ECE 231A Discussion 5

TA: Hengjie Yang

Email: hengjie.yang@ucla.edu

05/01/2020

Fano's inequality and converse to channel coding theorem

Fano's inequality: Let $X \to Y \to \hat{X}$ and $P_e \triangleq \Pr\{\hat{X} \neq X\}$, then

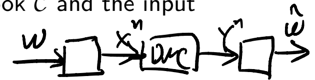
$$H(P_e) + P_e \log(|\mathcal{X}|) \geq H(X|\hat{X}) \geq H(X|Y)$$

≤ 1

$P_e \geq \frac{H(X|\hat{X}) - 1}{\log(|X|)}$

Proof: Define $E = \mathbb{I}_{\{\hat{X} \neq X\}}$. Expand $H(E, X|\hat{X})$ w.r.t. X and E by chain rule.

Fano's inequality on DMC: For a DMC with a codebook $\mathcal{C}$ and the input message W uniformly distributed over 2^{nR}, we have



$$H(W|\hat{W}) \leq 1 + P_e^{(n)} nR.$$

$H(W|\hat{W}) \leq H(P_e) + P_e \log|W|$, $\log|W| = nR$

$P_e = \Pr\{W \neq \hat{W}\}$

$P_e^{(n)} = \frac{1}{2^{nR}} \sum_{i=1}^{2^{nR}} \lambda_i$

Proof of the converse of channel coding theorem: Since $W \to X^n(W) \to Y^n \to \hat{W}$, (M, n) with $\lambda^{(n)} \to 0$

$P_e^{(n)} \to 0$

$\Pr\{W \neq \hat{W}\}$

$$nR = H(W) = H(W|\hat{W}) + I(W;\hat{W}) \quad \text{(Fano's inequality and Markovity)}$$

$$\leq 1 + P_e^{(n)} nR + I(X^n;Y^n) \quad \text{(DMC property)}$$

$$\leq 1 + P_e^{(n)} nR + nC$$

$= \sum \lambda_i \Pr\{W = i\}$

$= \Pr\{W \neq \hat{W}\}$

$P_e^{(n)} = \frac{1}{2^{nR}} \sum \lambda_i$

$= \sum \lambda_i \Pr\{W = i\}$

$I(X^n;Y^n)$

$= \sum H(Y_i|Y^{i-1}) - \sum H(Y_i|Y^{i-1}, X^n)$

$\leq \sum H(Y_i) - \sum H(Y_i|X_i)$

$= \sum I(Y_i;X_i) \leq nC$

$= \Pr\{W \neq \hat{W}\}$

Thus, $R \leq P_e^{(n)} R + \frac{1}{n} + C$. Since the inequality holds for all n and $\lim_{n\to\infty} P_e^{(n)} = 0$, $R \leq C$.

$\to 0$

Proof of Fano's inequality

$X \to Y \to \hat{X}$

$$E = \begin{cases} 1 & X \neq \hat{X} \\ 0 & \text{otherwise} \end{cases}$$

$$H(X, E|\hat{X}) = \underline{H(X|\hat{X})} + \underline{\cancel{H(E|\hat{X}, X)}}^{=0}$$
$$= \underline{H(E|\hat{X})} + \underline{H(X|\hat{X}, E)}$$

$\le H(E)$

$= H(\Pr(X \neq \hat{X}))$

$= H(P_e)$

$=0$

$= \Pr\{E=0\} \underbrace{H(X|\hat{X}, E=0)} +$

$\underbrace{\Pr\{E=1\}}_{P_e} H(\underbrace{X|\hat{X}, E=1})$

Assume $x, \hat{x} \in \mathcal{X}$ $|\mathcal{X}|-1$

$\le \log(|\mathcal{X}|-1)$

$\le \log|\mathcal{X}|$

Example: $X = \{1, 2, 3\}$

$\hat{X} = \{2, 3, 4\}$

$$H(X|\hat{X}) = H(E|\hat{X}) + H(X|\hat{X}, E)$$
$$\le H(P_e) + P_e \log|\mathcal{X}|$$

$$I(X;Y) \ge I(X;\hat{X})$$
$$\cancel{H(X)} - H(X|Y) \ge$$
$$\cancel{H(X)} - H(X|\hat{X})$$
$$H(X|Y) \le H(X|\hat{X})$$

