码长连续变化的 QC-LDPC 码的设计

刘 磊 周武旸
(中国科学技术大学无线网络通信实验室 合肥 230027)

摘 要：该文基于有限多项式环的理论，提出了码长连续变化的准循环低密度奇偶校验(Quasi-Cyclic Low Density Parity Check, QC-LDPC)码的设计方法。当有限环基数大于某个门限值时，在此环内通过一定规则选择参数生成移位项，利用它们构造出的校验矩阵均可以达到较大的圈长(girth)值。在设计中，有限环基数为连续的整数，且基数与码长呈线性关系，因此能够在 girth 值不变的前提下实现码长的连续变化。该文分析并证明了该构造方法大大增加了可用的高性能 QC-LDPC 码数量，更好地服务于自适应链路系统。

关键词：低密度奇偶校验码；准循环；有限多项式环；圈长；连续可变码长
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2009)10-2523-04

Design of QC-LDPC Code with Continuously Variable Length

Liu Lei Zhou Wu-yang
(*Wireless Information Network Lab*, *Dept. Electronic Engineering and Information Science*, *University of Science and Technology of China*, *Hefei* 230027, *China*)

Abstract: Based on the theory of finite polynomial ring, a novel code design method for Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes with continuously variable length is proposed. When the cardinal number of the ring is larger than a certain threshold, the shift offset values can be formulated by the parameters selected in the ring. Thus all $\boldsymbol{H}$ matrices constructed by them have larger girth. In the design, the cardinal number of the ring is a continuously variable integer, which has a linear relation with the code length, so that the code length can be increased continuously. Analyses and proofs show that, the method can enlarge the number of QC-LDPC codes greatly, which can serve the adaptive link systems better.

Key words: LDPC codes; Quasi-Cyclic; Finite polynomial ring; Girth; Continuously variable code length

1 引言

QC-LDPC 码的校验矩阵 $\boldsymbol{H}$ 具有类循环特性，与随机构造的码字相比，其优点是可以利用移位寄存器实现线性时间编码，并且只需要很少的存储空间来存储编码矩阵。

因为 $\boldsymbol{H}$ 矩阵中的短循环会影响迭代解码过程中外信息的相关性，从而降低解码性能，所以 QC-LDPC 码的研究主要集中于构造具有较高圈长(girth)值的 $\boldsymbol{H}$ 矩阵及性能优异的中短码长的码字。Zhang 等人提出了一种基于均衡不完全区组设计(Balanced Incomplete Block Designs, BIBD)的 $\boldsymbol{H}$ 矩阵构造方法[1]，利用 3 维网格(3D-Lattice)结构构造出的 $\boldsymbol{H}$ 矩阵 girth 值为 10。除了上述方法，基于有限域的构造方法也被大量的使用。在有限域 GF(p) 内，通过计算机搜索，当 p=15m+1(其中 m 为正整数)时，随着码长的增加，可以构造出 girth 值为 10 或 12 的(3,5)QC-LDPC 码[2]。Kim 等人还讨论了这种 $\boldsymbol{H}$ 矩阵 girth 值与用于构造子矩阵的移位项之间的关系，并进行了理论分析[3]。为了进一步增大 $\boldsymbol{H}$ 矩阵的 girth 值，可以通过设计母矩阵来实现，利用这种方法构造的 $\boldsymbol{H}$ 矩阵的 girth 值可以达到 14 或 18[4]。虽然上述研究构造的 $\boldsymbol{H}$ 矩阵都具有高 girth 值，但所得到的码字码长都是跳跃的。如果要求 girth 值达到 14，则 $\boldsymbol{H}$ 矩阵的子矩阵长度就必须很长，达到 37^5 或 4^{15}[4]，无法满足系统自适应要求，限制了在实际系统中的应用。

在未来移动通信系统中，传输的多媒体业务(如语音、视频会议、流媒体、Web 浏览等)具有不同的 QoS 需求，这就需要无线链路具备自适应的能力，即能够根据业务和信道情况自适应调整链路参数，如数据帧长、信道编码的码率与码长等[5]。基于此，本文提出了一种基于有限多项式环(Finite Polynomial Ring, FPR)理论的 QC-LDPC 码的构造方法，设计出的 $\boldsymbol{H}$ 矩阵具有较大 girth 值，且码长

