Introduction to Coding

After this lecture you should be able to:

- *distinguish between source coding, encryption and channel coding*
- *compute the minimum distance of a code from its codewords*
- *find n, k and the code rate for systematic block codes*

Coding

The term coding has three different meanings when used in communication systems:

Source Coding Often called "compression," source coding attempts to reduce the data rate to more closely match the information rate by removing redundancy. This reduces the complexity of the remainder of the communication system.

Security Techniques such as signatures and encryption can be used to ensure the integrity, authenticity and the privacy of the information being transmitted over the channel.

Channel Coding Used to detect and correct errors introduced by the channel.

The first two are typically covered in courses in signal processing and data communications respectively. In this course we will concentrate on the third meaning.

Parity

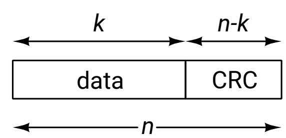
A technique for detecting errors in received frames is for the transmitter to compute one or more bits called "parity bits" from the transmitted data and append them to the frame. The receiver computes the parity bits itself from the received data and compares them to the received parity bits. If the computed and received parity bits match then either there were no errors or the received bits were corrupted in such a way the received parity bits are valid for the received data.

The probability of the latter event is called the *undetected error probability*. Good error detecting codes try to make this probability as low as possible.

Block Codes

More complex channel codes use multiple parity bits. Each parity bit is computed from a different subset of data bits. This makes the code more "powerful" in the sense that it can detect (and potentially correct) more errors.

A block code where each block of n bits contains k data bits is called an (n, k) code:



Note that an (n, k) code contains $n - k$ parity bits.

A "code" is defined by the set of all possible n-bit codewords.

Exercise 1: A (5,3) code computes the two parity bits as: $p_0 = d_0 \oplus d_1$ and $p_1 = d_1 \oplus d_2$ where d_i is the i'th data bit. What codeword is transmitted when the data bits are $(d_0, d_1, d_2) = (0, 0, 1)$? How many different codewords are there in the code? What are the first four codewords? In general, how many codewords are there for an (n, k) code?

Hamming Distance

The *Hamming Distance*, D, is the number of bits that differ between two code words.

The performance of a particular code is mainly determined by the minimum (Hamming) distance (D_{min}) between any two code words in the code.

Exercise 2: What is the Hamming distance between the codewords 11100 and 11011? What is the minimum distance of a code with the four codewords 0111, 1011, 1101, 1110?

A code constructed as above (2^k codewords each with $n - k$ parity bits) is a linear code because each codeword can be created by (modulo-2) sum of the other codewords. The weight of a codeword is the number of 1's. For a linear code the minimum Hamming distance is equal to the minimum weight of the non-zero codewords.

Exercise 3: A (5,2) block code has codewords constructed as $d_0, d_1, d_0 \oplus d_1, d_0, d_1$. Is this a linear code? List the codewords. What is the minimum weight of this code? What is the minimum distance?

Code Rate

The *rate* of a code is the ratio of information bits to total bits, or k/n. This is a measure of the efficiency of the code. As we add parity bits the code rate decreases but, for a well-designed code, the minimum distance and thus the error-correcting ability increases.

Exercise 4: What is the code rate of a code with 4 codewords each of which is 4 bits long? *Hint: If a code has 2^k codewords, what is k?*.

Exercise 5: The data rate over the channel is 50 Mb/s; a rate 1/2 code is used. What is the throughput?