

不同置换矩阵对基于分块 H 矩阵的 LDPC 码性能的影响

彭 立 朱光喜

(华中科技大学电子与信息工程系 武汉 430074)

摘 要 研究了三种结构的循环移位置换矩阵,分别称为定义在 $GF(2)$ 有限域上的 I 矩阵、 D 矩阵和 Q 矩阵,讨论了这些置换矩阵的结构特征和性质,主要研究了 D 和 Q 矩阵对基于单位矩阵 I 的规则 QC-LDPC 码和 IEEE 802.16e 标准草案中推荐的不规则 QC-LDPC 码性能的改进. 该文的另一个贡献是以 Q 矩阵为分块矩阵,构造了 S-LDPC 码新码族. S-LDPC 码在性能和编码计算复杂度方面都略优于 IEEE 标准中的不规则 QC-LDPC 码.

关键词 低密度奇偶校验码(LDPC 码); 编码算法; 奇偶校验矩阵; 循环移位置换矩阵; 递归编码器

中图法分类号 TP393

Performance Impact of Deferent Permutation Matrix on LDPC Codes Based on Partitioned H -Matrix

PENG Li ZHU Guang-Xi

(Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)

Abstract The authors investigate three kinds of circulant-shift permutation matrices, which are called I (identity matrix), D and Q matrices, and discuss their structural characteristics and several properties in this paper. Computer simulating tests show that D and Q matrices can improve performance of the regular QC-LDPC codes based on identity matrix, including irregular QC-LDPC codes in IEEE 802.16e standard draft. The other contribution in the paper is designing the new family of S-LDPC codes by using Q matrix as partitioned matrices of H -matrix, which have the advantage of irregular QC-LDPC codes presented in IEEE 802.16e standard draft in performance and calculating complexity.

Keywords low-density parity-check codes; encoder; parity-check matrix; circulant-shift permutation matrix; recursive encoder

1 引 言

自 LDPC 码^[1-2]1996 年复出以来,通信工程师和编码理论家进行了大量的研究工作,普遍认为目前阻碍 LDPC 码走向应用的瓶颈问题是 LDPC 码稀疏奇偶校验矩阵 H 的代数结构设计问题和线性

开销 LDPC 码编码器的设计问题.

LDPC 码定义为有限域 $GF(2)$ 上的稀疏奇偶校验矩阵的零空间,即 $Hc^T = 0^T$,其中 H 是稀疏奇偶校验矩阵,矢量 c 即是 LDPC 码字序列. H 矩阵与 Tanner 图具有关联特征,已知 H 矩阵可以画对应的 Tanner 图,已知 Tanner 图可以写出对应的 H 矩阵.由此可见,设计 LDPC 码,关键是设计稀疏 H 矩

阵或稀疏 Tanner 图. LDPC 码 \mathbf{H} 矩阵的构造算法主要分为两大类,一类是随机结构的^[2-3];另一类是代数结构的.文献[4-5]对不规则 LDPC 码进行了研究,采用离散密度进化的算法设计度数分布对,使随机搜索的不规则码的阈值达到 0.0045dB^[5].文献[6-7]分别提出了一类代数结构的准循环码,称为 QC-LDPC 码.其 \mathbf{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置换矩阵组成,由于对分块矩阵维数 n 的取值进行了限制,使这两类 QC-LDPC 码的码参数选择不灵活.文献[8]给出了 LDPC 码编码器具有线性复杂度的结论,并提出一种系统形式的 \mathbf{H} 矩阵设计方法.2006 年 2 月公布的 IEEE 802.16e 标准草案推荐一种不规则 QC-LDPC 码的选择方案^[9],其编码方案需要存储事先经优化设计、计算机搜索的基矩阵,然后用全零子矩阵和单位置换子矩阵对这个基矩阵进行填充,构造出的 \mathbf{H} 矩阵是系统形式的,其编码计算复杂度与码长成线性关系.由此可见,对 LDPC 码编码器线性复杂度算法研究的突破性进展,促使 LDPC 码最终走向实用,并成功进入标准.

本文在基于单位置换矩阵 \mathbf{I} 构造的 QC-LDPC 码研究成果的基础上,提出两种新的置换矩阵构造方法,分别称为 \mathbf{D} 矩阵和 \mathbf{Q} 矩阵.仿真实验表明对大多数规则和不规则 QC-LDPC 码,由 \mathbf{D} 和 \mathbf{Q} 矩阵取代单位矩阵 \mathbf{I} ,能使规则 QC-LDPC 码的性能得到 2.0dB 的改善.利用 \mathbf{Q} 矩阵中非零元素分布的无序性、随机性、不规则性的特征,本文构造一类特殊的 LDPC 码集合,称为 S-LDPC 码. S-LDPC 码的稀疏奇偶校验矩阵 \mathbf{H} 是校验位与信息位分开的系统形式,即 $\mathbf{H} = [\mathbf{H}^p \quad \mathbf{H}^d]$,其中, \mathbf{H}^p 是校验位对应的矩阵,由确定结构的双对角矩阵构成^[10]; \mathbf{H}^d 是信息位对应的矩阵,由循环移位置换矩阵构成,这组循环移位置换矩阵不仅可以是单位矩阵 \mathbf{I} ,还可以是文献[11]定义的 \mathbf{Q} 矩阵和文献[12]定义的 \mathbf{D} 矩阵.由于 \mathbf{H}^p 矩阵的双对角结构,使 S-LDPC 码完全不同于 QC-LDPC 码,即它不是准循环结构的. S-LDPC 码的特殊性就在于,其 \mathbf{H} 矩阵中包含一列度数为 1 的列矢量,或对应的 Tanner 图中存在一个度数为 1 的变量节点.本文提出的 S-LDPC 码与 QC-LDPC 码相比,具有许多优点,如在性能方面基于 \mathbf{Q} 矩阵的 S-LDPC 码比不规则 QC-LDPC 码有将近 0.5dB 的改善;在编码复杂度方面, S-LDPC 码不需要转换成 \mathbf{G} 生成矩阵,利用 \mathbf{H} 矩阵直接导出编码算法,

其编码算法复杂度与校验位长度成线性关系.而 QC-LDPC 码需要求解 \mathbf{G} 矩阵^[13],其编码计算复杂度至少为 $O(N^2)$;在解码复杂度方面,由于 S-LDPC 码的 \mathbf{H} 矩阵中有一半的列重量不超过 2,另一半的列重量最大为 6,使 \mathbf{H} 矩阵的稀疏度达到最低程度,其置信传播迭代解码算法的计算复杂度不仅低于相同参数的 QC-LDPC 码的解码计算复杂度,而且还低于现有不规则码的解码计算复杂度;此外, S-LDPC 码的码数量更丰富,码长和码率的取值更灵活,能很容易地构造码率为 0.1~0.95 的大范围变化的 LDPC 码,对所有码率都不会产生错误平层问题.可以说 S-LDPC 码为 LDPC 码在无线传输系统中的应用提供了一种有效途径.

2 新型置换矩阵 \mathbf{D} 矩阵和 \mathbf{Q} 矩阵的定义与性质

定义 1. 等差数列的通项公式为 $a_n = a_1 + (n-1)d$,其中 a_1 是首项, d 是公差, n 是矢量长度.对于给定的 a_1, d, n ,计算 n 次通项公式 a_n ,得到一个任意顺序排列的 n 元组序列,称这个 n 元序列为 \mathbf{D} 矢量. \mathbf{D} 矢量定义在十进制正整数域上,将 \mathbf{D} 矢量展开成二进制有限域 $GF(2)$ 上的矩阵,则称为 \mathbf{D} 矩阵.

