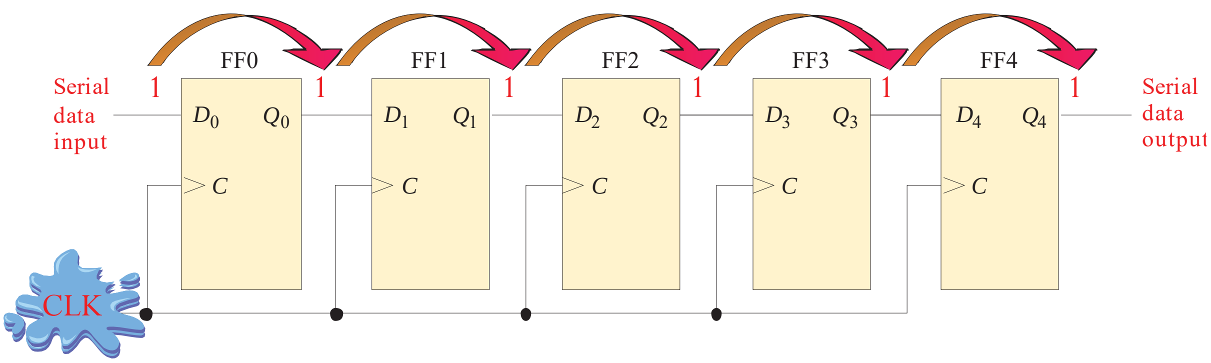
m-Sequences

- **Maximal-length sequences**
- A type of **cyclic code**
  - Generated and characterized by a generator polynomial
  - Properties can be derived using algebraic coding theory [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 [Ziemer, 2007, p 11]

Longer name: Maximal length linear shift register sequence.

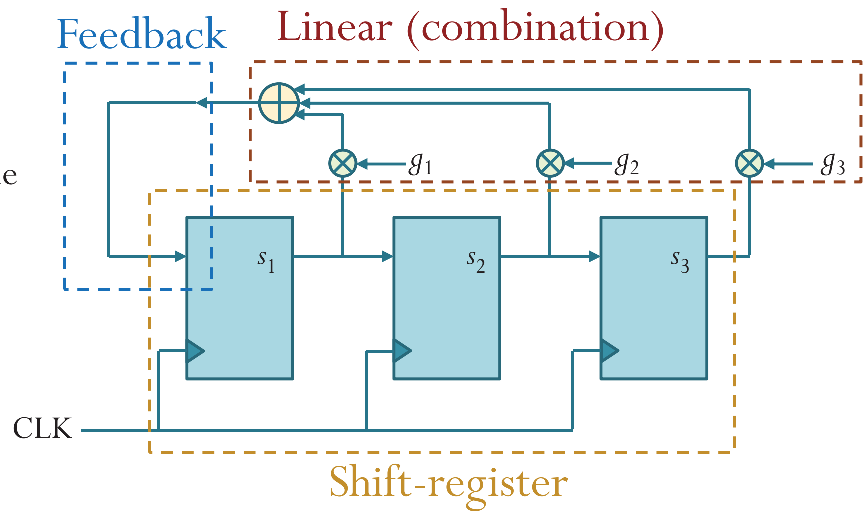
(Serial-in/Serial-out) Shift Register

- 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 $\underline{\mathbf{s}}$ of the SR can be represented by r bits.
  - There are 2^r possible states.
  - There are $2^r - 1$ non-zero states.



GF(2)

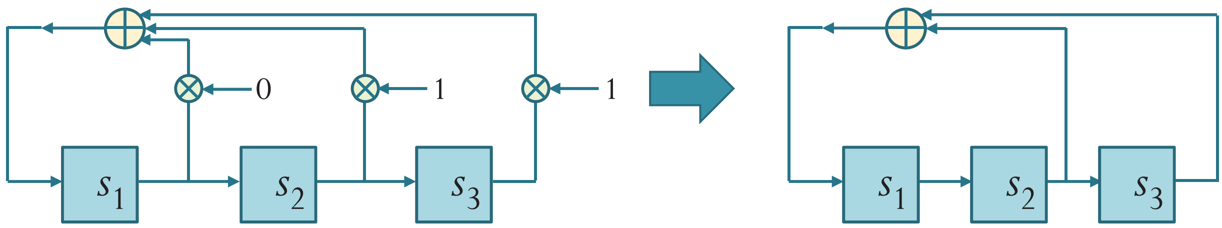
- **Galois field** (finite field) of two elements
- Consist of
  - the symbols 0 and 1 and
  - the (binary) operations of
    - **modulo-2** addition (XOR) and
    - **modulo-2** multiplication.
- The operations are defined by

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

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.



(See Section 13.4.1 in [Lathi, 1998])

m-sequence generator (1)

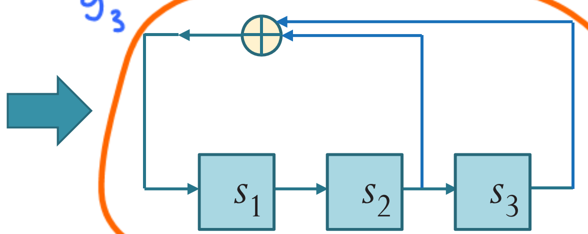
- Start with a "**primitive polynomial**"
  - $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$
  - r = degree of the polynomial
- Use r flip-flops.
- The feedback taps in the feedback shift register are selected to correspond to the coefficients of the primitive polynomial.
- Ex. $g(x) = 1 + x^2 + x^3$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

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

g_0 g_1 g_2 g_3

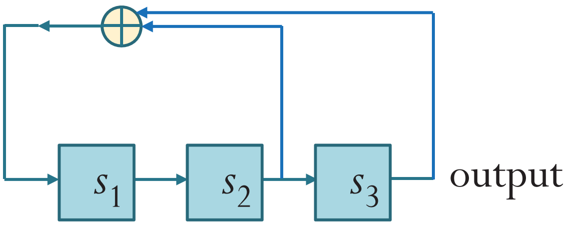
circuit diagram

(Degree: r = 3 ➔ 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.



