Exercises to Chapter 5

Exercise 5.1. Let C be a linear code of length n and weight 1. Show: $C^\perp$ has no codevectors of weight n.

$w(C) = 1 \iff \exists\, \underline{c} \in C : \ w(\underline{c}) = 1$

$\underline{c} \in C,\ w(\underline{c}) = 1 \Rightarrow \quad \underline{c} = (0, 0, \dots, 0, \underset{(i)}{a}, 0, \dots, 0) \quad a \neq 0$

also $a^{-1}\underline{c} = (0, \dots, 0, 1, 0 \dots, 0) \in C$

Let $\underline{z} \in C^\perp$. Then $\underline{z} \cdot (a^{-1}\underline{c}) = 0$ $= z_i$ so $z_i = 0$. So $w(\underline{z}) \leq n-1$.

Exercise 5.2. Use Theorem 5.1 to show that $(C^\perp)^\perp = C$ for every linear code C.

$C \subseteq \mathbb{F}_q^n$, $\dim C = k \Rightarrow \dim C^\perp = n-k$.

$\dim (C^\perp)^\perp = n - (n-k) = k = \dim C$.

Moreover, if $\underline{c} \in C$, then $\forall \underline{z} \in C^\perp$, $\underline{c} \cdot \underline{z} = 0$. This means $\underline{c} \in (C^\perp)^\perp$. So $\underset{\dim = k}{C} \subseteq \underset{\dim = k}{C^{\perp\perp}}$

$\#C = q^k = \# C^{\perp\perp}$

$C \subseteq C^{\perp\perp}$

$\Rightarrow C = C^{\perp\perp}$.

Exercise 5.3. A linear code C is called ***self-orthogonal*** if $C \subseteq C^\perp$, and ***self-dual*** if $C = C^\perp$. Clearly, a self-dual code is self-orthogonal.

(a) Show: C is self-orthogonal, if and only if $\forall \underline{v}, \underline{w} \in C$, $\underline{v} \cdot \underline{w} = 0$.

(b) Let G be a generator matrix for C. Show: C is self-orthogonal $\iff$ $\boxed{GG^T = \mathbf{0}}$ (zero matrix).

$\underline{v}, \underline{w} \in C \quad \underline{v} = \underline{u}G, \ \underline{w} = \underline{u}'G, \ \underline{u}, \underline{u}' \in \mathbb{F}_q^k$

$\underline{v} \cdot \underline{w} = 0 \iff \underline{v}\,\underline{w}^T = 0 \iff \underline{u}\,G(\underline{u}'G)^T = \underline{u}(GG^T)(\underline{u}')^T = 0$

$\iff GG^T = \mathbf{0}$.

(c) [*2013 exam, B6b*] Show that *binary* self-orthogonal codes have even weight. *Hint*: if $\underline{c} \in C$, what is $\underline{c} \cdot \underline{c}$?

(d) [*2016 B5f*] Show that *ternary* self-orthogonal codes have weight divisible by 3. (Same hint as in (c).)

(e) Which of the following codes are self-orthogonal: $\mathrm{Rep}(n, \mathbb{F}_2)$, E_n?

Exercise 5.4. (a) Show: a linear $[n, k, d]_q$-code C is self-dual $\iff$ C is self-orthogonal and $\boxed{k = n/2}$. Deduce that self-dual codes have even length.

$\dim C = k$
$\qquad \ \, \|$
$\dim C^\perp = n-k$

$C \subseteq C^\perp$

$C = C^\perp$

(b) [*2013 B6c*] Show that a binary code generated by $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ is self-dual.

(c) [*2015 B4g*] Prove that for every even n there exists a 5-ary self-dual code of length n. (*Hint*: look for a matrix.)