研 究 生 数 学 丛 书 4
Mathematics Series for Graduate Students

纠错码的代数理论

Algebraic Theory of Error-Correcting Codes

冯克勤 著
Feng Keqin

清华大学出版社
Springer

研 究 生 数 学 丛 书 4
Mathematics Series for Graduate Students

纠错码的代数理论

Algebraic Theory of Error-Correcting Codes

冯克勤 著
Feng Keqin

清华大学出版社
北京
Springer

内 容 简 介

本书概要介绍半个世纪以来由数字通信的可靠性要求所建立和不断发展的纠错码数学理论。书中不涉及纠错技术和工程具体实现问题，但也介绍了一些纠错译码算法。

本书适用于代数专业的研究生和具有较好代数基础的高年级本科生。书中所讲述的知识和方法对于研究信息科学与计算机科学中许多其他问题也会有所帮助。

图书在版编目(CIP)数据

纠错码的代数理论＝Algebraic Theory of Error-Correcting Codes/冯克勤著. —北京：清华大学出版社，2005.10

(研究生数学丛书；4)

ISBN 7-302-11254-1

Ⅰ. 纠… Ⅱ. 冯… Ⅲ. 纠错码-编码理论-研究生-教材-英文 Ⅳ. O157.4

中国版本图书馆 CIP 数据核字(2005)第 068873 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
责任编辑：陈朝晖
印 装 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：170×230　**印张**：10　**字数**：193 千字
版　　次：2005 年 10 月第 1 版　2005 年 10 月第1 次印刷
书　　号：ISBN 7-302-11254-1/O·474
印　　数：1～3000
定　　价：29.00 元

编审委员会

研究生数学丛书 Mathematics Series for Graduate Students

1. 连续介质力学中的数学模型
(Mathematical Modeling in Continuum Mechanics)

2. 应用密码学
(Applied Cryptography)

3. Introduction to Malliavin Calculus
(Malliavin 随机变分引论)

4. 纠错码的代数理论
(Algebraic Theory of Error-Correcting Codes)

5. 抽象代数学基础
(Fundamentals of Abstract Algebra)

6. Algebraic Geomefry
(代数几何)

7. 反问题
(Inverse Problem)

总　序

数学是一门在非常广泛的意义下研究自然和社会现象中的数量关系和空间形式的科学。长期以来，在人们认识世界和改造世界的过程中，数学作为一种精确的语言和一个有力的工具一直发挥着重要的作用。在现代，数学科学已构成包括纯粹数学及应用数学内涵的众多分支学科和许多新兴交叉学科的庞大的科学体系。作为各门科学的重要基础，作为“四化”建设的重要武器，作为人类文明的重要支柱，数学科学在很多重要的领域中已起着关键性甚至决定性的作用，数学技术已成为高技术的突出标志和重要组成部分，数学的影响和作用已深入到各行各业，可以说无处不在。马克思当年的预言：“一门科学只有当它成功地运用了数学之后，才算达到了真正完善的地步”，正在不断得到证实。在这样的背景下，数学科学的重要性已得到空前广泛的认同。在研究生（不限于数学专业的研究生）的培养中，重视数学基础的训练，强调数学思想的熏陶，也已成为一种必然的趋势。但是，国内研究生数学教材及参考读物的实际情况，无论从品种、数量及质量哪一方面来看，都远远不能适应这个形势，甚至也远远落后于本科生的数学教材。这已成为制约提高研究生培养质量的一个重要瓶颈。清华大学出版社和施普林格出版社(Springer-Verlag)合作，倡议出版这一套《研究生数学丛书》(Mathematics Series for Graduate Students)，可望改善这方面的状况，为我国的研究生打好数学基础、提高数学素质起到积极的作用。

根据数学这门科学的特点，同时考虑到研究生学习数学的基本要求和特有方式，这套以面向研究生（包括高年级本科生、硕士及博士研究生）的数学教材或参考读物，将力求体现以下的一些原则：