output

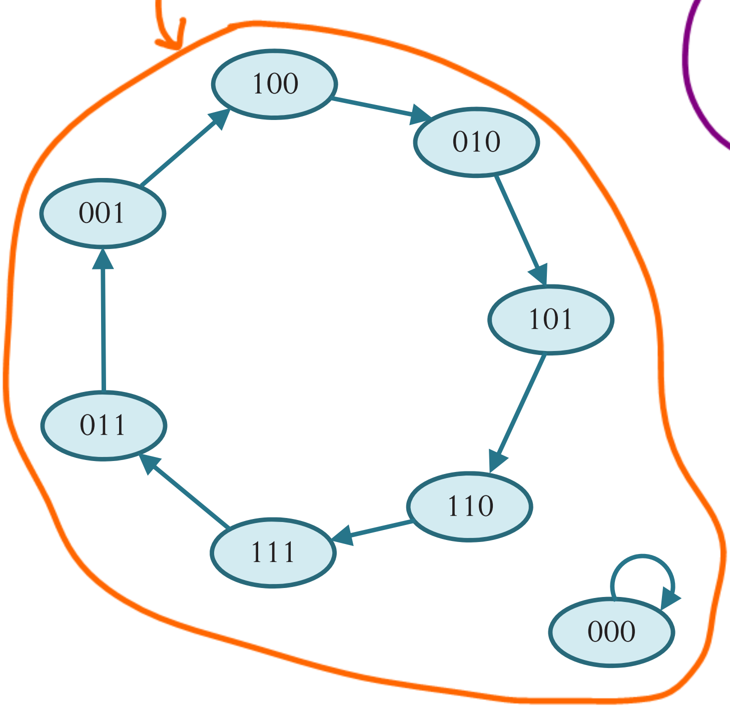
Time	s_1	s_2	s_3
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4			
5			
6			
7			

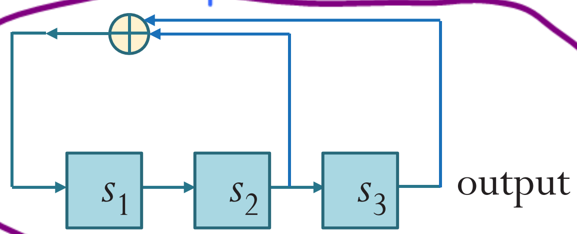
- Any polynomial generates periodic sequence.
  - The maximum period is $2^r - 1$.
- In this example, the state cycles through all $2^3 - 1 = 7$ non-zero states.

m-sequence : 0010111 0010111 0010111 - - -

periodic with period = 7

State Diagram





circuit diagram

output

Time	s_1	s_2	s_3
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0
8	0	1	0
9	1	0	1

(repeat)

m-sequence : 0010111 0010111 0010111 - - -

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

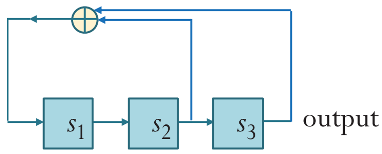
Draw the complete **state diagrams** for linear feedback shift registers (LFSRs) using the following polynomials.
Does either LFSR generate an m-sequence?

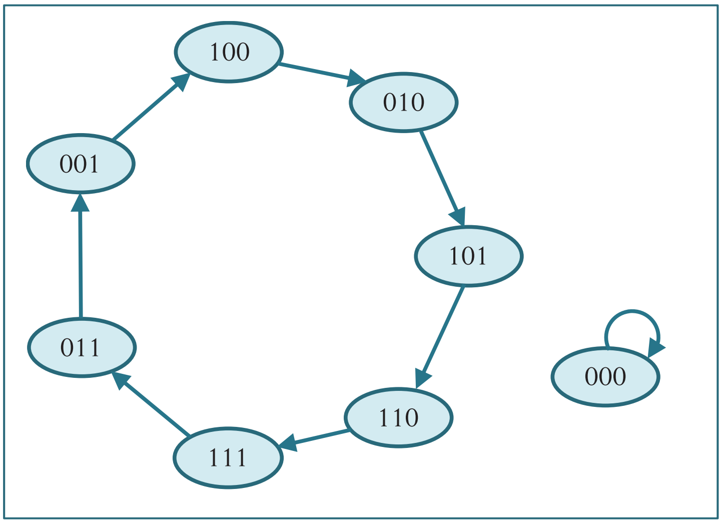
1. $g(x) = 1 + x^2 + x^3$
2. $g(x) = 1 + x + x^2 + x^3$

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)

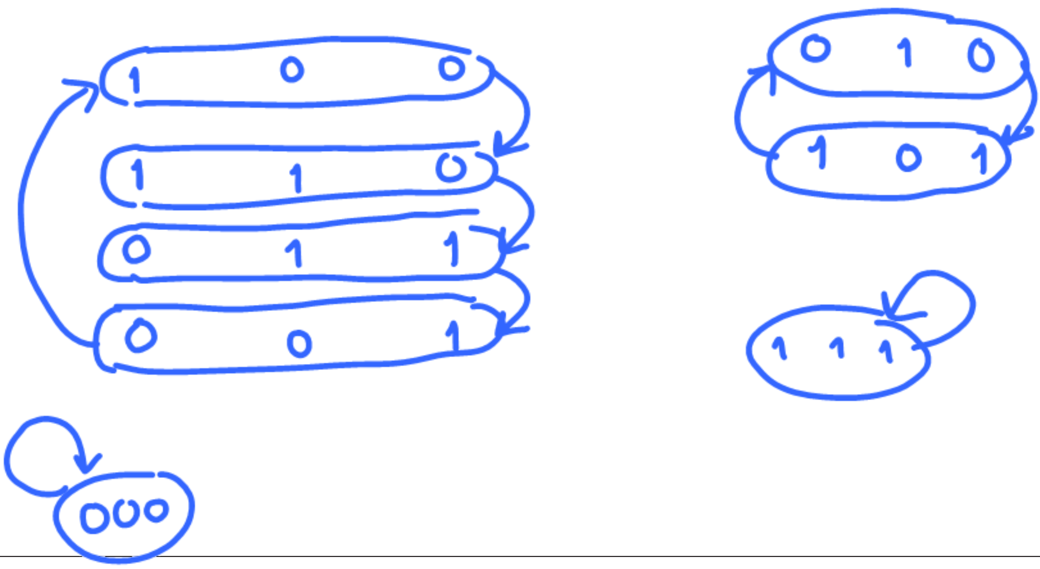
$g_0 \quad g_1 \quad g_2 \quad g_3$

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

The corresponding LFSR does not create m-sequence.

