信息论基础

李 莹 liying2009@ecust.edu.cn

第二章: 信息的度量

- 一、自信息和互信息
- 二、平均自信息
- 三、平均互信息

- 1. 平均自信息的概念
- 2. 熵函数的性质
- 3. 联合熵与条件熵

1. 平均自信息的概念

自信息是一个随机变量:

自信息是指信源发出的某一消息所含有的信息量。不同的消息,它们所含有的信息量也就不同。

平均自信息(信息熵/信源熵/香农熵/无条件熵/熵函数/熵):

$$H(X) \triangleq E[I(x_i)] = E[-\log p(x_i)] = -\sum_{i=1}^n p(x_i)\log p(x_i)$$

信息熵的单位,取决于对数选取的底:

- ▶ 以2为底,单位为比特/符号
- ▶ 以e为底,单位为奈特/符号
- ▶ 以10为底,单位为哈特莱/符号。

信息熵的意义:

信源的信息熵是从<u>整个</u>信源的统计特性来考虑的。它是从<u>平均</u>意义上来表征信源的总体特性的。对于某特定的信源,其信息熵只有一个。不同的信源因统计特性不同,其信息熵也不同。

信息熵是从平均意义上表征随机变量总体特性的一个量, 其含义体现在如下几方面:

- (1) 在事件发生后,表示平均每个事件(或符号)所提供的信息量;
- (2) 在事件发生前,表示随机变量取值的平均不确定性;
- (3) 表示随机变量随机性大小, 熵大的, 随机性大;
- (4) 当事件发生后,其不确定性就被解除,熵是解除随机变量 不确定性平均所需信息量。

离散随机变量的概率空间为:

$$\begin{bmatrix} X \\ P(X) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ p(x_1) & p(x_2) & \dots & p(x_n) \end{bmatrix} \quad 0 \le p(x_i) \le 1, \quad \sum_{i=1}^n p(x_i) = 1$$

$$0 \le p(x_i) \le 1, \quad \sum_{i=1}^n p(x_i) = 1$$

记
$$p_i = p(x_i)$$
, 则
$$H(X) = -\sum_{i=1}^n p_i \log p_i$$

$$= H(p_1, p_2, ..., p_n) = H(\mathbf{p})$$

通常把一个随机变量的样本 空间和样本空间中的元 素对应的概率称为概率 空间。

由于概率的完备性,即 $\sum_{i=1}^{n} p_i = 1$,所以 $H(\mathbf{p})$ 实际上是 (n-1)元函数。

当
$$n=2$$
 时, $H(\mathbf{p}) = H(p,1-p) = H(p)$

例1 掷一个六面均匀的骰子,每次出现朝上一面的点数是随机的,以朝上一面的点数作为随机试验的结果,并把试验结果看作一个信源的输出,试建立数学模型。

解: 信源的输出: 离散随机变量X

X: {1, 2, 3, 4, 5, 6} ——样本空间

$$P(X)$$
 : $\{P(X=1)=1/6, P(X=2)=1/6, \dots, P(X=6)=1/6\}$

$$[X \cdot P] = \begin{cases} X: & 1 & 2 & 3 & 4 & 5 & 6 \\ P(X): & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 \end{cases}$$

$$0 \le p(x_i) \le 1 (i = 1, 2 \cdots, 6)$$

$$\sum_{i=1}^{6} p(x_i) = 1$$

$$H(X) = \log 6$$
 bit/symbol

例2: 一信源有6种输出符号,概率分别为P(A)=0.5,P(B)=0.25,P(C)=0.125,P(D)=P(E)=0.05,P(F)=0.025。

- 1)计算*H(X)*。
- 2)求符号序列ABABBA和FDDFDF的信息量,并将之与6位符号的信息量期望值相比较。

解: 1)由信息熵定义,该信源输出的信息熵为

$$H(X) = \sum_{i=1}^{6} p(x_i) \log \frac{1}{p(x_i)}$$
= 0.5 \log 2 + 0.25 \log 4 + 0.125 \log 8 + 2 \times 0.05 \log 20 + 0.025 \log 40
= 1.94 bit/symbol

