Entropie,

relativní entropie

a sdílená (vazební) informace

Pojem informace je příliš rozsáhlý na to, abychom jej komplexně popsali jednoduchou definicí.
Pro libovolnou distribuci pravděpodobnosti můžeme definovat tzv. entropii, jež má mnoho vlastností potřebných pro měření informace.
Vzájemná informace je speciální případ – více obecné veličiny – relativní entropie , což je míra diference mezi dvěma pravděpodobnostmi rozděleními.
Nyní odvodíme jednoduché vlastnosti těchto veličin.

1. Entropie

– míra nejistoty náhodné proměnné na množině **X**

X diskrétní náhodná proměnná s pravděpodobností $p(x) = \{X = x\}$ $x \in X$

Definice:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x) \qquad [\text{ bit}]$$

Pozn.: 0 log 0 = 0 (x log x $\to$ 0 x $\to$ 0)

Entropie je funkcionál distribuce,
nezáleží na skutečných hodnotách, ale na pravděpodobnostech.

Označme střední hodnotu E, $X \sim p(x)$,
pak očekávaná hodnota náhodné proměnné $g(X)$ je :

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

Pozn.: $g(X) = \log (1/p(X))$ $\quad H(X) = E_p \log (1/p(X))$

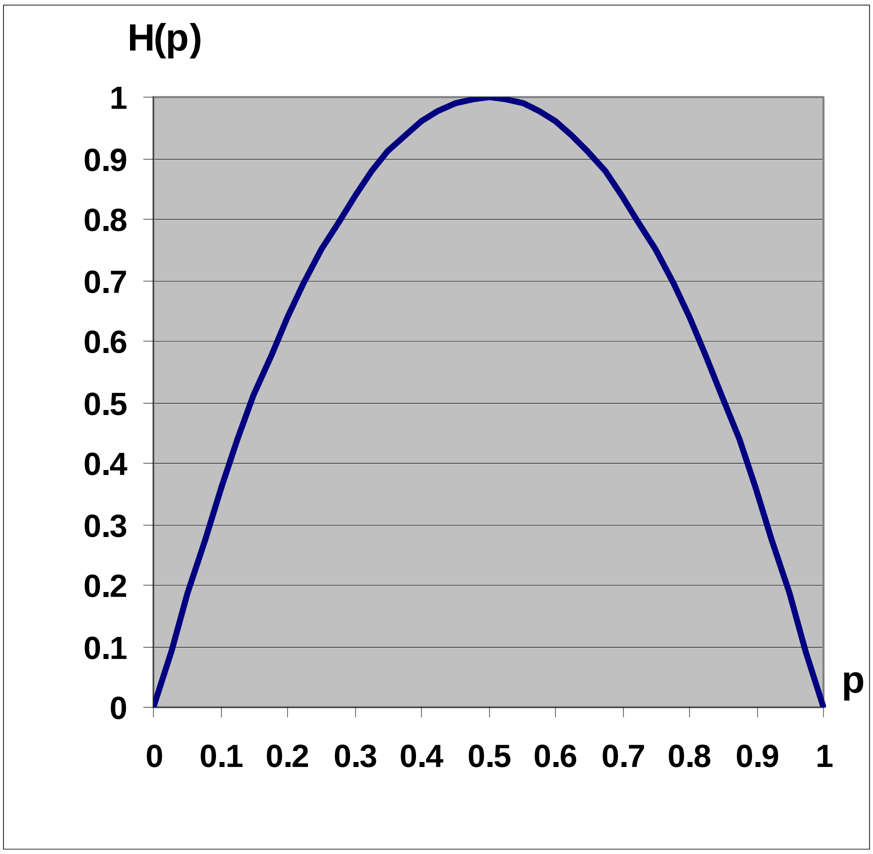
Lemma1: $H(X) \geq 0$
Dk: $0 \leq p(x) \leq 1 \;\to\; \log(1/p(x)) \geq 0$

Lemma2: $H_b(X) = (\log_b a)\, H_a(X)$
Dk: $\log_b p \;\to\; \log_b a \log_a p$

Př.1:

$$\mathbf{X} = \begin{cases} 1 & \dots\; p \\ 0 & \dots\; 1-p \end{cases}$$

$$H(X) \overset{\text{def}}{=} -p \log p - (1-p)\log(1-p) = H(p)$$



Př.2:

$$X = \begin{cases} a & p = \ 1/2 \\ b & \quad\ \ 1/4 \\ c & \quad\ \ 1/8 \\ d & \quad\ \ 1/8 \end{cases}$$

H(X) =

$- \ 1/2 \log 1/2 \ - 1/4 \log 1/4 - \ 1/8 \log 1/8 \ - 1/8 \log 1/8 \ = -1/2 \log 2^{-1} - \ \dots =$

