ADDITIONAL EXERCISE SHEET #1 FOR CODING THEORY

Convention/Notation. Let F be any field, if you understand what it means. If you do not, then simply let $F = \mathbb{B}$ for now. We will soon learn what field is and see more example of fields F than $\mathbb{B}$ (namely, $\mathrm{GF}(2^k)$ in the engineers' notation and $\mathbb{F}_{2^k}$ in mathematicians' notation), which we use to construct better error-correcting codes. All the results below will apply to this more general choice of F.

Since $1 + 1 = 0$ in $\mathbb{B}$, we have $1 = -1$ in $\mathbb{B}$. Therefore, you may ignore all minus signs below. I do not drop the minus sign only for the sake of conceptual clarity.

Let $v_1, v_2, \cdots v_r$ be r vectors in F^c. We say that they are *linearly dependent* if they satisfy an equation

$$a_1v_1 + a_2v_2 + \cdots + a_rv_r = 0,$$

where $a_1, \cdots, a_r \in F$ and not all of them are zero. We say that the vectors $v_1, v_2, \cdots v_r$ are *linearly independent* if they are not linearly dependent.

Let A be an $d \times c$ matrix with entries in F. We intentionally confuse the matrix A with the map $F^c \to F^d$ 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 $e_i \in F^c$ 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.

I. This exercise is about generator and check matrices in standard form.

(1) Let $A : F^c \to F^d$ be a linear map (i.e., given by a suitable matrix multiplication). Show that Ae_i is the ith column vector of A for any $i = 1, 2, \cdots, c$.

(2) Show that A is an injective map if and only if all the columns of A are linearly independent.

(3) Let n and m be integers with $n > m$. Consider an $n \times m$ matrix $G = \left(\begin{smallmatrix} I_m \\ A \end{smallmatrix}\right)$ for some $(n-m) \times m$ matrix A with entries in F. Then show that the map $G : F^m \to F^n$ is injective. In particular, the image $\mathrm{im}(G)$ is m-dimensional. (Hint: the previous part could be useful.)

(4) Let n and k be integers with $n > k$. Consider an $k \times n$ matrix $H := \left(\begin{smallmatrix} -A & I_k \end{smallmatrix}\right)$ for some $k \times (n-k)$ matrix A with entries in F. Then show that the map $H : F^n \to F^k$ is surjective. In particular, the kernel $\ker(H)$ is $(n-k)$-dimensional, which directly follows from the rank-nullity theorem.

(5) Let $G = \left(\begin{smallmatrix} I_m \\ A \end{smallmatrix}\right)$ be as before. Then for any $v \in F^m$ show that $Gv = \left(\begin{smallmatrix} v \\ Av \end{smallmatrix}\right)$.

(6) Let $H := \left(\begin{smallmatrix} -A & I_k \end{smallmatrix}\right)$ be as before. Then for any $w \in F^k$ show that $Hw = \underline{0}$ if and only if $w = \left(\begin{smallmatrix} v \\ Av \end{smallmatrix}\right)$ for some $v \in F^{n-k}$.

(7) Let $C \subset \mathbb{B}^n$ be a linear code. "Conclude" from the previous two parts that $G = \left(\begin{smallmatrix} I_m \\ A \end{smallmatrix}\right)$ is a generator matrix for C if and only if $H := \left(\begin{smallmatrix} -A & I_{n-m} \end{smallmatrix}\right)$ is a check matrix for C where A is an $(n-m) \times m$ matrix with entries in F.

II. 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 $d(C)$ is the minimal number of linearly dependent column vectors in H. (*Hint:* **I.**(1) 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 $v, w \in F^n$.)

III. Let $C = \{(a, b, c, x, y, z) \in \mathbb{B}^6 \mid b + c + x = 0,\ c + a + y = 0,\ a + b + z = 0\}$.

(1) Explain why $C \subset \mathbb{B}^6$ is a binary *linear* code (using the very definition of linear code).
(2) Find a generator matrix G and a check matrix H, both in standard form.
(3) Compute $d(C)$. (You may use **II.**)
(4) Assume that $\underline{0} := (0, \cdots, 0)$ is transmitted. Write down all the possible error words with weight $\leqslant 2$; i.e. all vectors that is not equal to $\underline{0}$ and has at most two non-zero bits. For each of such error words, find all codewords that are closest. (There could be more than one such codewords.)
(5) How many errors can be corrected in a single block? If we do not correct any errors, how many errors can we detect? If we correct at most one error, how many errors can we detect?
(6) Assume that we have 300,000 bits of binary message to transmit. Assume that the probability for an error to occur in a single bit is 1/10,000. Compute the probability of correct transmission (without using the code). Now, assume that we use the code C and the generator matrix G in standard form. Compute the probability of correct transmission when we correct as many errors as possible.

