Wireless Networks:
Physical Layer: Modulation, FEC

Guevara Noubir

Noubir@ccs.neu.edu

Lecture focus

- Modulation techniques
- Bit Error Rate
- Reducing the BER
- Forward Error Correction
  - Block codes
  - Convolutional codes

Modulation

- What is modulation?
  - Mapping a digital sequence of information bits into an analog signal suitable for transmission over the communication medium (channel)
  - Process during which the amplitude, frequency, or the phase of a carrier changes in accordance with the information to be transmitted
  - Modulation associates each n bits to a signal $S_i(t)$ chosen among $M = 2^n$ signals
- Baseband transmission versus carrier modulation transmission
  - Baseband: signal within $[0, f_s]$ (e.g., cable)
  - Carrier modulation: signal within $[f-f_s, f+f_s]$
- Basic modulation schemes:
  - Amplitude modulation, Phase modulation, Frequency modulation

Fourier Transforms

- Any function $s(t)$ can be represented as a superposition of complex sinusoids of weight: $S(f)$
  - Fourier transform $$S(f) = \int_{-\infty}^{+\infty} s(t) e^{-j2\pi ft} \mathrm{d}t$$
  - Inverse Fourier transform $$s(t) = \int_{-\infty}^{+\infty} S(f) e^{j2\pi ft} \mathrm{d}f$$
- *Cos* and *Sin* are orthogonal => can be used to independently modulate 2 sequences of symbols => I (In-phase) and Q (Quadrature phase) channels

Modulation Schemes

- Analog:
  - Amplitude modulation
  - Frequency modulation
- Main digital modulation schemes:
  - Amplitude modulation:
    - On-Off Keying (OOK): simplest modulation scheme (AM): carrier amplitude is 1 or 0 depending on the value of the information to be transmitted
    - Pulse Amplitude Modulation (PAM): use $M = 2^m$ amplitudes
  - Frequency-Shift Keying (FSK):
    - BFSK: use two different tones (frequencies) f_0, f_1. Use f_0 to transmit a 0 information bit, and f_1 to transmit an information bit equal to 1
    - MFSK: generalized to $M = 2^m$ frequencies to transmit m bits simultaneously
  - Phase-Shift Keying (PSK):
    - BPSK: use two signals shifted by 180 degrees: s_0, and s_1
    - MPSK: use signals with different phases and amplitudes: QPSK etc.

Modulation Schemes

- Phase Shift Keying:

$$s_i(t) = \sqrt{\frac{2E}{T}} \cos[w_0 t + \phi_i(t)]$$

$$0 \le t \le T; i = 1,.., M; \phi_i(t) = \frac{2\pi i}{M}$$

- Frequency Shift Keying:

$$s_i(t) = \sqrt{\frac{2E}{T}} \cos[w_i t + \phi]$$

$$0 \le t \le T; i = 1,.., M$$

- Amplitude Shift Keying:

$$s_i(t) = \sqrt{\frac{2E_i}{T}} \cos[w_0 t + \phi]$$

$$0 \le t \le T; i = 1,.., M$$

- Amplitude Phase Keying:

$$s_i(t) = \sqrt{\frac{2E_i}{T}} \cos[w_0 t + \phi_i(t)]$$

$$0 \le t \le T; i = 1,.., M$$

Choosing the Modulation Scheme

- Compactness of the power spectrum density: minimize interference on adjacent channels (60-80dB)
- Good performance in terms of BER
- Envelope properties: constant envelope to avoid problems caused by non-linear amplifiers

Additive White Gaussian Noise

- Noise:
  - As previously seen, noise has several sources
  - Thermal noise source is the motion of electrons in amplifiers and circuits
  - Its statistics were determined using quantum mechanics
  - It is flat for all frequencies up to 10^{12}Hz.
  - We generally call it: Additive White Gaussian Noise (AWGN)
  - Its probability density function (pdf) (zero mean noise voltage): $$p(n) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{n}{\sigma} \right)^2 \right]$$

Bit Error Rate [Sklar1988]

- BER for coherently detected BPSK:

$$P_B = \int_{\sqrt{2E_b/N_0}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{u^2}{2}) du$$

$$P_B = Q(\sqrt{2E_b / N_0})$$

- BER for coherently detected BFSK:

$$P_B = \int_{\sqrt{E_b/N_0}}^{\infty} \frac{1}{\sqrt{2\pi}} \exp(-\frac{u^2}{2}) du$$

$$P_B = Q(\sqrt{E_b / N_0})$$

Error Control

- Two main techniques:
  - Forward Error Correction
  - Automatic Repeat reQuest
- In practice:
  - Combinations: Hybrid ARQ I and Hybrid ARQ II

