CPTH II 1

Saswata Mukherjee
Somnath Bhattacharjee

January 8, 2023

Question 1. Exercise 2.5

a. Let f be a D degree polynomial over a finite field $\mathbb{F}$ with $|\mathbb{F}| = q$, now for some $d \leq D$, the number of distinct irreducible factors of f of degree D polynomials will be atmost $\dfrac{D}{d}$. This is because if there are l such factors then $ld \leq D$.

Now we know that for some constant c there are atleast $c\dfrac{q^{d+1}}{d}$ many ireeducible polynomials of degree d. (As we know that number of irreducible degree d monic polynomial N_d is nearly $\dfrac{q^d}{d} + O(\dfrac{q^{\frac{d}{2}}}{d})$). Also there are q^{d+1} many polynomials of degree d (as there can be $d+1$ many coefficients and each has q many choices). Now

$$\begin{aligned}
\Pr[g(x) \not| f(x)] &\geq \Pr[g(x) \not| f(x) \text{ and } g(x) \text{ is irreducible}] \\
&= \Pr[g(x) \not| f(x) \Big| g(x) \text{ is irreducible }] \times \Pr[g(x) \text{ is irreducible }] \\
&\geq \left[1 - \frac{D/d}{cq^{d+1}/d}\right] \times \frac{cq^{d+1}/d}{q^{d+1}} \\
&= \frac{1}{d} - \frac{D}{dq^{d+1}}
\end{aligned}$$

Now if we set $d = \log_q(2D) - 1$, we will have $\Pr[g(x) \not| f(x)] \geq \dfrac{1}{2d} = \dfrac{1}{\Omega(\log D)}$

So we are done $\square$

Say our input is a s size circuit C computing $f(x)$. Assume k is the maximum number of bits of the exponents in C.
Now our algorithm is :
- Pick $ts \log k$ many random $d := cs \log k$ degree univariate polynomials $\{g_i(x)\}$ independently
- For each $i = 1(1)t \log D$ check whether $g_i(x)$ divides $f(x)$ or not.
- If all the $g_i(x)$ divides $f(x)$ return $f(x) \equiv 0$, else $f(x)$ is non zero.

To check whether $g(x)$ divides $f(x)$ or not, we can simply do a BFS from bottom in the circuit of f, for each node v we will divide v by g, note v mod g is univariate d degree polynomial, so sparsity will be $d + 1$, so entire checking can be done in $poly(d) = O(poly(s))$ time.

So the running time is surely $poly(ts)$, we will take $t = poly(s)$ to adjust the error value.

Note the maximum degree computed by the circuit C is $k^s =: D$, so degree of $f \leq D$ Now if $f(x) \equiv 0$ then the algorithm will not give any error, but if $f(x) \neq 0$ then the error probability is less than $(1 - \dfrac{1}{c' \log D})^{ts} \leq e^{-tc'}$.
Now we can adjust t s.t. the error probability becomes less than $\frac{1}{2}$. $\square$

b. Let C be a multivariate s size circuit computing $f(x_0, \ldots, x_n)$ od degree d we will apply Kronecker map on f to make it univariate. Let say $q(y)$ be the polynomial after setting $x_i = y^{d^i}$ in f, we have proved in the class that this map preserves the non-zeroness ,ie, $f = 0$ iff $q = 0$. To compute y^{d^i} we need $i \log d$ size univariate exponentiation circuit. To create the circuit that computes q, we can construct the circuit for y^{d^i} individually and then connect the output gate with the x_i input gate of C. So total size of the final circuit computing q will be $n^2 \log d$ and since $n, s = O(s^c)$ the circuit size will be poly of s.

Question 2. Exercise 2.7

1. Let λ be an eigen value of M with eigen vector v, then

$$\begin{aligned} ||\lambda v|| &= ||Mv|| \\ &\leq ||M||.||v|| \\ \implies |\lambda| &\leq ||M|| \end{aligned}$$

Now from birkhoff von newmann theorem we know M is in convex span of the permutation matrices ,ie, there exists $0 \leq \lambda_1, \ldots, \lambda_k \leq 1$ with $\sum \lambda_i = 1$ s.t. if P_is are the permutation matrices

$$\begin{aligned} M &= \sum \lambda_i P_i \\ \implies ||M|| &\leq ||\sum \lambda_i P_i|| \\ &\leq \sum \lambda_i ||P_i|| \\ &\leq \sum \lambda_i = 1 && \text{(norm of permutation matrices is 1)} \end{aligned}$$

