文章编号:1001 - 893X(2012)08 - 1395 - 09

低密度奇偶校验码构造及编译码研究进展*

张用宇,吴东伟,左丽芬,刘 冰

(解放军 91469 部队,北京 100841)

摘 要:低密度奇偶校验(LDPC)码具有接近 Shannon 限的良好性能,能有效提高数据传输的可靠性。为提高 LDPC 码的性能,对码字的研究多集中于构造、编码和译码这几方面的基础研究。首先简要给出了 LDPC 码的基本描述,然后对二进制和多进制 LDPC 码的关键技术进行了系统归纳和全新分类,分别从构造、编码和译码 3 个方面进行了详细探讨,重点对最新的研究成果进行了全面分析和总结,对 LDPC 码今后的研究具有指导意义。

关键词:低密度奇偶校验码;奇偶校验矩阵;构造;编码;译码

中图分类号:TN911.22 **文献标志码**:A doi:10.3969/j.issn.1001 - 893x.2012.08.035

Survey on Construction, Encoding and Decoding of Low-Density Parity-Check Codes

ZHANG Yong-yu, WU Dong-wei, ZUO Li-fen, LIU Bing

(Unit 91469 of PLA, Beijing 100841, China)

Abstract: Low - density parity - check (LDPC) codes are considered as a class of codes with Shannon - limit - approaching performance, which can improve reliability of data transmission effectively. In order to improve the performance of LDPC codes, most of the research is focused on construction, encoding and decoding which are the basis research. The basic description of LDPC codes is given firstly. The key technologies of binary and nonbinary LDPC codes are summarized systematically and classified in new ways, and the construction, encoding and decoding are investigated in detail. A comprehensive survey of the latest literatures is provided. The review is of high theoretical significance for the future work.

Key words: low-density parity-check(LDPC) code; parity-check matrix; constructions; encoding; decoding

1 引 言

回顾 60 多年来编码领域的发展,低密度奇偶校验(Low - Density Parity - Check, LDPC)码和 Turbo 码是到目前为止在纠错编码领域中最具代表性的成果。LDPC 码是继 Turbo 码之后的又一重大进展,也是目前距离 Shannon 限最近的纠错码,是当今信道编码领域的研究热点之一。

1962 年,Gallager 在其博士论文中首次提出了 LDPC 码[1],并在论文中提出了两种递归概率译码算法,但是由于当时计算机运算能力水平的限制,未能证明其具有接近 Shannon 限的能力。Gallager 提出了两个具有创造性的观点[1]:一是用简单稀疏校验矩阵的随机置换和级联来模拟随机码;二是采用迭代译码的方法逼近最大似然译码。由于当时 RS 码和卷积码的级联被认为非常适于实际的差错控制系

* **收稿日期**:2012 - 03 - 27;**修回日期**:2012 - 05 - 15
基金项目:国家高技术研究发展计划(863 计划)项目(2010AA7010422)
Foundation Item: The National High - tech R&D Program(863 Program) of China (2010AA7010422)

统,致使 Gallager 的工作被忽视了近 30 年,在此期间,Zyablov、Pinsker、Margulis 以及 Tanner 仍然还致力于 LDPC 码的研究。直到 Turbo 码提出以后,人们才发现 Turbo 码实质上就是 LDPC 码的一个特例,LDPC 码又重新燃起了人们的兴趣。1996 年,Mackay 等人的研究使 LDPC 码的研究跨入了一个新阶段[2],他指出 LDPC 码可以像 Turbo 码一样接近 Shannon 限。2001 年,Sae - Young Chung 将密度演化算法进行简化,提出一种高斯近似(Gaussian Approximation,GA)的近似算法[3],将原来无限维的密度迭代计算转化为一维的高斯期望计算,提高了求取 LDPC 码门限值的速度,在 AWGN 信道下进行二进制传输,码率为 1/2 的最好不规则 LDPC 码的门限值距离 Shannon 限仅仅0.004 5 dB,仿真结果显示,码长为 10^7时,在误比特率(Bit Error Rate,BER)为 10^{-6}的情况下,离 Shannon 限的距离低于0.04 dB,这一结果超过了 Turbo 码。在近十几年里,对 LDPC 码的研究主要集中于以下 4 个方面[4]:校验矩阵的构造、编译码算法的优化、性能分析和优化设计以及 LDPC 码在实际系统中的应用。本文对二进制和多进制 LDPC 码的关键技术从构造、编码和译码 3 个方面进行了系统归纳和详细探讨,总结了目前已取得的最新成果,为进一步研究提供了思路。

