

一种基于循环移位矩阵的LDPC码构造方法

乔华 管武 董明科 项海格
(北京大学卫星与无线通信实验室 北京 100871)

摘要: 具有准循环结构的低密度奇偶校验码(QC-LDPC Codes)是目前被广泛采用的一类LDPC码。本文提出了一种结合PEG算法构造基于循环移位矩阵的QC-LDPC码的方法。该方法首先将QC-LDPC码传统的基于比特的二分图简化为基于Block的二分图,然后在图中采用PEG算法遵循的环路最大原则确定每一个循环移位矩阵的位置,最后根据QC-LDPC码的环路特性为每一个循环移位矩阵挑选循环移位偏移量。利用该算法,本文构造了长度从1008bit到8064bit,码率从1/2到7/8各种参数的LDPC码。仿真结果表明,本文构造的LDPC码性能优于目前采用有限几何、两个信息符号的RS码、组合数学等常用的代数方法构造的QC-LDPC码。

关键词: 准循环低密度奇偶校验码; PEG算法; 循环移位矩阵

中图分类号: TN911.22

文献标识码: A

文章编号: 1009-5896(2008)10-2384-04

Construction of LDPC Codes Based on Circulant Permutation Matrices

Qiao Hua Guan Wu Dong Ming-ke Xiang Hai-ge

(Satellite and Wireless Communication Laboratory, Peking University, Beijing 100871, China)

Abstract: Quasi Cyclic LDPC (QC-LDPC) codes are of particular interest in various areas. In this paper, a method to construct a class of QC-LDPC codes based on circulant permutation matrices is showed. The method chooses the position of each non-zero sub-matrix in the bipartite graph based on blocks. Then the circulant permutation value of each sub-matrix is decided. With the proposed algorithm, a few LDPC codes were constructed with the code length from 1008 bit to 8064 bit and with code rate from 1/2 to 7/8. Simulation results show that the proposed LDPC codes are superior to QC-LDPC codes with other construction algorithms.

Key words: Quasi-Cyclic LDPC (QC-LDPC) codes; Progressive Edge Growth (PEG) algorithm; Circulant permutation matrices

1 引言

LDPC码以其接近香浓极限的优异性能得到了广泛的青睐。目前PEG算法^[1]被认为是有限码长条件下LDPC码的最优构造方法。但PEG-LDPC码的H矩阵结构完全随机,译码器实现复杂度太高^[2],因此具有准循环结构的LDPC码(Quasi-Cyclic LDPC Codes, QC-LDPC Codes)的构造方法得到了深入研究^[3-8]。

最常见的QC-LDPC码又被称为Block-LDPC码。Block-LDPC码的H矩阵可以表示成如式(1)所示的形式^[8],其中I(p_{i,j})表示循环移位偏移量为p_{i,j}的p×p循环移位单位矩阵,若偏移量p_{i,j}小于0,则代表一个全零矩阵:

$$H = \begin{bmatrix} I(p_{0,0}) & I(p_{0,1}) & \cdots & I(p_{0,n-1}) \\ I(p_{1,0}) & I(p_{1,1}) & \cdots & I(p_{1,n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ I(p_{m-1,0}) & I(p_{m-1,1}) & \cdots & I(p_{m-1,n-1}) \end{bmatrix} \quad (1)$$

Block-LDPC码的H矩阵可以被简化为式(2)中B矩阵的形

式,它的每一个元素都对应H矩阵中每一个循环移位矩阵的循环移位偏移量:

$$B = \begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m-1,0} & p_{m-1,1} & \cdots & p_{m-1,n-1} \end{bmatrix} \quad (2)$$

由于Block-LDPC码H矩阵中的所有非零元素都各自属于特定的循环移位矩阵,因此可以将基于比特的二分图简化为如图1所示的基于Block的二分图。在基于比特二分图中,每一个虚线框中包含的p个节点,在右边的基于Block的二分图中被简化表示为一个节点。基于Block的二分图的每一条边线则对应基于比特二分图中属于同一个循环移位矩阵的p条边线,每一条边线的权重等于该循环移位矩阵的循环移位偏移量p_{i,j}。

基于Block的二分图中每一条长度为2l的环路都可以被等价表示为^[8] p_{i₀,j₀}, p_{i₁,j₁}, ..., p_{i_{l-1},j_{l-1}}, p_{i₀,j₀}。

