Digital Communications

Chapter 12 Spread Spectrum Signals for Digital Communicaitons

Po-Ning Chen, Professor

Institute of Communications Engineering
National Chiao-Tung University, Taiwan

12.1 Model of spread spectrum digital communications system

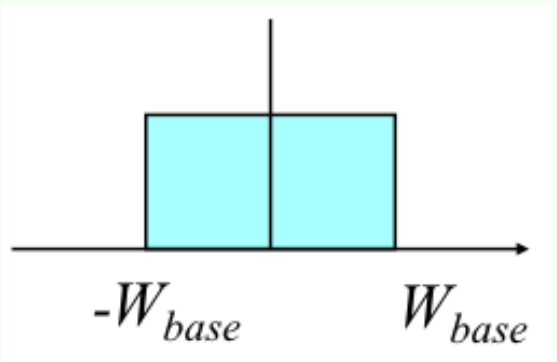
What is "spread spectrum communications?"

- A rough definition: The signal spectrum is wider than "necessary," i.e., $1/T$.

Recollection: Sampling theorem

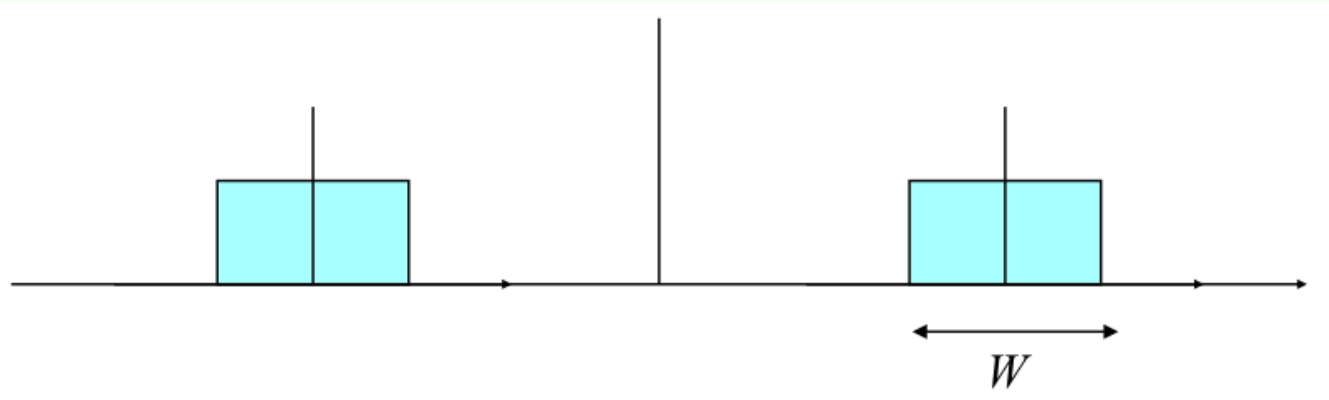
- A signal of (baseband or single-sided) bandwidth W_{base} can be reconstructed from its samples taken at the Nyquist rate ($= 2W_{\text{base}}$ samples/second) using the interpolation formula

$$s(t) = \sum_{n=-\infty}^{\infty} s\left(\frac{n}{2W_{\text{base}}}\right) \text{sinc}\left(2W_{\text{base}}\left(t - \frac{n}{2W_{\text{base}}}\right)\right)$$



Thus, $T = \dfrac{1}{2W_{\text{base}}}$.

However, for a signal that consumes $W = W_{\text{pass}} = 2W_{\text{base}}$ Hz bandwidth after upconvertion, we should put $T = \frac{1}{W}$.



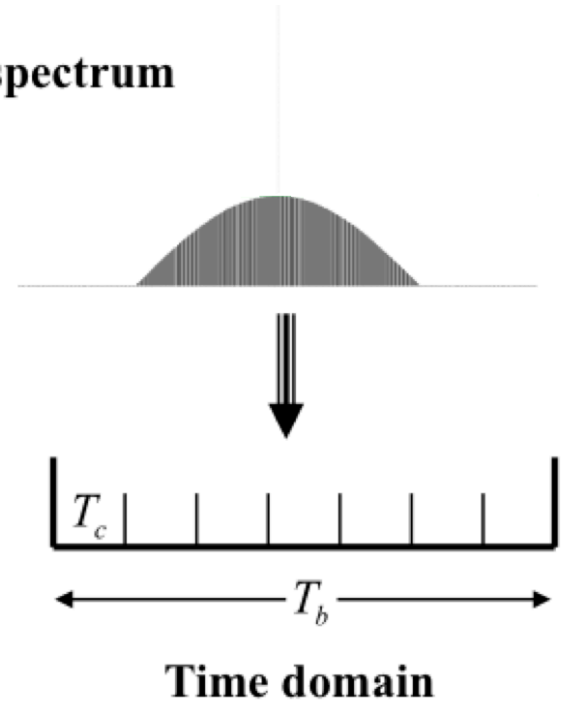
Thus, $T = \dfrac{1}{W}$ or $W = \dfrac{1}{T}$.

Since we have spectrum wider than "necessary," we have **extra spectrum** to make the system more "robust."

$$\text{(digital information)...}\vec{0}\vec{1}\vec{1}\vec{0} \longrightarrow$$

$$\text{where } \begin{cases} \vec{0} = (1100011) \\ \vec{1} = (0011100) \end{cases}.$$

$$\text{Subdivision in time}: W = \frac{1}{T_c} \text{ and } \frac{T_b}{T_c} = 7$$



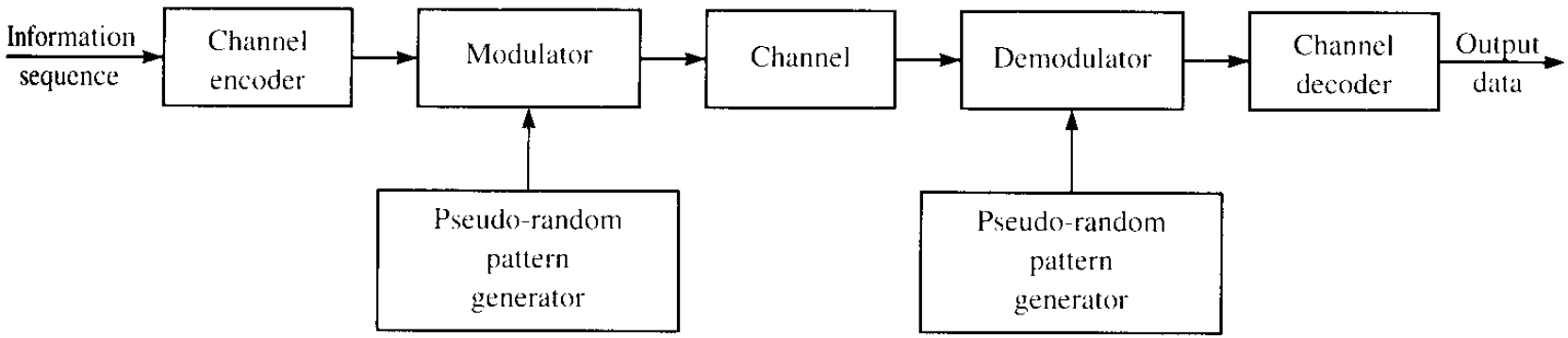
Applications of spread spectrum technique

- Channels with power constraint
  - E.g., power constraint on unlicensed frequency band
- Channels with severe levels of interference
  - Interference from other users or applications
  - Self-interference due to multi-path propagation
- Channels with possible interception
  - Privacy

Features of spread spectrum technology

- Redundant codes (anti-interference)
- Pseudo-randomness (anti-interception from jammers)
  - Or anti-interference in the sense of "not to interfere others"

Model of spread spectrum digital com system

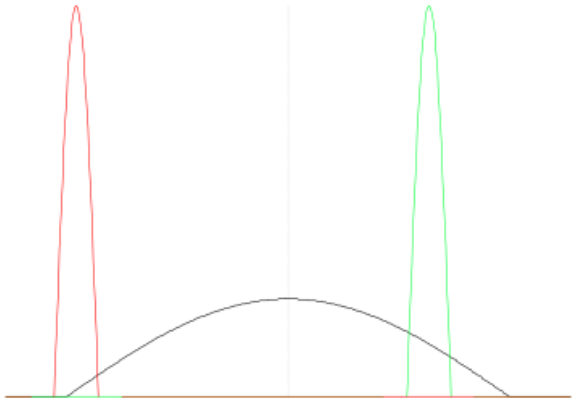


Usage of pseudo-random patterns

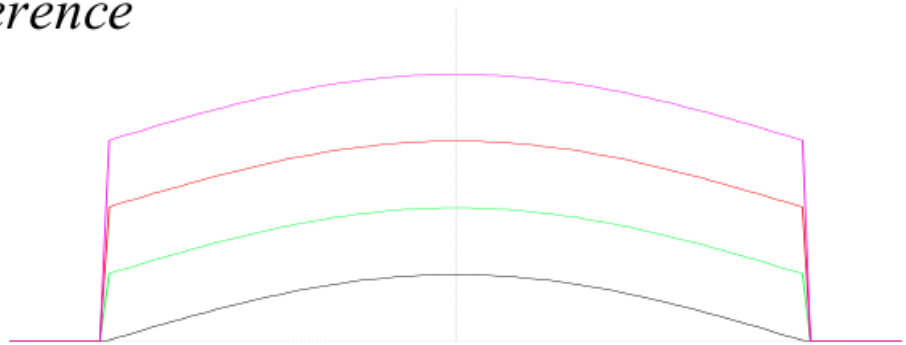
- Synchronization
  - Achieved by a fixed pseudo-random bit pattern
- The interference (from other users) may be characterized as an equivalent additive white noise.

Two different interferences (from others)

- *Narrow-band interference*



- *Broadband interference*



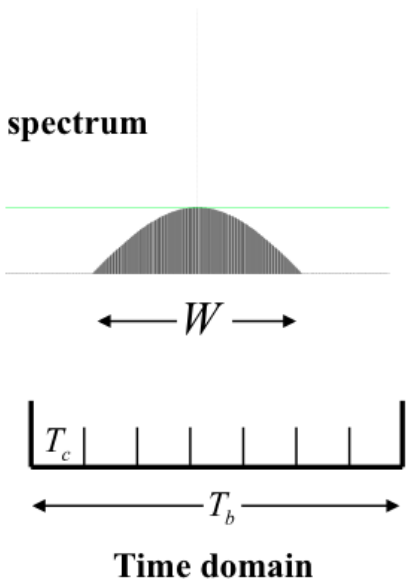
Two types of modulations are majorly considered in this subject.

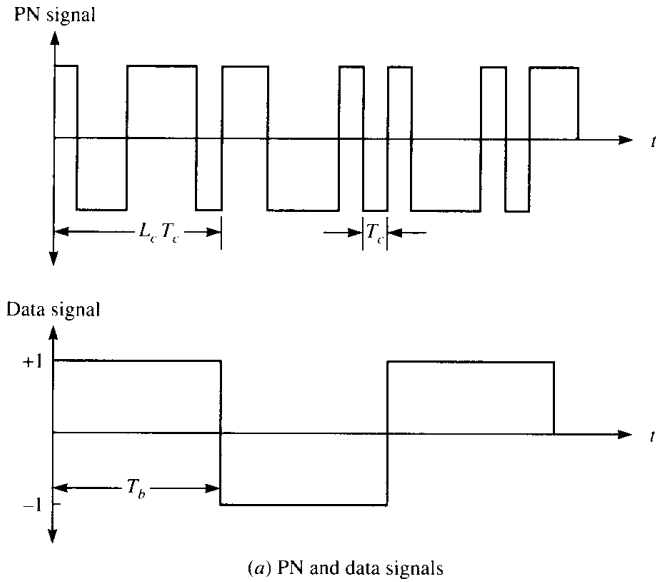
- PSK
  - This is mostly used in direct sequence spread spectrum (DSSS), abbreviated as DS-PSK.
  - Note that some also use MSK in DSSS, abbreviated as DS-MSK.
- FSK
  - This is mostly used in frequency-hopped spread spectrum (FHSS).
  - The FHSS will not be introduced in our lectures.

12.2 Direct sequence spread spectrum signals

A simple spread spectrum system

- Chip interval: $T_c = \frac{1}{W}$
- BPSK is applied for each chip interval.
  - Bandwidth expansion factor $B_e = \frac{W}{R} \left(= \frac{1/T_c}{1/T_b} = \frac{T_b}{T_c} \right)$
  - Number of chips per information bit $L_c = \frac{T_b}{T_c}$





(a) PN and data signals

In practice, the spread spectrum system often consists of an encoder and a modulo-2 adder.

- Encoder : Encode the original information bits (in a pre-specified block) to channel code bits, say (7, 3) linear block code.
- Modulo-2 adder : Directly alter the coded bits by modulo-2 addition with the PN sequences.