(We can prove it directly as well by taking a λ eigen value with $|\lambda| > 1$, Now say $Mv = \lambda v$, say v_i is the highest entry of v in absolute value, WLOG $v_i > 0$, Now $|\lambda| v_i$ can be written as convex sum of all the v_js which contradicts $|\lambda| > 1$. But we need the operator norm upper bound in the next problem.) $\square$

2. ($\implies$) Let the graph G is not connected and WLOG it has two connected components, then we can say the normalised matrix M for G is a diagonal block matrix with two blocks $A_{n_1 \times n_1}, B_{n_2 \times n_2}$ (where $n_1 + n_2 = N$) each is normalised adjacency matrix for the connected components ,ie,

$$M = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$$

And each A and B are doubly stochastic matrix, hence each have eigen value 1 with multiplicity atleast 1, so M has eigen value 1 with multiplicity atleast 2.

($\Longleftarrow$) We will prove a lemma first, which says for a set of variables $\{x_1, \dots, x_n\}$, if x_i can be written as convex combination of all the x_js then $x_i = x_j$.

Lemma 1. For any k, for any $0 < \lambda_1, \dots, \lambda_k < 1$, and $\sum \lambda_i = 1$, if $x_1 = \sum \lambda_i x_i$ has some real solution, then $x_i = x_1$ for all i

We will induct strongly on k.
When $k = 2$

$$x_1 = \lambda x_1 + (1-\lambda)x_2 \implies x_1 = x_2$$

Assume it is true for all $k \leq t$ for some $t \geq 2$. Now for $t+1$, since $\lambda_1 \neq 0$ we can say $\lambda_{t+1} \neq 1$

$$\begin{aligned} x_1 &= \sum \lambda_i x_i + \lambda_{t+1} x_{t+1} \\ &= (1-\lambda_{t+1}) \frac{\sum \lambda_i x_i}{1-\lambda_{t+1}} + \lambda_{t+1} x_{t+1} \end{aligned}$$

Hence from induction hypothesis, $x_{t+1} = x_1$ and $\dfrac{\sum_{i=1}^{t} \lambda_i x_i}{1-\lambda_{t+1}} = x_1$
Now as

$$\sum_{i=1}^{t} \frac{\lambda_i}{1-\lambda_{t+1}} = \frac{1-\lambda_{t+1}}{1-\lambda_{t+1}} = 1$$

So again from induction hypothesis $x_i = x_1 \ \forall i = 1(1)t$ $\square$

Now say $Mv = v$ for some v then any v_i can be written as convex combination of v_rs where rs are the neighbours of i. So from the lemma $v_i = v_r$. Now the graph is connected, so v_1 will be same with all the neighbours of 1, and they will be same as their neighbours and so on , and this way all the v_i will be same. So $v = \mathbf{1}_v$. $\square$

3. ($\implies$) Say the vertex sets are A, B. It can also be seen that M has two diagonal 0 blocks of order $|A| \times |A|$ and $|B| \times |B|$. So

$$M = \begin{bmatrix} 0_A & P_{|A|\times|B|} \\ Q_{|B|\times|A|} & 0_B \end{bmatrix}$$

Also P, Q are doubly stochastic.
Consider the vector $v = (\underbrace{1, \dots, 1}_{|A| \text{ many}}, \underbrace{-1, \dots, -1}_{|B| \text{ many}})$
So $Mv = -v$ as P, Q are doubly stochastic.

($\Longleftarrow$) Let v be an eigen vector of M with eigen value -1. Let u be the vector with $u_i = |v_i|$. Now

$$\begin{aligned}
||v||^2 &= -\langle v, Mv\rangle \\
&= -v^T Mv \\
&= -\sum_{i,j} v_i M_{ij} v_j \\
&= -\sum_i v_i^2 M_{ii} - 2\sum_{(i,j)\in E, i\neq j} v_i M_{ij} v_j \\
&\leq |\sum_i v_i^2 M_{ii} + 2\sum_{(i,j)\in E, i\neq j} v_i M_{ij} v_j| && (\text{......................(i)}) \\
&\leq \sum_i |v_i^2 M_{ii}| + 2\sum_{(i,j)\in E, i\neq j} |-v_i M_{ij} v_j| \\
&= \sum_i u_i^2 M_{ii} + 2\sum_{(i,j)\in E, i\neq j} u_i M_{ij} u_j \\
&= \sum_{i,j} u_i M_{ij} u_j \\
&= \langle u, Mu\rangle \\
&\leq ||u||.||Mu|| \\
&\leq ||u||^2.||M|| \leq ||u||^2 && \text{(From the first problem)}
\end{aligned}$$

