CONTENTS

LEARNING OBJECTIVES

After studying this lecture, students should be able to:

1. Understand the **basic concept of Spread Spectrum communication**.
2. Define **Spread Spectrum and explain its operating principle**.
3. Identify the **main advantages of Spread Spectrum systems**, such as interference rejection, message privacy, and frequency diversity.
4. Recognize the **limitations and disadvantages** of Spread Spectrum communication systems.
5. Differentiate between the **main types of Spread Spectrum techniques**, including:
   - Direct Sequence Spread Spectrum (DSSS)
   - Frequency Hopping Spread Spectrum (FHSS)
6. Understand the **role of PN (Pseudo-Noise) codes** in spreading and despreading the signal.
7. Explain important **parameters of spreading codes** such as chip rate, chip duration, and processing gain.
8. Describe the **basic transmitter and receiver structures** used in DSSS and FHSS systems.

1 INTRODUCTION

Spread Spectrum is a communication technique in which the transmitted signal bandwidth is intentionally expanded to be much wider than the minimum bandwidth required for transmitting the information signal. This technique produces signals that resemble random noise, making them difficult to detect, intercept, or jam.

In Spread Spectrum systems, the energy of the transmitted signal is distributed over a wide frequency band rather than being concentrated in a narrow band. As a result, the power spectral density becomes very low, which improves resistance to interference and enhances communication security.

One of the major advantages of Spread Spectrum communication is its **Anti-Jamming (AJ)** capability and **Low Probability of Intercept (LPI)**. Because the signal appears similar to background noise, unauthorized receivers find it difficult to detect or demodulate the signal. For this reason, Spread Spectrum technology has been widely used in **military communication systems**, secure wireless networks, satellite communication, and modern digital communication systems.

In addition to security advantages, Spread Spectrum also provides improved performance in environments affected by interference, multipath propagation, and fading. These characteristics make it a valuable technique in both **military and commercial communication applications**

2 DEFINITION OF SPREAD SPECTRUM

Spread Spectrum is a communication technique that uses wideband, noise-like signals. Because these signals resemble noise, they are difficult to detect, intercept, or demodulate. In addition, Spread Spectrum signals are more resistant to jamming than narrowband signals. These properties give Spread Spectrum two important features:

- Low Probability of Intercept (LPI)
- Anti-Jamming (AJ)

Due to these advantages, Spread Spectrum has been widely used in military communication systems for many years. In Spread Spectrum systems, the transmitted signal is intentionally spread over a much wider bandwidth than the bandwidth of the information signal. This spreading makes the signal appear more noise-like.

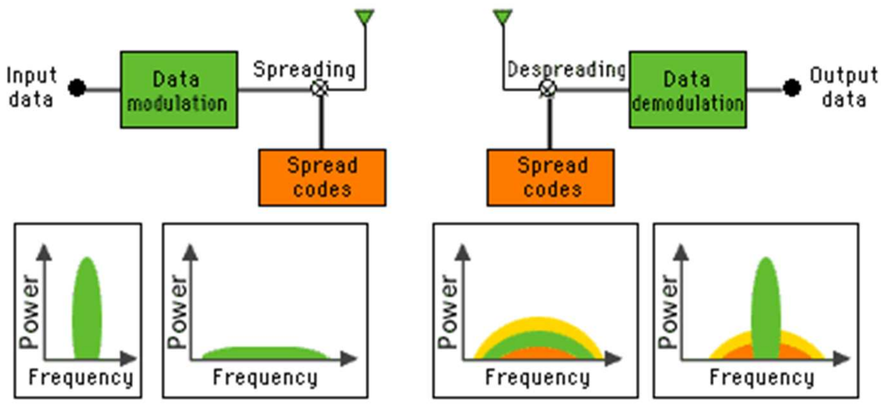

Figure 1: Spread Spectrum System.

3 REASONS FOR USING SPREAD SPECTRUM (ADVANTAGES)

There are several important reasons for spreading the information signal and then despreading it at the receiver using coherent correlation. These advantages make Spread Spectrum a valuable technique for both military and commercial applications.

3.1 INTERFERENCE REJECTION

Undesired signals such as jamming and interference are not synchronized with the receiver's code. As a result, when these unwanted signals enter the receiver, they undergo the despreading process improperly and become spread over a wide bandwidth. Most of their power is then rejected by the correlator's bandpass filter, which only passes the narrowband desired signal. This inherent interference rejection capability is one of the most powerful features of Spread Spectrum systems.

