$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log p(x).$$

$$E_p g(X) = \sum_{x \in \mathcal{X}} g(x) p(x),$$

$$g(X) = \log \frac{1}{p(X)}.$$

$$H(X) = E_p \log \frac{1}{p(X)}.$$

MINH

H(x)=-Elosp(x) 3

LLELLY

Et Zp(x) Elittle

이번 된지로 H(Y|X) 를 구하면

H(YK) = -E105P(Y|X) 0 12=1

3, H(Y|X) = - 2p(x) 2 p(Y|X) los p(Y|X)

H(Y|X=x)

H(Y|X) = -2P(x)H(Y|X=x)

H(XIX) = -E/DP(XIX) Chain Rule 30% = - EP(XIY) {P(Y) / P(XIX) H(X, Y) = H(X) + H(Y|X).= = {P(Y) 2 p(X|Y) /3 p(X|Y) $H(X,Y) = -E \log P(X,Y)$ =- & 1/4) H (X1 X=A) 0(E4 P(Z|Y) = P(X,Y) 0) 5/ E= 2, P/x) 2, P(4) 6/23 H(X,Y)= - 2 p(x) & p(Y) /05 p(X) p(X(Y) $= -\left(\frac{2}{2}P(x)\left(\frac{2}{3}P(y)\right)/_{6y}P(x) + \frac{2}{2}P(x)\frac{2}{3}P(y)/_{6y}P(x)\right)$ = - ({ p(x) / p(x) + (-{ 2p(x) H(x) }) --(-HK)-HKIY)= H(X) +H(X1Y)

Introduction to Computer Science & Engineering

Lecture 11: A Few Basics of Information Systems

Jeonghun Park

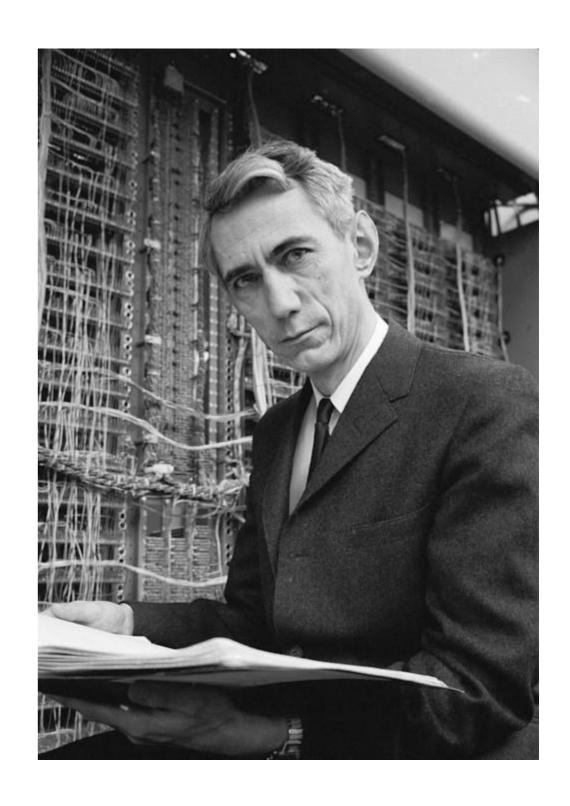


Introduction

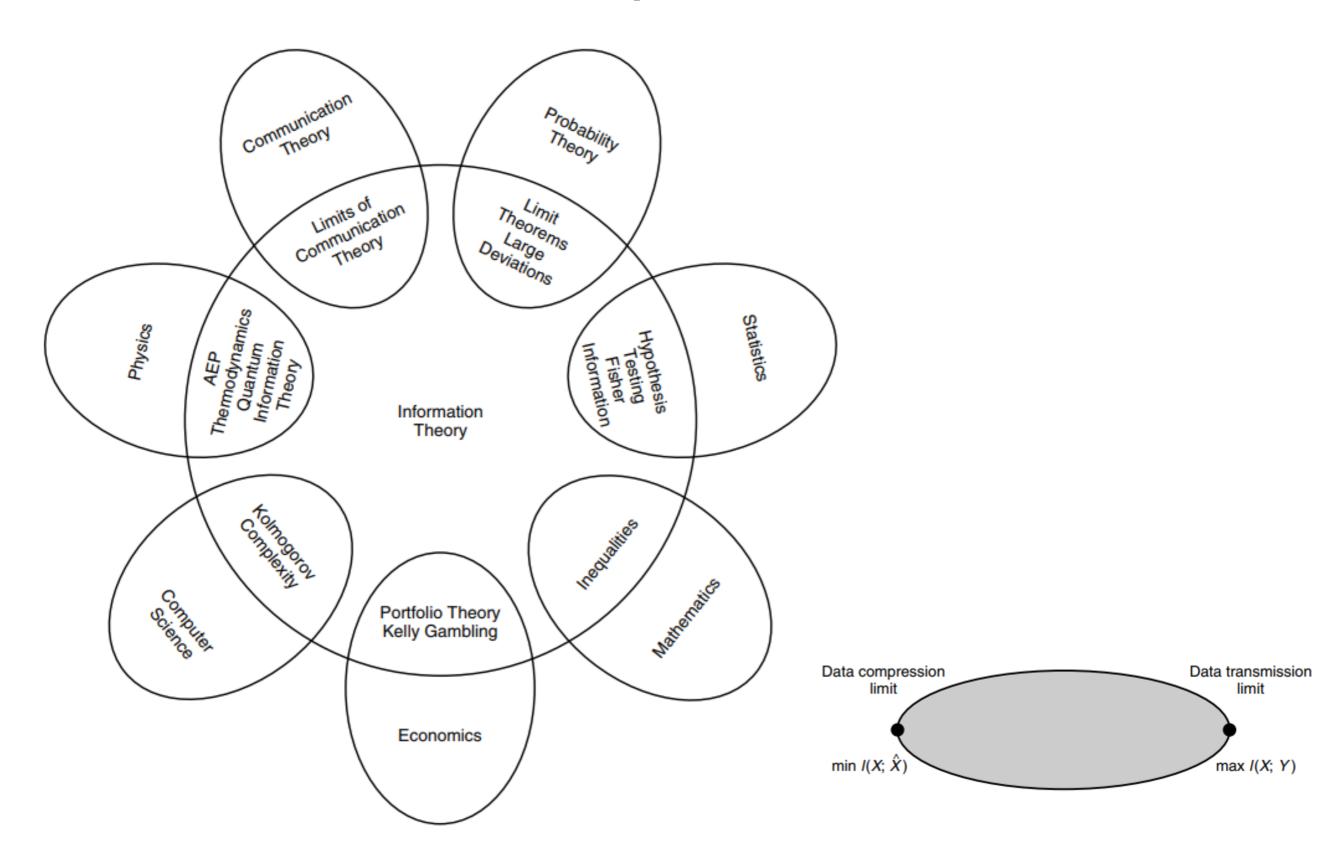
- What is information theory?
 - Define and play with the information measure
 - Mathematical answers for two fundamental questions:
 - What is the ultimate data compression?
 - What is the ultimate transmission rate of communication?
 - Beyond this, it has significant contributions to make in statistical physics, computer science, statistical inference, and probability and statistics etc..

