该书由国家自然科学基金重大项目（No. 60496313）、东南大学移动通信国家重点实验室开放课题基金（A200506）和电子科技大学青年基金联合资助

LDPC 码原理与应用

文　红　符初生　周　亮　编著

电子科技大学出版社

图书在版编目（CIP）数据

LDPC 码原理与应用/文红，符初生，周亮编著. —成都：电子科技大学出版社，2006.5
ISBN 7-81114-114-0

Ⅰ. L … Ⅱ. ①文… ② 符… ③周… Ⅲ. 纠错码—通信理论 Ⅳ. TN911.2

中国版本图书馆 CIP 数据核字（2006）第 042411 号

内 容 简 介

LDPC 信道编码技术是编码界的重要成果之一。美国的 Gallager 教授早在 1962 年就提出了 LDPC 码，一直没有得到编码界的重视， 英国的 Mackay 教授等人在 1996 年“再发现”LDPC 码后，才轰动编码界，成为自信息论提出以来最重大的研究进展之一。LDPC 码迭代译码的思想也广泛用于通信技术的其他方面，如迭代信道估计、迭代均衡以及信号检测等。

本书介绍了 LDPC 码的编、译码基本原理及各种译码算法；详细分析了 LDPC 码的特点、分析方法；对无线移动通信信道模型下 LDPC 码的性能进行了剖析。各章原理的叙述力求概念清晰，注重理论推导和仿真试验验证相结合。

本书适用对象为大专院校信息类各专业本科高年级、研究生、教师及科研院所从事纠错编码、信号处理等领域研究的科研技术人员。

LDPC 码原理与应用

文 红 符初生 周 亮 编著

出　　版：电子科技大学出版社(成都建设北路二段四号　邮编：610054)
责任编辑：张　俊
发　　行：新华书店经销
印　　刷：四川锦祝印务公司
开　　本：185mm×260mm　　**印张**　11.25　　**字数**　273　千字
版　　次：2006 年 4 月第一版
印　　次：2006 年 4 月第一次印刷
书　　号：ISBN 7-81114-114-0/TN・3
印　　数：1—1000 册
定　　价：24.80 元

■ 版权所有 侵权必究 ■

◆ 邮购本书请与本社发行科联系。电话：（028）83201635　邮编：610054
◆ 本书如有缺页、破损、装订错误，请寄回印刷厂调换。

序　言

21 世纪，随着经济的增长、社会的发展和人们物质生活及精神生活水平的提高，人们对通信提出了更新、更高的要求。特别是近十年来，随着无线与移动通信应用的持续快速发展，使人类离实现无所不在的通信理想向前大大地迈进了一步。随着全球移动通信用户量和业务的高速增长，研究和应用新技术以提高无线通信的频谱利用率，最大限度地利用频域、时域、码域、空域等各种资源，为未来需求提供大容量通信能力，是全球无线通信技术领域的研究热点。

无线通信领域正在发展很多面向未来的先进技术，这些先进技术将大大提高无线通信系统的频谱利用率和信息传输容量，增强系统的性能和功能。其中，LDPC 信道编码技术是近年来全球的热点研究新技术，在该技术上取得的突破，将使未来的无线与移动系统更加先进，能够更好地满足人类的需要。

LDPC 信道编码技术是编码界的重要成果之一。美国的 Gallager 教授早在 1962 年提出 LDPC 码，一直没有得到编码界的重视，英国的 Mackay 教授等人在 1996 年“再发现”LDPC 码后，才轰动编码界，成为自信息论提出以来最重大的研究进展之一。理论研究表明：1/2 码率的 LDPC 码在 BPSK 调制下的性能距信息论中的 Shannon 限仅差 0.0045dB，是目前距 Shannon 限最近的纠错码。LDPC 码与高效调制相结合，能满足下一代移动通信高速数据大容量传输的迫切要求。LDPC 码迭代译码的思想现已广泛用于通信技术的其他方面，为实现迭代信道估计、迭代均衡以及信号检测提供了新的思路。

本书是国内第一本系统介绍 LDPC 编、译码基本原理及其应用技术的著作。作者是从事该技术研究的青年研究工作者，作者结合近年来的研究成果，介绍了 LDPC 码的基本编码和译码原理及各种译码算法；详细分析了 LDPC 码的特点、分析方法；对无线移动通信信道模型下 LDPC 码的性能进行了剖析。本书通俗易懂，对于有志于从事 LDPC 码理论及应用研究的人员来说，本书有助于引导其快速进入该研究领域；也适合从事无线与移动通信技术研究和应用的各类技术人员了解 LDPC 编码技术。

本书的出版将促进 LDPC 码在面向未来的下一代移动通信中应用。

李少谦

2006 年 4 月

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

纠错编码是数字通信系统和计算机系统的重要组成部分。随着信息时代的到来及飞速发展，今天的纠错码已不单是一个理论上探讨的问题，它已成为现代通信领域不可或缺的一项标准技术。现代通信系统要求能够对话音、数据以及图像等大数据信息量实现高速实时传输；同时无线与移动通信应用的持续快速发展，使得对高数据率数字移动通信等领域所采用的纠错编码技术要求越来越高。

