信 道 编 码

刘玉君 编著

河南科学技术出版社

前　言

信道编码是本世纪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40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以及改进意见进行了深入的讨论，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。

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，并对非系统卷积码的译码恢复问题进行了系统研究。

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。

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详细讨论。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。在本书写作和定稿过程中，我院宋惠元副教授以及左金明、张水莲等同志审阅了全部或部分章节初稿，提出了许多宝贵意见，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

1992年5月于解放军信息工程学院

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等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尽论述，这里仅对本书常用到的一些重要数学概念给以简要介绍，许多严格证明都已略去。

1.1　整数的可除性

1.1.1　整除的概念

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

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

自然数、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中可以作加、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　整数集合Z中任意两个数a和b，如果存在一个$q\in Z$，使得$a=bq$，则称b整除a，记为$b\mid a$。否则称b不能整除a。若$b\mid a$，也称b是a的因数，或a是b的倍数。

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$b\neq 0$，则一定存在唯一的两个整数q和r，使得

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

1.1.2　最大公因数和最小公倍数

若$b\mid a$，则$-b\mid a$及$b\mid(-a)$，因此我们只讨论正整数和零的正因数和正倍数。

定义 1.2　若d是a的因数，又是b的因数，则称d是a与b的公因数。若m是a的倍数，又是b的倍数，则称m为a与b的公倍数。

一般地，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，因而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° $d\mid a$，$d\mid b$　；

2° 若e是a与b的任一个公因数，则有$e\mid d$；

那么就称d是a与b的最大公因数，记为$d=(a,\ b)$，或者$d=\mathrm{GCD}(a,\ b)$。

定义 1.4　设a与b不全为零，如果a与b的一个公倍数有如下性质：a与b的任一个公倍

数都是m的倍数，则m称为a与b的最小公倍数，记为$m=[a,\ b]$，或者$m=\mathrm{LCM}(a,\ b)$。

最大公因数是我们今后经常用到的，这里我们列举有关它的一些简单性质。

1° $d \mid a$与$d \mid b$的充分必要条件是$d \mid (a,\ b)$；

2° $(a,\ b)=d$的充分必要条件是$(\frac{a}{d},\ \frac{b}{d})=1$；

3° 如果$d=(a,\ b)$，则一定存在一对整数u，v使得$ua+vb=d$，而且还可以进一步要求u，v适合条件：$0\leqslant u<b/d$，$0\leqslant |v|<a/d$，其中a与b均不为0，$a\neq b$。且适合上述条件的u和v是唯一的。

定义 1.5 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称为素数或质数。大于1不是素数的数称为合数。

定义 1.6 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互素。

类似性质3°，我们有

4° 如果$(a,\ b)=1$，则存在一对整数u和v，使得$ua+vb=1$，其中$0\leqslant u<b$，$0\leqslant |v|<a$，而且u与v是唯一确定的($a\neq 0$，$b\neq 0$，且a，b不全为1)。

5° 如果$a \mid bc$，且$(a,\ b)=1$，则$a \mid c$；

6° 如果$(a,\ c)=1$，$(b,\ c)=1$，则$(ab,\ c)=1$。

1.1.3 欧几里德算法

求两个数的最大公因数的常用方法是辗转相除法。该算法是以下面定理为基础的。

定理 1.2 若 $a>b>0$，且

$$a=bq+r\quad ,\qquad 0<r<b, \tag{1.1.2}$$

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。由此得到辗转相除求最大公因数的方法，即欧几里德算法。

定理 1.3（欧几里德算法） 设 $a>b>0$，

$$\begin{aligned}
a&=bq_1+r_1\quad ,\qquad 0<r_1<b;\\
b&=r_1q_2+r_2\quad ,\qquad 0<r_2<r_1;\\
r_1&=r_2q_3+r_3\quad ,\qquad 0<r_3<r_2;\\
&\cdots\cdots\\
r_{n-3}&=r_{n-2}q_{n-1}+r_{n-1}\quad ,\qquad 0<r_{n-1}<r_{n-2};\\
r_{n-2}&=r_{n-1}q_n\ 。
\end{aligned}$$

