Math 4452, Spring 2024. Final exam

due Friday, May 10th, by NOON 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 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 system: The base score is the sum of the top 5 scores on the first 6 problems. The maximum base score is 60 points; however, not all problems have the same weight, so it is not sufficient to solve any 5 problems correctly to get 60 points. The bonus problem is worth 7 points, so the maximum score with the bonus is 67.

1. (10 pts) Problem 5.18 from the book.

2. (12 pts) Let F be a field and $n \in \mathbb{N}$. Given two words $v, w \in F^n$ define the *burst distance* between v and w, denoted by $BD(v, w)$ by $BD(v, w) = BL(v - w)$ (where as usual BL stands for burst length). One can think of $BD(v, w)$ as the burst length of the transmission error that must occur if v is the word sent and w is the word received.

(a) Give a specific example showing that BD does NOT satisfy the triangle inequality.

(b) Use the notion of burst distance to formulate an explicit decoding rule, let us call it *NBND (nearest burst neighbor decoding)* that is analogous to the usual NND (nearest neighbor decoding), but designed specifically for correcting burst errors. Your rule should satisfy the following property: if C is a linear code which is l-burst error correcting for some $l \in \mathbb{N}$ and if the transmission error e satisfies $BL(e) \leq l$, then NBND works correctly (that is, correctly recovers the codeword sent).

(c) Now prove that your NBND rule satisfies the property stated in part (b). **Hint:** Use Lemma 22.2 from Spring 24 online notes.

(d) Give an example of a specific code $C \subseteq F^n$ and an element $w \in F^n$ such that NND and NBND will decode w to different codewords in C.

3. (12 pts)

(a) Let $C \subseteq F^n$ be an MDS code and $I \subseteq \{1, \dots, n\}$ with $|I| < d(C)$. Prove that the punctured code C_I is also MDS. (Recall that C_I is obtained from C by removing the i^{th} coordinate for every $i \in I$).

(b) (not directly related to (a)) Let F be a finite field, $q = |F|$, $\alpha_1, \dots, \alpha_n$ distinct elements of $F \setminus \{0\}$ (so that $n \le |F| - 1$) and $v_1, \dots, v_n, u, w$ nonzero elements of $F \setminus \{0\}$ (total of $n + 2$ elements, repetitions allowed). Let $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$ and $\vec{v} = (v_1, \dots, v_n)$. Finally fix $1 \le k \le n$. Recall that the doubly extended GRS code $GRS_k(\vec{\alpha}, \vec{v}, u, w)^{\text{DE}}$ is a linear code of length $n + 2$ over F defined by

$$GRS(\vec{\alpha}, \vec{v}, u, w)^{\text{DE}} = (v_1 f(\alpha_1), \dots, v_n f(\alpha_n), u f(0), v f_{k-1})$$

where f ranges over all polynomial of degree $< k$ in $F[x]$ and f_{k-1} is the coefficient of x^{k-1} in f. Prove that $GRS(\vec{\alpha}, \vec{v}, u, w)^{\text{DE}}$ is an MDS code.

4. (12 pts) Let C be an $[n, k]$-linear MDS code over $\mathbb{F}_q$, and assume that $k \neq n$ (that is, C is not the full code).

(a) Prove that if $k = n - 1$, then C is equivalent to the zero sum code ZS_n.

(b) Prove that if $k = 1$, then C is equivalent to the simple repetition code $Rep(1, n)$.

In parts (c) and (d) we assume that $1 < k < n - 1$.

(c) Prove that $k \le q - 1$.

(d) Now prove that $n - k \le q - 1$ and deduce that $n \le 2q - 2$.

Hint: build on the idea from HW#10.3. Here is an additional observation that may be helpful. Note that if H is a PCM for a code C and we multiply a fixed row of H by a nonzero scalar, the code will not change (explain why). If we multiply a fixed column of H by a nonzero scalar, the code will be replaced by an equivalent one (so will still be MDS if C was MDS). Using these operations, we can assume that all the entries in any fixed row or column of H are equal to 0 or 1 (again explain why).

5. (14 pts)

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

(b) Use (a) to show that there are exactly 81 binary cyclic codes of length 24.