符号序列ABABBA所含的信息量为

$$I_1 = 3I_A + 3I_B = 3(-\log P_A - \log P_B) = 3(\log 2 + \log 4) = 9$$
 bit

符号序列FDDFDF所含的信息量为

$$I_2 = 3I_D + 3I_F = 3(-\log P_D - \log P_F) = 3(\log 20 + \log 40) = 28.932$$
 bit

6位符号序列的信息量平均值为

$$\bar{I} = 6H(X) = 11.64$$
 bit

三者比较为
$$I_1 < \overline{I} < I_2$$

2. 熵函数的性质

熵函数的数学特性包括:

(1)对称性

(5)连续性

(2)确定性

(6)递增性

(3)非负性

(7)上凸性

(4)扩展性

(8)极值性

2. 熵函数的性质-对称性

(1) 对称性

当概率矢量 $\mathbf{p} = (p_1, p_2, ..., p_n)$ 中各分量的次序任意变更时,熵函数的值不变,即

$$H(p_1, p_2, ..., p_n) = H(p_2, p_1, ..., p_n)$$

= $H(p_3, p_1, ..., p_2)$
= ...
= $-\sum_{i=1}^{n} p_i \log p_i$

该性质说明: 熵只与随机变量(信源)的<u>总体统计特性</u>有关。 如果某些信源的统计特性相同(含有的<u>符号数</u>和<u>概率分布</u> 相同),那么这些信源的熵就相同。

2. 熵函数的性质-对称性

例3: 三个信源分别为:

$$\begin{bmatrix} X \\ P(X) \end{bmatrix} = \begin{bmatrix} x_1(\mathfrak{U}) & x_2(\mathbf{黄}) & x_3(\mathbf{\mathring{E}}) \\ 1/3 & 1/6 & 1/2 \end{bmatrix}$$

$$\begin{bmatrix} Y \\ P(Y) \end{bmatrix} = \begin{bmatrix} y_1(x) & y_2(x) & y_3(x) \\ 1/6 & 1/2 & 1/3 \end{bmatrix}$$
② X与Y信源的差别:

$$\begin{bmatrix} Z \\ P(Z) \end{bmatrix} = \begin{bmatrix} z_1(\mathbb{R}) & z_2(\mathbb{R}) & z_3(\mathbb{R}) \\ 1/3 & 1/6 & 1/2 \end{bmatrix}$$
 ② 但它们的信息熵是相同的。

- |① X与Z信源的差别: 具体消息其含义不同:
 - 同一消息的概率不同:

2. 熵函数的性质-确定性

(2) 确定性

$$H(1,0)=H(1,0,0)=H(1,0,0,0)=...=H(1,0,...,0)=0$$

(:
$$1\log 1 = 0$$
, $\lim_{p_i \to 0} p_i \log p_i = 0$)

在概率空间中,只要有一个事件是必然事件,那么其它事件一定是不可能事件,因此信源没有不确定性,熵必为0。

2. 熵函数的性质-非负性

(3) 非负性

$$H(\mathbf{p}) = H(p_1, p_2, ..., p_n) \ge 0$$

$$\therefore 0 \le p_i \le 1$$

$$\therefore -\log p_i \ge 0$$

$$\therefore H(\mathbf{p}) = -\sum_{i=1}^{n} p_i \log p_i \ge 0$$

只有当随机变量是一确知量时,熵H(X)=0。 离散信源的熵满足非负性,而连续信源的熵可能为负。

2. 熵函数的性质-扩展性

(4) 扩展性

$$\lim_{\varepsilon \to 0} H_{n+1}(p_1, p_2, ..., p_n - \varepsilon, \varepsilon) = H_n(p_1, p_2, ..., p_n)$$

$$\left(:: \lim_{\varepsilon \to 0} \varepsilon \log \varepsilon = 0, \lim_{\varepsilon \to 0} (p_n - \varepsilon) \log(p_n - \varepsilon) = p_n \log p_n \right)$$

- 扩展性说明,增加一个概率接近于零的事件,信源熵保持不变。
- 虽然小概率事件出现后,给予收信者较多的信息,但从 总体来考虑时,因为这种概率很小的事件几乎不会出 现,所以它对于离散集的熵的贡献可以忽略不计。这 也是熵的总体平均性的一种体现。

