CS3200: Computer Networks

Lecture 6

IIT Palakkad

06 Aug, 2019

Error Detection and Correction

- Transmission errors are unavoidable. We need to develop techniques to deal with them.
- One strategy is to include enough redundant information to enable the receiver to deduce what the transmitted data must have been — **Forward Error Correction (FEC)**
- The other is to include only enough redundancy to allow the receiver to deduce that an error has occurred and have it request a retransmission.
- Which of the above technique is better?

Error Detection and Correction

The codes we will look at are linear, systematic block codes unless otherwise noted.

- A frame consists of m data (i.e., message) bits and r redundant (i.e. check) bits.
- **Block code**: the r check bits are computed solely as a function of the m data bits with which they are associated
- **Systematic code**: the m data bits are sent directly, along with the check bits, rather than being encoded themselves before they are sent.
- **Linear code**: the r check bits are computed as a linear function of the m data bits. Exclusive OR (XOR) or modulo 2 addition is a popular choice.

Let the total length of a block be n (i.e., $n = m + r$). We will describe this as an (n, m) code. An n-bit unit containing data and check bits is referred to as an n-bit codeword. The **code rate** is the fraction of the codeword that carries non-redundant information i.e., m/n.

Hamming Codes

- Given two code words 10001001 and 10110001 — is to possible to determine how many corresponding bits differ?
- This difference is called the **Hamming distance**
- If two code words are a Hamming distance of d apart, d single-bit errors are needed to convert one into the other.
- In most data transmission applications, all 2^m possible data messages are legal, but due to the way the check bits are computed, not all of the 2^n possible codewords are used. In fact, when there are r check bits, only the small fraction of $2^m/2^n$ or $1/2^r$ of the possible messages will be legal codewords.

Hamming Codes

- To reliably detect d errors, you need a distance $d + 1$ code because with such a code there is no way that d single-bit errors can change a valid codeword into another valid codeword.
- To correct d errors, you need a distance $2d + 1$ code because that way the legal codewords are so far apart that even with d changes the original codeword is still closer than any other codeword.
- Consider the following codewords 0000000000, 0000011111, 1111100000, and 1111111111. Upto how many bit errors can we correct? How many can we detect?

Hamming Codes

- We want to design a code with m message bits and r check bits that will allow all single errors to be corrected.
- Each of the 2^m legal messages has n illegal codewords at a distance of 1 from it.
- Each of the 2^m legal messages requires $n + 1$ bit patterns dedicated to it.
- We get the requirement that $(m + r + 1) \leq 2^r$.