

# Spread Spectrum Techniques and Technology

Mark A. Sturza

3C Systems Company

“Spread spectrum is a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information: the band spread is accomplished by means of a code which is independent of the data, and synchronized reception with the code at the receive is used for de-spreading and subsequent data recovery.”

# Advantages of Spread Spectrum

- Anti-jamming (A/J)
- Anti-interference (A/I)
- Low Probability of Intercept (LPI)
- Code Division Multiple Access (CDMA)
- Message Privacy
- High Resolution Ranging and Timing

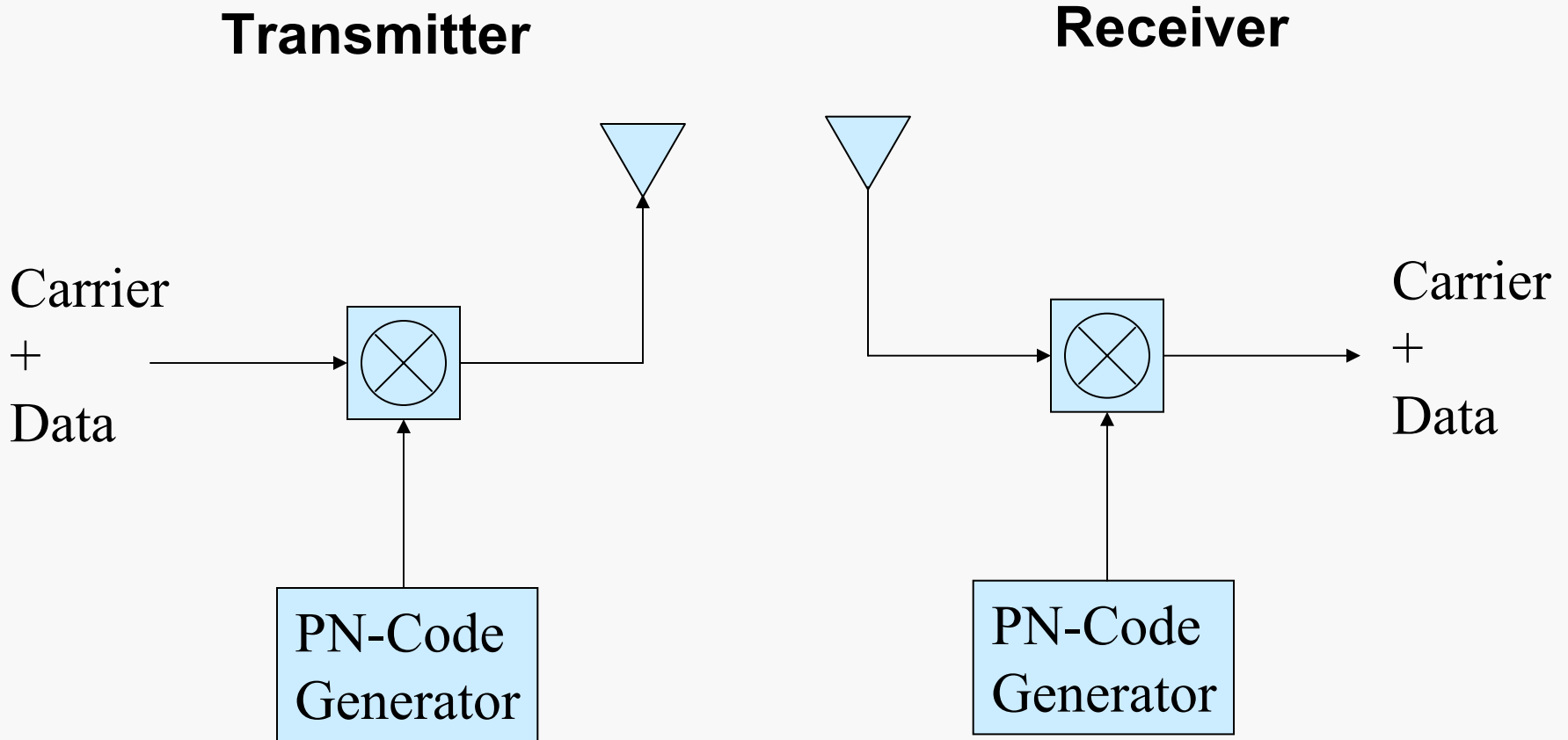
# Spread Spectrum Techniques and Technology

- Spectrum Spreading Techniques
- Processing Gain
- Jamming Margin
- System Comparison
- PN-Codes
- Gold Codes
- Other Codes

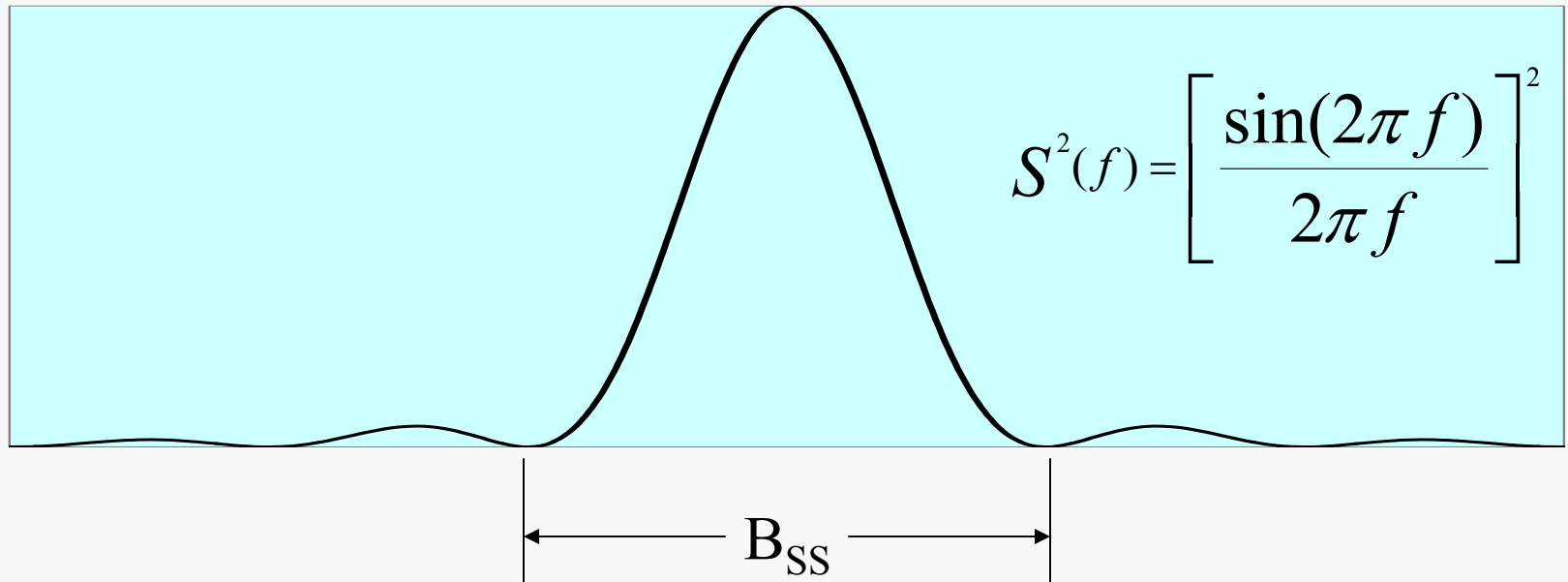
# Spectrum Spreading Techniques

- Direct Sequence (DS)
- Frequency Hopping (FH)
- Time Hopping (TH)
- Hybrids

# DS System Block Diagram



# DS Spectrum



$$B_{SS} = 2 \times R_C$$

$R_C$  – chip rate (bps)