Now since $||u|| = ||v||$, we can say all the inequalities will convert to equality. From the (i) step $v_i v_j \leq 0$ and $M_{ii} = 0$. So for all $(i,j) \in E$ we have $i \neq j$ and one $v_i > 0$ and another $v_j < 0$. So the vertex decomposition is $A = \{i \big| v_i \geq 0\}, B = \{j \big| v_j < 0\}$. We can say there are no internal edges in A or B, hence G is bipartite. $\square$

4. We will prove the hint first. Say the $n \times n$ matrix $D = dM$, so D_{ij} is the number of edges between v_i and v_j. So $\sum_{i,(i,j)\in E} D_{ij} = \sum_{j,(i,j)\in E} D_{ij} = d$

$$\begin{aligned}
\langle v, Mv\rangle = \sum_{i,j} v_i M_{ij} v_j &= \sum_i v_i^2 M_{ii} + 2\sum_{(i,j)\in E, i\neq j} v_i M_{ij} v_j \\
&= \frac{1}{d}\sum_i v_i^2 D_{ii} + \frac{1}{d}\sum_{(i,j)\in E, i\neq j} D_{ij}(2v_i v_j) \\
&= \frac{1}{d}\sum_i v_i^2\big(d - \sum_{j,(i,j)\in E, i\neq j} D_{ij}\big) + \frac{1}{d}\sum_{(i,j)\in E, i\neq j} D_{ij}(2v_i v_j) \\
&= \sum_i v_i^2 + \frac{1}{d}\sum_{(i,j)\in E, i\neq j} D_{ij}(2v_i v_j - v_i^2 - v_j^2) \\
&= ||v_i||^2 - \frac{1}{d}\sum_{(i,j)\in E, i\neq j} D_{ij}(v_i - v_j)^2 \\
&= 1 - \frac{1}{d}\sum_{(i,j)\in E} D_{ij}(v_i - v_j)^2
\end{aligned}$$

$$\implies \max_{v \text{ with the conditions}} \langle v, Mv\rangle = 1 - \min_{v \text{ with the conditions}} \sum_{(i,j)\in E} D_{ij}(v_i - v_j)^2$$

Now note $W := \{x | \sum x_i = 0\} = \{x | \langle x, \mathbf{1}\rangle = 0\} = \mathbf{1}^\perp$
Hence $\dim(W) = n-1$
Now say multiplicity of 1 eigen value is t ($\lambda_1, \ldots, \lambda_t = 1$) and λ_{t+1} is largest eigen value which is not 1.
So if $\{v_1, \ldots, v_{n-1}\}$ are the basis of W and $\{u_1, \ldots, u_{t-1}, u_t\}$ be the eigenvectors corresponding to the eigen values $\lambda_1 = 1, \lambda_2$ of M, then all of them cannot be linearly independent together else the dimension of $\mathbb{R}^n$ will be $n-1+t+1 = n+t$ which is not possible. so $\exists\ k_o, \ldots, k_t, a_1, \ldots, a_{n-1}$ s.t. $\sum k_i^2 = 1$ and not all a_is are zero, $v := k_0u_0 + \cdots + k_tu_t = a_1v_1 + \cdots + a_{n-1}v_{n-1}$

Note $||v|| = 1$, now

$$
\begin{aligned}
1 - \min_{x, x\in W, ||x||=1} \frac{1}{d} \sum_{(i,j)\in E} d_{ij}(x_i - x_j)^2 &= \max_{x, x\in W, ||x||=1} \langle x, Mx\rangle \\
&\geq \langle v, Mv\rangle \\
&= \langle v, \sum \lambda_i k_{i-1} u_{i-1}\rangle \\
&= \sum \lambda_i k_{i-1}^2 + \\
&\geq \lambda_{t+1} \sum k_i^2 = \lambda_{t+1}
\end{aligned}
$$

Now assume G be the graph whoose all eigenvalues are non-negative. Now if we can prove that $\sum_{(i,j)\in E} (x_i - x_j)^2 \geq 1/poly(n,d)$ then it will essentially imply

$$
1 - \min_{x, x\in W, ||x||=1} \sum_{(i,j)\in E} d_{ij}(x_i - x_j)^2 \leq 1 - poly(n,d)
$$

as $d_{ij} \geq 1$ if $(i,j) \in E$. Hence largest eigen value (in terms of absolute value) after 1 is atmost $1 - 1/poly(n,d)$. Following claim will prove the remaining part.

