Homework #4. Due Saturday, February 19th, by 11:59pm in filedrop

All reading assignments and references to exercises, definitions etc. are from our main book 'Coding Theory: A First Course' by Ling and Xing

Reading and plan for the next week:

1. For this homework assignment read 4.2-4.8

2. The main topics next week we will be decoding for linear codes (4.8) and Hamming codes(5.3.1, page 84).

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. (practice, no need to turn in). Recall that most linear codes have more than one generator matrix (GM) and more than one parity-check matrix (PCM). This problem gives a simple characterization of all GMs/PCMs for a given code in terms of a particular GM/PCM.

So let C be an $[n, k]$-linear code over a field F, and let G be a GM for C.

(a) Prove that if G' is an arbitrary GM for C, there exists an invertible $k \times k$ matrix P such that $G' = PG$.

(b) Conversely, prove that for any invertible $k \times k$ matrix P, the matrix $G' = PG$ is a GM for C.

(c) Prove that the analogues of (a) and (b) hold if we replace GMs by PCMs and k by $n - k$.

Note: see page 3 for a detailed hint.

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 $A \in Mat_{5\times5}(F)$. Prove that C is **self-dual** if and only if $A^TA = -I_5$ (equivalently A is invertible and $A^{-1} = -A^T$). **Hint:** Use

Problem 1 and Theorem 6.5 from class relating a GM in standard form to a PCM in standard form.

(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.

Hint for 1. (a) Since G is a GM for C and rows of G' are elements of C, each row of G' can be expressed as a linear combination of rows of G. Show that the latter is equivalent to saying that $G' = PG$ for some $k \times k$ matrix P. Then prove that P is invertible by contradiction: assume that P is not invertible, deduce that $\mathrm{rk}(G') < k$, and then explain why the latter is impossible.

(b) Reversing the argument from (a), use the equality $G' = PG$ to show that $\mathit{Rowspace}(G') \subseteq \mathit{Rowspace}(G)$. Then using the fact that P is invertible, deduce the opposite inclusion $\mathit{Rowspace}(G) \subseteq \mathit{Rowspace}(G')$ and thus $\mathit{Rowspace}(G') = \mathit{Rowpsace}(G)$. Now deduce that rows of G' are linearly independent and conclude that G' is a GM for C.