Math 4452, Spring 2024. Midterm #1
due Friday, March 2nd, by 11:59pm on Canvas

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 Canvas), 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.

1. (8 pts) Let C be a linear code of length n over some field F, and let $v, w \in F^n$. Prove that the following 3 conditions CANNOT hold simultaneously:

(a) $d(C) = 10$
(b) $wt(v) = 4$, $wt(w) = 5$
(c) w and v lie in the same coset of C.

2. (10 pts) Let C be the linear code over some finite field F spanned by the following 3 vectors: $100111, 110122, 112344$. Find

(a) a generator matrix for C
(b) a parity-check matrix for C
(c) $d(C)$, the distance of C
(d) an element of C with the smallest possible nonzero weight.

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 or 3 (by definition, $2 = 1 + 1$, $3 = 1 + 1 + 1$ etc. which makes sense in an arbitrary ring with 1).

3. (12 pts) For each of the following statements determine whether it is true (in all cases) or false (in at least one case). If the statement is true, prove it; if not, give a counterexample (in this case no explanation is needed, but make sure to clearly describe the counterexample).

(a) There exists a linear code C with $|C| = 100$.

(b) Let C be a linear code over some field F, let G be a generator matrix of C. Suppose that $wt(x) \geq 3$ for every row x of G. Then $d(C) \geq 3$.

(c) Let C be an $[n, k]$-linear code, and assume that C is **self-orthogonal**. Then $n \geq 2k$.

(d) Let C be a binary code of length 2024, size 2^{2023} and distance 2. Then C is LINEAR.

4. (10 pts) Problem 4.23 from the book.

5. (10 pts)

(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! (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. (10 pts) Find (with proof) all fields F with the following property:

(*) If C and D are linear codes of the same length over F, C and D are equivalent codes and C is self-dual, then D is also self-dual.

For each field F which has property (*) you need to prove it (for all possible C and D). For each field F which does not have (*), you need to give specific examples of C and D showing that (*) fails (it is enough to give a single example of any length; no need to produce examples of each length).

You may use the following 2 properties of fields without proof. You do not need to use both of them, but you can find either of them helpful:

(i) Fields have no zero divisors: $ab = 0$ implies $a = 0$ or $b = 0$ in any field.

(ii) If F is any field and $u(x) \in F[x]$ is a nonzero polyomial of degree d, then $u(x)$ has at most d roots in F.