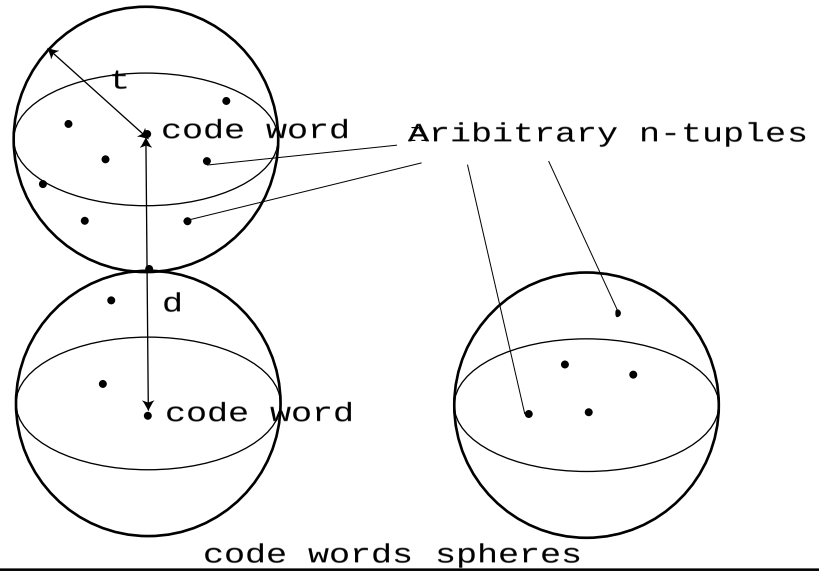
- ARQ:
  - Stop&Wait, GoBackN, Selective Repeat
- FEC:
  - Block codes, convolutional codes

Block Codes

- Information bits (word):
  - $u = (u_1, u_2, \ldots, u_k)$
- Code word ($n>k$):
  - $v = (v_1, v_2, \ldots, v_n)$
- Systematic versus non-systematic
- Binary versus Non-Binary
- Use of codes:
  - Error detection, error correction, erasure correction
  - How to build codes with high error correction capability?
- Examples:
  - Hamming code, BCH codes, RS codes

Hamming Distance for Block Codes

- The Hamming distance between two code words is the number of places where they differ
- The Hamming distance *d* of a Block code is the minimum distance between two code words
- Error Detection:
  - Upto *d*-1 errors
- Error Correction:
  - Upto $\left\lfloor \frac{d-1}{2} \right\rfloor$
- Combine: $d \geq 2\lambda + l + 1$



Coding Gain

- Definition:
  - The coding gain is the amount of additional SNR that would be required to provide the same BER performance for an uncoded signal

- If the code is capable of correcting at most t errors and P_{UC} is the BER of the channel without coding, then the probability that a bit is in error using coding is:

$$P_{CB} \cong \frac{1}{n} \sum_{i=t+1}^{n} i \binom{n}{i} P_{UC}^{i} (1 - P_{UC})^{n-i}$$

Example of Binary Block Code (7, 4)

- Any two different code words are different on at least three different coordinates. This code has Hamming distance 3.

Message block	Code word
(0 0 0 0)	(0 0 0 0 0 0 0)
(1 0 0 0)	(1 1 0 1 0 0 0)
(0 1 0 0)	(0 1 10 1 0 0)
(1 1 0 0)	(1 0 1 1 1 0 0)
(0 0 1 0)	(1 1 1 0 0 1 0)
(1 0 1 0)	(0 0 1 1 0 1 0)
(0 1 1 0)	(1 0 0 0 1 1 0)
(1 1 1 0)	(0 1 0 1 1 1 0)
(0 0 0 1)	(1 0 1 0 0 0 1)
(1 0 0 1)	(0 1 1 1 0 0 1)
(0 1 0 1)	(1 1 0 0 1 0 1)
(1 1 0 1)	(0 0 0 1 1 0 1)
(0 0 1 1)	(0 1 0 0 0 1 1)
(1 0 1 1)	(1 0 0 1 0 1 1)
(0 1 1 1)	(0 0 1 0 1 1 1)
(1 1 1 1)	(1 1 1 1 1 1 1)

- Notice that the last 4 bits of the code word are the same as the message
  - This is a systematic coding
  - The other 3 bits are redundancy bits

Linear Block

- A block code of length n and 2^k code words is called a *linear* (n, k) code *iff* its 2^k code words form a k-dimensional subspace of the vector space of all n-tuples over the field GF(2)
- Informal Meaning: linear combinations of codewords are also codewords
- The linear code is completely specified by k independent codewords (G generator matrix)
- The encoder needs only to store the matrix G
- Example: Linear code (7, 4)

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- To encode $\boldsymbol{u}$ = (1 1 0 1): $\boldsymbol{v} = 1g_0 + 1g_1 + 0g_2 + 1g_3$

Parity-Check Matrix (H)

- For every *k*x*n* generator matrix *G* (with *k* linearly independent rows), there exists a (*n*-*k*)x*n* matrix *H* (with (*n*-*k*) linearly independent rows) called *parity check matrix* such that: any vector in the row space of *G* is orthogonal to any row of *H* and any vector that is orthogonal to all the rows of *H* is in the row space of *G:*

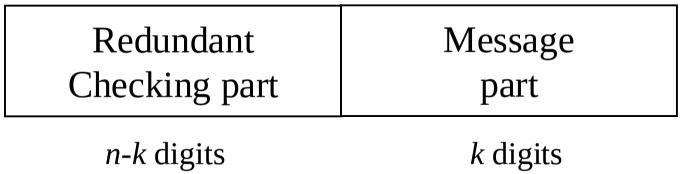
$$v = uG \Leftrightarrow vH^T = 0$$

- The 2^{n-k} combinations of the rows of *H* form an (*n*-*k*)-dimensional subspace. It is the null space of *C* the (*n*, *k*) code generated by *G*. It is called the dual space of *C* and noted C_d.