性质 1^[8] 基于Block的二分图中的一条长度为2l的环路,对应基于比特的二分图中一条长度为2l的环路的充分必要条件是环路偏移量序列满足: $\sum_{k=0}^{2l-1} (-1)^k p_{i_k, j_k} = 0 \pmod p$ 。

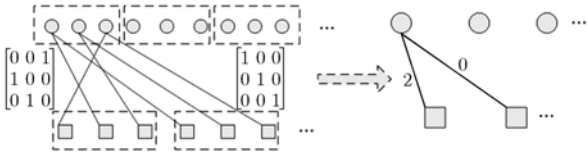


图 1 Block-LDPC 码的二分图

性质 2^[9] 基于 Block 的二分图中每一条长度为 $2l$ 的环路, 对应基于比特的二分图中一条长度为 $2rl$ 的环路, 其中 r 满足等式 $r \sum_{k=0}^{2l-1} (-1)^k p_{k, k} = 0 \pmod p$ 。

本文的主要工作是: 提出一种结合 PEG 算法的 Block-LDPC 码构造方法, 并在此基础上构造了一系列具有不同参数的性能优异的 QC-LDPC 码。本文的第 2 节将给出一种结合 PEG 算法的 Block-LDPC 码构造方法——Block-PEG 算法。第 3 节给出利用此算法构造的 Block-PEG-LDPC 码的误比特性能仿真结果, 并与利用其它方法构造的具有不同参数的 QC-LDPC 码进行对比。最后是结束语。

2 构造方法

构造 Block-LDPC 码的过程就是构造矩阵 B 的过程。矩阵 B 包含了 Block-LDPC 码的两个关键参数: 每一个循环移位矩阵的位置和相应的循环移位偏移量。因此可以将构造算法分为两个主要的步骤: 首先确定循环移位矩阵的位置, 再确定相应的循环移位偏移量。为了方便后续的说明, 设每一个循环移位矩阵大小为 $p \times p$, 码长为 $N = np$, 校验方程数 $M = mp$ 。

2.1 循环移位矩阵位置的确定

确定每一个循环移位矩阵的位置等价于为基于 Block 的二分图中的每一条边线确定端点。本文在确定每一个循环移位矩阵的位置时将遵循最大环路准则。通过性质 2 可知, 基于 Block 的二分图中的每一个长度为 $2l$ 的环都会导致基于比特的二分图中出现长度是 $2l$ 整数倍的环。因此扩大基于 Block 的二分图的周长, 基于比特的二分图周长也相应得到扩大。而基于 Block 的二分图周长与每条边线权重无关, 所以本文在此处借鉴 PEG 算法^[1], 步骤如下:

(1)初始化:

(a)向基于 Block 的二分图中填充 m 个没有任何连接的校验节点, 它们的当前维度为 0, 记作 $\{d_c^1, d_c^2, \dots, d_c^m\}$;

(b)根据维度分布, 将 n 个变量节点按照维度从低到高排列为 $\{v_1, v_2, \dots, v_n\}$ 的顺序, 它们的维度记作 $\{d_v^1, d_v^2, \dots, d_v^n\}$;

(2)构造: For $i = 1$ to n

(a)取出变量节点 v_i 添加到基于 Block 的二分图中, 当前维度 $d_i = 0$;

(b)以 v_i 为根节点, 按照 PEG 算法的方法, 对当前二分图做树状展开^[1](图 2);

(c)统计距离根节点最远的校验节点集合, 它们的维度记作 $\{d_c^1, d_c^2, \dots\}$;

(d)从 $\{d_c^1, d_c^2, \dots\}$ 中挑选出最小的维度 d_c^j , 找到与之对应的校验节点 c_j 。如果同时存在多个校验节点的维度相同而且最小, 就从中随机选择一个;

(e) $d_i = d_i + 1$, 判断 d_i 是否等于 d_c^j , 如果是则返回步骤(2)(a), 否则返回步骤(2)(b)。

上述确定每一个循环移位矩阵位置的过程实际上是 PEG 算法在基于 Block 的二分图中的应用, 因此在后面将把本文提出的 QC-LDPC 码构造方法称为 Block-PEG 算法。

2.2 循环移位偏移量的确定

构造 Block-LDPC 码的另外一个关键步骤就是确定每一个循环移位矩阵的偏移量, 即基于 Block 的二分图中每一条边线的权重。根据性质 2 知道, 当基于 Block 的二分图中的环路确定以后, 边线权重的选择最终决定了基于比特的二分图中环的长度。

