

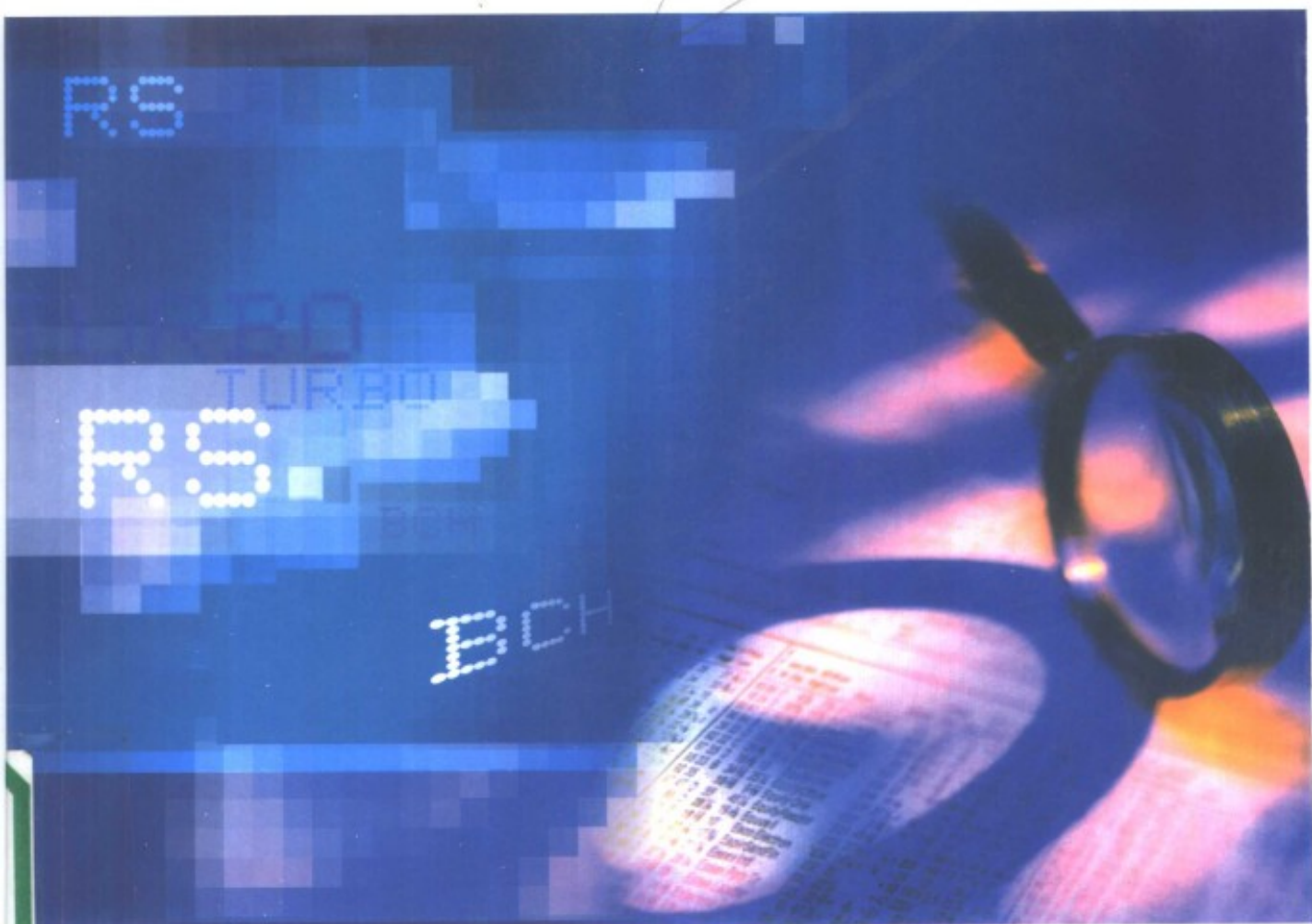
21世纪

高等学校通信类系列教材

纠错码——原理与方法

(修订版)

王新梅 肖国镇 编著



西安电子科技大学出版社

[http:// www.xduph.com](http://www.xduph.com)

21 世纪高等学校通信类系列教材

纠 错 码

——原理与方法

(修订版)

王新梅 肖国镇 编著

西安电子科技大学出版社

2001

内 容 简 介

纠错码是一门新的差错控制技术,目前已广泛应用于各种通信系统和计算机系统中。本书着重阐述纠错码的基本原理和各种编、译码方法。全书共分十三章。前九章介绍各种线性分组码(如循环码、BCH码、RS码、不等保护能力码和代数几何码等)的基本原理和必要的数学基础,还介绍了各种实用的编、译码技术和方法。后四章介绍卷积码的基本概念以及代数译码和概率译码的方法和Turbo码。全书对材料的阐述循序渐进;在内容上,既有必要的数学基础,又着重于物理概念的解释;在每章之后均附有习题。本书可作为高等学校本科生、研究生的教材和参考书,也可作为从事通信、计算机等领域中工程技术人员的参考书。

