m-Sequences

- **Maximal-length sequences**
  - A type of **cyclic code**
    - Generated and characterized by a generator polynomial
    - Properties can be derived using algebraic coding theory
  - Simple to generate with **linear feedback shift-register (LFSR)** circuits
    - Automated
  - Approximate a random binary sequence.
  - Disadvantage: Relatively easy to intercept and regenerate by an unintended receiver

(Serial-in/Serical-out) Shift Register

- Accept data serially: one bit at a time on a single line.
- Each clock pulse will move an input bit to the next FF. For example, a 1 is shown as it moves across.
- Example: five-bit serial-in serial-out register.
Linear Feedback Shift-Register (LFSR)

- Binary sequences drawn from the alphabet \{0,1\} are shifted through the shift register in response to clock pulses.
  - Each clock time, the register shifts all its contents to the right.
  - The particular 1s and 0s occupying the shift register stages after a clock pulse are called states.

- Suppose there are \( r \) FFs. Then a state \( \mathbf{s} \) of the SR can be represented by \( r \) bits.
  - There are \( 2^r \) possible states.
  - There are \( 2^r - 1 \) non-zero states.

\[
\begin{array}{c|c|c}
\text{GF(2)} & \text{Galois field (finite field) of two elements} \\
\text{Consist of} & \text{the symbols 0 and 1 and} \\
& \text{the (binary) operations of} \\
& \text{mod \- 2 addition (XOR) and} \\
& \text{mod \- 2 multiplication.} \\
& \text{The operations are defined by} \\
+ & \begin{array}{c|c|c}
0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array} & \begin{array}{c|c|c}
0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}
\end{array}
\]
Linear Feedback Shift-Register (LFSR)

- All the values are in GF(2) which means they can only be 0 or 1.
- The value of $g_i$ determines whether the output of the $k^{th}$ FF will be in the sum that produce the feedback bit.
  - 1 signifies closed or a connection and
  - 0 signifies open or no connection.
- Ex. Suppose $g_1 = 0$, $g_2 = 1$, $g_3 = 1$ in our LFSR.

m-sequence generator (1)

- Start with a “primitive polynomial”
  - $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$
  - $r = \text{degree of the polynomial}$
- Use $r$ flip-flops.
- The feedback taps in the feedback shift register are selected to correspond to the coefficients of the primitive polynomial.
- Ex. $g(x) = 1 + x^2 + x^3$ is a primitive polynomial.
  
  $= 1 + 0x + 1x^2 + 1x^3$

  (Degree: $r = 3 \Rightarrow$ use 3 flip-flops)
m-sequence generator (2)

- We start with state 100.
  - You may choose different non-zero state.
  - Note that if we start with 000, we won’t go anywhere.

- Any polynomial generates periodic sequence.
  - The maximum period is $2^r - 1$.
- In this example, the state cycles through all $2^3 - 1 = 7$ non-zero states.

State Diagram

The m-sequence is: 00101110010111001011...

Periodic with period = 7

Circuit diagram

The output sequence is periodic with period 7.

<table>
<thead>
<tr>
<th>Time</th>
<th>$s_1$</th>
<th>$s_2$</th>
<th>$s_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The m-sequence cycle is: 0010111001011100101110010111...
Primitive Polynomial

- Definition: A LFSR **generates an m-sequence** if and only if (starting with any nonzero state,) it visits all possible nonzero states (in one cycle).

- Technically, one can define primitive polynomial using concepts from finite field theory.

- Fact: A polynomial generates m-sequence if and only if it is a primitive polynomial.
  - Therefore, we use this fact to define primitive polynomial.

- For us, a polynomial is **primitive** if the corresponding LFSR circuit generates m-sequence.

Sample Exam Question

Draw the complete **state diagrams** for linear feedback shift registers (LFSRs) using the following polynomials. Does either LFSR generate an m-sequence?