History

- Originated from one genius
 - Claude Shannon (1916.4.30 ~ 2001.2.24)
 - ► Ph.D. from MIT
 - The author of
 - A Mathematical Theory of Communications
 - The farther of digital comm.
 - Stock master
 - Isaac Newton
 - Warren Buffett



Impact



Entropy (吳根)

- Measure of the fundamental uncertainty of randomness
- Let X be a discrete random variable 了 = 46(支持
- $p(x) = \mathbb{P}[X = \widetilde{x}]$ Random Wiable
- Then the entropy is

$$H(X) = -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x)$$

$$H(X, Y) = -E \log p(X, Y).$$

More on Entropy

화물보 아다면 구설수 있습. Binary tree 커럽 동영한 method 를 뜨게이닝

- The units of the entropy is "bits"
- Some properties
- Let X = 1 with probability p $X = 0 \quad \text{with} \quad (-p)$
 - ▶ Then we have $H(X) = -p \log_2 p (1-p) \log_2 (1-p)$

$$H(x) = -\mathcal{E}_{x \in \mathcal{X}} P(x) |_{y \geq p(x)}$$

$$= -P(0)|_{\partial y_2}P(0) - P(1)|_{\partial y_2}P(1)$$

$$= -(1-P)|_{\partial y_2}(1-P) - P|_{\partial y_2}P(1)$$

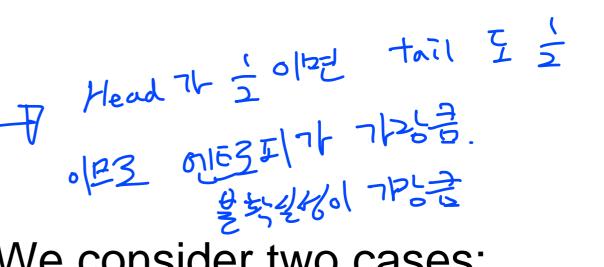


So, What is Entropy?

 It presents the fundamental uncertainty of the 24 E/O) EUS 95/268 LIEIUS randomness

Coin toss example



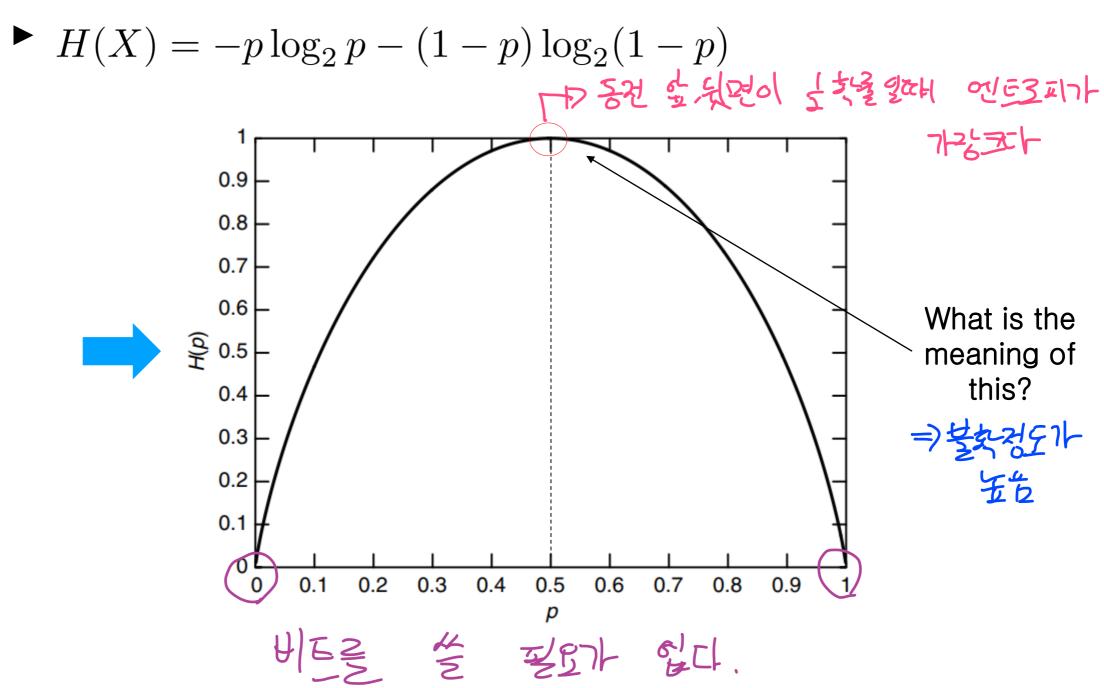


- We consider two cases:
- Head with probability ½
 - Head with probability 0

Which case is more uncertain? 0123 Head It o objet tott 1 F37 tail OEZ LA ZIANT ESECT

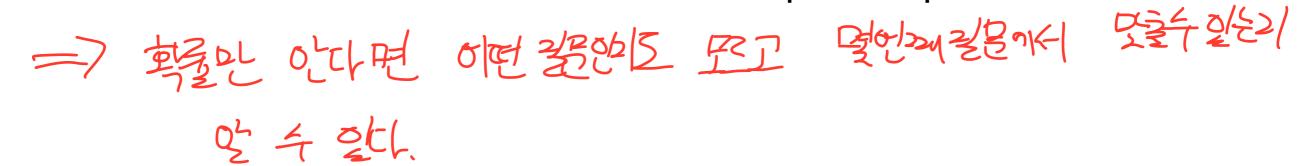
Entropy of Coin Toss

• Remember?