2 校验矩阵的构造

2.1 二进制校验矩阵构造方法

LDPC 码的结构决定了码的性能,同时也决定了编译码方案的选择和复杂度。LDPC 码的校验矩阵具有两种形式:随机化结构和结构化结构。到目前为止,有关 LDPC 码的构造方法数不胜数。二进制 LDPC 码校验矩阵的构造方法主要可以分为两大类:随机化构造法和结构化构造法。随机化构造法主要是按照特定的设计准则和 Tanner 图结构、度分布、停止集等条件来搜寻满足要求校验矩阵。典型方法主要有 1962 年 Gallger 提出的 Gallager 构造法[1],其基本思想是第一个子矩阵采用满足要求的固定设置,其余矩阵是第一个子矩阵的随机列重排。1997 年,Mackay 在 Gallager 的基础上给出了几种校验矩阵的随机构造方法,使 Tanner 图中短环的数量最少,为了保证线性时间编码复杂度,将校验矩阵的构造强制为下三角阵的形式[2],但是这种约束太强,必然破坏校验矩阵的 girth 约束和变量节点及校验节点的度数约束,从而导致性能下降。2001 年,Yongyi Mao 和 Amir Banihashemi 提出一种通过 girth 分布在码字集合中寻求好码的启发式方法,Jorge Campello 提出了具有启发式的比特填充(Bit-Filling)算法,Xiaoyu Wu 提出了一种渐进边增长(Progressive Edge Growth,PEG)方法[5],其在变量节点和校验节点边逐渐增加的过程,使 Tanner 图具有最大的 girth,该方法可以产生具有线性编码复杂度的下三角形式校验矩阵,也可扩展到多进制 LDPC 码的构造上。结构化构造方法则是利用抽象代数、有限几何和组合数学等数学理论构造出具有规律可循结构的校验矩阵。在中、短码长 LDPC 码的构造上,好的结构化构造可能会优于随机化构造;在长码长 LDPC 码的构造上,采用 Thomas Richardson 的密度进化理论可以构造出误码性能很好的校验矩阵,结构化构造校验矩阵的性能很难与随机构造的相媲美。但从实际角度来看,随机化校验矩阵缺少有规律的结构,致使 LDPC 码编码和译码过程变得复杂,且需要较大的存储空间来存储校验矩阵,在中短码长上随着码率的升高,随机化构造法很难保证校验矩阵的稀疏性,也难以避免 Tanner 图中的短环,构造出好 LDPC 码也就相对更难,这些缺陷都阻碍了随机化构造的发展和应用。而结构化码的优势在于矩阵存储空间小,编译码时延短,具有良好的最小距离和 girth 特性,易于实现。2001 年,Yu Kou 提出了基于有限几何(Finite Geometries)的 LDPC 码构造方法[6],该方法主要是利用欧氏和射影几何中的点、线和超平面的关系,这种方法构造出的码已经被美国国家航空航天局推荐在深空卫星通信中使用。2004 年,Bassem Ammar 提出了基于平衡不完全区组设计(Balanced Incomplete Block Design,BIBD)的 LDPC 码,BIBD 设计是组合数学中组合设计的一种方法,除此之处,相关的设计还有 Steiner 和 Kirkman 三重系统[7]、Bose 设计、反 Pasch 技术等。同年,Fossorier 提出了基于循环置换矩阵的 LDPC 码构造方法,并给出了 girth 为 12 以下的充分必要条件或必要条件。2006 年,Lan Lan 提出了基于有限域(Finite Field)的 LDPC 构造方法[8],这种方法奠定了准循环 LDPC 码构造的一种基调,后续一些学者深入研究采用不同的数学方法构造出满足 RD 约束的基矩阵。2007 年,Jun Xu 提出对 LDPC 码的分解(Decomposition)和掩蔽(Masking)技术。2010 年,Jingyu Kang 提出了一种满足 RD 约束更大类构造 LDPC 码校验矩阵的方法,其涵盖了 Lan Lan

提出的有限域的第一类方法,同年,Li Zhang 对准循环校验矩阵进行了秩分析,并给出了基于 Latin 方格校验矩阵具体秩表达式[9]。从上述的发展可以看出,Shu Lin 课题研究小组在二进制准循环 LDPC 码上的研究做出了开创和突出性的贡献,并且其研究仍在继续。2005 年到 2008 年间,华中科技大学的彭立、朱光喜等人提出了基于等差数列、斐波那契数列、二次同余序列、Q 矩阵等 LDPC 码构造方法。2007 年,Norifumi Kamiya 提出了基于有限域仿射平面的高码率 QC LDPC 码,并且给出了码字的循环置换矩阵明确的秩公式,Li Zhang 对秩的分析正是来源于 Kamiya 的启示。QC LDPC 码的构造方法层出不穷,如中国剩余定理、二次同余序列、量子理论、整数网格等,但是这些方法都是采用不同的数学方式来构造满足 RD 约束的基矩阵或是与之相关的扩展研究。

2.2　多进制校验矩阵构造方法

二进制 LDPC 码的构造只需确定校验矩阵中 1(非零)的位置,多进制 LDPC 码的构造与二进制不同,除了位置的确定,还有数值的选取。近些年来,许多学者把目光从二进制投向到多进制上。多进制 LDPC 码的构造方法与二进制是一样的,但为了更为明确,我们将多进制 LDPC 码的构造方法分为 3 类:随机化构造法、结构化构造法和混合构造法。这 3 种构造方法构造出的校验矩阵只会具有两种形式:随机化结构和结构化结构,形成随机码和结构化码。只有非零值的位置和取值两个参数同时具有结构化的特性时,才认为矩阵是结构化的。多进制随机化和结构化构造法的主要思路与二进制相同,混合构造法的主要思路是在结构化构造的基础上融入随机化方法,比如非零值位置的选择采用结构化方法,数值的选取采用随机方法,或是在结构化构造的基础上采用随机化方法进行处理,由此构造的码可能是随机码,也可能是结构化码。多进制 LDPC 码的构造吸取了二进制发展的经验,大部分研究放在了结构化构造法上。2008 年,Lingqi Zeng 在二进制的基础上提出了有限域和有限几何的多进制 QC LDPC 码构造方法[10-11]。2009 年,Bo Zhou 提出了基于有限欧氏几何平面和阵列掩蔽(Array Masking)技术的多进制 QC LDPC 码的构造,其中采用的阵列掩蔽技术是在 Jun Xu 基础上的扩展,还提出了通过阵列分散(Array Dispersion)技术构造的多进制 QC LDPC 码,具有很好纠正突发错误的能力,实验结果表明在 AWGN 信道和衰落信道下,多进制 QC LDPC 码的性能明显优于同码长码率的 RS 码。2010 年,Jingyu Kang 提出的满足行距离(Row - Distance,RD)约束更大类 QC LDPC 码构造方法[12],其中包括了多进制的情况。上述方法是 Shu Lin 课题研究小组在多进制 LDPC 码构造方面做出的主要工作,这些方法在继承二进制 LDPC 码构造方法的同时,也继承了其优缺点,有限几何由于几何结构的固定化,构造出的码字数量有限,码长码率受限,但存在的好处在于校验矩阵存在较多的冗余行,码字在迭代译码过程中能更快地收敛;有限域法构造的具有多进制循环置换阵列结构的校验矩阵具有较大的灵活性,辅以上述相关技术可以得到不同码长、不同码率、不同最小距离的规则和非规则多进制 LDPC 码。2008 年,北京理工大学刘珂珂、匡镜明等人在满足 RD 约束要求基矩阵的框架下构造了 6 种多进制 QC LDPC 码。2010 年,西安电子科技大学的陈超、白宝明、王新梅等人提出了基于 Singer 完备差分集构造的多进制 QC LDPC 循环码[13],其 Tanner 图的 girth 为 12,最小符号 Hamming 距离为 6,同时也提出了基于循环最大距离可分码的多进制 QC LDPC 码等。到目前为止,纵观多进制 QC LDPC 码的发展,其基本思想还是停留在构造满足 RD 约束的基矩阵上,至于如何满足,研究学者可谓各显神通,从数学理论的各个角度设法进行挖掘研究。