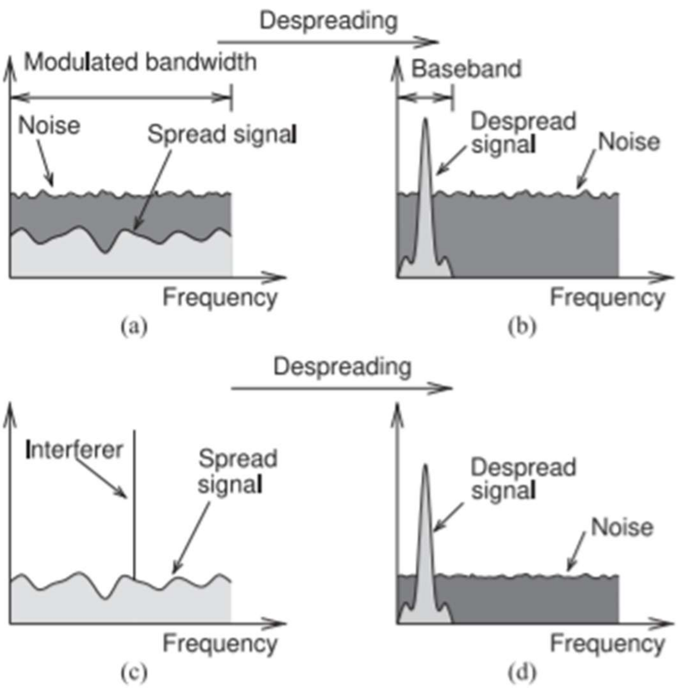

Figure 2: Interference Rejection.

3.2 LOW PROBABILITY OF INTERCEPT (LPI)

Because Spread Spectrum signals have very wide bandwidths, the transmitted power is distributed thinly across the entire frequency band. Consequently, the power spectral density (power per Hertz) is extremely low in any narrow frequency band. This makes the signal difficult to detect using conventional spectrum analyzers or intercept receivers. To an unintended observer, the signal appears indistinguishable from background noise.

3.3 SELECTIVE ADDRESSING

Spread Spectrum allows multiple users to transmit simultaneously over the same wide bandwidth. Each user is assigned a different code sequence with minimal cross-correlation. When a receiver uses a specific code to despread the incoming signal, only the message intended for that user is recovered. Messages from other users, which use different codes, remain spread and appear as low-level noise. This enables selective addressing without requiring separate frequency bands or time slots.

3.4 MESSAGE PRIVACY

Message privacy is inherent in Spread Spectrum systems because of coded transmission. Only authorized receivers possessing the correct code can properly despread and demodulate the signal. Without knowledge of the spreading code, an eavesdropper cannot recover the original information, even if the signal is successfully intercepted. This provides a fundamental layer of security without requiring additional encryption.

3.5 FREQUENCY DIVERSITY

Spread Spectrum systems inherently provide frequency diversity. Because the signal bandwidth spans a wide range of frequencies, it covers multiple fading regions. If some frequency components experience deep fade due to multipath propagation, other components at different frequencies may remain strong. This prevents complete signal loss and improves overall link reliability without requiring separate diversity schemes.

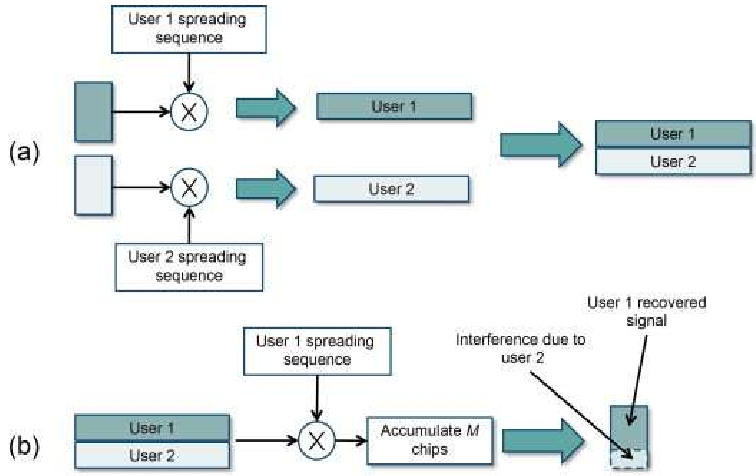

Figure 3: Multi-User System.

3.6 PROTECTION AGAINST MULTIPATH

Spread Spectrum systems are significantly less affected by multipath interference than conventional narrowband systems:

System Type	Multipath Protection Mechanism
Direct Sequence Systems	Delayed reflected signals that arrive after one code chip duration are treated as uncorrelated noise. Increasing the code chip rate (making chips shorter) reduces multipath interference because more reflections arrive after the correlation peak.
Frequency Hopping Systems	Multipath effects are reduced when the hopping rate is sufficiently high. By the time a reflected signal arrives, the receiver may have already hopped to a different frequency, so the delayed signal does not interfere with the current transmission.

