Soham Chatterjee
Email: sohamc@cmi.ac.in
Course: Algorithmic Coding Theory

Assignment - 1
Roll: BMC202175
Date: September 10, 2023

Problem 1 Chapter 1

Ex 1.18

Solution:

(a) If all the first $n-1$ people pass and the last person guess his hat color then the last person gets it right with probability $\frac{1}{2}$. Hence They win with probability $\frac{1}{2}$. Hence the n people can win with probability at least $\frac{1}{2}$.

(b) We can only consider the graphs which for $u, v \in V$ do not contain both the edges $u \to v$ and $v \to u$ cause the graph doesn't have a larger $K(G)$ than the graph which has neither of the edges. We will form a bijection with the strategies for guessing with the directed subgraphs of hypercube. Now in the hypercube every vertex represents a configuration of the hat colors of the n people. Let in the original graph both the edges $u \to v$ and $v \to u$ are there. So u, v differ in at one positions, let at i-th position. Now in a strategy if the i-th player among u, v guesses u then we keep the edge $v \to u$ and if he guesses v then we keep the edge $v \to u$ and if he passes then we dont draw any edge. This forms a bijection between the strategies for guessing and the subgraphs of the hypercube. So in such a subgraph the vertices with 0 outdegree are the winning positions. Hence winning probability becomes $\frac{K(G)}{2^n}$. Therefore over all subgraphs the maximum of $\frac{K(G)}{2^n}$ is the winning probability of the hat problem.

(c) Let I be the set of vertices which have out-degree 0 and in-degree at least 1. So

$$\sum_{v \in V} in-degree(v) \geq \sum_{v \in I} in-degreev \geq |S| = K(G)$$

And we also have

$$\sum_{v \in V} out-degree(v) = \sum_{v \in V-I} out-degree(v) \leq n(2^n - K(G))$$

Since $\sum_{v \in V} in-degree(v) = \sum_{v \in V} out-degree(v)$ we have

$$K(G) \leq n(2^n - K(G)) \implies (n+1)K(G) \leq n2^n \implies \frac{K(G)}{2^n} \leq \frac{n}{n+1}$$

Hence the value of $\frac{K(G)}{2^n}$ is atmost $\frac{n}{n+1}$.

(d) First take a code $C \subseteq \{0,1\}^n$ where the distance is 3. Then for any $u \in C$ add the edges $u \to v$ for all $v \notin C$ such that $\Delta(u, v) = 1$ i.e. u, v differ in one position. So for every $u \in C$, $out-degree(u) = n$. So for no pair of vertices x, y both the edges $x \to y$ and $y \to x$ are in the graph. So $K(G) = n|C|$. Now if we take C to be the hamming code $[2^l - 1, 2^l - l - 1, 3]$ then $|C| = \frac{2^{2^l-1}}{2^l} = \frac{2^n}{n+1}$. Hence $\frac{K(G)}{n} = \frac{2^n}{n+1} \iff \frac{K(G)}{2^n} = \frac{n}{n+1}$.

□

Problem 2 Chapter 2

Ex 2.13

Solution: The parity check matrix G of $C^\perp$ is the generator matrix of C. Now $C^\perp$ has distance $d^\perp$. So the smallest set of linearly independent columns of G is of size $d^\perp$. Hence for any set of $d^\perp - 1$ columns of G they are linearly independent.

So for any I with $|I| = d^\perp - 1$ we take the ith columns for the i's in I. So we have this new matrix A of dimention $k \times (d^\perp - 1)$. Since the columns are linearly independent A has full rank. By singelton bound on $C^\perp$ we have

$$n - k \leq n - d^\perp + 1 \implies d^\perp - 1 \leq k$$

Now we want to show that for any $v \in \mathbb{F}_q^{d^\perp - 1}$ there exists a solution of $A^T x = v$ in C. Since A has full rank there are $d-1$ columns of A^T which are linearly independent. So those $d^\perp - 1$ columns of A^T can span the $\mathbb{F}_q^{d^\perp - 1}$. Hence there exists a solution of $A^T x = v$. Now by Ex 2.6(4) for all $v \in \mathbb{F}_q^{d^\perp - 1}$ there are same number of solutions. Hence C is $d^\perp - 1$ wise independent.

