第 32 卷第 5 期 电 子 与 信 息 学 报 Vol.32No.5
2010 年 5 月 Journal of Electronics & Information Technology May 2010

Girth-8 (3,L)-规则QC-LDPC码的一种确定性构造方法

张国华 陈 超 杨 洋 王新梅
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要：对于围长(girth)至少为8的低密度奇偶校验(LDPC)码，目前的绝大多数构造方法都需要借助于计算机搜索。受贪婪构造算法启发，该文利用完全确定的方式构造出一类围长为8的 $(3,L)-$规则QC-LDPC码。这类QC-LDPC码的校验矩阵由 $3\times L$ 个 $P\times P$ 的循环置换矩阵构成。对于任意整数 $P\geq 3L^2/4$，这类校验矩阵的围长均为8。

关键词：低密度奇偶校验码；准循环；围长
中图分类号：TN911.22 **文献标识码**： A **文章编号**：1009-5896(2010)05-1152-05
DOI: 10.3724/SP.J.1146.2009.00838

Girth-8 (3,L)-Regular QC-LDPC Codes Based on Novel Deterministic Design Technique

Zhang Guo-hua Chen Chao Yang Yang Wang Xin-mei
(*State Kay Laboratory of Integrated Service Networks*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Most of the proposed constructions for Low-Density Parity-Check (LDPC) codes with girth at least eight are focused on (semi-) stochastic methods with the aid of computer search. Motivated by the resulting parity-check matrices obtained from the Greedy construction idea, a deterministic method is presented to construct a novel family of girth-8 (3,L)-regular Quasi-Cyclic (QC-) LDPC codes. The parity-check matrix of the new code consists of $3\times L$ $P\times P$ cyclic permutation matrices and the girth of its Tanner graph is eight for arbitrary integer $P\geq 3L^2/4$.

Key words: Low-Density Parity-Check (LDPC) code; Quasi-Cyclic (QC); Girth

1 引言

消除短环是提高低密度奇偶校验(LDPC)码译码性能的重要手段之一。目前消除4环(即围长至少为6)的研究成果已经非常丰富[1,2]，因此如何消除6环(甚至更长的环)已经成为LDPC码构造方面的一个研究热点。虽然对于列重为2的情形人们已构造出围长高达12的LDPC码[3]，但是对于列重大于2的情形构造围长大于6的LDPC码却并非易事。本文的研究目标是列重为3且围长至少为8的LDPC码。

本文将围长至少为 g 记为girth-g^+，将围长恰好为 g 记为girth-g；若LDPC码的校验矩阵列重为 J、行重为 L，则称为 $(J,L)-$规则。下文涉及到的LDPC码的列重均为3。文献[4]利用“容许斜度对”和计算机搜索设计了几种girth-8$^+$ LDPC码。文献[5]基于“三维点阵”和计算机搜索设计了一种girth-8$^+$ LDPC码，文献[6]基于环数检测算法和计算机搜索设计了一种girth-8$^+$ LDPC码。文献[7]基于“爬山”算法提出了一种girth-8$^+$ LDPC码的优化设计方法：首先利用计算机随机产生一个基矩阵，然后利用爬山算法逐步优化该基矩阵，直到满足设计要求为止；该算法虽然可以设计出码长非常短的LDPC码，但是算法存在运行失败的可能性。总之，这些依赖于计算机搜索和计算的方法，虽然可以比较有效地构造出girth-8$^+$ LDPC码，但是存在两个不足：第一，难以给出校验矩阵的简洁表达式；第二，由于没有研究相应LDPC码的存在性问题，因此这些方法不能避免运行失败(即始终无法获得满足条件的校验矩阵)的可能性。

本文工作的创新点是，提出了一种girth-8 $(3,L)$-规则QC-LDPC码的确定性构造方法，并且解决了这类QC-LDPC码的存在性问题。这种构造方法具有两个显著优点：第一，构造过程不需要借助于计算机搜索；第二，对于任意码长 $N=LP(P\geq 3L^2/4)$，该方法都可以构造出girth-8 $(3,L)$-规则QC-LDPC码。

