一种优化 Girth 分布的准循环 LDPC 码设计方法研究

徐 华　　徐澄圻
(南京邮电大学通信与信息工程学院　南京　210003)

摘　要：在准循环 LDPC 码的构造中，校验矩阵拥有尽可能好的 girth 分布对于改善码的性能有着重要的意义。该文提出了构造准循环 LDPC 码的 GirthOpt-DE 算法，优化设计以获得具有好 girth 分布的移位参数矩阵为目标。仿真结果表明，该文方法得到的准循环 LDPC 码在 BER 性能和最小距离上均要优于固定生成函数的准循环 LDPC 码，Arrary 码和 Tanner 码，并且使用上更为灵活，可以指定码长，码率及尽可能好的 girth 分布。

关键词：准循环 LDPC 码；差分进化；Girth 分布；最小距离
中图分类号：TN911.22　　**文献标识码**：A　　**文章编号**：1009-5896(2008)07-1640-04

A Method for Designing Quasi-Cyclic LDPC Codes Based on Girth Optimization

Xu Hua　Xu Cheng-qi
(*College of Communications and Information Engineering*, *Nanjing University of Posts & Telecommunications*, *Nanjing* 210003, *China*)

Abstract: The key to improving the performance of QC LDPC codes is how to construct a parity-check matrix $\boldsymbol{H}$ with a girth distribution as good as possible. In this paper, a novel algorithm for constructing QC LDPC codes, GirthOpt-DE algorithm, is proposed, which achieves a good girth distribution based on the differential evolution. Simulation results show that the performance of the QC LDPC codes constructed with the proposed algorithm is superior to Array codes and Tanner codes in both BER and the minimum distance. Besides, the proposed algorithm is more flexible for designing the QC LDPC codes with desired block length and rate as well as good girth.

Key words: QC LDPC codes; Differential evolution; Girth distribution; Minimum distance

1　引言

LDPC 码的构造研究对于进一步推动 LDPC 码的实际应用，有着重要意义。LDPC 码的构造方法中基于循环置换矩阵(circulant permutation matrix)的方法由于其编码的简单以及易于进行性能分析，受到相当的重视[1−3]。而准循环(Quasi Cyclic, QC) LDPC 码由于能够采用移位寄存器进行线性时间的编码，非常适合于高速 VLSI 的设计[4]，有着很好的应用前景。LDPC 码的 $\boldsymbol{H}$ 矩阵及对应的 Tanner 图的 girth(最短长度环)分布对于码的性能有着重要的影响，通过改善 girth 分布可以有效地改善相应的码的性能[5−8]。

在基于循环置换矩阵方法的码构造中，Tanner 码[1]和 Array 码[3]的不足之处是构造不够灵活，不能通过改善 girth 分布来获得更好的性能。针对这个问题，本文提出一种准循环 LDPC 码的设计方法，该方法采用优化技术结合 girth 检测算法，来得到具有尽可能好的 girth 分布(即有尽可能大的 girth 以及长度为 girth 的短环尽可能的少)的 $\boldsymbol{H}$ 矩阵，以期有较好的码性能。

2006-12-18 收到，2007-06-18 改回

2　移位参数矩阵的 Girth 检测

QC LDPC 码的 $\boldsymbol{H}$ 矩阵一般由基矩阵以及基矩阵的循环移位累积堆砌而成。基矩阵一般可选取大小为 $P\times P$ 的单位阵，定义基矩阵为 $\boldsymbol{B}$，经循环移位 i 得到的子矩阵为 $\boldsymbol{B}^i, i\in\{0,1,\cdots,P-1\}$，而移位参数矩阵指由每个子矩阵对应的循环移位位数组成的矩阵(也称为 $\boldsymbol{S}$ 矩阵)，令矩阵中的元素为 $s_{jk}, (0\le j\le J-1, 0\le k\le K-1)$ (注：$i=s_{jk}$)，则 $\boldsymbol{H}$ 矩阵可以表示为由 $B^{S_{jk}}$ 累积堆砌而成，其中 $J\times K$ 为 $\boldsymbol{S}$ 矩阵的大小，而最终的 $\boldsymbol{H}$ 矩阵的大小则为 $JP\times KP$，由于每个子矩阵均为单位阵及其循环移位阵，子矩阵的每行每列均只有一个“1”，因此 $\boldsymbol{H}$ 矩阵表示了列重、行重分别为 J，K 的规则 LDPC 码。

移位参数矩阵中的每一个元素对应着一个大小为 $P\times P$ 的子矩阵，就移位参数矩阵的 girth 检测，在 Fossorier 的基础上[2]，本文给出了以下的定理。