□

> Problem 3 Chapter 2
> Ex 2.14

Solution:

1. Let G be the generator matrix of C. So G is a $k \times n$ matrix. Let the columns of G are $c_1, c_2, \ldots, c_n$. Take $S = \{c_i \mid i \in [n]\}$. So $|S| = n$. Now for any $x \in \mathbb{F}_q^k$, $\langle x, c_i \rangle$ is the i-th coordinate of xG. We are given that $wt(xG) \in \left[\left(\frac{1-\epsilon}{2}\right)n, \left(\frac{1+\epsilon}{2}\right)n\right]$. Hence

   $$Pr[\langle x, c_i \rangle = 1] \in \left[\frac{1-\epsilon}{2}, \frac{1+\epsilon}{2}\right] \implies Pr[\langle x, c_i \rangle = 0] \in \left[\frac{1-\epsilon}{2}, \frac{1+\epsilon}{2}\right]$$

   Therefore

   $$\left|\Pr_{c \in S}[\langle x, c_i \rangle = 0] - \Pr_{c \in S}[\langle x, c_i \rangle = 1]\right| \leq \left|\frac{1+\epsilon}{2} - \frac{1-\epsilon}{2}\right| \leq \epsilon$$

   Now for any $I \subseteq [k]$ take $e_I = \sum_{i \in I} e_i$. Then for any $x \in \mathbb{F}_q^K$, $\sum_{i \in I} x_i = \langle x, e_I \rangle$. Hence from above we have

   $$\left|\Pr_{c \in S}[\langle c_i, e_I \rangle = 0] - \Pr_{c \in S}[\langle c_i, e_I \rangle = 1]\right| = \left|\Pr_{c \in S}\left[\sum_{j \in I} c_{i,j} = 0\right] - \Pr_{c \in S}\left[\sum_{j \in I} c_{i,j} = 1\right]\right| \leq \epsilon$$

   Hence S is ϵ-biasesd.

2. We have the code $[n, k, \delta n]_2$. Which have hamming weight in the range $\left(\left(\frac{1}{2} - \gamma\right)n, \left(\frac{1}{2} + \gamma\right)n\right) \implies \delta \in \left(\frac{1}{2} - \gamma, \frac{1}{2} + \gamma\right)$. Now if we construct a code with relative hamming weight in the range $\left(\frac{1-\epsilon}{2}, \frac{1+\epsilon}{2}\right)$ whose generator matrix is $k \times n^{O(\gamma^{-1} \log \frac{1}{\epsilon})}$ then by part (1) we have a code with ϵ-bias of size $n^{O(\gamma^{-1} \log \frac{1}{\epsilon})}$. So for that need $m = O\left(\gamma^{-1} \log \frac{1}{\epsilon}\right)$

   Now we construct a new code $\left[n^m, k, \frac{1}{2}(1 - (1-2\delta)^m)n^m\right]_2$ by Ex 2.17(e) from $[n, k, d]_2$. We claim that this new code has relative hamming weight in the range $\left(\frac{1-\epsilon}{2}, \frac{1+\epsilon}{2}\right)$.

   $$\begin{aligned}
   &\delta \in \left(\frac{1}{2} - \gamma, \frac{+}{\gamma}\right) \\
   &\implies 2\delta \in (1 - 2\gamma, 1 + 2\gamma) \\
   &\implies 1 - 2\delta \in (= 2\gamma, 2\gamma) \\
   &\implies (1 - 2\delta)^m \in (-(2\gamma)^m, (2\gamma)^m) \\
   &\implies \frac{1}{2}(1 - (1-2\delta)^m) \in \left(\frac{1 - (2\gamma)^m}{2}, \frac{1 + (2\gamma)^m}{2}\right)
   \end{aligned}$$

   We need

   $$\frac{1 - (2\gamma)^m}{2} \geq \frac{1-\epsilon}{2} \iff \epsilon \geq (2\gamma)^m$$

Now

$$\begin{aligned}\epsilon \geq (2\gamma)^m &\iff \log\epsilon \geq m(\log\gamma + 1)\\ &\iff \frac{\log\epsilon}{1+\log\gamma} \geq m = \omega\gamma^{-1}\log\frac{1}{\epsilon} \quad [\omega \text{ is a constant}]\\ &\iff \frac{-\gamma}{1+\log\gamma} \geq \omega\end{aligned}$$

