Hans Journal of Wireless Communications 无线通信, 2013, 3, 56-59
http://dx.doi.org/10.12677/hjwc.2013.32008 Published Online April 2013 (http://www.hanspub.org/journal/hjwc.html)

Analysis of Non-Binary LDPC Codes in the Application of Satellite Communications*

Huan Xu[1], Lei Wen[2,3], Yongjie Xie[1], Wenming Zhang[1], Jianqian Long[1]

[1]188 Branch of 21 Mail Box, Urumqi
[2]College of Electronic Science & Engineering, National University of Defense Technology, Changsha
[3]Centre for Communication Systems Research, University of Surrey, London, UK
Email: newton1108@sina.com

Received: Oct. 9th, 2012; revised: Oct. 26th, 2012; accepted: Dec. 15th, 2012

Copyright © 2013 Huan Xu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract: In deep space communication system, improving ability of error correction is a key technique. Non-binary LDPC Codes are hotspot and outperform Binary LDPC Codes. Based on application of satellite communications, the universal encoding algorithm based on LU factorization is researched. In order to keep low density of matrix, criteria of row pivot is analyzed. Iterative decoding algorithm is researched. By comparing simulation performance of Non-binary LDPC Codes and Binary LDPC Codes, it shows that Non-binary LDPC Codes are better than Binary LDPC Codes. The result is helpful to application of Non-binary LDPC Codes in satellite communications.

Keywords: Satellite Communications; Non-Binary LDPC Codes; LU Factorization; Belief Propagation; Iterative Decoding Algorithm

多元域 LDPC 码在卫星通信中的应用研究*

徐　欢[1]，文　磊[2,3]，谢永杰[1]，张文明[1]，龙建乾[1]

[1]乌鲁木齐 21 信箱 188 分箱，乌鲁木齐
[2]国防科学技术大学，电子科学与工程学院，长沙
[3]萨里大学通信系统研究中心，伦敦，英国
Email: newton1108@sina.com

收稿日期：2012 年 10 月 9 日；修回日期：2012 年 10 月 26 日；录用日期：2012 年 12 月 15 日

摘　要：在卫星通信中，如何提高抗干扰能力是需要重点关注的问题之一。多元域 LDPC 码是通信界研究的热点课题，较二进制 LDPC 码有更优的纠错性能。本文从卫星通信的应用角度出发，对利用 LU 分解进行编码的通用编码算法展开研究，以保证矩阵稀疏性为目标，分析了行主元选取策略。同时研究了多元域 LDPC 码的迭代译码算法。对多元域 LDPC 码纠错系统的纠错性能进行了仿真，测试结果表明多元域 LDPC 码的性能优于信源信息速率和码率相同的二进制 LDPC 码，为多元域 LDPC 码在卫星通信中的应用奠定了基础。

关键词：卫星通信；多元域 LDPC 码；LU 分解；置信度传递；迭代译码算法

1. 引言

卫星通信由于其覆盖区域大、信道容量大，并具有多址联接能力等优点，已成为国际和国内远距离通信的重要手段。由于卫星通信系统是一种无线通信系统，而在无线信道中，因受到环境的影响和外来无线信号的干扰，通信质量较有线信道相差许多。为了提

*基金项目：湖南省自然科学基金资助项目(S2012J5042)，稀疏图码在多媒体通信中的应用研究。

 Copyright © 2013 Hanspub

高系统的抗噪声性能，必须设计合理的信道编译码部分，要求不但可以纠正随机错，更重要是可以纠正突发错。众所周知，随机错误即数据序列中前后码元之间是否发生错误彼此无关，而突发错误则是错误之间体现出相关性，一个错误的出现往往影响后面的数据也出现错误。

