Math 4452, Spring 2020. Midterm #2

due Tuesday, April 14th, by 23:59pm 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: The best 4 out of 5 problems will count. Note that problems are not weighted equally! The maximum possible score is 44, but the score of 40 will count as 100%. Solving any 4 problems completely correctly is sufficient to get 40 points.

1. (8 pts) In each part determine if a code with given parameters exists. Make sure to prove your answer.

(a) binary $[12, 11, 2]$-linear code
(b) binary $[12, 6, 5]$-linear code
(c) binary $[12, 5, 6]$-linear code
(d) ternary $[12, 6, 6]$-linear code

2. (10 pts) Problem 5.18. **Hint:** there is something very special about distance 3.

3. (12 pts) In HW#6 we determined the distribution of weights in the extended binary Golay code G_{24} assuming without proof that G_{24} has exactly 759 words of weight 8. The goal of this problem is to prove the latter statement.

Parts (a)-(d) below deal with G_{23}, not G_{24}. For each $k \in \mathbb{N}$ let us denote by $n_k(G_{23})$ the number of words of weight k in G_{23}.

(a) According to Problem 4(c) in HW#6 the following holds: For every $w \in \mathbb{F}_2^{23}$ with $wt(w) = 4$ there exists $c \in G_{23}$ such that $wt(c) = 7$ and $d(w, c) = 3$. Explain why such c must be unique.

(b) Use the result of (a) (as well as Problem 4(c) in HW#6) to prove that

$$\binom{7}{4} \cdot n_7(G_{23}) = \binom{23}{4}.$$

Deduce that $n_7(G_{23}) = 253$.

(c) Now prove that for every $w \in \mathbb{F}_2^{23}$ with $wt(w) = 5$ there exists unique $c \in G_{23}$ such that either $wt(c) = 7$ and $d(w, c) = 2$ or $wt(c) = 8$ and $d(w, c) = 3$.

(d) Use (c) to find a relation of the form $An_7(G_{23}) + Bn_8(G_{23}) = C$ where A, B, C are some (explicit) binomial coefficients. Use this relation to prove that $n_8(G_{23}) = 506$.

(e) Now use (b) and (d) to prove that G_{24} has exactly 759 words of weight 8.

4. (10 pts) Problem 7.35.

5. (12 pts)

(a) Factor $x^{24} - 1$ as a product of monic irreducibles in $\mathbb{F}_2[x]$. Make sure to prove your answer.

(b) List all polynomials $g(x) \in \mathbb{F}_2[x]$ which are generators for binary cyclic codes of length 24 and dimension 18.

(c) Prove that there exists unique binary cyclic code of length 24 which is self-dual. What is the generator polynomial for that code? You may use without proof that $\overline{u(x) \cdot v(x)} = \overline{u(x)} \cdot \overline{v(x)}$ for any polynomials $u(x), v(x) \in F[x]$ (F is any field) where $\overline{f(x)}$ is the reciprocal polynomial of $f(x)$.

(d) Use (c) to prove that the extended Golay code G_{24} is NOT equivalent to a cyclic code.

(e) Find (with proof) $n \in \mathbb{N}$ such that there exists more than one binary cyclic self-dual code of length n.