Homework #1. Due Thursday, January 23rd, by 2pm in my mailbox

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: Chapters 1 and 2
2. Before the class on Wed, Jan 22: 3.1 and 4.1

Problems:

1. Recall that the parity-check code of length n, denoted below by PCC_n, is defined by

$$PCC_n = \{x_1 \ldots x_n \in \{0,1\}^n : \sum_{i=1}^{n} x_i \text{ is even}\}.$$

(a) Prove formally that PCC_n is 1-error detecting in the sense of Definition 2.5.4 (page 12).

(b) As observed in Lecture 1, $|PCC_n| = 2^{n-1}$. Prove that PCC_n is the largest possible 1-error detecting binary code of length n, that is, prove that if $C \subseteq \{0,1\}^n$ is any binary code of length n which is 1-error detecting, then $|C| \leq 2^{n-1}$.

2. Given an integer $n \geq 2$, let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ (here we are thinking of elements of $\mathbb{Z}_n$ as integers, not as congruence classes mod n, the latter being a typical convention in MATH 3354). Recall that the ISBN-10 code I_{10} is defined by

$$I_{10} = \{x_1 x_2 \ldots x_{10} \in (\mathbb{Z}_{11})^{10} \text{ s.t. } 11|(10x_1 + 9x_2 + \ldots + 2x_9 + x_{10})\}$$

(The notation $a|b$ means that a divides b, that is, $b = ac$ for some integer c).

The ISBN-13 code C, which replaced the ISBN-10 code in 2007, is defined by

$$I_{13} = \{x_1 x_2 \ldots x_{13} \in (\mathbb{Z}_{10})^{13} \text{ s.t. } 10 \mid (x_1+3x_2+x_3+3x_4+\ldots+3x_{12}+x_{13})\}$$

(the coefficients are alternating between 1 and 3). Thus, the ISBN-13 code has larger length (13 instead of 10), but uses smaller alphabet (10 symbols instead of 11).

(a) Prove that I_{10} and I_{13} are both 1-error detecting.

(b) Prove that I_{10} detects any transposition error, that is, any error where two different symbols in the original word are swapped (e.g. 1357924687 is sent and 1327954687 is received).

(c) Prove that I_{13} does not necessarily detect transposition errors. Does it detect some transposition errors? If yes, which ones?

(d) How would the properties of I_{13} change if the weights 1 and 3 in the definition were replaced by another pair of integers?

3. Let C be a code of Hamming distance d. Suppose that a codeword $v_0 \in C$ was transmitted, and let k be the number of errors that occurred during the transmission, that is, $k = d_{Hamm}(v_0, w)$ where w is the received. In class we proved (Theorem 2.2) that if $k \leq \frac{d-1}{2}$, then NND (nearest neighbor decoding) rule works correctly, that is, $v_0 = c(w)$ where $c(w)$ is the result of applying NND to w.

Now assume that d is even and we only know that $k \leq \frac{d}{2}$. Prove that while NND rule may not work correctly in this case, it still correctly determines the number of transmission errors, that is,

$$d_{Hamm}(v_0, w) = d_{Hamm}(c(w), w).$$

4. Problem 2.7, page 15. Replace IMLD by INND in the instructions for this problem.

5. Problem 2.8, page 15. Make sure to prove your answer.

6.

(a) Problem 2.3, page 15.

(b) Give an example of a word w showing that if the memoryless binary channel from Problem 2.3 is used for transmission and w is the received word, then both the complete NND rule and the complete MLD rule apply to w without getting to the "random choice" stage, but yield different answers.