设边线参与的最短环路共有 t 个, 边线权重值为 x , 则可以得到 t 个环路的路径累计值集合 $\{s_i = (\sum_{k=0}^{2l-2} (-1)^k p_{k, k} - x) \pmod p, 1 \leq i \leq t\}$ 。特别地, 当最短环路长度为 4 时, 就必须根据性质 1 计算出不能选择的边线权重值集合:

$$X = \{x_i \mid (\sum_{k=0}^{2l-2} (-1)^k p_{k, k} - x_i) \pmod p = 0, 0 \leq x_i < p, 1 \leq i \leq t\} \quad (3)$$

在此基础上, 本文给出两种确定边线权重的准则: 环路最大化原则和随机原则。随机原则是一种挑选权重的低复杂度准则。该准则只保证 Block-LDPC 码不出现长度为 4 的环, 即在选取权重时, 只保证不选择出现在公式(3)中集合 X 的所有数值, 对于其余的任意小于 p 的非负数值进行等概率随机挑选。随机原则的最大优点就是复杂度很低, 因为每一个循环移位矩阵位置的选择是在保证基于 Block 的二分图环路最大的基础上进行的, 所以随机挑选的权重并不会导致二分图中出现大量的短环。最大化环路原则以最大化局部环路为最终目的。根据性质 2, 当选择的边线权重 x 使得环路权重累计值 s 与子矩阵大小 p 互质时, 得到的环路长度是最长的, 因此在采用最大化环路原则确定权重时, 必须针对每一个环路计算环路累计值 s_i , 得出满足互质条件的权重候选集合 Y_i , 最终的权重候选集合 $Y = \bigcap Y_i$, 如果 Y 为空集, 则按照随机原则的方法, 从所有不会构成 4 元环的权重中随机选择一个; 如果不为空, 则在 Y 中随机挑选一个数值作为权重。不难发现, 当 p 为素数时, 随机原则与最大化环路原则是等价的。最大化环路原则的构造结果与文献[10]的构造结果等价。

2.3 算法流程

在整个基于 Block 的二分图的边线连接关系完全确定之后再确定每条边线的权重, 面临的将是一个环路长度的全局优化问题, 复杂度太高。本文采用 PEG 算法优化局部环路长度的思路^[1], 每一个循环移位偏移量的选择仅考虑它对当前二分图环路的影响, 如图 2 所示。

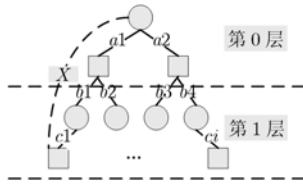


图2 Block-PEG 算法示意图

(1)初始化参数:

(a)令码长 $N = np$, 校验方程数目 $M = mp$, 每个 block 的大小为 $p \times p$, 偏移量矩阵的大小为 $m \times n$;

(b)利用密度推演^[11]等方法确定变量节点的维度分布。

(2)初始化基于 Block 的二分图: 向基于 Block 的二分图中填充 m 个没有任何连接的校验节点。

(3)构造: 向基于 Block 的二分图中逐个添加变量节点, 挑选校验节点建立连接, 并确定边线权重。

(a)以当前变量节点为根节点, 将基于 Block 的二分图展开为树状图(图2);

(b)从距离根节点最近的校验节点中挑选当前维度最低的节点作为目的节点;

(c)遍历根节点到目的节点的所有路径, 根据 $s =$

$$\sum_{k=0}^{l-1} (-1)^k p_{i_k, j_l} \text{ 计算累积权重 } s;$$

(d)根据公式(3)求出根节点到目的节点, 边线不能选择的权重集合以及候选权重集合;

(e)从候选权重集合中挑选出边线的权重;

(f)判断根节点维度是否已经满足初始维度分布, 如果不是则返回步骤(3)(a), 否则进入下一个步骤;

(4)判断是否已经添加完 n 个变量节点, 如果是则进入下一步骤, 否则返回步骤(3);

(5)根据构造得到矩阵 B , 在 H 矩阵相应位置填充进相应偏移量的循环移位矩阵。

3 仿真及分析

近年来, QC-LDPC 码的构造方法研究取得了许多进展。其中以有限几何方法^[3]、基于两个信息符号的 RS 码的方法^[4]、基于组合数学 BIBD 的方法^[5]等最为著名。为了能够充分衡量 Block-PEG 算法的有效性, 本文构造了不同码长不同码率的 Block-PEG-LDPC 码, 并与文献[3-6]提供的利用上述方法构造的具有代表性的 QC-LDPC 码以及 PEG-LDPC 码进行了误比特性能的仿真比较。所有仿真都在 BIAWGN(Binary Input Additive White Gaussian Noise)信道下进行, 译码算法采用和积算法, 最大迭代次数为 50 次, 当错误 50 个 LDPC 码码字时, 仿真终止。