Example

1) Choose $T_c = 1$ ms, $T_{ib} = 14$ ms and $T_{cb} = 7$ ms,

$$\text{where} \begin{cases} T_c & \text{length of a chip} \\ T_{ib} & \text{length of an information bit} \\ T_{cb} & \text{length of a code bit} \end{cases}$$

2) Use $(6, 3)$ linear block code (3 information bits $\rightarrow$ 6 code bits)

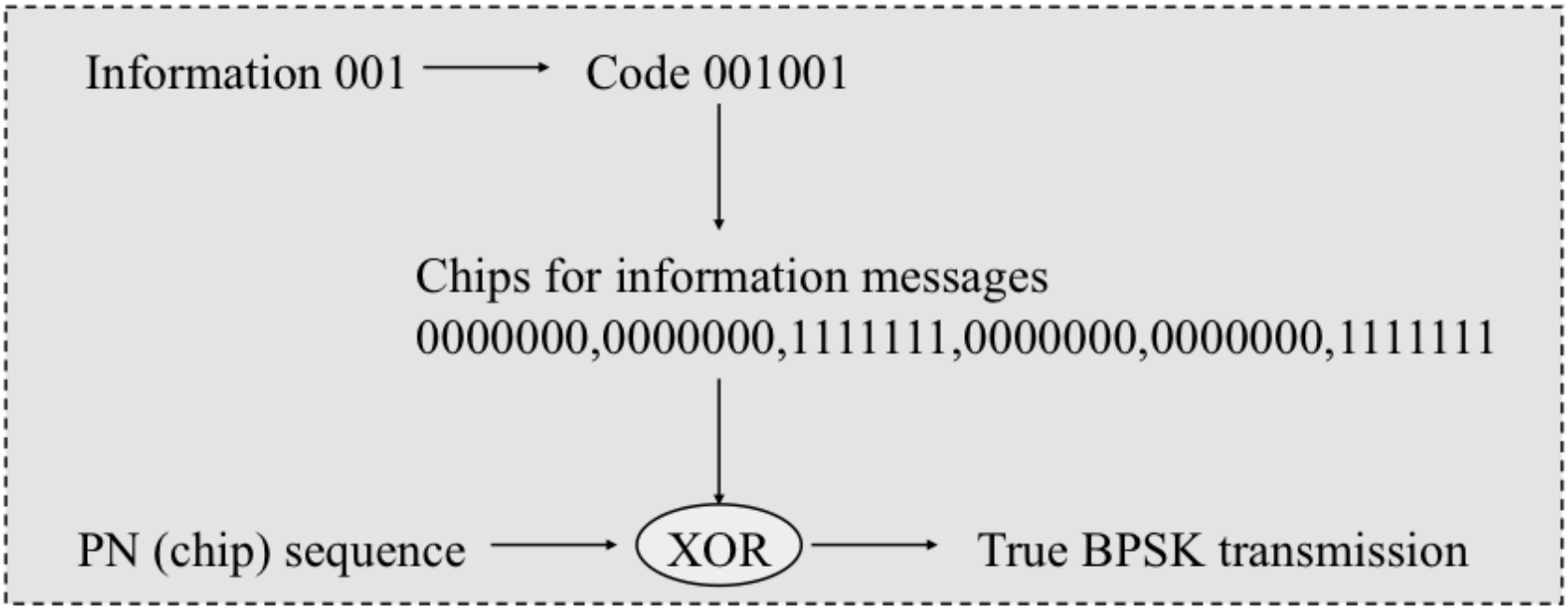
$$\underbrace{\begin{bmatrix} 100 \\ 010 \\ 001 \\ 100 \\ 010 \\ 001 \end{bmatrix}}_{\text{generator matrix}} \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}}_{\text{info bits}} = \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}}_{\text{code bits}}$$

3) **Use the repetition code for chip generation:**

$$\begin{cases} \text{code bit } 0 \rightarrow 0000000 \\ \text{code bit } 1 \rightarrow \underbrace{1111111}_{\substack{\text{seven} \\ \text{chips}}} \end{cases}$$

$$\Longrightarrow L_c = \frac{T_{ib}}{T_c} = 14$$

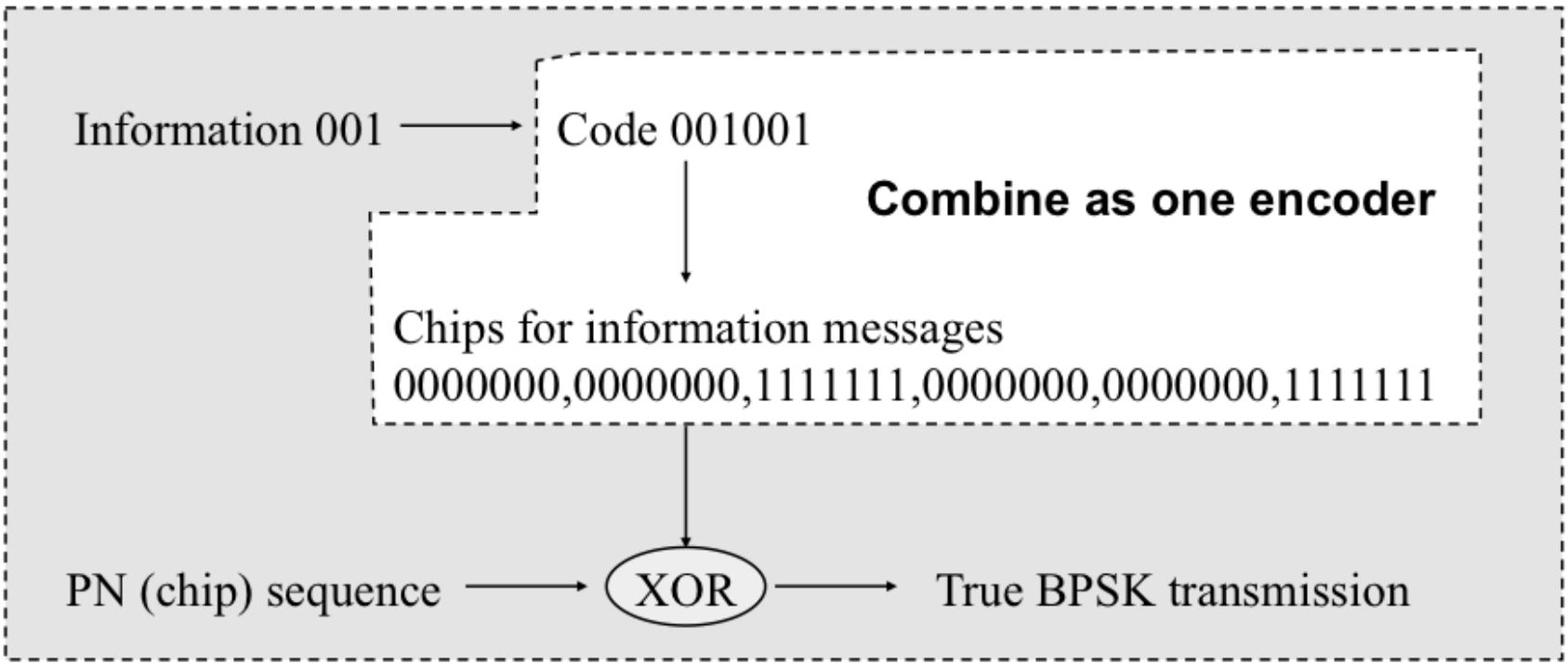
4) **XOR with the PN sequence:**



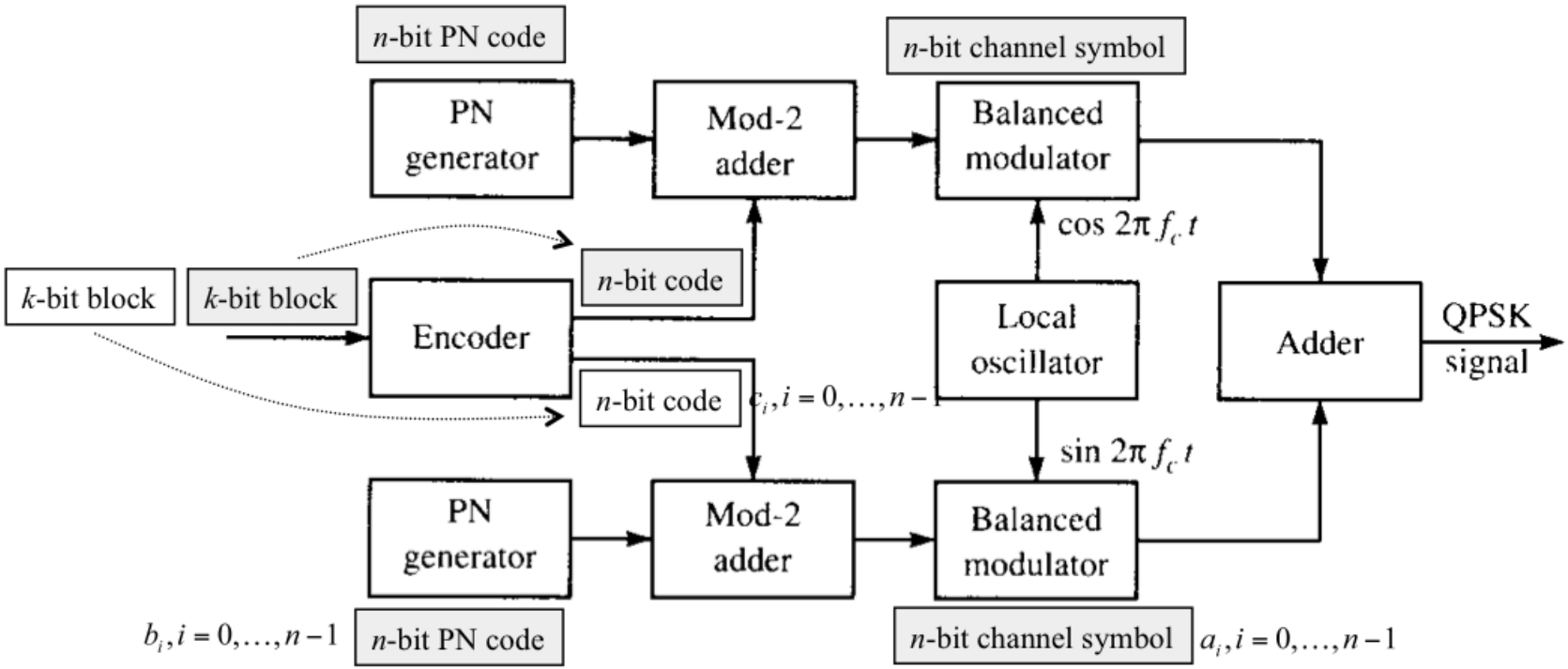
Example (Revisited)

How about we combine Step 2) and Step 3)?

2&3) Use $(n = 6 \times 7, k = 3 \times 1)$ linear block code (3 information bits $\rightarrow$ 42 code bits)



Combined DSSS system



$a_i = b_i \oplus c_i,\ i = 0, \ldots, n-1$ and each a_i is BPSK-transmitted.

Performance analysis

Let $g(t)$ be the baseband pulse shape of duration T_c. Notably, we drop the subscript ℓ for lowpass equivalent signals in this chapter for convenience.

$$g_i(t) = \begin{cases} g(t - iT_c) & \text{if } a_i = 0 \\ -g(t - iT_c) & \text{if } a_i = 1 \end{cases} \text{ for } i = 0, 1, \ldots, n-1$$

Then

$$\begin{aligned} g_i(t) &= (1 - 2a_i)g(t - iT_c) \\ &= [1 - 2(b_i \oplus c_{m,i})]g(t - iT_c) \\ &= [(1 - 2b_i)p(t - iT_c)] \times [(1 - 2c_{m,i})g(t - iT_c)] \\ &\quad \text{or } [(2b_i - 1)p(t - iT_c)] \times [(2c_{m,i} - 1)g(t - iT_c)] \\ &= p_i(t) \times c_{m,i}(t) \end{aligned}$$

where $p(t)$ =rectangular pulse of height 1 and duration T_c.

Consequently,

$$
\begin{aligned}
\text{channel symbol } g_s(t) &= \sum_{i=0}^{n-1} g_i(t) \\
&= \sum_{i=0}^{n-1} p_i(t) c_{m,i}(t) \\
&= \left(\sum_{i=0}^{n-1} p_i(t) \right) \left(\sum_{i=0}^{n-1} c_{m,i}(t) \right) \\
&= p_{\text{PN}}(t) \times c_m(t) \quad \text{where } m = 1, 2, \ldots, M
\end{aligned}
$$

- In implementation (e.g., spectrum), the DSSS channel symbol is the modulo-2 addition between code bits/chips and the PN chips, followed by a chip-based BPSK modulation.
- In analysis, DSSS channel symbol can be conveniently expressed as a coded BPSK signal $c_m(t)$ multiplying a randomly polarized sequence $p_{\text{PN}}(t)$.

DSSS receiver design

For $iT_c \le t < (i+1)T_c$,

$$r_i(t) = p_i(t)c_{m,i}(t) + z(t)$$

where $z(t)$ is the interference introduced mainly by other users and also by background noise.

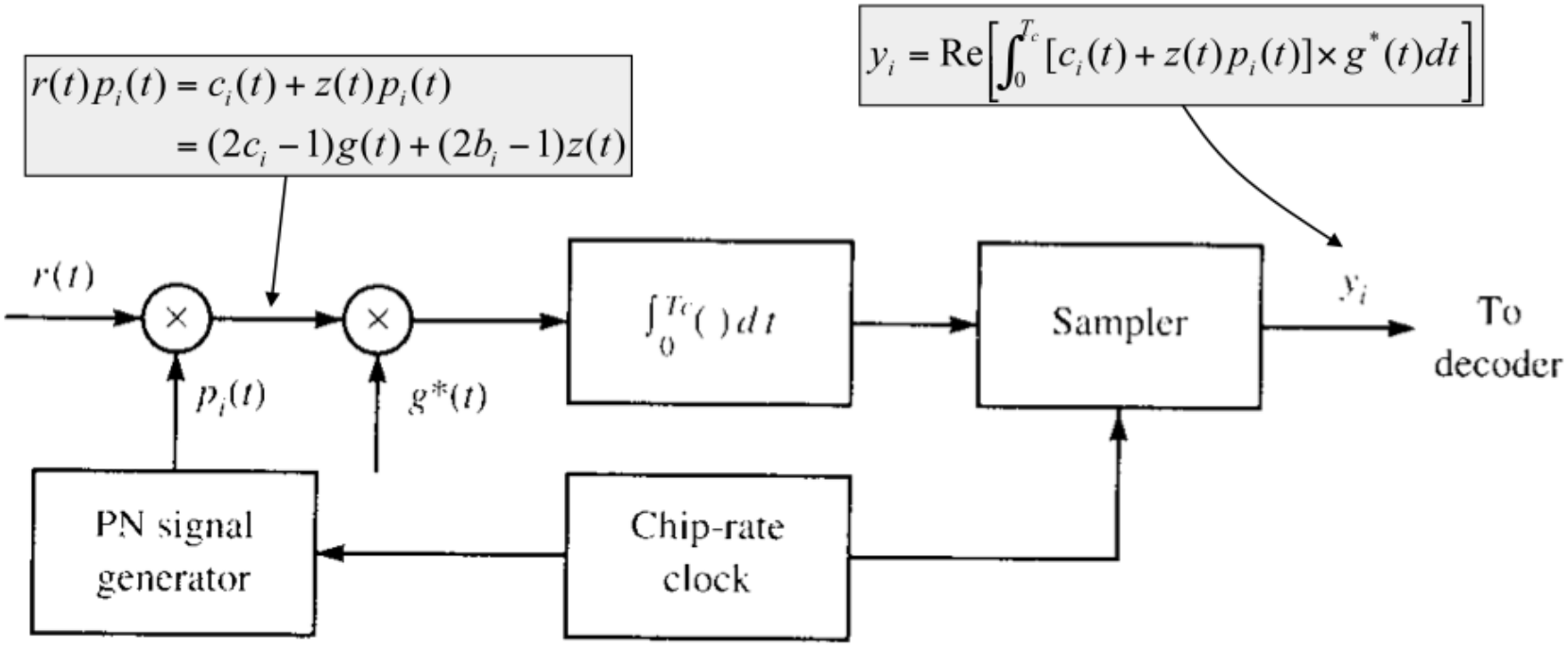
Since for $iT_c \le t < (i+1)T_c$,

$$\begin{aligned} p_i(t) \times p_i(t) &= [(2b_i - 1)p(t - iT_c)] \times [(2b_i - 1)p(t - iT_c)] \\ &= 1 \end{aligned}$$

we have

$$\begin{aligned} c_{m,i}(t) &= [p_i(t)c_{m,i}(t)] \times p_i(t) \\ &= [r_i(t) - z(t)] \times p_i(t) \\ &= r_i(t) \times p_i(t) - z(t) \times p_i(t) \end{aligned}$$

Conclusion: The estimator $\hat{c}_{m,i}(t)$ can be obtained from $r_i(t) \times p_i(t)$ if the channel is interference free.