2 构造方法

根据文献[8]，$(3,L)$-规则QC LDPC码的校验矩阵可以表示为

2009-06-03收到，2009-11-19改回
国家973计划项目(2010CB328300)，国家自然科学基金(U0635003)和111基地项目(B08038)资助课题
通信作者：张国华 zhangghcast@163.com

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{I}(0) & \boldsymbol{I}(0) & \cdots & \boldsymbol{I}(0)\\ \boldsymbol{I}(0) & \boldsymbol{I}(p_{1,1}) & \cdots & \boldsymbol{I}(p_{1,L-1})\\ \boldsymbol{I}(0) & \boldsymbol{I}(p_{2,1}) & \cdots & \boldsymbol{I}(p_{2,L-1})\end{bmatrix} \tag{1}$$

其中$\boldsymbol{I}(x)$是受移位值x控制的一个$P\times P$循环置换矩阵，具体定义见文献[8]。在式(1)定义中可以认为$p_{1,0}=0, p_{2,0}=0$。

2.1 由贪婪算法得到的启发

QC-LDPC 码的围长依赖于移位值$p_{i,j}(0<i\le 2, 0<j<L)$的取值[8]。首先，利用贪婪算法为$p_{i,j}$依次赋值，从而得到校验矩阵$\boldsymbol{H}$；然后，分析校验矩阵$\boldsymbol{H}$的规律。

贪婪算法：对于$p_{i,j}(0<i\le 2, 0<j<L)$，尝试从$p_{i,j-1}+1$开始的每个整数，将第 1 个使校验矩阵$\boldsymbol{H}$的围长至少为 8 的整数赋给$p_{i,j}$。当所有移位值均处理完毕后，就得到了目标校验矩阵。在贪婪算法执行之前，校验矩阵$\boldsymbol{H}$的移位值$p_{i,j}(0<i\le 2, 0<j<L)$均被初始化为-1，-1 表示$P\times P$的全零矩阵。赋值顺序为$p_{1,1},\cdots,p_{1,L-1},p_{2,1},\cdots,p_{2,L-1}$。

对$L=4-10$执行贪婪算法，可以发现：移位值$p_{1,0},p_{1,1},\cdots,p_{1,L-1}$等于 0 至$L-1$，而$p_{2,0},p_{2,1},\cdots,p_{2,L-1}$分别如表 1 所示：

表1　$L=4-10$时移位值$p_{2,k}$(0 ? k　　L) 的取值

L	$p_{2,0},p_{2,1},\cdots,p_{2,L-1}$
4	0,4,7,11
5	0,5,9,13,18
6	0,6,11,15,20,26
7	0,7,13,18,23,29,36
8	0,8,15,21,26,32,39,47
9	0,9,17,24,30,36,43,51,60
10	0,10,19,27,34,40,47,55,64,74

根据式(1)，利用$p_{1,k}$和$p_{2,k}(0\le k<L)$可以直接得到校验矩阵$\boldsymbol{H}$。例如，当$L=10$时，校验矩阵$\boldsymbol{H}$为

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0)\\ \boldsymbol{I}(0) & \boldsymbol{I}(1) & \boldsymbol{I}(2) & \boldsymbol{I}(3) & \boldsymbol{I}(4) & \boldsymbol{I}(5) & \boldsymbol{I}(6) & \boldsymbol{I}(7) & \boldsymbol{I}(8) & \boldsymbol{I}(9)\\ \boldsymbol{I}(0) & \boldsymbol{I}(10) & \boldsymbol{I}(19) & \boldsymbol{I}(27) & \boldsymbol{I}(34) & \boldsymbol{I}(40) & \boldsymbol{I}(47) & \boldsymbol{I}(55) & \boldsymbol{I}(64) & \boldsymbol{I}(74)\end{bmatrix} \tag{2}$$