\mathbf{D} 矩阵的结构特点是 $GF(2)$ 有限域上取值的 $n \times n$ 阶方阵,它的每行、每列均只有一个“1”元素,其余元素都是“0”.在某些文献中^[14]每行、每列只有一个 1 的子矩阵均有研究和应用,所不同的是这里 \mathbf{D} 矩阵所对应的 \mathbf{D} 矢量由等差数列形成.由 \mathbf{D} 矩阵构成的 LDPC 码称为 D-LDPC 码.

由等差数列构成 \mathbf{D} 矢量的具体实施方法描述如下:根据等差数列的通项公式 $a_n = a_1 + (n-1)d$,如取矢量长度为 $n = 12$,公差为 $d = 2$,当首项为 $a_1 = 1$ 时,得到等差数列 1, 3, 5, 7, 9, 11, 当 $a_1 = 2$ 时,得到另一个等差数列 2, 4, 6, 8, 10, 12, 将两个数列合并在一起,并表示成矢量形式,即为 \mathbf{D}_0 矢量 (1, 3, 5, 7, 9, 11, 2, 4, 6, 8, 10, 12). 数列的合并方式也可以是第 2 个数列在前,第 1 个数列在后,即 (2, 4, 6, 8, 10, 12, 1, 3, 5, 7, 9, 11). 又如,取公差 $d = 3$,当 $a_1 = 1$ 时,得到等差数列 1, 4, 7, 10, 当 $a_1 = 2$ 时,得到等差数列 2, 5, 8, 11, 当 $a_1 = 3$ 时,得到等差数列 3, 6, 9, 12, 将 3 个数列合并在一起,得另一个 \mathbf{D}_0 矢量 (1, 4, 7, 10, 2, 5, 8, 11, 3, 6, 9, 12). 3 个数列可以有 6 种排列方式,因此可以得到 6 个不同的 \mathbf{D}_0 矢

量. 当公差 $d=1$ 时, \mathbf{D}_0 矢量为 $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$, 对应的 \mathbf{D}_0 矩阵是单位矩阵 \mathbf{I} , 由这个单位矩阵及其一组循环矩阵所生成的规则 LDPC 码正是已被多人研究的准循环 QC-LDPC 码, 所以 QC-LDPC 码是 D-LDPC 码在公差 $d=1$ 情况下的特例.

定义 2. 任意一个矩阵元素在 $GF(2)$ 有限域上取值的 $n \times n$ 阶非对角方阵 (n 为任意正整数), 它的每行、每列、每对角线均只有一个元素取 1, 其余元素为 0, 则该矩阵称为 \mathbf{Q} 矩阵^[10]. 由 \mathbf{Q} 矩阵构成的 LDPC 码称为 Q-LDPC 码.

由于 \mathbf{Q} 矩阵的定义与 n 维皇后问题的描述等效, 所以 \mathbf{Q} 矩阵的获取可由 n 维皇后搜索算法得到. n 维皇后问题是这样描述的: 由 n^2 个方块排成 n 行 n 列的正方形称为“ n 元棋盘”. 若任意两个皇后位于 n 元棋盘上同一行、或同一列、或同一对角线, 则称它们为互相攻击. 要求找出使 n 元棋盘上的 n 个皇后互不攻击的布局. 如果建立如下的数学模型: 棋盘上出现皇后的位置设为“1”, 没有出现皇后的位置设为“0”, 那么寻找皇后互不攻击的布局就相当于求解 \mathbf{Q} 矩阵中“1”元素的分布问题. 实际上, 搜索 \mathbf{Q} 矩阵的算法是约束满足问题的解, n 维皇后问题是完全 NP-问题. n 维皇后问题求解的具体方法不是本文的研究重点, 本文感兴趣的是 \mathbf{Q} 矩阵的作用: 利用现有的 n 维皇后搜索算法获取 \mathbf{Q} 矩阵, 利用 \mathbf{Q} 矩阵来构造稀疏奇偶校验矩阵 \mathbf{H} , 从而寻找性能优良的 LDPC 码.

用循环移位置换矩阵来构造 \mathbf{H} 矩阵是一种针对 LDPC 码的面向应用的设计方法, 因为基于循环移位置换矩阵的 \mathbf{H} 矩阵, 更容易用硬件来实现快速的编码算法和快速的部分并行解码算法, 因此有必要对置换矩阵的特性进行讨论. 目前, 存在三种置换矩阵, 即 \mathbf{I} , \mathbf{D} 和 \mathbf{Q} 循环移位置换矩阵, 它们有如下的共同性质:

(1) 它们所有的行或列均是线性独立的, 所以它们都是满秩矩阵, 秩为 n . \mathbf{D} 和 \mathbf{Q} 矩阵经有限次初等矩阵变换, 均可转换为单位矩阵 \mathbf{I} .

(2) 它们的稀疏度相同, 在一个 $n \times n$ 的方阵中, 每行每列均只有一个 1.

(3) 矢量表示性, 即每个置换矩阵都可以表示成矢量形式, 矢量与矩阵的对应关系是: 矢量中每个元素所在位置的序号表示矩阵中“1”元素所在列的序号, 矢量中元素的值表示矩阵中“1”元素所在行的序号. 置换矩阵的矢量表示提供了非零元素在置换

矩阵中的位置坐标, 并为大型 \mathbf{H} 矩阵提供了压缩存储形式.

(4) 循环移位性, 每个 $n \times n$ 的置换矩阵经 $n-1$ 次循环移位后, 得到 n 个置换矩阵, 形成一个置换矩阵集合, 这个集合中的每个置换矩阵中“1”元素的分布都是不同的.

(5) 集合中的 n 个置换矩阵的 1 元素分布具有互不重叠性, 将这 n 个置换矩阵模 2 相加得到全 1 矩阵. 利用特性(4)和(5)可以构造不含小循环的 \mathbf{H} 矩阵, 或者说同一个置换矩阵集合中的元素能完全确定一个不含小循环的 \mathbf{H} 矩阵, 但某个 \mathbf{H} 矩阵中所包含的子矩阵可以取自不同的置换矩阵集合;

(6) 置换矩阵中每个 1 元素的坐标是确定, 如果用这些置换矩阵构成 \mathbf{H} 矩阵, 只要构成 \mathbf{H} 矩阵的分块置换矩阵的循环移位次数已知, 那么整个 \mathbf{H} 矩阵中 1 元素的位置坐标就可以计算得到, 这个特性可简化 LDPC 码编码器和解码器硬件体系结构的实现.