LDPC 信道编码技术是编码界的重要成果之一。1/2 码率的二元 LDPC 码在 AWGN 信道下的性能距信息论中的 Shannon 限仅差 0.0045dB，是目前距 Shannon 限最近的纠错码。LDPC 码与高效调制相结合，能满足下一代移动通信高速数据大容量传输的迫切要求。LDPC 码迭代译码的思想也为实现迭代信道估计、迭代均衡以及信号检测提供了新的思路。

LDPC 码“再发现”近十年来国内、外研究成果丰硕，本书在参考这些国内、外研究硕果的同时，结合自己的研究成果编写了本书。本书反映了 LDPC 码领域有实际应用意义的研究成果和最新的研究进展。

本书编写过程中参考了众多的国内、外参考文献，在本书最后均列出，在此对参考文献的作者表示感谢。

作者要感谢西南交通大学的靳蕃教授，是他引领作者走入纠错编码的研究领域；还要感谢师兄张忠培，在本书的编写中得到了他大力的鼓励和支持。

在这里，要特别感谢电子科技大学通信抗干扰试验室的李少谦教授为本书作序，正是通信抗干扰试验室的科研氛围和各方面的支持使作者完成本书的撰写。

由于作者水平有限，错误、遗漏之处在所难免，恳请专家和读者批评指正。

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第一章 绪 论

本章介绍信道编码在数字通信系统中所处的地位，信道编码技术的发展历史及 LDPC 码目前的研究现状。

1.1 数字通信系统的结构

通信的目的是把对方不知道的消息及时可靠地传送给对方。随着对高效、高可靠性数字通信系统需求的迅猛增长，大规模高速宽带网络的发展使语音、图像和其他多媒体信息的传输成为可能。通信系统设计人员最关心的是如何在数据源功率和带宽有限，系统复杂性和设备造价尽可能小的条件下实现尽可能准确的信息传输，即使信息传输的误码率最小化。信道编码是消除或降低信息错误概率的有效手段之一。为更好的理解信道编码在数字通信系统中的地位和作用，下面首先介绍通用数字通信系统的基本组成结构。

所有数字通信系统如通信、雷达、遥控遥测、数字计算机存储系统的内部运算以及数字计算机之间的数据传输等，都可归纳成如图 1-1 所示的模型。

图中，信源是产生需要传输的信息。信息可以是模拟信号，也可以是数字信号。如果信源是模拟信号，则在送入数字系统传输之前需要进行采样和数字化处理；如果是数字信号则可以是字、码字等符号，一般将这些称为码元。信源的输出根据给定的码表转化成符号序列，一般情况下常用的是二元符号序列，码字符号中的码元取自集合{0，1}，这时码元又称为比特。如果信源编码器的输出信号为 r_b bit/s，则称 r_b 为数据传输速率，简称为数据率。

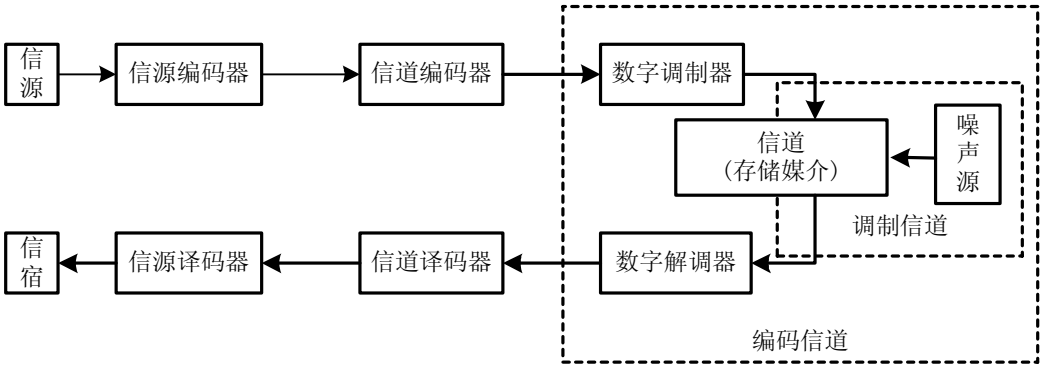

图 1-1 数字通信系统基本组成

信源编码器的任务是将信源发出的消息如语言、图像、文字等转换成为能够抵抗信道噪声和失真以及有利于在传输媒质上进行的传输形式，信源输出经过信源编码器编码后得到的数字序列称为信息序列。

信道编码是在发送器和接收器之间实现信号可靠传输的必要手段之一。传输信道存在

一定的噪声和衰落，必然会对其上传输的信息引入失真和信号判决错误，因此需要采用差错控制码来检测和纠正这些比特错误。信道编码器的作用是在信息序列中嵌入冗余码元，提高其纠错能力。信道编码的冗余码元的作用是减小传输中发生的信号和码元错误，提高系统的可靠性。

