Soham Chatterjee
Email: sohamc@email.com
Course: Algorithmic Coding Theory

Assignment - 1
Roll: BMC202175
Date: September 7, 2023

Problem 1 Chapter 1
Ex 1.18

Solution:

□

Problem 2 Chapter 2
Ex 2.13

Solution:

□

Problem 3 Chapter 2
Ex 2.16

Solution:

(a) Since G has full rank, $rank(G) = k$. Therefore in the reduced column echelon form of G the first k columns forms a identity matrix I_k. We denote the matrix formed by the rest $n-k$ columns by A. Since the reduced column echelon form of a matrix and the matrix generate the same vector space they are equivalent. And since the reduced column echelon form can be obtained through the Gaussian elimination method we can convert G to a matrix G' of the form $G' = [I_k|A]$ in polynomial time where G' and G are equivalent.

(b) We should have $GH^T = 0$ where G is of the form $G = [I_k|A]$. where A is a $k \times (n-k)$ matrix. Take $H = [-A^T|I_{n-k}]$. Suppose we denote $G = (g_{i,j})_{\substack{1\leq i\leq k\\ 1\leq j\leq n}}$ and $H = (h_{i,j})_{\substack{1\leq i\leq n\\ 1\leq j\leq n-k}}$. Let $C = GH^T = (c_{i,j})_{\substack{1\leq i\leq k\\ 1\leq j\leq n-k}}$

$$c_{i,j} = \sum_{m=1}^{n} g_{i,m}h_{m,j} = \sum_{m=1}^{k} \delta_{i,m}h_{m,j} + \sum_{m=k+1}^{n} g_{i,m}\delta_{m-k,j} = h_{i,j} + g_{i,k+j} = -a_{i,j} + a_{i,j} = 0$$

So we get every entry of C is 0. Hence $GH^T = 0$. Therefore H is the parity check matrix of G and since H is of the form $H = [-A^T|I_{n-k}]$ so it has full rank $n-k$. Hence H is a parity check matrix.

(c) The general parity check matrix H of the hamming code $[2^r, 2^r - 1 - r, 3]$ is the the ith column is the binary representation of i. Now by gaussian elimination we can convert it to the form $H' = [A \mid I_r]$. So now in H' for the last r many columns the ith columns is the binary representation of 2^i. In H the ith column for which $2^k < i < 2^{k+1}$ in H' it is the $(i-k)$th column. So then the generator matrix of the hamming code $[2^r - 1, 2^r - 1 - r, 3]$ is the matrix $G = [I_{2^r-1-r} \mid -A^T]$ by part (b)

□

Problem 4 Chapter 2
Ex 2.17

Solution:

(a) We encode each alphabet in $(n, k, d)_{2^m}$ in binary $\{0, 1\}$. So each alphabet takes m bits to encode. So now in the old code to encode each code in binary we have to encode all the n alphabets in binary which takes total nm bits to encode. So in the new code the code length becomes nm.

Initially $|C| = (2^m)^k = @^{mk}$. Hence the new dimention of the code becomes km. And the distance becomes at least the same as old one since we are just encoding all the alphabets in binary. So the new distance $d' \geq d$. The new code is $(nm, km, d' \geq d)_2$.

(b) Like the same logic as for the part (a) we encode all the alphabets in binary which takes m bits. So for each n length old code the new code is of nm length. So the new dimention of the code becomes like before km and the distance is at least d. So the new linear code is $[nm, km, d' \geq d]_2$

(c)

(d) For each $c \in C$ where C is the given linear code $[n, k, d]_q$ we form the new code $c^{\otimes m} := \underbrace{c \otimes c \otimes \cdots \otimes c}_{m \text{ times}}$.

Let the old alphabet set is Σ. We create the new alphabet set of size q^m which is the set of all possible $m - tuples$ i.e. $\Sigma' = \{(q_1, \ldots, q_m) \mid q_i \in \Sigma \,\forall\, i \in [m]\}$. So the new alphabet size becomes $|\Sigma'| = q^m$. Now let $c \in C$ is $c = (q_1, \ldots, q_n)$. Now if we expand out the $c^{\otimes m}$ each element of it is a m-product of the letters from the set $\{q_1, \ldots, q_n\}$. So we can represent each element of it as a m-tuple. Now each of this tuple is an element of the alphabet set we created just now. So

□

Problem 5 Chapter 5

Ex 5.8

Solution:

□

Problem 6 Chapter 5

Ex 5.15

Solution:

□

Problem 7 Chapter 5

Ex 5.16

Solution:

1. We have $f(X + Z) = \sum_{i=0}^{t} r_i(X)Z^i$. Now differentiating f with respect to Z we have

$$f'(X + Z) = \sum_{i=0}^{t-1}(i + 1)r_{i+1}(X)Z^i$$

Let for $n = k - 1$ we have

$$f^{(k-1)}(X + Z) = \sum_{i=0}^{t-k+1} \frac{(i + k - 1)!}{i!} r_{i+k-1}(X)Z^i$$

Denote $\frac{(i+k-1)!}{i!}r_{i+k-1}(X) = g_i(X)$. Then for $n = k$ we have

$$f^{(k)}(X+Z) = \sum_{i=0}^{t-k}(i+1)g_{i+1}Z^i = \sum_{i=0}^{t-k}\frac{((i+1)+k-1)!}{i!}r_{(i+1)+k-1}(X)Z^i$$
$$= \sum_{i=0}^{t-k}\frac{(i+k)!}{i!}r_{i+k}(X)Z^i$$

Hence by mathematical induction we have

$$f^{(n)}(X+Z) = \sum_{i=0}^{t-n}\frac{(i+n)!}{i!}r_{i+n}(X)Z^i$$

Therefore

$$f^{(n)}(X) = f^{(n)}(X+0) = \sum_{i=0}^{t-n}\frac{(i+n)!}{i!}r_{i+n}(X)0^i = \frac{n!}{0!}r_n(X) = n!r_n(X)$$

2. Let $char(\mathbb{F}_q) = m$. So $j \geq m$. Hence $j! = j(j-1)\cdots(m+1)m(m-1)! = mk$ where $k = j(j-1)\cdots(m+1)(m-1)!$. Since $f^{(j)}(X) = j!r_j(X) = m\left(kr_j(X)\right) \equiv 0$.

$\square$

Problem 8 Chapter 5

Ex 5.17

Solution:

$\square$