

Exercises to Chapter 5

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

$$w(c) = 1 \Leftrightarrow \exists c \in C : w(c) = 1$$

$$c \in C, w(c) = 1 \Rightarrow c = (0, 0, \dots, 0, a, 0, \dots, 0)$$

also (i) $a \neq 0$

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

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

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 $c \in C$, then $\forall z \in C^\perp, c \cdot z = 0$. This means $c \in (C^\perp)^\perp$. So $C \subseteq (C^\perp)^\perp$. $\#C = q^k = \#C^\perp$. $\Rightarrow C = (C^\perp)^\perp$.

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 $\forall v, w \in C, v \cdot w = 0$.

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

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

$$v \cdot w = 0 \Leftrightarrow v w^T = 0 \Leftrightarrow uG(u'G)^T = u(GG^T)(u')^T = 0$$

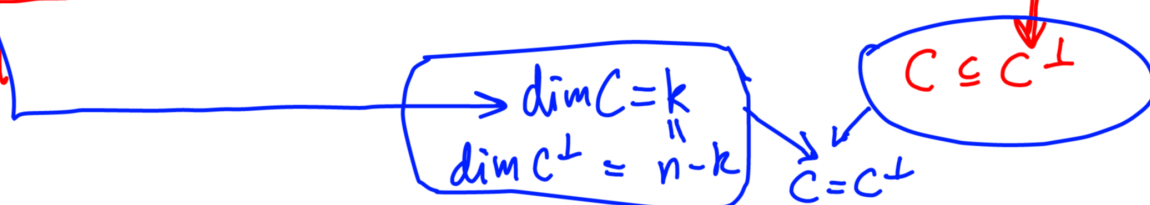
$$\Leftrightarrow GG^T = 0.$$

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

(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: $\text{Rep}(n, \mathbb{F}_2)$, E_n ?

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



(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.)