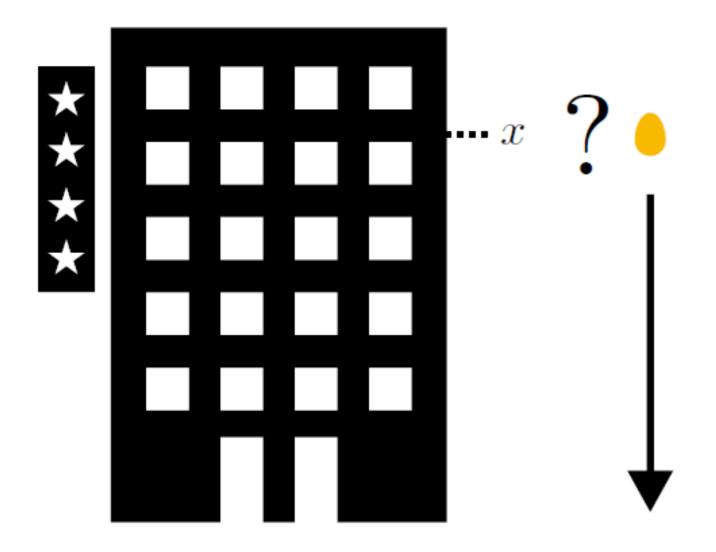


Twenty-Questions Interpretations

- Entropy can be interpreted as follows:
 - The minimum number of the questions to eliminate the randomness
 - ▶ Think about 스무고개
- One important (and surprising) fact:
 - We don't have to know about the specific questions!



Egg Drop Rerevisit



This time, think this in a probabilistic way!

- $X \sim \mathcal{U}(1, N)$
- Then what is the fundamental uncertainty?

Compute Entropy (Randomless 1971)

인숙 스투고에이서 $P[X=X]= \sqrt{\forall x \in [I,N]}$ 일대 $P(x) = \sqrt{\cdot 3}$ 수고

$$\bullet \left[\mathbb{P}[X=x] = \frac{1}{N}\right] \forall x \in [1,N]$$

$$H(X) = -\frac{1}{N}\log_2(\frac{1}{N}) - \frac{1}{N}\log_2(\frac{1}{N}) - \ldots - \frac{1}{N}\log_2(\frac{1}{N})$$

$$F((X) = -\log_2 \frac{1}{N} = \log_2 N$$

•
$$H(X) = -\log_2(N^{-1}) = \log_2(N)$$

* Binary Search 6141 $\frac{N}{2^n} \leq 1$ $\frac{2}{3}$

Entropy 们们是 整三 子哲、

Compare the complexity of our binary search method

= The fundamental number of the questions to eliminate the randomness

n = loy2/ & = 10/2/82

H(X)가 크다는건, 불학정성이 된다는것이다.

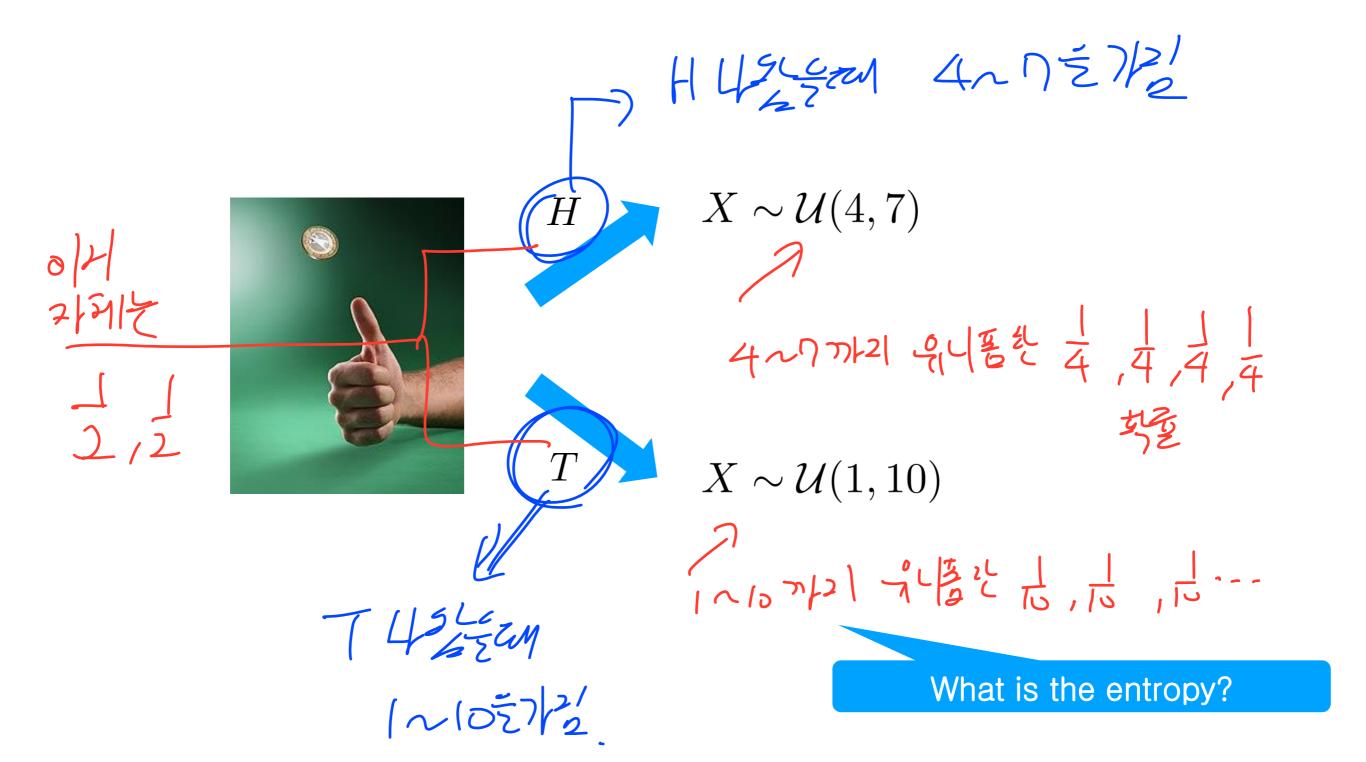
$$X_1 = 1, 2, 3$$
 $P(X_1) = \frac{1}{3}, \frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$
 $\frac{1}{3}$

One Surprise

- In entropy computation, we did not use any specific egg drop method
- Try to understand what this means:
 - Without any specific question, we can calculate the fundamental limit of the number of questions to find an answer



