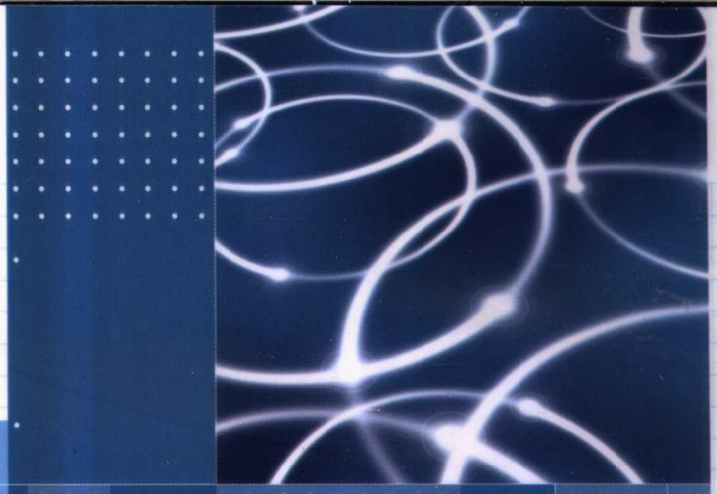

http://www.phei.com.cn

高等学校电气信息类教材

纠错编码原理和应用

张宗橙　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

高等学校电气信息类教材

纠错编码原理和应用

张宗橙　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书介绍了纠错编码的基本原理、设计方法与应用实例。全书共分 7 章，介绍了信道与编码的基本原理，近世代数中与编码相关的主要内容，线性分组码、循环码、卷积码结构及特性，网格编码调制（TCM）、级联码与 Turbo 码的设计应用等。各章原理的叙述力求突出概念和思路，尽量去除烦琐的数学推导，设计与应用尽量采用实例分析，并附有一定数量的习题。

本书可作为高等学校电气信息类专业本科高年级学生的教材，也可作为研究生和工程技术人员的参考书。

图书在版编目(CIP)数据

纠错编码原理和应用/张宗橙编著. —北京：电子工业出版社，2003.4
高等学校电气信息类教材
ISBN 7-5053-8667-0

Ⅰ. 纠… Ⅱ. 张… Ⅲ. 编码理论—高等学校—教材 Ⅳ. 0157.4

中国版本图书馆 CIP 数据核字（2003）第 029493 号

责任编辑：刘宪兰　特约编辑：方方
印　　刷：北京兴华印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：17.5　字数：472 千字
版　　次：2003 年 4 月第 1 版　2003 年 4 月第 1 次印刷
印　　数：5 000 册　　定价：23.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077

前　言

信息论是信息科学的基础理论，而纠错编码与信源编码、保密编码一起被称为信息论的“三大码”，构成了信息论的核心内容。纠错编码主要用于数字系统的差错控制，对于保证通信、存储、媒体播放和信息转移等数字传递过程的质量有着重要意义，是通信、信息类学科知识结构中不可缺少的一环。

正如现代科学技术体系分为三个层次——自然科学、技术科学和工程技术一样，纠错编码也可以从三个层次上去学习和理解：理论层次、技术层次和应用层次。目前全国开办电气信息类专业的高校不下几百所，由于基础不同、侧重不同、办学层次不同，对纠错编码的学习要求各不相同。另一方面，对于工程技术人员而言，工作性质不尽相同，有的搞研发，有的搞运维，有的搞管理，对纠错编码知识要求的深度与广度必然也是不同的。正是这种需求的多样性，产生了对纠错编码教材多层次、多样性的要求，这也就是我为什么在国内外已有不少名家大作情况下还要编写这本书的原因。

很多有关信息编码、通信原理、数字系统等的教材中均有纠错编码内容，但限于篇幅，一般只能讲些常用码结构，不讲原理与设计；另一方面，许多纠错编码的专著具有很高的学术水平，对于大多数非专业研究人员来说显得过于深奥。因此，本书从技术和工程层面来描述纠错编码的原理、设计与应用，其中原理的叙述力求突出概念和思路，尽量去除烦琐的数学推导；设计与应用则尽量具体化，采用实例分析。纠错编码理论性强，各类纠错码名目繁多，其中有的理论意义较大而实用性不强，有的过去常用而现在已趋于淘汰。有鉴于此，本书在选材上不求面面俱到，而是兼顾先进性和实用性，有重点地介绍一些主流、实用的码型，不把面铺得太宽。

