I. The Wireless Physical Medium

♦ Unique Benefits – The wireless medium is unique in its capabilities.
  ➢ For users to be mobile
  ➢ Easy reconfiguration at new locations
  ➢ Ability to be “connected” at all times with people who wish to contact them.

♦ Unique Challenges – However, the wireless medium is also particularly difficult to use.
  ➢ Signal Propagation
    • Signal strength decreases rapidly with distance.
  ➢ Multipath Propagation
    • Multiple signals arrive at a receiver.
      - From reflections off hard, smooth surfaces.
      - From diffusion caused by vegetation, rough surfaces, etc.
      - From signals diffracted around objects.
    • These signals add together at the receiver antenna.
      - Which results in a signal that can be much stronger or weaker (usually weaker) than desired.

♦ Therefore, special mechanisms have been developed to combat the problems of the wireless domain.
  ➢ Diversity
  ➢ Modulation
  ➢ Specialized Multiple Access Methods
    • Code Division Multiple Access (CDMA)
    • Orthogonal Frequency Division Multiplexing (OFDM)
  ➢ Error Control Coding

♦ This lecture gives an overview of propagation issues and the mechanisms that are used.
II. Antennas (Section 5.1)

Note: Many sections from the book are skipped in this lecture. If a section is not explicitly mentioned, you are not responsible for this material. And in those sections which are mentioned, only the material presented in this lecture is covered.

♦ Here is a picture of the overall process of transmitting and receiving in a wireless communication system (not in the book):
♦ The antenna converts the modulated signal into a signal to be sent over the air.

➤ Radiation Patterns
- Antennas radiate power in all directions.
- But typically do not perform equally well in all directions.
- One type of idealized antenna is isotropic.
  - Radiates equally well in all directions.
  - Also called ________________________________.
- But other antennas are designed with directional patterns.

![Diagram of radiation patterns](image)

(a) Omnidirectional  (b) Directional

Figure 5.1 Idealized Radiation Patterns

♦ Antenna Gain
  ➢ Measure of the directionality of the antenna.
  ➢ Defined as power output in a particular direction compared to that produced by an omnidirectional antenna.

III. Propagation Modes (Section 5.2)

♦ Electromagnetic waves travel in three different ways, depending on their frequency.
Ground Wave
- More or less follows the earth
- Can propagate considerable distances, well over the visual horizon.
- Up to 2 MHz
- U.S. AM Radio is 535 to 1605 kHz in this band.
- The wave interacts with the ground and is refracted.

Sky Wave
- The upper atmosphere bends waves back toward the earth.
- Can also bounce off the earth.
- Can travel long distances, through hops bouncing back and forth between the ionosphere and the earth’s surface.

Line-of-Sight Propagation
- Above 30 MHz, communication must be line of sight (maybe through obstructions).
- Waves travel directly between transmitter and receiver.

See Table 5.3 for discussions of different types of communications at different frequencies.