Conditional Coin Toss



Joint and Conditional Entropy

Only one Conditional Entropy $H(X) = - E_X P(X) I_{00} P(X)$

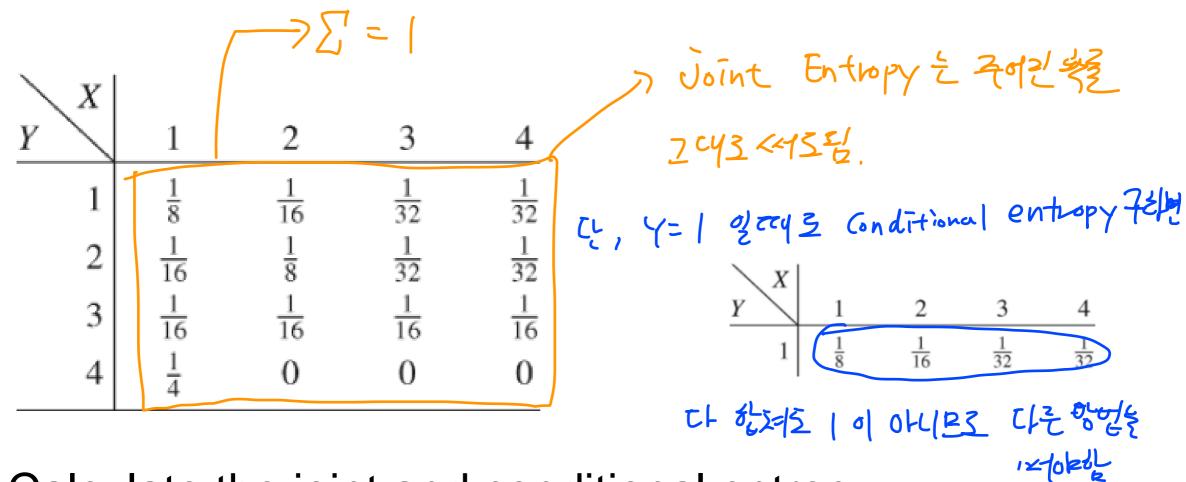
- Let Y = coin.
- The joint entropy is

$$H(X,Y) = -\sum_{x} \sum_{y} p(x,y) \log_2 p(x,y)$$

- The conditional entropy is বুলুকুল।
 - $ightharpoonup H(X|Y = H) = -\sum_{x} p(x|Y = H) \log_2 p(x|Y = H)$
- $\longrightarrow H(X|Y) = \mathbb{P}[Y=H]H(X|Y=H) + \mathbb{P}[Y=T]H(X|Y=T)$

Joint and Conditional Entropy

Consider the following joint distribution:



- Calculate the joint and conditional entropy
 - Understand the marginal distribution

3 H(X,Y)

$$H(Y) = -\frac{2}{y}P(y) \cdot \frac{1}{9}P(y) = \frac{2}{4} + \frac{2}{4} + \frac{2}{4} + \frac{2}{4} + \frac{2}{4} = 2$$

$$H(x) = -\frac{2}{y}P(x) \cdot \frac{1}{9}P(x) = \frac{1}{2} + \frac{2}{4} + \frac{2}{3} + \frac{2}{3} = \frac{7}{4}$$

$$\frac{1}{4}XH(\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{8})=\frac{1}{4}(\frac{1}{3}+\frac{1}{2}+\frac{3}{8}+\frac{3}{8})=\frac{1}{4}\cdot\frac{1}{4}$$

$$\frac{1}{4}H(1,0,0,0) = \frac{1}{4}(0tototo) = 0$$

$$= \frac{1}{4} \left(\frac{n}{4} + \frac{n}{4} + 2 \right) = \frac{1}{8}$$

H,т ЧЕ КЕН Math Fun: Complicated Coin Toss

- A fair coin is flipped until the first head occurs. We are interested in X, the number of toss required.
 - ► Find the entropy

$$H(X) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{4} \log_2 \frac{1}{4} - \frac{1}{8} \log_2 \frac{1}{8} - \dots - \frac{1}{2^{N}} \log_2 \frac{1}{2^{N}}$$

$$= +\frac{1}{4} \log_2 2 + \frac{1}{4} \log_2 2^2 + \frac{1}{8} \log_2 3 + \dots + \frac{1}{2^{N}} \log_2 N$$

$$= \frac{1}{2} + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \dots + \frac{1}{2^{N}} N$$

$$= \sum_{n=1}^{\infty} 2^{-n} \cdot n$$

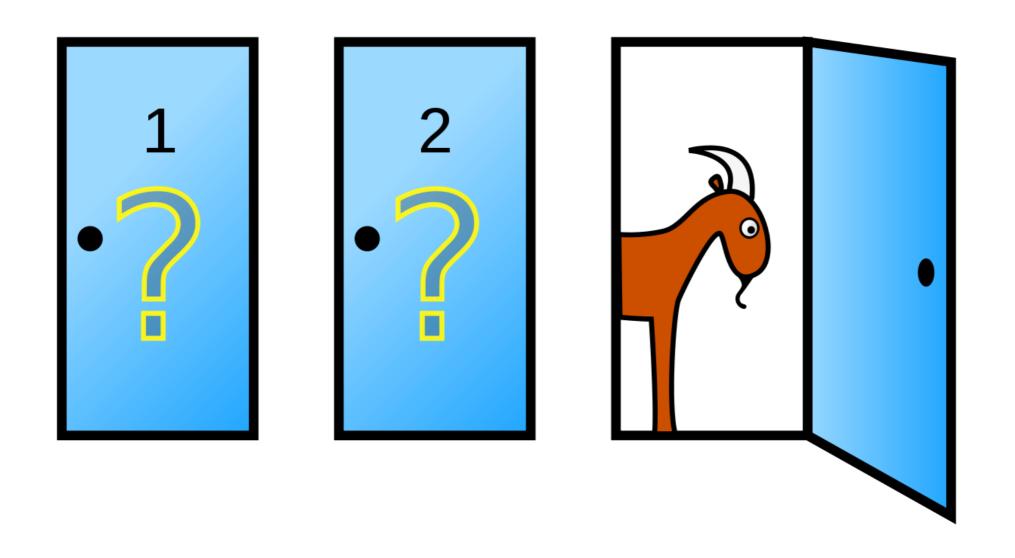
$$= \sum_{n=1}^{\infty} 2^{-n} \cdot n$$

