

摘要

低密度校验码是一种能逼近 Shannon 容量限的渐进好码，在长码时其性能甚至超过了 Turbo 码。它的译码采用的是基于置信传播的软输出迭代译码算法，复杂度很低，是一种次优的译码算法。由于低密度校验码具有诸多优点，它在信息可靠传输中的良好应用前景已经引起学术界和 IT 业界的高度重视，成为当今信道编码领域最受瞩目的研究热点之一，低密度校验码的应用也已经被提到日程上。

作者在理解 LDPC 码基本编译码理论的基础之上，深入分析了影响 LDPC 码性能的因素；并研究了采用最小和算法 LDPC 码的量化译码方案。

本文主要完成的工作有以下几个方面：

1. 基于因子图模型，介绍了 LDPC 码的表示和构造；详细介绍了 LDPC 码基于多种测度的软判决迭代译码（和积算法和最小和算法）。

2. 概括了影响 LDPC 码性能的主要因素。分析了度序列对长码性能的影响，介绍了结合密度进化（高斯逼近）和差分进化优化高斯信道下度序列的方法。分析了环对中、短码性能的影响，介绍了 PEG 构造方法。最后分析了 LDPC 码错误平层产生的原因，介绍并仿真了能有效的降低 LDPC 码错误平层的 ACE 算法。

3. 研究了 LDPC 码的量化译码，提出了一种基于密度进化理论优化设计低密度校验码最小和量化译码器的算法，该算法能够大大降低译码复杂度，同时译码性能损失很小。

LDPC 码的实用化还要走较长的一段路，虽然 LDPC 码的性能优越，但是编码问题一直很难解决。因此，LDPC 码的编码方面还需要进一步研究，如码的构造及线性编码问题。量化译码也是 LDPC 码实用化过程中的关键问题。本文仅对 LDPC 码量化译码做了粗浅的研究，如何设计一个复杂度低但性能好的量化译码器是值得研究的。

关键词：低密度校验码 性能分析 量化译码

Abstract

Low-Density Parity-Check (LDPC) codes are a class of capacity approaching error-correcting codes. By using low complexity algorithms based on belief propagation, LDPC codes can get near Shannon limit decoding performance. For long code lengths, LDPC codes can even outperform Turbo codes. Due to the advantages of LDPC codes, their applications in reliable communications have received great interests and have become one of most attractive field in channel coding community. Now, the application of LDPC has been put on the agenda.

This thesis investigates some aspects of LDPC codes with emphasis on performance analysis and quantization decoding schemes of LDPC codes. The main results and contents are as follows.

1. Based on Factor graph, the representation and construction of LDPC codes are addressed, and the soft decoding algorithm for LDPC codes, i.e., sum-product algorithm and minimum-sum algorithm, are discussed.

2. The major factors which impact LDPC codes' performance are summarized. *Analyzing the impact of degree distribution on the long-length LDPC codes and introducing the optimized degree distribution algorithm under the AWGN channel based on density evolution or Gaussian approximation and differential evolution.* The impact of cycles on the short-length LDPC codes is analyzed and the PEG algorithm is introduced. The ACE algorithm which can degrade the error floor efficiently is introduced.

3. Quantization decoding of LDPC codes is studied. An efficient quantization-decoding scheme is proposed which can greatly reduce the decoding complexity with a little performance loss.

Although long LDPC codes are good, the encoding problem is hard to solve. So the study of encoding and quantization decoding algorithm is essential to the practical use.

Keywords: Low-Density Parity-Check (LDPC) Codes performance analysis
quantization decoding

创新性声明

本人声明所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果；也不包含为获得西安电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中做了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：包晓燕

日期 2006年1月

关于论文使用授权的说明

本人完全了解西安电子科技大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属西安电子科技大学。本人保证毕业离校后，发表论文和使用论文工作成果时署名单位仍然为西安电子科技大学。学校有权保留送交论文的复印件，允许查阅和借阅论文；学校可以公布论文的全部或部分内容，可以允许采用影印、缩印或其它复印手段保存论文。（保密的论文在解密后遵循此规定）

本人签名：包晓燕

日期 2006年1月

导师签名：王树梅

日期 2006.1.12

第一章 绪论

本章简要介绍了数字通信与信道编码的关系，回顾了信道编码理论与技术的发展历程；给出了常见的几种信道模型及其容量计算；结合图模型的发展历史概述了LDPC码的历史和现状；最后总结了作者在攻读硕士期间所做的主要工作并给出了本文内容安排。

1.1 数字通信与信道编码

通信系统旨在将信息由信源高效、可靠、有时还需安全地传送到信宿。有扰通信信道的噪声会对传输信息产生干扰，从而可能降低通信可靠性。所以，通信系统设计的中心问题是在随机噪声干扰下如何有效而可靠地传输信息。一般地，通信系统的可靠性用错误比特率(BER)衡量，有效性用传输速率 R 比特/信道符号衡量。早期的人们普遍认为：通信系统的可靠性与有效性是一对不可调和的矛盾，在有扰通信信道上实现任意小错误概率的信息传输的唯一途径就是把传输速率降低至零^[2]。Shannon信息和编码理论的奠基性论文“通信的数学理论^[1]”于1948年发表之后，改变了这一观念。他首次阐明了在有扰信道中实现可靠通信的方法，指出实现有效而可靠地传输信息的途径是编码。在这篇论文中Shannon证明了数据压缩和传输的基本定律从而奠定了信息理论的基石，Shannon也因此被称为“信息论之父”。根据Shannon的信息理论，数字通信系统的基本组成如图1.1所示^[3]。

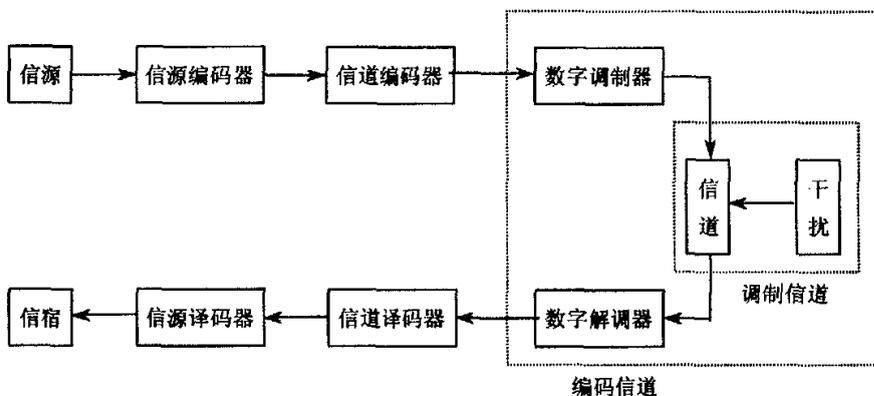


图 1.1 数字通信系统的模型

一般的通信系统均可以用图1.1来表示（如果将存储介质看成信道的话，存储系统也可以用上述模型表示，这时数字调制/解调器分别对应于写入/写出单元）。

如上图所示，发送端包含四个模块：信源、信源编码、信道编码和数字调制器。信源编码就是用二进制（或多进制）序列来表示信源输出的过程，其目的是除去信源的冗余以减少通信负担，因而也称为数据压缩。任何信源都有一个被称为信源熵的量，它表征了信源的平均不确定程度。信源编码定理^[4]指出信源熵是数据压缩的下界；信道编码与信源编码正相反，它通过在信息序列中引入冗余来实现通信的可靠性，任何信道都存在一个被称为信道容量的值，它表征了信道的传输能力；数字调制就是将信息序列映射成适合信道传输的信号的过程。对应地在接收端也有相应的四个模块用于实现相反的过程。

由于噪声是影响通信可靠性的关键因素，一个自然的想法是构建可靠的信道以减少噪声。但是这种想法在很多情况下是无法实现的，而且也没有必要。R. E. Blahut曾指出“与其花费大量的金钱去建造一条好的通信信道不如采用信道编码！”。因此，从通信系统的经济性角度考虑信道编码也是必不可少的。

综上所述，信道编码是解决通信有效性和可靠性这对矛盾的关键，也是实现通信系统经济性所必需的。但是，Shannon在[1]中关于信道编码定理的证明是存在性的，因而如何在实际系统中实现信道编码仍然是一个难题。

定理1.1（信道编码定理）^[5]

任意离散输入无记忆平稳有噪信道都有一个被称为信道容量的值 C ，它标志着信道传输能力的上限，只要信息传输速率 $R \leq C$ ，就存在一种编码方式，当平均码长足够大时，译码错误概率可以做到任意小；反之，则无论采用何种编码方式也不可能保证错误概率任意小。

信道编码定理和信源编码定理、率失真理论一起构成了Shannon三大编码定理。Shannon在证明上述信道编码定理时采用了三种技术：

- 1) 编码采用了随机编码思想；
- 2) 让码长趋于无穷；
- 3) 译码采用了最大似然译码。

1)、2)使得码本身具有卓越的纠错性能，而3)中的最大似然译码使得码的纠错性能得以充分发挥。但是，采用随机编码，使码长趋于无穷大并且采用最大似然译码将会使系统的复杂度和延时变得太大，因而无法在实际中使用。在半个多世纪的编码发展历程中，从Hamming码、BCH码、RS码、RM码、卷积码、级联码、代数几何码到逼近容量限的Turbo码和LDPC码，数学家和信息理论专家们为了达到Shannon容量限作了不懈的努力。在编码理论的最初阶段，人们一直倾向于用代数方法来实现差错控制编码，有限域、数论和有限几何等数学理论成了编码理论的主要工具。然而有趣的是，最终能够逼近Shannon容量限的Turbo码和LDPC码都部分地引入了随机编码的思想：Turbo码的交织器和LDPC码的稀疏校验矩阵，并

且它们的码长都较长，译码均采用了近似最大后验概率译码（当输入等概时，最大后验概率译码等价于最大似然译码）的迭代译码算法。换句话说，Shannon在证明信道编码定理的三种技术在最终逼近容量限的Turbo码和LDPC码中都有所体现。

1.2 信道模型和信道容量

信道就是信息传输的媒质。如图1.1所示，按照功能不同，信道可以分为调制信道和编码信道^[6]。这里只考虑编码信道。

假定平稳无记忆信道的输入取自 M 元符号集合，信道的输出取自 Q 元符号集合。在数字通信的接收端，解调器对接收波形进行处理，将受扰波形转换成一个标量或向量作为对传输数据的估计值，并将它送入判决器进行判决，判决输出 Q 元符号。实际上，可以将判决过程看成是一种量化过程，而判决器输出所采用符号集的大小对应为量化级数。当量化级数 $Q = M$ 时，称判决器作了一次硬判决；当量化级数 $Q > M$ 时，我们称判决器作了一次软判决^[3]。判决器的输出将作为译码器的输入。

1.2.1 几种常见的信道模型

1.2.1.1 二进制对称信道 (Binary Symmetric Channel, BSC)

考察一个二元输入加性噪声信道，令判决器作硬判决。如果信道噪声造成的错误是统计独立的，平均错误概率为 p ，那么可以用如下的转移概率来描述这个信道的统计特性：

$$\begin{aligned} P(Y=0|X=1) &= P(Y=1|X=0) = p \\ P(Y=1|X=1) &= P(Y=0|X=0) = 1-p \end{aligned} \quad (1-1)$$

我们称这种信道为二进制对称信道，其信道模型可以用图1.2表示。

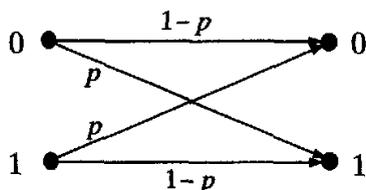


图1.2 二进制对称信道

1.2.1.2 离散输入连续输出信道

假定信道编码器的输出符号取自 $X = \{x_0, x_1, \dots, x_{q-1}\}$ ，译码器输入为连续值

$Y = R$ ，我们称这类信道为离散输入连续输出信道，典型的有二元输入高斯白噪声信道 (BIAWGN) 和二元拉普拉斯(Laplace) 信道^[7]。

二元输入高斯白噪声信道的输出可以用下式表示：

$$Y = X + N \quad (1-2)$$

其中， N 为加性高斯白噪声，其均值为零，方差为 σ^2 。给定一个输入 $X = x_k$ ， $k = 0, 1, \dots, q-1$ ，则 Y 是均值为 x_k ，方差为 σ^2 的高斯变量：

$$p(y | X = x_k) = \frac{1}{\sqrt{2\pi}\sigma} \exp\{-(y - x_k)/2\sigma^2\} \quad (1-3)$$

如果信道是无记忆的，则满足

$$p(y_1, y_2, \dots, y_n | X_1 = u_1, \dots, X_n = u_n) = \prod_{i=1}^n p(y_i | X_i = u_i) \quad (1-4)$$

1.2.2 信道容量

信道容量定义为信道输入与信道输出的互信息，它表征了信道可靠传输的最大速率。最常见的信道容量计算式就是带宽、功率受限下的加性高斯白噪声

(AWGN) 信道容量计算式。设 AWGN 信道带宽受限为 $[-W, W]$ ，噪声双边功率谱密度为 $N_0/2$ ，信号功率为 P ，则

$$C = W \log \left(1 + \frac{P}{N_0 W} \right) \quad (\text{bits/s}) \quad \text{式(1-5)}$$

这个容量仅在输入服从高斯分布的情况下可以达到。如果输入信号调制受限，那么容量将会小于上面这个值。下面我们考察其他几种典型信道的容量计算。

1.2.2.1 离散无记忆信道(Discrete Memoryless Channel, DMC)的容量

考虑一个离散无记忆信道，它的输入符号集为 $X = \{x_0, x_1, \dots, x_{q-1}\}$ ，输出符号集为 $Y = \{y_0, y_1, \dots, y_{q-1}\}$ ，并且转移概率为 $P(y_i | x_j)$ 。假定传输符号为 x_j ，接收到符号为 y_i ，则事件 $X = x_j$ 和事件 $Y = y_i$ 的互信息是 $\log[P(y_i | x_j)/P(y_i)]$ ，其中

$$P(y_i) = P(Y = y_i) = \sum_{x_0}^{x_{q-1}} P(x_i) P(y_i | x_i) \quad (1-6)$$

因此，输入集 X 和输出集 Y 之间的平均互信息为^[9]

$$I(X; Y) = \sum_{j=0}^{q-1} \sum_{i=0}^{q-1} P(x_j) P(y_i | x_j) \log \frac{P(y_i | x_j)}{P(y_i)} \quad (1-7)$$

由上式可知， $I(X; Y)$ 的值取决于输入符号集的概率分布 $\{P(x_j)\}$ 和信道的特性，即转移概率 $\{P(y_i | x_j)\}$ 。令 $I(X; Y)$ 在所有输入分布 $\{P(x_j)\}$ 中取得最大值，则这个最大值只与信道的特性 $\{P(y_i | x_j)\}$ 有关，它标志着信道的传输能力，称为信道

容量(capacity), 记为 C 。这样我们就得到了离散无记忆信道的容量计算式:

$$C = \max_{P(x_i)} I(X;Y) \\ = \max_{P(x_i)} \sum_{j=0}^{q-1} \sum_{i=1}^{Q-1} P(x_j) P(y_i | x_j) \log \frac{P(y_i | x_j)}{P(y_i)} \quad (1-8)$$

对转移概率为 p 的二进制对称信道而言, 当输入等概时, 互信息取得最大值, 信道容量为

$$C = 1 + p \log_2 p + (1-p) \log_2 (1-p) = 1 - H(p) \quad (1-9)$$

其中, $H(p)$ 是二元熵函数。

1.2.2.2 离散输入连续输出信道(Discrete-input, Continuous-output Channel)的容量

对于离散输入连续输出信道, 记输入符号集为 $X = \{x_0, x_1, \dots, x_{q-1}\}$, 输出符号集为 $Y = (-\infty, +\infty)$ 。在式(1-8)中, 将对输出符号的求和换成积分, 相应的概率 $P(y_i | x_j)$ 换成概率密度 $p(y | x_j)$, 这样就得到了离散输入连续输出信道的容量计算式^[3]

$$C = \max_{P(x_i)} \sum_{i=0}^{q-1} \int_{-\infty}^{+\infty} p(y | x_i) P(x_i) \log_2 \frac{p(y | x_i)}{p(y)} dy \quad (1-10)$$

按照式(1-10), 对二元输入高斯白噪声信道而言, 信道容量为

$$C = \frac{1}{2} \int_{-\infty}^{+\infty} p(y | \sqrt{E_s}) \log_2 \frac{p(y | \sqrt{E_s})}{p(y)} dy \\ + \frac{1}{2} \int_{-\infty}^{+\infty} p(y | -\sqrt{E_s}) \log_2 \frac{p(y | -\sqrt{E_s})}{p(y)} dy \quad (1-11)$$

其中 E_s 为每符号能量。

若对二元输入高斯信道的输出作硬判决, 则信道等效为一个BSC, 其转移概率为

$$p = \int_0^{+\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(y + \sqrt{E_s})^2}{2\sigma^2}\right\} dy \\ = \int_0^{+\infty} \frac{1}{\sqrt{\pi N_0}} \exp\left\{-\frac{(y + \sqrt{E_s})^2}{N_0}\right\} dy \\ = \int_0^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{[(y + \sqrt{E_s})/\sqrt{N_0/2}]^2}{2}\right\} d(y/\sqrt{N_0/2}) \quad (1-12) \\ = \int_{\sqrt{2E_s/N_0}}^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{t^2}{2}\right\} dt \quad (\text{令 } t = (y + \sqrt{E_s})/\sqrt{N_0/2}) \\ = Q(\sqrt{2E_s/N_0})$$

其中 $Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right) dx$ 。

将式(1-12)的转移概率代入式(1-9)就可以计算得出硬判决时的信道容量。图1.3给出了BIAWGN信道的软判决容量/硬判决容量与 $SNR = E_b/N_0$ 的关系。图1.4给出了AWGN信道的BPSK容量限和调制不受限的Shannon容量限。

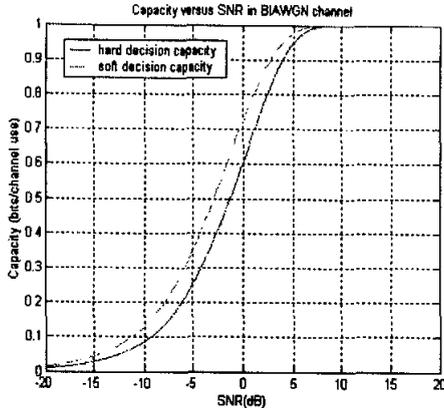


图1.3 BIAWGN信道的软判决与硬判决容量

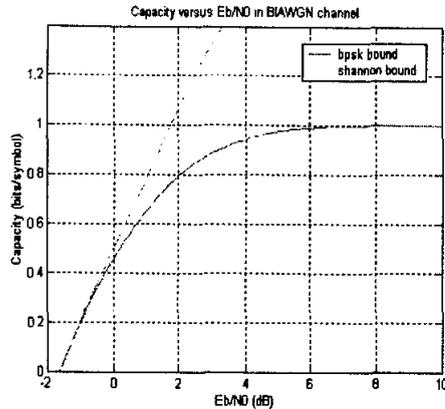


图1.4 BPSK容量限与Shannon容量限

由图1.3可知调制器采用软输出比硬输出有2dB左右的附加增益,这也就解释了为什么软判决译码一般要优于硬判决译码。由图1.4可以看出随着码率的增加BPSK容量限离Shannon容量限越来越远,而当码率较小时BPSK容量限基本与Shannon容量限一致。因此BPSK调制下,系统一般工作在中低噪比,同时码率也较小(小于等于1/2)。若系统工作在高信噪比,则可以选择更高维的调制以提高容量。

由图1.4 可得常见码率的Shannon容量限,例如1/2码率时Shannon容量限为0dB,相应的BPSK容量限约为0.2dB; 1/3码率时Shannon容量限约为-0.55dB,相应的BPSK容量限约为-0.5dB。

1.2.2.3 误比特率 p_b 与单位比特信噪比 E_b/N_0

给定信道容量 C , 由信道编码定理可知, 只要传输码率 R 低于 C , 就可以获得任意小的误比特率 p_b 。但是如果允许 p_b 大于零, 那么可获得更大的编码增益(即 E_b/N_0 可以进一步减小)。由信道编码逆定理^[5],

$$p_b \log(M-1) + H(p_b) \geq H_\infty(U) - \frac{\tau_s}{\tau_c} C \quad (1-13)$$