仿真 1 构造了长度为 1008bit, 码率为 1/2 的 Block-PEG-LDPC 码, 每一个循环移位矩阵大小为 36×36 , 将变量节点的维度分布优化为 $\lambda(x) = 0.3x + 0.16x^2 + 0.17x^3 + 0.37x^6$ 。同时本文利用 PEG 算法^[1]构造了同样参数的 PEG-

LDPC 码, 也利用随机搜索方法构造了同样参数的 Random-Block-LDPC 码, 误比特性能的仿真比较结果(图 3)表明, Block-PEG-LDPC 码的误比特性能已经能够非常接近 PEG-LDPC 码, 并且在误比特率为 10^{-5} 时, 归一化信噪比优于随机搜索得到的 Block-LDPC 码 0.3dB。

仿真 2 构造了码率为 1/2 的(8064, 4032)Block-PEG-LDPC 码, 每一个循环移位矩阵大小为 126×126 , 将变量节点的维度分布优化为 $\lambda(x) = 0.27x + 0.24x^2 + 0.49x^8$ 。将它与文献[6]给出的利用代数方法构造的基于循环移位矩阵的(8176, 4088)LDPC 码进行误比特性能的仿真比较(图 4)。仿真结果表明, Block-PEG-LDPC 码在误比特率为 10^{-5} 时, 归一化信噪比优于文献[6]的方法构造的 LDPC 码约 0.35dB。

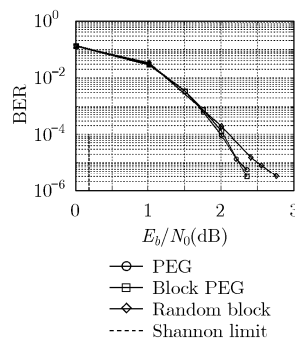


图3 与 PEG-LDPC 以及随机搜索的 LDPC 码比较

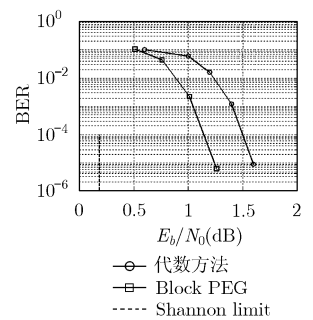


图4 与代数方法构造的循环移位矩阵 LDPC 码比较

仿真 3 构造了长度为 1008bit, 码率为 3/4 的 Block-PEG-LDPC 码, 每一个循环移位矩阵的大小为 28×28 , 变量节点的维度分布优化为 $\lambda(x) = 0.13x + 0.19x^2 + 0.25x^3 + 0.43x^6$ 。将它与文献[3]给出的长度为 1023bit, 码率为 0.76 的有限几何 LDPC 码进行了误比特性能的仿真比较(图 5)。仿真结果表明, Block-PEG-LDPC 码在误比特率为 10^{-5} 时, 归一化信噪比优于有限几何 LDPC 码接近 0.4dB。

仿真 4 构造了码率为 0.8125 的(8064, 6552)Block-PEG-LDPC 码, 每一个循环移位矩阵大小为 126×126 , 将变量节点的维度分布优化为 $\lambda(x) = 0.09x + 0.455x^2 + 0.455x^6$ 。将它与文献[4]给出的利用两个信息符号的 RS 码构造的码率为 0.82 的(8192, 6754)LDPC 码进行误比特性能的仿真比较(图 6)。仿真结果表明, Block-PEG-LDPC 码在误比特率为 10^{-5} 时, 归一化信噪比优于基于 RS 码的 LDPC 码约 0.5dB。

仿真 5 构造了长度分别为 8064bit, 码率 3/4 的 Block-PEG-LDPC 码, 每一个循环移位矩阵大小为 168×168 , 将变量节点的维度分布优化为 $\lambda(x) = 0.137x + 0.315x^2 + 0.548x^{11}$ 。将它与文献[5]给出的利用组合数学方法构造的(8420, 6319)码率 3/4 的 LDPC 码进行了误比特性能仿真比