下面主要考虑二元有限域上的信道编码，因此不再区分码元和比特的概念。信道编码的基本思想是将每 k 个连续的信息比特分为一组，经过适当的编码后得到 n 个比特的输出，这 n 个比特组成的序列称为一个码字。好的差错控制码所生成的码字应该是在码字集合中，所有码字之间的区别尽可能大，从而使通信系统中的无法纠正或检测的信道错误尽可能少，k 个信息比特与 n 个码字比特的比值称为编码速率，简称码率 R，即：

$$R = \frac{k}{n}$$

从而经过信道编码后的数据率为

$$r_c = \frac{r_b}{R} = \frac{r_b n}{k} (\text{bit/s})$$

差错控制码的基本目标是在有限的信号功率、系统带宽和硬件复杂性要求下使通信的可靠性最大，这个目标是通过在信息序列中引入冗余比特来实现的。与未编码系统相比，信道编码会导致数据传输率的降低或者对信道带宽的要求增加。

数字调制器的作用是使信息变成能够适应信道传输的信号。如比特形式的信息是不适合在物理信道上传输的，因此需要利用数字调制器将这些编码比特转化成适合于在信道上传输的连续波形信号。通过相应方式调制可以在相同的物理信道上同时传输多个信息比特（数目与具体的调制方式有关：如 8PSK 调制下可同时传输 3 比特信息，16QAM 调制下可同时传输 4 比特信息），从而提高信息传输速率。调制器的基本思想是将编码的数字序列映射成适合在信道上传输的模拟连续信号。具体地说，M 维调制器可以将 l 个二元数字符号映射成一个有 M 种不同波形的模拟连续信号

$$M = 2^l$$

如果调制器输出的每个信号的持续时间为 T，则称 T 为信号间隔，而称 $1/T$ 为符号速率。如果定义信号带宽的最小值为 r_s (Hz)，则可以表示为

$$r_s = \frac{r_b}{Rl} = \frac{r_b n}{kl} (\text{Hz})$$

信号经过调制器后送入物理信道进行传输。典型的传输信道包括有线信道、光纤信道、无线信道、卫星信道、磁记录信道以及水下声音信道等。无论是哪一种传输媒体，都会引入一定的传输噪声，使传输信号发生一定的失真。而且由于信道带宽资源有限，通常需要为不同的通信业务分配不同的传输频率和带宽。因此，在实际的信道中存在的两个主要问题就是信道固有的噪声和有限的带宽限制。此外，移动信道会受到多径传播的影响，卫星信道会受到信号功率衰减的影响等，这些在系统设计过程中都应该考虑。

信号到达接收端，在接收机中，数字解调器的作用是通过对接收到的调制信号序列或传输码字进行最优估计，然后输出数字编码序列到信道译码器。信道译码器对传输消息进行估计和判决，估计准则是根据编码准则和信道特性而确定的，目的是使信道噪声所造成的信号判决错误最小化。

最后，信源译码器根据信源编码准则将得到的信道译码器输出的编码信息序列经过相应的信源译码后，得到对原始信源序列的估计并传递给用户。

因此，我们首先关心的是图 1-1 中的信道编、译码器两个方框。为了便于研究，将图 1-1 模型再进一步简化成如图 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、实际信道和接收机在内的广义信道（又称编码信道），它输入二（多）进制数字序列，输出一般也是二（多）进制数字序列。

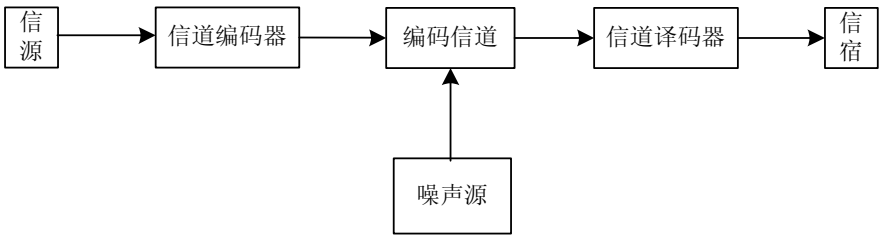

图 1-2　数字通信系统简化系统

1.2　信道编码技术的发展史

伴随着通信技术的飞速发展以及各种传输方式对可靠性要求的不断提高，差错控制编码技术作为抗干扰技术的一种重要手段，在数字通信领域和数字传输系统中显示出越来越重要的作用。由于通信信道固有的噪声和衰落特性，信号在经过信道传输到达通信接收端的过程中不可避免的会受到干扰而导致信号失真。通常需要采用差错控制码来检测和纠正有信道失真引起的信息传输错误。最早的纠错码主要是用于深空通信和卫星通信，随着数字蜂窝电话、数字电视以及高分辨率数字存储设备的出现，编码技术的应用已经不仅仅局限于科研和军事领域，而是逐渐在各种实现信息交流和存储的设备中得到成功应用。

1948 年 C. E. Shannon 发表的著名的《通信的数学理论》一文，为信道编码技术的发展指明了方向。Shannon 在著名的有噪信道编码定理中，给出了在数字通信系统中实现可靠通信的方法以及在特定信道上实现可靠通信的信息传输速率上限。Shannon 在他的证明中引用了三个基本条件：