高等学校教材

纠 错 码

——原理与方法

(修订版)

王新梅 肖国镇 编著

责任编辑 李纪澄

西安电子科技大学出版社出版发行

陕西画报社印刷厂印刷

新华书店经销

开本 787×1092 1/16 印张 34.125 字数 812千字

1991年12月第1版 2001年4月修订版 2001年4月第3次印刷 印数 5 001~9 000

ISBN7-5606-0163-4/TN·0059(课)

定价: 35.00元

序

提高信息传输的可靠性和有效性，始终是通信工作所追求的目标。纠错码是提高信息传输可靠性的一种重要手段。它已经历了 40 年的历史，在此期间有了很大的进展。

伴随着信息时代的到来以及微电子技术的飞速发展，今天纠错码已不再单纯是一个理论上探讨的课题了，它已成为一门标准技术而被广泛采用。在通信领域中，CRC 校验已成为 CCT 对各类线路传输建议中必不可少的一部分；在移动通信中，纠错码被广泛用于模拟体制的信令传输及数字体制的整个传输，以提高传输的可靠性和节省珍贵的频谱资源；在卫星通信中，纠错码技术已成为用来降低对高功放的要求和减少地球站天线孔径的尺寸的经济可靠的方法，VSAT 和 USAT 的兴起，都是和纠错码技术的应用有关的；在电话网上的数据传输中，纠错码、差错控制技术已是使高速数据传输(9.6 kbit/s 以上的数据率)成为现实的关键技术。纠错码技术还广泛应用于计算机存贮和运算系统中，此外，纠错码技术还应用于超大规模集成电路(VLSI, ULSI)设计中，以提高集成电路芯片的成品率，降低芯片的成本。

因此，纠错码已不再是致力于专门研究的专业人员才应掌握的一门学科，而成为从事通信、计算机、电子系统工程的有关工程技术人员都必需掌握的一门技术。纠错码的内容十分丰富，涉及的领域亦很广，很需的数学知识较多、较深，为此，应在大学本科生及研究生中开设纠错码课程，而实施纠错码教学的关键在于有一本好教材。西安电子科技大学的王新梅教授、肖国镇教授编著的《纠错码——原理与方法》一书正是适应这一需要的一本很好的专著。

西安电子科技大学是我国最早从事纠错码研究工作的基地之一，在纠错码发展第一阶段的后期，即 60 年代初，西电就系统地进行了这方面的研究工作，30 年来锲而不舍。本书的作者及王育民、梁传甲等教授带领一批青年学者在这一方面做出了不少贡献，并与国际上编码学界有着广泛的联系与交流，在科研与教学方面也积累了丰富的经验，正如作者在本书的前言中所述，本书可以说是编码讨论班的集体结晶。

尽管国内外在纠错码方面已出版了相当多的著作，但本书吸收了各家之长而有其显著的特色。本书对材料的选择和问题的阐述循序渐进，在内容上既有必要的数学证明又着重于物理概念的解释，内容新颖、全面、系统，并反映了纠错码理论的最新成果，贯彻了理论与实际相结合的原则。相信本书的出版，将对纠错码的普及与提高起到积极的推动作用。

值此岁暮之际，我谨向充满团结、友谊、进取精神的西电信息论编码集体祝贺他们所取得的丰硕成果，并预祝他们今后为我们的祖国做出更大贡献。

陈太一

1991 年 12 月 25 日

于北京雁栖湖畔

前 言

1948年香农(Shannon)在他的开创性论文“通信的数学理论”中,首次阐明了在有扰信道中实现可靠通信的方法,提出了著名的有扰信道编码定理,奠定了纠错码的基石。自此以后汉明(Hamming)、斯列宾(Slepian)、普兰奇(Prange)等人在50年代初,根据香农的思想,给出了一系列设计好码和有效译码的方法。以后,纠错码受到了越来越多的通信和数学工作者,特别是代数学家的重视,使纠错码无论在理论还是在实际中都得到飞速发展。

迄今,纠错码已有40年的历史,其发展过程大致分以下几个阶段。

50年代至60年代初,主要研究各种有效的编、译码方法,奠定了线性分组码的理论基础;提出了著名的BCH码编、译码方法以及卷积码的序列译码;给出了纠错码的基本界限;还出版了纠错码的第一本专著。这是纠错码从无到有得到迅速发展的年代。

自60年代至70年代初,这是纠错码发展过程中最为活跃的时期。不仅提出了许多有效的编译码方法,如门限译码、迭代译码、软判决译码和卷积码的维特比(Viterbi)译码等。而且注意到了纠错码的实用化问题,讨论了与实用有关的各种问题,如码的重量分布、译码错误概率和不可检错误概率的计算、信道的模型化等,所有这些问题的研究为纠错码的实用打下了坚实基础。在此期间,以代数方法特别以有限域理论为基础的线性分组码理论已趋成熟。

