

# 任意列重大围长 QC-LDPC 码的确定性构造

张 轶, 达新宇, 苏一栋

(空军工程大学信息与导航学院, 陕西西安 710077)

**摘 要:** 针对准循环低密度奇偶校验(Quasi-Cyclic Low-Density Parity-Check, QC-LDPC)码中准循环基矩阵的移位系数确定问题, 提出基于等差数列的确定方法. 该方法构造的校验矩阵围长为 8, 列重可任意选取, 移位系数由简单的数学表达式确定, 编码复杂度与码长呈线性关系, 节省了编解码存储空间. 研究结果表明, 列重和围长是影响码字性能的重要因素. 在加性高斯白噪声(Additive White Gauss Noise, AWGN)信道和置信传播(Belief Propagation, BP)译码算法下, 该方法构造的码字在短码时可以获得与 IEEE 802. 11n、802. 16e 码相一致的性能, 在长码时误比特率性能接近 DVB-S2 码. 同时表明该方法对码长和码率参数的设计具有较好的灵活性.

**关键词:** 准循环低密度奇偶校验码; 列重; 围长; 准循环基矩阵; 高效编码

**中图分类号:** TN911. 22

**文献标识码:** A

**文章编号:** 0372-2112 (2016)08-1814-06

**电子学报 URL:** <http://www. ejournal. org. cn>

**DOI:** 10. 3969/j. issn. 0372-2112. 2016. 08. 006

## Deterministic Construction of QC-LDPC Codes for Any Column Weight with a Large Girth

ZHANG Yi, DA Xin-yu, SU Yi-dong

(Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

**Abstract:** To cope with the issue of determining cyclic shift coefficients of the quasi-cyclic sub-matrix in the Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) codes, a method was presented based on the arithmetic progression to compute the cyclic shift coefficients. By this method, a class of girth eight QC-LDPC codes for any column weight is obtained, and the cyclic shift coefficients can be expressed in simple analytic expressions to reduce required memory usage. Meanwhile, the encoding complexity is linearly proportional to code length due to the lower triangular parity matrix. The simulation result shows that column weight and girth have important influences on code performance. Furthermore, over an Additive White Gauss Noise (AWGN) channel and under the Belief Propagation (BP) decoding algorithm, the simulation results represent that bit error rate of the proposed QC-LDPC codes is no less than the LDPC codes in IEEE 802. 11n and 802. 16e with short code length, and is close to the LDPC codes in DVB-S2 with long code length. Moreover, the study result also confirms that the proposed algorithm has high flexibility with respect to the design of code length and rate.

**Key words:** quasi-cyclic low-density parity-check (QC-LDPC) codes; column weight; girth; quasi-cyclic sub-matrix; efficient encoding

## 1 引言

码的结构决定了低密度奇偶校验(Low-Density Parity-Check, LDPC)码的性能. 基于循环移位矩阵构造的 QC-LDPC 码, 其校验矩阵的准循环特性使其易于高效编解码, 码的代数结构为超大规模集成电路的实现提供了可能, 因此受到广泛关注和研究. 围长是码中最小的环长度, 增大围长可以提高码字的性能. 借助于计算

机搜索, 人们已经提出了一些围长大于 6 的 QC-LDPC 码构造方法<sup>[1-6]</sup>, 但为了满足各种约束条件, 这些准随机方法通常花费时间长、存在失败可能, 且对编解码存储空间提出了更高要求.

针对上述问题, 国内外学者对确定性构造方法的研究屡有成果涌现. Tanner<sup>[7]</sup>和 Zhang Fan<sup>[8]</sup>分别采用群结构法、3 维循环网络法构造出了围长在 10 以上的 QC-LDPC 码, 但是校验矩阵的行重只局限于特定范围

内;Zhang Guo-hua<sup>[9]</sup>提出了基于二次函数的确定性方法,但方程系数与行重有关,任意行重只能构造两种校验矩阵;张国华<sup>[10-12]</sup>基于贪婪算法构造了围长为 8 的 QC-LDPC 码,其循环移位矩阵尺寸具有连续变化的优点,但该方法要求准循环基矩阵首行首列元素必须为 0;Zhang Jian-hua<sup>[13]</sup>首次提出任意列重的构造方法,然而固定码参数下的校验矩阵形式是唯一的.此外,以上方法均未考虑由校验矩阵直接编码的方案,这在一定程度上限制了它们的实际应用.

