ECS455: Chapter 4

Multiple Access

4.5 m-sequence

Dr.Prapun Suksompong
prapun.com/ecs455

Office Hours:
BKD 3601-7

Tuesday	**9:30-10:30**
Tuesday	**13:30-14:30**
Thursday	**13:30-14:30**

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.

Binary Random Sequence

	X_{-4}	X_{-3}	X_{-2}	X_{-1}	X_{-0}	X_1	X_2	X_3	X_4
Coin-flipping sequence	H	H	T	H	H	T	H	T	T
Bernoulli trials/sequence	1	1	0	1	1	0	1	0	0
Binary (indp.) random sequence	-1	-1	1	-1	-1	1	-1	1	1

- 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 sequence is expressed in a particular version.

Properties of Binary Random Sequences

Note: A run is a subsequence of identical symbols within the sequence.

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 (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.

[Goldsmith, 2005, p. 387 & Viterbi, p. 12]

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
- Quaternary sequences
- Walsh functions

m-Sequences

Longer name: Maximal length linear shift register sequence.

- **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]

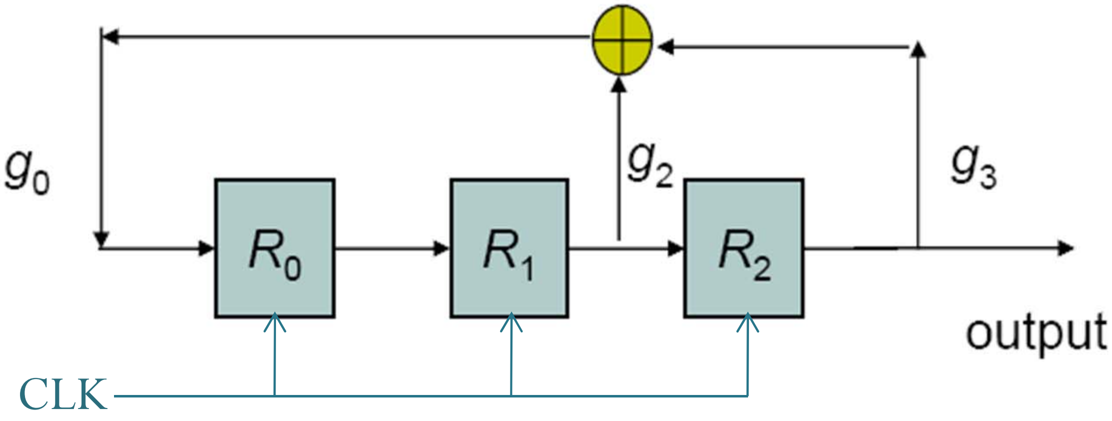
- Simple to generate with **linear feedback shift-register** (**LFSR**) circuits
  - Automated
- Approximate a random binary sequence.
- Disadvantage: Relatively easy to intercept and regenerate by an unintended receiver

[Ziemer, 2007, p 11]

(See Section 13.4.1 in [Lathi, 1998])

m-sequence generator (1)

- Start with a "**primitive polynomial**"
- The feedback taps in the feedback shift register are selected to correspond to the coefficients of the primitive polynomial.



$g(x) = x^3 + x^2 + 1$ (Degree: r = 3 → use 3 flip-flops)

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

The g_i's are coefficients of a primitive polynomial.

1 signifies closed or a connection and
0 signifies open or no connection.

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

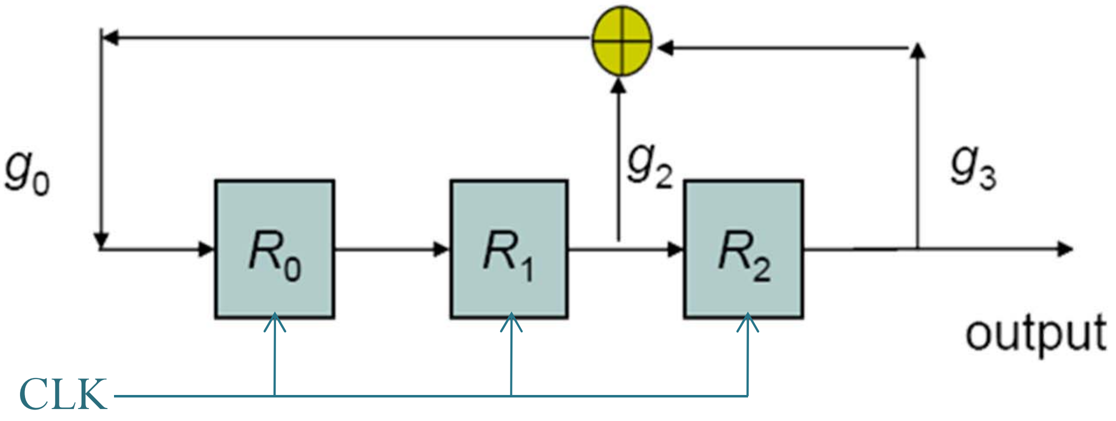
$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0$$