70年代初至80年代,这是纠错码发展史中具有极其重要意义的时期。在理论上以戈帕(Goppa)为首的一批学者,构造了一类Goppa码,其中一类子码能达到香农在信道编码定理中所提出的码——香农码,所能达到的性能,这在纠错码历史上具有划时代意义。在这期间大规模集成电路和微机的迅速进展,为纠错码的实用打下了坚实的物质基础,因而与实用相关的各种技术及有关问题得到了极大关注,并在实用中取得了巨大成功。如美国在70年代初发射的“旅行者”号宇宙飞船中,成功地应用了纠错码技术,使宇宙飞船在极其遥远的距离(30亿公里),向地面传回了天王星、海王星等星体的天文图片,发现了天王星的9个卫星和光环以及海王星的6个卫星和光环等许多极其宝贵的资料。若不应用纠错码,这些成就的取得是不可想象的。应当指出,在此期间利用FFT技术,从频谱观点研究纠错码,受到了特别重视,使得很多熟悉信号处理技术但不熟悉有限域理论的工程师们,能够较快地掌握纠错码理论,并能熟练地应用于实际中,从而为纠错码在各类通信系统中的广泛使用,起到了极好的推动作用。

自80年代初以来,戈帕等从几何观点讨论分析码,利用代数曲线构造了一类代数几何码。在这些码中,某些码的性能达到了香农码所能达到的性能。由于代数几何码是一类范围非常广的码,在理论上已证明它具有优越的性能,因而一开始就受到了编码理论工作者,特别是代数几何学家的重视,使代数几何码的研究得到了非常迅速的进展,取得了许多成果。现在,代数几何码的研究方兴未艾。

目前,利用纠错码降低各类数字通信系统以及计算机存贮和运算系统中的误码率,提高通信质量,延长计算机无故障运行时间等,在美国等西方国家中已作为一门标准技术而

广泛采用。而且纠错码技术还应用于超大规模集成电路设计中,以提高集成电路芯片的成品率,降低芯片的成本。不仅如此,自70年代末以来,纠错码技术已开始渗透到很多领域。利用纠错码中的许多编、译码原理和方法,与通信系统中的其它有关技术相结合,得到了令人惊喜的结果。例如,纠错码与调制技术相结合所产生的TCM技术,已作为国际通信中标准技术而推广使用。又如纠错码与密码相结合,可以构造出一类既能加密、签名,又具有纠、检错功能的密码系统;纠错码与信源编码相结合的结果,使得通信系统更为有效与可靠。不仅如此,纠错码中的许多译码思想和方法,与神经网络中的能量函数有密切关系,纠错码中的许多译码技术,可以用来解决神经网络中的一些问题。因此,可以预料,随着科学的进步和实际的需要,纠错码理论必将进一步发展,它的应用范围必将进一步扩大。

本书共分三部分。第一部分介绍学习纠错码所必需的数学基础,包括第二、四章和第八章的前一部分。这部分内容介绍了群、环、域、格、线性空间和矩阵等的基本概念,详细讨论了有限域的性质和构造,以及代数几何的基本知识。这一部分内容也可以作为一门基础课(约3学分)单独讲述。第二部分包括第一、三章及第五章至第九章的内容。这部分介绍了线性分组码的基本概念和主要码类,如:汉明码、循环码、BCH码、RS码、不等保护能力码和代数几何码等的基本原理与构造方法。这部分还介绍了各种译码方法如:最小汉明距离译码、捕错译码、大数逻辑译码、迭代译码、频域译码和软判决译码等。第二部分是本书的主要内容。第三部分包括第十章至第十二章,主要介绍卷积码的基本概念及其有关的译码方法,如大数逻辑译码、维特比译码和序列译码等,并讨论了编码与调制相结合的TCM技术。第二、三部分内容是纠错码的核心(约需3~4学分)。

纠错码的内容非常丰富,涉及的领域较广,所需的数学知识较多、较深。由于篇幅所限,本书不可能详细介绍所有内容,仅讨论纠错码理论中比较基本和重要的,并在实际中用得较多的各种码的编译码原理和方法。

本书对材料的选择和问题的阐述循序渐进,在内容上既有必要的数学证明,又着重于物理概念的解释。内容比较新颖、全面和系统,并力求反映出纠错码理论的最近成果。全书中有大量的各种最佳码表,以便读者选择应用。每章后都附有习题,以便读者加深对内容的了解和掌握各种编译码方法。书中有*号的章节为较深或较新的内容,可视情况选读。

本书第十三章由孙蓉同志编写,第八章由肖国镇同志编写,其余各章均由王新梅同志编写。

作者衷心地感谢我们的老师陈太一教授和胡征教授。早在60年代初,他们领导的信息论和编码讨论班上,不仅为年青一代讲授了当时最新的科学知识,把我们带入了信息论这一领域。而且,他们所提倡的那种自由争论的学术气氛和民主、平等的学术环境,使当时作为学生和讨论班成员的第一作者终身难忘,并深刻地影响了作者以后的工作和发展方向。

在70年代初、中期,由王育民、梁传甲、顾慰文和尹克震等教授以及我们一起组成的编码和密码讨论班上,共同经历了风风雨雨的几年,在那动荡、压抑的年代编写了几套讲义。其中《纠错编码讲义》比较全面系统地收集了当时最新的研究成果。文革后,在此讲义基础上,并参考了当时美国夏威夷大学林舒(S. Lin)教授和科斯特洛(J. Costello)教授合著