Now since $0 < \gamma < \frac{1}{2}$ we have $\log gm < -1$ So $\frac{-\gamma}{1+\log\gamma} > 0$. So we take $\omega = \frac{-\gamma}{1+\log\gamma}$. Hence for this value of c we have the relative hamming weight $\geq \frac{1-\epsilon}{2}$. Similarly we have the relative hamming weight $\leq \frac{1+\epsilon}{2}$. Hence this new formed code has relative hamming weight in the range $\left(\frac{1-\epsilon}{2}, \frac{1+\epsilon}{2}\right)$. The generator matrix of this code is of the dimension $k \times n^{O(\gamma^{-1}\log\frac{1}{\epsilon})}$. Hence by using part (1) we have a ϵ-biased space of size $n^{O(\gamma^{-1}\log\frac{1}{\epsilon})}$.

□

Problem 4 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 5 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 $|C| = (2^m)^k = 2^{mk}$. 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 previos part we again encode the alphabets in binary so the new code length becomes nm. $\mathbb{F}_{2^m} \cong \frac{\mathbb{F}_2[x]}{p(x)}$ where $p(x)$ is a irreducible polybomial of degree m. So we can think $\mathbb{F}_{2^m}$ as a vector space over $\mathbb{F}_2$ where the basis is $x^{n-1}, \ldots, x, 1$. So we can think of an isomorphism φ between the vector spaces $\mathbb{F}_{2^m}$ and $(\mathbb{F}_2)^m$ by

$$\varphi\left(\sum_{i=0}^{n-1} a_i x^i\right) = (a_1, \ldots, a_{n-1}) \qquad \forall\ a_i \in \mathbb{F}_2$$

This creates an isomorphism between the vector spaces. So after the binary conversion this still remains as vector space. 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) Since the distance is d hence the minimum weight is d. Hence there exists a code c_0 for which $wt(c_0) = d$. WLOG suppose in the last d many positions c_0 has nonzero words. Then we drop the last d many positions from all the code words. We obtain a new code C' of length d.

Take the set $S = \{c \in C \mid wt(c) = d$ the first d positions have the nonzero elements$\}$. S is also a vector space. By rank nullity theorem we can say $\dim S + \dim C' = k$ since all vectors of S becomes the zero vector in C'. Now we claim that S is spanned by one vector. If not let $c_1, c_2 \in C$ which are linearly independent. Then there exists an $\alpha \in \mathbb{F}_q$ such that the first element of $c_1 + \alpha c_2$ becomes zero and this new code is also in S. But this code has at most $d-1$ many nonzero elements and at least 1 nonzero element. But we created S where all codes have d many nonzero elements in the first d positions. Hence contradiction. Therefore $\dim S = 1$. Hence $\dim C' = k-1$

We can assume $d > q$ cause if $d \leq q$ then $\left\lceil \frac{d}{q} \right\rceil = 1$ that means the new code has distance at least 1 which is obviously true for any code. So we take $d > q$. Consider the codes $c + \alpha c_0$ where $\alpha \in \mathbb{F}_q$. Since α varies over all elements of the field all the elements of αc_0 varies over all elements of $\mathbb{F}_q$. So every nonzero element of c becomes zero in $c + \alpha c_0$ for some α. Since there are d many symbols by pegion hole principle there exists an α such that $\left\lceil \frac{d}{q} \right\rceil$ many elements of $c + \alpha c_0$ becomes zero. Now this $c + \alpha c_0 \in C$. Now $wt(c + \alpha c_0) \geq d - \left\lceil \frac{d}{q} \right\rceil + d'$. Since the distance of C is d we have

$$d - \left\lceil \frac{d}{q} \right\rceil + d' \geq d \implies d' \geq \left\lceil \frac{d}{q} \right\rceil$$

So we have distance $d' \geq \left\lceil \frac{d}{q} \right\rceil$. So this new code becomes $\left[n-d, k-1, d' \geq \left\lceil \frac{d}{q} \right\rceil\right]$

