

Homework #4. Due Thursday, Feb 13th, by 1pm in my mailbox

Reading and plan for the next week:

1. For this homework assignment read 4.3-4.8
2. Plan for next week: 4.8, 5.1 and start 5.2.

Problems:

Note: The order of problems below roughly follows the order in which material was covered in class. In each problem you are allowed to use the results of earlier problems from HW#4 or any problem from HW#1-3 or any theorem from the book (up to Ch 4) or from class, but state clearly what you are using.

1. Problem 4.33.
2. Problem 4.18.
3. Problem 4.21.
4. Problem 4.40.

5.(a) Let C be a $[10, 5]$ -linear code over some finite field F . Suppose that C has a generator matrix G in standard form, so that $G = (I_5|A)$ for some $A \in \text{Mat}_{5 \times 5}(F)$. Prove that C is **self-dual** if and only if $A^T A = -I_5$ (equivalently A is invertible and $A^{-1} = -A^T$). **Hint:** Use Theorem 5.3-5.3' from class and Corollary from Lecture 6 relating a GM in standard form to a PCM in standard form. Remember that most codes have more than one GM and more than one PCM.

(b) Give an example of a self-dual **binary** $[10, 5, 2]$ -linear code. Make sure to explain why your code has distance 2.

(c) Prove that there is no self-dual **binary** $[10, 5, 3]$ -linear code.

(d) **Bonus:** Now prove that there is no self-dual **binary** $[10, 5, 4]$ -linear code.

Hint for (c) and (d): Use the fact that $A^T A = I_n$ for a square matrix $A \iff$ the columns of A are orthogonal to each other and $v \cdot v = 1$ for every column of A . (c) follows quite easily from this fact, (a) and something else you proved earlier. It takes more work prove (d).

6. Problem 4.32. **Note:** Formally, this problem does not fit the setup of Section 4.7 in the book. What is meant here is that we use C to encode each letter individually and then concatenate the results.

7. Problem 4.41.