$$S = r + 2r^{2} + 3r^{3} + \dots + nr^{n}$$

$$rS = r^{2} + 2r^{3} + 3r^{4} + \dots + nr^{n+1}$$

$$S(1-r) = r + r^{2} + r^{3} + \dots + r^{n} - nr^{n+1}$$

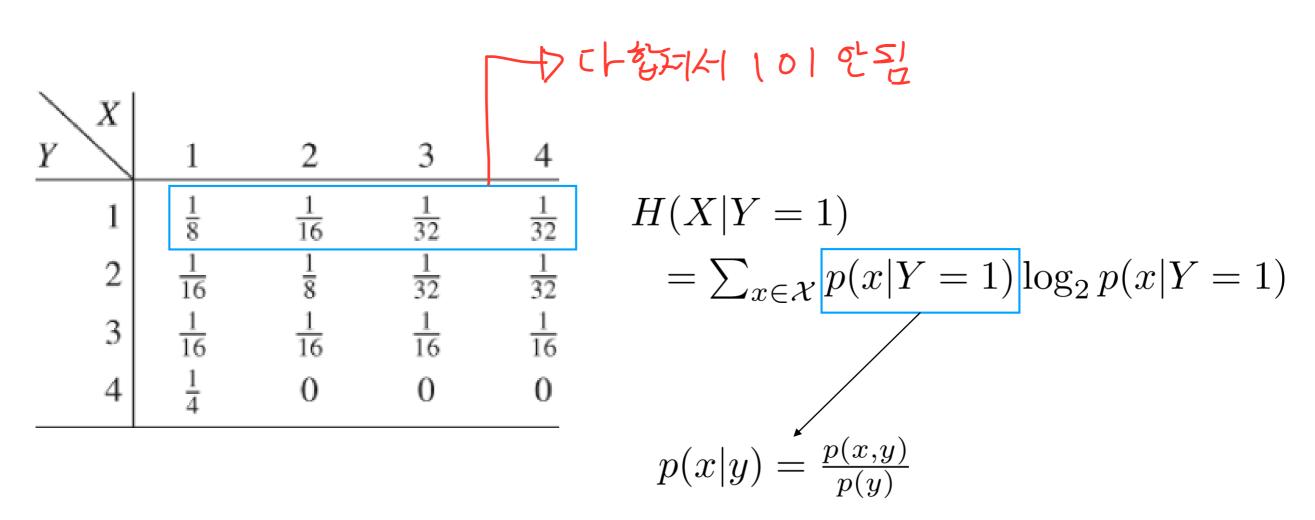
Math Fun: Monty-Hall Problem



Math Fun: Monty-Hall Problem

- Can we use information theory to analyze this problem?
- We can interpret that $H(X) \ge H(X|Y)$
 - Where the equality holds iff Y is independent to X

Conditional Entropy and Computer Science and Engineering Marginal Distribution



- Then what is p(Y=1) ?
- This is called "marginal distribution," and this can be obtained as:

$$p(Y = 1) = \sum_{x \in \mathcal{X}} p(Y = 1, x)$$
$$= \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{32} = \frac{1}{4}$$



Chain Rule

• The following chain rule is satisfied:

$$H(X,Y) = H(X) + \mathbf{R}(Y|X) \qquad \qquad P(Y|X) = \frac{P(Y,Y)}{P(X)}$$
Proof:
$$H(X,Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log_2 p(x,y) \implies \text{voint Entropy}$$

$$= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log_2 p(x) p(y|x)$$

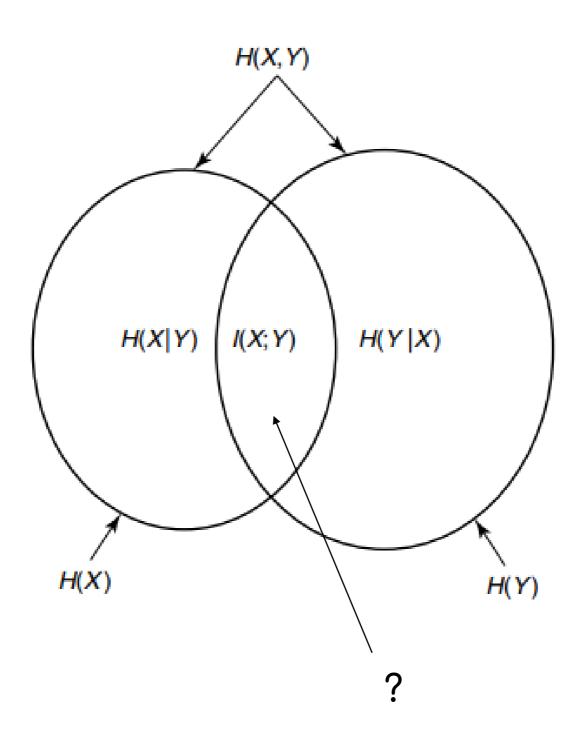
$$= -\sum_{x \in \mathcal{X}} p(x) \log_2 p(x) - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log_2 p(y|x)$$

$$\frac{P(Y|X) = \frac{P(Y,Y)}{P(X)} = \frac{P(Y,Y)}{P(X)}$$

$$= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log_2 p(y|x)$$

$$\frac{P(Y|X) = \frac{P(Y,Y)}{P(X)} = \frac{P(Y,Y)}{P(X)}$$

Intuitive Description



Relations of Multiple Randomness

- Entropy
 - Measure of the *uncertainty* of the randomness
 - Measure of the amount of information required on the average to describe the random variable
- Now we focus on some relationships of two randomness

The relative entropy is a measure of the distance between two distributions. In statistics, it arises as an expected logarithm of the likelihood ratio. The relative entropy D(p||q) is a measure of the inefficiency of assuming that the distribution is q when the true distribution is p. For example, if we knew the true distribution p of the random variable, we could construct a code with average description length H(p). If, instead, we used the code for a distribution q, we would need H(p) + D(p||q) bits on the average to describe the random variable.

Definition The relative entropy or Kullback–Leibler distance between two probability mass functions p(x) and q(x) is defined as

$$D(p||q) = \sum_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)}$$
 (2.26)

$$= E_p \log \frac{p(X)}{q(X)}. \tag{2.27}$$

Relative Entropy

- Measure of distance between two distributions
 - ▶ Denote as D(p||q)
- It can be interpreted as:
 - ► The amount of inefficiency of assuming that the distribution is q when the true distribution is p
 - For example, assume that we use the distribution q, while the true distribution is p
 - ▶ Then the code length is H(p) + D(p||q)
 - ► (Think our example)

Relative Entropy

- The relative entropy (or denoted as *Kullback-Leibler distance*) between two probabilities p(x) and q(x) is defined as
 - $D(p||q) = \sum_{x \in \mathcal{X}} p(x) \log_2 \frac{p(x)}{q(x)} \eta = \frac{p(z)}{q(x)}$
- If it is a distance, the following should be satisfied:

$$ightharpoonup D(p||q) = D(q||p)$$
 $ightharpoonup False$

P, 0 = 72223

Is this true?