Weak converse and strong converse

Weak converse: for any DMC with capacity C and an (M, n) code with rate $R > C$,

$$P_e^{(n)} \geq \left(1 - \frac{C}{R}\right) - \frac{1}{nR}.$$

Implication: For $R > C$, $P_e^{(n)} > 0$ for all blocklength n.

Strong converse (Wolfowitz, 1957): for any DMC with capacity C and an (M, n) code with rate $R > C$,

$$P_e^{(n)} \geq 1 - \frac{4A}{n(R-C)^2} - \exp\left(-\frac{n(R-C)^2}{2}\right),$$

where $A > 0$ is some constant only dependent on the channel.
Implication: For $R > C$, $P_e^{(n)} \to 1$ as $n \to \infty$.

Continuous random variable and differential entropy

Continuous r.v.: R.v. X is continuous if its CDF $F(x) \triangleq \Pr(X \leq x)$ is continuous. $f(x) = F'(x)$ is the PDF of X. $S \triangleq \{x \in \mathbb{R} : f(x) > 0\}$ is the support set of X.

Differential entropy: for a continuous r.v. X with support set S,

$$h(X) \triangleq -\int_S f(x) \log f(x) \, \mathrm{d}x.$$

if the defining integral exists and is finite.

Remark:

(i) $h(X)$ could be negative, e.g., $h(X) = \log a$ for Unif$[0, a]$, $0 < a < 1$.

(ii) If $X \sim \mathcal{N}(0, \sigma^2)$, $h(X) = \frac{1}{2} \log 2\pi e \sigma^2$ bits.

Derivation of $h(X)$ for $X \sim N(0, \sigma^2)$

$$f(x) = \frac{1}{\sqrt{2\pi}\,\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right)$$

$$h(f) = -\int \underbrace{f \left[-\frac{x^2}{2\sigma^2}\right.}_{} \left. - \frac{1}{2}\ln 2\pi\sigma^2 \right]$$

$$= \frac{1}{2} \cdot \cancel{\frac{1}{\sigma^2} E}[X^2] + \frac{1}{2}\ln 2\pi\sigma^2$$

$$= \frac{1}{2}\ln(2\pi e \sigma^2) \quad \text{nats}$$

Joint differential entropy:

$$h(X_1, \ldots, X_n) \triangleq -\int f(x^n) \log f(x^n)\, \mathrm{d}x^n.$$

Conditional differential entropy:

$f(y)f(x|y)$ (or $f(x)f(y|x)$)

$$h(X|Y) \triangleq -\int f(x, y) \log f(x|y)\, \mathrm{d}x\, \mathrm{d}y.$$

Entropy of multivariate normal distribution: Let $X_1, \ldots, X_n \sim \mathcal{N}_n(\mu, K)$.

$$h(X_1, \ldots, X_n) = \frac{1}{2} \log(2\pi e)^n |K|.$$

Relative entropy: for two densities f and g,

$$D(f\|g) \triangleq \int f \log \frac{f}{g}.$$

Mutual information: $I(X;Y) \triangleq D(f(x,y)\|f(x)f(y))$.