2.2 构造方法

分析移位值$p_{2,k}(0\le k<L)$的规律性，可以得到一种构造$(3,L)$-规则QC-LDPC码的新方法。

构造　令$p_{1,k}=k\ (0\le k<L)$。根据L的奇偶性，对$p_{2,k}(0\le k<L)$分别赋值：

若L为偶数：

$$p_{2,k}=\begin{cases}kL-k(k-1)/2,\ 0\le k\le L/2\\ L(L-2)/4+k(k+3)/2,\ L/2\le k<L\end{cases} \tag{3a}$$

若L为奇数：

$$p_{2,k}=\begin{cases}kL-k(k-1)/2,\ 0\le k\le (L-1)/2\\ (L-1)^2/4+k(k+3)/2,\ (L-1)/2\le k<L\end{cases} \tag{3b}$$

式(3a)和式(3b)可以统一表示为

$$p_{2,k}=\begin{cases}f_1(k)\coloneqq kL-k(k-1)/2,\ 0\le k\le L/2\\ f_2(k)\coloneqq\{L(L-2)+L\bmod(2)\}\\ \qquad /4+k(k+3)/2,\ L/2\le k<L\end{cases} \tag{3c}$$

注 1：可以验证，当L为偶数时$f_1(L/2)=f_2(L/2)$，当L为奇数时$f_1\{(L-1)/2\}=f_2\{(L-1)/2\}$。

3　Girth-8性质的证明

定理 1　对于任意$P\ge 3L^2/4$，由式(3c)定义的校验矩阵$\boldsymbol{H}$的围长至少为 8。

证明　$\boldsymbol{H}$由 3 行循环置换矩阵组成，在贪婪算法执行之前，校验矩阵$\boldsymbol{H}$的移位值$p_{i,j}(0<i\le 2, 0<j<L)$均被初始化为-1。

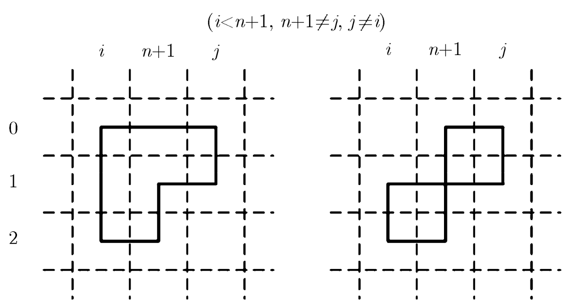
假定 1　P是一个非常大的确定的正整数。

(1)根据贪婪算法，$\boldsymbol{H}$的第 2 行循环置换矩阵的移位值$p_{1,0},p_{1,1},\cdots,p_{1,L-1}$必然被赋值为 0 至$L-1$。这种赋值不会在$\boldsymbol{H}$中引起 4 环和 6 环。

(2)显然$p_{2,0}$满足式(3c)，对于$p_{2,n+1}(0<n+1<L)$的取值采用数学归纳法证明。设$p_{2,n}(0\le n<L-1)$的取值满足式(3c)，下面证明$p_{2,n+1}\ (0<n+1<L)$的取值也满足式(3c)。由于$p_{2,n+2},\cdots,p_{2,L-1}$尚未被赋值，因此均取初始化数值-1。

首先，考虑经过循环置换矩阵$\boldsymbol{I}(p_{2,n+1})$的 6 环。这种 6 环只可能出现图 1 所示的两种情况。

图 1(a)类 6 环不会出现的充分必要条件是$p_{2,n+1}$满足



(a)　　(b)

图 1 经过$\boldsymbol{I}(p_{2,n+1})$的两种 6 环

$$(0-p_{2,i})+\{p_{2,n+1}-(n+1)\}+(j-0)\neq 0(\bmod P) \quad (4a)$$

在假定 1 下，式(4a)等价于

$$p_{2,n+1}\neq p_{2,i}+(n+1)-j \quad (4b)$$

式(4b)成立的必要条件是

$$p_{2,n+1}\neq p_{2,n}+(n+1)-j \quad (4c)$$

由于构造过程要求 $p_{2,n+1}>p_{2,n}$，因此式(4c)等价于

$$p_{2,n+1}\neq p_{2,n}+(n+1)-\{n-1,n-2,\cdots,0\} \quad (4d)$$

由于 $p_{2,n+1}\neq p_{2,n}+1$（否则将在 $\boldsymbol{I}(p_{1,n}),\boldsymbol{I}(p_{1,n+1}),\boldsymbol{I}(p_{2,n+1}),\boldsymbol{I}(p_{2,n})$ 出现 4 环)且 $p_{2,n+1}>p_{2,n}$，因此式(4d)等价于