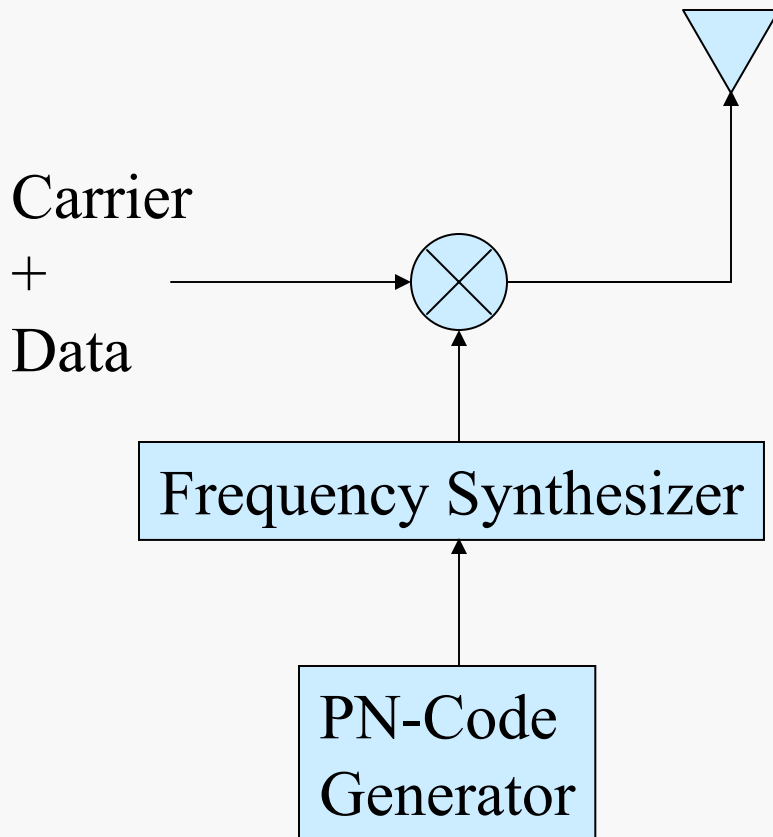
$$B_{IN} = B_{SS}$$

Given  $R_C = 10$  Mbps

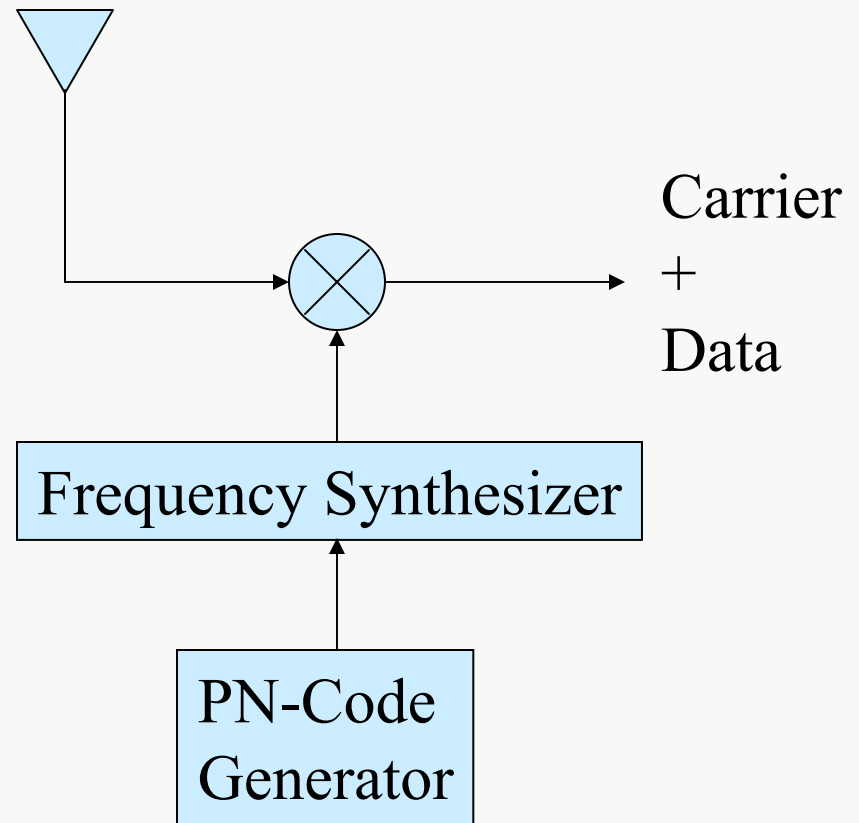
Calculate  $B_{SS} = B_{IN} = 20$  MHz

# FH System Block Diagram

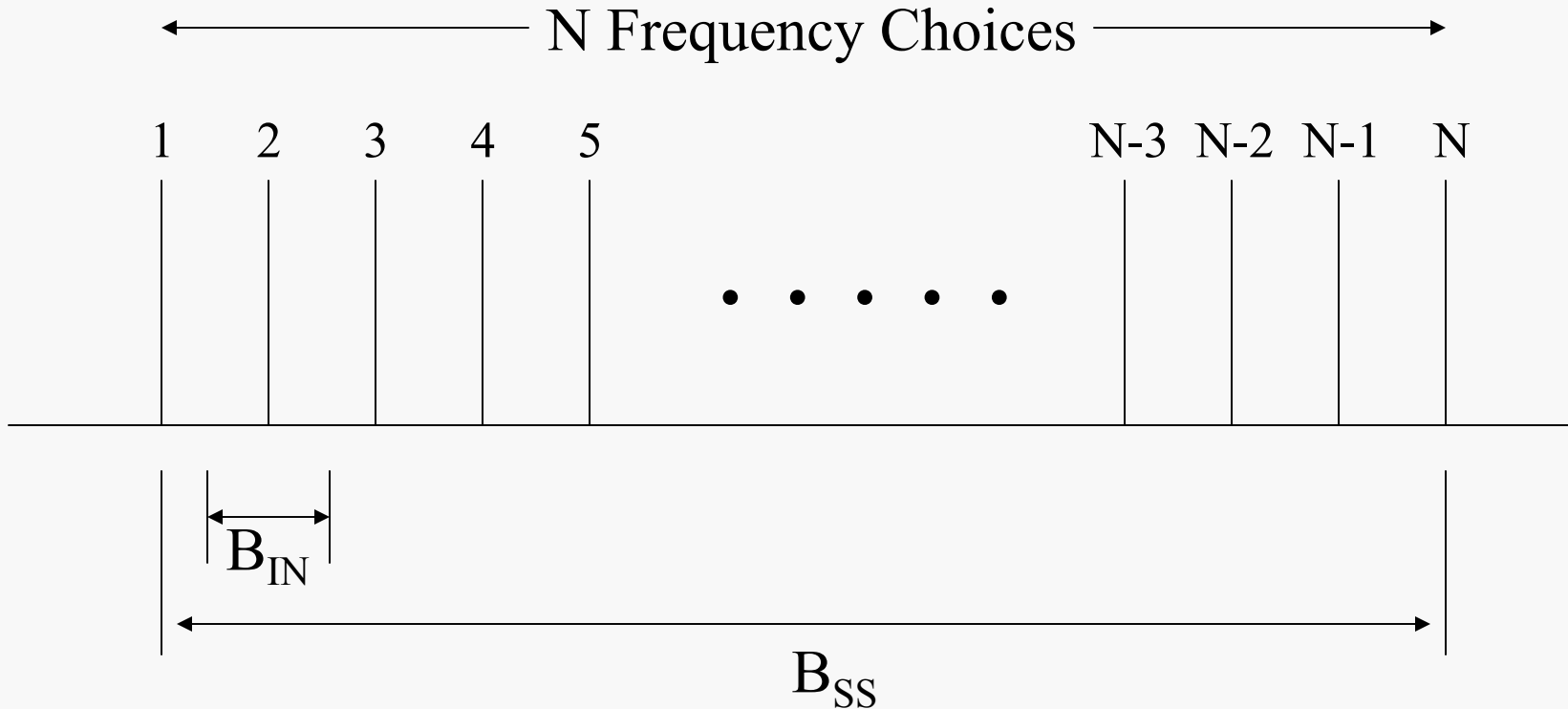
## Transmitter



## Receiver



# FH Spectrum



- $B_{SS} = N \times B_{IN}$
- $B_{IN}$  – instantaneous bandwidth (Hz)