Claim. $\sum_{(i,j)\in E} (x_i - x_j)^2 \geq 1/poly(n,d)$

We know that $\sum |x_i^2| = 1$, hence there exists a x_i s.t. $|x_i| \geq \dfrac{1}{\sqrt{n}}$.
Now there must be one x_j s.t. $x_i.x_j < 0$ and since G is connected, i and j is also connected, say via the path $i = i_0, i_1, \ldots, i_k = j$.
So

$$
\begin{aligned}
\sum_{r=0}^{k-1} (x_{i_r} - x_{i_{r+1}})^2 &\geq \frac{\left(\sum_{r=0}^{k-1} (x_{i_r} - x_{i_{r+1}})\right)^2}{k+1} \\
&= \frac{(x_i - x_j)^2}{k+1} \geq \frac{1}{nD} \qquad (D \text{ is the diameter}) \\
\implies \sum_{(i,j)\in E} (x_i - x_j)^2 &\geq \frac{1}{nD}
\end{aligned}
$$

□

So the overall bound will be $1 - \frac{1}{ndD}$ if all the eigen values are non-negative. Now if not all eigen values are nonnegative then G^2 will have all the eigen values non-negative, and then we can apply the previous part to get largest eigen value (in terms of absolute value) after 1

$$\lambda_2 \geq (1 - 1/ndD)^{\frac{1}{2}} \geq (1 - \frac{1}{2ndD})$$

$\square$

5. G is connected means multiplicity of 1 as an eigen value is exactly one and non bipartite means -1 is not an eigen value. Hence the second largest eigen value in terms of absolute value $\lambda_2 \leq 1 - 1/poly(n,d)$, or the spectral gap $\gamma(G) \geq 1/poly(n,d)$

6. Consider G as $2k$ cycle. Clearly here $n = 2k$, $d = 2$, $D = 2k - 1$, so $\lambda_2 \leq 1 - \frac{1}{\Omega(k^2)}$ from the above calculations.
Now consider

$$J_{2k \times 2k} = \frac{1}{2} \begin{bmatrix} 0 & \dots & 0 & 1 \\ & I_{2k-1 \times 2k-1} & & 0 \end{bmatrix}$$

It can be seen that the normalised adjacency matrix of G is just $J + J^T$ and the eigen values of J are $\frac{1}{2} \times$ $2k$th roots of unity. Now let M, M^T diagonalise J, ie, $MJM^T =$ some diagonal matrix D then

$$\begin{aligned} M(J + J^T)M &= MJM^T + MJ^TM^T \\ &= D + M(MJ)^T \\ &= D + (MJM^T)^T \\ &= D + D^T \end{aligned}$$

Hence M, M^T can diagonalize $J + J^T$ as well. So the eigen values of $J + J^T$ is $\frac{1}{2}(e_i + \overline{e_i})$ where e_is are the $2k$th roots of unity. Hence the second largest eigen value will be

$$\cos\frac{\pi}{k} \geq 1 - \frac{1}{k^2\pi^2/2} = 1 - \frac{1}{O(k^2)}$$

Hence the bound is tight.

Now we know $\gamma(G) \geq \frac{1}{\Omega(ndD)}$ and D can be atmax n, so

$$\gamma(G) \geq \frac{1}{\Omega(n^2 d)} \geq \frac{1}{\Omega(n^2 d^2)}$$

Question 3. Exercise 3.2

1. Say, we have $S_1, \dots, S_{i-1}$ fixed such that $\forall j \in [i-1], |S_j| = l$ and $|S_j \cap S_k| < a$ for $j \neq k$. Now we are randomly choosing S_i.
Say, X_j is the event of $|S_i \cap S_j| \geq a$.
i.e.,

$$X_j = \begin{cases} 1 & \text{if } |S_i \cap S_j| \geq a \\ 0 & \text{otherwise} \end{cases}$$

for $j \leq i-1$.
Now,

$$\begin{aligned}
E_{S_i}[\#\{j < i : |S_i \cap S_j| \geq a\}] &= E_{S_i}[\sum_{j=1}^{i-1} X_j] \\
&= \sum_j E_{S_i}[X_j] \\
&= \sum_j \Pr_{S_i}[|S_i \cap S_j| \geq a] \\
&= \sum_{j=1}^{i-1} \frac{\binom{l}{a}\binom{d-a}{l-a}}{\binom{d}{l}} \\
&< m \frac{\binom{l}{a}\binom{d-a}{l-a}}{\binom{d}{l}} \\
&= m \frac{\binom{l}{a}^2}{\binom{d}{l}} < 1
\end{aligned}$$