(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 in the new code number of codes remains same but the alphabet size is now q^m. Now originally $|C| = q^k = (q^m)^{\frac{k}{m}}$ So the dimention is $\frac{k}{m}$. Now for the distance initially the distance was $d = \delta n$. So between any two code words at most $n-d$ many positions can be same. So If we tensor each code words m times then at most $(n-d)^m$

many positions can be same. Hence at least $n^m-(n-d)^m$ many positions are different. Now we have to show that there exists a pair of code words which are of $n^m-(n-d)^m$ distance. Take the 0 code. So $0^{\otimes m}$ is also a 0 code with n^m many 0's. Now take the code c_0 which had weight d. Hence c_0 has only d many nonzero alphabets and rest $n-d$ alphabets are 0's. So $c_o^{\otimes m}$ has at least $(n-d)^m$ many zeros. Hence it has most $n^m-(n-d)^m$ many nonzero elements. Hence the new distance is $n^m-(n-\delta n)^m=(1-(1-\delta)^m)n^m$. Hence the new code is $\left(n^m,\frac{k}{m},(1-(1-\delta)^m)n^m\right)_{q^m}$

(e) Let the generator matrix of $[n,k,d]_2$ ($d=\delta n$) is G which is a $k\times n$ matrix. Now we create a new generator matrix G' of dimension $n^m\times k$ where we represent a column by a m-tuple $(i_1,\ldots,i_m)$ where $1\le i_j\le n$. We denote the i-th column of G by c_i. We first represent each bit b by $(-1)^b$ i.e instead of $\{0,1\}$ we will use $\{1,-1\}$. Now in G' the $(i_1,\ldots,i_m)$th column is the sum of the $i_1,\ldots,i_m$-th columns. So now for any x xG is a n^m length code. Hence the new code has code length n^m. Since the number of codes remains same and so is the alphabets we have dimension same as before, k. We denote $n^m=N$. Now for any $i\in[n]$, $\langle c_i,x\rangle$ is the i-th coordinate of xG.

So for any N-tuple v

$$\mathbb{E}[x]=\frac{\#0 \text{ in } v-\#1 \text{ in } v}{N}$$

So

$$\begin{aligned}\mathbb{E}[xG']&=\frac{1}{N}\sum_{i_1,\ldots,i_m\in[n]}(-1)^{\left\langle\sum_{j=1}^m c_{i_j},x\right\rangle}=\frac{1}{N}\sum_{i_1,\ldots,i_m\in[n]}(-1)^{\sum_{j=1}^m\langle c_{i_j},x\rangle}\\&=\frac{1}{N}\sum_{i_1,\ldots,i_m\in[n]}\left[\prod_{j=1}^m(-1)^{\langle c_{i_j},x\rangle}\right]=\prod_{j\in[m]}\left[\frac{1}{n}\sum_{i\in[n]}(-1)^{\langle c_i,x\rangle}\right]\\&=\prod_{j\in[m]}\mathbb{E}[xG]=\left[\frac{\#0 \text{ in } xG-\#1 \text{ in } xG}{n}\right]^m\ge\left[\frac{n-2d}{n}\right]^m\end{aligned}$$

So $\#0 \text{ in } xG'-\#1 \text{ in } xG'\ge n^m\left[\frac{n-2d}{n}\right]^m=(n-2d)^m$. So $\#1 \text{ in } xG'\ge\frac{n^m-(n-2d)^m}{2}=\frac{1}{2}(1-(1-2\delta)^m)n^m$. Now let c be the code in $[n,k,d]_2$ such that $wt(c)=d$ let x' be such that $x'G=c$. Then

$$\mathbb{E}[x'G']=\left[\frac{\#0 \text{ in } xG-\#1 \text{ in } xG}{n}\right]^m=\left[\frac{\#0 \text{ in } c-\#1 \text{ in } c}{n}\right]^m=\left[\frac{n-d-d}{n}\right]^m=\left[\frac{n-2d}{n}\right]^m$$

Hence $\#1 \text{ in } x'G'$ is $\frac{n^m-(n-2d)^m}{2}$. Hence this new code is $\left[n^m,k,\frac{1}{2}(1-(1-2\delta)^m)n^m\right]_2$

□

> Problem 6 Chapter 5
> Ex 5.4

Solution: Let γ be the premitive element of $\mathbb{F}_q^*$. Then the generator matrix of $RS_{\mathbb{F}_q^*}[n,k]$ is the matrix

$$G=\begin{bmatrix}1&1&1&\cdots&1\\0&\gamma&\gamma^2&\cdots&\gamma^{n-1}\\0&\gamma^2&\gamma^4&\cdots&\gamma^{2(n-1)}\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&\gamma^{k-1}&\gamma^{2(k-1)}&\cdots&\gamma^{(n-1)(k-1)}\end{bmatrix}$$