2.3　girth 对校验矩阵构造的影响

Tanner 图中最短环的长度定义为 girth。由于短环的存在会破坏变量节点和校验节点信息传递的独立性假设,使相关信息在两类节点之间传递,影响码字的迭代收敛过程。上述消除 4 环的研究成果已经非常丰富,但是也有特例存在,Heng Tang 给出了存在 4 环且性能优良的有限几何 LDPC 码,定性地说明了产生的结果与多种因素有关,具体还不明确之间存在的关系。小 girth 对低码率、长度较短(10^3以下)的码影响较大,消除这类码的短环或减少其分布可以带来明显的性能改善,但是一味地增大 girth 并不能一直提高码字的性能。2007 年,电子科技大学的敬龙江提出了一大类基于图形理论的无小环高度结构化的 QC LDPC 码构造方法,该方法通过设计一个有几类特殊路径的连接图,来保证由此连接图映射而得的校验矩阵对应的 Tanner 图无小环。2009 年,Xueqin Jiang 和 Moon Ho Lee 提出了基于欧氏几何两个不同维超平面的大 girth 多进制 LDPC 码构造方法,同年,也提出了基于中国剩余定理的大 girth

二进制 QC LDPC 码构造方法。2010 年,Morteza Esmaeili 分别提出了采用两配置之积 girth 为 8 和基于两个循环置矩阵的斜率和斜率矩阵 girth 为 18 的二进制 QC LDPC 的构造[14]。

3 编码设计

虽然 LDPC 码的校验矩阵是非常稀疏的,但是其对应的生成矩阵却并不稀疏,这使得 LDPC 码面临着一个主要瓶颈——较高的编码复杂度和编码时延。目前,大部分编码算法主要是集中在二进制 LDPC 码上,专门针对多进制 LDPC 码编码方面的研究相对较少,对于多进制 LDPC 码编码来说,主要思想与二进制 LDPC 码相同,只是数域和运算规则有所不同。一般来说,设计 LDPC 码编码器存在以下 4 种方法。

(1)传统的直接编码方法

一种直接编码方法是从生成矩阵出发,将信息位与生成矩阵相乘得到发送的码字,其编码的复杂度与 LDPC 码码长的二次方成正比,而且直接编码产生的生成矩阵过于稠密,存储需要大量的空间;另一种是从校验矩阵的角度出发,采用高斯消去法(加减消元法)将校验矩阵变为下三角矩阵,进而采用递推的方式获得校验位。这两种直接方法从复杂度、时延和存储量角度来看,完全不利于工程实现。

(2)Richardson – Urbanke(RU)方法

2001 年,由 Richardson 和 Urbanke 提出的基于近似下三角矩阵的编码复杂度接近线性[15],其基本思想是利用 LDPC 码校验矩阵的稀疏性去减小产生稠密矩阵逆矩阵的尺寸,很大程度上减轻了在编码上巨大运算量和存储量需求。RU 方法从校验矩阵出发,只进行行列置换,不破坏校验矩阵的结构,同时避开了采用非稀疏的生成矩阵对 LDPC 码进行编码,充分利用了校验矩阵稀疏的特点,是 LDPC 码一种通用的编码方式,可应用于任何 LDPC 码。整体计算复杂度从 $O(n^2)$降低到了 $O(n+g^2)$,其中 g 为校验矩阵与近似下三角矩阵之间的"距离"。然而,RU 方法的缺点也是比较明显的。首先,RU 方法的流水线安排不合理[16],每一级流水线复杂度不同会导致消耗的时钟数相差比较大,降低了硬件资源的利用效率。其次,后向递推方法在解决了下三角非稀疏矩阵与向量乘法的同时,也引入了串行的计算结构,使得目标向量中下一个分量的求解依赖于该向量之前求得的所有分量,因此后向递推必须逐符号串行进行,大大限制了吞吐量的提升。最后,在 ϕ^{-1}没有被强制设计为某些特殊简单矩阵的情况下,它与向量的乘法没有办法做任何简化,这使 RU 算法在支持自适应编码时显得力不从心。综上所述,RU 算法只适合应用在码长不太长、吞吐量要求不太高、不要求自适应编码的场合。RU 方法只要求矩阵为非奇异稀疏矩阵,这一宽松的条件使其具有普适性,但同时也导致了该方法不会"随机应变",对一些特殊结构的校验矩阵不会加以利用,可能会通过行列置换将其打乱。引入一些特殊矩阵结构可改进 RU 方法,得到更为实用的编码算法,复杂度可达到完全线性化程度,这种改进与下述构造特定的校验矩阵实现线性化编码的方法有交叉之处。2005 年,Seho Myung 提出了一种二进制 QC LDPC 码的快速编码方法,其校验矩阵具有 QC 形式,而且 RU 算法中的 ϕ 取的是单位阵,将计算校验位的复杂度降至线性。2007 年,Sung – Eun Park 在 Seho Myung 的基础上提出了多进制 QC LDPC 码的有效编码方法,其只是将 ϕ 设计为 GF(q)域下的单位阵,无需计算 ϕ^{-1}。2009 年,陈超、白宝明、王新梅提出了基于 RU 算法线性复杂度的多进制 QC LDPC 码有效编码方法。RU 算法的改进是 LDPC 编码发展的一个分支方向,其编码的方法及复杂度与码的构造密切相关,比如块 LDPC 码,分层近似规则 LDPC 码等都是采用 RU 方法进行编码。

