16.36: Communication Systems Engineering

Lectures 14: Cyclic Codes and error detection

Eytan Modiano

Cyclic Codes

- A cyclic code is a linear block code where if c is a codeword, so are all cyclic shifts of c
  - E.g., {000,110,101,011} is a cyclic code
- Cyclic codes can be dealt with in the very same way as all other LBC's
  - Generator and parity check matrix can be found
- A cyclic code can be completely described by a generator string G
  - All codewords are multiples of the generator string
- In practice, cyclic codes are often used for error detection (CRC)
  - Used for packet networks
  - When an error is detected by the received, it requests retransmission

Error detection techniques

- Used by the receiver to determine if a packet contains errors
- If a packet is found to contain errors the receiver requests the transmitter to re-send the packet

- Error detection techniques
  - Parity check
    - E.g., single bit
  - Cyclic redundancy check (CRC)

Parity check codes

k Data bits	r Check bits

- Each parity check is a modulo 2 sum of some of the data bits

Example:

$$c_1 = x_1 + x_2 + x_3$$
$$c_2 = x_2 + x_3 + x_4$$
$$c_3 = x_1 + x_2 + x_4$$

Single Parity Check Code

- The check bit is 1 if frame contains odd number of 1's; otherwise it is 0

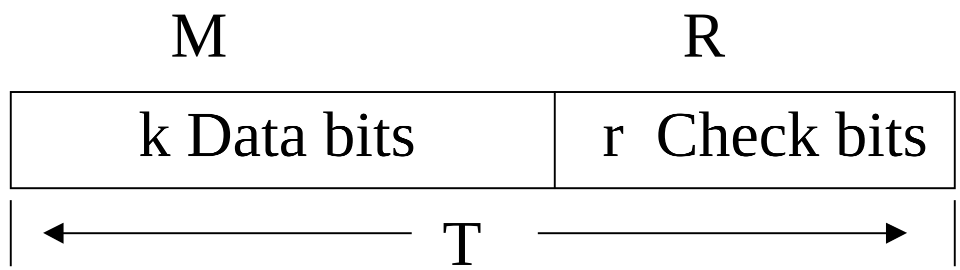
  1011011 -> 1011011 1
  1100110 -> 1100110 0

- Thus, encoded frame contains even number of 1's
- Receiver counts number of ones in frame
  - An even number of 1's is interpreted as no errors
  - An odd number of 1's means that an error must have occured
    - A single error (or an odd number of errors) can be detected
    - An even number of errors cannot be detected
    - Nothing can be corrected
- Probability of undetected error (independent errors)

$$P(undetected) = \sum_{i\ even} \binom{N}{i} p^i (1-p)^{N-i}$$

N = packet size
p = error prob.

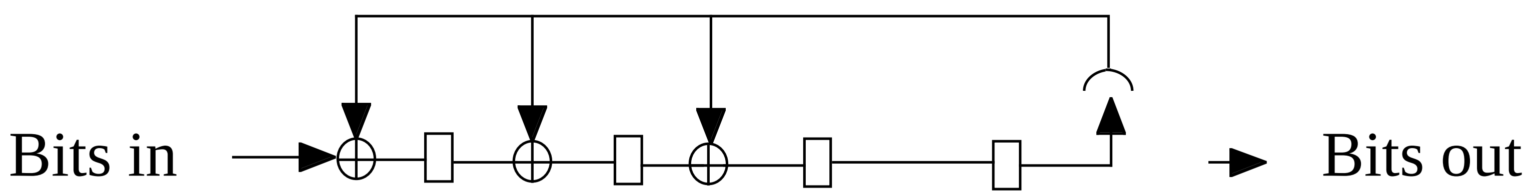
Cyclic Redundancy Checks (CRC)



M = info bits
R = check bits
T = codeword

$$T = M\,2^r + R$$

- A CRC is implemented using a feedback shift register



Cyclic redundancy checks

$$T = M\,2^r + R$$

- How do we compute R (the check bits)?
  - Choose a generator string G of length r+1 bits
  - Choose R such that T is a multiple of G (T = A*G, for some A)
  - Now when T is divided by G there will be no remainder => no errors
  - All done using mod 2 arithmetic

$T = M\,2^r + R = A*G \Rightarrow M\,2^r = A*G + R$ (mod 2 arithmetic)

Let R = remainder of $M\,2^r/G$ and T will be a multiple of G

- Choice of G is a critical parameter for the performance of a CRC

Example

r = 3, G = 1001

M = 110101 => $M2^r$ = 110101000

```
          110011
      ___________
1001 | 110101000
       1001
       ----
       01000
        1001
        ----
        0001100
           1001
           ----
           01010
            1001
            ----
             011 = R (3 bits)
```

Modulo 2 Division

Checking for errors

- Let T’ be the received sequence
- Divide T’ by G
  - If remainder = 0 assume no errors
  - If remainder is non zero errors must have occurred

Example:
Send T = 110101011
Receive T’ = 110101011
(no errors)

```
1001 | 110101011
       1001
       -----
       01000
        1001
        -----
        0001101
            1001
            -----
            01001
             1001
             -----
              000 => No errors
```

No way of knowing how many errors occurred or which bits are In error

Mod 2 division as polynomial division

Implementing a CRC

Effectiveness of error detection technique

- Effectiveness of a code for error detection is usually measured by three parameters:

  1) minimum distance of code (d) (min # bit errors undetected)

  The minimum distance of a code is the smallest number of errors that can map one codeword onto another. If fewer than d errors occur they will always detected. Even more than d errors will often be detected (but not always!)

  2) burst detecting ability (B) (max burst length always detected)

  3) probability of random bit pattern mistaken as error free (good estimate if # errors in a frame >> d or B)

  – Useful when framing is lost

  – K info bits => 2^k valid codewords

  – With r check bits the probability that a random string of length k+r maps onto one of the 2^k valid codewords is $2^k/2^{k+r} = 2^{-r}$

Performance of CRC

- For r check bits per frame and a frame length less than 2^{r-1}, the following can be detected

  1) All patterns of 1,2, or 3 errors (d > 3)
  2) All bursts of errors of r or fewer bits
  3) Random large numbers of errors with prob. $1-2^{-r}$

- Standard DLC's use a CRC with r=16 with option of r=32

  – CRC-16, $G = X^{16} + X^{15} + X^2 + 1 = 11000000000000101$

Physical Layer Error Characteristics

- Most Physical Layers (communications channels) are not well described by a simple BER parameter
- Most physical error processes tend to create a mix of random & bursts of errors
- A channel with a BER of 10^{-7} and a average burst size of 1000 bits is very different from one with independent random errors
- Example: For an average frame length of 10^4 bits
  - random channel: E[Frame error rate] ~ 10^{-3}
  - burst channel: E[Frame error rate] ~ 10^{-6}
- Best to characterize a channel by its Frame Error Rate
- This is a difficult problem for real systems