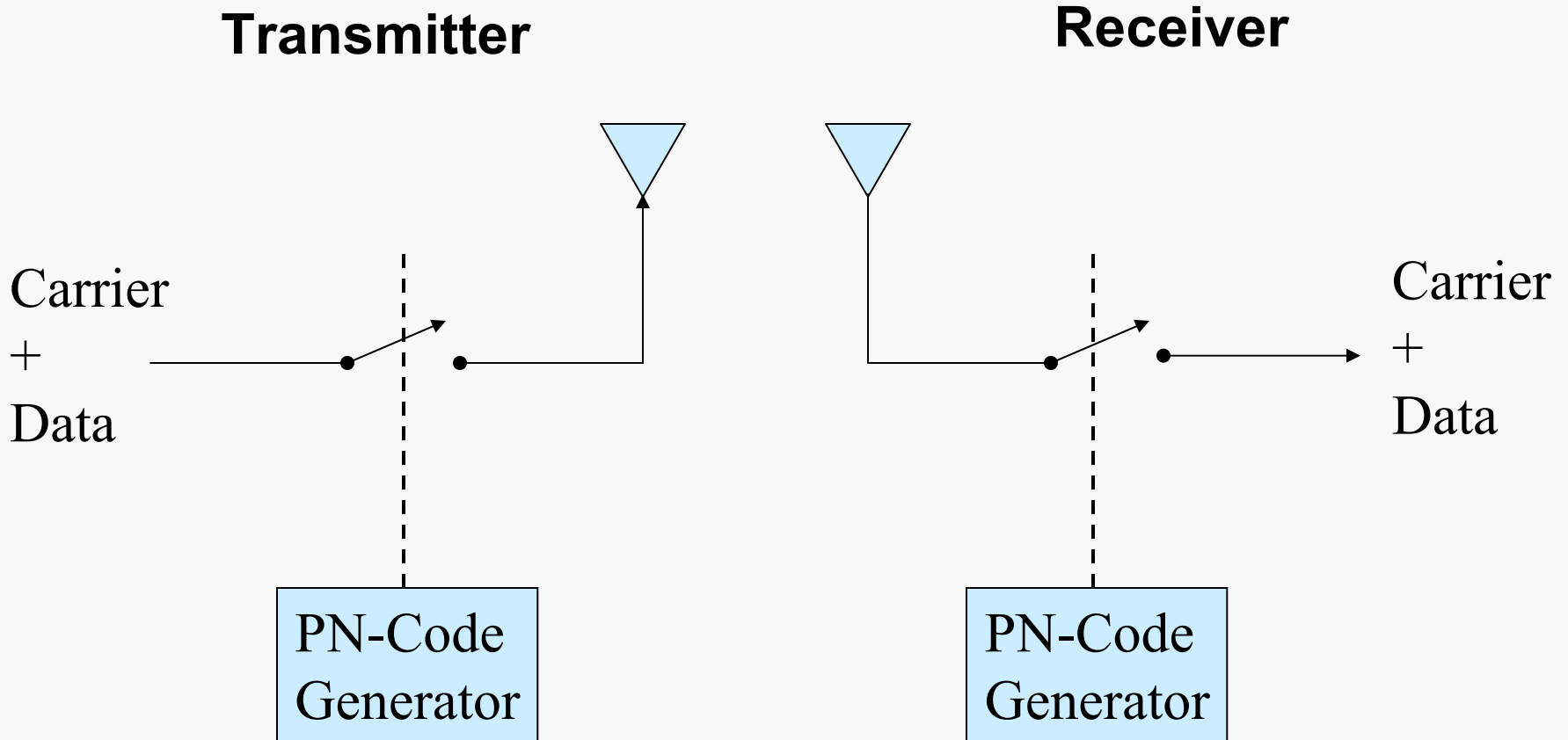
Given

$$B_D = 2 \text{ kHz} \quad N = 5000 \quad R_H = 1000 \text{ hops/sec}$$

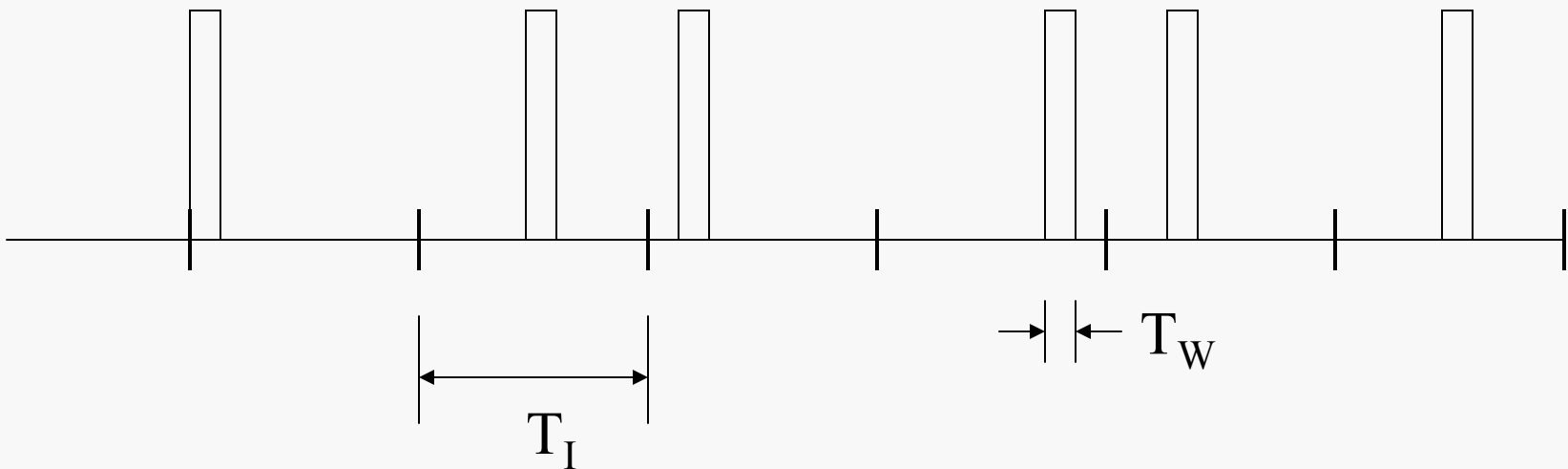
Calculate

$$B_{SS} = 10 \text{ MHz} \quad B_{IN} = 2 \text{ KHz}$$

# TH System Block Diagram



# TH Waveform



- $T_W$  – pulse width (sec)
- $T_I$  – average pulse interval (sec)
- $\beta = T_W / T_I$  – duty cycle factor