在此基础上,本文提出一种构造任意列重、围长为 8 的 QC-LDPC 码确定性方法.首先构造了列重为 4 的基矩阵,分析了其围长特性;通过总结推导将特殊情形推广,进而提出任意列重的确定性构造方法,并证明了该码的围长至少为 8;然后利用特殊的子矩阵结构实现了由校验矩阵进行迭代编码,降低了编码复杂度;最后通过软件仿真,验证了该方法构造的 QC-LDPC 码参数设置灵活、性能优良.

## 2 QC-LDPC 码

QC-LDPC 码的校验矩阵以单位阵的循环移位阵和零方阵为子阵,可表示为

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}(p_{11}) & \mathbf{I}(p_{12}) & \cdots & \mathbf{I}(p_{1j}) \\ \mathbf{I}(p_{21}) & \mathbf{I}(p_{22}) & \cdots & \mathbf{I}(p_{2j}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}(p_{i1}) & \mathbf{I}(p_{i2}) & \cdots & \mathbf{I}(p_{ij}) \end{bmatrix} \quad (1)$$

其中: $\mathbf{I}(p_{ij})$ 表示一个  $p \times p$  的循环移位矩阵.把循环右移系数  $p_{ij}$  写成一个矩阵  $\mathbf{P}$ ,称为准循环基矩阵,如式(2)所示<sup>[14]</sup>:

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1j} \\ p_{21} & p_{22} & \cdots & p_{2j} \\ \vdots & \vdots & \ddots & \vdots \\ p_{i1} & p_{i2} & \cdots & p_{ij} \end{bmatrix} \quad (2)$$

在基矩阵  $\mathbf{P}$  中,若干个节点(元素) $p_1, p_2, \dots, p_{2k}$  构成一个环,则对应的  $\mathbf{H}$  矩阵也存在与之对应的  $p$  个同样大小的环.显然,环的长度只能是大于或等于 4 的偶数.表示  $\mathbf{H}$  中长为  $2k$  环的序列 $(p_1, p_2, \dots, p_{2k})$  满足如下定理:

**定理 1**<sup>[15]</sup> 对于基矩阵  $\mathbf{P}$  中的序列 $(p_1, p_2, \dots, p_{2k})$ ,其中  $p_i$  和  $p_{i+1}$  在同一行或同一列,  $p_i$  和  $p_{i+2}$  在不同行且不同列,则 $(p_1, p_2, \dots, p_{2k})$  构成长为  $2k$  环的充要条件是

$$\sum_{i=1}^{2k} (-1)^i p_i \equiv 0 \pmod{p} \quad (3)$$

短环的存在使 LDPC 码在译码时不能快速收敛,造成误比特率(Bit Error Rate, BER)性能变差.因此,为了使校验矩阵不含长为  $2k$  的环,就必须通过某种设计,使得式(3)不成立.图 1 给出了 6 环存在的六种形状.

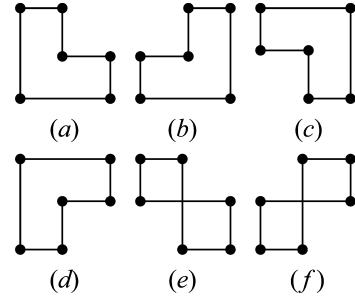


图1 六种形状的6环

## 3 构造方法

将校验矩阵  $\mathbf{H}$  分为校验部分  $\mathbf{H}_a$  和信息部分  $\mathbf{H}_b$ , 如式(4)所示:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I}(p_{1,2}) & \cdots & \mathbf{I}(p_{1,m}) & \mathbf{I}(p_{1,m+1}) & \mathbf{I}(p_{1,m+2}) & \cdots & \mathbf{I}(p_{1,n}) \\ \mathbf{0} & \mathbf{I} & \cdots & \mathbf{I}(p_{2,m}) & \mathbf{I}(p_{2,m+1}) & \mathbf{I}(p_{2,m+2}) & \cdots & \mathbf{I}(p_{2,n}) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{I}(p_{m,m+1}) & \mathbf{I}(p_{m,m+2}) & \cdots & \mathbf{I}(p_{m,n}) \end{bmatrix} \quad (4)$$