- 2. 熵函数的性质-连续性
- (5) 连续性

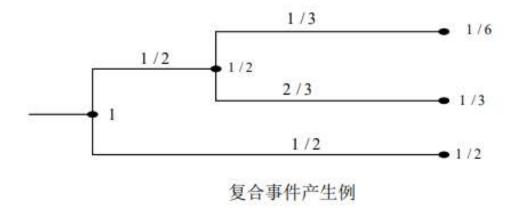
$$\lim_{\varepsilon \to 0} H(p_1, p_2, \cdots, p_{q-1} - \varepsilon, p_q + \varepsilon) = H(p_1, p_2, \cdots, p_q)$$

概率分量的微小波动不会引起熵的变化。

(6) 可加性(递推性、递增性)

先看一个简单例子,某随机事件集合有3个事件,概率 分别为: $p_1 = 1/2$, $p_2 = 1/3$, $p_3 = 1/6$;

这3个事件可以直接产生,也可分两步产生,即先以1/2的概率产生两个事件,选择其中之一作为输出,或者在另一事件发生条件下再以2/3和1/3的概率产生两事件,选择其中的一个作为输出。



(6) 递增性(递推性)

熵的可加性首先由香农提出,含义如下:如果一个事件可以分成两步连续选择来实现(多步产生的事件也称复合事件),那么原来的熵H应为H的单独值的加权和。注:"H的单独值"是指每次选择的熵值,"权值"就是每次选择的概率。

H(1/2,1/3,1/6) = H(1/2,1/2) + (1/2)H(1/3,2/3)

上式等号右边的第1项是第1步选择的熵;由于第2步选择只有1/2的概率发生,所以第2项是第2步选择的熵与权值1/2的乘积。

(6) 递推性(可加性)

$$H(p_{1}, p_{2}, \dots, p_{n-1}, q_{1}, q_{2}, \dots, q_{m})$$

$$= H(p_{1}, p_{2}, \dots, p_{n}) + p_{n}H(\frac{q_{1}}{p_{n}}, \frac{q_{2}}{p_{n}}, \dots, \frac{q_{m}}{p_{n}})$$
其中:
$$\sum_{i=1}^{n} p_{i} = 1, \sum_{j=1}^{m} q_{j} = p_{n}$$

2. 熵函数的性质-递推性

例4: 利用递推性计算熵函数 H(1/3, 1/3, 1/6, 1/6)的值。

解:
$$H(\frac{1}{3}, \frac{1}{3}, \frac{1}{6}, \frac{1}{6}) = H(\frac{1}{3}, \frac{2}{3}) + \frac{2}{3}H(\frac{1}{2}, \frac{1}{4}, \frac{1}{4})$$

 $= H(\frac{1}{3}, \frac{2}{3}) + \frac{2}{3}H(\frac{1}{2}, \frac{1}{2}) + \frac{2}{3}\cdot\frac{1}{2}H(\frac{1}{2}, \frac{1}{2})$
 $= H(\frac{1}{3}, \frac{2}{3}) + H(\frac{1}{2}, \frac{1}{2})$

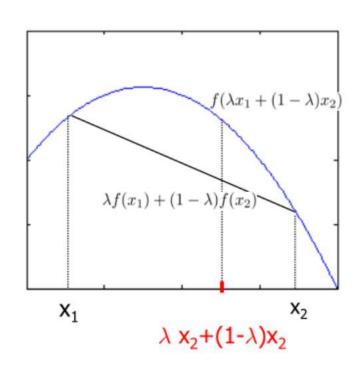
2. 熵函数的性质-递推性

例 设某地气象为随机变量X,符号集A={晴,多云,阴,雨,雪,雾,霾},概率分别为 0.3,0.2,0.2,0.05,0.05,0.05,0.15;现将多云和阴用阴代替,雨和雪用降水代替,雾和霾用雾霾代替,得到简化气象Y,符号集B={晴,阴,降水,雾霾},求两气象熵的差。

解:

 $H(X)-H(Y)=0.4\times H(1/2)+0.1\times H(1/2)+0.2\times H(1/4)=0.6623$ 比特/符号

(7) 上凸性 凸函数的定义



$$\forall \lambda (0 < \lambda < 1)$$

$$f[\lambda x_1 + (1 - \lambda)x_2] \ge \lambda f(x_1) + (1 - \lambda)f(x_2)$$

几何描述:

在上凸函数的任意两点之间画一条 割线, 函数曲线总在割线上面。

凸函数的定义及詹森不等式

$$f\left[\sum_{k=1}^{q} \lambda_k x_k\right] \geq \sum_{k=1}^{q} \lambda_k f(x_k)$$

引理(香农辅助定理):

$$H(p_1, p_2, ..., p_n) = -\sum_{i=1}^n p_i \log p_i \le -\sum_{i=1}^n p_i \log q_i$$
其中 $\sum_{i=1}^n p_i = 1$, $\sum_{i=1}^n q_i = 1$

证明:
$$H(p_{1,}p_{2},...,p_{n}) + \sum_{i=1}^{n} p_{i} \log q_{i} = -\sum_{i=1}^{n} p_{i} \log p_{i} + \sum_{i=1}^{n} p_{i} \log q_{i}$$

$$= \sum_{i=1}^{n} p_{i} \log \frac{q_{i}}{p_{i}}$$

$$\frac{q_{i}}{p_{i}} = 1, \quad i = 1, 2, \cdots, n \quad \text{时等号成立}_{\circ} \qquad \leq \log \sum_{i=1}^{n} \left(p_{i} \cdot \frac{q_{i}}{p_{i}} \right) = 0$$

$$H(p_1, p_2, ..., p_n)$$
是概率分布 $(p_1, p_2, ..., p_n)$ 的严格上凸函数,即 $H[\alpha \mathbf{p} + (1-\alpha)\mathbf{p'}] > \alpha H(\mathbf{p}) + (1-\alpha)H(\mathbf{p'})$ $0 < \alpha < 1$ 证明: $\alpha p_i + (1-\alpha) \ p_i$ '可以被看做是一种新的概率分布。 (因为 $0 \le \alpha p_i + (1-\alpha) \ p_i$ ' ≤ 1)
$$H[\alpha \mathbf{p} + (1-\alpha)\mathbf{p'}] = -\sum_{i=1}^n [\alpha p_i + (1-\alpha) \ p_i$$
 ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i + (1-\alpha) \ p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i - (1-\alpha) \sum_{i=1}^n p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i - (1-\alpha) \sum_{i=1}^n p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i - (1-\alpha) \sum_{i=1}^n p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i - (1-\alpha) \sum_{i=1}^n p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i - (1-\alpha) \sum_{i=1}^n p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i - (1-\alpha) \sum_{i=1}^n p_i$ ' $= -\alpha \sum_{i=1}^n p_i \log[\alpha p_i]$ 等号成立条件 $= -\alpha H(\mathbf{p}) + (1-\alpha) H(\mathbf{p'})$

当
$$\frac{\alpha p_i + (1-\alpha) p_i'}{p_i} = 1$$
 且 $\frac{\alpha p_i + (1-\alpha) p_i'}{p_i'} = 1$ 时等号成立。

但是

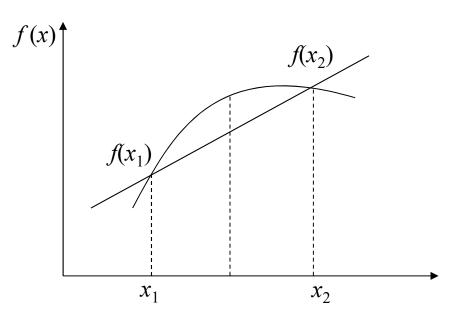
当
$$\mathbf{p} \neq \mathbf{p}$$
'时, $\frac{\alpha p_i + (1-\alpha) p_i}{p_i} \neq 1$ 且 $\frac{\alpha p_i + (1-\alpha) p_i}{p_i} \neq 1$ (因为 $0 < \alpha < 1$)

所以等号不成立。

上凸性的几何意义:

在上凸函数的任两点之间画一条割线,函数总在割线的上方.