$$p_{2,n+1}\geq p_{2,n}+n+2 \quad (4e)$$

由于式(4e)成立时式(4b)必然成立，因此式(4e)与式(4b)等价。即，在 $p_{2,n+1}>p_{2,n}$ 的限制条件下，图 1 不出现(a)类 6 环的充要条件是式(4e)成立。

图 1(b)类 6 环不会出现的充分必要条件是 $p_{2,n+1}$ 满足

$$(i-p_{2,i})+(p_{2,n+1}-0)+(0-j)\neq 0(\bmod P) \quad (5a)$$

在假定 1 下，式(5a)等价于

$$p_{2,n+1}\neq p_{2,i}+j-i \quad (5b)$$

式(5b)成立的必要条件是

$$p_{2,n+1}\neq p_{2,n}+j-n \quad (5c)$$

由于构造过程要求 $p_{2,n+1}>p_{2,n}$，因此

(情况 1)当 $n+1<L-1$ 时式(5c)等价于

$$p_{2,n+1}\neq p_{2,n}+\{n+2,\cdots,L-1\}-n \quad (5d)$$

(情况 2)当 $n+1=L-1$ 时式(5c)等价于

$$p_{2,L-1}>p_{2,L-2} \quad (5e)$$

由于 $p_{2,n+1}\neq p_{2,n}+1$（否则将在 $\boldsymbol{I}(p_{1,n}),\boldsymbol{I}(p_{1,n+1}),\boldsymbol{I}(p_{2,n+1}),\boldsymbol{I}(p_{2,n})$ 出现 4 环)且 $p_{2,n+1}>p_{2,n}$，因此式(5d)和式(5e)等价于

$$p_{2,n+1}\geq p_{2,n}+L-n \quad (5f)$$

由于式(5f)成立时式(5b)必然成立，因此式(5f)与式(5b)等价。即，在 $p_{2,n+1}>p_{2,n}$ 的限制条件下，图 1 不出现(b)类 6 环的充要条件是式(5f)成立。

其次，考虑经过循环置换矩阵 $\boldsymbol{I}(p_{2,n+1})$ 的 4 环。这种 4 环只可能出现图 2 所示的两种情况。

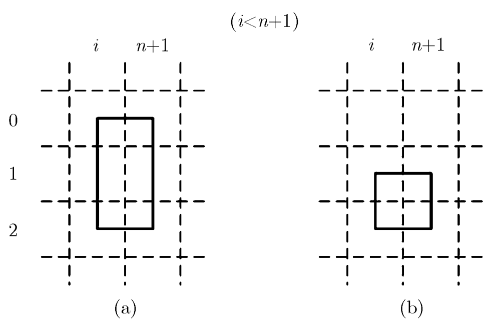


图 2 经过 $\boldsymbol{I}(p_{2,n+1})$ 的两种 4 环

图 2(a)类 4 环不会出现的充分必要条件是 $p_{2,n+1}$ 满足

$$(0-p_{2,i})+(p_{2,n+1}-0)\neq 0(\bmod P) \quad (6a)$$

在假定 1 下，式(6a)等价于

$$p_{2,n+1}\neq p_{2,i} \quad (6b)$$

图 2(b)类 4 环不会出现的充分必要条件是 $p_{2,n+1}$ 满足

$$(i-p_{2,i})+\{p_{2,n+1}-(n+1)\}\neq 0(\bmod P) \quad (7a)$$

在假定 1 下，式(7a)等价于

$$p_{2,n+1}\neq p_{2,i}+n+1-i \quad (7b)$$

显然，若式(4e)成立，则式(6b)和式(7b)必然成立。

因此，根据式(4e)和(5f)，不产生经过 $\boldsymbol{I}(p_{2,n+1})$ 的 4 环和 6 环的最小整数是

$$p_{2,n+1}=p_{2,n}+\max(n+2,L-n) \quad (8)$$

式(8)可以表示为

$$p_{2,n+1}=\begin{cases}p_{2,n}+L-n, n+1\leq L/2\\ p_{2,n}+n+2, n+1\geq L/2\end{cases} \quad (9)$$