$\Rightarrow$ g(x) is not primitive.

block diagram



m-Sequences: More properties

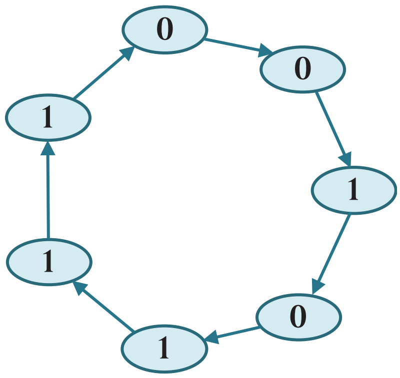
1. The contents of the shift register will cycle over all possible 2^r-1 nonzero states before repeating.
2. Contain one more 1 than 0 (Slightly unbalanced)
3. **Shift-and-add property**: Sum of two **(cyclic-)shifted** m-sequences is another (cyclic-)shift of the same m-sequence
4. If a window of width 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)

$2^{r-1} - 1$ 0s
2^{r-1} 1s

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



period $= 2^r - 1 = 2^3 - 1 = 7$

4 1s
3 0s

0010111001011100101110010111001011100101110010111001011100101110010111

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

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

$\boxed{0010111}$ is shown inside this sequence:

00101110010111001011100101110010111001011100101110010111

0 phase shift: 0010111
1 phase shift: 0101110
2 phase shift: 1011100
3 phase shift: 0111001
4 phase shift: 1110010
5 phase shift: 1100101
6 phase shift: 1001011

$\oplus$ = 1100101

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

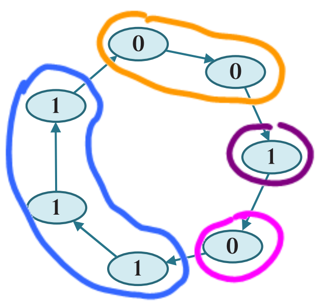
0010111001011100101110010111001011100101110010111

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



$\underbrace{0010111}_{}$0010111001011100101110010111001011100101110010111

Runs:
111
00
1
0

There are 4 runs

$\frac{2}{4} = \frac{1}{2}$ of these are of length 1

[S.W. Golomb, *Shift 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 Run Lengths

Run Length	Rel. Freq.
5	1/16
4	1/16
3	2/16
2	4/16
1	8/16

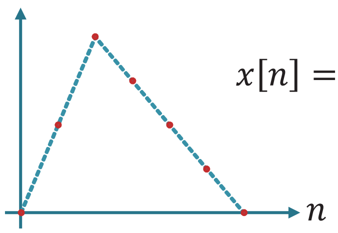
$$\begin{cases} \frac{1}{2^\ell}, & \ell < 5, \\ \frac{1}{2^{\ell-1}}, & \ell = 5. \end{cases}$$

- Rel. Freq of Runs

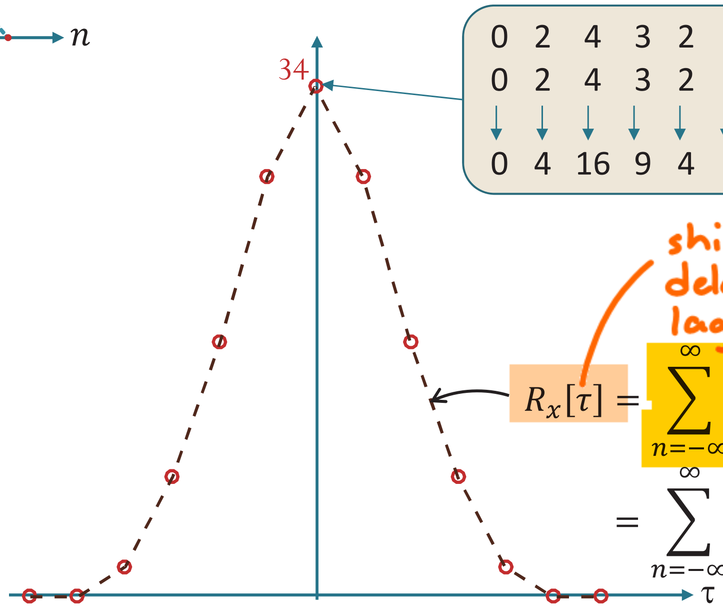
11111	1/16
0000	1/16
111	1/16
000	1/16
11	2/16
00	2/16
1	4/16
0	4/16

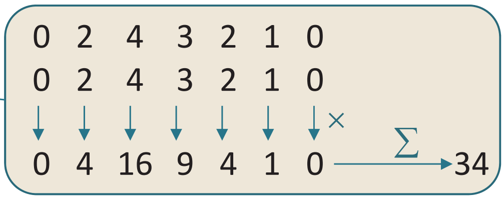
[S.W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.]

(Time) Autocorrelation Function for Energy Sequence



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



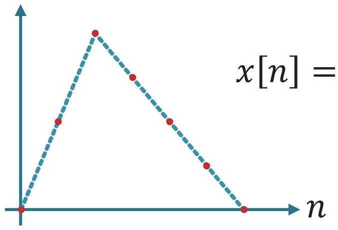


shift/delay/lag

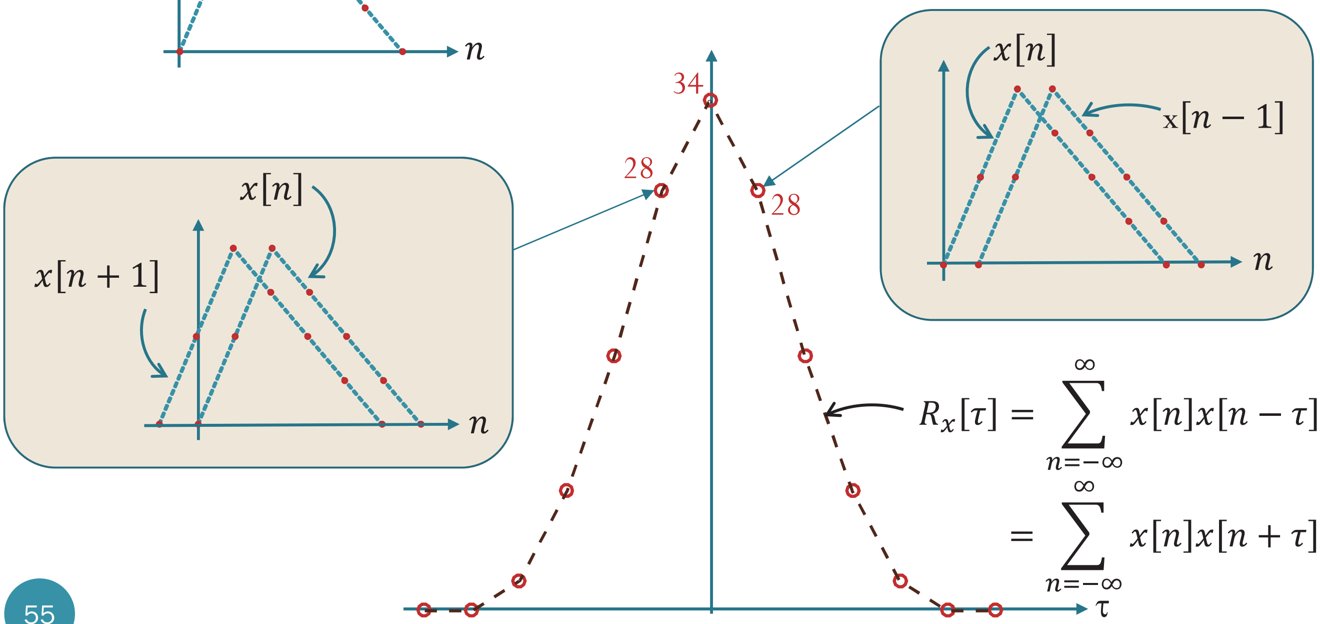
$$R_x[\tau] = \sum_{n=-\infty}^{\infty} x[n]x[n-\tau]$$

