

Để chứng minh định lý của Bregman, ta sử dụng 3 mệnh đề dưới đây:

- (A) $H(X) \leq \log_2(|\text{supp}X|)$. Dấu "=" xảy ra khi và chỉ khi X là phân phối đều trên $\text{supp} X$ (tức $\text{Prob}(X = a) = \frac{1}{n}$ với $a \in \text{supp} X, n = |\text{supp} X|$).

Chứng minh: Không mất tính tổng quát, giả sử $p_i > 0 \forall i$. Áp dụng bất đẳng thức **AM-GM**: $a_1^{p_1} \dots a_n^{p_n} \leq p_1 a_1 \dots p_n a_n$: Đặt $a_i = \frac{1}{p_i}$ và lấy log 2 vế, ta được:

$$H(X) = \sum_{i=1}^n p_i \log_2 \frac{1}{p_i} \leq \log_2 \left(\sum_{i=1}^n p_i \frac{1}{p_i} \right) = \log_2 n.$$

Dấu "=" xảy ra khi và chỉ khi $p_1 = \dots = p_n = \frac{1}{n}$

- (B) $H(X, Y) = H(X) + H(Y|X)$, và tổng quát ta có $H(X_1, \dots, X_n) = H(X_1) + H(X_2|X_1) + \dots + H(X_n|X_1, \dots, X_{n-1})$

Chứng minh:

$$\begin{aligned} H(X, Y) &= - \sum_{i,j} p(a_i, b_j) \log_2 p(a_i, b_j) \\ &= - \sum_{i,j} p(a_i, b_j) \log_2 p(a_i) p(b_j|a_i) \\ &= - \sum_{i,j} p(a_i, b_j) [\log_2 p(a_i) + \log_2 p(b_j|a_i)] \\ &= - \sum_{i,j} p(a_i, b_j) \log_2 p(a_i) - \sum_{i,j} p(a_i, b_j) \log_2 p(b_j|a_i) \\ &= - \sum_{i,j} p(a_i, b_j) \log_2 p(a_i) - \sum_{i,j} p(a_i) \cdot p(b_j|a_i) \log_2 p(b_j|a_i) \\ &= - \sum_{i=1}^m p(a_i) \log_2 p(a_i) \sum_{j=1}^n p(b_j|a_i) + H(Y|X) \\ &= - \sum_{i=1}^m p(a_i) \log_2 p(a_i) + H(Y|X) = H(X) + H(Y|X) \end{aligned}$$

$$\left(\text{Do } \sum_{j=1}^n p(b_j|a_i) = \sum_{j=1}^n \frac{P(b_j \cdot a_i)}{P(a_i)} = \frac{1}{P(a_i)} \sum_{j=1}^n P(b_j \cdot a_i) = \frac{1}{P(a_i)} P(a_i) = 1 \right)$$

- (C) Nếu $\text{supp} X$ được chia thành d tập E_1, \dots, E_d sao cho $E_j := \{a \in \text{supp} X : |\text{supp}(Y|a)| = j\}$ thì:

$$H(Y|X) \leq \sum_{j=1}^d \text{Prob}(X \in E_j) \log_2 j.$$

Chứng minh: Ta có $\text{supp}(Y|a) = \{b : \text{Prob}(Y = b|X = a) > 0\}$. Vì $\text{Prob}(Y = b|X = a)$ là 1 biến ngẫu nhiên trên tập $\text{supp}(Y|a)$ (Do $\sum_{i=1}^m \text{Prob}(Y = b_i|a) = 1$) Tiến hành chia tập a_1, \dots, a_m thành các tập con E_j theo giả thuyết và sử dụng kết quả từ (A), ta có:

$$\begin{aligned}
H(X, Y) &= \sum_{i=1}^m p(a_i) H(Y|a_i) \\
&= \sum_{j=1}^d \sum_{a \in E_j} p(a) H(Y|a) \\
&\leq \sum_{j=1}^d \sum_{a \in E_j} p(a) \log_2 j \\
&= \sum_{j=1}^d \text{Prob}(X \in E_j) \log_2 j.
\end{aligned}$$

