七彩数学

姜伯驹 主编

QICAISHUXUE

通信纠错中的数学

冯克勤□著

科学出版社
www.sciencep.com

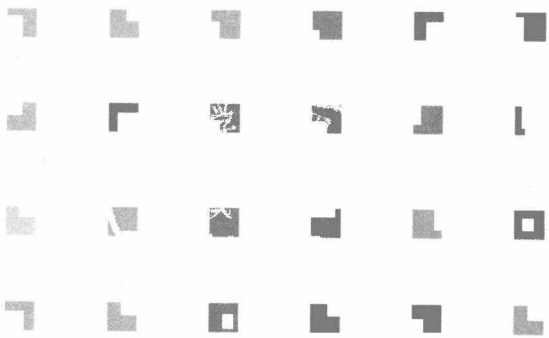
七彩数学

姜伯驹 主编

QICAISHUXUE

通信纠错中的数学

冯克勤□著



科学出版社

北京

内 容 简 介

在数字通信中如何纠正在传输中出现的错误，是保证通信可靠的重要问题. 自 1960 年以来，人们采用了许多数学工具，构作性能良好的纠错码，并且有效地运用在通信中. 本书主要介绍纠错的基本数学问题，如何用组合学、有限域和简单的线性代数知识，构作性能良好的纠错码，使读者认识到这些数学知识能有效地运用到实际当中.

本书的读者对象是高中教师和学生、信息专业的大学生，以及从事信息事业的技术人员和数学爱好者.

图书在版编目(CIP)数据

通信纠错中的数学/冯克勤著. —北京：科学出版社，2009
(七彩数学/姜伯驹主编)
ISBN 978-7-03-023518-3

Ⅰ. 通… Ⅱ. 冯… Ⅲ. 数学-普及读物 Ⅳ. O1-49

中国版本图书馆 CIP 数据核字(2009)第 185770 号

责任编辑：陈玉琢/责任校对：鲁 素

责任印制：钱玉芬/封面设计：王 浩

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2009 年 1 月第 一 版 开本：A5(890 × 1240)
2009 年 1 月第一次印刷 印张：5 7/8
印数：1—5 000 字数：85 000

定价：26.00 元

(如有印装质量问题，我社负责调换<长虹>)

丛书序言

2002 年 8 月，我国数学界在北京成功地举办了第 24 届国际数学家大会，这是第一次在一个发展中国家举办这样的大会. 为了迎接大会的召开，北京数学会举办了多场科普性的学术报告会，希望让更多的人了解数学的价值与意义. 现在由科学出版社出版的这套小丛书就是由当时的一部分报告补充、改写而成的.

数学是一门基础科学. 它是描述大自然与社会规律的语言，是科学与技术的基础，也是推动科学技术发展的重要力量. 遗憾的是，人们往往只看到技术发展的种种现象，并享受由此带来的各种成果，而忽略了其背后支撑这些发展与成果的基础科学. 美国前总统的一位科学顾问说过："很少有人认识到，当前被如此广泛称颂的高科技，本质上是数学技术."

在我国，在不少人的心目中，数学是研究古老难题的学科，数学只是为了应试才要学的一门学科. 造成这种错误印象的原因有很多. 除了数学本身比较抽象，不易为公众所了解之外，还

有学校教学中不适当的方式与要求、媒体不恰当的报道等. 但是,从数学家自身来检查,工作也有欠缺,没有到位. 向社会公众广泛传播与正确解释数学的价值,使社会公众对数学有更多的了解,是义不容辞的责任. 因为数学的文化生命的位置,不是积累在库藏的书架上,而应是闪烁在人们的心灵里.

20 世纪下半叶以来,数学科学像其他科学技术一样迅速发展. 数学本身的发展以及它在其他科学技术的应用,可谓日新月异,精彩纷呈. 然而许多鲜活的题材来不及写成教材,或者挤不进短缺的课时. 在这种情况下,以讲座和小册子的形式,面向中学生与大学生,用通俗浅显的语言,介绍当代数学中七彩的话题,无疑将会使青年受益. 这就是这套丛书的初衷.

这套丛书还会继续出版新书,诚恳地邀请数学界同行们参与,欢迎有合适题材的同志踊跃投稿. 这不单是传播数学知识,也是和年轻人分享自己的体会和激动. 当然,由于水平所限,未必能完全达到预期的目标,丛书中的不当之处,也欢迎大家批评指正.