Figure 5.5 Wireless Propagation Modes
<table>
<thead>
<tr>
<th>Band</th>
<th>Frequency Range</th>
<th>Free-Space Wavelength Range</th>
<th>Propagation Characteristics</th>
<th>Typical Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELF (extremely low frequency)</td>
<td>30 to 300 Hz</td>
<td>10,000 to 1,000 km</td>
<td>GW</td>
<td>Power line frequencies; used by some home control systems.</td>
</tr>
<tr>
<td>VF (voice frequency)</td>
<td>300 to 3000 Hz</td>
<td>1,000 to 100 km</td>
<td>GW</td>
<td>Used by the telephone system for analog subscriber lines.</td>
</tr>
<tr>
<td>VLF (very low frequency)</td>
<td>3 to 30 kHz</td>
<td>100 to 10 km</td>
<td>GW; low attenuation day and night; high atmospheric noise level</td>
<td>Long-range navigation; submarine communication</td>
</tr>
<tr>
<td>LF (low frequency)</td>
<td>30 to 300 kHz</td>
<td>10 to 1 km</td>
<td>GW; slightly less reliable than VLF; absorption in daytime</td>
<td>Long-range navigation; marine communication radio beacons</td>
</tr>
<tr>
<td>MF (medium frequency)</td>
<td>300 to 3000 kHz</td>
<td>1,000 to 100 m</td>
<td>GW and night SW; attenuation low at night, high in day; atmospheric noise</td>
<td>Maritime radio; direction finding; AM broadcasting.</td>
</tr>
<tr>
<td>HF (high frequency)</td>
<td>3 to 30 MHz</td>
<td>100 to 10 m</td>
<td>SW; quality varies with time of day, season, and frequency.</td>
<td>Amateur radio; international broadcasting, military communication, long-distance aircraft and ship communication</td>
</tr>
<tr>
<td>VHF (very high frequency)</td>
<td>30 to 300 MHz</td>
<td>10 to 1 m</td>
<td>LOS; scattering because of temperature inversion; cosmic noise</td>
<td>VHF television; FM broadcast and two-way radio, AM aircraft communication; aircraft navigational aids</td>
</tr>
<tr>
<td>UHF (ultra high frequency)</td>
<td>300 to 3000 MHz</td>
<td>100 to 10 cm</td>
<td>LOS; cosmic noise</td>
<td>UHF television; cellular telephone; radar; microwave links, personal communications systems</td>
</tr>
<tr>
<td>SHF (super high frequency)</td>
<td>3 to 30 GHz</td>
<td>10 to 1 cm</td>
<td>LOS; rainfall attenuation above 10 GHz; atmospheric attenuation due to oxygen and water vapor</td>
<td>Satellite communication; radar; terrestrial microwave links; wireless local loop</td>
</tr>
<tr>
<td>EHF (extremely high frequency)</td>
<td>30 to 300 GHz</td>
<td>10 to 1 mm</td>
<td>LOS; atmospheric attenuation due to oxygen and water vapor</td>
<td>Experimental; wireless local loop</td>
</tr>
<tr>
<td>Infrared</td>
<td>300 GHz to 400 THz</td>
<td>1 mm to 770 nm</td>
<td>LOS</td>
<td>Infrared LANs; consumer electronic applications</td>
</tr>
<tr>
<td>Visible light</td>
<td>400 THz to 900 THz</td>
<td>770 nm to 330 nm</td>
<td>LOS</td>
<td>Optical communication</td>
</tr>
</tbody>
</table>
IV. Line of Sight Transmission (Section 5.3)

♦ See the following figure.

![Graph showing typical slow and fast fading in an urban mobile environment.]

Figure 5.13 Typical Slow and Fast Fading in an Urban Mobile Environment

- The smooth line is the average signal strength. The actual is the more jagged line.
- Actual received signal strength can vary by a factor of 100 (20 dB) over a few centimeters.
- The average signal strength decays with distance from the transmitter, and depends on terrain and obstructions.

♦ Two basic goals of propagation modeling:

1. Predict magnitude and rate (speed) of received signal strength fluctuations over short distances/time durations
   - “short” → typically a few wavelengths (λ) or seconds
   - At 1 Ghz, \( \lambda = \frac{c}{f} = \frac{3 \times 10^8}{1 \times 10^9} = 0.3 \) meters
   - Received signal strength can vary drastically by 30 to 40 dB
small-scale fluctuations \( \rightarrow \) called ________________
- caused by received signal coming from a sum of many signals at a receiver
- multiple signals come from reflections and scattering
- these signals can destructively add together by being out-of-phase

2. Predict **average** received signal strength for a given Tx/Rx separation

- Characterize received signal strength over distances from 20 m to 20 km

- ________________ models

- Needed to estimate the coverage area of a base station

- In general, large scale path loss decays ________________
  with distance from the transmitter

- Will also be affected by geographical features like hills and buildings

- **Free-Space Signal Propagation**
  - Clear, unobstructed line-of-sight path \( \rightarrow \) for example, satellite and fixed microwave
  - Friis transmission formula \( \rightarrow \) Receiver power \( (P_r) \) vs. Transmitter-Receiver separation \( (d) \)

\[
P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 L d^2}
\]

where

\( P_t = \) Tx power (W)
\( G = \) Tx or Rx antenna gain (unitless)
  \( \rightarrow \) relative to the isotropic source
\( \lambda = \) wavelength \( = c / f \) (m).