Derivation of $h(X_1 \cdots X_n)$ for multivariate normal

$$\underline{X} \triangleq \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix} \qquad \underline{\mu} = \begin{bmatrix} \mathbb{E}[X_1] \\ \vdots \\ \mathbb{E}[X_n] \end{bmatrix} = \begin{bmatrix} \mu_1 \\ \vdots \\ \mu_n \end{bmatrix} \qquad \underline{\underline{K}} = \mathbb{E}[(\underline{X}-\underline{\mu})(\underline{X}-\underline{\mu})^T]$$

$$f(\underline{x}) = \frac{1}{(\sqrt{2\pi})^n |K|^{1/2}} \exp\left(-\frac{1}{2}(\underline{x}-\underline{\mu})^T K^{-1}(\underline{x}-\underline{\mu})\right)$$

$$h(X_1 \cdots X_n) = -\int f(x)\left[\underbrace{-\frac{1}{2}(\underline{x}-\underline{\mu})^T K^{-1}(\underline{x}-\underline{\mu})}_{\text{scalar}} - \frac{1}{2}\ln(2\pi)^n|K|\right]$$

$$= \frac{1}{2}\mathbb{E}[(\underline{X}-\underline{\mu})^T K^{-1}(\underline{X}-\underline{\mu})] + \frac{1}{2}\ln(2\pi)^n|K|$$

$\mathrm{trace}(AB) = \mathrm{trace}(BA)$

$$= \frac{1}{2}\mathbb{E}[\mathrm{trace}((\underline{X}-\underline{\mu})^T K^{-1}(\underline{X}-\underline{\mu}))] + \frac{1}{2}\ln(2\pi)^n|K|$$

$$= \frac{1}{2}\mathbb{E}[\mathrm{trace}(K^{-1}(\underline{X}-\underline{\mu})(\underline{X}-\underline{\mu})^T)] + \frac{1}{2}\ln(2\pi)^n|K|$$

$$= \frac{1}{2}\mathrm{trace}(K^{-1}\underbrace{\mathbb{E}[(\underline{X}-\underline{\mu})(\underline{X}-\underline{\mu})^T]}_{K}) + \cdots$$

$$= \frac{n}{2} + \frac{1}{2}\ln(2\pi)^n|K| = \frac{1}{2}\ln(2\pi e)^n|K|$$

Properties of differential entropy, relative entropy and mutual information

Theorem: $D(f\|g) \geq 0$ with equality iff $f = g$ almost everywhere (a.e.).

Corollary:

(i) $I(X;Y) \geq 0$ with equality iff X and Y are independent.

(ii) $h(X) \geq h(X|Y)$ with equality iff X and Y are independent.

Chain rule: $h(X_1,\ldots,X_n) = \sum_{i=1}^{n} h(X_i|X_1,\ldots,X_{i-1}) \leq \sum_{i=1}^{n} h(X_i)$.

Corollary (Hadamard's inequality): for any cov. matrix K, $|K| \leq \prod_{i=1}^{n} K_{ii}$.

$X_1 \cdots X_n \quad h(X_1 \cdots X_n) = \frac{1}{2} h (2\pi e)^n |K|$

$h(X_i) = \frac{1}{2} h (2\pi e) K_{ii}$

Theorem:

$$\begin{aligned} h(X+c) &= h(X) \\ h(aX) &= h(X) + \log|a| \\ h(A\boldsymbol{X}) &= h(\boldsymbol{X}) + \log|\det(A)| \quad (A \in \mathbb{R}^{n\times n}, \boldsymbol{X} \in \mathbb{R}^n,) \end{aligned}$$

Exercise 1: mutual information of Gaussian r.v.'s (easy)

Let $(X,Y) \sim \mathcal{N}(\underset{\text{a zero vector}}{0}, K)$ where $\rho = \frac{\operatorname{cov}(X,Y)}{\sigma_X \sigma_Y} \in [-1,1]$ is some constant and

$$K = \begin{bmatrix} \mathbb{E}[X^2] & \mathbb{E}[XY] \\ \mathbb{E}[XY] & \mathbb{E}[Y^2] \end{bmatrix} \qquad K = \begin{bmatrix} \sigma^2 & \rho\sigma^2 \\ \rho\sigma^2 & \sigma^2. \end{bmatrix}$$

$$\underline{\mu} = \begin{bmatrix} \mathbb{E}[X] \\ \mathbb{E}[Y] \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$|K| = \sigma^4 - \sigma^4\rho^2 = \sigma^4(1-\rho^2)$$