# TH Waveform (cont.)

- Typically  $T_W$  is selected such that

$$B_D / \beta > 1 / 2T_W$$

- Then

$$B_{SS} = B_D / \beta$$

Given

$$T_W = 1 \text{ msec}, T_I = 100 \text{ msec}, B_D = 100 \text{ Hz}$$

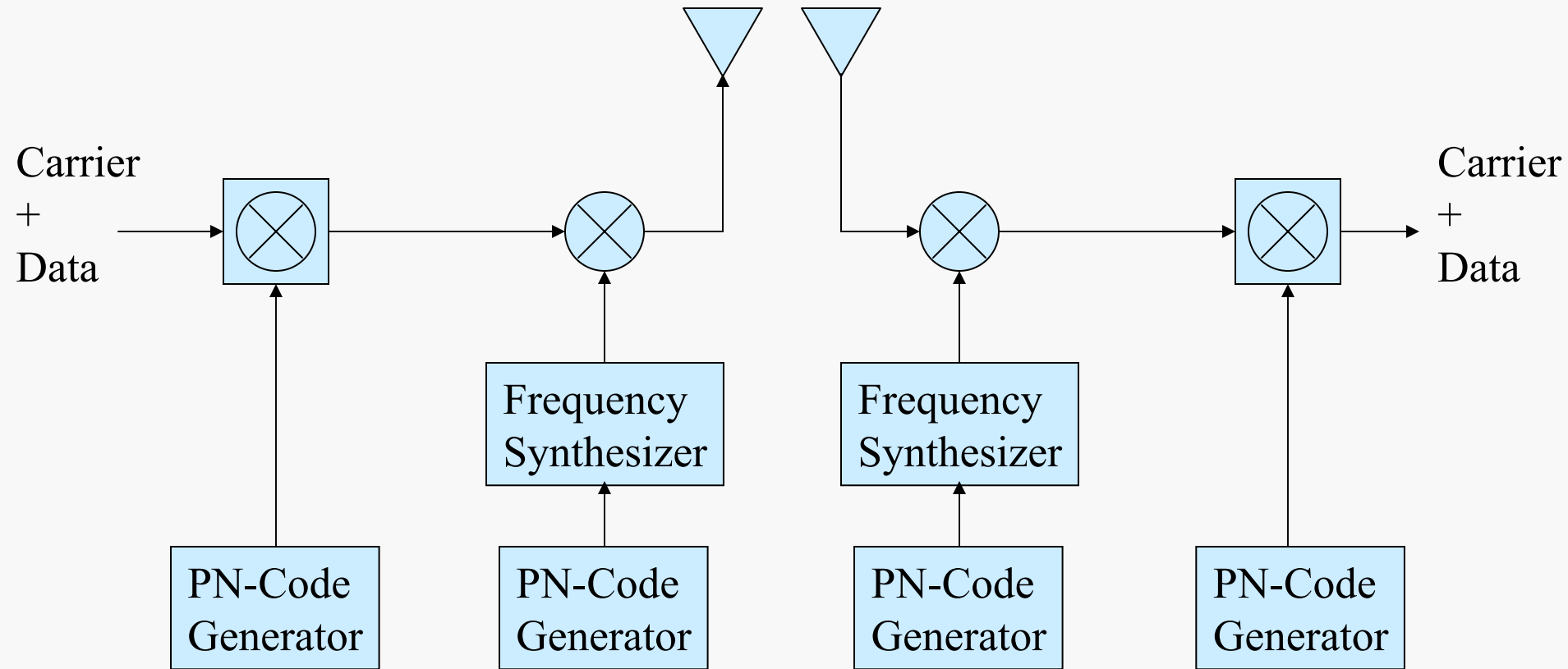
Calculate

$$\beta = 0.01, B_{SS} = 10 \text{ kHz}$$

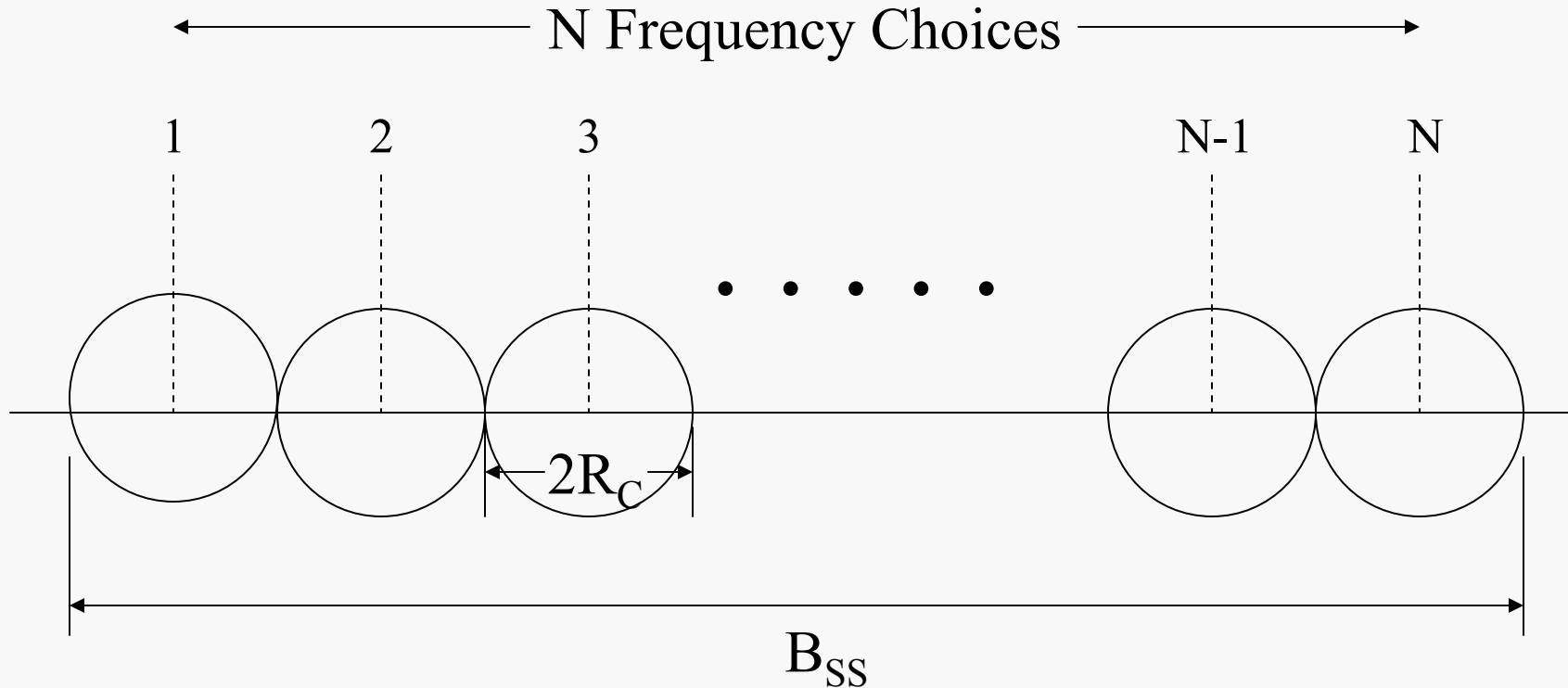
# FH-DS System Block Diagram

## Transmitter

## Receiver



# FH-DS Spectrum



- $B_{SS} = 2 \times N \times R_C$
- $R_C = \text{chip rate (bps)}$

Given  $R_C = 10 \text{ Mbps}$      $N = 50$

Calculate  $B_{SS} = 1 \text{ GHz}$      $B_{IN} = 20 \text{ MHz}$

# Processing Gain

$$PROCESSING\_GAIN = \frac{SPREAD\_SPECTRUM\_BANDWIDTH}{MINIMUM\_INFORMATION\_BANDWIDTH}$$

$$G_P = \frac{B_{SS}}{B_D}$$

Given

$$B_{SS} = 100 \text{ MHz} \quad B_D = 2 \text{ kHz}$$

Calculate

$$GP = 50,000 \text{ (47 dB)}$$

# DS Processing Gain

- $G_p^{DS} = [\text{Chip Rate}] / [\text{Data Bit Rate}] = R_C / R_D$   
 $= [\text{Data Bit Duration}] / [\text{Chip Duration}] = \tau_D / \tau_C$

Given

$$R_C = 10 \text{ Mbps} \quad R_D = 5 \text{ kbps}$$

Calculate

$$\tau_C = 100 \text{ nsec} \quad \tau_D = 200 \mu\text{sec}$$

$$G_p^{DS} = 2,000 \text{ (33 dB)}$$

# FH Processing Gain

- $G_p^{FH} = \text{Number of frequency choices} = N$

Given

$$N = 20,000$$

Calculate

$$G_{PFH} = 20,000 = 43 \text{ dB}$$

Given

$$\beta = 1.0\% \quad T_I = 100 \text{ msec} \quad T_W = 1 \text{ msec}$$

Calculate

$$G_p^{\text{TH}} = 100 \text{ (20 dB)}$$

# Hybrid Processing Gain

- The processing gain of a hybrid spread spectrum system is the product of the processing gains for the component systems assuming that orthogonality is maintained

$$- G_p^{\text{FH-DS}} = G_p^{\text{FH}} \times G_p^{\text{DS}}$$

$$- G_p^{\text{TH-DS}} = G_p^{\text{TH}} \times G_p^{\text{DS}}$$

$$- G_p^{\text{TH-FH}} = G_p^{\text{TH}} \times G_p^{\text{FH}}$$

$$- G_p^{\text{TH-FH-DS}} = G_p^{\text{TH}} \times G_p^{\text{FH}} \times G_p^{\text{DS}}$$

# Hybrid Processing Gain (cont.)

- $G_p^{\text{TH-FH-DS}} \text{ (dB)} = G_p^{\text{TH}} \text{ (dB)} + G_p^{\text{FH}} \text{ (dB)} + G_p^{\text{DS}} \text{ (dB)}$

Given