- For any $\boldsymbol{v}$ in *C* and $\boldsymbol{w}$ in C_d we have $\boldsymbol{v}\,\boldsymbol{w} = \boldsymbol{0}$

Systematic Coding

- A linear block code is called systematic *iff* the code words can be divided into two parts: *Message part* (*k* bits), and a *redundancy checking part* (*n-k* bits)



- Systematic code generator matrix: $G = [P\ I_k]$; $H = [I_{n-k}\ P^T]$; $GH^T = 0$

$$G = \begin{bmatrix} g_0 \\ g_1 \\ \cdot \\ \cdot \\ \cdot \\ g_{k-1} \end{bmatrix} = \left[\begin{array}{ccccc|cccccc} p_{0,0} & p_{0,1} & p_{0,2} & \cdots & p_{0,n-k-1} & 1 & 0 & 0 & . & . & 0 \\ p_{1,0} & p_{1,1} & p_{1,2} & \cdots & p_{1,n-k-1} & 0 & 1 & 0 & . & . & 0 \\ p_{2,0} & . & . & & p_{2,n-k-1} & 0 & 0 & 1 & . & . & 0 \\ . & . & . & & . & . & . & . & . & . & . \\ . & . & . & & . & . & . & . & . & . & . \\ p_{k-1,0} & p_{k-1,1} & p_{k-1,2} & \cdots & p_{k-1,n-k-1} & 0 & 0 & 0 & . & . & 1 \end{array}\right]$$

P: $kx(n-k)$ parity matrix; kxk identity matrix

Hamming Codes (2^m-1, 2^m-m-1)

- Parameters of Hamming codes (m>2):
  - Code length: $n = 2^m$-1
  - Number of information bits: $k = 2^m$-m-1
  - Number of parity check bits: n-$k = m$
  - Minimum distance: 3
  - Error-correcting capability: $t = \lfloor (3\text{-}1)/2 \rfloor = 1$

- Parity check matrix of a Hamming code: $H = [I_m \; Q]$
  - I_m is the identity matrix mxm
  - Q consists of 2^m-m-1 columns which are the m-tuples of weight 2 or more
  - Example:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Minimum Distance of Block Codes

- The minimum distance d_{min} of a block code is the minimum distance between any two code words:
  - $d_{min} = \min \{d(\boldsymbol{v}, \boldsymbol{w}), s.t.\ \boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{C}, \boldsymbol{v} \neq \boldsymbol{w}\}$
  - $d_{min} = \min \{w(\boldsymbol{v} + \boldsymbol{w}), s.t.\ \boldsymbol{v}, \boldsymbol{w} \in \boldsymbol{C}, \boldsymbol{v} \neq \boldsymbol{w}\}$
  - $d_{min} = \min \{w(\boldsymbol{x}), s.t.\ \boldsymbol{x} \in \boldsymbol{C}, \boldsymbol{x} \neq \boldsymbol{0}\}$ (because C is a vector sub-space)
- Example: Minimum Distance of Hamming Codes?

Cyclic Block Codes

- Definition:
  - An (n, k) linear code C is called a *cyclic code* if every cyclic shift of a code vector in C is also a code vector
  - Codewords can be represented as polynomials of degree n. For a cyclic code all codewords are multiple of some polynomial $g(X)$ modulo X^n+1 such that $g(X)$ divides X^n+1. $g(X)$ is called the generator polynomial.
- Examples:
  - Hamming codes, Golay Codes, BCH codes, RS codes
  - BCH codes were independently discovered by Hocquenghem (1959) and by Bose and Chaudhuri (1960)
  - Reed-Solomon codes (non-binary BCH codes) were independently introduced by Reed-Solomon

Systematic Cyclic Codes

- Data bits: $s_{K-1}, s_{K-2}, \ldots, s_1, s_0$
- Polynomial representation:

$$S(X) = s_{K-1}X^{K-1} + s_{K-2}X^{K-2} + \ldots + s_1X + s_0$$

- The CRC is also viewed as a polynomial:

$$C(X) = c_{L-1}X^{L-1} + c_{L-2}X^{L-2} + \ldots + c_1X + c_0$$

- The transmitted frame can be represented as:

$$V(X) = s(X)X^L + c(X)$$

$$V(X) = s_{K-1}X^{L+K-1} + \ldots + s_0X^L + c_{L-1}X^{L-1} + c_{L-2}X^{L-2} + \ldots + c_1X + c_0$$

Systematic Cyclic Codes

- The CRC is the remainder of dividing the information polynomial $S(D)$ by a generator polynomial $g(D)$.

$$c(D) = \text{Remainder}[\frac{s(D)D^L}{g(D)}]$$

- Example: divide D^5+D^3 by D^3+D^2+1

Cyclic Block Codes

- A cyclic Hamming code of length 2^m-1 with m>2 is generated by a primitive polynomial $p(X)$ of degree m
- Hamming code (31, 26)
  - $g(X) = 1 + X^2 + X^5$, $l = 3$
- Golay Code:
  - cyclic code (23, 12)
  - minimum distance 7
  - generator polynomials: either $g_1(X)$ or $g_2(X)$

$$g_1(X) = 1 + X^2 + X^4 + X^5 + X^6 + X^{10} + X^{11}$$

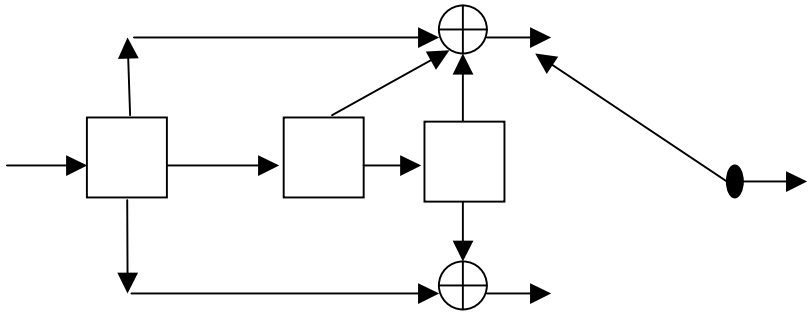
$$g_2(X) = 1 + X + X^5 + X^6 + X^7 + X^9 + X^{11}$$

