1 Энтропия Шенона
— математика
— комб. приложения
— Коммуникац. св-ва
— передача инфо.

— Криптография

2. Колмогоровская сложность (Алг. теория информации)

---

§1 Энтропия Шенона

X - случ. величина $\underset{\parallel}{supp}(X) < +\infty$
A

$$A = \{a_1, a_2, -\ -, a_n\}$$
$$\quad p_1 \quad p_2 \qquad\quad p_n$$

$$H(X) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i}$$

Примеры 1) X равномерна по A

$$p_i = \frac{1}{|A|} \qquad H(X) = \log |A|$$

2) X — случ. битовая строка длины n

$$H(X) = n$$

3) X $\frac{1}{2}$ $*$
$\frac{1}{2}$ случ. строка длины n

$$H(X) = \frac{1}{2}\log 2 + \frac{1}{2}\sum 2^{-n} \cdot \log 2^{n+1} = \frac{1}{2} + \frac{n+1}{2} = \frac{n}{2} + 1$$

$*$ 0

$\frac{1}{2} \cdot 1 + \frac{1}{2}(n+1) = \frac{n}{2} + 1$

s 1 s

4) (X, Y, Z) — равн. распр $(1,1,1), (1,1,0)$
$(0,1,1)$ $(1,0,1)$

$\frac{1}{4}$ $\frac{3}{4}$

$$H(X,Y,Z) = 2$$
$$H(X) = H(Y) = H(Z) = \frac{1}{4}\log 4 + \frac{3}{4}\log\frac{4}{3}$$
$$H(X,Y) = \frac{1}{2}\cdot\log 2 + \frac{1}{4}\log 4 + \frac{1}{4}\log 4 = \frac{3}{2}$$

5) (X, Y, Z) равн. распр на

$\{(a,b,c) \in \{0,1\}^3 \mid a \oplus b \oplus c = 0\}$

$H(X) = H(Y) = H(Z) = 1$

$H(XY) = H(XZ) = H(YZ) = 2$

$\quad \| $

$H(XYZ)$

$\sum_{i=1}^{n} p_i \log \frac{1}{p_i} \qquad 0 \cdot \log \frac{1}{0} = 0$

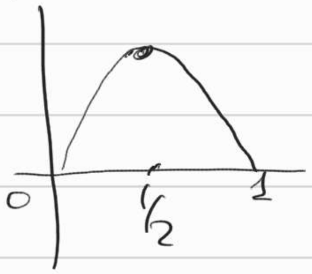
<u>св-ва энтропии</u>

1) $H(X) \geq 0$

2) $\begin{matrix} a_1 & a_2 \\ p & 1-p \end{matrix}$ $\qquad H(X) = h(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$

$h(0) = 0 \qquad h(p) = h(1-p)$

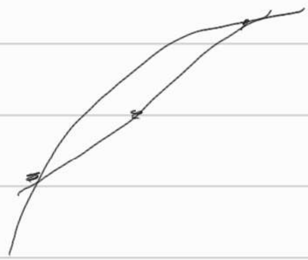
$h(1) = 0 \qquad h(1/2) = 1$



3) $A = supp(X)$

Тогда $H(X) \leq \log|A|$ $\quad = \Leftrightarrow$ X равномерно на A.

<u>Д-во</u> $H(X) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i} \leq$



$\leq \log\left(\sum_{i=1}^{n} p_i \cdot \frac{1}{p_i}\right) = \log n = \log|A|$

$= \Leftrightarrow \frac{1}{p_1} = \frac{1}{p_2} = \ldots = \frac{1}{p_n}$

4) Полуаддитивность энтропии

$H(X,Y) \leq H(X) + H(Y)$ $\quad = \Leftrightarrow X$ и Y незав.

<u>Д-во</u> $X \; \begin{matrix} a_1 & \ldots & a_n \\ p_1 & \ldots & p_n \end{matrix} \qquad Y \; \begin{matrix} b_1 & \ldots & b_m \\ q_1 & \ldots & q_m \end{matrix}$

$r_{ij} = Pr[X = a_i, Y = b_j]$

$H(X,Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} \log \frac{1}{r_{ij}}$

$H(X) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i} = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} \log \frac{1}{p_i}$

$H(Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} \log \frac{1}{q_j}$

$\ldots = \sum^{n} \sum^{m} \ldots \log \frac{p_i q_j}{\ldots}$

$$H(X,Y)-H(X)-H(Y) = \sum_{i=1} \sum_{j=1} r_{ij} \log \frac{}{r_{ij}} =$$

$$\le \log \sum_{i,j} p_i q_j = \log\left(\sum p_i\right)\left(\sum q_j\right) = 0$$

$$\Leftrightarrow \quad \frac{p_i q_j}{r_{i,j}} = const$$

const = 1

$$\Pr[X=a_i]\cdot \Pr[Y=b_j] = \Pr[X=a_i, Y=b_j]$$

$$1 = \sum_{i,j} p_i q_j = const$$

Пример. Если $k \le \frac{n}{2}$, тогда

$$\sum_{i=0}^{k} \binom{n}{i} \le 2^{n\cdot h\left(\frac{k}{n}\right)} \qquad \frac{k}{n} \quad \frac{n-k}{n}$$