其中, M 为信源字母表的大小, $H_\infty(U)$ 为信源熵, 信源每 τ_s 秒产生一个字母, 信道容量为 C , 每 τ_c 秒产生一个信道符号, 则码率 $R = \tau_c/\tau_s$ 。对BPSK调制信号有 $M = 2$, $H_\infty(U) = 1$, 式(1-13)化为

$$C \geq R(1 - H(p_b)) \quad (1-14)$$

上式也可以从另外一个角度得到。通常，为了考察特定码的性能，可以通过仿真画出其误比特率和信噪比的关系曲线图，再与相同条件下的其它码作比较从而判断码的性能。下面讨论给定码率条件下误比特率和信噪比的理论最佳曲线的作法。接收端译码后误比特率为 p_b 的情形等效于发送端对信源作误比特率为 p_b 的编码而接收端译码无误的情形。由率失真理论可知，对二元输出信源作误比特率为 p_b 的编码所需的信源编码速率为 $1-H(p_b)$ 。令信道编码速率为 R ，则实际需要的 BIAWGN 信道容量为 $R(1-H(p_b))$ ，由信道编码定理即可得式(1-14)。图1.5为 BIAWGN 信道下码率为 $1/2$ 时，误比特率与单位比特信噪比的曲线图。

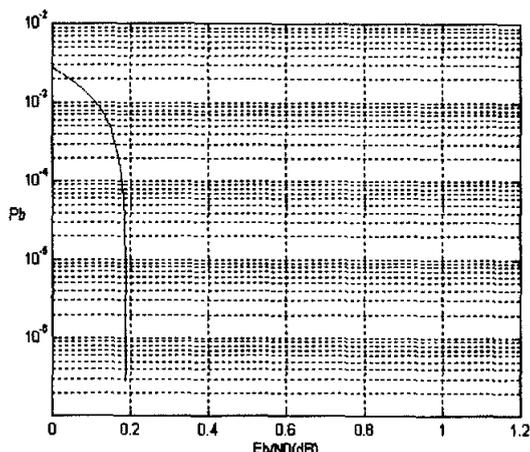


图1.5 BIAWGN信道下误比特率和信噪比的理论最佳曲线图（码率=1/2）

1.3 低密度校验码的历史和发展现状

早在1962年Gallager已经提出正则低密度校验码(regular low density parity check codes)和迭代译码(iterative decoding)的概念^[8]，然而直到上世纪90年代中期LDPC码被Spielman、Mackay和Neal等学者^[9,10]重新发现后，它才重新引起人们的广泛关注。为什么性能如此杰出的码会沉寂几十年才被人们认识呢？Gallager曾说过这是因为在LDPC码提出不久，Forney提出了级联码的思想，而当时大多数人都认为级联码更有可能取得好的性能。当然，还有一个原因就是当时的硬件水平尚未成熟，实现那么长的LDPC码(LDPC码的短、中码的码长已经达到几百、几千的量级)非常困难，致使LDPC码几十年来一直无人问津，只有寥寥几篇文章。其中有一篇是1981年Tanner发表的获奖文章“A recursive approach to low complexity codes”^[11]，当然这篇文章获奖已经是低密度校验码重新被人们认识后的事了。通过这篇文章，Tanner为基于图模型的码奠定了基石。文中引入了LDPC码的二部图模型

(bipartite graphical model, 现在称为Tanner图)。图1.6给出了一般LDPC码的Tanner图表示。图1.6中黑色圆圈表示码字中的符号, 方框表示局部约束关系。Tanner将LDPC码中的局部约束关系推广到一般的线性码中, 并发现上述模型包含了乘积码以及由简单码递归构造的码类。同时, Tanner还提出了现在所说的“最小和”算法(或者称为“最大积”算法)。Tanner对基于图模型码类的贡献使我们认识到: 如果对相对简单的码进行迭代译码, 那么译码器可以采用并行结构, 符合当今大规模集成电路技术的要求; 因为译码器可以有效地使用软判决信息, 并且采用了并行结构, 此外译码复杂度也很低, 所以即使对长码进行译码, 速度也很快。

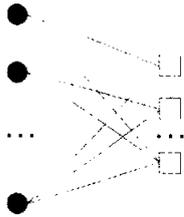


图1.6 LDPC码的Tanner图

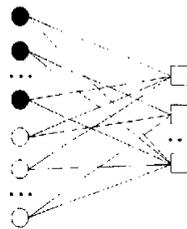


图1.7 因子图

LDPC码的复兴和Turbo码的出现紧密相关。1993年, C. Berrou, A. Glavieux, and P. Thitimajshima 提出令人震惊的Turbo码^[12]——离BIAWGN信道Shannon容量限只有0.5dB! Turbo码成为继Ungerboeck提出TCM^[13]之后信道编码的又一里程碑。Turbo码给人们带来了一个重要启示: 迭代译码可以获得接近最大似然译码的性能。于是, 迭代译码思想成为信道编码理论界的研究热点, 也被用在通信的各个方面, 如信道均衡。经过J.Hagenauer等人的总结, 迭代译码思想上升为现在我们所熟知的Turbo原理 (Turbo Principle)。与此同时, 各种Turbo-like码也纷纷涌现: Benedetto的串行级联Turbo码、Sipsier和Spilman的扩展码、Tornado码、重复累积(RA)码和李坪的CT码等等。当然这其中也有同样采用迭代译码的低密度校验码。(所有的Turbo-like码都由结构简单、译码复杂度低的分量码和伪随机置换矩阵组成, 并且Turbo-like码有两个共同点: 可以采用图模型表示、构造; 采用迭代译码思想。)

LDPC码研究的兴起, 除了Turbo码的研究热潮为它提供了契机, 还有两方面原因^[14]: 一方面是由于Spielman、Mackay等几位学者独立研究了低密度校验码, 发现LDPC码有杰出的纠错能力; 而另一方面是由于Wiberg在他的关于基于图模型码的论文中作了拓荒性的研究工作^[15,16]。Spielman在他的论文中基于扩展图(expander graphs), 基于LDPC码设计了一种具有渐进好纠错性能的码类, 称为扩展码^[9]。这种码可以线性时间编、译码。此后不久, Alon和Luby把这些结果应用到Internet丢包的问题中, 设计了Tornado码^[17]。Tornado码是第一个商用化的LDPC码。在删除信道中, 线性码的译码问题等价于解线性线性方程组, 通常求解一般线性方程组的时间复杂度不是线性的, 但是如果方程组中的每个方程都只有一个未知

数（或者通过迭代等效于每个方程只有一个未知数）的话，那么译码将变得非常简单。此后，Luby研究发现使用非规则图并优化度分布序列可以使码的性能逼近删除信道的容量限，即当传输速率接近 $1 - p$ 时（ p 为删除概率）可以取得非常小的误比特率。

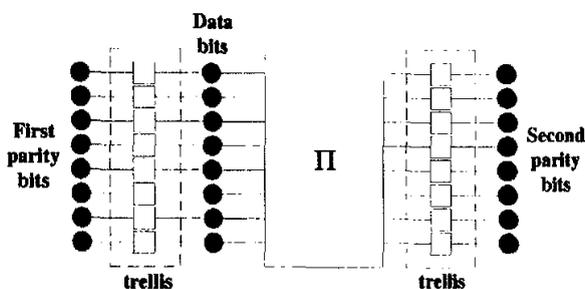


图1.8 Turbo码的因子图模型

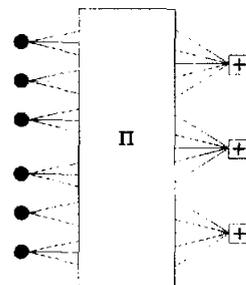


图1.9 LDPC码的因子图模型

Wiberg的最大贡献在于他把Tanner图进行了扩展，引入了状态节点。扩展后的图仍然是二部图，称为因子图（factor graph），因子图模型如图1.7所示。图1.8和图1.9分别为Turbo码和LDPC码的因子图模型。因子图中的符号节点与Tanner图中的符号节点含义一致，是可以观测得到的；而状态节点是内部的，不能由外部观测得到，它是由设计者添加用以简化码的图模型表示。引入状态节点使得图码和网格码得到了统一，图1.10为通常网格码的因子图模型。图中 A_k 为符号节点， S_k 为状态节点，而 C_k 是约束关系，它决定了允许的状态转移和输出 (s_k, a_k, s_{k+1}) （trellis section）。

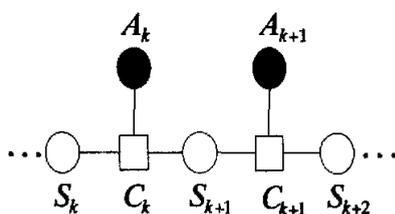


图1.10 网格码的因子图模型

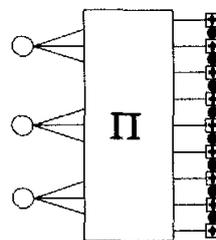


图1.11 RA码的因子图模型

除了对码的图模型表示作出了杰出贡献之外，Wiberg对译码也作了深入的研究。他明确地给出了最小和算法(min-sum algorithm)及和积算法(sum-product algorithm)的特征，并且指出如果用“求最小值”(min)运算代替“求和”(sum)运算，用“求和”(sum)运算代替“求积”(product)运算，那么这两种算法在本质上是一样的，更进一步他给出了“半环”(semiring)扩展。此外，Wiberg还证明了无环图上这两种算

法分别对应着最大似然译码和最大后验概率译码。特别地，在网格图上分别退化成Viterbi算法和BCJR算法。这些结果促使研究工作者将这两种算法应用到有环图中，也取得了令人非常满意的结果。

此后，经过众多学者的研究，LDPC码的理论研究得到了蓬勃发展。Tornado码的理论分析技术被Richardson、Urbanke等学者的发展之后，可以应用到AWGN信道中非规则LDPC码的长码设计当中以满足各种不同应用目的。给定一个具有任意度分布的二元LDPC码，这几位学者指出^[19]在对称信道中采用和积译码算法时概率密度的进化可以精确计算出来。此外，他们还证明了当码长足够大、迭代次数足够多时，存在一个门限值，如果噪声低于这个门限就可以实现无误传输。而这个门限值可以通过选择度分布序列进行优化。仿真结果表明用这种方法设计的码，当码长达到 10^5 时其性能要优于Turbo码。Chung等人设计了1/2码率的LDPC码，其门限值离Shannon限在0.0045dB之内^[20]。

Divsalar、McEliece等人提出的重复累积码(RA codes, repeat-accumulate codes)^[21]是一种构造非常简单的Turbo-like码，然而其性能却比Turbo码出现之前的任何码都好，离Shannon限在1.5dB之内。RA码的分量码是 $(n,1,n)$ 的重复码和2状态、码率为1的卷积码(其生成多项式为 $g(D)=1/(1+D)$)，分量码之间通过伪随机交织器连接，如图1.11所示。其他一些学者也提出一些简单码类，其性能与RA码相当，有的甚至更好。香港城市大学李坪博士所提出的CT码(concatenated tree codes)^[23]就是一例。CT码由M个2状态网格码通过交织器交错连接在一起。CT码可以看成是一种LDPC码，其译码复杂度很低，但是性能却和同样码长的Turbo码相当。这样看来，简单的码通过大的伪随机交织器连接在一起并且采用和积算法(sum-product algorithm)译码将会获得接近Shannon容量限的纠错性能。

近年来，LDPC码的理论研究已经取得了相当丰硕的成果。研究表明LDPC码具有如下一些优点：1)长码时，LDPC码的性能优于Turbo码。在二元输入加性白高斯噪声信道(BIAWGNC)下，Chung等人所优化设计的非规则LDPC码离Shannon容量限只有0.0045dB^[20]；2)LDPC码具有一套线性复杂度的译码算法，即消息传递算法，相比Turbo码的译码算法要简单得多，而且可以实现并行处理，因此其译码延时短，更适用于大吞吐量的应用场合；3)相对Turbo码而言，LDPC码具有更低的错误平层，并且多数译码错误都是可以检测的；4)由于LDPC码完全由其校验矩阵决定，因此可以灵活设计各种参数的LDPC码。正是因为这些原因，LDPC码已经被DVB-S2等一些国际标准所采纳。

正是由于LDPC码具有上述诸多优点，它在通信领域的许多方面都有很好的应用前景，如网络数据传输、光纤通信、深空通信、图像传输、下一代无线通信系统、磁记录、用户数据线(DSL)、数字图像水印等。LDPC码已经为几个国际标

准所采纳，国内外一些单位和公司已经研制开发出相应的LDPC码编译码器。2004年1月正式颁布的DVB-S2标准采用了LDPC码和BCH码级联的方式来实现纠错功能。Flarion公司已经开发出名为Vector-LDPC的LDPC码编译码器^[54]。

1.4 本文的主要研究工作和内容安排

作者采用理论分析和计算机仿真相结合的方法，对低密度校验码的理论进行了深入研究，取得了一些研究成果。全文共分四章，具体安排如下：

第一章回顾了信道编码理论与技术的发展历程，介绍了常见的几种信道模型及其容量计算，最后结合图模型的发展历程概述了LDPC码的历史和现状；第二章系统地阐述了低密度校验码基于图模型的编译码原理；第三章分析了影响低密度校验码性能的因素，介绍和仿真了相关优化算法；第四章介绍了低密度校验码的量化译码，提出了一种优化设计最小和量化译码器算法，该算法可以大大降低译码复杂性并且译码性能损失不大。

第二章 基于图模型的低密度校验码编译码原理

本章系统地概述了LDPC码的因子图表示,包括校验约束编码结构和后验概率译码结构;阐述了低密度校验码的构造方法;最后给出了置信传播算法在不同消息空间的等价性描述,介绍了和积算法和最小和算法。

2.1 LDPC码的因子图表示

因子图是一个表示因式分解结构的二部图(bipartite),图中每一个变量节点对应一个变量,每一个因子节点对应一个局部函数,当且仅当变量是局部函数的自变量时,相应的变量节点和函数节点之间存在一条连接边^[29]。

因子图是一个通用模型,它归纳了目前所有的图模型定义,认为图模型本质上是要表达一个全局函数到一组局部函数乘积的有效分解。在码表示应用中,因子图把编码过程中产生的码字约束分解为基于码元子集的局部约束,或者基于全概率公式把译码过程中码字的后验概率(APP)测度分解为码的先验约束和信道转移概率的乘积,实现基于局部函数的迭代边界计算,最后渐进地逼近最佳译码。

2.1.1 码结构表示

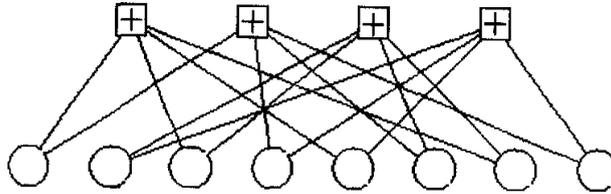
一个码长为 N 、信息位数为 k 的线性码由一个生成矩阵 $G_{k \times N}$ 定义,信息序列分组 $s_{1 \times k}$ 通过 G 被映射到码字 $x = sG$ 。线性码可以由一致校验矩阵 $H_{M \times N}$ 等效描述,所有码字均满足 $Hx^T = 0$ 。校验矩阵的每一行表示一个校验约束 z_i ,其中所有非零元素对应的码元变量 x_j 构成一个校验集,由一个校验方程表示。校验矩阵的每一列表示一个码元符号参与的校验约束。码元变量与校验方程之间的关系称为结构^[15]。下面,我们主要对二元LDPC码进行讨论。

LDPC码是一类线性码,由其校验矩阵具有的稀疏特点而命名,即 H 中的元素几乎全部是0,只有极少量的非零元素。Gallager最早定义的二元 (N, d_v, d_c) LDPC码是码字长度为 N 、设计码率为 $R_0 = 1 - d_v/d_c$ 的线性码,其校验矩阵 H 的每一列都包含正好 d_v 个“1”、每一行都包含正好 d_c 个“1”。由于满足这个结构条件的校验矩阵并不唯一,所以具有参数 (N, d_v, d_c) 的LDPC码构成了一个码集合。

一般, H 可以依上述结构条件随机生成,但所给码的性能差异较大。如果 H 矩阵各行线性独立,则实际码率 $R = R_0$;否则,实际码率 $R = (N - M')/N > R_0$,其中 M' 是 H 行空间的维数。

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \begin{cases} x_1 + x_3 + x_5 + x_7 = 0 \\ x_1 + x_4 + x_6 + x_8 = 0 \\ x_2 + x_3 + x_6 + x_7 = 0 \\ x_2 + x_4 + x_5 + x_8 = 0 \end{cases}$$

(a) 校验矩阵和方程组



(b) 因子图表示

图2.1 (8,2,4)LDPC码的校验系统及因子图表示

设一个 (N, d_v, d_c) 码 C 具有校验矩阵 $H = (h_{ij})_{M \times N}$, 其因子图模型可以表示为一个二部图。码字向量 $\mathbf{x} = (x_1, x_2, \dots, x_N)$ 表示为一组变量节点 $\{x_j : j = 1, \dots, N\}$, 校验约束表示为一组校验节点 $\{z_i : i = 1, \dots, M\}$ 。仅当 $h_{ij} = 1$ 时, 节点 x_j 和 z_i 之间由一条边连接, 节点 x_j 和 z_i 互称相邻节点, 其间连接边称为这两个节点的相邻边。因子图上每个变量节点具有 d_v 条入射边, 即度数为 d_v ; 每个校验节点具有 d_c 条入射边, 即度数为 d_c , 共有 $E = Nd_v = Md_c$ 条边。令集合 $M(j) = \{i : h_{ij} = 1\}$ 表示变量 x_j 的受限范围; 令 $N(i) = \{j : h_{ij} = 1\}$ 表示校验 z_i 的约束范围。

图2.1(a)是一个 $(8, 2, 4)$ 短码的校验矩阵及校验方程组, 图2.1(b)是相应的因子图表示。该图表示了校验约束结构码的全局函数 $f(x_1, \dots, x_8)$, 也称码特征函数。每个校验节点 z_i 表示一个局部约束函数 $f_i(\{x_j : j \in N(i)\})$ 。全局函数因式分解为

$$f(x_1, \dots, x_8) = f_1(x_1, x_3, x_5, x_7) f_2(x_1, x_4, x_6, x_8) f_3(x_2, x_3, x_6, x_7) f_4(x_2, x_4, x_5, x_8) \quad (2-1)$$

定义指示函数为一个把布尔逻辑命题 P 映射到 $\text{GF}(2)$ 上的二值函数^[29]:

$$[P] = \begin{cases} 1, & P = \text{true} \\ 0, & P = \text{false} \end{cases} \quad (2-2)$$

式(2-1)中的各个函数均为指示函数, 其中全局函数的逻辑命题为“ \mathbf{x} 是一个码字”, 每个局部函数的逻辑命题为图2.1(a)中的校验方程。式(2-1)又写作为

$$\begin{aligned} [\mathbf{x} \in C] = & [x_1 + x_3 + x_5 + x_7 = 0][x_1 + x_4 + x_6 + x_8 = 0] \\ & \cdot [x_2 + x_3 + x_6 + x_7 = 0][x_2 + x_4 + x_5 + x_8 = 0]. \end{aligned} \quad (2-3)$$

图2.1(b)的因子图实际上是一个有环Tanner图。注意到矩阵的第三列和第七列中, 1出现在第一行和第三行两个两行位置上, 对应在因子图中, 依照无向边连接关系, 存在一个长度为4的循环路径 (x_3, z_1) 、 (z_1, x_7) 、 (x_7, z_3) 、 (z_3, x_3) 。类似地, 图中还存在另一个长度为4的循环路径 (x_4, z_2) 、 (z_2, x_8) 、 (x_8, z_4) 、 (z_4, x_4) 。采用迭代置信传播算法译码时, 这种短环路将极大地影响码性能。码的最小汉明(Hamming)距离及距离谱直接取决于环路的分布情况。因此构造码时, 应该尽量消除短环路^[8,30,67]。