上凸函数在定义域内的 极值必为最大值,这对 求最大熵很有用。



- 2. 熵函数的性质-极值性
- (8) 极值性(最大离散熵定理)

定理: 离散无记忆信源输出n个不同的信息符号, 当且仅当各个符号出现概率相等时($\mathbb{P}_{p_i} = \frac{1}{n}$), 熵最大, 即

$$H(p_1, p_2, ..., p_n) \le H(\frac{1}{n}, \frac{1}{n}, ..., \frac{1}{n}) = \log n$$

2. 熵函数的性质-极值性

$$\frac{\partial}{\partial p(x_i)} \left(\sum_{i=1}^n p(x_i) \right) = \frac{\partial}{\partial p(x_i)} \left[p(x_1) + \dots + p(x_i) + \dots + p(x_n) \right] = 1$$

在约束条件
$$\sum_{i=1}^{n} p(x_i) = 1$$
下求 $H(\mathbf{p}) = -\sum_{i=1}^{n} p(x_i) \log_e p(x_i)$ 的极值。

解: 作辅助函数
$$F = -\sum_{i=1}^{n} p(x_i) \log_e p(x_i) - \lambda \left(\sum_{i=1}^{n} p(x_i) - 1\right)$$

$$\frac{\partial F}{\partial p(x_i)} = -\log_e p(x_i) - 1 - \lambda \qquad i = 1, 2, \dots, n$$

$$\Rightarrow \frac{\partial F}{\partial p(x_i)} = 0,$$
 得 $p(x_i) = e^{-(\lambda + 1)}$

曲
$$\sum_{i=1}^{n} p(x_i) = 1$$
 得 $e^{-(\lambda+1)} = \frac{1}{n}$ ∴ $p(x_i) = \frac{1}{n}$ $i = 1, 2, \dots, n$

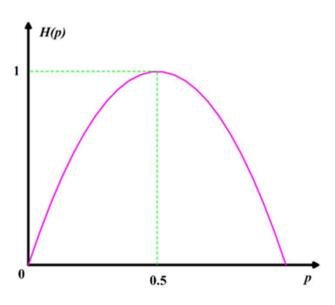
2. 熵函数的性质

例5:

以二进制信源为例,信源的概率空间为 $\begin{bmatrix} X \\ P(X) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ p & 1-p \end{bmatrix}$

二进制信源的信息熵为 $H(X) = -[p \log p + (1-p) \log(1-p)]$ 这时信息熵H(X)是p的函数,

熵函数H(p)的曲线如图所示:



2. 熵函数的性质

从图中可以得出熵函数的一些性质:

- 如果二进制信源的输出是确定的(p=0或p=1),则该信源不提供任何信息;
- 当二进制信源符号0和1等概率发生时,信源的熵达到最大值,等于1比特/符号;
- 在等概率的二进制信源输出的二进制数字序列中,每一个二元数字提供1比特的信息量。如果符号不是等概率分布,则每一个二元数字所提供的平均信息量小于1比特。
- 这也进一步说明了计算机术语中的"比特"与信息量单位"比特"的关系。

定义2.4 随机变量X和Y的联合分布为 $p(x_iy_j)$,则这两个随机变量的联合熵定义为:

$$H(XY) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_i y_j) \log p(x_i y_j)$$

联合熵表示对于二维随机变量的平均不确定性。

- 表示通信完成之后,观察者对通信系统仍然存在的平均不确定度
- 对于观察来说
 - H(X)+H(Y)称为先验不确定度
 - H(XY)称为后验不确定度

定义2.5 随机变量X和Y的条件熵定义为:

$$H(X \mid Y) = -\sum_{i} \sum_{j} p(x_i y_j) \log p(x_i \mid y_j)$$

$$H(Y \mid X) = -\sum_{i} \sum_{j} p(x_i y_j) \log p(y_j \mid x_i)$$

条件熵表示已知一个随机变量时,对另一个随机变量的平均不确定性。

- 表示接收者收到Y后,对信源X仍然存在的平均不确定度
- 对于接收者来说, H(X)称为先验不确定度, H(X|Y) 称为后验不确定度。

$$H(Y \mid X) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p(x_{i}y_{j}) \log p(y_{j} \mid x_{i})$$

$$= -\sum_{i=1}^{n} p(x_{i}) \sum_{j=1}^{m} p(y_{j} \mid x_{i}) \log p(y_{j} \mid x_{i})$$

$$= -\sum_{i=1}^{n} p(x_{i}) H(Y \mid x_{i})$$

$$= E[H(Y \mid x_{i})]$$

 $H(Y | X = x_i)$ 表示在已知 $X = x_i$ 的情况下,Y的平均不确定性。

对于不同的 x_i , $H(Y | X = x_i)$ 是变化的。因此, $H(Y | X = x_i)$ 是一个随机变量。

例6: 已知联合概率分布如下,求: $\underline{H(XY)}$, $\underline{H(X)}$,



解: 1)
$$H(XY) = -\sum_{i} \sum_{j} p(x_{i}y_{j}) \log p(x_{i}y_{j})$$

= $-0.25 \log 0.25 - 0.10 \log 0.10 - ...$
= 2.665

2)
$$\begin{bmatrix} X \\ P \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ 0.25 & 0.40 & 0.15 & 0.15 & 0.05 \end{bmatrix}$$
 $H(X)=2.066$