- 主题有理论或（和）应用方面的重要性；
- 在重点介绍基础性内容的前提下，兼顾学科前沿的重要发展趋势和研究成果；
- 在讲授数学内容的同时，充分体现数学的思想方法和精神实质；
- 少而精，在较小的篇幅中展现基本的内容；

• 有相当好的可读性，适宜读者自学；

• 附有习题、思考题及参考资料目录，书末有索引，方便读者深入学习与思考。

为了有利于体现这些原则，本丛书将采取相当灵活的体例及风格：内容可以是纯粹数学、应用数学或数学与其他学科的交叉；可以是较系统地介绍某一个分支的教材，或是介绍某一前沿分支状况的综述，也可以是课外参考书；可以是原著，也可以是译著；可以是国内作者，也可以是国外作者；可以用中文编写，也可以用英文编写，等等。

要实现本丛书的目标和宗旨，任重而道远，但千里之行，始于足下，在学界同仁和广大读者的支持和帮助下，让我们共同努力。

李大潜

2003 年 9 月于上海

前　言

纠错码的代数理论

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。在今天，人们从每个层面上都能感受到计算机和通信的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。数字脉冲信号的数学描述方式，从连续性数学（Fourier分析和Laplace变换）一下子扩展到离散性数学（组合学、数论、代数）。与此同时，数字计算和数字通信中提出许多具有重要应用背景的数学问题，也促进离散性数学自身的发展，注入新的活力。本书的目的是介绍半个世纪以来，由数字通信的可靠性要求所建立和不断发展的纠错码数学理论。

纠错码的数学理论是一个很好的题目，用来表达理论和应用之间相互联系和促进的过程。通信的可靠性提出纠错的要求，建立起明确的数学概念和问题，以反映工程上的需求，然后数学家用各种数学工具构作性能愈来愈好的纠错码。纯粹数学和应用数学具有不尽相同的价值观念和美学标准。本书讲述纠错码的数学理论，不涉及纠错技术和工程具体实现问题，但是也要介绍一些纠错译码算法，这是应用中十分关心的数学问题。纯粹数学家可能只对构作好的纠错码更有兴趣，但是像关于BCH码的Berlekamp-Massey算法这样的内容，对于工程师和应用数学家来说，不仅是必需和重要的，而且也是美的。

纠错码的数学理论也是一个很好的场所，在这里，不同的数学知识和方法被用来解决通信中一个共同的课题，本书所用的数学工具主要涉及到组合学、初等数论、线性代数和抽象代数（群、环、域的基本知识）。事实上，近20年来纠错码的研究用到了更深刻的数学：代数几何、代数数论和群表示理论。这本书希望代数专业的研究生和具有较好代数基础的高年级本科生能够使用。

本书的基本内容是前三章（到BCH码为止）。由于代数几何码需要较为专门的代数几何和代数数论知识（有限域上的代数曲线和代数函数域），本书略去这方面内容。最后一章介绍1996年产生的量子纠错码的数学理论，其中用到一点群表示论（有限交换群的特征理论）。附录中介绍有限域的基本知识和线性移存器序列。

读者在本书中可以学到纠错码的基本知识，并通过这些材料能复习和加深关于初等数论、线性代数和抽象代数的知识与方法，这些知识和方法对于研究信息科学与计算机科学中许多其他问题也是有用的，我们希望读者通过对这些材料的学习，感受到数学工具和思考方式对应用领域的重要作用，并且能够在今后从事各种工作中，有意识地采用数学工具和思考方式，从而终生与数学相伴并喜欢它。

冯克勤

于清华园

目　录

纠错码的代数理论

1 什么是纠错码

1.1 通信和纠错的数学模型

1948 年 Shannon 发表《通信的数学理论》一文，奠定了通信的数学基础——信息论和通信的可靠性理论。具体的通信方式可以是多种多样的(打电话，传送电子邮件，宇宙飞船将金星图片传回地球，邮差传送信件和公文，……)，它们的抽象的数学模型可以表示成以下最基本的形式：

$$\boxed{\text{发方}} \xrightarrow{x} \overset{\text{信道}}{\cdots\cdots} \xrightarrow{x} \boxed{\text{收方}}$$