通过整理可知式(9)给出的 $p_{2,n+1}$ 与式(3)在 $k=n+1$ 下的取值完全相同。

在从式(4a)到式(4b)，从式(5a)到式(5b)，从式(6a)到式(6b)，从式(7a)到式(7b)的推导中采用了假设1，即 P 是一个非常大的确定的正整数。下面将证明，只要 $P\geq 3L^2/4$，式(4a)与式(4b)，式(5a)与式(5b)，式(6a)与式(6b)，式(7a)与式(7b)就相互等价。

式(4a)等价于

$$p_{2,n+1}-(n+1)+j\neq p_{2,i}(\bmod P) \quad (10)$$

不等式左边

$$0<p_{2,n+1}-(n+1)+j\leq p_{2,L-1}-(L-1)$$
$$+j\leq p_{2,L-1}-(L-1)+(L-1)<3L^2/4$$

不等式右边 $0\leq p_{2,i}<3L^2/4$， 因此当 $P\geq 3L^2/4$ 时式(10)等价于

$$p_{2,n+1}-(n+1)+j\neq p_{2,i} \quad (11)$$

式(5a)等价于

$$p_{2,n+1}-j\neq p_{2,i}-i(\bmod P) \quad (12)$$

不等式左边 $0<p_{2,n+1}-j<3L^2/4$，不等式右边 $0\leq p_{2,i}-i<3L^2/4$，因此，当 $P\geq 3L^2/4$ 时式(12)等价于

$$p_{2,n+1}-j\neq p_{2,i}-i \quad (13)$$

类似地，可以证明：当 $P\geq 3L^2/4$ 时，式(6a)与式(6b)、式(7a)与式(7b)相互等价。 证毕

根据定理1，可以得到一个关于girth-$8^+(3,L)$-规则QC-LDPC码存在性的重要结论。

推论1　给定任意正整数$L(L \ge 4)$，对于任意正整数$P(P \ge 3L^2/4)$，存在长度为PL、设计码率为$1-3/L$的girth-8^+ $(3,L)$-规则QC-LDPC码。

由定理1的证明过程，可知

推论 2　贪婪算法构造出的校验矩阵与式(3)定义的校验矩阵$\boldsymbol{H}$完全相同。

观察校验矩阵$\boldsymbol{H}$的前2行和前3列，可知存在由关系式

$$(0\text{-}0)+(1\text{-}0)+(0\text{-}2)+(1\text{-}0)=0(\mathrm{mod}\ P) \tag{14}$$

描述的8环，因此有

推论3　对于任意$P \ge 3L^2/4$，由式(3)定义的校验矩阵$\boldsymbol{H}$的围长恰好为8。

4　与其他方法的比较

文献[9]提出了一个girth-g^+ (J,L)-规则 QC-LDPC码的存在性定理，该定理指出：当$P \ge [(J-1)(L-1)]^{(g/2-1)}/(J\cdot L-J-L)$时，girth-$g^+$ (J,L)-规则QC-LDPC码一定存在。

令$J=3$，$g=8$，可知

性质　当$P>4(L-1)^2$时，存在girth-8^+ $(3,L)$-规则 QC-LDPC码。

虽然文献[9]讨论了girth-g^+ (J,L)-规则 QC-LDPC码的存在性问题，但是具体构造过程仍然基于计算机搜索。由定理1可知，相对于性质1给出的P值下界，(当L较大时)本文将P的取值下界降低了约5.3倍，因而在很大程度上改进了girth-8^+ $(3,L)$-规则 QC-LDPC码存在性的理论结果。此外，本文所述方法以完全确定的方式直接构造出了这类girth-8 $(3,L)$-规则 QC-LDPC码(记为Greedy-QC-LDPC)。

