利用等差数列构造大围长准循环低密度奇偶校验码

张 轶* 达新宇 苏一栋 (空军工程大学信息与导航学院 西安 710077)

摘 要: 针对准循环低密度奇偶校验(QC-LDPC)码中准循环基矩阵的移位系数确定问题,该文提出基于等差数列 (AP)的确定方法。该方法构造的校验矩阵的围长至少为8,移位系数由简单的数学表达式确定,节省了编解码存储 空间。研究结果表明,该方法对码长和码率参数的设计具有较好的灵活性。同时表明在加性高斯白噪声(AWGN) 信道和置信传播(BP)译码算法下,该方法构造的码字在码长为1008、误比特率为10⁻⁵时,信噪比优于渐进边增长 (PEG)码近 0.3 dB。 关键词:准循环低密度奇偶校验码;等差数列;围长;准循环基矩阵

文章编号: 1009-5896(2015)02-0394-05 中图分类号: TN911.22 文献标识码: A DOI: 10.11999/JEIT140538

Construction of Quasi-cyclic Low-density Parity-check Codes with a Large Girth Based on Arithmetic Progression

Zhang Yi Da Xin-yu Su Yi-dong

(Information and Navigation College, Air Force Engineering University, Xi'an 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 is presented based on the Arithmetic Progression (AP) to compute the cyclic shift coefficients. By this method, the girth of its Tanner graph is at least eight, and the cyclic shift coefficients can be expressed in simple analytic expressions to reduce required memory usage. The simulation results show that the proposed algorithm has high flexibility with respect to the design of code length and rate. Furthermore, over an Additive White Gauss Noise (AWGN) channel and under the Belief Propagation (BP) decoding algorithm, the simulation result also represents that the SNR of the proposed QC-LDPC codes is better than the Progressive Edge-Growth (PEG) codes close to 0.3 dB at the code length of 1008 and BER performance of 10^{-5} .

Key words: Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) codes; Arithmetic Progression (AP); Girth; Quasi-cyclic sub-matrix

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 构造的准循环低密度奇偶检验 (Quasi-Cyclic Low-Density Parity-Check, 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[1-7],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

2014-04-24 收到, 2014-07-25 改回

国家自然科学基金(60972042, 61271250)资助课题

*通信作者: 张轶 zhangyi1290@163.com

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。文献[8]和文献[9]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; 文献[10-12]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; 文献[13]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。这在一定程度上限制了它们的实际 应用。

在此基础上,本文利用等差数列提出一种列重 为3、围长至少为8的QC-LDPC码构造方法。首 先通过举例归纳得到约束条件,总结出推导思路和 方法; 然后将特殊情形推广, 进而提出基于一般等 差数列的确定性构造方法,并证明了其围长特性;

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 码是一类非常特殊的高度结构化的 LDPC 码,它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

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

其中: $I(p_{ij})$ 表示一个 $p \times p$ 的循环移位矩阵, $p_{ij} \in \{0,1,2,\dots,p-1,\infty\}$ 。易知I(0) 就是单位阵 $I_{p\times p}$, 零方阵用 $I(\infty)$ 表示。把循环右移系数 p_{ij} 写成一个 矩阵P,称为准循环基矩阵,如式(2)所示^[14]。当P确定后,校验矩阵H也随之确定。

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

在基矩阵 P 中,若干个点(元素) p_1, p_2, \dots, p_{2k} 构成一个环,则对应的 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 H 中长为 2k 环的序列(p_1, p_2, \dots, p_{2k})满足定理 1。

定理 1^[15] 对于基矩阵 **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环的充分必要条件是

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

短环的存在使 LDPC 码在译码时不能快速收 敛,甚至不能收敛,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 6 种形状。



3 基于等差数列的确定性构造

3.1 归纳推导

对列重为 3 的校验矩阵的基矩阵采取的配置方 式为

$$p_{m,j} = m \cdot j, \ m \in \{1,2\}, \ 1 \le j \le n$$
 (4)

$$\Delta_j = p_{3,j+1} - p_{3,j}, \quad 1 \le j \le n - 1 \tag{5}$$

其中 n 为基矩阵的列数。显然,此时 { $p_{1,j}$ } 为正整数 列, { $p_{2,j}$ } 为正偶数列。对 $p_{3,2}$ 进行赋值时,为避免 出现短环,则 Δ_1 应满足:

 $\Delta_1 \ge (p_{2,n} - p_{2,1}) - (p_{1,n} - p_{1,2}) + 1 = n + 1$ (6) 依此类推,可以得到满足围长至少为 8 的 $\{\Delta_j\}$ 的取 值下界,如表 1 所示。

