Homework #2. Due Saturday, February 5th, by 11:59pm in filedrop

All reading assignments and references to exercises, definitions etc. are from our main book 'Coding Theory: A First Course' by Ling and Xing

Reading:

1. For this homework assignment: Chapter 2, 3.1 and 3.2.

2. For the classes next week. Tue, Feb 1: 3.1 and 4.1. Thu, Feb 3: 4.2-4.5. We will definitely not cover all the material from those sections, but I might touch on at least one topic from each section.

Problems:

1. Let C be a code of Hamming distance d. Suppose that a codeword $c \in C$ was transmitted, let w be the received word and k the number of transmission errors, that is, $k = d(c, w)$. By Theorem 3.1(b) from class (= Theorem 2.5.10 from the book), if $d > 2k$, then NND (nearest neighbor decoding) rule works correctly, that is, $c_w = c$ where c_w is the decoded word (the result of applying NND to w).

Now assume that $d = 2k$. By Theorem 3.1(b) NND rule may not work correctly in this case (we did not prove this part of Theorem 3.1(b) in class, but it is proved in the book). Prove that NND still correctly determines the number of transmission errors, that is,

$$d(c_w, w) = d(c, w) = k.$$

2. Let $k, r \in \mathbb{N}$, and let $C = \mathit{Rep}(k, r)$ be the repetition code with parameters k (length of the original message) and r (number of repetitions) over the binary alphabet $A = \{0, 1\}$, that is,

$$C = \{v^r = \underbrace{v \dots v}_{r \text{ times}} : v \in \{0,1\}^k\}.$$

The goal of this problem is to estimate the probability that NND works correctly for C if we transmit over $BSC(p)$, the binary symmetric channel with crossover probability p, with $p < \frac{1}{2}$ (we started discussing this problem at the end of Lecture 3 on Thu, Jan 27). To simplify some of the formulas below we will assume that r *is even*.

Note that C has length $n = kr$. In parts (a) and (b) below we assume that $k = 1$, so $n = r$.

(a) Assume that $k = 1$. For each $0 \leq i \leq r$ let $p(i)$ be the probability that exactly i errors occur during the transmission. Prove that $p(i) = \binom{r}{i} p^i (1-p)^{r-i}$.

(b) We still assume that $k = 1$. As discussed in Lecture 3, NND works correctly if and only if the number of transmission errors is $< \frac{r}{2}$. Thus, if $f(p, r)$ is the probability that NND works correctly, then

$$f(p,r) = 1 - \sum_{i=r/2}^{r} p(i) = 1 - \sum_{i=r/2}^{r} \binom{r}{i} p^i (1-p)^{r-i}$$

(recall that r is assumed to be even). Prove that

$$f(p,r) > 1 - (4p(1-p))^{r/2}$$

and deduce that if p is fixed, then $f(p,r) \to 1$ as $r \to \infty$.

(c) Now assume that k is arbitrary, and let $f(p, r, k)$ be the probability that NND works correctly. Prove that $f(p, r, k) = f(p, r)^k$ (where $f(p, r)$ is defined as in (b)). Deduce that if p and k are fixed, then $f(p, r, k) \to 1$ as $r \to \infty$.

Hints: For (b) use the following facts (make sure to prove them first):

(i) $g(i) = p^i (1-p)^{r-i}$ is decreasing as a function of i

(ii) $\sum\limits_{i=0}^{r} \binom{r}{i} = 2^r$.

For (c) explain why transmitting a codeword $c \in \mathit{Rep}(k, r)$ and then applying NND is essentially equivalent to independently transmitting k codewords from $\mathit{Rep}(1, r)$ and then applying NND to each of them. Then use this observation to deduce the equality in (c).

3. Problem 3.1, page 36

4. Problem 3.2, page 36

5.

(a) Use the Euclidean algorithm to find integers u and v such that $127u+35v = 1$. If you have not studied this before, see Lecture 4 of my 3354 notes.

(b) Use your answer in (a) to compute 35^{-1} in $\mathbb{Z}_{127}$. Make sure to explain your logic.

6. Problem 3.4, page 36. **Hint:** (a) can be proved directly from the standard formula for binomial coefficients and basic divisibility properties. Then use (a) to solve both (b) and (c).

7. Problem 3.5, page 36