MATH 525
Section 2.9: Distance of a Linear Code

October 2, 2020

Recall:

- If C is a linear code, then:

$$\begin{aligned} d(C) &= \min\{d(\mathrm{u},\mathrm{v}) \mid \mathrm{u},\mathrm{v} \in C, \mathrm{u} \neq \mathrm{v}\} \\ &= \min\{\mathrm{wt}(\mathrm{u}+\mathrm{v}) \mid \mathrm{u},\mathrm{v} \in C, \mathrm{u} \neq \mathrm{v}\} \\ &= \min\{\mathrm{wt}(\mathrm{w}) \mid \mathrm{w} \in C, \mathrm{w} \neq 0\} \end{aligned}$$

- That is, the distance of C equals the minimum weight of its nonzero codewords.
- For a "small" linear code, one can simply enumerate the weights of the nonzero codewords and then quickly determine the distance of the code. However, this becomes tedious and worse yet, computationally infeasible, as the size of the code grows.
- Fortunately, the distance of a linear code can be determined more easily than brute-forcing through all codewords. The method involves looking for a minimum linearly dependent set of rows of the parity-check matrix H. This is what we will study next.

Lemma

Let H be a parity-check matrix for a linear code C. For each $v \in C$ such that $\mathrm{wt}(v) = \ell$, there exist ℓ rows of H that add up to the zero vector. Conversely, for each set of ℓ rows of H add up to the zero vector, there exists $v \in C$ such that $\mathrm{wt}(v) = \ell$.

The idea for the proof will be discussed during the lecture.

Corollary (Theorem 2.9.1)

Let H be a parity-check matrix for a linear code C. Then C has distance d if and only if any set of $d - 1$ rows of H is linearly independent, and at least one set of d rows of H is linearly dependent.

Example

Determine the distance of the code whose parity-check matrix is

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

The example will be worked out during the lecture.