姜伯驹

2007 年 3 月

前　言

拉格朗日认为，一个数学家，只有当他能够走出去，对他在街上碰到的第一个人清楚地解释自己的工作时，他才完全理解了自己的工作.

——贝尔(E. T. Bell)〈数学大师〉

本书向大家介绍数字通信中如何发现和纠正在传输中信息发生错误的故事. 这个故事有五十余年的历史，至今还在继续. 我们试图向读者展示数学在通信纠错方面所起的重要作用.

20 世纪 50 年代以来，数字计算机和数字通信得到极大的发展. 今天，人们从每个层面上都能感受到计算机和通信的数字化这种进步所产生的广泛而深刻的影响. 除了技术进步之外，这种发展也得益于新的数学思想和工具的运用. 连续性的(三角函数)信号变成离散性的脉冲数字信号，使得数学工具从连续性数学(傅里叶分析和拉普拉斯变换)一下子扩展到离散

性数学(组合学、数论和代数). 数字通信中提出许多具有重要应用背景的数学问题,也促进了离散性数学自身的发展,使过去不登大雅之堂的组合数学、被高斯称为"数学皇后"的过于高雅的数论以及抽象深奥的代数学走向应用,为这些学科注入了新的活力. 本书主要介绍组合学、初等数论和线性代数的基本知识,如何用来解决通信中的纠错问题. 事实上,相当高深的近代数论、代数与代数几何的研究结果对于信息领域有多方面的重大应用,有些可以说是促使通信体制发生了革命性的变化(如纠错理论中的代数几何码和信息安全方面的公开密钥体制),但是在这本通俗性读物中,只限于运用初等数论和线性代数中最基本的知识.

我们希望通过这本书,使读者感受到数学是活生生的有用的知识,感受到数学工具和数学思考方式对应用领域的重要作用,并且能够在各种工作中有意识地采用数学工具和思考方式,从而终生与数学为伴并喜欢它.

冯克勤

2006 年夏于清华大学

目　录

1 什么是纠错码?

数学家就像法国人一样,无论你对他们讲什么,他们都把它翻译成自己的语言,并且立刻成为一些全新的东西.

——歌德(Goethe)

f 是本章介绍通信的最一般化的数学模型以及纠错的数学描述. 先给出纠错的通俗例子以说明纠错的原理. 然后抽象出纠错码的 3 个基本参数:码长 n,信息位数 k 和最小距离 d. 讲述纠错码理论最基本的两个问题:构造性质好的纠错码和构造好的纠错译码算法. 用进一步的例子表明:构造好码和好的译码算法都是很有学问的,需要利用组合学,数论和代数学等方面的数学工具.

1.1 通信和纠错:数学模型

现代人们在生活中的通信方式是多种多样的,如打电话、传送电子邮件以及宇宙飞船将金星图片传回地球等. 虽然它们的形式不同,但是它们的数学模型可以表示成以下最简单的形式:

发方把信息 x 通过信道传给收方. 在有线电话系统中,电话线就是传输信息的信道. 在唐诗"烽火连三月,家书抵万金"中,烽火台燃起的烽火和邮差(驿站)分别是传递敌人入侵消息和寄送家书的信道.

要发送的信息也可以有不同的形式(声音、文字、图像、数据……). 在近几十年所发展的数字通信中,各种信息都用物理手段编成离散的脉冲信号发出,而脉冲信号只有有限多个状态. 于是,数论便派上了用场.

早在 18 世纪,大数学家欧拉在研究整数性质的过程中发明了"同余"的概念. 后来,另一

个大数学家高斯发明了同余式符号，一直沿用至今. 设 m 是正整数. 两个整数 a 和 b 叫做模 m 同余，是指 m 整除 $a-b$，即 $\frac{a-b}{m}$ 是整数. 这表示成如下同余式的形式：

$$a \equiv b(\mathrm{mod}\ m).$$

在初等数论中，如果非零整数 a 整除 b，则表示成 $a|b$. 若 a 不能整除 b，则表示成 $a\nmid b$. 于是 $a\equiv b(\mathrm{mod}\ m)$ 当且仅当 $m|(a-b)$，而这也相当于 $a=b+ml$，其中 l 是整数.

