信道编码

（修订版）

刘玉君编著

河南科学技术出版社

信 道 编 码

（修 订 版）

刘玉君 编 著

河南科学技术出版社

内 容 提 要

本书比较详细地论述了信道编码理论和主要纠错码类的编、译码原理。内容包括：数学预备知识；线性分组码、循环码、BCH 码和卷积码等主要纠错码类的编、译码原理，译码算法和实现方法；最后两章着重介绍纠突发错误编、译码技术和扰乱器。本书可作为高等院校通信、计算机等专业的高年级本科生、研究生教材和参考书，也可供从事通信与计算机等工作的技术人员参考。

信 道 编 码

（修 订 版）

刘玉君 编著

责任编辑 袁元

河南科学技术出版社出版发行

解放军信息工程大学印刷厂印刷

787×1092 毫米 16 开本 23 印张 589 千字

1992 年 6 月第 1 版 2001 年 9 月第 2 次印刷

印数：3001—5000 册

ISBN 7-5349-1090-0/G・252

定 价：(精)59.80 元

前　言

信道编码是二十世纪40年代末提出、60年代发展起来的一门提高数据传输可靠性的理论与技术，至今已有50余年的历史。随着数字通信的发展，特别是70年代以来，随着卫星通信和高速数据网的飞速发展，对数据传输的可靠性提出了越来越高的要求，因此，如何提高数据传输的可靠性已成为一个迫切需要解决的问题。

在有扰信道上传输数字数据时，所收到的数据将不可避免地含有差错。通常，用户提出一个差错率，当超出此差错率时，接收数据即不予使用。若采用信道编码技术，则可将差错减少到容许的限度以内。因此说，信道编码是用来改善数字通信可靠性的一种信号处理技术。

代数理论为信道编码提供了理论基础，大规模集成电路和微型计算机的发展为信道编码技术的应用开拓了广阔的前景。我们将会看到，随着我国四化建设的飞速发展，信道编码技术将得到更加广泛的应用。

本书是在笔者所编的《信道编码分析》和《信道编码》两套教材的基础上，经过多年试用修改并加进了笔者近年来的研究成果编写而成的。全书共分九章，包括以下内容：

第一、二两章分别介绍了学习“信道编码”所需要的数学知识和信道编码理论中的一些基本概念。

线性分组码是信道编码中最基本的一类码，它有明显的数学结构，是讨论各类码的基础，因此我们首先在第三章中介绍了线性分组码，并讨论了三个基本码限和两类基本线性分组码——汉明码和RM码。

为了使编、译码手续更为简单，多年来人们一直致力于分组码的研究，希望找到一种编、译码较易实现的分组码，而循环码就是这样的码。因此，我们在第四章介绍了循环码的基本理论及其编、译码实现电路。

BCH码是一类纠多个随机错误的循环码，它纠错能力强，构造方便，编码简单，译码也较易实现，在编码理论中起着重要作用。因此我们在第五章对BCH码作了较为详细的论述，对主要的译码算法的原理和实现方法作了系统介绍，特别对BCH码的迭代译码原理及译码算法的改进进行了深入的讨论，并对RS码的频域编、译码方法作了简单介绍。

1954年里德(Reed)在译RM码时首先提出了大数逻辑译码的思想，以后许多编码工作者推广并发展了这一算法。1963年梅西(Massey)首先把大数逻辑译码算法予以系统化，并提出了软判决的大数逻辑译码。因此，我们在第六章中对循环码的大数逻辑译码作了系统的介绍，并对软判决的大数逻辑译码，即APP算法作了推广工作，提出了L步APP门限译码算法。

卷积码是区别于分组码的又一种新型信道编码，它广泛应用于卫星通信中，从性能上讲优于一般的分组码。因此，我们在第七章中详细论述了卷积码的有关概念，对卷积码的代数译码和维特比译码算法进行了较为深入的讨论，并用不变因子分解定理，从理论上彻底解决了非系统卷积码中由生成多项式矩阵求解监督多项式矩阵的问题和非系统卷积码的译码恢复问题.