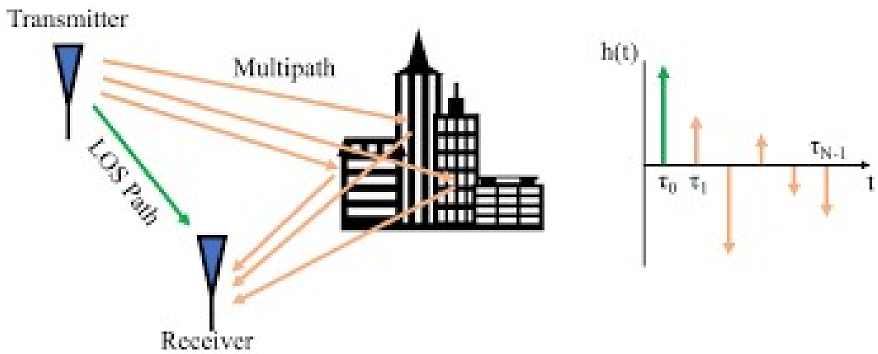

Figure 4: Multipath Interference.

4 DISADVANTAGES OF SPREAD SPECTRUM

Despite its numerous advantages, Spread Spectrum technology presents certain challenges and limitations that must be considered in system design.

4.1 MORE DIFFICULT FREQUENCY ALLOCATION

Spread Spectrum systems require significantly wider bandwidths than conventional narrowband systems. This makes frequency allocation and spectrum management more challenging, particularly in already crowded frequency bands. Coordinating wideband signals with existing narrowband users requires careful planning and regulatory approval.

4.2 GREATER SYSTEM COMPLEXITY

Spread Spectrum systems are inherently more complex than conventional communication systems. They require:

- Precision code generators
- High-speed digital processing
- Sophisticated synchronization circuits
- Wideband RF components
- More complex receiver architectures

This increased complexity translates to higher development costs, more expensive components, and greater power consumption.

4.3 CODE SYNCHRONIZATION PROBLEMS

Achieving and maintaining code synchronization between transmitter and receiver is one of the most challenging aspects of Spread Spectrum systems. The receiver must:

- **Acquire synchronization**: Initially align its locally generated code with the incoming signal
- **Track synchronization**: Continuously maintain alignment despite oscillator drift, Doppler shifts, and channel variations

Synchronization becomes increasingly difficult with longer codes, higher chip rates, and weaker signal conditions. Loss of synchronization can result in complete communication failure until reacquisition occurs.

5 TYPES OF SPREAD SPECTRUM

Spread spectrum systems are classified according to their modulation formats. The main types are:

5.1 DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

Direct Sequence Spread Spectrum (DSSS) is a spreading technique where the carrier is modulated by a digital code sequence (the **Spread Code**) whose bit rate is much higher than the information signal bandwidth. In this method, the data signal is directly multiplied by a "Pseudo-Noise" (PN) code, causing the resulting signal to "spread" across a wide frequency range.

5.1.1 THE SPECTRUM

The spectral shape of a DSSS signal is characterized by a **Sinc-squared (sinc2)** function.

- **Main Lobes:** The bandwidth of the main lobe is determined by the **Chip Rate** (Rc). Specifically, the null-to-null bandwidth is 2×Rc.
- **Power Density:** Because the total power is constant but spread over a wide bandwidth, the **Power Spectral Density (PSD)** is very low, often falling below the thermal noise floor. This provides the "protective envelope" mentioned in your notes, making the signal difficult to detect or jam.

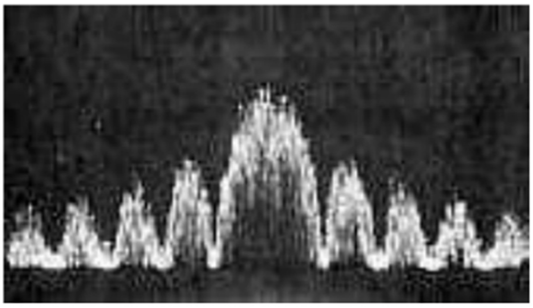

Figure 5: PSD of DSSS.

5.1.2 DSSS TRANSMITTER BLOCK DIAGRAM

The transmitter's job is to "spread" the narrowband data into a wideband signal before sending it through the air.

- **Binary Data Input (d(t)):** The original information at bit rate Rb.
- **PN Code Generator (c(t)):** A high-speed generator producing the "chips" at rate Rc.
- **Product Modulator (Multiplier/XOR):** This is the **Spreading Stage**. Each data bit is multiplied by the PN code.
- **BPSK Modulator:** The spread signal is modulated onto a carrier wave (typically using Binary Phase Shift Keying) for RF transmission.