的《差错控制编码：基础和应用》一书初稿中的内容，于1981年由第一作者编写出版了《纠错码》讲义，作为我校研究生和有关专业学生的教材。根据近十年教学实施的经验，以及纠错码的最近成果，对该讲义进行了补充、修改和删节编写了本书。因此，可以说本书是编码讨论班的集体结晶。

我们要特别感谢近几年来编码和密码讨论班中的所有老师和研究生们，特别是王育民教授和梁传甲教授。在这个温暖的集体中，我们不仅共同学习，讨论最新的成果、理论和方法，相互交流学术思想和观点，而且相互鼓励与支持，使我们在精神上得到了极大的鼓舞，谨以此书献给该集体的所有同志们。

此外，我们还要感谢关心该书出版的美国 Lehigh 大学的曾开明(K. M. Tzeng)教授、总参 57 所的宋国文总工程师以及西南交通大学的靳蕃教授和其他同志们。对吉筮琴工程师的大力支持与鼓励，以及细心、认真负责地抄写该书的全稿，表示深切谢意。

最后，我们还要特别感谢西安电子科技大学出版社和本书的责任编辑，在出版经费非常紧张的艰难时刻，大力支持本书的出版，并认真细致地编辑，使本书能顺利地与读者见面。

由于作者水平有限，错误遗漏在所难免，恳请读者批评指正。

本书得到国家自然科学基金的资助。

作 者

1991年2月

于西安电子科技大学



XDUP 0330

封面设计:年代设计有限公司



ISBN 7-5606-0163-4



9 787560 601632 >

ISBN 7-5606-0163-4/TN·0059 (课)

定价: 35.00元

目 录

第一章 纠错码的基本概念

§ 1.1 数字通信系统的组成及信道模型	1
§ 1.2 差错控制系统和纠错码分类	5
§ 1.3 最大似然译码和纠错码的基本概念	7
§ 1.4 信道编码定理	13
参考文献	16

第二章 代数初步

§ 2.1 整数的一些基本知识	17
§ 2.2 群和格的基本概念	25
§ 2.3 环与域的基本概念	30
§ 2.4 子群、正规子群和商群	32
§ 2.5 子格与划分	36
§ 2.6 线性空间和矩阵	38
习题	50
参考文献	51

第三章 线性分组码

§ 3.1 线性分组码的基本概念	52
§ 3.2 码的一致校验矩阵与生成矩阵	54
§ 3.3 伴随式与标准阵列及其它译码	59
* § 3.4 线性码的覆盖半径	65
§ 3.5 由一个已知码构造新码的简单方法	67
* § 3.6 用多个已知码构造新码的方法	70
§ 3.7 线性码的重量分布与译码错误概率	73
§ 3.8 线性码的纠错能力	79
* § 3.9 不等保护能力线性分组码	83
* § 3.10 纠非对称、单向错误及 t -EC/AUED 码	89
习题	97
参考文献	99

第四章 多项式环与有限域

§ 4.1 子环与理想	101
§ 4.2 多项式剩余类环	103
§ 4.3 循环群	113
§ 4.4 有限域(Galois 域)的乘法结构	117
§ 4.5 有限域加法结构	120

§ 4.6	有限域的代数结构与多项式的因式分解	130
* § 4.7	迹与对偶基	137
* § 4.8	孙子定理(中国剩余定理)	141
	习题	143
	参考文献	144
第五章 循环码		
§ 5.1	循环码与理想	145
§ 5.2	由生成多项式的根定义循环码	152
* § 5.3	幂等多项式和最小循环码	157
§ 5.4	缩短循环码与准循环码	159
* § 5.5	平方剩余码	162
§ 5.6	多项式及域元素运算电路	165
§ 5.7	循环码的编码电路	174
* § 5.8	循环码的谱表示与 MS 多项式	178
* § 5.9	序列线性复杂度与勃拉哈特(Blahut)定理	183
	习题	188
	参考文献	189
第六章 循环码的译码		
§ 6.1	循环码译码的一般原理	190
§ 6.2	捕错译码	197
§ 6.3	大数逻辑译码原理	206
§ 6.4	大数逻辑可译码的构造	213
§ 6.5	软判决译码的基本原理	220
§ 6.6	码字错误概率最小的软判决译码	229
	习题	239
	参考文献	240
第七章 BCH 码与 Goppa 码		
§ 7.1	BCH 码的描述及其距离限	242
§ 7.2	二进制 BCH 码及其扩展	251
§ 7.3	Reed—Solomon(RS)码	259
§ 7.4	BCH 码的一般译码方法	268
§ 7.5	BCH 码的迭代译码算法	277
* § 7.6	BCH 码的纠错删译码	291
§ 7.7	BCH 码的频域译码	293
§ 7.8	超 BCH 限译码	295
§ 7.9	Goppa 码的一般描述	298
§ 7.10	Goppa 码的扩展及其它特殊子类	304
* § 7.11	交替码(Alternant 码)和 GBCH 码	309
* § 7.12	交替码的欧几里德译码算法	313

