ASSIGNMENT #1 FOR CODING THEORY

Instruction. It is *okay* to discuss the problems with your friends, but *you should be by yourself when you write up the solutions.* This is to prevent the situation that you end up "dictating" your friend's explanation without really digesting it.

You should present all the steps in each questions. You may assume without proof all the results covered in the lectures, provided that

- you clearly state the result you're using, and
- the result you assume is not a mere paraphrasing of the question itself.

Convention/Notation. Let A be an $d \times c$ matrix with entries in $\mathbb{B}$. We intentionally confuse the matrix A with the map $\mathbb{B}^c \to \mathbb{B}^d$ defined by multiplying A to column vectors of length c; i.e., we also denote by A the map defined by multiplication by A. (As I remarked in the lecture, this causes no practical confusion.)

For any $i = 1, 2, \cdots, c$, we let $e_i \in \mathbb{B}^c$ be the vector which has the ith entry 1 and all other entries 0. For any c, we let I_c denote the $c \times c$ matrix with diagonal entries 1 and all non-diagonal entries 0.

By Hamming code Ham(3), we mean the codes given by the following (choiceof) check matrix:

$$H_3 := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

I. Let $C \subset \mathbb{B}^n$ be a binary *linear* code. Recall that $d(C) := \min_{v,w \in C} d(v, w)$.

(1) For any $v, w \in \mathbb{B}^n$, show that $d(v, w) = d(v - w, \underline{0})$.
(2) Show that $d(C) := \min_{v \in C} d(v, \underline{0})$.
(3) Let $H : \mathbb{B}^n \to \mathbb{B}^k$ be a check matrix for C; i.e., $C = \ker(H)$. Show that He_i is the ith column vector of H for any $i = 1, 2, \cdots, n$.
(4) Show that $d(C)$ is the minimal number of linearly dependent column vectors in H. (*Hint:* **I**.(3) could be useful. Note that $v = (v_1, \cdots, v_n) = v_1 e_1 + \cdots v_n e_n$. Note also that $H(v + w) = Hv + Hw$ for any $v, w \in F^n$.)

II. Let $C \subset \mathbb{B}^n$ be a binary code, not necessarily linear.

(1) Show that if C is r-perfect for some integer r, then $d(C) = 2r + 1$
(2) Find an example of a binary linear code C such that $d(C) = 3$ but C is not 1-perfect.

III. We define a $(8, 4)$-code Ham$'(3)$ by adding an "overall parity check bit" to Ham(3); i.e. a codeword of Ham$'(3)$ is of the form $(v_1, \cdots, v_7, \sum_{i=1}^{7} v_i)$ where $(v_1, \cdots, v_7)$ is a codeword of Ham(3).

(1) Write down a generator matrix and a check matrix in <u>standard</u> form. (*Hint*: It is easier to find a generator matrix in standard form.)

(2) Show that the minimal distance of $\mathrm{Ham}'(3)$ is 4. (*Hint*: This can be easily deduced from the fact that the minimal distance of $\mathrm{Ham}(3)$ is 3, which you can use without proof.)
(3) Is $\mathrm{Ham}'(3)$ r-perfect for any r?
(4) Let p be a probability of an error occurring in a single bit during transmission, and assume $p < 1/2$. We will encode a message of 4000 bits using $\mathrm{Ham}'(3)$ and transmit them. For error processing, we'll choose to correct as many errors as possible (and generate an error message when an error cannot be corrected). Find (i) the probability of correct transmission, i.e. the probability that the corrected message is same as the sent message; and (ii) the probability that all the errors are either corrected or detected. (You do not have to simplify the expressions.)

IV. Let $H_{4,2} : \mathbb{B}^{15} \to \mathbb{B}^8$ be defined by the following matrix.

$$H_{4,2} := \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

We denote by $\mathrm{BCH}(4,2)$ the code defined by $H_{4,2}$; i.e., $\mathrm{BCH}(4,2) := \ker H_{4,2}$.

(1) Only by adding one row to another and swapping two rows on $H_{4,2}$, find a check matrix $H'_{4,2}$ of the following form which defines the same code as :

$$H'_{4,2} := \begin{pmatrix} 0_{(8-m)\times(15-m)} & 0_{(8-m)\times m} \\ A & I_m \end{pmatrix},$$

where m is a suitable integer, A is some $m \times (15-m)$ matrix, and $0_{a\times b}$ is the $a \times b$ matrix with all entries zero.
(2) What is the dimension of $\mathrm{BCH}(4,2)$? (*Hint*: Rank-nullity theorem.)
(3) Write down the generator matrix in standard form.
(4) Find the minimal distance of $\mathrm{BCH}(4,2)$. (You may use **I.**)
(5) Is $\mathrm{BCH}(4,2)$ r-perfect for any r?

V. With no further mention, all poiynomials here are "binomial polynomials" (i.e.,the coefficients are binary numbers).

(1) For any $a \in \mathbb{B}$ and any $f(X) \in \mathbb{B}[X]$, show that $X - a$ divides $f(X)$ if and only if $f(a) = 0$. (*Hint*: First, show that the remainder of $f(X)$ modulo $X - a$ is $f(a)$. Then, argue that this implies the claim.)
(2) Show that X^2 and $X^2 + 1$ are reducible, and $X^2 + X + 1$ is irreducible.
(3) Show that $X^4 + X + 1$ and $X^4 + X^3 + 1$ are irreducible.
(4) Find all the irreducible binary polynomial of degree 4. (*Hint:* There are exactly three.)
(5) Compute α^{10} in $\mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$.
(6) Compute β^{10} in $\mathbb{B}[\beta]/\beta^4 + \beta^3 + 1$.
(7) Find the multiplicative inverse of $\alpha^3 + \alpha + 1$ in $\mathbb{B}[\alpha]/\alpha^4 + \alpha + 1$.