

# Minimal Distance of Linear Codes

Apart from the trivial way to determine the minimal distance of a code (which is listing the entire codebook and comparing all the codeword pairs), there is a much faster way if the code is linear. It turns out that it already suffices to consider just the Hamming weights of the (nonzero) codewords:

## Proposition

For a linear code  $C$ , the minimal distance is equal to the minimal weight of the nonzero codewords.

Proof

The following derivation proves the claim:

$$d_{\min} = \min_{\substack{x, y \in C \\ x \neq y}} d(x, y) = \min_{\substack{x, y \in C \\ x \neq y}} \sum_{i=1}^n |x_i - y_i| = \min_{\substack{x, y \in C \\ x \neq y}} d(x - y, 0) = \min_{\substack{z \in C \\ z \neq 0}} d(z, 0) = \min_{\substack{z \in C \\ z \neq 0}} |z|,$$

where  $|z|$  denotes the **Hamming weight** of a string  $z$ .

An equivalent way to determine the minimal distance of a linear code is possible if the parity check matrix is known.

## Proposition

For a linear code  $C$  with parity check matrix  $H$ , the minimal distance  $d_{\min}$  equals the minimum number of columns of  $H$  that are **linearly dependent**.

Proof

Left as an exercise.