2008-05-21 收到，2009-06-29 改回
国家 863 计划重点项目(SQ200802LS1480497)，国家 973 计划项目(2007CB310602)，中瑞国际合作项目(2008DFA11950)和安徽省自然科学基金(070412044)资助课题

可以连续变化。

2 基于 FPR 理论的 QC-LDPC 码 $\boldsymbol{H}$ 矩阵的构造方法

首先，给出本文的数学基础——有限多项式环(FPR)理论以及基于此理论如何构造 QC-LDPC 码。

2.1 一元 FPR 的概念[6]

定义 1 若环 R 与整数集合{1,2,⋯,n}同基数，则称 R 为有限环，称其基数为 n。

利用定义 1，可以得到一元 FPR 的定义。

定义 2 设 R 为一个有限环，x 为 R 中的一个变量，a_i 为一元多项式环 $R[x]$的系数，则 $R[x]$可表示为

$$R[x]=\left\{\sum_{\text{finite}} a_i x^i:\ i \text{ 是非负整数},\ a_i\in R\right\} \tag{1}$$

其中 x^0 定义为 1。

2.2 基于 FPR 理论的 QC-LDPC 码的定义

定义 QC-LDPC 码的校验矩阵 $\boldsymbol{H}$ 为

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{P}^{a_{00}} & \boldsymbol{P}^{a_{01}} & \cdots & \boldsymbol{P}^{a_{0(n-1)}} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{P}^{a_{(m-1)0}} & \boldsymbol{P}^{a_{(m-1)1}} & \cdots & \boldsymbol{P}^{a_{(m-1)(n-1)}} \end{bmatrix} \tag{2}$$

其中每个子矩阵 $\boldsymbol{P}^{a_{ij}}$ 为 $L\times L$ 的单位阵向右循环移位 a_{ij} 得到，其生成多项式环为 $R_{ij}=x+a_{ij}$，其中 a_{ij} (i=0,1,⋯,m−1; j=0,1,⋯,n−1)为移位项，它们都定义在同一个有限环 $\mathfrak{R}_L$ 上，L 为环的基数。当如式(2)所示的 $\boldsymbol{H}$ 矩阵满秩时，其码率 $R=(n-m)/n$，码长 $N=nL$。

在 $\boldsymbol{H}$ 矩阵中存在一个长为 $2q$ 的块循环，表示为[7]

$$(i_0,j_0);(i_1,j_1);\cdots;(i_k,j_k);\cdots;(i_{q-1},j_{q-1});(i_0,j_0) \tag{3}$$

其中 (i_k,j_k) 标识处于矩阵 $\boldsymbol{H}$ 中位于第 i_k 行，第 j_k 列的子矩阵 $\boldsymbol{P}^{a_{i_kj_k}}$，且 $i_k\neq i_{k+1}$，$j_k\neq j_{k+1}$。

依照上面的定义，移位项与 girth 值的关系具有如下定理[7]：

定理 1 如式(2)所示的 $\boldsymbol{H}$ 矩阵，考虑其中所有如式(3)所示的块循环，其 girth 至少为 2 s 的的充分必要条件为

$$\sum_{k=0}^{q-1}\left(a_{i_kj_k}-a_{i_{k+1}j_k}\right)\neq 0 \mod L,\ \forall q=2,\cdots,s-1 \tag{4}$$

设循环子矩阵 $\boldsymbol{P}^{a_{ij}}$ 的移位项为

$$a_{ij}=2^{i-1}\cdot l_{j-1} \tag{5}$$

基于上文的结论以及 FPR 理论，本文的主要结论如下。

2.3 移位项系数的确定以及有限环基数 L 的选取

根据定理 1，可以推导出：

定理 2 当 m=3 且移位项如式(5)所示，当有限环基数 $L\geqslant L_{\min}$，且如下条件成立时，所构造的校验矩阵 $\boldsymbol{H}$ 可以达到 girth≥10：

$$l_{j_0}\neq l_{j_1} \tag{6}$$

$$\alpha\left|l_{j_0}-l_{j_1}\right|\neq\beta\left|l_{j_1}\neq l_{j_2}\right|,\ \forall\alpha,\beta\in\{\pm1,\pm2,\pm3\} \tag{7}$$

$$\alpha\left|l_{j_0}-l_{j_1}\right|\neq\beta\left|l_{j_2}\neq l_{j_3}\right|,\ \forall\alpha,\beta\in\{\pm1,\pm2,\pm3\} \tag{8}$$