则$(a,\ b)=(b,\ r_1)=(r_1,\ r_2)=\cdots=(r_{n-2},\ r_{n-1})=(r_{n-1},\ 0)=r_{n-1}$。这就是说，最后一个余数就是要求的最大公因数。

求有限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，首先从它们当中随意挑出两个数，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，最后可求得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

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

我们知道，q和r是由a和n唯一确定的。为此引进符号$r = (a)_n$，表示a除以n的余数，于是上式可以写成

$$a = nq + (a)_n。 \tag{1.2.2}$$

设 Z 是所有整数的集合。若a，$b \in Z$，按下面规则定义a与b的和(记为$a \oplus b$)及a与b的积(记为$a \odot b$)为

$$a \oplus b = (a + b)_n\ ,\quad a \odot b = (ab)_n。 \tag{1.2.3}$$

我们把Z中的加法$\oplus$叫做模n加法，把乘法$\odot$叫做模n乘法。按此定义的运算，显然有

$$0 \leqslant a \oplus b < n\ ,\quad 0 \leqslant a \odot b < n。$$

下面给出整数按模运算的一些简单性质。

1° 设a_1，a_2是给定的两个整数，n是给定的正整数，则$(a_1)_n = (a_2)_n$的充分必要条件是 $n \mid (a_1 - a_2)$ 。

2° $(a_1 \pm a_2)_n = ((a_1)_n \pm (a_2)_n)_n\ ,\quad (a_1 a_2)_n = ((a_1)_n (a_2)_n)_n$。

3° $(a_1 + a_2 + \cdots + a_m)_n = ((a_1)_n + (a_2)_n + \cdots + (a_m)_n)_n$。

1.2.2 同余式

定义 1.7 如果任意两个整数a和b被正整数n除所得的余数相同，我们就说a与b模n同余，记为

$$a \equiv b \mod n, \tag{1.2.4}$$

否则，我们说a与b模n不同余。

下面给出两个判定a和b同余的定理。

定理 1.4 $a \equiv b \mod n$ 的充分必要条件是a可以表成$a = b + nt$。

定理 1.5 $a \equiv b \mod n$ 的充分必要条件是$n \mid a - b$。

同余式和普通等式有许多相似的性质，而且可以进行运算。下面将同余式的主要性质列举出来，以便今后应用。

1° 如果$a \equiv b \mod n$，$c \equiv d \mod n$，则$a + c \equiv b + d \mod n$，$ac \equiv bd \mod n$.

2° 如果$a \equiv b \mod n$，c为任意整数，则$ac \equiv bc \mod n$。

3° 如果$a \equiv b \mod n$，$b \equiv c \mod n$，则$a \equiv c \mod n$。

4° 如果$ac \equiv bc \mod n$，且$(c, n) = 1$，则$a \equiv b \mod n$。

5° 如果$a \equiv b \mod n$，则$(a, n) = (b, n)$。特别地，当$(a, n) = 1$时有$(b, n) = 1$。

6° 如果$a \equiv b \mod n$，d是a，b，n的一个公因数，则$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{n}{d}$。

7° 如果 $a \equiv b \mod n$，且$n_1 \mid n$，则$a \equiv b \mod n_1$。

8° 如果$a \equiv b \mod n$，且$n_1 \mid n$，$n_1 \mid a$，则$n_1 \mid b$。

1.2.3 模 n 剩余系和剩余缩系

定义 1.8 如果有n个整数r_0，r_1，…，r_{n-1}，任何两个都 mod$n$不同余，那么这n个数叫做 mod$n$的一个剩余系，每一个r_i叫做一个代表。

实际上，所有整数集合Z中元素被n除所得的余数只可能是 0，1，2，…，$n-1$，因此一个 mod$n$剩余系中只有n个两两不同的整数，即一个 mod$n$剩余系中只有n个代表。下面给出 mod$n$剩余系的一个重要性质，即如果$(a, n)=1$，则当x取遍 mod$n$剩余系中n个值时，$ax+b$也取遍 mod$n$剩余系中n个值。

