Minimal Distance Between Codewords

The following is a distance measure between two strings (or codewords).

Definition: Hamming distance

The Hamming distance between two n-bit strings x and y is defined as

$$d(x, y) := \sum_{i=1}^{n} |x_i - y_i|.$$

One can equivalently define $d(x, y) = |x - y|$ where $|z|$ denotes the **Hamming weight** of a binary string: the number of ones in that string.

The number of bit flips a code can correct depends on the minimal (Hamming) distance between the words in the codebook:

Definition: Minimal distance

Given a code with codebook C, the minimal distance of that code is defined as

$$d_{\text{min}} := \min_{\substack{x,y \in C \\ x \neq y}} d(x, y).$$

By checking all pairs of codewords of the $[7, 4]$ Hamming code, one can verify that its minimal distance is 3 (for this reason, it is often called a $[7, 4, 3]$ code). Hence, if two bits in a codeword are flipped, it will be closer to some other codeword in terms of number of bit flips. By flipping a single bit, the channel output is (incorrectly) decoded into the message that corresponds to that other codeword.

In general, a code that encodes k input symbols into n output symbols (i.e., that is a $(2^k, n)$ code) and has distance d is often called a $[n, k, d]$ **code**. If the distance is not made specific, it can also be written as an $[n, k]$ **code** (see, for example, the $[7, 4]$ Hamming code).