measure of space

$$I(X;Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}$$
$$= D(p(x,y)||p(x)p(y))$$
$$= E_{p(x,y)} \log \frac{p(X,Y)}{p(X)p(Y)}.$$

Example 2.3.1 Let $\mathcal{X} = \{0, 1\}$ and consider two distributions p and q on \mathcal{X} . Let p(0) = 1 - r, p(1) = r, and let q(0) = 1 - s, q(1) = s. Then

$$D(p||q) = (1-r)\log\frac{1-r}{1-s} + r\log\frac{r}{s}$$
 (2.31)

and

$$D(q||p) = (1-s)\log\frac{1-s}{1-r} + s\log\frac{s}{r}.$$
 (2.32)

If r = s, then D(p||q) = D(q||p) = 0. If $r = \frac{1}{2}$, $s = \frac{1}{4}$, we can calculate

$$D(p||q) = \frac{1}{2}\log\frac{\frac{1}{2}}{\frac{3}{4}} + \frac{1}{2}\log\frac{\frac{1}{2}}{\frac{1}{4}} = 1 - \frac{1}{2}\log 3 = 0.2075 \text{ bit},$$
 (2.33)

whereas

$$D(q||p) = \frac{3}{4}\log\frac{\frac{3}{4}}{\frac{1}{2}} + \frac{1}{4}\log\frac{\frac{1}{4}}{\frac{1}{2}} = \frac{3}{4}\log 3 - 1 = 0.1887 \text{ bit.}$$
 (2.34)

Note that $D(p||q) \neq D(q||p)$ in general.

$$P(P114) = P(0) / 65 \frac{P(0)}{4(0)} + P(1) / 65 \frac{P(D)}{9(1)}$$

4- -

Mutual Information

The mutual information is defined as follows:

$$I(X;Y) = \sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} = D(p(x,y)||p(x)p(y))$$

$$= \sum_{x,y} p(x,y) \log_2 \frac{p(x|y)}{p(x)}$$

$$= \sum_{x,y} p(x,y) \log_2 p(x) + \sum_{x,y} p(x,y) \log_2 p(x|y)$$

$$= H(X) - H(X|Y)$$

By symmetry, we also have

$$I(X;Y) = I(Y;X) = H(Y) - H(Y|X)$$



$$I(X;Y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} \qquad p(\chi|Y) = \frac{p(\chi,y)}{p(\chi,y)}$$

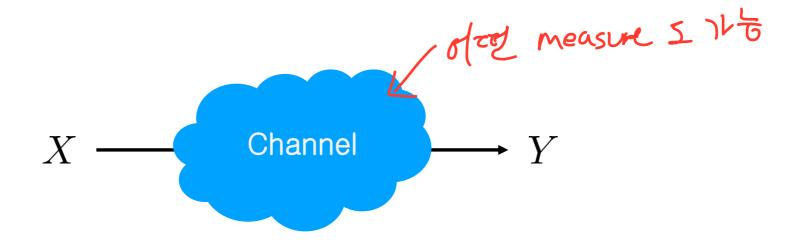
$$I(X)Y) = \frac{2}{xy}P(x,y)/oy \frac{P(x|Y)}{P(x)}$$

$$z - H(X|Y) + P(X)$$

Mutual Information

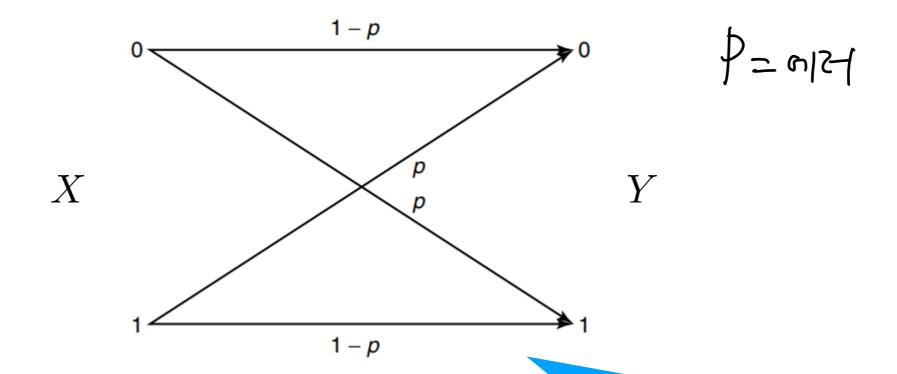
Fundamental of communications





- X is random, and Y is also random
 - They are not same (because of the channel), but "related" each other
 - How to define the maximum information amount that can be successfully delivered through the channel?

Toy Example



Binary symmetric channel

$$I(X;Y) = H(Y) - H(Y|X)$$

$$= H(Y) - \sum p(x)H(Y|X = x)$$

$$= H(Y) - H(p)$$

$$\leq 1 - H(p)$$

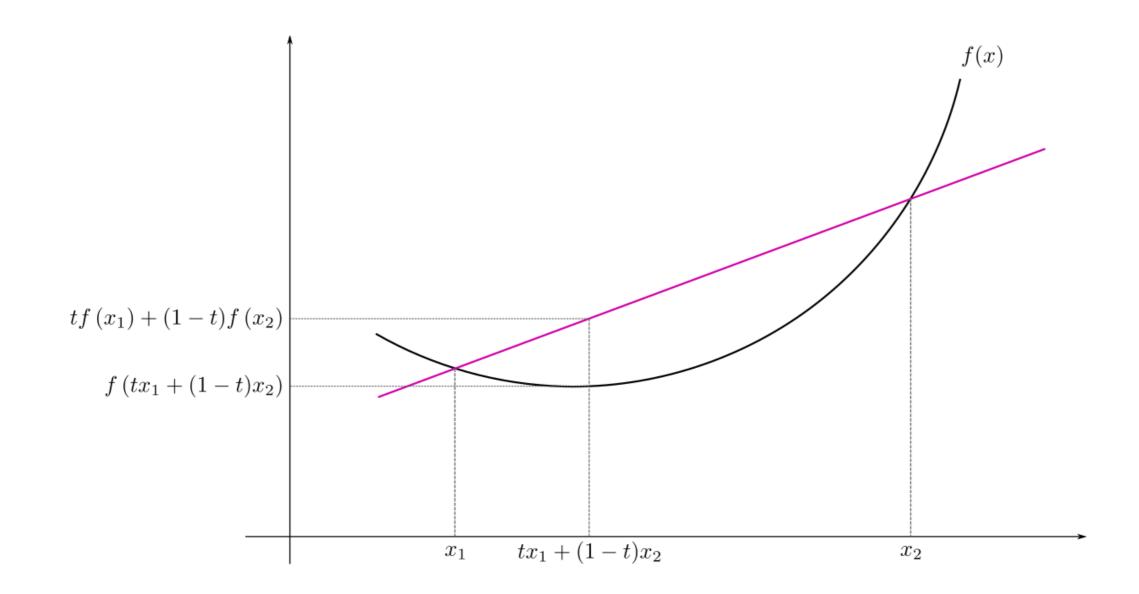
Maximum information rate = Channel capacity