习题	317
参考文献	318
第八章 代数几何码	
§ 8.1 代数几何的研究对象	319
§ 8.2 仿射空间与仿射变换	320
§ 8.3 射影空间与射影变换	323
§ 8.4 在有限域上的仿射曲线与射影曲线	324
§ 8.5 RS 码与 Goppa 码	325
§ 8.6 代数几何码的构成	329
§ 8.7 代数曲线中的一些重要概念	331
§ 8.8 Riemann-Roch 定理	335
§ 8.9 椭圆曲线码	338
习题	339
参考文献	340
第九章 纠突发错误循环码	
§ 9.1 基本码限	341
§ 9.2 纠单个错误循环码的构造	344
§ 9.3 纠定段(字节)突发错误码	352
§ 9.4 交错码与乘积码	356
§ 9.5 组合信道纠错码	361
* § 9.6 级联码与贾斯特逊(Justesen)码	363
§ 9.7 纠突发错误码的译码	369
习题	375
参考文献	376
第十章 卷积码基础	
§ 10.1 卷积码的基本概念	378
§ 10.2 卷积码的矩阵和多项式描述	380
§ 10.3 伴随式计算与一般译码	394
§ 10.4 误差传播	398
§ 10.5 卷积码的树图描述和距离特性	402
* § 10.6 卷积码的状态图表示和码的重量分布	409
习题	414
参考文献	415
第十一章 纠随机错误与纠突发错误卷积码	
§ 11.1 卷积码的大数逻辑译码	419
§ 11.2 非系统卷积码的大数逻辑译码	426
§ 11.3 纠突发错误卷积码的基本概念	428
§ 11.4 交错码	430
* § 11.5 岩垂(Iwadare)码	431

§ 11.6 扩散卷积码.....	435
* § 11.7 加拉格尔(Gallager)码	439
习题.....	441
参考文献.....	442
第十二章 卷积码的概率译码	
§ 12.1 Viterbi(VB)译码算法的基本原理和实现	443
§ 12.2 Viterbi 译码算法的性能	452
§ 12.3 适用于 VB 译码算法的码和删余码	455
§ 12.4 序列译码——Fano 译码算法	466
* § 12.5 序列译码——ST 译码算法	476
* § 12.6 序列译码的性能	479
* § 12.7 适用于序列译码的码	483
§ 12.8 调制与卷积码的结合(TCM 技术)	487
习题.....	502
参考文献.....	503
第十三章 Turbo 码	
§ 13.1 Turbo 码的提出	505
§ 13.2 Turbo 码编码器的组成	506
§ 13.3 Turbo 码的译码	507
§ 13.4 Turbo 码的分量码、交织器与性能限	517
§ 13.5 Turbo 码在实际通信系统(3GPP)中的应用	528
习题	531
附录 Turbo 码不同译码算法的比较	532
参考文献.....	533

第一章 纠错码的基本概念

本章主要介绍纠错码在数字通信系统中所处的地位，信道模型以及纠错码的某些基本概念和信道编码定理。

§ 1.1 数字通信系统的组成及信道模型

一、数字通信系统的组成

通信的目的是要把对方不知道的消息及时可靠地(有时还须秘密地)传送给对方,因此,要求一个通信系统传输消息必须可靠与快速,在数字通信系统中可靠与快速往往是一对矛盾。若要求快速,则必然使得每个数据码元所占的时间缩短、波形变窄、能量减少,从而在受到干扰后产生错误的可能性增加,传送消息的可靠性减低。若要求可靠,则使得传送消息的速率变慢。因此,如何较合理地解决可靠性与速度这一对矛盾,是正确设计一个通信系统关键问题之一。通信理论本身(包括纠错码)也正是在解决这对矛盾中不断发展起来的。

所有数字通信系统如通信、雷达、遥控遥测、数字计算机的存贮系统和内部运算以及数字计算机之间的数据传输等,都可归结成如图 1-1 所示的模型。

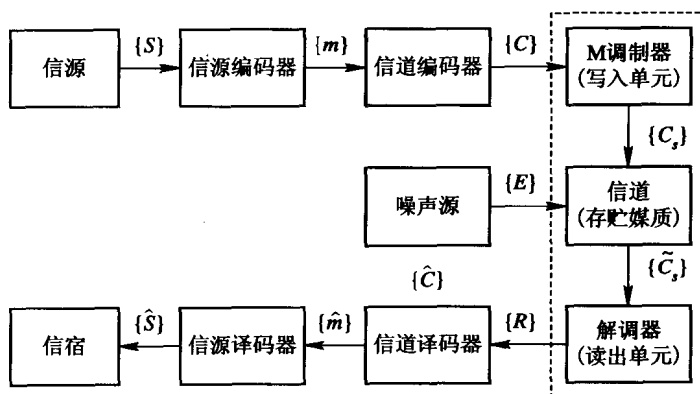


图 1-1 数字通信系统模型

图中,信源编码器是把信源发出的消息如语言、图像、文字等转换为二进制(也可转换为多进制)形式的信息序列,并且为了使传输有效,还去掉了一些与传输信息无关的多余度(有时为了保密,信源编码器后还可接上加密器)。为了抗击传输过程中的各种干

