The Art of Error Correcting Coding

SECOND EDITION

纠错编码的艺术

（第2版）

（美）Robert H. Morelos-Zaragoza 著

张立军 译

WILEY

北京交通大学出版社

http://press.bjtu.edu.cn

纠错编码的艺术

（第2版）

The Art of Error Correcting Coding

Second Edition

（美）Robert H. Morelos-Zaragoza 著

张立军 译

北京交通大学出版社

·北京·

图书在版编目（CIP）数据

纠错编码的艺术/（美）莫雷洛斯 - 萨拉戈萨（Morelos-Zaragoza, R. H.）著；张立军译. —北京：北京交通大学出版社，2007.8
ISBN 978-7-81123-194-6

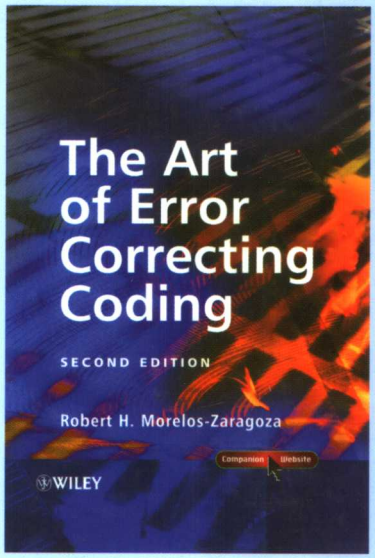
Ⅰ. 纠… Ⅱ. ①莫… ②张… Ⅲ. 纠错码—通信理论 Ⅳ. TN911.22

中国版本图书馆 CIP 数据核字（2007）第 125416 号

责任编辑：王晓春
出版发行：北京交通大学出版社 电话：010-51686414
北京市海淀区高梁桥斜街 44 号 邮编：100044
印 刷 者：北京宏伟双华印刷有限公司
经 销：全国新华书店
开 本：185 × 230 印张：18.75 字数：346 千字
版 次：2007 年 8 月第 1 版 2007 年 8 月第 1 次印刷
书 号：ISBN 978-7-81123-194-6/TN·54
印 数：1 ～ 4 000 册 定价：29.80 元

译者简介

张立军　男，博士、副教授。1999年6月毕业于山东大学电子工程系，先后获得学士学位和硕士学位；2003年6月毕业于清华大学电子工程系，获得通信与信息系统专业博士学位；现为北京交通大学电子与信息工程学院副教授，主要研究方向包括通信理论、信息论、信道编码及其在宽带无线通信中的应用，以及协作网理论等，在国内外重要学术刊物和国际会议发表专业论文30多篇。



责任编辑：王晓春
封面设计：七星工作室

中译本序

差错控制编码技术，特别是纠错编码技术，是提高数字通信可靠性的一个主要手段。自 Shannon 创立信息论以来，纠错编码的发展已历经 60 余年，在理论上得到了长足的发展，比如近年来重新被认识的 LDPC 码，其性能距离 Shannon 限仅有 0.004 5 dB。在实际应用方面，差错控制编码技术在移动通信、卫星通信、宇航通信、有线通信、多媒体数字传输、因特网、计算机、信息存储等领域得到越来越广泛的应用，成为数字信息传输、处理和存储系统及通信网络中不可或缺的一个组成部分。

纠错编码的理论性强，透彻了解其原理，需要较为深厚的数学基础，特别是近世代数方面的知识，这往往使许多想要从事该方面应用和研究的人员望而却步，在一定程度上限制了这门学科的应用和发展。为了使科技工程人员易于了解和掌握纠错编码技术，美国加州圣何塞（San Jose）州立大学的 Robert H. Morelos-Zaragoza 博士，于 2002 年编著了《纠错编码的艺术》一书。该书涵盖当前纠错编码技术的几乎全部内容。全书的指导思想是，重点阐述纠错编译码是“如何做”的，至于“为什么”，则仅在必要的时候给予简单阐述，尽量避免繁杂难懂的数学分析和推导。这本书的最大特点是备有一个配套的网站， http://the-art-of-ecc.com，该网站提供了书中所述的重要编解码程序和性能估测程序。此外，书中具有大量的实例说明如何选择、分析和实现一些重要的编解码方案。