Math Fun

Jensen's inequality

是生活 0 例外是年发儿。



Jensen's Inequality 對例如此 进 ①Convex 实义 Convex

• If f is a convex function and X is a random variable, then $\mathbb{E}[f(X)] \geq f(\mathbb{E}[X])$

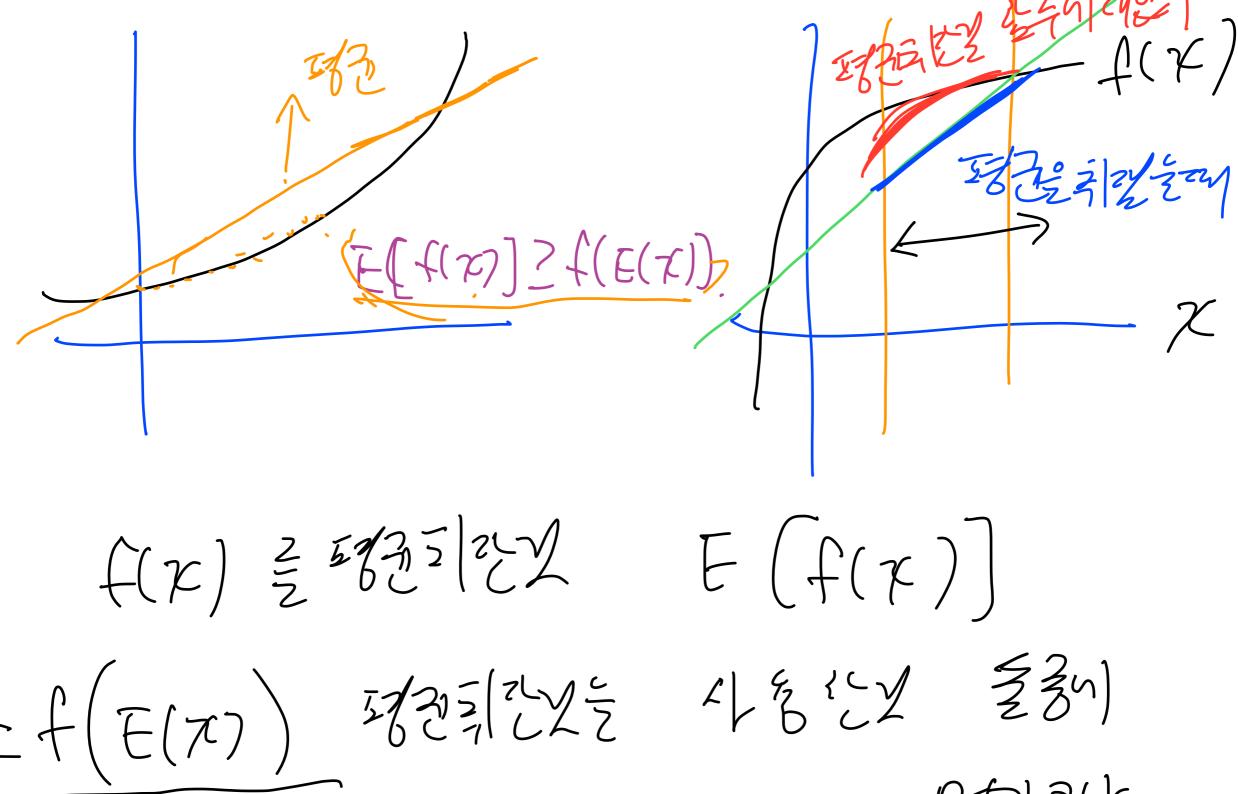
• Then we naturally have $I(X;Y) \ge 0$

Information amount is non-negative

• This leads to $H(X|Y) \leq H(X)$

Information cannot hurt





21/21/2

Proof

• The mutual information can be written as $\log |x| > \log |x|$ $\mathbb{E}[f(X)] \ge f(\mathbb{E}[X])$

$$I(X;Y) = D(p(x,y)||p(x)p(y))$$
$$= \mathbb{E}[\log_2 \frac{p(X,Y)}{p(X)p(Y)}]$$

 $=\log_2 1$

$$\mathbb{E}(f(X)] \ge f(\mathbb{E}[X])$$

$$\circ (\mathbb{E}[X])$$

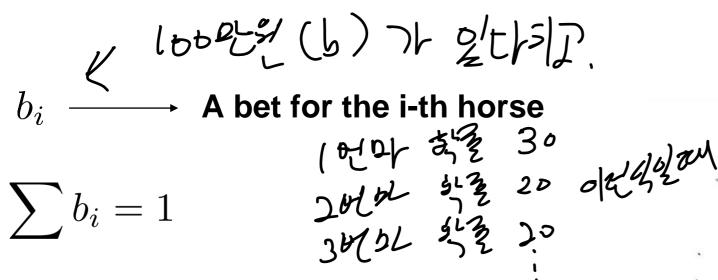
$$\vdash (\omega_2 | P(Y) | Z | \log_2 EP(Y))$$

• This also can be $-\frac{2}{y} \rho(y)$ $-D(p||q) = \underbrace{\sum_{x} \log_2 \frac{p(x)}{q(x)}}_{x} = \underbrace{\mathbb{E}[\log_2 \frac{q(x)}{p(x)}]}_{x}$ $\leq \log_2 \mathbb{E}[\frac{q(x)}{p(x)}]$ $= \log_2 \sum_{x} p(x) \frac{q(x)}{p(x)}$