要发送的原始信息可以有不同形式(声音、文字、图像、数据、……)。利用各种物理技术手段，把原始信息统一编成离散的脉冲电信号发出，脉冲信号只有有限多个状态，假设有 m 个状态($m\geqslant 2$)，可以表示成 $0,1,\cdots,m-1$，并且将集合 $\{0,1,\cdots,m-1\}$ 按模 m 做加、减、乘运算，即状态集合是模 m 同余类环 Z_m。也可把状态集合取成有限域 $\mathbb{F}_q$，其中 $q=p^l$(p 为素数，$l\geqslant 1$)，这时还可做除法运算。本书只研究状态集合为 q 元有限域 $\mathbb{F}_q$ 的情形。事实上，数字通信中最常用的脉冲信号只有两个状态，即最常用的是二元域 $\mathbb{F}_2=\{0,1\}(1+1=0)$，关于有限域的基本知识见附录 A。

以 $\mathbb{F}_q^n$ 表示 $\mathbb{F}_q$ 上的 n 维向量空间，其中 q^n 个不同向量 $(c_0,\cdots,c_{n-1})(c_i\in\mathbb{F}_q)$ 可以表示 q^n 个不同的信息，比如 $\mathbb{F}_2^3$ 中有 8 个向量，可表示 0,1,…,7 这 8 个信息：

$$0=(000),1=(100),2=(010),3=(110),$$
$$4=(001),5=(101),6=(011),7=(111)。$$

设想发方把数字 3 传给对方，即把码字(110)传出去。如果信道(电话线，大气层，……)受到干扰(或发生设备故障)使信息(110)的某位出错，比如第 3 位由 0

变成 1,则收方得到(111)。由于(111)也代表信息(数字 7),收方无法发现传送的错误,即无法判定发来的就是 7(无错),还是发来其他数字错成了 7。这表明,通信系统完全没有检查错误和纠正错误的能力。

如何使通信系统具有纠错能力?这需要将信息进行一次纠错编码。我们先举两个最简单的例子,它们也是通信系统最早采用的检错和纠错方式。

例 1(奇偶校验码) 前面已经把 0,1,…,7 分别用长为 3 的二元向量(000),(100),…,(111)传输,现在再把每个向量后面加上 1 位(0 或 1),使新的码字有偶数个 1,于是均变成长为 4 的二元向量:

$$0=(0000),1=(1001),2=(0101),3=(1100),$$
$$4=(0011),5=(1010),6=(0110),7=(1111)。$$

长为 4 的二元向量共 16 个,其中只有上述 8 个是有意义的码字(codeword),其余 8 个$(a_0a_1a_2a_3)$($a_i\in\mathbb{F}_2$,$a_0+a_1+a_2+a_3=1$)均没有意义,不是码字。

如果码字在传输中只有 1 位出错,比如(1100)错成(1110),收到的(1110)不是码字,这是由于任意两个不同码字至少有 2 位是不同的,所以一个码字出现 1 位错误不可能变成另一个码字,收方收到的(1110)不是码字,便知出了错误。但是收方不能纠错,因为(1110)也可能是码字(1111)的最后一位出错而造成的,这表明:奇偶校验码可检查出 1 位错(收到向量有奇数个 1,便知出错),但不能纠正 1 位错(即不知哪位出错)。另一方面,8 个信息本来用长为 3 的二元向量即可表示,现在为了检查 1 位错误,改用长为 4 的向量,传输信息的速度为原来的 $\frac{4}{3}$,从而效率为原来的 $\frac{3}{4}$。