LDPC码的因子图表示中, E 条边对校验节点的入射关系和对变量节点的入射关系可以看作是相互置换, 所以一个特定的码集合实际是满足特定条件的随机置换函数集合。如果不限制变量节点和校验节点度数, 那么随机置换函数有可能导致变量节点和校验节点各自的度数不再恒定, 这时入射边分布表示为一对度数分布序列 $\lambda = (\lambda_1, \dots, \lambda_{d_v})$ 和 $\rho = (\rho_1, \dots, \rho_{d_c})$ ^[19,31], 其中 λ_j 和 ρ_i 分别表示度数 j 变量节点的入射边比例和度数 i 校验节点的入射边比例, d_v 和 d_c 分别是最大变量节点度数和最大校验节点度数。或用多项式 $\lambda(x) = \sum_{j=1}^{d_v} \lambda_j x^{j-1}$ 和 $\rho(x) = \sum_{i=1}^{d_c} \rho_i x^{i-1}$ 表示, 这时设计码率 $R_0(\lambda, \rho) = 1 - \int_0^1 \rho(x) dx / \int_0^1 \lambda(x) dx = 1 - (\sum_{i=2}^{d_c} \rho_i / i) / (\sum_{j=2}^{d_v} \lambda_j / j)$ 。

当度数分布多项式退化为 $\lambda(x) = x^{J-1}$ 和 $\rho(x) = x^{K-1}$ 时, 变量节点和校验节点的度数分别恒定为 J 和 K , 相应的码就称为 (N, J, K) 规则(regular)LDPC码, 反之称为非规则(irregular)LDPC码。规则LDPC码通常也称为Gallager码。具有优化度数分布 $\lambda(x)$ 和 $\rho(x)$ 的非规则LDPC码一般要好于规则LDPC码^[18], 而且优化的非规则LDPC长码的性能已经超过了最好的turbo码^[20,32]。

2.1.2 后验概率分布表示

考虑时间离散信道上的一个分组码 C , 设传输码字为 $\mathbf{x} = (x_1, x_2, \dots, x_N)$, 接收码字为 $\mathbf{y} = (y_1, y_2, \dots, y_N)$ 。根据全概率公式, 信道输入和输出向量的联合概率(密度)函数 $f(\mathbf{x}, \mathbf{y}) = P(\mathbf{x})f(\mathbf{y}|\mathbf{x})$, 其中 $P(\mathbf{x})$ 是发送码字 \mathbf{x} 的先验概率, $f(\mathbf{y}|\mathbf{x})$ 是发送码字 \mathbf{x} 时接收 \mathbf{y} 的条件概率(密度)函数或似然函数。基于给定的信道观察 \mathbf{y} , 对码字集合 C 的后验概率(APP)测度 $P(\mathbf{x}|\mathbf{y})$ 与联合概率函数 $f(\mathbf{x}, \mathbf{y})$ 成比例, 即^[49]

$$P(\mathbf{x}|\mathbf{y}) = f(\mathbf{x}, \mathbf{y})/f(\mathbf{y}) \propto f(\mathbf{x}, \mathbf{y}). \quad (2-4)$$

对于时间离散的平稳无记忆信道, 似然函数具有如下的乘积形式

$$f(\mathbf{y}|\mathbf{x}) = f(y_1, y_2, \dots, y_N | x_1, x_2, \dots, x_N) = \prod_{j=1}^N f(y_j | x_j), \quad (2-5)$$

其中 $f(y_j | x_j)$, $j = 1, \dots, N$, 是平稳信道的标量转移概率密度函数。

码字 \mathbf{x} 允许服从任何分布^[15]。如果假定所有码字被等概选取, 即先验概率 $P(\mathbf{x})$ 为一个常数, 结合形如式(2-1)的码特征函数, 可以表示为^[29]

$$P(x_1, x_2, \dots, x_N) = \frac{1}{|C|} f(x_1, x_2, \dots, x_N)。 \quad (2-6)$$

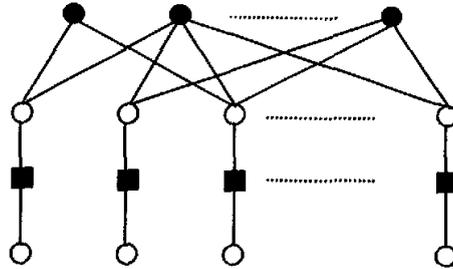


图2.2 LDPC码的后验概率测度因子图

因此, 联合概率函数 $f(\mathbf{x}, \mathbf{y})$ 可以比例表示为

$$f(x_1, x_2, \dots, x_N; y_1, y_2, \dots, y_N) \propto \prod_{i=1}^M f_i(\{x_k : k \in N(i)\}) \prod_{j=1}^N f(y_j | x_j)。 \quad (2-7)$$

代入式(2-4)得到后验概率测度, 即给定信道观察 \mathbf{y} 时, $\mathbf{x} \in C$ 的后验概率为

$$P(\mathbf{x} | \mathbf{y}) = \alpha \prod_{i=1}^M f_i(\{x_k : k \in N(i)\}) \prod_{j=1}^N f(y_j | x_j), \quad (2-8)$$

其中 α 是使 $\sum_{\mathbf{x} \in C} P(\mathbf{x} | \mathbf{y}) = 1$ 的归一化因子。

在表示LDPC码校验约束的因子图上, 增加接收变量节点 $\{y_j\}$ 及信道转移函数节点 $\{f(y_j | x_j)\}$, 得到如图2.2所示的表示码字后验概率分布 $P(\mathbf{x} | \mathbf{y})$ 的因子图。图中, 黑圆点表示局部校验函数, 等同于图2.1中的校验节点; 黑方块表示转移函数节点; 圆圈表示发送变量和接收变量节点。

2.2 LDPC码的构造

2.2.1 正则低密度校验码的构造

校验矩阵可以唯一确定一个线性分组码, 因此构造正则低密度校验码只需要构造它的校验矩阵。Gallager在文献[4,8]中采用 (n, j, k) 来表示一个正则低密度校验码, 其中 n 表示码长, j 表示校验矩阵中每列所含1的个数, 而 k 则表示校验矩阵中每行所含1的个数。Gallager采用随机置换的方法来构造校验矩阵, 方法如下:

Gallager构造正则低密度校验码的方法:

- 1) 将校验矩阵 H 分成 j 个子矩阵 H^1, H^2, \dots, H^j , 每个子矩阵有 $(n-k)/j$ 行, 并且每个子矩阵的每列有且只有一个 1;
- 2) 子矩阵 H^1 中的 1 呈下降的阶梯状排列, 即第 i 行的 k 个 1 从第 $(i-1)k+1$ 位排到第 ik 位;
- 3) 其余的子矩阵通过对 H^1 进行随机列置换得到, 所有置换是等概出现的。

若一个 (n, j, k) 正则低密度校验码的校验矩阵是满秩的, 设校验矩阵有 m 行, 根据校验矩阵中 1 的总数是固定的, 有:

$$mk = nj \Rightarrow \frac{m}{n} = \frac{j}{k} \quad (2-9)$$

因此, 这个 (n, j, k) 正则低密度校验码的码率可以简单计算如下:

$$R = \frac{n-m}{n} = 1 - \frac{m}{n} = 1 - \frac{j}{k} \quad (2-10)$$

从上面的构造方法不难知道, 由Gallager的方法构造的校验矩阵并不是满秩的。因此, 由Gallager的方法构造的低密度校验码的码率要略大于式(2-10)所计算的码率。Gallager曾给出了一个 $(20,3,4)$ 低密度校验码的校验矩阵, 如图2.3所示。

这里, 我们称由上述方法可以构造的低密度校验码类(ensemble)为Gallager码类。Gallager证明了关于Gallager码类的两个结果: 第一个是关于最小距离的。Gallager码类中, 码的最小距离是一个随机变量, 这个随机变量的分布函数可以用图2.4所示曲线作为上界。对 $j \geq 3$ 和 $k > j$ 的Gallager码类而言, 当码长趋于无穷时, 图2.4中的曲线逼近阶跃函数(跃变点处的坐标值与码长的比值是一个固定值, 记为 δ_{jk})。因此, 当码长 n 足够长时, 实际上Gallager码类中的所有码的最小距离至少为 $n\delta_{jk}$ 。第二个结果是关于误比特率的。Gallager证明: 对于Gallager码类, 在对称无记忆信道中, 采用最大似然译码时, 其误比特率随着码长的增加呈指数形式下降。这两个结果说明Gallager码类是相当好的码类。MacKay和Davey曾指出对任何码长和码率, 当平均列重 $j \sim 3$ 时, 随机构造的Gallager码离现在所知最好的码在零点几个dB之内^[33]。

1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1
0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0
0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0
0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0
0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1

图 2.3 (20,3,4)低密度校验码的校验矩阵

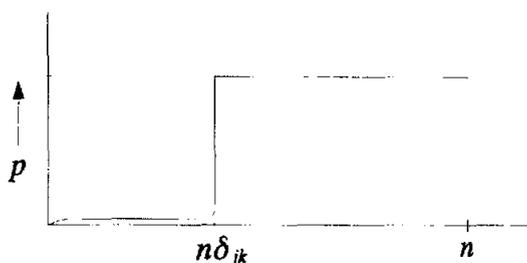


图2.4 最小距离分布函数简图

2.2.2 非正则低密度校验码的构造

理论上, 正则低密度校验的性能能够逼近Shannon容量限^[34], 但是这是当码长趋于无穷并采用最优译码器的情况下取得的。然而, 当码长无穷时, 最优译码的复杂度太高, 无法在实际应用中实现。实际上, 对于低密度校验码, 一般码长不可能太大而译码采用逼近最大后验概率译码的和积译码算法。因此, 正则低密度校验码的性能是否能完全被挖掘出来还要看具体的译码算法。

Gallager最初构造的低密度校验码是正则低密度较码, 它的校验矩阵的列重是个常数。另一种可选方案是允许校验矩阵的列重可以取几种不同的值, 这样构造的码称为非正则低密度校验码。Luby, Mitzenmacher, Shokrollahi和Spielman证明了精心选择非正则码的列重可以使它的性能超过相同参数的正则码^[25,36]。

非正则低密度校验码和正则码一样也可以通过它的图模型来描述。记度为 i 的

变量节点的个数为 Λ_i ，度为 j 的校验节点的个数为 P_j 。若非正则码的码长为 n ，码率为 R ，则有^[65]

$$n = \sum_i \Lambda_i, \sum_j P_j = n(1-R) \quad (2-11)$$

类似式(2-9)，根据Tanner图中按校验节点所连边的数目等于按变量节点所连边的数目，有

$$\sum_i i\Lambda_i = \sum_j jP_j \quad (2-12)$$

由变量节点度分布序列 $\{\Lambda_i\}$ 和校验节点度分布序列 $\{P_j\}$ ，定义多项式

$$\Lambda(x) = \sum_i \Lambda_i x^i \quad \text{和} \quad P(x) = \sum_j P_j x^j \quad (2-13)$$

由式(2-11)有 $\Lambda(1) = n, P(1) = n(1-R)$ ，码率为 $R = 1 - \Lambda(1)/P(1)$ 。对 $\Lambda(x)$ 和 $P(x)$ 求导可得，

$$\Lambda'(x) = \frac{d\Lambda(x)}{dx} = \sum_i i\Lambda_i x^{i-1} \quad (2-14)$$

$$P'(x) = \frac{dP(x)}{dx} = \sum_j jP_j x^{j-1} \quad (2-15)$$

令 $x=1$ ，有

$$\Lambda'(1) = P'(1) = \text{总边数} \quad (2-16)$$

从边的角度考虑，定义度分布序列 $\{\lambda_i\}$ 和 $\{\rho_j\}$ ，其中 λ_i 为与度为 i 的变量节点连接的边的数目占总边数的比例， ρ_j 为与度为 j 的校验节点的边的数目占总边数的比例。类似地定义多项式

$$\lambda(x) = \sum_i \lambda_i x^{i-1} \quad (2-17)$$

$$\rho(x) = \sum_j \rho_j x^{j-1} \quad (2-18)$$

由式(2-14)-(2-18)有

$$\lambda(x) = \frac{\Lambda'(x)}{\Lambda'(1)} \quad \text{及} \quad \rho(x) = \frac{P'(x)}{P'(1)}$$

2.2.3 快速编码LDPC码的构造

近年来，信道编码的研究者们都以解决以下问题作为最终目标：对一个给定的信道，找到一种码字同时具备两种性质：(1)存在线性时间编码算法；(2)对任意逼近信道容量的编码速率可以可靠线性时间译码。但是对一般的LDPC码来说，若按传统的编码方法编码，复杂度是 $O(n^2)$ (n 为码长)，这是无法用硬件实现的。编码问题可以从两方面着手去解决：一是研究编码算法，试图提出一种低复杂度的编码算法，如Richardson等人提出的快速编码算法^[44]。或者是从研究码的结构入

手, 寻找能快速编码的特殊结构^[45-48]。如zigzag型的LDPC码^[22]即使用传统方法编码, 复杂度也低很多: 由矩阵循环移位构造的LDPC码^[47]的编码和LDPC分组和卷积编码^[45,48]都可用移位寄存器实现, 具有线性复杂度。

2.3 置信传播算法

因子图中, 函数节点对每一个相邻变量节点根据其它相邻变量节点传递的消息并行求和计算边界消息, 变量节点对每一个相邻函数节点根据其它相邻函数节点传递的边界消息并行求积计算, 乘积消息又将调整对应函数节点的边界计算。经过若干次迭代, 最终准确地或渐近准确地完成因式分解。对这个过程引入半环 (R, \oplus, \otimes) , 其中 R 表示消息空间, “ \oplus ”和“ \otimes ”分别表示定义在空间 R 上的“和”、“积”运算。不同半环的引入, 和积算法将演化为涉及人工智能、信号处理和数字通信等不同领域的特定算法。它们包括贝叶斯网络的Pearl置信传播算法、快速傅立叶变换算法、BCJR前向/后向算法、VA算法、LDPC码的迭代大数判决译码算法, 也包括最小和算法。在纠错码的译码算法中, 无论引入何种半环, 事实上都是依据概率测度进行的。所以, 和积算法应用于纠错码的译码时, 统称为概率传播算法, 我们在本文中继续统称置信传播(BP)算法。

2.3.1 信号检测与测度

设随机变量 $x \in X$ 和 $y \in Y$ 分别表示信道的输入和输出字符, 其中 X 和 Y 分别表示相应的字符集。对于二元输入信道, 信道编码器输出比特序列经双极映射后进入信道。假设比特 $u \in \{0, 1\}$, 双极映射为 $x = 1 - 2u$, 则 $X = \{+1, -1\}$ 。双极映射后, $GF(2)$ 上的“和”运算转化为实数域上的“积”运算。在这个意义上, $GF(2)$ 和 $\{+1, -1\}$ 是一对同构空间。 Y 既可以为离散集也可以为连续集。比如, 对于二元对称信道(BSC), $Y=X$; 对于二元纯删除信道(BEC), $Y = \{+1, 0, -1\}$; 对于AWGN半连续信道, Y 等于实数域 R 。

软判决译码器将基于观察 $y \in Y$ 产生一个关于 X 的测度(measure) $\mu(x)$, 其值域令 A 表示。这种测度一般等价于 X 的一个概率分布。产生测度最常用的两种方法是最大似然法(ML)和最大后验法(MAP), 即 $\mu_{ML}(x) = p(y|x) = p(x,y)/p(x)$, $\mu_{MAP}(x) = p(x|y) = p(x,y)/p(y)$ 。硬判决译码器则产生两个极端取值的测度 $\mu(x)$, 由随机变量 r 表示, 称为硬判决测度, 这时 $A = \{0, 1\}$, 传输信道被模型化为一个二元输入二元输出离散信道。

对测度 $\mu(x)$ 可以引入不同的量度(metric), 以适应不同的计算需要。最常用的对数量度定义为 $v(x) = -\log(\mu(x))$, 则 $\mu(x) = \exp\{-v(x)\}$ ^[49]。如果测度 $\mu(x)$ 表示概率, 那么量度 $v(x)$ 为非负实数, 这时 $A = [0, +\infty)$, 即非负实数环 R_+ 。对数量度使

乘积运算转化为求和运算。

二元输入信道中,对码符号 $u \in \{0, 1\}$ 和信道输入符号 $x \in \{+1, -1\}$ 的讨论是等价的,因此我们在下文中不致混淆时,将在适当场合等效使用集合 $\{0, 1\}$ 和 $\{+1, -1\}$ 。设一个二元随机变量的概率分布率由 (p_{+1}, p_{-1}) 或 (p_0, p_1) 等价表示,下面式子定义了似然比(LR)、对数似然比(LLR)和概率差三种量度

$$v = p_{+1}/p_{-1}, \quad (2-19a)$$

$$m = \log(p_{+1}/p_{-1}), \quad (2-19b)$$

$$\Delta p = p_{+1} - p_{-1}, \quad (2-19c)$$

它们对应的值域 A 分别是 $[0, +\infty)$ 、 $(-\infty, +\infty)$ 和 $[-1, 1]$ 。这三种量度使一个比特概率测度的两种取值由一个量度值替代,从而大大减少了置信传播算法中需要传递的消息数量。这些量度的相互转换公式为

$$\begin{cases} v = \frac{1 + \Delta p}{1 - \Delta p} \\ \Delta p = \frac{v - 1}{v + 1} \end{cases} \quad (2-20a)$$

$$\begin{cases} v = \frac{1 + \Delta p}{1 - \Delta p} \\ \Delta p = \frac{v - 1}{v + 1} \end{cases} \quad (2-20b)$$

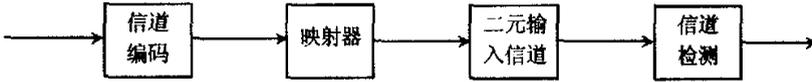


图2.5 信道传输与检测模型

$$\begin{cases} m = \log \frac{1 + \Delta p}{1 - \Delta p} \\ \Delta p = \frac{e^m - 1}{e^m + 1} = \tanh \frac{m}{2} \end{cases} \quad (2-10c)$$

$$\begin{cases} m = \log \frac{1 + \Delta p}{1 - \Delta p} \\ \Delta p = \frac{e^m - 1}{e^m + 1} = \tanh \frac{m}{2} \end{cases} \quad (2-10d)$$

其中函数 $\tanh(x/2) = (e^x - 1)/(e^x + 1)$ [15]。

无论是概率测度还是引入的各种量度,都相当于引用了不同的成本函数,并可以统一简记为 $\mu(x)$ [15]。图2.5给出了信道编码与调制分离的信道传输与检测模型,主要目的在于说明迭代译码中涉及到的消息量度选择问题。

2.3.2 和积算法与最小和算法

下面,我们主要讨论二元LDPC码的译码。信道模型为第一章1.2中介绍的二元输入平稳遍历无记忆AWGN信道,假设采用双级信号的BPSK调制,噪声具有高斯密度 $N(0, \sigma_n^2)$ 。

任意给定信道观察向量 \mathbf{y} , 式(2-8)中后验概率测度 $P(x | \mathbf{y})$ 是 x 的函数,准确地说,是以 \mathbf{y} 为参数和以 x 为自变量的函数。所以,已知信道输出 \mathbf{y} 时,图2.2中的每个函数节点 $f(y_j | x_j)$ 只需进行一次计算,存储在本节点,使译码器获得从信

道采集到的概率测度的样本值,该值相对迭代过程而言命名为初始消息。节点 $\{y_j\}$ 不参与迭代计算,可从图中去掉,于是简化得到图2.6所示的标准因子图,它实际也是一个迭代置信消息传递和更新(update)的贝叶斯网络。从密度进化特性,本文把“更新”也写为“修正”或“进化”,并在讨论中应用到一些贝叶斯网络术语。

基于局部有向树概念,图2.6中所有变量节点称为父亲,其邻居函数节点称为孩子,转移函数节点简称 f_j 节点,初始消息 f_j^a 也称为局部成本。 R_{ij}^a 是 z_i 节点向 x_j 节点传递的校验消息, Q_{ij}^a 是 x_j 节点向 z_i 节点传递的变量消息, R_{ij}^a 和 Q_{ij}^a 是中间消息或中间成本。用贝叶斯网络术语, R_{ij}^a 表示 z_i 根据其他父亲 $\{x_k:k \neq j,k \in N(i)\}$ 当前状态向 x_j 宣称的“ $x_j=a$ 使 z_i 满足”的可信度, Q_{ij}^a 表示 x_j 根据其他孩子包括 f_j 和 $\{z_k:k \neq i,k \in M(j)\}$ 向 z_i 宣称的“ $x_j=a$ ”的可信度。按照turbo原理,每个局部约束 z_i 视为一个子码,这时 R_{ij}^a 也称为子码 z_i 产生的外信息。

