ECS455: Chapter 4

Multiple Access

4.4 DS/SS

Dr.Prapun Suksompong
prapun.com/ecs455

Office Hours:
BKD 3601-7
Wednesday 15:30-16:30
Friday 9:30-10:30

Spread spectrum (SS)

- Historically spread spectrum was developed for *secure* communication and *military* uses.
- **Difficult to intercept** for an unauthorized person.
- Easily **hidden**. For an unauthorized person, it is difficult to even detect their presence in many cases.
- **Resistant to jamming**.
- Provide a measure of immunity to distortion due to multipath propagation.
  - In conjunction with a RAKE receiver, can provide coherent combining of different multipath components.
- Asynchronous multiple-access capability.
- Wide bandwidth of spread spectrum signals is useful for location and timing acquisition.

[Goldsmith, 2005, Ch 13]

Spread spectrum: Applications

- First achieve widespread use in **military** applications due to
  - its inherent property of *hiding the spread signal below the noise floor* during transmission,
  - its resistance to narrowband jamming and interference, and
  - its low probability of detection and interception.
- The narrowband interference resistance has made spread spectrum common in **cordless phones**.
- The basis for both 2nd and 3rd generation **cellular systems** as well as 2nd generation wireless LANs (**WLAN**).
  - The ISI rejection and bandwidth sharing capabilities of spread spectrum are very desirable in these systems

[Goldsmith, 2005, Ch 13]

Spread spectrum conditions

Spread spectrum refers to any system that satisfies the following conditions [Lathi, 1998, p 406 & Goldsmith, 2005, p. 378]:

1. The spread spectrum may be viewed as a kind of modulation scheme in which **the modulated (spread spectrum) signal bandwidth is much greater than the message (baseband) signal bandwidth.**
2. The **spectral spreading** is performed by a **code** that is **independent** of the message signal.
   - This same code is also used at the receiver to despread the received signal in order to recover the message signal (from the spread spectrum signal).
   - In secure communication, this code is known only to the person(s) for whom the message is intended.

[R. Pickholtz, D. Schilling, L. Milstein, "Theory of Spread-Spectrum Communications - A Tutorial," IEEE Trans. Commun., Vol. 30 , pp. 855-884, May 1982.]

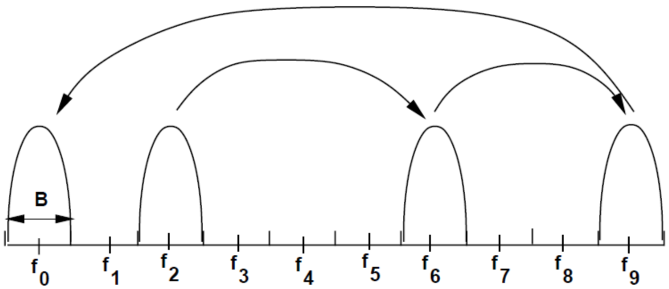
Spread spectrum (2)

- Increase the bandwidth of the message signal by a factor ***N***, called the **processing gain** (or bandwidth spreading factor).
  - In practice, *N* is on the order of **100-1000**. [Goldsmith, 2005, p 379]
    - N = 128 for IS-95 [T&V]
  - Wasteful?
- Although we use much higher BW for a spread spectrum signal,
  - **Multiplexing**: we can also multiplex large numbers of such signals over the same band.
  - **Multiple Access**: many users can share the same spread spectrum bandwidth without interfering with one another.
    - Achieved by assigning different code to each user.
    - Frequency bands can be reused without regard to the separation distance of the users.

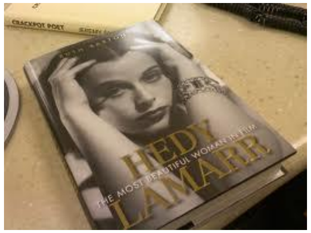
Spread Spectrum (3)

Two forms of spread spectrum (SS)

1. **Frequency Hopping** (FH)
   - Hop the modulated data signal over a wide BW by changing its carrier frequency
   - BW is approximately equal to *NB*
     - *N* is the number of carrier frequencies available for hopping
     - *B* is the bandwidth of the data signal.



   - The most celebrated invention of frequency hopping was that of actress Hedy Lamarr and composer George Antheil in 1942



2. **Direct Sequence** (DS)

UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

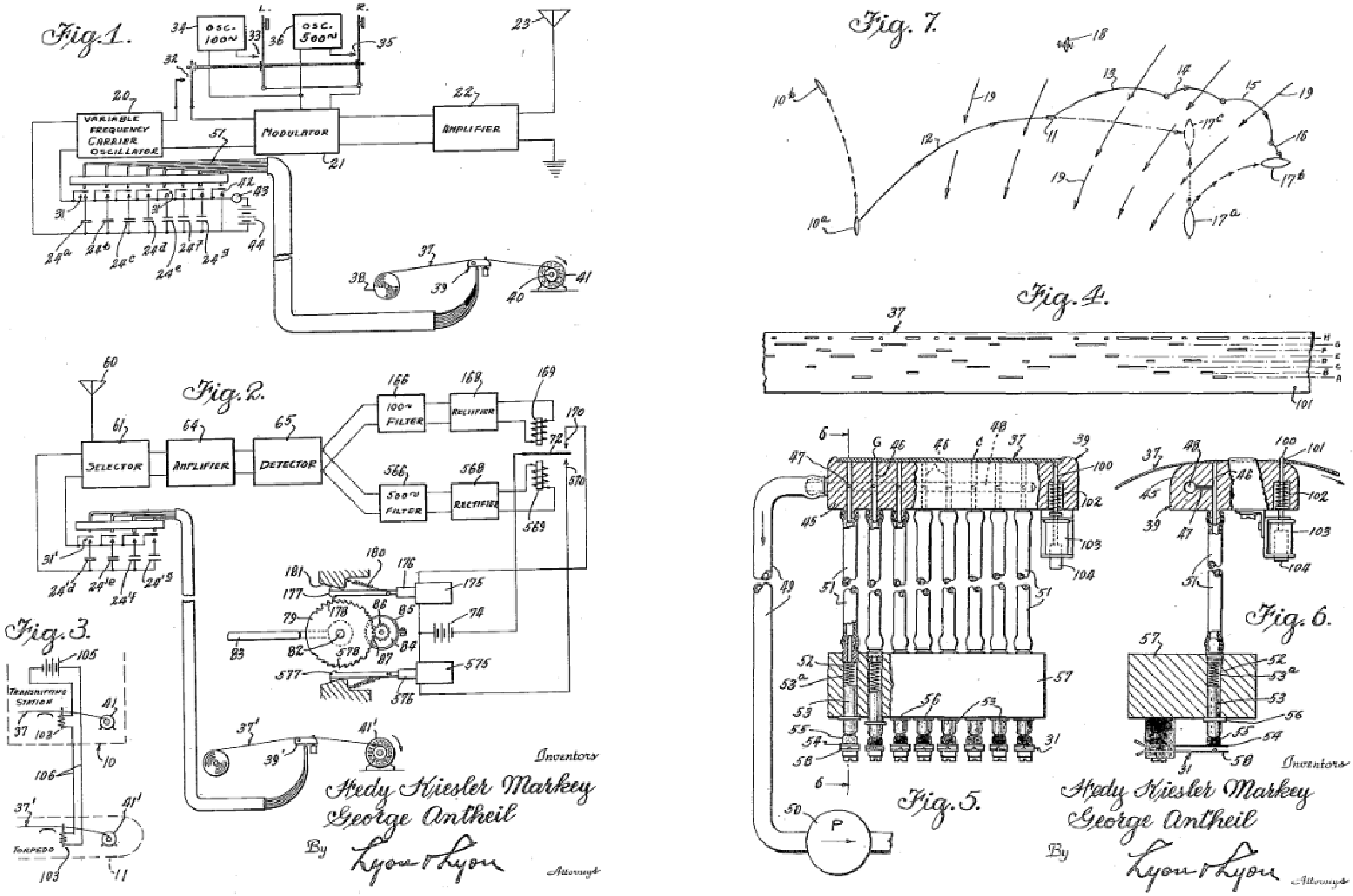
Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

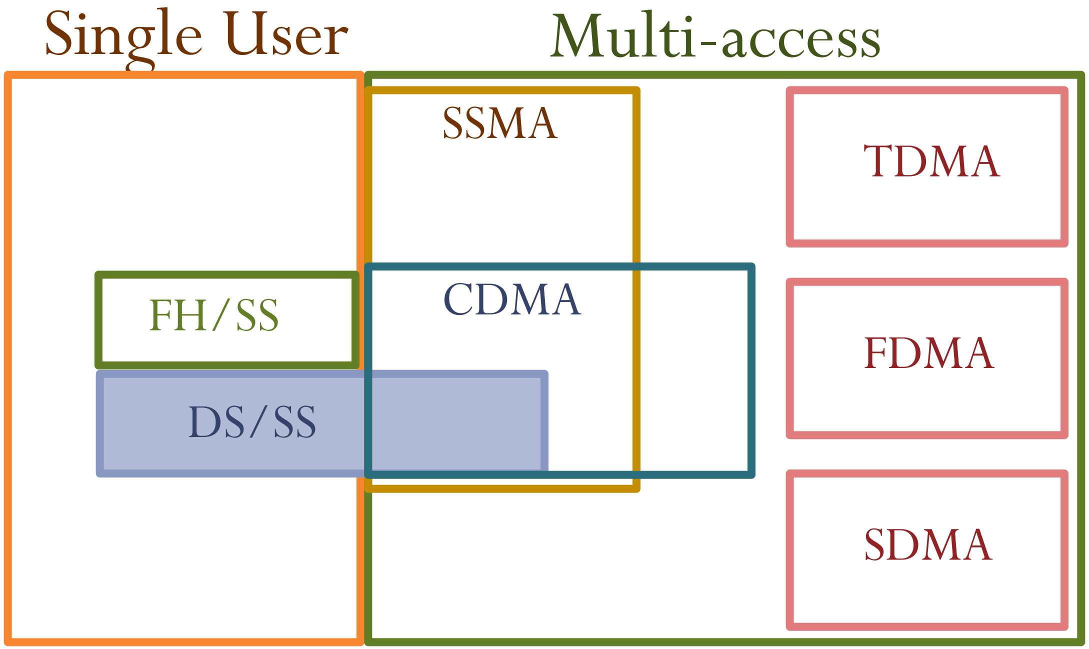
Aug. 11, 1942. H. K. MARKE ET AL 2,292,387