除了上述 6 个相同特性外, \mathbf{I} , \mathbf{D} 和 \mathbf{Q} 矩阵还存在如下的不同特性:

(1) 结构不同, \mathbf{I} 和 \mathbf{D} 矩阵都是有序的、规则的, 能用数学表达式实现, \mathbf{I} 对“1”元素的分布是单一的, 成对角线分布; \mathbf{D} 矩阵对“1”元素的分布形成一个有限的集合, 集合中的每一元素对应一个等差数列的公差值, 集合的大小由 \mathbf{D} 矩阵的维数 n 确定 (注意 \mathbf{D} 矩阵集合中的每一个元素都能形成一个 n 维的置换矩阵集合, n 维的 \mathbf{D} 矩阵集合与 n 维的 \mathbf{D} 置换矩阵集合是不同的概念). \mathbf{Q} 矩阵对“1”元素的分布是无序的、随机的, 形成一个无限集合, \mathbf{Q} 矩阵没有具体的数学表达式实现, 要靠计算机搜索才能得到;

(2) 自身循环特征不同. 对 \mathbf{I} 矩阵: 每一行是它上面一行循环右移 (或左移) 一次得到, 最后一行是最后一行循环右移 (或左移) 一次得到, 每一列是它左边一列循环下移一次得到, 第一列是最后一列循环下移一次得到. 对 \mathbf{D} 矩阵: 每一行是它上面一行循环右移 i 次 (或左移 j 次, $j \neq i$, $i, j \neq 1$) 得到, 但第一行不是最后一行循环右移 i 次得到, 每一列是它左边一列循环下移 k 次得到, 但第一列不是最后一列循环下移 k 次得到. 对 \mathbf{Q} 矩阵: 每一行也可以通过上面一行循环右移 (或左移) 得到, 但各行的循环移位次数均不相同, 每一列也可以通过它左边一列循环下移得到, 但各列的循环次数也均不同, 并且从目前看来, 各行和各列的不同循环移位次数没有规

律可循.

(3) 多个置换矩阵求和的结构与循环的关系. 文献[13]给出了循环(circulant)的定义: 一个循环是行重量和列重量均相等的、矩阵元素定义在 $GF(2)$ 有限域上的方阵, 在这个方阵中每一行可由上一行循环移位得到, 第一行是最后一行的循环移位, 每一列是它左边一列的循环移位, 第一列是最后一列的循环移位. 设循环的重量为 w , 如果 $w=1$, 那么这个循环就是循环移位置换矩阵. 以 $n=8, w=2$ 为例, 分别用置换矩阵 I, D 和 Q 来构成循环, 循环本身是一个方阵, 这里用 A 表示.

$$A_I = I_0 + I_3 =$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

同理有

$$A_D = D_0 + D_3 =$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$A_Q = Q_0 + Q_3 =$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

上面基于单位置换矩阵的 A_I 、基于 D 置换矩阵的 A_D 和基于 Q 置换矩阵的 A_Q 都是重量为 2 的方阵, 它们均由 I, D 和 Q 各自的原始置换矩阵加循环移位 3 次的置换矩阵构成. 由 A_I 和 A_D 的结构可以看出它们均满足上述循环的定义, 所以它们是一种循环, 而 A_Q 并不满足循环的定义, 它的结构中包含两种循环, 所以它是准循环的结构. 如果循环移位次数选择合适, 即使循环的维数 n 很小(如上面的 $n=8$),

也能保证 A_I, A_D 和 A_Q 中不存在 4 线循环. 讨论具有循环特征的矩阵的重要性在于由循环构成的 H 矩阵能用简单的循环移位寄存器构成编码电路^[14].

3 利用置换矩阵和循环构造规则 QC-LDPC 码

以 Gallager 提出的规则 LDPC 码的定义为基本出发点, 其 H 矩阵的结构特点可归纳如下: (1) 每列含 1 的个数是一个固定的较小数 $q, q \geq 3$; (2) 每行含 1 的个数也是固定的较小数 $t, t \geq q$; (3) 任何两列之间同为 1 的行数(称为重叠数)不超过 1, 即 H 矩阵中不含四角为 1 的小方阵, 也即 H 矩阵对应的 Tanner 图中无 4 线循环, 最小围线至少应为 6; (4) q 和 t 均远小于码字长度 N 和矩阵的行数 $M (= Nq/t)$, 且当 $N \rightarrow \infty$ 时, $q/N = t/M \rightarrow 0$, 表明 H 矩阵是稀疏的.

以一组互不重叠的循环 A 方阵作为分块子矩阵, 将这组 A 方阵进行适当排列组合可构造满足上述 4 个条件的稀疏奇偶校验矩阵 $H = [h_{ij}; i = 1, 2, \dots, M; j = 1, 2, \dots, N]$. 在 $GF(2)$ 上, 利用 $n \times n$ 循环 A , 可以构造如下形式 $q \times t$ 阵列, 它是 H 矩阵的基矩阵:

$$B(H) = \begin{bmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,t} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ A_{q,1} & A_{q,2} & \cdots & A_{q,t} \end{bmatrix} \quad (1)$$

由式(1) H 矩阵的零空间所定义的 LDPC 码是准循环 QC-LDPC 码, 码长为 $N = n(q+t)$, 它的码率为 $R \geq (t-q)/t$, 如果 H 矩阵不存在冗余校验行, 则取等号.

无论是置换矩阵, 还是循环, 用来构造规则 LDPC 码的 H 矩阵, 均得到准循环 QC-LDPC 码. 对置换 D 和 Q 矩阵或它们构成的循环 A_D 和 A_Q 矩阵进行初等行列变换, 均可变换成单位置换矩阵 I 或它所构成的循环 A_I . 所以, 无论是由置换矩阵 D 和 Q 去填充式(1)的 $B(H)$ 基矩阵, 还是由循环 A_D 和 A_Q 构成的 $B(H)$ 矩阵, 对填充后的 H 矩阵进行行列变换, 它们均分别与 I 构成的 H 矩阵和 A_I 构成的 H 矩阵等效. 由此可见, 由相同尺寸的 I, D 和 Q 分别构成的相同参数的规则 H 矩阵是同构的, 换句话说, 不同的置换矩阵 I, D 和 Q 构成的规则 QC-LDPC 码, 其性能是相同的. 大量软件仿真实验也表明: 由 I, D 和 Q 矩阵分别构成的相同参数的 QC-LDPC

码均具有相同的性能. 因此, QC-LDPC 码的仿真实验, 均采用单位置换矩阵 \mathbf{I} 来填充基矩阵式(1).

需要注意的是: 实验表明由置换矩阵 \mathbf{I} 或由 \mathbf{I} 构成的循环 \mathbf{A}_i 来填充基矩阵 $\mathbf{B}(\mathbf{H})$, 所产生的 \mathbf{H} 矩阵均不是行满秩的, 即 \mathbf{H} 矩阵的秩不等于其行数 M , 意味着 \mathbf{H} 矩阵存在冗余校验行. 这会带来两方面的不利因素:

(1) 由于基于基矩阵式(1)的任意 \mathbf{H} 矩阵的冗余校验行不能确定, 使实际码率略大于设计码率, 造成 QC-LDPC 码的码率设计不可控;

(2) 由式(1)填充的 \mathbf{H} 矩阵不是行满秩矩阵, 意味着它的生成矩阵不存在, 因此编码器设计存在困难.

分析基矩阵式(1)的结构发现, 如果采用单一的置换矩阵或单一的循环去填充基矩阵, 所产生的 \mathbf{H} 矩阵始终存在冗余校验行. 现引入 $n \times n$ 的全零矩阵, 记为 \mathbf{L} . 如果, 同时用置换矩阵、循环和全零矩阵去填充基矩阵, 经适当排列, 可以消除上面两种不利因素, 即(1)可以构成不含冗余校验行的规则 \mathbf{H} 矩阵; (2) 不同的置换矩阵导致 QC-LDPC 码的性能不同, \mathbf{Q} 置换矩阵集之中一定存在最优 \mathbf{Q} 矩阵, \mathbf{D} 置换矩阵集之中一定存在最优 \mathbf{D} 矩阵, 最优 \mathbf{Q} 矩阵的性能优于最优 \mathbf{D} 矩阵的性能, 最优 \mathbf{D} 矩阵的性能优于 \mathbf{I} 置换矩阵的性能. 换句话说, 对不含冗余校验的 \mathbf{H} 矩阵, 引入 \mathbf{Q} 矩阵和 \mathbf{D} 矩阵后, 能使基于 \mathbf{I} 矩阵的 QC-LDPC 码的性能得到改善.