The \( \lambda^2/4\pi \) term is related to antenna gain.
So, as frequency increases, what happens to the propagation characteristics?

\[ L = \text{system losses (antennas, transmission lines between equipment and antennas, atmosphere, etc.)} \]
\[ \rightarrow \text{unitless} \]
\[ \rightarrow L = 1 \text{ for no loss} \]
\[ \rightarrow L > 1 \text{ in general} \]

\[ d = \text{Transmitter-receiver separation distance (m)} \]
\[ \rightarrow \text{For free space, the signal fades in proportion to } \frac{1}{d^2} \]

- More general propagation
  - Signal fades in proportion to \( \frac{1}{d^n} \), where \( n \) varies from 2 to 4 or more.
    - \( n \) is called the *path loss exponent*.
    - Indoor obstructed environments have larger values of \( n \).

<table>
<thead>
<tr>
<th>Environment</th>
<th>Path Loss Exponent, ( n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free space</td>
<td>2</td>
</tr>
<tr>
<td>Urban area cellular radio</td>
<td>2.7 to 3.5</td>
</tr>
<tr>
<td>Shadowed urban cellular radio</td>
<td>3 to 5</td>
</tr>
<tr>
<td>In building line-of-sight</td>
<td>1.6 to 1.8</td>
</tr>
<tr>
<td>Obstructed in building</td>
<td>4 to 6</td>
</tr>
<tr>
<td>Obstructed in factories</td>
<td>2 to 3</td>
</tr>
</tbody>
</table>
Computation

It is easiest to compute received power by comparison with received power at another location, say \(d_0\).
- For a value of \(d_0\) that is sufficiently far from the antenna.

\[
\frac{P_r(d)}{P_r(d_0)} = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 L d^n} = \left(\frac{d_0}{d}\right)^n
\]

\(P_r(d) = P_r(d_0) \left(\frac{d_0}{d}\right)^n\)

Example: Given the following system characteristics for large-scale propagation, find the reference distance \(d_0\).

Received power at \(d_0 = 20\) W
Received power at 5 km = 10 mW
Pathloss exponent = 3.7

Noise

Received signals consist of the following.
- Transmitted signal
- Distortion – signal modifications caused by the wireless channel.
- Additional unwanted signals, which we generally call noise.

Thermal noise
- Due to thermal agitation of electrons.
- Present in all electronic devices and transmission media.
- Cannot be eliminated.
- Present in all frequency bands.
  - Therefore, commonly called “white” noise.
Intermodulation noise
- Caused by other valid signals at different frequencies.
- Ideally these signals should stay perfectly inside their frequency bands.
- But that is not possible.
- Sometimes called “adjacent channel interference.”
  - Interference from signals in nearby channels (frequencies).

Crosstalk
- Other signals at the same frequency.
  - Hopefully the other sources are far enough away not to cause a significant problem.
- Sometimes called “co-channel interference”.
- Crosstalk is also an issue in wired telephone systems.
  - When groups of wires close together are magnetically coupled and induce signals in other wires.

Impulse noise
- Noncontinuous, irregular pulses or noise spikes.
  - Of relatively high amplitude to cause significant problems to signals.
- Variety of causes

Relationship to signal power
- We can find the relationship between signal power and noise power (S/N).
- We can also consider the ratio of signal energy ($E_b$) to noise energy ($N_0$) as $E_b/N_0$.
- Bit error performance of a system is usually judged in relationship with $E_b/N_0$. 

![Graph showing the relationship between signal-to-noise ratio (S/N) and bit error rate (BER). The graph has the x-axis labeled $(E_b/N_0)$ (dB) and the y-axis labeled Probability of bit error (BER). There are two curves, one showing better performance and the other showing worse performance.]
- The “Better Performance” curve shows that a mechanism is being used that handles noise better.

V. Fading in the Mobile Environment (Section 5.4)

♦ Multipath Propagation

➢ Multiple versions of the transmitted signal will arrive at a receiver.

![Multipath Propagation Diagram](image)

- Reflections – Waves bouncing off objects.
- Diffractions – Waves “bending around” sharp objects (not exactly, but close enough).
- Scattering – Rough surfaces creating multiple reflections.