本书适合高等学校电气信息类高年级学生用做教材，也可供研究生和工程技术人员作为参考教材或资料使用。

限于作者的水平，书中难免有不妥和谬误之处，敬请读者指正。

作者

目　录

第 1 章
信道与编码

1.1 信息论与编码

客观世界有三大要素：物质、能量、信息。在研究其规律之前，首先要给它们下定义，并确定度量方法。目前，虽然“信息社会”、“信息经济”等名词人人皆知，但何谓信息、如何度量却没有确切和统一的定义。倾向性的看法是：信息是认识的主体（人、生物、机器）与外部世界双向作用时所交换的内容。要对这些内容，包括通常含义下的信息（知识、情报）给出统一的量度是困难的，但要研究信息又不能没有一个量度方法。迄今为止，最成功且最普及的信息量度是香农（C.E.Shannon）在其经典著作《通信的数学理论》[1] 中提出的建立在概率论基础上的信息量度方法。他定义：“信息是不确定性的量度。”比如“太阳从东方升起”这句话，由于其发生概率为 1（必然事件），而被认为是不含信息量的废话；而“今年中秋节日全食”这句话，由于发生概率小而信息量极大。作为定义，若事件 A 发生的概率是 $P(A)$，则其自信息量定义为：

$$I(A) = -\log_2 P(A) \qquad \text{b（比特）} \tag{1-1}$$

或

$$I(A) = -\ln P(A) \qquad \text{nat（奈特）}$$

由于 $0 \leqslant P(A) \leqslant 1$，其对数为负数，所以定义时加一个负号“－”，使信息量为正值。信息量的基本单位是比特或奈特，两者的换算关系是 1b = 1.443nat。

通信过程中，传送的最小信号波形单位是符号（symbol），编码情况下也叫码元。假定有一个 8 电平码元，其电平可以是 8 个值（0,1,…,7）中的任意一个。若各电平出现的概率相等，均为 1/8，那么“码元电平值为 5”这样一个事件的自信息量是：

$$I(5) = -\log_2 \frac{1}{8} = 3\,\text{b}$$

若前后码元相互独立，单个码元 X 的平均自信息量称为 X 的信息熵，它是码元在不同取值下自信息量的加权和，定义为：

$$H(X) = E[I(x_i)] = -\sum_{x_i \in X} P(x_i) \log_2 P(x_i) \tag{1-2}$$

在码元取值等概时，一个 8 电平码的信息熵是：

$$H(x)=E[I(x_i)]=-\sum_{i=0}^{7}P(x_i)\log_2 P(x_i)=-8\cdot\frac{1}{8}\log_2\frac{1}{8}=3\,\text{b}$$

从通信的角度看，发送一个上述码元可以携带 3b 信息量。同理，如果发送一个等概、16 种电平的码元，由于不确定性更大，因而携带的信息量更大，达 4b。

若码元 X 的各电平不等概，比如发生概率为：

信号电平	0	1	2	3	4	5	6	7
出现概率	1/4	1/8	1/8	1/8	1/8	1/8	1/16	1/16

则：

$$H(X)=-\sum_{i=0}^{7}P(x_i)\log_2 P(x_i)=\left(\frac{1}{4}\times 2+5\times\frac{1}{8}\times 3+2\times\frac{1}{16}\times 4\right)=2.875\,\text{b}$$