图2.7是描述消息传递和修正规则的局部因子图。图中的虚方框表示可以给 z_i 产生一个局部成本函数 g_i^b ,当码字先验不等概时,描述局部结构 $\{x_j:j \in N(i)\}$ 的先验分布,其中 $b \in \{0,1\}^{M(i)}$ 是局部结构的一组特定取值^[15]。

迭代置信传播算法将做如下工作:

1 初始化: 计算初始消息 $\{f_j^a\}$ 和初始化 $\{R_{ij}^a\}$

2 迭代消息传递和修正:

阶段1: 各个 f_j 和 z_i 节点向其所有 x_j 父亲节点分别传递消息 f_j^a 和 R_{ij}^a ,而各个 x_j 节点根据接收消息修正 Q_{ij}^a ;

阶段2: 各个 x_j 节点向其所有 z_i 孩子节点传递已更新的消息 Q_{ij}^a ,而各个 z_i 节点根据接收消息修正 R_{ij}^a 。

3 迭代终止: z_i 和 x_j 节点根据所有接收消息分别计算最终消息 R_i^b 和 Q_j^a 。

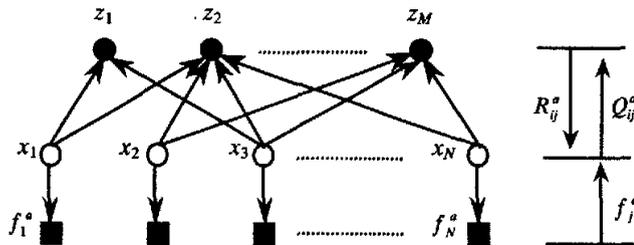


图2.6 置信传播译码网络的因子图表示

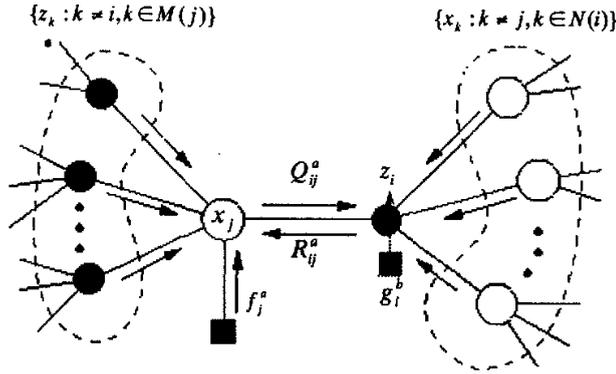


图2.7 消息传递和修正规则

迭代过程中, f_j 节点只传递消息, 但不接收消息。另外, 迭代算法只局部进行消息传递和修正并在迭代终止时计算最终消息(或成本) R_i^b 和 Q_j^a , 但不做任何判决工作。对于LDPC译码器, 最终函数成本 R_i^b 不必计算, 其中 b 表示 $\{x_j : j \in N(i)\}$ 的特定取值。 Q_j^a 表示 $P(x|y)$ 的近似后验边界分布 $P(x_1|y), \dots, P(x_N|y)$ 。需要设计一种迭代终止策略, 并根据消息量度的选择作出相应的判决。

LDPC码一般采取的最优策略为:

(1) 每轮迭代结束时, 立即计算最终消息并判决 \hat{x} , 计算伴随式 $H\hat{x}^T$;

(2) 如果伴随式为零向量, 则宣告成功, 终止迭代; 否则继续迭代。若迭代次数达到预先设定的最大次数 I_{\max} 仍未成功, 则宣告失败, 终止迭代。

2.3.2.1 基于概率测度的和积算法

根据上述关于消息传递和修正过程的分析, 概率测度下, 变量消息和校验消息分别定义为 $Q_{ij}^a = P(x_j = a | y_j, \{z_k : k \in M(j) \setminus i\})$ 和 $R_{ij}^a = P(z_i | x_j = a)$, 且 R_{ij}^a 初始化为1。相对迭代过程, 初始概率消息 f_j^a 表示 $x_j = a$ 的先验信息, $a \in \{+1, -1\}$ 。假定等概传输 ± 1 , 定义 $f_j^a = P(x_j = a | y_j) = \alpha_j f(y_j | x_j = a)$, 其中 α_j 是归一化常数, 保证 $f_j^{+1} + f_j^{-1} = 1$ 。高斯信道的似然函数为

$$f(y | x = a) = \frac{1}{\sqrt{2\pi\sigma_n^2}} \exp\left\{-\frac{(y-a)^2}{2\sigma_n^2}\right\}. \quad (2-21)$$

给定信道输出 y , 对 $j = 1, \dots, N$, 算得

$$f_j^a = 1 / (1 + \exp\{-2ay_j / \sigma_n^2\}), \quad a \in \{+1, -1\}. \quad (2-22)$$

变量消息 Q_{ij}^a 和校验消息 R_{ij}^a 的修正公式推导如下^[30,37]:

$$\begin{aligned}
Q_{ij}^a &= P(x_j = a | y_j, \{z_k : k \in M(j) \setminus i\}) = \frac{P(x_j = a, y_j, \{z_k : k \in M(j) \setminus i\})}{P(y_j, \{z_k : k \in M(j) \setminus i\})} \\
&= \frac{P(x_j = a | y_j) P(\{z_k : k \in M(j) \setminus i\} | y_j, x_j = a)}{P(\{z_k : k \in M(j) \setminus i\} | y_j)} \\
&= \frac{P(x_j = a | y_j) P(\{z_k : k \in M(j) \setminus i\} | x_j = a)}{P(\{z_k : k \in M(j) \setminus i\})} = \frac{P(x_j = a | y_j) \prod_{k \in M(j) \setminus i} P(z_k | x_j = a)}{P(\{z_k : k \in M(j) \setminus i\})} \\
&= \alpha_{ij} f_j^a \prod_{k \in M(j) \setminus i} R_{kj}^a, \quad (2-23)
\end{aligned}$$

$$\begin{aligned}
R_{ij}^a &= P(z_i | x_j = a) = \sum_{x: x_j = a} P(z_i, x | x_j = a) = \sum_{x: x_j = a} P(z_i | x_j = a, x) P(x | x_j = a) \\
&= \sum_{x: x_j = a} P(z_i | x) P(x | x_j = a) = \sum_{x: x_j = a} P(z_i | x) \prod_{k \in N(i) \setminus j} P(x_k) \\
&= \sum_{x: x_j = a} P(z_i | x) \prod_{k \in N(i) \setminus j} Q_{ik}^x, \quad (2-24)
\end{aligned}$$

其中式(2-23)中, α_{ij} 为归一化常数, R_{ij}^a 是从上一次迭代中传递来的函数消息, 首次迭代时为初始值。式(2-24)中, $P(x_k)$ 是指特定求和组合 x 中各分量 x_k 取相应值的概率, 显然, R_{ij}^a 是一个似然概率。用于逐符号判决的最终变量消息为

$$Q_j^a = \alpha \cdot f_j^a \prod_{i \in M(j)} R_{ij}^a, \quad (2-25)$$

其中, α 为归一化因子。相应的判决准则是

$$\hat{x}_j = \arg \max_{a \in \{+1, -1\}} Q_j^a. \quad (2-26)$$

2.3.2.2 基于似然比量度的和积算法

令似然比量度下的初始消息、校验消息和变量消息分别用 γ_j 、 γ_{ij} 和 τ_{ij} 表示。根据式(2-19a)、(2-20a)、(2-20b)、(2-22)和(2-23), 似然比消息重新定义如下

$$\gamma_j = f_j^0 / f_j^1 = \exp\{2y_j / s_n^2\}, \quad (2-27a)$$

$$\gamma_{ij} = R_{ij}^0 / R_{ij}^1 = (1 + \Delta R_{ij}) / (1 - \Delta R_{ij}), \quad (2-27b)$$

$$\tau_{ij} = Q_{ij}^0 / Q_{ij}^1 = \gamma_j \prod_{k \in N(j) \setminus i} \gamma_{kj}. \quad (2-27c)$$

由以上定义可知, 校验消息 R_{ij}^a 应该初始化为1。而基于 $\{0, 1\}$ 的判决规则为 $\hat{x}_j = [\tau_j \leq 1]$, 其中 $[P]$ 是式(2-2)定义的布尔指示函数。

基于概率测度和似然比量度的和积算法, 校验消息和变量消息采用混合量度的有效计算, 要求在消息传递过程中必须做额外的量度转换。

2.3.2.3 基于对数似然比量度的和积算法

对数似然比量度的初始消息、校验消息和变量消息分别定义为 $u_j = \log(\gamma_j)$ 、 $u_{ij} = \log(\gamma_{ij})$ 、 $v_{ij} = \log(\tau_{ij})$ 。根据以上定义， u_j 的初始值为 0，判决规则为 $\hat{x}_j = [v_j \leq 0]$ 。初始消息(2-22)和消息修正公式(2-23)最终被重写为^[19]

$$u_j = 2y_j / s_n^2, \quad (2-28)$$

$$v_{ij} = u_j + \sum_{k \in \mathcal{N}(j) \setminus i} u_{kj}, \quad (2-29)$$

$$\tanh\left(\frac{u_{ij}}{2}\right) = \prod_{k \in \mathcal{N}(i) \setminus j} \tanh\left(\frac{v_{ik}}{2}\right). \quad (2-30)$$

2.3.2.4 最小和算法

最小和算法是在网格图上只挑选一条最可能的有效路径。正是这个思想，使最小和算法在无环图上实现了最小化码字错误概率的译码。但对于有环图码，比如LDPC码，最小和算法则认为退化的和积算法，其性能更差一些。这一点在以误比特率(BER)评价码的性能时，尤为明显。

考虑一个度数为3的校验节点，令 $(p_0^{(1)}, p_1^{(1)})$ 和 $(p_0^{(2)}, p_1^{(2)})$ 是两个输入概率分布，输出概率分布 (p_0, p_1) 由下式给出：

$$p_0 = \alpha \max(p_0^{(1)} p_0^{(2)}, p_1^{(1)} p_1^{(2)}), \quad (2-31a)$$

$$p_1 = \alpha \max(p_0^{(1)} p_1^{(2)}, p_1^{(1)} p_0^{(2)}), \quad (2-31b)$$

其中， α 是归一化因子。

因此，按概率测度的术语，最小和算法也称为最大乘积算法(max-product)。令 v_1 、 v_2 和 u 分别表示上述输入、输出概率测度的对数似然比量度消息，有

$$u = \begin{cases} v_2, & v_1 \geq |v_2| \\ -v_2, & v_1 \leq -|v_2| \\ v_1, & v_2 \geq |v_1| \\ -v_1, & v_2 \leq -|v_1| \end{cases} = \operatorname{sgn}(v_1) \operatorname{sgn}(v_2) \min(|v_1|, |v_2|),$$

其中， $\operatorname{sgn}(x)$ 是正负符号函数，当 $x \geq 0$ 时， $\operatorname{sgn}(x) = 1$ ；否则 $\operatorname{sgn}(x) = -1$ 。

若一个校验节点的度数为 $d_c \geq 2$ ，输入对数似然比消息为 $\{v_j : j = 1, \dots, d_c - 1\}$ ，则输出消息 u 必然等于^[15,51]

$$u = M_{d_c-1}(v_1, v_2, \dots, v_{d_c-1}), \quad (2-32)$$

其中， $M_n(\cdot)$ 是一个 $\mathbb{R}^n \rightarrow \mathbb{R}$ 的映射函数，并定义为

$$M_n(v_1, v_2, \dots, v_n) = \min(|v_1|, |v_2|, \dots, |v_n|) \prod_{j=1}^n \operatorname{sgn}(v_j), \quad (2-33)$$

所以，对数似然比消息空间上的最小和算法包括式(2-28)、(2-29)和(2-32)。

2.4 本章小结

本章首先系统地概述了LDPC码的因子图表示，包括校验约束编码结构和后验概率译码结构。然后阐述了低密度校验码的构造方法。最后从信号检测角度给出了基于概率测度的似然比、对数似然比、概率差等不同消息量度，并作了等价性描述，同时相应地介绍了和积算法和最小和算法。

第三章 低密度校验码的性能分析

本章分析了影响LDPC长码和中、短码性能的主要因素并仿真了相应的优化算法。分析了错误平层产生的原因,介绍了ACE算法,该算法能有效的降低LDPC码的错误平层。

3.1 影响LDPC码性能的因素

影响LDPC码性能的因素概括起来主要是度分布序列对和环。但对长码和中、短码来说这些因素的影响力各有不同。长码受度分布序列好坏的影响很大,而环的影响基本不用考虑:MacKay曾指出在长码时消除4环以后译码性能已经有很大提高,继续消环对译码性能影响不大^[34];此外,Sae-Young Chung等人^[20]设计了码长为 10^7 、码率为1/2的低密度校验码,在误比特率为 10^{-6} 时离Shannon限不到0.0045dB,同时,他们的仿真结果表明通过密度进化设计在迭代算法下最优的低密度校验码随着码长的增加可以逼近Shannon限。对中、短码来说,通过密度进化优化的度分布序列同样适用,但环的影响变得非常的重要^[20]。

3.1.1 度分布序列对的影响

在长码时,LDPC码的性能有可能超过Turbo码,逼近香农限^[20]。而已有的一些研究表明:在长码时,LDPC码的度分布序列对的优劣对其性能的好坏起到了决定性作用;而在中、短码长时,在长码下最优的度分布序列对也是次优的。所以要设计一个好的LDPC码,度分布序列对的优化设计很关键。T. J. Richardson等学者提出的密度进化(density evolution)理论可以精确分析给定度分布序列对的无环LDPC码在消息传递译码算法下的误比特性能,因此可以用它来指导LDPC码度分布序列对的优化设计^[53]。

3.1.2 环的影响

为了分析方便起见,先给出一些概念的明确定义。所谓环(cycle)是指图中的一条路径,它由一些节点和边构成,任选一个节点作为起始节点,这条路径经过每个节点一次,经过每条边一次,最后返回所选的起始节点。而环长指的是环上的节点数或边数(由环的定义可知,环上的节点数等于环上的边数)。因为Tanner图是二部图,所以Tanner图中只有长为偶数的环。Tanner图的围长(girth)是指Tanner图上的最小环长。特别地,如果Tanner图上没有环(此时Tanner图退化为树图),那么定义其围长为无穷大。

由2.3.2节对和积算法迭代过程的分析中不难发现：如果低密度校验码对应的Tanner图存在环的话，那么由和积算法计算所得的概率并不是真正的后验概率(这是因为迭代过程中的独立性假设不能成立)，因而译码并不是最优的逐符号最大后验概率译码。因此，环的存在使得译码的最优性得不到满足。

由于环对译码的影响，设计围长(girth)大的Tanner图成为研究的热点之一。那么是否围长越大码的性能就越好？如果是这样的话，那么树图所对应的LDPC码应该是最优的。而实际上已经有结论^[72]：如果对应Tanner图是无环的，那么：1)当对应码的码率大于1/2时，码的最小距离小于等于2；2)当对应码的码率小于1/2时，码可以由最小距离小于等于2的码重复某些位生成，更进一步，记码率为 R ，则最小距离满足 $d_{\min} < 2/R$ 。因此，无环图对应的码并不是好码，相反地，环的存在改善了码的性能。

经过上面的论述，可以得出以下两点：

- 1) 环的存在对码本身的性能带来好处，或者说可以改善码的最小距离(更进一步可以改善距离谱)；
- 2) 环的存在使得独立性假设不能成立，给和积译码带来困难，译码性能并不能达到码本身的性能。

因此，环的问题是一个矛盾的混合物，一方面码本身的性能要求必须有环的存在；而另一方面和积译码却要求没有环。

3.2 度分布序列对的优化设计

3.2.1 连续密度进化

利用置信传播算法对LDPC码译码，迭代消息传递和修正的目的在于使图上流动的消息向正确方向集中。Gallager在研究规则LDPC码时，发现该算法存在不动点，即当迭代超过一定次数时，消息不再发生或几乎不再发生进化，这种现象称为阈值现象^[8,30]。Luby等人发现引入非规则图可以有效地改进阈值^[31,36,52]。Richardson等人则基于Gallager的思想，引入密度进化的概念，系统建立了无环图上的密度进化理论，提出了有环随机图上迭代算法的性能渐进收敛于无环图的集中定理^[19]。密度进化理论允许应用数值方法计算和积译码器对于LDPC码的平均渐进性能。他们证明，对于许多人们感兴趣的信道，可以计算出和积算法对随机构造的LDPC码集合的阈值，该阈值在分组长度趋于无穷大时可以渐进地确定无错区域的边界。

3.2.1.1 对称条件和独立性假设

第 $\ell \geq 1$ 轮迭代中, 一个度数为 $d_c \geq 2$ 的校验节点 z 向一个邻居变量节点 x 传递的边界消息 u 是来自其他 $d_c - 1$ 个邻居变量节点的输入消息 v_1, \dots, v_{d_c-1} 的函数, 记为 $u = \varphi_c^{(\ell)}(v_1, \dots, v_{d_c-1})$ 。同样, 一个度数为 $d_v \geq 1$ 的变量节点 x 向一个邻居校验节点 z 输出的消息 v 是初始消息 u_0 和来自其他 $d_v - 1$ 个邻居校验节点的输入消息 u_1, \dots, u_{d_v-1} 的函数, 记为 $v = \varphi_v^{(\ell)}(u_0, u_1, \dots, u_{d_v-1})$ 。在 $\ell = 0$ 即初始化中, 所有变量节点获得初始消息, 并向校验节点传递。

二元输入编码信道和迭代算法需要满足的对称条件定义如下:

定义3.1 (对称条件)

- (1) 信道对称: 设二元输入信道的输入和输出分别为 x 和 y , 如果信道转移概率满足下式, 则称信道是输出对称的, 或简称对称信道。

$$P(y | x = +1) = P(-y | x = -1); \quad (3-1a)$$

- (2) 校验节点对称: 如果校验消息修正函数满足符号齐次性, 即对于任意 ± 1 序列 (b_1, \dots, b_n) 下式总成立, 则称校验节点具有对称性。

$$\varphi_c^{(\ell)}(b_1 v_1, \dots, b_n v_n) = \varphi_c^{(\ell)}(v_1, \dots, v_n) \prod_{j=1}^n b_j \quad (3-1b)$$

- (3) 变量节点对称: 如果变量消息修正函数满足下列符号变反映射不变性, 则称变量节点具有对称性。

$$\varphi_v^{(\ell)}(-u_0, -u_1, \dots, -u_n) = -\varphi_v^{(\ell)}(u_0, u_1, \dots, u_n), \quad (3-1c)$$

$$\varphi_v^{(0)}(-u_0) = -\varphi_v^{(0)}(u_0). \quad (3-1d)$$

当信道和置信传播译码器满足上述对称条件时, 可以证明线性码译码错误概率独立于传输的码字^[19,30,53]。显然, AWGN信道满足式(3-1a)定义的信道对称条件, 只用一个信道转移概率函数 $P(y|x=1)$ 就可以完全描述信道特征。对于置信传播算法, 不同消息空间理论上是等价的, 但是只有基于LLR量度的消息修正公式满足式(3-1b)~(3-1d)定义的对称条件。因此, 我们在分析AWGN信道中置信传播译码器的性能时, 采用LLR量度, 并假设编码器输出零码字, 或信道传输全“1”码字。这时, 正值和负值消息分别称为“正确消息”和“错误消息”, 消息0分别以1/2的概率视为正确或错误^[19]。

3.2.1.2 消息空间的概率测度及密度进化

引入符号集合的勒贝格(Lebesgue)概率测度空间。令 Π_A 和 Π_M 分别为消息空间 A 和 M 的概率分布空间。校验消息和变量消息的传递及修正将导致测度空间的如下进化:

$$\Psi_c^{(\ell)}: \Pi_M^{d_c-1} \rightarrow \Pi_A$$

$$\Psi_v^{(\ell)}: \Pi_A \times \Pi_M^{d_v-1} \rightarrow \Pi_M.$$

离散消息空间的概率测度用概率分布律表示, 连续消息空间的概率测度用概率密度函数表示, 它们统一简称为密度。测度空间的进化由密度进化反映。假设在第 ℓ 轮迭代中, $P(v)$ 是输入消息密度, 它在 $\ell=1$ 时表示初始消息密度; $R(u)$ 是校验节点传递的消息密度, 是输入消息的函数 $\varphi_c^{(\ell)}$ 的密度; $Q(v)$ 是变量节点传递的消息密度, 是校验消息的函数 $\varphi_v^{(\ell)}$ 的密度, 也是本次迭代完成的进化密度, 它将作为下一轮迭代的输入密度。消息密度的进化直接受到初始消息密度的影响, 所以取决于信道模型的初始消息密度也称为先验密度。