一个可行的基矩阵构造方案设计如下(参数为列重量 $q=3$, 行重量 $t=6$, 码率 $R=1/2$):

$$\mathbf{B}(\mathbf{H}) = \mathbf{B}([\mathbf{H}^p \mathbf{H}^d]) = \begin{bmatrix} \mathbf{A}_1^3 & \mathbf{L} & \mathbf{L} & \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \mathbf{A}_{1,3} \\ \mathbf{L} & \mathbf{A}_2^3 & \mathbf{L} & \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \mathbf{A}_{2,3} \\ \mathbf{L} & \mathbf{L} & \mathbf{A}_3^3 & \mathbf{A}_{3,1} & \mathbf{A}_{3,2} & \mathbf{A}_{3,3} \end{bmatrix} = \begin{bmatrix} \mathbf{I}_6 + \mathbf{I}_9 + \mathbf{I}_{13} & \mathbf{L} & \mathbf{L} & \mathbf{I}_0 & \mathbf{I}_1 & \mathbf{I}_2 \\ \mathbf{L} & \mathbf{I}_9 + \mathbf{I}_{12} + \mathbf{I}_{16} & \mathbf{L} & \mathbf{I}_3 & \mathbf{I}_5 & \mathbf{I}_8 \\ \mathbf{L} & \mathbf{L} & \mathbf{I}_{10} + \mathbf{I}_{14} + \mathbf{I}_{17} & \mathbf{I}_4 & \mathbf{I}_7 & \mathbf{I}_{11} \end{bmatrix} \quad (2)$$

其中, \mathbf{A}_i^3 表示重量 $w=3$ 的循环, \mathbf{I} 的下标值表示单位置换矩阵的循环左移次数. \mathbf{I} 矩阵也可以用 \mathbf{D} 和 \mathbf{Q} 矩阵取代. 式(2)可扩展成列重量为 3、行重量为 6 的 \mathbf{H} 矩阵, 实际上定义了一种(3,6)规则 QC-LDPC 码的结构. 式(2)的 \mathbf{H} 矩阵具有系统结构, 校验位和信息位对应的矩阵是分开的, 校验位对应的 \mathbf{H}^p 矩阵考虑了削去冗余校验行的结构设计, 因此编码器的设计码率为 1/2. 同时还考虑了不存在小 girth 的设计约束条件, 即 \mathbf{H}^p 矩阵中不存在 4 线循环, 而 \mathbf{H}^d

矩阵中不存在 6 线循环, 综合二者的结构是 \mathbf{H} 矩阵中至少不存在 4 线循环, 存在少量的 6 线循环.

对式(2)的规则 QC-LDPC 码进行了数字仿真, 编码器输出的码字由 (0,1) 构成, 经 BPSK 调制成发射信号 $(-1,1)$, 运行在均值为零, 方差为 σ_N^2 的高斯白噪声信道上, 接收序列服从 $N(0, \sigma^2)$ 分布. 编码器采用行列变换方式, 计算复杂度为 $O(N^2)$. 编码码长采用 802.16e 标准中提供的参数, $N=576$ 和 $N=2304$. 对应不同的码长, 分别用 \mathbf{D} 矩阵和 \mathbf{Q} 矩阵取代式(2) \mathbf{H}^d 矩阵中的 \mathbf{I} 矩阵, \mathbf{H}^p 矩阵保持不变, 进行三种置换矩阵的仿真实验, 发送分组为 1000 分组, 最大迭代次数均为 50.

图 1 演示了码长为 $N=576$ 的性能比较情况, \mathbf{Q} 矩阵比 \mathbf{I} 矩阵性能改善接近 2 dB, \mathbf{D} 矩阵改善 1.54 dB. 图 2 演示了 $N=2304$ 的性能比较情况, \mathbf{Q} 矩阵比 \mathbf{I} 矩阵改善性能 2.585 dB, \mathbf{D} 矩阵改善 1.1 dB. 由于式(2)的下标矩阵并不是用优化技术设计的, 所以由式(2)扩展成的 \mathbf{H} 矩阵所定义的 QC-LDPC 码的性能并不理想, 例如, 对 $N=576$ 的性能曲线, 最好性能的 Q-LDPC 码离香农限 2.37 dB; 对 $N=2304$ 的性能曲线, 最好性能离香农限 1.94 dB. 此外对 \mathbf{I} 矩阵和 \mathbf{D} 矩阵而言, 随着码长增加, 性能有所下降, 但对 \mathbf{Q} 矩阵而言, 仍然有好的表现, 随着码长增加, 性能是增加的, 这个实验体现了 \mathbf{Q} 矩阵的优势.

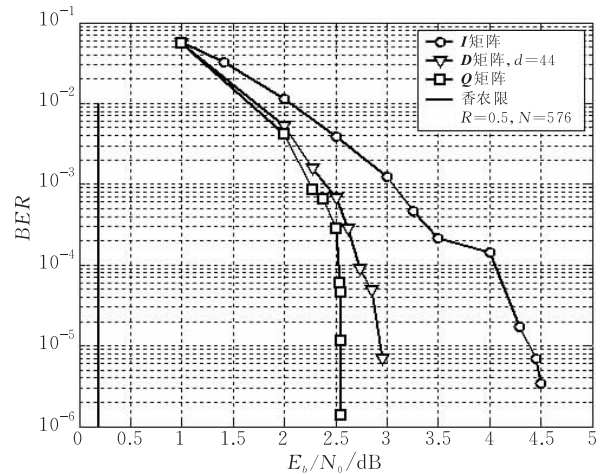


图 1 基于 \mathbf{I} 、 \mathbf{D} 和 \mathbf{Q} 矩阵的 $N=576$ 和 $R=0.5$ QC-LDPC 码的性能比较(列重量 3, 行重量 6)

从仿真结果可以看出 \mathbf{Q} 矩阵构成的 LDPC 码优于 \mathbf{D} 矩阵构成的 LDPC 码, 而基于 \mathbf{D} 矩阵的 LDPC 码又比基于单位矩阵 \mathbf{I} 的 LDPC 码性能优越. 这三种置换矩阵构成的 LDPC 码在性能上的差别, 主要是由于置换矩阵中非零元素分布规律的不

同所造成的. \mathbf{I} 矩阵中的非零元素具有唯一确定的、规则的分布规律, 主要是成对角线分布. \mathbf{D} 矩阵中的非零元素也具有代数可实现的、规则的分布规律, \mathbf{I} 矩阵是 \mathbf{D} 矩阵的子集, \mathbf{D} 矩阵比 \mathbf{I} 矩阵有更多的选择方案, 一个 $n \times n$ 的 \mathbf{D} 矩阵能产生 $n-1$ 种分布, 其中一定存在比 \mathbf{I} 矩阵优的分布. \mathbf{Q} 矩阵中非零元素的分布是无序的、随机的、不规则的, \mathbf{Q} 矩阵集合也是一个无限集合, 因此可以说基于 \mathbf{Q} 矩阵的 QC-LDPC 码是随机码. 实验表明在 \mathbf{Q} 矩阵的无限集合中, 确实存在比 \mathbf{D} 矩阵和 \mathbf{I} 矩阵更优的分布, 因此基于 \mathbf{Q} 矩阵的 LDPC 码的性能自然优于 \mathbf{D} 矩阵和 \mathbf{I} 矩阵构成的 QC-LDPC 码的性能.