$\mathbf{H}_a$   $\mathbf{H}_b$

其中,  $\mathbf{H}_a$  为下三角结构,大小为  $mp \times mp$ ,主对角线由单位阵构成,  $\mathbf{0}$  表示零矩阵;  $\mathbf{H}_b$  大小为  $mp \times kp$  ( $k = n - m$ ).

首先考虑一种  $(4, n)$  基矩阵  $\mathbf{P}$  的配置方式:

$$p_{1,j+1} - p_{1,j} = d_1 > 0, 1 \leq j < n \quad (5)$$

$$p_{2,j+1} - p_{2,j} = d_2 > d_1, 2 \leq j < n \quad (6)$$

$$p_{3,j+1} - p_{3,j} = \max[(n-j) \cdot (d_2 - d_1) + d_1 + 1, (j-1) \cdot (d_2 - d_1) + d_1 + 1], 3 \leq j < n \quad (7)$$

$$p_{4,j+1} - p_{4,j} = p_{3,j+1} - p_{3,j} + 1, 4 \leq j < n \quad (8)$$

显然  $\mathbf{P}$  中第 1、2 行元素分别构成单增等差数列. 首先证明一些引理.

**引理 1**  $\mathbf{P}$  中无 4 环.

**证明** 由式(5)~式(8),对任意  $4 \leq i < j \leq n$ ,有

$$p_{4,j} - p_{4,i} > p_{3,j} - p_{3,i} > p_{2,j} - p_{2,i} > p_{1,j} - p_{1,i} > 0 \quad (9)$$

同理对任意  $2 \leq i < j \leq n$ ,  $\mathbf{P}$  中均不存在 4 环.

**引理 2**  $\mathbf{P}$  中无图 1(a)~(d)所示 6 环.

**证明** 根据引理 1 的证明过程,引理 2 显然成立.

**引理 3**  $\mathbf{P}$  中无图 1(e)~(f)所示 6 环.

**证明** 令  $\mathbf{P}$  中第  $x, y, z$  行 ( $1 \leq x, y, z \leq 4$ ) 构成的矩阵为  $\mathbf{P}(x, y, z)$ . 考虑  $\mathbf{P}(1, 2, 3)$  和图 1(e) 的情形,不失一般性,令  $2 \leq i < l < j \leq n$ .

$$\begin{aligned} & \text{由式(7)可得 } p_{3,j} - p_{3,i} \geq (d_2 - d_1) \cdot l + d_1 + 1, \text{ 故} \\ & (p_{3,j} - p_{3,i}) + (p_{1,l} - p_{1,i}) + (p_{2,i} - p_{2,j}) \\ & \geq (d_2 - d_1) \cdot l + d_1 + 1 + (l - i) \cdot d_1 + (i - j) \cdot d_2 \\ & = (d_2 - d_1) \cdot (i - 1) + 1 > 0 \end{aligned} \quad (10)$$

因此  $P(1,2,3)$  中无图 1(e) 所示 6 环, 同理也不存在图 1(f) 所示 6 环. 采用相同的分析方法易知  $P(1,2,4)$ 、 $P(1,3,4)$  和  $P(2,3,4)$  的中均无 6 环.

将其推广至任意列重的基矩阵, 令  $d_{i,j} = p_{i,j+1} - p_{i,j}$ ,  $1 \leq i \leq m, i \leq j < n$ , 具体构造方法为:

(1) 当  $m \leq 4$  时, 按照式(5) ~ 式(8)配置  $P$ .