SECRET COMMUNICA N SYSTEM

Filed June 1 1941 2 Sheets-Sheet 2

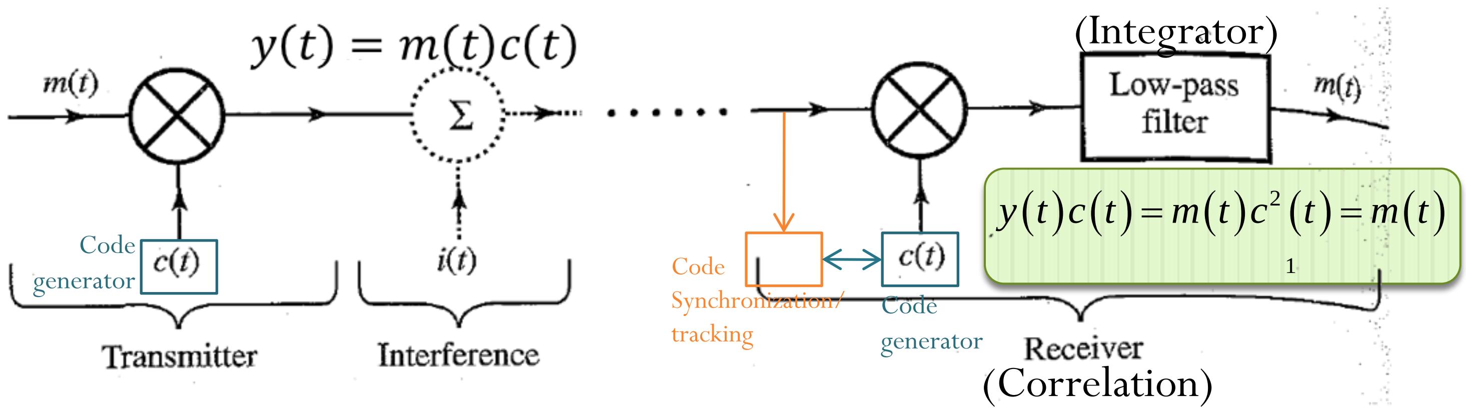


SSMA, CDMA, DS/SS

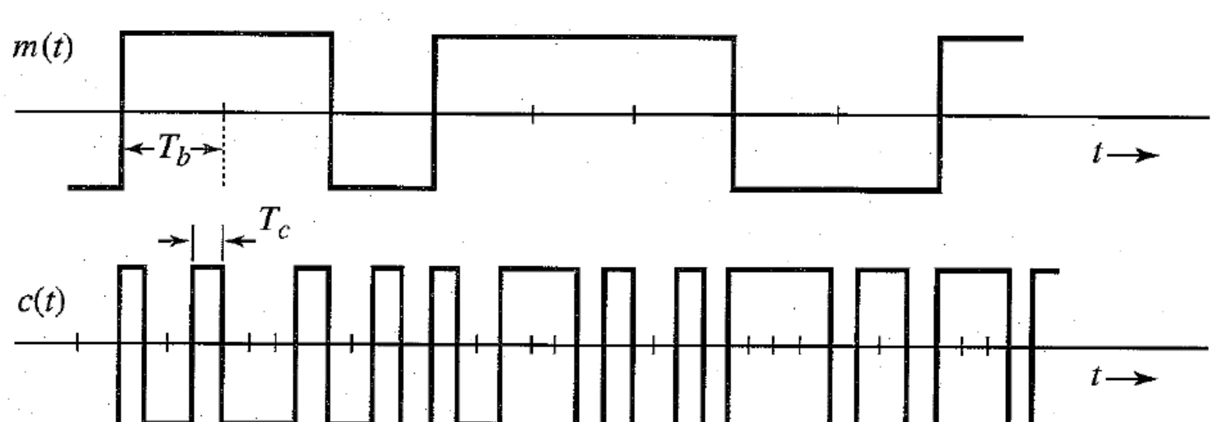


Useful even for single user!

DS/SS System

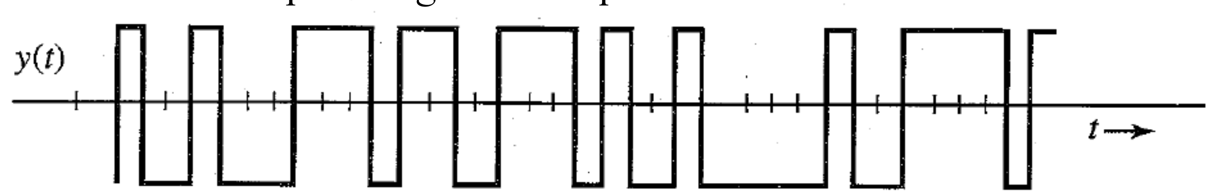


Message signal
(data/information signal)



Pseudonoise (PN) sequence. (Think of this as a pseudorandom carrier).

Here, we refer to it as spreading code/sequence.