1. $g(x) = 1 + x^2 + x^3$
2. $g(x) = 1 + x + x^2 + x^3$
Solution (1)

Draw the complete state diagrams for linear feedback shift registers (LFSRs) using the following polynomials. Does either LFSR generate an m-sequence?

1. \( g(x) = 1 + x^2 + x^3 \)

   The corresponding LFSR generates an m-sequence because the state diagram contains a cycle that visits all possible nonzero states.
   We can also conclude that \( g(x) = 1 + x^2 + x^3 \) is a primitive polynomial.

Solution (2)

\[ g(x) = 1 + x + x^2 + x^3 \]

The corresponding LFSR does not create m-sequence. \( \Rightarrow g(x) \) is not primitive.
m-Sequences: More properties

1. The contents of the shift register will cycle over all possible $2^r - 1$ nonzero states before repeating.
2. Contain one more 1 than 0 (Slightly unbalanced)
3. **Shift-and-add property**: Sum of two (cyclic-)shifted m-sequences is another (cyclic-)shift of the same m-sequence
4. If a window of width $r$ is slid along an m-sequence for $N = 2^r - 1$ shifts, each $r$-tuple except the all-zeros $r$-tuple will appear exactly once
5. For any m-sequence, there are
   - One run of ones of length $r$
   - One run of zeros of length $r - 1$
   - One run of ones and one run of zeroes of length $r - 2$
   - Two runs of ones and two runs of zeros of length $r - 3$
   - Four runs of ones and four runs of zeros of length $r - 4$
   - ...
   - $2^{r-3}$ runs of ones and $2^{r-3}$ runs of zeros of length 1

---

m-Sequences: More Properties

1. The contents of the shift register will cycle over all possible $2^r - 1$ nonzero states before repeating.
2. Each cycle contains exactly one more 1s than 0s (Slightly unbalanced)

$$g(x) = 1 + x^2 + x^3$$

Period $= 2^r - 1 = 2^{3} - 1 = 7$

m-Sequences: More Properties

3. **Shift-and-add property**: Sum of two (cyclic-)shifted m-sequences is another (cyclic-)shift of the same m-sequence.

![Shift-and-add property example](image)

4. If a window of width \( r \) is slid along an m-sequence for \( N = 2^r - 1 \) shifts, each \( r \)-tuple except the all-zeros \( r \)-tuple will appear exactly once.

![Example of window sliding](image)

m-Sequences: More Properties

5. For any m-sequence, there are \( 2^{r-1} \) runs.
   - One run of ones of length \( r \)
   - One run of zeros of length \( r-1 \)
   - One run of ones and one run of zeroes of length \( r-2 \)
   - Two runs of ones and two runs of zeros of length \( r-3 \)
   - Four runs of ones and four runs of zeros of length \( r-4 \)
   - \( \ldots \)
   - \( 2^{r-3} \) runs of ones and \( 2^{r-3} \) runs of zeros of length 1

In other words, the relative frequency for runs of length \( \ell \) is

\[
\begin{cases}
\frac{1}{2^\ell}, & \ell < r, \\
\frac{1}{2^{r-1}}, & \ell = r.
\end{cases}
\]

![Runs and relative frequency diagram](image)

\[\text{There are 4 runs, } \frac{2}{4} = \frac{1}{2}, \text{ of these are of length 1}\]

m-Sequences: Another Example

- $2^5 - 1 = 31$-chip m-sequence
- The following sequence contains 16 runs

000111110011010010000101011101

- Rel. Freq of Run Lengths

<table>
<thead>
<tr>
<th>Run Length</th>
<th>Rel. Freq</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1/16</td>
</tr>
<tr>
<td>4</td>
<td>1/16</td>
</tr>
<tr>
<td>3</td>
<td>2/16</td>
</tr>
<tr>
<td>2</td>
<td>4/16</td>
</tr>
<tr>
<td>1</td>
<td>8/16</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\text{Rel. Freq of Runs} & \\
11111 & 1/16 \\
00000 & 1/16 \\
111    & 1/16 \\
000    & 1/16 \\
11     & 2/16 \\
00     & 2/16 \\
1      & 4/16 \\
0      & 4/16
\end{align*}
\]

\[
\begin{align*}
\frac{1}{2^\ell}, & \quad \ell < 5, \\
\frac{1}{2^{\ell-1}}, & \quad \ell = 5.
\end{align*}
\]


