Math 4452, Spring 2020. Final exam

due Thursday, May 7th, 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 system: The best 5 out of 6 problems will count. Each problem is worth 12 points, so the entire exam is worth 60 points.

1. Problem 4.26 from the book.

2. 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 21.2.

(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. Let $n \geq 2$ be an integer.

(a) Find the parity-check matrix in STANDARD FORM for each of the following codes: PCC_n (parity-check code of length n) and Rep_n, the simple binary repetition code of length n. Prove your answer.

(b) Let C be a BINARY MDS code of length n. Prove that C is equal to the full code F^n, PCC_n or Rep_n. **Hint:** Let $k = \dim(C)$. Assuming that $C \neq F^n$, we get that $k < n$, so that PCM of C is non-empty. After replacing C by an equivalent code, we can assume that C has a PCM H in the standard form, so that the last $n-k$ columns of H form the identity matrix. Now use a suitable theorem to show that there are very few choices for the remaining columns of H and eventually deduce that H must coincide with one of the two matrices from your answer in (a). Note that this would only prove that C is equivalent to PCC_n or Rep_n. You still have to explain why C is EQUAL to one of those codes.

4. 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.

5. We are back to studying the Hamming code. First we need some general terminology. Let p be a prime, $r \in \mathbb{N}$ and let $F = \mathbb{F}_{p^r}$. One can show that for any $\alpha \in F$ there exists unique monic polynomial $\mu_\alpha(x) \in \mathbb{F}_p[x]$ of smallest possible degree such that $\mu_\alpha(\alpha) = 0$. The polynomial μ_α is called the *minimal polynomial of* α *over* $\mathbb{F}_p$. It is not hard to show that

(i) $\deg(\mu_\alpha) \leq r$ for all $\alpha \in F$
(ii) If α is primitive, then $\deg(\mu_\alpha) = r$

Now the actual problem. Let $p = 2$, $r \geq 2$, and assume that $\alpha \in \mathbb{F}_{2^r}$ is primitive, and let $g(x) = \mu_\alpha(x)$ be its minimal polynomial. Let C be the binary cyclic code of length $2^r - 1$ generated by $g(x)$. Prove that C is a $[2^r - 1, 2^r - r - 1, 3]$-code and deduce from Problem 4(a) that C is equivalent to $Ham(r, 2)$. This proves that binary Hamming codes can be made cyclic with a suitable ordering of columns of PCM.

Hint: To prove that $d(C) = 3$ argue by elimination. The possibility that $d \geq 4$ can be eliminated from very general considerations; $d \neq 1$ follows easily from the fact that C is cyclic, and finally prove that $d \neq 2$ using that C is cyclic and α is primitive.

6. The goal of this problem is to prove an analogue of Theorem 24.2 from class for arbitrary q.

(a) Fix integers $n, q \geq 2$, and for $0 \leq i \leq n-1$ let

$$f(i) = \binom{n}{i}(q-1)^i.$$

Let $i_0 = \lfloor n \cdot \frac{q-1}{q} \rfloor$. Prove that $f(j) \leq f(i_0)$ for all $1 \leq j \leq i_0$.

(b) Recall that for $0 \leq d \leq n$ we defined $V_n^q(d) = \sum_{i=0}^{d} \binom{n}{i}(q-1)^i$. Now fix a real number $0 < \delta < \frac{q-1}{q} = 1 - \frac{1}{q}$, and for each $n \in \mathbb{N}$ let $d_n = \lfloor n\delta \rfloor$. Compute

$$\lim_{n\to\infty} \frac{\log_q V_n^q(d_n)}{n}.$$

Hint: The answer will be similar to the entropy function H we got in the case $q = 2$ except that it will have 3 terms (one of the terms will vanish for $q = 2$).