近年来，由 Gallager 于 1962 年发现的低密度校验(LDPC)码由于其接近信道容量的纠错性能而受到人们的极大关注[1]，关于二进制 LDPC 码(Binary-LDPC)的研究已经有了大量的工作。Davey 和 MacKay [2]研究发现通过合理设计多元域校验矩阵得到的 LDPC(Non-binary LDPC)码的性能可以超过二进制 LDPC，且多元域 LDPC 码还具有很强的抗突发错误的能力[3,4]，其性能超过了同码参数下的 RS 码[5]。多元域 LDPC 码的译码采用快速傅立叶变换在频域进行译码能够使译码复杂度从 $O\left(q^2\right)$ 降到 $O\left(pq\right)$ [6]。从现有的卫星通信传输标准和研究文献来看，尚未发现多元域 LDPC 码在卫星通信中的成功应用，因此开展卫星通信中的多元域 LDPC 码应用研究具有很强的工程应用背景和实际应用价值。

本文安排如下，引言部分指出研究多元域 LDPC 码的意义，第二部分对多元域 LDPC 码的通用编码算法进行分析，第三部分研究了迭代译码的方法，第四部分将多元域 LDPC 码与二进制 LDPC 码在卫星通信中的性能进行对比，指出下一步研究方向。

2. 基于 LU 分解的多元域 LDPC 码编码算法

现有的 LDPC 码构造方法大多基于两个考虑：一是追求好的纠错性能，二是使其具有特定的结构从而能进行快速编码。二者往往不能兼得，通过随机构造法构造的码尽管具有很好的性能，但编码复杂度太高而没有实用价值[7]。考虑 $GF\left(2^p\right)$ 上的多元域 $\left(n,k\right)$ LDPC 码，将校验矩阵分成 $\left[\boldsymbol{A},\boldsymbol{B}\right]$ 两部分，其中 $\boldsymbol{A}$ 是 $\left(n-k\right)\times\left(n-k\right)$ 的满秩矩阵，码字则对应为[*t*, *s*]形式，其中 *t* 代表校验符号，*s* 代表信息符号，由于码字空间即为校验矩阵的零空间：

$$\left[\boldsymbol{A},\boldsymbol{B}\right]\times\begin{bmatrix}t^T\\ s^T\end{bmatrix}=0\text{，即 }t^T=\boldsymbol{A}^{-1}\times\boldsymbol{B}\times s^T \qquad (1)$$

式中乘法与加法运算都在多元域上进行，编码即通过解上面方程组得到校验符号的过程。然而矩阵求逆的运算非常复杂，并且 $\boldsymbol{A}^{-1}$ 是稠密矩阵，直接对其进行处理会呈指数级地增加硬件开销及系统时延。如果 $\boldsymbol{A}$ 可以分解为 $\boldsymbol{L}$、$\boldsymbol{U}$ 两部分 $\boldsymbol{A}=\boldsymbol{L}\times\boldsymbol{U}$，$\boldsymbol{L}$ 为下三角矩阵，$\boldsymbol{U}$ 为上三角矩阵，通过引入中间变量 v，方程(1)变成如下两组：

$$\boldsymbol{L}\times v=B\times s^T \qquad (2)$$

$$\boldsymbol{U}\times t^T=v \qquad (3)$$

利用 $\boldsymbol{L}$ 和 $\boldsymbol{U}$ 的三角结构，(2)式采用前向迭代算法、(3)式采用后向迭代算法能够快速计算出方程的解，这样可以避免矩阵求逆等效率极低的繁杂运算[8]。对于多元域上的稀疏矩阵，其 $\boldsymbol{LU}$ 分解最重要的目的就是要尽量保证分解矩阵的稀疏性，以及分解过程的稳定性，否则就失去研究价值。同时考虑到 $\boldsymbol{LU}$ 分解只需通过计算机软件进行运算，得到的 $\boldsymbol{L}$、$\boldsymbol{U}$ 能够以稀疏矩阵的形式存储到编码器硬件设备中，每次进行编码时，可以直接调用这些矩阵实现连续编码。

行主元策略的基本思想是：第 *i* 步寻找校验矩阵中第 *i* 列上包含非零元素的行，选取其中具有最小行重的某一行作为主行，进行行交换后再高斯消元。分解流程如下：

1) 初始化

设 $\boldsymbol{L}=E_{(n-k)\times(n-k)}$ (单位阵)，$\boldsymbol{U}=A$，$i=1$；定义维数为 $n-k$ 的行标数组 *R*，赋初值 1 到 $n-k$。

