frame

- 14400 bps family of rates (Rate Set 2)
  - 14400, 7200, 3600, and 1800 bps
  - Can select one of the four rates every 20 ms frame

- Extended rates (extended Rate Set 1)
  - Adds 19200, 38400, and 76800 bps
  - At most four rates can be active
  - Can select one of the four active rates every 20 ms frame
Link Waveform

- CDMA Forward Link Waveform
  - Pilot Channel
  - Sync Channel
  - Paging Channel
  - Traffic Channel

- CDMA REVERSE Link Waveform
  - Access Channel
  - Traffic Channel
Forward CDMA Channel

- A 64 x 64 Hadamard matrix is used to produce 64 orthogonal channels.
- Each row of a Hadamard matrix is used to uniquely identify channels from 0 to 63.
- This is possible since each row (as a binary vector of length 64) of the 64 x 64 Hadamard matrix is orthogonal to any other row.
- If we call 64 row vectors as $W_0, W_1, ..., W_{63}$, then the waveform for Channel #k is obtained by multiplying $W_k$ to the input signal.
**Forward CDMA Channel**

FORWARD CDMA CHANNEL
(1.23 MHz channel transmitted by base station)

- Pilot Chan
- Sync Chan
- Paging Ch 1
- Paging Ch 7
- Traffic Ch 1
- Traffic Ch 25
- Traffic Ch 55

W = Code Channel

Traffic Data
Personal Station
Power Control
Sub-Channel

W0 W32 W1 W7 W8 W31 W33 W63
A Reverse Channel is uniquely identified by an initial phase of a binary PN sequence (so called, the long code) of length $2^{42} - 1$.

Different initial phases correspond to different shift of the PN sequence, hence they are orthogonal.

Only $1/256$ positions of the length are used to address all the users in the system.
Reverse Traffic Channel Structure for Rate Set 1

- Reverse Traffic Channel Information Bits (172, 80, 40, or 16 bits/frame)
- Add Frame Quality Indicators (12, 8, 0, or 0 bits/frame)
- 8.6 kbps, 4.0 kbps, 2.0 kbps, 0.8 kbps
- Add 8 bit Encoder Tail
- 9.6 kbps, 4.8 kbps, 2.4 kbps, 1.2 kbps
- Convolutional Encoder \( r=1/3, K=9 \)
- Symbol Repetition
- Code Symbol
- Block Interleaver
- 28.8 kbps

- Frame Data Rate
- 28.8 kbps
- Modulation Symbol (Walsh chip)
- 64-ary Orthogonal Modulator
- 4.8 ksps (307.2 kcps)
- Data Burst Randomizer
- PN chip 1.2288 Mcps
- Long Code Generator
- Long Code Mask
- I-channel Sequence 1.2288 Mcps
- Q-channel Sequence 1.2288 Mcps

- Baseband Filter
- \( s(t) = \cos(2\pi f_c t) \)
- \( q(t) = \sin(2\pi f_c t) \)
Orthogonal Modulation (R. Link)

- For every 6 symbols in, 64 Walsh chips are out.
- Here, 64 Walsh chips are 64 components of a row of the $64 \times 64$ Hadamard matrix.
- Note the different role of the same $64 \times 64$ Hadamard matrix in Reverse Link.
PN Long Code Spreading

64 chip pattern of Walsh Code \# k

1 0 0 0 1 \ldots 1 1 0 1 0

(307.2 kHz)

1.2288 Mcps

Channel Mask

Long Code \(2^{42} - 1\)

PN Generator

1.2288 Mcps
PN Long Code

- Long Code
  - Maximal Linear Feedback Shift Register Sequence
  - Length (Period) is $2^{42}-1$
- Unique identifier for:
  - Access and Traffic Channel (R. Link)
  - Paging and Traffic Channel (F. Link)
- Functions
  - Access, Paging, Traffic Channel spreading
  - DBR on the Reverse Traffic Channel
  - Power Control Bit randomization
  - Data Scrambling (encryption) and Authentication
PN Short Codes of length $2^{15}$

1.2288 Mcps

To Tx

I PN

Q PN
Short Code

- Short Code \((2^{15})\)
  - Unique identifier for a Cell or a Sector
  - Repeats every 26.67 ms
  - Consists of I and Q codes (different polynomials)
- It is called a Modified Maximal Length Sequence or a de bruijn sequence or span-\(n\) sequence.
- It is obtained by adjoining one extra bit “1” after the unique run of 1 of length 14 in the PN sequence of length \(2^{15}-1\).
Summary of Application to DS-CDMA systems

- Orthogonality -- Channelizing and Coding
  - Scrambling and Authentication
  - Spectrum Spreading