(c) Prove that there exists a unique binary cyclic code of length 24 which is self-dual. What is the generator polynomial for that code? **Hint:** A problem from HW#9 is relevant here.

(d) Use (c) to prove that the extended Golay code G_{24} is NOT equivalent to a cyclic code. **Hint:** A problem from Midterm #1 us relevant here.

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

6. (12 pts) Let $r \geq 2$ be an integer.

(a) Let C be $[2^r-1, 2^r-r-1, 3]$-linear code and let H be a PCM of C. Prove that every nonzero element of $\mathbb{F}_2^r$ must appear among the columns of H exactly once. Note that this implies two things:

(i) Any such code C is equivalent to $Ham(r,2)$ (in fact, we can say "equal to $Ham(r,2)$" since the latter is only defined up to equivalence)

(ii) Any two possible PCMs of $Ham(r,2)$ are obtained from each other by permutation of columns. This is a very rare property – for most codes one can find two very different looking PCMs.

(b) Prove that $Ham(r,2)$ is NOT 2-burst error correcting no matter how one orders the columns of its PCM. **Note:** If C and C' are equivalent codes, they have the same distance and hence the maximal number of random errors they can correct are the same. This is not the case for burst-error correction: in general one may be able to improve the burst-error correcting capability of a code by permuting the coordinates. What you have to show in (b) is that there will be no such improvement for the Hamming code.

Bonus. (7 pts) Prove Theorem 27.1(a) from class restated below. Consider a concatenated code $C = B \circ A$, and suppose we are using the errors-and-erasures decoding rule EED_s for some $0 \leq s \leq \lfloor \frac{d(B)-1}{2} \rfloor$. Let $c = c_1 \ldots c_N$ be the codeword sent, $w = w_1 \ldots w_N$ the received word and $u = u_1 \dots u_N$ the semi-decoded word (in the terminology of Lecture 26, 27).

(i) Let e_s be the number of errors in u (in the notations from Lecture 27), that is, e_s is the number of indices i for which $u_i \neq c_i$ and EED_s does not replace u_i by the erasure symbol (which by definition happens if and only if $d(u_i, w_i) \leq s$).

(ii) Let E_s be the number of erasures in u (in the notations from Lecture 27), that is, e_s is the number of indices i for which $u_i \neq c_i$ and EED_s does replace u_i by the erasure symbol (which by definition happens if and only if $d(u_i, w_i) > s$).

Assume that the total number of transmission errors (which by definition is $d(c, w)$) is at most $\lfloor \frac{d(B)d(A)-1}{2} \rfloor$. Prove that there exists s such that $2e_s + E_s < d(A)$. **Hint:** Argue by contrapositive (assume that $2e_s + E_s \geq d(A)$ for all s and deduce that $d(c, w) > \lfloor \frac{d(B)d(A)-1}{2} \rfloor$)

Note: This result is essentially proved in Lemma 7.5 of Lindell's notes; however, the proof uses continuous random variables. The goal of this problem is to give a completely elementary argument, not involving any probability techniques or terminology.

A detailed hint: Note that $d(c, w) = \sum_{i=1}^{N} d(c_i, w_i)$. Fix s and for each $1 \leq i \leq N$ determine whether

(a) c_i is decoded correctly ($u_i = c_i$ and u_i is not replaced by erasure)

(b) erasure occurs (u_i is replaced by erasure);

(c) possible error (it is possible that $u_i \neq c_i$ and u_i is NOT replaced by erasure)

based on $d(c_i, w_i)$ and s.

You can assume that errors do occur whenever they can occur since replacing a correctly decoded symbol or an erasure by an error will only increase the quantity $2e_s + E_s$. Now for $k = 1, 2, \dots$ let n_k be the number of indices i such that $d(c_i, w_i) = k$. For each $0 \leq s \leq \lfloor \frac{d(B)-1}{2} \rfloor$ express $2e_s + E_s$ in terms of the numbers $n_1, n_2, \dots$ and get a system of inequalities. Now combine these inequalities in a suitable way to dedice that $d(c, w) > \lfloor \frac{d(B)d(A)-1}{2} \rfloor$. Consider separately the cases where $d(B)$ is even and where $d(B)$ is odd.