4 \mathbf{Q} 矩阵对 IEEE 802. 16e 标准 LDPC 码性能的改进

\mathbf{Q} 置换矩阵对基于单位置换矩阵的规则 QC-LDPC 码的性能有 1.0~2.5dB 的改善. 从大量发表的文献看, 在高斯白噪声信道上, 10^{-5} 以下误码率时, 实用 1/2 码率规则 QC-LDPC 码的性能很难达到 2dB 以下. 如果构造不规则 QC-LDPC 码, 能使性能达到 2dB 以下. 下面以 IEEE802. 16e 标准草案推荐使用 LDPC 码的选择方案为例, 通过仿真实验来验证如下两点: (1) 基于单位矩阵的不规则 QC-LDPC 码的性能优于规则 QC-LDPC 码的性能; (2) 用 \mathbf{Q} 矩阵取代不规则 \mathbf{H} 矩阵(IEEE802. 16e 标准草案提供)中的单位矩阵 \mathbf{I} , 能使基于标准的不规则 QC-LDPC 码的性能得到改善(以下将基于标准的不规则 QC-LDPC 码简称为 IQC-LDPC 码).

IEEE802. 16e 标准草案推荐的 LDPC 码, 其 \mathbf{H} 矩阵由分块置换单位矩阵构成, 具有不规则 QC-LDPC 码结构. 标准中, 设计了 19 种码长, 从最小码长 $N=576$ 到最大码长 $N=2304$, 4 种码率, 即 $R=1/2, 2/3, 3/4, 5/6$. 对应不同的码率, 提供了 6 种基矩阵结构. 本文对其中的 1/2 和 3/4B 两种基矩阵结构^[9]进行了仿真实验. 由于上一节已给出 \mathbf{Q} 矩阵构成的规则 QC-LDPC 码能提供更好的性能, 因此这里仅将 \mathbf{Q} 矩阵取代信息位对应的 \mathbf{I} 矩阵, 进行性能比较. 图 3 和图 4 分别给出了 $R=0.5$ 码率和 $R=0.75$ 码率 B 方案^[9]两种标准基矩阵的模拟仿真实验结果, 采用 \mathbf{I} 和 \mathbf{Q} 分别填充这两个基矩阵中信息位对应的分块矩阵, 而校验位对应的分块矩阵仍然用单位矩阵 \mathbf{I} 填充, 对应最小码长 $N=576$ 和最大码长 $N=2304$, 最大迭代次数是 50 次, 传输分组数是 1000, 信道条件同上一节. 由图 3 可知, 对

0.5 码率短码 ($N=576$) \mathbf{Q} 矩阵比 \mathbf{I} 矩阵性能改善 0.38dB, 对长码 ($N=2304$) 性能改善 0.288dB. 由图 4 可知, 对 0.75 码率 B 型基矩阵短码 ($N=576$), \mathbf{Q} 矩阵比 \mathbf{I} 矩阵性能改善 0.416dB, 对长码 ($N=$

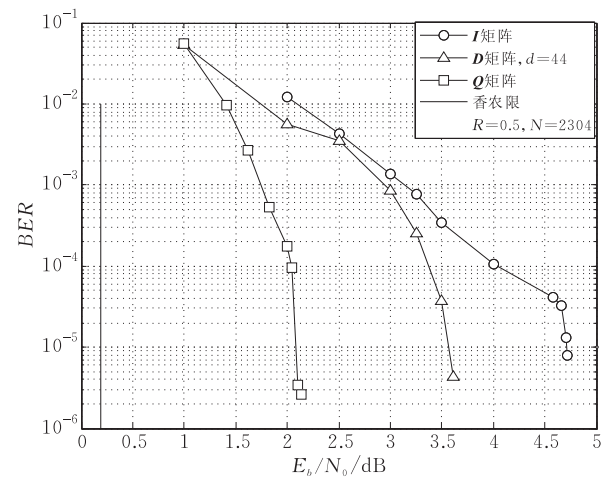


图 2 基于 \mathbf{I} 、 \mathbf{D} 和 \mathbf{Q} 矩阵的 $N=2304$ 和 $R=0.5$ QC-LDPC 码的性能比较(列重量 3, 行重量 6)

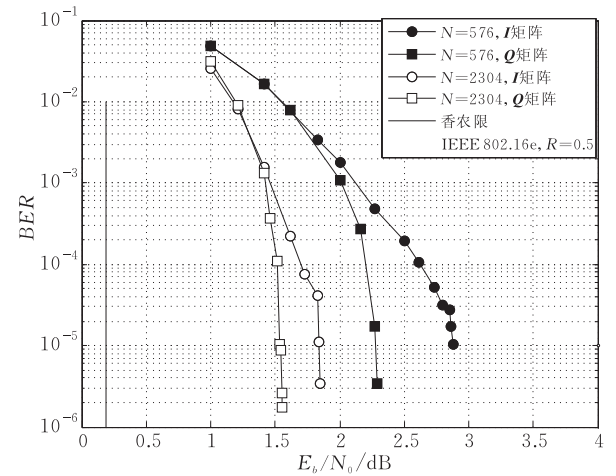


图 3 \mathbf{Q} 矩阵对 IQC-LDPC 码性能的改善($R=0.5$)

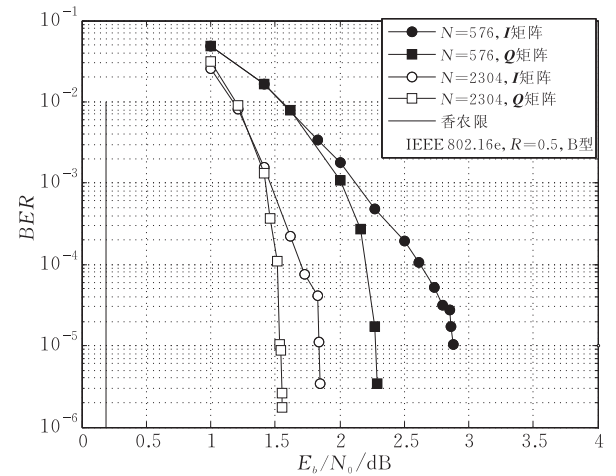


图 4 \mathbf{Q} 矩阵对 IQC-LDPC 码性能的改善($R=0.75$, B 型)

2304)性能改善 0.33dB. 总的来看,用 \mathbf{Q} 矩阵取代标准中 \mathbf{H} 矩阵中的 \mathbf{I} 矩阵,能使不规则 QC-LDPC 码的性能改善 0.2~0.4dB,并且 IEEE802.16e 标准中的不规则 LDPC 码存在一定的错误平层问题,而经 \mathbf{Q} 矩阵修改后,错误平层问题得到改善.从图 3 还可以看出,当 $R=0.5, N=2304$ 时,基于单位矩阵的不规则 QC-LDPC 的性能达到 2.0dB 以下,并且比图 2 中基于 \mathbf{Q} 矩阵的规则 QC-LDPC 码的性能改善了 0.365dB.

5 不规则 S-LDPC 码的编码算法设计

基于分块置换 \mathbf{H} 矩阵结构的 LDPC 码,除了规则和规则 QC-LDPC 码类外,还有另一类特殊的 LDPC 码类,本文称为 S-LDPC 码集合. S-LDPC 码的 \mathbf{H} 矩阵具有系统的结构形式.也就是将矩阵 \mathbf{H} 分解为校验位矩阵 \mathbf{H}^p 和信息位矩阵 \mathbf{H}^d , \mathbf{H}^p 由双对角下三角矩阵构成^[10], \mathbf{H}^d 矩阵由分块置换矩阵或循环构成.