许多实际信道中所产生的错误大部分是突发性的，或是突发错误与随机错误并存的。针对

这类信道，需要设计专门用来纠突发错误的码类。因此，我们在第八章着重讨论了针对突发错误的编码技术，其中包括各种交错技术，如矩阵交错、卷积交错以及伪随机交错等，并对级连码、Turbo 码等与实际通信结合密切的重要码类作了简要介绍。

实际数字通信系统的设计通常都受待传送的数据序列统计特性的影响，为了改善数据序列的统计特性，需要调制前的预编码，这就构成了数字通信系统设计中的一种专门技术——扰乱技术。本书最后一章首先介绍了与扰乱技术有关的线性移位寄存器和 m 序列理论，然后对几种主要扰乱器作了较为详细地讨论。扰乱技术已用于 PCM 数字通信和保密通信中，所以介绍这方面的有关内容对于读者拓宽知识面和理论联系实际都是有益的。

笔者由衷地感谢窦瑞华、聂涛、党明瑞等教授以及我院、系、教研室、教保处的领导和同志们对本书的写作和出版所给予的支持、鼓励和帮助。特别是窦瑞华教授在百忙中认真审阅了初稿全文，改正了其中一些错误，并提出了许多具体的修改意见，笔者再次表示深切谢意。在本书这次修改重印过程中，北京理工大学安建平教授，对本书修改提出了许多建设性意见，我校宋惠元教授、张水莲副教授和刘建洲、巩克现、周山等同志分别对部分章节进行了认真校对，改正了其中许多错误，巩克现，赵仁才等同志为本书修改工作提供许多可靠数据，在此一并致谢。

由于笔者水平有限，书中缺点在所难免，敬请广大读者批评指正。

刘玉君

2001 年 9 月

于解放军信息工程大学

目　录

第一章　数学预备知识

信道编码理论与代数学有着密切的关系. 多项式、向量、矩阵运算以及近世代数的有关理论是研究信道编码必不可少的数学工具. 鉴于这些数学知识在有关教科书中都有详细论述，这里仅对本书常用到的一些主要数学概念，给以简要介绍.

1.1　整数的可除性

1.1.1　整除的概念

我们把 $1,2,3,\cdots,n,\cdots$ 称为自然数，并用 N 表示自然数全体所成的集合，即：

$$N=\{1,2,\cdots,n,\cdots\}.$$

显然，任意两个自然数的和与积仍然是自然数，但两个自然数相减就不一定是自然数，因为减法运算产生了零和负数. 通常我们把正整数、负整数的全体与零所成的集合称为整数集合，并用 Z 表示，即

$$Z=\{\cdots,-n,\cdots,-2,-1,0,1,2,\cdots,n,\cdots\}.$$

在整数集合 Z 中可以做加、减和乘法等运算，但除法不总是可以进行的，因为任意两个整数作除法，结果可能不再是整数.

定义 1.1　对于整数集合 Z 中任意两个数 a,b，如果存在一个 $q\in Z$，使得 $b=aq$，则称 a 整除 b，记为 $a|b$. 否则称 a 不能整除 b. 若 $a|b$，也称 a 是 b 的因数，或 b 是 a 的倍数.

下面列举有关整除的一些性质.

1° 如果 $a|b$，则 $a|(-b)$，$-a|b$，$-a|(-b)$.

有了性质 1°，我们今后只需考虑正整数和零的正因子和正倍数即可.

2° 如果 $a|b$ 及 $a|c$，则 $a|mb+nc$，$m,n\in Z$.

该性质还可以推广到有限个的情况，即

如果 $a|b_i$，$i=1,2,\cdots,n$，则

$$a\Big|\sum_{i=1}^{n}k_ib_i,\qquad k_i\in Z,i=1,2,\cdots,n.$$

3° 如果 $a|b$，$b|c$，则 $a|c$.

