LDPC 码的原理与介绍

LDPC 码简介

LDPC码是一种线性分组码，它于1962年由Gallager提出，之后很长一段时间没有收到人们的重视。直到1993年Berrou等提出了turbo码，人们发现turbo码从某种角度上说也是一种LDPC码，近几年人们重新认识到LDPC码所具有的优越性能和巨大的实用价值。1996年MacKay和Neal的研究表明.采用LDPC长码可以达到turbo码的性能，而最近的研究表明，被优化了的非规则LDPC码采用可信传播(Belief Propagation)译码算法时，能得到比turbo码更好的性能。目前，LDPC码被认为是迄今为止性能最好的码。LDPC码是当今信道编码领域的最令人瞩目的研究热点，近几年国际上对LDPC码的理论研究以及工程应用和VLSI(超大规模集成电路)实现方面的研究都已取得重要进展。基于LDPC码的上述优异性能可广泛应用于光通信、卫星通信、深空通信、第四代移动通信系统、高速与甚高速率数字用户线、光和磁记录系统等。

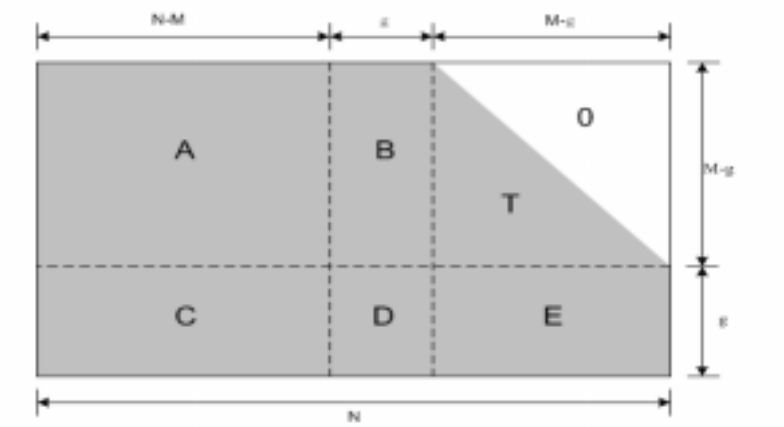
LDPC码可以用非常稀疏的校验矩阵或二分图来描述，也就是说LDPC码的校验矩阵的矩阵元除一小部分不为0外，其它绝大多数都为0。通常我们说一个(n,j,k) LDPC码是指其码长为n，其奇偶校验矩阵每列包含j个1，其它元素为0；每行包含k个1，其它元素为0。j和k都远远小于n，以满足校验矩阵的低密度特性。校验矩阵中列和行的个数即j和k为固定值的LDPC码称为规则码，否则称为非规则码。一般来说非规则的性能优于规则码。

LDPC 码的编码方法

LDPC 码所面临的一个主要问题是其较高的编码复杂度和编码时延。对其采用普通的编码方法，LDPC 码具有二次方的编码复杂度，在码长较长时这是难以接受的，幸运的是校验矩阵稀疏性使得 LDPC 码的编码成为可能。目前，好的编码方法一般有如下几种情况：１、T.J.Richardson 和 R.L.Urbanke 给出了利用校验矩阵的稀疏性对校验矩阵进行一定的预处理后，再进行编码。２、设计 LDPC 码时，同时考虑编码的有效性，使Ｈ矩阵具有半随机矩阵的格式。３、H 矩阵具有某种不变特性所采用的其他编码方法，例如基于删除译码算法提出的编码方案。这几种编码方案都是在线性时间内编码的有效算法，初步解决了 LDPC 码的应用所面临的一个主要问题。下面对这几种编码方案作一些简单的说明。