2) 选取主元及更新行标数组 *R*

在 $\boldsymbol{U}$ 的剩余矩阵中寻找第 *i* 列上包含非零元素的行，统计行重，选取具有最小行重的作为主行，有多种选择时取第一个作为主行，如选取的主行在第 *j* 行，则主元为 $\boldsymbol{U}_{ji}$；将 $\boldsymbol{U}$ 中 *i*、*j* 两行互换，并交换 $\boldsymbol{L}$ 中第 *i* 行和第 *j* 行前 $i-1$ 个元素，同时更新行标数组 *R*。

3) 高斯消元

选定主元后，把 $\boldsymbol{U}$ 的剩余矩阵的第一列赋给 $\boldsymbol{L}$ 中的对应列，即 $\boldsymbol{U}$ 中第 *i* 列上为 $\alpha\left(\alpha\in GF\left(2^p\right),\alpha\neq 0\right)$，则 $\boldsymbol{L}$ 中对应的位置赋为 α；再将 $\boldsymbol{U}$ 中 *i* 行上所有元素都除以主元：

$$\boldsymbol{U}_{if}^{(i)}=\boldsymbol{U}_{if}^{(i-1)}\Big/\boldsymbol{U}_{ii}^{(i-1)} \qquad i\le f\le n-k \qquad (4)$$

式中的上标 i、$i-1$ 表示循环的次数，此时主元变为 1；$\boldsymbol{U}$ 的剩余矩阵其它元素计算如下：

$$\boldsymbol{U}_{ef}^{(i)}=\boldsymbol{U}_{ef}^{(i-1)}-\boldsymbol{U}_{ei}^{(i-1)}\times\boldsymbol{U}_{if}^{(i)} \qquad i<e,f\le n-k \qquad (5)$$

Copyright © 2013 Hanspub

所有元素更新之后 $i+1$，如果 $i=n-k$ 则计算结束并跳出迭代，否则回到第二步继续计算。

分解过程中涉及到行交换，根据线性代数相关原理，矩阵行交换相当于左乘一个单位行交换矩阵，列交换相当于右乘一个单位列交换矩阵。出于实用考虑，我们不引入单位行/列交换矩阵，而是以行标数据 R 来记录行交换次序，所以(2)式右边的列向量根据 R 作相应调换即可，不会影响最终解的结果。

3. 多元域 LDPC 码的迭代译码算法

多元域译码与二进制译码最大的区别就是它将码字元素的取值从二元域扩展到 2^m 域，这样无疑是增加了迭代算法的复杂度[9]。与二进制 LDPC 码的迭代译码算法相类似，迭代包含以下几个步骤：

1) 初始化

信度传播译码算法为软判决译码，所以在进入译码器之前，需要根据信道状态信息对变量点的初始概率进行估计。在实际中采用 m 个二进制信道来实现 $GF\left(2^m\right)$ 上一个码元的传输，因此 $GF\left(2^m\right)$ 上的一个元素可以由 m 比特的二进制序列来表示，即将一个 2^m 元的信道等价于 m 个二元信道并行传输。

因此，这里计算 q_{mn}^t 的初始化时，可以先将 t 表示为二进制序列的形式 $X=\left(x_1,x_2,\cdots,x_m\right)$，然后利用二进制译码中初始化的结论可得 $P_n^t=\prod_i^m p_n^{x_i}$。其中 P_n^t 为多元信道估计量，$p_n^{x_i}$ 为二元信道估计量。

