Math 5251 Error-correcting codes and finite fields
Spring 2022, Vic Reiner
Final exam
Due Wednesday May 4 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. (30 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 $\mathbb{F}_3[x]/(x^2+x+1)$ is a finite field with 9 elements.

(b) In the field $\mathbb{F}_3[x]/(x^2+1)$, the element $\alpha = \overline{x}$ is a primitive root.

(c) In a finite field $\mathbb{F}_{2^5}$, having 2^5 elements, there will be 30 elements which are primitive roots.

(d) When decoding using an $[7, 5, 4]$ $\mathbb{F}_3$-linear code $\mathcal{C}$, the syndrome table must list 9 possible syndromes.

(e) The first-order Reed-Muller code with blocklength $n = 32$ can *detect* up to 15 errors.

(f) One can create a Reed-Solomon code with parameters $[n, k, d] = [24, 9, 20]$.

2. (15 points total; 5 points each) Let $R = \mathbb{F}_5[x]/(x^3+x+1)$, a quotient ring of $\mathbb{F}_5[x]$.

(a) (5 points) Prove that R is a field.

(b) (5 points) What is the cardinality (=size) of R?

(c) (5 points) Let α denote the image of the polynomial $x + 1$ in the quotient ring R. Find its multiplicative inverse α^{-1} in R explicitly.

3. (30 points total; 5 points each) Let H be this matrix with entries in $\mathbb{F}_2$

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

whose rowspace is the dual code $\mathcal{C}^{\perp}$ to an $[n,k,d]$ $\mathbb{F}_2$-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?

(e) (5 points) Write down a generator matrix G whose row space is $\mathcal{C}$.

(f) (5 points) Write down a syndrome table that you could use in decoding transmitted words from $\mathcal{C}$. Explain how you got the table.

4. (15 points total; 5 points each) Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[n,k,d]$-code with blocklength $n = 11$ and minimum distance $d = 5$ that achieves the *highest possible* dimension k among all such $\mathbb{F}_2$-linear $[11,k,5]$ codes. For these specific values of n and d, what ...

(a) (5 points) does Hamming's sphere-packing bound say about k?
(b) (5 points) does the Gilbert-Varshamov bound say about k?
(c) (5 points) are the only two possibilities for the *exact* number m of codewords in $\mathcal{C}$?
(Your answer to (c) should be two integers less than 2000.)

5. (10 points total; 5 points each) Let $\mathcal{C}$ be the cyclic code inside $(\mathbb{F}_2)^9$ defined as the row space of the 9×9 circulant matrix with first row $[1,1,1,0,0,0,0,0,0]$.

(a) (5 points) Find $k = \dim_{\mathbb{F}_2}(\mathcal{C})$.

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