Bose Chaudhuri and Hocquenghem (BCH) Codes

- For any positive integer m ($m>2$) and t ($t<2^{m-1}$), there exists a BCH code:
  - Block length: 2^m-1
  - Parity bits: $n - k \leq mt$
  - Minimum distance: $d_{min} \geq 2t + 1$
  - generator polynomial is the *lowest-degree polynomial* over GF(2) such that: $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ are its roots. α is the primitive root of unity in the extension field GF(2^n).
- Such a BCH code is capable of correcting t errors
- The generator polynomial is:
  - $g(X) = \text{LCM}\{\phi_1(X), \phi_2(X), \ldots, \phi_{2t}(X)\}$
  - for $i = i'2^l$, $\phi_i(X) = \phi_{i'}(X)$ (because α^i and $\alpha^{i'}$ are conjugates), thus $g(X) = \text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{2t-1}(X)\}$
- Since any minimal polynomial has degree m or less, then degree ($n - k$) of g is at most mt
- If $t = 1$, then g is a primitive polynomial and we have a Hamming code

Convolutional codes

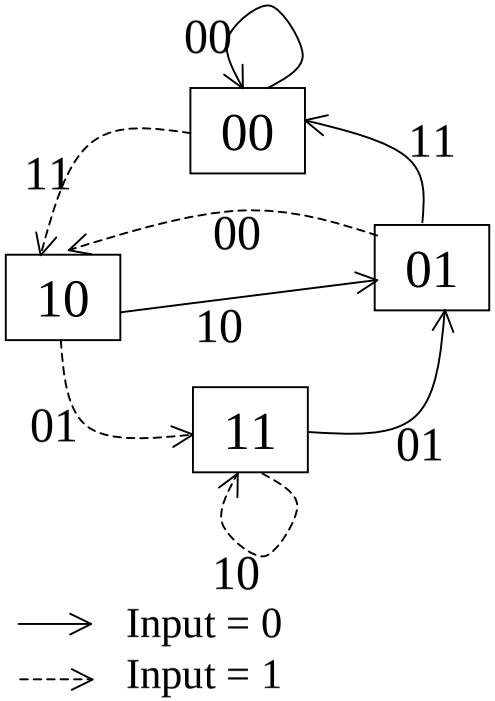
- (*n*, *k*, *K*) convolutional code: *inputs k* bits, *outputs n* bits and has *register depth K*
- Rate: *k/n*
- Example of binary convolutional encoder
  - n = 2, k = 1, K = 3. Rate ½



- Representations:
  - State, Tree, Trellis
- Decoding:
  - Soft decision vs. Hard decision
  - Viterbi Algorithm, sequential decoding, feedback decoding

Representations of Convolutional Codes

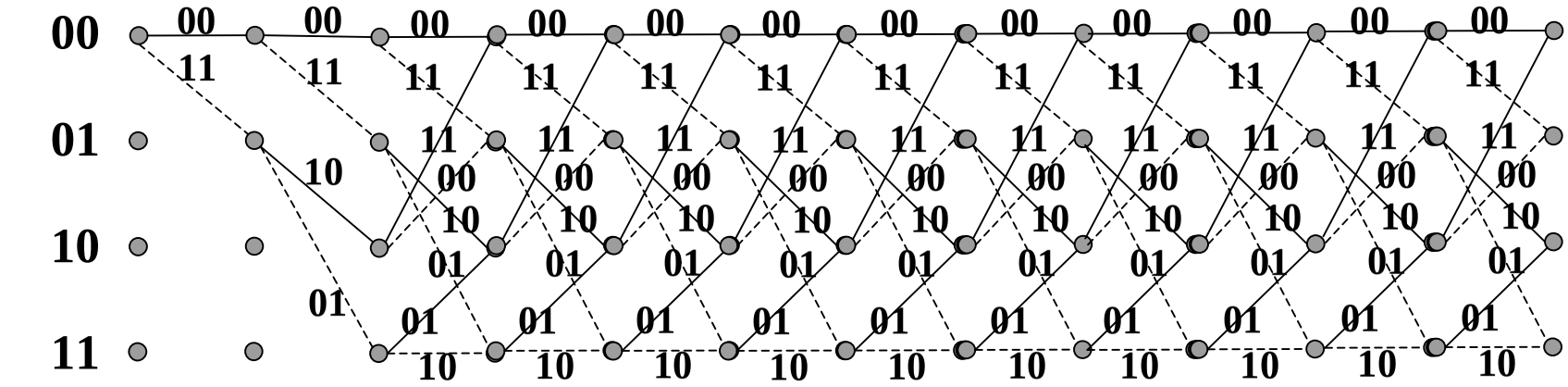
- State Coding:
  - *K*-1 registers + input => state diagram (finite state machine)