2006 年作者又推出了该书的第 2 版，在第 1 版的基础上做了修订：增加了一些新的内容和实例，如 LDPC 的译码实例和迭代译码的实例；在每章增加了习题；配套网站上增加了编译码的 Matlab 脚本程序（原来只有 C 程序）和部分习题答案，使之更加适合作为教材使用。

为便于国内读者学习和参考此书，北京交通大学的张立军博士将此书的第 2 版译为中文。我相信，由于该书的特点，中译本的出版，将会有助于纠错编码的教学、应用和研究，对纠错编码的普及与提高起到积极的促进作用。

曹志刚 教授

2007 年 6 月于北京清华园

引　言

这本书的第 1 版是数百封发自全球各地的电子邮件的产物，这些邮件中包含了来自学术界和工业界的同行关于纠错编码 (error correcting coding, ECC) 理论和应用方面的问题。大多数问题源自工程师和计算机科学家，他们要选择、实现或者仿真某个特定的编码方案。这些问题是由一个流行的网站[1]引发的，该网站最初建于东京大学工业科学院的 Imai 实验室，时间在 1995 年伊始。本书的一个重要特点是缺少定理和相应的证明，采用的方法是利用简单例子教授基本概念，只是在需要的时候才提及理论推导。对于想学习纠错编码基本概念和应用的研究生及专业人员，本书是一本关于纠错编码技术的参考指南。实际编码方案的编解码计算机程序可以从本书的配套网站获得，该网站在本书中称为“ECC 网站”，它位于：

http://the-art-of-ecc.com

通过简单易懂的实例介绍纠错编码的基本概念，是本书的特色。从 ECC 网站可以获取用 C 语言和全新的 Matlab[2]脚本编写的计算机程序，这些程序有助于阐明一些重要的编码方案，如卷积码、Hamming 码、BCH 码、Reed-Solomon 码、turbo 码的基本编译码算法是如何实现的，以及它们在编码调制系统中的应用。通过参考合适的资料，读者可以涉及丰富的 ECC 理论。这方面的优秀著作有很多，比如参考文献 [LC05]、[MS77]、[PW72]、[Blah84]、[Bos99]、[Wic95]，不能一一列举。读者可以在阅读本书之前、之中或者之后来参考这些文献。本书的每一章均采用简单易懂的数值实例而非这些方案背后的理论细节来描述特定编解码方案的基本概念。书中给出了基本的分析工具，以便于评价特定 ECC 方案的错误性能。

本书从纠错和检测码的编译码算法的选择、实现和仿真这些方面，探讨了纠错编码的技巧。第 2 版的新特色包括正文中增加的实例和每一章末尾用于 ECC 课程的习题。本书还为那些希望学习更多 ECC 运作的完美理论的读者提供了一个综合参考书目。本书的组织结构如下：第 1 章介绍了纠错的基本概念和编解码技术；第 2 章涉及一些简单而重要的码族，如 Hamming 码、Golay 码和 Reed-Muller 码；第 3 章中介绍了循环码，以及其中重要的 BCH 码族，还介绍了有限域算术和基本译码算法，如 Berlekamp-Massey、Euclidean 和 PGZ 算法，并通过一些易懂的实例来说明这些算法是如何操作的；第 4 章讲述了 Reed-Solomon 码和纠错纠删译码方法，对可

