第五章离散信道编码

第二节有噪信道编码定理

陈兴同

中国矿业大学 数学学院

2021 年 8 月

内容提要

内容提要

定理 5.2.1: 编码定理

有噪离散无记忆信道编码与传输模型如图 5-1，它的编码定理是仙农信息论中的第二个基本定理，它指出了信道编码时应当遵守的基本原则。

*（**信道编码定理**）设离散无记忆信道的容量为 C 个 D 进制单位，如果码率 $R \leq C$，则当 n 充分大时，总存在一系列 (D^{nR}, n) 信道码使得译码错误 P_e 可以任意的小。*

这是信道编码定理的一般形式，它的证明需要用到联合典型序列法，可参考文献 [10,20] 中相关章节。

定理 5.2.2：二进信道编码定理

对二进对称信道来说，信道编码定理可以叙述为如下定理。

设二进对称信道中传错概率 $0 < p < 0.5$，再设 ϵ, δ 是两个任给正数，则当 n 足够大时，一定存在长度为 n 的二进码满足

（1） *码率从左侧接近信道容量 $C = 1 - h(p)$，即 $C - \epsilon \leq R < C$。*

（2） *最小汉明距离译码方法译码错误 $P_e < \delta$。*

这个定理证明仍然比较长，有兴趣同学可以参考文献 [19] 中第五章。

信道编码逆定理:5.2.3

设离散无记忆信道的容量为 C 个 D 进制单位，如果给定码率 $R > C$，则不论 n 多么大，都不可能存在一种 (D^{nR}, n) 信道码使得译码错误 P_e 任意小。

Fano 不等式:定理5.2.4

为了证明信道的逆定理，需要用到 Fano 不等式，这个不等式描述的是两个定义在同样字符空间中的随机变量相互确认时不确定性的上界。

设随机变量 $W, \hat{W}$ 定义在字符空间 $\mathcal{W} = \{1, 2, \cdots, M\}$ 中两个随机变量，则如下概率

5.6

$$P_e = P\left\{\mathcal{W} \neq \hat{\mathcal{W}}\right\} \tag{2.1}$$

满足不等式

5.7

$$H(W|\hat{W}) \leq h(P_e) + P_e \log(M-1), \qquad \cancel{(2.2)}$$

*其中 $h(x)$ 是熵函数（??）*1.23。

证明:

记联合概率与条件概率为

$$p(j,k) = P\left\{W=j, \hat{W}=k\right\}, p(j|k) = P\left\{W=j|\hat{W}=k\right\},$$

则有

$$P_e = \sum_{j=1}^{M}\sum_{k=1,k\neq j}^{M} P\left\{W=j, \hat{W}=k\right\} = \sum_{j=1}^{M}\sum_{k=1,k\neq j}^{M} p(j,k). \tag{2.3}$$

5.8

根据条件熵及熵函数（1-23）得

$$\begin{aligned} & H(W|\hat{W}) - h(P_e) - P_e \log(M-1) \\ &= -\sum_{j=1}^{M}\sum_{k=1}^{M} p(j,k)\log p(j|k) + \sum_{j=1}^{M}\sum_{k=1,k\neq j}^{M} p(j,k)\log P_e \\ &+ \sum_{j=1}^{M} p(j,j)\log(1-P_e) - \sum_{j=1}^{M}\sum_{k=1,k\neq j}^{M} p(j,k)\log(M-1) \end{aligned}$$

续证明：

$$
\begin{aligned}
&= \sum_{j=1}^{M} \sum_{k=1,k\neq j}^{M} p(j,k) \log \frac{P_e}{(M-1)p(j|k)} + \sum_{j=1}^{M} p(j,j) \log \frac{1-P_e}{p(j|j)} \\
&\leq \sum_{j=1}^{M} \sum_{k=1,k\neq j}^{M} p(j,k) \left[\frac{P_e}{(M-1)p(j|k)} - 1 \right] + \sum_{j=1}^{M} p(j,j) \left[\frac{1-P_e}{p(j|j)} - 1 \right] \\
&= \frac{P_e}{M-1} \sum_{j=1}^{M} \sum_{k=1,k\neq j}^{M} p_{\hat{W}}(k) + (1-P_e) \sum_{k=1}^{M} p_{\hat{W}}(k) - \sum_{j=1}^{M} \sum_{k=1}^{M} p(j,k) \\
&= \frac{P_e}{M-1} \sum_{j=1}^{M} [1 - p_{\hat{W}}(j)] + (1-P_e) - 1 = 0.
\end{aligned}
$$

