# 第 9 讲 信道容量

信道容量

信道容量的几个例子

无噪声二元信道

二元对称信道

二元擦除信道

对称信道

并联信道

信道容量的性质

一些关键定义

信道容量
信道容量的几个例子
无噪声二元信道
二元对称信道
二元擦除信道
对称信道
并联信道
信道容量的性质
一些关键定义

**定义 1.1**

离散信道是由输入字母表 $\mathcal{X}$，输出字母表 $\mathcal{Y}$ 和概率转移矩阵 $p(y|x)$ 构成的系统，其中 $p(y|x)$ 表示发送字符 $x$ 的条件下收到输出字符 $y$ 的概率. 如果输出的概率分布仅依赖于它的所对应的输入，而与先前信道的输入或者输出条件独立，就称这个信道是无记忆的.

**定义 1.2**

离散无记忆信道的“信息”信道容量定义为

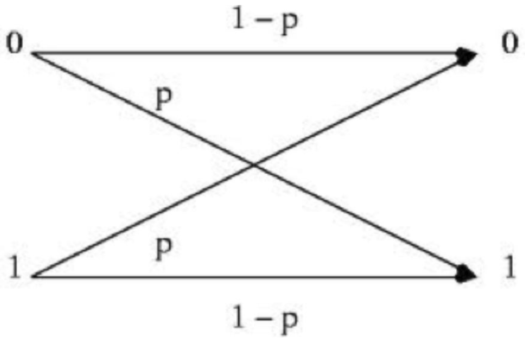
$$C = \max_{p(x)} I(X;Y).$$

这里的最大值取自所有可能的输入分布 $p(x)$.

信道容量
信道容量的几个例子
无噪声二元信道
二元对称信道
二元擦除信道
对称信道
并联信道
信道容量的性质
一些关键定义

对于无噪声二元信道，它的二元输入在输出端能精确地重现.
在这种情况下，任何一个传输的比特都能被无误差地接收到. 因此，每次使用该信道，都可以毫无误差地传输一个比特，信道容量就是一个比特. 当然，也可以计算得到信道容量 $C = \max I(X;Y) = 1$比特，且在 $p(x) = (\frac{1}{2}, \frac{1}{2})$ 时达到.

考虑下图所示的二元对称信道. 这个二元信道的输入字符以概率 $p$ 互补. 这是一个有误差信道的最简单模型.




在出现错误时，发出的信息 0 接受到的结果是 1，或者正好相反. 从接收到的比特我们并不能看出哪里发生了错误. 从某种意义上说，所有接收到的比特都不可靠. 我们稍后将证明，我们仍然可以使用这样的通信信道以非 0 的传输码率发送信息，并且误差概率可以任意小.

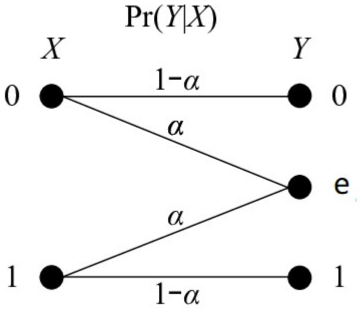
我们可以给出互信息的一个界

$$
\begin{aligned}
I(X;Y) &= H(Y) - H(Y|X) \\
&= H(Y) - \sum p(x)H(Y|X=x) \\
&= H(Y) - \sum p(x)H(p) \\
&= H(Y) - H(p) \\
&\leq 1 - H(p).
\end{aligned}
$$

其中最后一个不等式成立是因为 $Y$ 是一个二元随机变量．当输入分布是均匀分布时等号成立．因此，参数为 $p$ 的二元对称信道的信道容量为

$$C = 1 - H(p) \text{ 比特.}$$

有一种信道类似于二元对称信道，会损失一些比特（不是被损坏），这种信道称为二元擦除信道. 在二元擦除信道中，比例为 $\alpha$ 的比特被擦除掉，并且接收者知道是哪些比特已经被擦除掉了. 如下图所示，二元擦除信道有两个输入和三个输出.



我们尝试利用和二元对称信道类似的方法, 计算二元擦除信道的容量如下:

$$
\begin{aligned}
C &= \max_{p(x)} I(X;Y) \\
&= \max_{p(x)}(H(Y) - H(Y|X)) \\
&= \max_{p(x)} H(Y) - H(\alpha).
\end{aligned}
$$

初看，似乎 $H(Y)$ 的最大值是 $\log 3$. 但是实际上在绝大多数情况下 (除了 $\alpha = 1/3$ 时)，无论如何选取初始分布 $p(x)$，我们都无法让 $H(Y)$ 达到这个值. 所以我们需要另辟蹊径.

设 $E$ 代表事件 $\{Y=e\}$，设 $P(X=1)=\pi$，由表达式

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

我们有

$$H(Y)=H((1-\pi)(1-\alpha),\alpha,\pi(1-\alpha))=H(\alpha)+(1-\alpha)H(\pi).$$

因此

$$\begin{aligned} C &= \max_{p(x)} H(Y)-H(\alpha) \\ &= \max_{\pi}(1-\alpha)H(\pi)+H(\alpha)-H(\alpha) \\ &= \max_{\pi}(1-\alpha)H(\pi) \\ &= 1-\alpha. \end{aligned}$$

其中，当 $\pi=1/2$ 时，达到该信道容量.

