Math 5251 Error correcting codes and finite fields
Final Exam

Spring 2023, Trevor Karn

Due May 3, 2023, by 4:00pm via Canvas or Hardcopy

Instructions: This is an open book, open library, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult. All sources used must be cited. In particular, Artificial Intelligence, class notes, and textbook use must be cited.

1. (20 points total; 5 points each) **True or False.** Your answers must by justified either by counter examples or proofs to recieve full credit.

   (a) The quotient ring $\mathbb{F}_5[x]/(x^2+3x+1)$ is a finite field with 25 elements.

   (b) Let α denote the image of x in the field $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$. Then the element α^2 is a primitive root.

   (c) A finite field $\mathbb{F}_{10007}$ with 10007 elements has 5000 primitive roots.

   (d) There are three cosets of the code $\mathcal{C}$ generated by the matrix

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

   inside of $(\mathbb{F}_7)^7$.

2. (a) (10 points) Give a finite number $q > 2$ and a polynomial $f \in \mathbb{F}_q[x]$ of degree 3 or 4 such that $R = \mathbb{F}_q[x]/(f)$ is a finite field different from all of the fields in question 1. Prove that R is a field.[1]

   (b) (5 points) What is the cardinality of the field R from 2(a)?

   (c) (5 points) Let α denote the image of x in R, the field from 2(a). Explicitly compute $\frac{1}{\alpha+2}$, the multiplicative inverse of $\alpha+2$ in R.

3. (a) (5 points) Write down a 3×5 matrix H with entries in $\mathbb{F}_2$ that is a standard form matrix generating a dual code $\mathcal{C}^{\perp}$.[2]

   (b) (15 points) The matrix you wrote down in 3(a) is dual to an $[n,k,d]$ $\mathbb{F}_2$-linear code $\mathcal{C}$. What are the values of n,k,d?

   (c) (5 points) What is the maximum number of errors the code $\mathcal{C}$ from 3(b) can correct?

[1] If you would like to skip this question and earn no points for part 2(a), you may use $R = \mathbb{F}_2[x]/(x^2+x+1)$ for parts 2(b) and 2(c).

[2] If you would like to skip this question and earn no points for part 3.(a), you may use

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

for parts 3.(b)-3.(e).

(d) (5 points) Write down a generator matrix G in standard form whose row space is $\mathcal{C}$, the code from 3(b).

(e) (10 points) Write down a syndrome table (consisting of column for coset leaders and a column for syndromes) that you could use to decode transmitted words from $\mathcal{C}$, the code from 3(b). Explain how you find the table.

4. (a) (5 points) Give a number q with $2 < q < 10$ and polynomial $g \in \mathbb{F}_q[x]$ of degree 5 generating a cyclic code $\mathcal{C}$ with block size 9 over $\mathbb{F}_q$.[3]

(b) (5 points) Give another polynomial $\tilde{g}$ generating the code $\mathcal{C}$ from part 4(a).

(c) (5 points) What is the dimension of $\mathcal{C}$, the code from 4(a)?

(d) (5 points) Give a circulant matrix generating the dual code $\mathcal{C}^{\perp}$, dual to the code $\mathcal{C}$ from 4(a).

[3] If you would like to skip this question and earn no points for part 4(a), you may use $g(x) = 1 + x + x^4 + x^5$ in $\mathbb{F}_2[x]$ for parts 4.(b)-4.(d).