可见，8 电平码元不一定能携带 3 bit 信息。一般规律是：当各信号等概出现时，信息熵最大。从这一点出发，编码时总是希望各码元等概取值。

香农以概率信息为基础，给出了三个定理一个公式，即

香农第一定理：无失真信源编码定理

香农第二定理：有扰离散信道的信道编码定理

香农第三定理：限失真信源编码定理

以及计算有扰信道容量的香农公式，形成了完整的理论体系。以此为基础的信息论称为香农信息论，或叫做狭义信息论。

狭义信息论中的信息是概率信息，只与信息（事件）出现的概率有关，与信息本身是否重要无关。从完美的观点看，信息理论除包含概率（信息量）因素外，还应该包含语义（信息含义）和语用（对接受者的作用大小）的因素。由于新的信息论尚在讨论之中，目前广泛使用的是狭义信息论。狭义信息论的核心内容有三大码，即信源编码、信道编码（纠错编码）和保密编码（Cryptographic Encoding）。本课程研究的是纠错编码。

1.2　编码信道模型与信道容量

本节先回顾通信系统模型。在信道编码器和信道解码器之间相隔着许多其他部件，如调制解调器、放大器、滤波器、均衡器等，以及光纤、铜线、无线、微波等物理信道。这些信道受到不同类型的噪声干扰，如随机噪声、突发噪声等，使传输的信息遭受损伤。信道编码可以从窄义和广义两方面去理解。窄义信道编码的目标是使信号与信道匹配，包括频谱匹配、阻抗匹配、时基匹配等，称为线路编码（Line Code）。比如，PCM 为了消除直流分量，便于时基提取进行的 AMI 或 HDB3 编码；铜线传输中为了降低波特率、减小占用带宽而进行的 2B1Q 和 4B3T 编码；基带传输时为了有控制地利用码间干扰而设计的部分响应系统；频带调制系统为了压缩过渡带宽而施加的一定约束条件也可视做

一种编码。这种窄义的线路编码与具体物理信道有关，而从信息论的角度来看，我们对信号在信道中传输的具体物理过程不感兴趣，仅对传输的结果感兴趣，即输入什么信号、在怎样的噪声干扰下得到怎样的输出信号、差错概率的大小和分布如何、怎样从输出信号中最佳地恢复输入信号等。为了集中精力研究以上问题，把信道编、解码器之间的所有部件看成一个“黑箱（Blackbox）”，称之为广义信道，也叫做编码信道，像研究多端口网络那样把问题归结为输入、输出和转移概率矩阵三个要素，如图 1-1 所示。

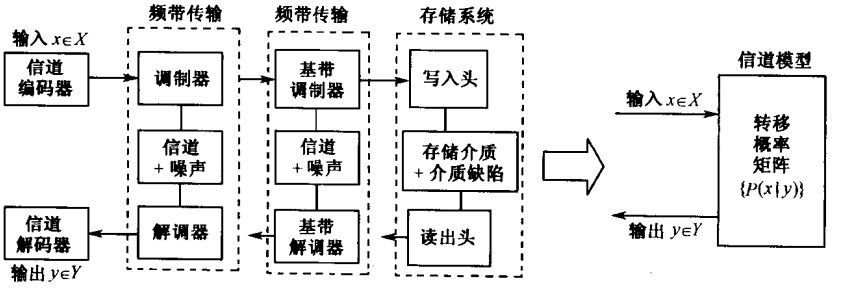

图 1-1　信道模型

其中，$X=\{x_0, x_1, \cdots, x_{q-1}\}$是包含 q 个元素的输入符号集，$Y=\{y_0, y_1, \cdots, y_{Q-1}\}$是包含 Q 个元素的输出符号集。

广义信道中，调制、均衡、滤波等终端处理一般是可预知的，信道本身的参数大多也是可测试的，最不确定的因素就是噪声干扰了。从噪声的发生规律来分，有加性和乘性两种。加性噪声的影响是做加法（噪声＋信号），它与信号的有无及大小无关，即使信号为零，它也存在。这类噪声有热噪声，以及无线电、工频、雷电、火花、电脉冲干扰等。乘性噪声的影响是做乘法（噪声×信号），信号为零时，噪声干扰影响也就不存在了。这类噪声有线性失真、交调干扰、码间干扰，以及信号的多径时变干扰等。由于不确定，只能用随机信号或随机过程的理论来研究它们的统计特性。不同类型的信道加不同类型的噪声构成了不同类型的信道模型。就噪声引发差错的统计规律而言，分为随机差错信道和突发差错信道两类。