Ｒichardson 等提出的有效编码方案

LDPC 码的直接编码方法就是利用高斯消去法，产生一个下三角矩阵，然后进一步初等变换得到右边单位阵形式 H=[P|I]，由 G＝[I|P’]得到生成矩阵，从而由 C=M*G 直接编码。这样的编码方法是复杂的，主要原因是由于高斯消去法破坏了原有奇偶校验矩阵的稀疏性。为了保持矩阵的稀疏性，Richardson 提出了有效编码方案，首先可以对矩阵的列做重排，这样虽然不能得到一个完全的下三角形式的矩阵，但可以获得一个近似的下三角矩阵。如图所示，分成六个分块的稀疏矩阵,其中 g 是一个相当小的数。如下图所示，



对于要发送的信息序列，依然直接作为 LDPC 码字的前 N-M 个信息位比特输出，对于其生成的校验比特，将其分成两块[p1,p2]，v=[u,p1,p2],根据 $H \cdot v^T = 0$，,我们将得到以下的两个关系式

$$Au^T + Bp_1^T + Tp_2^T = 0 \qquad (1)$$

$$Cu^T + Dp_1^T + Ep_2^T = 0 \qquad (2)$$

由（1）式乘以 $-ET^{-1}$ 再加上（2）式，我们可以得到式（3）如下：

$$(-ET^{-1}A + C)u^T + (-ET^{-1}B + D)p_1^T = 0 \qquad (3)$$

通过（3）式求出 p1,代入（1）式，就可以得到 p2, 从而完成编码过程。

编码复杂度的分析，因为这六个分块阵是通过对原有稀疏矩阵的列做重排获得的，所以这些分块阵依然满足稀疏性，我们可以进一步分析出求解 P1 和 P2 的运算量分别为 $o(N+g^2)$ 和 $o(N)$。由此可以看出，当 g 尽量小的时候，LDPC 码的编码运算量，就可以控制在线性复杂度附近。

在特殊情况下，设计码字时，考虑令 $\Phi = -ET^{-1}B + D$,当其为Ⅰ阵时，又可以进一步降低编码的复杂度，此时编码步骤可以参考如下：

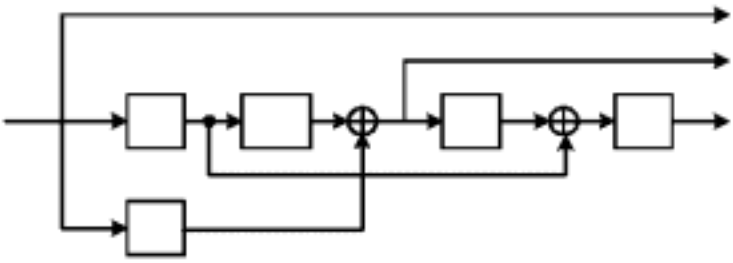
步骤 1）计算 Au^T 和 Cu^T ,

步骤 2）计算 $ET^{-1}(Au^T)$

步骤 3）计算 $p_1^T = ET^{-1}(Au^T) + Cu^T$

步骤 4）计算 p_2^T ,根据 $Tp_2^T = Au^T + Bp_1^T$

编码结构图如下所示：



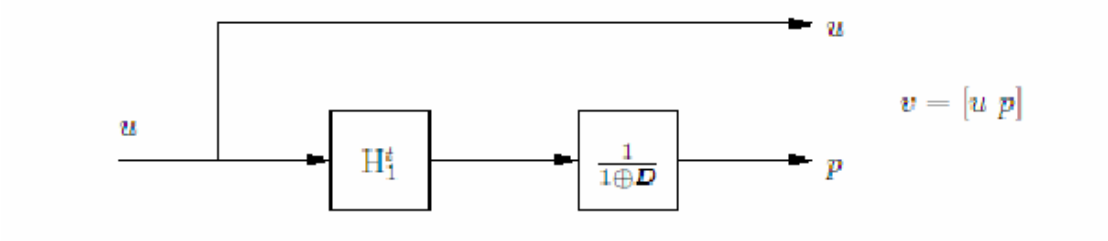
构造半随机校验矩阵 H

定义校验矩阵 H=[H_1 H_2]，H1 是 k*(n-k)， H_2 是(n-k)*(n-k)；设计码字时，令 H_2 矩阵具有如下的形式：

$$H_2 = \begin{bmatrix} 1 & 1 & 0 & \ddots & 0 \\ 0 & 1 & 1 & 0 & \vdots \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}$$