(2) 当  $m > 4$  时, 设

$$d_{4k+1,j} = p_{4k-1,n} - (n-4k) \cdot d_1 + 1, k \geq 1 \quad (11)$$

$$d_{2k+2,j} = d_{2k+1,j} + 1, k \geq 2 \quad (12)$$

$$d_{4k+3,j} = \max(d_{4k+1,j} + n - j + 1, d_{4k+1,j} + j - 4k), k \geq 1 \quad (13)$$

**引理 4**  $(m,n)$  基矩阵  $P$  中无 6 环.

**证明** 不失一般性, 令  $1 \leq r < s < t \leq m, 2 \leq i < l < j \leq n$ . 不妨设  $m = 4w (w \geq 3)$ , 则基矩阵  $P$  可由  $w$  个  $(4,n)$  子矩阵构成, 因此行指数  $r, s, t$  存在以下 4 种关系: ①  $r < 4k+1 \leq s \leq 4k+4 < t, 1 \leq k \leq w-2$ ; ②  $4k+1 \leq r < s < t \leq 4k+4, 0 \leq k \leq w-1$ ; ③  $4k+1 \leq r < s \leq 4k+4 < t, 0 \leq k \leq w-2$ ; ④  $r < 4k+1 \leq s < t \leq 4k+4, 1 \leq k \leq w-1$ .

考虑关系①和图 1(e) 的情形, 注意到此时  $4k+1 \leq i \leq 4k+4$ , 得到:

$$\begin{cases} \min(p_{t,j} - p_{t,i}) = (j-l) \cdot d_{4k+5,l} \\ \quad = p_{4k+3,n} - (n-4k-4) \cdot d_1 + 1 \\ \max(p_{s,j} - p_{s,i}) = p_{4k+4,n} \\ \min(p_{r,l} - p_{r,i}) = (l-i) \cdot d_1 \\ \quad = (n-4k-5) \cdot d_1 \end{cases} \quad (14)$$

因此有

$$\begin{aligned} & (p_{t,j} - p_{t,i}) + (p_{r,l} - p_{r,i}) + (p_{s,i} - p_{s,j}) \\ & \geq p_{4k+3,n} - (n-4k-4) \cdot d_1 + 1 + (n-4k-5) \\ & \quad \cdot d_1 - p_{4k+4,n} \\ & = p_{4k+3,n} - p_{4k+4,n} - d_1 + 1 \end{aligned} \quad (15)$$

由式(12)易知

$$p_{4k+4,n} = p_{4k+3,n} - p_{4k+3,4k+4} + (n-4k-4) \quad (16)$$

再由式(13)可得:

$$\begin{aligned} p_{4k+3,4k+4} & = d_{4k+3,4k+3} \\ & = d_{4k+1,4k+3} + n - 4k - 2 \end{aligned} \quad (17)$$

将式(16)、式(17)代入式(15)可知其结果大于 0. 同理可得, 当行指数满足关系②、③、④, 以及  $m$  为任意值时引理 4 成立. 证毕.

根据引理 1 ~ 4 可得到定理 2.

**定理 2** 对于任意列重  $m$ 、任意行重  $n$ , 由式(4) ~ 式(8)、式(11) ~ 式(13)定义的基矩阵  $P$  的围长至少为 8.

可以发现, 基矩阵  $P$  的第  $4k+1, 4k+2 (k \geq 0)$  行元

素均构成单增等差数列; 当初始值  $m, n, d_1, d_2$  确定后, 移位系数可由数学公式计算得到; 本文方法参数设置灵活, 而移位矩阵的维数  $p$  大于移位系数, 故  $p$  的取值下界为

$$\inf p = \max(p_{i,n}) + 1, 1 \leq i \leq m \quad (18)$$

**例 1** 利用本文方法设计的一种  $(6,8)$  基矩阵如式(19)所示:

$$P = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & 0 & 2 & 4 & 6 & 8 & 10 & 12 \\ & & 0 & 7 & 13 & 19 & 26 & 34 \\ & & & 0 & 7 & 14 & 22 & 31 \\ & & & & 0 & 31 & 62 & 93 \\ & & & & & 0 & 32 & 64 \end{bmatrix} \quad (19)$$

## 4 编码复杂度分析

由式(4)易知  $H_a$  满秩, 因此  $H$  是非奇异的, 即可回避生成矩阵  $G$  而直接由校验矩阵进行编码.