Input bit m_i	Registers	State at t_i	State at t_{i+1}	Output
-	000	00	00	-
1	100	00	10	11
1	110	10	11	01
0	011	11	01	01
1	101	01	10	01
1	110	10	11	00
0	011	11	01	01
0	001	01	00	11

Representations of Convolutional Codes

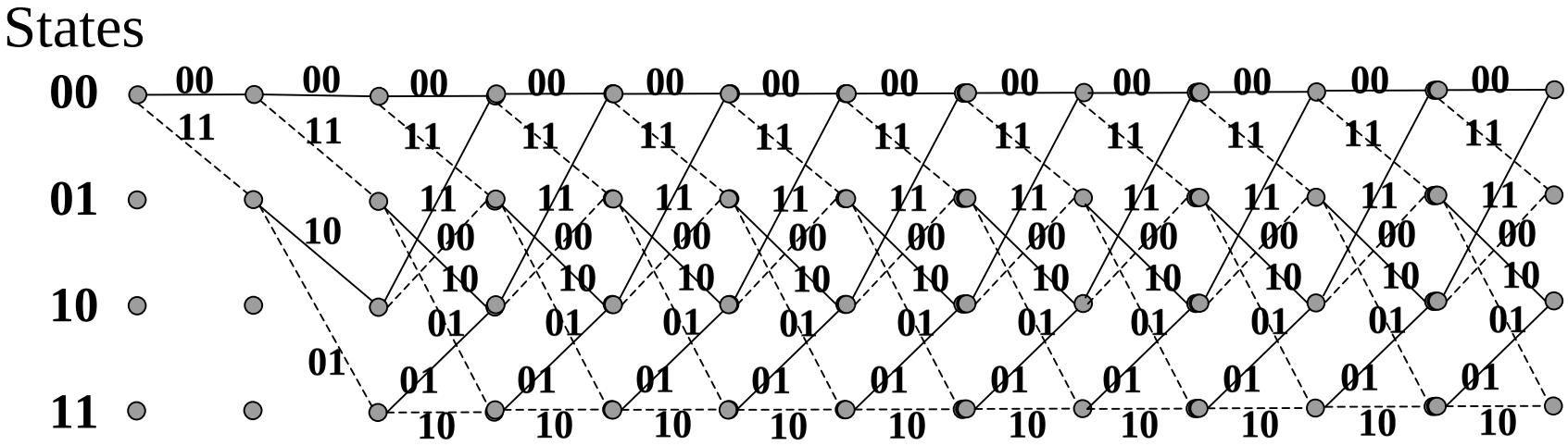
- Trellis representation:



Viterbi Decoding Algorithm

- Principle:
  - Computes a measure of similarity (distance) between the received signal and all potential trellis paths
  - For each state keeps only one “more likely” path
- Algorithm:
  - For each input
    - For each state:
      - Determine the distance/weight of the branches leading to it
      - Keep only the best branch
    - If all surviving paths at time t_i pass through some state S at time t_{i-j} then commit to $S(t_{i-j})$

Viterbi Decoding



- Input: 11011011111
- Codeword: 11 01 01 00 01 10 10 10 10 10
- Received: 11 01 01 10 01 10 10 10 10 10

Other Techniques

- Equalization:
  - Reason: multi-path generates Inter-Symbol Interference (ISI)
  - An equalizer is a filter that inverts the effect of the channel
  - Generally uses training sequences to estimate the channel
- Interleaving:
  - Reason: in some channels errors occur in bursts and channel coding is only efficient when errors are randomly distributed
  - Goal: transforms a burst of errors into randomly distributed errors
  - Types: bit level, frame level
  - Drawbacks: delay
  - How: matrix bit-interleaving. Bits enter on the rows and are output column by column

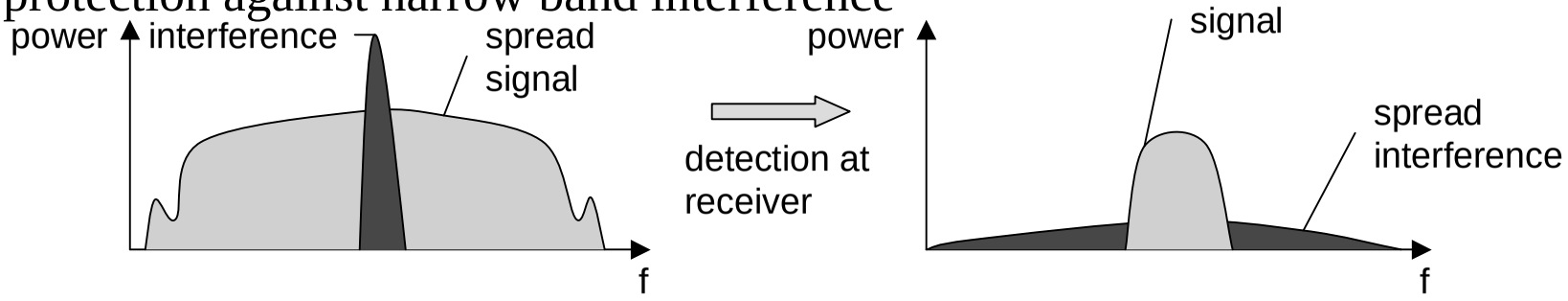
Other Techniques (Cont'd)