That means, if we randomly choose S_i, with probability < 1, it will intersect with some $S_j, j \in [i-1]$ in at least a elements.
$\implies \exists S_i$ so that $|S_j \cap S_i| < a$ for all $j \in [i-1]$.
$\implies \exists S_1, \ldots, S_m$ where $m \leq \dfrac{\binom{d}{l}}{\binom{l}{a}^2}$ and $|S_i| = l, |S_i \cap S_j| < a$.

2. $m \leq \dfrac{\binom{d}{l}}{\binom{l}{a}^2}$.

we know $\dfrac{(d/a)^a}{(le/a)^{2a}} \leq \dfrac{\binom{d}{l}}{\binom{l}{a}^2}$.

Now, if $d = O(\dfrac{l^2}{a}) \implies d \approx cl^2/a$ for some c.

$\implies \dfrac{(\frac{cl^2}{a^2})^a}{e^{2a}(\frac{l^2}{a^2})^a} = \dfrac{c^a}{e^{2a}} \leq \dfrac{\binom{d}{l}}{\binom{l}{a}^2}$.

Take $c_0 = (\dfrac{c}{e^2})^\gamma$ where $a = \gamma \log m$.

If we assume $c_0 \geq 2$, then, $m = 2^{\log m} \leq (c_0)^{\log m} \leq \dfrac{\binom{d}{l}}{\binom{l}{a}^2}$.

So, we can find $S_1, \ldots, S_m \subset [d]$ with $d = O(\dfrac{l^2}{a})$ and $a = \gamma \log m$.

3. Initially take $A = \{S_1\}$ where $S_1 \subset [d]$ be any of size l.
While $|A| < m$:
    for all $S_0 \subset [d]$ so that $|S_0| = l$:
        if $|S \cap S_0| < a, \quad \forall S \in A$, add S_0 to A.
    end for.
end while.

Part 1,2 shows that the algorithm will not stop at any intermediate step for some specific choice of d, l, a. And the algorithm runs in $poly(m, d)2^d$ time.
Now, $d = O(l) \approx cl$ for some c and $m = 2^l$. So, $2^d \approx (2^l)^c = poly(m)$.

Hence, algorithm runs in $poly(m, d)$ time.

Question 4. Problem 4.9

1. As given as a hint, we can prove that $(G_1 \text{ⓡ} G_2)^3$ has $G_1 \text{ⓩ} G_2$ as subgraph via some calculations. Let $H = G_1 \text{ⓡ} G_2$ and M be the normalised adjacency matrix of H, clearly H is D_2+1 regular, hence H^3 is $(D_2+1)^3$ regular. Let for $u \in [N_1]$ A_u be the permutation matrix corresponds to the bijection on $[D_2]$ which is i is mapped to j iff i th neighbour of u is v and jth neighbour of v is u. Now let $\tilde{A}$ be the $N_1D_1 \times N_1D_1$ matrix whoose uth $D_1 \times D_1$ diagonal block is A_u, (basically $\tilde{A}$ is the permutation matrix we will use to construct the zigzag product). Let B be the normalized adjacency matrix of G_2 and $\tilde{B} = B \otimes I_{N_1 \times N_1}$.
So the normalized adjaceny matrix of $H' := G_1 \text{ⓩ} G_2$ is $\tilde{B}\tilde{A}\tilde{B} =: C$
Now the adjacency matrix of M^3

$$\begin{aligned}(D_2+1)^3 M &= (\tilde{A} + D_2\tilde{B})^3 \\ &= D_2^2(\tilde{B}\tilde{A}\tilde{B}) + (\dots)\end{aligned}$$

Now note if we remove the subgraph H' from H, the graph will be $(D_2+1)^3 - D_2^2$ regular. Let the normalised adjacency matrix of it be D and $x = \dfrac{D_2^2}{(D_2+1)^3}$ then

$$\begin{aligned} M &= xC + (1-x)D \\ \implies \max_{v, v \perp \mathbf{1}} &\leq \max_{v, v\perp \mathbf{1}} C + (1-x) \max_{v, v \perp \mathbf{1}} D \\ \implies (1-g)^3 &\leq x(1 - \gamma_1\gamma_2^2) + (1-x) \\ &= 1 - x\gamma_1\gamma_2^2 < 1 \\ \implies g(\gamma_1, \gamma_2, D_2) > 0 & \end{aligned}$$

