Math 5251 Error-correcting codes and finite fields
Fall 2021, Vic Reiner
Midterm exam 2
Due Wednesday Nov. 17 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) In $\mathbb{Z}/98765432$, the element $\overline{10000000000000000000}$ has a multiplicative inverse.

(b) In $\mathbb{Z}/987654321$, the element $\overline{10000000000000000000}$ has a multiplicative inverse.

(c) There exist integers $m > 1$ for which $\mathbb{Z}/(3^m - 1)$ is a field.

(d) When n is odd, an $\mathbb{F}_2$-linear code $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$ inside $(\mathbb{F}_2)^n$ will always intersect only in the zero vector $\underline{0}$, that is, $\mathcal{C} \cap \mathcal{C}^\perp = \{\underline{0}\}$.

(e) Let $\mathcal{C}$ be the $\mathbb{F}_7$-linear code in $(\mathbb{F}_7)^5$ whose *dual* code $\mathcal{C}^\perp$ has as its generator matrix the 1×5 matrix

$$H = \begin{bmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \end{bmatrix}.$$

Then $m = |\mathcal{C}| = 2401$.

(f) For $\mathcal{C}$ the same code as in part (e), the minimum distance $d(\mathcal{C}) = 3$.

2. (a) (10 points) The integer 1223 is prime, and so we know $\alpha = \overline{200}$ in $\mathbb{F}_{1223}$ has a multiplicative inverse α^{-1}. Find α^{-1} explicitly, using the extended Euclid algorithm.

(b) (10 points) The polynomials

$$f(x) = x^2 + 1$$
$$g(x) = x^4 + x + 1$$

in $\mathbb{F}_2[x]$ have no common factors. Hence there will exist polynomials $a(x), b(x)$ in $\mathbb{F}_2[x]$ satisfying $a(x)f(x) + b(x)g(x) = 1$. Find such polynomials $a(x), b(x)$ explicitly, using the extended Euclid algorithm.

3. (a) (5 points) List all of the irreducible polynomials in $\mathbb{F}_2[x]$ whose degrees are $1, 2$ or 3, and explain how you know that they are irreducible.

(b) (10 points) Write down the unique factorization into irreducibles in $\mathbb{F}_2[x]$ for $x^7 + x^2 + x + 1$, with proof that it is correct.

4. (15 points total) Let G be the following matrix

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

(a) (5 points) Thinking of the entries of G as elements of $\mathbb{F}_2$, let $\mathcal{C}_1$ be the $\mathbb{F}_2$-linear code in $(\mathbb{F}_2)^8$ having G as its generator matrix, that is, $\mathcal{C}_1$ is the row space of G. What is the (binary) rate of $\mathcal{C}_1$?

(b) (5 points) What is the minimum distance of $\mathcal{C}_1$, and up to how many errors can it correct?

(c) (5 points) Now think of the entries of G as elements of $\mathbb{F}_3$. so that G generates an $\mathbb{F}_3$-linear code $\mathcal{C}_2$ in $(\mathbb{F}_3)^8$. What is the (ternary) rate of $\mathcal{C}_2$?

5. (a) (5 points) Find a representative for $\overline{1000}$ in $\mathbb{Z}/37$ that lies within the set of residues $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{36}\}$.

(b) (5 points) Do the same for $\overline{1,000,000}$ in $\mathbb{Z}/37$.

(c) (10 points) Prove that if a number N is written in decimal notation with digits $a_\ell a_{\ell-1} \cdots a_2 a_1 a_0$ (so that a_0 is the ones digit, a_1 is the tens digit, a_2 the hundreds digit, etc) then in $\mathbb{Z}/37$ one has

$$\overline{N} = \cdots + \overline{a_5 a_4 a_3} + \overline{a_2 a_1 a_0}.$$

For example, in $\mathbb{Z}/37$ one has $\overline{41,246,789,963} = \overline{41} + \overline{246} + \overline{789} + \overline{963}$.