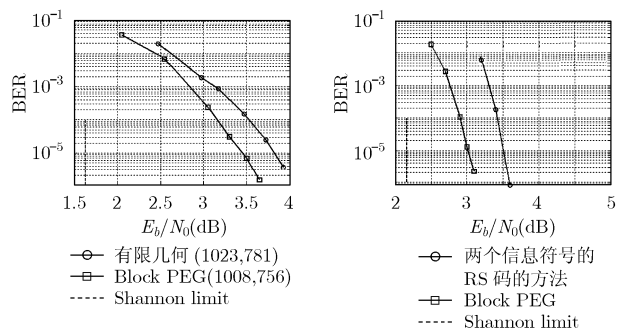


图 5 与有限几何 LDPC 码比较 图 6 与基于 RS 码的 LDPC 码比较

较(图 7)。仿真结果表明, 8064bit, 3/4 码率的 Block-PEG-LDPC 码即使是在码长稍短的条件下, 误比特率为 10^{-5} 时, 归一化信噪比依然优于利用组合数学方法构造的 LDPC 码 0.5dB。

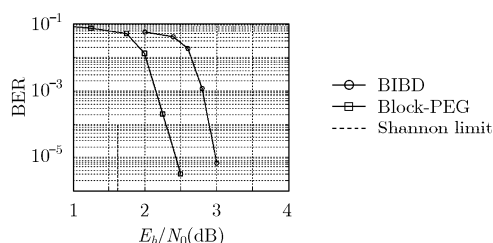


图 7 与组合数学方法构造的 LDPC 码比较

4 结束语

本文给出了一种有效的构造基于循环移位矩阵的 QC-LDPC 码的方法。该方法吸收了 PEG 算法的特点, 能够构造出不同码长和码率参数的 LDPC 码。仿真结果表明, 利用本文提出的方法构造的 QC-LDPC 码具有优秀的误比特特性, 优于目前大部分利用代数方法构造的 QC-LDPC 码, 是一种能够用于实际通信系统的 LDPC 码。

参 考 文 献

- [1] Hu X Y, Eleftheriou E, and Arnold D M. Regular and irregular progressive edge-growth tanner graphs. *IEEE Trans. on Inf. Theory*, 2005, 51(1): 386-398.
- [2] Mansour M M and Shanbhag N R. A novel design methodology for high-performance programmable decoder cores for AA-LDPC codes. SIPS'03., Seoul, Aug. 2003: 29-34.

- [3] Kou Y, Lin S, and Fossorier M P C. Low-density parity-check codes based on finite geometries: A rediscovery and new results. *IEEE Trans. on Inf. Theory*, 2001, 47(7): 2711-2736.
- [4] Djurdjevic I, Xu J, Abdel-Ghaffar K, and Lin S. A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols. *IEEE Comm. Lett.*, 2003, 7(7): 317-319.
- [5] Ammar B, Honary B, Kou Y, Xu J, and Lin S. Construction of low-density parity-check codes based on balanced incomplete block designs. *IEEE Trans. on Inf. Theory*, 2004, 50(6): 1257-1269.
- [6] Xu J, Zeng L, Lan L, Chen L, and Lin S. Construction of low-density parity-check codes by superposition. *IEEE Trans. on Comm.*, 2005, 53(2): 243-251.
- [7] Kim K S, Lee S H, Kim Y H, and Ahn J Y. Design of binary LDPC code using cyclic shift matrices. *Elec. Lett.*, 2004, 40(5): 325-326.
- [8] Fossorier M P C. Quasicyclic low-density parity-check codes from circulant permutation matrices. *IEEE Trans. on Inf. Theory*, 2004, 50(8): 1788-1793.
- [9] Myung Scho, Yang Kyeongcheol, and Kim Jaeyoel. Quasi-cyclic LDPC codes for fast encoding. *IEEE Trans. on Inf. Theory*, 2005, 51(8): 2894-2901.
- [10] Li Z W and Kumar B V K V. A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph. Signals, Systems and Computers'04., California, 2004: 1990-1994.
- [11] Chung S Y, Richardson T J, and Urbanke R L. Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation. *IEEE Trans. on Inform. Theory*, 2001, 47(2): 657-670.

- 乔 华: 男, 1980 年生, 博士生, 研究方向为信道编码以及卫星通信网。
- 管 武: 男, 1981 年生, 博士生, 研究方向为信道编码以及通信信号处理。
- 董明科: 男, 1973 年生, 硕士, 研究领域为数字通信、软件无线电。
- 项海格: 男, 1941 年生, 主要研究领域为数字通信、无线和卫星通信网、软件无线电以及基于芯片的通信系统(SOC)。