4° 如果 $a|b$，且 $b|a$，则 $a=b$.

5° 如果 $a|b$，$c\neq 0$，则 $ac|bc$.

6° 如果 $ac|bc$，则 $a|b$.

既然除法运算在整数集合中不总是可以进行的，那么用整数集合 Z 中一个非零整数去除 Z 中任一个整数，就有除得尽与除不尽两种可能. 下面定理给出了用 b 去除 Z 中任一个数 a 所得的结果，这就是带余除法定理.

定理 1.1　设 a,b 是整数集合 Z 中任意两个数，且 $a\neq 0$，则一定存在唯一的两个整数 q 和 r，使得

$$b=aq+r,\qquad 0\leqslant r<|a|. \tag{1.1.1}$$

1.1.2 最大公因数和最小公倍数

若 $a|b$，则 $-a|b$，及 $a|(-b)$，因此我们只讨论正整数和零的正因数及正倍数.

定义 1.2 若 d 是 a 的因数，又是 b 的因数，则 d 称为 a 与 b 的公因数；

若 m 是 a 的倍数，又是 b 的倍数，则 m 称为 a 与 b 的公倍数.

一般情况下，a 与 b 的公因数不是唯一的，它有有限多个，当然这些公因数中一定有一个最大的. 然而两个数的公倍数有无限多个，因为若 m 是 a 与 b 的公倍数，则 $2m,3m,\cdots$，等也都是 a 与 b 的公倍数，a 与 b 的公倍数中一定有一个最小的.

定义 1.3 设 a 与 b 不全为零，如果有一个 d，满足

1° $d|a,d|b$；

2° 若 e 是 a 与 b 的公因数，则有 $e|d$.

我们就称 d 是 a 与 b 的最大公因数，记为 $d=(a,b)$，或者 $d=\mathrm{GCD}(a,b)$.

最大公因数是我们今后经常用到的，因此下面给出最大公因数的一些简单性质.

1° $d|a$ 与 $d|b$ 同时成立的充分必要条件是 $d|(a,b)$.

2° 设 $(a,b)=d$，则 $(ka,kb)=kd$；

若 $k|a,k|b$，则 $\left(\frac{a}{k},\frac{b}{k}\right)=\frac{(a,b)}{k}$.

3° $(a,b)=d$ 的充分必要条件是 $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

4° 如果 $(a,b)=d$，则一定存在一对整数 u,v，使得

$$ua+vb=d, \tag{1.1.2}$$

而且还可以进一步要求 u,v 适合条件

$$0\leqslant u<\frac{b}{d},\qquad 0\leqslant |v|<\frac{a}{d}.$$

其中 $a\cdot b\neq 0,a\neq b$，且适合上述条件的 u,v 是唯一的.

定义 1.4 设 a,b 不全为零，如果 a,b 的一个公倍数 m 具有如下性质：a 与 b 的任何一个公倍数都是 m 的倍数，则 m 叫做 a 与 b 的最小公倍数，记为 $m=[a,b]$ 或 $m=LCM(a,b)$.

定义 1.5 如果两个数 a 与 b 的最大公因数是 1，即 $(a,b)=1$，则称 a 与 b 是互素的.

类似性质 4°，我们有

5° 如果 $(a,b)=1$，则存在一对整数 u 和 v 使得

$$ua+vb=1,$$

其中 $0\leqslant u<b,0\leqslant |v|<a(a\neq 0,b\neq 0$，且 a,b 不全为 1)，而且 u,v 是唯一确定的.

6° 如果 $a|b\cdot c$，且 $(a,b)=1$，则 $a|c$.

7° 如果 $a|c,b|c$，且 $(a,b)=1$，则 $a\cdot b|c$.

8° 如果 $(a,c)=1,(b,c)=1$，则 $(a\cdot b,c)=1$.