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

(Time) Autocorrelation Function for Energy Sequence



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

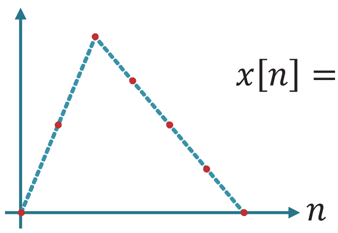


$$R_x[\tau] = \sum_{n=-\infty}^{\infty} x[n]x[n-\tau]$$

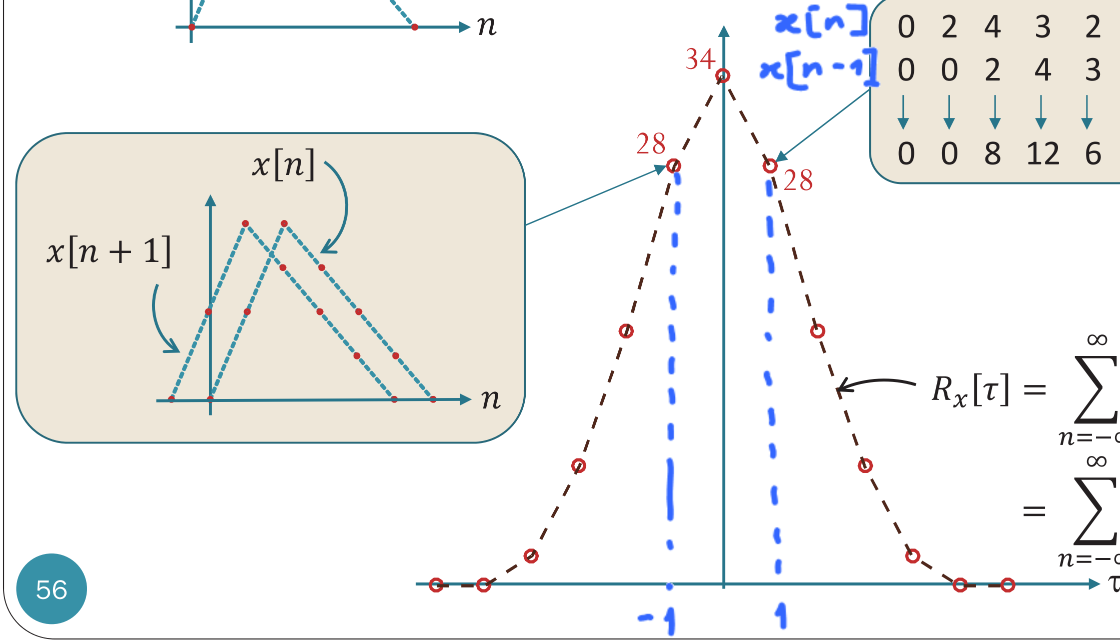
$$= \sum_{n=-\infty}^{\infty} x[n]x[n+\tau]$$

(Time) Autocorrelation Function for Energy Sequence

$\tau = 1$



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



$x[n]$	0	2	4	3	2	1	0	
$x[n-1]$	0	0	2	4	3	2	1	0
	↓	↓	↓	↓	↓	↓	↓ ×	
	0	0	8	12	6	2	0	$\xrightarrow{\Sigma}$ 28

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

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

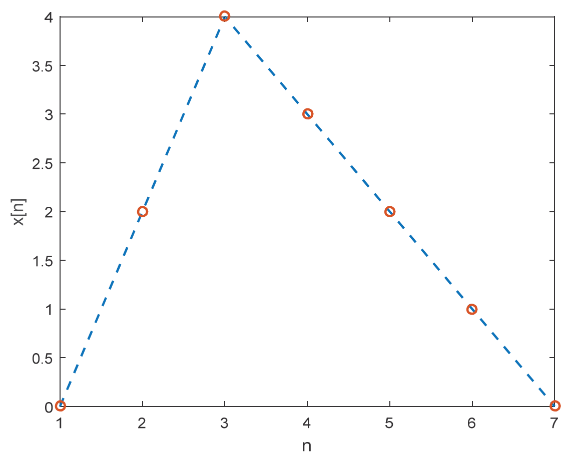
MATLAB: xcorr

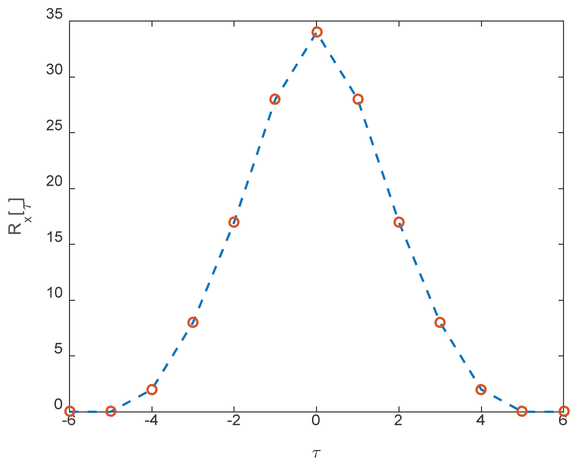
cross

- `r = xcorr(x,y)` plug-in x here to find autocorrelation
  - 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 (τ) 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 (τ) at which the correlations are computed.