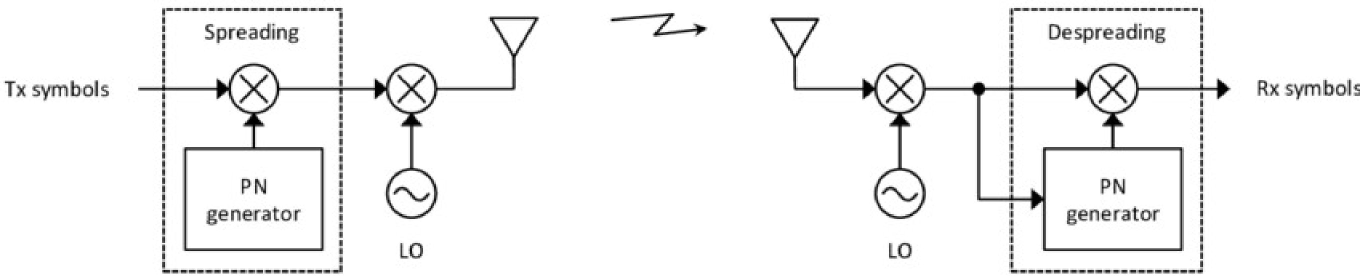

Figure 6: DSSS Block diagram.

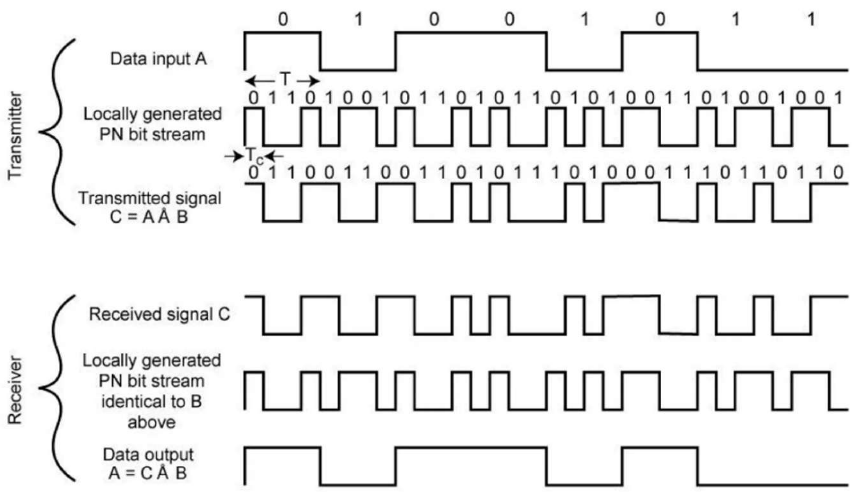

Figure 7: Example of DSSS Waveform.

5.1.3 DSSS RECEIVER BLOCK DIAGRAM

The receiver must perform the "Inverse" operation to recover the data while rejecting interference.

- **BPSK Demodulator:** Converts the incoming RF signal back to a wideband baseband signal.
- **Synchronized PN Generator:** The "Key." It produces an identical PN code that must be perfectly aligned in time with the transmitter's code.
- **Correlator (Multiplier + Integrator):**
  - **Despreading:** The multiplier combines the received signal with the local PN code, collapsing the signal back to its original narrow bandwidth.
  - **Low Pass Filter / Integrator:** This stage filters out the high-frequency components and any "spread" interference, leaving only the original data.
- **Decision Circuit:** Uses a threshold to decide if the recovered bit is a '0' or a '1'.

5.2 FREQUENCY HOPPING SPREAD SPECTRUM (FHSS)

Frequency Hopping Spread Spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. The sequence of these channels is determined by a **Spread Code** (PN code) known only to the transmitter and the receiver.

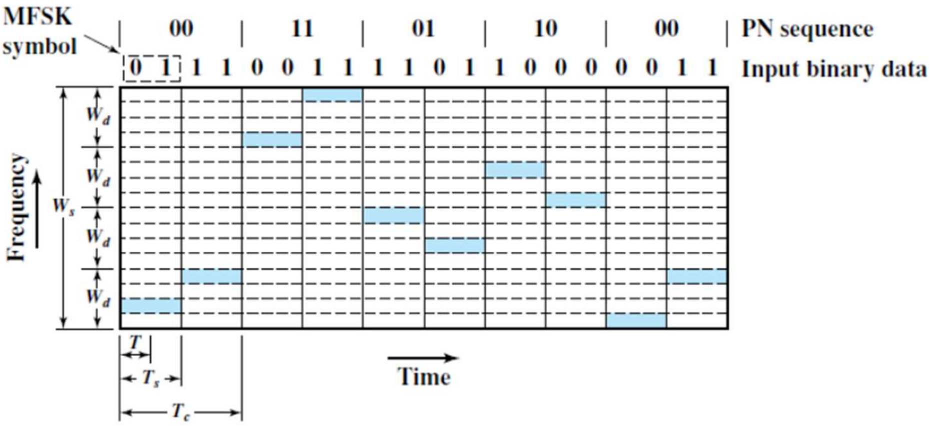

Figure 8: Example of FHSS (Code vs frequencies).

5.2.1 THE SPECTRUM

Unlike the constant "smeared" look of DSSS, the FHSS spectrum looks like a series of narrow peaks appearing and disappearing across a wide band.