1．随机差错信道

信道中，各码元是否出现差错，与其前、后码元是否差错无关，每个码元独立地按一定的概率产生差错。从统计规律看，可以认为这种随机差错是由加性高斯白噪声（AWGN）引起的，主要的描述参数是误码率 p。

2．突发差错信道

信道中，差错成片出现，一个差错片称为一个突发差错。突发差错总是以差错码元开头、以差错码元结尾，头尾之间并不是每个码元都错，而是码元差错概率大到超过了

某个标准值。通信系统中的突发差错是由突发噪声（比如雷电、强脉冲、时变信道的衰落等）引起的。存储系统中，磁带、磁盘物理介质的缺陷或读写头的接触不良等造成的差错均为突发差错。

实际信道中往往既存在随机差错又有突发差错，我们取其主流来研究。如果两类差错都必须考虑，可采用组合编码信道模型。

1.2.1　随机差错编码信道模型

随机差错编码信道的差错是由高斯白噪声（AWGN）引起的。根据编码信道的输入、输出是 2 电平、多电平或是模拟量（多电平电平数的极限），可分为如下编码信道模型。

1. 二进制对称信道

该信道模型有一个输入取值集合 $X=\{0,1\}$和输出值集合 $Y=\{0,1\}$，以及一组表示输入、输出关系的条件概率（转移概率）。如果 AWGN 导致统计独立的差错且条件概率对称，即

$$P(Y=0|X=1)=P(Y=1|X=0)=p \qquad (1\text{-}3)$$
$$P(Y=1|X=1)=P(Y=0|X=0)=1-p$$

则称这种对称二进制输入、二进制输出的编码信道为二进制对称信道，简写为 BSC，其信道模型如图 1-2 所示。由于这种信道的输出仅与对应时刻的输入有关，与前、后输入无关，我们说这种信道是无记忆的。当图 1-1 所示通信系统采用二进制调制，检测器实行门限硬判决且信道对称时，就可以用 BSC 编码信道模型描述它。BSC 是研究二元编解码最简单、最常用的信道模型。

若转移概率不对称，即 $P(Y=0|X=1)\neq P(Y=1|X=0)$，称这样的信道为 Z 信道。

2. 离散无记忆信道

BSC 可视为一种更广义的离散输入、离散输出信道的特例。假设信道编码器的输入是 q 元符号，即输入符号集由 q 个元素 $X=\{x_0, x_1,\cdots, x_{q-1}\}$构成；检测器的输出是 Q 元符号，即信道输出符号集由 Q 个元素 $Y=\{y_0, y_1,\cdots, y_{Q-1}\}$构成；且信道和调制过程是无记忆的，那么图 1-1 所示信道模型“黑箱”的输入—输出特性可以用一组共 qQ 个条件概率来描述：

$$P(Y=y_j|X=x_i)=P(y_j|x_i)=p_{ij} \qquad (1\text{-}4)$$

式中，输入 $i=0, 1, \cdots, q-1$，输出 $j=0, 1, \cdots, Q-1$，三种表达式等效。这样的信道称为离散无记忆信道，简写为 DMC（Discrete Memoryless Channel），其示意图如图 1-3 所示。

若 DMC 信道的输入、输出是一个由 n 个符号组成的序列，其中输入序列的 n 个符号 $u_1, u_2, \cdots, u_n$选自符号集 X（$u_i\in X$），对应的 n 个输出符号 $v_1, v_2, \cdots, v_n$选自符号集 Y，

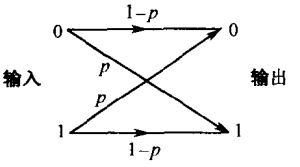

图 1-2　二进制对称信道（BSC）

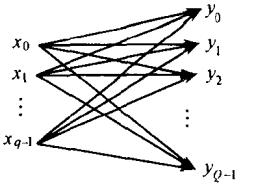

图 1-3　离散无记忆信道（DMC）

即 $v_i \in Y$，则联合条件概率是：

$$P(Y_1=v_1, Y_2=v_2, \cdots, Y_n=v_n \mid X_1=u_1, \cdots, X_n=u_n) = \prod_{k=1}^{n} P(Y_k=v_k \mid X_k=u_k) \tag{1-5}$$