(1) 采用随机的编译码方法；

(2) 构造码长的渐进好码或 Shannon 码；

(3) 译码采用最佳的最大似然译码算法。

50 多年来构造好码的思想基本上是按照 Shannon 所引用的基本条件的后两条为主线进行研究的。经过 50 年的不懈努力，各种差错控制编码方案不断涌现。

在 20 世纪 40 年代，R.Hamming 和 M.Golay 提出了第一个实用的差错控制编码方案，使编码理论这个应用数学分支的发展得到了极大的推动。Hamming 所采用的方法就是将输入数据每 4 个比特分为一组，然后通过计算将这些信息比特的线性组合得到 3 个校验比特，然后将得到的 7 个比特送入计算机。计算机按照一定的原则来读取这些码字，通过采用一定的算法，不仅能够检测到是否有错误发生，同时还可以找到发生单个比特错误的比特的

位置，该码可以纠正 7 个比特中所发生的单个比特错误。这个编码方法就是分组码的基本思想，Hamming 提出的编码方案后来被命名为汉明码。

虽然汉明码的思想是比较先进的，但是它也存在许多难以接受的缺点。首先，汉明码的编码效率比较低，它每 4 个比特编码就需要 3 个比特的冗余校验比特；另外，在一个码组中只能纠正单个的比特错误。M.Golay 研究了汉明码的这些缺点，并提出了两个以他自己的名字命名的高性能码字：一个是二元 Golay 码，在这个码字中 Golay 将信息比特每 12 个分为一组，编码生成 11 个冗余校验比特。相应的译码算法可以纠正 3 个错误。另外一个是三元 Golay 码，它的操作对象是三元而非二元数字。三元 Golay 码将每 6 个三元符号分为一组，编码生成 5 个冗余校验三元符号。这样由 11 个三元符号组成的三元 Golay 码码字可以纠正 2 个错误。

1954 年 Reed 在 Muller 提出的分组码的基础上得到了一种新的分组码，称为 Reed-Muller 码（简记为 RM 码）。RM 码在汉明码和 Golay 码的基础上前进了一大步，在码字长度和纠错能力方面具有更强的适应性，RM 码是一类参数选择范围很广的分组码。1969 年到 1977 年之间，RM 码在火星探测方面得到了极为广泛的应用。即使在今天，RM 码也具有很高的研究价值，其快速的译码算法非常适合于光纤通信系统。

在 RM 码提出之后人们又提出了循环码的概念。循环码实际上也是一类分组码，但它的码字具有循环移位特性，即码字比特经过循环移位后仍然是码字集合中的码字。这种循环结构使码字的设计范围大大增加，同时大大简化了编译码结构。循环码的另外一个特点就是它可以用一个幂次为 $n-k$ 的多项式来表示，循环码也称为循环冗余校验（CRC，Cyclic Redundancy Check）码，并且可以用 Meggitt 译码器来实现译码。

Hocquenghem 在 1959 年，Bose 和 Ray-Chaudhuri 研究组在 1960 年几乎同时提出了 BCH 码（BCH，Bose Chaudhuri Hocquenghem），BCH 码是循环码的一个非常重要的子集，BCH 码的码字长度为 $n=q^m-1$，其中 m 为一个整数。二元 BCH 码的纠错能力限为 $t<(2^m-1)/2$。1960 年 Reed 和 Solomon 将 BCH 码扩展到了非二元的情况，得到了 RS（Reed-Solomon）码。RS 码的最大优点是其非二元特性可以纠正突发错误。但直到 1967 年 Berlekamp 给出了一个非常有效的译码算法之后，RS 码才得到了广泛的应用。此后，RS 码在 CD 播放器、DVD 播放器以及 CDPD(Cellular Digital Packet Dara)标准中都得到了很好的应用。

1955 年 Elias 等人提出了卷积码，卷积码与分组码的不同在于分组码在编码之前先将信息序列按照一定的数据块长度分组，然后对每一组信息进行独立编码，即对于 (n,k) 分组码来说，码字中的 $n-k$ 个检验元仅与本码字的 k 个信息元有关，而与其他码字的信息元无关。卷积码中的 $n-k$ 个校验元不仅与本码字的 k 个信息元有关，还与之前码字的信息元有关。

Forney 在 1966 年提出的两个短码构造长的串行级联的思想。其基本思想是将编制长码的过程分级完成，从而通过用短码级联构造长码的方法来提高纠错码的纠错能力。级联码的目标是构造具有较大等效分组长度的纠错码，并且允许将最大似然译码分为几个较简单的译码步骤，这样便得到一个次最优但实际可行的译码策略。其纠错能力强，译码也不复杂，展现了构造 Shannon 码美好前景。

20 世纪 70 年代期间，在构造 Shannon 码中一个重要成果是 1972 年由 Justeson 用级联构造的 Justeson 码，另一个重要成果是前苏联学者 Goppa 在用有理分式表示码字基础上所构造的 Goppa 码，其渐进性很好，但 n 很长时，真正构造出这种好码仍然很困难。构造

