高等学校教学参考书

实用纠错编码

上海铁道学院　杨　爵　郎宗棪　编

中国铁道出版社

高等学校教学参考书

实用纠错编码

上海铁道学院　杨　爵　郎宗校　编
北方交通大学　张树京　主　　审

中国铁道出版社
1988年·北京

内 容 简 介

全书共分八章：第一章为纠错编码基础，第二章为线性分组码，第三章为循环码，第四章为BCH码和哥拔码，第五章为卷积码，第六章为门限逻辑译码技术，第七章为纠算术差错码，第八章为纠突发差错码。

本书着眼于实际应用，避免涉及深奥的编码理论。具有一般工程数学基础的读者都能掌握本书内容。本书为通信、信号专业本科高年级学生作选修课教材，教学时数在65学时左右。也可供从事通信、信号及计算机专业信道编码设备设计的工程技术人员作参考。

高等学校教学参考书

实 用 纠 错 编 码

上海铁道学院　杨　爵　郎宗桢　编

中国铁道出版社出版

责任编辑　倪嘉寒　封面设计　刘景山

新华书店总店科技发行所发行

各 地 新 华 书 店 经 售

北京通县张家湾印刷厂印

开本：787×1092毫米 1/32　印张：10.875　字数：282 千

1 9 8 8 年 3 月 第 1 版　第 1 次印刷

印数：0001— 5,000册　定价：1.80元

前　言

纠错编码是随着通信和遥控技术的数字化和自动数据处理机的广泛使用而日益受到重视的。其基本原因是：

1. 联网计算机及其远程终端由于资源共享而极大地增加了数据高速传输的需要。对传输精确性的要求越来越高，传统技术已不能将出错概率降低到要求的标准因而只能借助于纠错编码技术。

2. 同步通信卫星的广泛应用推动了传输速率的极大提高。由于卫星通信的功率和带宽都受到严格限制，就必须充分利用信道资源以获得较大的经济效益。而纠错编码就是使数字技术在确保高度精确性要求前提下充分利用信道资源的有力手段。

集成电路的迅猛发展和价格的大幅度下降及其继续下降的趋势使得纠错编码技术的广泛使用变成了现实。在过去二十年间，高效、灵活和无差错数字通信系统已得到大量使用。为使纠错编码技术能在我国社会主义四化建设中发挥较大的作用，本书着重从实际应用方面对纠错编码技术作了有选择的介绍。对一些在实际中得到应用但功能较差，技术也较简单的码一般不作介绍，对于一些有理论价值，但实际使用在技术上还有困难的码也不作介绍。本书的读者对象主要是通信专业，尤其是着重数字通信，计算机通信和遥控技术方面的高年级本科大学生作选修课用。本书也适合从事编译码设备设计和数字通信系统设计的通信工程师工作时的参考。

本书内容的第一章对纠错编码基础作一概括性介绍。第

二章介绍线性分组码。第三章介绍线性分组码中应用最广的循环码。第四章介绍纠多位错循环码中占主要地位的 BCH 码。第五章介绍和分组码完全不同的卷积码。第六章介绍译循环码和卷积码都十分有效的门限逻辑译码技术。以上各章涉及的都是二元序列。第七章介绍纠正二进制数差错的纠算术差错码。从第二章到第七章都着眼于抗高斯白噪声干扰所引起的随机差错。第八章则着重介绍抗脉冲干扰所引起的突发差错技术。

