**Linear Codes**

Let: $F = \mathbb{F}_q$ be a finite field with $q = |F|$ elements.

**Definition:** A *linear code* of dimension $k$ and length $n$ (briefly: an $[n, k]$-code) over a field $F$ is a subspace $C \subset F^n$ with $\dim_F(C) = k$.

**Remark:** By definition, a code $C \subset F^n$ is linear $\iff$ $v_1, v_2 \in C, a_1, a_2 \in F \Rightarrow a_1v_1 + a_2v_2 \in C$.

**Definition:** The *Hamming weight* of $v \in F^n$ is

$$\text{wt}(v) = d(0, v) = \#\{i : x_i \neq 0\}, \text{ if } v = (x_1, \ldots, x_n).$$

Thus, the Hamming distance of $v, w \in F^n$ is

(1) \hspace{1cm} d(v, w) = \text{wt}(v - w).

**Proposition 1:** If $C$ is a linear code, then

(2) \hspace{1cm} d(C) = \text{wt}(C) := \min\{\text{wt}(v) : v \in C, v \neq 0\}.

**Definition:** A *generating matrix* of an $[n, k]$-code $C$ is a $k \times n$ matrix $G$ such that

$$C = \text{Rowsp}(G) := \{uG : u \in F^k\}.$$ We say that $G$ is *systematic* if $G = (I_k | P)$. 
**Remark:** By row reduction, every code $C$ is equivalent to a code $C'$ which can be generated by a systematic matrix. (Here, two codes $C, C' \subset F^n$ are called *equivalent* if there exists an $n \times n$ permutation matrix $T$ such that $C' = CT := \{vT : v \in C\}$.)

**Definition:** A *parity-check matrix* of an $[n, k]$-code $C$ is an $m \times n$-matrix $H$ such that

$$C = \text{Null}(H) := \{v \in F^n : Hv^t = 0\}.$$  

**Remark:** Thus, $n - k = \text{rk}(H) \leq m$, so we usually take $m = n - k$.

**Proposition 2:** If $G = (I_k | P)$ is a systematic generating matrix of an $[n, k]$-code $C$, then a parity-check matrix for $C$ is

$$H = (-P^t | I_{n-k}).$$  

**Theorem 4:** If $H$ is a parity-check matrix for $C$, then

$$d(C) = r^*(H) + 1,$$  

where $r^*(H) = \max\{t : \text{every set of } t \text{ columns of } H \text{ is linearly independent}\}$.

**Remark:** We have $r^*(H) \leq \text{rk}(H) = n - k$, so by (4) we get $k \leq n - d + 1$ (Singleton bound).