例 2(重复码) 电话中噪音很大时,常常把讲话重复几遍。现在我们也把每个信息 0=(000),1=(100),…,7=(111)重复三遍,即改用

0=(000000000),1=(100100100),2=(010010010),…,7=(111111111)。

长为 9 的二元向量共 $2^9=512$ 个,其中只有形如$(c_0c_1c_2c_0c_1c_2c_0c_1c_2)$的 8 个是码字,不同的码字至少有 3 位是不一样的,所以若一个码字在传输中有 1 位或 2 位发生错误,收到的不是码字,即发现错误。如果码字 $\boldsymbol{x}=(c_0c_1c_2c_0c_1c_2c_0c_1c_2)$ 只有 1 位出错,变成 $\boldsymbol{y}$,则 $\boldsymbol{y}$ 与 $\boldsymbol{x}$ 只有 1 位不同,而 $\boldsymbol{y}$ 与其他码字至少有 2 位不同,于是收方便可把 $\boldsymbol{y}$ 译成与 $\boldsymbol{y}$ 最“相近”的码字 $\boldsymbol{x}$。事实上,设 $\boldsymbol{y}=(a_0a_1a_2a_3a_4a_5a_6a_7a_8)$,如果它只有 1 个错位,那么$(a_0a_1a_2)$,$(a_3a_4a_5)$,$(a_6a_7a_8)$

当中有两个相同，而另一个和它们相差 1 位，那 1 位的数字改动，就可纠正错误。例如若 $\boldsymbol{y}=(101111101)$，马上知道中间那位出错，纠正成(101101101)，这叫纠错译码。

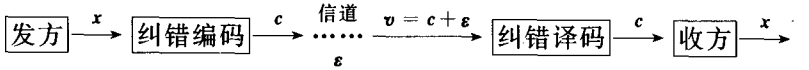
总之，上述纠错码可检查 2 位错误，也可纠正 1 位错误。另一方面，效率是原来的$\frac{3}{9}=\frac{1}{3}$。

从以上两个例子可以看出纠错码的本质。

(1) 为了使通信系统具有检错和纠错能力，我们把每个信息$(c_0,\cdots,c_{k-1})\in\mathbb{F}_q^k$的长度加大，即将信息编成$\mathbb{F}_q^n$中的向量 $\boldsymbol{x}$，使$\mathbb{F}_q^n$中只有一部分是码字(代表信息)，效率为原来的$\frac{k}{n}$。所以，我们是在降低通信效率的情况下提高通信纠错能力的。

(2) 为了使纠错编码具有好的检错和纠错能力，我们要使不同码字之间，有许多位上均是不同的元素(这叫相异位)。在例 1 中，不同码字之间至少有 2 个相异位，从而可检查 1 位错。在例 2 中，不同码字之间至少有 3 个相异位，从而可检查 2 位错，也可纠正 1 位错。

将通信系统加上纠错功能之后，数学模型便成为如下形式：



发方将信息 $\boldsymbol{x}\in\mathbb{F}_q^k$编成有纠错能力的码字 $\boldsymbol{c}\in\mathbb{F}_q^n$，传给收方的过程中信道出现错误 $\boldsymbol{\varepsilon}\in\mathbb{F}_q^n$($\boldsymbol{\varepsilon}$ 叫错误向量)，从而收方得到$\boldsymbol{v}=\boldsymbol{c}+\boldsymbol{\varepsilon}$。收方进行纠错，恢复成正确的码字 $\boldsymbol{c}$，然后得到信息 $\boldsymbol{x}$。

习题 1(书号的纠错编码)　国际上标准的书号设计 ISBN(International Standard Book Number)是将每本书编成$\mathbb{F}_{11}=\{0,1,2,\cdots,10\}$上的十位数字。例如书号为

$$\text{ISBN}\quad 0\text{-}19\text{-}859617\text{-}0,$$

其中 0 表示语种(英语)，19 表示出版社(牛津大学出版社)，859617 是该出版社真正的书号，末位 0 是校验位，使得每个书号 $a_1\text{-}a_2a_3\text{-}a_4a_5a_6a_7a_8a_9\text{-}a_{10}$ 都满足

$$\sum_{i=1}^{10} ia_i\equiv 0 \pmod{11}。$$

前九位均用 0 到 9 中的数字，如果末位为 10，则表示成 X，如 ISBN　0550-10206-X

(各出版社在10个数字之间加横线的方式不尽相同)。证明如此设计的书号有以下纠错功能。

(1) 可以检查任何1位发生错误;