定理 1　在移位参数矩阵 $\boldsymbol{S}$ 中，元素 $s_1, s_2, \cdots, s_{2n}$ 构成一个短环的充要条件为沿某一确定方向(行或列)的模 P 和为零，即

$$s_2-s_1+s_4-s_3+\cdots+s_{2n}-s_{2n-1} = 0 \mod P \tag{1}$$

定理 1 是 girth 检测的基础，$\boldsymbol{S}$ 矩阵的 girth 检测方法主要步骤为：循环遍历移位参数矩阵中的每个元素，根据定理 1 计算相应的模 P 和，并判断是否为零，以确定是否有短环的存在，一旦检测到有 4girth 或者 6girth，则放弃该矩阵，重新搜索 $\boldsymbol{S}$ 矩阵，这样可以保证得到的移位参数矩阵至少为 8girth。由于 $\boldsymbol{S}$ 矩阵相对较小，循环遍历计算其中相应元素的模 P 和，进而判断相应的 girth 是可能的。如果需要判断 8girth 的个数，则在判断时，当模 P 和为 0 时，累计和为 0 的次数，即为 8girth 的个数。

得到移位参数矩阵的 girth 分布后，移位参数矩阵的 girth 和据此构建的 $\boldsymbol{H}$ 矩阵的 girth 间有着对应的关系，在定理 1 的基础上有如下的推论。

推论 1　移位参数矩阵中的元素 $s_1,s_2,s_3,s_4,\cdots,s_{2n}$ 构成一个短环，则由此构建的 $\boldsymbol{H}$ 矩阵存在对应的 P 个同样的短环(P 为子矩阵的阶数)。

QC LDPC 码可以通过移位参数矩阵 $\boldsymbol{S}$ 来描述、生成，根据推论 1，通过对 $\boldsymbol{S}$ 矩阵的 girth 检测可以得到相应的 $\boldsymbol{H}$ 矩阵的 girth 分布，而 $\boldsymbol{S}$ 矩阵的大小要比 $\boldsymbol{H}$ 矩阵小得多，它的 girth 检测相对要容易得多。

3　一种基于优化 girth 分布的准循环码构造方法：GirthOpt-DE 算法

QC LDPC 码的构造方法中，生成函数的形式主要有用于 Tanner 码[1,2]和用于 Array 码[3]两种。Tanner 码和 Array 码都属于固定生成函数构造出的码，固定生成函数构造 QC LDPC 码具有简单方便的优点，且有些构造的码性能也很好，但是同时也有着构造不够灵活的不足。

差分进化(Differential Evolution, DE)是一种并行，直接的搜索技术，它对于解决具有连续空间参数的非线性代价函数最小化问题十分有效，本文尝试将差分进化技术推广应用于移位参数矩阵的优化搜索中，提出一种优化 girth 分布的准循环码构造方法，GirthOpt-DE 算法，优化的直接目标是使得移位参数矩阵对应的 $\boldsymbol{H}$ 矩阵具有好的 girth 分布，即 girth 尽可能的大，而大小等于 girth 的短环数目尽可能的少。优化搜索过程中应消除 4girth 和 6girth。

算法具体步骤如下：

(1)初始化　对于第一代(G=0)代价函数，随机选择 NP 个 L 维矢量 $\boldsymbol{p}_{i,G}$(i=0,1,⋯,NP−1，NP 取 10*L，L 为移位参数矩阵中的非零元素个数)。对于每个 $\boldsymbol{p}_{i,G}$，根据第 2 章中的方法进行 girth 检测，搜索时，确定的目标是待优化的矢量(即 $\boldsymbol{S}$ 矩阵)没有长度为 4 和 6 的短环，因而将环长为 8 的环的个数作为代价函数值，对于存在长度为 4 和 6 的短环的矢量，将其代价函数直接置为最大值 MAXVALUE，保证在后面的比较中将其去除。如果搜索到的矢量中没有环长为 4、6 以及 8 的，则重新调整代价函数，而将环长为 10 的数目设为代价函数值。在保存的代价函数值 $f_{u_i,G}$ 中，找出最小的 $f_{u_i,G}$ 对应的 $\boldsymbol{p}_{i,G}$，标记为最优矢量 $\boldsymbol{p}_{\mathrm{best},G}$。

(2)进化　令新的一代为 G+1，根据进化方案再生成新的矢量，对于每一个 i，$i\in\{0,1,\cdots,\mathrm{NP}-1\}$，在[0,NP−1]中随机选择 4 个除该 i 外的不相同的整数 $r1,r2,r3,r4$，据此执行下面的进化方案：

$$\boldsymbol{v}_{i,G+1}=\boldsymbol{p}_{\mathrm{best},G}+F*(p_{r1,G}-p_{r2,G}+p_{r3,G}-p_{r4,G}) \quad (2)$$

式中 F 为进化过程的控制常数，仿真中取 0.9(经验值)。对于得到的每一个新的矢量 $\boldsymbol{v}_{i,G+1}$，可以按照步骤(1)的方法，再得到新的代价函数 $f_{v_i,G+1}$。