[1] http://www.eccpage.com

[2] Matlab 是 The Mathworks, Inc. 的注册商标。

用的算法进行了全面详尽的描述并给出应用实例；第 5 章介绍了二进制卷积码，重点是这些码的基本结构和采用 Hamming 度量的 Viterbi 算法的基本解释，另外还讨论了一些算法实现方面的问题；第 6 章中阐述了单码修改和多码合并的几种技术，并给出了相应的实例；第 7 章涉及软判决译码算法，其中有一些并未在文献中得到重视，比如软输出排序统计译码算法；第 8 章从编码理论的角度给出了 turbo 码、并行级联码和串行级联码、块乘积码的介绍，并对低密度校验码进行了分析，对于所有这些码，给出了基本的译码算法和简单的实例；最后，第 9 章阐述了纠错编码与数字调制相结合的技术，并给出了几种巧妙的译码方法。

我要向下面这些激励我写这本书的人们致谢。墨西哥 Nacional Autónoma 大学的 Francisco Garcia Ugalde 教授，是他引导我进入纠错编码这个激动人心的领域。本书的部分内容基于由他指导的我的学士学位论文。夏威夷大学的 Edward Bertram 教授，是他教授了我抽象代数的基本内容。墨西哥 Instituto Tecnológico y de Estudios Superiores de Monterrey 的 David Muñoz 教授，感谢他的热心和支持。感谢广岛城市大学的 Tadao Kasami 教授，大阪大学的 Toru Fujiwara 教授和东京大学的 Hideki Imai 教授，是他们为我在日本做访问学者提供支持。感谢 LSI 逻辑公司的 Dan Luthi 和 Advait Mogre 进行的诸多鼓舞人心的讨论，并有机会将一些想法用集成电路实现。感谢夏威夷大学 Marc P. C. Fossorier 教授的帮助。感谢我以前的同事，Sony 计算机科学实验室的 Misa Mihaljević 博士，指出了解码和密码学之间的联系。我还要诚恳地感谢 Sony 计算机科学实验室的主任 Mario Tokoro 博士和横滨国立大学的 Ryuji Kohno 教授，他们使我有可能在一个良好的环境下完成本书的第 1 版。我还要特别感谢现任职加州大学 Davis 分校的 Shu Lin 教授。我也要感谢 San Jose 州立大学的研究生，他们学习了该课程并帮助设计和检验了第 2 版中的一些习题。

谨以此书纪念 Richard W. Hamming、Claude Shannon 和 Gustave Solomon，正是这三位杰出的人士极大地影响了今天人们生活和工作的方式。

Robert H. Morelos-Zaragoza

于美国加利福尼亚 San Jose

序

在现代数字通信和存储系统设计中，信息论正变得日益重要。其中一个最典型的例子就是 turbo 码和块乘积码的出现，并迅速地在许多实际的卫星和无线通信系统中获得应用。我很高兴向那些对纠错编码感兴趣或需要应用它们的读者推荐这本由 Robert Morelos-Zaragoza 博士写的新书。这本书用易懂的方式介绍了纠错编码 (ECC) 中的关键概念。本书逻辑严密，用了很多实例说明问题，再辅以能够从网站获得的计算机程序，以一种独特的方式讲授了纠错编码设计及应用的基本技术。

本书的最大特色之一是从代数信道编码的角度，以简单自然的方式阐述了 turbo 码、LDPC 码和乘积码的原理和译码方法。本书将 turbo 码看作是一种打孔的乘积码，通过简单的例子将乘积码的生成和迭代译码算法背后的思想和结构，用一种前所未有的方式展现出来。同样值得提及的是，书中详尽介绍了利用 Reed-Solomon 码来纠错纠删的各种代数译码算法。关于纠错编码在信道编码和数字调制的结合，即编码调制方面的应用，作者很好地介绍了几类重要的编码调制系统构成的基本原理。

我相信工程师和计算机科学家会发现本书是一个很好的学习工具和有价值的参考书。配套的 ECC 网站是本书最具特色之处。附带说一下，这个网站 1995 年诞生于东京大学我的实验室中，Morelos-Zaragoza 博士在那里一直工作到 1997 年 6 月，作为一个副研究员，他工作很出色，写出了许多高质量的论文。他很有礼貌、谦虚、工作刻苦，而且对人总是很友好。总之，《纠错编码的艺术》是一本关于纠错编码的原理和应用的优秀入门参考书，我强烈推荐。