➢ Extreme Case – Signal Cancellation

- Two signals can add together as follows for the electric field at the receiver:

\[
\vec{E}(d,t) = E_0 \cos(2\pi f_c t) + \Gamma E_0 \cos(2\pi f_c t + 180^\circ)
\]

\[
= E_0 \cos(2\pi f_c t) + \Gamma E_0 (\cos(2\pi f_c t + 180^\circ)\cos(180^\circ) + \sin(2\pi f_c t + 180^\circ)\sin(180^\circ))
\]

\[
= E_0 \cos(2\pi f_c t) - \Gamma E_0 \cos(2\pi f_c t + 180^\circ)
\]

\[
= 0 \quad \text{if } \Gamma = 1
\]
• If two signals are perfectly out-of-phase and the same amplitude, signals would completely cancel each other.
  - $\Gamma = 1$ means a perfect reflection
• Signals arrive out-of-phase because they travel different distances.
  ➢ This is generally called the problem of *fading*.
  ➢ Realistic Situations
    • Signals do not completely cancel each other.
      - But can still make large changes in received signal strength.
    • And this received strength can change over a few centimeters.
      - Because the composition of the multipath components changes.
      - So the changes can be very rapid.
  ➢ Dependency on the environment
    • The time delays of the multipath components make a big difference on the received signal.
      - If time differences are minimal, the effect is minimal.
    • Speed of movement also has an effect.
    • If there is a line-of-sight path, less fading occurs.
  ♦ Diversity
    ➢ Goal: Try to receive more than one signal.
      • By using more than one antenna
        - Spaced far enough apart.
      • By waiting a short period of time.
      • Etc.
    ➢ Since signal strengths change so rapidly, the second or third one is likely to be much better if the first one is bad.
      • Then combine the signals in a weighted fashion.
      • Give the best signal more weight.
    ➢ This being exploited in MIMO technology.
      • MIMO = Multiple Input, Multiple Output.
        - Multiple transmit and receive antennas.
      • The next generation of 802.11 (802.11n) is planned to use this.
      • The gains are substantial.
        - 802.11n plans 4 times the data rate.
        - Plus better distance coverage.
Multiuser Diversity

Consider the case where a base station has packets to send to more than one user.
- It could always choose to send a packet to the user with the best channel.
  - This would optimize the use of the channel.
  - But it might also be unfair. Why?

- The base station could also try to be more fair.
  - It could also consider how much service the node has been receiving relative to that node’s requirements.
- And the base station could also consider the delay and loss requirements of packets.
  - And send packets anyway, even with higher power, if their delay requirement was close to being violated.
  - What types of packets might have these requirements?

So, packet transmissions can make use of multiuser diversity.
- But lose capacity efficiency as fairness and packet quality of service is added.
- This is a big issue for service providers to balance of capacity, fairness, and quality.

Chapter 6 – Signal Encoding Techniques

VI. Signal Encoding Techniques

- All digital data is ultimately converted into an analog signal to be sent over an antenna.
  - This process is called modulation.
  - Receivers demodulate.
Goals
- Highest bit rate as possible.
- But also with low bit error rates.
- Why can the benefits of high bit rates be negated if there are also high bit error rates?

♦ Digital Data, Analog Signals (Section 6.2)

- Many approaches have been devised to do this as seen below.

![Diagram of modulation of analog signals for digital data](image)

Figure 6.2 Modulation of Analog Signals for Digital Data
• ASK – Amplitude Shift Keying – Change the signal amplitude based on the 1’s and 0’s.
• BFSK – Binary Frequency Shift Keying – Change the frequency.
• BPSK – Binary Phase Shift Keying – Change the phase.
➢ One can even use multiple bits at a time.
• Example: Use 4 amplitudes for ASK
  - +3 Volts for “01”
  - +1 Volt for “00”
  - -1 Volt for “10”
  - -3 Volts for “11”
• Then the bit rate is doubled.
  - Two bits at a time, instead of one.
• But the bit error rate increases.
  - If the signal power cannot be also increased.

Much, much more can be said about this, but is saved for other courses.