定理3.1

设随机变量 X 具有密度 $f_X(x)$, $-\infty < x < +\infty$ 。 $Y=g(X)$, 函数 $g(x)$ 为严格单调函数, 则随机变量 Y 的密度为

$$f_Y(y) = \begin{cases} f_X(h(y))|h'(y)|, & \alpha < y < \beta \\ 0 & \text{其它} \end{cases}, \quad (3-2)$$

其中, $\alpha = \min\{g(-\infty), g(+\infty)\}$, $\beta = \max\{g(-\infty), g(+\infty)\}$, $h(y)$ 为 $g(x)$ 的反函数。

考虑 AWGN 信道的初始消息及其概率密度函数。设信道输入 $x=+1$ 。

对于均值为 0、方差为 σ^2 的 AWGN 信道, 初始消息为 $u_0 = (2/\sigma^2)x$ 。应用定理 3.1, 求得先验密度函数为

$$P_{AWGN}^{(0)}(v) = \frac{\sigma}{2\sqrt{2\pi}} \exp\left[-\frac{(v\sigma^2/2-1)^2}{2\sigma^2}\right]. \quad (3-3)$$

为了方便分析, 把一个度数为 $d_v \geq 1$ 的变量节点 x 向邻居 z 传递的消息 v 的计算写为

$$v = \sum_{i=0}^{d_v-1} u_i, \quad (3-4)$$

其中, u_0 是 x 的初始消息, u_1, \dots, u_{d_v-1} 是来自其他 d_v-1 个邻居的输入消息。同样, 把一个度数为 $d_c \geq 2$ 的校验节点 z 向邻居 x 传递的消息 u 的计算写为

$$\tanh\left(\frac{u}{2}\right) = \prod_{j=1}^{d_c-1} \tanh\left(\frac{v_j}{2}\right). \quad (3-5)$$

其中, v_1, \dots, v_{d_c-1} 是来自其他 d_c-1 个邻居的输入消息。

设一个二元随机变量的概率分布由量度 $\Delta p \in (-1, +1)$ 描述, 它还可以分解为符号与绝对值两个部分, 即用序偶 $(\lg \operatorname{sgn} \Delta p, -\log |\Delta p|) \in \text{GF}(2) \times \mathbb{R}_+$ 作变换表示, 其中正负号在 $\text{GF}(2)$ 上同构表示为 $\lg \operatorname{sgn} \Delta p = (1 - \operatorname{sgn}(\Delta p))/2$, $\Delta p = 0$ 时应予以单独考虑。所以, 式(3-5)能够变换表示为^[8,19,30]

$$\left(\lg \operatorname{sgn}(\tanh \frac{u}{2}), -\log \left| \tanh \frac{u}{2} \right| \right) = \left(\sum_{j=1}^{d_c-1} \lg \operatorname{sgn}(\tanh \frac{v_j}{2}), -\sum_{j=1}^{d_c-1} \log \left| \tanh \frac{v_j}{2} \right| \right), \quad (3-6)$$

其中等式右边的第一个分量采用GF(2)域上的加法。

式(3-6)使校验消息空间得到变换，将校验消息的计算转化为求和运算。消息空间的变换导致其测度密度的相应变换。这时，校验消息和变量消息形式上是若干个独立同分布的输入消息之和，其密度通过卷积计算，而卷积运算在傅立叶变换域上又转换为乘积运算。

从因子图的观点来看，式(3-5)和(3-6)互为对偶表示，如图3.1所示。对偶表示使局部函数节点等同于变量节点来处理，即在变换域上函数节点也只是集中和承载信息^[29]。

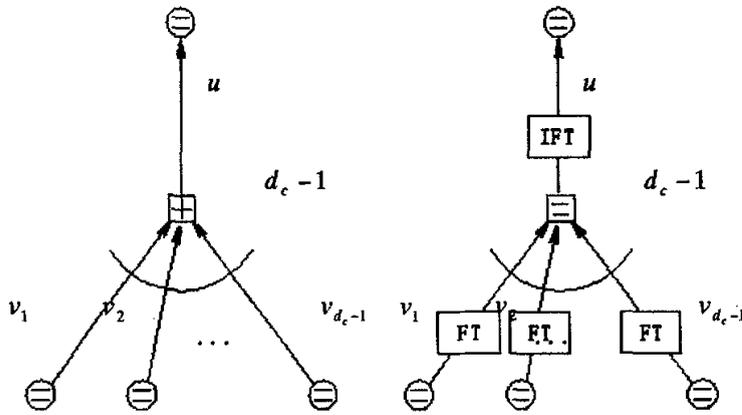


图3.1 校验节点修正函数的变换表示

函数 $y = -\log |\tanh(v/2)| \in \mathbb{R}_+$ 在 $v > 0$ 和 $v < 0$ 两个区间内分别严格单调，与其反函数具有对称形式。当 $v > 0$ 时，互逆函数对为 $y = -\log[\tanh(v/2)]$ 和 $v = -\log[\tanh(y/2)]$ ；当 $v < 0$ 时，互逆函数对为 $y = -\log[\tanh(-v/2)]$ 和 $-v = -\log[\tanh(y/2)]$ 。设对变换空间 $\text{GF}(2) \times \mathbb{R}_+$ 测度的概率密度函数表示为 $P_Y = (P_Y^0(y), P_Y^1(y))$ ，其中 $P_Y^0(y) = P_Y(0, y)$ 和 $P_Y^1(y) = P_Y(1, y)$ 分别对应 $v > 0$ 和 $v < 0$ 两种情况。已知对数似然比消息 v 的密度 $P(v)$ ，由定理3.1得变换消息 $y > 0$ 的密度 P_Y 为^[19]

$$P_Y^0(y) = \frac{1}{\sinh y} P \left[-\log \left(\tanh \frac{y}{2} \right) \right], \quad (3-7a)$$

$$P_Y^1(y) = \frac{1}{\sinh y} P \left[\log \left(\tanh \frac{y}{2} \right) \right]. \quad (3-7b)$$

同样，若已知变换消息 y 的密度 P_Y ，则对数似然比消息 v 的密度 $P(v)$ 为^[19]

$$P(v) = \begin{cases} \frac{1}{\sinh v} P_Y^0 \left[-\log \left(\tanh \frac{v}{2} \right) \right], & v > 0 \\ \frac{1}{\sinh(-v)} P_Y^1 \left[-\log \left(\tanh \frac{-v}{2} \right) \right], & v < 0 \end{cases} \quad (3-8)$$

其中, $\sinh x = (e^{2x} - 1)/2e^x$ 。

变换空间 $\text{GF}(2) \times \mathbb{R}_+$ 上的式(3-6)表示校验消息是函数 $\varphi_c^{(\ell)}$ 的 $d_c - 1$ 个独立同分布输入消息的变换之和, 所以其密度 $R_Y = (R_Y^0(y), R_Y^1(y))$ 是 $d_c - 1$ 个相同变换密度 P_Y 的卷积, 记为 $R_Y = \otimes^{d_c-1} P_Y$, 其中 \otimes 为卷积运算符。 P_Y 由对数似然比输入消息的密度 $P(v)$ 按式(3-7a)和(3-7b)计算得到。空间 $\text{GF}(2) \times \mathbb{R}_+$ 上的函数 P_Y 经过傅立叶变换后得到 $F(P_Y)$ 为

$$F_P[s, 0] = L_P^0(s) + L_P^1(s), \quad (3-9a)$$

$$F_P[s, 1] = L_P^0(s) - L_P^1(s), \quad (3-9b)$$

其中 $L_P^0(s) = L[P_Y^0(y)]$ 和 $L_P^1(s) = L[P_Y^1(y)]$ 是拉普拉斯变换, 即实数域的傅立叶变换域。设第 $\ell - 1$ 轮迭代结束后变量节点传递的对数似然比消息密度为 $P^{(\ell-1)}$, 空间 $\text{GF}(2) \times \mathbb{R}_+$ 上消息密度相应为 $P_Y^{(\ell-1)}$, 则第 ℓ 轮迭代中在 $\text{GF}(2) \times \mathbb{R}_+$ 空间上校验消息的密度 $R_Y^{(\ell)}$ 的傅立叶变换 $F(R_Y^{(\ell)})$ 的计算式为

$$F_R^{(\ell)}[s, 0] = [L_P^{(\ell-1),0}(s) + L_P^{(\ell-1),1}(s)]^{d_c-1}, \quad (3-10a)$$

$$F_R^{(\ell)}[s, 1] = [L_P^{(\ell-1),0}(s) - L_P^{(\ell-1),1}(s)]^{d_c-1}, \quad (3-10b)$$

该式计算结果经傅立叶反变换得 $R_Y^{(\ell)}$, 再由式(3-8)计算出对数似然比消息空间上校验消息的密度 $R^{(\ell)}(u)$ 。

如式(3-4)所示, 变量节点传递的消息 v 是该节点的初始消息 u_0 与函数 $\varphi_v^{(\ell)}$ 的其它 $d_v - 1$ 个独立同分布输入消息 u_i 之和, 所以密度 $Q(v)$ 是先验密度 $P^{(0)}(u)$ 和 $d_v - 1$ 个相同密度 $R(u)$ 的卷积, 即 $Q = P^{(0)} \otimes (\otimes^{d_v-1} R)$ 。第 ℓ 轮的密度 $Q(v)$ 就是该轮迭代结束后所有变量节点传递的 nd_v 个独立同分布消息的密度 $P^{(\ell)}$ 。应用傅立叶变换对, 求得第 ℓ 轮迭代结束后的消息密度为^[19]

$$P^{(\ell)} = F^{-1}(F(P^{(0)})F(R^{(\ell)})^{d_v-1}) \quad (3-11)$$

密度进化可以采用数值方法进行计算, 尽管计算量非常大, 但是可以精确地跟踪消息进化过程。当分组长度足够大和迭代次数趋于无穷时, LDPC码集合平均性能收敛于基于独立性和对称性假设的分析性能^[19,53]。

3.2.1.3 密度进化的参数化

置信传播算法的收敛性反映于消息空间分布密度向正确方向集中。随着迭代次数的增加,因子图中传播的不正确消息的比例应该逐渐趋于0,使译码器高概率正确译码。首先,SBIC信道模型可以用一个特征参数来描述,如零均值AWGN信道的均方差 σ 。先验密度是信道特征参数的函数,先验密度直接影响着密度进化。初看,密度进化似乎取决于初始密度,事实上密度进化对初始密度并不敏感,而真正是对信道参数敏感。因为正是信道参数决定了初始密度。第二,给定码参数 $\lambda(x)$ 和 $\rho(x)$,密度函数是信道特征参数 α 的单调增函数,存在一个极值 α^* ,当 $\alpha \leq \alpha^*$ 时,算法高概率收敛。极值 α^* 就定义为置信传播算法的容量或阈值^[19, 53]。第三,容量 α^* 是编码参数的函数,不同的码参数将导致不同的容量。给定设计码率 R_c ,使信道容量 $C = R_c$ 的信道特征参数上限 α_c 就是该码率下的Shannon限。译码器容量 α^* 与信道特征参数具有同样的量纲,它与上限 α_c 之间的差异表征了码集合的最佳性能与Shannon限的距离。

连续消息密度进化的分析是基于无环树图的,但是当码长足够大时,译码器统计平均性能一致收敛于译码器容量。一方面,若信道参数 $\alpha \leq \alpha^*$,给定足够大的码长,当迭代次数趋于无穷时,任意 (N, d_v, d_c) 规则码均可以实现信息的可靠传输。另一方面,设定预期译码错误概率,经过相应的迭代次数后,当码长 N 趋于大时,任意 (N, d_v, d_c) 规则码的性能按码长 N 指数地依概率1界定于该错误概率,这就是所谓的集中定理^[19]。

密度进化理论最重要的地方在于分析不动点。Richardson把上述基于规则码的密度进化理论推广到非规则码的分析和设计^[53]。任意一个给定的度数分布对 (λ, ρ) ,总存在一个相应的阈值 $\alpha^*(\lambda, \rho)$,优化的码设计就是基于一个特定的SBIC信道,搜索最佳的分布对,以最大化该阈值。一般来说,要求搜索的分布对满足稳定性条件,即不动点为零^[53]。

3.2.2 密度进化的高斯逼近

高斯逼近原理以较低的精度损失实现了密度进化的快速计算。因子图上流动的独立同分布消息具有近似的高斯密度或高斯混合(mixture)密度,利用对称条件约束逼近进程,高斯逼近方法实现了以高斯均值为—维参数的消息进化特性跟踪,最终实现了迭代译码器的品质分析和非规则码的优化设计。应用高斯逼近原理,我们能够比较容易地确定消息进化的快慢交替阶段及(如果收敛时的)收敛速度^[55]。通过联合高斯密度方法,高斯逼近原理可被用于有环图上的和积算法分析^[56,57]。

3.2.2.1 对称约束条件

当信道满足对称条件时, 转移概率密度函数 $P(y|x=1)$ 完全描述了信道特征, 初始消息 u 仅是信道观察 y 的函数, 满足奇对称特性, 即 $u(-y) = -u(y)$ 。所以, 给定任意 SBIC 信道观察 y , 先验密度为 $p(u) = P(y|x=1)$, 根据对称条件有 $p(-u) = P(-y|x=1)$, 则^[19]

$$p(u) = e^u p(-u)。 \quad (3-12)$$

该式综合了式(3-1a)~(3-1d)的要求, 建立了标准信道下的对称条件。

对于密度为 $N(m, \sigma^2)$ 的高斯随机变量, 对称条件简化为 $\sigma^2 = 2m$, 均值 m 是该变量的唯一参数。对于双极调制的、方差为 σ^2 的零均值 AWGN 信道, 先验密度实际是 $N(2/\sigma^2, 4/\sigma^2)$ 高斯密度。

高斯变量的信噪比定义为 $\text{SNR}_g = m^2/\sigma^2$, 对称条件满足时有 $\text{SNR}_g = m/2 = 1/\sigma^2$ [55]。对于物理高斯信道, SNR_g 显然表达了接收信噪比。已知高斯信道硬判决的错误比特率为 $P_e = Q(1/\sigma) = Q(\sqrt{m/2})$, 其中 $Q(x) = \int_x^\infty N(0,1) dx$ 。所以高斯逼近也便于计算迭代译码的错误比特率。

3.2.2.2 规则码的高斯逼近

已知初始消息 u_0 具有密度为 $N(2/\sigma^2, 4/\sigma^2)$ 的高斯分布, 假如式(3-4)中所有独立同分布的 u_i , $i=1, \dots, d_c-1$, 都服从高斯分布, 那么独立高斯变量之和 v 也服从高斯分布; 即使 u_i 不服从高斯分布, 对于有限信噪比译码器来说, 它们的均值和方差总是有限的, 所以当 d_c 趋于无穷大时, 根据中心极限定理, 这些独立同分布随机变量之和收敛于一个高斯分布。然而校验消息的分析就困难的多, 即使能假定所有 v_j , $j=1, \dots, d_c-1$, 都是高斯变量, 从式(3-5)仍不能确定 u 逼近高斯分布的可能程度。迭代过程中这种校验节点和变量节点的相互作用, 最终使变量消息的高斯逼近程度很难作出严格分析。

按照对称约束条件, 假定在第 ℓ 次迭代中, 对数似然比消息空间中消息变量 $u^{(\ell)}$ 和 $v^{(\ell)}$ 分别是密度为 $N(m_u^{(\ell)}, 2m_u^{(\ell)})$ 、 $N(m_v^{(\ell)}, 2m_v^{(\ell)})$ 的高斯变量。设初始消息 u_0 的均值为 m_0 , 有 $m_v^{(0)} = m_0$ 。一次迭代中, 所有 u_i 都统计独立同分布, 所有的 v_j 也统计独立同分布, 所以由式(3-5)得

$$E \left[\tanh \left(\frac{u^{(\ell)}}{2} \right) \right] = E \left[\prod_{j=1}^{d_c-1} \tanh \left(\frac{v_j^{(\ell-1)}}{2} \right) \right] = E \left[\tanh \left(\frac{v^{(\ell-1)}}{2} \right) \right]^{d_c-1} \quad (3-13)$$

其中, $E[\cdot]$ 表示求数学期望, 第二个等式表示独立随机变量乘积的期望等于期望的

乘积。由式(3-4)直接得

$$m_v^{(\ell)} = m_0 + (d_v - 1)m_u^{(\ell)}. \quad (3-14)$$

为表达式(3-13)中高斯变量函数的期望, 定义 $x \in \mathbb{R}_+$ 的函数^[55]

$$\phi(x) = \begin{cases} 1 - \frac{1}{\sqrt{4\pi x}} \int_{-\infty}^{\infty} \tanh\left(\frac{u}{2}\right) \exp\left[-\frac{(u-x)^2}{4x}\right] du, & x > 0; \\ 1, & x = 0. \end{cases} \quad (3-15)$$

显然, $\phi(x)$ 是 \mathbb{R}_+ 上的连续单调递减函数, $\phi(0) = 1$, $\phi(\infty) = 0$ 。则式(3-13)写为

$$1 - \phi(m_u^{(\ell)}) = [1 - \phi(m_v^{(\ell-1)})]^{d_v - 1}.$$

结合式(3-14), 校验消息均值的进化为^[55]

$$m_u^{(\ell)} = \phi^{-1}(1 - [1 - \phi(m_0 + (d_v - 1)m_u^{(\ell-1)})]^{d_v - 1}). \quad (3-16)$$

为从数学上分析该式, 可令 $m_u^{(0)} = 0$ 。一般地, $\phi(x)$ 只能通过数值积分计算。为提高计算有效性, 可以利用下列非常紧密的近似式子:

$$\phi(x) = \begin{cases} \sqrt{\frac{\pi}{x}} \left(1 - \frac{10}{7x}\right) \exp\left[-\frac{x}{4}\right], & x \geq 14.3987; \\ \exp\{-0.4527x^{0.86} + 0.0218\}, & x \in (0, 14.3987). \end{cases} \quad (3-17)$$

3.2.2.3 非规则码的高斯逼近

基于AWGN信道和规则码推导的高斯逼近公式可以直接推广到非规则码, 主要的概念区别在于: 非规则码中一个节点的所有输入消息均视为独立同分布, 但是每个输入消息是进入相应源节点的不同密度的高斯混合。具体理解请参见下列推导过程中的解释。

考虑具有度分布多项式 $\lambda(x)$ 和 $\rho(x)$ 的随机码集合。一个度数为 i 的校验节点输出消息的均值由式(3-13)得

$$m_{v,j}^{(\ell)} = \phi^{-1}\left(1 - E\left[\tanh\left(\frac{v^{(\ell-1)}}{2}\right)\right]^{i-1}\right), \quad (3-18)$$

其中, $E[\cdot]$ 项表示上次迭代中传递的、混合高斯分布变量消息的函数的均值。

设一个度数为 j 的变量节点输出的高斯消息均值为 $m_{v,j}^{(\ell)}$, 不同度数变量节点输出的消息经过混合, 形成均值为 $m_v^{(\ell)} = \sum_{j=2}^{d_v} \lambda_j m_{v,j}^{(\ell)}$ 的独立同分布高斯混合消息, 进入校验节点。应用定义式(3-15), 可得

$$E\left[\tanh\left(\frac{v^{(\ell)}}{2}\right)\right] = 1 - \sum_{j=2}^{d_v} \lambda_j \phi(m_{v,j}^{(\ell)}). \quad (3-19)$$

于是, 式(3-18)写为

$$m_{u,i}^{(t)} = \phi^{-1} \left(1 - \left[1 - \sum_{j=2}^{d_t} \lambda_j \phi(m_{v,j}^{(t-1)}) \right]^{i-1} \right). \quad (3-20)$$

不同度数校验节点输出的高斯消息经过混合, 形成均值为 $m_u^{(t)} = \sum_{i=2}^{d_t} \rho_i m_{u,i}^{(t)}$ 的独立同分布高斯混合消息, 进入变量节点。由式(3-14)得

$$m_{v,j}^{(t)} = m_0 + (j-1)m_u^{(t)}. \quad (3-21)$$

综合上两式, 得校验消息的均值进化公式为

$$m_u^{(t)} = \sum_{i=2}^{d_t} \rho_i \phi^{-1} \left(1 - \left[1 - \sum_{j=2}^{d_t} \lambda_j \phi(m_0 + (j-1)m_u^{(t-1)}) \right]^{i-1} \right). \quad (3-22)$$