Д-во. $(X_1, \ldots, X_n)$ — равномерное распред. на мн-ве битовых строк длины n, кот. сод. $\le k$ единиц.

$$H(X_1, X_2, \ldots, X_n) = \log\left(\sum_{i=0}^{k} \binom{n}{i}\right)$$

$$\Pr[X_i = 1] = E[X_i] = \frac{1}{n}\sum E[X_i] = \frac{1}{n} E\left[\sum X_i\right] \le$$

$$\le \frac{k}{n} \Rightarrow H(X_i) \le h\left(\frac{k}{n}\right)$$

$$H(X_1, X_2, \ldots, X_n) \le \sum H(X_i) \le \underline{n\cdot h\left(\frac{k}{n}\right)}$$

$$\overset{\shortparallel}{\underline{\log\left(\sum_{i=1}^{k} \binom{n}{i}\right)}}$$

Условная энтропия

$$H(X\mid Y) \qquad X \mid Y = a$$

$$p_b = \Pr[X=b \mid Y=a]$$

$$H(\overset{A}{X} \mid \overset{B}{Y} = b) = \sum_a \Pr[X=a \mid Y=b]\cdot \log \frac{1}{\Pr[X=a\mid Y=b]}$$

$$H(X\mid Y) = \sum \Pr[Y=b]\cdot H(X\mid Y=b)$$

$H(X|Y) \quad \sum_{b \in B} \ldots$

Лемма $H(X,Y) = H(X) + H(Y|X)$

$H(X,Y) - H(X) \ominus$

$$H(X,Y) = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} \log \frac{1}{r_{i,j}}$$

$$H(X) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i} = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} \log \frac{1}{p_i}$$

$$\ominus \sum_{i,j} r_{i,j} \log \frac{p_i}{r_{i,j}} = \sum_{i,j} \frac{r_{i,j}}{p_i} \cdot p_i \log \frac{p_i}{r_{i,j}}$$

$$\frac{p_i}{r_{i,j}} = \frac{\Pr[X = a_i]}{\Pr[X = a_i, Y = b_j]} = \Pr[Y = b_j | X = a_i]$$

$$= \sum_i p_i H(Y | X = a_i) = H(Y|X)$$

Сл-ие $H(Y) \geq H(Y|X)$

Д-во

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

$$H(X) + H(Y)$$

Пр-ло Цепочки

$$H(X_1 X_2 \ldots X_n) = H(X_1) + H(X_2|X_1) + H(X_3|X_1 X_2) + H(X_4|\ldots) + \ldots + H(X_n|X_1 \ldots X_{n-1})$$

Релятивизация

Пр-р $H(X|Y) \le H(X)$

$$H(X|YZ) \le H(X|Z)$$

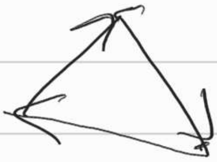
$$Z=z$$

$$H(X,Y|Z) = H(X|Z) + H(Y|XZ)$$

Пр-р $G(V,E)$ ор. граф

$E \subseteq V \times V$

$(x,y,z) \in V^3$ наз-ся Δ, если

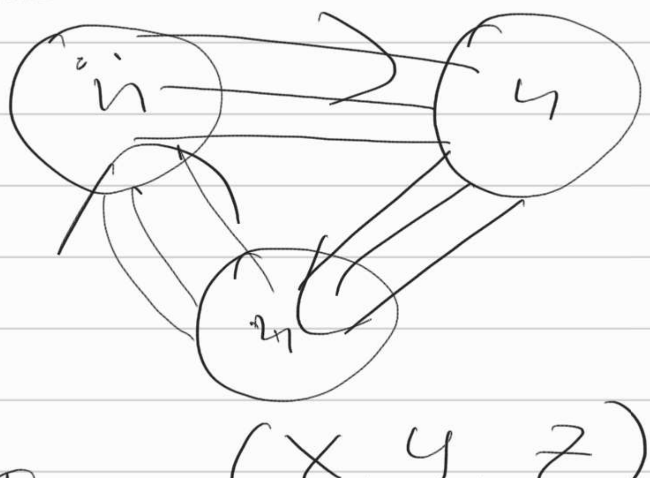


$(x,y),(y,z),(z,x) \in E$

Галочка $(x,y,z) \in V^3$

$(x,y),(x,z) \in E$

Лемма $\# \Delta \le \#$ галочек



$3n^3$

Д-во $(X,Y,Z) \in V^3$

равномерное распр. на всех Δ

$0 \quad H\Delta = H(X,Y,Z) - H(X) +$

$\log \# \Delta = H(X,Y,Z) = H(X)$

$+ H(Y|X) + H(Z|X,Y) \le$

$\le H(X) + \underbrace{H(Y|X)} + \underbrace{H(Z|Y)} \underset{\text{симметрия}}{\overset{\text{п}}{=}}$