Chapter 7 – Spread Spectrum

VII. The Concept of Spread Spectrum (Section 7.1)

♦ A signal is spread over a wider bandwidth.
  ➢ Originally developed for military purposes.
    • To make jamming more difficult.
    • To make interception more difficult.
  ➢ Now used for public applications.
  ➢ Several users at a time can use the same frequency at the same time.
    • Instead of making different users have different frequencies or different time slots.
    • Since the signal is spread over a wide bandwidth, it is weak at any particular bandwidth over a time period.
    • So it just looks like a moderate level of noise to other users.

♦ Frequency Hopping Spread Spectrum (Section 7.2)
  ➢ A signal is broadcast over a seemingly random series of radio frequencies.
    • Hopping from frequency to frequency at fixed intervals.
    • According a random sequence known only to sender and receiver.
• 802.11 hops every 300 milliseconds (3.3 times per second).
• Bluetooth hops 1600 times per second (every 0.625 msec.).

➢ For multiple users
  • Although signals are generally using the same wide frequency band, they only collide when using the same specific narrowband channel.
  • Which happens infrequently.

➢ None of the other details from this section are important for this class.

♦ Direct Sequence Spread Spectrum (DSSS) (Section 7.3)

➢ Each bit in the original signal is represented by multiple bits in the transmitted signal.
  • By using a spreading code.
    - Also called a pseudonoise (almost noise) signal.
  • If a 10-bit code is used, the transmitted signal bit rate is 10 times higher.
    - And the signal bandwidth is approximately 10 times wider.
  • And the signal looks like noise to other users.
    - Since the signal was spread by a pseudonoise signal.
The spreading code in Figure 7.6 is 0110.

Figure 7.9 Approximate Spectrum of Direct-Sequence Spread Spectrum Signal

Figure 7.6 Example of Direct Sequence Spread Spectrum

- The spreading code in Figure 7.6 is 0110.
IS-95 cellular (Sprint and Verizon) use a spreading code of 128 bits.
- Spreads the data rate from 9.6 kbps to 1.2288 Mbps.
- Spreads the bandwidth from about 10 kHz to 1.25 MHz.

DSSS limits the number of users to the “noise level” tolerable for acceptable reception.
- “Noise level” is really all of the other users, but it just looks like noise.

♦ Code Division Multiple Access

- Frequency Hopping and DSSS both use a spreading code.
- Multiple access is provide based on using different codes.
  - Hence the term Code Division Multiple Access (CDMA).
  - As compared to Frequency Division Multiple Access (users use different frequencies).
  - Or compared to Time Division Multiple Access (users use different time slots).

Chapter 8 – Coding and Error Control

VIII. Error Detection (Section 8.1)

♦ Two approaches can be used to cope with data transmission errors.

1. Use codes to detect errors, then have mechanisms to automatically retransmit corrupted packets.

2. Detect and correct errors – called Forward Error Correction (FEC).

♦ Bit errors and Packet Errors.

- Given the following definitions:
  - \( P_b \) = probability of a single bit error
  - \( P_l \) = probability that a frame of \( F \) bits arrives with no errors

\[
P_l = (1 - P_b)^F
\]

- \( P_2 \) = probability that a frame arrives with one or more errors,

\[
P_2 = 1 - (1 - P_b)^F
\]
• Example:

\[ F = 500 \text{ bytes (4000 bits)} \]
\[ P_b = 10^{-6} \text{ (a very good performing wireless link)} \]
\[ P_1 = (1-10^{-6})^{4000} = 0.9960 \]
\[ P_2 = 1-(1-10^{-6})^{4000} = 0.0040 \]

4 out of every 1000 packets have errors
At 100 kbps, this means 6 packets per minute are in error.

Given 100 kilobyte data files:
200 packets per file
Probability that the file is corrupted is \(1-(1-P_1)^{200} = 0.551\)

➢ If we do nothing, then a significant amount of our data will be corrupted
• For this example, it is more likely that a complete file would be transmitted with corruption than without corruption.