\mathbf{H}^p 矩阵的构造:在 $GF(2)$ 有限域上构造 $M \times M$ 的 $\mathbf{H}^p = [h_{ij}^p; i=1, 2, \dots, M, j=1, 2, \dots, M]$ 矩阵,它由双对角下三角矩阵构成^[10],形式如下:

$$\mathbf{H}^p = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ & \ddots & \ddots & & & \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (3)$$

由式(3)的 \mathbf{H}^p 矩阵结构可以看出, \mathbf{H}^p 矩阵是 $M \times M$ 的方阵,它是满秩矩阵,因此 S-LDPC 码类均不含冗余校验方程, \mathbf{H}^p 矩阵中非零元素的分布特征是:有 $M-1$ 列的重量为 2,有一列的重量为 1. 其对应的 Tanner 图有 $M-1$ 个变量节点的度数为 2,一个变量节点的度数为 1,这一特殊的结构使 S-LDPC 码得名 (Special Low-density Parity-check Codes, S-LDPC 码). 这种结构最早由 Li、Leung 和 Phamdo 等在文献 [10] 中提出,在欧洲 DVB-S2 卫星通信标准中得到应用^[15].

\mathbf{H}^d 矩阵的构造:按照第 3 节中式(1)构造 \mathbf{H} 矩阵的方法,给出下列 $q \times t = 4 \times 4$ 的 \mathbf{H}^d 矩阵的基矩阵阵列,

$$\mathbf{B}(\mathbf{H}^d) = \begin{bmatrix} \mathbf{A}_0 & \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 \\ \mathbf{A}_4 & \mathbf{A}_6 & \mathbf{A}_9 & \mathbf{A}_{13} \\ \mathbf{A}_5 & \mathbf{A}_8 & \mathbf{A}_{12} & \mathbf{A}_{17} \\ \mathbf{A}_7 & \mathbf{A}_{11} & \mathbf{A}_{16} & \mathbf{A}_{22} \end{bmatrix} \quad (4)$$

其中的 \mathbf{A}_i 可以分别用 \mathbf{I} , \mathbf{D} 或 \mathbf{Q} 置换矩阵填充. 由式(4)构成的 \mathbf{H}^d 矩阵是一个 $q \times t$ 的置换矩阵阵列, \mathbf{H}^d 矩阵的列重量为 q 、行重量为 t , \mathbf{H}^d 矩阵的维数是 $(q \times t)n = M \times K$. 如果式(4)中的 \mathbf{A}_i 是用循环 \mathbf{A}_1 , \mathbf{A}_6 和 \mathbf{A}_9 构成,则 \mathbf{H}^d 矩阵的列重量为 wq 、行重量为 wt , \mathbf{H}^d 矩阵的维数仍是 $(q \times t)n = M \times K$. 需要说明的是欧洲 DVB-S2 卫星通信标准中采用的 LDPC 码,虽然利用了双对角矩阵来构造校验码位对应的 \mathbf{H}^p 矩阵,但信息码位对应的 \mathbf{H}^d 矩阵并没有采用分块置换矩阵的结构,因此它与本文提出的 S-LDPC 码类是不同的. 当 Li、Leung 和 Phamdo 提出双对角矩阵结构时,并没有对 \mathbf{H}^d 矩阵的结构进行研究,而是采用了随机结构. 本文给出了 \mathbf{H}^d 矩阵的代数结构.

\mathbf{H} 矩阵的构造:将式(3)的 \mathbf{H}^p 矩阵和式(4)的 \mathbf{H}^d 矩阵并置在一起,得如下的 \mathbf{H} 矩阵:

$$\mathbf{H} = [\mathbf{H}^p \quad \mathbf{H}^d] = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & \mathbf{A}_0 & \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 \\ 1 & 1 & 0 & \cdots & 0 & \vdots & 0 & & & & \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & \mathbf{A}_4 & \mathbf{A}_6 & \mathbf{A}_9 & \mathbf{A}_{13} \\ \vdots & 0 & \ddots & \ddots & 0 & 0 & \vdots & & & & \\ 0 & \vdots & 0 & 1 & 1 & 0 & 0 & \mathbf{A}_5 & \mathbf{A}_8 & \mathbf{A}_{12} & \mathbf{A}_{17} \\ 0 & 0 & \cdots & 0 & 1 & 1 & 0 & & & & \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 & \mathbf{A}_7 & \mathbf{A}_{11} & \mathbf{A}_{16} & \mathbf{A}_{22} \end{bmatrix} \quad (5)$$

由式(5) \mathbf{H} 矩阵的零空间定义了不规则 S-LDPC 码,它的码率为 $R = t/(t+q)$,码长为 $N = n(t+q)$. 式(5) \mathbf{H} 矩阵的独特之处在于:它不是计算机搜索的,而是确定结构的、系统的、可进行递归编码的 \mathbf{H} 矩阵. 由于 \mathbf{H}^p 矩阵的第 1 行不能循环产生第 2 行,第 M 行也不能循环产生第 1 行,所以 \mathbf{H}^p 矩阵不是循环矩阵,它所对应的校验码位也不具有循环特性,由此可断言:由式(5)中 \mathbf{H} 矩阵的零空间所定义的 LDPC 码,不是目前普遍研究的 QC-LDPC 码. 由于它的 \mathbf{H}^d 矩阵由置换矩阵或循环(也由置换矩阵构成)构成,所以 S-LDPC 码类仍可认为是基于分块置换矩阵的码类.

不规则 S-LDPC 码编码器的算法实现:将码序列 \mathbf{c} 分解成校验位序列 $\mathbf{c}^p = \{p_i, i=1, 2, \dots, M\}$ 和信息位序列 $\mathbf{c}^d = \{d_j, j=1, 2, \dots, K\}$,其中, M 是校验位长度, K 是信息位长度. 对任给的信息序列 $\mathbf{c}^d = \{d_j, j=1, 2, \dots, K\}$,利用上面构造的 $\mathbf{H}^p = [h_{ij}^p; i=1, 2, \dots, M; j=1, 2, \dots, M]$ 和 $\mathbf{H}^d = [h_{ij}^d; i=1, 2, \dots, M; j=1, 2, \dots, K]$ 矩阵,根据下面的式(6):

$$\mathbf{H}\mathbf{c}^T = [\mathbf{H}^p \mathbf{H}^d] \begin{bmatrix} \mathbf{c}^p \\ \mathbf{c}^d \end{bmatrix} = \mathbf{H}^p \mathbf{c}^p + \mathbf{H}^d \mathbf{c}^d = 0 \quad (6)$$

求解校验位序列 \mathbf{c}^p , 由于 \mathbf{H}^p 的结构是双对角下三角矩阵, 所以在利用式(6)求解校验位序列 \mathbf{c}^p 时, 不需要对 \mathbf{H}^p 矩阵求逆, 而是通过回代和递推的方法, 如下面式(7)求解 $\mathbf{c}^p = \{p_i, i=1, 2, \dots, M\}$:

$$p_i = \begin{cases} p_1 = \sum_{j=1}^K h_{1j}^d d_j = \sum_{j=1}^t h_{1j}^d d_j, & i=1 \\ p_i = p_{i-1} + \sum_{j=1}^K h_{ij}^d d_j = p_{i-1} + \sum_{j=1}^t h_{ij}^d d_j, & i=2, 3, \dots, M \end{cases} \quad (7)$$

由此求解码字序列 $\mathbf{c} = [\mathbf{c}^p \ \mathbf{c}^d] = \{c_l, l=1, 2, \dots, N\}$.