DSSS demodulator

In this figure, we drop subscript m for $c_{m,i}$ for convenience.

$$
\begin{aligned}
y_i &= \mathbf{Re}\left[\int_0^{T_c}\left[(2c_{m,i}-1)g_i(t)+(2b_i-1)z(t)\right]\times g_i^*(t)dt\right] \\
&= (2c_{m,i}-1)\mathbf{Re}\left[\langle g_i(t),g_i(t)\rangle\right]+(2b_i-1)\mathbf{Re}\left[\langle z(t),g_i(t)\rangle\right] \\
&= (2c_{m,i}-1)2\mathcal{E}_c+(2b_i-1)\nu_i
\end{aligned}
$$

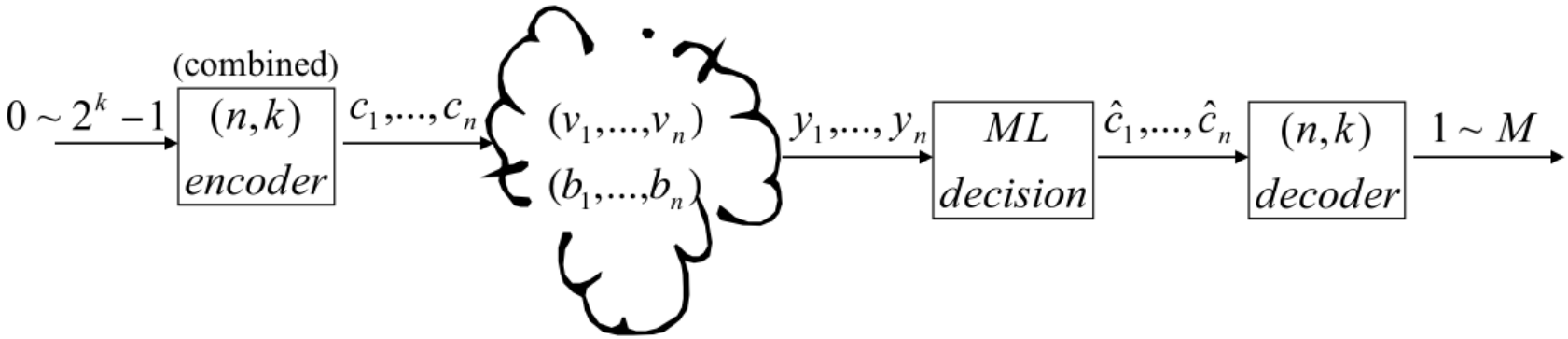
where $\nu_i = \mathbf{Re}\left[\langle z(t), g_i(t)\rangle\right]$.

Recall that Slide 2-24 has derived:

$$\langle x(t), y(t)\rangle = \frac{1}{2}\mathbf{Re}\left\{\langle x_\ell(t), y_\ell(t)\rangle\right\}.$$

or

$$
\begin{aligned}
\mathcal{E}_c = \langle g_{passband}(t), g_{passband}(t)\rangle &= \frac{1}{2}\mathbf{Re}\left\{\langle g(t), g(t)\rangle\right\} \\
&= \frac{1}{2}\langle g(t), g(t)\rangle
\end{aligned}
$$



$$y_i = (2c_{m,i} - 1)2\mathcal{E}_c + (2b_i - 1)\nu_i$$

Assumptions:

- $z(t)$ is a baseband interference (hence, complex).
- $z(t)$ is a (WSS) broadband interference, i.e., PSD of $z(t)$ is

$$S_z(f) = 2J_0 \quad \text{for } |f| \leq \frac{W}{2}.$$

- $z(t)$ Gaussian
- $(2b_i - 1)$ is known to Rx

ML decision

$$\begin{aligned}
\hat{m} &= \arg \min_{1\le m\le M} \|\boldsymbol{y} - 2\mathcal{E}_c(2\boldsymbol{c}_m - 1)\|^2 \\
&= \arg \max_{1\le m\le M} \langle \boldsymbol{y}, 2\mathcal{E}_c(2\boldsymbol{c}_m - 1)\rangle \text{ since } \|2\boldsymbol{c}_m - 1\|^2 \text{ constant} \\
&= \arg \max_{1\le m\le M} 2\mathcal{E}_c \sum_{i=1}^{n}(2c_{m,i} - 1)y_i \\
&= \arg \max_{1\le m\le M} \sum_{i=1}^{n}(2c_{m,i} - 1)y_i
\end{aligned}$$

Suppose

- linear code is employed, and
- the transmitted codeword is the all-zero codeword (i.e., $c_{1,i}$).

$$\hat{m} = \arg \max_{1\le m\le M} \sum_{i=1}^{n}(2c_{m,i} - 1)[(2c_{1,i} - 1)2\mathcal{E}_c + (2b_i - 1)\nu_i]$$

$$\Pr[\text{error}] = \Pr[\hat{m} \neq 1]$$

$$= \Pr\left[\begin{array}{l} \sum_{i=1}^{n}(2\underbrace{c_{1,i}}_{=0}-1)[(2\underbrace{c_{1,i}}_{=0}-1)2\mathcal{E}_c+(2b_i-1)\nu_i] \\ < \max\limits_{2\le m\le M}\sum_{i=1}^{n}(2c_{m,i}-1)[(2\underbrace{c_{1,i}}_{=0}-1)2\mathcal{E}_c+(2b_i-1)\nu_i] \end{array}\right]$$

$$= \Pr\left[\begin{array}{l} 2n\mathcal{E}_c-\sum_{i=1}^{n}(2b_i-1)\nu_i \\ < \max\limits_{2\le m\le M}\left[-2\mathcal{E}_c\sum_{i=1}^{n}(2c_{m,i}-1)+\sum_{i=1}^{n}(2c_{m,i}-1)(2b_i-1)\nu_i\right] \end{array}\right]$$

$$= \Pr\left[\begin{array}{l} \cancel{2n\mathcal{E}_c-\sum_{i=1}^{n}(2b_i-1)\nu_i} \\ < \max\limits_{2\le m\le M}\left[2\mathcal{E}_c(\cancel{n}-2w_m)+\sum_{i=1}^{n}(2c_{m,i}-\cancel{1})(2b_i-1)\nu_i\right] \end{array}\right]$$

$$= \Pr\left[\min_{2\le m\le M}\left(2\mathcal{E}_c w_m-\sum_{i=1}^{n}c_{m,i}(2b_i-1)\nu_i\right)<0\right]$$

where w_m is the number of 1's in codeword m.

Let $R_m = 2\mathcal{E}_c w_m - \sum_{i=1}^{n} c_{m,i}(2b_i - 1)\nu_i$.

Note that R_m given $\boldsymbol{b}$ is Gaussian with

mean $\mathbb{E}[R_m|\boldsymbol{b}] = 2\mathcal{E}_c w_m$ and variance $\mathrm{Var}[R_m|\boldsymbol{b}] = w_m \mathbb{E}[\nu_i^2]$.

We have the union bound:

$$\Pr\left\{\mathcal{N}\left(m, \sigma^2\right) < r\right\} = Q\left(\tfrac{m-r}{\sigma}\right)$$

$$\begin{aligned}
\Pr[\text{error}|\boldsymbol{b}] &= \Pr\left[\min_{2\le m\le M} R_m < 0 \,\middle|\, \boldsymbol{b}\right] \\
&\le \sum_{m=2}^{M} \Pr\left[R_m < 0 | \boldsymbol{b}\right] = \sum_{m=2}^{M} Q\left(\frac{2\mathcal{E}_c w_m}{\sqrt{w_m \mathbb{E}[\nu_i^2]}}\right)
\end{aligned}$$

Since the upper bound has nothing to do with $\boldsymbol{b}$, we have

$$\Pr[\text{error}] = \sum_{\boldsymbol{b}} \Pr(\boldsymbol{b}) \Pr[\text{error}|\boldsymbol{b}] \le \sum_{m=2}^{M} Q\left(\frac{2\mathcal{E}_c w_m}{\sqrt{w_m E[\nu_i^2]}}\right).$$

$$\begin{aligned}
\nu_i &= \mathbf{Re}\left[\langle z(t), g_i(t)\rangle\right] \\
&= \mathbf{Re}\left[\int_{iT_c}^{(i+1)T_c} z(t)g^*(t-iT_c)dt\right] \\
&\overset{d}{=} \mathbf{Re}\left[\int_0^{T_c} z(t)g^*(t)dt\right] = \mathbf{Re}\left[\nu_i + \imath\,\hat{\nu}_i\right]
\end{aligned}$$

where "$\overset{d}{=}$" means "equality in distribution."

Assumption: ν_i and $\hat{\nu}_i$ are zero mean and uncorrelated.

$$\begin{aligned}
\mathbb{E}[\nu_i^2] &= \frac{1}{2}\mathbb{E}\left[|\nu_i + \imath\,\hat{\nu}_i|^2\right] = \frac{1}{2}\mathbb{E}\left[\left|\int_0^{T_c} z(t)g^*(t)dt\right|^2\right] \\
&= \frac{1}{2}\int_0^{T_c}\int_0^{T_c} \mathbb{E}[z(t)z^*(s)]g^*(t)g(s)dtds \\
&= \frac{1}{2}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} R_z(t-s)g^*(t)g(s)dtds
\end{aligned}$$

$$\begin{aligned}
\mathbb{E}\left[\left|\nu_i + \imath\,\hat{\nu}_i\right|^2\right] &= \int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty} g(s)R_z(t-s)ds\right)g^*(t)dt \\
&= \int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty} G(f)S_z(f)e^{\imath 2\pi ft}df\right)g^*(t)dt \\
&= \int_{-\infty}^{\infty}|G(f)|^2 S_z(f)df
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \mathbb{E}[\nu_i^2] &= \frac{1}{2}\int_{-\infty}^{\infty}|G(f)|^2 S_z(f)df \\
&= J_0\int_{-W/2}^{W/2}|G(f)|^2 df \\
&\approx 2J_0\mathcal{E}_c
\end{aligned}$$

$$
\begin{aligned}
\Pr[\text{error}] &\leq \sum_{m=2}^{M} Q\left(\frac{2\mathcal{E}_c w_m}{\sqrt{2 w_m \mathcal{E}_c J_0}}\right) \\
&= \sum_{m=2}^{M} Q\left(\sqrt{\frac{2\mathcal{E}_c w_m}{J_0}}\right) \\
&= \sum_{m=2}^{M} Q\left(\sqrt{\frac{2(k/n)\mathcal{E}_b w_m}{J_0}}\right) \\
&= \sum_{m=2}^{M} Q\left(\sqrt{2 R_c \gamma_b w_m}\right)
\end{aligned}
$$

where

- $R_c = k/n$ code rate
- $\gamma_b = \mathcal{E}_b/J_0$ signal-to-interference ratio per info bit

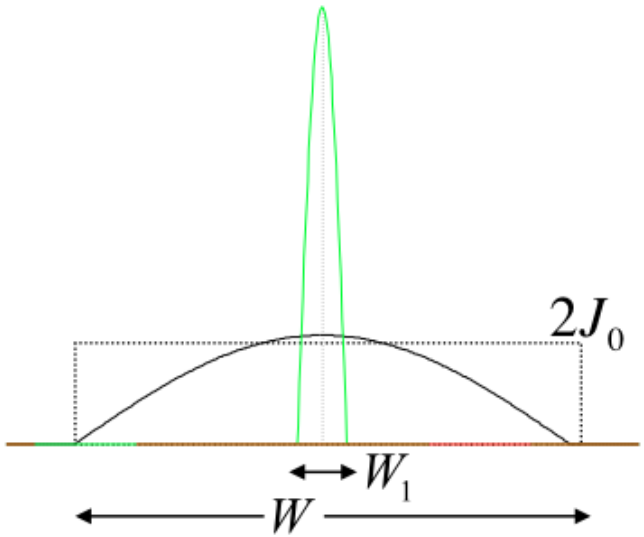
How about $z(t)$ being narrowband interference?

Assumptions:

- $z(t)$ is a baseband interference (hence, complex).
- $z(t)$ is a (WSS) narrowband interference (around zero freq), i.e., PSD of $z(t)$ is

$$S_z(f) = \begin{cases} \frac{J_{av}}{W_1} = 2J_0\left(\frac{W}{W_1}\right), & \text{for } |f| \le \frac{W_1}{2} \\ 0, & \text{otherwise} \end{cases}$$

where $J_{av} = 2WJ_0$.



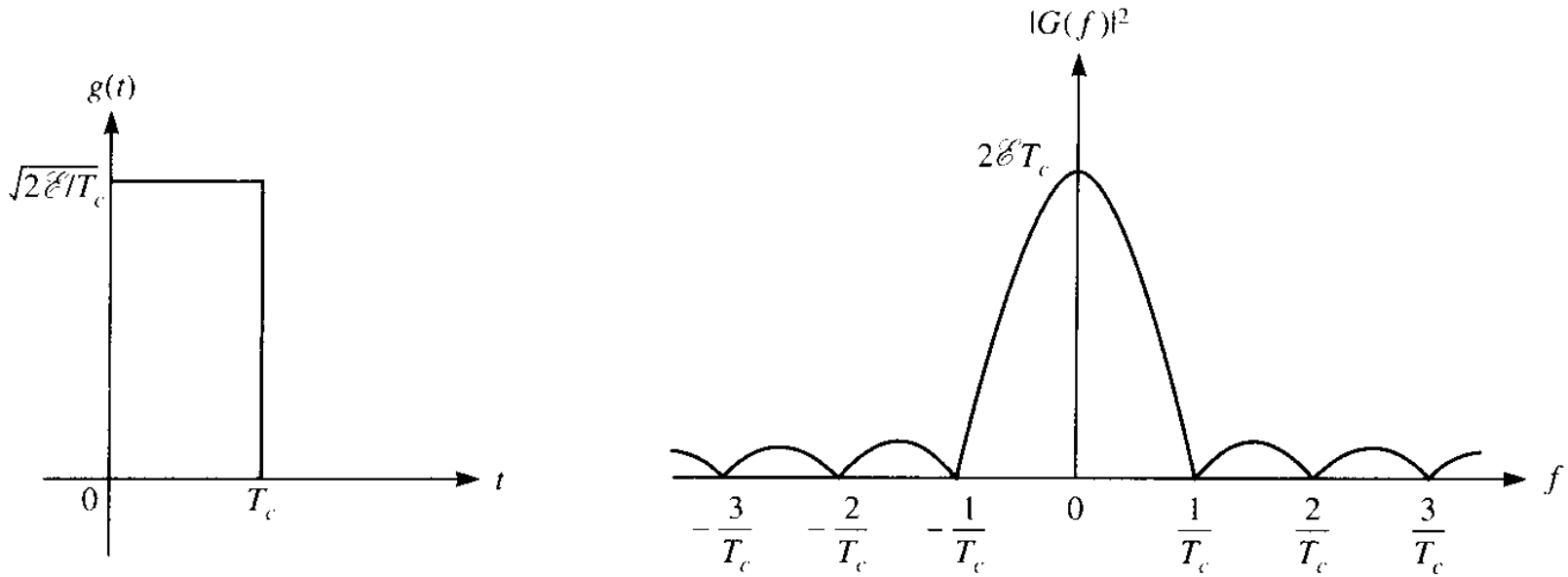
All the derivations remain unchanged except

$$\begin{aligned}\mathbb{E}[\nu_i^2] &= \frac{1}{2}\int_{-\infty}^{\infty}|G(f)|^2 S_z(f)df \\ &= \frac{J_{av}}{2W_1}\int_{-W_1/2}^{W_1/2}|G(f)|^2 df\end{aligned}$$

The value of $\mathbb{E}[\nu_i^2]$ hence depends on the spectra of $g(t)$ and the location of the narrowband jammer.