采用 LU 分解法, 令信息比特向量为  $s = [s_1 s_2 \cdots s_k]$ , 校验比特向量为  $p = [p_1 p_2 \cdots p_m]$ , 编码器输出向量为  $c$ , 它的长度  $N = np = (m+k)p$ , 则有

$$c = [p \quad s] \quad (20)$$

根据校验等式  $H \cdot c^T = 0$  可得:

$$H_a \cdot p^T + H_b \cdot s^T = 0 \quad (21)$$

由于运算在  $GF(2)$  中进行, 所以有

$$\begin{aligned} & \begin{bmatrix} I(p_{1,m+1}) & I(p_{1,m+2}) & \cdots & I(p_{1,n}) \\ I(p_{2,m+1}) & I(p_{2,m+2}) & \cdots & I(p_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ I(p_{m,m+1}) & I(p_{m,m+2}) & \cdots & I(p_{m,n}) \end{bmatrix} \begin{bmatrix} s_1^T \\ s_2^T \\ \vdots \\ s_k^T \end{bmatrix} \\ & = \begin{bmatrix} I & I(p_{1,2}) & \cdots & I(p_{1,m}) \\ 0 & I & \cdots & I(p_{2,m}) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & I \end{bmatrix} \begin{bmatrix} p_1^T \\ p_2^T \\ \vdots \\ p_m^T \end{bmatrix} \end{aligned} \quad (22)$$

将式(22)展开由第  $m$  式可得:

$$p_m^T = \sum_{j=1}^k H_b(m, j) \cdot s_j^T \quad (23)$$

将式(23)回代到方程组式(22)的第  $m-1$  式可得:

$$p_{m-1}^T = \sum_{j=1}^k H_b(m-1, j) \cdot s_j^T + I(p_{m-1,m}) \cdot p_m^T \quad (24)$$

依次类推可得到各个  $p_i$ , 代入到式(20), 编码完毕.

编码复杂度主要关注编码过程的运算量、运算复杂度和编码所需存储的参数. 运算量即乘法和加法次数, 运算复杂度即运算量与码长的变化关系. QC-LDPC 码的各个子矩阵都是稀疏矩阵, 因此按照稀疏矩阵的运算方式可大大减小运算量. 现计算  $p_i$  的运算量如表 1

所示.

表 1 编码算法的运算量

	乘法次数	加法次数
$p_i (1 \leq i \leq m)$	$N - i \cdot p$	$N - (i + 1) \cdot p$

从表 1 可明显地看到,计算各个校验分向量  $p_i$  的运算复杂度为  $O(N)$ ,即运算复杂度与码长呈线性关系.同时由于该码采用代数构造法,校验矩阵中的元素由简单的数学运算得到,只需要存储一组初始参数和几个数学表达式即可,编码器的实际存储量需求非常小.

## 5 仿真与实验

### 5.1 最小码重、码距分析

一般认为码重小于 10 的码为低码重码<sup>[16]</sup>,这类码的存在使 LDPC 译码器纠错能力低下.目前尚没有办法准确求出码字的最小码重,本文采用文献[16]给出的搜索算法,即通过生成矩阵的行向量估计 LDPC 码的最小码重和最小码距的上界.仿真选取 4 种码字,基矩阵尺寸分别为  $(4, 8)$ ,  $(4, 12)$ ,  $(5, 10)$ ,  $(6, 12)$ , 初始参数均为  $d_1 = 1, d_2 = 2$ . 各码字码长及码重分布情况如图 2 所示,计算机搜索得到的最小码重、最小码距的上界如表 2 所示.