定义 1.6 如果一个大于 1 的整数 a，除了 1 和它本身以外，没有其它因数，则 a 称为素数，大于 1 不是素数的数叫做合数.

素数有以下性质：

1° 对于一个素数 p 和任一个整数 a，$p|a$ 或者 $(p,a)=1$，两者必有且仅有其一成立.

2° 如果一个素数 $p|a\cdot b$，则 $p|a$ 或者 $p|b$.

定义 1.7 如果一个素数 $p|a$，则 p 叫做 a 的素因子.

根据互素和素数的性质，应用数学归纳法，可以证明整数的基本定理，即因子分解唯一性

定理，这就是定理 1.2.

定理 1.2 任何一个大于 1 的整数 a 可以分解成有限个素因子 $p_1, p_2, \cdots, p_r$ 的乘积

$$a = p_1 p_2 \cdots p_r,$$

且上述分解是唯一的，这就是说，如果还有一种分解

$$a = q_1 q_2 \cdots q_s,$$

其中 p_i 和 q_i 都是素数，则 $r=s$ 且将 q_i 的脚标作适当调换之后可使

$$q_1 = p_1, \quad q_2 = p_2, \quad \cdots, \quad q_r = p_r.$$

最后，我们还可以得到两个整数 a 与 b 的最大公因数和最小公倍数之间的关系.

定理 1.3 设两个整数 a 与 b 的最大公因数和最小公倍数分别为 (a,b) 和 $[a,b]$，则有

$$a \cdot b = (a,b) \cdot [a,b].$$

1.1.3 欧几里德算法

如何求两个数的最大公因数是我们今后经常遇到的问题. 求两个数的最大公因数的常用方法是辗转相除法，即欧几里德(Euclid)算法. 欧几里德算法是以下面定理为基础的.

定理 1.4 若 $a>b>0$，且

$$a = bq + r, \qquad 0 < r < b, \tag{1.1.3}$$

则 $(a,b)=(b,r)$.

根据这个定理可以把求两个较大数 a 与 b 的最大公因数的问题化成求两个较小数 b 与 r 的最大公因数的问题. 由此得到用辗转相除法求两个数的最大公因数的方法.

定理 1.5(Euclid) 设 $a>b>0$，那么

$$\left.\begin{aligned} a &= bq_1 + r_1, && 0 < r_1 < b; \\ b &= r_1 q_2 + r_2, && 0 < r_2 < r_1; \\ r_1 &= r_2 q_3 + r_3, && 0 < r_3 < r_2; \\ &\cdots\cdots \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, && 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} &= r_{n-1} q_n. \end{aligned}\right\} \tag{1.1.4}$$

则 $(a,b)=(b,r_1)=(r_1,r_2)=\cdots(r_{n-2},r_{n-1})=(r_{n-1},0)=r_{n-1}$.

该定理告诉我们，在对 a,b 作辗转相除时，最后一个余数 r_{n-1} 就是要求的最大公因数.

求有限多个数的最大公因数可以用连续求两个数的最大公因数的方法来完成，具体办法是，在求 n 个数的最大公因数时，首先从它们当中任意挑出两个数，求它们的最大公因数，然后再求这个最大公因数与其它 $n-2$ 个数的最大公因数，这样就把求 n 个数的最大公因数的问题化成求 $n-1$ 个数的最大公因数的问题，如此反复作下去，最后求得 n 个数的最大公因数.

1.2 同余式和欧拉-费尔马定理

1.2.1 整数按模运算

设 n 是任意给定的正整数，a 是一个整数，用 n 去除 a 得到的商为 q，余数为 r，于是有

$$a = nq + r, \qquad 0 \leqslant r < n. \tag{1.2.1}$$

我们知道，q 和 r 是由 a 和 n 唯一确定的，为此引入符号 $(a)_n$，它表示用 n 去除 a 所得的余数，因此(1.2.1)式可以写成

$$a = nq + (a)_n.$$