这个表达式正是满足无记忆条件的数学表述。

条件概率$\{P(y_j \mid x_i)\}$决定了 DMC 特征，可以写成矩阵形式 $\boldsymbol{P}=[p_{ij}]$。根据定义，式中的 $p_{ij} \equiv P(y_j \mid x_i)$，$\boldsymbol{P}$ 称为信道的转移概率矩阵。

$$\boldsymbol{P}=\begin{bmatrix} P(y_0 \mid x_0) & P(y_1 \mid x_0) & \cdots & P(y_{Q-1} \mid x_0) \\ P(y_0 \mid x_1) & P(y_1 \mid x_1) & \cdots & P(y_{Q-1} \mid x_1) \\ \vdots & \vdots & & \vdots \\ P(y_0 \mid x_{q-1}) & P(y_1 \mid x_{q-1}) & \cdots & P(y_{Q-1} \mid x_{q-1}) \end{bmatrix} = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,Q-1} \\ p_{10} & p_{11} & \cdots & p_{1,Q-1} \\ \vdots & \vdots & & \vdots \\ p_{q-1,0} & p_{q-1,1} & \cdots & p_{q-1,Q-1} \end{bmatrix} \tag{1-6}$$

在信道输入为 x_i 的条件下，由于干扰的存在，信道输出不是一个固定值，而是概率各异的一组值，这种信道就叫做有扰离散信道。显然，输入 x_i 时，各可能输出值 y_j 的概率之和必定等于 1，即

$$\sum_{j=0}^{Q-1} P(y_j \mid x_i) = 1 \qquad i=0, 1, \cdots, q-1 \tag{1-7}$$

如果信道转移概率矩阵的每一行中只包含一个“1”而其余元素均为“0”，说明信道无干扰，称之为无扰离散信道。

3. 离散输入、连续输出信道

假设信道输入符号选自一个有限的、离散的输入符号集 $X=\{x_0, x_1, \cdots, x_{q-1}\}$，而信道（检测器）输出未经量化（$Q=\infty$），这时的译码器输入可以是实轴上的任意值，即 $Y=\{-\infty, \infty\}$。定义这样的信道模型为离散时间无记忆信道，它的特性由离散输入 X、连续输出 Y 以及一组条件概率密度函数 $p(y \mid X=x_i)$，$i=0,1,\cdots,q-1$ 来决定。这类信道中最重要的一种是加性高斯白噪声（AWGN）信道，对它而言，

$$Y=X+G \tag{1-8}$$

式中，G 是一个零均值、方差为σ^2的高斯随机变量，$X=x_i$, $i=0,1,\cdots,q-1$。

当 X 给定后，Y 是一个均值为 x_i 、方差为σ^2的高斯随机变量，

$$P(y \mid x_i) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(y-x_i)^2/2\sigma^2} \tag{1-9}$$

在分析问题时，选用何种信道模型完全取决于研究的目的。如果研究兴趣在于工程实现，最常用的是 DMC 信道模型或其简化形式 BSC 模型。从译码角度来看，BSC 是硬判决，DMC 是软判决。若想分析编解码器性能的理论极限，或者说软判决性能的理论极限，可选用离散时间无记忆信道。

1.2.2 随机差错编码信道容量

任何一种编码信道模型的通信能力都不是无限的，其极限值就叫做信道容量。几种信道模型通信容量的分析如下。

1. DMC 信道的容量

考虑一个 DMC 信道，其输入符号集是 $X=\{x_0, x_1, \cdots, x_{q-1}\}$，输出符号集是 $Y=\{y_0, y_1, \cdots, y_{Q-1}\}$，转移概率为 $P(y_j|x_i)$，如式（1-4）的定义。若发送信号是 x_i，接收到的信号是 y_j，那么由事件 $Y=y_j$ 的发生而提供的关于 $X=x_i$ 的互信息是 $\log_2[P(y_j|x_i)/P(y_j)]$，这里，

$$P(y_j)=P(Y=y_j)=\sum_{i=0}^{q-1}P(x_i)P(y_j|x_i) \tag{1-10}$$

把输出 Y 对输入 X 提供的平均互信息定义为：

$$I(X;Y)=\sum_{i=0}^{q-1}\sum_{j=0}^{Q-1}P(x_i)P(y_j|x_i)\log_2\frac{P(y_j|x_i)}{P(y_j)} \tag{1-11}$$