其中 $j_0\neq j_1\neq j_2\neq j_3$，并且

$$L_{\min}=2(2^{m-1}-2^0)(l_{n-1}-l_0)+1 \tag{9}$$

证明 为了实现校验矩阵 $\boldsymbol{H}$ 的 girth 达到 10，其中长度为 4，6，8 的环必须被消除。在如式(2)所示的 $\boldsymbol{H}$ 矩阵中，存在一种长度为 4 的环，即 $(i_0,j_0);(i_1,j_1)$[3]。为了消除所有的 4 循环，设式(4)中 q=2 得到

$$\left(2^{i_0}-2^{i_1}\right)\left(l_{j_0}-l_{j_1}\right)\neq 0 \tag{10}$$

这里 $i_0\neq i_1$，$j_0\neq j_1$，因此可以得到式(6)。

其中存在一种长度为 6 的环，即 $(i_0,j_0);(i_1,j_1);(i_2,j_2)$[3]。为了消除所有的 6 循环，设式(4)中 q=3 得到

$$\left(2^{i_0}-2^{i_1}\right)\left(l_{j_0}-l_{j_2}\right)\neq\left(2^{i_2}-2^{i_1}\right)\left(l_{j_1}-l_{j_2}\right) \tag{11}$$

这里 $i_0\neq i_1\neq i_2$，$j_0\neq j_1\neq j_2$。由于 $i_k\in\{0,1,2\}$, $\forall k$，式 $(2^{i_{k_1}}-2^{i_{k_2}})$, $i_{k_1}\neq i_{k_2}$ 的取值为 $\{\pm1,\pm2,\pm3\}$。因此式(11)在交换角标 j_1 与 j_2 后可以得到式(7)。

基于环中包含矩阵 $\boldsymbol{H}$ 行或列子矩阵的不同，其中存在 6 种不同类型的 8 循环。第 1 种类型的环包含两行以及两列：$(i_0,j_0);(i_1,j_1);(i_0,j_0);(i_1,j_1)$。第 2 种类型的环包含 3 行以及 2 列：$(i_0,j_0);(i_1,j_1);(i_0,j_0);(i_2,j_1)$。上面两种类型的环都可以通过式(6)来消除。第 3 种类型的环包含 2 行以及 3 列：$(i_0,j_0);(i_1,j_1);(i_0,j_0);(i_1,j_2)$，而第 4 种类型的环包含 3 行以及 3 列：$(i_0,j_0);(i_1,j_1);(i_2,j_2);(i_1,j_1)$。这两种类型的环可以通过式(7)来消除。第 5 种类型的环包含 2 行以及 4 列：$(i_0,j_0);(i_1,j_1);(i_0,j_2);(i_1,j_3)$。同时第 6 种类型的环包含 3 行以及 4 列：$(i_0,j_0);(i_1,j_1);(i_2,j_2);(i_1,j_3)$。这两种类型的环可以通过式(8)来消除。

随后定义 $L_{\min}$，当 q=2 时，式(4)左边绝对值得最大值为 $(2^{m-1}-2^0)(l_{n-1}-l_0)$。当 q=3 时，此绝对值的最大值小于 $(2^{m-1}-2^0)(l_{n-1}-l_0)$。当 q=4 时，此绝对值得最大值为 $2(2^{m-1}-2^0)(l_{n-1}-l_0)$。因此，当 $L_{\min}$ 满足式(9)时，可以保证得到的矩阵 $\boldsymbol{H}$ 的 girth 不小于 10。 证毕

定理 3 当 m=2 且 a_{ij} 如式(5)所示，当有限环

基数 $L \geqslant L_{\min}$，且如下条件成立时，所构造的校验矩阵 $\boldsymbol{H}$ 可以达到 girth 为 12：

$$l_{j_0} \neq l_{j_1} \tag{12}$$

$$\left|l_{j_0} - l_{j_1}\right| \neq \left|l_{j_2} \neq l_{j_3}\right| \tag{13}$$