(Time) Autocorrelation Function for Energy Sequence

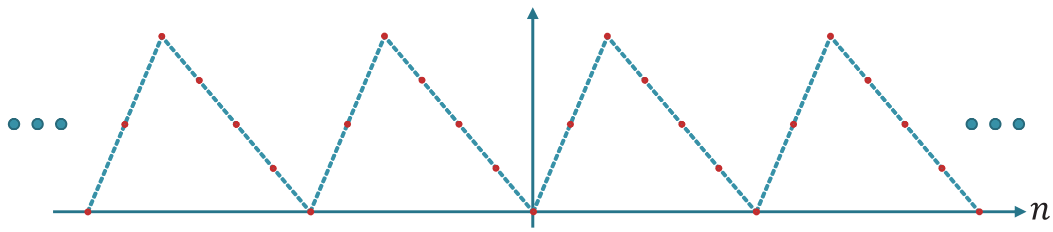
```
close all
x = [0 2 4 3 2 1 0];

% plot the signal
plot(x,'--','LineWidth',1.5)
hold 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')
```



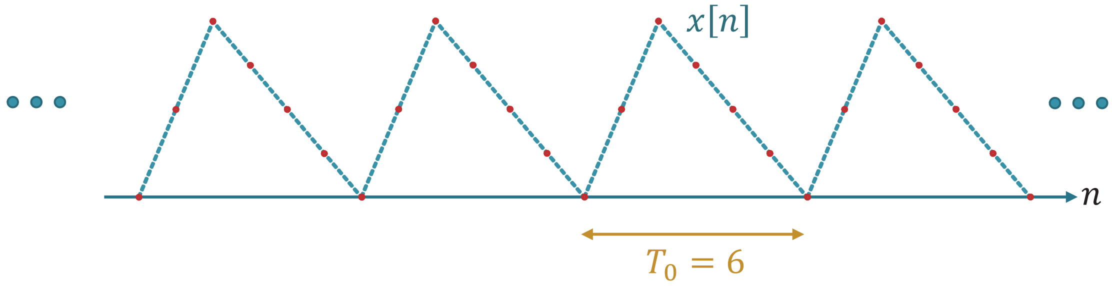


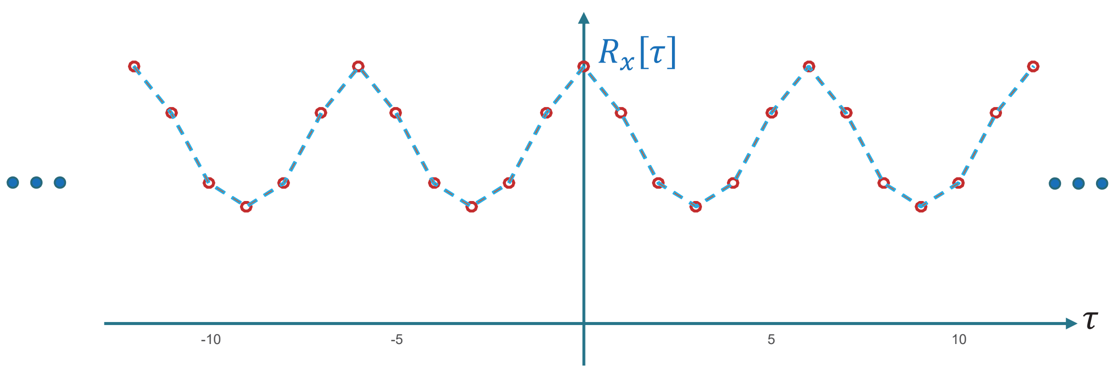
(Time) Autocorrelation Function for Power and Periodic Sequence

	Time average $\langle x[n] \rangle$	Autocorrelation $R_x[\tau]$
Power Sequence	$\lim\limits_{T\to\infty} \frac{1}{2T} \sum\limits_{n=-T}^{T} x[n]$	$\langle x[n]x[n-\tau] \rangle = \lim\limits_{T\to\infty} \frac{1}{2T} \sum\limits_{n=-T}^{T} x[n]x[n-\tau]$ $\langle x[n]x[n+\tau] \rangle = \lim\limits_{T\to\infty} \frac{1}{2T} \sum\limits_{n=-T}^{T} x[n]x[n+\tau]$
Periodic Sequence with period T_0	$\frac{1}{T_0} \sum\limits_{T_0} x[n]$	$\frac{1}{T_0} \sum\limits_{T_0} x[n]x[n-\tau] = \frac{1}{T_0} \sum\limits_{T_0} x[n]x[n-\tau]$



Example: (Time) Autocorrelation Function for Periodic Sequence





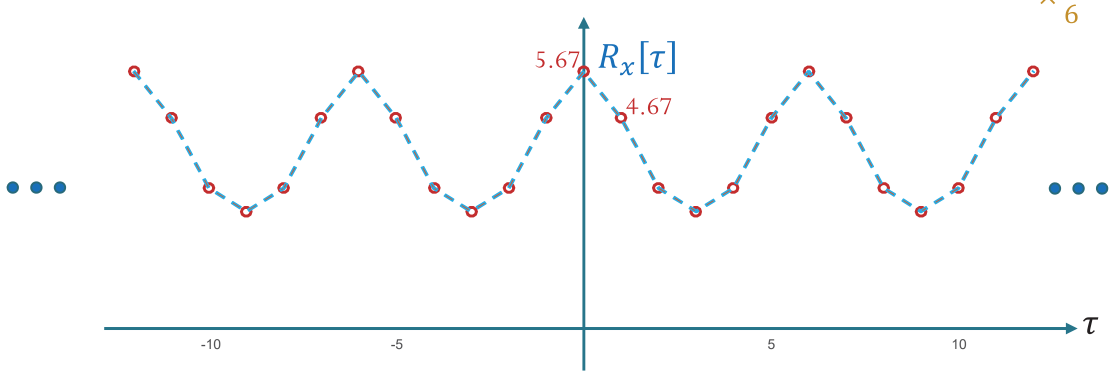
Example: (Time) Autocorrelation Function for Periodic Sequence

$x[n]$	0	2	4	3	2	1	0	2	4	3	2	1	0	2	4	3	2	1	0	2	4	3	2	1
$x[n-0]$	0	2	4	3	2	1	0	2	4	3	2	1	0	2	4	3	2	1	0	2	4	3	2	1
$\times$													0	4	16	9	4	1						

$\sum \rightarrow 34 \xrightarrow{\times \frac{1}{6}} 5.67$

$x[n]$	0	2	4	3	2	1	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	0	2	4	3	2
$\times$													0	0	8	12	6	2						