$= \ 1/2+2/4+3/8+3/8 \ = 7/4$

2. Sdružená entropie a podmíněná entropie

Nyní rozšíříme definici pro 2 náhodné proměnné.
(X,Y) - vektorové vyjádření náhodné proměnné, sdružená distribuce p(x,y)

Definice1: Sdružená entropie

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

což lze vyjádřit jako:

$$H(X,Y) = - \mathrm{E} \log p(X, Y)$$

Definice2: Podmíněná entropie
Nechť $(X,Y) \sim p(x, y)$

$$H(Y|X) = \sum_{x\in X} p(x)\, H(Y|X=x)$$

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

Teorém: Řetězové pravidlo

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

Dk.:

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

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

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

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

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

Ekvivalentně lze psát:

$$\log p(X,Y) = \log p(X) + \log p(Y|X)$$

Př.1:

Y \ X	1	2	3	4
1	**1/8**	**1/16**	**1/32**	**1/32**
2	**1/16**	**1/8**	**1/32**	**1/32**
3	**1/16**	**1/16**	**1/16**	**1/16**
4	**1/4**	**0**	**0**	**0**

$$H(X|Y) = \sum_{i=1}^{4} p(Y=i)\, H(X|Y=i)$$

$= 1/4H(1/2, 1/4, 1/8,1/8) + 1/4H(1/4, 1/2, 1/8,1/8) + 1/4H(1/4, 1/4, 1/4,1/4) +$
$+ 1/4\ H(1, 0, 0, 0)$

$= 1/4*7/4+1/4*7/4+1/4*2+1/4*0 = 11/8$ [bitů]

Pozn.:
$H(Y|X) \neq H(X|Y)$ **ale:** $H(X) - H(X|Y) = H(Y) - H(Y|X)$

3. Relativní entropie a sdílená (vazební) informace

- míra diference mezi 2 distribucemi

Definice: Relativní entropie mezi dvěma pravděpodobnostmi p(x) a q(x)

$$D(p||q) = \sum_{x \in X} p(x) \log p(x)/q(x) = E_p \log p(X)/q(X)$$

Pozn.: $0 \log 0/q = 0,\ p \log p/0 = \infty$

$$D(p||q) \geq 0 \;\Leftrightarrow\; p = q$$

Sdílená informace – míra množství informace, že jedna náhodná proměnná obsahuje další náhodnou proměnnou. To snižuje nejistotu jedné náhodné proměnné vzhledem ke znalosti druhé.

Uvažujme X,Y se sdruženou pravděpodobností p(x,y) a marginálními pravděpodobnostmi p(x), p(y).
Vazební informace I(X;Y) je relativní entropie mezi sdruženou distribucí p(x)p(y).

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

$$= E_{p(x,y)} \log \frac{p(X,Y)}{p(X)p(Y)}$$

Př.2: Nechť **X** = (0, 1) a existují distribuce p, q;

p(0) = 1 – r p(1) = r q(0) = 1 – s q(1) = s

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

a

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

Je-li r = s pak $D(p||q) = D(q||p) = 0$

Je-li r = 1/2 s = 1/4 pak:

$$D(p||q) = \frac{1}{2} \log \frac{\frac{1}{2}}{\frac{3}{4}} + \frac{1}{2} \log \frac{\frac{1}{2}}{\frac{1}{4}} = 1/2 \log 3^{-1} 2 + 1/2 \log 2 =$$

$$= -1/2 \log 3 + 1/2 + 1/2 = 1 - 1/2 \log 3 = 0{,}2075 \text{ [bitů]}$$

ale

$$D(q||p) = \frac{3}{4} \log \frac{\frac{3}{4}}{\frac{1}{2}} + \frac{1}{4} \log \frac{\frac{1}{4}}{\frac{1}{2}} = 3/4 \log 3 - 1 = 0{,}1887 \text{ [bitů]}$$

Obecně: $D(p||q) \neq D(q||p)$

4. Vzájemný vztah mezi entropií a sdílená informace

Sdílená informace

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

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

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

Vzhledem k symetrii lze psát:

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

Platí-li

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

pak

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

tudíž

$$I(X;X) = H(X) + H(X|X) = H(X)$$

Aplikací těchto výsledků dostáváme následující teorém:

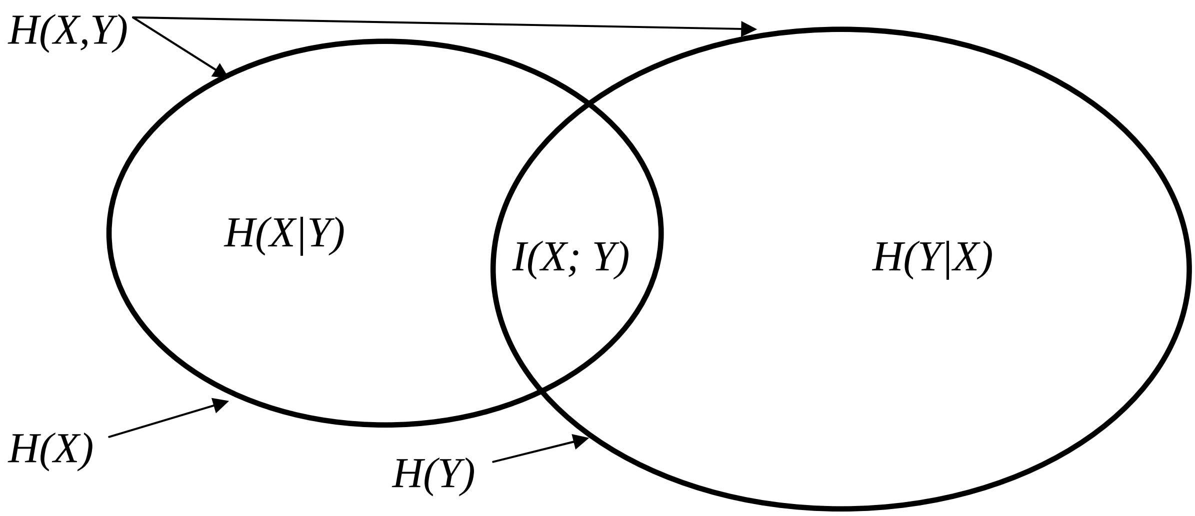
$$I(X;Y) = H(X) - H(X|Y)$$

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

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

$$I(X;Y) = I(Y;X)$$

$$I(X;X) = H(X)$$



Př.: pro zadání z př. 2.1 spočtěte**:**

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

$$= 7/4 - 11/8 = 3/8 = 0{,}375 \text{ [bitů]}$$

5. Řetězová pravidla pro entropii, relativní entropii a sdílenou informaci

Entropie kolekce náhodných proměnných je součtem podmíněných entropií

Teorém1: Nechť $X_1, X_2, \dots, X_n$ je popsáno $p(x_1, x_2, \dots, x_n)$ pak¨

$$H(X_1, X_2, \dots, X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1}, \dots, X_1)$$

Dk.: $$H(X_1, X_2) = H(X_1) + H(X_2|X_1)$$

$$H(X_1, X_2, X_3) = H(X_1) + H(X_2, X_3|X_1)$$

$$= H(X_1) + H(X_2|X_1) + H(X_3|X_2, X_1)$$

$$\dots$$

$$H(X_1, X_2, \dots, X_n) = H(X_1) + H(X_2|X_1) + H(X_n|X_{n-1}, \dots, X_1)$$

$$= \sum_{i=1}^{n} H(X_i|X_{i-1}, \dots, X_1)$$

Nyní definujeme podmíněnou sdílenou informaci jako zmenšení nejistoty o X vzhledem ke znalosti Y, je-li dáno Z.

Definice1:

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

$$= E_{p(x,y,z)} \log \frac{p(X,Y|Z)}{p(X|Z)\,p(Y|Z)}$$

Teorém2: Řetězové pravidlo pro informaci

$$I(X_1, X_2, \dots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y| X_{i-1}, \dots, X_1)$$

Dk.:

$$I(X_1, X_2, \dots, X_n; Y) = H(X_1, X_2, \dots, X_n; Y) - H(X_1, X_2, \dots, X_n | Y) =$$

$$= \sum_{i=1}^{n} H(X_i | X_{i-1}, \dots, X_1) - \sum_{i=1}^{n} H(X_i | X_{i-1}, \dots, X_1, Y) =$$

$$= \sum_{i=1}^{n} I(X_i; Y| X_1, \dots, X_{i-1})$$

Definice2: Podmíněná relativní entropie

$$D(p(y|x)||q(y|x)) = \sum_x p(x) \sum_y p(x|y) \log \frac{p(x|y)}{q(y|x)} =$$

$$= E_{p(x,y)} \log \frac{p(Y|X)}{q(Y|X)}$$

Relativní entropii mezi 2 vlastními distribucemi dvojice náhodných proměnných je možno vyjádřit součtem relativní entropie a podmíněné relativní entropie.

Teorém3: Řetězové pravidlo pro relativní entropii

$$D(p(x,y)||q(x,y)) = D(p(x)||q(x)) + D(p(y|x)||q(y|x))$$

Dk.:

$$D(p(x, y)||q(x, y)) = \sum_{x} \sum_{y} p(x, y) \log \frac{p(x,y)}{q(x,y)}$$

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

$$= \sum_{x} \sum_{y} p(x, y) \log \frac{p(x)}{q(x)} + \sum_{x} \sum_{y} p(x, y) \log \frac{p(y|x)}{q(y|x)}$$

$$= D(p(x)||q(x)) + D(p(y|x)||q(y|x))$$

Ing. Arnoštka Netrvalová
(e-mail: netrvalo@kiv.zcu.cz, ZČU v Plzni, FAV, KIV - místnost: UK 412, tel.: 377632425)