□

2. Now the idea is simple, for $G = (N, D, \gamma)$ (where D is constant) we will take G' as a D cycle, in the 2nd problem we have proved that $\gamma(G')$ is $\Theta(1 - \frac{1}{D^2})$,
Now $G \text{ⓡ} G'$ is $(ND, 3, \gamma')$ expander (since D is constant, there is no big blow up in vertex size), so we have converted the degree into the constant 3.

3. Let $h := \min\{\dfrac{D_2\varepsilon_1\varepsilon_2}{(D_2+1)(\varepsilon_1+6)}, \quad \dfrac{\varepsilon_1}{(D_2+1)(\varepsilon_1+6)}, \quad \dfrac{D_2\varepsilon_2}{2(D_2+1)}\}$
We will prove that $H := G_1 \text{ⓡ} G_2$ is h edge expander.(clearly $h \geq 0$)

Let S be a vertex subset of H with $|S| \leq N_1D_1/2$
As given in the hint, we will make two partitions on S: A and B, where A is the set of all *half full* clouds (ie, $(u, v) \in A$ if there is atleast $\frac{D_1}{2}$ many v_is in $V(G_2)$ s.t. $(u, v_i) \in S$), B is set of *half empty* clouds defined by $S - A$.
Define $C = \{u \in V(G_1) \big| \exists v \in V(G_2) \text{ s.t. } (u, v) \in A\}$. Basically C is the projection of A on $V(G_1)$.

Note that

$$|S| \leq |B| + |C|D_1$$
$$\implies |C| \geq \frac{|S| - |B|}{D} \qquad (.............(i))$$

Now
Case 1: $|B| > \frac{\varepsilon_1}{\varepsilon_1 + 6}|S|$
We will have atleast $D_2\varepsilon_2|B| \geq \frac{D_2\varepsilon_1\varepsilon_2}{\varepsilon_1 + 6}|S|$ many edges from S to S^c (that is because we are applying G_2 edge expansion in each clouds of B). Hence edge expansion is

$$\frac{\frac{D_2\varepsilon_1\varepsilon_2}{\varepsilon_1 + 6}|S|}{(D_2 + 1)|S|} \geq h$$

Case 2: $|B| \leq \frac{\varepsilon_1}{\varepsilon_1 + 6}|S|$ and $|C| \leq \frac{N_1}{2}$

Note if E is the set of edges between C and C^c in G_1, then there will be atleast $|E| - |B|$ many edges between S and S^c in H, as any vertex in H will have exactly one G_1 neighbour. So there can be atmost $|B|$ many edges corresponds to E in H which are from half full clouds to half empty clouds in S, and remaining edges are going outside of S.

Now there are atleast $|C|\varepsilon_1 D_1$ many edges from C to C^c in G_1 (edge expansion on G_1),

$$\begin{aligned}
|C|\varepsilon_1 D_1 &\geq \frac{|S| - |B|}{D_1}\varepsilon_1 && \text{(from (i))}\\
&\geq |S|(1 - \frac{\varepsilon_1}{\varepsilon_1 + 6})\varepsilon_1 \\
&= 2 \times 3|S|\frac{\varepsilon_1}{\varepsilon_1 + 6} && (.............(ii))\\
&> 2|B|
\end{aligned}$$

Hence edges in H between S and S^c is atleast

$$\begin{aligned}
|C|\varepsilon_1 D_1 - |B| &\geq \frac{|C|\varepsilon_1 D_1}{2} \\
&\geq 3|S|\frac{\varepsilon_1}{\varepsilon_1 + 6} && \text{(from (ii))}
\end{aligned}$$

Hence the edge expansion is $\frac{3\varepsilon_1}{(\varepsilon_1 + 6)(D_2 + 1)} \geq h$.