$\sum \rightarrow 28 \xrightarrow{\times \frac{1}{6}} 4.67$



Back to m-Sequences

$c[n]$: 0010111001011100101110010111001011100101110010111001011100101110010111

0010111

$\oplus$

1001011

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

0	$\oplus$	0	=	0
0	$\oplus$	1	=	1
1	$\oplus$	0	=	1
1	$\oplus$	1	=	0

−1	?	−1	=	−1
−1	?	1	=	1
1	?	−1	=	1
1	?	1	=	−1

~~0 → −1~~
~~1 → 1~~

1	?	1	=	1
1	?	−1	=	−1
−1	?	1	=	−1
−1	?	−1	=	1

0 → 1
1 → −1

→ Easy to see that "?" is "multiplication"

Back to m-Sequences

From the previous slide, the mapping that we will use is $\begin{cases} 0 \to 1 \\ 1 \to -1 \\ \oplus \to \times \end{cases}$

$c[n]$: 00101110010111$\boxed{0010111}$0010111001011100101110010111

$$\begin{array}{c} 0010111 \\ \downarrow \\ \oplus \\ \downarrow \\ 1001011 \end{array}$$

property #2 + property #3

"one more 1s than 0s"

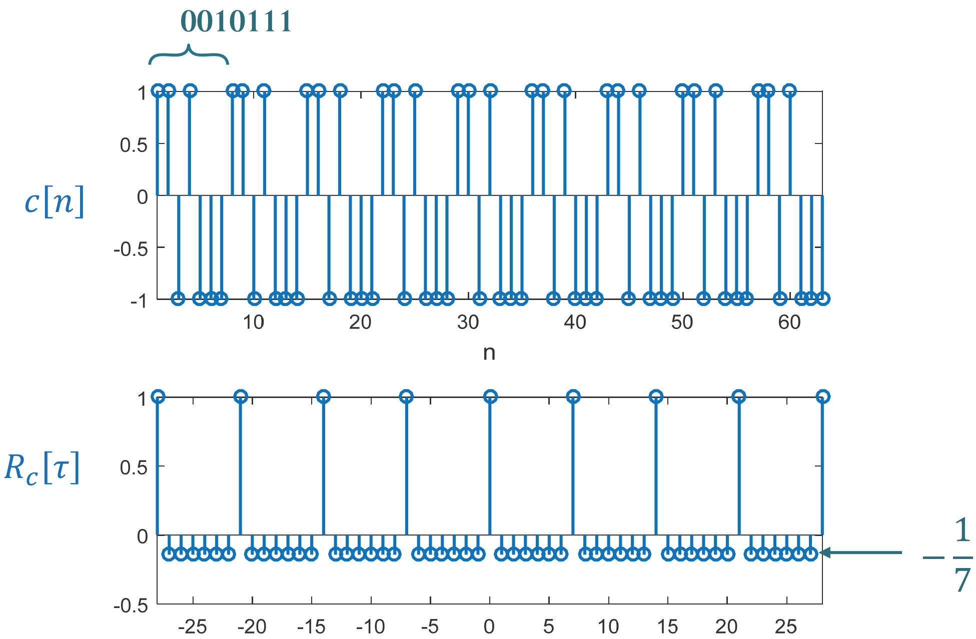
In actual transmission, we will map "0 and 1" to "+1 and -1", respectively.

Autocorrelation when not aligned:

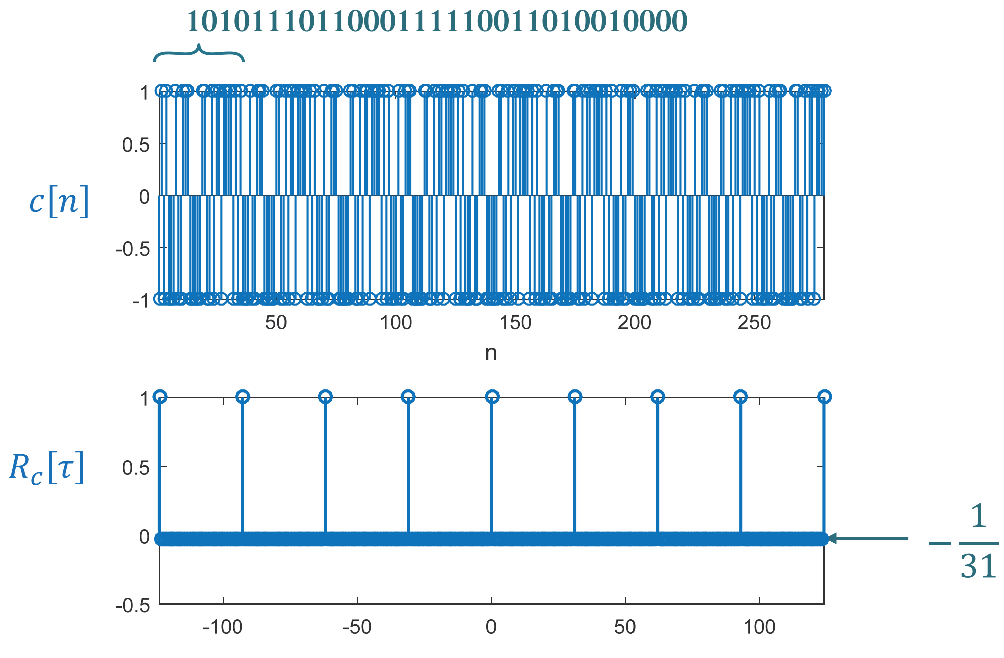
$$\begin{array}{rrrrrrrl} -1 & 1 & -1 & -1 & -1 & 1 & 1 & \times \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & \\ \hline -1 & 1 & 1 & -1 & 1 & -1 & -1 & \longrightarrow \sum = -1 \xrightarrow[\times \frac{1}{7}]{} -\frac{1}{7} \end{array}$$