Hideki Imai 教授

于日本东京，东京大学

ECC 网站

《纠错编码的艺术》一书的配套网站业已建立，并永久的位于如下 URL 地址：

http://the-art-of-ecc.com

ECC 网站包含同时用 C 和 Matlab[3]书写的程序，实现了重要的纠错码族的编译码算法，并增加了用于分析纠错码方案性能的新脚本。同时，网站还提供教师手册，其中包含每一章末尾习题的答案。网站由作者维护，以确保域名保持不变。拥有配套网站的一个重要优点是，作者可以张贴更新通知，发布与本书内容相关的新程序和仿真结果。

ECC 网站的程序以主题和功能两种方式组织起来。

根据主题划分的程序基本遵循本书的逻辑结构，从简单的基于校正子的线性分组码译码到更加精细的 BCH 码和 Reed-Solomon 码的有限域代数译码，然后是卷积码的 Viterbi 译码和合并码的译码，最后是 turbo 码、乘积码的迭代译码，低密度奇偶校验码的置信传播译码，以及编码调制技术的应用。ECC 网站的程序同时按照功能分类，主要是针对那些已经确知查找对象的读者。程序的这种分类是特意围绕译码算法进行的。

[3]Matlab 是 The Mathworks, Inc. 的注册商标。

目　录

第 1 章　绪　　论

纠错编码的历史可以追溯到 Hamming 码的出现 [Ham74]，那时 Shannon 的工作才刚刚起步 [Sha48]。不久以后，Golay 码出现了 [Gol74]。这两种最早出现的码是最优的，它们的定义将在后面的章节给出。

图 1.1 所示为数字通信/存储系统的规范方框图，该图是大多数有关纠错编码理论和数字通信的书中著名的“图 1”[BB99]。信源和信宿包括了针对信息特征进行的任何信源编码方案。来自信源的信息符号进入纠错编码器，编码器为它增加冗余符号，从而能够纠正大部分在信号调制、有噪媒介中传输和解调过程中引入的错误[Mas84, McE77, Moo05]。

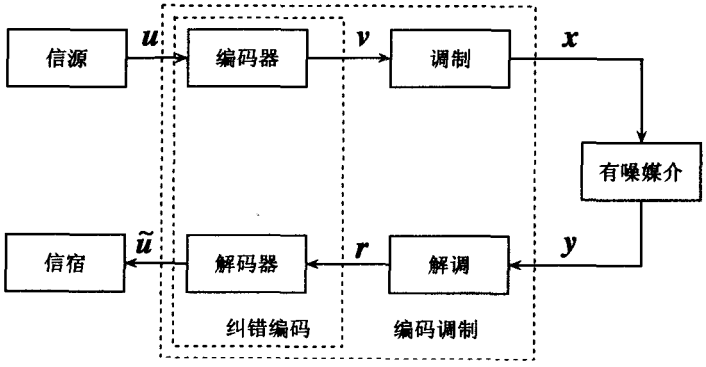


图 1.1　规范的数字通信系统

通常，假定信道是在调制符号（复基带表示）上面附加加性噪声过程的抽样，噪声抽样独立于信源符号。该信道模型相对易于处理，包括加性白色 Gaussian 噪声 (additive white Gaussian noise, AWGN) 信道、平坦 Rayleigh 衰落信道和二进制对称信道 (binary symmetric channels, BSC)。频率选择性信道也可以包含进来，因为诸如扩频和多载波调制 (muticarrier modulation, MCM) 技术可以有效的将其转化为 AWGN 信道或者平坦 Rayleigh 衰落信道。

在接收端，译码器利用冗余符号和它们与信息符号的关系来纠正信道错误。当用于检错时，最好将纠错编码译码器想像为对接收信息重新编码的编码器，并检查生成的冗余符号与接收的冗余符号是否相同。