$$0 \cdot 0 = 0, \qquad 0 \cdot 1 = 0, \qquad 1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1$$

(See Section 13.4.1 in [Lathi, 1998])

m-sequence generator (2)

- 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**.



Time	R_0	R_1	R_2
0	1	0	0
1			
2			
3			
4			
5			
6			
7			

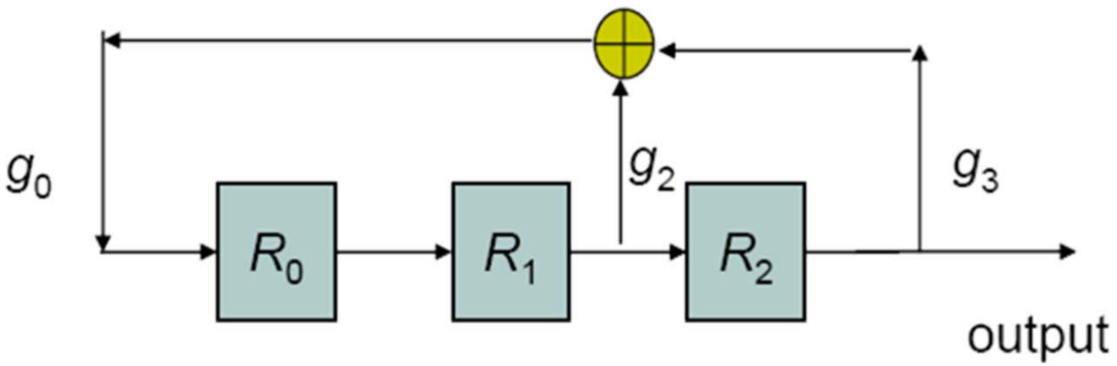
$$g(x) = x^3 + x^2 + 1 \qquad \text{(Degree: r = 3)}$$

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

The g_i's are coefficients of a primitive polynomial.

1 signifies closed or a connection and
0 signifies open or no connection.

State Diagram



Time	R_0	R_1	R_2
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

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**.