"one more "-1"s than 1s"

m-Sequences: Autocorrelation function



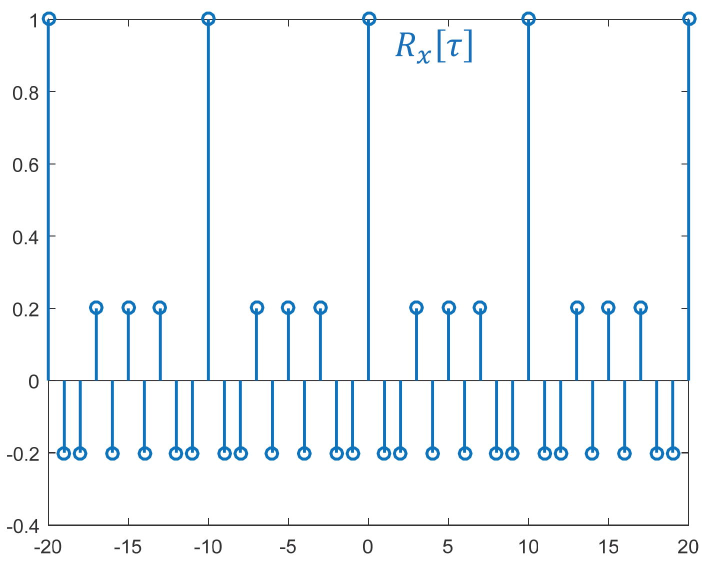
m-Sequences: Autocorrelation function



Autocorrelation Function for Periodic Binary Random Sequence

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

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

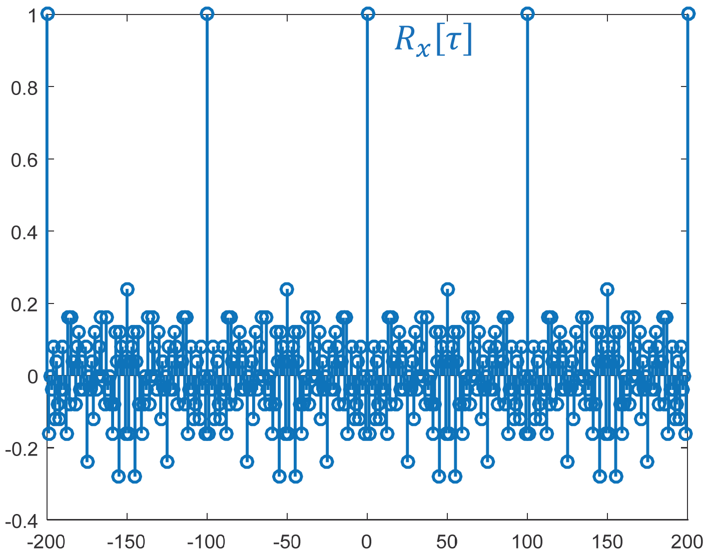
$$\xrightarrow[\text{LLN}]{n\to\infty} \mathbb{E}\left[x[n]x[n-\tau]\right]$$

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

Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by

```
1-2*randi([0 1],1,100)
```



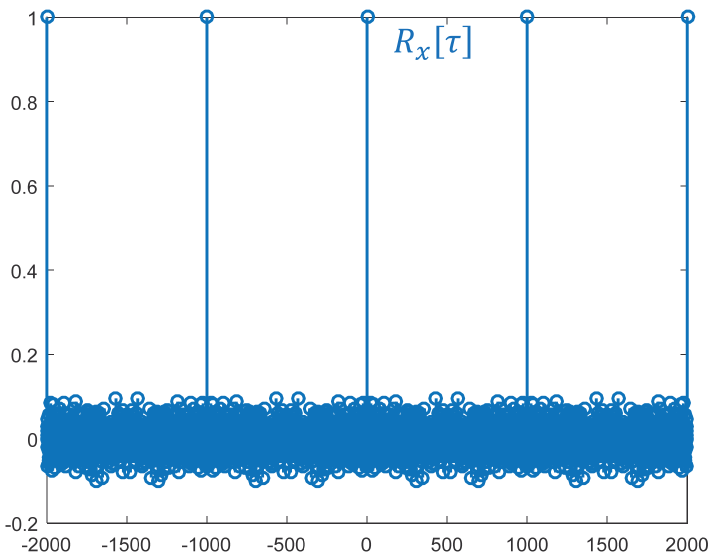
The shift property of binary random sequence implies that

$$R_x[\tau]=\langle x[n]x[n-\tau]\rangle \xrightarrow[\text{LLN}]{n\to\infty} \mathbb{E}\left[x[n]x[n-\tau]\right] =1\times\frac{1}{2}+(-1)\times\frac{1}{2}=0$$

Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by

```
1-2*randi([0 1],1,1000)
```



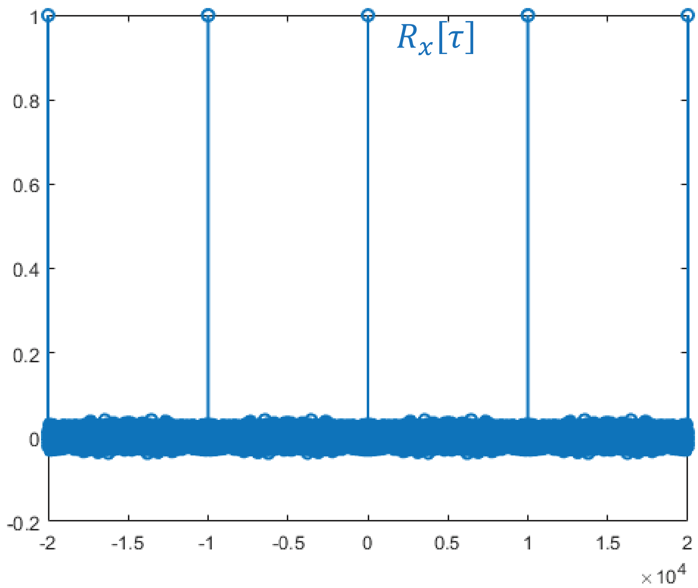
The shift property of binary random sequence implies that

$$R_x[\tau]=\langle x[n]x[n-\tau]\rangle \xrightarrow[\text{LLN}]{n\to\infty} \mathbb{E}\left[x[n]x[n-\tau]\right] =1\times\frac{1}{2}+(-1)\times\frac{1}{2}=0$$

Example: Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by

```
1-2*randi([0 1],1,10000)
```



