## ECS455: Chapter 4 <br> Multiple Access

## 4.4 m -sequence

Office Hours:
BKD, 6th floor of Sirindhralai building
Tuesday $\quad 14: 20-15: 20$
Wednesday $\quad$ 14:20-15:20

Dr.Prapun Suksompong

prapun.com/ecs455

Friday $\quad 9: 15-10: 15$

## Binary Random Sequence



- These names are simply many versions of the same sequence/process.
- You should be able to convert one version to others easily.
- Some properties are conveniently explained when the
- Consider the sequence $X_{1}, X_{2}, X_{3}, \ldots, X_{n^{\prime}}, \ldots$
- Disadvantages
- Can not further "compress" the sequence
- Difficult to convey the sequence from the Tx to Rx
- Require large storage at both Tx and Rx
- Advantages
- Random = unpredictable

1. Balanced property
2. Run length property
3. Shift property
sequence is expressed in a particular version.

## Properties of Binary Random Sequences:

## Binary Random Sequences

- While DSSS chip sequences must be generated deterministically, properties of binary random sequences are useful to gain insight into deterministic sequence design.
- A random binary chip sequences consists of i.i.d. bit values with probability one half for a one or a zero.
- Also known as Bernoulli sequences/trials, "coin-flipping" sequences
- A random sequence of length $N$ can be generated, for example, by flipping a fair coin $N$ times and then setting the bit to a one for heads and a zero for tails.


## Properties of Binary Random Sequences: Balanced Property

- $\{0,1\}$ version

$$
\frac{1}{N} \sum_{i=1}^{N} X_{i} \xrightarrow[\text { LLN }]{N \rightarrow \infty} \mathbb{E}\left[X_{i}\right]=0 \times \frac{1}{2}+1 \times \frac{1}{2}=\frac{1}{2}
$$

- $\{ \pm 1\}$ version

$$
\frac{1}{N} \sum_{i=1}^{N} X_{i} \xrightarrow[\text { LLN }]{N \rightarrow \infty} \mathbb{E}\left[X_{i}\right]=(-1) \times \frac{1}{2}+1 \times \frac{1}{2}=0
$$

## Properties of Binary Random Sequences: Run Length Property

Start of a
run of 1 s

\[

\]

## FYI: Run-Length Encoding (RLE)

- A very simple form of lossless data compression in which runs of data (that is, sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run.
- Most useful on data that contains many such runs.
- Example: Consider a screen containing plain black text on a solid white background.
A line, with B representing a black pixel and W representing white, might read as follows:

With a RLE data compression algorithm applied to the above line, it can be rendered as follows:
12W1B12W3B24W1B14W

## Properties of Binary Random Sequences: Shift Property

Original sequence: $X_{1} \quad X_{2} \quad X_{3} \quad X_{4} \quad \cdots \quad X_{N}$

Shifted sequence: $X_{-1} \quad X_{0} \quad X_{1} \quad X_{2} \quad \cdots \quad \bar{X}_{N-2}$ (amount of shift (delay) $=2$ )

- When the shifted amount $=0$, the two sequences are exactly the same.
- When the shifted amount $=s$,
we want to compare $X_{j}$ and $X_{j-s}$.
- What proportion are the same?
- What proportion are different?
- Recall that the numbers in the sequence are independent results (from several Bernoulli trials)



## Key randomness properties

[Golomb, 1967][Viterbi, 1995, p. 12] Binary random sequences with length $N$ asymptotically large have a number of the properties desired in spreading codes

- Balanced property: Equal number of ones and zeros.
- Should have no DC component to avoid a spectral spike at DC or biasing the noise in despreading
- Run length property: The run length is generally short.
- half of all runs are of length 1
- a fraction $1 / 2^{n}$ of all runs are of length $n \quad$ (Geometric)
- Long runs reduce the BW spreading and its advantages
- Shift property: If they are shifted by any nonzero number of elements, the resulting sequence will have half its elements the same as in the original sequence, and half its elements different from the original sequence.


## Properties of Binary Random Sequences: Shift Property

- $\{0,1\}$ version: The comparison is done via the $\operatorname{XOR}(\bigoplus)$ operation
- $\mathrm{x} \bigoplus \mathrm{y}=0$ iff they are the same
- $\mathrm{x} \oplus \mathrm{y}=1$ iff they are different
- $\{ \pm 1\}$ version: The comparison is done via the multiplication operation
- $x \times y=1$ iff they are the same
- $x \times y=-1$ iff they are different


## Pseudorandom Sequence

- A deterministic sequence that has the balanced, run length, and shift properties as it grows asymptotically large is referred to as a pseudorandom sequence (noiselike or pseudonoise (PN) signal).
- Ideally, one would prefer a random binary sequence as the spreading sequence.
- However, practical synchronization requirements in the receiver force one to use periodic Pseudorandom binary sequences.
- m-sequences
- Gold codes
- Kasami sequences


## m-Sequences

- Maximal-length sequences

Longer name: Maximal length linear shift register sequence.

