Math 4452, Spring 2020. Midterm #2

due Friday, March 4th, by 5pm in filedrop

Directions: Provide complete arguments (do not skip steps). State clearly any result you are referring to. Partial credit for incorrect solutions, containing steps in the right direction, may be given.

Rules: You are not allowed to discuss midterm problems with each other. You may ask me any questions about the problems (e.g. if the formulation is unclear), but as a rule I will only provide minor hints. You may freely use class notes (your own notes as well as notes posted on collab), previous homework assignments, our main textbook "Coding theory: a first course" and lectures notes by J. Hall and Y. Lindell. The use of other books or other online resources is prohibited.

Scoring: To be announced by Sunday, Feb 27th.

1. Let C be a linear code over some field F.

(a) Suppose that $d(C) = 2k$ for some $k \in \mathbb{N}$ and there exists a coset D of C such that the **maximum** weight of an element of D is equal to k. Prove that all elements of D have weight k.

(b) Give an example of a code C satisfying the hypotheses of (a). You can pick your field, but you are not allowed to specify k (so you should give a family of examples, one for each k).

2. Let C be the linear code over some finite field F spanned by the following 3 vectors: $10112, 11212, 21021$. Find

(a) a generator matrix for C

(b) a parity-check matrix for C

(c) $d(C)$, the distance of C

Include all the computations and justify all the statements (especially your answer for the distance)

Note: The answer will depend on the characteristic of F. We are not excluding characteristic 2 (by definition, $2 = 1 + 1$ which makes sense in an arbitrary ring with 1).

3. Problem 4.23 from the book.

4. Problem 4.26 from the book.

5.

(a) Write down the parity-check matrix in standard form for the Hamming code $Ham(5, 2)$. **Note:** Recall that Hamming codes are only defined up to equivalence, so the first 26 columns of the matrix can be ordered arbitrarily.

(b) Assuming $Ham(5, 2)$ is used for encoding, decode

$$w = 1^{23}0^8$$

using NND decoding. Make sure to prove your answer! (note that your answer will depend on the order of columns you chose in (a)).

Note for (b): You do not have to use NND decoding as initially defined – instead you can apply any of the algorithms we discussed that yield the same result.

6. In Homework 1 we proved that if C is a binary code of length n and distance 2, then $|C| \leq 2^{n-1}$; thus, if in addition C is linear, then $\dim C \leq n - 1$. The main goal of this problem (part (b) below) is to show that if C is a binary $[n, n - 1, 2]$-linear code, then C is the parity-check code.

(a) Let C be any binary $[n, n - 1]$-linear code. Prove that $d(C) \leq 2$. **Note:** This can be proved in many different ways and the statement actually holds for codes over arbitrary fields.

(b) Prove that if C is a binary $[n, n-1, 2]$-linear code, then C is the parity-check code. **Hint:** Use induction on n and Problem 4.27 (for $q = 2$). If you need a more detailed hint, see next page.

(c) Does there exist a non-linear binary $(n, 2^{n-1}, 2)$-code? Give an example or show that such a code does not exist.

Hint for 6(b): For the induction step take an arbitrary binary $[n, n-1, 2]$-linear code C, consider the set $C' = \{w \in \mathbb{F}_2^{n-1} : w0 \in C\}$ (here $w0$ is the concatenation of w and 0) and show that C' is an $[n-1, n-2, 2]$-linear code.