MA4891 Error-Correcting Codes
W. J. Martin
March 25, 2020

Codes Assignment 1

DUE DATE: Thursday, April 2, by 11:59pm sent to me (as a single readable PDF file) via email.

Please carefully read the presentation rules below. The problem statements begin below the rules at the bottom of the page.

BASIC RULES FOR MA4891 ASSIGNMENTS

I) Each student must compose his/her assignments independently. However, rough work may be done in groups;

II) Write legibly and use only one side of each sheet of paper;

III) Show your work. Explain your answers using FULL SENTENCES;

IV) Scan the pages and submit the assignment as a single PDF document via email. (Pro tip: Learn how to do this ASAP, not at the deadline.)

Please complete the following five problems.

1. Working over the finite field $\mathbb{F}_7$,

   (a) find the inverse of the matrix $M = \begin{bmatrix} 1 & x \\ 0 & 2 \end{bmatrix}$ where $a \in \mathbb{F}_7$ is arbitrary.

   (b) find the inverse of

   $$N = \begin{bmatrix} 4 & 0 & 2 \\ 2 & 4 & 0 \\ 0 & 2 & 4 \end{bmatrix}$$

   (c) perform the appropriate row operations to bring the following matrix into reduced row echelon form (RREF):

   $$A = \begin{bmatrix} 1 & 1 & 4 & 0 & 0 \\ 1 & 6 & 1 & 1 & 3 \\ 5 & 1 & 0 & 1 & 4 \\ 0 & 0 & 0 & 3 & 6 \end{bmatrix}.$$

2. Let $C \subset \mathbb{F}_q^n$ be any non-empty code and let $C^+ \subseteq \mathbb{F}_q^{n+1}$ be the *extended code*[1] of C:

$$C^+ = \left\{ \mathbf{x} \in \mathbb{F}_q^{n+1} \,\middle|\, (x_1, \ldots, x_n) \in C, \ \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

   Prove:

   (a) $|C^+| = |C|$

   (b) $d_{\min}(C^+) = d_{\min}(C)$ or $d_{\min}(C^+) = d_{\min}(C) + 1$.
   (When does the second case occur?)

   (c) C^+ is additive (resp., linear) if and only if C is additive (resp., linear)

3. The *International Standard Book Number* (ISBN) employs an error-detecting code.

   (a) Using the internet, give the matrix H whose null space is the set of valid ISBN-10 numbers. (HINT: This is a 1×10 matrix over $\mathbb{F}_{11}$.)

   (b) Briefly describe the two classes of errors this code is designed to detect and explain why it works.

   (c) The modern ISBN-13 does not use a vector space. Why? (I.e., what about it does not satisfy the definition of a vector space?)

4. Consider the following channel $\mathbb{P}$ with input alphabet $X = \{0, 3, 6\}$ and output alphabet $Y = \{0, 1, \ldots, 6\}$:

$$\begin{array}{cc|ccccccc|} \Pr(x) & x & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0.3 & 0 & 0.8 & 0.15 & 0.05 & & & & \\ 0.1 & 3 & & 0.2 & 0.2 & 0.2 & 0.2 & 0.2 & \\ 0.6 & 6 & & & & & 0.05 & 0.15 & 0.8 \end{array} = \mathbb{P}$$

   (a) Give the maximum likelihood decoding **MLD** algorithm for this channel as a lookup table.

   (b) If you were to adjust this to **IMLD**, what are the first two changes you would make and why?

   (c) Give the maximum *a posteriori* decoding **MAP** algorithm for this channel as a lookup table.

5. Suppose your input and output alphabets are both $\mathbb{F}_2^6$; so you are sending binary 6-tuples. Suppose that, in your channel model, the only errors that occur are a 1 occasionally falling to a zero. (But zeros are never changed to ones.) What is the largest single-error-correcting code you can find in this setting?

[1] On p71, Hall gives a more general concept than what we use here.