同余式有像等式一样的类似性质，并且也可以像等式那样作加减乘法：

(1) $a\equiv a(\mathrm{mod}\ m)$；

(2) 若 $a\equiv b(\mathrm{mod}\ m)$，则 $b\equiv a(\mathrm{mod}\ m)$；

(3) 若 $a\equiv b(\mathrm{mod}\ m)$，$b\equiv c(\mathrm{mod}\ m)$，则 $a\equiv c(\mathrm{mod}\ m)$；

(4) 若 $a\equiv b(\mathrm{mod}\ m)$，$c\equiv d(\mathrm{mod}\ m)$，则

$$a+c \equiv b+d(\mathrm{mod}\ m),$$

$$a-c \equiv b-d(\mathrm{mod}\ m),$$

$$ac \equiv bd(\mathrm{mod}\ m).$$

但是对于同余式作除法时要小心. 例如，$2\equiv 6(\mathrm{mod}\ 4)$，但是两边不能除以 2，因为 $1\not\equiv 3(\mathrm{mod}\ 4)$，这里 $a\not\equiv b(\mathrm{mod}\ m)$ 表示 a 和 b 模 m

不同余，即$m\nmid(a-b)$. 事实上，同余式除法有以下结果：

(5) 若$ad\equiv bd(\mathrm{mod}\ m)$并且$d$和$m$互素(即$d$和$m$的最大公因子为1)，则$a\equiv b(\mathrm{mod}\ m)$.

对一个固定的正整数m，如果把模m与a同余的所有整数放在一起，叫做模m的一个同余类，表示成$\bar{a}$. 由于每个整数模m必同余于$0,1,\cdots,m-1$当中的一个，所以模m共有m个同余类$\bar{0},\bar{1},\cdots,\overline{m-1}$，它们形成的$m$元集合表示成$Z_m$：于是对两个整数$a$和$b$，$\bar{a}=\bar{b}$当且仅当$a\equiv b(\mathrm{mod}\ m)$. 可以在$m$元集合$Z_m$中自然地定义加减乘运算：对于整数$a,b$，

$$\bar{a}+\bar{b}=\overline{a+b},\quad \bar{a}-\bar{b}=\overline{a-b},\quad \bar{a}\cdot\bar{b}=\overline{ab},$$

那么前面的性质(4)相当于

(4′) 在Z_m中，若$\bar{a}=\bar{b},\bar{c}=\bar{d}$，则

$$\bar{a}+\bar{c}=\bar{b}+\bar{d},\quad \bar{a}-\bar{c}=\bar{b}-\bar{d},$$

$$\bar{a}\cdot\bar{c}=\bar{b}\cdot\bar{d}.$$

类似可知，同余类的加法和乘法运算还满足交换律、结合律与分配律. 这样的集合在数学中叫做(交换)环，于是Z_m叫做模m同余类环.

性质(5)可以表述如下：

(5′) 在Z_m中，若$\bar{a}\cdot\bar{d}=\bar{b}\cdot\bar{d}$并且$d$和$m$

互素，则$\bar{a}=\bar{b}$，即等式两边可以消去$\bar{d}$（作除法）.

前面的例子取$m=4$，$2\equiv 6 \pmod 4$可以表示成$\bar{1}\cdot\bar{2}=\bar{3}\cdot\bar{2}$，不能消去$\bar{2}$而得到$\bar{1}=\bar{3}$，因为2和4不互素. 但是若$m$是一个素数$p$，$\bar{a}\cdot\bar{d}=\bar{b}\cdot\bar{d}$并且$\bar{d}\neq\bar{0}$，这表明$d$不被$p$整除. 由于$p$是素数，$d$必然与$p$互素. 于是可得到$\bar{a}=\bar{b}$. 这表明，在$Z_p$中，每个不为$\bar{0}$的元素$\bar{d}$都可以作为除数. 换句话说，在$Z_p$中可以像有理数全体、实数全体或者复数全体那样进行加减乘除四则运算，只有零($\bar{0}$)不能作除数. 这样的集合在数学中叫做一个域(field). 于是对每个素数p都有一个p个元素的有限域$Z_p=\{\bar{0},\bar{1},\cdots,\overline{p-1}\}$，今后把它改记成$F_p$. 例如，对于$p=3$，表1.1.1与表1.1.2是域$F_3=\{\bar{0},\bar{1},\bar{2}\}$中的加法和乘法运算表.