同样可令 $m_u^{(0)} = 0$ 以方便数学分析该进化函数。

任意给定一个规则码或非规则码集合, AWGN信道下高斯逼近的唯一启动值就是由信道参数确定的 $m_0 = 2/\sigma^2$ 。当 $l \rightarrow \infty$ 时, 使得 $m_u^{(t)} \rightarrow \infty$ 或 $m_v^{(t)} \rightarrow \infty$ 成立的下确界 m_0^* 对应的 σ^* 就是该给定码的阈值。

3.2.3 度分布序列对的优化设计

对任意固定码率的LDPC码集合, 阈值唯一由它的度分布序列对 (λ, ρ) 决定。如何搜索使阈值最大的度分布序列对, 这等价于如何在连续空间上确定参数使非线性代价函数最小的问题, 可以用差分进化^[58~60]方法解决。

首先我们分析度序列中各个值之间的相关性。假设 d_t 是最大变量节点度, d_c 是最大校验节点度。可以证明度序列 (λ, ρ) 满足以下约束条件^[60]:

$$\sum_i \frac{\rho_i}{i} = K \sum_j \frac{\lambda_j}{j}, \quad (3-23)$$

其中 $K = 1 - R$, R 是码率。而且

$$\lambda_2 = 1 - \sum_{j=3}^{d_t} \lambda_j, \quad \rho_2 = 1 - \sum_{i=3}^{d_c} \rho_i. \quad (3-24)$$

结合(3-23)和(3-24)可以得到

$$\lambda_{d_t} = \frac{\frac{1-K}{2} + \sum_{i=3}^{d_t} \rho_i \left(\frac{1}{i} - \frac{1}{2} \right) - K \sum_{j=3}^{d_t-1} \lambda_j \left(\frac{1}{j} - \frac{1}{2} \right)}{K \left(\frac{1}{d_t} - \frac{1}{2} \right)}. \quad (3-25)$$

假设度序列 (λ, ρ) 中独立元素的个数为 L 。因为 $\lambda_1 = \rho_1 = 0$, 所以根据式(3-23)~(3-25) 有 $L = d_t + d_c - 5$ 。将度序列 (λ, ρ) 表示成向量

$$P = (\lambda_3, \dots, \lambda_{d_i-1}, \rho_3, \dots, \rho_{d_i})。$$

差分进化是一个并行直接搜索的过程。由初始的向量组开始，并行迭代更新向量组里的各个向量直到找到满足代价函数最小的最佳向量。度序列的优化算法如下^[60]：

(1) 初始化：迭代次数 $G=0$ 时，随机选择 NP 个 L 维向量 $p_{i,G}$ ， $i=0,1,\dots, NP-1$ ，其中 $NP=10L$ 。根据密度进化或高斯逼近计算这 NP 个向量所对应的阈值 $\sigma_{i,G}$ 以及所需的迭代次数 $l_{i,G}$ 。比较这 NP 个阈值，将阈值最大或阈值相等但所需迭代次数最小的向量记做 $p_{best,G}$ ，对应的阈值记为 $\sigma_{best,G}$ ，迭代次数记为 $l_{best,G}$ 。

(2) 生成新向量：在下次迭代 $G+1$ 中，根据如下方法生成新向量：对每个向量 $i=0,1,\dots, NP-1$ ，随机选择不同于 i 的四个各不相同的正整数 $r1$ 、 $r2$ 、 $r3$ 和 $r4$ ，定义

$$v_{i,G+1} = p_{best,G} + F(p_{r1,G} - p_{r2,G} + p_{r3,G} - p_{r4,G}) \quad (3-26)$$

其中 F 是实数，控制了差分进化的幅度。式(3-26)中选用两组向量差来控制进化是为了避免算法局部最小化。计算每个新向量对应的阈值 $\sigma_{i,G+1}$ 和迭代次数 $l_{i,G+1}$ 。

(3) 更新：对每个 i ， $i=0,1,\dots, NP-1$ ，比较 $\sigma_{i,G}$ 和 $\sigma_{i,G+1}$ 的大小。若 $\sigma_{i,G+1} > \sigma_{i,G}$ 或 $\sigma_{i,G+1} = \sigma_{i,G}$ ， $l_{i,G+1} < l_{i,G}$ ，则 $p_{i,G+1} = v_{i,G+1}$ ；否则 $p_{i,G+1} = p_{i,G}$ 。比较更新后的 NP 个阈值，将阈值最大或阈值相等但迭代次数最小的向量记做 $p_{best,G+1}$ ，对应的阈值记为 $\sigma_{best,G+1}$ ，迭代次数记为 $l_{best,G+1}$ 。

(4) 终止规则：若 $\sigma_{best,G+1} - \sigma_{best,G} > 0$ 或 $\sigma_{best,G+1} = \sigma_{best,G}$ 且 $l_{best,G+1} < l_{best,G}$ ，返回到(2)。否则终止。

Richardson等人发现，较好的度分布序列对中一般只有少数的非0元素。所以在实际的搜索中，限制校验节点度为两、三个非零度（这些度可以连续选择），而且限制变量节点的度为2、3以及最大变量节点度 d_i 。我们结合高斯逼近原理和差分进化方法，搜索了在AWGN信道下码率为1/2的度分布序列对，其中最大变量节点度为 $d_i = 4, 5, 6, 7, 8, 9, 10, 15, 20$ 。这些度分布序列对均满足稳定性条件： $\lambda_2 < \lambda_2^*$ ，其中 $\lambda_2^* = e^{1/2\sigma^2} / \prod_{j=2}^{d_i} (j-1)^{\rho_j}$ 。结果见表3.1。

图3.2和图3.3^[52]分别是码长8000和2000的无四环规则和非规则LDPC码的译码性能曲线。非规则码的度序列取自表3.1中 $d_i = 4$ 列。从这些曲线中可以看到规则码没有出现错误平层，而非规则码却有明显的错误平层。规则码没有出现不可检错误，而非规则码却出现了大量的不可检错误。这主要是因为非规则码中有大量的度为2的节点，而其中有些节点又构成了环长较短的环，这样导致译出错误的码字。但是我们不能因此就说非规则码没有规则码好，因为在低性噪比时非规则码的性能比规则码要好。尤其码长越长，这种优势就越明显。这也说明了根据DE或GA优

化的度序列对短码来说并不是最优的。所以，如何建立一套分析有限长LDPC码的理论是值得研究的。另外，如何降低非规则码的错误平层这个问题也很重要。

表3.1 AWGN信道下，码率为1/2的度序列分布对(σ 表示能达到的阈值， σ_c 表示shannon 限)

d_i	4	5	6	7	8	9	10	15	20
λ_2^*	0.3835	0.3572	0.3357	0.3128	0.3067	0.2812	0.2705	0.2416	0.1996
λ_2	0.3830	0.3568	0.3340	0.3116	0.2911	0.2713	0.2602	0.2412	0.1935
λ_3	0.0107	0.1679	0.2245	0.2397	0.2970	0.2714	0.2521	0.1310	0.0852
λ_4	0.6064		0.0056				0.0359	0.1397	0.2271
λ_5		0.4753						0.0937	
λ_6			0.4359						
λ_7				0.4487					
λ_8					0.4119				
λ_9						0.4573			
λ_{10}							0.4519		
λ_{15}								0.3943	
λ_{20}									0.4942
ρ_5	0.1994								
ρ_6	0.8006	0.9179	0.6337	0.2960	0.2168	0.0645			
ρ_7		0.0821	0.3663	0.7040	0.7832	0.6036	0.5116		
ρ_8						0.3319	0.4884	0.7930	0.0921
ρ_9								0.2070	0.0914
ρ_{10}									0.8165
σ	0.9079	0.9168	0.9247	0.9321	0.9362	0.9428	0.9452	0.9508	0.9519
σ_c	0.979	0.979	0.979	0.979	0.979	0.979	0.979	0.979	0.979

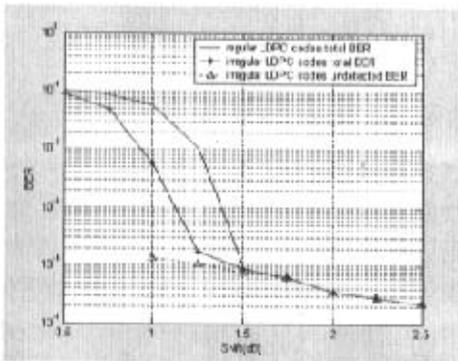


图3.2 (8000,4000)LDPC码的译码性能图

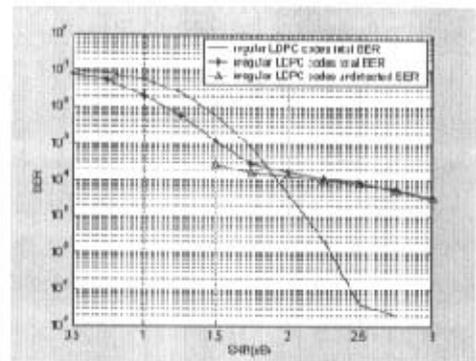


图3.3 (2000,1000)LDPC码的译码性能图

3.3 中、短码的优化设计

影响中、短码性能的主要因素是环。对短码来说,用密度进化优化的度序列也是次优的,在此不考虑度序列对码的影响。如3.1.2节所述,环的存在对码本身的性能是有好处的,但是会给和积算法译码带来困难。我们如何降低环对迭代译码算法的影响呢?

短环的存在使迭代译码性能恶化。下面举个例子以说明短环对译码和最小码重的影响。考察代表校验矩阵的二部图的一部分:

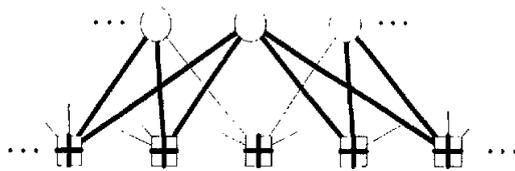


图3.4 低密度校验码二部图的一部分

图3.4中存在两个4环(如粗线所示)。如果三个变量节点的接收值都发生错误(考虑硬判决的情况),即它们的取值由 x_i 变为 $x_i \oplus 1$ (\oplus 表示模二加),则5个校验节点代表的校验关系仍然成立!在这种情况下,这部分无法正确译码。

上面的分析虽然很简单,但是它表明:短环的存在会损害和积算法译码的有效性,并且还有可能导致低码重码字的出现(上图导致了一个重量为3的码字)。

避免出现短环的方法有很多^[37-43],大部分方法都属于代数方法,也有一些是采用启发式搜索,比如Xiao-Yu Hu的PEG(progressive edge growth)方法^[22]。低密度校验码的译码复杂度与校验矩阵的密度紧密相关:校验矩阵的密度越大,译码复杂度越大;校验矩阵的密度越小,译码复杂度越小。因此,适当引入一些重量为2的列会降低译码复杂度,同时也可以提高码率,不过必须采用一些方法以避免小重量码字的出现。

3.3.1 PEG算法

PEG是一种简单有效构造LDPC码的算法,它按某种规则逐步向Tanner图添加连接变量节点和校验节点的边。这种规则可以使Tanner图中的环比较大。用PEG算法构造的中、短码长低密度校验码是当前所知具有相同参数的最好的低密度校验码之一^[43]。在介绍具体的PEG算法之前,先作一些参数的说明。

假设LDPC码的变量节点集合为 $V_v = \{s_0, s_1, \dots, s_{n-1}\}$, 校验节点集合为 $V_c = \{c_0, c_1, \dots, c_{m-1}\}$ 。Tanner图由集合 (V, E) 表示。其中 V 是节点的集合,

$V = V_c \cup V_s$ 。 E 是边的集合, 当且仅当 $h_{i,j} \neq 0$, $h_{i,j} \in H$, $0 \leq i \leq m-1$, $0 \leq j \leq n-1$ 时, 边 $(c_i, s_j) \in E$ 。假设变量节点的度序列为 $D_s = \{d_{s_0}, d_{s_1}, \dots, d_{s_{n-1}}\}$, 其中 d_{s_j} 是变量节点 s_j 的度。校验节点的度序列为 $D_c = \{d_{c_0}, d_{c_1}, \dots, d_{c_{m-1}}\}$, 其中 d_{c_i} 是校验节点 c_i 的度。 $E = E_{s_0} \cup E_{s_1} \cup \dots \cup E_{s_{n-1}}$, 其中 E_{s_j} 包含了连接节点 s_j 的所有边, 连接节点 s_j 的第 k 条边表示为 $E_{s_j}^k$, $0 \leq k \leq d_{s_j} - 1$ 。定义在以变量节点 s_j 为根节点扩展的深度为 l 的树中所包含的校验节点集合为 $N_{s_j}^l$, 其补集为 $\bar{N}_{s_j}^l$ 则 $N_{s_j}^l + \bar{N}_{s_j}^l = V_c$ 。

基于上面的参数定义, 具体的PEG算法如下^[22]:

(1) 初始化: $j = 0, k = 0$ 。

(2) 若 $k = 0$, $E_{s_j}^0 = \text{边}(c_i, s_j)$, 其中 c_i 是当前图 $E_{s_0} \cup E_{s_1} \cup \dots \cup E_{s_{j-1}}$ 中度最小的校验节点。 $k = k + 1$ 。若 $k < d_{s_j}$, 继续执行下一步骤, 否则执行步骤(4)。

(3) 若 $k \neq 0$ 且 $k < d_{s_j}$, 将当前图以 s_j 为根节点扩展成深度为 l 的树。若 $\bar{N}_{s_j}^l \neq \emptyset$, 但 $\bar{N}_{s_j}^{l+1} = \emptyset$ 或者 $\bar{N}_{s_j}^l$ 随着 l 的增加不再增加但始终小于 m , $E_{s_j}^k = \text{边}(c_i, s_j)$, 其中 c_i 是 $\bar{N}_{s_j}^l$ 中度最小的校验节点。 $k = k + 1$ 。若 $k < d_{s_j}$, 执行步骤(3), 否则执行步骤(4)。

(4) 若 $k = d_{s_j}$, $j = j + 1$, $k = 0$ 。若 $j < n$, 执行步骤(2), 否则终止整个过程。

为何PEG构造的中、短码长的LDPC码的性能要优于随机构造的LDPC码的性能呢? 这是因为随机构造的Tanner图无法保证环长和码最小距离的下限, 而PEG算法构造的Tanner图具有优秀的环长和码最小距离的特性^[22]。

3.3.2 仿真结果

我们比较了用PEG算法和用随机方法构造LDPC中、短码的性能。首先我们构造了一个码率 $r = 1/2$, 码长 $n = 504$ 的规则(3,6)LDPC码。图3.5a是PEG码和随机码的最小环长柱状图, 可以看到PEG码的平均围长比随机码长。图3.5b比较了这两种码的误比特率和误码率性能, 译码迭代次数均为200次。PEG码的误比特率性能比随机码在 $p_e = 10^{-5}$ 时要好0.25dB。然后我们又构造了一个码率 $r = 1/2$, 码长 $n = 1008$, 变量节点度 $d_v = 3$ 的IRA^[71]码。从图3.6a中我们可以看到PEG码的围长为10和12, 而随机码的围长为6, 8, 10, 12, 明显PEG码的平均环长比随机码大。图3.6b比较了这两种码的译码性能, 译码迭代次数均为200次。PEG码的性能要好些。在仿真(3,6)LDPC码和IRA码时, 我们发现在仿真中(3,6)码并没有出现不可检错误, 而IRA码却出现了少量的不可检错误。这是因为IRA码中有大量的度为2和一个度为1的变量节点。虽然IRA码的性能不是很优, 但是它的结构特殊, 可以线性时间编码。而且我们也可以根据3.2.3节优化度序列的方法来设计好的IRA码。

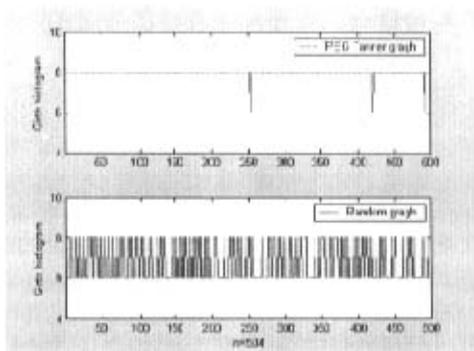


图3.5a PEG和随机构造(252,504)(3,6)LDPC码所对应Tanner图的最小环长柱状图

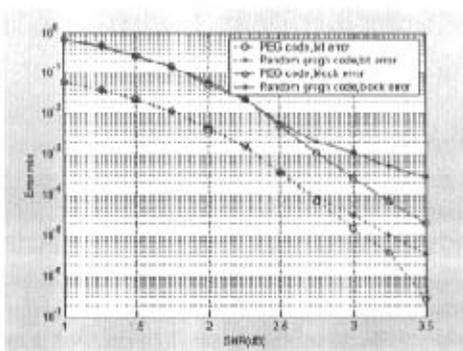


图3.5b PEG和随机构造(252,504)(3,6) LDPC码的译码性能图

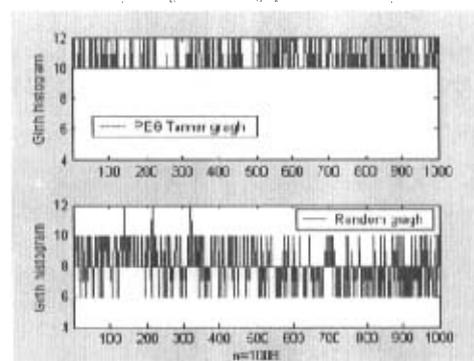


图3.6a PEG和随机构造(504,1008)IRA码所对应Tanner图的最小环长柱状图

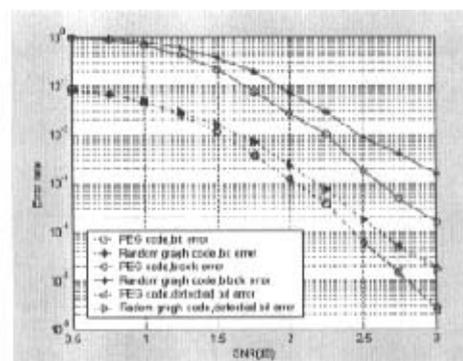


图3.6b PEG和随机构造(504,1008)IRA码的译码性能图

3.4 ACE算法

3.4.1 错误平层

LDPC码和Turbo码的迭代译码性能曲线被认为是“降水”曲线。有时候可以观察到“降水”区域的底部是较平的曲线，我们称之为错误平层。并行级联Turbo码的错误平层是由低重码字造成的。以前大家都认为规则LDPC码没有错误平层，这是因为计算机仿真能力有限，我们观察不到。但是Richardson使用硬件平台仿真发现甚至连(3,x)和(5,x)这种规则Gallager码都有错误平层^[63]。MacKay不仅仿真出Margulis和Ramanujan-Margulis LDPC码有错误平层，而且还分析了导致错误平层的原因^[64]。LDPC码与并行级联Turbo码不同的是，造成错误平层原因不仅有低重码字，还有相近码字。这些相近码字的产生一般是因为由这些变量节点所构成子图的邻居节点个数很少。环中的变量节点与剩余Tanner图中校验节点的连通性是影响错误平层区性能的重要因素。文[61]中提出的ACE算法不仅考虑了最小环长，更重

要的是它考虑了连通性的影响。通过计算机仿真可以发现ACE算法能有效的降低错误平层。

3.4.2 ACE算法

在分析环对迭代译码性能的影响时，我们必须认识到并不是环长越小对译码性能的影响就越大。有时候环长稍长但与剩余图连通性较差的环对译码性能的影响比环长稍短但与剩余图连通性较好的环大。若在构造LDPC码时抑制掉影响较大的环，就可以降低LDPC码的错误平层。在介绍ACE算法^[61]之前，为了方便我们对算法的理解，先介绍几个定义、定理。