- A type of cyclic code
- Generated and characterized by a generator polynomial
- Properties can be derived using algebraic coding theory
[Goldsmith, 2005, p 387
- 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


## GF(2)

- Galois field (finite field) of two elements
- Consist of
- the symbols 0 and 1 and
- the (binary) operations of
- modulo-2 addition (XOR) and
- modulo-2 multiplication.
- The operations are defined by

$$
\begin{array}{c|ll}
+ & 0 & 1 \\
\hline 0 & 0 & 1 \\
1 & 1 & 0
\end{array} \quad \begin{array}{c|cc}
. & 0 & 1 \\
\hline 0 & 0 & 0 \\
1 & 0 & 1
\end{array}
$$

## 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 1 s and 0 s occupying the shift register stages after a clock pulse are called states.
- Suppose there are $r$ FFs. Then a state $\underline{\mathbf{S}}$ of the SR can be represented by $r$ bits.
- There are $2^{r}$ possible states.
- There are $2^{r}-1$ non-zero states.



## Linear Feedback Shift-Register (LFSR)

- All the values are in $\mathrm{GF}(2)$ which means they can only be 0 or 1 .
- The value of $g_{i}$ determines whether the output of the $k^{\text {th }} \mathrm{FF}$ 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"
- $g(x)=g_{0}+g_{1} x+g_{2} x^{2}+\cdots+g_{r} x^{r}$
${ }_{r}=$ 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.

$$
=1+0 x+1 x^{2}+1 x^{3}
$$

(Degree: $\mathrm{r}=3 \boldsymbol{\rightarrow}$ 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


State Diagram


000

output
Time

| $s_{1}$ | $s_{2}$ | $s_{3}$ |
| :---: | :---: | :---: |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |
| 1 | 0 | 0 |

## 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. through all $2^{3}-1=7$ non-zero states.


## 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 (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 msequence 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.

## 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
- $2^{\mathrm{r}-3}$ runs of ones and $2^{\mathrm{r}-3}$ 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 1 s than 0 s (Slightly unbalanced)
$g(x)=1+x^{2}+x^{3}$


00101110010111001011100101110010111001011100101110010111

50

## m-Sequences: More Properties

3. Shift-and-add property: Sum of two (cyclic-)shifted msequences is another (cyclic-)shift of the same m-sequence
$0 0 \longdiv { 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 }$
0 phase shift: 0010111
1 phase shift: 0101110
2 phase shift: 1011100
$\rightarrow 3$ phase shift: 0111001
$\lambda_{\lambda} \oplus=1100101$
4 phase shift: 1110010
5 phase shift: 1100101
6 phase shift: 1001011
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

00101110010111001011100101110010111001011100101110010111
[S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.]

## 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
- ..
- $2^{r-3}$ runs of ones and $2^{r-3}$ runs of zeros of length 1

In other words, relative frequency for runs of length $\ell$ is $\begin{cases}\frac{1}{2^{\ell}}, & \ell<r, \\ \frac{1}{2^{\ell-1}}, & \ell=r .\end{cases}$

$\underbrace{001011100101110010111001011100101110010111}$
Runs:
111
1,0
[S.W. Golomb, Shijt Register Sequences, Holden-Day, San Francisco, 1967.]

## m-Sequences: Another Example

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

0001111100110100100001010111011

- Rel. Freq of Runs
- Rel. Freq of Run Lengths

| Run Length | Rel. Freq. |
| :---: | :---: |
| 5 | $1 / 16$ |
| 4 | $1 / 16$ |
| 3 | $2 / 16$ |
| 2 | $4 / 16$ |
| 1 | $8 / 16$ |

11111 1/16
0000 1/16
111 1/16
000 1/16
11 2/16
$00 \quad 2 / 16$
1 4/16

## (Time) Autocorrelation Function for Energy Sequence



$$
x[n]=\left(\begin{array}{lllllll}
0 & 2 & 4 & 3 & 2 & 1 & 0
\end{array}\right)
$$

54


## (Time) Autocorrelation Function for Energy Sequence



## MATLAB: xcorr

- $r=x \operatorname{cor}(x, y)$
- 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 $-(N-1)$ 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

```
close all
x = [0 2 4 3 2 1 0];
```

\% plot the signal
plot(x,'--','LineWidth',1.5) hold , hold on
plot(x,'o','LineWidth',1.5) ylabel('x[n]')
xlabel('n')
\% plot auto-correlation function figure
$[\mathrm{R} \operatorname{lag}]=x \operatorname{corr}(x, x)$;
plot(R,'--','LineWidth', 1.5) hold on
plot(R,'o','LineWidth',1.5) ylabel('R_x[\tau]') xlabel('\tau')

58


(Time) Autocorrelation Function for Power and Periodic Sequence

|  | Time average <br> $\langle x[n]\rangle$ | Autocorrelation <br> $R_{x}[\tau]$ |
| :--- | :---: | :---: |
| Power Sequence | $\lim _{T \rightarrow \infty} \frac{1}{2 T} \sum_{n=-T}^{T} x[n]$ | $\langle x[n] x[n-\tau]\rangle=\lim _{T \rightarrow \infty} \frac{1}{2 T} \sum_{n=-T}^{T} x[n] x[n-\tau]$ |
| $\langle x[n] x[n+\tau]\rangle=\lim _{T \rightarrow \infty} \frac{1}{2 T} \sum_{n=-T}^{T} x[n] x[n+\tau]$ |  |  |
| Periodic Sequence <br> with period $T_{0}$ | $\frac{1}{T_{0}} \sum_{T_{0}} x[n]$ | $\frac{1}{T_{0}} \sum_{T_{0}} x[n] x[n-\tau]=\frac{1}{T_{0}} \sum_{T_{0}} x[n] x[n-\tau]$ |