将生成的码字 v 分成两部分[u,p]，u 代表信息比特，p 代表生成的校验比特。考虑 G=[I,P]，由 $GH^T = 0$，可以得到 $IH_1^T + PH_2^T = 0$,所以 $P = H_1^T H_2^{-T}$，根据 H_2 的特性可知， H_2^{-T} 可以由一个特征多项式为 $f(D) = 1/(1+D)$ 的递归卷积码来表示。

此时编码结构如下图所示：



这种编码算法的缺点在于，H2 矩阵存在列重为 1 的列，这对迭代译码过程不利，会产生误码平台，可以通过改变这一列重的方法来优化，降低误码平台。

其它编码方案

1. 基于删除信道 LDPC 迭代译码算法的编码方法，这种方法的主要核心思想在于将信息比特看作码字通过 BEC 信道后，没有发生错误的比特，而校验比特看作错误码比特，这样可以利用迭代消息传播算法，准确的求出校验比特，从而完成编码结构。这种算法的缺点在于如果在译码过程中，遇到 stopping set，就会发生不能完全实现编码的结果，因此，这种算法只适用于一些特定的H矩阵，如有关文献中提到的有准循环特性的一类 LDPC 码。

2．根据H矩阵自身的特点所产生的一类编码算法，这部分的H矩阵主要还是以准循环矩阵为主，其具有准循环不变性，编码可以通过移位寄存器来实现。甚至通过有限几何设计的 LDPC（m,s）码,当 m=2 时，其码字本身就是一个循环码，可以利用生成多项式来实现编码。其编码复杂度是线性的复杂度。

编码方案小结

传统的 LDPC 码的编码复杂度比较复杂，与码长成平方的关系，大大不利用于 LDPC 码的推广，因此在设计码字的H矩阵时，不仅要考虑到码字的性能，同时要考虑到编译码的复杂度。

上述提到的几种编码结构或算法说明，通过对H矩阵的处理或者利用矩阵自身的一些特性，都可以把编码的复杂度降低到线性复杂度。比较以上几种编码方案，Richardson 提出的有效编码方法适用于一般的 H 的矩阵，通过对原始矩阵进行适当处理，实现编码。而其他的编码方案则是主要利用矩阵自身的特性，如循环不变性，半随机特性等有效地降低编码复杂度。同时从性能上考虑，具有大的最小距离的码字很多落在准循环码这个集合内，因此构造具有较大最小距离的准循环 LDPC 码未来研究 LDPC 码的热点之一。

LDPC 码的译码算法

LDPC 码有很多种译码方法，本质上大都是基于 Tanner 图的消息迭代译码算法。根据消息迭代过程中传送消息的不同形式，可以将 LDPC 的译码方法分为硬判决译码和软判决译码。如果在译码过程中传送的消息是比特值，称之为硬判决译码；如果在译码过程中传送的消息是与后验概率相关的消息，称之为软判决译码，有时也称为和积译码算法。硬判决译码计算比较简单，但性能稍差；软判决译码计算比较复杂，但性能较好。为了平衡性能和计算复杂度，可以将两者结合使用，称为混合译码算法。 根据消息迭代过程中传送的消息是否进行了量化及量化所使用的比特数，我们可以将译码方法分为无量化译码和量化译码。硬判决译码可以看成是 1 比特量化译码，软判决译码可以看成无穷多比特量化译码，而混合译码可以看成变比特量化译码。从量化译码的角度看，硬判决译码和软判决译码属于同一类译码方法，已有的研究表明，可以用 3 比特量化取得和和积译码算法非常接近的性能。目前主要的硬判译码算法有一步大数逻辑译码算法（MLG），Gallager 提出的比特翻转算法(BF)，加权的大数逻辑译码算法（WMLG），加权的比特翻转算法（WBF）以及一些对以上几种算法作改进的算法如 IWBF 等硬判译码算法；软译码算法主要有迭代结构的置信传播算法（BP）（有时也称之为和积算法（SPA)），以及基于标准 BP 算法，对信息进行部分处理，降低译码复杂度的译码算法，如 UMP BP-based 算法(min-sum 算法)，Normlized BP-based 算法，还有基于最优化理论的译码算法如线性规化算法（LP)。下面首先对译码算法作简单的介绍，然后从性能与译码复杂度两个角度分析比较各种译码算法。