$$G_p^{\text{DS}} = 17 \text{ dB} \quad G_p^{\text{FH}} = 25 \text{ dB} \quad G_p^{\text{TH}} = 10 \text{ dB}$$

Calculate

$$G_p^{\text{FH-DS}} = 42 \text{ dB} \quad G_p^{\text{TH-DS}} = 27 \text{ dB}$$

$$G_p^{\text{TH-FH}} = 35 \text{ dB} \quad G_p^{\text{TH-FH-DS}} = 52 \text{ dB}$$

# Hybrid Processing Gain (cont.)

Given

FH-DS SS System

$$R_D = 1 \text{ kbps} \quad R_C = 1 \text{ Mbps} \quad N = 1,000$$

Calculate

$$G_P^{DS} = 30 \text{ dB} \quad G_P^{FH} = 30 \text{ dB} \quad G_P^{FH-DS} = 60 \text{ dB}$$

$$R_D = 1 \text{ kbps} \Rightarrow B_D = 2 \text{ kHz}$$

$$G_P^{FH-DS} = 60 \text{ dB} \Rightarrow B_{SS} = 2 \text{ GHz}$$

# Jamming Margin

$$M_J = G_P / [(S/N)_{REQ} \times L]$$

$M_J$  – Jamming Margin

$G_P$  – Processing Gain

$(S/N)_{REQ}$  – minimum required output SNR

$L$  – system implementation loss

$$M_J \text{ (dB)} = G_P \text{ (dB)} - (S/N)_{REQ} \text{ (dB)} - L \text{ (dB)}$$

Given  $G_P = 43 \text{ dB}$   $(S/N)_{REQ} = 10 \text{ dB}$   $L = 2 \text{ dB}$

Calculate  $M_J = 31 \text{ dB}$

# Jamming Margin (cont.)

$$S = E_B R_D \text{ \& } N = N_0 \Rightarrow R_D (S/N)_{\text{REQ}} = (E_b/N_0)_{\text{REQ}}$$

$E_b$  – energy per bit (W)

$N_0$  – one-sided noise spectral density (W/Hz)

$R_D$  – data bit rate (bps)

$$M_J \text{ (dB)} = G_P \text{ (dB)} - (E_b/N_0)_{\text{REQ}} \text{ (dB)} - L \text{ (dB)}$$

Given a FH SS system with FSK modulation and required BER of  $10^{-5} \Rightarrow (E_b/N_0)_{\text{REQ}} = 13 \text{ dB}$  with  $G_P = 43 \text{ dB}$  &  $L = 2 \text{ dB}$

Calculate  $M_J = 28 \text{ dB}$

# Jamming Margin - Coding

- Coding does not reduce the jamming margin of a SS system

$$M_J = G_P / [(E_b/N_0)_{REQ} \times L] = (B_{SS} / B_D) \times (N_0 / E_b) \times L$$

$$E_B = E_S / r \quad B_D = B_S \times r$$

$E_S$  – energy per code symbol (W)

$B_S$  – code symbol bandwidth (Hz)

$r$  – code rate (data bit/code symbol)

$$M_J = (B_{SS} / B_S) \times (N_0 / E_S) \times L$$

# Jamming Margin - Coding (cont.)

Given

DS SS system with PSK modulation

$$R_D = 1 \text{ kbps} \quad R_C = 10 \text{ Mbps} \quad L = 1 \text{ dB} \quad \text{BER} = 10^{-5}$$