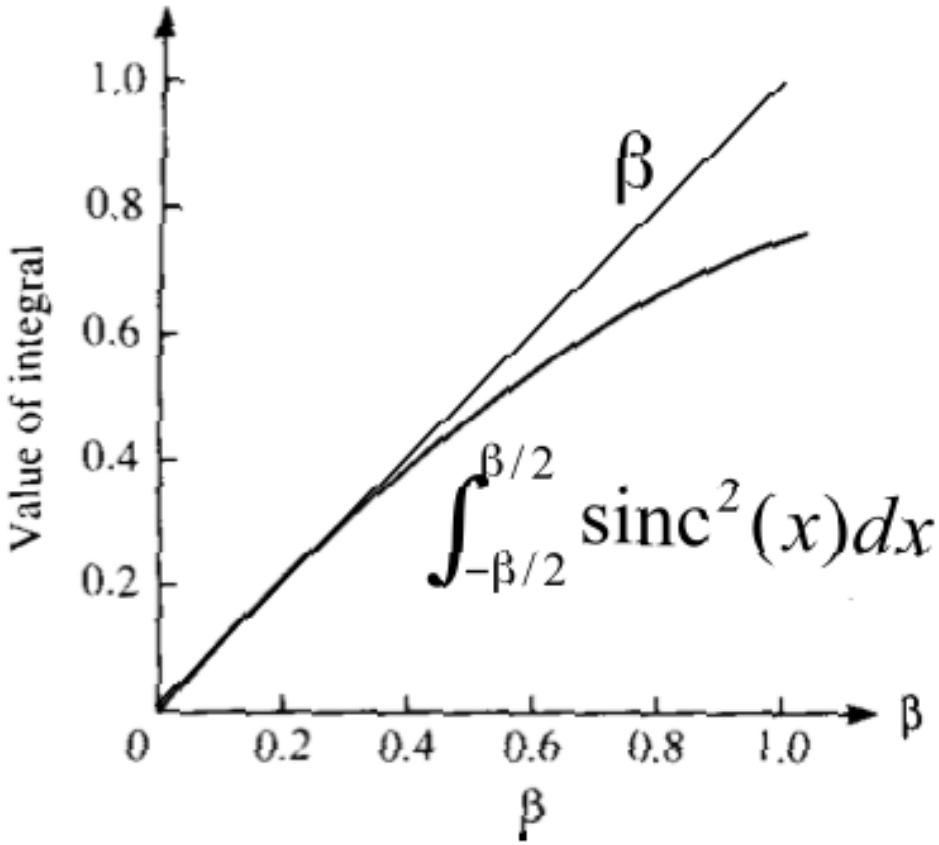
Example 12.2-1

Rectangular pulse and its energy density spectrum.



$$\begin{aligned}\mathbb{E}[\nu_i^2] &= \frac{J_{av}}{2W_1}\int_{-W_1/2}^{W_1/2}|G(f)|^2 df = \frac{J_{av}\mathcal{E}_c}{W_1}\int_{-\beta/2}^{\beta/2}\text{sinc}^2(x)dx \\ &\leq \frac{J_{av}\mathcal{E}_c}{W_1}\beta = J_{av}\mathcal{E}_c T_c = 2J_0\mathcal{E}_c\end{aligned}$$

where we use $x = fT_c$ and $\beta = W_1 T_c = \frac{W_1}{W}$ in the derivation.


1.0
0.8
0.6
0.4
0.2
Value of integral
β
$\int_{-\beta/2}^{\beta/2} \mathrm{sinc}^2(x)dx$
0
0.2
0.4
0.6
0.8
1.0
β
β

How about $z(t)$ being CW jammer?

Assumptions:

- $z(t)$ is a CW (continuous wave) interference (hence, complex).
- $z(t)$ is a (WSS) CW (continuous wave) interference, i.e., PSD of $z(t)$ is

$$S_z(f) = J_{av}\delta(f)$$

$$\begin{aligned}\mathbb{E}[\nu_i^2] &= \frac{1}{2}\int_{-\infty}^{\infty}|G(f)|^2 S_z(f)df \\ &= \frac{J_{av}}{2}|G(0)|^2 = 2J_0\mathcal{E}_c \text{ for Example 12.2-1}\end{aligned}$$

where $G(0) = \sqrt{2\mathcal{E}_c T_c}$ (and $J_{av} = 2J_0 W$ and $WT_c = 1$).

From the above discussion, we learn that

- Under narrowband jammer, the DSSS performance depends on the shape of $g(t)$.
- For example (Example 12.2-2), if $g(t)=\sqrt{\frac{4\mathcal{E}_c}{T_c}}\sin\left(\frac{\pi t}{T_c}\right)$ for $0\le t<T_c$, then $G(0)=\int_{-\infty}^{\infty}g(t)dt=\frac{4}{\pi}\sqrt{\mathcal{E}_c T_c}$ and

$$\begin{aligned}\Pr[\text{error}] &\le \sum_{m=2}^{M} Q\left(\sqrt{\frac{\pi^2}{4}R_c\gamma_b w_m}\right)\\ &= \sum_{m=2}^{M} Q\left(\sqrt{(2.4674)R_c\gamma_b w_m}\right)\end{aligned}$$

The error bound for one half cycle sinusoidal $g(t)$ is about 0.9dB better than that of rectangular $g(t)$.

Alternative union bound

Since $\boxed{J_{av} = 2J_0 W = 2J_0/T_c}$ and $\boxed{P_{av} = \mathcal{E}_b/T_b}$,

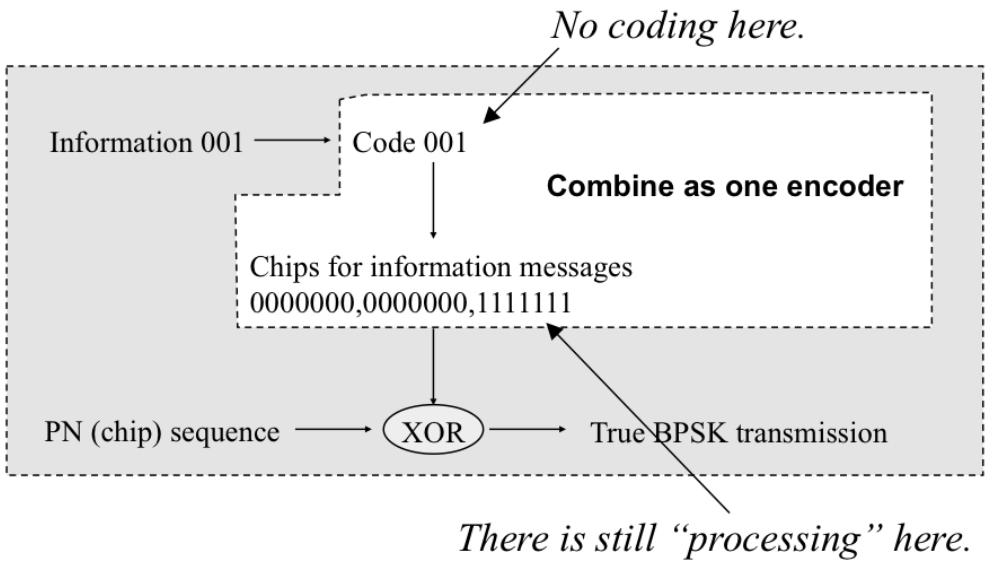
$$\gamma_b = \frac{\mathcal{E}_b}{J_0} = \frac{P_{av} T_b}{J_{av} T_c/2} = \frac{2L_c}{J_{av}/P_{av}}$$

$$\begin{aligned}
\Pr[\text{error}] &\leq \sum_{m=2}^{M} Q\left(\sqrt{2R_c\gamma_b w_m}\right) = \sum_{m=2}^{M} Q\left(\sqrt{4\frac{L_c R_c w_m}{J_{av}/P_{av}}}\right) \\
&\leq (M-1) Q\left(\sqrt{4\frac{L_c}{J_{av}/P_{av}} \min_{2\leq m\leq M} R_c w_m}\right)
\end{aligned}$$

where
- $\frac{J_{av}}{P_{av}}$ Jamming-to-signal power ratio
- L_c Processing gain
- $\min_{2\leq m\leq M} R_c w_m$ Coding gain (Recall $w_1 = 0$)

Interpretation

- Processing gain:
  - Theoretically, it is the number of chips per information bit, which equals the bandwidth expansion factor B_e.
  - Practically, it is the gain obtained via the uncoded DSSS system (e.g., uncoded BPSK DSSS) in comparison with the non-DSSS system (e.g., BPSK $Q(\sqrt{2\gamma_b})$).
  - So, it is the advantage gained over the jammer by the processing of spreading the bandwidth of the transmitted signal.



- Coding gain
  - It is the advantage gained over the jammer by a proper code design.

Example. Uncoded DSSS: Assume we use $(n, 1)$ code. Then,

$$R_c = \frac{1}{n}, M = 2^1 = 2, w_1 = 0, w_2 = n.$$

Hence, coding gain $= \min_{2 \le m \le M} R_c w_m = \frac{1}{n} n = 1 = 0$ dB.

- **Definition:** Jamming margin
  - The largest **jamming-to-signal power ratio** that achieves the specified performance (i.e., error rate) under fixed processing gain and coding gain.

Example 12.2-3

Problem: Find the jamming margin to achieve error rate 10^{-6} with $L_c = 1000$ and uncoded DSSS.

For $M = 2$ (uncoded DSSS), the union bound is equal to the exact error.

Answer:

$$\Pr[\text{error}] = Q\left(\sqrt{4\frac{L_c}{J_{av}/P_{av}}R_c w_2}\right) = Q\left(\sqrt{4\frac{1000}{J_{av}/P_{av}}}\right) \leq 10^{-6}$$

where $R_c = 1/n$ and $w_2 = n$.

Then, $J_{av}/P_{av} = 22.5$ dB. □

Example 12.2-3 (revisited)

Problem: Given that $\gamma_b = 10.5$ dB satisfies $Q(\sqrt{2\gamma_b}) = 10^{-6}$, find the jamming margin to achieve error rate 10^{-6} with $L_c = 1000$ and uncoded DSSS.

Answer:

$$\Pr[\text{error}] = Q\left(\sqrt{4\frac{L_c}{J_{av}/P_{av}} \min_{2\le m\le M} R_c w_m}\right) = 10^{-6}$$

Then,

$$2\frac{L_c}{J_{av}/P_{av}} \min_{2\le m\le M} R_c w_m = 10.5 \text{ dB}$$

or equivalently,

$$10\log_{10}(2) \text{ dB} + L_c \text{ dB} + \min_{2\le m\le M} R_c w_m \text{ dB} - (J_{av}/P_{av}) \text{ dB} = 10.5 \text{ dB}.$$

Thus,

$$3 \text{ dB} + 30 \text{ dB} + 0 \text{ dB} - (J_{av}/P_{av}) \text{ dB} = 10.5 \text{ dB} \Rightarrow (J_{av}/P_{av}) \text{ dB} = 22.5 \text{ dB}$$

□

Spectrum analysis

We now demonstrate why it is named spread spectrum system!
Assume the uncoded DSSS system, where all-zero and all-one codes are used.
Then

$$\text{channel symbol } g_s(t) = p_{\text{PN}}(t) \times c(t) + z(t)$$

where

$$c(t) = \sum_{n=-\infty}^{\infty} I_n s(t - nT_b) \text{ with } s(t) = \begin{cases} g(t \bmod T_c) & 0 \le t < T_b \\ 0 & \text{otherwise} \end{cases}$$

and

$$\{I_n \in \{\pm 1\}\}_{n=-\infty}^{\infty} \text{zero-mean i.i.d.}$$

From Slide 3-117,

$$\bar{S}_c(f) = \frac{1}{T_b} S_I(f) |S(f)|^2 = \frac{1}{T_b} |S(f)|^2$$

where $S_I(f) = \sum_{k=-\infty}^{\infty} R_I(k) e^{-\imath 2\pi k f T_b} = 1$.