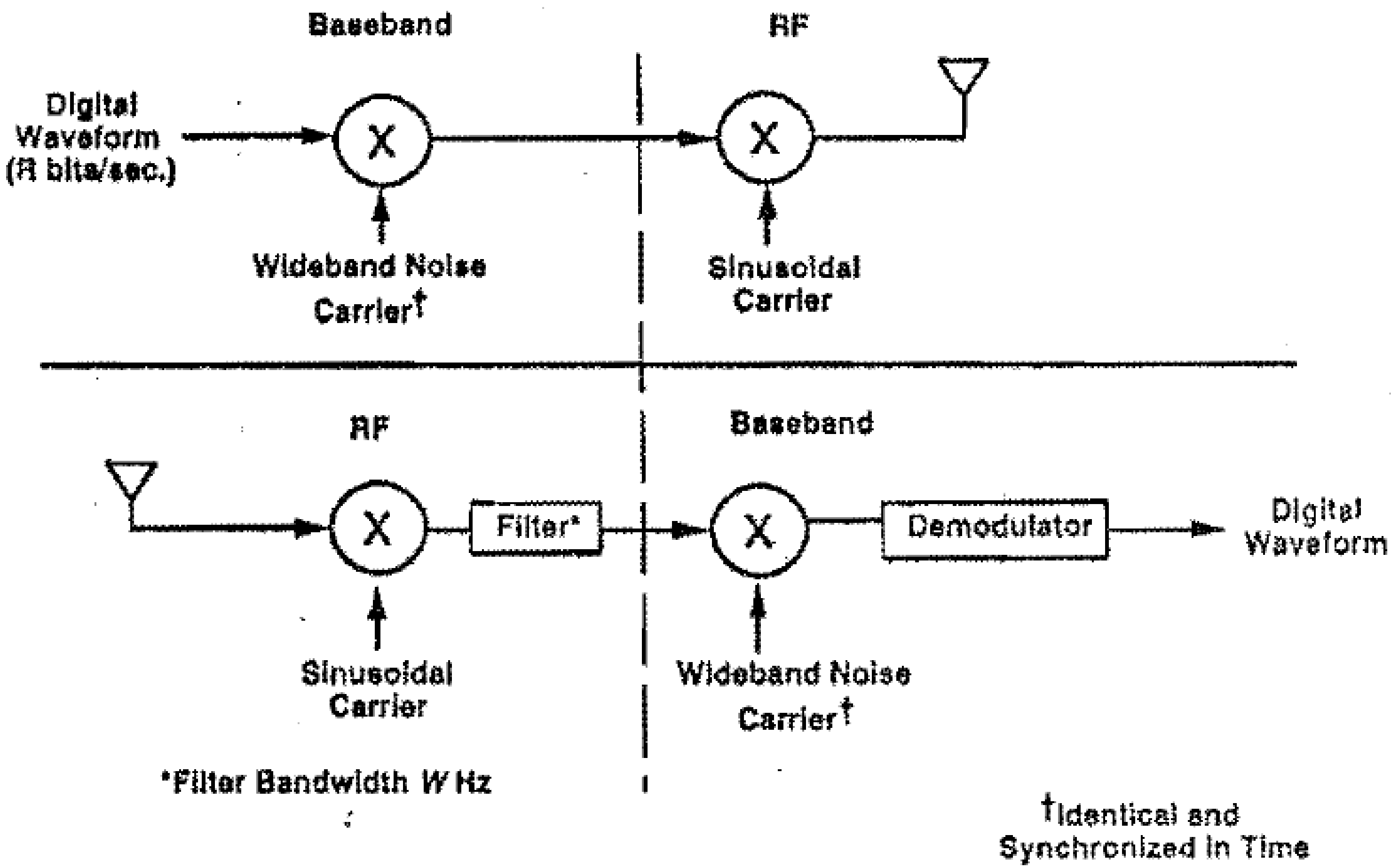
$$N = \frac{T_b}{T_c}$$

DS/SS System (Con't)

Observe that…

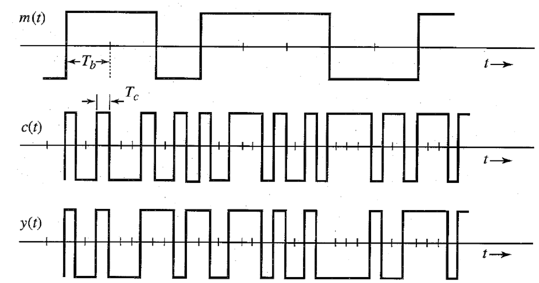
- To be able to perform the despreading operation, the receiver must
  - **know** the **code** sequence $c(t)$ used at the Tx to spread the signal
  - **synchronize** the codes of the received signal and the locally generated code.
- The process of detection (despreading) is **identical** to the process of spectral spreading.
  - Recall that for DSB-SC, we have a similar situation in that the modulation and demodulation processes are identical (except for the output filter).

Spread spectrum modem



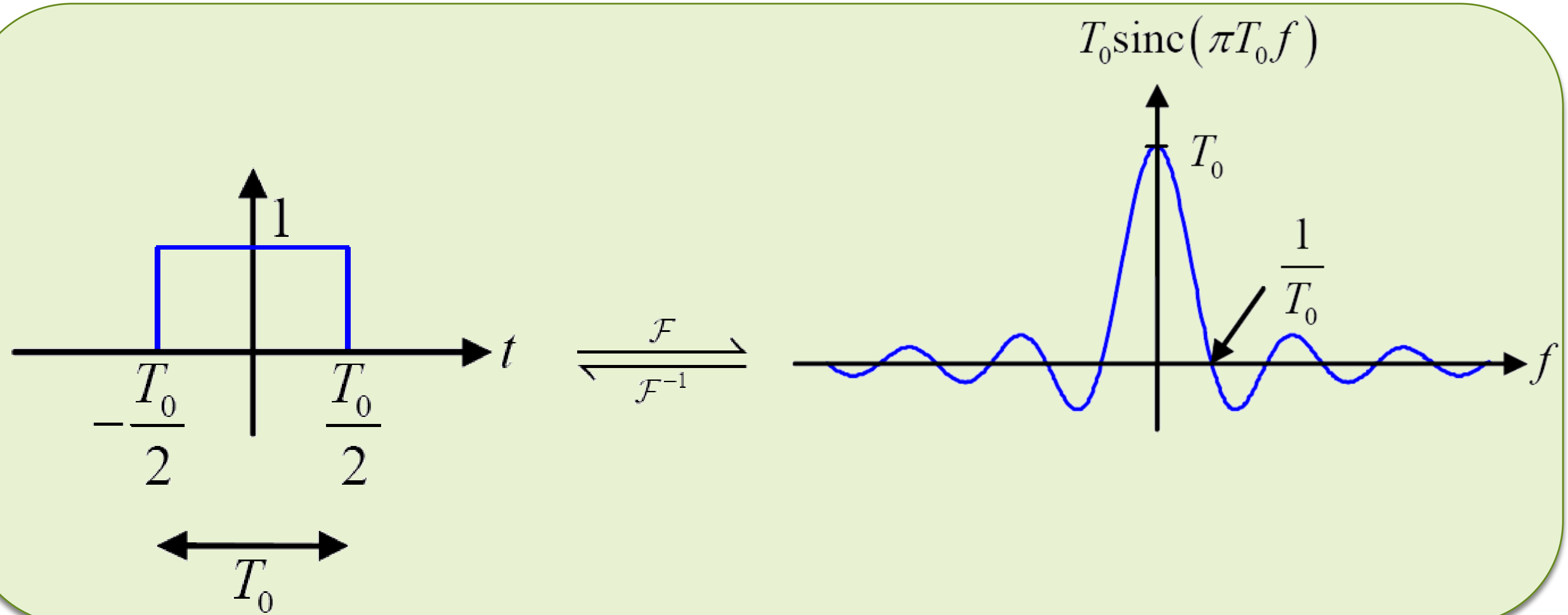
[Viterbi, 1995, Fig. 1.2]