♦ Error Detection

➢ Basic Idea: Add extra bits to a block of data bits.
• Data block: \(k\) bits
• Error detection: \(n-k\) more bits
  - Based on some algorithm for creating the extra bits.
• Results in a frame of \(n\) bits

➢ The receiver separates the data bits and the error correction bits.
• Then performs the same algorithm used at the source to see if the received bits are what they should have been.
• Hopefully if errors have occurred, the packet can be retransmitted or corrected.
• “Hopefully” because there are always some error patterns that could go undetected.

♦ Parity Check

➢ Simplest scheme: Add one bit to the frame.
• The value of the bit is chosen so as to make the number of 1’s even (or odd, depending on the type of parity).
• Example
  7 bit character: 1110001

Even parity would make an 8 bit character of what?

Odd parity would make an 8 bit character of what?

• So, this can be used to detect errors. For example, a received 10100010 (when using even parity) would be invalid and an error is detected.
• But what types of errors would NOT be detected?

➤ Errors can come from impulse noise or deep fades – so one cannot always assume individual bit errors will occur.
  • Parity checks, therefore, have limited usefulness.

➤ For \( n \) bits in error over \( N \) total bits in a character, the probability follows a Binomial distribution.

\[
\Pr\{n \text{ bits in error}\} = \binom{N}{n} p^b (1 - p_b)^{N-n}
\]
Example:
Given is a bit error probability of $10^{-2}$. What is the probability that even parity will fail for a 7 bit character plus a parity bit?
Cyclic Redundancy Check (CRC)

- Uses more than a single parity bit.
  - Adds an \((n-k)\) bit frame check sequence.

![Diagram of Error Detection Process]

**Figure 8.1 Error Detection Process**

- Takes the source data and creates a sequence of bits that is only valid if divisible by a predetermined number (with no remainder).
  - Using modulo-2 arithmetic.
    - Binary addition with no carries.
    - The same as exclusive-OR operations (XOR).
    - Also can be implemented by polynomial operations.
  - Divide the received frame by a standardized sequence of bits, \(P\).
    - If the remainder is zero, assume no error occurred.
    - See Example 8.3.

- When would CRC codes fail?
• In this case, the frame is really in error, but it is not detected.
➢ It can be shown that the following errors can be prevented by suitably chosen values for $P$.
• All single bit errors will be detected.
• All double-bit errors.
• Any odd number of errors.
• Any burst error for which the length of the burst is less than or equal to $(n-k)$
  - A burst error is a contiguous set of bits where all of the bits are in error.
➢ Four versions of $P$ are widely used, in different bit lengths.
• For example, CRC-16.

  Specified as $P(X) = X^{16} + X^{15} + X^2 + 1$
  Which means $P = 11000000000000101$

IX. Block Error Correction Codes (Section 8.2, but not from “Hamming Code” through “Reed-Solomon Codes”)

♦ Error detection requires blocks to be retransmitted when an error is found. This is inadequate for wireless communication for two reasons. Why?
♦ It is desirable to be able to correct errors without requiring retransmission.
  ➢ Using the bits that were transmitted.

![Diagram](image-url)

**Figure 8.5  Forward Error Correction Process**

➢ On transmission, the $k$-bit block of data is mapped into an $n$-bit block called a ________________.

- Using a ________________ encoder.
  - A codeword may or may not have similar format to those from the CRC approach above.
  - It may come from taking the original data and adding extra bits (as with CRC).
  - Or it may be created using a completely new set of bits.
- The codewords are longer (maybe much longer) than the original data.
- Then the block is transmitted.
Block Code Principles

- Hamming Distance
  - Given are two example sequences.
    
    \[ v_1 = 011011, \quad v_2 = 110001 \]

  - The Hamming Distance is defined as the number of bits which disagree.
    
    \[ d(v_1, v_2) = 3 \]

- Example: Given \( k = 2, n = 5 \)

<table>
<thead>
<tr>
<th>Data block</th>
<th>Codeword</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00000</td>
</tr>
<tr>
<td>01</td>
<td>00111</td>
</tr>
<tr>
<td>10</td>
<td>11001</td>
</tr>
<tr>
<td>11</td>
<td>11110</td>
</tr>
</tbody>
</table>

- Suppose the following is received: 00100
  - This is not a valid codeword.
  - An error is detected