Calculate

$$(E_b/N_0)_{\text{REQ}} = 10 \text{ dB} \quad G_P = 40 \text{ dB} \quad M_J = 29 \text{ dB}$$

Encode the data with 4 code symbols per data bit,  $r = 1/4$

Calculate

$$R_S = 4 \text{ kbps} \quad G_P = 34 \text{ dB} \quad (E_S/N_0)_{\text{REQ}} = 4 \text{ dB} \quad M_J = 29 \text{ dB}$$

# Processing Gain Vulnerability – Predictor Jammer

- A predictor jammer observes the SS signal and via computational capabilities breaks the PN-code. It uses this knowledge of the code to predict the PN-code choice made by the SS system and allocates its resources to jam that choice
- The predictor jammer's ability to break the PN-code is a function of the code type and not a function of the SS technique used

# Processing Gain Vulnerability – Follower Jammer

- A follower jammer observes the PN-code choice made by the SS system and allocates its resources to jam that choice
- To be effective the follower jammer must determine the PN-code choice, generate the appropriate jamming signal, and deliver that jamming signal to the receiver prior to the receiver switching to the next PN-code choice

# Processing Gain Vulnerability – Follower Jammer (cont.)

- Even an infinitely fast follower jammer is totally ineffective if

$$1 / R_{PN} \leq [RNG_{TJ} - RNG_{TR} + RNG_{JR}] / c$$

PRN – PN-code rate (bps)

c – speed of light (  $3 \times 10^8$  m/s)

$RNG_{TJ}$  – range from transmitter to jammer (m)

$RNG_{TR}$  – range from transmitter to receiver (m)

$RNG_{JR}$  – range from jammer to receiver (m)

# Processing Gain Vulnerability – Follower Jammer (cont.)

Given

$$RNG_{TJ} = 10 \text{ km} \quad RNG_{TR} = 10 \text{ km} \quad RNG_{JR} = 1 \text{ km}$$

Calculate

$$1 / R_{PN} \leq 3 \text{ } \mu\text{sec}$$

The follower jammer is totally ineffective if  $R_{PN} \geq 300 \text{ kbps}$

- In practice, follower jammers are significant threats to FH and TH SS systems, and insignificant to DS SS systems

# Comparison – Processing Gain

- For given  $B_{SS}$  and  $B_D$

SS Technique	Processing Gain	Relative Comparison
DS	$G_P$	1
FH	$G_P$	1
TH	$G_P$	1

$$G_P = B_{SS} / B_D$$

# Comparison – Instantaneous Bandwidth

- For given  $B_{SS}$  and  $B_D$

SS Technique	Instantaneous BW	Relative Comparison
DS	$B_{SS}$	1
FH	$B_D$	$B_D / B_{SS} = 1 / G_P$
TH	$B_{SS}, 0$	1, 0

- The SS system must support the instantaneous BW
  - The combined coherence bandwidth of the SS equipment and RF link must equal or exceed the instantaneous BW
  - $B_C = 1 / (2T_D)$ , where  $T_D$  is the group delay variation (sec)

# Comparison - LPI

- For given  $B_{SS}$ ,  $B_D$ , and average transmit power  $P_S$

SS Technique	Peak Transmit Power Density	Relative Comparison
DS	$P_S / B_{SS}$	1
FH	$P_S / B_D$	$G_P$
TH	$P_S / B_D$	$G_P$

# PN-Codes

- Pseudorandom noise (PRN) code sequences are deterministically generated but have properties similar to random sequences generated by sampling a white noise process
- PN-code sequences have pseudo-randomness properties

# Pseudo-Randomness Properties

- 1) Over the sequence period, the number of 1's and 0's differs by at most 1
- 2) Over the sequence period, half the runs have length 1, one-fourth have length 2, one-eighth have length 3, etc. For each of the run lengths there are equally many runs of 0 and of 1
- 3) The autocorrelation function,  $R(M)$ , is binary valued, equal to 1 if  $M$  equals 0, and  $-1/N$  otherwise

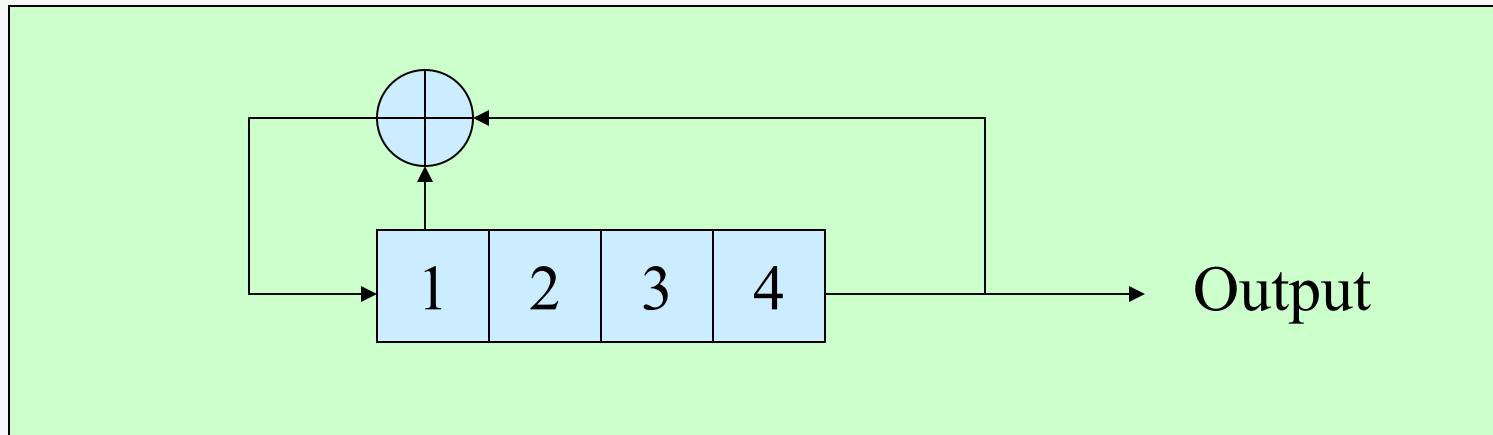
Where  $\{A_N\}$  is the sequence with period  $N$

$$B_N = 1 - 2A_N$$

$$R(M) = \frac{1}{N} \sum_{n=1}^N B_n B_{n+M}$$

# Simple Shift Register Generator

- A simple shift register generator (SSRG) is a shift register generator (SRG) in which all feedback signals are returned to a single input



# Maximal Length Sequences

- The sequence generated by an N-stage SSRG is a maximal length sequence if it has length  $2^N - 1$
- All N-tuples are contained in a maximal length sequence except the sequence of N zeros

SSRG Stages	Maximal Length Sequence Length
	1
	3
	7
	15
	31
	63
	127
	255
	511
	1023

# SSRG Properties

- To generate a maximal length sequence a SSRG must have an even number of taps
- If  $\{a\}$  and  $\{b\}$  are two output sequences of a SSRG then so is  $\{a\} + \{b\}$
- If a maximal length SSRG sequence is added to a shift of itself then the resulting sequence is another shift of the original sequence