2004年，Vasic基于矩形整数网格和“最早序列”[10]构造了一类girth-8 $(3,L)$-规则QC-LDPC码(记为Lattice-QC-LDPC码)，并且讨论了P的取值范围。这是目前已知的构造girth-8 $(3,L)$-规则QC-LDPC码的唯一的确定性方法。

对于$L=4-12$，Fossorier[8]利用计算机进行大量随机搜索，给出了一类girth-8 $(3,L)$-规则 QC-LDPC码(记为Fossorier-QC-LDPC码)的最小P值(记为$P_{\mathrm{Fossorier}}$)；Wang[7]利用爬山算法也给出了$L=4-12$时P的最小取值。Wang的结果与Fossorier的结果基本相同，但考虑数据的权威性，本文选择Fossorier给出的最小P值作为各种方法的比较基准。将Lattice-QC-LDPC码所给出的P值下界记为P_{Lattice}，将本文新构造的Greedy-QC-LDPC码的P值下界记为P_{Greedy}。

图3描绘了3种方法所给出的最小P值随L变化的关系曲线。

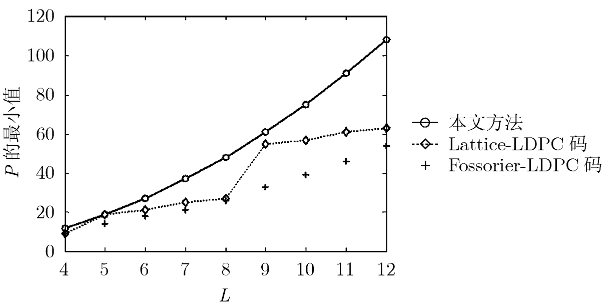


图3 3种girth-8 $(3,L)$-规则QC-LDPC码的最小P值比较

对于Lattice-QC-LDPC码和Greedy-QC-LDPC码，给定L，校验矩阵的移位值不随P值变化。当$P \ge P_{\mathrm{Lattice}}$时，Lattice-QC-LDPC码的围长均为8；当$P \ge P_{\mathrm{Greedy}}=3L^2/4$时，Greedy-QC-LDPC码的围长也均为8。因此，P_{Lattice}和P_{Greedy}可以分别作为Lattice-QC-LDPC码和Greedy-QC-LDPC码的P值允许连续取值的下界。由图3可知，P_{Lattice}与L之间的关系十分复杂，该函数关系无法用解析式表达。而P_{Greedy}与L之间的关系非常简单，并且对于$L=4-12$ P_{Greedy}不超过$P_{\mathrm{Fossorier}}$的两倍。

虽然$P_{\mathrm{Fossorier}}$在3种方法中最小，但是当$P>P_{\mathrm{Fossorier}}$时，如果校验矩阵的移位值仍然选为$P=P_{\mathrm{Fossorier}}$时的数值，则Fossorier-QC-LDPC码的围长不能保证必然为8。例如，式(15)所示的Fossorier-QC-LDPC码的校验矩阵在$P=9$时围长为8，而在$P=10$时围长减少为6。

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0)\\ \boldsymbol{I}(0) & \boldsymbol{I}(1) & \boldsymbol{I}(4) & \boldsymbol{I}(6)\\ \boldsymbol{I}(0) & \boldsymbol{I}(5) & \boldsymbol{I}(2) & \boldsymbol{I}(3)\end{bmatrix} \tag{15}$$

本节的比较结果说明，本文提出的Greedy- QC-LDPC码可以为girth-8 $(3,L)$-规则QC-LDPC码提供一个允许P值连续取值的优良下界。

5　结束语

相对于基于计算机搜索的girth-8^+ LDPC码的构造方法，本文提出了一种构造LDPC码的确定性方法，得到了一类girth-8 $(3,L)$-规则QC-LDPC码(Greedy-QC-LDPC码)。这种构造方法具有两个优点：(1)校验矩阵可以直接表示出来；(2)这类编码的存在性问题得到了完全解决：对于任意$P \ge 3L^2/4$，Greedy-QC-LDPC码的围长均为8。本文构造方法不仅丰富了girth-8^+ $(3,L)$-规则QC-LDPC码的确定性构造方法，而且针对girth-8^+ $(3,L)$-规则QC-LDPC码的存在性，提出了一个P值允许连续取值的简单下界。