定义3.1^[61]：若一个变量节点集合的所有邻居节点都连接这个集合至少两次，则这个变量节点集合称为一个stopping set。

引理3.1^[61]：若二部图中没有度为1的变量节点，则每个stopping set 都存在环。

定义3.2^[61]：若一个变量节点集合中不存在环，则这个集合称为无环集合。

引理3.2^[61]：一个度为2的变量节点集合为无环集合的充要条件是这个集合里所有变量节点对应的向量都线性无关。

推论3.1^[61]：最多只能有 $n-k-1$ 个度为2、长为 $n-k$ 的列向量线性无关。

定理3.1^[61]：在没有变量节点度为1的 (n, k) 码中，无环的变量节点集合 $\{v_1, v_2, \dots, v_s\}$ 满足 $\sum_{i=1}^s (d_i - 1) \leq n - k - 1$ ，其中 d_i 是节点 v_i 的度数。

文[65]中提出：LDPC码在删除信道下的迭代译码性能主要受最小的stopping set大小的限制。所以增大LDPC码最小的stopping set可以提高迭代译码性能。而通过改进LDPC码环的边扩展特性^[65]就可以增大最小的stopping sets。文[61]中的ACE算法就是基于此提出的。算法中有两个相关的参数—EMD和ACE（环的近似EMD），定义如下：

定义3.3^[61]：若一个校验节点仅与一个变量节点集合连接一次，则这个校验节点称为这个变量节点集合的外节点。集合外节点的个数由EMD表示。

定义3.4^[61]：长为 $2d$ 的环的ACE值等于 $\sum_i (d_i - 2)$ ，其中 d_i 是环中第 i 个变量节点的度数。我们可以认为度为 d 的变量节点的ACE值等于 $d - 2$ ，而校验节点的ACE值等于0。

可以证明若一个变量节点集合的EMD值较大，则它可以包含更多的节点来形成一个stopping set。EMD可用于任何一个变量节点集合，而ACE仅用于环。对一个环中的变量节点集合来说，ACE值是EMD值的上限。为了简单起见，ACE算法中的参数是ACE而不是EMD。如定义3.4所述，度数低的变量节点的ACE值小。相对的，度数低的变量节点容易形成环，ACE值较小的环与图中其他节点的连接也较少，而连接较少的子图容易受到噪声的影响。ACE算法可以较好地解决这个问题，它的基本思想是：构造LDPC码时，保证所有环长小于一定值的环都有一定的

ACE值。

假设 (n, k) LDPC码满足参数 (d_{ACE}, η_{ACE}) ，则所有环长不大于 $2d_{ACE}$ 的环的ACE值至少为 η_{ACE} 。要求构造的码为消息比特在前，校验比特在后。假设变量节点集合为 $\{v_0, v_1, \dots, v_{n-1}\}$ ，度序列为 $\{d_{v_0}, d_{v_1}, \dots, d_{v_{n-1}}\}$ ；校验节点集合为 $\{c_0, c_1, \dots, c_{n-k-1}\}$ ，度序列为 $\{d_{c_0}, d_{c_1}, \dots, d_{c_{n-k-1}}\}$ 。将变量节点按度数由高到低排列（若 $i < j$ 则 $d_{v_i} \geq d_{v_j}$ ）。因为度数高的节点译码收敛得快，这样会使消息比特得到更多的保护。具体的ACE算法如下：

(1) 初始化： $i = n - 1$ 。

(2) 根据度序列随机产生列向量 v_i 。若 $i \geq k$ 即 v_i 是校验比特，执行步骤(3)；否则，执行步骤(4)。

(3) 用高斯消去法判断 v_i 是否与 $v_{i+1}, v_{i+2}, \dots, v_{n-1}$ 线性相关，若线性相关则执行步骤(2)；否则，执行步骤(4)。

(4) 检测当前图中节点 v_i 所在环的ACE值是否符合约束条件：当环长 $l \leq 2d_{ACE}$ 时， $ACE \geq \eta_{ACE}$ 。若不符合，则执行步骤(2)；否则继续下一步骤。

(5) $i = i - 1$ 。若 $i \geq 0$ ，执行步骤(2)；否则终止整个过程。

步骤(3)的目的是保证生成的校验矩阵满秩，即保证了不存在只有度为2节点的环。步骤(4)中检测 v_i 所在环的ACE值的方法有两种，一种基于树图检测，另一种基于网格图检测。本文用的是基于树图检测的方法。假设Tanner图中变量节点集合为 $\{v_0, v_1, \dots, v_m\}$ ，校验节点集合为 $\{c_0, c_1, \dots, c_{n-k-1}\}$ 。按下述方法检测Tanner图中 v_0 所在环的ACE值：

(1) 初始化：所有变量节点和校验节点的 $p(\mu_i) = \infty$ ，其中 $p(\mu_i)$ 为路径 (v_0, μ_i) 的ACE值。 $p(v_0) = ACE(v_0)$ 。根节点 v_0 的深度为 $l = 0$ 。令 $l = 1$ 。

(2) 对任一深度为 $l - 1$ 的节点 w_s ，寻找它的孩子节点集合 $Ch(w_s)$ 。对集合中的每个节点 $\mu_i \in Ch(w_s)$ ，有 $p_{temp} = p(w_s) + ACE(\mu_i)$ 。若 $p_{temp} + p(\mu_i) - ACE(v_0) - ACE(\mu_i) < \eta_{ACE}$ ，返回（失败），终止整个过程。否则，若 $p_{temp} \geq p(\mu_i)$ ，表明 p_{temp} 所对应的路径不是最短路径，从图上删去路径 (w_s, μ_i) ；若 $p_{temp} < p(\mu_i)$ ，则 $p(\mu_i) = p_{temp}$ 。

(3) $l = l + 1$ 。若 $l \leq d_{ACE}$ ，执行步骤(2)；否则，返回（成功），终止整个过程。

其中步骤(2)、(3)中的失败、成功分别表示 v_i 所在环的ACE值不符合、符合约束条件。

Ramamoorthy在文[62]中分析了ACE算法比随机构造校验矩阵的方法好的原因，他证明了ACE算法可以减少stopping set的数量和降低错误平层。

3.4.3 仿真结果

我们用ACE算法分别构造了(1000,500)和(2000,1000)LDPC码，度序列均为

$\lambda(x) = 0.25105x + 0.30938x^2 + 0.00104x^3 + 0.43853x^9$, $\rho(x) = 0.63676x^6 + 0.36324x^7$ [53]。在AWGN信道下,用和积算法对这些码译码,迭代译码次数均为200次,图3.7和3.8是它们的译码性能图。参数 (d_{ACE}, η_{ACE}) 表示所有环长不大于 $2d_{ACE}$ 的环都有不小于 η_{ACE} 的ACE值。若 η_{ACE} 值越大,则Tanner图的连通性越好;若 d_{ACE} 值越大,则越大的环要受 η_{ACE} 值的限制。 d_{ACE} 和 η_{ACE} 是一对矛盾的值:增大其中一个参数必然导致另一个参数难以执行。所以只有选择适当的 (d_{ACE}, η_{ACE}) 值,才能构造出较好的LDPC码。

图3.7和3.8中与 (d_{ACE}, η_{ACE}) 码作比较的是无四环的随机码。从这两幅图中可以看到只要选择适当的参数 (d_{ACE}, η_{ACE}) ,就可以得到较低的错误平层。像图3.7中的(9,4)码的错误平层在 $BER = 2 \cdot 10^{-7}$ 处,大概要比随机码低2个数量级。图3.8中的(5,3)码的错误平层在 $BER = 9 \cdot 10^{-8}$ 处,大概要比随机码低1.5个数量级。但是这些有较低错误平层的码在低信噪比时的性能比随机码稍差一点。从图3.8中还可以发现无四环的(5,3)码与有四环的(5,3)码的性能只是稍有差别。而在3.3节中曾指出短环对中、短码长的LDPC码的性能影响很大。这就说明了有些环长稍长的环对码性能的影响可能会更大。而ACE算法就是在构造LDPC码时抑制掉影响较大的环。

以上讨论了图的连通性对错误平层的影响,介绍了构造低错误平层LDPC码的ACE算法。若将ACE算法和优化的度序列结合在一起构造LDPC码,将会得到性能优异且错误平层低的好码。

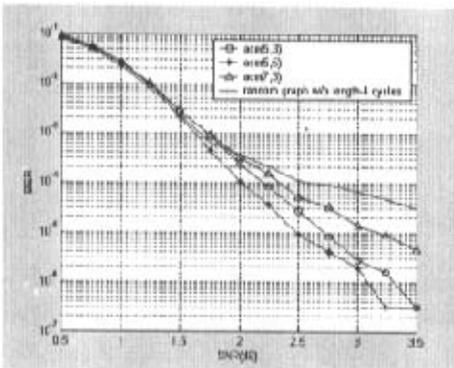


图3.7 (1000,500)LDPC码译码性能

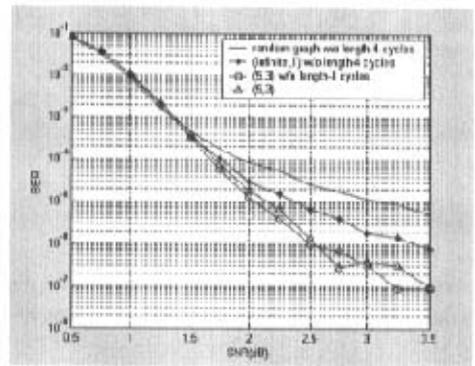


图3.8 (2000,1000)LDPC码译码性能

3.5 本章小结

本章概括了影响LDPC码性能的主要因素。分析了度序列对长码性能的影响,介绍了优化高斯信道下度序列的方法。分析了环对中、短码性能的影响,介绍了能使Tanner图拥有较大围长的PEG构造方法。最后分析了LDPC码错误平层产生的原因,介绍并仿真了能有效的降低LDPC码错误平层的ACE算法。

第四章 低密度校验码的量化译码

本章根据最小和译码算法的特点,研究了LDPC码量化译码的实现方法。首先介绍了LDPC码量化的研究背景;然后提出了一种基于密度进化理论优化设计LDPC码最小和量化译码器的算法。该算法可用于规则/非规则LDPC码最小和均匀/非均匀量化译码器的优化设计。

4.1 量化译码的研究背景

低密度校验码^[30]是一类逼近Shannon容量限的好码,当码长较长时其纠错性能甚至优于Turbo码。低密度校验码的优异性能及其在信息可靠传输中的良好应用前景已引起学术界和IT业界的高度重视,成为当今信道编码领域最瞩目的研究热点之一,低密度校验码的应用也已经被提到日程上。

实现低密度校验码的应用,译码器的设计是关键。目前低密度校验码的硬件实现引起了人们越来越多的关注^[66],而低密度校验码的量化译码设计是译码器硬件实现所必须考虑的关键环节。

LDPC码一般采用连续空间上和积(Sum-Product)算法进行译码,该算法虽然具有线性复杂度,但在码长较长时,其空间复杂度和时间复杂度仍然比较高。因此,设计实现复杂度可接受的、编码增益损失小的译码器是当前研究的热点问题之一^[68]。其中译码算法的选择及运算中数据的量化是译码器设计的关键所在。密度进化理论是一种用于分析迭代系统性能的有效方法:给定译码算法和信道,可以分析特定度序列LDPC码(也可以是其它类turbo码)的阈值^{[19],[53],[69]};给定LDPC码,也可以分析不同译码算法在不同信道下的收敛特性。因此,密度进化理论可以用来指导量化译码器的优化设计。

基于密度进化理论,本章给出了一种LDPC码最小和量化译码器的设计算法。与和积译码器相比,用此算法设计的译码器进行译码,虽然在性能上有所损失,但它的计算仅涉及整数加法运算,极大降低了计算复杂度和硬件实现难度,具有很好的实用性。

4.2 最小和量化译码器的密度进化

在3.2.1节中较详细的介绍了连续密度进化,其中要求信道和译码算法都满足式(3-1b)~(3-1d)定义的对称条件。对于置信传播算法,不同消息空间理论上是等价的,但是只有基于LLR量度的消息修正公式满足对称条件。因此,我们在分析AWGN

信道中置信传播译码器的性能时,采用LLR测度。最小和算法是退化的和积算法,虽然性能比和积算法大约有0.3dB的损失,但是计算复杂度相对要低一些。在LDPC码的硬件设计中低复杂度就意味着易于实现,这种折中的选择也是可以接受的。具体的最小和算法见2.3.2.4节。量化是指按某种规则将连续消息映射成离散消息。译码器的量化处理包含两部分:信道接收值的量化和译码中间变量的量化。量化译码器的密度进化是离散密度进化,它与连续密度进化不同的是密度不再是指概率密度而是指概率。下面介绍具体的基于LLR测度的最小和量化译码器的密度进化。

假设LDPC码的度序列生成多项式为 $\lambda(x) = \sum_{j=2}^K \lambda_j x^{j-1}$ 和 $\rho(x) = \sum_{j=2}^J \rho_j x^{j-1}$,其中 K, J 分别为最大变量节点度和最大校验节点度, λ_j (ρ_j)表示度为 j 的变量节点(校验节点)发出的边数占总边数的比例。假设量化的阶数为 $2s+1$ 。令 $\bar{P}^0 = [p_{-s}^0, \dots, p_1^0, \dots, p_s^0]$ 、 $\bar{Q}^{(l)} = [q_{-s}^{(l)}, \dots, q_1^{(l)}, \dots, q_s^{(l)}]$ 、 $\bar{P}^{(l)} = [p_{-s}^{(l)}, \dots, p_1^{(l)}, \dots, p_s^{(l)}]$ 和 $\bar{P}_r = [pr_{-s}, \dots, pr_1, \dots, pr_s]$ 分别为信道接收量化值的概率、校验消息的概率、变量消息的概率和最终变量消息的概率,其中 $p_i^0, q_i^{(l)}, p_i^{(l)}, pr_i$ 均是指消息值为 i 的概率, l 指迭代次数。最小和量化译码器的密度进化过程如下:

a) 初始化: 计算 \bar{P}^0 和初始化 $\bar{Q}^{(0)} = \bar{0}$;

b) 消息概率的更新计算:

阶段1: 校验节点向变量节点传递消息概率 $\bar{Q}^{(l)}$, 变量节点根据 $\bar{Q}^{(l)}$ 和 \bar{P}^0 计算 $\bar{P}^{(l+1)}$;

阶段2: 变量节点向校验节点传递已更新的消息概率 $\bar{P}^{(l+1)}$, 校验节点根据 $\bar{P}^{(l+1)}$ 计算 $\bar{Q}^{(l+1)}$;

c) 迭代终止: 变量节点根据 $\bar{Q}^{(l+1)}$ 计算最终变量消息的概率 \bar{P}_r 和译码错误概率 Pe 。

LDPC码一般采取的最优迭代终止策略为:

(1) 每轮迭代结束时, 计算译码错误概率 Pe ;

(2) 如果 $Pe < \xi$, 则宣告成功, 迭代终止, 否则继续迭代; 若迭代次数到达预先设定的最大次数仍未成功, 则宣告失败, 迭代终止。这里我们选 $\xi = 1e-6$ 。

在上述译码步骤中, b)中的消息概率更新是关键, 具体计算如下^[70]:

阶段1:

$$\bar{P}^{(l+1)} = \sum_{j=2}^K \lambda_j [\bar{P}^0 \otimes \bar{Q}^{(l) \otimes (j-1)}]; \quad (4-1)$$

阶段2: 计算 $\bar{Q}^{(l+1)} = [q_{-s}^{(l+1)}, \dots, q_1^{(l+1)}, \dots, q_s^{(l+1)}]$, 其中 $q_i^{(l+1)}$ 根据式(4-2)、(4-3)和(4-4)计算。

若 $i > 0$, 则

$$q_i^{(l+1)} = \sum_{j=2}^J \rho_j \sum_{\substack{t=0 \\ t \text{ 为偶数}}}^{j-1} \binom{j-1}{t} \left\{ \left[\sum_{x=1}^s p_{-x}^{(l+1)} \right] \left[\sum_{x=1}^s p_x^{(l+1)} \right]^{j-1-t} - \left[\sum_{x=+1}^s p_{-x}^{(l+1)} \right] \left[\sum_{x=+1}^s p_x^{(l+1)} \right]^{j-1-t} \right\}; \quad (4-2)$$

若 $i < 0$, 则

$$q_i^{(l+1)} = \sum_{j=2}^J \rho_j \sum_{\substack{t=-1 \\ t \text{ 为奇数}}}^{j-1} \binom{j-1}{t} \left\{ \left[\sum_{x=-s}^i p_x^{(l+1)} \right] \left[\sum_{x=-s}^i p_{-x}^{(l+1)} \right]^{j-1-t} - \left[\sum_{x=-s}^{i-1} p_x^{(l+1)} \right] \left[\sum_{x=-s}^{i-1} p_{-x}^{(l+1)} \right]^{j-1-t} \right\}; \quad (4-3)$$

若 $i = 0$, 则

$$q_i^{(l+1)} = 1 - \sum_{\substack{x=s \\ x=0}}^{x=-s} q_x^{(l+1)}. \quad (4-4)$$

译码错误概率由(4-5)式计算:

$$P_e = \sum_{i=-s}^{-1} pr_i + \frac{1}{2} pr_0 \quad (4-5)$$

其中 $\bar{Pr} = \sum_{j=2}^K \lambda_j [\bar{P}^0 \otimes \bar{Q}^{(l) \otimes j}]$, \otimes 表示线性卷积。

4.3 最小和量化译码器的设计

4.3.1 量化译码器的设计

最小和量化译码器设计的基本思想是: 根据密度进化理论优化量化译码器参数, 使量化译码器能达到最高的阈值。一般来说, 量化译码器若对性能要求越高, 其实现的复杂度也就越高, 根据密度进化理论优化设计的过程也就越复杂。为了简单起见, 作者根据此思想设计了两个不同阶数的均匀量化译码器, 均采用如下的基于对数似然比测度的量化规则^[70]:

$$\hat{q}_i = \begin{cases} t & , \quad (t - \frac{1}{2})\Delta \leq q_i < (t + \frac{1}{2})\Delta \\ -s & , \quad q_i < (\frac{1}{2} - s)\Delta \\ s & , \quad q_i \geq (\frac{1}{2} + s)\Delta \end{cases} \quad (4-6)$$

其中 $t = -s + 1, \dots, s - 1$, 量化阶数是 $2s + 1$, 量化间隔是 Δ , q_i 是消息值, \hat{q}_i 是其量化值。

在固定阶数的均匀量化译码器中所需要优化的参数只有量化间隔这一个参数，则量化间隔在 $[\Delta_{\min}, \Delta_{\max}]$ 内按下述算法优化：

(1) 取量化间隔 $\Delta = \Delta_{\min}$ ，根据密度进化理论计算阈值 σ 以及得到 σ 时所需的迭代次数 l ，并初始 $\Delta_{opt} = \Delta, \sigma_{max} = \sigma, l_{opt} = l$ 。

(2) 另取一个量化间隔 $\Delta' = \Delta + step$ ，计算信道值 σ' 和 l' 。

(3) 如果 $\sigma' > \sigma_{max}$ 或 $\sigma' = \sigma_{max}, l' < l_{opt}$ ，则 $\Delta_{opt} = \Delta', \sigma_{max} = \sigma', l_{opt} = l'$ ；若 $\Delta' > \Delta_{max}$ ，则迭代终止，否则 $\Delta = \Delta'$ ，重复步骤(2)。

4.3.2 数值结果

在AWGN信道下，对一个随机构造的(2094,3,6)规则LDPC码做33阶和65阶均匀量化译码仿真。LDPC码的码率为1/2，调制方式为BPSK，仿真中最大迭代次数为50次。图4.1显示33阶量化和65阶量化译码器的最大阈值均为0.825。图4.2表示在不同的量化间隔下，为得到图4.1中的阈值所需的迭代次数。结合图4.1、图4.2可知这两个译码器在达到最大阈值时的译码收敛速度相差很小。结合图4.1和图4.2，33阶量化的量化间隔取0.25，65阶量化的量化间隔取0.14。

针对上述随机构造的(2094,3,6)规则LDPC码，图4.3给出了和积连续译码和采用上述两个量化译码器译码的误比特率性能。如图所示，采用量化译码器的译码性能在高信噪比时比采用和积连续译码的性能差0.25dB。65阶和33阶量化译码器的性能非常接近，只是在高信噪比时前者略好些。