定义 1.9 设r_0，r_1，…，r_{n-1}是 mod$n$的一个剩余系，从中挑出那些与n互素的全部代表，记为r_{α_1}，r_{α_2}，…，r_{α_m}，它们叫做 mod$n$的一个剩余缩系。

例 1.1 0，1，2，…，11 是 mod12 的一个剩余系，而 1，5，7，11 是 mod12 的一个剩余缩系。

最后，我们给出剩余缩系的两个性质。

1° 任何一个与n互素的整数a必和剩余缩系中一个且仅与其中一个代表 mod$n$同余。

2° 如果$(a, n)=1$，当x取遍 mod$n$剩余缩系的m个值时，ax也取遍 mod$n$剩余缩系的m个值。

1.2.4 欧拉-费尔马定理

定义 1.10 设n为任意正整数，下列n个数

$$0,\ 1,\ 2,\ \cdots,\ n-1$$

中与n互素的个数记为$\varphi(n)$，称为欧拉函数。

显然$\varphi(n)$就是 mod$n$剩余缩系中代表的个数。当n是一个较大数时，$\varphi(n)$究竟等于多少呢？下面定理给出了明确的结果。

定理 1.6 设 $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，当 $i\neq j$ 时，$p_i\neq p_j$，p_i为素数，$e_i\geqslant 1$，$(i=1, 2, \cdots, r)$，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)。\tag{1.2.5}$$

定理 1.7(欧拉-费尔马定理) 设n是大于 1 的整数，对于任意整数a，$(a, n)=1$，则

$$a^{\varphi(n)}\equiv 1 \bmod n.\tag{1.2.6}$$

特别地，当$n=p$为素数时，$\varphi(n)=p-1$，于是

$$a^p\equiv a \bmod p。\tag{1.2.7}$$

1.3 群

1.3.1 群的概念

设G是由一些元素组成的集合，a，b，…表示元素，$a\in G$表示a属于G，$a\bar{\in}G$表示a不属于G。

定义 1.11 如果集合G中任意两个元素按照一定的法则结合起来等于G中一个确定的元素，那么这个结合法则称为集合G的一个运算。

定义 1.12 一个非空集合G，对于一个称为乘法的运算“·”，如果它满足以下条件：

1° 对于G中任意三个元素a，b，c，结合律

$$(a\cdot b)\cdot c=a\cdot(b\cdot c)$$

成立;

2° 在G中存在一个单位元素e，对于G中一切元素都有

$$e\cdot a=a\cdot e=a \quad ;$$

3° 对于G中任意一个元素a，在G中都有一个称为a的逆元的元素a^{-1}存在，满足

$$a^{-1}\cdot a=a\cdot a^{-1}=e \quad ;$$

那么G对于乘法运算"$\cdot$"来说构成一个群。

由以上两个定义可以看出，要验证一个集合G对于某一结合法则是否成群，首先应验证这个结合法则是否是G的一个运算，然后还要验证它是否满足定义中的三个条件。

在一个群里，由于结合律成立，故$a_1\cdot a_2\cdot\cdots\cdot a_n$是有意义的，它是$G$中某个元素，当然也可以把$G$中$n$个相同的$a$作乘法，如果用普通乘法符号表示群的乘法运算，这样$n$个$a$作乘法可以用$a^n$表示。

定义 1.13 如果一个群G还满足交换律，即对于G中任意两个元素 a，b，都有$a\cdot b=b\cdot a$，则称G为交换群。

定义 1.14 一个群G的非空子集H，对于G中所定义的乘法运算也构成一个群，则称H为群G的子群。

1.3.2 有限群

定义 1.15 若群G中只含有限个元素，则称G为有限群，否则称为无限群。一个有限群所含元素的个数叫做这个群的阶。

定义 1.16 a是群G中任一个元素，若对于任意整数n都有$a^n\neq e$，则称a为无限阶元，否则，若有正整数n使$a^n=e$成立，则称a为有限阶元，具有性质$a^n=e$的最小正整数n称为a的阶。