Case 3: $|B| \leq \dfrac{\varepsilon_1}{\varepsilon_1+6}|S|$ and $\dfrac{3N_1}{4} \geq |C| \geq \dfrac{N_1}{2}$

In this case we know $|C^c| \leq \frac{N_1}{2}$ hence number of edges between T and T^c is atleast

$$
\begin{aligned}
|C^c|\varepsilon_1 D_1 &\geq \frac{N_1\varepsilon_1 D_1}{4} \\
&\geq \frac{|C|\varepsilon_1 D_1}{3} \\
&\geq \frac{(|S|-|B|)\varepsilon_1}{3} \\
&\geq 2|S|\frac{\varepsilon_1}{\varepsilon_1+6} && (\text{..........(iii)}) \\
&\geq 2|B|
\end{aligned}
$$

Similarly from the fact we used in the previous case, the edges between S and S^c in H is atleast

$$
\begin{aligned}
|C^c|\varepsilon_1 D_1 - |B| &\geq \frac{|C^c|\varepsilon_1 D_1}{2} \\
&\geq |S|\frac{\varepsilon_1}{\varepsilon_1+6} && (\text{from (iii)})
\end{aligned}
$$

Hence the edge expansion is $\dfrac{\varepsilon_1}{(\varepsilon_1+6)(D_2+1)} \geq h$

Case 4: $|B| \leq \dfrac{\varepsilon_1}{\varepsilon_1+6}|S|$ and $|C| \geq \dfrac{3N_1}{4}$

Claim. there are atleast $\frac{N_1}{4}$ many clouds in C who have paired with atmost $\frac{3D_1}{4}$ many vertices from $V(G_2)$ and are contained in S

Let x be the number of clouds who have atmost $\frac{3D_1}{4}$ many pairs from $V(G_2)$ inside S. Then

$$
\begin{aligned}
& x\frac{D_1}{2} + (|C|-x)\frac{3D_1}{4} \leq |S| \leq \frac{N_1D_1}{2} \\
\implies & \frac{N_1D_1}{2} + x\frac{D_1}{4} \geq |C|\frac{3D_1}{4} \geq \frac{9N_1D_1}{16} \\
\implies & x \geq \frac{N_1}{4}
\end{aligned}
$$

□

Now let $W \subseteq V(G_2)$ be the pairs of any of the above vertices, then $|W| \leq \frac{3D_1}{4}$, so number of edges between W and W^c is atleast $\varepsilon_2 D_2|W^c| \geq \varepsilon_2 D_2\frac{D_1}{4}$ and all such edges will be present in H as edges between S and S^c. So number of edges between S and S^c in H is atleast $\dfrac{\varepsilon_2 D_2 N_1}{4} \geq \dfrac{|S|\varepsilon_2 D_2}{2}$.

Hence the edge expansion is $\dfrac{\varepsilon_2 D_2}{2(D_2+1)} \geq h$

4. Construct S such a way that every cloud in S is *completely full*, ie, if $(u, v) \in S$ then $\forall w \in V(G_2)$, $(u, w) \in S$. Note now any edge corresponds to G_2 can not go outside of S as all the G_2 neighbours of some $(u, v) \in S$ is inside S since the u-cloud in S is completely full. So only G_1 edges can go outside S, and each vertes in H has exactly one G_1 neighbour,

so # edges outgoing from $S \leq$ number of G_1 edges of $S = |S|$, hence $\varepsilon_2 \leq \dfrac{1}{D_2 + 1}$

Question 5. Problem 5.5

1. Let $A_{M \times N}$ be the adjacency matrix of the corresponding bipartite graph.

Claim. $x = (x_1, \ldots, x_N) \in \{0, 1\}^N$ is a code word $\iff Ax = 0 \pmod 2$.

Proof : Clearly, ith coordinate of Ax is $\sum_{j \in \Gamma(i)} x_j$.
So, for $i \in [M]$, $\bigoplus_{j \in \Gamma(i)} x_j = 0 \iff \sum_{j \in \Gamma(i)} x_j = 0 \pmod 2$.
$\implies \forall i \in [M], \bigoplus_{j \in \Gamma(i)} x_j = 0 \iff \forall j \in [M], \sum_{j \in \Gamma(i)} x_j = 0 \pmod 2$.
$\implies \forall i \in [M], \bigoplus_{j \in \Gamma(i)} x_j = 0 \iff \forall j \in [M], \bigoplus_{j \in \Gamma(i)} x_j = 0$.