Example: (Time) Autocorrelation Function for Periodic Sequence


Example: (Time) Autocorrelation Function for Periodic Sequence

$\begin{array}{lllllllllllllllllllllll}x[n] & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 3 & 2\end{array}$ $x[n-1] 1 \begin{array}{llllllllllllllllll:lllll} & 0 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 2 & 1 & 0 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 3 & 2\end{array}$ $x\left[\begin{array}{lllllllllllll:llllll:lll}n-1] & 1 & 0 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 4 & 3 & 2 & 1 & 0 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \\ 0\end{array}\right.$ $\rightarrow 4.67$

## Back to m-Sequences

$c[n]: 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 \longdiv { 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 }$ 0010111

1001011
In actual transmission, we will map " 0 and 1 " to " +1 and -1 ", respectively.


## Back to m-Sequences

$c[n]: 00101110010111001011100101110010111001011100101110010111$

001011
In actual transmission, we will map " 0 and 1 " to " +1 and -1 ", respectively.

Autocorrelation when not aligned:

63

$$
\begin{array}{rrrrrrr}
-1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1
\end{array} \underset{-1}{ } 1 \begin{array}{rrrrrr}
\longrightarrow & 1 & -1 & 1 & -1 & -1 \\
-1 & \\
\times \frac{1}{7}
\end{array}
$$

m-Sequences: Autocorrelation function

$R_{c}[\tau]$

m-Sequences: Autocorrelation function


## Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by
$\left[\begin{array}{llllllllll}-1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1\end{array}\right]$

66)

## Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by $1-2^{*}$ randi([0 1 1 , 1, 100000)


## Autocorrelation and PSD

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

- Power spectral density of maximal sequence.


$$
\begin{aligned}
& \text { where the integration is over ayy period, } T_{0}=N T_{F} \\
& \qquad S_{i}(f)=\sum_{N=-\infty}^{P_{\infty} \delta\left(f-m f_{0}\right) . f_{0}=1 / N T_{*} .}
\end{aligned}
$$

- 

$$
=\left\{\begin{array}{l}
{\left[(N+1) / N^{2}\right] \sin ^{2}(m / N), m \neq 0 \cdot \operatorname{sinc}(x)=(\sin \pi x) /(\pi x)} \\
1 / N^{2}, m=0 .
\end{array}\right.
$$

(71)


## References: m-sequences

- Karim and Sarraf, W-CDMA and cdma2000 for 3G Mobile Networks, 2002.
- Page 84-90
- Viterbi, CDMA: Principles of Spread Spectrum Communication, 1995
- Chapter 1 and 2
- Goldsmith, Wireless Communications, 2005

W-CDMA ${ }^{\text {end }}$ cdma2000

$=$
[TK5103.452 K37 2002]

[TK5103.45 V57 1995]

- Chapter 13
- Tse and Viswanath, Fundamentals of Wireless Communication, 2005
- Section 3.4.3



## Review: m-sequence



## ECS455: Chapter 4 <br> Multiple Access

## 4.4 m -sequence

(Additional Remarks)

Dr.Prapun Suksompong

prapun.com/ecs455

| Office Hours: |  |
| :--- | :--- |
| BKD, th floor of Sirindhrala building |  |
| Tuesday | $14: 20-15: 20$ |
| Wednesday | $14: 20-15: 20$ |
| Friday | $9: 15-10: 15$ |

## Example: (Time) Autocorrelation

 Function for Periodic Sequence
 $\left.x[n-1] 10 \begin{array}{lllllllllll:llllll:llllll} & 0\end{array}\right)$



## Example: (Time) Autocorrelation Function for Periodic Sequence



$$
x[n-1]
$$

$\left[\begin{array}{llllll}0 & 2 & 4 & 3 & 2 & 1\end{array}\right.$



Example: (Time) Autocorrelation Function for Periodic Sequence

Q. $\quad$, a "normalization" operation. So, the combined computation can be called "normalized sumproduct" operation. We may also refer to this as the (sliding computation of) "autocorrelation" $\rightarrow \tau$ operation as well.


Wireless Comm. and Multipath Fading


## Wireless Comm. and Multipath Fading

The signal received consists of a number of reflected rays, each characterized by a different amount of attenuation and

Here, let's consider the discrete-time version of fading:

$$
y[n]=\sum_{i=0}^{v} \beta_{i} c\left[n-\tau_{i}\right]
$$

In particular, let's try

$$
y[n]=5 c[n]-3 c[n-4]+c[n-10]
$$

Identifying Parameters of Multipath Fading via Autocorrelation
$y[n]=5 c[n]-3 c[n-4]+c[n-10]$