下面是F_3中运算的例子：

$$\bar{2}+\bar{2}=\bar{4}=\bar{1},\qquad \bar{1}-\bar{2}=\overline{-1}=\bar{2},$$

$$\bar{2}\cdot\bar{2}=\bar{4}=\bar{1},$$

$$\frac{\bar{1}}{\bar{2}}=\frac{\overline{1+3}}{\bar{2}}=\frac{\bar{4}}{\bar{2}}=\bar{2}.$$

由于有限域F_p中可以进行四则运算，通常把通信中的信息用F_p中的p个元素来表示.

表 1.1.1

加法	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

表 1.1.2

乘法	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

为了书写方便，在给定素数 p 之后，把 F_p 中元素 $\bar{a}$ 简记成 a. 于是在 F_3 中，$-1=2, 2\cdot 2=1$. 事实上，通信中使用最多的是二元域 $F_2=\{0,1\}$. 这是最简单的域，运算为：

$$1+0=0+1=1,\quad 0+0=1+1=0,$$

$$1\cdot 0=0\cdot 1=0\cdot 0=0,\quad 1\cdot 1=1.$$

现在假设要传递 8 个信息{赵，钱，孙，李，周，吴，郑，王}. 如果每位数字取自二元域 F_2 中的 0 或 1，可以用长为 3 的 8 个向量来表示它们：

赵 $=(000)$，　钱 $=(100)$，　孙 $=(010)$，

李 $=(110)$，　周 $=(001)$，　吴 $=(101)$，

郑 $=(011)$，　王 $=(111)$.

设想把“钱$=(100)$”传出，如果信道中出错，如第二位的 0 变成 1，收方收到了(110). 这时收方对于出错毫无所知，因为收方可认为没有出错，即发来的是$(110)=$李，也有可能是第 1 位

出错,即发来的是(010)=孙,如此等等. 总之,这种传输方式完全没有检查和纠正错误的能力. 其主要原因是收方收到的任何向量($a_1a_2a_3$)都是有意义的,从而收方没有任何判别能力.

如何设计有检查和纠正错误能力的通信系统? 先举两个例子.

例 1.1.1(奇偶校验码) 前面把"赵、钱、孙、李、周、吴、郑、王"8 个信息编成 3 位的向量. 现在把每个向量后面增加 1 位,变成 4 位的向量,使得其中 1 的个数是偶数. 例如,"钱"为(100),后面加上 1 成为(1001),而"李"为(110),后面加上 0 成为(1100). 这样一来,8 个姓分别重新编成(这叫纠错编码):

赵 = (0000), 钱 = (1001), 孙 = (0101),
李 = (1100), 周 = (0011), 吴 = (1010),
郑 = (0110), 王 = (1111).

于是,长为 4 的二元向量共有 $2^4=16$ 个,其中,1 的个数为偶数的向量占一半,是有意义的信息,而另一半(即 1 的个数为奇数的 8 个向量(1000),(0100),…,(0111))是没有意义的,不代表任何信息.

现在如果有 1 位发生错误,如李=(1100)的第 2 位出错,则收方得到(1100)+(0100)=

(1000),其中,1 的个数为奇数,它没有意义,于是收方可以断定信道发生了错误. 所以这种编码方式可以检查任何一位出错. 但是收方并不能判定错在哪一位,因为赵=(0000)的第 1 位出错也可以收到(1000). 所以收方不能纠正任何 1 位的错误. 类似地可以看出,对于这种编码方式,收方不能检查 2 位出错,如赵=(0000)和钱=(1001)只有首末两位不同,赵=(0000)的首末两位出错就错成钱=(1001).

例 1.1.2(重复码) 将表示 8 个姓的 3 位向量都重复 3 次,即进行一次纠错编码,成为:

赵 = (000000000), 钱 = (100100100),
孙 = (010010010), 李 = (110110110),
周 = (001001001), 吴 = (101101101),
郑 = (011011011), 王 = (111111111).

这就好像是军舰上旗手打旗语时重复 3 次,或者电话中有杂音时,每句话都重复说 3 次. 这时,每个姓的编码都是相同的 3 段(每段 3 位). 对于不同的姓,在一段中至少有 1 位不同,所以 3 段中至少有 3 位不同. 也就是说,不同姓的 9 位向量中,至少有 3 位不同,所以若一个姓(如钱=(100100100))的9 位中有 1 位或 2 位出错(如前两位出错,收到(010100100)),收到向量