我们今后经常遇到有限群，因此下面列举有限群的一些性质。

1° 若G是有限群，则G中每一个元都是有限阶元。

2° 若a是n阶元，当且仅当$n\mid m$时，$a^m=e$。

3° a，$b\in G$，G是一个有限交换群，a是m阶元，b是n阶元，且$(m,\ n)=1$，则$a\cdot b$是$m\cdot n$阶元。

4° G是有限交换群，a是G的一个n阶元，k是任意正整数，那么a^k是$\dfrac{n}{(k,\ n)}$阶元。

5° 设G是有限交换群，n阶元a是G中阶数最大的元，那么G中任一元的阶数均是n的因数。

6° 设G是有限交换群，a是G的一个n阶元，那么下面n个元

$$a^n=e,\ a,\ a^2,\ \cdots,\ a^{n-1}$$

是G中n个两两不同的元，a的任意次幂皆在其中，且$[a]=\{e,\ a,\ a^2,\ \cdots,\ a^{n-1}\}$对于$G$中的运算是一个$n$阶交换群。

1.3.3 循环群

定义 1.17 若一个群G的每一个元都是G的某一个固定元a的幂，我们就称G为循环群，也说G是由生成元a生成的群，记为$G=(a)$。

下面列举循环群的主要性质。

1° 若生成元a是n阶元，则(a)是n阶循环群。

2° 若$G=(a)$是n阶循环群，则a^k是G的一个生成元的充分必要条件是$(k, n)=1$。

3° n阶循环群G有$\varphi(n)$个生成元。特别地，当n为素数时，G有$n-1$个生成元，即G中所有非单位元的元素都是G的生成元。

4° 设$G=(a)$是一个n阶循环群，则G的任一个子群H也是一个循环群，且H中存在一个a的最小正整数次幂a^m，它生成H，即$H=(a^m)$，且有$m \mid n$。

5° 如果G是一个n阶循环群，则对于n的任一个因子m，a^m生成一个循环子群H_m，且H_m是$\frac{n}{m}$阶循环群。

1.4 域

1.4.1 域的概念

域是信道编码理论中另一个较为重要的概念，它是具有两种运算的代数系统。

定义 1.18 设F是一个非空集合，F 中规定两种运算，一个叫做加法，另一个叫做乘法，如果满足下列条件:

1° F对加法构成一个交换群;

2° F中至少有一个非零元;

3° F中非零元的全体F^*对乘法构成一个交换的乘法群;

4° 乘法和加法有分配律，$a(b+c)=ab+ac$;

则F叫做一个域。

在编码理论中我们经常遇到的是包含有限个元素的域。

定义 1.19 如果一个域只包含有限个元，则我们称它为有限域或伽罗华(Galois)域。如果这个域含有q个元，则这个域简记为$GF(q)$。

从域的定义可以看出，一个域至少含有两个元素，即零元和单位元。我们常用的正是这个最简单的域。

例 1.2 由 0 和 1 组成集合$F_2=\{0, 1\}$，F_2上的加法和乘法用下列两个表给出:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

不难验证，对于如上规定的加法和乘法F_2是一个域，我们把这个域记为$GF(2)$。事实上，$GF(2)$上的加法和乘法就是 mod2 加法和 mod2 乘法。

类似地，任取一个素数p，若

$$F_P=\{0, 1, 2, \cdots, p-1\},$$

在F_p上规定加法为 mod$p$ 加法，乘法为 mod$p$ 乘法，即如果$a+b\equiv c \pmod p$，则规定a与b的和$a+b=c$；如果$a\cdot b\equiv d \pmod p$，则规定a与b的积$a\cdot b=d$。不难证明F_p对于以上规定的加法和乘法是一个域。

例 1.3 $F_3=\{0, 1, 2\}$，在F_3上规定加法和乘法分别为 mod3 加法和乘法，$p=3$是