Gambling and Information Theory

The world's best gambler is playing the horse race

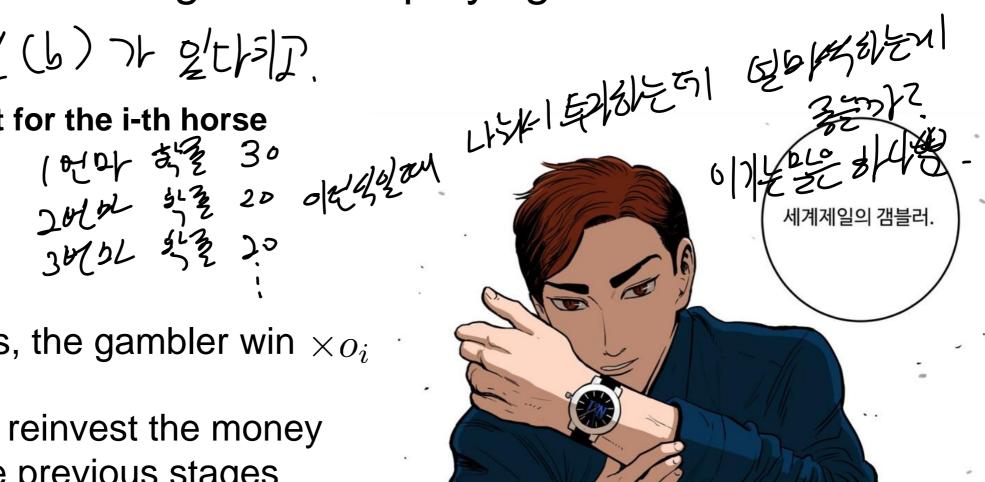


If the horse i wins, the gambler win \times_{O_i}

The gambler can reinvest the money that earned in the previous stages

Since the gambler can reinvest his money, his wealth is the product of the gains for each race $S_n = \prod S(X_i)$

$$S_n = \prod_{i=1}^n S(X_i)$$





b= [b1, b2, b3, ..., bk] 100022 12/2/26 kny=1 20) 0/ch 2/24. bi 은 1번말기 두가하는 금액 (Oi) 岛是 工學可知是 音叫 (02) LKE KYME (0492 OK 2/5/24) 이글이 LIPA CL 기고 LK 925세달이 이긴다던? (1000 22 X bk X Ok) 를 현게될 7 다음 216 도에서 이 돈3 투가에서 b, 42에 학이 이 2012 2 Cto 2125 Em4-1 62 822M 1501 0/21016 (1000 % X br X5k) X 61 X01) X bz-Oz

Gambling and Information Theory

• The wealth relatives S(X) = b(X)o(X) is the factor $\frac{2\pi}{2}$ by which the gambler's wealth grows if horse X

wins the race

• The doubling rate of a horse race is

$$\frac{1}{n}\log S_n = \frac{1}{n}\sum_{i=1}^{n}\log S(X_i) \to \mathbb{E}[\log S(X_i)] \quad \therefore S_n = 2^{\frac{nW(\mathbf{b}, \mathbf{p})}{n}}$$

Theory

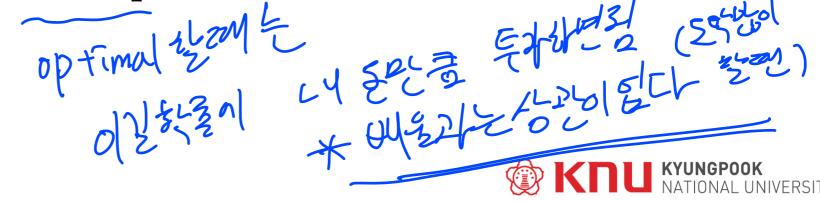
The optimum doubling rate

$$W^{\star}(\mathbf{p}) = \max_{\mathbf{b}} W(\mathbf{b}, \mathbf{p}) = \max_{\sum b_i = 1}^{K} p_i \log b_i o_i$$

Solving the above problem, we have >

$$W^{\star}(\mathbf{p}) = \sum p_i \log o_i \left(-H(\mathbf{p}) \right) \mathcal{C}_{\mathbf{p}} \mathcal{C}_{\mathbf{p}}$$

• The above is achievable by the proportional gambling scheme $\mathbf{b}^* = \mathbf{p}$



Proof

Another case

 If we allow that the gambler the option of retaining some of his wealth as case, the solution becomes different

Side Information

Consider two doubling rate:

$$W(X) = \max \sum p(x) \log b(x) o(x)$$

$$W(X|Y) = \max \sum p(x,y) \log b(x|y) o(x)$$

$$\Delta W = W(X|Y) - W(X)$$

The side information is helpful?



Side Information

 $W(X) = \frac{2 p(x)}{p(x)} \log \frac{L(x)}{p(x)} \cdot p(x) \sigma(x)$

-I(X,Y)

• We have:

$$\Delta W = I(X;Y) = \frac{1}{2} \frac{1}{$$

• When is the side information helpful?

Theorem 6.2.1 The increase ΔW in doubling rate due to side information Y for a horse race X is

$$\Delta W = I(X;Y). \tag{6.25}$$

Proof: With side information, the maximum value of $W^*(X|Y)$ with side information Y is achieved by conditionally proportional gambling [i.e., $b^*(x|y) = p(x|y)$]. Thus,

$$W^{*}(X|Y) = \max_{\mathbf{b}(x|y)} E[\log S] = \max_{\mathbf{b}(x|y)} \sum p(x,y) \log o(x) b(x|y)$$
 (6.26)

$$= \sum p(x, y) \log o(x) p(x|y)$$
 (6.27)

$$= \sum p(x) \log o(x) - H(X|Y).$$
 (6.28)

Without side information, the optimal doubling rate is

$$W^*(X) = \sum p(x) \log o(x) - H(X). \tag{6.29}$$

Thus, the increase in doubling rate due to the presence of side information *Y* is

$$\Delta W = W^*(X|Y) - W^*(X) = H(X) - H(X|Y) = I(X;Y). \quad \Box \quad (6.30)$$

Hence, the increase in doubling rate is equal to the mutual information between the side information and the horse race. Not surprisingly, independent side information does not increase the doubling rate.

This relationship can also be extended to the general stock market (Chapter 16). In this case, however, one can only show the inequality $\Delta W \leq I$, with equality if and only if the market is a horse race.

Example

- Consider the case of betting on the color of the next card in a deck of 26 red and 26 black
- Bets are placed on whether the next card will be red or black
- The game pays 2-for-1 (2 times payoff for win and nothing for lose)
- What will be the best betting schemes?

Two Different Approaches

$$S_{52}^* = \frac{2^{52}}{\binom{52}{26}} = 9.08.$$

- Sequential bet
- One-shot bet (Let each bet ride)

$$\begin{pmatrix} 52 \\ 26 \end{pmatrix}$$

Consider their differences!