Math 601 Homework #6. Due Wed., Feb. 28, 2018

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

1. Let $C = \{0000, 1001, 0101, 1100\}$. (This is the code from Problem #4 on Homework #5.)
   (a) Which error patterns does C detect? (Your answer may be in the form, "all words in $\mathbf{F}^4$ except ....")
   (b) Which error patterns does C correct?

2. Consider the Hamming code $\mathcal{H}_3$ whose 3×7 parity-check matrix has as columns the 7 nonzero binary vectors in numerical order (binary representations of the integers 1 through 7 in that order).
   (a) Write down five different codewords of $\mathcal{H}_3$.
   (b) Decode the received word $w = 0101000$.
   (c) Decode the received word $z = 0001111$.

3. Prove: If $\mathcal{H}_r$ ($r \geq 2$) is a Hamming code of length $2^r - 1$, then the vector of all ones (of length $2^r - 1$) is in $\mathcal{H}_r$.

4. Prove: If $\mathcal{H}_r$ ($r \geq 2$) is a Hamming code, and v is a codeword, then $\bar{v}$ is a codeword, where $\bar{v}$ is obtained from v by changing all 0s to 1s and all 1s to 0s. (You can use #3, even if you didn't succeed in proving #3.)

5. Prove: The maximum dimension of a binary linear code of length $2^r - 1$ ($r \geq 2$) and distance 3 is $2^r - 1 - r$.

   Note: you have to show two things: if C is a code of that length and distance, then $\dim(C) \leq 2^r - 1 - r$, AND there is a code of that length and distance with $\dim(C) = 2^r - 1 - r$.

6. Use the Gilbert-Varshamov inequality to show that there exists a binary linear $[15, 6, 5]_2$ code.

7. (a) The Gilbert-Varshamov inequality guarantees the existence of a binary linear $[9, 3, 4]_2$ code. Give a parity check matrix for such a code.
   (b) Prove there is no binary linear $[8, 3, 5]_2$ code. Warning: the fact that these parameters do not satisfy the Gilbert-Varshamov inequality does not prove it.

8. Prove that the maximum dimension k of a binary linear code with length $n = 15$ and distance $d = 3$ is $k = 11$. (As in #5, you have to show two things.)

9. The various inequality theorems are not enough to tell us exactly the maximum dimension of a binary linear code with length $n = 12$ and distance $d = 4$. Let J be this maximum dimension. Give the best lower and upper bounds for J based on the inequality theorems.

Extra credit:

1. Prove: if C is a perfect binary linear code and $d(C) = 3$, then there exists an integer r such that C is a $[2^r - 1, 2^r - r - 1, 3]_2$ code.

2. Prove the following Corollary to the Gilbert-Varshamov Theorem:

   Corollary. Let $n \geq d \geq 2$. There exists a linear code C of length n and distance at least d satisfying
   $$|C| \geq \frac{2^{n-1}}{\binom{n-1}{0} + \binom{n-1}{1} + \cdots \binom{n-1}{d-2}}.$$

   Hint: Consider the largest value of k that satisfies the hypothesis of the Gilbert-Varshamov inequality.