(3)构造特定代数结构的校验矩阵实现线性化编码

特定结构中一类最重要的结构是循环或准循环结构,具有循环或准循环结构的校验矩阵可以得到系统循环阵形式的生成矩阵,仅采用简单的移位寄存器就可以实现线性编码,是 QC LDPC 编码的一种有效实现方式。随着 QC 结构的流行,人们开始重新审视基于生成矩阵的编码方法。此时的生成矩阵虽然仍是非稀疏矩阵,但是却赋予了 QC 结构的特点,只需存储矩阵的第一行元素即可。这种 QC LDPC 码的有效编码方法是由 Zongwang Li 于 2006 年提出的[17],对于串行编码,复杂度与校验比特的位数成正比;对于高速的并行编码,复杂度与码字的长度成正比。同年,Lingqi Zeng 在其博士论文中将上述二进制编码方法扩展到多进制,实现了多进制 QC LDPC 码的高效编码。基于 QC 结构的编码算法从系统型生成矩阵出发,计算步骤比从校验矩阵角度

出发的 RU 算法显得简单明了。这种编码方式可以根据实际需求控制吞吐量的大小,从串行结构到并行乃至全并行结构。由于通用的循环移位寄存器结构可以为不同的 LDPC 码所共用,因此很容易就能实现可变码长、可变码率的自适应 LDPC 码编码。其不足之处在于,提升吞吐量所需要的代价是增加寄存器数量,两者几乎是呈线性关系的,难以满足在有限资源下追求最大吞吐量的设计要求。除了重要的 QC 结构,下面对其他一些用于有效编码的典型校验矩阵构造方法简要地给予介绍。2003 年,Jin Lu 提出了列重为 2 的 LDPC 循环码的线性编码方法。同年,Sarah Johnson 提出了一种采用循环码编码方式的准规则 LDPC 码构造方法。2006 年,Zhiyong He 设计了一种具有下三角加双对角线形式的校验矩阵来实现线性递推的编码方式。2009 年,Norifumi Kamiya 提出了与循环最大距离可分码相关的有效系统编码方法[18],这种编码方式的实现主要采用的循环码的多项式乘除法电路。总之,基于特定结构校验矩阵的 LDPC 码编码,一类方法是从校验矩阵的角度切入,采用递推等方式得到校验位;一类方法则是从生成矩阵或生成多项式的角度切入,采用反馈移位寄存器或多项式乘除法电路实现。

(4)基于迭代译码的编码方法

基于迭代译码的编码方法的主要原理是,把编码过程看成是一个编码后码字经过二进制删余信道(Binary Erasure Channel,BEC)后的置信传播译码的恢复过程。具体来说,可认为编码后码字经过 BEC 后,所有信息位均得到保留,所有校验位均被删除,可以采用信度传播译码算法来恢复未知的校验位。这种迭代译码方式简单,主要是由于变量节点和校验节点之间传递的信息只有两种:要么知道(概率为 1)要么不知道(概率为 0.5)。这种方法属于校验矩阵的编码方式,不足之处在于不能保证迭代编码能够成功得到码字,如果所有校验位的节点组成的子集中存在停止集,迭代编码很容易陷入其中。2002 年,David Haley 受译码方式的影响,提出了 LDPC 码的迭代编码方法,在有限的迭代次数下,采用 Jacobi 方法实现低复杂度编码,而且可以与译码共用同一电路结构。2007 年,Mohamed Shaqfeh 和 Norbert Goertz 提出了一种基于迭代译码的改进编码算法,这种算法对校验矩阵删除相关行并添加很少的新行,以使得迭代算法不会陷入到停止集中,这种编码复杂度是近似线性的,因为引入的新行是非稀疏的。目前,该类 LDPC 码编码方法只应用于二进制,多进制上还未有发展。

从上述编码方法来看,通用的方法适用范围广,可用于所有的 LDPC 码编码,与码的具体构造基本上没有关系,其复杂度较高;而校验矩阵具有特定结构的 LDPC 码则会充分利用其结构特性,把编码过程的复杂度尽量降至最低,但是其可扩展性不强。