DS/SS: Spectral Spreading Signal $c(t)$



- A **pseudorandom** signal
  - **Appear** to be **unpredictable**
  - Can be generated by **deterministic** means (hence, pseudorandom)
- The bit rate is chosen to be much higher then the bit rate of $m(t)$.
- The basic pulse in $c(t)$ is called the **chip**.
- The bit rate of $c(t)$ is known as the **chip rate**.
- The autocorrelation function of $c(t)$ should be very narrow.
  - Small similarity with its delayed version
- Remark: In multiuser (CDMA) setting, the cross-correlation between any two codes $c_1(t)$ and $c_2(t)$ should also be very small
  - Negligible interference between various multiplexed signals.

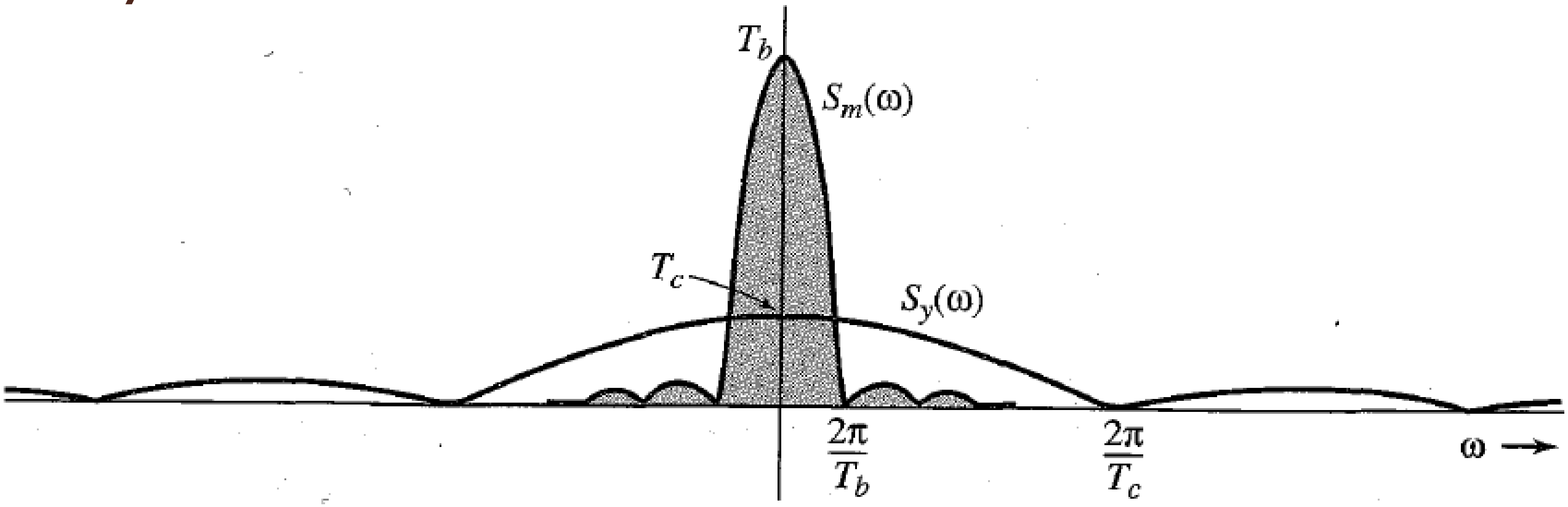
Frequency-Domain Analysis



Shifting Properties: $g(t-t_0) \overset{\mathcal{F}}{\rightleftharpoons} e^{-j2\pi f t_0} G(f)$ $\quad e^{j2\pi f_0 t} g(t) \overset{\mathcal{F}}{\rightleftharpoons} G(f-f_0)$