(Time) Autocorrelation Function for Energy Sequence

\[
x[n] = (0\ 2\ 4\ 3\ 2\ 1\ 0)
\]

\[
R_x[\tau] = \sum_{n=-\infty}^{\infty} x[n]x[n-\tau]
\]

\[
= \sum_{n=-\infty}^{\infty} x[n]x[n + \tau]
\]
(Time) Autocorrelation Function for Energy Sequence

$x[n] = (0 \ 2 \ 4 \ 3 \ 2 \ 1 \ 0)$

$R_x[\tau] = \sum_{n=-\infty}^{\infty} x[n]x[n - \tau] = \sum_{n=-\infty}^{\infty} x[n]x[n + \tau]$
MATLAB: `xcorr`

- `r = xcorr(x, y)`
  - Return the cross-correlation of two discrete-time sequences, `x` and `y`.
  - If `x` and `y` have different lengths, the function appends zeros at the end of the shorter vector so it has the same length as the other.
  - The lag (`\tau`) is varied from \(-N\) to \((N - 1)\) where `N` is the longer length of the two sequences.
- `[r, lags] = xcorr(__)`
  - Also returns vector with the lags (`\tau`) at which the correlations are computed.

(Time) Autocorrelation Function for Energy Sequence

```matlab
close all
x = [0 2 4 3 2 1 0]; % plot the signal
plot(x,'--','LineWidth',1.5)
hold on
plot(x,'o','LineWidth',1.5)
ylabel('x[n]')
xlabel('n')

% plot auto-correlation function
figure
[R lag] = xcorr(x,x);
plot(R,'--','LineWidth',1.5)
hold on
plot(R,'o','LineWidth',1.5)
ylabel('R_x[tau]')
xlabel('tau')
```
(Time) Autocorrelation Function for Power and Periodic Sequence

<table>
<thead>
<tr>
<th></th>
<th>Time average $\langle x[n] \rangle$</th>
<th>Autocorrelation $R_x[\tau]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Sequence</td>
<td>$\lim_{T \to \infty} \frac{1}{2T} \sum_{n=-T}^{T} x[n]$</td>
<td>$\langle x[n]x[n-\tau] \rangle = \lim_{T \to \infty} \frac{1}{2T} \sum_{n=-T}^{T} x[n]x[n-\tau]$</td>
</tr>
<tr>
<td>Periodic Sequence</td>
<td>$\frac{1}{T_0} \sum_{T_0} x[n]$</td>
<td>$\frac{1}{T_0} \sum_{T_0} x[n]x[n-\tau] = \frac{1}{T_0} \sum_{T_0} x[n]x[n-\tau]$</td>
</tr>
</tbody>
</table>

Example: (Time) Autocorrelation Function for Periodic Sequence

$T_0 = 6$
Example: (Time) Autocorrelation Function for Periodic Sequence

\[
x[n] = 0 2 4 3 2 1 0 2 4 3 2 1 0 2 4 3 2 1
\]
\[
x[n-1] = 1 0 2 4 3 2 1 0 2 4 3 2 1 0 2 4 3 2 1
\]

\[
R_x[\tau] = \sum \frac{1}{N} x[n]x[n-\tau]
\]

\[
\sum_{\tau=-N}^{N} x[n]x[n-\tau]
\]

Back to m-Sequences

\[
c[n]: 00101110010111001011100101110010111001011100101110010111
\]

In actual transmission, we will map “0 and 1” to “+1 and -1”, respectively.
Back to m-Sequences

$c[n]$: 00101110010111001011100101110010111001011100101110010111

\[ \text{property } \ast 2 + \text{ property } \ast 3 \]

In actual transmission, we will map “0 and 1” to “+1 and -1”, respectively.