表 2 最小码重、最小码距搜索结果

	$(4, 8)$	$(4, 12)$	$(5, 10)$	$(6, 12)$
最小码重 $w_{\min}(c) \leq$	14	14	28	54
最小码距 $d_{\min}(c) \leq$	22	22	46	78

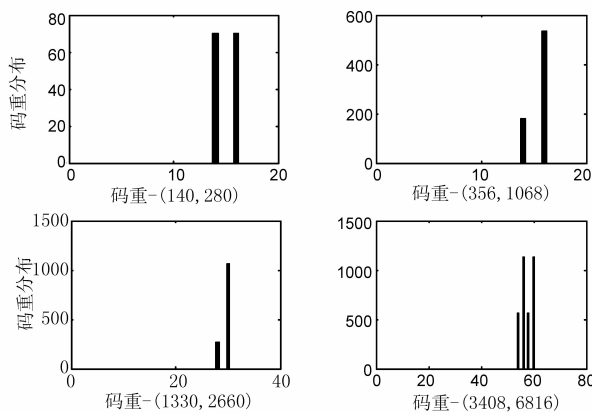


图 2 4种码字的码重分布

仿真结果表明,  $(4, 8)$  和  $(4, 12)$  两种基矩阵下其最小码重的上界均为 14, 这是因为两种校验矩阵的列重结构是一样的, 都包含 4 种列重, 而  $(4, 12)$  中小列重的比例更小, 因此码重为 16 的行向量所占比重较大; 随着列重的增大, LDPC 码的最小码重和码距也增大, 因此校验矩阵使用大的列重可减小产生低码重码的可能性.

### 5.2 性能分析

IEEE 802. 11n、802. 16e 以及 DVB-S2 标准中均采

用准双对角线子矩阵实现迭代编码, 与本文设计的方法类似, 故与这 3 种码字进行性能比较. 仿真环境为加性高斯白噪声 (AWGN) 信道, 译码采用置信传播 (BP) 算法, 最大迭代次数为 30, 调制方式为 BPSK.

**实验 1** 与 IEEE 802. 11n、802. 16e 标准 LDPC 码的比较

根据 IEEE 802. 11n 标准选择 2 种参数的基矩阵: 维数  $p = 27$ , 码长  $N = 648$ , 码率  $R = 1/2$ ; 维数  $p = 54$ , 码长  $N = 1296$ , 码率  $R = 2/3$ . 利用本文方法构造同码长码率的 2 种基矩阵分别为: 维数  $p = 81, d_1 = 5, d_2 = 7$ ; 维数  $p = 108, d_1 = 3, d_2 = 4$ . 仿真结果如图 3 所示.

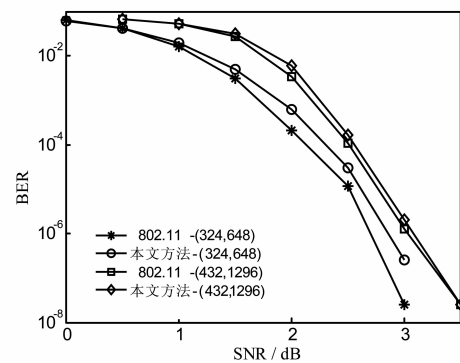


图 3 与 IEEE 802.11n 标准 LDPC 码的比较

根据 IEEE 802. 16e 标准选择 2 种参数的基矩阵: 维数  $p = 24$ , 码长  $N = 576$ , 码率  $R = 1/2$ ; 维数  $p = 48$ , 码长  $N = 1152$ , 码率  $R = 2/3$  B 类. 利用本文方法构造同码长码率的 2 种基矩阵分别为: 维数  $p = 72, d_1 = 3, d_2 = 5$ ; 维数  $p = 96, d_1 = 1, d_2 = 2$ . 仿真结果如图 4 所示.

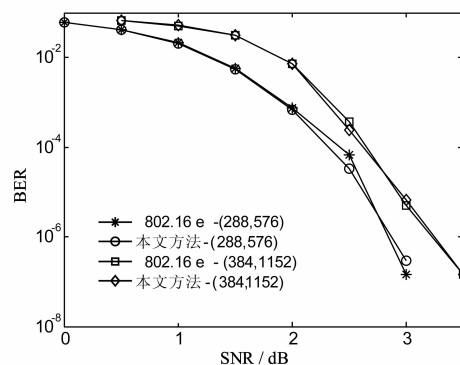


图 4 与 IEEE 802.16e 标准 LDPC 码的比较

仿真结果表明, 在中短码条件下, 本文构造的码字与 IEEE 802. 11n、802. 16e 标准的 LDPC 码相比 BER 性能相一致. 从仿真参数可以看到, 本文给出的校验矩阵的列重显然比上述两类标准的要小, 即最小码重更小, 然而 BER 性能却并未由此下降, 说明大围长特性促进了该部分的性能增益, 验证了理论推导的正确性. 此外, IEEE 802. 11n、802. 16e 标准的 LDPC 码分别只提供了 4

种和 6 种基矩阵形式,不同码率下需要存储不同的移位系数,随着通信技术的不断发展在实际应用中难免受到约束.而本文方法可根据需求灵活地设置初始参数,校验矩阵由数学公式自动计算得到,大大节省了编解码存储空间,校验矩阵形式也更加多样化.