此为试读，需要完整PDF请访问：www.ertongbook.com

Shannon 码的一个重要突破是 80 年代初由 Goppa 提出的代数几何码。他将代数几何的理论和方法系统地应用于编码理论中，使得原来线性码中的重要参数如码长、距离、维数等具有全新的几何意义，代数几何码的研究成为 80 年代和 90 年代编码领域中研究热点之一。

在传统通信系统的最佳接收机中，解调器和译码器是独立的两个部分。在处理接收信号的过程中，解调器首先对调制器输入符号做最佳判决，然后将硬判决结果送给译码器；译码器再对编码器输入消息做最佳判决，纠正解调器可以发生的错误判决，这是硬判决译码的思想。事实上，经过解调器对符号的硬判决，丢失了很多有利于译码的信息。为了提高编码通信系统的性能，人们从信息论的角度对接收机中解调器与信道译码器的功能划分和接口重新进行了审视，提出了软判决译码方法，即解调器对输出不进行判决，送到译码器的是判决符号可能的概率值或未量化输出，而非硬判决值，则译码器就可以利用这些信息与编码信息综合做出判决，从而提高系统性能，这就是软判决译码的基本思想。研究表明，在接收机中解调器采用软输出可以得到比硬输出高 2dB 左右的附加编码增益。

软判决译码算法主要分为两大类：一类是使符号错误概率最小的逐位软判决译码算法，如 1974 年有 Bahl，Cocke，Jelinek 和 Raviv 共同提出的前向后向最大后验概率（MAP）译码算法（也称为 BCJR 算法）和 Lee 提出的前向 MAP 算法，1976 年 Hartman 和 Rudolph 提出的逐位译码算法（HR 算法）以及 1971 年 Weldon 提出的重量删除译码算法（WED 算法）等。另一类是使码字错误概率最小的逐组软判决译码方法，如 1966 年 Forney 提出的广义最小距离译码（GMD）算法、1972 年 Chase 提出的 Chase 算法以及 1967 年 Viterbi 提出的 Viterbi 译码算法等。

1974 年 J.Massey 提出了将编码与调制作为一个整体看待可能会提高系统性能的设想。此后，许多学者研究了将此设想付诸于实践的途径。其中，1982 年 Ungerboeck 提出的 TCM 概念是解决带宽和纠错这对矛盾的一个理想方案，它将纠错编码技术与调制技术有机结合，在不增加系统带宽要求的条件下通过扩展符号映射空间来达到提高编码增益的目的。TCM 技术奠定了限带信道上编码调制技术的研究基础，被认为是信道编码发展中的一个里程碑。另外，几乎在同一时期日本学者 Imai 提出了一种采用分组码的编码调制技术，称为 BCM(Block Coding Modulation)技术。它在衰落信道中的性能比较突出。

虽然软判决译码、级联码和编码调制技术都对信道码的设计和发展产生了重大影响，但是其增益与 Shannon 理论极限始终都存在 2~3dB 的差距。因此，在 Turbo 码提出以前，信道截止速率 R_0 一直被认为是差错控制码性能的实际极限，Shannon 极限仅仅是理论上的极限，是不可能达到的。

直到 1993 年 Turbo 码的提出以及 1996 年又发现的低密度校验（Low Density Parity Check，LDPC）码，才让人们看到了逼近 Shannon 限的可能。

1.3 LDPC 码的研究现状

Shannon 提出的有噪信道编码定理作为现代通信理论的基础，给出了在有噪信道上实现可靠通信的理论极限。虽然该定理指出了可以通过差错控制码在信息传输速率不大于信道容量的前提下实现可靠通信，但却没有给出具体实现差错控制编码的方法。

根据 Shannon 有噪信道编码定理，在信道传输速率 *R* 不超过信道容量 *C* 的前提下，只有在码组长度无限的码集合中随机地选择编码码字并且在接受端采用最大似然译码算法时，才能使误码率接近为零。但是最大似然译码的复杂性随着编码长度的增加而加大，当编码长度趋于无穷大时，最大似然译码是不可能实现的。所以人们认为随机性编译码仅仅是为证明定理存在性而引入的一种数学方法和手段，在实际的编码构造中是不可能实现的。

1993 年于瑞士日内瓦召开的国际通信会议上，C.Berrou、A.Glavieux 和 P.Thitimajshima 首次提出了一种新型信道编码方案——Turbo 码，由于它们很好地应用了 Shannon 信道编码定理中的随机性编、译码条件，从而获得了几乎接近 Shannon 理论极限的译码性能。

然而，虽然 Turbo 码标志着人们构造其性能接近 Shannon 限的好码的开始，但 Turbo 码仍未将随机化思想真正贯穿于其编译码的始终，而且它也有许多缺点：1) 译码时延大，这就使 Turbo 码在某些对时延要求高的通信系统(如数字电话)中的应用受到限制；2) 计算量大，为达到高码率需要很大的交织器，这就增加了时延；3) 有所谓的错误平层(error-floor)效应。