4　译码算法

衡量 LDPC 码译码方法的指标主要有:误码性能、计算复杂度、译码延迟、存储容量,其中误码性能和计算复杂度是衡量的两个最重要指标。根据实际需求的不同会有不同的 LDPC 码迭代方法,但是基本原理是相通的:在表示 Tanner 图中的变量(符号或比特)节点和校验节点之间反复交换和更新信息。如图 1 所示,无论是二进制,还是多进制,对于 LDPC 码的译码方法,大体可分为 4 类:软判决译码,该算法主要是处理接收到的符号软信息,直接利用信道输出的信息进行迭代译码;硬判决译码,该算法是处理接收到的符号硬判决信息,译码端处理的接收符号集合与发送符号集合相同,都为 GF(q)($q\geqslant 2$)域中的元素,不需要信道的先验信息;基于可靠性度量的译码,该算法是处理接收到符号的硬判决值,而且还要利用未作硬判决的软信息作为可靠性度量,其目的是在少量增加硬判决算法的复杂度的前提下来提高纠错性能,是软判决和硬判决译码的折衷;混合译码,采用上述 3 类算法中的两种及两种以上组合而成的译码算法,目的是为了在误码性能和计算复杂度上找到不同的权衡点。

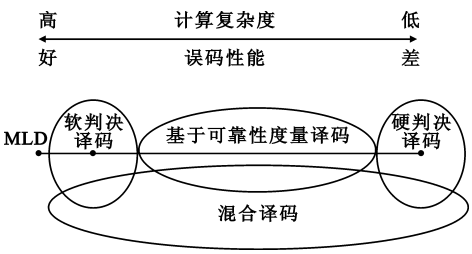

图 1　LDPC 码的译码方法的分类

Fig. 1 Classification of decoding algorithms for LDPC codes

译码的任务是在已知接收码字的条件下找出可能性最大的发送码字作为译码码字。最大似然译码(Maximum Likelihood Decoding,MLD)算法是在已知实际接收码字序列的条件下使先验概率最大的译码算法,该算法被认为是最好的译码方法,但对于 LDPC

码来说,由于码长较长,MLD 算法随码长呈现指数级增长导致复杂度极高而不利于实现。如图 1 所示,MLD 算法处于最高复杂度和最好性能的左端点上;软判决译码是一种次最优译码,复杂度偏高,虽取得的性能与 MLD 算法有一定差距,但却是可实现译码中性能最好的译码方法;硬判决译码主要是处理接收到码字的硬判决值,只需简单的实数运算和逻辑运算,以牺牲性能为代价而具有很低的复杂度,适合于信道条件较好的高速通信系统;而介于软、硬判决两者之间的便是基于可靠性度量的译码。为了不同的目的而产生了两种不同的思想,一个是从软判决算法向下简化,另一个是从硬判决向上优化,这两种思想形成了两种截然不同的发展方向,也提供了纠错性能和算法复杂度两者权衡的一系列满足于不同需求的算法;而混合译码算法实际上是一种组合算法,其目的和基于可靠性度量译码一样,而方式却完全不同,为了得到性能和复杂度的折衷而采用两种或两种以上的算法,获取两者的优势,削弱其劣势,是算法的一种扩展手段。

4.1 二进制 LDPC 码译码算法

二进制 LDPC 码可采用上述各种方式译码,第一个软判决译码算法——概率译码方法是 1962 年由 Gallager 提出来的[1],从本质上来说,与 1988 年 Pearl 给出的信度传播(Belief Propagation,BP)算法是一致的,只是两者问题切入角度和应用环境不同罢了,前者是在 LDPC 译码时充分利用了其他比特的相关性得到最佳后验概率,后者是在人工智能领域用于 Bayesian 网络的消息传递。在 Mackay、Neal、McEliece、Frey 和 Kschischang 等人将信度传播算法引入到 Turbo 码和 LDPC 码之前,广泛应用于人工智能领域的信度传播算法是不为信息理论学家所熟知的,其中 Kschischang 证明了在因子图上概率 BP 算法或消息传递(Message Passing,MP)算法是和积算法(Sum - Product Algorithm,SPA)的特例,而这 3 个概念在 LDPC 码译码中是等同的。由于概率 BP 算法计算复杂,需耗费较多运算时间和硬件资源,表达形式也不够简洁,采用对数似然比(Log - Likelihood Ratio,LLR)后得到的 LLR BP 算法误码性能不变,但具有更低的复杂度。从 LLR BP 角度出发,多数研究学者都致力于降低复杂度而形成从 LLR BP 向下简化的软判决算法。在 LLR BP 的简化上,Fossorier 做了大量且系统的工作,1999 年,Fossorier 提出了比特节点简化处理的 APP 译码算法、校验节点简化处理的 BP - Based 译码算法、比特节点和校验节点同时简化的 APP - Based 译码算法,这类算法有属于软判决译码的简化算法,也有属于基于可靠性度量的译码算法,但都是从 LLR BP 信息的近似处理着手取得性能和复杂度的权衡,其中 BP - Based 软判决译码算法与 Wiberg 提出的最小和算法(Min - Sum Algorithm,MSA)是同一概念。2002 年,Fossorier 研究小组中的 Jinghu Chen 提出了 Normalized BP - Based(或记为 NMS,Normalized Min - Sum)算法和 Offset BP - Based(或记为 OMS,Offset Min - Sum)算法,在原有 BP - Based 译码算法的基础上引入了校正因子和偏移因子,这两种修正的译码算法以少量复杂度的增加取得了接近 BP 译码算法的性能,而两个因子参数的选取既可以通过数值仿真手段获得,也可以通过理论推导得出。总的来说,Fossorier 的贡献主要是对 LLR BP 算法的简化,其在校验节点、变量节点或两者的计算上做简化近似或修正处理形成了一系列低复杂度的软判决译码算法和基于可靠性度量的译码算法。译码算法的节点消息更新策略也是译码中的研究热点之一,采用串行的方式可以比并行的方式获得更好的性能,其主要思想是改变了变量节点和校验节点之间全并行的消息传递方式,采用本次迭代中已更新的节点消息及时代替前次迭代中的节点消息参与本次更新。