(2) 可以检查任何2位数字相互置换的错误(即 $i\neq j$ 时,a_i 印成 a_j,而 a_j 印成 a_i,其余不变)。

习题2 构作一个二元纠错码,可传送8个信息,能纠正2位错误。

1.2　纠错码的基本概念和主要数学问题

有了以上直观描述，现在可以给出纠错码确切的数学概念。

定义 1.2.1　$\mathbb{F}_q^n$表示有限域$\mathbb{F}_q$上的 n 维向量空间。$\mathbb{F}_q^n$的每个非空子集合 C 都叫作一个 q 元码，n 叫该码的码长，C 中向量叫作码字。

用 K 表示 C 中码字个数，即 $K=|C|$，则 $1\leqslant K\leqslant q^n$。

$k=\log_q K$ 叫作码 C 的信息位数（k 为实数，$0\leqslant k\leqslant n$）。

$\frac{k}{n}$叫作码 C 的效率（或叫信息率）。

我们还需要一个概念来衡量码 C 的纠错能力，由上节直观描述可知，这个概念应当是不同码字之间的相异位个数。

定义 1.2.2　设 $\boldsymbol{a}=(a_1,\cdots,a_n)$和 $\boldsymbol{b}=(b_1,\cdots,b_n)$是$\mathbb{F}_q^n$中两个向量，则向量 $\boldsymbol{a}$ 的 Hamming 权（weight）定义为非零分量 a_i 的个数，表示成 $w_{\mathrm{H}}(\boldsymbol{a})$，即

$$w_{\mathrm{H}}(\boldsymbol{a}) = \#\{i \mid 1\leqslant i\leqslant n, a_i\neq 0\}。$$

而向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 之间的 Hamming 距离是指它们相异位的个数，表示成 $d_{\mathrm{H}}(\boldsymbol{a},\boldsymbol{b})$，即

$$d_{\mathrm{H}}(\boldsymbol{a},\boldsymbol{b}) = \#\{i \mid 1\leqslant i\leqslant n, a_i\neq b_i\} = w_{\mathrm{H}}(\boldsymbol{a}-\boldsymbol{b})。$$

$\mathbb{F}_q^n$中这个距离的定义非常简单，下面习题表明它具有通常距离类似的性质，本书除最后一章之外，均研究 Hamming 距离，所以将 $w_{\mathrm{H}}(\boldsymbol{a})$和 $d_{\mathrm{H}}(\boldsymbol{a},\boldsymbol{b})$分别简记为 $w(\boldsymbol{a})$和 $d(\boldsymbol{a},\boldsymbol{b})$。

习题 1　对于 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in\mathbb{F}_q^n$，证明

(1) $d(\boldsymbol{a},\boldsymbol{b})\geqslant 0$，并且 $d(\boldsymbol{a},\boldsymbol{b})=0$，当且仅当 $\boldsymbol{a}=\boldsymbol{b}$；

(2) $d(\boldsymbol{a},\boldsymbol{b})=d(\boldsymbol{b},\boldsymbol{a})$；

(3)（三角形不等式）　$d(\boldsymbol{a},\boldsymbol{c})\leqslant d(\boldsymbol{a},\boldsymbol{b})+d(\boldsymbol{b},\boldsymbol{c})$。

定义 1.2.3　设 C 是码长为 n 的 q 元码（即 C 为$\mathbb{F}_q^n$的非空子集合），$K=|C|\geqslant 2$，定义 C 的最小距离为不同码字之间 Hamming 距离的最小值，表示成 $d(C)$，即

$$d = d(C) = \min\{d(\boldsymbol{c},\boldsymbol{c}') \mid \boldsymbol{c},\boldsymbol{c}'\in C, \boldsymbol{c}\neq\boldsymbol{c}'\}。$$

