LINEAR CODES

Definition: C is a linear code of length n over $GF(q)$ if C is a subspace of $V(n,q)$.

By Theorem 2.4, a non-empty subset C of $V(n,q)$ is a linear code if and only if

1. $\underline{u} + \underline{v} \in C$ for all $\underline{u}, \underline{v} \in C$
2. $a\underline{u} \in C$ for all $\underline{u} \in C$ and $a \in GF(q)$.

Definitions:

C is a q-ary $[n,k]$-code if C is a k-dimensional subspace of $V(n,q)$.

Furthermore, if C has minimum distance d, then we say that C is a q-ary $[n,k,d]$-code.

So, if C is a q-ary $[n,k,d]$-code, then

C is a q-ary (n, q^k, d)-code.

If q is prime, then $GF(q) = (\mathbb{Z}_q, +, \cdot)$, an we then take as our alphabet

$$F_q = \mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$$ with mod q arithmetic

Definition: For $\underline{x} \in V(n,q)$, the **weight** $w(\underline{x})$ of $\underline{x}$ is the number of non-zero entries of $\underline{x}$.

Example: In $V(3,3)$, let $\underline{x} = 012$ and $\underline{y} = 111$. Then $w(\underline{x}) = 2$ and $w(\underline{y}) = 3$. Also, $w(\underline{x} - \underline{y}) = 2$ since $\underline{x} - \underline{y} = 201$. Note that $w(\underline{x} - \underline{y}) = d(\underline{x}, \underline{y})$.

In general, ...

Lemma 3.1 If $\underline{x}, \underline{y} \in V(n,q)$, then $d(\underline{x}, \underline{y}) = w(\underline{x} - \underline{y})$.

Proof: — (follow in the notes)

Theorem 3.2 If C is a non-trivial linear code, and $w(C) = \min\{ w(\underline{x}) : \underline{x} \in C \text{ and } \underline{x} \neq \underline{0} \}$, then

$$\boxed{d(C) = w(C)}.$$

Proof: Suppose $\underline{x}, \underline{y} \in C$ with $d(\underline{x}, \underline{y}) = d(C)$.
By Lemma 3.1, $d(C) = d(\underline{x}, \underline{y}) = w(\underline{x} - \underline{y}) \geq w(C)$.

Suppose $\underline{x} \in C$ with $w(\underline{x}) = w(C)$.
By Lemma 3.1, $w(C) = w(\underline{x} - \underline{0}) = d(\underline{x}, \underline{0}) \geq d(C)$.

It follows that $d(C) = w(C)$. ∎