Now consider this vandermonde matrix which is $(n-k)\times n$ matrix

$$H=\begin{bmatrix}1&1&1&\cdots&1\\0&\gamma&\gamma^2&\cdots&\gamma^{n-1}\\0&\gamma^2&\gamma^4&\cdots&\gamma^{2(n-1)}\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&\gamma^{n-k-1}&\gamma^{2(n-k-1)}&\cdots&\gamma^{(n-1)(n-k-1)}\end{bmatrix}$$

If we show that $GH^T = 0$ then we can say H is the generator matrix of $C^\perp$. And since it is vanderminde matrix $C^\perp$ is Reed Solomon Code. Since $Rank(H) = n-k$. $C^\perp = RS[n, n-k]$.

Claim: For all $0 \le l \le n-1$ and we have $\sum_{i=0}^{n-2} \left(\gamma^i\right)^l = 0$

Proof:

$$\sum_{i=0}^{n-2} \left(\gamma^i\right)^l = \sum_{i=0}^{n-2} \left(\gamma^l\right)^i = \frac{1-\left(\gamma^l\right)^{n-1}}{1-\gamma^l} = \frac{1-1}{1-1} = 0$$

□

Now

$$GH^T = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & \gamma & \gamma^2 & \cdots & \gamma^{n-1} \\ 0 & \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \gamma^{k-1} & \gamma^{2(k-1)} & \cdots & \gamma^{(n-1)(k-1)} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \gamma & \gamma^2 & \cdots & \gamma^{n-k-1} \\ 1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma^{n-1} & \gamma^{2(n-1)} & \cdots & \gamma^{(n-1)(n-k-1)} \end{bmatrix}$$

Now denote $G = (g_{i,j})_{\substack{1 \le i \le k \\ 1 \le j \le n}}$ and $H = (h_{i,j})_{\substack{1 \le i \le n-k \\ 1 \le j \le n}}$. So when $i = 1$

$$\sum_{k=1}^{n} g_{1,k} h_{k,1} = \sum_{k=1}^{n} 1 \times 1 = 0, \quad \sum_{k=1}^{n} g_{1,k} h_{k,j} = \sum_{k=1}^{n} h_{k,j} = \sum_{k=2}^{n} \gamma^{(k-1)(j-1)} = \sum_{k=1}^{n-1} \left(\gamma^k\right)^{j-1} = \gamma^{j-1} \sum_{k=0}^{n-2} \left(\gamma^k\right)^{j-1} = 0$$

where the last equality came using the claim. When $i > 1$ then

$$\sum_{k=1}^{n} g_{i,k} h_{k,j} = \sum_{k=2}^{n} \gamma^{(i-1)(k-1)} \gamma^{(k-1)(j-1)} = \sum_{k=1}^{n-1} \left(\gamma^k\right)^{(i-1)+(j-1)}$$

$$= \gamma^{(i-1)+(j-1)} \sum_{k=0}^{n-2} \left(\gamma^k\right)^{(i-1)+(j-1)} = \gamma^{(i-1)+(j-1)} \sum_{k=0}^{n-2} \left(\gamma^k\right)^{\omega} = 0$$

Since for any element $\alpha \in \mathbb{F}_q$ then α^{n-1} so we can take $\omega = (i-1)+(j-1) \pmod{n-1}$. Hence again the last equality came using the claim. Hence we get that $GH^T = 0$. Therefore $C^\perp$ is $RS[n, n-k]$.

□

> Problem 7 Chapter 5
> Ex 5.8

Solution:

1. Let the set $S \subseteq \mathbb{F}_q^n$ is t-wise independent source for some t, $1 \le t \le n$. If we take any random vector $v \in S$ where $v = (v_1, \ldots, v_n)$ then for any $I \subseteq [n]$ where $|I| = t$, we have $Pr[X_i = v_i \ \forall \ i \in I] = \frac{1}{q^t}$. Since the probability is same for all I and for all vectors $v \in S$ that means for all $I \subseteq [n]$ where $|I| = t$, S projected to I has each vectors of $\mathbb{F}_q^t$ appear same number of times Hence the set S is t-wise independent.