Figure 9: PSD of FHSS.

- **Instantaneous Bandwidth:** At any single moment, the signal is narrowband.
- **Average Bandwidth:** Over time, the signal occupies a very large bandwidth.
- **Non-Interference:** Since the signal is only on one frequency for a fraction of a second, it avoids persistent interference and is very difficult to jam without blocking the entire range.

5.2.2 TRANSMITTER BLOCK DIAGRAM

The core difference here is the use of a **Frequency Synthesizer** that can change its output frequency almost instantly based on the PN code.

- **Data Source:** Standard digital data input.
- **Modulator:** Usually uses **FSK (Frequency Shift Keying)** or M-ary FSK to convert data into a basic modulated signal.
- **PN Code Generator:** Produces the "pattern" of the hop.
- **Frequency Synthesizer:** This is the "Engine." It takes the PN code and uses it to select which carrier frequency to use for the next "hop."
- **Mixer/Up-converter:** Combines the modulated data with the hopping carrier for transmission.

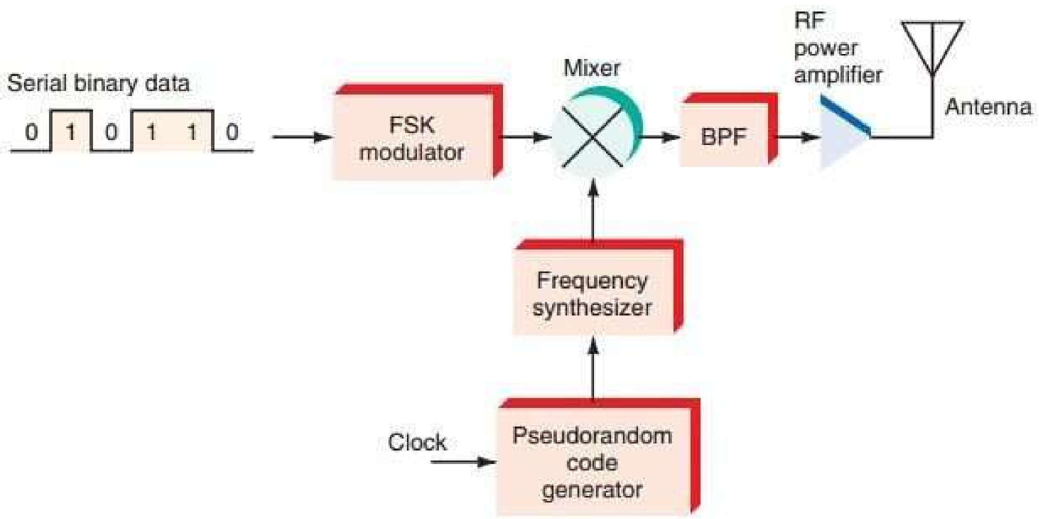

Figure 10: FHSS Transmitter.

5.2.3 RECEIVER BLOCK DIAGRAM

- **PN Code Generator:** Must produce the **exact same** sequence as the transmitter.

- **Synchronized Frequency Synthesizer:** Must change frequencies at the exact same time as the transmitter.
- **Mixer (Down-converter):** If the receiver "hops" to the same frequency as the incoming signal, the signal is successfully down-converted to a stable intermediate frequency (IF).
- **Demodulator:** Recovers the original data from the IF signal.

5.3 HYBRID SYSTEMS

A **Hybrid Spread Spectrum System** is a sophisticated communication technique that integrates the unique strengths of both Direct Sequence (DSSS) and Frequency Hopping (FHSS) to achieve maximum signal security and robustness. In this architecture, the data is first multiplied by a high-speed PN code to spread its bandwidth (the DSSS component), and this wideband signal is then used as the input for a frequency-hopping modulator that shifts the entire "spread" signal to different carrier frequencies over time (the FHSS component). By combining these methods, hybrid systems provide an extremely high processing gain and a "double-layered" defense: the DSSS part offers high-precision timing and multipath rejection, while the FHSS part provides excellent avoidance of narrow-band jamming and detection. Consequently, these systems are primarily utilized in high-stakes military data links and secure satellite communications where resistance to sophisticated electronic warfare is a critical requirement.

6 DIRECT SEQUENCE CODING

Direct Sequence Coding is a fundamental part of Direct Sequence Spread Spectrum (DS/SS) communication systems. In this technique, a Pseudo-Random Noise (PN) code is used to spread the signal bandwidth rather than to carry information. Therefore, the codes used in spread spectrum systems are much longer than those used in conventional digital communication systems.

6.1 PN CODE

A **Pseudo-Noise (PN) code**, also known as a Pseudo-Random Noise (PRN) code, is a deterministic binary sequence that appears random but is actually generated by a mathematical algorithm. In Direct Sequence Spread Spectrum (DSSS), these codes are used to "spread" the signal's energy across a wider bandwidth, making it more resistant to interference and harder to intercept

6.1.1 CHIP

- Definition: A chip is the smallest unit of a spreading code. It is similar to a "bit" but contains no actual information.
- Role: It is the "pulse" used to chop up the data bit into many smaller pieces. For example, if you multiply 1 data bit by 11 chips, that bit is now represented by 11 chips.