转移概率 $P(y_j|x_i)$是由信道特征决定的，而输入符号的发生概率受离散信道编码器的控制。对于一组输入符号概率 $P(x_i)$而言，$I(X;Y)$的最大值仅仅取决于由条件概率 $P(y_j|x_i)$ 决定的 DMC 信道的特性。$I(X;Y)$的最大值定义为信道容量，用符号 C 来表示：

$$C=\max_{P(x_i)}I(X;Y)=\max_{P(x_i)}\sum_{i=0}^{q-1}\sum_{j=0}^{Q-1}P(x_i)P(y_j|x_i)\log_2\frac{P(y_j|x_i)}{P(y_j)} \tag{1-12}$$

C 的单位是信道上每传送一个符号（每使用一次信道）所能携带的比特数，即比特/符号（bit/symbol 或 bit/channel use）。以上 $I(X;Y)$值的最大化是在下列限制条件下进行的：

$$P(x_i)\geqslant 0$$

$$\sum_{i=0}^{q-1}P(x_i)=1 \tag{1-13}$$

如果每符号周期是 T 秒，也可用“秒”为单位来计算信道容量，此时 $C_s=C/T$，信道容量的单位是比特每秒（b/s）。

转移概率矩阵 $\boldsymbol{P}$ 已知后，由式（1-12）计算 DMC 信道容量的关键是找出能使 $I(X;Y)$ 最大的 $P(x_i)(i=0,1,\cdots,q-1)$的概率分布。若将输入符号发生概率写成矩阵形式 $\boldsymbol{P}_x=[P(x_0), P(x_1),\cdots, P(x_{q-1})]$，称之为输入概率矢量，则由式（1-12）及关系式：

$$I(X;Y)=H(X)-H(X|Y)=H(Y)-H(Y|X) \tag{1-14}$$

可得：

$$C=\max_{P(x_i)} I(X;Y)=\max_{P(x_i)}[H(X)-H(X|Y)]=\max_{P(x_i)}[H(Y)-H(Y|X)] \qquad (1\text{-}15)$$

式（1-14）的物理意义是：从输出 Y 得到的关于输入 X 的平均互信息等于 X 本身的信息熵 $H(X)$ 减去由信道造成的不确定性即条件熵 $H(X|Y)$。

这里存在两个问题，第一个问题是信道容量存在性，即 $I(X;Y)$ 的最大值是否存在？如果最大值存在，就产生第二个问题：如何才能找到它？

第一个问题可用存在性定理来回答。

存在性定理　给定转移概率矩阵 $\boldsymbol{P}$ 后，平均互信息 $I(X;Y)$是输入概率矢量 $\boldsymbol{P}_x$ 的上凸函数（证明略）。

该定理说明：若用 $I(\boldsymbol{P}_x)$表示 I 是 $\boldsymbol{P}_x$ 的函数，则 $I\sim\boldsymbol{P}_x$ 曲线是上凸的，其极值就是信道容量，极值点所在位置的 $\boldsymbol{P}_x$ 就是取得信道容量所要求的输入概率矢量。

以下从简到繁来分析信道容量的计算。

（1）BSC 信道的容量

由于 $C=\max_{P(x_i)} I(X;Y)$，可见信道容量与输入符号的概率分布有关。对于转移概率 $P(0|1)=P(1|0)=p$ 及 $P(0|0)=P(1|1)=1-p$ 的 BSC 信道而言，当输入概率 $P(0)=P(1)=0.5$ 时，其平均互信息最大。代入式（1-12），BSC 的信道容量是：

$$\begin{aligned}C&=P(0)P(0|0)\log_2[P(0|0)/P(0)]+P(0)P(1|0)\log_2[P(1|0)/P(1)]\\&\quad+P(1)P(0|1)\log_2[P(0|1)/P(0)]+P(1)P(1|1)\log_2[P(1|1)/P(1)]\\&=p\log_2 2p+(1-p)\log_2 2(1-p)\qquad \text{b/符号}\end{aligned} \qquad (1\text{-}16)$$