   Let the set $S \subseteq \mathbb{F}_q^n$ is t-wise independent for some t, $1 \le t \le n$. So for all $I \subseteq [n]$ where $|I| = n$ the set S projected to I has each vector of $\mathbb{F}_q^t$ appear same number of times. Let each vector of $\mathbb{F}_q^t$ appear m number of times. So $|S| = mq^t$. So if we take any random code $v \in S$ where $v = (v_2, \ldots, v_n)$ for all $I \subseteq [n]$

$$Pr[X_i = v_i \ \forall \ i \in I] = \frac{\#\text{vectors for which the } i\text{-th position element equals to } v_i \text{ for all } i \in I}{mq^t}$$

For all vectors $v \in S$ for which the i-th position equals to v_i for all $i \in I$. if we project them to I then they give the $\mathbb{F}_q^t$ vector $(v_i)_{i\in I}$. This vector in $\mathbb{F}_q^t$ appears m number of times. So the number of vectors $v \in S$ for which the i-th position equals to v_i for all $i \in I$ is m. Hence $Pr[X_i = v_i \ \forall \ i \in I] = \frac{m}{mq^t} = \frac{1}{q^t}$. Hence the set S is t-wise independent source.

2. Here there should be a condition that the code C has at least one code which nonzero at every position cause otherwise if we take $C = \langle e_q \rangle$ then for all positions execpt the first position it is gurrented to be a 0.

   Now since there is a vector which has nonzero element at every positon if we take any vector randomly then for any random position all alphabets can be present in that position. Because since there is a code in C which has nonzero element at every positon for any position if we multiply the element in that position with all the elements of $\mathbb{F}_q$ then it goes through all the elements of $\mathbb{F}_q$. So for any random vector and any random position the alphabet $Pr[X = \alpha] = \frac{1}{q}$, $\alpha \in \mathbb{F}_q$. Hence any cpde $[n,k]_q$ is 1-wise independent source.

3. The dual of MDS code is also a MDS code. To prove this let a MDS code is $[n,k]$. Then the dual of this code has dimenstion $n-k$ and distance at most $n-(n-k)+1 = k+1$. So if we show that the generator matrix of $[n,k]$ every k columns are linearly independent we are done. Suppose not. WLOG the first k columns are linarly dependent. Hence there is a linear combination of the rows of the generator matrix such that the first k elements becomes 0. Hence this linear combination gives a code which has at least k many zeros. So it has weight at most $n-k$. But the MDS code $[n,k]$ has distance $n-k+1$. Hence contradiction. So the dual of MDS code is also MDS and has distance $k+1$. By Ex 2.13 we have the code $[n,k]$ is k wise independent. Hence by part (a) we have MDS code is k-wise independent source.

4. Since the MDS code $[n',k]_{2^m}$ can be converted to a linear code $[n'm,km,d]_2$ by Ex 2.17(b). Since $[n',k]_{2^m}$ is k-wise independent we claim that $[n'm,km,d]_2$ is also k-wise independent. For any code $c \in [n'm,km,d]_2$ and for any $I \subseteq [n'm]$

$$Pr[X_i = v_i \ \forall \ i \in I] = \frac{\#\text{vectors for which the } i\text{-th position element equals to } c_i \text{ for all } i \in I}{2^{km}}$$

   Now since $[n',m]_{2^m}$ is a MDS code there is also codes with no zero elements. Hence for every $X_i = c_i$ there are exactly half of all codes which have the value c_i at i-th position. Hence for $X_i = c_i, X_j = c_j$ where $i \neq j$ there exactly half of the codes with c_i at i-th position. Hence like this there exactly 2^{km-k} many codes which have $X_i = c_i$ for all $i \in I$. Hence $Pr[X_i = v_i \ \forall \ i \in I] = \frac{2^{km-k}}{2^{km}} = \frac{1}{2^k}$. Hence $[n'm,km,d]_2$ is also k-wise independent source.

   So now we take $n' = \frac{n}{m}$ and $m = 1+\log n \implies 2^m = 2 \times 2^{\log n} = 2n$ then the code $[n'm,km,d]_2 = [n,km,d]_2$ has size $2^{mk} = (2^m)^k = (2n)^k$. Hence this code $[n,km,d]_2$ is k-wise independent. Hence $\log((2n)^k) = k\log(2n) = k(1+\log n)$ random bits are enough to compute n random bits that are k-wise independent.