6.1.2 CHIP RATE (R_c)

- Definition: The speed at which chips are transmitted, typically measured in megachips per second (Mcps).
- Significance: The chip rate is always much higher than the data bit rate. It directly determines the bandwidth of the transmitted signal; the faster the chip rate, the wider the signal.

6.1.3 CHIP DURATION (T_c)

- Definition: The time it takes for one chip to be transmitted ($T_c = 1/R_c$).

- Comparison: This is significantly shorter than the duration of a single data bit (T_b). The relationship is often expressed as $T_c \ll T_b$.

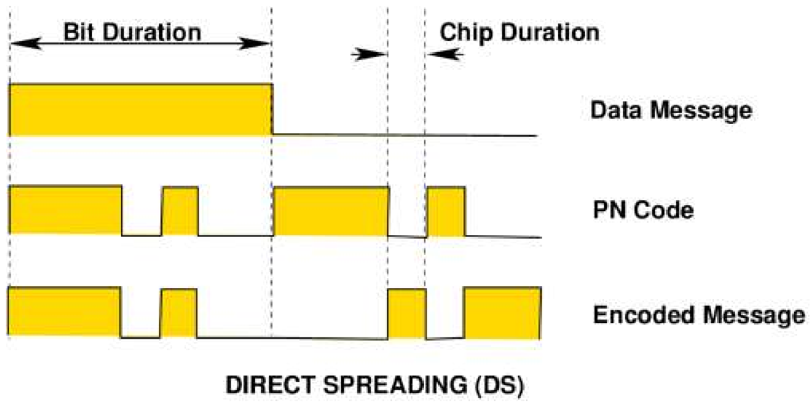

Figure 11: Chip vs Bit.

6.1.4 CODE LENGTH (N)

- Definition: The total number of chips in one full cycle of the PN sequence before it repeats.
- Calculation: For standard m -sequences generated by an m-stage register, the length is $N = 2^m - 1$.
- Short Code: The entire sequence length matches one data bit.
- Long Code: The sequence is much longer than a single bit, spanning many bits before repeating.

6.1.5 SPREADING FACTOR / PROCESSING GAIN (PG)

- Definition: The ratio of the chip rate to the data bit rate ($PG = R_c/R_b$).
- Benefit: It represents the system's "advantage" over interference. A higher PG means the receiver can better extract the signal from heavy noise or jamming.

6.2 PROPERTIES OF PN CODES

Pseudo-Noise (PN) sequences are designed to behave like random noise while remaining deterministic and repeatable. For use in spread spectrum systems, PN sequences must satisfy several important properties.

Pseudo-Noise (PN) sequences are the high-speed codes used in Direct Sequence Spread Spectrum (DSSS) systems. They possess several critical mathematical and statistical properties that allow them to function effectively for spreading, synchronization, and multi-user access.

6.2.1 DETERMINISTIC NATURE

PN codes are not truly random; they are **deterministic**. They are generated using specific mathematical algorithms, typically via a Linear Feedback Shift Register (LFSR). This allows the receiver to perfectly replicate the exact same sequence used by the transmitter to "despread" and recover the data.

6.2.2 BALANCE PROPERTY

In any single period of a maximal-length sequence (m-sequence), the number of ones and zeros is nearly equal. Specifically, the number of ones exceeds the number of zeros by exactly one. This ensures the signal has a negligible DC component.

6.2.3 SHARP AUTOCORRELATION

A PN code has a very high correlation (a sharp peak) only when it is perfectly aligned with its own replica (zero time-shift). If the code is shifted by even one chip, the correlation drops to a very low value. This property is essential for the receiver to achieve perfect **synchronization** and timing.

The autocorrelation of a periodic PN sequence is defined as:

- The number of agreements minus the number of disagreements

- Obtained by comparing one full period of the sequence with a cyclically shifted version of itself

$$R_a(\tau) = \int_{-N_cT_c/2}^{N_cT_c/2} pn(t) \cdot pn(t+\tau)dt \qquad (1)$$

$$\begin{array}{r} pn(0) = +1+1+1-1+1-1-1 \\ pn(0) = +1+1+1-1+1-1-1 \\ \hline +1+1+1+1+1+1+1 \end{array} \quad = \sum = 7 = R_a(\tau = 0)$$

$$\begin{array}{r} pn(0) = +1+1+1-1+1-1-1 \\ pn(1) = +1+1-1+1-1-1+1 \\ \hline +1+1-1-1-1+1-1 \end{array} \quad = \sum = -1 = R_a(\tau = 1)$$

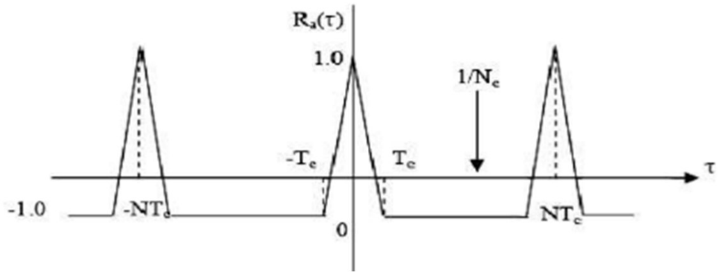

Figure 12: Autocorrelation of PN codes.