信道容量
信道容量的几个例子
无噪声二元信道
二元对称信道
二元擦除信道
对称信道
并联信道
信道容量的性质
一些关键定义

二元对称信道是 $C = 1 - H(p)$ 比特/传输，二元擦除信道的容量是 $C = 1 - \alpha$ 比特/传输. 下面考虑具有如下转移矩阵的信道：

$$p(y|x) = \begin{bmatrix} 0.3 & 0.2 & 0.5 \\ 0.5 & 0.3 & 0.2 \\ 0.2 & 0.5 & 0.3 \end{bmatrix}$$

上述矩阵中的第 $x$ 行第 $y$ 列的元素表示条件概率 $p(y|x)$，即传输 $x$ 收到 $y$ 的概率. 在该信道中，概率转移矩阵中所有的行都可以通过其他行置换得到，每一列也如此. 这样的信道称为对称的.

**例 3.1**

另一个对称信道的例子是

$$Y = X + Z \pmod{c}$$

其中 $Z$ 服从整数集 $\{0, 1, 2, \cdots, c-1\}$ 上的某个分布，$X$ 与 $Z$ 拥有相同的字母表，并且 $Z$ 独立于 $X$.

设 $\mathbf{r}$ 表示转移矩阵中的一行，则有

$$I(X;Y) = H(Y) - H(Y|X) = H(Y) - H(\mathbf{r}) \leq \log|\mathcal{Y}| - H(\mathbf{r}),$$

当输出是均匀分布时等号成立. 而且，$p(x) = 1/|\mathcal{X}|$ 可以使 $Y$ 达到均匀分布，这可以由如下式子看出

$$p(y) = \sum_{x\in\mathcal{X}} p(y|x)p(x) = \frac{1}{|\mathcal{X}|}\sum p(y|x) = c\frac{1}{|\mathcal{X}|} = \frac{1}{|\mathcal{Y}|}$$

其中 $c$ 是概率转移矩阵的一列中所有元素之和，不难证明 $c = \frac{|\mathcal{X}|}{|\mathcal{Y}|}$.

**定义 3.2**

如果信道转移矩阵 $p(y|x)$ 的任何两行互相置换；任何两列也互相置换，那么称该信道是对称的. 如果转移矩阵的每一行 $p(\cdot|x)$ 都是其它每行的置换，而所有列的元素和 $\sum_x p(y|x)$ 相等，则称这个信道是弱对称的.

**定理 3.3**

对于弱对称信道，

$$C = \log|\mathcal{Y}| - H(\text{转移矩阵的行}),$$

当输入字母表上的分布为均匀时达到该容量.

我们考虑两个信道 $\{\mathcal{X}_1, p_1(y_1|x_1), \mathcal{Y}_1\}$ 和 $\{\mathcal{X}_2, p_2(y_2|x_2), \mathcal{Y}_2\}$ 并联后的信道容量 $C$，其中要求每次发送字符时，要么是通过信道 1，要么是通过信道 2 发送，而不能同时发送，假定两者的输出字母表不相交.

**命题 4.1**

$$2^C = 2^{C_1} + 2^{C_2}.$$

**证明.**
我们考虑下面的信道：

$$X = \begin{cases} X_1 & \text{概率}\alpha \\ X_2 & \text{概率}(1-\alpha). \end{cases}$$

设

$$\theta(X) = \begin{cases} 1 & X = X_1 \\ 2 & X = X_2 \end{cases}$$

**证明.**

由于 $\mathcal{Y}_1 \cap \mathcal{Y}_2 = \emptyset$，我们有 $X \to Y \to \theta$，从而

$$\begin{aligned} I(X;Y,\theta) &= I(X;\theta) + I(X;Y|\theta) \\ &= I(X;Y) + I(X;\theta|Y). \end{aligned}$$

由 $\mathcal{Y}_1 \cap \mathcal{Y}_2 = \emptyset$ 我们有 $I(X;\theta|Y) = 0$，从而

$$\begin{aligned} I(X;Y) &= I(X;\theta) + I(X;Y|\theta) \\ &= H(\theta) - H(\theta|X) + \alpha I(X_1;Y_1) + (1-\alpha) I(X_2;Y_2) \\ &= H(\alpha) + \alpha I(X_1;Y_1) + (1-\alpha) I(X_2;Y_2). \end{aligned}$$

于是我们不难得出

$$C = \sup_{\alpha} \{H(\alpha) + \alpha C_1 + (1-\alpha) C_2\}.$$

**证明.**

于是我们把问题化归为求函数最值问题. 不难验证，当 $H'(\alpha)+C_1-C_2=0$ 时，即 $\alpha=2^{C_1}/(2^{C_1}+2^{C_2})$ 时达到最大值，此时

$$2^C=2^{C_1}+2^{C_2}. \qquad \square$$

- 由 $I(X;Y) \geq 0$ 我们知 $C \geq 0$.
- 由于 $C = \max I(X;Y) \leq \max H(X) \leq \log|\mathcal{X}|$，所以 $C \leq \log|\mathcal{X}|$.
- 同理知 $C \leq \log|\mathcal{Y}|$.
- $I(X;Y)$ 是关于 $p(x)$ 的一个连续函数.
- $I(X;Y)$ 是关于 $p(x)$ 的凹函数. 由于 $I(X;Y)$ 是闭凸集上的凹函数，因此局部最大值也是全局最大值. 最大值可以利用标准的非线性最优化技术求解.