Find $I(X;Y)$.

$$H(Y) - \underline{H(Y|X)}$$

$$= H(X) + H(Y) - H(X,Y)$$

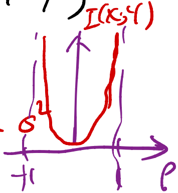
differential entropy

$$H(X) = \frac{1}{2}\log(2\pi e)\sigma^2$$

$$H(Y) \;\,\text{''}$$

$$\underline{H(X,Y)} = \frac{1}{2}\log(2\pi e)^2|K| = \frac{1}{2}\log(2\pi e)^2\sigma^4(1-\rho^2)$$

$\operatorname{cov}(X) = \mathbb{E}[X^2] = \sigma^2$



$$I(X;Y) = \frac{1}{2}\log(2\pi e)\sigma^2 + \frac{1}{2}\log(2\pi e)\sigma^2 - \frac{1}{2}\log(2\pi e)^2\sigma^4(1-\rho^2)$$

$$= -\frac{1}{2}\log(1-\rho^2)$$

if $\rho = 0$ $\quad I(X;Y) = 0$

if $\rho = \pm 1$ $\quad I(X;Y) = \infty$

Exercise 2: mutual information of Gaussian r.v.'s (advanced)

Let (X, Y, Z) be jointly Gaussian and that $X \to Y \to Z$ forms a Markov chain. Let X and Y have correlation coefficient ρ_1. Let Y and Z have correlation coefficient ρ_2. Find $I(X; Z)$.

Hint: For multivariate Gaussian, $\mathbb{E}[X|Y = y] = \frac{\operatorname{cov}(X,Y)y}{\mathbb{E}[Y^2]}$; Tower property: $\mathbb{E}[XZ] = \mathbb{E}_{p(y)}[\mathbb{E}_{p(xz|y)}[XZ|Y]]$.

$$= \int_{xz} f(x,y,z)\, xz$$

$$= \int_{xz} f(y) f(x,z|y)\, xz$$

$$= \int_y f(y) \left[\int_{xz} f(x,z|y)\, xz \right]$$

$$= \int_y f(y)\, \mathbb{E}[XZ | Y = y]$$

$$= \mathbb{E}[XZ]$$

$$\Lambda = \begin{bmatrix} \sigma_x^2 & \rho_{xz}\sigma_x\sigma_z \\ \rho_{xz}\sigma_x\sigma_z & \sigma_z^2 \end{bmatrix}$$

$$\rho_{xz} = \frac{\operatorname{cov}(x,z)}{\sigma_x\sigma_z}$$

$$= \frac{\mathbb{E}[XZ]}{\sigma_x\sigma_z}$$

$$= \frac{\mathbb{E}[\mathbb{E}[XZ|Y]]}{\sigma_x\sigma_z}$$

$$= \frac{\mathbb{E}[\mathbb{E}[X|Y]\,\mathbb{E}[Z|Y]]}{\sigma_x\sigma_z}$$

$$= \frac{\mathbb{E}\left(\frac{\cancel{\sigma_x}\rho_{xy}}{\sigma_y} Y\right)\left(\frac{\cancel{\sigma_z}\rho_{zy}}{\sigma_y} Y\right)}{\cancel{\sigma_x}\cancel{\sigma_z}}$$

$$= \frac{\mathbb{E}[\cancel{Y^2}]\,\rho_{xy}\,\rho_{zy}}{\sigma_{\cancel{Y}}^{2}}$$

$$= \rho_{xy}\,\rho_{zy}$$

$$= \rho_1\,\rho_2$$

$$I(X;Z) = -\frac{1}{2}\log\left(1 - \rho_1^2\rho_2^2\right)$$