在深入研究 Turbo 码原理的过程中，1996 年 Mackay、Spielman 和 Wiberg 几乎同时发现：Gallager 早在 1962 年提出的低密度校验码(简称 LDPC 码，也称 Gallager 码)也是一个好码，具有更低的线性译码复杂度。Gallager 提出 LDPC 码后一直没有得到编码界的重视，只有 1981 年 Tanner 从图论的角度研究过 LDPC 码。

自 Mackay 等“再发现”LDPC 码后，人们的进一步研究表明：基于非规则双向图的 LDPC 长码的性能可以优于 Turbo 码，而且这样的码的性能可以非常接近 Shannon 限。其中一个原因也在于 LDPC 码具有良好的距离特性。由于 LDPC 码不仅具有良好的距离特性、小的译码错误概率和较低的译码复杂度，而且适当码长(比如大于 200)时，不存在错误平台，其码率容易调整。实验结果中的错误几乎均为可检测错误。所以 LDPC 码无论在理论上还是在实际上都具有极其重要的价值。LDPC 的重新发现是继 Turbo 码后在纠错编码领域又一重大进展。

下面简要介绍一下目前 LDPC 码在编、译码和理论研究的一些成就。

无论 Gallager 还是 Mackay 等都是用随机方法构造 LDPC 码，用随机法构造的 LDPC 码的码字参数选择灵活，但对于高码率、中短长度的 LDPC 码用随机法进行构造，要避免双向图中的四线循环是困难的，其没有一定的码结构，编码复杂度高。于是人们考虑用代数法构造 LDPC 码。

LDPC 码代数构造可采用几何方法、图论方法、实验设计方法、置换方法来设计。不同的构造方法都是为了实现以下几个目的：增大图中的环，优化非规则码的节点分布，减小编码复杂度，构造的 LDPC 码要有好的码性能。

M.G.Luby 等[19、20]指出，基于非规则图定义的码性能优于相应的基于规则图定义的码，在非二元有限域中定义码和采用具有非均匀行、列重量的非规则校验矩阵均可改善码的性能。在寻找好的码结构方面，Mackay 等[21]提出对非规则码采用先选择轮廓再选择结构的两步选择方法，验证了超泊松(Super Poisson)结构具有较好性能，并指出：能快速编码的 LDPC 矩阵通常具有下三角形结构。

T.J.Richardson 等[22]通过优化非规则图的次数结构来寻找逼近容量的非规则 LDPC 码。T.J.Richardson[23]探讨了要获得高效编码器如何确定校验矩阵稀疏度的问题，以及如何构造

码，使编码时间与码块长度实际上符合线性关系(线性时间编码)，而非通常认为的平方关系。M.G.Luby[24]等也提出了一类基于级联双向图的 LDPC 码，用于可删除信道，称为可删除码，它不仅是线性时间编码，而且也可实现线性时间译码。

D.A.Spielman[25]开发了一种试探法来寻找非规则 LDPC 码参数的好的分布，据此构建了在很低信噪比下误码率(Bit Error Rate ，BER)低于 Turbo 码的码率为 1/2 的 LDPC 码。Y.Mao 等[26]则基于性能准则，提出根据图中最小环长的分布来设计好的 LDPC 码的方法。

Y.Kou 和 S.Lin 等[27]探讨了基于有限几何学的 LDPC 码结构。S.Lin 研究团队的 B. Ammar 等提出用均衡不完全区组设计方法(Balanced Incomplete Block Design，BIBD)构造好的 LDPC 码[28]。J.Rosenthal 和 P.Von tobel[29]研究了基于 Ramanuja 图和按照 Margullis 的概念构建的规则 LDPC 码，其性能优于随机构造的(3，6)规则码。N.Vanica 等[30]则对 T.J.Richardson[22]的优化方法作了修正，用于存在符号间干扰的部分响应信道中 LDPC 码的优化。

Gallager[2、3]曾给出了两种 LDPC 码的迭代译码算法：硬判决和软判决算法。后者虽有好的性能，但太复杂；文献[31]中提出的消息传递算法可认为是二者的折衷。消息传递算法(Message Propagation，MP)有时也称置信传播(Belief Propagation，BP)算法。在 MP 译码算法中，节点到节点的消息是通过 Tanner 图传递的。D.Burshtein 和 G.Miller[32]利用扩展图的理论证明了消息传递算法具有的某些特性。F.R.Kschichang 等[33]指出：作为一种通用的消息传递算法，和积算法(Sum-Product Algorithm)实际上包含了大量的实际译码算法(如前向/后向算法、VB 算法、Pearls 传播算法等)，它可应用于任何因子图(factor graph)，众多的实际译码算法均可由和积算法框架导出。

Mackay 和 C.P.Heskth[34]研究了 LDPC 码采用 BP 算法译码并假定某个噪声电平时，译码性能随实际噪声变化的敏感程度，得出了实际与假定噪声失配对译码性能影响的函数关系。