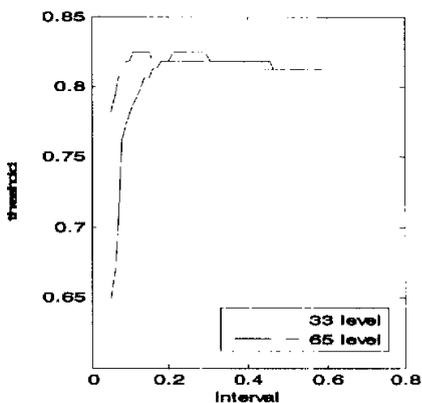


图4.1 量化间隔和信道阈值的关系

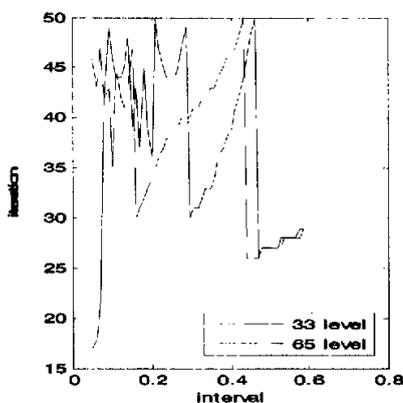


图4.2 量化间隔和迭代次数的关系

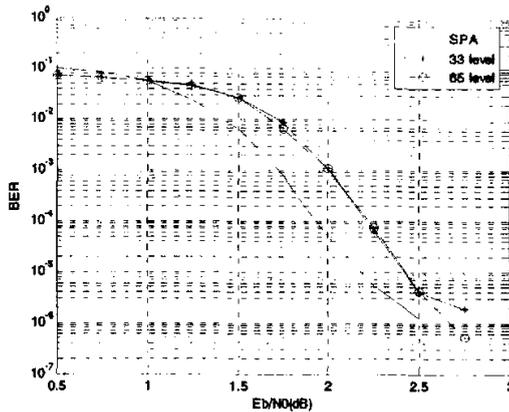


图4.3 (2094,3,6)规则LDPC码的译码性能（最大迭代次数为50次）

在本章中，作者只设计了初始消息和中间消息量化规则相同的均匀量化译码器。因为均匀量化简单，对性能要求不太高的量化译码器而言还是实用的，而且均匀量化译码器的硬件实现复杂度较低。但是若对量化译码器的性能要求较高，就要考虑非均匀量化译码器的设计了。本章提出的设计方法同样可以用于非均匀量化译码器的设计。首先要考虑选择怎样的量化规则，然后提取出参数，最后再根据密度进化理论优化参数。我们进一步的工作将是如何优化设计非均匀量化译码器，使它的量化阶数更低但是性能更好。

4.4 本章小结

本章介绍了一种优化LDPC码最小和量化译码器设计的算法，算法具有如下特点：

- (1) 根据密度进化理论指导量化译码器的优化设计；
- (2) 设计的最小和量化译码器的运算只涉及整数加法和比较运算，计算复杂度低；
- (3) 低阶均匀量化译码器的性能比和积连续译码的性能稍差一些。

虽然设计的低阶均匀量化译码器性能比和积连续译码的性能稍差一些，但是由于运算简单，使LDPC码译码器的硬件实现变得非常容易。而且该算法同样可以用于低阶非均匀量化译码器的优化设计。这样量化译码器的性能跟和积连续译码的性能更接近，但是计算复杂度和硬件实现难度还是要低一些。该算法对LDPC码的实用化有较大意义。

结 论

低密度校验码是能够逼近 Shannon 容量限的好码，它的诸多优点：如译码具有线性时间复杂度、长码的性能甚至超越 Turbo 码，使得低密度校验码的研究成为信道编码理论界的热点之一。自上世纪 90 年代中期低密度校验码的重新发现，对它的理论研究已经取得丰硕的成果，关于低密度校验码的应用研究也已经全方位展开。

作者在总结已有的理论成果基础上，分析了低密度校验码的性能，研究了低密度校验码的量化译码问题。

作者在理解密度进化和高斯逼近的思想基础上，介绍了优化度序列的方法；分析了环对 LDPC 码性能的影响，介绍并仿真了 PEG 算法；最后分析了 LDPC 码错误平层产生的原因，介绍了 ACE 算法，通过仿真发现 ACE 算法能有效的降低错误平层。

对于量化译码问题，提出了一种优化设计最小和量化译码器的方案，该方案具有如下特点：

- (1) 根据密度进化理论指导量化译码器的优化设计；
- (2) 设计的最小和量化译码器的运算只涉及整数加法和比较运算，计算复杂度低；
- (3) 低阶均匀量化译码器的性能比和积连续译码的性能稍差一些。

因此采用优化的最小和量化译码算法，LDPC 码译码器的硬件实现变得非常容易，且译码性能损失很小。该实现方案对 LDPC 码的实用化有较大意义。

图模型上 LDPC 码的研究内容相当广泛，还有许多理论和实际应用问题没有得到解决。本文的研究只涉及了其中个别问题，着重于 LDPC 码的性能分析和量化译码设计，这些研究成果还有待于做进一步的扩展研究。主要包括：

- (1) LDPC 码的和积译码算法只有在无环图上才能获得最优的译码性能，如何优化能够在有环图上也能获得最优或近似更优的译码性能；
- (2) 利用密度进化理论分析 LDPC 码译码只能是无限长分析，如何建立 LDPC 码有限长分析的理论，为构造良好的 LDPC 码尤其是短码奠定基础；
- (3) 如何设计实际可行的 LDPC 码量化译码器是一个值得研究的问题。
- (3) 如何设计实际可行的 LDPC 码量化译码器是一个值得研究的问题。

致 谢

很荣幸能够进入信道编码实验室，很荣幸能够遇上我的博士生导师王新梅教授。在此，我将我最诚挚的谢意和深深的祝福献给我的导师王新梅教授和师母吉筮琴老师。王老师渊博的知识、平易近人和淡泊名利的待人处世方式为学生树立良好的榜样。在学习上，王老师倡导自由、开放的学术氛围和每周一次的学术讨论使我受益匪浅；在生活上，虽然王老师工作繁忙，但是他仍然很关心学生，每逢节假日尽可能组织一些集体活动。在这里，我衷心地感谢您。

衷心感谢白宝明教授。白老师在生活和学习上都给了我莫大的帮助。感谢李颖老师和郭旭东夫妇。李老师不仅给我树立了榜样而且在许多具体的工作中给了我许多指导与帮助；与郭旭东讨论经常给我许多启发。特别感谢童胜博士、王单博士。论文中的一些工作使我们共同完成的。

感谢信道编码实验室的马文平教授、贺玉成教授、徐朝军博士、王鹏博士、许卫东博士、周秦英博士、刘景美博士、车书玲博士、池凯凯博士、孙岳博士、孙蓉博士、苏加军博士、张庆治硕士、汶丽硕士、张善旭硕士、王静博士、李卓博士、廖婷硕士、陈超博士、荆莉娟博士、董磊硕士、王晶硕士、李丹硕士。

感谢和我一起学习的金莹硕士、黄建忠硕士、寇倩硕士、鲁慧硕士、邓双成博士、刘海波硕士、邓杰硕士、李浩硕士、郑贱平博士、冀晓征硕士、付家乐硕士、冯俊平硕士、陈学亮硕士。

最后，我要深深感谢我的父母和亲人，感谢他们多年来无私的养育和关怀！人生是一种经历，我很高兴经历了这丰富多彩的硕士生活，在这里我感谢所有关心和帮助过我的人，谢谢你们！

参考文献

- [1] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. J.*, vol.27, pp.379-423, 623-656. July, October, 1948.
- [2] A.R.Calderbank, "The art of signaling: Fifty years of coding theory," *IEEE Trans. IT*, vol.44, No.6, pp. 2561-2595, Oct. 1998.
- [3] J.G Proakis. *Digital Communications*, 4th.ed. McGraw-Hill Companies, Inc., 2001
- [4] R. G. Gallager, "Information theory and reliable communication," MIT, John Wiley&Sons, Inc, 1968.
- [5] 王育民, 梁传甲, "信息与编码理论", 西北电讯工程学院, 1986.
- [6] 张辉, 曹丽娜, "现代通信原理及技术", 西安电子科技大学出版社, 2002.
- [7] T. J. Richardson, R. L. Urbanke, "The capacity of low-density parity-check codes", *IEEE Trans. IT*, vol.47, No.2, pp.599-618, Feb. 2001.
- [8] R. G. Gallager, "Low-Density Parity-Check Codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21-28, Jan. 1962.
- [9] M. Siper and D. A. Spielman, "Expander codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp.1710-1722, November 1996.
- [10] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low-density parity-check codes," *Electronics Letters*, vol.32, pp.1645-1646, August 1996.
- [11] Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol.27, no.5, pp.533-547, Sept. 1981.
- [12] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," In *Proc. of ICC'93*, pp.1064-1070, May 1993.
- [13] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol.28, no.1, pp.55-67, Jan.1982.
- [14] G. David Forney, Jr, "Codes on Graphs: News and Views," 2nd International Symposium on Turbo Codes&Related Topics, pp. 9-16, Brest, France, 2000.
- [15] N. Wiberg, "Codes and decoding on general graphs," Ph. D. Thesis, U. Linkoping, Sweden, 1996.
- [16] N. Wiberg, H.-A. Loeliger and R. Kotter, "Codes and iterative decoding on general graphs," *Euro. Trans. Telecomm.*, vol. 6, pp. 513-525, Sept./Oct., 1996.
- [17] N. Alon and M. Luby, "A linear-time erasure-resilient code with nearly optimal recovery," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1732-1736, Nov. 1996.

- [18] Proc. 2000 IEEE Intl. Symp. Inform. Theory (Soorrento, Italy), p. 5, June 2000.
- [19] T. J. Richardson and Rüdiger L. Urbanke, "The Capacity of Low-Density Parity-Check Codes Under Message-Passing Decoding," IEEE Trans. Inform. Theory, vol. 47, no.2, Feb. 2001.
- [20] Sae-Young Chung, G. D. Forney, Jr., T. J. Richardson, and Rudiger Urbanke, "On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit," IEEE Comm. Letters, vol.5, no.2, Feb. 2001.
- [21] D. Divsalar, H. Jin and R. J. McEliece, "Coding theorem for 'Turbo-like' codes," Proc. 1998 Allerton Conf. (Allerton, IL), pp.201-210, Sept. 1998.
- [22] Xiao-Yu Hu, Evangelos Eleftheriou, and Dieter-Michael Arnold, "Progressive Edge-Growth Tanner Graphs," Globecom2001.
- [23] Li Ping and Keying Y. Wu, "Concatenated Tree Codes: A Low-Complexity, High-Performance Approach," IEEE Trans. Inform. Theory, vol. 47, no.2, Feb. 2001.
- [24] H.-A. Loeliger, F. Lustenberger, M. Helfenstein and F. Tarkoy, "Probability propagation and decoding in analog VLSI," Proc. 1998, IEEE Intl. Symp. Inform. Theory (Cambridge, MA), p.146, Aug. 1998.
- [25] J. Hagenauer and M. Winklhofer, "The analog decoder," Proc. 1998 IEEE Intl. Symp. Inform. Theory (Cambridge, MA), p.145, Aug. 1998.
- [26] Y. Weiss, "Correctness of local probability propagation in graphical models and loops," Neural computation, vol.12, pp.1-41, 2000.
- [27] 贺玉成, 孙韶辉, 慕建君, 王新梅. 快速低密度校验码迭代译码量化算法. 西安电子科技大学学报, 2002, 29(3):338-342.
- [28] ZHANG T, PARHI KK. "VLSI Implementation 2 Oriented (3,K) . Regular Low-Density Parity-Check Codes. From Internet," {tzhang, parhi}@ece. umn. edu.
- [29] F.R. Kschischang, B.J. Frey, and H.-A. Loeliger. "Factor graphs and the sum-product algorithm." IEEE Trans. Inf. Theory, 47(2): 498~519, 2001.
- [30] R.G. Gallager. "Low density parity-check codes." Cambridge, MA: MIT Press, 1963.
- [31] M.G. Luby and M. Mitzenmacher. "Improved low-density parity-check codes using irregular graphs." IEEE Trans. Inf. Theory, 47(2):585-598, 2001.
- [32] M.C. Davey and D.J.C. Mackay. "Low density parity check codes GF(q)." IEEE Comm. Letters, 2(6):165-167, June 1998.
- [33] 盛骤, 谢式千, 潘承毅, 概率论与数理统计 (第二版), 高等教育出版社, 1998

- 年8月.
- [34]David J. C. MacKay and Matthew C. Davey, "Two Small Gallager Codes," [online] available at <http://wol.ra.phy.cam.ac.uk/mackay/>
- [35]D. J. C. MacKay, S. T. Wilson, and M. C. Davey, "Comparison of constructions of irregular Gallager codes," *IEEE Trans. on Commun.*, vol.47, no.10, pp:1449-1454, Oct. 1999.
- [36]M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. "Improved low-density parity-check codes using irregular graphs and belief propagation. "In *Proc. IEEE international Symposium on Information Theory (ISIT)*, page 117, 1998.
- [37]D. J. C. MacKay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol.45, no.2, pp.399-431, 1999.
- [38]J. Campello, D. S. Modha, and S. Rajagopalan, "Designing ldpc codes using bit-filling," in *Proc. Int. Conf. Communications (ICC)*, Helsinki, Finland, 2001.
- [39]Jorge Campello and Dharmendra S. Modha, "Extended Bit-Filling and LDPC Code Design," *Globecom* 2001.
- [40]Sarah J. Johnson and Steven R. Weller, "Construction of Low-density Parity-check Codes from Kirkman Triple Systems," *IEEE Global Telecommunications Conference, Incontrol Productions, Monterey California*, 2001.
- [41]Jon-Lark Kim, Uri N. Peled, Irina Perepelitsa, and Vera Pless, "Explicit Construction of Families of LDPC Codes with Girth at Least Six," *Proceedings of the 40th Allerton Conference on Communication, Control, and Computing (10/2-10/4) at Allerton, IL.*, Oct. 2002, pp. 1024-1031.
- [42]Joachim Rosenthal, Pascal O. Vontobel, "Constructions of Regular and irregular LDPC codes using Ramanujan graphs and ideas from Margulis," *ISIT2001, Washington, DC*, June, 2001.
- [43]Abhiram Prabhakar and Krishna Narayanan, "Pseudorandom Construction of Low-Density Parity-Check Codes Using Linear Congruential Sequences," *IEEE Trans. on Commun.*, vol. 50, no.9, Sept. 2002.
- [44]T. J. Richardson, R. L. Urbanke, "Efficient Encoding of Low-Density Parity-Check Codes," *IEEE Trans. On Info.*, vol.47, no.2, Feb.2001.
- [45]Michael Yang, William E. Ryan, Yan Li, "Design of Efficiently Encodable Moderate-Length High-Rate Irregular LDPC codes," *IEEE Trans. on Commun.*, vol. 52, no.4, April 2004.
- [46]Tong Zhang, Keshab K. Parhi, "A Class of efficient encoding generalized

- low-density parity-check codes,"IEEE 2001.
- [47]Hachiro Fujita, Kohichi Sakaniwa, "An efficient encoding method for ldpc codes based on cyclic shift,"ISIT 2004, Chicago, USA, June 27-July 2, 2004.
- [48]R.Michael Tanner,Deepak Sridhara,Arvind Sridharan,Thomas E.Fuja,Daniel J.Costello, "LDPC Block and Convolutional Codes Based on Circulant Matrics," IEEE Trans. On Info., vol.50, no.12, Dec.2004.
- [49]C. Heegard and S.B. Wicker. "Turbo Coding."Norwell, MA: Kluwer Academic Publishers, 1999.
- [50]A. Vardy. "Trellis structure of codes." In Handbook of Coding Theory, V.S. Pless and W.C. Huffman, Eds. Amsterdam, The Netherlands:Elsevier, Vol.2, 1998.
- [51]S.-Y. Chung. "On the construction of some capacity-approaching coding schemes."Ph.D. Dissertation, Massachusetts Institute of Technology, 2000.
- [52]M.G. Luby, M. Mitzenmacher, M.A. Shokrollahi, and D.A. Spielman. "Analysis of low-density codes and improved designs using irregular graphs."In Proc. 30th Annu. Symp. Theory of Computing, pp.249-258, 1998.
- [53]T. J. Richardson, M. Amin Shokrollahi, and R. L. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," IEEE Trans. Inform. Theory, vol.47, no.2, pp.619-637, 2001.
- [54]Flarion Technologies Inc, Vector-Low-Density Parity-Check Coding Solution Data Sheet.
- [55]S.-Y. Chung, T.J. Richardson, and R.L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation." IEEE Trans. Inf. Theory, 47(2):657-670, Feb. 2001.
- [56]P. Rusmevichientong and B.V. Roy, "An analysis of belief propagation on the turbo decoding graph with Gaussian densities. IEEE Trans." Inf. Theory, 47(2):745-765, Feb. 2001.
- [57]Y. Weiss and W.T. Freeman, "Correctness of belief propagation in Gaussian graphical models of arbitrary topology."In Proc. Adv. Neural Inf. Processing Syst., vol.12, Dec. 1999.
- [58]Rainer Storn and Kenneth Price, "Differential Evolution-A simple and efficient adaptive scheme for global optimization over continuous spaces,"TR-95-012, March 1995.
- [59]R.Storn and K.Price, "Differential evolution-A simple and efficient heuristic adaptive scheme for global optimization over continuous spaces,"J.Global Optimization, vol.11, pp.341-359, 1997.

- [60] Jilei Hou, Paul H. Suelgel and Laurence B. Milstein, "Performance Analysis and Code Optimization of Low Density Parity-Check Codes on Rayleigh Fading Channels," *IEEE Jour. Selected Areas. Commun.*, vol.19, no.5, May 2001.
- [61] Tao Tian, Christopher R. Jones, John D. Villasenor and Richard D. Wesel, "Selective avoidance of cycles in Irregular LDPC code Construction," *IEEE Trans. on Commun.*, vol.52, no.8, pp. 1242-1247, Aug. 2004.
- [62] Aditya Ramamoorthy and Richard D. Wesel, "Analysis of an algorithm for irregular LDPC code construction," *ISIT2004, Chicago, USA, June 27-July 2, 2004.*
- [63] Tom Richardson, "Error floors of LDPC codes," tjr@flarion.com.
- [64] David J.C. MacKay and Michael S. Postol, "Weaknesses of Margulis and Ramanujan-Margulis Low-Density Parity-Check Codes," available at <http://www.elsevier.nl/locate/entcs/volume74.html>.
- [65] C. Di, D. Proietti, E. Telatar, T. Richardson and R. Urbanke, "Finite length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, pp. 71-78, 1982.
- [66] 童胜, "低密度校验码理论及其量化译码," 西安电子科技大学硕士论文, 2004.
- [67] 贺玉成, "基于图模型的低密度校验码理论及应用研究," 西安电子科技大学博士论文, 2002.
- [68] Jianguang zhao, Farhad Zarkeshvari, Amir H. Banihadhemi, "On Implementation of Min-Sum Algorithm and Its Modifications for Decoding Low-Density Parity-Check(LDPC) Codes." *IEEE Commun. Lett.*, 2005, 53(4), 549-554.
- [69] T. Richardson and R. Urbanke, "Multi-edge type ldpc codes," draft.
- [70] Alberto Jimenez Felstrom, Kamil sh. Zigangirov, "Time-Varying Periodic Convolutional Codes With Low-Density Parity-Check Matrix[J]," *IEEE Trans on IT*, 1999, 45(6): 2181-2191.
- [71] H. Jin, A. Khandekar, and R. McEliece, "Irregular repeat-accumulate codes," *Proc. 2nd Int. Symp. on Turbo Codes & Related Topics*, pp. 1-8, 2000.
- [72] Tuvi Etzin, Ari Trachtenberg and Alexander Vardy, "Which codes have cycle-free Tanner graphs," *IEEE Trans. Inform. Theory*, vol.45, no.6, Sept. 1999.

作者在攻读硕士期间完成的工作

一、完成论文

- [P1] 包晓燕, 王新梅, “基于密度进化的 LDPC 码最小和量化译码器设计”, 北京电子科技学院学报.
- [P2] 包晓燕, 王新梅, “低密度校验码最小和量化译码器的设计”, 2005 年西安电子科技大学研究生学术年会.

二、主要科研

1. 国家自然科学基金项目, “基于图模型的低密度校验码编码理论研究”, 项目编号: 60272057;
2. 华为基金项目, “LDPC 码的实用化编译码技术研究”。