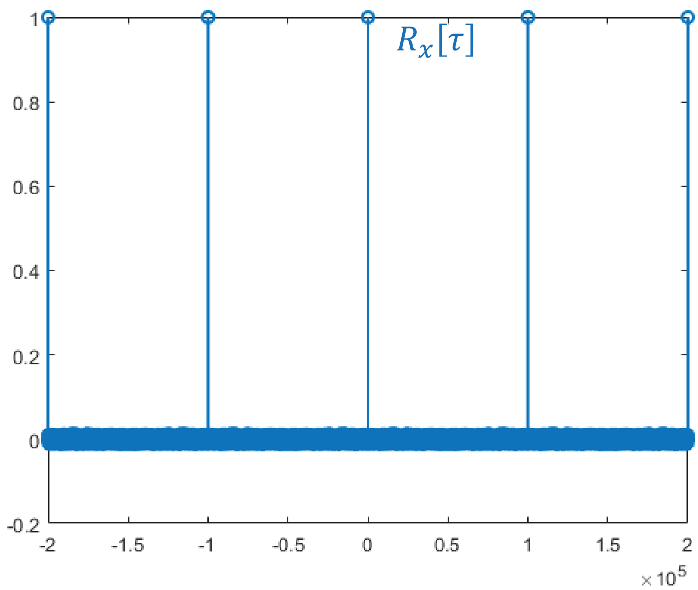
The shift property of binary random sequence implies that

$$R_x[\tau] = \langle x[n]x[n-\tau] \rangle \xrightarrow[\text{LLN}]{n\to\infty} \mathbb{E}\left[x[n]x[n-\tau]\right] = 1\times\frac{1}{2} + (-1)\times\frac{1}{2} = 0$$

Autocorrelation Function for Periodic Binary Random Sequence

Consider a periodic sequence whose one period is given by

```
1-2*randi([0 1],1,100000)
```

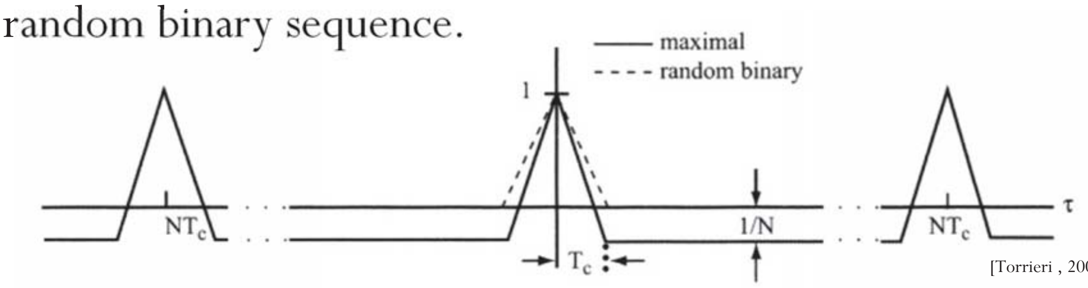


The shift property of binary random sequence implies that

$$R_x[\tau] = \langle x[n]x[n-\tau] \rangle \xrightarrow[\text{LLN}]{n\to\infty} \mathbb{E}\left[x[n]x[n-\tau]\right] = 1\times\frac{1}{2} + (-1)\times\frac{1}{2} = 0$$

Autocorrelation and PSD

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



[Torrieri , 2005, Fig 2.9]

- Power spectral density of maximal sequence.

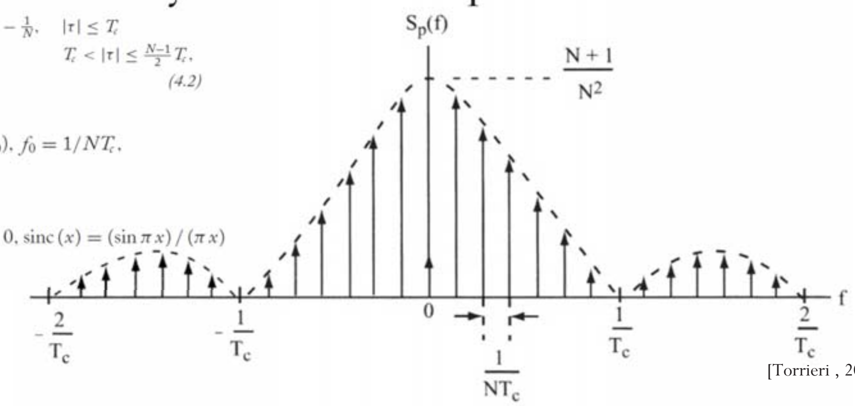
$$R_c(\tau) = \frac{1}{T_0}\int_{T_0} x(t)x(t+\tau)\,dt = \begin{cases} \left(1-\frac{|\tau|}{T_c}\right)\left(1+\frac{1}{N}\right)-\frac{1}{N}, & |\tau| \le T_c \\ -\frac{1}{N}, & T_c < |\tau| \le \frac{N-1}{2}T_c. \end{cases} \quad (4.2)$$

where the integration is over any period, $T_0 = NT_c$.

$$S_c(f) = \sum_{m=-\infty}^{\infty} P_m \delta(f - mf_0),\ f_0 = 1/NT_c.$$

where

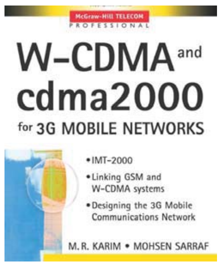
$$P_m = \begin{cases} \left[(N+1)/N^2\right] \operatorname{sinc}^2(m/N),\ m \neq 0,\ \operatorname{sinc}(x) = (\sin \pi x)/(\pi x) \\ 1/N^2,\ m = 0. \end{cases}$$



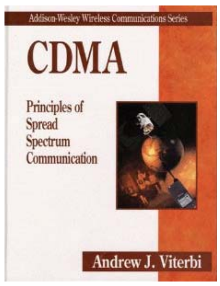
[Torrieri , 2005, Fig 2.10]

References: m-sequences

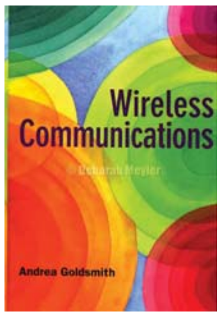
- Karim and Sarraf, ***W-CDMA and cdma2000 for 3G Mobile Networks***, 2002.
    - Page 84-90
- Viterbi, ***CDMA: Principles of Spread Spectrum Communication***, 1995
    - Chapter 1 and 2
- Goldsmith, ***Wireless Communications***, 2005
    - Chapter 13
- Tse and Viswanath, ***Fundamentals of Wireless Communication***, 2005
    - Section 3.4.3



[TK5103.452 K37 2002]



[TK5103.45 V57 1995]



Review: m-sequence

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

Spectral spreading waveform

Spreading code/sequence	**1 1 -1 1 -1 -1 -1 1 1 -1 1 -1**
$c[n]$	**0 0 1 0 1 1 1 0 0 1 0 1**

Imitate properties of Bernoulli trials

Pseudo-random

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.