ACT I: Assignment II

Due date: 20th October 2024

---

1. All the statements proven in the class, or given in the exercise sheet / previous assignments can be used without proof. Other than that, anything you use needs to be proven.
2. Encouraged, but not compulsory, to write the solutions in Latex.
3. Allowed to discuss with others but write the solutions independently.
4. Total marks: **80**

---

1. So far in this course we have seen multiple ways of modifying a code to get another code. In this problem, you will need to come up with more 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) (**8 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.

2. 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.

3. In this problem, we shall learn about the *cyclic codes*. Over the alphabet set $\mathbb{F}_q$, a linear code C of block length n is called a cyclic code if

$$\forall\, (c_0, c_1, c_2, \ldots, c_{n-1}) \in C,\ (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

Assume that $\gcd(n, q) = 1$. Let

$$\mathbb{F}_q[x]/\langle x^n - 1 \rangle = \left\{ a_0 + a_1 x + a_2 x + \cdots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_q,\ 0 \leq i < n \right\}.$$

Observe that $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ forms a ring under polynomial addition and multiplication *modulo* $x^n - 1$. Consider the following association between the elements of $\mathbb{F}_q^n$ and the elements of $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$,

$$(a_0, a_1, a_2, \ldots, a_{n-1}) \longleftrightarrow a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x]/\langle x^n - 1 \rangle \tag{1}$$

This natural association between the elements of $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ gives an *isomorphism* from $\mathbb{F}_q^n$ to $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ (considered only as an additive group). We shall often speak of a codeword $\mathbf{c}$ as the codeword $\mathbf{c}(x)$, using Equation 1. Extending this, over the alphabet $\mathbb{F}_q$, we interpret a linear code C of block length n as a subset of $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$. Now show the following.

a) (**5 marks**) Over the alphabet $\mathbb{F}_q$, a linear code C in $\mathbb{F}_q^n$ is cyclic if and only if C is an ideal in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$.

From the above problem and Problem 12 in Section 3 of Exercise Sheet, we know that every cyclic code C is a principal ideal in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$, that is, there exists a unique monic polynomial [1] $g(x)$ over $\mathbb{F}_q$ such that every codeword is a multiple (modulo $x^n - 1$) of $g(x)$. The polynomial $g(x)$ is called the *generator polynomial* of the cyclic code. Note that a cyclic code is uniquely defined by its generating polynomial. Let $x^n - 1 = f_1(x) f_2(x) \cdots f_t(x)$ be the decomposition of $x^n - 1$ into irreducible factors. Because of Problem 13 in Section 3 of Exercise Sheet, these irreducible factors are different. Then, show the following.

[1] An univariate polynomial is called *monic* if its leading coefficient, that is the coefficient of the highest degree monomial, is one.

b) (**4 marks**) Over the alphabet $\mathbb{F}_q$, the generating polynomial $g(x)$ of a cyclic code C of block length n divides $x^n - 1$.

c) (**3 marks**) Over the alphabet $\mathbb{F}_q$, describe the set of all possible cyclic codes of block length n in terms of their generating polynomials.

d) (**2 marks**) Over the alphabet $\mathbb{F}_q$, there exists 2^t many distinct cyclic codes of block length n.

e) (**4 marks**) For a cyclic code C in $\mathbb{F}_q^n$ and its generating polynomial $g(x)$, the dimension of C is $n - \deg(g)$. Furthermore, given $g(x)$, describe a generator matrix for C.

f) (**4 marks**) Given a generator matrix G for a cyclic code C in $\mathbb{F}_q^n$, design an algorithm that computes the generating polynomial of C in $\text{poly}(n)$ $\mathbb{F}_q$-operations.

g) (**6 marks**) Let C be a cyclic code in $\mathbb{F}_q^n$ and $g(x)$ be its generating polynomial. Then, there exists a unique monic polynomial of degree $n - \deg(g)$ such that any $\mathbf{c} \in \mathbb{F}_q^n$, $\mathbf{c} \in C$ if and only if $\mathbf{c}(x) \cdot h(x)$ is zero in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$. The polynomial $h(x)$ is called the *check polynomial* of C. Furthermore, given the check polynomial $h(x)$, describe a parity matrix for C.

h) (**3 marks**) Design an algorithm such that given the generating polynomial $g(x)$ of a cyclic code C in $\mathbb{F}_q^n$ as input, it outputs the check polynomial of C in $\text{poly}(n)$ $\mathbb{F}_q$-operations.

Note: Observe that the BCH code is a cyclic code.