- Diversity techniques:
  - Micro-diversity:
    - Time diversity: transmit at different moments (separated by channel coherence time: inverse of the Doppler frequency). Generally combined with ARQ and FEC
    - Drawback may reduce throughput
  - Space diversity:
    - Use multiple antennas separated by 0.5λ and/or 0.8λ: ~3dB gain.
    - Drawback: requires equipment to process multiple input signals
  - Polarization: orthogonally polarized signals are uncorrelated
    - Multiple polarization achieves 6-10dB gain
  - Frequency diversity:
    - Use frequencies separated by a value higher than the coherence bandwidth (=> frequency hopping schemes)
- Smart antennas

Spread Spectrum Technology

- Problem of radio transmission:
  - frequency dependent fading can wipe out narrow band signals for duration of the interference; multi-path fading; eavesdropping; collisions; time imprecision
- Solution: spread the narrow band signal into a broad band signal using a special code

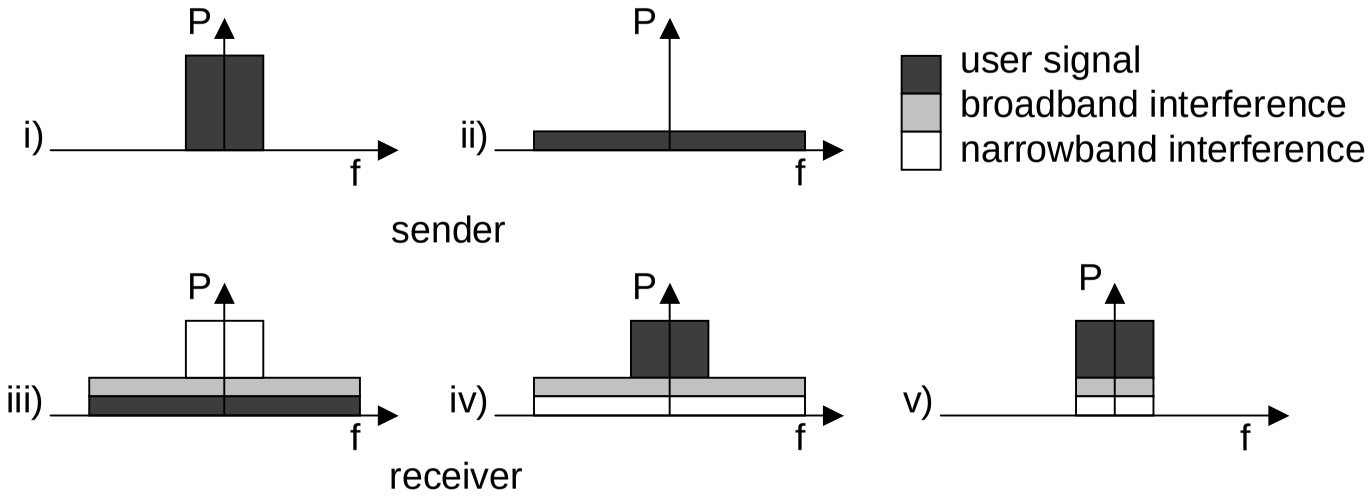
  protection against narrow band interference



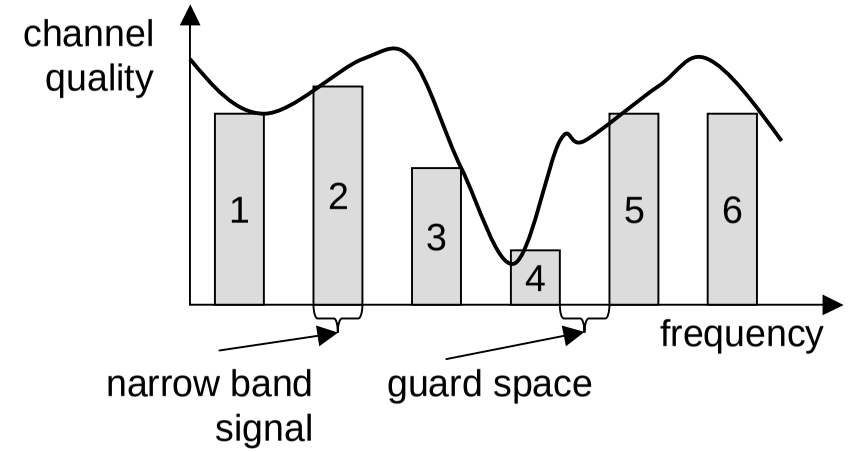
protection against narrowband interference

- Side effects:
  - coexistence of several signals without dynamic coordination (CDMA); “tap-proof”, fine time resolution (GPS); clock recovery …
- Techniques: Direct Sequence, Frequency Hopping, (Time Hopping)

