MODERN CODING THEORY: HOMEWORK 9

RETHNAKARAN PULIKKOONATTU

1. HOMEWORK 9

1.1. **Problem-1.** Rank of a matrix G is essentially the number of nonzero rows when the matrix G is expressed in echelon form. So, we just need to compute the ways these matrices can be created with k non zero rows. Since the elements of the matrix are binary (from $\mathbb{F}_q$, we can simply do a counting.

It is trivial to compute $R(l,m,k)$ for $k=0$ and $k>l$. For $k=0$, only all zero matrix possible, and only one such matrix exist. Hence $R(l,m,0)=1$. For $l>k>0$, since $k>\min(l,m)$, no matrix exist, which means $R(l,m,k>l)=0$. Now we consider $l=k>0$.

How many ways? We have $k=l$ non zero rows of the $l\times m$ matrix, which means all rows must be nonzero. Without loss of generality, for counting, we could assume that, the rows are ordered. The last row (l^{th} row can be be done in 2^m-1, since there anything other than all 0 vector (of size m) is allowed. On $(l-1)$-th row, anything other than that of row l is allowed. There are 2^m-2 ways here. $l-2$-th row can have anything except any linear combination of the rows l and $l-1$. This is nothing but $2^m-\left(\binom{2}{0}+\binom{2}{1}+\binom{2}{2}\right)=2^m-2^2$. Row $l-3$ then have $2^m-\left(\binom{3}{0}+\binom{3}{1}+\binom{3}{2}\right)=2^m-2^3$ and so on. In all, Following the procedure, we can have a total of,

$$\begin{aligned}
&= (2^m-1)\left(2^m-2^1\right)\left(2^m-2^2\right)\ldots\left(2^m-2^{l-1}\right)\\
&= (2^m-1)\,2^1\left(2^{m-1}-1\right)2^2\left(2^{m-2}-1\right)\ldots 2^{l-1}\left(2^{m-l+1}-1\right)\\
&= 2^0 2^1 2^2\ldots 2^{l-1}(2^m-1)\left(2^{m-1}-1\right)\left(2^{m-2}-1\right)\ldots\left(2^{m-l+1}-1\right)\\
&= \prod_{i=0}^{l-1}2^i\left(2^{m-i}-1\right)\\
&= \prod_{i=0}^{l-1}\left(2^m-2^i\right)\\
&= \prod_{i=0}^{l-1}2^m\left(1-2^{i-m}\right)\\
&= 2^{ml}\prod_{i=0}^{l-1}\left(1-2^{i-m}\right)
\end{aligned}$$

ways.

For $l>k>0$, we can construct a rank k matrix of size $l\times m$ in any of the following ways:

(1) Take a rank $k-1$ matrix of size $(l-1)\times m$ and add and independent row.
(2) Take a rank k matrix of size $(l-1)\times m$ and add a dependent row.

For every $(l-1)\times m$ matrix, (1) can be done in

$$\begin{aligned}
2^m-\left[1+\binom{k-1}{1}+\binom{k-1}{2}+\ldots+\binom{k-1}{k-1}\right] &= 2^m-2^{k-1}\\
R(l-1,m,k-1)\left(2^m-2^{k-1}\right) &= R_1(l,m,k)
\end{aligned}$$

ways. (Essentially avoid all possible linear combinations of existing $k-1$ rows).

Date: June 13, 2008.

Using the (2) method, we can have,

$$\begin{aligned} 1+\binom{k}{1}+\binom{k}{2}+\ldots+\binom{k}{k} &= 2^k \\ R_2(l,m,k) &= 2^k R(l-1,m,k) \end{aligned}$$

different ways a rank k matrix can be formed.

Where,the first term $(=1)$ is when the all zero row is picked as the new row .In$\binom{k}{1}$ ways we can pick any one of the exisiting row as a dependent (new row). In general for $0 \leq j \leq k$ we can have combination of j existing rows out of k in $\binom{k}{j}$ different ways to make a dependent (new) row.

So using (1) and (2) we get,

$$R(l,m,k) = 2^k R(l-1,m,k) + \left(2^m - 2^{k-1}\right) R(l-1,m,k-1) \tag{1}$$

Putting everything together,

$$R(l,m,k) = \begin{cases} 1, & k=0, \\ 2^{ml}\prod_{i=0}^{l-1}\left(1-2^{i-m}\right), & l=k>0 \\ 2^k R(l-1,m,k) + \left(2^m - 2^{k-1}\right) R(l-1,m,k-1), & l>k>0 \\ 0, & k>l>0 \end{cases} \tag{2}$$

1.2. **Problem 2: From 3.31** [1]**.** (i) is simply perform the integration inside the summation and apply the limits. (ii) is by just by summing over the permutation group.(iii) is by change of summation order and chain rule (reverse chain rule). The step (iv) is simply by taking all the permutations and (v) is from the definition of code rate.

1.3. **problem 3: From C.5** [1]**.** G is a random graph with n vertices. If p is the probability that a given edge is in G. The probability space be $G(n,p)$. Let χ be a filter on the set of all such random graphs. We can define a Martingale as follows:

$$\begin{aligned} X_0 &= E[X(G)] \\ X_i &= E[X(G)|1_1,1_2,\ldots,1_i], \forall 1 \leq i \leq \binom{n}{2} \\ 1_i &= \begin{cases} 1, & \text{if edge} \quad e_i \in G \\ 0, & \text{if edge} \quad e_i \ni G \end{cases} \end{aligned}$$

χ is the Chromatic number of G. Chromatic number changes at most by one , when the information about the new edge comes in. Clearly, χ satisfies the conditions for Azuma's inequality. ($\{X_i\}_{i\geq 0}$ is a Martingale, with $|X_i - X_0| \leq 1$).

Let $Z_i = X_i - E[X_i]$. Clearly

$$\begin{aligned} E[Z_i] &= E[X_i] - E[x_i] = 0 \\ Z_m &= X_m - E[X_m] \\ &= X_m - E[X_m] \\ &= \mathrm{E}[\chi(G)|1_1,1_2,\ldots,1_m] - \mathrm{E}[\chi(G)] \\ &= \chi(G) - \mathrm{E}[\chi(G)] \end{aligned}$$

Now we can use the Azuma's inequality on $\{Z_i\}$ to get,

$$\begin{aligned} \mathbb{P}\left(|Z_n - Z_0| \geq \lambda\sqrt{n}\right) &= \mathbb{P}\left(|\chi(G) - \mathrm{E}[\chi(G)]| \geq \lambda\sqrt{n}\right) \\ &\leq 2e^{\frac{-\lambda^2}{2}}. \end{aligned}$$

Since $\mathbb{P}\left(|\chi(G) - \mathrm{E}[\chi(G)]| \geq \lambda\sqrt{n}\right) = \mathbb{P}\left(|\chi(G) - \mathrm{E}[\chi(G)]| > \lambda\sqrt{n-1}\right)$, the result

$$\mathbb{P}\left(|\chi(G) - \mathrm{E}[\chi(G)]| > \lambda\sqrt{n-1}\right) \leq 2e^{\frac{-\lambda^2}{2}}.$$

follows.

REFERENCES

[1] T.Richardson, R.Urbanke, Modern Coding theory, Cambridge University Press, 2007.

E-mail address: rethnakaran.pulikkoonattu@epfl.ch