3)
$$\begin{bmatrix} \mathbf{Y} \\ \mathbf{P} \end{bmatrix} = \begin{bmatrix} \mathbf{y}_1 & \mathbf{y}_2 & \mathbf{y}_3 & \mathbf{y}_4 \\ 0.35 & 0.35 & 0.20 & 0.10 \end{bmatrix}$$
 $H(Y)=1.856$

4)
$$H(Y|X) = -\sum_{i} \sum_{j} p(x_{i}y_{j}) \log p(y_{j}|x_{i})$$
 $p(y_{j}|x_{i}) = \frac{p(x_{i}y_{j})}{p(x_{i})}$

$$H(Y|X) = -0.25 \log 1 - 0.10 \log \frac{1}{4} - 0.30 \log \frac{3}{4} - \dots$$
$$= 0.600$$

$$H(X|Y) = -0.25 \log \frac{5}{7} - 0.10 \log \frac{2}{7} - 0.30 \log \frac{6}{7} - \dots$$

= 0.809

各种熵之间的关系

熵的可加性

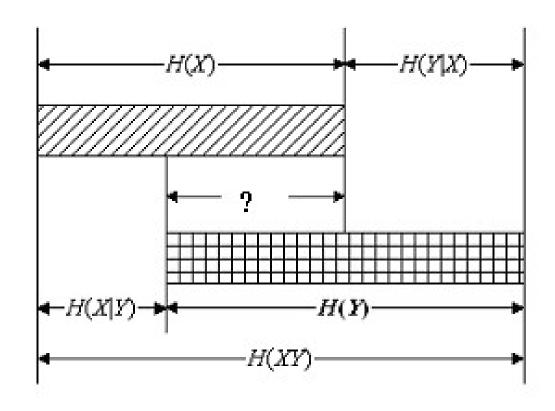
- H(XY)=H(X)+H(Y|X)=H(Y)+H(X|Y)
- $H(X|Y) \leq H(X)$, $H(Y|X) \leq H(Y)$

熵的不增原理

H(*XY*)≤*H*(*X*)+*H*(*Y*)
 若*X*与*Y*统计独立,则*H*(*XY*)=*H*(*X*)+*H*(*Y*)

可推广到多个随机变量的情况:

$$H(X_1X_2...X_N)$$
= $H(X_1) + H(X_2 | X_1) + H(X_3 | X_1X_2) + ... + H(X_N | X_1X_2...X_{N-1})$



$$? = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X) = H(X) + H(Y) - H(XY)$$

加权熵

引入事件的重量,度量事件的重要性或主观价值。

$$\begin{bmatrix} X \\ P \\ W \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ p(x_1) & p(x_2) & \dots & p(x_n) \\ w_1 & w_2 & \dots & w_3 \end{bmatrix}$$

加权熵定义为:

$$H_W(X) = -\sum_{i=1}^n w_i p(x_i) \log p(x_i)$$

例7: 信源 $X=\{A,B,C\}$, 信源 $Y=\{D,E,F,G\}$, 已知条件概率分布和X的概率分布,求联合熵和条件熵。

P(Y X)	D	Е	F	G	P(X)
A	1/4	1/4	1/4	1/4	1/2
В	3/10	1/5	1/5	3/10	1/3
С	1/6	1/2	1/6	1/6	1/6

解:

P(XY)	D	Е	F	G
A	1/8	1/8	1/8	1/8
В	1/10	1/15	1/15	1/10
C	1/36	1/12	1/36	1/36
P(Y)	91/360	33/120	79/360	91/360

$$H(XY) = 3.41$$

 $H(X) = 1.46$ $H(Y) = 1.99$
 $H(Y|X) = 1.95$ $H(X|Y) = H(XY) - H(Y) = 1.42$