Assume $g(t)$ rectangular pulse of height $1/\sqrt{T_b}$ and duration T_c (hence, $\int_0^{T_b} s^2(t)dt = 1$). Then (cf. Slide 12-31 by replacing T_b with T_c and letting $\mathcal{E} = 1/2$),

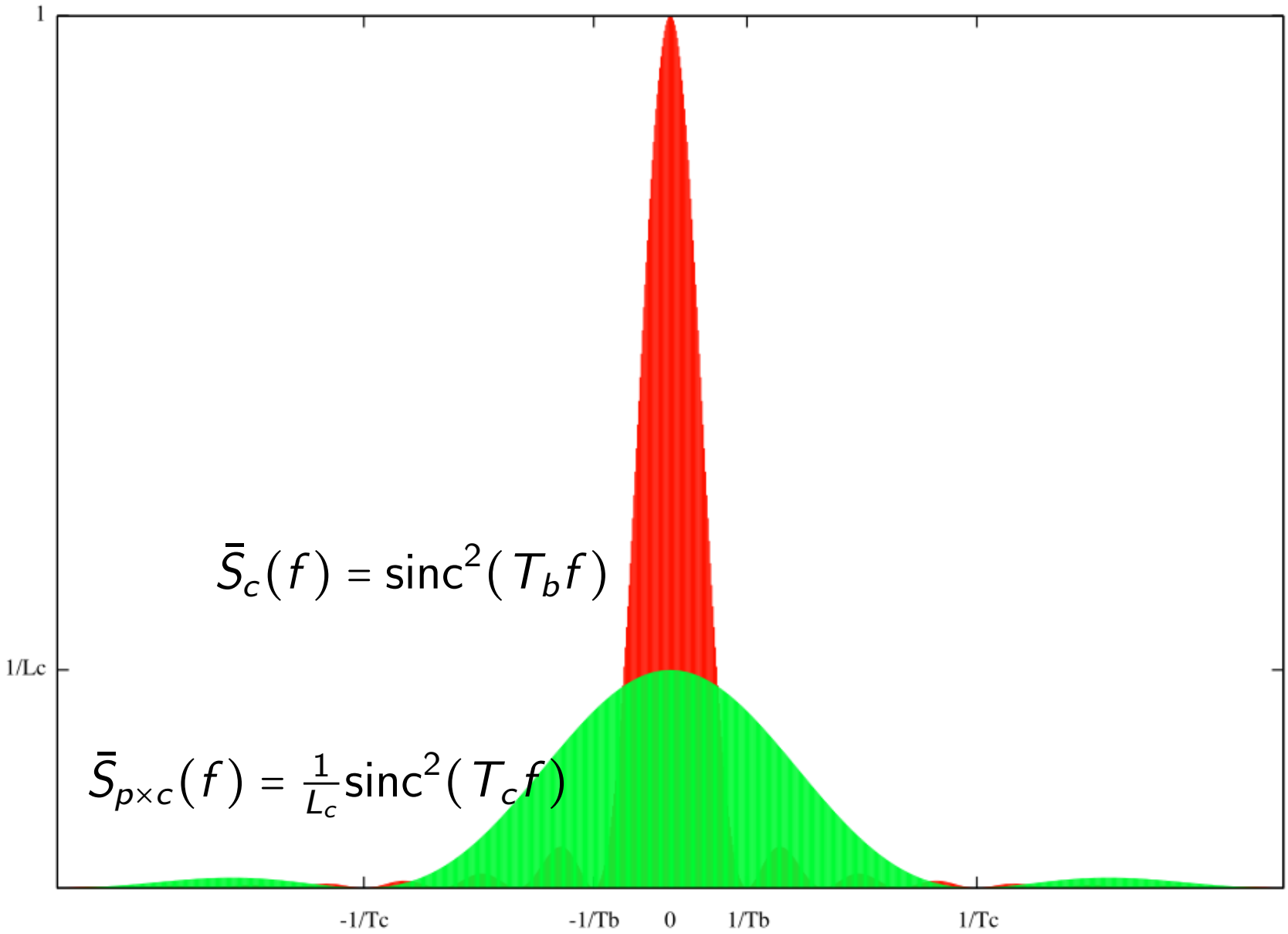
$$\boxed{\bar{S}_c(f) = \frac{1}{T_b}\left(T_b \text{sinc}^2(T_b f)\right) = \text{sinc}^2(T_b f)}$$

Similarly,

$$\begin{aligned} p_{\text{PN}}(t)c(t) &= \sum_{i=-\infty}^{\infty} (2b_i - 1)p(t - iT_c)I_{\lfloor i/n \rfloor}s(t - \lfloor i/n \rfloor T_b) \\ &\overset{d}{=} \sqrt{\frac{T_c}{T_b}} \sum_{i=-\infty}^{\infty} (2b_i - 1)\frac{1}{\sqrt{T_c}}p(t - iT_c) \end{aligned}$$

where here $\{2b_i - 1\}_{i=1}^{\infty}$ and $\{(2b_i - 1)I_{\lfloor i/n \rfloor}\}_{i=1}^{\infty}$ actually have the same distribution. Then from Slide 3-117,

$$\boxed{\bar{S}_{p\times c}(f) = \frac{1}{T_c}\left|\sqrt{\frac{T_c}{T_b}}\right|^2 \left|\frac{1}{\sqrt{T_c}}P(f)\right|^2 = \frac{1}{T_b}\left(T_c \text{sinc}^2(T_c f)\right) = \frac{1}{L_c}\text{sinc}^2(T_c f)}$$


1
1/Lc
$\bar{S}_c(f) = \text{sinc}^2(T_b f)$
$\bar{S}_{p\times c}(f) = \frac{1}{L_c}\text{sinc}^2(T_c f)$
-1/Tc
-1/Tb
0
1/Tb
1/Tc

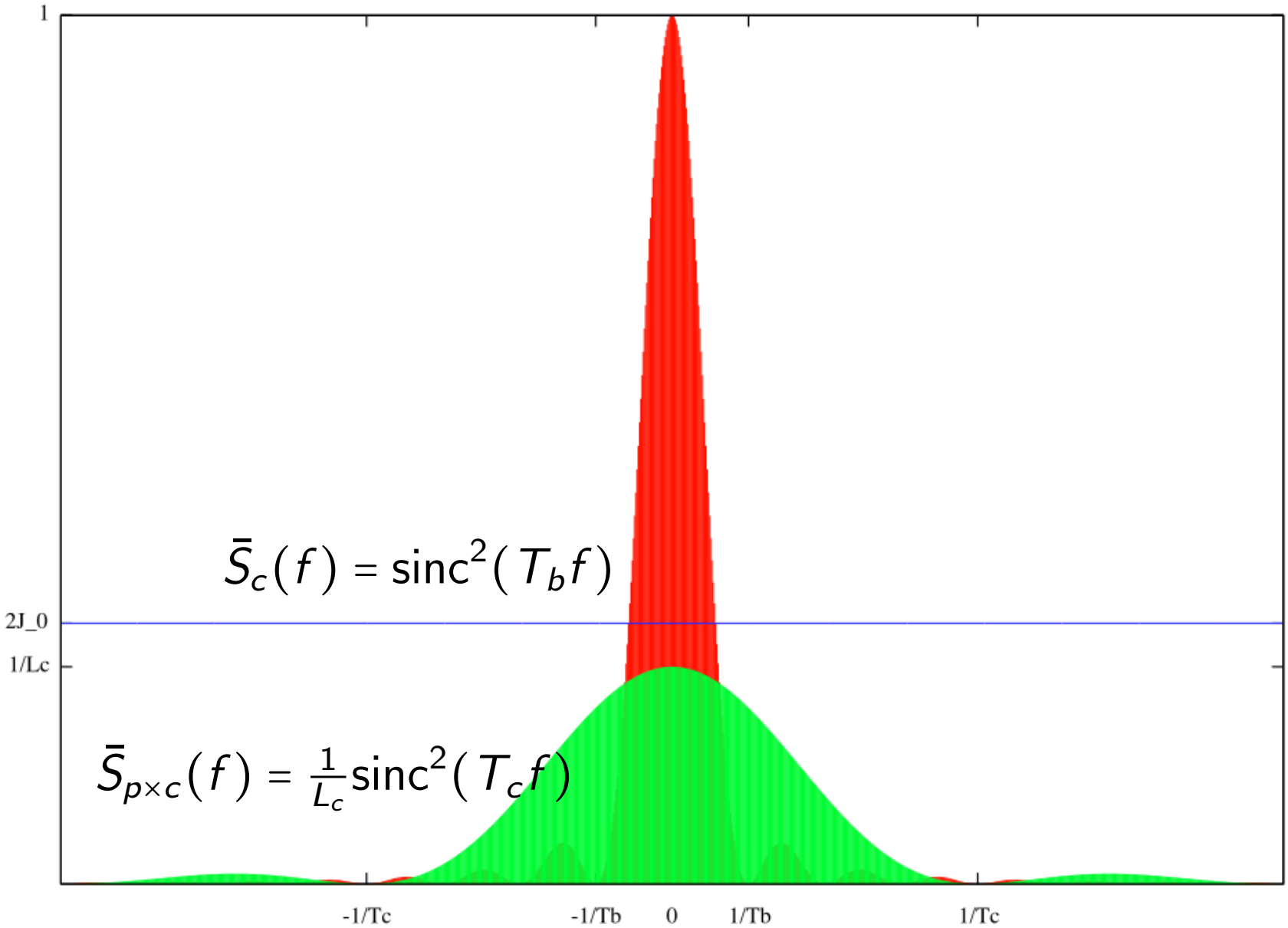
Recovered symbol at the receiver end:

$$\begin{aligned} p_{\text{PN}}(t)g_s(t) &= p_{\text{PN}}^2(t) \times c(t) + p_{\text{PN}}(t)z(t) \\ &= c(t) + p_{\text{PN}}(t)z(t) \end{aligned}$$

This indicates that for WSS $z(t)$, the PSD of the new noise $p_{\text{PN}}(t)z(t)$ is:

$$\begin{aligned} \bar{S}_{p\times z}(f) &= \bar{S}_p(f) \star S_z(f) \\ &= \int_{-\infty}^{\infty} \bar{S}_p(s) S_z(f-s) ds = 2J_0 \int_{-\infty}^{\infty} \bar{S}_p(s) ds \\ &= 2J_0 \int_{-\infty}^{\infty} \frac{1}{T_c} |P(s)|^2 ds = 2J_0 \int_{-\infty}^{\infty} T_c \text{sinc}^2(T_c s) ds \\ &= 2J_0 \end{aligned}$$

where for simplicity we let $S_z(f) = 2J_0$ for $f \in \mathbb{R}$.


1
2J_0
1/Lc
$\bar{S}_c(f) = \text{sinc}^2(T_b f)$
$\bar{S}_{p\times c}(f) = \frac{1}{L_c}\text{sinc}^2(T_c f)$
-1/Tc
-1/Tb
0
1/Tb
1/Tc

Summary

- Multiplication of $p_{\text{PN}}(t)$ = spreading the power over the bandwidth of $p_{\text{PN}}(t)$ (so that the transmitted signal could be "hidden" under the broadband interference.)
- Multiplication twice of $p_{\text{PN}}(t)$ recovers the original signal.
- The spreading fraction is approximately equal to the processing gain.

- Modulator: Transmit $p_{\text{PN}}(t)c(t)$
- Demodulator: Based on $r(t)p_{\text{PN}}(t) = c(t) + z(t)p_{\text{PN}}(t)$

Further performance enhancement by coding

$$\text{Coding gain} = \min_{2 \le m \le M} R_c w_m (\text{Recall } w_1 = 0)$$

Use (n_1, k) code as the outer code, and $(n_2, 1)$ repetition code as the inner code, where $n = n_1 n_2$.

Then

$$\begin{aligned} \text{Coding gain} &= \min_{2 \le m \le M} R_c w_m \\ &= \min_{2 \le m \le M} \frac{k}{n_1 n_2} n_2 w_m^{(out)} \\ &= \min_{2 \le m \le M} R_c^{(out)} w_m^{(out)} \end{aligned}$$

The use of the inner code here is to align the length of the outer code n_1 to the length of the PN sequence n.

Since the inner code is the binary repetition code, the bit error rate p of the outer code is the symbol error rate of the inner code, where under broadband interference,

$$p = Q\left(\sqrt{2R_c^{(in)}\gamma_b^{(in)}w_2^{(in)}}\right)$$

For $M = 2$, we have "equality", not "$\leq$."

$$= Q\left(\sqrt{2\frac{1}{n_2}\frac{n_2\mathcal{E}_c}{J_0}n_2}\right) = Q\left(\sqrt{2\frac{1}{n_2}\frac{n_2(k/n)\mathcal{E}_b}{J_0}n_2}\right)$$

$$= Q\left(\sqrt{2\gamma_b R_c^{(out)}}\right) = Q\left(\sqrt{2\frac{2L_c}{J_{av}/P_{av}}R_c^{(out)}}\right). \quad \text{(cf. Slide 12-35)}$$

Then the symbol error rate of the entire system satisfies

$$P_e \leq \sum_{m=t+1}^{n_1}\binom{n_1}{m}p^m(1-p)^{n_1-m} \leq \underbrace{\sum_{m=2}^{2^k}[4p(1-p)]^{w_m/2}}_{\text{Chernoff bound}}$$

where $t = \lfloor (d_{\min}-1)/2 \rfloor$ and $d_{\min}$ is the minimum Hamming distance among outer codeword pairs.

Golay $(24, 12)$ (outer) code

Example. Use Golay $(24, 12)$ outer code and set $L_c = 100$.

- We need to first determine n_2 based on $n_1 = 24$.

$$12T_b = nT_c = n_1 n_2 T_c = 24 n_2 T_c$$
$$\Rightarrow n_2 = \frac{12T_b}{24T_c} = \frac{1}{2}L_c = \frac{1}{2}100 = 50.$$

- Then $p = Q\left(\sqrt{2\frac{2\cdot 100}{J_{av}/P_{av}}\frac{12}{24}}\right) = Q\left(\sqrt{\frac{200}{J_{av}/P_{av}}}\right)$.
-

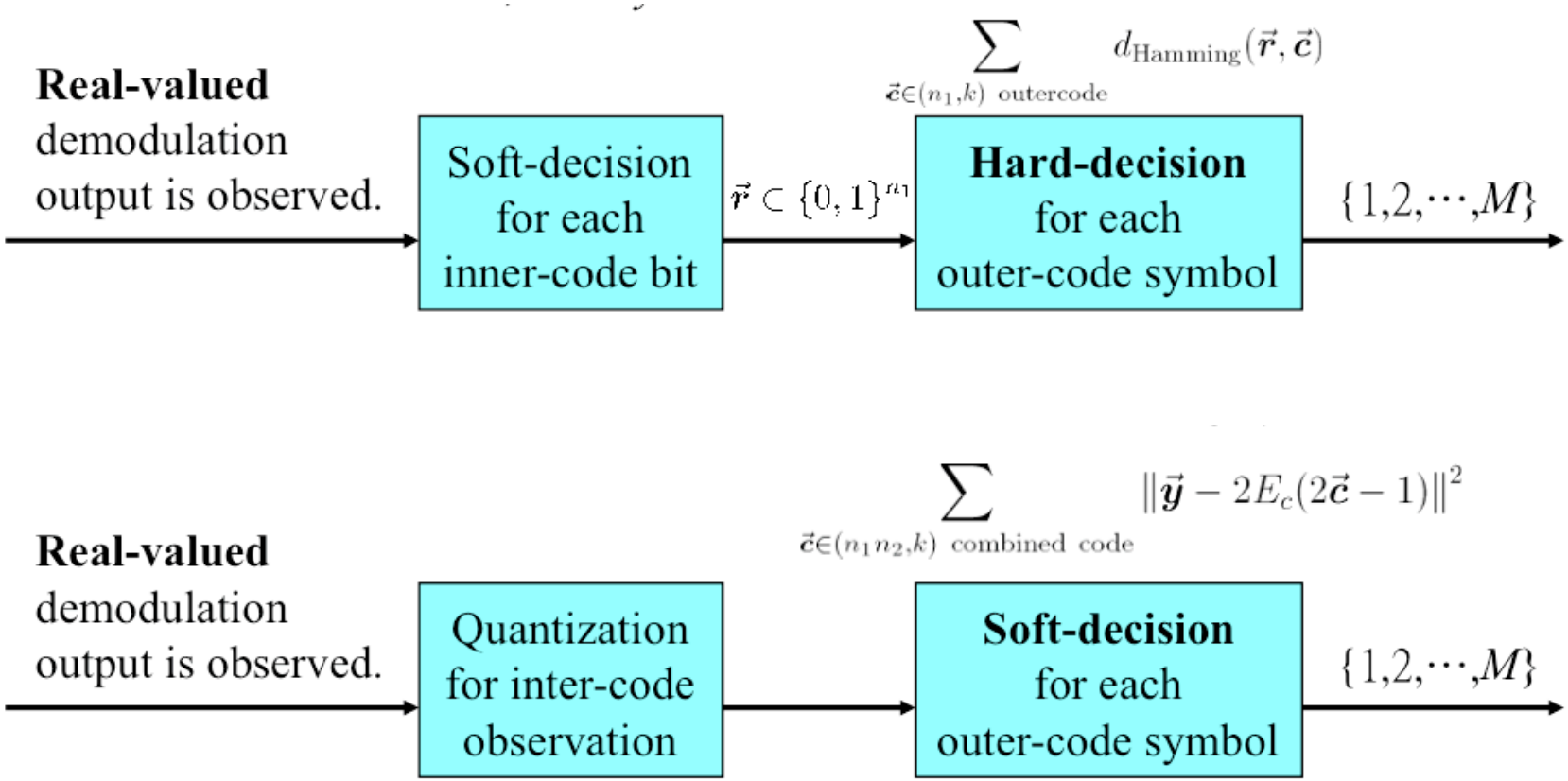
$$\begin{aligned} P_e &\leq \sum_{m=4}^{24}\binom{24}{m}p^m(1-p)^{24-m} \\ &\leq 759[4p(1-p)]^4 + 2576[4p(1-p)]^6 + 759[4p(1-p)]^8 \\ &\quad +[4p(1-p)]^{12}. \end{aligned}$$