在与上述规则 QC-LDPC 码相同的调制和信道条件下, 对不规则 S-LDPC 码编码算法进行了模拟仿真, 参数设置为码率 $R=0.5$, 码长 $N=576, 1056, 1536, 2304$, \mathbf{H} 矩阵的结构参数设置为 $q=t=6$, 与码长对应的置换矩阵维数分别为 $n=48, 88, 128, 192$. 图 5 和图 6 分别给出误码率和误分组率与信噪比的特性曲线图, 传输分组为 100000, 最大迭代次数 50.

由图 5 可以看出, 在 10^{-5} 误码率时, S-LDPC 码在 1/2 码率, 码长 $N \geq 576$ 时, 性能均在 3dB 以下, 码长为 2304 和 1536 的 S-LDPC 码错误平层能延伸到 10^{-8} 以下, 1056 和 576 的错误平层也能延伸到 10^{-7} 以下. 图 6 的误分组率均达到了 10^{-5} , 随着码长增加性能变好. 当码长超过 1000 位时, 在 10^{-5} 误分组率下, 性能均能达到 3dB 以下.

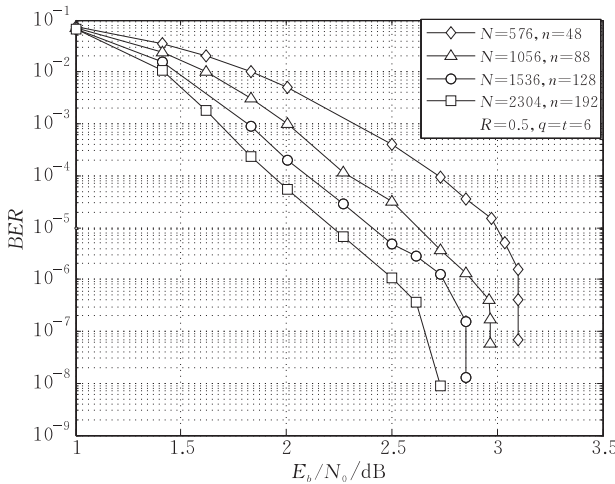


图 5 不同码长 1/2 码率 S-LDPC 码的误码率性能比较 (其中长码的错误平层延伸到 10^{-8} 以下)

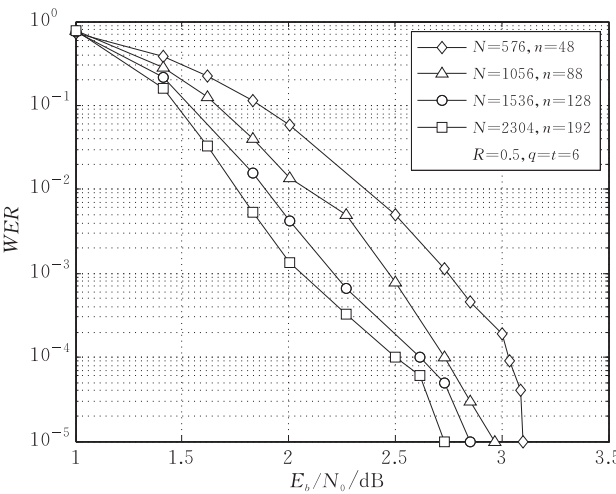


图 6 不同码长 1/2 码率 S-LDPC 码的误分组率性能比较

6 S-LDPC 码与 IQC-LDPC 码的比较

6.1 性能比较

为了有效地说明问题, 本文选择 1/2 码率、三种码长 $N=576, 1536, 2304$ 的 S-LDPC 码和 IQC-LDPC 码, 对其进行误码率的性能比较, 比较结果如图 7 所示, 传输分组为 1000, 最大迭代次数 50. 图中实线表示 S-LDPC 码的性能, 虚线表示 IQC-LDPC 码的性能.

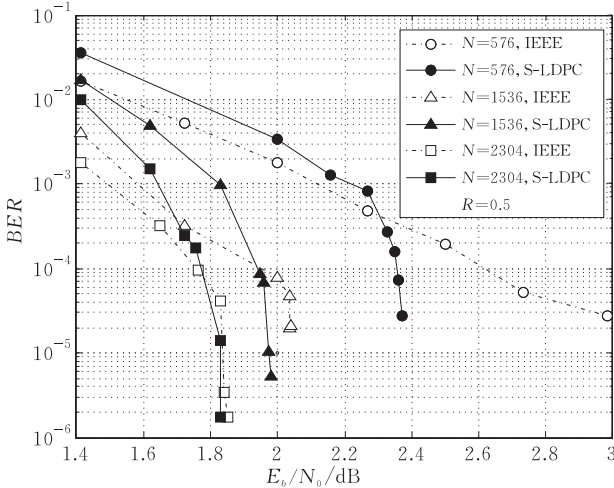


图 7 1/2 码率 S-LDPC 码与 IEEE802.16e 标准中不规则 QC-LDPC 码的误码率性能比较

从图 7 的三组曲线来看, 可以得到如下结论: (1) 误码率在 10^{-4} 以下, 均在 S-LDPC 不同程度上优于 IQC-LDPC 码, 在 10^{-4} 以上, 或者说低信噪比时, IQC-LDPC 码优于 S-LDPC 码. (2) 随着码长增加, 达到标准中的最大码长 2304 时, S-LDPC 码的性能略优于 IQC-LDPC 码的性能; (3) 当码长大于

1000 位时, S-LDPC 码的性能可以达到 10^{-5} 以下, 信噪比在 3.0dB 以下, 而 IQC-LDPC 码在码长为 1536 时, 存在错误平层, 误码率伸不到 10^{-5} , 信噪比也达不到 3.0dB 以下。(4) 随着码长减小, 达到标准中的最小码长 576 时, 在误码率为 10^{-4} 以下, S-LDPC 码的性能明显优于 IQC-LDPC 码的性能, 达 0.5dB 以上。

6.2 复杂度比较

S-LDPC 编码器的计算复杂度可根据递归表达式(7)分析如下: 式(7)的两个求和表达式均为 K 项求和, 表明求解每一位校验位的计算量最多为 K 次乘法和 K 次加法。实际上由于 \mathbf{H}^d 矩阵的每行只有 t 个“1”, 每次求和, 式(7)的两个表达式只有 t 项相加, 实际的加法次数为 t 次, 乘法次数为 t 次, 完成一位校验位的计算量不会超过 $2t$ 次(包括加法和乘法)。完成整个编码运算共需要 M 个校验位, 最多需要计算 $2tM$ 次加法和乘法就可完成整个编码计算, 一般而言 t 的取值远远小于 M 的取值, 所以 S-LDPC 码的编码计算复杂度为 M 的线性复杂度, 即为 $O(M)$ 。由于所有的加法和乘法运算都在 $GF(2)$ 有限域上进行, 所以也可用异或运算次数来表示运算复杂度。完成一位校验位的编码需要 $t-1$ 次异或运算, 完成整个编码运算共需要 $(t-1)M$ 次异或运算。要使 1/2 码率的 S-LDPC 码的性能对 19 种码长均优于 IQC-LDPC 码, 至少应使 $t=6$, 所以 S-LDPC 码的编码计算复杂度大约是 $5M=2.5N$ 次异或运算。