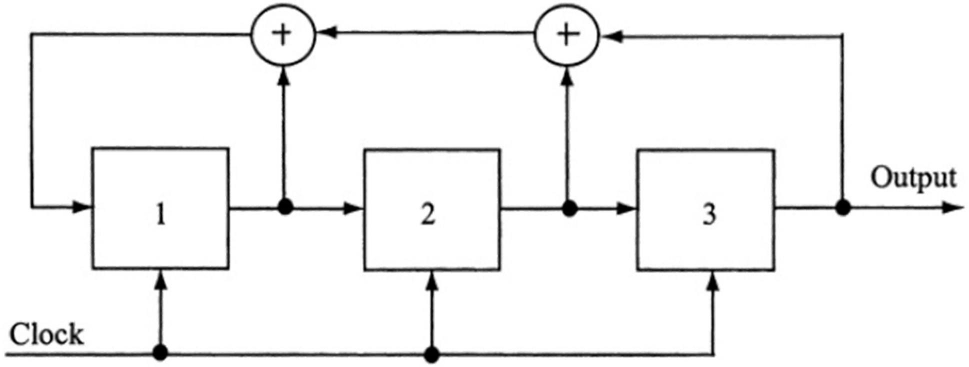
Sample Exam Question

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

1. $x^3 + x^2 + 1$
2. $x^3 + x^2 + x + 1$

Nonmaximal linear feedback shift register

$$x^3 + x^2 + x + 1$$



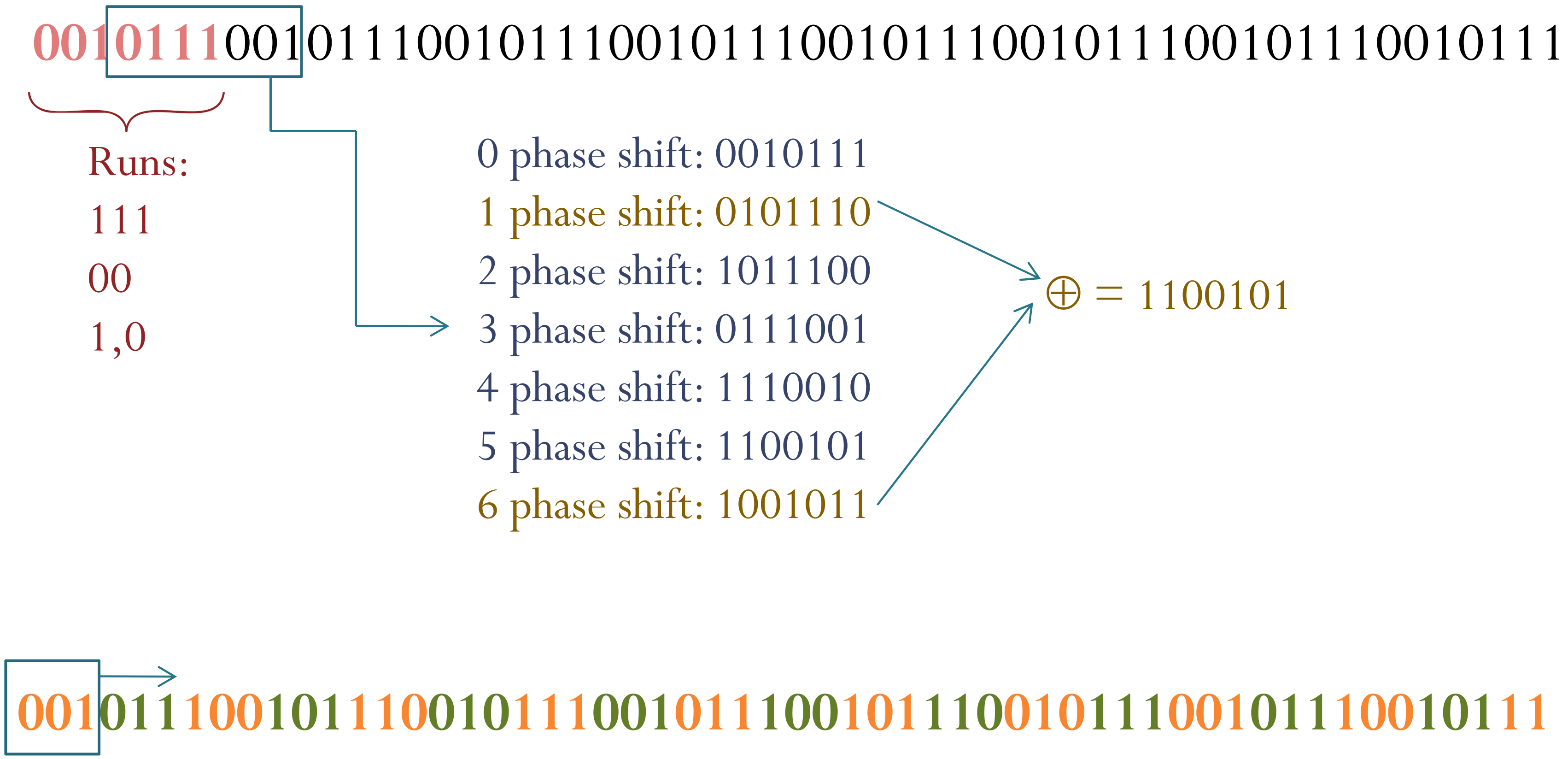
[Torrieri , 2005, Fig 2.8]

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

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

Ex: Properties of m-sequence



00101110010111001011100101110010111001011100101110010111

Runs:

111

00

1,0

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

00101110010111001011100101110010111001011100101110010111

Ex: Properties of m-sequence (con’t)