□

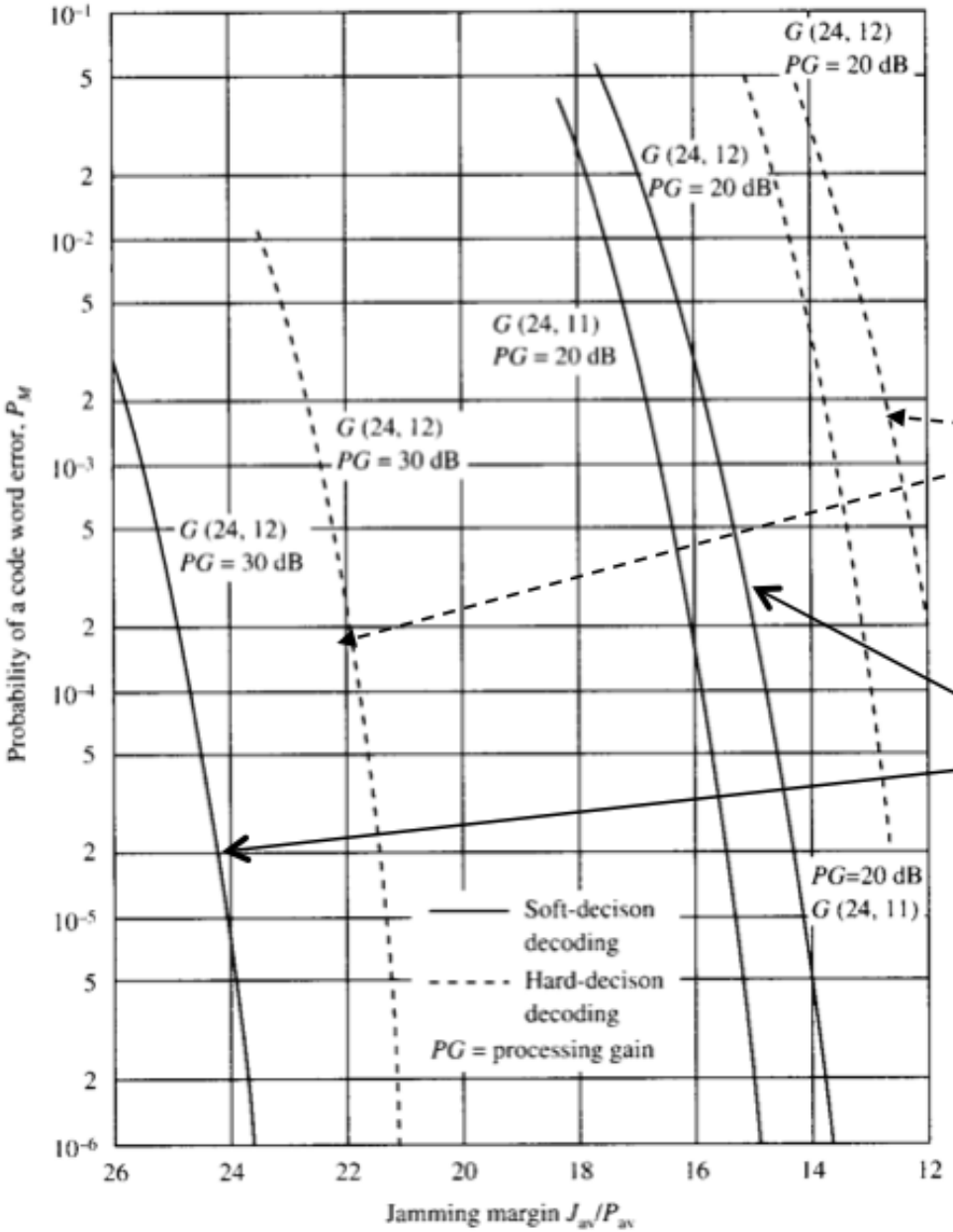
Golay $(24, 12)$ code

Weight	number of codewords
0	1
8	759
12	2576
16	759
24	1

Appendix: Hard-decision versus soft-decision



The performance usually improves 3 dB by using soft-decision.



Shift-10dB due to processing gain

Shift-10dB due to processing gain

12.2-2 Some applications of DS spread spectrum signals

Code division multiple access (CDMA)

If each user has its own PN sequence (with good properties), then many DSSS signals are allowed to occupy the same channel bandwidth.

$$r(t) = p^{(1)}(t)c^{(1)}(t) + \underbrace{p^{(2)}(t)c^{(2)}(t) + \cdots + p^{(N_u)}(t)c^{(N_u)}(t) + z(t)}_{\tilde{z}(t)}$$

$$\Rightarrow \quad p^{(1)}(t) \cdot r(t) = c^{(1)}(t) + p^{(1)}(t) \cdot \tilde{z}(t)$$

How to determine the number of users (capacity)?

- Each user is a broadband interference with power P_{av} (cf. Slide 12-8)

$$\frac{P_{av}}{J_{av}} = \frac{P_{av}}{(N_u - 1)P_{av}} = \frac{1}{N_u - 1}.$$

By this, we can obtain for $L_c = 100$ and Golay $(24, 12)$ outer code and $P_e \leq 10^{-6}$, $\boxed{N_u = 41}$. (For details, see (12.2-48) in text.)

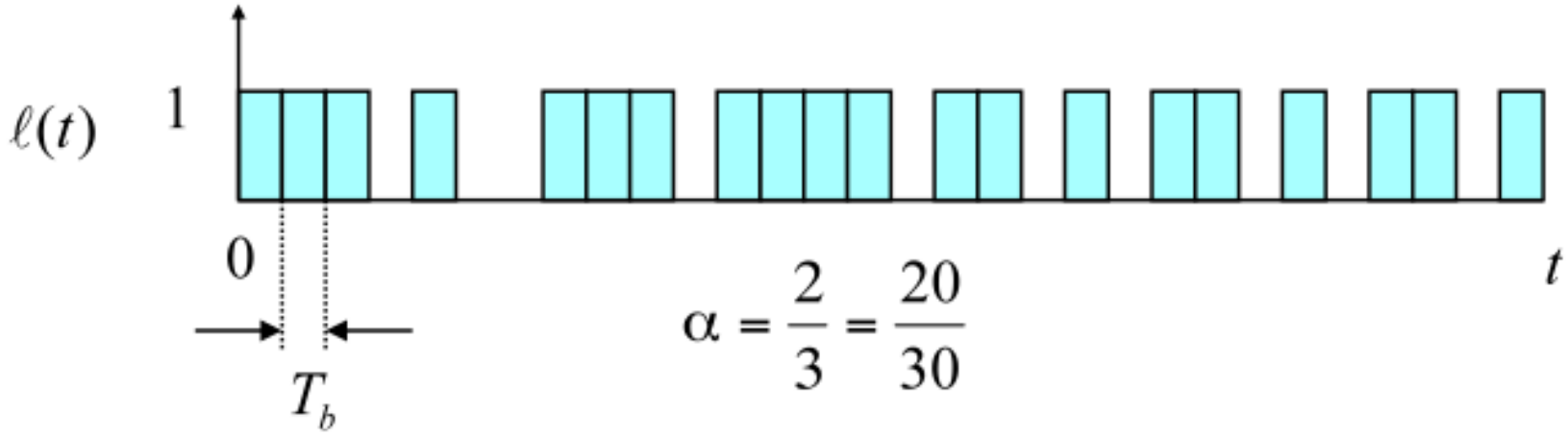
12.2-3 Effect of pulsed interference on DS spread spectrum systems

Types of interferences

- CW jammer $S_z(f) = J_{av}\delta(f)$
- Broadband interference $S_z(f) = 2J_0$ for $|f| \leq W/2$
- Pulsed interference

$$z_p(t) = z'(t)\ell(t)$$

where $z'(t)$ is a broadband interference with $S_{z'}(f) = S_z(f)/\alpha$ for some $0 < \alpha \leq 1$ and $\ell(t)$ is a 0-1-valued random pulse of duration T_b, which equals 1 with probability α.



Hence, for uncoded DSSS (no coding gain),

- when $\ell(t) = 0$, the system is error free,
- when $\ell(t) = 1$, the system suffers broadband interference with

$$\Pr[\text{error}] = Q\left(\sqrt{4\frac{L_c}{(J_{av}/\alpha)/P_{av}}}\right)$$

$$= Q\left(\sqrt{4\frac{(W/R)}{(2J_0W/\alpha)/(\mathcal{E}_bR)}}\right) = Q\left(\sqrt{2\alpha\frac{\mathcal{E}_b}{J_0}}\right)$$

The system error under pulsed interference is

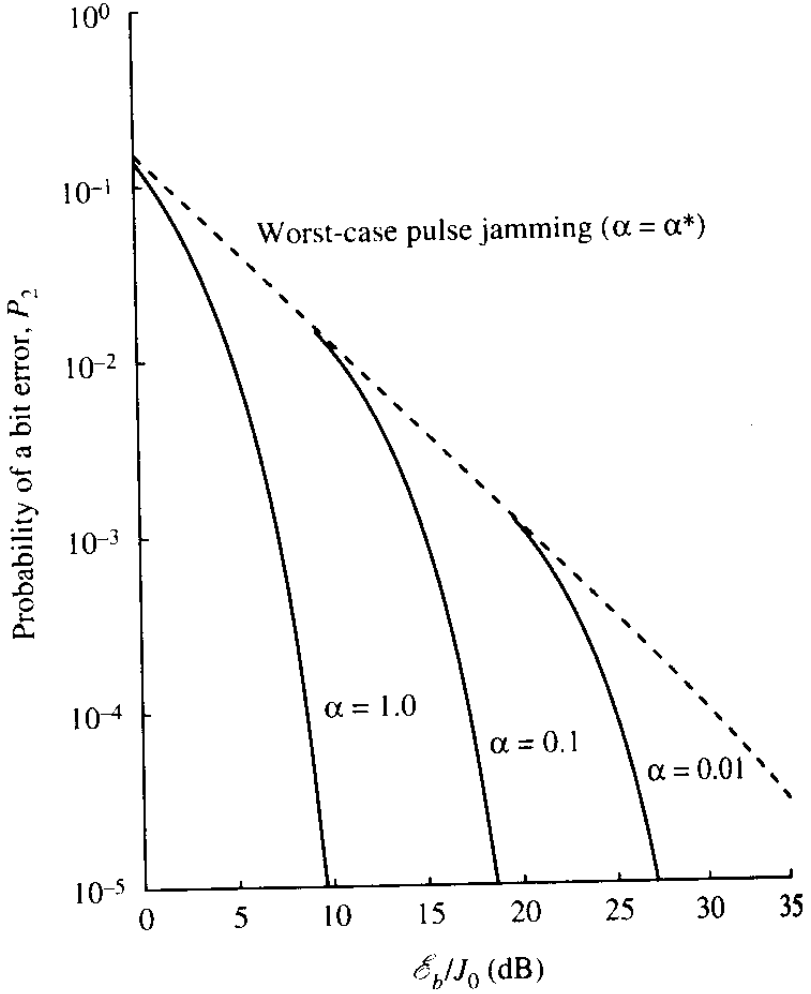
$$P_e(\alpha) = (1-\alpha)\cdot 0 + \alpha Q\left(\sqrt{2\alpha\frac{\mathcal{E}_b}{J_0}}\right) = \alpha Q\left(\sqrt{2\alpha\frac{\mathcal{E}_b}{J_0}}\right).$$

What is the α that **maximizes** P_e from an attacker's standpoint?

$$\frac{dP_e(\alpha)}{d\alpha} = 0 \Rightarrow \alpha^* = \begin{cases} \frac{0.71}{\mathcal{E}_b/J_0} & \text{if } \mathcal{E}_b/J_0 \geq 0.71 \approx -1.49\text{dB} \\ 1 & \text{if } \mathcal{E}_b/J_0 < 0.71 \end{cases}$$

and

$$P_e(\alpha^*) \begin{cases} \approx \frac{0.083}{\mathcal{E}_b/J_0} & \text{if } \mathcal{E}_b/J_0 \geq 0.71 \\ = Q\left(\sqrt{2\frac{\mathcal{E}_b}{J_0}}\right) & \text{if } \mathcal{E}_b/J_0 < 0.71 \end{cases}$$



Worst-case pulse jamming: $\alpha = \alpha^*$; hence it is not a constant on the dotted line.

Summary

- The DSSS system performs poor under burst-in-time jammer, not under burst-in-frequency jammer (CW jammer).
- For example, by comparing the error rate for continuous Gaussian noise jamming with worst-case pulse jamming, the performance difference at $P_e = 10^{-6}$ is as large as 40 dB.

Cutoff rate (Omura and Levitt, 1982)

Performance index

- Usual measure: The required SNR for a specified error rate
- Analytically convenient measure: Cutoff rate

Definition 1 (Cutoff rate)

The maximum R_0 that satisfies

$$P_e(R_c) \leq 2^{-n(R_0-R_c)} \quad \textit{i.e.,}\ R_0 \leq R_c + \Big(-\tfrac{1}{n} \log_2 P_e(R_c) \Big)$$

is called the cutoff rate, where R_c is the code rate and n is the blocklength.

Interpretation: If $R_c < R_0$, then $P_e \to 0$ as $n \to \infty$.