   We have to have $k(\log n - \log\log n + O(1))$ random bits. If we take $m = \log n - \log\log n + O(1) = \log\left(\frac{n2^{O(1)}}{\log n}\right)$ then the field size at first becomes $2^m = \frac{n2^{O(1)}}{\log n}$. Then the size of the code becomes $2^{km} = (2^m)^k = \left(\frac{n2^{O(1)}}{\log n}\right)^k$ then the number of random bits needed is

$$\log\left(\left(\frac{n2^{O(1)}}{\log n}\right)^k\right) = k(\log n - \log\log n + O(1))$$

   Since in the original MDS code $[n',k]_{2^m}$ where $n' = \frac{n}{m}$, $m = \log n - \log\log n + O(1)$ the code $[n'm = n, km = k(\log n - \log\log n + O(1)), d]_2$ is k-wise independent code of size $\left(\frac{n2^{O(1)}}{\log n}\right)^k$. So if we take 1 in place of $O(1)$ then we have a code of size $\left(\frac{2n}{\log n}\right)^k$ which is k-wise independent.

5. Let $p = \frac{1}{2^k} \implies \log \frac{1}{p} = k$ and $X-1,\ldots,X_n$ be tk wise independent random variables. Now we group the random variables into $\frac{n}{k}$ groups where each group contains k random variables. Let the groups are $U_1,\ldots,U_{\frac{n}{k}}$. Now we create new random variables $Z_1,\ldots,Z_{\frac{n}{k}}$ where $Z_i = \bigwedge_{i\in U_i} X_i$. We claim that Z_i's are t-wise independent and p-biased. They are p-biased because

$$Pr[Z_i = 1] = \prod_{i\in U_i} Pr[X_i = 1] = \prod_{i\in U_i} \frac{1}{2} = \frac{1}{2^k} = p$$

So we need to show that Z_i's are t-wise independent. For any $I \subseteq [n-k]$ where $|I| = t$

$$Pr\left[\bigwedge_{i\in I}(Z_i = z_i)\right] = Pr\left[\bigwedge_{i\in I}\left(\bigwedge_{j\in U_i} X_j = z_i\right)\right]$$

since Z_i are disjoint and each X_i are independent. Since the random variables X_i are tk-wise independent we can say from here that z_I's are t-wise independent.

□

Problem 8 Chapter 5

Ex 5.15

Solution: Given that $m_1 \neq m_2$. Then there exists at least one prime p_i where $i \leq k$ such that $m_1 - m_2 \pmod{p_i} \neq 0$. Now since $m_1, m_2 \in \mathbb{Z}_K$ we have $m_1 - m_2 \in \mathbb{Z}_K \implies m_1 - m_2 \leq K$. So therefore for all primes p_j where $k < j \leq n$ we have $m_1 - m_2 \pmod{p_j} = m_1 - m_2 \neq 0$ Hence $b_i = 1$ and for all $k < i \leq n$, $b_i = 1$. Therefore

$$\prod_{i=1}^{n} p_i^{b_i} \geq p_i \prod_{j=k+1}^{n} p_j > \prod_{j=k+1}^{n} p_j = \frac{N}{K}$$

Therefore $b_j = 1$ for at least $n-k+1$ many positions (one for i and the positions form $k+1$ to n). Therefore $E(m_1) - E(m_2) \neq 0$ at atleast $n-k+1$ many positions. So $E(m_1)$ and $E(m_2)$ differ at atleast $n-k+1$ many positions.

□

Problem 9 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

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

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 $f^{(j)}(X) = j! r_j(X) = m\Big(k r_j(X)\Big) \equiv 0$.

3. Given that $f(\alpha) = 0$. Hence $X - \alpha \mid f(X)$. So $f(X) = (X-\alpha)^m q(X)$ for some $m \in \mathbb{N}$ such that $q(\alpha) \neq 0$. Now $f'(X) = m(X-\alpha)^{m-1} q(X) + (X-\alpha)^m q'(X)$. Since $f'(\alpha) = 0$ we have $m \geq 2$. Hence $(X-\alpha)^2$ divides $f(X)$. Hence the given statement is true for $j = 2$. Let this statement is true form $j = k < char(\mathbb{F}_q)$. So for all $0 \leq i < k$, $f^{(i)}(\alpha) = 0$ and hence $(X-\alpha)^k$ divides $f(X)$. Let for all $0 \leq i < k+1$, $f^{(i)}(\alpha) = 0$. Since $f(\alpha) = 0$ we have $f(X) = (X-\alpha)q(X)$.