6.2.4 LOW CROSS-CORRELATION

Cross-correlation measures the similarity between two different PN codes. In a multi-user system, different codes must have very low cross-correlation to minimize **Multiple Access Interference (MAI)**. This ensures that one user's signal does not "leak" into and interfere with another user's signal.

6.2.5 ORTHOGONALITY

In multi-user systems like CDMA, codes are designed to be **orthogonal**. Two codes are orthogonal if the sum of their bit-by-bit products over one full period is exactly zero. This mathematical independence allows a receiver to "cancel out" all other users and extract only the intended data stream.

6.2.6 RUN-LENGTH DISTRIBUTION

A "run" is a sequence of identical consecutive bits (e.g., 111 or 00). In a PN sequence, the distribution of these runs is strictly defined:

- **Half** of all runs have a length of 1.
- **One-quarter** of all runs have a length of 2.
- **One-eighth** of all runs have a length of 3, and so on. This specific distribution ensures the signal's power is spread evenly across the frequency spectrum, making it look like white noise.

Example of Run Distribution

Run Length (bits)	Ones	Zeros	Total Bits Included
1	16	16	32
2	8	8	32
3	4	4	24
4	2	2	16
5	1	1	10
6	0	1	6
7	1	0	7

Figure 13: Run Length.

6.3 TYPES OF PN CODE

6.3.1 M-SEQUENCE

A **Maximum Length Sequence (M-Sequence)** is a type of Pseudo-Noise (PN) code that is generated using a Linear Feedback Shift Register (LFSR). It is defined as the longest possible sequence that a shift register of a given size (n) can produce before it begins to repeat its pattern.

For a register with n stages, the maximum length (L) is: $L = 2^n - 1$

L	$N_c = 2^L - 1$	Feedback Taps for m-sequences
2	3	[2,1]
3	7	[3,1]
4	15	[4,1]
5	31	[5,3] [5,4,3,2] [5,4,2,1]
6	63	[6,1] [6,5,2,1] [6,5,3,2]
7	127	[7,1] [7,3] [7,3,2,1] [7,4,3,2][7,6,4,2] [7,6,5,2][7,6,5,4,2,1] [7,5,4,3,2,1] [7,6,3,1]
8	255	[8,4,3,2] [8,6,5,3] [8,6,5,2][8,5,3,1] [8,7,6,1][8,7,6,5,2,1] [8,6,4,3,2,1] [8,6,5,1]
9	511	[9,4] [9,6,4,3] [9,8,5,4] [9,8,4,1] [9,5,3,2] [9,8,6,5] [9,8,7,2] [9,6,5,4,2,1] [9,7,6,4,3,1] [9,8,7,6,5,3]
10	1023	[10,3] [10,8,3,2] [10,4,3,1] [10,8,5,1] [10,8,5,4][10,9,4,1][10,8,4,3][10,5,3,2] [10,5,2,1[10,9,4,2][10,6,5,3,2,1] [10,9,8,6,3,2][10,9,7,6,4,1] [10,7,6,4,2,1] [10,9,8,7,6,5,4,3] [10,8,7,6,5,4,3,1]
11	2047	[11,2] [11,8,5,2] [11,7,3,2] [11,5,3,2] [11,10,3,2] [11,6,5,1] [11,5,3,1][11,9,4,1] [11,8,6,2][11,9,8,3][11,10,9,8,3,1]

Figure 14: M-sequence Feedback Taps Table.

6.3.2 PROPERTIES OF M-SEQUENCES

6.3.2.1 The Balance Property

In every full period of the sequence, the number of **1s** is always exactly one more than the number of **0s**.

Formula: There are 2n−1 ones and 2n−1−1 zeros.

Example (n=3): In a 7-bit sequence, there are 4 ones and 3 zeros.

6.3.2.2 The Run Property

A "run" is a subsequence of identical symbols (all 1s or all 0s). In an m-sequence:

- Half of the runs have a length of **1**.
- One-fourth of the runs have a length of **2**.
- One-eighth of the runs have a length of **3**, and so on.
- This distribution is what gives the sequence its "noise-like" statistical appearance.

6.3.2.3 Autocorrelation Property (The Most Important)

The autocorrelation function of an m-sequence is periodic and binary.