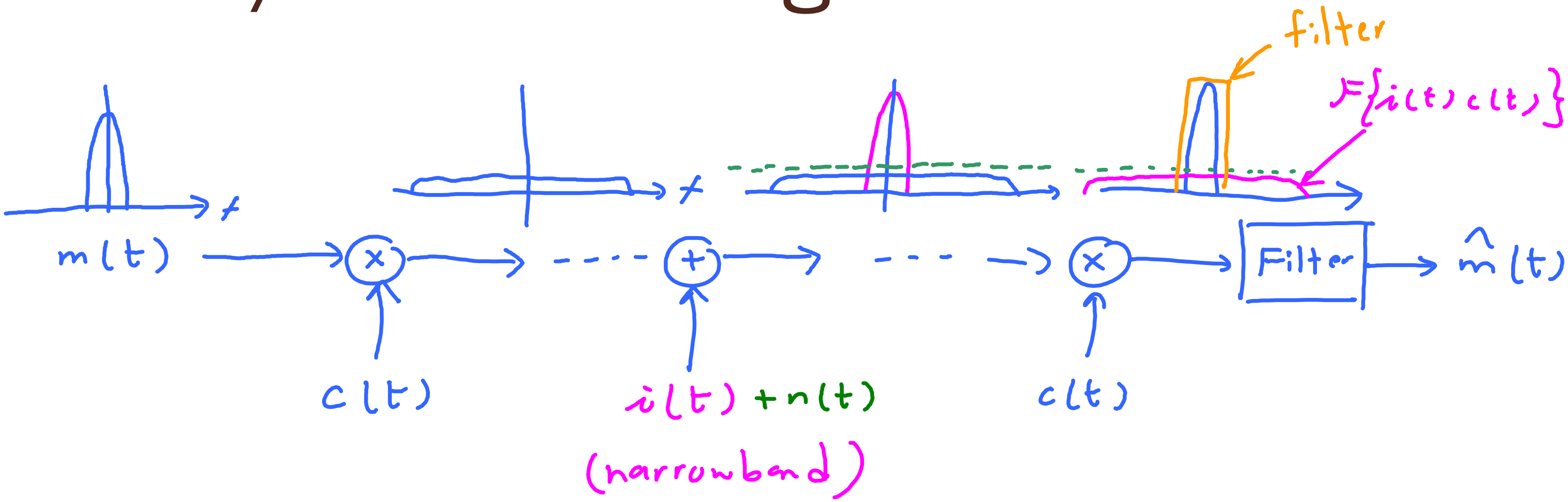
Modulation: $m(t)\cos(2\pi f_c t) \overset{\mathcal{F}}{\rightleftharpoons} \frac{1}{2}M(f-f_c)+\frac{1}{2}M(f+f_c)$

DS/SS: Secure Communication



- Secure communication
  - Signal can be detected only by **authorized** person(s) who **know** the pseudorandom code used at the transmitter.
  - Signal spectrum is spread over a very wide band, the signal **PSD is very small**, which makes it easier to hide the signal within the noise floor

DS/SS: Jamming Resistance



$$\left(y(t)+i(t)\right)c(t)=m(t)c^2(t)+i(t)c(t)=m(t)+i(t)c(t)$$

- Jamming Resistance / Narrowband Interference rejection
  - The decoder despreads the signal $y(t)$ to yield $m(t)$.
  - The jamming signal $i(t)$ is spread to yield $i(t)c(t)$.
  - Using a LPF, can recover $m(t)$ with only a small fraction of the power from $i(t)$.
- Caution: Channel noise will not spread.

DS/SS: Multipath Fading Immunity

- The signal received from any undesired path is a delayed version of the DS/SS signal.
- DS/SS signal has a property of low autocorrelation (small similarity) with its delayed version, especially if the delay is of more than one chip duration.
- The delayed signal, looking more like an interfering signal, will not be despread by $c(t)$ effectively minimizes the effect of the multipath signals.
- What is more interesting is that DS/SS cannot only mitigate but may also exploit the multipath propagation effect.
  - This is accomplished by a **rake receiver**.
  - This receive designed as to coherently combine the energy from several multipath components, which increases the received signal power and thus provides a form of diversity reception.
  - The rake receiver consists of a bank of correlation receivers, with each individual receiver correlating with a different arriving multipath component.
  - By adjusting the delays, the individual multipath components can be made to add coherently rather than destructively.

ECS455: Chapter 4

Multiple Access

4.5 m-sequence

Dr.Prapun Suksompong
prapun.com/ecs455

Office Hours:
BKD 3601-7
Wednesday 15:30-16:30
Friday 9:30-10:30

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.

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

Key randomness properties

[Golomb, 1967] 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]

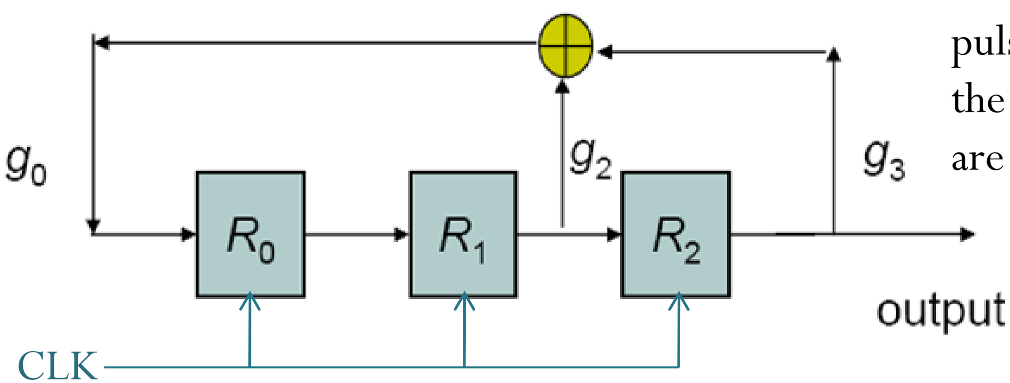
- Simple to generate with **linear feedback shift-register** (**LFSR**) circuits
  - Automated
- Approximate a random binary sequence.
- Disadvantage: Relatively easy to intercept and regenerate by an unintended receiver

[Ziemer, 2007, p 11]

m-sequence generator

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

Binary sequences drawn from the alphabet {0,1} are shifted through the shift register in response to clock pulses. 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	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

Sequence repeats from here onwards

$$g(x) = x^3 + x^2 + 1 = 1 + 0x + 1x^2 + 1x^3$$ (Degree: r = 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

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0$$
$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1$$