IQC-LDPC 码的 \mathbf{H} 矩阵也分解为信息位和校验位对应的矩阵, 校验位对应的矩阵是下三角矩阵, 在处理时又可分解为两部分 \mathbf{H}^{p_1} 和 \mathbf{H}^{p_2} 。IQC-LDPC 码的编码计算完全不同于式(6)和式(7)所完成的 S-LDPC 码的编码运算, 它需要进行如下的分块矩阵运算。

$$\mathbf{H}\mathbf{c}^T = [\mathbf{H}^d \quad \mathbf{H}^{p_1} \quad \mathbf{H}^{p_2}] \begin{bmatrix} \mathbf{d}^T \\ \mathbf{p}_1^T \\ \mathbf{p}_2^T \end{bmatrix} = \begin{bmatrix} \mathbf{A} & \mathbf{B} & \mathbf{T} \\ \mathbf{C} & \mathbf{D} & \mathbf{E} \end{bmatrix} \begin{bmatrix} \mathbf{d}^T \\ \mathbf{p}_1^T \\ \mathbf{p}_2^T \end{bmatrix} = \mathbf{0}^T \quad (8)$$

式(8)可分解为

$$\mathbf{A}\mathbf{d}^T + \mathbf{B}\mathbf{p}_1^T + \mathbf{T}\mathbf{p}_2^T = \mathbf{0},$$

$$(\mathbf{E}\mathbf{T}^{-1}\mathbf{A} + \mathbf{C})\mathbf{d}^T + (\mathbf{E}\mathbf{T}^{-1}\mathbf{B} + \mathbf{D})\mathbf{p}_1^T = \mathbf{0} \quad (9)$$

式(9)的计算复杂度分析仍很繁琐, 可以参考文献[16]。这里直接引用文献[16]的结论, IQC-LDPC 编码算法需要异或运算 $(c-1+R)N-2n$ 次, 其中 c 是平均列重量, R 是码率, N 是码长, n 是分块置换

矩阵维数。对于 1/2 码率的 IQC-LDPC, 其平均列重量为 $c=3.17$, 异或计算量为 $2.67N-2n$ 。与 S-LDPC 码的 $2.5N$ 异或运算量相比, 相差 $2.67N-2n-2.5N=0.17N-2n$ 。当 $N=2304$ 和 $n=96$ 时, IQC-LDPC 码的异或运算量比 S-LDPC 码的异或运算量多出近 200 次, 相应硬件电路的异或门也多出 200 个。

7 结束语

本文研究不同于单位矩阵 \mathbf{I} 的循环移位置换矩阵, 提出了两种新置换矩阵: \mathbf{D} 矩阵和 \mathbf{Q} 矩阵的构造方法。对这些置换矩阵的共同特征和个别特征进行了描述和分析。设计新置换矩阵的目的有两个: (1) 置换矩阵不仅只有单位矩阵一种, 新置换矩阵为构造 \mathbf{H} 矩阵提供了更多的设计手段和选择方案; (2) 新置换矩阵的丰富性和随机性使基于分块矩阵的 \mathbf{H} 矩阵所定义的 LDPC 码比仅仅基于 \mathbf{I} 矩阵的 \mathbf{H} 矩阵所定义的 LDPC 码有更好的性能。本文的后续研究有待解决的问题是: \mathbf{Q} 矩阵的生成机制问题; 它的快速搜索 \mathbf{Q} 矩阵的优化技术; 何种 \mathbf{Q} 矩阵能使 LDPC 码的性能达到最优?

参 考 文 献

- [1] Gallager R G. Low density parity check codes[Ph. D. dissertation]. Cambridge, MA: Massachusetts Institute of Technology, 1960
- [2] MacKay D J C. Good error-correcting codes based on very sparse matrices. IEEE Transactions on Information Theory, 1999, 45(2): 399-431
- [3] Richardson T, Urbanke R. The capacity of low-density parity check codes under message-passing decoding. IEEE Transactions on Information Theory, 2001, 47(2): 599-618
- [4] Richardson T, Shokrollahi A, Urbanke R. Design of capacity-approaching irregular low-density parity-check codes. IEEE Transactions on Information Theory, 2001, 47(2): 619-637
- [5] Chung S Y, Forney G D, Richardson T J, Urbanke R. On the design of low-density parity-check codes within 0.0045dB of the shannon limit. IEEE Communications Letters, 2001, 5(2): 58-60
- [6] Tanner R M, Sridhara D, Sridharan A, Fuja T E, Costello D J. LDPC block and convolutional codes based on circulant matrices. IEEE Transactions on Information Theory, 2004, 50(12): 2966-2984
- [7] Fossorier M P. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. IEEE Transactions on

- Information Theory, 2004, 50(8): 1788-1793
- [8] Richardson T, Urbanke R. Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, 2001, 47(2): 638-656
- [9] IEEE STD 802.16e-2005 Approved 7 December 2005. Publishing 28 February 2006
- [10] Li Ping, Leung W K, Phamdo Nam. Low density parity check codes with semi-random parity check matrix. Electronics Letters, 1999, 35(1): 38-39
- [11] Peng Li, Zhu Guang-Xi. An exploit of designing encoder for LDPC codes based on Q -matrix. Acta Electronica Sinica, 2005, 33(10): 1734-1740(in Chinese)
(彭立, 朱光喜. 基于 Q -矩阵的 LDPC 码编码器设计. 电子学报, 2005, 33(10): 1734-1740)
- [12] Peng Li, Zhu Guang-Xi, Wu Xiao-Xiao. A designing method of LDPC encoder based on algorithm sequence. Acta Electronica Sinica, 2007, 35(5): 950-954(in Chinese)
(彭立, 朱光喜, 吴晓晓. 基于等差数列的 LDPC 码编码器设计. 电子学报, 2007, 35(5): 950-954)
- [13] Li Zong-Wang, Chen Lei, Zeng Ling-Qi, Lin Shu, Fong W H. Efficient encoding of quasi-cyclic low-density parity-check codes. IEEE Transactions on Communications, 2006, 54(1): 71-82
- [14] Echard R, Chang S C. The π -rotation low-density parity check codes//Proceedings of the IEEE Global Telecommunications Conference. San Antonio, TX, 2001, 2: 980-984
- [15] Frank Kienle, Torben Brack, Norbert When. A synthesizable IP core for DVB-S2 LDPC code decoding//Proceedings of the Design, Automation and Test in Europe Conference. Munich, Germany, 2005: 1530-1535
- [16] Myung Seho, Yang Kyeongcheol, Kim Jaeyoel. Quasi-cyclic LDPC codes for fast encoding. IEEE Transactions on Information Theory, 2005, 51(8): 2894-2901



PENG Li, Ph. D. candidate. Her research interests include information theory, channel coding, wireless transmission technique.

ZHU Guang-Xi, born in 1945, professor, Ph. D. supervisor. His research interests include electronics, signal & information processing, communication and multimedia.

Background

Low-density parity-check (LDPC) codes belong to a class of linear block code in error-correcting code fields. The LDPC codes, discovered by Gallager in early 1960's, were rediscovered in the late 1990s, and have lately attracted a great deal of attention because of showing Shannon-limit-approaching performance and low-complexity parallel decoding architecture. Since their rediscovery, design, construction,

theoretical analyses and applications of these codes have become focal points of research. Especially, code constructions and linear-complexity encoding algorithms were paid attention in error-correcting code fields. Because of breakthrough development of linear encoding algorithm, the encoding and decoding systems of several classes of LDPC codes are introduced in industry standard.