信道容量
信道容量的几个例子
无噪声二元信道
二元对称信道
二元擦除信道
对称信道
并联信道
信道容量的性质
一些关键定义

取自下标集 $\{1,2,\cdots,M\}$ 的消息 $W$，产生信号 $X^n(W)$，这个信号以随机序列 $Y^n \sim p(y^n|x^n)$ 的方式被接收者收到. 然后，接收者使用适当的译码规则 $\hat{W}=g(Y^n)$ 猜测消息 $W$. 如果 $\hat{W}$ 与所传输的消息 $W$ 不同，则表明接受者出错. 下面我们严格定义这些思路.

**定义 5.1**

用 $(\mathcal{X}, p(y|x), \mathcal{Y})$ 表示的离散信道由两个有限集 $\mathcal{X}$ 和 $\mathcal{Y}$ 以及一簇概率密度函数 $p(y|x)(x\in\mathcal{X})$ 构成，其中对任意 $x$ 与 $y$，有 $p(y|x)\geq 0$，以及对任意的 $x$，有 $\sum_y p(y|x)=1$，而 $X$ 和 $Y$ 分别看作信道的输入和输出.

**定义 5.2**

离散无记忆信道 (DMC) 的$n$ 次扩展是指信道 $(\mathcal{X}^n, p(y^n|x^n), \mathcal{Y}^n)$，其中

$$p(y_k|x^k, y^{k-1}) = p(y_k|x_k), \ \ k = 1, 2, \cdots, n.$$

## 注记 5.3

如果信道不带反馈，也就是说，如果输入字符不依赖于过去的输出字符，即 $p(x_k|x^{k-1}, y^{k-1}) = p(x_k|x^{k-1})$，那么离散无记忆信道的 $n$ 次扩展的信道转移函数就可以转化为

$$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i).$$

为证明上式，我们首先注意到

$$p(y^n|x^n) = p(y_n|y^{n-1}, x^n)p(y^{n-1}|x^n) = p(y_n|x_n)p(y^{n-1}|x^n).$$

为计算 $p(y^{n-1}|x^n)$，我们利用下式

$$p(y^{n-1}|x^n)p(x_n|x^{n-1}) = p(y^{n-1}, x_n|x^{n-1}) = p(x_n|y^{n-1}, x^{n-1})p(y^{n-1}|x^{n-1}).$$

注意到信道不带反馈，$p(x_n|x^{n-1}) = p(x_n|y^{n-1}, x^{n-1})$. 从而

$$p(y^{n-1}|x^n) = p(y^{n-1}|x^{n-1}).$$

再利用归纳法我们可得所需结论.

**定义 5.4**

信道 $(\mathcal{X}, p(y|x), \mathcal{Y})$ 的 $(M, n)$ 码由以下部分构成:

1. 下标集 $\{1, 2, \cdots, M\}$.
2. 编码函数 $X^n : \{1, 2, \cdots, M\} \to \mathcal{X}^n$，生成码字 $x^n(1), x^n(2), \cdots, x^n(M)$. 所有码字的集合称作码簿.
3. 译码函数
$$g : \mathcal{Y}^n \to \{1, 2, \cdots, M\}$$
其为一个确定性规则，为每个收到的字符向量指定一个猜测.

**定义 5.5: 条件概率误差**

设

$$\lambda_i = P\{g(Y^n) \neq i | X^n = x^n(i)\} = \sum_{y^n} p(y^n | x^n(i)) I(g(y^n) \neq i)$$

为已知下标 $i$ 被发送的条件下的条件误差概率，其中 $I(\cdot)$ 为示性函数.

## 定义 5.6

$(M,n)$ 码的最大误差概率 $\lambda^{(n)}$ 定义为

$$\lambda^{(n)} = \max_{i\in(1,2,\cdots,M)} \lambda_i.$$

## 定义 5.7

$(M,n)$ 码的平均误差概率 $P_e^{(n)}$ 定义为

$$P_e^{(n)} = \frac{1}{M}\sum_{i=1}^{M} \lambda_i.$$

**定义 5.8**

$(M, n)$ 码的码率定义为

$$R = \frac{\log M}{n} \text{ 比特/传输.}$$

**定义 5.9**

如果存在一个 $(\lceil 2^{nR} \rceil, n)$ 码序列，满足当 $n \to \infty$ 时，最大误差概率 $\lambda^{(n)} \to 0$，则称码率 $R$ 是可达的.

**定义 5.10**

信道的容量定义为所有可达码率的上确界.