Edoardo Persichetti Lecture 12: Codes 21/05/2014

Exercise 1 Prove that the Hamming distance is indeed a distance in the metric sense.

Exercise 2 Let $\mathcal{C}$ be an (n, k, d) linear code over $\mathbb{F}_q$. Show that $\mathcal{C}$ is able to correct at most $w = \lfloor \frac{d-1}{2} \rfloor$ errors.

Exercise 3 Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Prove the following facts about the dual code:

- $\mathcal{C}^\perp$ is an $[n, n-k]$ linear code
- $(\mathcal{C}^\perp)^\perp = \mathcal{C}$
- If $G = (I_k|M)$ is a generator matrix in systematic form for $\mathcal{C}$, then $H = (-M^T|I_{n-k})$ is a generator matrix for $\mathcal{C}^\perp$

Exercise 4 Let H be a parity-check matrix for a linear code $\mathcal{C}$. Show that the minimum distance of $\mathcal{C}$ is at least d if and only if every subset of $d-1$ columns of H is composed by linearly independent columns.

Exercise 5 Prove that BCH codes satisfy the BCH bound.