Math 5251 Error-correcting codes and finite fields
Fall 2024, Vic Reiner
Final exam
Due Wednesday December 11 by 11:59pm, on Canvas

Instructions: This is an open book, open notes, open web, take-home exam, but you may *not* collaborate. You must **clearly indicate** any such sources used, including AI sources such as ChatGPT. The instructor is the only human source that you are allowed to consult.

1. True or False. Your answers must be justified either by counterexamples or proofs to receive full credit.

(a) (10 points) The quotient ring $\mathbb{F}_2[x]/(x^4 + x^2 + 1)$ is a finite field with 16 elements.

(b) (10 points) The first order Reed-Muller code of blocklength 128 can correct up to 64 errors.

2. (20 points) Prove that in any binary Huffman encoding of a memoryless source W with m words having probabilities $(p_1, \ldots, p_m)$, the longest code word has length **at most** $m - 1$.

3. (20 points total; 5 points each) Consider an $\mathbb{F}_2$-linear code $\mathcal{C}$ with generator matrix

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

(a) (5 points) What are the parameters $[n, k, d]$ for $\mathcal{C}$?

(b) (5 points) Compute a generator matrix H for the dual code $\mathcal{C}^{\perp}$.

(c) (5 points) Write down a syndrome table listing all possible syndromes for the cosets of $\mathcal{C}$, along with a choice of at least one coset leader for each coset having that syndrome.

(d) (5 points) Are all the choices of coset leaders in (c) unique?

4. (20 points total) Let $\mathcal{C}$ be the $\mathbb{F}_2$-linear cyclic code whose generator matrix G is the circulant matrix having first row

$$[1, 1, 1, 1, 0, 0, 0, 0, 0] .$$

Compute the parameters $[n, k, d]$ for $\mathcal{C}$.

5. (20 points total) Let $\mathcal{C}$ be any $\mathbb{F}_2$-linear code that achieves the maximum possible dimension k among all codes with parameter list $[n, k, d] = [9, k, 5]$, so $\mathcal{C}$ has blocklength 9 and minimum distance 5.

(a) (10 points) What does the Gilbert-Varshamov bound say about k?

(b) (10 points) What does the Plotkin bound say about k?