表1 $n = 6 \sim 9$ 时 { Δ_i } 的取值下界

n	$\inf\{\Delta_j\}$	
6	$\{7, 6, 5, 6, 7\}$	
7	$\{8, 7, 6, 6, 7, 8\}$	
8	$\{9, 8, 7, 6, 7, 8, 9\}$	
9	$\{10,9,8,7,7,8,9,10\}$	

观察表 1 可以发现: 若 *n* 为奇数, $1 \le j \le \frac{n-1}{2}$ 时 inf{ Δ_j } 为单减等差数列, $\frac{n-1}{2} < j \le n-1$ 时 inf{ Δ_j } 为单增等差数列, $j = \frac{n-1}{2}$ 时 Δ_j 可取到最 小值: 若 *n* 为偶数, $1 \le j \le \frac{n}{2}$ 时 inf{ Δ_j } 为单减等 差数列, $\frac{n}{2} < j \le n-1$ 时 inf{ Δ_j } 为单增等差数列, $j = \frac{n}{2}$ 时 Δ_j 可取到最小值。综上分析, 并根据等差 数列性质得到 Δ_i 的约束条件为

$$n 为奇数, \Delta_{j} \ge \begin{cases} (n+1) + (j-1) \cdot (-1) \\ = n - j + 2, \quad 1 \le j \le \frac{n-1}{2} \\ \left(n - \frac{n-1}{2} + 2\right) + \left[\left(j - \frac{n-1}{2}\right) - 1\right]^{\binom{n}{2}} \\ = j + 2, \quad \frac{n-1}{2} < j \le n-1 \end{cases}$$
$$\binom{(n+1) + (j-1) \cdot (-1)}{= n - j + 2, \quad 1 \le j \le \frac{n}{2}} \\ \left(n - \frac{n}{2} + 2 + 1\right) + \left[\left(j - \frac{n}{2}\right) - 1\right] \\ = j + 2, \quad \frac{n}{2} < j \le n-1 \end{cases}$$
(8)

3.2 构造方法

上节的结论是基于一种特例推导给出的。若采 取相同的分析方法,将式(4)推广至一般等差数列, 则得到一种(3,*n*)基矩阵的构造方法为

$$p_{1,j} = p_{1,1} + (j-1) \cdot d_1, \quad 1 \le j \le n \tag{9}$$

 $p_{2,j} = p_{2,1} + (j-1) \cdot d_2, \quad 1 \le j \le n \tag{10}$

$$d_2 > d_1 \ge 0 \tag{11}$$

$$p_{3,j+1} - p_{3,j} \ge \max\left[(n-j) \cdot (d_2 - d_1) + d_1 + 1, \\ (d_2 - d_1) \cdot j + d_1 + 1\right], \ 1 \le j \le n - 1 \ (12)$$

其中 d1, d2 分别为两个等差数列的公差。

4 围长至少为 8 的性质证明

定理 2 对于任意 *n* ≥ 3,满足式(9)~式(12)定 义的基矩阵 **P** 的围长至少为 8。

- 证明 围长至少为8即不存在4环和6环。
- (1)4 环检验 不失一般性, 令1≤s<t≤n。
 若 **P** 中存在4环,则满足式(13)中的至少一项

$$\begin{aligned} & (p_{2,t} - p_{2,s}) + (p_{1,s} - p_{1,t}) = 0 \mod p \\ & (p_{3,t} - p_{3,s}) + (p_{1,s} - p_{1,t}) = 0 \mod p \\ & (p_{3,t} - p_{3,s}) + (p_{2,s} - p_{2,t}) = 0 \mod p \end{aligned}$$
 (13)

这是不可能的,因为当 n 为奇数时,

$$(p_{3,s+1} - p_{3,s}) - (p_{2,s+1} - p_{2,s}) \geq \min \Delta_s - d_2 = \left(n - \frac{n-1}{2}\right) (d_2 - d_1) + d_1 + 1 - d_2 = \frac{n-1}{2} (d_2 - d_1) + 1 > 0$$
 (14)

当 n 为偶数时,同理可得

$$(p_{3,s+1} - p_{3,s}) - (p_{2,s+1} - p_{2,s}) \ge \left(\frac{n}{2} - 1\right) (d_2 - d_1) + 1 > 0$$
(15)

因此有

$$p_{3,t} - p_{3,s} = p_{3,t} - p_{3,t-1} + p_{3,t-1} - p_{3,t-2} + \dots + p_{3,s+1} - p_{3,s}$$

$$> p_{2,t} - p_{2,t-1} + p_{2,t-1} - p_{2,t-2} + \dots + p_{2,s+1} - p_{2,s}$$

$$(16)$$

$$= p_{2,t} - p_{2,s} > p_{1,t} - p_{1,s}$$
(16)