IV. Repeat **III.** for the following code $C \subset \mathbb{B}^7$:

$$C = \{(a, b, c, x, y, z, p) \in \mathbb{B}^7 \mid b + c + x = 0,\ c + a + y = 0,\ a + b + z = 0,\\ a + b + c + x + y + z + p = 0\}$$

V. This exercise is about the proof of part (c) of the proposition at page 7 of the lecture note. Let $C \subset \mathbb{B}^n$ be a code (not necessarily linear), and choose an integer s. For any received message $v \in B^n$ not in C, we replace v with a codeword $w \in C$ with $d(w, v) \leqslant s$ if there exists such a $w \in C$ and if w is a unique codeword with this property. Otherwise, we generate an error message.

(1) Assume that the process described above corrects all weight s errors and detects all weight t errors. Then show that $d(C) \geqslant s + t + 1$.
(2) Assume that $s < d(C)/2$. Then show that we can correct all weight s errors and detect all weight $d - s - 1$ errors.

VI. Read I.4 of the lecture notes or the textbook about the coset table, and make a coset table for C as in **IV.**

VII. This question is about elementary row and column operations. Let $A : \mathbb{B}^c \to B^d$ be a linear map, which we identify with a $d \times c$ matrix with entries in $\mathbb{B}$.

(1) Choose $1 \leqslant a, b \leqslant c$ such that $a \neq b$. Let $U = (U_{ij})$ be an $c \times c$ matrix such that $U_{ii} = 1$ for all i, $U_{ab} = 1$, and $U_{ij} = 0$ for any other i and j. Then show that AU is the matrix obtained by adding the ath column of A to the bth column of A.

(2) Choose $1 \leqslant a, b \leqslant c$ such that $a \neq b$. Let $U = (U_{ij})$ be an $c \times c$ matrix such that $U_{ii} = 1$ if $i \neq a$ and $i \neq b$, $U_{aa} = U_{bb} = 0$, $U_{ab} = U_{ba} = 1$ and $U_{ij} = 0$ for any other i and j. Then show that AU is the matrix obtained by swapping the ath column of A with the bth column of A.

(3) Using the previous two parts, explain why elementary column operations on a generator matrix do not alter the code it defines. Also, explain why switching columns of a check matrix does not change the minimal distance of the code it defines (though this operation may alter the code itself).

(4) Choose $1 \leqslant a, b \leqslant d$ such that $a \neq b$. Let $V = (V_{ij})$ be an $d \times d$ matrix such that $V_{ii} = 1$ for all i, $V_{ab} = 1$, and $V_{ij} = 0$ for any other i and j. Then show that VA is the matrix obtained by adding the bth row of A to the ath row of A.

(5) Choose $1 \leqslant a, b \leqslant d$ such that $a \neq b$. Let $V = (V_{ij})$ be an $d \times d$ matrix such that $V_{ii} = 1$ if $i \neq a$ and $i \neq b$, $V_{aa} = V_{bb} = 0$, $V_{ab} = V_{ba} = 1$ and $V_{ij} = 0$ for any other i and j. Then show that VA is the matrix obtained by swapping the ath rowof A with the bth row of A.

(6) Using the previous two parts, explain why elementary row operations on a check matrix do not alter the code it defines. Also, explain why switching rows of a generator matrix does not change the minimal distance of the code it defines (though this operation may alter the code itself).

VIII. This exercise is about BCH(k, d)-code. Later in the course, we will be able to do this exercise in a much better and simpler way using finite fields (which we will study from next week). This exercise would provide some motivation to study finite fields. For this reason, I strongly encourage you to try this though it involves quite a lot of computations.

(1) Let $H_{3,2} : \mathbb{B}^7 \to \mathbb{B}^6$ be defined by the following matrix.

$$H_{3,2} := \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Only using **VII.**(4) and (5) on $H_{3,2}$, obtain the following check matrix $H'_{3,2}$ in standard form which defines the same code:

$$H'_{3,2} := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Conclude that the code defined by $H_{3,2}$ is the "(7,1)-repetition code"; i.e., there are only two codewords $(0, \cdots, 0)$ and $(1, \cdots, 1)$. (This is an instance of BCH$(3,2)$-code.)

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

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

Only using **VII.**(4) and (5) on $H_{4,2}$, find a check matrix $H'_{4,2}$ of the following form which defines the same code:

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

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

(3) What is the dimension of BCH$(4,2)$? Write down the generator matrix in standard form.

(4) Find the minimal distance of BCH$(4,2)$. (You may use **II.**)

VIIII. This exercise is to show that for any linear code one can find the generator matrix and the check matrix in standard form. In this sense, this exercise generalises **VIII.** (1) and (2). It is a more mathematical and more difficult exercise than the previous ones. Maths students are especially encouraged to do this exercise.

You are welcome to look up any standard linear algebra textbook on Gaussian elimination and reduced eschelon form, which provides the answer to this exercise.

(1) Let $G : \mathbb{B}^m \to \mathbb{B}^n$ be an injective linear map. Find an algorithm only using **VII.**(1) and (2) on G to obtain G' in standard form.

(2) Let $H : \mathbb{B}^n \to \mathbb{B}^k$ be any linear map. Find an algorithm only using **VII.**(4) and (5) on H to obtain H' which looks like a check matrix in standard form possibly with some zero row vectors augmented at the bottom. Show that if H is a check matrix for an m-dimensional code, then the number of zero rows in H' is exactly $k - (n - m)$.