Autocorrelation when not aligned:

\[
\begin{array}{cccccccc}
-1 & 1 & -1 & -1 & 1 & 1 & \times \\
1 & 1 & -1 & 1 & -1 & -1 & -1 \\
\end{array}
\]

\[ \sum = -1 \times \frac{1}{7} = \frac{-1}{7} \]

In actual transmission, we will map “0 and 1” to “+1 and -1”, respectively.
m-Sequences: Autocorrelation function

Consider a periodic sequence whose one period is given by

\[-1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1 \ 1 \ -1 \ -1\]

The shift property of binary random sequence implies that

\[
R_x[\tau] = \langle x[n]x[n-\tau] \rangle
\]

\[
\xrightarrow{n \to \infty} E[x[n]x[n-\tau]]
\]

\[
= 1 \times \frac{1}{2} + (-1) \times \frac{1}{2} = 0
\]
Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by
\[1 - 2 \times \text{randi}([0 \ 1], 1, 100)\]

The shift property of binary random sequence implies that
\[R_x[\tau] = \langle x[n] x[n - \tau] \rangle\]
\[
\overset{n \to \infty}{\text{LLN}} \Rightarrow \mathbb{E}[x[n] x[n - \tau]]
\]
\[= 1 \times \frac{1}{2} + (-1) \times \frac{1}{2} = 0\]
Example: Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by

\[ 1 - 2 \times \text{randi}([0 1], 1, 10000) \]

The shift property of binary random sequence implies that

\[ R_x[\tau] = \langle x[n] x[n - \tau] \rangle \]

\[ \xrightarrow{n \to \infty \text{ LLN}} \mathbb{E}[x[n] x[n - \tau]] \]

\[ = 1 \times \frac{1}{2} + (-1) \times \frac{1}{2} = 0 \]

Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by

\[ 1 - 2 \times \text{randi}([0 1], 1, 100000) \]

The shift property of binary random sequence implies that

\[ R_x[\tau] = \langle x[n] x[n - \tau] \rangle \]

\[ \xrightarrow{n \to \infty \text{ LLN}} \mathbb{E}[x[n] x[n - \tau]] \]

\[ = 1 \times \frac{1}{2} + (-1) \times \frac{1}{2} = 0 \]
Autocorrelation and PSD

- (Normalized) autocorrelations of maximal sequence and random binary sequence.

\[ R(t) = \frac{1}{NT_c} \int_{-T_c/2}^{T_c/2} y(t) y(t+r) \, dr = \begin{cases} 1, & |r| \leq \frac{T_c}{2} \\ \frac{-1}{N^2}, & \frac{T_c}{2} < |r| \leq \frac{N+1}{2} \frac{T_c}{N} \end{cases} \]

where the integration is over any period, \( Z_0 = NT_c \).

\[ S_n(f) = \sum_{m=-N}^{N} P_n \delta (f - m f_0), \quad f_0 = 1/NT_c, \]

where

\[ P_n = \left( \frac{(N+1)N}{N^2} \right) \sin^2 \left( \frac{m \pi}{N} \right), \quad m \neq 0, \quad \sin(x) = (\sin \pi x) / (\pi x) \]

\[ \frac{1}{N^2}, \quad m = 0. \]

Power spectral density of maximal sequence.

References: m-sequences

  - Page 84-90
  - Chapter 1 and 2
- Goldsmith, *Wireless Communications*, 2005
  - Chapter 13
  - Section 3.4.3
Review: m-sequence

DSSS: $m(t) \times c(t)$

Spectral spreading waveform

Spreading code/sequence

<table>
<thead>
<tr>
<th>$c[n]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 1 0 1 1 1 0 0 1 0 1</td>
</tr>
</tbody>
</table>

One important collection of these is the collection of m-sequences.

Generated with LFSR whose connections corresponds to coefficients of primitive polynomials. The resulting sequence achieves the maximum period (length) of $N = 2^r - 1$ where $r$ is the degree of primitive polynomial.