- 2^5-1 = 31-chip m-sequence

1010111011000111110011010010000

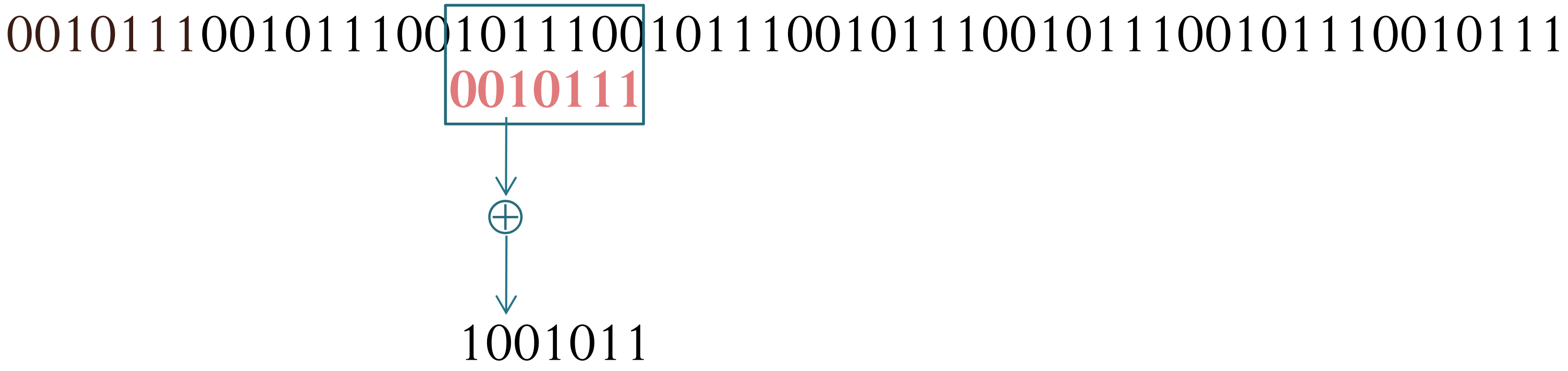
1010111011000111110011010010000

Runs:

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

There are 16 runs.

m-Sequences (con’t)



00101110010111001011100101110010111001011100101110010111

0010111

$\oplus$

1001011

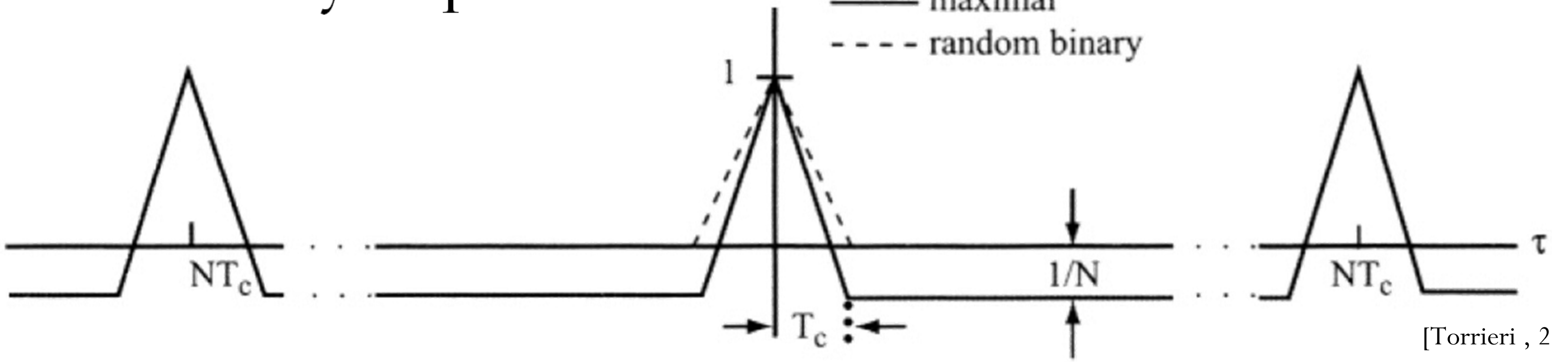
In actual transmission, we will map 0 and 1 to +1 and -1, respectively.

Autocorrelation:

$$\begin{array}{rrrrrrrl} -1 & 1 & -1 & -1 & -1 & 1 & 1 & \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & \times \\ \hline -1 & 1 & 1 & -1 & 1 & -1 & -1 & \qquad \sum = -1 \end{array}$$

Autocorrelation and PSD

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



[Torrieri , 2005, Fig 2.9]

- Power spectral density of maximal sequence.