译码算法的改进和优化离不开译码性能的分析。在译码性能分析的研究方面，M.G.Luby 等在文献[19]中给出了一种新的基于弓形连线的 concentration bounds 方法来分析 LDPC 码。对于 MP 译码器的收敛性能分析，存在这样的情况：当码块长度有限时，分析十分困难；而当允许码长趋于无限时则可大大简化分析。这可以理解为：给定迭代次数 t，从某个随机构造的 LDPC 图中随机选取某个信息(比特)节点，其成为长度小于 t 的环的组成部分的概率，当码长无限时趋于 0，因而可不考虑环，而将任一节点上的消息视为独立的。T.J.Richardson 等[20]将文献[19]中的方法(concentration theorem)从二元对称信道(Binary Symmetrical Channel，BSC)和二元 MP 译码算法的约束条件推广到各类信道模型，开发了一种在码块无限长假设条件下跟踪 LDPC 码 Tanner 图中消息概率的技术，称为“密度进化”算法的数值程序，来近似估计噪声门限(在该门限以下可望成功地采用 BP 算法)，提出了一种通用的方法来确定具有离散或连续输出字符集的任何二元输入无记忆信道中采用 MP 译码的 LDPC 码的性能。特别对于 BP 译码算法，该方法可提供任何所需精度的性能估计。

S.Y.Chung 等[35]利用消息分布的高斯近似(即假设所有消息具有不变的高斯概率密度函数(Probabibity density function)简化了密度演进算法，可在不降低精度前提下快速找到门限和快速、容易地优化密度的分布，有助于了解和-积算法译码器性能和优化非规则 LDPC 码。S.Y.Chung 等[46]将消息离散化，通过计算机迭代搜索寻找最优的节点次数分布，特别适合于

非规则码的分析，在二进制输入 AWGN 信道下，设计的码率 1/2、码长 10^7 的非规则 LDPC 码在错误概率 10^{-6} 时离 Shannon 限仅 0.0045dB。这是迄今为止报道出的性能最接近 Shannon 限的信道编码。

M.P.C.Fossorior[36][37]研究了降低复杂度的 LDPC 码的基于信度传播的迭代译码，提出了基于可靠性译码与信度传播译码相结合的 LDPC 译码算法，以获取译码性能和译码复杂性的折衷。“密度进化”应用于基于 BP(BP based)的译码算法的还包括 Pearls 的最大积(Max Product)算法[28][39][40]和 X.Wei[41]的最大对数映射(Max Log Map)算法等。为了改善 BP based 算法因在校验节点上作简化处理而导致性能的下降，J.Chen[42][43]提出了两种改进算法：采用归一化的近似最佳通用 BP based 译码算法(亦称为 Normalized BP based 算法)和通过降低可靠性值来改善外信息精度的 Offset BP based 算法。

近年来，LDPC 码的很多研究成果表明 LDPC 码是一类性能优异的好码。LDPC 码比 Turbo 码在技术上更具有优势，更能适应未来系统高速数据传输和高性能的要求。由于 LDPC 码提出较晚，因此与第三代移动通信标准失之交臂，但基于 LDPC 编码的方案极有可能成为第四代移动通信系统的应用方案，目前已有很多系统采用 LDPC 码。

基于 LDPC 码的编码方案已经被下一代卫星数字视频广播标准 DVB-S2 采纳。休斯网络系统是首批把 LDPC 码重新投入商用的公司之一。休斯将其 LDPC 作为可合成核心，向半导体公司发放许可证。目前至少有一个持有许可证的半导体公司已于 2004 年下半年提供业界首款基于 LDPC 的数字解调芯片，并将用于遵循 DVB-S2 的机顶盒。在我国地面数字电视传输标准建设备选的方案中，广电总局广科院的 Timi 方案性能较好。该方案最大的技术亮点就是采用了 LDPC 码信道编码技术。

在芯片方面，Comtech Telecommunications 旗下的 Comtech AHA 公司(AHA)已推出一种低密度奇偶校验码(LDPC)前向纠错(FEC)编/解码器内核。该 LDPC 码比其他商用 FEC 方式具有更高的误码率(BER)性能。由于整合了高反复性能，该 LDPC 码的 BER 比现有其他纠错技术更接近香农极限。此次推出的 LDPC 内核支持多种编码、调制格式及数据率，可动态改变以适应变化的信道条件。该内核以 FPGA 实现，支持高达 30Mbit/s 的数据率，块大小最高为 30kbit/s，输入量化多达 6 位，每块可编程反复达 256 次。此外该内核还可根据需求以 A-SIC 实现。AHA 的 LDPC 码适用于远距离传输或减少多种通信系统的传输功率，其应用包括无线、卫星通信、磁存储器及其他数据通信等。除了 30 Mb/s LDPC 内核外，AHA 还于 2005 年初推出一种单机的 LDPC 内核。

第二章　信道编码基础

不论那种编码方法，都需要遵循一些基本的定义和定理，都要使用一些恰当的表达方法。不同编码方法的性能差异因信号传输信道的不同而有所区别，因此需要考虑不同信道条件下的信道模型，不同的信道，其容量也不同。LDPC 码是一类分组码，本章首先简单介绍分组码的概念、编码方法以及译码方法；接着对几类典型信道模型的信道容量进行简单的介绍。