对于本书书稿的完成，首先要感谢北方交通大学校长张树京教授，承他在百忙中主审了书稿并提出了许多宝贵的意见。由于我们水平有限，错误和不妥之处望读者批评指正。

目　录

第一章　纠错编码基础

本章第一节介绍熵、互信息量和信道容量等信息论的一些基本概念。目的是建立起信息论和纠错编码的直接联系。第二节从信道容量与信道传输速率的关系出发，着重介绍香农噪声编码定理。以及与此直接关联的编码后出错概率的计算公式。最后用一实例阐明香农噪声信道编码定理的现实意义。第三节介绍纠错编码原理，这就是用添加不携带信息量的余裕码元的办法以构成相关性很强的码字，接着介绍通信系统的组成，这就是信源、信道编码器、调制器、噪声信道、解调器和信道译码器。第四节介绍三种差错控制方式，这就是前向纠错，自动回询重传和混合纠错。侧重点是自动回询重传。第五节介绍几种信道模型，这就是二进制对称信道，二进制删除信道，Z信道和记忆信道的马尔柯夫过程。应该注意，信道模型不但和差错类型有关，而且也和判决方法有关。第六节简略介绍纠错编码的分类。如何进行分类还没有统一标准，各书说法很不一致。提出的目的只是使读者对众多的码有一个总体印象。

第一节　熵、互信息量和信道容量

虽然本书的目的是研究在噪声信道上纠错编码的有关方面。但是先了解信息论和纠错编码有关的几个重要结果会有助于对纠错编码的理解。

假定数据是从无记忆信源产生的。所谓无记忆指的是信源任一输出a_i和其先前以及后续输出都没有关系。信源输出

可看成是信源状态的时间序列

$$A=(a_1,\ a_2,\ \cdots,\ a_i,\ \cdots)$$

其每一状态a_i的取值是按概率规律取自信源有限字符集X。

$$X=(x_1,\ x_2,\ \cdots,\ x_N)$$

最常用的信源字符集是只有两个元素的信源，其字符集

$$X=(0,\ 1)$$

如果0和1的概率相等，则称为二进制对称信源（BSS）。它在任何时刻都随机地发送1码元或0码元，例如发送二元序列

$$A=1,1,0,0,1,0,1,1,\cdots$$

一、信息与熵

设信源输出的符号取值于$X=\{x_1,\ x_2,\ \cdots,\ x_n\}$，则收到$x_i$时的信息量为它出现的概率的负对数。即

$$I(x_i)=-\log_a p(x_i) \qquad (1-1)$$

这里$p(x_i)$是信源状态的概率。对数的底a是任意的。由于当今世界大量使用二进制数字计算机和二进制数传系统，对数的底通常是2，这时信息量的单位是bit（比特）。

由（1—1）式看到，信息量是信源状态概率的单调减函数。事件概率越小，其负对数就越大，表示它的出现提供了大量信息，随着出现概率的增大，所提供的信息量越来越小。如果某一状态x_i出现的概率接近于1，它的负对数接近于零，只能提供极少的信息。

在实际应用时，重要的不是某一状态的信息量，而是信源全部状态的平均信息量。平均信息量叫做熵。离散无记忆信源（DMS）的熵为

$$H(X)=-\sum_{i=1}^{N}p(x_i)\log p(x_i) \qquad (1-2)$$

例如设二进制对称信源输出字符1和0的概率分别为α

及$1-\alpha$。则它的熵为

$$H(\alpha)=-\alpha\log_2\alpha-(1-\alpha)\log_2(1-\alpha) \quad (1-3)$$

其熵函数$H(p)$如图 1 — 1 所示。它对称于$\alpha=\frac{1}{2}$且在这时有最大值 1 。不管信源输出有多少状态，只有当它们都以等概出现时，信源的熵才有最大值。即

若 $p(x_i)=\frac{1}{N}$，全部 i

则

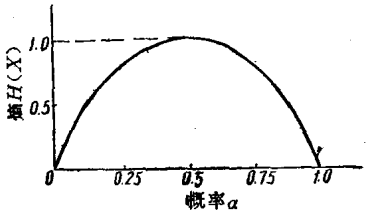

图 1 — 1　离散二进制信源的熵

$$H(X)_{max}=-\sum_{i=1}^{N}\frac{1}{N}\log_2\frac{1}{N}=\log_2 N \quad (1-4)$$

二、互信息量和信道容量

对于一个有N个输入和M个输出的信道，可用一组转移概率$p(y_j\mid x_i)$，$1\leqslant i\leqslant N$，$1\leqslant j\leqslant M$确定。这里x_i和y_j分别表示信道输入和输出。这一组转移概率可用矩阵表示成

$$P(Y|X)=\begin{pmatrix} p(y_1|x_1) & p(y_2|x_1) & \cdots & p(y_M|x_1) \\ p(y_1|x_2) & p(y_2|x_2) & \cdots & p(y_M|x_2) \\ \vdots & \vdots & & \vdots \\ p(y_1|x_N) & p(y_2|x_N) & \cdots & p(y_M|x_N) \end{pmatrix} \quad (1-5)$$