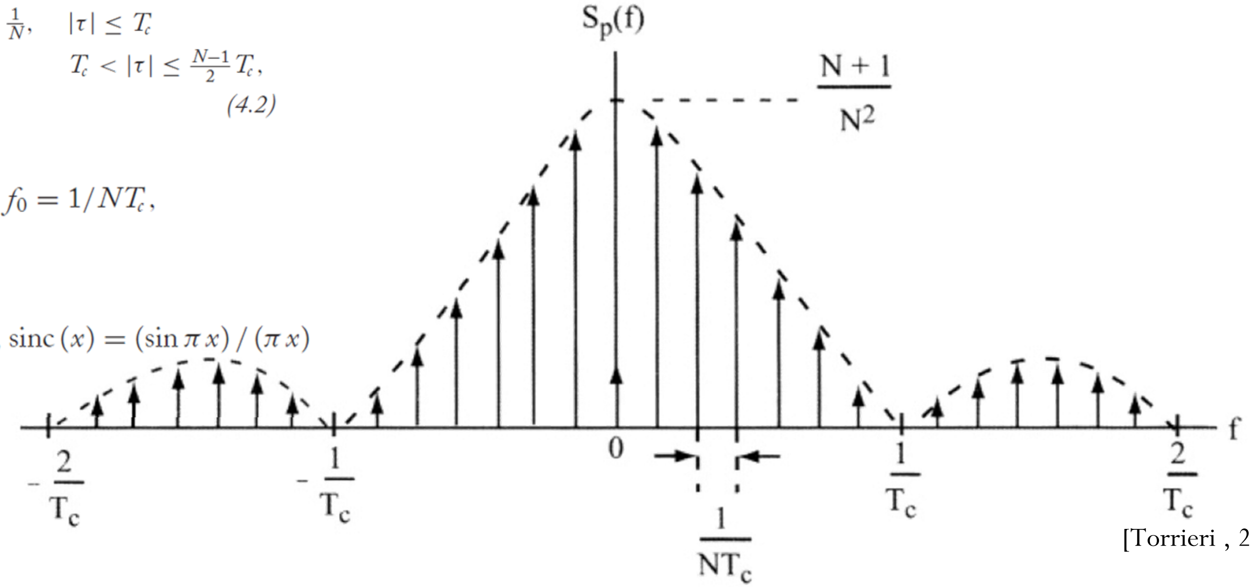
$$R_c(\tau) = \frac{1}{T_0}\int_{T_0} x(t)x(t+\tau)\,dt = \begin{cases} \left(1 - \frac{|\tau|}{T_c}\right)\left(1 + \frac{1}{N}\right) - \frac{1}{N}, & |\tau| \le T_c \\ -\frac{1}{N}, & T_c < |\tau| \le \frac{N-1}{2}T_c, \end{cases} \quad (4.2)$$

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

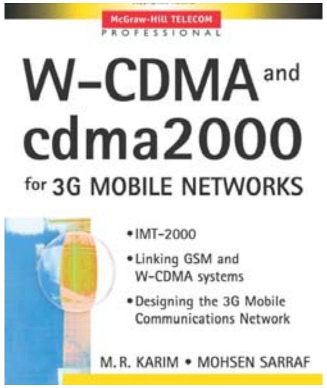
$$P_m = \begin{cases} \left[(N+1)/N^2\right] \mathrm{sinc}^2(m/N),\ m \ne 0,\ \mathrm{sinc}(x) = (\sin \pi x)/(\pi x) \\ 1/N^2,\ m = 0. \end{cases}$$



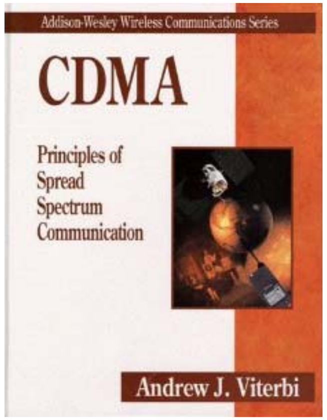
[Torrieri , 2005, Fig 2.10]

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


McGraw-Hill TELECOM PROFESSIONAL
W-CDMA and cdma2000 for 3G MOBILE NETWORKS
•IMT-2000
•Linking GSM and W-CDMA systems
•Designing the 3G Mobile Communications Network
M. R. KARIM • MOHSEN SARRAF

[TK5103.452 K37 2002]


Addison-Wesley Wireless Communications Series
CDMA
Principles of Spread Spectrum Communication
Andrew J. Viterbi

[TK5103.45 V57 1995]