- Can the error be corrected?
  - We cannot be sure.
  - 1, 2, 3, 4, or even 5 bits may have been corrupted by noise.
  - However, only one bit is different between this and 00000.
    \[ d(00100,00000) = 1 \]
  - Two bit changes would have been required between this and 00111.
    \[ d(00100,00111) = 2 \]
  - Three bits with 11110.
    \[ d(00100,11110) = 3 \]
  - And four bits with 11001.
    \[ d(00100,11001) = 4 \]

- Thus the most likely codeword that was sent is 00000.
  - The output from the decoder is then the data block 00.
  - But there could be a failed correction and some other data block should have been decoded.
- Decoding rule: Use the closest codeword (in terms of Hamming distance).
- Why is it okay to do this? How much less likely are two errors than one error? Assume BER = $10^{-3}$.

- And only certain patterns of bit errors will create a failure of the channel coding to correct the error properly.

- At the receiver, comparing the received codeword with the set of valid codewords can result in one of five possible outcomes (Stallings only lists four on pp.202-203).

1. There are no bit errors
   - The received codeword is the same as the transmitted codeword.
   - The corresponding source data for that codeword is output from the decoder.

2. An error is detected and can be corrected
   - For certain bit error patterns, it is clear that the received codeword is close to a valid codeword.
   - It is assumed that the close-by codeword was sent.
   - It is assumed that the source data for that codeword should be used.

3. An error is detected but cannot be corrected.
   - The received codeword is equally close to two or more valid codewords.
   - One cannot assume which codeword was the original.
   - So, it is decided only that an error has been detected and the frame should be retransmitted.
4. An error is detected and is erroneously corrected.
   - An error pattern creates a new codeword that is close to a valid codeword.
   - But the one it is close to is not the one that was sent.
   - Therefore, the decoder outputs the source data for a wrong codeword.

   - This is a _________________.

5. An error is not detected.
   - An error pattern occurs that transforms the transmitted codeword into another valid codeword.
   - The receiver assumes no error has occurred.
   - The output from the decoder is the source data for a wrong codeword.

   - This is a _________________.
   - Hopefully other application processes will also check the validity of the data.

➢ Now, for all cases…
   - There are five bits in the codeword, so there are $2^5=32$ possible received codewords.
     - Four are valid, the other 28 would come from bit errors.
   - See pages 203-204.
   - In many cases, a possible received codeword is a Hamming distance of 1 from a valid codeword.
   - But in eight cases, a received codeword would be a distance of 2 away from two valid codewords.
     - The receiver does not know which one to choose.
     - A correction decision is undecided.
     - An error is detected but not correctable.
   - So, we can conclude that in this case an error of 1 bit is always correctable, but not errors of two bits.

♦ Block code design

➢ With an $(n,k)$ code, there are $2^k$ valid codewords out of a possible $2^n$ codewords.
   - Data block: $k$ bits
   - Total frame: $n$ bits
• The ratio of \( k/n \) is called the ________________.
  - For example, a \( 1/2 \) rate code needs double the bandwidth of the raw data for the same net data rate.
  - \( 1/2 \) of the bits are for error control purposes.
  - Example: A 2/5 rate code over a 30 kbps channel.
    - Net data rate?

  - Data rate for error control codes?

➢ For a code consisting of codewords denoted \( w_i \), the minimum Hamming distance is defined as the minimum distance over all possible combinations.

\[
d_{\text{min}} = \min_{i \neq j} \left[ d(w_i, w_j) \right]
\]

• Some combinations have larger distances, but the Hamming distance gives the worst case.
• For the example above, \( d_{\text{min}} = 3 \).
• The maximum number of guaranteed correctable errors is

\[
t_{\text{corr}} = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor
\]

  - The symbol \( \lfloor x \rfloor \) means to round down to the next lowest integer.
• From the example, \( t_{\text{corr}} = (3-1)/2 = 1 \) bit error can be corrected.
  - A two-bit error will cause either an undecided correction or a failed correction.
• The number of errors that can be detected is

\[ t_{\text{det}} = d_{\text{min}} - 1 \]

• From the example, \( t_{\text{det}} = 3-1 = 2 \)
  - All two-bit errors will be detected.
  - As little as a three bit error might cause a failed detection, since a change in 3 bits might create another valid codeword.