译码算法简单描述

硬判译码算法

一步大数逻辑译码算法，主要原理是根据通过一系列的正交方程，比较校验结果 1 和 0 的数目来完成译码过程。这种译码算法译码结构简单，复杂度较低，但是应用场合有限，只

适用于某些码结构比较特殊的码字，如有限几何 LDPC 码。

基于 Tanner 图的信息传递的比特翻转算法，在每一次迭代过程，根据某一种准则，决定将其中的某一个比特进行翻转，直至迭代过程结束，或者校验方程全部满足。这种译码算法的核心在于确定比特翻转的准则，如 Gallager 最初提出的 BF 算法，准则是不满足校验方程个数最多的比特进行翻转，后来提出的加权算法主要是在翻转准则加入变量节点可靠性度量，改进算法主要是在检测翻转过程中防止出现翻转成环的现象，这些改进都进一步提高了性能，而没有增加复杂度。

软判译码算法

软判译码算法主要包含 BP 算法及其简化形式，LP 算法等。

BP 算法中消息的传递形式是对数似然比(LLR)，在迭代过程中，每次在变量结点和校验结点分别按照和规则与 tanh 规则更新节点的信息。直至译码结束或者校验方程全满足。BP 算法适用于各类信道，具有逼近香农限的优异性能，但校验节点的消息计算复杂度非常复杂，为了简化校验节点的消息计算，人们提出了很多简化算法，如 UMP（min-sum）译码算法就是一个有代表性的简化算法，另外为了保证性能上接近与 BP 算法，以提出了归一化的 BP 算法。各种译码简化译码算法的目的就是在计算复杂度、译码性能及译码时延等方面取得最优的折中。

线性规化算法（LP）是基于最优化理论提出的一种新的译码算法，主要思想是可以把译码问题看作一个整数优化问题，通过对约束条件的放缩，形成一个简单的线性规化问题，利用最优化理论的知识完成译码。这种译码算法的好处在于译码复杂度是线性的，性质便于分析，开拓了新的译码思路。