所以不等式（5-7）成立。

改写平均译码错误:

根据信道模型图 5-1，W 是信道编码器输入，$X^{(n)}$ 是信道输入，$Y^{(n)}$ 是信道输出，$\hat{W}$ 是信道译码器输出，则可以形成马氏链 $W \to X^{(n)} \to Y^{(n)} \to \hat{W}$，译码器其实就是由信道输出 $Y^{(n)}$ 确定信道编码器输入消息的过程，即 $\hat{W} = g(Y^{(n)})$，这里 g 就是译码准则。因此概率（5-8）还可以写成如下形式

$$
\begin{aligned}
P_e &= \sum_{j \neq k} P\left\{W = j, \hat{W} = k\right\} = \sum_{j=1}^{M} \sum_{k=1, k\neq j}^{M} P\left\{W = j\right\} P\left\{\hat{W} = k | W
\right. \\
&= \sum_{j=1}^{M} P\left\{W = j\right\} \sum_{k=1, k\neq j}^{M} P\left\{\hat{W} = k | W = j\right\} = \sum_{j=1}^{M} P\left\{W = j\right\} e_j
\end{aligned}
$$

它正好就是信道编码的平均译码错误（5-4）。这样就可以将 Fano 不等式应用于信道编码逆定理的证明中了。

引理 5.2.1：

设字符串 $X^{(n)}$ 经过离散无记忆信道（如图??5.1）的输出字符串为 $Y^{(n)}$，该信道容量为 C，则有 $I\left(X^{(n)};Y^{(n)}\right) \leq nC$。

证明：

$$
\begin{aligned}
I\left(X^{(n)};Y^{(n)}\right) &= H\left(Y^{(n)}\right) - H\left(Y^{(n)}|X^{(n)}\right) \\
&= H\left(Y^{(n)}\right) - \sum_{i=1}^{n} H\left(Y_i|Y_1,\cdots,Y_{i-1},X^{(n)}\right) \\
&= H\left(Y^{(n)}\right) - \sum_{i=1}^{n} H\left(Y_i|X_i\right) \\
&\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H\left(Y_i|X_i\right), \\
&= \sum I\left(X_i;Y_i\right) \leq nC.
\end{aligned}
$$

信道编码逆定理的证明：

在信道模型（5-1）中，对于任意编码方案，存在马氏链 $W \to X^{(n)} \to Y^{(n)} \to \hat{W}$，根据码率 R 的定义，利用数据传输不等式、Fano 不等式及引理 ?? 可得

5.2.1

$$
\begin{aligned}
nR &= H(W) = H(W|\hat{W}) + I(W;\hat{W}) \\
&\leq H(W|\hat{W}) + I(X^{(n)};Y^{(n)}) \\
&\leq h(P_e) + P_e \log(M-1) + I(X^{(n)};Y^{(n)}) \\
&\leq 1 + P_e \log(M-1) + nC,
\end{aligned}
$$

续证明：

从而得到不等式

$$P_e \geq \frac{n(R-C)-1}{\log(M-1)} > \frac{n(R-C)-1}{\log M} = 1 - \frac{C}{R} - \frac{1}{nR},$$

对于任意的 $\delta > 0$，当 $n > n_0 \geq 1/(R(1-\delta)-C)$ 时就有 $P_e > \delta$。这说明当 $R > C$ 时，不管信道码怎样编码，码长取多么大，译码误差都不会小。

信道编码定理及其逆定理说明：

（1） 只要你希望的码率不超过信道容量，就存在“好码”— 既具有高效率即接近信道容量，又具有高可靠性即平均译码错误小的信道编码。

（2） 这个定理的无论是内容还是证明都没有给出一个可行的算法来构造“好码”。

（3） 一个“好码”可能需要很长码字，这将会增加编码与译码的复杂性。