Định lý 1. Đặt $M = (m_{ij})$ là ma trận $n \times n$ chỉ chứa hai giá trị 0,1 và đặt d_1, \dots, d_n là tổng các hàng của ma trận M , hay $d_i = \sum_{j=1}^n m_{ij}$. Khi đó:

$$\text{per} M \leq \prod_{i=1}^n (d_i!)^{1/d_i}.$$

Chứng minh: Xét $G = (U \cup V, E)$ là đồ thị hai phía tương ứng với ma trận M , trong đó d_i là bậc tương ứng của các đỉnh u_i , và kí hiệu Σ là tập các *perfect matching* của G . Vì $\text{per} M = m(G) = |\Sigma|$ nên thay vì tìm cận trên cho $\text{per} M$ như định lý 1, ta sẽ tìm cận trên cho $|\Sigma|$. Giả sử $|\Sigma| \neq 0$ và mỗi $\sigma \in \Sigma$ là một hoán vị tương ứng $\sigma(1)\sigma(2)\dots\sigma(n)$ của các chỉ số. Vì vậy, tương ứng với mỗi giá trị $u_i \in U$ là một giá trị $v_{\sigma(i)} \in V$ theo phép song ánh σ .

Ý tưởng ban đầu là chọn σ một cách ngẫu nhiên và xét biến ngẫu nhiên $X = (X_1, X_2, \dots, X_n) = (\sigma(1), \sigma(2), \dots, \sigma(n))$.

Theo mệnh đề **(A)**,

$$H(\sigma(1), \sigma(2), \dots, \sigma(n)) = \log_2(|\Sigma|)$$

Do đó chỉ cần chỉ ra

$$H(\sigma(1), \dots, \sigma(n)) \leq \log_2 \left(\prod_{i=1}^n (d_i!)^{1/d_i} \right) = \sum_{i=1}^n \frac{1}{d_i} \log_2(d_i!). \quad (1)$$

Sử dụng mệnh đề **(B)**, ta có

$$H(\sigma(1), \sigma(2), \dots, \sigma(n)) = \sum_{i=1}^n H(\sigma(i) | \sigma(1), \sigma(2), \dots, \sigma(i-1)) \quad (2)$$

Ý tưởng của Radhakrishnan là xét các đỉnh u_1, u_2, \dots, u_n theo một *thứ tự ngẫu nhiên* $\tau \in S_n$, với xác suất là như nhau và bằng $\frac{1}{n!}$, và lấy giá trị kì vọng của các entropy. Nói cách khác, ta xét các cặp *matching* theo thứ tự $\tau_1, \tau_2, \dots, \tau_n$. Xét τ cố định, khi đó $k_i = \tau_i^{-1}$ được hiểu là vị trí của u_i theo thứ tự ngẫu nhiên τ là k_i . Khi đó, biểu thức (2) trở thành:

$$H(\sigma(1), \dots, \sigma(n)) = \sum_{i=1}^n H(\sigma(i) | \sigma(\tau_1), \dots, \sigma(\tau_{k_i-1}))$$

Khi đó

$$H(\sigma(1), \dots, \sigma(n)) = \frac{1}{n!} \sum_{i=1}^n H(\sigma(i) | \sigma(\tau_1), \dots, \sigma(\tau_{k_i-1}))$$

Xét biểu thức

$$H(\sigma(i) | \sigma(\tau_1), \dots, \sigma(\tau_{k_i-1})) \quad (3)$$

Để tìm cận trên cho , ta sẽ sử dụng mệnh đề **(C)**, áp dụng với biến ngẫu nhiên $X = (\sigma(\tau_1), \dots, \sigma(\tau_{k_i-1}))$ và $Y = \sigma(i)$. Với τ cố định $\in S_n$ và $\sigma \in \Sigma$ đặt $N_i(\sigma, \tau)$ là số các giá trị $k \in [n]$ sao cho $u_i v_k \in E(G)$ và $k \notin (\sigma(\tau_1), \dots, \sigma(\tau_{k_i-1}))$ (nói cách khác, $N_i(\sigma, \tau)$ là số khả năng còn lại cho $\sigma(i)$ khi đã biết $\sigma(\tau_1), \dots, \sigma(\tau_{k_i-1})$). Vì $\deg(u_i) = d_i$ đồng thời u_i phải được ghép cặp trong σ nên $1 \leq N_i(\sigma, \tau) \leq d_i$ với mọi $\sigma \in \Sigma$. Tiến hành chi tập $\text{supp}X$ thành các tập con $E_{i,j}^{(\tau)}$ sao cho :

$$(\sigma(\tau_1), \dots, \sigma(\tau_{k_i-1})) \in E_{i,j}^{(\tau)} \iff N_i(\sigma, \tau) = j, \text{ với } 1 \leq j \leq d_i$$