$= H(X) + 2H(Y|X)$ $\quad X \; Y \; Z$

$(A, B, C) \in U^3$

$A \sim X$

B при усл $A \to$ такое же как Y при усл. X

C при усл $A \to$

$q(a,b,c) = \Pr[X=a] \cdot \Pr[Y=b | X=a] \cdot \Pr[Y=c | X=a]$

Носитель распр — голим

$H(A,B,C) = H(A) + H(B|A) + H(C|AB)$

$= H(A) + H(B|A) + H(C|A) =$

$= H(X) + H(Y|X) + H(Y|X) = H(X) + 2H(Y|X) \ge$

$\ge H(X,Y,Z) = \log \# \Delta$

<u>Теорема</u> (Брегман)

d_1

d_2

d_n

$n \quad n$

$\# PM \le d_1 d_2 \ldots d_n$

$\underline{\cancel{\# PM} \le (d_1!)^{1/d_1} (d_2!)^{1/d_2} \ldots (d_n!)^{1/d_n}}$

Лемма $\operatorname{Supp} X = A = A_1 \sqcup A_2 \sqcup \dots \sqcup A_m$

$\forall a \in A_i$ Y при $X = a$ прин. $\le i$ значений

Тогда $H(Y|X) \le \sum_{i=1}^{m} \Pr[X \in A_i] \cdot \log i$

Д-во (т-мы) $\sigma = \sigma(1)\sigma(2)\dots\sigma(n)$ — случ. совершенное паросочет.

$$\underset{\log \#PM}{H(\sigma)} = H(\sigma(1)\sigma(2)\dots\sigma(n)) \le \sum H(\sigma(i)) \le \sum \log d_i$$

$$H(\sigma(1)\dots\sigma(n)) = H(\sigma(1)) + H(\sigma(2) \mid \sigma(1)) + \dots$$

$H(\sigma)$

$\tau \in S_n$

$$H(\sigma(\tau(1)), \sigma(\tau(2)), \dots \sigma(\tau(n))) =$$

$$= H(\sigma(\tau(1))) + H(\sigma(\tau(2)) \mid \sigma(\tau(1))) + \dots + H(\sigma(\tau(n)) \mid \sigma(\tau(1)) \dots \sigma(\tau(n-1)))$$

$H(\sigma) =$

$$\mathop{E}_{\tau}\left[H(\sigma(\tau(1))) + H(\sigma(\tau(2)) \mid \sigma(\tau(1))) + \dots + H(\sigma(\tau(n)) \mid \sigma(\tau(1)) \dots \sigma(\tau(n-1))) \right]$$

$$= E \left[\sum^{n} H(\sigma(i) \mid \sigma(\tau(1)) \dots \sigma(\tau(k-1)) \right]$$

$$k = \tau^{-1}(i)$$

$$= \sum_{i=1}^{n} \mathop{E}_{\tau} \left[H(\sigma(i) \mid \sigma(\tau(1)) \ldots \sigma(\tau(k-1)) \right] \leq$$
$$k = \tau^{-1}(i)$$

$R_i(\sigma, \tau)$ число соседей i-ой вершины, за исключением $\sigma(\tau(1)), \ldots, \sigma(\tau(k-1))$

$$\leq \sum_{i=1}^{n} \mathop{E}_{\tau} \left[\sum_{j=1}^{d_i} \Pr_{\sigma} [R_i(\sigma, \tau) = j] \cdot \log j \right]$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{d_i} \Pr_{\sigma, \tau} [R_i(\sigma, \tau) = j] \cdot \log j =$$

$$? \ \| \ \frac{1}{d_i}$$

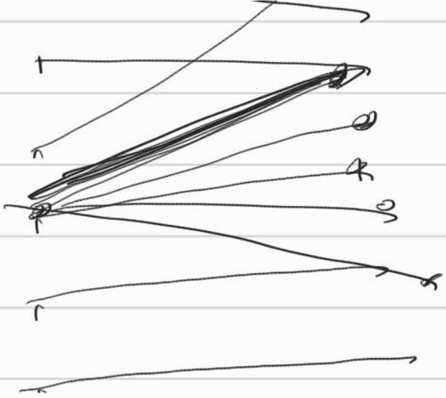
$$= \sum_{i=1}^{n} \sum_{j=1}^{d_i} \frac{1}{d_i} \log j = \sum_{i=1}^{n} \frac{1}{d_i} \cdot \log (d_i!)^{\frac{1}{d_i}}$$

$\log \# PM$

$$\Pr_{\sigma, \tau} [R_i(\sigma, \tau) = j] = \frac{1}{d_i}$$

$$\sigma(\tau(1)), \sigma(\tau(2)) \ldots \sigma(\tau(k-1))$$

Достаточно $\sigma \leftarrow$ fix



$0 \ldots d_i - 1$

dmitrits@
pdmi.ras.ru