扰, 往往要人为地增加一些多余度, 使其具有自动检错或纠错能力, 这种功能由图中的信道编码器即纠错编码器完成。发射机(调制器)的功用是把纠错码送出的信息序列通过调制器转换成适合于信道传输的信号。数字信号在信道传输过程中, 总会遇到各种干扰而使信号失真, 这种失真信号传输到接收端的接收机, 进行解调, 变成二进制(或多进制)信息序列。由于信道干扰的影响, 该信息序列中可能已有错误, 经过信道译码器即纠错码译码器, 对其中的错误进行纠正, 再通过信源译码器(及解密器)恢复成原来的消息送给用户。

我们关心的是图中的信道编、译码器即纠错编、译码器两个方框, 为了研究方便, 将上述模型再进一步简化成图 1-2 所示的模型。在此模型中, 信源是指原来的信源和信源编码器, 其输出是二(多)进制信息序列。信道是包括发射机、实际信道(或称传输媒质)和接收机在内的广义信道(又称编码信道), 它的输入是二(多)进制数字序列, 输出一般也是二(多)进制数字序列, 而图中的信宿可以是人或计算机。

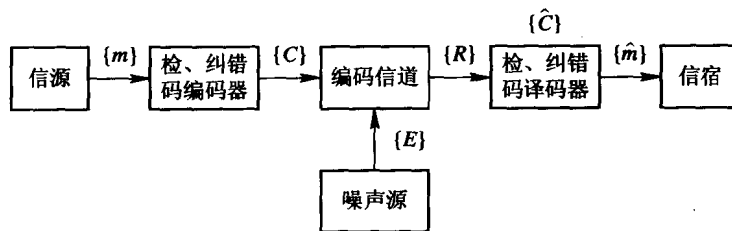


图 1-2 数字通信系统简化模型

二、信道模型

现在以图 1-2 的模型来讨论二进制数字序列通过该系统时所发生的情况。设从信源送出字母 A, 它的二进制序列为 11000, 以基带信号传送, 经发射机调制后, 送往信道的已调信号如图 1-3 所示。由于信道的干扰, 从信道输出端的信号产生了失真, 如图 1-4 所示。这些失真信号送入接收机进行判决时, 由于第一、二、四、五码元的波形失真不大, 容易正确地判为 1、1 和 0、0; 但对第三个码元来说, 由于失真严重而难于判决。这时有以下三种判决方法: 一是勉强作出是 0 还是 1 的判决, 即所谓**硬判决**; 另一种是对该码元暂且不作判决, 而输出一个未知或待定的信号“x”, 称其为**删除符号**; 第三种方法是输出一种有关该码元的信息, 例如关于 0 和 1 的后验概率或似然函数, 这种作法称为**软判决**。当然软判决的性能较好, 但实现起来较复杂。

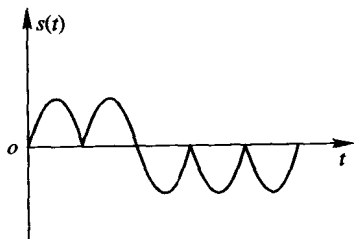


图 1-3 11000 发送的已调信号波形

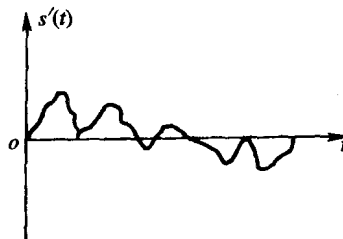


图 1-4 接收端收到的失真信号波形

在二进制硬判决情况下，信道可用图 1-5 所示的简单模型表示。图中， p_{01} 和 p_{10} 分别是 0 错成 1 和 1 错成 0 的概率，称信道转移概率。该信道的信道转移概率矩阵可用

$$P = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix} = \begin{bmatrix} 1 - p_{01} & p_{01} \\ p_{10} & 1 - p_{10} \end{bmatrix}$$

描述。如果 $p_{01} = p_{10} = p_e$ ，则称这种信道为**二进制对称信道**，简称 **BSC**。否则，称为**不对称信道**。若 p_{01} 或 p_{10} 等于零，则称为 **Z 信道**。通常 BSC 是一种**无记忆信道**，所以也称**随机信道**，它说明数据序列中出现的错误彼此无关。

如果信道的输入是二进制符号，而输出是离散的 $q (q = p^m \geq 2)$ 进制符号，如图 1-6 所示，且 $p(i|0) = p(q-1-i|1)$, $i = 0, 1, \dots, q-1$ ，则这种信道称为**离散无记忆信道 (DMC)**，显然 BSC 是 DMC 的一种特殊情况。DMC 的信道转移概率矩阵

$$P = \begin{bmatrix} p(0|0) & p(1|0) & \cdots & p(q-1|0) \\ p(0|1) & p(1|1) & \cdots & p(q-1|1) \end{bmatrix}$$