Coi $N_i(\sigma, \tau)$ là một biến ngẫu nhiên trên Σ , ta có:

$$\text{Prob}(X \in E_{i,j}^{(\tau)}) = \text{Prob}(N_i(\sigma, \tau) = j)$$

Từ mệnh đề **(C)**, với τ cố định:

$$\begin{aligned} H(\sigma(i) | \sigma(\tau_1), \dots, \sigma(\tau_{k_i-1})) &\leq \sum_{j=1}^{d_i} \text{Prob}(|N_i(\sigma, \tau)| = j) \log_2 j \\ &= \sum_{j=1}^{d_i} \log_2 j \sum_{\sigma \in \Sigma} P(\sigma) \cdot P(N_i(\sigma, \tau) = j | \sigma) \quad (\text{Do } \sigma \in \Sigma \text{ là 1 nhóm đầy đủ}) \\ &= \sum_{j=1}^{d_i} \log_2 j \sum_{\sigma \in \Sigma} \frac{P(N_i(\sigma, \tau) = j | \sigma)}{|\Sigma|} \end{aligned}$$

Kết hợp với ...

$$H(\sigma(1), \dots, \sigma(n)) \leq \sum_{j=1}^{d_i} \log_2 j \left(\frac{1}{n! |\Sigma|} \sum_{\sigma \in \Sigma} \sum_{\tau \in S_n} P(N_i(\sigma, \tau) = j | \sigma) \right) \quad (4)$$

$$\text{Xét } \sum_{\tau \in S_n} P(N_i(\sigma, \tau) = j | \sigma)$$

Với mỗi σ cố định $\in \Sigma$ và trên từng hoán vị $\tau \in S_n$, $N_i(\sigma, \tau)$ nhận các giá trị từ 1 tới d_i với xác suất như nhau là $\frac{1}{d_i}$, vì $N_i(\sigma, \tau)$ chỉ phụ thuộc vào vị trí của $\sigma(i)$ trong hoán vị τ (do σ đã cố định), tương ứng với các đỉnh k thỏa mãn $u_i v_k \in E(G)$ (Nếu $\sigma(i)$ là lân cận gần nhất của i theo thứ tự của hoán vị (giả sử là τ_1). Khi đó $N_i(\sigma, \tau_1) = d_i$ và $P(N_i(\sigma, \tau_1) = d_i | \sigma) = \frac{1}{d_i}$; Nếu $\sigma(i)$ là lân cận gần thứ hai của i theo thứ tự của hoán vị (giả sử τ_2). Khi đó $N_i(\sigma, \tau_2) = d_i - 1$ và $P(N_i(\sigma, \tau_2) = d_i - 1 | \sigma) = \frac{1}{d_i}, \dots$ tương tự với $n!$ hoán vị của S_n . Do đó, giá trị của biểu thức trên bằng:

$$\sum_{\tau \in S_n} P(N_i(\sigma, \tau) = j | \sigma) = n! \cdot \frac{1}{d_i} = \frac{n!}{d_i}$$

Và biểu thức (2) trở thành:

$$\begin{aligned} H(\sigma(1), \sigma(2), \dots, \sigma(n)) &= \sum_{i=1}^n H(\sigma(i) | \sigma(1), \sigma(2), \dots, \sigma(i-1)) \\ &= \sum_{i=1}^n \sum_{j=1}^{d_i} \log_2 j \left(\frac{1}{n! |\Sigma|} \sum_{\sigma \in \Sigma} \frac{n!}{d_i} \right) \\ &= \sum_{i=1}^n \sum_{j=1}^{d_i} \log_2 j \left(\frac{1}{n! |\Sigma|} \cdot |\Sigma| \cdot \frac{n!}{d_i} \right) \\ &= \sum_{i=1}^n \sum_{j=1}^{d_i} \log_2 j \cdot \frac{1}{d_i} = \sum_{i=1}^n \frac{\log_2 d_i!}{d_i} \quad (\text{đpcm}) \end{aligned}$$