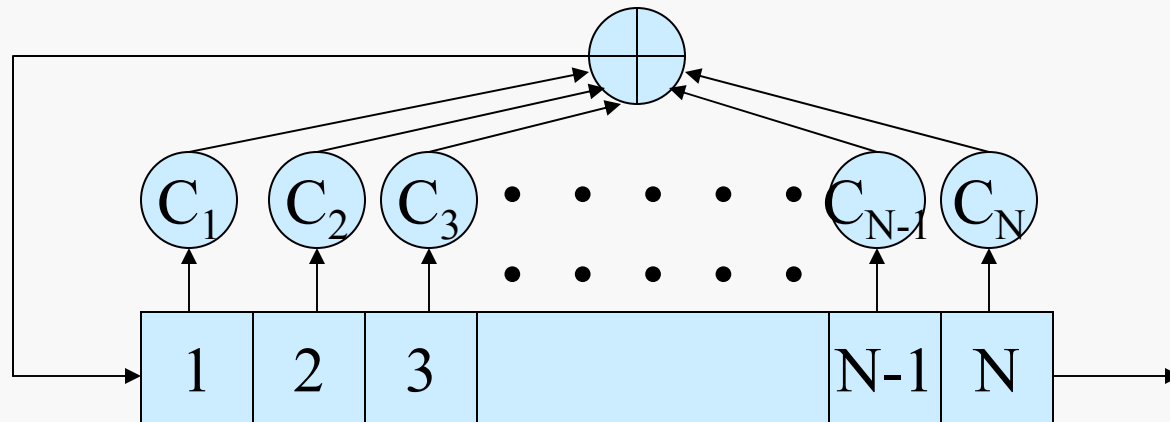
# Maximal Length Sequence Properties

- Maximal length sequences have pseudorandomness properties
  - $2^{N-1}$  ones and  $2^{N-1} - 1$  zeros
  - Balanced runs, except there is no run of  $N$  zeros
  - Binary valued autocorrelation function, equal to 1 if  $M$  equals 0 and  $-1/N$  otherwise

# SSRG Generating Function

- The SSRG and its generating function are related as follows

SSRG:



Generating Function:

$$G(X) = 1 + C_1 X + C_2 X^2 + C_3 X^3 + \dots + C_{N-1} X^{N-1} + C_N X^N$$

# Maximal Length Sequence Generating Functions

- If  $2^N - 1$  is prime, then every irreducible polynomial of degree  $N$  is a maximal length sequence generating function (MLSGF)
  - A polynomial is irreducible if it can not be factored
- If  $2^N - 1$  is not prime, then every primitive irreducible polynomial of degree  $N$  is a MLSGF
  - A polynomial of degree  $N$  is primitive if and only if it divides  $X^M - 1$  for no  $M < 2^N - 1$

# Number of Maximal Length Sequences

<b>SSRG Stages</b>	<b>Sequence Length</b>	<b># of Sequences</b>
1	1	1
2	3	1
3	7	2
4	15	3
5	31	6
6	63	6
7	127	18
8	255	16
9	511	48
10	1023	60
11	2047	176
12	4095	144
13	8191	630

# Reciprocal Generating Functions

- The reciprocal of a primitive polynomial is primitive
- The reciprocal of an irreducible polynomial is irreducible
- Hence the reciprocal of a MLSGF is another MLSGF
- The reciprocal of a polynomial of degree N is

$$R(X) = X^N G(1/X)$$

Given

$$G(X) = 1 + X + X^3, \text{ a MLSGF}$$

Calculate

$$R(X) = 1 + X^2 + X^3, \text{ another MLSGF}$$

# Table of MLSGF'S

SSRG Stages	MLSGF's
2	$[1,2] = 1 + X + X^2$
3	$[1,3] = 1 + X + X^3$
4	$[1,4] = 1 + X + X^3$
5	$[2,5]$ $[2,3,4,5]$ $[1,2,4,5]$
6	$[1,6]$ $[1,2,5,6]$ $[2,3,5,6]$
7	$[3,7]$ $[1,2,3,7]$ $[1,2,4,5,6,7]$ $[2,3,4,7]$ $[1,2,3,4,5,7]$ $[2,4,6,7]$ $[1,7]$ $[1,3,6,7]$ $[2,5,6,7]$

# Gold Codes

- Let  $F(X)$  and  $G(X)$  be MLSGF's of degree  $N$  whose cross correlation function,  $R(K)$ , satisfies

$$|R(K)| \leq \begin{cases} [2^{(N+1)/2} + 1] / 2^{N-1}, & N \text{ odd} \\ [2^{(N+2)/2} + 1] / 2^{N-1}, & N \text{ even, } N \neq 0 \pmod{4} \end{cases}$$

- Then the product polynomial  $F(X) G(X)$  will generate  $2N + 1$  different sequences of period  $2N - 1$ , the cross correlation of all pairs satisfying the above inequality
- These sequences form the Gold code family of order  $N$