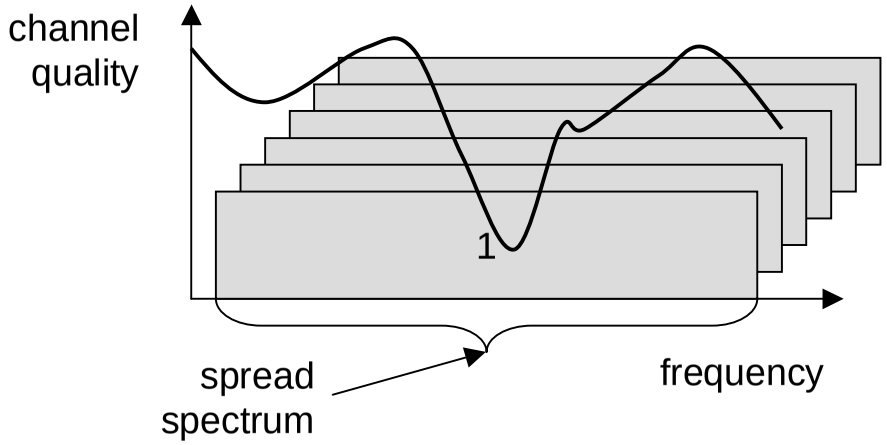
Effects of Spreading and Interference



Spreading and Frequency Selective Fading



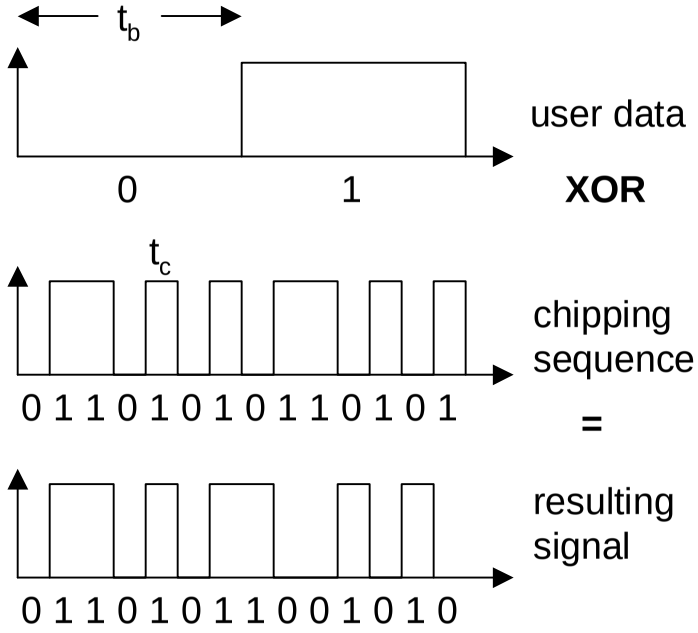
narrowband channels



spread spectrum channels

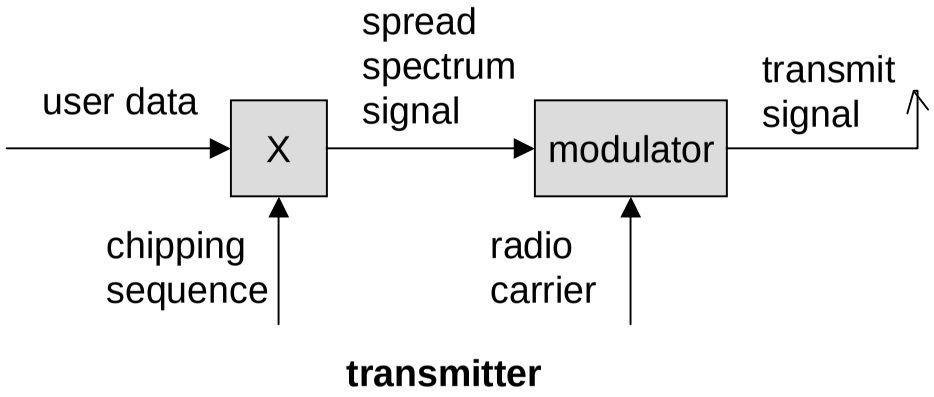
DSSS (Direct Sequence Spread Spectrum)

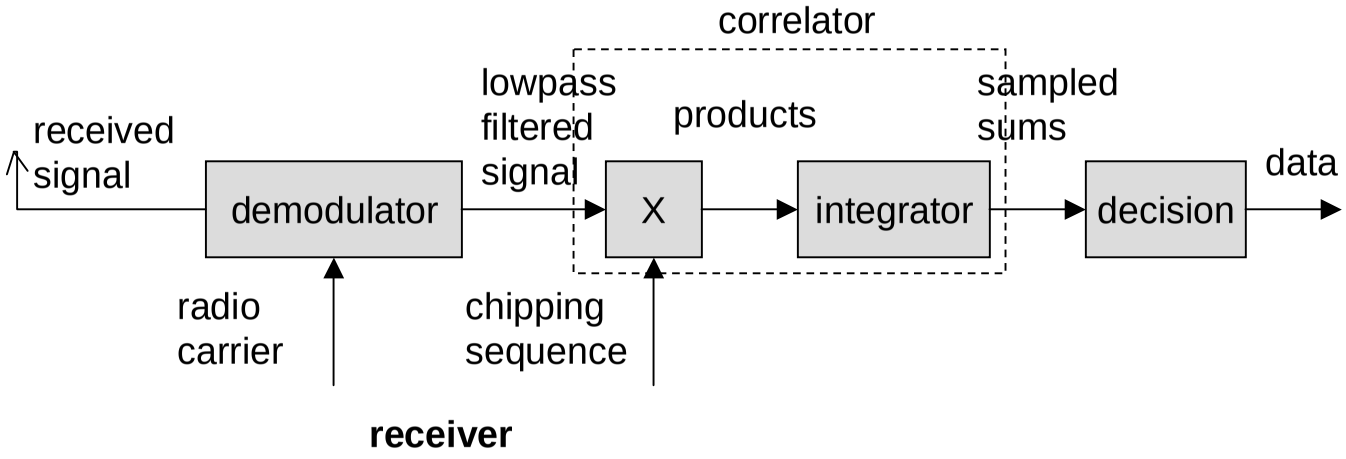
- XOR of the signal with pseudo-random number (chipping sequence)
  - many chips per bit (e.g., 128) result in higher bandwidth of the signal
  - Examples: Barker code: 11100010010(IEEE802.11), Hadamard, Kazami codes
- Advantages
  - reduces frequency selective fading
  - in cellular networks
    - base stations can use the same frequency range
    - several base stations can detect and recover the signal
    - soft handover
- Disadvantages
  - precise power control necessary