$$\begin{aligned} f'(X) &= (X-\alpha)q'(X) + q(X) \\ f^{(2)}(X) &= (X-\alpha)q^{(2)}(X) + q^{(1)}(X) \\ f^{(3)}(X) &= (X-\alpha)q^{(3)}(X) + q^{(2)}(X) \\ &\vdots \qquad \vdots \\ f^{(k)}(X) &= (X-\alpha)q^{(k)}(X) + q^{(k-1)}(X) \end{aligned}$$

For all $0 \leq i \leq k$ $f^{(i)}(\alpha) = 0 \implies \forall\ 0 \leq i < k$ $q^{(i)}(\alpha) = 0$. By induction hypothesis we have $(X-\alpha)^k \mid q(X)$. Hence $q(X) = (X-\alpha)^k g(X)$. Therefore $f(X) = (X-\alpha)(X-\alpha)^k g(X) = (X-\alpha)^{k+1} g(X)$. Hence $(X-\alpha)^{k+1}$ divides $f(X)$. Therefore the given statement is true for all $j \leq char(\mathbb{F}_q)$.

4. Suppose there are more than $\lfloor \frac{t}{m} \rfloor$ distinct elements $\alpha \in \mathbb{F}_q$ such that $f^{(j)}(\alpha) = 0$ for all $0 \leq j < m$. Such elements is then at least $\lfloor \frac{t}{m} \rfloor + 1$. Let these elements are $\alpha_1, \ldots, \alpha_k$. By part (3) for each of these elements $\alpha \in \mathbb{F}_q$ we have that $(X-\alpha)^m$ divides $f(X)$. Then we have $g(X) = \prod_{i=1}^{k} (X-\alpha)^m$ divides $f(X)$. Now $\deg((X-\alpha_i)^m) = m$. So $\deg(g) = km$. Now

$$km \geq \left(\left\lfloor \frac{t}{m} \right\rfloor + 1 \right) m \geq t + m > t$$

But $\deg(f) = t$. Hence contradiction. Therefore there can be at most $\lfloor \frac{t}{m} \rfloor$ distinct elements satisfying $f^{(j)}(\alpha) = 0$ for all $0 \leq j < m$.

□

Problem 10 Chapter 5

Ex 5.17

Solution: Each alphabet of the new code is a m-tuple where each element is from $\mathbb{F}_q$. So for any polynomial f_m of a message m and a value α, $(f_m(\alpha), f_m^{(1)}(\alpha), \ldots, f_m^{(m-1)}(\alpha))$ is an alphabet of this code system. Hence code length is n. Since the number of code is still same $|C| = q^k = (q^m)^{\frac{k}{m}}$. So dimension becomes $\frac{k}{m}$.

Consider the polynomial $f_{m_1}(X) - f_{m_2}(X) = f_{12}(X)$. Now $\deg(f_{12}(X)) = k-1$. Now take the m-tuple $(f_{12}(X), f_{12}^{(1)}(X), \ldots, f_{12}^{(m-1)}(X)) = u_{12}(X)$. For any $\alpha \in \mathbb{F}_q$ $u_{12}(\alpha) = \overline{0}$ when for all $0 \leq i \leq m-1$ we have $f_{12}^{(i)}(\alpha) = 0$. Such distinct $\alpha \in \mathbb{F}_q$ can exist at most $\left\lfloor \frac{k-1}{m} \right\rfloor$ many. So distance of this new code is $d \geq n - \left\lfloor \frac{k-1}{m} \right\rfloor$. Now let $l = \left\lceil \frac{k-1}{m} \right\rceil$. Then take the polynomial $g(X) = \prod_{i=1}^{l} (X - \alpha_i)^m$. So $(g(X), g^{(1)}(X), \ldots, g^{(m-1)}(X)) = \overline{0}$ for l many values. Hence in the code formed from $g(X)$ the weight is $n - (f_{12}(X), f_{12}^{(1)}(X), \ldots, f_{12}^{(m-1)}(X))$. Therefore the new code is $\left[n, \frac{k}{m}, n - \left\lfloor \frac{k-1}{m} \right\rfloor\right]$.

□