### 实验 2 与 DVB-S2 标准 LDPC 码的比较

DVB-S2 标准中的 LDPC 码只有两种码长,即使短码也长达 16200 bit,这对于编解码器的实现具有较大的难度,故采用文献[17]中的缩短码设计,选择 2 种码率  $R=1/2$  的基矩阵,码长分别为 5400 和 8100.利用本文方法构造同码长码率的 2 种基矩阵分别为:维数  $p=540, d_1=11, d_2=13$ ; 维数  $p=675, d_1=16, d_2=17$ ; 仿真结果如图 5 所示.

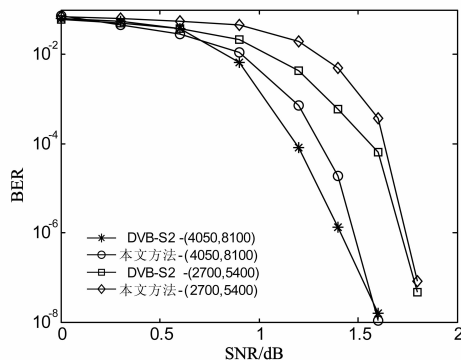


图5 与DVB-S2标准LDPC码的比较

仿真结果表明, DVB-S2 标准的 LDPC 码比本文构造的码字性能略优.这是因为该标准下校验矩阵的最大列重为 8, 在长码条件下的性能增益会更凸显, 而本文设计的码字在无列重优势的情况下, BER 性能已经可以与之接近.另外, 与 IEEE 802.11n、802.16e 标准类似, DVB-S2 标准针对不同码率规定了不同的编码信息表, 同样可能存在编码器存储与应用范围受限等问题.综上所述, 本文构造码字不失为一种好码.

## 6 结论

本文提出了一种构造围长至少为 8 的  $(m, n)$  QC-LDPC 码的确定性方法. 该码的准循环基矩阵由数学表达式确定, 构造方法简单, 节省了编解码存储空间, 校验矩阵可直接进行迭代编码, 降低了编码复杂度. 研究结果表明, 这类码只需少量的初始值控制就可设计任意参数的基矩阵, 同时在 AWGN 信道中能够获得较好的纠错能力, 因此对信道编码理论的研究和应用具有一定的参考价值. 在此方法基础上, 如何构造围长大于 8 的 QC-LDPC 码是今后深入研究的内容之一.

### 参考文献

[1] O'Sullivan M E. Algebraic construction of sparse matrices

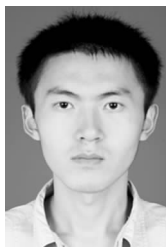
with large girth[J]. IEEE Transactions on Information Theory, 2006, 52(2): 718–727.