注意到 0 < p_{3,s} - p_{3,t} 2,s</sub> - p_{2,t} < p, 故式 (13)不成立。因此, **P**中不存在 4 环。

(2)6 环检验 不失一般性,
$$(1 \le i < k < j \le n)$$
。
若 P 中存在图 1(a)所示 6 环, 则

$$(p_{1,i} - p_{1,k}) + (p_{2,k} - p_{2,j}) + (p_{3,j} - p_{3,i}) = 0 \mod p$$
 (17)
这是不可能的,因为由 4 环检验的结论,有

$$p_{3,j} - p_{3,i} = p_{3,j} - p_{3,k} + p_{3,k} - p_{3,i}$$

> $p_{2,j} - p_{2,k} + p_{1,k} - p_{1,i}$ (18)

故式(17)不成立,同理可证 **P**中也不存在图 1(b)~ 图 1(d)所示 6 环。 下面考虑图 1(e)的情形:

由 { p_{3,i} } 为单增数列可得

$$(p_{3,j} - p_{3,k}) + (p_{1,k} - p_{1,i}) + (p_{2,i} - p_{2,j}) > (j-k) \cdot \min \Delta_j + (k-i) \cdot d_1 + (i-j) \cdot d_2 = (j-k) \cdot \left[\frac{n+1}{2} \cdot (d_2 - d_1) + d_1 + 1\right] + k \cdot d_1 + (d_2 - d_1) \cdot i - j \cdot d_2 \geq (d_2 - d_1) \cdot (n-k-1+i) + 2 > 0$$
(20)

因此 **P** 中不存在图 1(e) 所示 6 环,同理也不存在图 1(f) 所示 6 环。

综上,基矩阵 **P** 的围长至少为 8。 证毕 利用等差数列求和公式可求出 p_{3,n} 的通项表达 式。

当 n 为奇数时,

$$p_{3,n} = p_{3,1} + \frac{1}{4} \cdot [3(d_2 - d_1) \cdot n^2 + 4(2d_1 - d_2 + 1)]$$

 $\cdot n - (5d_1 - d_2 + 4)]$ (21)
当 n 为偶数时,

$$p_{3,n} = p_{3,1} + \frac{1}{4} \cdot \left[3(d_2 - d_1) \cdot n^2 + 4(2d_1 - d_2 + 1) \right]$$

$$\cdot n - 4(d_1 + 1)$$
(22)

可以发现,当 $p_{3,1}$, d_1 , d_2 确定后, $p_{3,n}$ 是关于 n的二次函数。由于本文方法中参数设置的灵活性, 而移位矩阵的维数 p大于移位系数,故 p的取值下 界为

$$\inf p = \max\left(p_{1,n}, p_{2,n}, p_{3,n}\right) + 1 \tag{23}$$

特别地,当 $p_{1,1} = p_{2,1} = p_{3,1} = d_1 = 0$, $d_2 = 1$ 时,式 (21)的计算结果为 $3(n^2 - 1)/4$,式(22)为 $3n^2/4 - 1$, 此时p的下界为 $3n^2/4$,与文献[10]给出的研究结果 相一致,说明该基矩阵是本文方法的一种特例。

5 仿真与分析

5.1 p 值下界分析

构造 3 种准循环基矩阵,设 $d_i = i, i \in \{1,2\}$,其 它参数如表 2 所示。图 2 描绘了这 3 种码字 p 的取 值下界随 n 的变化曲线。

表 2 $d_i = i, i \in \{1, 2\}$ 时的参数配置

	$p_{1,1}$	$p_{2,1}$	$p_{3,1}$
码 1	47	0	0
码 2	0	40	0
码 3	0	0	0

从图 2 中可以看到, *p* 的取值下界随 *n* 的增大 而增大。当3 \leq *n* < 8时,码 1、码 2 的 *p* 值下界与 *n* 呈线性关系,当*n* \geq 8 时,3 条曲线重合,此时 *p* 的取值仅与 *p*_{3,n} 有关。这是因为 3 种基矩阵的 {*p*_{3,j}} 完全一致,且由式(16)可知,{*p*_{3,j}} 中元素的增幅显 然大于 {*p*_{1,j}} 和 {*p*_{2,j}},随着 *n* 的增大,无论初始参 数如何设置, inf *p* = *p*_{3,n} +1都是必然结果。同时表 明,利用本文方法构造的任意参数的准循环基矩阵, 都可使 *p* 值获得连续取值的下界。

