Math 601 Homework #5. Due Wed., Feb. 21, 2018

Read Chapter 3 of the textbook (Bierbrauer)

Most of the exercises in the text are quick and easy, and you should try them all, to make sure you get the basics. I will assign some of the less routine exercises.

Write up and hand in solutions to the following exercises. You must give complete justification for all answers.

Exercises (to hand in)

1. Prove: If C is a binary linear code in $\mathbf{F}^n$, $u \in \mathbf{F}^n$, and $u \notin C$, then $C \cup (C + u)$ is also a linear code.

2. For each of the following, write a parity-check matrix for a binary linear $[n, k, d]_2$ code.

   (a) $[4, 2, 1]_2$

   (b) $[4, 2, 2]_2$

   (c) $[5, 2, 3]_2$

   (d) $[5, 1, 4]_2$

3. Using the connection between parity-check matrices and minimum distance, explain why there is no binary linear $[4, 2, 3]_2$ code. (Do not use the sphere-packing bound.)

4. Let $C = \{0000, 1001, 0101, 1100\}$.

   (a) List the cosets of C. (List each different set just once.)

   (b) Give a parity-check matrix for C.

   (c) Give the syndrome decoding array (SDA), relative to your parity-check matrix, for C. (This is the table like the one on page 68 of the textbook ... but a lot smaller.) Mark with a $*$ which coset leaders are unique coset leaders.

   (d) Using the SDA, decode the following received words: 1110, 1001, 1101. For which did you get the *unique* closest codeword?

   (e) Which error patterns does C detect? (Your answer may be in the form, "all words in $\mathbf{F}^4$ except ....")

   (f) Which error patterns does C correct?

5. Repeat #4 for the code C with generator matrix

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

   Use received words 01000, 11000, 10111 for part (d).

6. **T**heorem. Let C be a linear code of length n. The following are true for every u, v in $\mathbf{F}^n$.

   (1) If $u \in C + v$, then $C + u = C + v$.

   (2) $u \in C + u$.

   (3) If $u + v \in C$, then u and v are in the same coset.

   (4) If $u + v \notin C$, then u and v are in different cosets.

   (5) Either $C + u = C + v$ or $(C + u) \cap (C + v) = \emptyset$

   (6) $|C + u| = |C|$

   (7) If $\dim(C) = k$, then there are exactly 2^{n-k} different cosets of C, each with exactly 2^k words.

   (8) C is itself a coset.

   In class parts (1), (4), (5), (6) and (7) were proved.

   Prove parts (2), (3), and (8) of the above theorem. (You can use earlier parts of the theorem to prove later parts.)

Extra credit:

1. Prove: For each $n \geq 2$ there is exactly one binary linear code with parameters $[n, n-1, 2]_2$.

2. Prove: If C is a linear code in $\mathbf{F}^n$ of dimension 2 or more, then the sum of all the codewords in C is the zero vector. Furthermore, the same holds for cosets: if $u \in \mathbf{F}^n$, then the sum of all the vectors in the coset $C + u$ is the zero vector.