CS236/NetSys230
Wireless Networking

Coding and Error Control

Kasper B. Rasmussen
Computer Science Department
University of California, Irvine
Announcements

- Project is online at https://eee.uci.edu/12f/35240/

- No rooms available that will hold more than 30 people.
Agenda

- Error detection
- Block Error Correction Codes
- Convolutional Codes
Coping with Data Transmission Errors

- **Error detection codes**
  - Detects the presence of an error

- **Error correction codes, or forward correction codes (FEC)**
  - Designed to detect and correct errors

- **Automatic repeat request (ARQ) protocols**
  - Block of data with error is discarded
  - Transmitter retransmits that block of data
Error Detection Probabilities

- **Definitions**
  - $P_b$: Probability of single bit error (BER)
  - $P_1$: Probability that a frame arrives with no bit errors
  - $P_2$: Probability that a frame arrives with one or more undetected errors
  - $P_3$: Probability that a frame arrives with one or more detected bit errors but no undetected bit errors
Error Detection Probabilities

- With no error detection

\[ P_1 = (1 - P_b)^F \]
\[ P_2 = 1 - P_1 \]
\[ P_3 = 0 \]

- \( F = \) Number of bits per frame
Error Detection Process

- Transmitter
  - For a given frame, an error-detecting code (check bits) is calculated from data bits
  - Check bits are appended to data bits

- Receiver
  - Separates incoming frame into data bits and check bits
  - Calculates check bits from received data bits
  - Compares calculated check bits against received check bits
  - Detected error occurs if mismatch
Figure 8.1 Error Detection Process
Parity Check

- Parity bit appended to a block of data
- Even parity
  - Added bit ensures an even number of 1s
- Odd parity
  - Added bit ensures an odd number of 1s
- Example, 7-bit character [1110001]
  - Even parity [11100010]
  - Odd parity [11100011]
Cyclic Redundancy Check (CRC)

- **Transmitter**
  - For a k-bit block, transmitter generates an (n-k)-bit frame check sequence (FCS)
  - Resulting frame of n bits is exactly divisible by predetermined number

- **Receiver**
  - Divides incoming frame by predetermined number
  - If no remainder, assumes no error
CRC using Modulo 2 Arithmetic

- Exclusive-OR (XOR) operation
- Parameters:
  - $T = n$-bit frame to be transmitted
  - $D = k$-bit block of data; the first $k$ bits of $T$
  - $F = (n - k)$-bit FCS; the last $(n - k)$ bits of $T$
  - $P = \text{Divisor (pattern of } n-k+1 \text{ bits)}$
  - $Q = \text{Quotient}$
  - $R = \text{Remainder}$
CRC using Modulo 2 Arithmetic

- For T/P to have no remainder, start with
  \[ T = 2^{n-k} D + F \]

- Divide \(2^{n-k}D\) by \(P\) gives quotient \(Q\) and remainder \(R\)
  \[ \frac{2^{n-k} D}{P} = Q + \frac{R}{P} \]

- Use remainder as FCS
  \[ T = 2^{n-k} D + R \]
CRC using Modulo 2 Arithmetic

- Does R cause T/P have no remainder?

\[
\frac{T}{P} = \frac{2^{n-k} D + R}{P} = \frac{2^{n-k} D}{P} + \frac{R}{P}
\]

- Substituting,

\[
\frac{T}{P} = Q + \frac{R}{P} + \frac{R}{P} = Q + \frac{R + R}{P} = Q
\]

- No remainder, so T is exactly divisible by P
CRC using Polynomials

- All values expressed as polynomials
  - Dummy variable $X$ with binary coefficients

\[
\frac{X^{n-k} D(X)}{P(X)} = Q(X) + \frac{R(X)}{P(X)}
\]

\[
T(X) = X^{n-k} D(X) + R(X)
\]
CRC using Polynomials

- Widely used versions of $P(X)$
  - CRC–12
    \[ X^{12} + X^{11} + X^3 + X^2 + X + 1 \]
  - CRC–16
    \[ X^{16} + X^{15} + X^2 + 1 \]
  - CRC – CCITT
    \[ X^{16} + X^{12} + X^5 + 1 \]
  - CRC – 32
    \[ X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1 \]
CRC using Digital Logic

- Dividing circuit consisting of:
  - XOR gates
    - Up to \( n - k \) XOR gates
    - Presence of a gate corresponds to the presence of a term in the divisor polynomial \( P(X) \)
  - A shift register
    - String of 1-bit storage devices
    - Register contains \( n - k \) bits, equal to the length of the FCS
(a) Shift-register implementation

- **Reduction Step Output (15 bits)**
- Switch 1:
  - **A**
  - **B**

- **Input (10 bits)**
  - **A**
  - **B**

- **C₀, C₁, C₂, C₃, C₄**
- **Switch 2**
- **= 1-bit shift register**
- **= Exclusive-OR circuit**