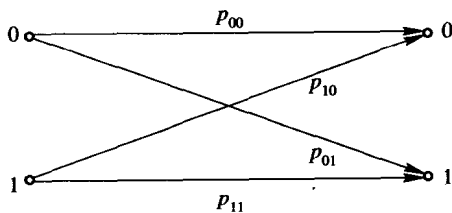


图 1-5 二进制信道

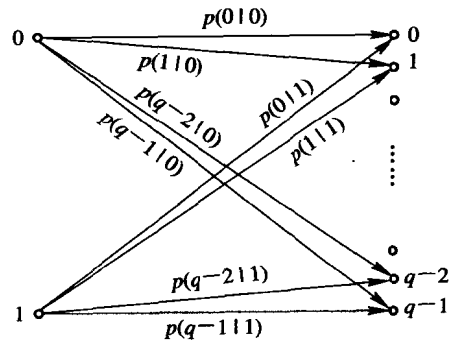


图 1-6 DMC

在作删除判决情况下，信道可用图 1-7 所示的模型表示，称为**二进制删除信道**，简称 **BEC**，一般它也是对称信道。图中， p_e 为信道的转移概率， q 为删除概率，在有删除处理情况下，信道的转移概率 p_e 一般很小，可忽略，因此把图 1-7 所示的模型用图 1-8 代替，称为**二进制纯删除信道**。以后所说的 BEC 都是指这种信道。应当指出，当码元作删除处理时，它在序列中的位置是已知的，仅不知其值是 0 还是 1，故对这种 BEC 信道的纠错要比 BSC 信道容易。

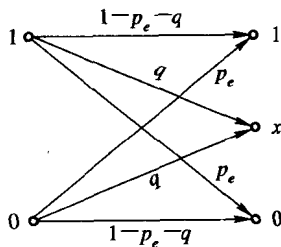


图 1-7 二进制删除信道

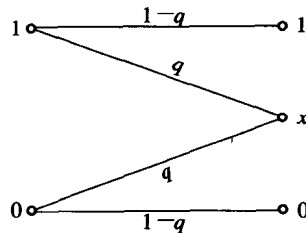


图 1-8 二进制纯删除信道

上述三种信道模型只是为了讨论问题方便而简化成理想的情况，它们表达了某些实际信道传送信号的主要特征。例如，卫星信道或深空信道，可近似看成是 BSC。但有很多实际信道如高频、散射、有线等信道，由于各种干扰所造成的错误，往往不是单个地而是成群成串地出现的，也就是一个错误的出现，往往引起其前后码元的错误(突发错误)，表现为错误之间的相关性。产生这种错误的信道称**有记忆信道或突发信道**。在计算机存贮系统中，磁带的缺陷或读写头接触不良所引起的错误，也属于这种类型。但由于实际信道干扰的复杂性，所引起的错误往往不是单纯的一种，而是两种错误形式并存，只不过有的信道以某种错误形式为主罢了。像这种随机错误与突发错误并存的信道，称为**组合信道或复合信道**。有关这些信道的模型请参阅[5]。作为检错与纠错用的抗干扰码，必须针对这几类信道，设计能纠正随机错误或纠正突发错误的码，或者设计既能纠正随机错误又能纠正突发错误的码。我们将首先讨论 BSC 和 BEC(包括多进制)的纠错编码问题，而后讨论纠正突发错误码，最后讨论组合信道的纠错码。

由于目前在信道中传输或计算机内部运算的数据序列，大部分是二进制数字序列，因此以后主要讨论二进制数字通信中的纠错码，当然这些纠错码往往可以推广到 q (素数或素数的幂)进制情况，这将在以后具体讨论时予以说明。二进制情况下，序列之间 0、1 两个符号按下列规则进行运算：

模 2 相加										
\oplus	<table style="border-collapse: collapse;"> <tr> <td style="border-right: 1px solid black; padding: 5px;"></td> <td style="padding: 5px;">0</td> <td style="padding: 5px;">1</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px;">0</td> <td style="padding: 5px;">0</td> <td style="padding: 5px;">1</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px;">1</td> <td style="padding: 5px;">1</td> <td style="padding: 5px;">0</td> </tr> </table>		0	1	0	0	1	1	1	0
	0	1								
0	0	1								
1	1	0								

模 2 相乘										
\otimes	<table style="border-collapse: collapse;"> <tr> <td style="border-right: 1px solid black; padding: 5px;"></td> <td style="padding: 5px;">0</td> <td style="padding: 5px;">1</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px;">0</td> <td style="padding: 5px;">0</td> <td style="padding: 5px;">0</td> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px;">1</td> <td style="padding: 5px;">0</td> <td style="padding: 5px;">1</td> </tr> </table>		0	1	0	0	0	1	0	1
	0	1								
0	0	0								
1	0	1								