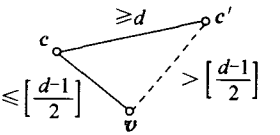
下面结果虽然简单，但却是整个纠错码理论的基础。对于实数 α，以 $[\alpha]$ 表示不超过 α 的最大整数，叫 α 的整数部分。

定理 1.2.4 如果纠错码 C 的最小距离为 d，则 C 可检查 $\leqslant d-1$ 位错，也可纠正 $\leqslant\left[\frac{d-1}{2}\right]$ 位错。

证明 设发出码字 $\boldsymbol{c}\in C$，信道出错，但错位不超过 $d-1$，即错误向量 $\boldsymbol{\varepsilon}$ 满足 $1\leqslant w(\boldsymbol{\varepsilon})\leqslant d-1$，则收到向量为 $\boldsymbol{v}=\boldsymbol{c}+\boldsymbol{\varepsilon}$。由 $\boldsymbol{\varepsilon}\neq 0$ 可知 $\boldsymbol{v}\neq\boldsymbol{c}$，进而 $d(\boldsymbol{c},\boldsymbol{v})=w(\boldsymbol{v}-\boldsymbol{c})=w(\boldsymbol{\varepsilon})\leqslant d-1$。由于对每个码字 $\boldsymbol{c}'\neq\boldsymbol{c}$，$d(\boldsymbol{c},\boldsymbol{c}')\geqslant d$，所以 $\boldsymbol{v}$ 也不为 $\boldsymbol{c}'$，这表明 $\boldsymbol{v}$ 不是码字，从而收方知道出错，即可检查出 $\leqslant d-1$ 位错。

现在设 $1\leqslant w(\boldsymbol{\varepsilon})\leqslant\left[\frac{d-1}{2}\right]$，这时 $d(\boldsymbol{c},\boldsymbol{v})=w(\boldsymbol{\varepsilon})\leqslant\left[\frac{d-1}{2}\right]$，而对每个码字 $\boldsymbol{c}'\neq\boldsymbol{c}$，由三角形不等式知

$$\begin{aligned} d(\boldsymbol{c}',\boldsymbol{v}) &\geqslant d(\boldsymbol{c}',\boldsymbol{c})-d(\boldsymbol{c},\boldsymbol{v}) \\ &\geqslant d-\left[\frac{d-1}{2}\right]>\left[\frac{d-1}{2}\right]。\end{aligned}$$



这表明 $\boldsymbol{c}$ 是惟一的与 $\boldsymbol{v}$ 最近的码字，收方将 $\boldsymbol{v}$ 译成 $\boldsymbol{c}$ 是正确纠错，从而可纠 $\leqslant\left[\frac{d-1}{2}\right]$ 位错，证毕。 ■

对每个固定的有限域 $\mathbb{F}_q$，q 元纠错码 $C(\subseteq\mathbb{F}_q^n)$ 有三个基本参数：

码长 n，

码字个数 $K=|C|$（或用信息位数 $k=\log_q K$），$0\leqslant k\leqslant n$，

最小距离 $d=d(C)$，$1\leqslant d\leqslant n$。

我们把这个纠错码表示成 $(n,K,d)_q$ 或者 $[n,k,d]_q$，也说成：q 元码 (n,K,d) 或 q 元码 $[n,k,d]$。

纠错码数学理论的最基本研究课题有以下两个：

(1) 构作性能良好的纠错码，即要求效率 $\frac{k}{n}$ 和反映纠错能力的 d 愈大愈好。

(2) 寻求好的译码算法。

对于问题(1)，易知三个参数 n,K（或 k）和 d 之间是相互制约的，有两个极端的情形：一种情形，若 $\frac{k}{n}$ 为最大值 1，即 $k=n$，则 $K=q^n$，从而 $C=\mathbb{F}_q^n$（每个向量