Math 5251 Error-correcting codes and finite fields
Fall 2021, Vic Reiner
Final exam
Due Wednesday Dec. 15 by 11:59pm, on Canvas

Instructions: This is an open book, open library, open notes, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult.

1. (20 points total; 5 points each) True or False. Your answers must be justified either by counterexamples or proofs to receive full credit.

(a) The quotient ring $\mathbb{F}_2[x]/(x^4+x^2+1)$ is a finite field with 16 elements.

(b) In $\mathbb{F}_5[x]/(x^2+x+1)$, the element $\alpha = \overline{x}$ is a primitive root.

(c) There exists at least one $\mathbb{F}_2$-linear code $\mathcal{C}$ of blocklength 5 for which the vector $[1,0,0,0,0]$ is **not** a coset leader.

(d) The first-order Reed-Muller code with blocklength $n = 64$ can correct up to 32 errors.

2. (20 points total) Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[n,k,d]$-code with blocklength $n = 9$ and minimum distance $d = 5$ that achieves the *highest possible* dimension k among all such $\mathbb{F}_2$-linear $[9,k,5]$ codes. For these specific values of n and d, what ...

(a) (4 points) does Hamming's sphere-packing bound say about k?
(b) (4 points) does the Singleton bound say about k?
(c) (4 points) does the Gilbert-Varshamov bound say about k?
(d) (4 points) does the Plotkin bound say about k?
(e) (4 points) are the only two possibilities for the *exact* number m of codewords in $\mathcal{C}$?
(Your answer to (e) should be two integers less than $1,000,000$.)

3. (10 points total) Compute explicitly the multiplicative inverse $[\overline{x^2+1}]^{-1}$ to the element $\overline{x^2+1}$ within $\mathbb{F}_2[x]/(x^5+x+1)$.

4. (15 points) Find **all** primitive roots in $\mathbb{F}_3[x]/(x^2+1)$, expressing each uniquely as an $\mathbb{F}_3$-linear combination $a+b\delta$ where $\delta=\overline{x}$ and $a,b\in\mathbb{F}_3$. Explain how you know that your list is correct.

5. (15 points total) Let $\mathcal{C}$ be the cyclic code inside $(\mathbb{F}_2)^{11}$ defined as the row space of the 11×11 circulant matrix with first row $[1,0,0,1,0,0,0,0,0,0,0]$.

(a) (10 points) Find $k=\dim_{\mathbb{F}_2}(\mathcal{C})$.

(b) (5 points) Find a matrix H whose rowspace is $\mathcal{C}^\perp$.

6. (20 points total) Let H be this matrix with entries in $\mathbb{F}_3$

$$H=\begin{bmatrix}1&2&1&1&0\\1&1&2&0&1\end{bmatrix}$$

whose rowspace is the dual code $\mathcal{C}^\perp$ to an $[n,k,d]$ $\mathbb{F}_3$-linear code $\mathcal{C}$.

(a) (5 points) What is n?

(b) (5 points) What is k?

(c) (5 points) What is d?

(d) (5 points) What is the maximum number of errors $\mathcal{C}$ can correct?