Sample derivation of cutoff rate

Give

$$\begin{cases} \text{Channel symbol } 1: \boldsymbol{s}_1 = [s_{1,1}, s_{1,2}, \ldots, s_{1,n}] \\ \text{Channel symbol } 2: \boldsymbol{s}_2 = [s_{2,1}, s_{2,2}, \ldots, s_{2,n}] \end{cases}$$

where $s_{m,j} = \pm\sqrt{\mathcal{E}_c}$.

From Slide 4-44,

$$P_2 = Q\left(\sqrt{\frac{d_{12}^2}{2N_0}}\right).$$

Now suppose we randomly assign each of $s_{m,j}$ independently (**random coding**) with

$$\Pr[s_{m,j} = \sqrt{\mathcal{E}_c}] = \Pr[s_{m,j} = -\sqrt{\mathcal{E}_c}] = \frac{1}{2}.$$

Then $\Pr[d_{12}^2 = 4d\mathcal{E}_c] = \binom{n}{d}2^{-n}$ for integer $0 \le d \le n$.

Using $Q(x) \le \frac{1}{2}e^{-x^2/2} \le e^{-x^2/2}$ yields:

$$\begin{aligned}
\mathbb{E}[P_2] &= \sum_{d=0}^{n}\binom{n}{d}2^{-n}Q\left(\sqrt{\frac{2d\mathcal{E}_c}{N_0}}\right) \\
&\le \sum_{d=0}^{n}\binom{n}{d}2^{-n}e^{-d\mathcal{E}_c/N_0} \\
&= 2^{-n}\left(1+e^{-\mathcal{E}_c/N_0}\right)^n \\
&= 2^{-n\left(1-\log_2\left(1+e^{-\mathcal{E}_c/N_0}\right)\right)}
\end{aligned}$$

The union bound for M-ary random code gives

$$\begin{aligned}
\mathbb{E}[P_M] &\le (M-1)\mathbb{E}[P_2] \le M\mathbb{E}[P_2] = 2^{nR_c}2^{-n\left(1-\log_2\left(1+e^{-\mathcal{E}_c/N_0}\right)\right)} \\
&= 2^{-n(\bar{R}_0-R_c)} \text{ where } \bar{R}_0 = 1-\log_2\left(1+e^{-\mathcal{E}_c/N_0}\right).
\end{aligned}$$

$$M\,\mathbb{E}[P_2] \approx 2^{nR_c}2^{-nR_0} = 2^{-n(R_0-R_c)}$$

Since $\mathbb{E}[P_M] \leq 2^{-n(\bar{R}_0 - R_c)}$, there must exist a code with

$$P_M \leq 2^{-n(\bar{R}_0 - R_c)}$$

and hence

$$R_0 \geq \bar{R}_0 = 1 - \log_2\left(1 + e^{-\mathcal{E}_c/N_0}\right).$$

As it turns out, this lower bound of cutoff rate is tight! So,

$$R_0 = \bar{R}_0.$$

□

$R_c = \frac{k}{n}$ (information) bits/chip; So R_0 is measured in bits/chip.

R_0 is usually in the shape of $1 - \log_2(1 + \Delta_\alpha)$, where

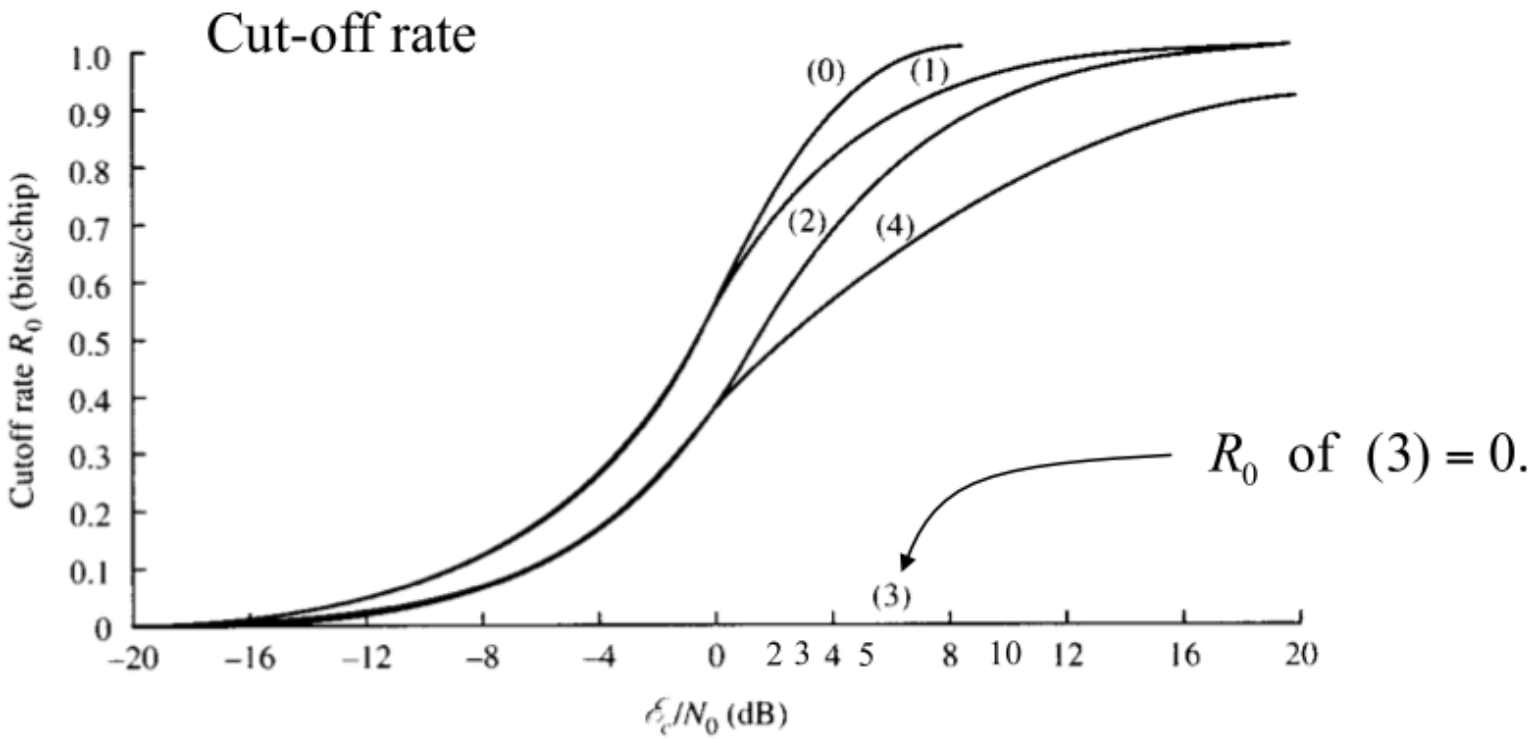
$$\Delta_\alpha = \begin{cases} e^{-\mathcal{E}_c/N_0} & \text{soft-decision decoding (as just derived)} \\ \sqrt{4p(1-p)} & \text{hard-decision decoding} \\ & \text{given } p = Q(\sqrt{2\mathcal{E}_c/N_0}) \end{cases}$$

For worst-case pulsed interference, Omura and Levitt (1982) derived

$$\Delta_\alpha = \begin{cases} \alpha e^{-\alpha \mathcal{E}_c/N_0} \\ \qquad \text{soft-decision with knowledge of jammer state} \\ \min_{\lambda \geq 0} \left\{ e^{-2\lambda \mathcal{E}_c} \left[1 - \alpha + \alpha e^{\lambda^2 \mathcal{E}_c / N_0 / \alpha} \right] \right\} \\ \qquad \text{soft-decision with no knowledge of jammer state} \\ \alpha \sqrt{4p(1-p)} \\ \qquad \text{hard-decision with knowledge of jammer state} \\ \sqrt{4\alpha p(1-\alpha p)} \\ \qquad \text{hard-decision with no knowledge of jammer state} \end{cases}$$

where $p = Q\left(\sqrt{2\alpha \mathcal{E}_c/N_0}\right)$ (and $N_0 = J_0$).

The receiver may know the jammer state (side information) by measuring the noise power level in adjacent frequency band.



Key
(0) Soft-decision decoding in AWGN ($\alpha = 1$)
(1) Soft-decision with jammer state information
(2) Hard-decision with jammer state information
(3) Soft-decision with no jammer state information
(4) Hard-decision with no jammer state information

Cutoff rate for coded DS binary PSK modulation. [*From Omura and Levitt (1982). © 1982 IEEE.*]

Observations from Omura and Levitt's results

- When $R_0 < 0.7$ bits/chip, soft-decision in AWGN (curve (0)) performs the same as soft-decision with jammer state information (curve (1)).

When **jammer state is known** under $R_0 < 0.7$, the **worse-case pulsed jammer** has no effect on **soft-decision** system performance.

- When $R_0 < 0.4$ bits/chip, hard-decision with jammer state information (curve (2)) performs the same as hard-decision with no jammer state information (curve (4)).

Under $R_0 < 0.4$, knowing the jammer state information does not help improving the **hard-decision** system performance.

Big question: Why (3) performs worse than (4)?

- Without jammer state information, the reception $\boldsymbol{y}$ is "untrustworthy."
- The soft-decision based on

$$\|\boldsymbol{y} - 2\mathcal{E}_c(2\boldsymbol{c}_m - 1)\|^2 = \sum_{i=1}^{n}(y_i - 2\mathcal{E}_c(2c_{m,i} - 1))^2$$

may eliminate the correct codeword at the time when a wrong codeword gives a slightly larger $\|\boldsymbol{y} - 2\mathcal{E}_c(2\boldsymbol{c}_{m'} - 1)\|^2$ due to one very dominant $(y_i - 2\mathcal{E}_c(2c_{m,i} - 1))^2$.

- However, the hard-decision based on

$$d_{Hamming}(\boldsymbol{r}, \boldsymbol{c}) = \sum_{i=1}^{n}(r_i \oplus c_i)$$

can limit the "dominant affection" from any single bit, and makes the decision based more on the entire receptions.

- One can use a quantizer (or a limiter) to achieve the same goal and improves the performance of the soft-decision decoding without jammer state information.

- The limiting action from quantizers or limiters ensures that any single bit does not heavily (and dominantly) bias the corresponding decision metric.

12.2-5 Generation of PN sequences

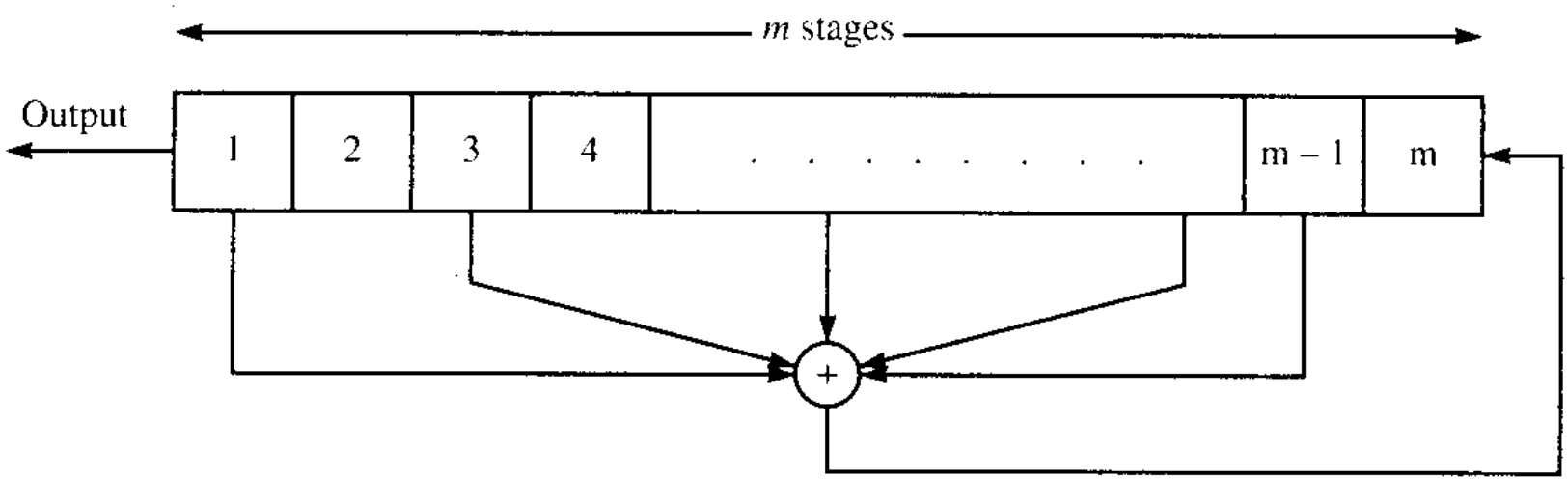
Properties of (deterministic) PN sequences

- Rule 1: Balanced property
  - Relative frequencies of 0 and 1 are each (nearly) 1/2.
- Rule 2: Run length property
  - Run length (of 0's and 1's) are as expected close to a fair-coin flipping.
  - 1/2 of run lengths are 1; 1/4 of run lengths are 2; 1/8 of run lengths are 3 ... etc.
- Rule 3: Delay and add property
  - If the sequence is shifted by any non-zero number of elements, the resulting sequence will have an equal number of agreements and disagreements with the original sequence.

Example of PN sequences

Maximum-length shift-register sequences $(n = 2^m - 1, k = m)$ code

- Also named m-sequences.

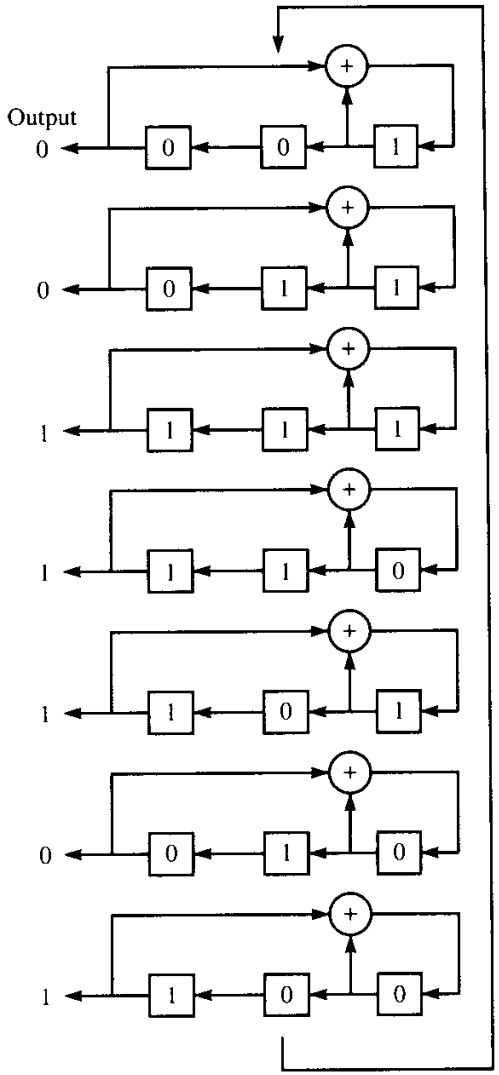


General m-stage shift register with linear feedback.