第一个二进制 LDPC 码硬判决译码算法也是由 Gallager 于 1962 年提出[1]并命名为比特翻转(Bit - Flipping,BF)译码算法,这种硬判决译码算法之后被 Yu Kou 进行了改进,于 2001 年提出了加权比特翻转译码(Weighted Bit - Flipping,WBF)算法[6],该算法加入了比特度量信息,但却仍保持了 BF 译码算法低复杂度的优势,属基于可靠性度量译码。之后,许多通信学者对 WBF 算法的误码率性能和计算复杂度加以改进。2002 年,Ahmed Nouh 提出了 LDPC 码的引导加权比特翻转(Bootstrap WBF,BWBF)译码算法,在引导部分首先通过预设阈值来划分可靠比特和不可靠比特,通过来自可靠比特的可靠校验方程的信度传播来重新对不可靠比特进行赋值,之后采用 WBF 算法处理信息,属混合译码算法,该算法在性能和复杂度上都取得了提升。2004 年,Juntan Zhang 提出了修正的加权比特翻转(Modified WBF,MWBF)算法,该算法在 WBF 的基础上同时考虑了伴随式的信息和每一比特自身包含的信息。F. Guo 和 L. Hanzo 提出了基于可靠率的加权比特翻转(Re-

liability Ratio based WBF, RRWBF)算法,其翻转函数不需要任何的离线处理。次年,Ming Jiang 提出了改进的修正加权比特翻转(Improved MWBF, IMWBF)算法。2005 年,Zhenyu Liu 提出了有限几何码的一种译码算法,在该算法中定义了一种新的翻转函数,其比特选取准则综合考虑了不满足校验方程的个数和接收比特的可靠性度量,并首次提出了环路检测和规避方法,记为 LP – WBF。2006 年,Inaba 和 Ohtsuki 提出的引导的修正加权比特翻转(Bootstrap MWBF, BMWBF)算法不仅具有低的译码复杂度,而且其性能都优于 WBF、MWBF 和 BWBF 算法。2007 年,吴晓富提出了并行加权比特翻转(Parallel WBF, PWBF)算法,在不损失性能的情况下加快了收敛速度。2009 年,吴晓富给出了不同 WBF 算法和 BP 算法的对偶映射关系,建立了基于可靠性度量译码算法和软判决译码算法之间的桥梁[19]。李广文、酆广增提出了改进的并行加权比特翻转算法(Improved PWBF, IPWBF),算法中融入了延迟处理方法,将比特按照可靠性度量分为延迟处理集合和非延迟处理集合,在延迟处理集合中,只有比特辅助计数器达到某一预设阈值,才进行翻转;而在非延迟集合中,则不需延迟直接翻转。另一种经典的二进制 LDPC 码硬判决译码算法是一步大数逻辑译码(One – Step Majority – Logic – Decoding, OSMLD)。2009 年,Shu Lin 课题研究小组的 Qin Huang 提出了基于软可靠性度量和硬可靠性度量的两种迭代大数逻辑译码算法,只需要低复杂度的逻辑运算和整数加法,其思路是从大数逻辑译码算法演变为基于可靠性度量的译码算法。

综上所述,1962 年 Gallager 给出了两个译码算法发展的根节点——软判决译码算法和硬判决译码算法。此后,Fossorier 研究小组在软译码算法 SPA 上做了大量的简化工作以及向下延拓了得到一些基于可靠性译码的算法;而 Kou 则开启了硬判决译码向基于可靠性译码算法发展的道路,引出了吴晓富、李广文、Zhenyu Liu 和 Ngatched 等人为代表在 WBF 算法所出的成果。如图 1 所示,二进制 LDPC 码的译码在各方面得到了全局性的发展,可以适用于不同通信系统 LDPC 码译码器的需求。

4.2　多进制 LDPC 码译码算法

而多进制 LDPC 码译码器的发展不像二进制 LDPC 码发展那样均衡,对于多进制 LDPC 译码算法目前还处于发展研究阶段,基本集中在软判决译码算法方向。1998 年,Davey 和 Mackay 在二进制 SPA 译码的基础上提出了基于 GF(q)($q>2$)域的多进制 LDPC 码译码算法——QSPA,被称为多进制经典译码算法,仿真表明相比于二进制 LDPC 码,Mackay 法构造的列重不大于 3 的多进制 LDPC 码可以在二进制对称信道(Binary Symmetric Channel, BSC)和二进制高斯信道上取得更好的性能,这种算法导致校验节点的计算复杂度为 $O(q^2)$,正是由于这种高复杂度制约了多进制 LDPC 码的发展,因此如何降低译码复杂度成为多进制 LDPC 码发展的大势所趋。在软判决译码中,为减少其译码复杂度,对 QSPA 的简化主要从两个分支上来进行研究:一是频域,二是对数似然比(Log – Likelihood Ratio, LLR)域。在频域中,2000 年,Mackay 提出了在 GF(q)域上采用快速傅里叶变换(Fast Fourier Transform, FFT)的多进制译码算法 FFT – QSPA,该算法通过 FFT 转换到频域,从而使在校验节点的卷积运算变成乘法运算,将计算的复杂度降低为 $O(q\ \mathrm{lb}q)$,但是在 FFT 和归一化时仍需要大量的实数乘法和除法运算。2003 年,Barnault 和 Declercq 采用张量表示法给出了快速译码算法 FFT – QSPA 的实现步骤[20]。同年,Hongxin Song 对 FFT – QSPA 中变量节点和校验节点的概率取对数,变乘法运算为加法运算,提出了 Log – FFT – QSPA 译码算法,这种算法结合了傅里叶变换和对数计算的优势,但其需要大量的对数和指数运算,不利于实用化,为了克服这个问题,可将对数和指数运算采用查找表(Look – Up Table, LUT)方式进行,但 LUT 的数量会随着伽罗华域值以 $q\ \mathrm{lb}q$ 的速度增长,只适合于伽罗华域元素较少的情况,同时 LUT 的近似也会带来误码性能的损失。在 LLR 域中,2004 年,Henk Wymeersch 在二进制 MS 译码算法的基础上,提出了采用对数似然比的多进制 LLR – QSPA,具有实现容易、复杂度低和数值稳定等特点,乘法和加法运算被加法和 Jacobi 对数运算所取代,但其复杂度仍为 $O(q^2)$。2007 年,David Declercq 提出了扩展最小和(Extended Min – Sum, EMS)算法[21],为减少迭代中的复杂运算,采用 LLR 域的对数似然比值作为传递的消息,在信度传播校验节点上只选取一部分($n_m \ll q$)有用值来计算度量值,算法具有与 FFT – QSPA 近似的复杂度 $O(n_m q)$,而且只有实数加法运算,没有乘法和除法运算,复杂度大大降低,但是相对于 QSPA 译码而言,误码性能有一定的损失。受二进制 BP – Based 和 APP – Based 译码算法思想的启发,加