2.1　分组码的基本原理

2.1.1　线性分组码的概念

分组码是纠错码中最基本的一类编码方法，这里仅限讨论分组码类中最常用的一个子类——线性分组码。同时由于本文只讨论二元码，即码元取值为0或1，因此下面只涉及符号取自二元有限域$GF(2)$的线性分组码，即二元线性分组码。

线性分组码是把信息划成k个码元为一段(称为信息组)，通过编码器变成长为n个码元的一组，这n个码元的一组称为码字(码组)。在二进制情况下信息组共有2^k个，因此通过编码器后，相应的码字也有2^k个，称这2^k个码字集合为线性分组码，用(n,k)表示，　n表示码长，k表示信息位，码率$R=k/n$。二元线性分组码必须满足如下两个条件：

（1）码字集合中的任意两个码字经过模2加之后得到的结果仍然是码字集合中的一个码字。

（2）码字集合中包含有全零码字。

从数学角度讲，可以把一个(n,k)线性分组码看成二元n维线性空间上的k维子空间。因此，(n,k)线性分组码可以通过由k个线性无关的二元n维矢量集合$\{\boldsymbol{g}_0,\boldsymbol{g}_1,\mathrm{L}\ ,\boldsymbol{g}_{k-1}\}$来得到。得到的码字实际上是这些$n$维矢量根据信息序列分组中各个比特的取值而得到的线性组合。

2.1.2　生成矩阵和校验矩阵

线性分组码的编码过程可以描述为一个信息矢量$\boldsymbol{m}$和一个矩阵相乘的结果

$$\boldsymbol{C}=\boldsymbol{m}\cdot\boldsymbol{G} \tag{2-1}$$

其中，$\boldsymbol{G}$是由k个n维矢量$\{\boldsymbol{g}_0,\boldsymbol{g}_1,\mathrm{L}\ ,\boldsymbol{g}_{k-1}\}$构成的矩阵；$\boldsymbol{m}$是信息序列分组$\{m_0,m_1,\mathrm{L}\ ,m_{k-1}\}$；$\boldsymbol{C}$是编码得到的$n$维编码输出$\{c_0,c_1,\mathrm{L}\ ,c_{n-1}\}$，其中矢量与矩阵的乘法是在二元域$GF(2)$上进行的。

根据式(2–1)，码字$\boldsymbol{C}$可以表示为

$$\boldsymbol{C} = m_0 \cdot \boldsymbol{g}_0 + m_1 \cdot \boldsymbol{g}_1, \mathrm{L}\ , m_{k-1} \cdot \boldsymbol{g}_{k-1} \tag{2-2}$$

而矩阵$\boldsymbol{G}$称为编码生成矩阵，形式为

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{g}_0 \\ \boldsymbol{g}_1 \\ \mathrm{M} \\ \boldsymbol{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \Lambda & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \Lambda & g_{1,n-1} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} \\ g_{k-1,0} & g_{k-1,1} & \Lambda & g_{k-1,n-1} \end{bmatrix} \tag{2-3}$$

例如，对于一个二元(7,3)线性分组码，其生成矩阵可以为

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

如果编码信息分组为$\boldsymbol{m} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$

$$\boldsymbol{C} = \boldsymbol{mG} = \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

表2-1给出了(7,3)线性分组码的所有信息分组和生成码字。

表 2-1　(7,3)线性分组码的信息分组和码字

信息序列分组$\boldsymbol{m}$	码字$\boldsymbol{C}$
0　0　0	0　0　0　0　0　0　0
0　0　1	0　0　1　1　1　0　1
0　1　0	0　1　0　0　1　1　1
0　1　1	0　1　1　1　0　1　0
1　0　0	1　0　0　1　1　1　0
1　0　1	1　0　1　0　0　1　1
1　1　0	1　1　0　1　0　0　1
1　1　1	1　1　1　0　1　0　0

和每个线性分组码相联系的还有另一种有用的矩阵，对于任意有k个线性独立行的$k \times n$矩阵$\boldsymbol{G}$，存在有一个具有$n-k$行线性独立的$(n-k) \times n$阶矩阵$\boldsymbol{H}$，它使得$\boldsymbol{G}$的行空间中的任意向量都和$\boldsymbol{H}$的行正交，且与$\boldsymbol{H}$的行正交的任意向量都在$\boldsymbol{G}$的行空间中。因此我们用另一种方法来描述由$\boldsymbol{G}$生成的(n,k)线性码：一个n维向量$\boldsymbol{C}$是$\boldsymbol{G}$生成的码字中的码字，其充要条件为

$$\boldsymbol{C} \cdot \boldsymbol{H}^T = \boldsymbol{O}^T \tag{2-4}$$

此时$\boldsymbol{H}$称为一致校验矩阵。一般情况下，一个(n,k)码的$\boldsymbol{H}$矩阵可表示为

此为试读，需要完整PDF请访问：www.ertongbook.com