Maximum-length shift-register sequence $(n, k) = (2^m - 1, m)$

By its name, the codewords are the sequential output of m-stage shift-register with feedback.

The maximum length of codewords is $2^m - 1$ because the register contents can only have $2^m - 1$ possibilities.



MAXIMUM-LENGTH SHIFT-REGISTER CODE FOR $m = 3$

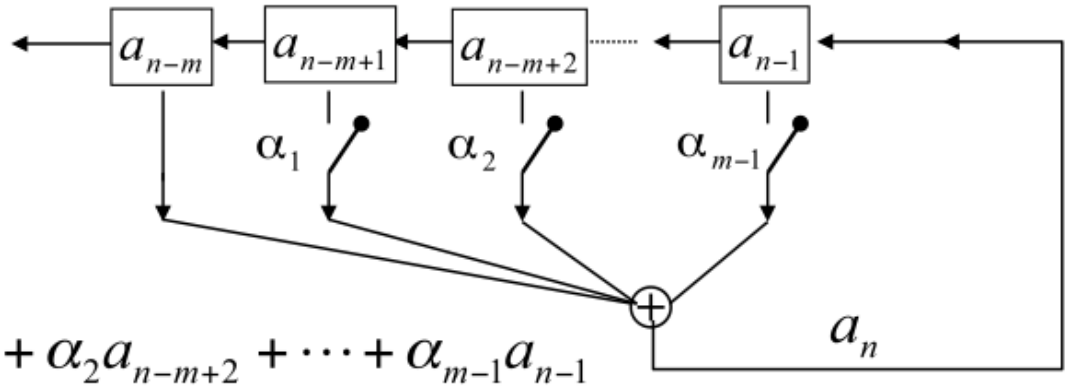
Information bits			Code words						
0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	1	1	1	0	1
0	1	0	0	1	0	0	1	1	1
0	1	1	0	1	1	1	0	1	0
1	0	0	1	0	0	1	1	1	0
1	0	1	1	0	1	0	0	1	1
1	1	0	1	1	0	1	0	0	1
1	1	1	1	1	1	0	1	0	0

Polynomial representation of m-sequences

The code can be specified by

$$g(p) = 1 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_{m-1} p^{m-1} + p^m$$

based on its structure.



$$a_n = a_{n-m} + \alpha_1 a_{n-m+1} + \alpha_2 a_{n-m+2} + \cdots + \alpha_{m-1} a_{n-1}$$

Vulnerability of m-sequences

Suppose the enemy knows the number of shift registers, m.

Then $(2m-1)$ observations are sufficient to determine $\alpha_1, \alpha_2, \ldots, \alpha_{m-1}$.

$$\begin{cases} a_{m+1} &= a_1 + \alpha_1 a_2 + \cdots + \alpha_{m-1} a_m \\ a_{m+2} &= a_2 + \alpha_1 a_3 + \cdots + \alpha_{m-1} a_{m+1} \\ & \vdots \\ a_{2m-1} &= a_{m-1} + \alpha_1 a_m + \cdots + \alpha_{m-1} a_{2m-2} \end{cases}$$

Possible solutions:

- Frequent change of $(\alpha_1, \alpha_2, \ldots, \alpha_{m-1})$.
- Combination of several m-sequences in a nonlinear way (without changing the necessary properties).

Periodic autocorrelation and crosscorrelation function

Periodic autocorrelation function

$$R_b(j) = \sum_{i=1}^{n} (2b_i - 1)(2b_{i+j} - 1)$$

Periodic crosscorrelation function

$$R_{b\hat{b}}(j) = \sum_{i=1}^{n} (2b_i - 1)(2\hat{b}_{i+j} - 1)$$

For m-sequences:

$$R_b(j) = \begin{cases} n & j = 0 \\ -1 & 1 \le j < n \end{cases}$$ but $R_{b\hat{b}}(j)$ may be large !

PEAK CROSS-CORRELATION OF m SEQUENCES AND GOLD SEQUENCES

m	$n = 2^m - 1$	Number of m sequences	Peak cross-correlation ϕ_{max}	$\phi_{max}/\phi(0)$	$t(m)$	$t(m)/\phi(0)$
3	7	2	5	0.71	5	0.71
4	15	2	9	0.60	9	0.60
5	31	6	11	0.35	9	0.29
6	63	6	23	0.36	17	0.27
7	127	18	41	0.32	17	0.13
8	255	16	95	0.37	33	0.13
9	511	48	113	0.22	33	0.06
10	1023	60	383	0.37	65	0.06
11	2047	176	287	0.14	65	0.03
12	4095	144	1407	0.34	129	0.03

Relatively large!!

Although it is possible to select a small subset of m-sequences that have relatively smaller cross-correlation peak values, the number of sequences in the set is usually too small for CDMA applications.

PEAK CROSS-CORRELATION OF m SEQUENCES AND GOLD SEQUENCES

m	$n = 2^m - 1$	Number of m sequences	Peak cross-correlation ϕ_{max}	$\phi_{max}/\phi(0)$	$t(m)$	$t(m)/\phi(0)$
3	7	2	5	0.71	5	0.71
4	15	2	9	0.60	9	0.60
5	31	6	11	0.35	9	0.29
6	63	6	23	0.36	17	0.27
7	127	18	41	0.32	17	0.13
8	255	16	95	0.37	33	0.13
9	511	48	113	0.22	33	0.06
10	1023	60	383	0.37	65	0.06
11	2047	176	287	0.14	65	0.03
12	4095	144	1407	0.34	129	0.03

Gold sequences (Gold 1967-1968)

Gold and Kasami proved that there exist certain pairs of m-sequences with crosscorrelation function taking values in $\{-1, -t(m), t(m)-2\}$, where

$$t(m) = \begin{cases} 2^{(m+1)/2}+1 & m \text{ odd} \\ 2^{(m+2)/2}+1 & m \text{ even} \end{cases}$$

Example. Gold sequence with $m = 10$.

- Periodic crosscorrelation function values

$$\{-1, -2^{(m+2)/2} - 1, 2^{(m+2)/2} - 1\} = \{-1, -65, 63\}$$

PEAK CROSS-CORRELATION OF m SEQUENCES AND GOLD SEQUENCES

m	$n = 2^m - 1$	Number of m sequences	Peak cross-correlation ϕ_{max}	$\phi_{max}/\phi(0)$	$t(m)$	$t(m)/\phi(0)$
3	7	2	5	0.71	5	0.71
4	15	2	9	0.60	9	0.60
5	31	6	11	0.35	9	0.29
6	63	6	23	0.36	17	0.27
7	127	18	41	0.32	17	0.13
8	255	16	95	0.37	33	0.13
9	511	48	113	0.22	33	0.06
10	1023	60	383	0.37	65	0.06
11	2047	176	287	0.14	65	0.03
12	4095	144	1407	0.34	129	0.03

Generation of Gold sequences

- Two m-sequences with periodic crosscorrelation function in $\{-1, -t(m), t(m)-2\}$ are called **preferred sequences**.
  - Existence of two preferred sequences has been proved by Gold and Kasami.
- Let $[a_1, a_2, \ldots, a_n]$ and $[b_1, b_2, \ldots, b_n]$ be the selected preferred sequences. Then

$$\text{Gold sequences} = \left\{ \begin{array}{c} [a_1, a_2, \ldots, a_n] \\ [b_1, b_2, \ldots, b_n] \\ [a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_{n-1} \oplus b_{n-1}, a_n \oplus b_n] \\ [a_1 \oplus b_2, a_2 \oplus b_3, \ldots, a_{n-1} \oplus b_n, a_n \oplus b_1] \\ \vdots \\ [a_1 \oplus b_n, a_2 \oplus b_1, \ldots, a_{n-1} \oplus b_{n-2}, a_n \oplus b_{n-1}] \end{array} \right\}$$

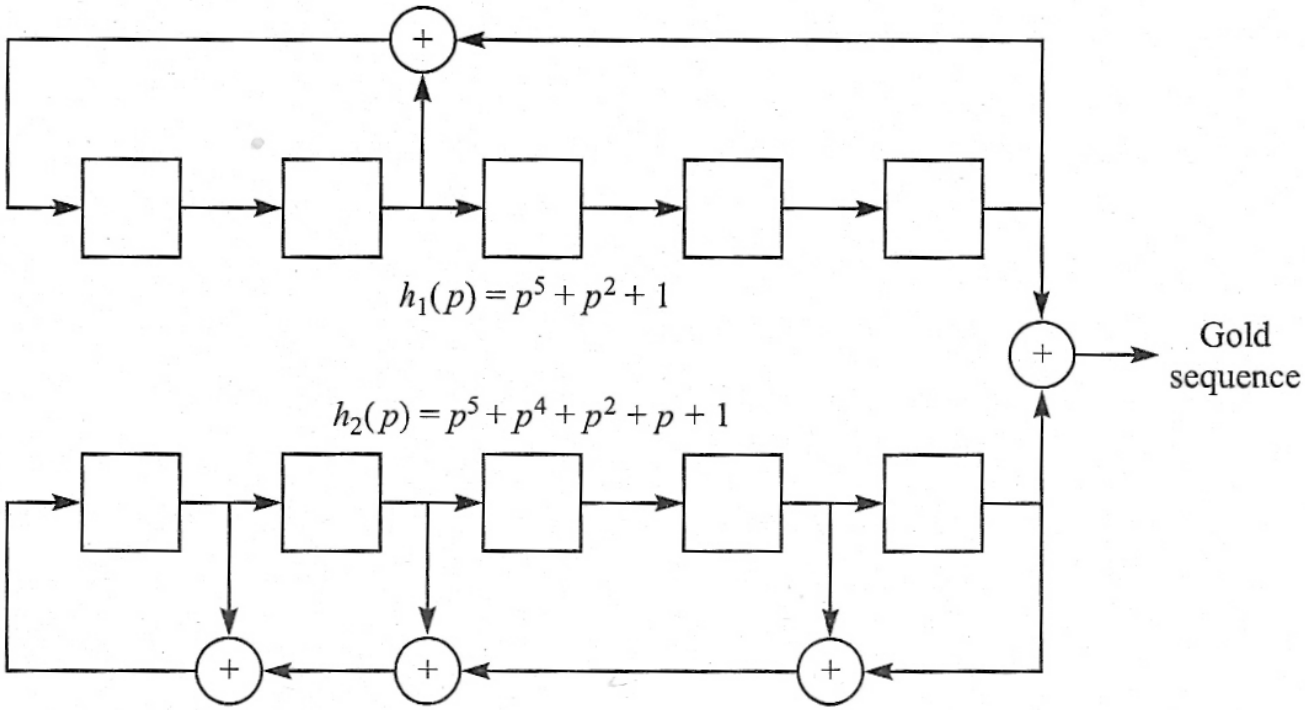
This gives $(n+2)$ Gold sequences in which some of them are no longer maximal length sequences. The autocorrelation function values are also in $\{-1, -t(m), t(m)-2\}$.

Example.

Construct $n = 31$ Gold sequences.

- Select two preferred sequences:

$$\begin{cases} g_1(p) = 1 + p^2 + p^5 \\ g_2(p) = 1 + p + p^2 + p^4 + p^5 \end{cases}$$



Welch bound

Theorem 1

Give a set of M binary sequences of length n. Then the peak crosscorrelation function value among them is lower-bounded by

$$n\sqrt{\frac{M-1}{Mn-1}}$$

- When $M \gg 1$,

$$n\sqrt{\frac{M-1}{Mn-1}} \approx n\sqrt{\frac{M}{Mn}} = \sqrt{n}.$$

- For Gold sequences ($n = 2^m - 1$),

$$\text{peak cross} = t(m) = \begin{cases} 2^{(m+1)/2} + 1 & m \text{ odd} \\ 2^{(m+2)/2} + 1 & m \text{ even} \end{cases}$$

$$= \begin{cases} \sqrt{2} \cdot \sqrt{2^m} + 1 & m \text{ odd} \\ 2 \cdot \sqrt{2^m} + 1 & m \text{ even} \end{cases}$$

$$= \begin{cases} \sqrt{2}\sqrt{n+1} + 1 & m \text{ odd} \\ 2 \cdot \sqrt{n+1} + 1 & m \text{ even} \end{cases}$$

Therefore, Gold sequences do not achieve the Welch bound.

Kasami sequences

- A set of $M = 2^{m/2}$ sequences of length $n = 2^m - 1$ for any m even.
- It is formed by the following procedure.
  1. Pick an m-sequence $\boldsymbol{a} = [a_1, a_2, \ldots, a_n]$.
  2. Since $n = 2^m - 1 = (2^{m/2} - 1)(2^{m/2} + 1)$, we can fragament $\boldsymbol{a}$ into $(2^{m/2} + 1)$-bit blocks.

$$[\underbrace{a_1, \ldots, a_{2^{m/2}+1}}_{\text{block 1}}, \underbrace{a_{2^{m/2}+2}, \ldots, a_{2(2^{m/2}+1)}}_{\text{block 2}}, a_{2\cdot 2^{m/2}+3}, \ldots]$$

  3. Let

$$\boldsymbol{b} = [a_k, a_{2k}, \ldots, a_{(2^{m/2}-1)k}, a_k, a_{2k}, \ldots, a_{(2^{m/2}-1)k}, \ldots]$$

  where $k = 2^{m/2} + 1$.

$$\text{Kasami sequences} = \left\{ \begin{array}{c} [a_1, a_2, \ldots, a_n] \\ [a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n] \\ [a_1 \oplus b_2, a_2 \oplus b_3, \ldots, a_n \oplus b_1] \\ \vdots \\ [a_1 \oplus b_{2^{m/2}-1}, a_2 \oplus b_{2^{m/2}}, \ldots, a_n \oplus b_{2^{m/2}-2}] \end{array} \right\}$$

The off-peak autocorrelation and crosscorrelation function values are in $\{-1, -(2^{m/2}+1), 2^{m/2}-1\}$ and the Welch bound is achieved (at a price of much less number of sequences, i.e., $\sqrt{n+1} = 2^{m/2}$, can be used!)

What you learn from Chapter 12

- Fundamental of spread spectrum technology
  - broadband interference versus narrowband interference
  - CW jammer
- Direct sequence spread spectrum
  - Basic structure with encoder and modulo-2 adder
  - Performance analysis under broadband interference, narrowband interference and CW jammer
  - Union bound (definitions of jamming margin, processing gain and coding gain)
- Performance enhancement from coding gain
  - Soft decision versus hard decision
- Pulsed interference – worst case pulse jammer

What you learn from Chapter 12

- Cut-off rate and its operational meaning and implication (for soft decision without jammer state info)
- Generation of PN sequences
  - *m* sequence, Gold sequence, Kasami sequences, Welch bound
  - Periodic autocorrelation and crosscorrelation function