t_b: bit period
t_c: chip period

DSSS (Direct Sequence Spread Spectrum)

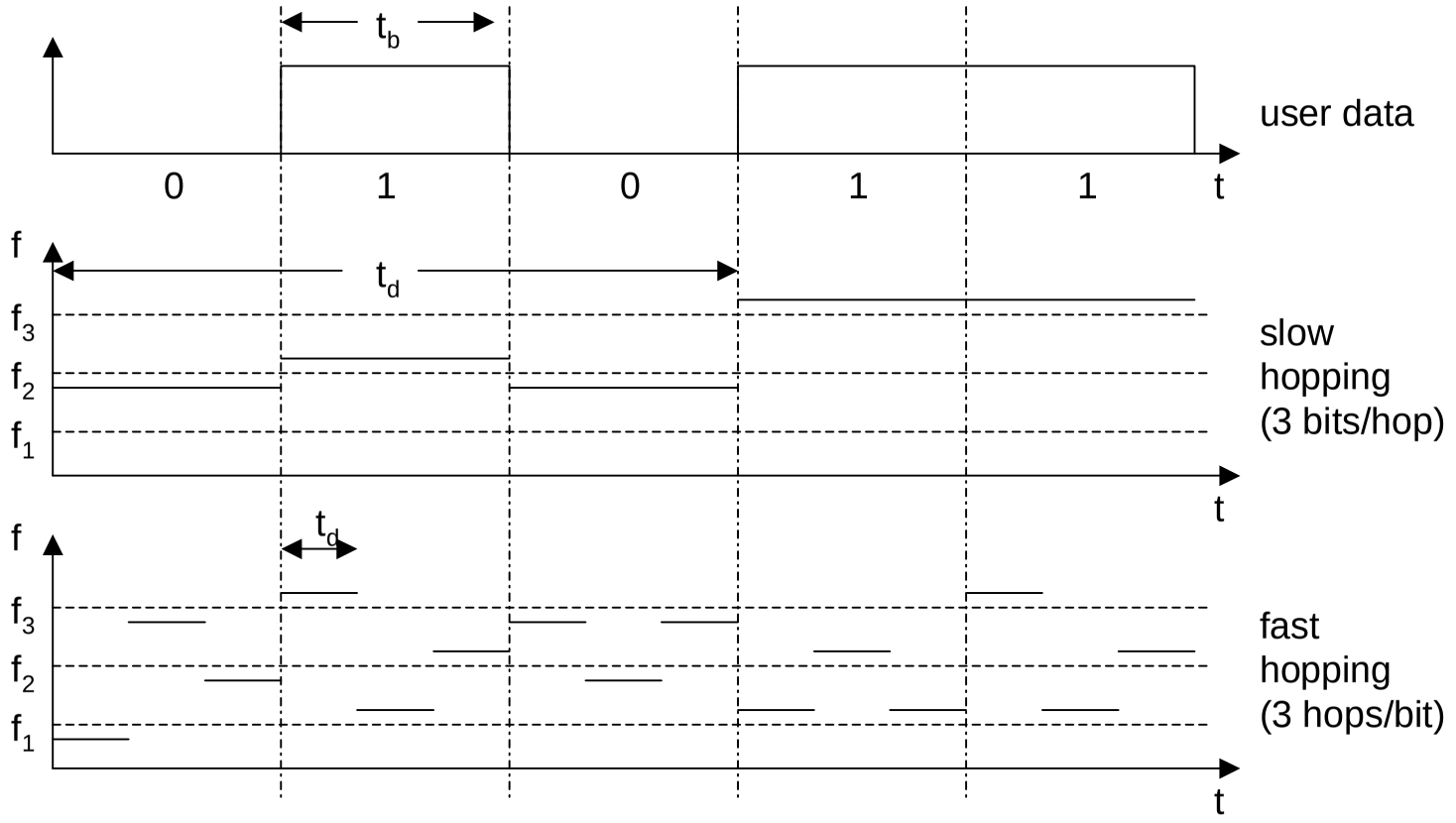




FHSS (Frequency Hopping Spread Spectrum) I

- Discrete changes of carrier frequency
  - sequence of frequency changes determined via pseudo random number sequence
- Two versions
  - Fast Hopping:
    several frequencies per user bit
  - Slow Hopping:
    several user bits per frequency
- Advantages
  - frequency selective fading and interference limited to short period
  - simple implementation
  - uses only small portion of spectrum at any time
- Disadvantages
  - not as robust as DSSS
  - simpler to detect

FHSS (Frequency Hopping Spread Spectrum)



t_b: bit period t_d: dwell time

FHSS (Frequency Hopping Spread Spectrum)