Identify $\{0, 1\}^N$ as a vector space of $\mathbb{F}_2$ and $\{0, 1\}^M$ as a subspace of $\{0, 1\}^N$ over $\mathbb{F}_2$.
By, rank nullity theorem, $\ker(A) + \text{rank}(A) = N$ and $\text{rank}(A) \leq M$
$\implies \ker(A) \geq N - M \implies |\mathcal{C}| \geq 2^{N-M}$.
Therefore, $\log |\mathcal{C}| \geq N - M \implies \text{rate} \geq \dfrac{N - M}{N} = 1 - \dfrac{M}{N}$.

2. Say, $c \in \mathcal{C}$, take $S_c = \{i \in [N] : c_i = 1\}$ and each $j \in [M]$ has even number of neighbours in S_c.
If $c \in \mathcal{C}$ be a codeword, and if possible hamming weight of $c \leq K$.
Then, $|S_c| < K \implies |\Gamma(S_c)| > \dfrac{D}{2}|S_c|$.
For $j \in \Gamma(S_c)$, take y_j = number of neighbours of j in S_c = number of edges from j to S_c.
So, $\sum_{j \in \Gamma(S_c)} y_j =$ number of edges from S_c to $\Gamma(S_c) \leq D|S_c|$.
$\implies$ average number of neighbours of each $j \in \Gamma(S_c) < 2$, as $|\Gamma(S_c)| > \dfrac{D}{2}|S_c|$.
$\implies \exists j \in \Gamma(S_c)$ so that there is unique $i \in S_c$, $(i, j) \in E$, Hence contradiction.
So, $d_H(c, 0) \geq \dfrac{K}{N}$ for all $c \in \mathcal{C}$.

Take $c, c' \in \mathcal{C}$, then, $d_H(c, c') = |S_c \Delta S_{c'}| = |S|$.
If, $d_H(c, c') < \dfrac{K}{N}$, $|S_c \Delta S_{c'}| < K \implies |\Gamma(S_c \Delta S_{c'})| > \dfrac{D}{2}|S_c \Delta S_{c'}|$.
take $c_0 \in \{0, 1\}^N$ so that $c_{0i} = 1 \iff i \in S_c \Delta S_{c'}$.
Now, $c, c' \in \mathcal{C} \implies Ac - Ac' = A(c - c') = 0 \pmod 2 \implies c_0$ is a codeword.
Hence, $d_H(c_0, 0) \geq \dfrac{K}{N} \implies d_H(c, c') \geq \dfrac{K}{N}$.

3. Decoding:

Definition 0.1.
$UNSAT(i) = \{j \in \Gamma(i) :$ parity check corresponding to j is not satisfied $\}$.
For $S \subseteq [N]$, $U(S) = \{j \in \Gamma(S) : j$ has a unique neighbour in $S\}$.

Say, received message is $r = (r_1, \ldots, r_N)$.
Algorithm:
While there is $i \in [N]$ so that number of $|UNSAT(i)| > 2/3|\Gamma(i)|$:
    flip r_i.
return r.

If at some stage number of wrong parity checks are $> k + \frac{2}{3}|\Gamma(i)|$ then after flipping that r_i, wrong parity checks $< k + \frac{1}{3}|\Gamma(i)|$. Initially we can have at most N corrupted bits, so this algorithm runs in at most $O(N)$ time as each iteration decreases total number of corrupted bits.

Claim. If G is $(K, (1-\epsilon)D)$ expander then,
for any $|S| < K, \quad |U(S)| > D(1-2\epsilon)|S|$.

Proof : Total number of edges out of $S = D|S|$ but we know $|\Gamma(S)| > D(1-\epsilon)|S|$.
Say, $NU(S) = \Gamma(S) - U(S)$, then, $|U(S)| + 2|NU(S)| \leq D|S|$.
And $|U(S)| + |NU(S)| > (1-\epsilon)D|S|$.
By this two inequalities, we have $|U(S)| > (1-2\epsilon)D|S|$.

Claim. If number of errors $< K$, then, there is a node in left vertex set, whose $> 2/3$ neighbours make wrong parity check. (For sufficiently small ϵ)

Proof : Say, S = set of corrupted vertices. Then after each iteration $|S| < K$ as, error does not increase. So, $|U(S)| > (1-2\epsilon)D|S| > 2D|S|/3$ if $\epsilon < 1/6$.
As, parity checks for all of $j \in U(S)$ is not satisfied, there is a vertex i in S so that $|UNSAT(i)| > 2D/3$.
$\implies$ i has $> 2/3$ neighbours which make wrong parity check.

Therefore, if r be the received message $d_H(r, w) < \frac{K}{N}$ where w is the nearest codeword to r, the algorithm ends up giving the codeword w.