我们定义信道输入和信道输出之间的互信息量为

$$I(X;Y)=\sum_{i=1}^{N}\sum_{j=1}^{M}p(x_i,y_j)\log_2\frac{p(x_i,y_j)}{p(x_i)p(y_j)} \quad (1-6)$$

$$=\sum_{i=1}^{N}\sum_{j=1}^{M}p(x_i,y_j)\left[\log_2\frac{1}{p(x_i)}\right.$$

$$+\log_2\frac{p(x_i,y_j)}{p(y_j)}\Big] \qquad (1-7)$$

但

$$\sum_{i=1}^{M} p(x_i,y_j)=p(x_i)$$

$$\frac{p(x_i,y_j)}{p(y_j)}=p(x_i|y_j)$$

因此

$$I(X;Y)=\sum_{i=1}^{N} p(x_i)\log_2\frac{1}{p(x_i)}$$

$$-\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i,y_j)\log_2\frac{1}{p(x_i|y_j)}$$

$$=H(X)-H(X|Y) \qquad (1-8)$$

前一项是信源的熵，或称为无条件熵，它是信源的平均不肯定度。后一项是在给定信道输出Y的条件下信源的条件熵，或者给定Y的条件下信源的平均不肯定度。两者之差是互信息量，它是经由信道所通过的信息量的量度。

用类似的推导可以证明，信道输入端和输出端的互信息量可表示成

$$I(X;Y)=H(Y)-H(Y|X) \qquad (1-9)$$

这里

$$H(Y|X)=\sum_{i=1}^{N}\sum_{j=1}^{M} p(x_i,y_j)\log_2\frac{1}{p(y_j|x_i)} \qquad (1-10)$$

互信息量的最大值是信道容量。由于信道固定不变，只能改变信源输入才能使之最大。

例如二进制对称信道BSC。设信源发送0码元的概率为a，信道转移概率为

$$p(0|1)=p(1|0)=p$$

$$p(1|1)=p(0|0)=1-p$$

则 $$H(Y)=-\alpha\log_2\alpha-(1-\alpha)\log_2(1-\alpha)$$

$$H(Y|X)=-\alpha(1-p)\log_2(1-p)-\alpha p\log_2 p$$
$$-(1-\alpha)(1-p)\log_2(1-p)-(1-\alpha)p\log_2 p$$
$$=-p\log_2 p-(1-p)\log_2(1-p)=H(p)$$

$$I(X;Y)=H(Y)-H(p) \qquad (1-11)$$

当$\alpha=1/2$即信源输出是等概的时，$I(X;Y)$为最大。因此

$$C=1+p\log_2 p+(1-p)\log_2(1-p) \qquad (1-12)$$

当$p=0$或1时，信道容量等于1。当$p=1/2$时，信道容量等于0。二进制对称信道模型及其信道容量分别见图1—2和图1—3。$p=0$或1时，输出完全由输入决定，如果输入每码元携带1比特的信息量，输出也携带相同的信息量，因此信道容量为每码元1比特。当$p=1/2$时，信道输出与输入无关，因此信道容量为0。