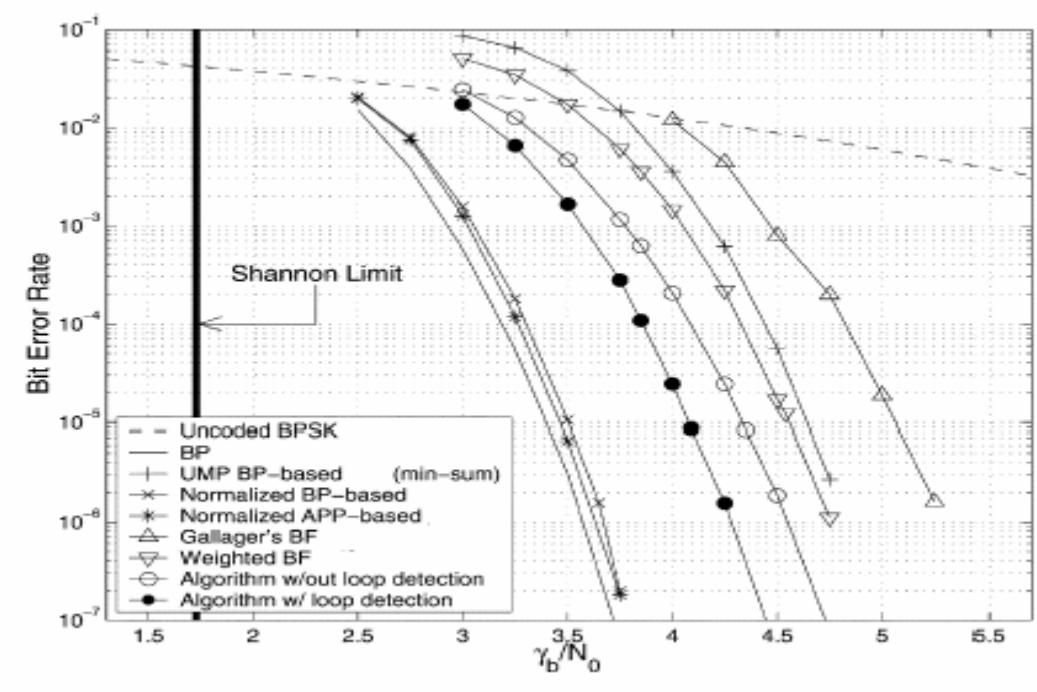
性能比较

从性能的角度来看，软译码算法普遍优于硬判译码算法。

在软译码算法中，标准 BP 算法的性能最好，Normlized BP-based 算法的性能与ＢP 算法相当接近，而 UMP BP-based 算法(min-sum 算法)的性能一般要比 BP 算法差１dB 左右。线性规化算法的性能与 min_sum 算法的性能比较接近。

在硬判译码算法中，一步大数逻辑译码算法不需要采用迭代结构，相对来说性能一般比较差，而比特翻转算法以及其加权、改进等多种形式算法的性能会随着加权、改进得到提高，但总的来说其性能还是不如软判译码算法。

下图是Ｔype-I 2-D(1023,781)EG_LDPC 码的在不同译码算法下性能曲线图：图中 Algorithm w/out loop dection 以及 algorithm w/loop dection 是WBF 的一种改进译码算法。



译码复杂度比较

在这里我们假定H矩阵的行重和列重分别为 w_r, w_c ，H矩阵行为N，列为M，则其中典型的几种译码算法，一次迭代译码的复杂度如下表所示

译码算法	乘法次数	除法次数	加法次数
标准 BP 算法	$11Nw_c - 6(N+M)$	$N(w_c+1)$	$N(3w_c+1)$
Normalized BP-based 算法	0	Nw_c	$4N(w_c-1)+N\log_2 2w_c/2$
UMP BP-based 算法	0	0	$4N(w_c-1)+N\log_2 2w_c/2$
WBF 算法	0	0	$N-1+w_c w_r$
IWBF 算法	0	0	$N-1+w_c w_r$
改进式WBF 算法	0	0	$N-1+w_c w_r$

在上表中，我们仅仅给出了几种典型译码算法的单次迭代译码复杂度，译码的复杂度还与迭代次数相关。通常针对不同的H矩阵，各种译码算法的迭代次数都不太一致，因此对于实际应用时，应该具体H矩阵具体分析。

译码方案小结

LDPC 码具有多种译码算法，性能较好的译码算法，复杂度越高，而复杂度较低的译码算法，其性能较差。LDPC 码译码算法的多样性，给我们提供了性能与复杂度折中的多种方案，让我们在不同的应用场合有更好的选择余地。

H 矩阵的构造方法

目前,稀疏奇偶校验矩阵的构造算法是研究LDPC 码的热点之一。LDPC码的构造算法主要包括两大类,一类是随机或伪随机结构的；另一类是代数结构的.