其中 $j_0 \neq j_1 \neq j_2 \neq j_3$，并且 $L_{\min}$ 如式(9)所示。

证明　由于 m=2，如式(2)所示的矩阵 $\boldsymbol{H}$ 中的环长一定为 4 的倍数。因此只需要消除 4 循环与 8 循环从而实现 girth 为 12。按照与定理 2 证明相似的步骤，可以得到式(12)以及式(13)。　　证毕

利用定理 2，按照如下步骤构造 girth 值为 10 的 $\boldsymbol{H}$ 矩阵：

(1)确定母矩阵。在本文中只讨论列重 m 为 2 或 3 的全 1 母矩阵，选定码率 R，利用公式：$n=m/(1-R)$，得到行重为 n。

(2)按照定理 2 选取移位项的参数以及最小环基数 $L_{\min}$。

(3)构造校验矩阵 $\boldsymbol{H}$，按照这样的参数可以构造码长为 $n(L_{\min}+k)$ 的码字，其中 k=0,1,2,…，从而 $\boldsymbol{H}$ 矩阵规模为 $m(L_{\min}+k)\times n(L_{\min}+k)$。

例　对列重 m 为 3 的情况，选取码率 2/5，得到行重 n 为 5。按照定理 2 选取参数，可得：l_0=0、l_1=1、l_2=5、l_3=14、l_4=25 以及 $L_{\min}=2(2^{3-1}-2^0)(25-0)+1=151$。从而可以构造码长为 $5(151+k)$, (k=0,1,2,…)的码字，即其码长按照 755，760，765，770，…以 755 为基础，行重 5 为步进连续变化。所构造出的码字均满足 girth 值为 10。　　证毕

按照上面的步骤，本文对不同的列重与码率的情况设计出了参数，所构造出的 $\boldsymbol{H}$ 矩阵均满足 girth 值为 10，而且码长可以做到以列重 n 为步进连续变化，并对这些矩阵进行了仿真。

3　仿真分析

在加性高斯白噪声信道下，信号采用 BPSK 调制，译码采用和积(Sum and Product Algorithm, SPA)算法，迭代次数为 100 次，对构造出的码字性能进行了蒙特卡洛仿真。对于列重为 2 和 3 的 $\boldsymbol{H}$ 矩阵，参数选取如表 1 所示，其中 l_i (i=0,1,…,8)的取值根据定理 2 以及定理 3 给出。

表 1 给出了不同列重和码率情况下所设计的 $\boldsymbol{H}$ 矩阵的参数，其 girth 至少为 10 并且码长可以以行重为步进地连续变化。设计出的码字码率范围为 1/4 至 2/3。特别对于固定的 m ，当 n 增加时参数 l_i 并不会发生改变，因此可以满足自适应链路系统的需求。

由图 1 可以看出，在 E_b/N_0 相同的情况下，FPR 方法构造的码字与 Mackay 随机方法[8]构造的码字以及 3D-Lattice 的方法[1]构造的码字性能上大致相当，在高信噪比条件下可以达到比另两种方法更快的收敛速度。但是利用 3D-Lattice 的方法无法生成码长连续的码字，因此 FPR 方法构造的码字在保证性能的前提下生成大量可用码字。

为了进一步说明 FPR 方法能构造出连续码长码字的特性，本文利用表 1 中，列重为 3，码率分别为 2/5 和 1/2 的参数，在各自固定的信噪比下构造出码长连续的码字进行仿真，仿真结果如图 2 所示。

由图 2 可以看出，FPR 方法在保证性能的前提下能够实现码字码长的连续变化。并且随着码长的增加，其性能逐渐提高。在现代通信系统中，较短码长的码字由于其解码时间短以及缩短包长度被广