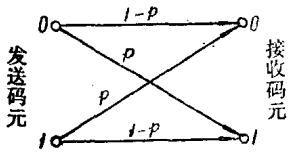

图1—2 二进制对称信道

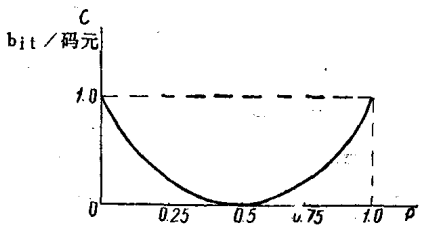

图1—3 二进制对称信道的信道容量

例1—1 卫星通信链路包括三个基本信道，即上链路、卫星上的信号处理设施和下链路，假定上链路出错概率为0.01，信号处理设施出错概率可以略去不计，下链路因为卫星发送功率受限，出错概率较大，假定为0.1。则三个信道的信道容量分别是

$$C_1=1+0.01\log_2 0.01+0.99\log_2 0.99$$

$$=0.9192\text{bit/码元}$$

$$C_2=1.0\text{bit/码元}$$

$$C_3=0.5310\text{bit/码元}$$

为了求整个链路的信道容量，必须首先确定总的差错转移概率矩阵。

$$P(Y|X)=\begin{pmatrix}0.99 & 0.01\\ 0.01 & 0.99\end{pmatrix}\begin{pmatrix}1.00 & 0\\ 0 & 1.00\end{pmatrix}\begin{pmatrix}0.90 & 0.10\\ 0.10 & 0.90\end{pmatrix}$$

$$=\begin{pmatrix}0.892 & 0.108\\ 0.108 & 0.892\end{pmatrix}$$

因此整个链路的信道容量是

$$C=1+0.892\log_2 0.892+0.108\log_2 0.108$$

$$=0.5061\text{bit/码元}$$

第二节　噪声信道编码定理

香农证明，在噪声信道上如果信源用固定速率R发送信息，而信道容量为C，当$R<C$时，存在有编码和调制方案，使译码的差错概率达到任意小。当$R>C$时，信道编码（纠错编码）只能降低通信系统的效能。

（1—12）式的信道容量是以每码元多少比特表示的。它可以轻易地转换成每秒多少比特。这只要乘以每秒多少码元就可以了。对于高斯白噪声信道，信道容量

$$C=B\log_2\left(1+\frac{P}{N_0B}\right)\text{bit/s}\qquad(1-13)$$

式中　B——信号带宽；

P——接收信号功率；

N_0——单边带噪声功率谱密度。

（1—13）式通常叫做香农-哈特利（Shannon Hartley）

定律。将（1—13）式稍微改变一下形式。在信道容量处，每一比特的能量是

$$E_b=\frac{P}{C}$$

则（1—13）式化为

$$C/B=\log_2\left(1+\frac{E_bC}{N_0B}\right) \qquad (1—14)$$

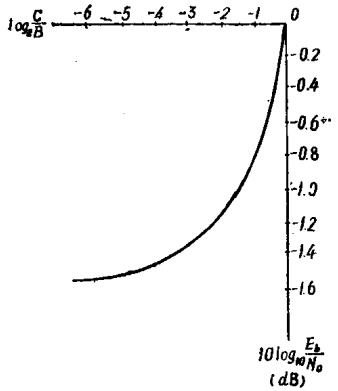

图1—4 功率受限区 E_b/N_0与C/B关系曲线

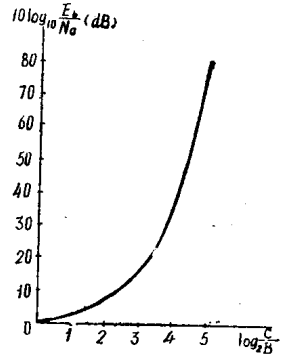

图1—5 带宽受限区 E_b/N_0与C/B关系曲线

（1—14）式可用图1—4和图1—5表示。当$C<B$时，E_b/N_0和C/B的关系曲线由图1—4表示，重要的结果是当$B\to\infty$时，E_b/N_0趋近于ln2，用dB来表示就是−1.6dB，这一数值通常称为香农界。这个区域称为功率受限区。当$C>B$时，E_b/N_0和C/B的关系曲线如图1—5所示。若C/B为任意大，则E_b/N_0也任意大。这一区域称为带宽受限区。上面两图说明：仅当E_b/N_0高于−1.6dB时，才能工作于信道容量处。当工作在低于信道容量处，即$R<C$时，出错概率P_e为