- If the sequence is compared to itself with **zero shift**, the correlation is at its maximum (100% match).
- If the sequence is shifted by even a single bit, the correlation drops to a very low constant value of $-1/L$.
- *Application:* This property allows the receiver to perfectly synchronize with the transmitter.

6.3.2.4 Shift-and-Add Property

If you take an m-sequence and add it (using XOR logic) to a shifted version of itself, the result is simply another shifted version of the same original m-sequence.

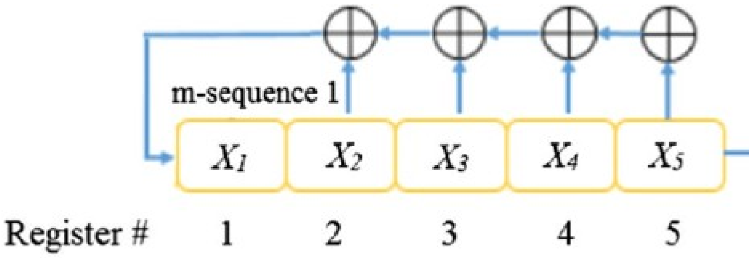

Figure 15: M-sequence with [2,3,4,5] Feedback Taps.

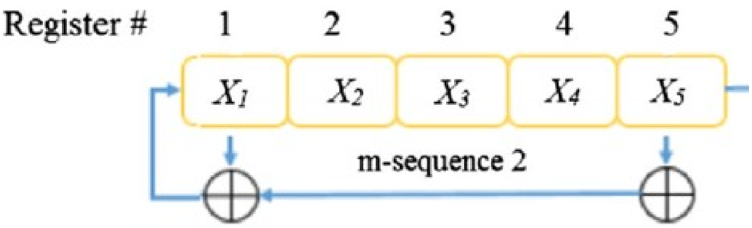

Figure 16: M-sequence with [1,5] Feedback Taps.

6.3.3 GOLD CODE

A **Gold Code** is a type of PN sequence formed by XORing two different **M-sequences** of the same length. These two M-sequences must be a "preferred pair" to ensure the resulting code has superior correlation properties.

6.3.3.1 Method of Implementation

To generate a Gold Code, you need:

- **Two LFSRs:** Both of the same length n.
- **Preferred Pair:** The feedback taps for both must be chosen carefully.
- **XOR Logic:** The outputs of both registers are combined.

- **Phase Shifting:** By shifting the starting point (the seed) of one register relative to the other, you can create a whole "family" of unique Gold Codes ($2^n + 1$ different codes).

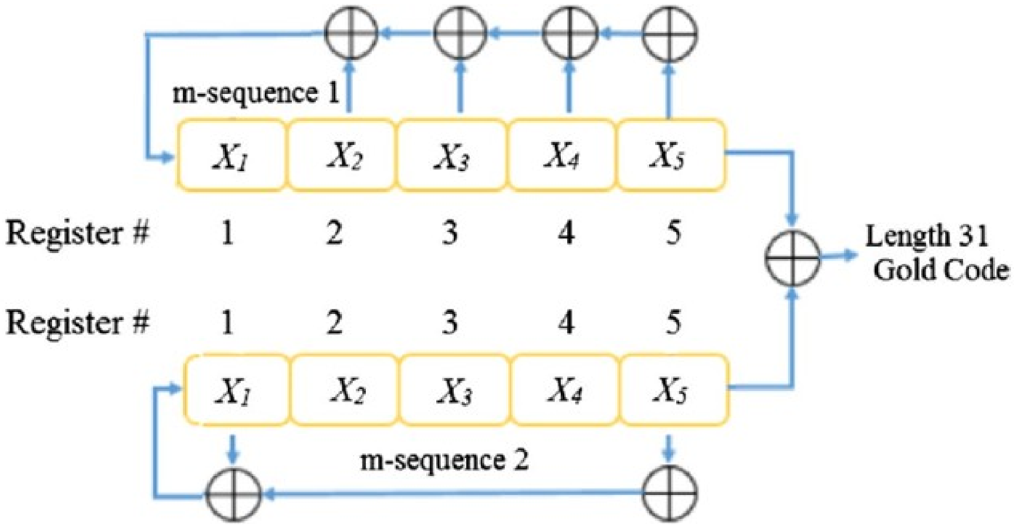

Figure 17: Gold Code Generation Example.

REFERENCES

- Communication Systems – Simon Haykin, 5th Edition, John Wiley & Sons, 2009.
- Modern Digital and Analog Communication Systems – B. P. Lathi and Zhi Ding, 4th Edition, Oxford University Press, 2009.
- Analog and Digital Communication Systems – Leon W. Couch II, 8th Edition, Pearson, 2013.
- Digital Communications – John G. Proakis and Masoud Salehi, 5th Edition, McGraw-Hill, 2007.