2) 计算校验节点向变量节点传送的信息

校验信息 r_{mn}^t 表示在第 n 个变量节点等于 t 的条件下，满足第 m 个校验方程的概率，即 $r_{mn}^t=\Pr\left(\text{满足第}m\text{校验方程}\middle|x_n=0\right)$。利用全概率公式可展开为下列形式：

$$\begin{aligned}r_{mn}^t&=\Pr\left(\text{满足第}m\text{校验方程}\middle|x_n=t\right)\\&=\sum\Pr\left(\text{满足第}m\text{校验方程}\middle|x_n=t,\left\{x_{n^\bullet}:n^\bullet\in N\left(m\right)\backslash n\right\}\right)\Pr\left(\left\{x_{n^\bullet}:n^\bullet\in N\left(m\right)\backslash n\right\}\right)\\&=\sum\Pr\left(\text{满足第}m\text{校验方程}\middle|x_n=t,\left\{x_{n^\bullet}:n^\bullet\in N\left(m\right)\backslash n\right\}\right)\prod_i\Pr\left(\text{其它第}i\text{个变量节点}\right)\\&=\sum\Pr\left(\text{满足第}m\text{校验方程}\middle|x_n=t,\left\{x_{n^\bullet}:n^\bullet\in N\left(m\right)\backslash n\right\}\right)\prod_{i\in N(m)\backslash n}q_{mi}^{x_{n^\bullet}}\end{aligned}$$

其中，$N\left(m\right)$ 表示参与第 m 个校验方程的变量节点，$N\left(m\right)\backslash n$ 表示除去第 n 个变量节点以外，参与第 m 个校验方程的其它变量节点。

变量信息 q_{mn}^t 表示在满足除了第 m 个校验方程以外的其他校验方程所得到的第 n 个变量节点为 t 的概率，即：

3) 计算变量节点向校验节点传送的信息

$$q_{mn}^t=\Pr\left(x_n=0\middle|\text{满足除第}m\text{个校验方程以外的其他校验方程}\right)$$

利用贝叶斯公式可以化为如下形式：

$$\begin{aligned}q_{mn}^t&=\Pr\left(x_n=t\middle|\text{满足除第}m\text{个校验方程以外的其他校验方程}\right)\\&=\frac{\Pr\left(\text{满足除第}m\text{个校验方程以外的其他校验方程}\middle|x_n=t\right)\Pr\left(x_n=t\right)}{\sum_i\Pr\left(\text{满足除第}m\text{个校验方程以外的其他校验方程}\middle|x_i\right)\Pr\left(x_i\right)}\\&=\frac{\prod_{i\in M(n)/m}r_{in}^t\Pr\left(x_n=t\right)}{\sum_i\Pr\left(\text{满足除第}m\text{个校验方程以外的其他校验方程}\middle|x_i\right)\Pr\left(x_i\right)}\\&=\alpha_{mn}\prod_{i\in M(n)/m}r_{in}^tP_n^t\end{aligned}$$

4) 计算后验概率进行判决 $q_n^t=\alpha_{mn}\prod_{j\in M(n)}r_{jn}^tP_n^t$

假设得到的码字 $C=\left\{C_n\right\}$，其中 C_n 为使得 q_n^t 最大的一系列 t 值。这样就完成了一次译码，得到一组

Copyright © 2013 Hanspub

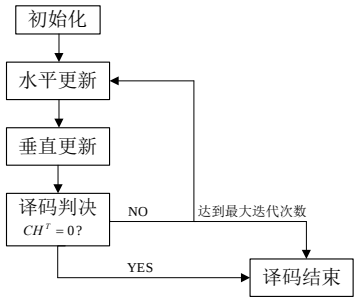

Figure 1. Diagram of iterative decoding for non-binary LDPC codes
图 1. 多元域 LDPC 码迭代译码算法流程图

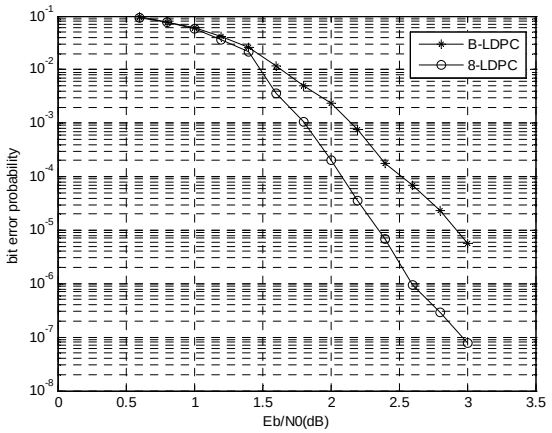

Figure 2. Error correcting performance of (1000, 500) 8-LDPC and (3000, 1500) B-LDPC Codes
图 2. (1000, 500) 8-LDPC 码和(3000, 1500)B-LDPC 码纠错性能