C 随 p 变化的曲线如图 1-4 所示。注意，$p=0$ 时的信道容量 $C=1$（b/符号），$p=1/2$ 时的信道容量是零，且信道容量以 $p=1/2$ 点为中心对称。

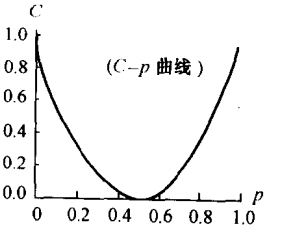

图 1-4　二进制信道的信道容量

从信息论的角度来看，式（1-14）的条件熵 $H(X|Y)$ 可以解释为由于信道干扰和噪声所造成的平均信息量的损伤。如果 BSC 信道中 $P(0|1)=P(1|0)=p=0$，即无误码，那么从接收的 Y 可完全确定发送的 X，信道的介入不产生任何不确定性。式（1-14）中 $H(X|Y)=0$，于是 $I(X;Y)=H(X)$，说明互信息等于输入符号的信息熵，即信道上传送的信息量正是输入信号的信息量。二进制等概符号的信息量是 $H(X)=1$b/符号，所以图 1-4 中，$p=0$ 时的信道容量 $C=1$。

若 $p=0.5$，说明接收的 Y 完全与发送的 X 无关，即 $H(X|Y)=H(X)$。式（1-14）中，$I(X;Y)=H(X)-H(X)=0$，信道容量 $C=0$，即信道上没有传送任何信息。

（2）对称 DMC 信道的容量

如果转移概率矩阵 $\boldsymbol{P}$ 的每一行都是第一行的置换（包含同样元素），称该矩阵是输

入对称的；如果转移概率矩阵 $\boldsymbol{P}$ 的每一列都是第一列的置换（包含同样元素），称该矩阵是输出对称的；如果输入、输出都对称，则称该 DMC 为对称的 DMC 信道。

可以证明，有扰的对称 DMC 信道具有如下性质：

① 条件熵 $H(Y|X)$与信道输入符号的概率分布无关，且有 $H(Y|X)=H(Y|x_i)$，$i=0,1,\cdots,q-1$。

② 当信道输入符号等概分布时，信道输出符号也等概分布；反之，若信道输出符号等概分布，信道输入符号必定也是等概分布。

③ 当信道输入符号等概分布时，对称 DMC 信道容量最大，

$$C=\log Q-H(Y|x_i)=\log Q-\sum_{j=0}^{Q-1}P(j|i)\log P(j|i) \tag{1-17}$$

由性质①，式（1-15）可化成：

$$C=\max_{P(x_i)}[H(Y)-H(Y|X)]=\max_{P(x_i)}[H(Y)-H(Y|x_j)]=\max_{P(x_i)}[H(Y)]-H(Y|x_j)$$

于是计算 C 简化为求 $\max\limits_{P(x_i)}[H(Y)]$。由信息论可知，当输出的各符号等概时，信源熵最大，即

$$H(Y)\leqslant\log Q \quad \text{或者} \quad \max[H(Y)]=\log Q \tag{1-18}$$

这就是式（1-17）的来历。

（3）准对称 DMC 信道的容量

如果转移概率矩阵 $\boldsymbol{P}$ 是输入对称而输出不对称，即转移概率矩阵 $\boldsymbol{P}$ 的每一行都包含同样的元素，而各列的元素可以不同，则称该矩阵是准对称 DMC 信道。例如，矩阵

$$\boldsymbol{P}=\begin{bmatrix}0.3 & 0.2 & 0.2 & 0.3\\ 0.2 & 0.3 & 0.2 & 0.3\end{bmatrix}$$