➤ Given these definitions for Hamming distance, why is it necessary that the codewords be longer than the original data?

➤ The following design considerations are involved with devising codewords.
  - For values of \( n \) and \( k \), we would like the largest possible value of \( d_{\text{min}} \).
  - The code should be relatively easy to encode and decode, with minimal memory and processing time.

  • We would like the number of extra bits, \( (n-k) \) to be ____________ to preserve bandwidth.

  • We would like the number of extra bits, \( (n-k) \) to be ____________ to reduce error rate (since it would create a larger Hamming distance).

➤ The last two objectives are in conflict.

➤ Real-world Implementations
  - Many cellular standards use 1/2 and 1/3 rate codes.
  - IEEE 802.11 Wireless LAN
    - Header fields are protected with CRC-16 for error detecting and assumes retransmission.
    - At 11 Mbps, a ½ rate coding can be applied to the payload of the packet and is optional.
- Called PBCC (Packet Binary Convolutional Code).
- For 802.11g, at 22 Mbps and 33 Mbps, a 2/3 rate code is used.

➢ Coding Gain

- Coding can allow us to use lower power (smaller $E_b/N_0$) to achieve the same error rate we would have had without using correction bits.
- Since errors can be corrected.

- The curve below on the right is for an uncoded modulation system.
- Above $E_b/N_0$ of 5.4 dB, a smaller bit error rate can be achieved using a $\frac{1}{2}$ rate code for the same $E_b/N_0$.
- But the $\frac{1}{2}$ rate code would require more bandwidth.

![Figure 8.6 How Coding Improves System Performance](image)

- The ________________ of a code is defined as the reduction in dB of $E_b/N_0$ that is required to obtain the same error rate.
- For example, for a BER of $10^{-6}$, 11 dB is needed for the $\frac{1}{2}$ rate code, as compared to 13.77 dB without the coding.
- This is a coding gain of 2.77 dB.
- What is the coding gain at a BER of $10^{-3}$?
X. Block Interleaving

⇒ Small scale fading causes deep fades
  • In that case, bits are not dropped randomly, but rather in large bursts of errors
  • Technically one half of the bits can be lost, since the other half are correct by coincidence.
⇒ But channel coding is only useful for detecting/correcting isolated errors, and only a few number of errors
⇒ Once a large number of errors occur in a packet, the packet cannot be recovered.

⇒ Interleaving can be used when combined with channel coding.
⇒ The interleaver spreads the bits from one packet out in time so that a sequence of many bits from one packet are not corrupted at the same time

⇒ Accomplished by interleaving (combining, interweaving) bits of multiple packets, like packets $P_1$ through $P_5$ below.

| $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_1$ |

Burst of Errors

⇒ No one packet is corrupted too much.

⇒ Block Interleaver

![Interleaving Diagram](image)

Note: The numbers in the matrix indicate the order in which bits are read in.
Interleaver output sequence: 1, $n+1$, $2n+1$, ...

Figure 8.8 Block Interleaving
• $m$ rows & $n$ columns; degree = $m$ packets at a time
• $mn$ bits interleaved at a time
• sequentially read \textit{in} to rows
• sequentially read \textit{out} of columns
• original source bits separated by $m$ \textbf{bits}

$\Rightarrow$ Interleaver delay
• $nm$ bits must arrive \textit{at} the receiver before the process can be inverted → “de-interleaved”
• delay = $nmT_b$
• The perceived quality of real-time data (voice, video, etc.) can be affected by this delay.

$\Rightarrow$ Suppose we have an $(n, k)$ code and one can correct $t$ or fewer errors.
• And we use an $m$ degree interleaver.
• Then the result is an $(mn, mk)$ code that can correct bursts of up to $mt$ errors.
• Since each block individually should correct $t$ errors.

♦ Error Control Coding

➢ Both error detection and error correction involve creating coded information to be transmitted.
  • Either in addition to the original data.
  • Or as a replacement for the original data.
➢ Hence, this whole topic is usually referred to in general as \textit{Error Control Coding}.

Next lecture: WiMax (IEEE 802.16), Chapter 11