为了简便，今后用 $+$ 和 \times 表示模 2 相加和相乘。在模 2 情况下，加和减是一回事。

三、错误图样

设发送的是 n 个码元长的序列 $C: (c_{n-1}, c_{n-2}, \dots, c_1, c_0)$ ，通过信道传输到达接收端(纠错码译码器输入端)的序列为 $R: (r_{n-1}, r_{n-2}, \dots, r_1, r_0)$ 。由于信道中存在干扰， R 序列中的某些码元可能与 C 序列中对应码元的值不同，也就是说产生了错误。由于二进制序列中的错误不外乎是 1 错成 0 或 0 错成 1，因此，如果把信道中的干扰也用二进制序列 $E: (e_{n-1}, e_{n-2}, \dots, e_1, e_0)$ 表示，则相应产生错误的各位 e_i 取值为 1，无错的各位取值为 0，而 R 就是 C 与 E 序列模 2 相加的结果，我们称 E 为信道的**错误图样**或干扰矢量。例如，发送序列 $C: (1111100000)$ ，收到的序列 $R: (1001010000)$ ，第二、三、五、六位产生了错误，因此信道的错误图样 E 的二、三、五、六位取值为 1，其它各位取值为 0，即 $E: (0110110000)$ 。用式子可表示成：

$$\begin{array}{r} \text{发送序列 } C: 1111100000 \\ \oplus \quad \text{错误图样 } E: 0110110000 \\ \hline \text{接收序列 } R: 1001010000 \end{array}$$

即 $R=C+E$ ，或 $E=R-C$ 。

信道干扰所造成的错误可在序列中的任一位出现，且也可以在 n 长序列中同时出现一位、二位……，甚至 n 位错误。因此，若发送的 C 序列长为 n ，则信道中可能产生的错误图

样 E 共有 2^n 种。

若为突发信道，则在错误图样 E 中，第一个 1 与最后一个 1 之间的长度称为**突发长度**，其图样称为**突发图样**。在该例中，突发图样是(11011)，突发长度为 5。

§ 1.2 差错控制系统和纠错码分类

一、差错控制系统分类

在数字通信系统中，利用纠错码或检错码进行差错控制的方式大致有以下几类：

(1) 重传反馈方式(ARQ)。应用 ARQ 方式纠错的通信系统如图 1-9 所示。发送端发出能够发现(检测)错误的码，接收端收到通过信道传来的码后，在译码器根据该码的编码规则，判决收到的码序列中是否有错误产生，并通过反馈信道把判决结果用判决信号告诉发端。发端根据这些判决信号，把接收端认为有错的消息再次传送，直到接收端认为正确接收为止。

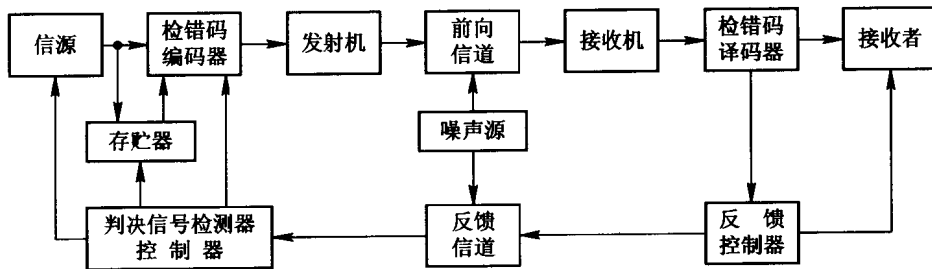


图 1-9 ARQ 通信系统

从上可知，应用 ARQ 方式必须有一反馈信道，一般较适用于一个用户对一个用户(点对点)的通信，且要求信源能够控制，系统收发两端必须互相配合、密切协作，因此这种方式的控制电路比较复杂。由于反馈重发的次数与信道干扰情况有关，若信道干扰很频繁，则系统经常处于重发消息的状态，因此这种方式传送消息的连贯性和实时性较差。该方式的优点是：编译码设备比较简单；在一定的多余度码元下，检错码的检错能力比纠错码的纠错能力要高得多，因而整个系统的纠错能力极强，能获得极低的误码率；由于检错码的检错能力与信道干扰的变化基本无关，因此这种系统的适应性很强，特别适应于短波、散射、有线等干扰情况特别复杂的信道中。

(2) 前向纠错方式(FEC)。利用前向纠错方式进行差错控制的数字通信系统如图 1-2 所示。发送端发送能够被纠错的码，接收端收到这些码后，通过纠错译码器不仅能自动地发现错误，而且能自动地纠正接收码字传输中的错误。这种方式的优点是不需要反馈信道，能进行一个用户对多个用户的同播通信，译码实时性较好，控制电路比 ARQ 的简单。其缺点是译码设备比较复杂，所选用的纠错码必须与信道的干扰情况相匹配，因而对信道的适应性较差。为了要获得比较低的误码率，往往必须以最坏的信道条件来设计纠错码，故所需的多余度码元比检错码要多得多，从而使编码效率很低。但由于这种方式能同播，特别适用于军用通信，并且随着编码理论的发展和编译码设备所需的大规模集成电路成本