表 1 FPR 方法构造高 girth 值且码长连续的 $\boldsymbol{H}$ 矩阵参数表

列重 m	行重 n	码率 R	girth	$L_{\min}$	码长 k=0,1,…	l_0	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8
2	3	1/3	12	7	3(7+k)	0	1	3	–	–	–	–	–	–
2	4	1/2	12	15	4(15+k)	0	1	3	7	–	–	–	–	–
2	5	3/5	12	25	5(25+k)	0	1	3	7	12	–	–	–	–
2	6	2/3	12	41	6(41+k)	0	1	3	7	12	20	–	–	–
3	4	1/4	10	84	4(84+k)	0	1	5	14	–	–	–	–	–
3	5	2/5	10	151	5(151+k)	0	1	5	14	25	–	–	–	–
3	6	1/2	10	343	6(343+k)	0	1	5	14	25	57	–	–	–
3	7	4/7	10	529	7(529+k)	0	1	5	14	25	57	88	–	–
3	8	5/8	10	733	8(733+k)	0	1	5	14	25	57	88	122	–
3	9	2/3	10	1189	9(1189+k)	0	1	5	14	25	57	88	122	198

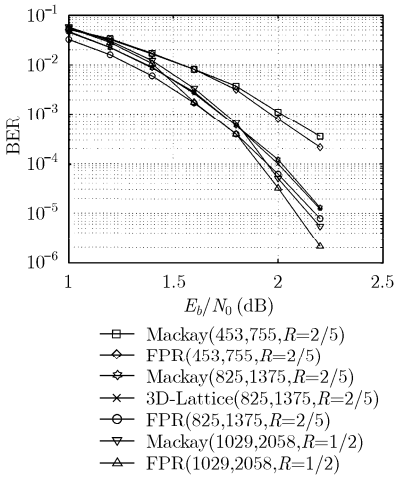

图 1 FPR 方法与 Mackay 随机方法以及 3D-Lattice 方法构造的码字的性能比较

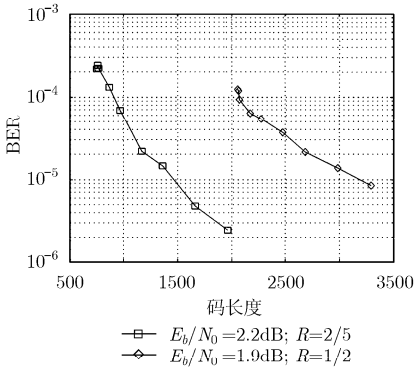

图 2 固定信噪比下 BER 随码长变化曲线

泛应用，因此 FPR 方法大大增加了目前系统中的可用码字。

4 结束语

本文基于有限多项式环理论提出了一种构造 QC-LDPC 码 $\boldsymbol{H}$ 矩阵的方法，即 FPR 方法。通过对不同 girth 值图样的推导，得到满足要求 girth 值的参数，从而由这些参数确定 QC-LDPC 码移位项的值，再通过这些参数计算出有限环的最小基数，从而确定最小码长。生成的码字长度可以在最小码长的基础之上以行重为步进连续变化，并且可以很大程度地覆盖列重为 2 和 3 的码率范围($R\leqslant 2/3$)。仿真表明，基于此方法生成的码字具有良好的性能，且可以在保证性能的前提下实现码长的连续变化。

参 考 文 献

[1] Zhang Fan, Mao Xue-hong, and 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.

[2] Tanner R, Sridhara D, and Fuja T. A class of group-structured LDPC codes[C]. http://citeseer.ist.psu.edu/old/tanner01class.html, 2001 July.

[3] Kim S, No J, and 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.

[4] Kim S, No J, and Chung H, *et al*.. Quasi-Cyclic Low-Density Parity-Check codes with girth larger than 12[J]. *IEEE Transactions on Information Theory*, 2007, 53(10): 2885–2891.

[5] Papadimitriou G I, Pallas G D, and Pomoportsis A S. A self-adaptive protocol for broadcast LAN's with variable packet length[J]. *IEEE Communication Letters*, 2004, 8(1): 72–74.

[6] 莫宗坚, 蓝以中, 赵春来. 代数学(上)[M]. 第一版, 北京: 北京大学出版社, 1986: 110–157.

[7] Fossorier M. Quasi-cyclic low-density parity-check codes from circulant permutation matrix[J]. *IEEE Transactions on Information Theory*, 2004, 50(8): 1788–1793.

[8] Mackay D. Good error-correcting codes based on very sparse matrices[J]. *IEEE Transactions on Information Theory*, 1999, 45(2): 399–431.

刘 磊： 男，1984年生，硕士生，研究方向为信道编码技术.

周武旸： 男，1972年生，教授，博士生导师，研究方向为通信信号处理、信道编码、无线资源管理等.