入校正因子和偏移因子给出了相应的修正算法。之后 David Declercq 在 EMS 算法的基础上,将上述原理同时应用于校验节点和变量节点,提出了低复杂度、低存储容量的 EMS 算法,具有 $O(n_m \text{ lb } n_m)$ 的复杂度。2008 年,北京邮电大学的周伟、全子一等人在 FFT – QSPA 基础上,提出了减小振荡的改进算法,使每个发生振荡的变量节点处输出的信息包含上次信息和当前迭代后得到的信息。同年,陈昕、全子一等人提出了部分更新策略的低复杂度译码算法,对高可靠性的变量节点停止更新,并利用高可靠性信息进行更新的同时防止低可靠性变量节点错误信息的传递。

多进制硬判决译码算法 2010 年才出现,其发展思路延续了二进制 LDPC 码硬判决译码的思路。西安电子科技大学陈超、白宝明、王新梅等人提出了多进制广义比特翻转(Generalized Bit Flipping, GBF)算法和修正的 GBF(Modified GBF, MGBF)算法[22],两种算法的每一个符号都有一个整数度量值,不同于 QSPA 中传播的实数概率值,每次迭代中对可靠的符号度量加 1,最后做大数判决(或多数投票)来确定译码符号。GBF 和 MGBF 算法的区别在于前者初始化条件直接采用了硬判决信息,而后者利用了信道软信息值,算法都只需要有限域运算、整数加法和整数比较,属基于可靠性度量的译码算法,其不足在于只针对校验矩阵列重较大的情况。同年底,中山大学赵大源、马啸提出了大数逻辑可译多进制 LDPC 码的低复杂度译码算法[23],该算法的译码过程与文献[22]提出算法一致,不同之处在于初始化选取,其采用星座图上的欧氏距离作为初始化度量值,算法的不足之处在于只适用于大数逻辑可译码。Shu Lin 课题研究小组的 Chao – Yu Chen 提出了多进制 LDPC 码基于软可靠性度量和硬可靠性度量的译码算法[24],两种算法不同之处在于初始化信息不同,不足之处在于只适用于二进制相移键控(Binary Phase Shift Keying, BPSK)调制,不适用于高阶调制,算法对列重很大的规则校验矩阵更为有效。

5 结束语

本文综述了 LDPC 码在构造、编码和译码三方面的研究情况。在构造方面,主要存在随机化和结构化两种构造方法,目前的研究主要集中于结合代数或几何方法的结构化构造方法;在编码方面,考虑到编码的复杂度,研究多集中于基于特定 LDPC 码结构的线性化编码;在译码方面,衍生出了软判决、硬判决、基于可靠性度量和混合的 4 类主要算法,为减小译码复杂度,目前多在基于可靠性度量和混合算法上进行研究。LDPC 码作为一种先进的编译码技术,是现代通信领域的研究热点,虽然经历了十几年的发展历程,但仍有很多技术有待研究,特别是多进制 LDPC 码还处在发展研究阶段,有更多的未知领域亟待探索。随着 LDPC 码的研究不断深入下去,将为数据传输质量的提高提供可靠保证。

参考文献:

[1] Gallager R G. Low – density parity – check codes[J]. IRE Transactions on Information Theory, 1962, 8(1): 21 – 28.

[2] MacKay D J C. Good error – correcting codes based on very sparse matrices[J]. IEEE Transactions on Information Theory, 1999, 45(2): 399 – 431.

[3] Chung S, Jr Forney G D, Richardson T J, et al. On the design of low – density parity – check codes within 0.0045 dB of the Shannon limit[J]. IEEE Communications Letters, 2001, 5(2): 58 – 60.

[4] Bonello N, Chen S, Hanzo L. Low – density parity – check codes and their rateless relatives[J]. IEEE Communications Surveys & Tutorials, 2011, 13(1): 3 – 26.

[5] Hu X, Eleftheriou E, Arnold D M. Regular and irregular progressive edge – growth tanner graphs[J]. IEEE Transactions on Information Theory, 2005, 51(1): 386 – 398.

[6] Kou Y, Lin S, Fossorier M P C. Low – density parity – check codes based on finite geometries: A rediscovery and new results[J]. IEEE Transactions on Information Theory, 2001, 47(7): 2711 – 2736.

[7] Falsafain H, Esmaeili M. A new construction of structured binary regular LDPC codes based on Steiner systems with parameter t > 2[J]. IEEE Transactions on Communications, 2012, 60(1): 74 – 80.