码字 C，再将 C 带入 CH^T 式，若为 0，则译码成功，反之再转入第二步继续进行迭代译码，直到 $CH^T=0$ 或者达到所规定的最高迭代次数，则停止迭代。图 1 给出了多元域 LDPC 码迭代译码的流程图。

4. 性能测试

为了测试多元域 LDPC 码的纠错性能，在 GF(8)上基于代数学构造方法设计了(1000, 500)的码率为 1/2 的多元域 LDPC 码(8-LDPC)，并对其性能进行了仿真。为了与码长和码率相同的二进制 LDPC 码进行性能比较，同时仿真了对应比特码长码率相同的(3000, 1500)二进制 LDPC 码性能(B-LDPC)。信道模拟为卫星通信的典型高斯噪声信道，调制方式采用 BPSK，最大迭代次数设置为 50 次。采用的仿真平台基于 matlab 的 simulink 进行开发，各部分分别进行模块化设计。其中多元域 LDPC 码的编译码模块根据理论算法自行编写与开发，进一步丰富了 simulink 的通信仿真库。

图 2 显示了(1000, 500)8-LDPC 码与(3000, 1500) B-LDPC 码的纠错性能。从图中可以看出，在比特码长与码率都相同的条件下，8-LDPC 码的性能要明显好于 B-LDPC 码性能。在 $E_b/N_0=3$ dB 时，8-LDPC 码的误比特率比 B-LDPC 码低一到两个数量级。相比于 B-LDPC 码，8-LDPC 码的编码增益提高了约 0.5 dB。

5. 结束语

本文研究了多元域LDPC码的LU分解编码算法，以及迭代译码算法。仿真结果表明，多元域 LDPC 的性能较二进制 LDPC 有明显提高。随着卫星探测的深入，对卫星通信在可靠性和带宽效率方面都提出了更高要求。在未来的工作中，如何改善多元域 LCPC 码的环结构，以及降低译码复杂度，是进一步研究的方向。

6. 致谢

感谢湖南省自然科学基金委员会对本论文的大力的支持。

参考文献 (References)

[1] R. G. Gallager. Low density parity check codes. IRE Transactions on Information Theory, 1962, 8(1): 21-28.
[2] M. Davey, D. J. C. MacKay. Low density parity check codes over GF(q). IEEE Communications Letters, 1998, 2(6): 165-167.
[3] A. Marinoni, P. Savazzi. Non-binary LDPC codes with good performance on channels affected by bursty noise, 2008. www.gtti.it/GTTI08/files/SessioneScientifica/marinoni.pdf
[4] H. Song, J. R. Cruz. Reduced-complexity decoding of q-ary LDPC codes for magnetic recording. IEEE Transactions on Magnetics, 2003, 39(2): 1081-1087.
[5] S.-E. Park, C. Lim. A class of structured LDPC codes over GF(q) for efficient encoding. IEEE Transactions on Communications, 2007, 6(37): 2218-2222.
[6] A. Braunstein, F. Kayhan and R. Zecchina. Efficient LDPC codes over GF(q) for lossy data compression. IEEE Transactions on Information Theory, 2009: arXiv:0901.4467.
[7] B. Zhou, J. Y. Kang, S. M. Song and S. Lin. Construction of non-binary quasi-cyclic LDPC codes by arrays and array dispersions. IEEE Transactions on Communications, 2009, 57(6): 1652-1662.
[8] R. M. Neal. Sparse matrics methods and probabilistic inference algorithms, 1999. http://www.cs.utoronto.ca/~radford/
[9] J. Lei, C. J. Tang and J. H. Wang. An effective algorithm for construction of LDPC codes. Changsha: Proceedings of 2008 IEEE International Conference on Information and Automation, 20-23 June 2008: 1542-1546.

Copyright © 2013 Hanspub