- [2] Jiang X, Lee M H. Large girth non-binary LDPC codes based on finite fields and Euclidean geometries[J]. IEEE Signal Processing Letters, 2009, 16(6): 521–524.
- [3] Huang Jen-Fa, Huang Chun-Ming, Yang Chao-Chin. Construction of one-coincidence sequence quasi-cyclic LDPC codes of large girth[J]. IEEE Transactions on Information Theory, 2012, 58(3): 1825–1836.
- [4] Zhang Guo-hua, Sun Rong, Wang Xin-mei. Construction of girth-eight QC-LDPC codes from greatest common divisor[J]. IEEE Communications Letters, 2013, 17(2): 369–372.
- [5] Park H, Hong S, NO J S, et al. Design of multiple-edge protographs for QC LDPC codes avoiding short inevitable cycles[J]. IEEE Transactions on Information Theory, 2013, 59(7): 4598–4614.
- [6] Wang Ju-hua, Zhang Guo-hua, Zhou Quan. Coset-based QC-LDPC codes without small cycles[J]. Electronics Letters, 2014, 50(22): 1597–1598.
- [7] Kim S, NO J S, Chung H, et al. On the girth of tanner (3, 5) quasi-cyclic LDPC codes[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1739–1744.
- [8] Zhang Fan, Mao Xue-hong, Zhou Wu-yang, et al. Girth-10 LDPC codes based on 3-D cyclic lattices[J]. IEEE Transactions on Vehicular Technology, 2008, 57(2): 1049–1060.
- [9] Zhang Guo-hua, Sun Rong, Wang Xin-mei. Deterministic construction of girth-eight (3, L) QC-LDPC codes from quadratic function[J]. Electronics Letters, 2013, 49(9): 600–602.
- [10] 张国华, 陈超, 杨洋, 等. Girth-8 (3, L)-规则 QC-LDPC 码的一种确定性构造方法[J]. 电子与信息学报, 2010, 32(5): 1152–1156.  
Zhang Guo-hua, Chen Chao, Yang Yang, et al. Girth-8 (3, L)-regular QC-LDPC codes based on novel deterministic design technique[J]. Journal of Electronics & Information Technology, 2010, 32(5): 1152–1156. (in Chinese)
- [11] Zhang Guo-hua, Sun Rong, Wang Xin-mei. Several explicit constructions for (3, L) QC-LDPC codes with girth at least eight[J]. IEEE Communications Letters, 2013, 17(9): 1822–1825.
- [12] 张国华, 孙蓉, 王新梅. 围长至少为 8 的 QC-LDPC 码的新构造: 一种显示框架[J]. 电子学报, 2012, 40(2): 331–337.  
Zhang Guo-hua, Sun Rong, Wang Xin-mei. Novel constructions of QC-LDPC codes with girth at least eight; an explicit framework[J]. Acta Electronica Sinica, 2012, 40

- (2):331–337. (in Chinese)
- [13] Zhang Jian-hua and Zhang Guo-hua. Deterministic girth-eight QC-LDPC codes with large column weight [J]. IEEE Communications Letters, 2014, 18(4):656–659.
- [14] 郑健, 别红霞, 类春阳, 等. 优化循环转移矩阵偏移量的 QC-LDPC 码构造 [J]. 北京邮电大学学报, 2014, 37(1):16–19.  
Zheng Jian, Bie Hong-xia, Lei Chun-yang, et al. A construction algorithm with optimized shift value of circulant permutation matrix for QC-LDPC codes [J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(1):16–19. (in Chinese)
- [15] Fossorier M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices [J]. IEEE Transactions on Information Theory, 2004, 50(8):1788–1793.
- [16] 肖扬. Turbo 与 LDPC 编解码及其应用 [M]. 北京:人民邮电出版社, 2010.  
Xiao Yang. Turbo and LDPC Codes and Their Applications [M]. Posts & Telecom Press, Beijing, 2010. (in Chinese)
- [17] 肖扬, 范俊, 黄希. DVB-S2 标准的 LDPC 码改进 [J]. 铁道学报, 2011, 33(2):52–59.

Xiao Yang, FAN Jun, HUANG Xi. Improvement in LDPC codes in DVB-S2 standard [J]. Journal of The China Railway Society, 2011, 33(2):52–59. (in Chinese)

#### 作者简介



张 轶 男, 1986 年 10 月出生, 山西太原人. 空军工程大学信息与导航学院博士研究生, 从事信道编码理论方面的有关研究.  
E-mail: zhangyi1290@163.com



达新宇 男, 1961 年 4 月出生, 陕西眉县人. 教授、博士生导师、国家精品课程《通信原理》负责人. 1983 年、1988 年和 2007 年分别在西安电子科技大学、空军地空导弹学院和西北工业大学获工学学士、工学硕士和工学博士学位. 现为空军工程大学信息与导航学院教授, 主要从事卫星通信、信道编码、认知无线电等方面的研究工作.