$$P_e\leqslant 2^{-nE_r(R)} \qquad (1—15)$$

这里 n 是码长，$E_r(R)$ 称为可靠性函数或随机编码指数。它随着 R 接近于 C 而单调下降，当 $R=C$ 时，$E_r(R)\to 0$。对于二进制对称信道，

$$E_r(R)=-R+\ln 2-\ln(1+2\sqrt{p(1-p)}) \qquad (1-16)$$

如果是线性分组码，则

$$P_e=\sum_{k=2}^{N} e^{W_k \ln 2\sqrt{p(1-p)}} \qquad (1-17)$$

这里 N 是码字集的码字总数。W_k 是非零码字重量。

（1—16）式是在所有码长为 n 的码的集合上的平均值，所以不够理想。对 $E_r(R)$ 的进一步研究结果可用图 1—6 来说明。图中有一条上界曲线和一条下界曲线，当 R 超过临界值 $R_{临界}$ 时上下界曲线合在一起。当 $R=C$ 时 $E_r(R)=0$，这时 $P_e=1$。

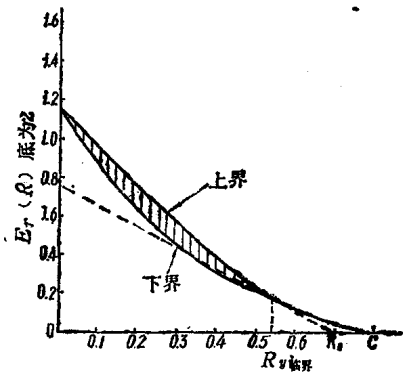

图 1—6　$p=0.01$ 时 BSC 的 $E_r(R)$

最后我们用一个简单的例子来说明香农的噪声信道编码原理。假定信源每单位时间发送 $R=1/3$ 码元，信道每单位时间传输 1 码元。则信源发送的每一码元可在信道中传送 3 次。接收端用多数表决的方法判断发送的是什么码元，设原始码元出错概率为 p，重传 3 次后出错码元的概率降为

$$P_e=3p^2(1-p)+p^3=3p^2-2p^3 \qquad (1-18)$$

因为 $p<\frac{1}{2}$，故有 $P_e<p$。这就改善了信道传送码元的可靠

性。当p很小时，改善的程度是惊人的。重复发送的次数越多，可靠程度就越高。如果重复发送$(2n+1)$次，即$R=1/(2n+1)$。则当出错$(n+1)$或更多次时接收端才会错译。则

$$P_e^{(2n+1)}=\binom{2n+1}{n+1}p^{n+1}+p\text{的更高阶次项}\quad(1-19)$$

只要p足够小，P_e就随着n的增加而很快趋近于零。但是应看到，重复发送n次所传输的信息量和发送一次所传输的信息量相同，编码效率R只为原来的$1/n$。注意信源每单位时间发送的码元数也用R表示，它们的意义并不相同。但从余裕码元（不携带信息的码元）的角度观察，它们是统一的。整个纠错编码的基础就是用增加余裕码元来使出错概率降到希望的数值。

上述关于重复码出错码元概率P_e随重复次数n而显著下降的结论是在每一码元的信噪比维持不变的条件下得出的。目的是用来示明香农噪声编码定理。如果信息元的发送机功率及发送速率固定不变，则编码后每一码元的功率及持续时间都下降到$1/n$，信噪比明显下降，导致系统效能明显变坏。这是必须注意的。正是因为这样，纠错编码才需要寻求更有效的编码理论和其实现方案。

第三节　纠错编码原理与通信系统模型

香农噪声编码定理仅是存在定理，它并没提出使出错概率达到任意小的有效途径。纠错编码就是用来纠正噪声信道中的差错。但迄今还没有哪一种码能达到香农定理的极限。通常通信系统有对容许出错概率的一定要求，并且要求经济合理且能用现有元件实现，通常是在携带消息的二元序列（信息序列）后面按一定规则添加若干余裕码元（校验元）构成相关性很强的码字。这些码字相互间的差别性（距离）