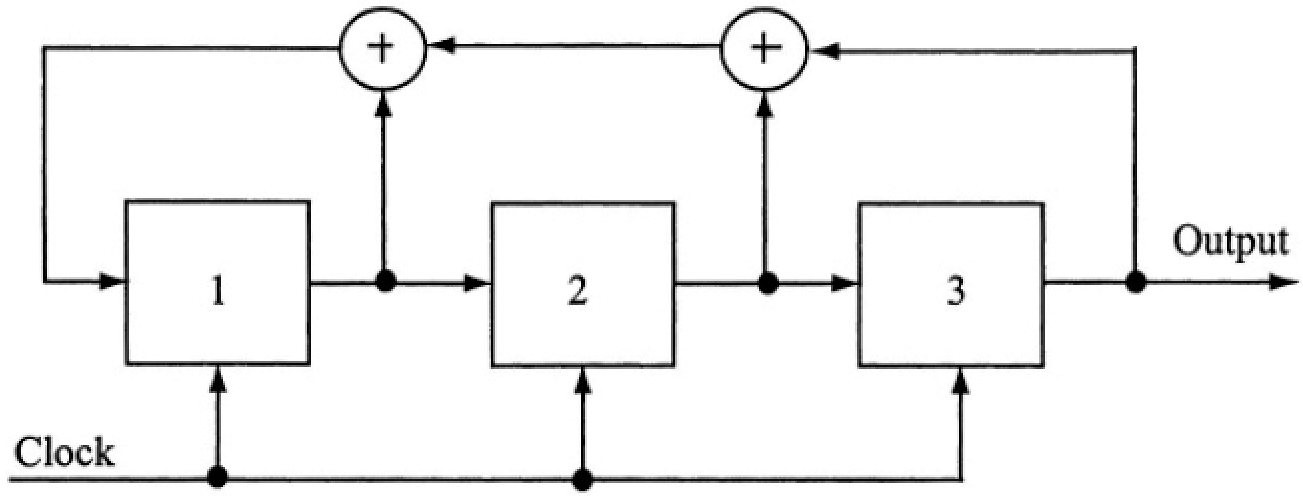
Sample Exam Question

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

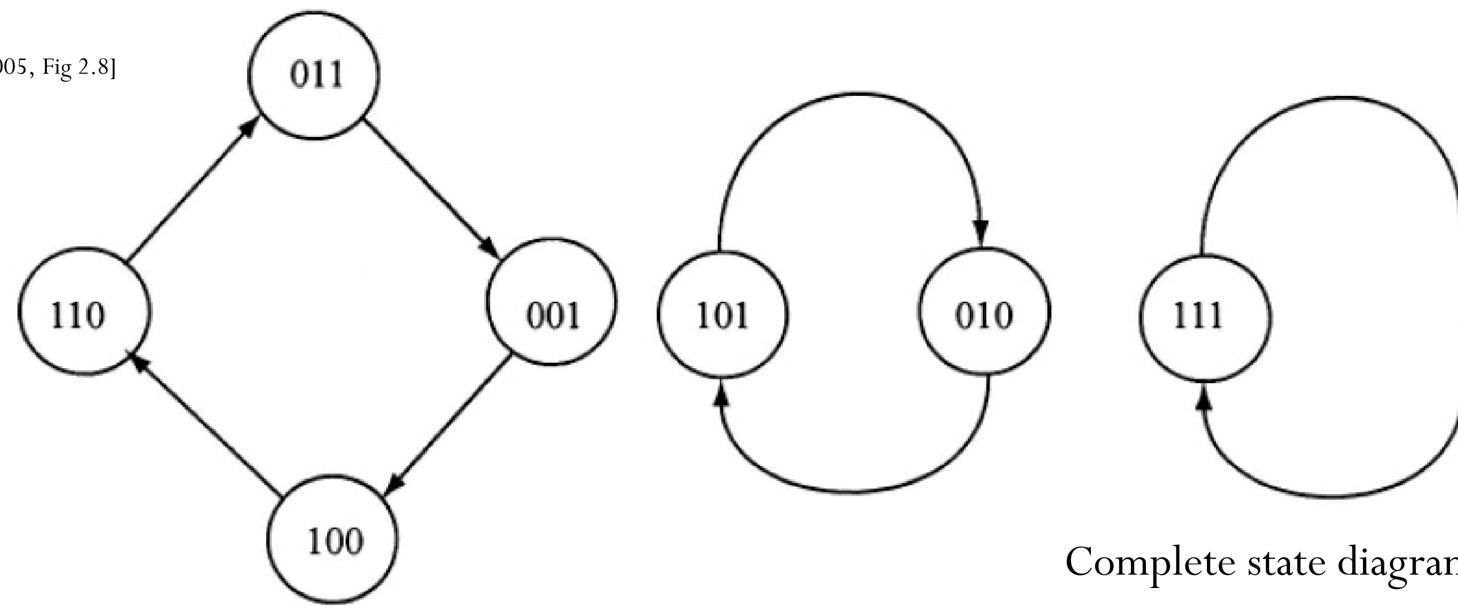
1. $x^3 + x^2 + 1$
2. $x^3 + x^2 + x + 1$

Nonmaximal linear feedback shift register

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



[Torrieri , 2005, Fig 2.8]



Complete state diagrams

Equivalent Statements

The three statements below are equivalent:

1. Polynomial $g(x)$ generates **m-sequence**
2. Polynomial $g(x)$ is a **primitive** polynomial.
3. The state diagram of the LFSR circuit generated by $g(x)$ visits all non-zero states in one cycle.

Implication:

We can use statement "3" to test whether a polynomial $g(x)$ is primitive.