随机构造方法

随机构造方法主要包括以下四种:Gallager的最初方法，Maykay的随机方法，PEG算法，Bit-filling和Extended Bit-filling算法。前两种方法，都是根据行和列的列重，随机产生H矩阵，主要是针对规则LDPC码。而后两者可以产生不规则LDPC码。下面主要就后两种算法作简单介绍。

PEG算法（progressive edge-growth）是一种构造Tanner图的简单有效方法，主要是在某准则条件下通过加边的方式随机构造LDPC码。具体操作是在给定变量节点数目、校验节点数目和变量节点分布的条件下，逐步地在变量节点和校验节点的边，选择加边时，尽可能保持大的girth，然后接着放新边，直至结束。

Bit-filling算法和Extend Bit-fillingt算法，是一种直接构造H矩阵的方法，主要是在某准则条件下通过逐步在H矩阵添加列的方式。具体操作是给定行重和列重的满足条件以及最小girth目标，初始H矩阵为空，每次随机生成列，若满足前提条件，则加入到矩阵H中去，然后接着加列，直至矩阵H生成。Extend Bit-filling算法是对Bit-filling算法的一个补充，当在操作过程中，不存在满足条件的列时，可以减少girth，从而使得操作能够继续。

在上述算法中，设计LDPC码前，需要知道变量节点和校验节点的分布，一般是通过密度演化算法或者EXIT图、高斯近似等方法得到的。一般来说随机构造的LDPC码，由于随机性，编码一般来说较复杂，而且不利于硬件实现。

代数构造方法

对于规则LDPC 码的代数构造算法目前已有多种研究方案,其中具有理论研究价值的有如下几个有代表性的研究成果: (1) Lin.S等提出的利用组合数学的分支---有限几何来构造LDPC码,这类码的特点是高码率、长分组时性能很好,而低码率、短分组长度时性能恶化,另外码率和码长的设计不够灵活,不具备与现有标准的兼容性; (2)BVasic和BAmmar等利用组合数学的另一分支———均衡不完全分组设计(BIBD) 来构造LDPC 码,他们设计的相同之处是H 矩阵采用分块矩阵法,而分块矩阵由BIBD 方法构成. 不同之处有两点:一是对BIBD 的五个参数(b, v, k, r, λ)进行不同的设计,得到不同的关联矩阵族;二是由这些关联矩阵族构成H 矩阵的排列和组合方式不同. 这类码的特点是适合于高码率,中等长度码,码率的取值范围在0. 75 到0. 96 之间,码长在1000 到8000 之间取值,最好性能离香农限0.

95dB. 由于5 个参数都要取整数并且它们之间有配合关系,使这类码的码长和码率的设计灵性受到限制; (3) Gallager 在其博士论文中提出了一种准循环的代数结构,后来又被Tanner和Fossorier等进行了深入研究,目前这类码称为准循环QC-LDPC 码. 其基本思想是: H 矩阵由一组分块矩阵按一定的规则排列,这组分块矩阵由单位矩阵及其单位矩阵的一组循环移位矩阵组成. 二者的不同之处在于,分块矩阵在H 矩阵中的排列规则不同. 此外在Tanner的设计中,要求分块矩阵的维数n 是素数或素数的偶数倍,这种限制导致码长和码率的取值不灵活,码集合中码的数量较少. 在Fossorier 的设计中, n 的限制条件较宽,可以取素数和其它整数,但不能取2 的幂这一类整数.对n 取值的限制致使这两类QC-LDPC 码参数的选择不灵活,如不能设计码率为0.5 的码. QC-LDPC 码在中、短分组长度和中、低码率时,有较好的性能,如Tanner 的(3 ,5) QC-LDPC 码,最好性能达到2. 5dB 左右;而Fossorier 的(4 ,18) QC-LDPC 码,最好性能达到2. 2dB 左右.

