Math 5251 Error-correcting codes and finite fields
Spring 2022, Vic Reiner
Midterm exam 2
Due Wednesday Apr. 6 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 $\mathbb{Z}/9876543$, the element $\overline{10000000000000000000}$ has a multiplicative inverse.

(b) In $\mathbb{Z}/987654$, the element $\overline{10000000000000000000}$ has a multiplicative inverse.

(c) There exists an integer $m \geq 1$ for which $\mathbb{Z}/(5^m - 1)$ 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 $\mathbb{F}_{11}$-linear code in $(\mathbb{F}_{11})^6$ whose *dual* code $\mathcal{C}^\perp$ has as its generator matrix the 1×6 matrix

$$H = \begin{bmatrix} \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{7} \end{bmatrix}.$$

Then $m := |\mathcal{C}| = 161051$.

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

2. (a) (10 points) The integer 7919 is prime, and so we know $\alpha = \overline{100}$ in $\mathbb{F}_{7919}$ has a multiplicative inverse α^{-1}. Find α^{-1} explicitly, using the extended Euclid algorithm.

(b) (10 points) The polynomials

$$f(x) = x^2$$
$$g(x) = x^5 + x + 1$$

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. Let $\mathcal{C} \subseteq (\mathbb{F}_5)^{12}$ be the following $\mathbb{F}_5$-linear code:

$$\begin{aligned}\mathcal{C} = \{\mathbf{x} = [x_1, \ldots, x_{12}] \in (\mathbb{F}_5)^{12} : \ & x_1 = x_2 = x_3 = x_4, \\ & x_5 = x_6 = x_7 = x_8, \\ & x_9 = x_{10} = x_{11} = x_{12}\}.\end{aligned}$$

So $\mathcal{C}$ is the third extension of the 4-fold repetition code over $\mathbb{F}_5$.

(a) (5 points) What is the dimension $k = \dim_{\mathbb{F}_5}(\mathcal{C})$?

(b) 5 points) What is the 5-ary rate of $\mathcal{C}$?

(c) (5 points) What is the minimum distance $d(\mathcal{C})$?

(d) (5 points) Write down a generator matrix G for $\mathcal{C}$.

(e) (5 points) Write down a generator matrix H for its dual code $\mathcal{C}^{\perp}$.

(f) (5 points) What is the 5-ary rate of its dual code $\mathcal{C}^{\perp}$?

4. (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 $\overline{41,246,789,963} = \overline{41} + \overline{246} + \overline{789} + \overline{963}$.