(b) Example with input of 1010001101

<table>
<thead>
<tr>
<th>Step</th>
<th>C₀</th>
<th>C₁</th>
<th>C₂</th>
<th>C₃</th>
<th>C₄</th>
<th>C₄ = C₃ = I</th>
<th>C₄ = C₁ = I</th>
<th>C₄ = I</th>
<th>I = input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Step 1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Step 2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Step 3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Step 4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Step 5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Step 6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Step 7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Step 8</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Step 9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Step 10</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Message to be sent:
Wireless Transmission Errors

- Error detection requires retransmission
- Detection inadequate for wireless applications
  - Error rate on wireless link can be high, results in a large number of retransmissions
  - Long round-trip-time delay
Block Error Correction Codes

Transmitter
- Forward error correction (FEC) encoder maps each k-bit block into an n-bit block codeword
- Codeword is transmitted; analog for wireless transmission

Receiver
- Incoming signal is demodulated
- Block passed through an FEC decoder
Figure 8.5  Forward Error Correction Process
FEC Decoder Outcomes

- No errors present
  - Codeword produced by decoder matches original codeword
- Decoder detects and corrects bit errors
- Decoder detects but cannot correct bit errors; reports uncorrectable error
- Decoder detects no bit errors, though errors are present
Block Code Principles

- **Hamming distance** – for 2 n-bit binary sequences, the number of different bits
  - E.g., v1=011011; v2=110001; d(v1, v2)=3

- **Redundancy** – ratio of redundant bits to data bits

- **Code rate** – ratio of data bits to total bits

- **Coding gain** – the reduction in the required $E_b/N_0$ to achieve a specified BER of an error-correcting coded system
Hamming Code

- Designed to correct single bit errors
- Family of \((n, k)\) block error-correcting codes with parameters:
  - Block length: \(n = 2^m - 1\)
  - Number of data bits: \(k = 2^m - m - 1\)
  - Number of check bits: \(n - k = m\)
  - Minimum distance: \(d_{\text{min}} = 3\)

- Single-error-correcting (SEC) code
  - SEC double-error-detecting (SEC-DED) code
Hamming Code Process

- **Encoding**: $k$ data bits + $(n-k)$ check bits
- **Decoding**: compares received $(n-k)$ bits with calculated $(n-k)$ bits using XOR
  - Resulting $(n-k)$ bits called syndrome word
  - Syndrome range is between 0 and $2(n-k)-1$
  - Each bit of syndrome indicates a match (0) or conflict (1) in that bit position
Cyclic Codes

- Can be encoded and decoded using linear feedback shift registers (LFSRs)
- Cyclic codes: a valid codeword \((c_0, c_1, \ldots, c_{n-1})\), shifted right one bit, is also a valid codeword \((c_{n-1}, c_0, \ldots, c_{n-2})\)
- Takes fixed-length input \((k)\) and produces fixed-length check code \((n-k)\)
  - In contrast, CRC error-detecting code accepts arbitrary length input for fixed-length check code
BCH Codes

- For positive pair of integers $m$ and $t$, a $(n, k)$ BCH code has parameters:
  - Block length: $n = 2^m - 1$
  - Number of check bits: $n - k \leq mt$
  - Minimum distance: $d_{\text{min}} \geq 2t + 1$

- Correct combinations of $t$ or fewer errors

- Flexibility in choice of parameters
  - Block length, code rate
Reed-Solomon Codes

- Subclass of nonbinary BCH codes
- Data processed in chunks of $m$ bits, called symbols
- Common parameters
  - RS(255, 223)
Block Interleaving

- Data written to and read from memory in different orders
- Data bits and corresponding check bits are interspersed with bits from other blocks
- At receiver, data are deinterleaved to recover original order
- A burst error that may occur is spread out over a number of blocks, making error correction possible
Interleaving Example

Error-free message:       aaaabbbbbcdddddeeeeffffgggg
Transmission with a burst error:  aaaabbbbbc____deeeeffffgggg

Error-free code words:   aaaabbbbbcdddddeeeeffffgggg
Interleaved:             abcdefgabcdefgabcdefgabcdefg
Transmission with a burst error:  abcdefgabcd____bcdefgabcdefg
After deinterleaving:    aa_abbbbccddddde_eef_ffg_gg
Convolutional Codes

- Generates redundant bits continuously
- Error checking and correcting carried out continuously

- \((n, k, K)\) code
  - Input processes \(k\) bits at a time
  - Output produces \(n\) bits for every \(k\) input bits
  - \(K\) = constraint factor
  - \(k\) and \(n\) generally very small

- \(n\)-bit output of \((n, k, K)\) code depends on:
  - Current block of \(k\) input bits
  - Previous \(K-1\) blocks of \(k\) input bits
Figure 8.9 Convolutional Encoder with \((n, k, K) = (2, 1, 3)\)
Decoding

- Trellis diagram – expanded encoder diagram
- Viterbi code – error correction algorithm
  - Compares received sequence with all possible transmitted sequences
  - Algorithm chooses path through trellis whose coded sequence differs from received sequence in the fewest number of places
  - Once a valid path is selected as the correct path, the decoder can recover the input data bits from the output code bits
Viterbi on 10010100101100...