上述代数结构规则LDPC 码类的共同缺陷是码率和码长的参数选择不够灵活,它们只能根据自身的设计规则首先构造H 矩阵,然后由H 矩阵求出码长和码率;而不能首先给定码率和码长的参数,然后根据这些参数设计H 矩阵,这导致上述构造算法所确定的LDPC 码类不能与现有标准兼容,实用性较差。

LDPC 码构造方法

LDPC 码的H矩阵设计不仅要考虑性能，编译码复杂度上的因素、还要考虑是否方便硬件实现，能否支持多速率变码长的情况。因此，设计H矩阵时，通常把随机方法与代数方法部分结合起来设计H矩阵，现在较为典型的一种 LDPC 码设计方法，就是设计块 LDPC 码（准循环码的一种），主要设计分为基矩阵和子矩阵两部分，子矩阵是一个循环子阵，行重列重都为 1。而基矩阵是可以通过计算机搜索方式来确定。这样设计出来的码字不仅具有结构上的不变性，在码长、码率方面也有较大的灵活性，性能上还保持着逼近香农限的特性。

如何结合随机方法与代数方法构造有效的 LDPC 码校验矩阵，将是未来构造 LDPC 码的研究重点。

LDPC 码小结

LDPC码是目前人们发现的纠错性能最好的一种码。为了说明这一问题，下面对LDPC码和turb。码进行了简要比较。简单的说，LDPC码比turbo码区别在于，LDPC码是一种线性分组码，采用BP迭代译码；而turbo码采用的是卷积码，译码方法主要有MAP类的算法和软输出Viterbi算法的迭代译码。LDPC码有理论极限性能优于turbo码，给定1/2码率条件下，采用BPSK调制的高斯信道中两种编码方法的纠错性能比较，LDPC码比turbo码更接近香农限，目前最优的LDPC码方案具有的香农限仅有0.0045dB。相对于turbo码而言，LDPC码具有更低的误码平台；其描述简单，对严格的理论分析具有可验证性；吐量大，极具高速译码潜力，而且因为LDPC码采用了并行的迭代译码算法，以及由于LDPC码具有随机码特性，在与信源或者信道级联时，不需要额外加交织器.系统的复杂度和延时都比turbo码要低。

LDPC 码的应用与进展

由于LDPC码提出较晚和第3代移动通信标准失之交臂，但基于LDPC编码的方案极有可能成为4G移动通信系统的应用方案。目前已有很多系统采用LDPC码。

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

据日经BP社报道，日本产业技术综合研究所、NEC电子和东京电力9月6日宣布，利用产综研的集群计算机“AIS下Super Cluster”成功验证了LDPC码的有效性。这次验证说明，验证了LDPC不存在Error Floor.据此，IEEE802.3an工作小组全体通过，在面向双绞线的10 Gbit/s以太网标准“10GBASE-T”的草案中采用LDPC码。

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

LDPC 码的展望

目前LDPC码研究领域的主要工作集中在译码算法的性能分析、编码方法、码的优化算法等方，经研究人员的努力，LDPC编码领域取得很大进展，但仍有许多问题需要研究：

1．LDPC码校验矩阵的构造，尽管在构造最优的LDPC码方面取得了一些进，但目前还没有一套系统的办法来构造所需要的好码，特别是在码字长度有限、码率一定的条件下，构造性能优异的好码是一个非常具有挑战性的课题，这方面的研究可以借助有限域理论、图论等相关理论。

2．LDPC编码系统的联合优化设计，将编码技术与调制技术、空时编码技术、OFDM技术结合进行性能优化是当前及将来的发展方向之一。

3．无线衰落信道及MIMO信道下LDPC码的性能分析方法及优化设计准则。目前LDPC码字的优化设计主要在加性高斯白噪声信道下得到的，而无线衰落信道下，特别是时变信道下码字的性能分析方法、优化设计准则和信道估计的影响也是非常关键的课题，需要进一步的研究探索。

4．寻找适合硬件实现的编译码方法也是一个非常值得研究的课题。