Coding Theory: Assignment I

16th August 2025

---

1. **Due date:** 20th September 2025
2. Write the solutions in LaTeX.
3. All the statements proven in the class, or given in the exercise sheet can be used without proof. Other than that, anything you use needs to be proven.
4. Although strongly discouraged, if you do use an external source (for example, other than the main text book and problems in the exercise sheet, lecture notes, or any material available online), **acknowledge all your sources** in your writeup. This will not affect your grades; failure to acknowledge sources will be treated as a serious case of academic dishonesty. .
5. Allowed to discuss with others but write the solutions independently, and **acknowledge your collaborators**. Failure to do so will be treated as a serious case of academic dishonesty.
6. **Total marks:** 125

---

1. (**10 marks**) Let C be an $[n,k,d]_q$ code over a finite field $\mathbb{F}_q$ with the generator matrix G. If G does not have a column containing all zeros, then show that

$$\sum_{\mathbf{c}\in C} \mathrm{wt}(\mathbf{c}) = n(q-1)q^{k-1},$$

   where $\mathrm{wt}(\mathbf{c})$ denotes the number of nonzero coordinates in $\mathbf{c} \in \mathbb{F}_q^n$.

2. (**20 marks**) Let C be an $[n,k]_q$ code with the block length and the dimension of C are n and k, respectively. The code C is called *self-dual* if $C = C^\perp$, that is, the code C is the same as its dual. For any prime q, is there an $[8,4]_q$ self-dual code over $\mathbb{F}_q$?

3. In this problem, you will see various new ways of constructing new codes from existing ones. Recall that the notation $(n,k,d)_q$ code is used for general code (over an alphabet of size q) with block length n, dimension k, and distance d, whereas the $[n,k,d]_q$ code stands for a linear code (over the alphabet $\mathbb{F}_q$) of block length n, dimension k, and distance d. Prove the following statements:

   a) (**3 marks**) If there exists an $(n,k,d)_{q^m}$ code, then there also exists an $(nm,km,d')_q$ code with $d' \geq d$.

   b) (**8 marks**) If there exists an $[n,k,d]_{q^m}$ code, then there also exists an $[nm,km,d']_q$ code with $d' \geq d$. Given a generator matrix G for the $[n,k,d]_{q^m}$ code, find a generator matrix for the $[nm,km,d']_q$ code.

   c) (**10 marks**) If there exists an $[n,k_1,d_1]_q$ code and an $[n,k_2,d_2]_q$ code, then there also exists a $[2n,k_1+k_2,\min(2d_1,d_2)]_q$ code. Given generator matrices G_1 and G_2 for the $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ codes, respectively, find a generator matrix for the $[2n,k_1+k_2,\min(2d_1,d_2)]_q$ code.

   d) (**5 marks**) If there exists an $(n,k,\delta n)_q$ code, then for every positive integer m, there also exists an $(n^m,k/m,(1-(1-\delta)^m)\cdot n^m)_{q^m}$ code.

   e) (**8 marks**) If there exists an $[n,k,\delta n]_2$ code, then for every positive integer m, there exists an $[n^m,k,\frac{1}{2}\cdot(1-(1-2\delta)^m)\cdot n^m]_2$ code.

4. Show the following.

   (a) (**2 marks**) For any $[n,k,d]_q$ code, there exists a generator matrix $G \in \mathbb{F}_q^{k\times n}$ such that the weight of the first row is exactly d.

   (b) (**10 marks**) If there exists an $[n,k,d]_q$ code, then there exists an $[n-d,k-1,d']_q$ code with $d' \geq \lceil d/q \rceil$.

   (c) (**5 marks**) For an $[n,k,d]_q$ code,

   $$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

   It is known as *Griesmer Bound*.

5. (**12 marks**) Show that $[15,8,5]_2$ code does not exist.

6. (**15 marks**) Let $q \geq 2$ be an integer. Let $\delta \in (0, 1-\frac{1}{q})$. Let $\epsilon \in [0, 1-H_q(\delta)]$ and n be a positive integer. Let $k = (1-H_q(\delta)-\epsilon)n$. Let H be an $(n-k)\times n$ matrix over $\mathbb{F}_q$ picked uniformly and randomly. Then, show that H is a *parity* matrix of a code of block length n, rate $1-H_q(\delta)-\epsilon$ and relative distance at least δ with probability $\geq 1-q^{-\epsilon n}$.

7. In class, we have seen various coding theoretic bounds. In this problem, we will see alternate proofs of some of those bounds.

   a) First, we will prove the Plotkin bound (at least part 2 of Theorem 4.4.1 in Essential Coding Theory) via a purely combinatorial proof.
   Given an $(n,k,d)_q$ code C with $d > (1-\frac{1}{q})n$, define

   $$S = \sum_{\mathbf{c}_1 \neq \mathbf{c}_2 \in C} \Delta(\mathbf{c}_1, \mathbf{c}_2).$$

   For the rest of the problem, think C as an $|C| \times n$ matrix where each row corresponds to a codeword in C. Now consider the following:

      i. (**6 marks**) Looking at the contribution of each column in the matrix above, argue that

      $$S \leq \left(1-\frac{1}{q}\right) \cdot n|C|^2.$$

      ii. (**2 marks**) Looking at the contribution of the rows in the matrix above, argue that

      $$S \geq |C|(|C|-1) \cdot d.$$

      iii. (**2 marks**) Conclude part 2 of Theorem 4.4.1 in Essential Coding Theory

   b) Recall the *Griesmer Bound* defined in the first assignment. It says that for an $[n,k,d]_q$ code,

   $$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

   Then, using Griesmer bound, show the following.

      i. (**3 marks**) For any $[n,k,d]_q$,

      $$k \leq n-d+1.$$

      ii. (**4 marks**) Part 2 of Theorem 4.4.1 in Essential Coding Theory for linear codes.