[8] Lan L, Zeng L, Tai Y Y, et al. Construction of quasi – cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach[J]. IEEE Transactions on Information Theory, 2007, 53(7): 2429 – 2458.

[9] Zhang L, Huang Q, Lin S, et al. Quasi – cyclic LDPC codes: An algebraic construction, rank analysis, and codes on Latin squares[J]. IEEE Transactions on Communications, 2010, 58(11): 3126 – 3139.

[10] Zeng L, Lan L, Tai Y Y, et al. Constructions of nonbinary quasi – cyclic LDPC codes: A finite field approach[J]. IEEE Transactions on Communications, 2008, 56(4): 545 – 554.

[11] Zeng L, Lan L, Tai Y Y, et al. Construction of nonbinary cyclic, quasi – cyclic and regular LDPC codes: a finite geom-

etry approach[J]. IEEE Transactions on Communications, 2008,56(3):378 – 387.

[12] Kang J, Huang Q, Zhang L, et al. Quasi – cyclic LDPC codes: An algebraic construction[J]. IEEE Transactions on Communications, 2010, 58(5): 1383 – 1396.

[13] Chen C, Bai B, Wang X. Construction of nonbinary quasi – cyclic LDPC cycle codes based on singer perfect difference set [J]. IEEE Communications Letters, 2010, 14(2): 181 – 183.

[14] Esmaeili M, Gholami M. Structured quasi – cyclic LDPC codes with girth 18 and column – weight J≥3[J]. International Journal of Electronics and Communications, 2010, 64 (3): 202 – 217.

[15] Richardson T J, Urbanke R L. Efficient encoding of low – density parity – check codes[J]. IEEE Transactions on Information Theory, 2001, 47(2): 638 – 656.

[16] Zhang H, Zhu J, Shi H, et al. Layered approx – regular LDPC: code construction and encoder/decoder design [J]. IEEE Transactions on Circuits and Systems I, 2008, 55(2): 572 – 585.

[17] Li Z, Chen L, Zeng L, et al. Efficient encoding of quasi – cyclic low – density parity – check codes[J]. IEEE Transactions on Communications, 2006, 54(1): 71 – 81.

[18] Kamiya N, Sasaki E. Efficient encoding of QC – LDPC codes related to cyclic MDS codes[J]. IEEE Journal on Selected Areas in Communications, 2009, 27(6): 846 – 854.

[19] Wu X, Ling C, Jiang M, et al. New insights into weighted bit – flipping decoding[J]. IEEE Transactions on Communications, 2009, 57(8): 2177 – 2180.

[20] Barnault L, Declercq D. Fast decoding algorithm for LDPC over GF(2^q)[C]//Proceedings of IEEE Information Theory Workshop. Paris, France: IEEE, 2003: 70 – 73.

[21] Declercq D, Fossorier M. Decoding algorithms for nonbinary LDPC codes over GF(q)[J]. IEEE Transactions on Communications, 2007, 55(4): 633 – 643.

[22] Chen C, Bai B, Wang X, et al. Nonbinary LDPC codes constructed based on a cyclic MDS code and a low – complexity nonbinary message – passing decoding algorithm[J]. IEEE Communications Letters, 2010, 14(3): 239 – 241.

[23] Zhao D, Ma X, Chen C, et al. A low complexity decoding algorithm for majority – logic decodable nonbinary LDPC codes[J]. IEEE Communications Letters, 2010, 14(11): 1062 – 1064.

[24] Chen C, Huang Q, Chao C, et al. Two low – complexity reliability – based message – passing algorithms for decoding non – binary LDPC codes[J]. IEEE Transactions on Communications, 2010, 58(11): 3140 – 3147.

作者简介:

张用宇(1977—),男,湖北武汉人,分别于 1999 年和 2002 年获海军工程大学通信工程专业学士学位和硕士学位,现为工程师,主要研究方向为无线通信系统;

ZHANG Yong-yu was born in Wuhan, Hubei Province, in 1977. He received the B.S. degree and the M.S. degree from Naval University of Engineering in 1999 and 2002, respectively. He is now an engineer. His research concerns wireless communication systems.

Email: zhang_yong_yu@yahoo.com.cn

吴东伟(1981—),男,河南项城人,分别于 2004 年和 2007 年获西北工业大学通信工程专业学士学位和硕士学位,现为工程师,主要研究方向为无线通信系统;

WU Dong-wei was born in Xiangcheng, Henan Province, in 1981. He received the B.S. degree and the M.S. degrees from Northwestern Polytechnical University in 2004 and 2007, respectively. He is now an engineer. His research concerns wireless communication systems.

Email: wuqqq111@hotmail.com.cn

左丽芬(1980—),女,湖北大冶人,分别于 2002 年和 2005 年获装备指挥技术学院通信工程专业学士学位和硕士学位,现为工程师,主要研究方向为通信工程和无线通信系统;

ZUO Li-fen was born in Daye, Hubei Province, in 1980. She received the B.S. degree and the M.S. degree from the Academy of Equipment Command & Technology in 2002 and 2005, respectively. She is now an engineer. Her research interests include communication engineering and wireless communication systems.

Email: xmeimeim@163.com

刘　冰(1984—),男,江西南昌人,2011 年于海军工程大学获通信工程专业博士学位,现为工程师,主要研究方向为差错控制编码和数字通信信号处理。

LIU Bing was born in Nanchang, Jiangxi Province, in 1984. He received the Ph. D. degree from Naval University of Engineering in 2011. He is now an engineer. His research interests include error control coding and signal processing for digital communications.

Email: liubing5275093@hotmail.com