For this class, we use "3" as the definition of being 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^{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

0010111001011100101110010111001011100101110010111001011100101110010111

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

0010111001011100101110010111001011100101110010111001011100101110010111

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

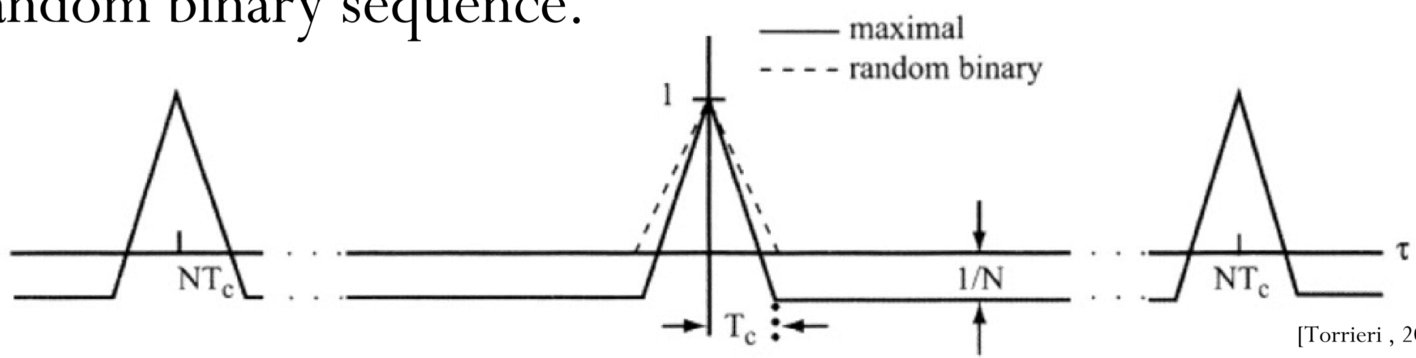
In actual transmission, we will map 0 and 1 to +1 and -1, respectively.

Autocorrelation:

-1	1	-1	-1	-1	1	1	
1	1	-1	1	-1	-1	-1	×
-1	1	1	-1	1	-1	-1	$\sum = -1$

Autocorrelation and PSD

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



[Torrieri , 2005, Fig 2.9]

- Power spectral density of maximal sequence.

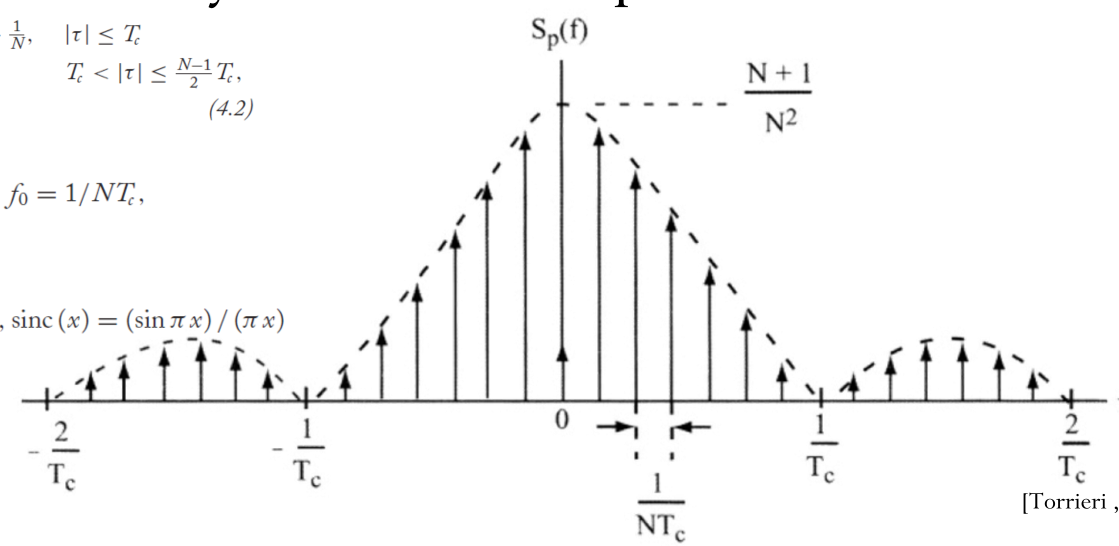
$$R_c(\tau) = \frac{1}{T_0}\int_{T_0} x(t)x(t+\tau)\,dt = \begin{cases} \left(1-\frac{|\tau|}{T_c}\right)\left(1+\frac{1}{N}\right)-\frac{1}{N}, & |\tau| \le T_c \\ -\frac{1}{N}, & T_c < |\tau| \le \frac{N-1}{2}T_c, \end{cases} \quad (4.2)$$

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

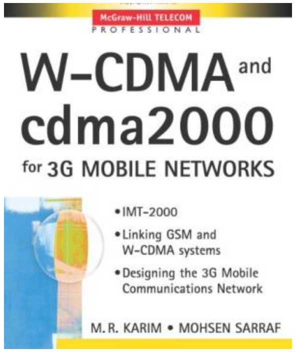
$$P_m = \begin{cases} \left[(N+1)/N^2\right]\operatorname{sinc}^2(m/N),\ m \ne 0,\ \operatorname{sinc}(x) = (\sin \pi x)/(\pi x) \\ 1/N^2,\ m = 0. \end{cases}$$



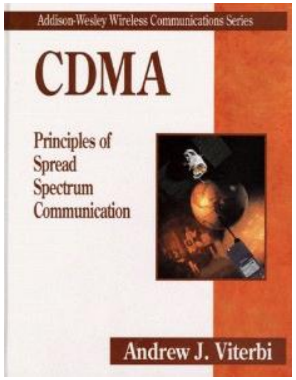
[Torrieri , 2005, Fig 2.10]

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]