5.2 围长分析

构造3种准循环基矩阵,设n = 6,其它参数如 表3所示。图3描绘了这3种码字的8环数目随p值的变化曲线,图4为码长一定($N = n \cdot p = 960$)条 件下,码3的8环数目随n的变化曲线。可以看到, 基矩阵一定时8环数随p值增大而增多;而当码长 一定时,p值越小则行重越大,意味着形成短环的 概率越大,造成环数增多。因此在构造基矩阵时, 针对不同的编码参数需求,本文方法提供了一种简 单、灵活的设计思路。

表 3 n = 6 时的参数配置

	$p_{1,1}$	$p_{2,1}$	$p_{3,1}$	d_1	d_2
码1	40	0	5	1	3
码 2	0	30	0	1	3
码 3	0	0	10	1	2

5.3 性能分析

构造两种准循环基矩阵,设码率 R = 1/2,其它 参数如表 4 所示。在加性高斯白噪声(Additive White Gauss Noise, AWGN)信道下进行仿真,译码 采用置信传播(Belief Propagation, BP)算法,最大 迭代次数为 30,调制方式为 BPSK,选取同码长码 率 的 渐 进 边 增 长 (Progressive Edge-Growth, PEG)^[16]码进行性能比较。仿真结果如图 5 所示。

表4 R = 1/2时的参数配置

	$p_{1,1}$	$p_{2,1}$	$\boldsymbol{p}_{3,1}$	d_1	d_2	p
码1	40	0	5	1	4	84
码 2	0	0	10	1	7	168

3

2

1

0



图 2 p 的取值下界随 n 的变化曲线



图 5 本文构造码字与 PEG 码的性能比较

仿真结果表明,码长为 504 时二者的译码性能 差异不大;当码长为 1008, BER 为 10⁻⁵时,与 PEG



图 38 环数目随 p 值的变化曲线



码相比本文构造码字信噪比增益约为 0.3 dB。此外, PEG 方法需要对度数的分布进行优化处理,其算法 复杂度也高于本文方法。

4 5 6

6 结束语

本 文 提 出 了 一 种 构 造 围 长 至 少 为 8 的 (3,*n*)QC-LDPC 码的确定性方法。该码的准循环基 矩阵由等差数列生成的数学表达式确定,构造方法 简单,节省了编解码存储空间。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,如何消除 8 环,从而 构造围长为10的QC-LDPC码是今后深入研究的内 容之一。

参考文献

- O'Sullivan M E. Algebraic construction of sparse matrices with large girth[J]. *IEEE Transactions on Information Theory*, 2006, 52(2): 718–727.
- [2] Milenkovic O, Kashyap N, and Leyba D. Shortened array codes of large girth[J]. *IEEE Transactions on Information Theory*, 2006, 52(8): 3707–3722.
- [3] Jiang X and 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.
- [4] Huang Jen-fa, Huang Chun-ming, and 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.
- [5] Zhang Guo-hua, Sun Rong, and Wang Xin-mei. Construction of girth-eight QC-LDPC codes from greatest common divisor[J]. *IEEE Communications Letters*, 2013, 17(2): 369–372.
- [6] 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.
- [7] Mohammad G and Ghaffar R. Column weight two and three LDPC codes with high rates and large girths[OL]. http://arxiv.org/abs/1403.6090, 2014.4.
- [8] 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.
- 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.
- [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.

- [11] Zhang Guo-hua, Sun Rong, and 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. 围长为8的QC-LDPC码的显示构造 及其在 CRT 方法中的应用[J]. 通信学报,2012,33(3): 171-176.

Zhang Guo-hua, Sun Rong, and Wang Xin-mei. Explicit construction of girth-eight QC-LDPC codes and its application in CRT method[J]. *Journal of Communications*, 2012, 33(3): 171–176.

- [13] Zhang Guo-hua, Sun Rong, and Wang Xin-mei. Deterministic construction of girth-eight (3, L) QC-LDPC codes from quadratic function[J]. *Electronics Letters*, 2013, 49(9): 600–602.
- [14] 杨民,张文彦, 钟杰, 等. 准循环多进制 LDPC 码构造[J]. 电 子与信息学报, 2013, 35(2): 297-302.
 Yang Min, Zhang Wen-yan, Zhong Jie, et al. Construction of non-binary QC-LDPC codes[J]. Journal of Electronics & Information Technology, 2013, 35(2): 297-302.
- [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] Hu Xiao-yu, Eleftheriou E, and Amold D M. Progressive edge-growth tanner graphs[C]. Proceedings of the IEEE Global Telecommunications Conference, San Antonio, USA, 2001: 995–1001.
- 张 轶: 男, 1986年生, 博士生, 研究方向为信道编码理论.
- 达新宇: 男,1961年生,教授,研究方向为卫星通信、通信信号 处理.
- 苏一栋: 男,1986年生,博士生,研究方向为认知无线电、压缩 感知理论.