

Math 5251 Error-correcting codes and finite fields, Fall 2024,  
Vic Reiner

Midterm exam 2

Due Wednesday November 13 by 11:59pm, via 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. (25 points total) Let  $p$  be a prime number, and  $\mathcal{C}$  an  $\mathbb{F}_p$ -linear code with a generator matrix

$$H = [\bar{3} \ \bar{4} \ \bar{5} \ \cdots \ \overline{m-1} \ \bar{m}]$$

for some integer  $m$  with  $5 \leq m \leq p-1$ .

(a) (15 points) Compute the three parameters  $[n, k, d]$  for  $\mathcal{C}$  as a linear code, and justify your answer.

(b) (10 points) Compute the three parameters  $[n, k, d]$  for its dual code  $\mathcal{C}^\perp$ , and justify your answer.

2. (25 points) For each prime number  $p$ , either construct explicitly a linear code  $\mathcal{C}$  having  $|\mathcal{C} \cap \mathcal{C}^\perp| = p$ , or prove that none can exist.

3. (25 points) Let  $a, b, c$  be distinct positive integers, and  $p$  a prime number. Does  $x^5$  have a multiplicative inverse in  $\mathbb{F}_p[x]/(1+x^a+x^b+x^c)$ ? Prove your answer.

4. (25 points total)

(a) (5 points) Compute  $GCD(41, 100000)$ , showing your work.

(b) (5 points) Compute  $(\overline{41})^{-1}$  in  $\mathbb{Z}/100000$ , showing your work.

(c) (5 points) Compute  $(\overline{100000})^{-1}$  in  $\mathbb{Z}/41$ , showing your work.

(d) (10 points) Let  $N$  be a positive integer written in decimal notation

$$N = \cdots d_{14}d_{13}d_{12}d_{11}d_{10}d_9d_8d_7d_6d_5d_4d_3d_2d_1d_0,$$

meaning that  $d_0$  is the ones digits,  $d_1$  is the tens digits,  $d_2$  is the hundreds digit, etc. Prove that in  $\mathbb{Z}/41$ , one has

$$\overline{N} = \cdots + \overline{d_{14}d_{13}d_{12}d_{11}d_{10}} + \overline{d_9d_8d_7d_6d_5} + \overline{d_4d_3d_2d_1d_0},$$

where each of  $d_4d_3d_2d_1d_0$ ,  $d_9d_8d_7d_6d_5$ ,  $d_{14}d_{13}d_{12}d_{11}d_{10}$ ,  $\dots$  is again a number written in decimal notation.