就是准对称的 DMC 信道。

可以证明，准对称 DMC 信道的容量为：

$$C\leqslant\log Q-\sum_{i=0}^{q-1}P(i|j)\log P(i|j) \tag{1-19}$$

当信道输入符号等概分布时，准对称 DMC 信道达到其信道容量 C。

（4）一般 DMC 信道的容量

以输入符号概率矢量 $\boldsymbol{P}_x$ 为自变量求函数 $I(\boldsymbol{P}_x)$的极大值，即信道容量计算问题，从数学上看是一个规划问题，这个问题已经解决。目前常用的方法是 1972 年由 R.Blahut 和 A.Arimoto 分别独立提出的算法，称为 Blahut-Arimoto 算法。一般地，为使 $I(X;Y)$最大化，输入概率集$\{P(x_j)\}$必须满足的充要条件是：

$$\begin{aligned}&I(x_i;Y)=C \quad \text{对于所有满足 } P(x_i)>0 \text{ 条件的 } i\\ &I(x_i;Y)\leqslant C \quad \text{对于所有满足 } P(x_i)=0 \text{ 条件的 } i\end{aligned} \tag{1-20}$$

这里

$$I(x_j;Y)=\sum_{i=0}^{q-1}P(y_i\mid x_j)\log\frac{P(y_i\mid x_j)}{P(y_i)}$$

2. 离散时间无记忆信道的容量

若 DMC 信道输出符号集 $Y=\{y_0, y_1,\cdots, y_{Q-1}\}$中 $Q\to\infty$，信道就成为离散输入、连续输出的离散时间无记忆信道。离散时间无记忆信道的容量可视做 DMC 信道软判决译码时的容量极限，具有研究价值。这类信道中最重要的是加性高斯白噪声（AWGN）信道，对它而言，离散输入 $X=\{x_0, x_1,\cdots, x_{q-1}\}$和模拟输出 $Y=\{-\infty, \infty\}$之间的最大平均互信息，即信道容量，由下式给出（单位是 b/符号）：

$$C=\max_{P(x_i)}\sum_{i=0}^{q-1}\int_{-\infty}^{\infty}P(y\mid x_i)P(x_i)\log_2\frac{P(y\mid x_i)}{P(y)}\mathrm{d}y \tag{1-21}$$

式中，

$$P(y)=\sum_{i=0}^{q-1}P(y\mid x_i)P(x_i)$$

作为特例，对于二进制输入的 AWGN 无记忆信道，若 $X=\{x_0, x_1\}=\{A, -A\}$，输入概率矢量 $\boldsymbol{P}_x=(0.5, 0.5)$。即等概输入时，平均互信息 $I(X;Y)$最大而达到信道容量，以 b/符号为单位是：

$$C=\frac{1}{2}\int_{-\infty}^{\infty}P(y\mid A)\log_2\frac{P(y\mid A)}{P(y)}\mathrm{d}y+\frac{1}{2}\int_{-\infty}^{\infty}P(y\mid -A)\log_2\frac{P(y\mid -A)}{P(y)}\mathrm{d}y \tag{1-22}$$

式中 $P(y\mid A)$，$P(y\mid -A)$和 $P(y)$ 均与信道中的噪声方差有关，C 作为 $A^2/2\sigma^2$ 比值函数的关系曲线如图 1-5 所示。注意，当比值增大时，C 在 0～1bit/符号之间单调递增。

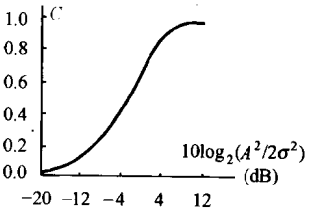

图 1-5　AWGN 无记忆信道二元输入时作为 $A^2/2\sigma^2$ 函数的信道容量

3. 带限波形信道的容量

香农（1948 年）定义一个受 AWGN 干扰、带宽为 W 的带限波形信道的容量为：

$$C=\lim_{T\to\infty}\max_{P(x_i)}\frac{1}{T}I(X;Y) \tag{1-23}$$

若把输入、输出和噪声波形 $x(t)$, $y(t)$ 和 $n(t)$ 展开成一个正交函数的完备集，可得到