值得进一步研究的内容：(1)本文只对Greedy-

QC-LDPC码的构造方法和存在性进行了理论分析与证明，Greedy-QC-LDPC码译码性能的计算机仿真研究值得继续开展。(2)受贪婪算法(按行遍历)启发，本文提出了围长为8的Greedy-QC-LDPC码。我们发现，当贪婪算法按列遍历时，对于几个较小的L，得到的校验矩阵与Lattice-QC-LDPC码的校验矩阵完全相同。这种有趣的发现启发我们提出一个猜想：(猜想1)对于任意L，当贪婪算法按列遍历时，得到的校验矩阵与Lattice-QC-LDPC码的校验矩阵完全相同。若猜想1得到证实，则在遍历顺序的意义下，本文提出的Greedy-QC-LDPC码和已有的著名Lattice-QC-LDPC码就成为两种具有对偶关系的确定性girth-8 QC-LDPC码。

参 考 文 献

[1] Zhang G H and Wang X M. Construction of low-density parity-check codes based on frequency-hopping sequences [J]. *Chinese Journal of Electronics*, 2009, 18(1): 141–144.

[2] 张国华, 王新梅. 利用双重扩展RS码及循环MDS码构造实用化的LDPC码[J]. 通信学报, 2008, 29(6): 100–105.
Zhang G H and Wang X M. Applied quasi-cyclic LDPC codes from doubly-extended RS code and cyclic MDS code [J]. *Journal on Communications*, 2008, 29(6): 100–105.

[3] Esmaeili M and Gholami M. Maximum-girth slope-based quasi-cyclic (2,k$\geq$5) low-density parity-check codes [J]. *IET Communications*, 2008, 2(10): 1251–1262.

[4] Zhang H and Moura J M F. Geometry based designs of LDPC codes [C]. Proceedings of the IEEE International Conference on Communications(ICC'04), Paris, France, 2004: 762–766.

[5] 陶雄飞, 刘卫忠, 邹雪城. 利用几何图形构造不含小环的LDPC码[J]. 系统工程与电子技术, 2007, 29(11): 1965–1968.
Tao X F, Liu W Z, and Zou X C. Construction of LDPC codes without small cycles based on geometry [J]. *Systems Engineering and Electronics*, 2007, 29(11): 1965–1968.

[6] 范俊, 肖扬, 李门浩 .一种围数为八的低密度校验码校验矩阵设计[J]. 北京交通大学学报, 2007, 31(2): 10–14.
Fan J, Xiao Y, and Lee M H. Design of parity check matrices of LDPC codes with girth 8 [J]. *Journal of Beijing Jiaotong University*, 2007, 31(2): 10–14.

[7] Wang Y, Yedidia J S, and Draper S C. Construction of high-girth QC-LDPC codes[C]. 5th International Symposium on Turbo Codes and Related Topics, Lausanne, Switzerland, 2008: 180–185.

[8] 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.

[9] Lu J and Moura J M F. Structured LDPC codes for high-density recording: large girth and low error floor [J]. *IEEE Transactions on Magnetics*, 2006, 42(2): 208–213.

[10] Vasic B, Pedagani K, and Ivkovic M. High-rate girth-eight low-density parity-check codes on rectangular integer lattices [J]. *IEEE Transactions on Communications*, 2004, 52(8): 1248–1252.

张国华： 男，1977年生，博士生，高级工程师，研究方向为信道编码理论.

陈 超： 男，1981年生，博士生，研究方向为信道编码理论.

杨 洋： 男，1981年生，博士生，研究方向为信道编码理论.

王新梅： 男，1937年生，教授，博士生导师，研究方向为信道编码理论、密码学.