# Gold Codes (cont.)

Given

$$F(X) = X^6 + X + 1$$

$$G(X) = X^6 + X^5 + X^2 + X + 1$$

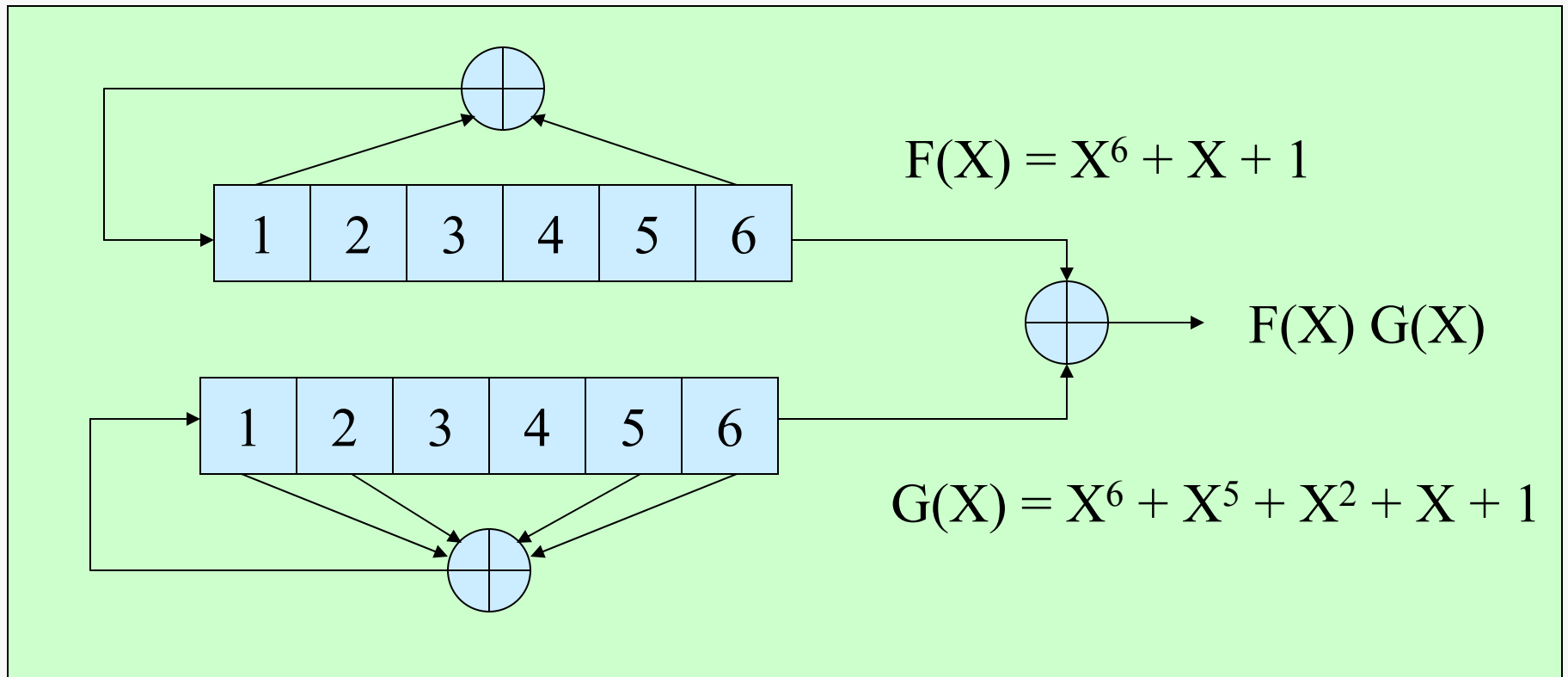
Calculate

$$F(X) G(X) = X^{12} + X^{11} + X^8 + X^6 + X^5 + X^3 + 1$$

65 Gold codes of period 63

$$|R(K)| \leq 17 / 63 \text{ (-11 dB)}$$

# Gold Codes (cont.)



# Gold Code Cross Correlation

Register Length	Code Length	Cross Correlation	Frequency
N odd	$L = 2^N - 1$	$-1 / L$	$\sim 0.5$
		$-(2^{(N+1)/2} + 1) / L$	$\sim 0.25$
		$(2^{(N+1)/2} - 1) / L$	$\sim 0.25$
N even ( $N \neq 0 \pmod{4}$ )	$L = 2^N - 1$	$-1 / L$	$\sim 0.75$
		$-(2^{(N+2)/2} + 1) / L$	$\sim 0.125$
		$(2^{(N+2)/2} - 1) / L$	$\sim 0.125$

Given  $N = 10$

Calculate  $L = 1023$  & Peak Cross Correlation = 0.064 (-24 dB)

# Balanced Gold Codes

- A balanced Gold code sequence is one in which the number of ones exceeds the number of zeros by 1
- Number of balanced and unbalanced Gold codes for odd N

	# Ones in Code Sequence	# Codes
Balanced	$2^{N-1}$	$2^{N-1} + 1$
Unbalanced	$2^{N-1} - 2^{(N-1)/2}$ $2^{N-1} - 2^{(N-1)/2}$	$2^{N-2} - 2^{(N-3)/2}$ $2^{N-2} - 2^{(N-3)/2}$

# Balanced Gold Codes (cont.)

- Any relative shift of the Gold code generator sequences such that the initial 1 of one sequence corresponds to a 0 of the second sequence will result in a balanced Gold code

$F(X) = X^3 + X + 1$		$G(X) = X^3 + X^2 + 1$																													
1110100		1001011																													
<table style="border-collapse: collapse; margin: auto;"> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>1110100</td></tr> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>0010111</td></tr> <tr><td colspan="2" style="border-top: 1px solid black; text-align: center;">1100011</td></tr> </table>	1	1110100	1	0010111	1100011		<table style="border-collapse: collapse; margin: auto;"> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>1110100</td></tr> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>0010111</td></tr> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>0110110</td></tr> <tr><td colspan="2" style="border-top: 1px solid black; text-align: center;">1011010</td></tr> </table>	1	1110100	1	0010111	1	0110110	1011010		<table style="border-collapse: collapse; margin: auto;"> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>1110100</td></tr> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>0010111</td></tr> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>0111001</td></tr> <tr><td colspan="2" style="border-top: 1px solid black; text-align: center;">1001101</td></tr> </table>	1	1110100	1	0010111	1	0111001	1001101		<table style="border-collapse: collapse; margin: auto;"> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>1110100</td></tr> <tr><td style="border: 1px solid black; padding: 2px;">1</td><td>0010111</td></tr> <tr><td colspan="2" style="border-top: 1px solid black; text-align: center;">0111111</td></tr> </table>	1	1110100	1	0010111	0111111	
1	1110100																														
1	0010111																														
1100011																															
1	1110100																														
1	0010111																														
1	0110110																														
1011010																															
1	1110100																														
1	0010111																														
1	0111001																														
1001101																															
1	1110100																														
1	0010111																														
0111111																															

# Message Privacy

- A SS system does not provide secure message privacy unless the PN-code used is cryptographically secure
- Maximal length and gold codes are not cryptographically secure

# JPL Ranging Codes

- Formed by modulo-2 addition of two or more maximal length sequences whose lengths are relatively prime
- The length of the JPL ranging code is the product of the lengths of the component sequences

Given maximal length sequences generated by SSRG's of lengths 7, 10, and 13

Calculate JPL ranging code length as

$$(2^7 - 1) \times (2^{10} - 1) \times (2^{13} - 1) = 1,064,182,911 \approx 2^{30}$$

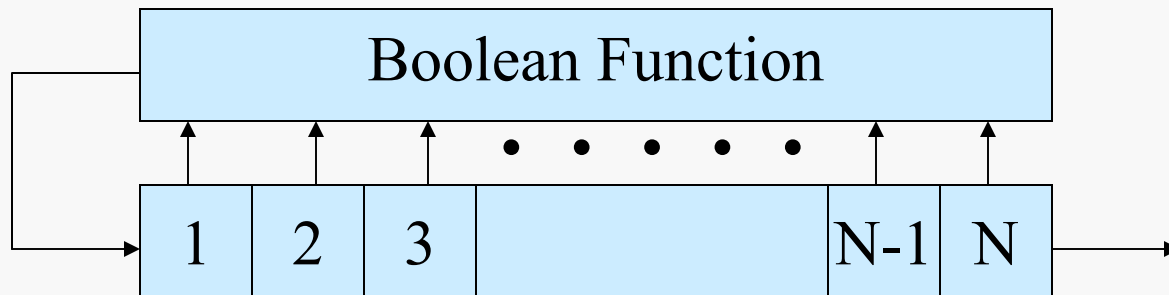
# JPL Ranging Codes (cont.)

- The JPL ranging codes have  $2N$  auto correlation values, where  $N$  is the number of component sequences
- Code synchronization is accomplished by sequentially synchronizing the component sequences
- Sequential synchronization requires searching through a maximum of  $\sum_{i=1}^N (2^{n_i} - 1)$  code chips vs.  $\prod_{i=1}^N (2^{n_i} - 1)$  for composite synchronization

Given  $N = 3, n_1 = 7, n_2 = 10, n_3 = 13$

Calculate  $(2^7 - 1) + (2^{10} - 1) + (2^{13} - 1) = 9,341$   
 $(2^7 - 1) \times (2^{10} - 1) \times (2^{13} - 1) \approx 10^9$

# Nonlinear Feedback Shift Registers



- $2^{2^N}$  possible function
- $2^{2^{N-1-N}}$  functions that generate on sequence of length  $2^N$

Given	N = 5	N = 7
Calculate	4,294,967,296	$3.4 \times 10^{38}$
	67,108,864	$1.3 \times 10^{36}$