(3)比较，更新　对于每一个 i，$i\in\{0,1,\cdots,\mathrm{NP}-1\}$，如果代价函数 $f_{u_i,G}>f_{v_i,G+1}$，则令 $\boldsymbol{p}_{i,G+1}=\boldsymbol{v}_{i,G+1}$；否则，置 $\boldsymbol{p}_{i,G+1}=\boldsymbol{p}_{i,G}$，经过两代代价函数的比较、更新，得到了新一代的矢量集$\{\boldsymbol{p}_{i,G+1}\}$，比较后找出最小的代价函数 $f_{v_i,G+1}$，记为 $f_{u_{\mathrm{best}},G+1}$，而拥有最小代价函数的矢量定义为 $\boldsymbol{p}_{\mathrm{best},G+1}$。

(4)停止准则　如果迭代次数没有达到最大迭代次数，则返回步骤(2)，继续搜索；否则停止搜索，此时的最优矢量对应于具有最好 girth 分布的移位参数矩阵。

通过数值优化技术，在搜索的过程中，待优化矢量即移位参数矩阵中的非零元素，能够朝着好的 girth 分布的方向进化，与固定生成函数相比，该算法通过优化搜索得到移位参数矩阵，方式更为灵活，通过仿真可以证明所构造的码性能有了较明显的改善。

4　数值仿真与性能分析

为了更好地比较分析文中给出的构造方法，选择如下码参数，码长分别为 192, 305, 504 和 1032；对应的子矩阵阶数分别为 32, 61, 84, 172；设计码率和(列重，行重)，除 305 码长为 2/5 和(3,5)，其余的码均为 1/2 和(3,6)。下面的仿真中，Tanner 方法构造移位参数矩阵对应的 QC LDPC 码称为 Tanner 码，如码长 1032，则称为 Tanner1032 码，其余类推。

4.1 优化构造出的移位参数矩阵

表 1 所示为优化搜索得到的前文给出的码参数的 QC LDPC 码的移位参数矩阵，以及对应的 girth 分布，为便于表示，表中给出的是移位矩阵中的非零元素。

从上述结果可见，DE1032 码和 DE192 码对应的矩阵为 8girth；DE305 码和 DE504 码达到了 10girth；DE305 码和 Tanner305 码均为 10girth，但是 DE305 码的最小环长的数目要小于 Tanner305 码。接着从最小距离和 BER 性能仿真两个方面分别对这几种 QC LDPC 码进行评价和比较。

4.2 最小距离的评价比较

LDPC 码仍然是一种线性分组码，最小距离是评价码性能的重要参数，本文采用 ANC(Approximately Nearest Codewords)算法[9]对前面得到的 QC LDPC 码进行了评价比较，结果如表 2 所示。

表 1 DE 码的移位参数矩阵及与 Tanner 码，Array 码的比较

	移位参数矩阵	girth 分布
DE1032	$\begin{bmatrix}125,144,63,94,119,\\53,97,120,76,106\end{bmatrix}$	8girth(Tanner1032: 6girth)
DE305	$\begin{bmatrix}56,6,38,53,\\45,4,9,26\end{bmatrix}$	10girth (Tanner305:10girth) DE305 环长为 10 的数目为 $8P$,Tanner305 为 $20P$; P=61
DE504	$\begin{bmatrix}34,72,64,83,36,\\25,1,81,66,41\end{bmatrix}$	10girth(Array504: 6girth)
DE192	$\begin{bmatrix}21,3,28,8,17,\\23,31,1,27,11\end{bmatrix}$	8girth(Array192: 6girth)

表 2 几种 QC LDPC 码的最小距离

码长	1032(DE/Tanner)	305(DE/Tanner)	504(DE/array)	192(DE/array)
最小距离	24/22	22/20	24/10	10/6

从表 2 的结果来看，由于采用了移位参数矩阵的 girth 优化，本文提出的 GirthOpt-DE 方法得到的 QC LDPC 码的最小距离好于 Array 码和 Tanner 码。需要说明的是对于 QC LDPC 码而言，增加码长并不一定能使得码的最小距离得到改善，它只是在中短码长的情况下有着较好的性能，而在码长较长时，随机构造的 LDPC 码仍然是很好的选择。

4.3 BER 性能的分析比较

BER 性能的仿真中，考虑在 AWGN 信道下，BPSK 调制，采用 BP 译码算法，最大的译码迭代次数设定为 50 次，图 1 所示为码长 1032 及 305 时 DE 码与 Tanner 码的 BER 性能比较，图 2 所示为码长 504 及 192 时 DE 码与 Array 码的 BER 性能比较。

从图 1 和图 2 中的结果可以看出，本文提出的方法得到的 DE 码性能均优于 Tanner 码和 Array 码，说明本文方法得到的 QC LDPC 码的 $\boldsymbol{H}$ 矩阵通过改善 girth 分布提高了码的性能。

文中的 GirthOpt-DE 方法在码长较短的时候，提高了相应 QC LDPC 码的性能，但是随着码长的进一步增加，一方面由于 QC LDPC 码的最小距离有着上界的限制，另一方面

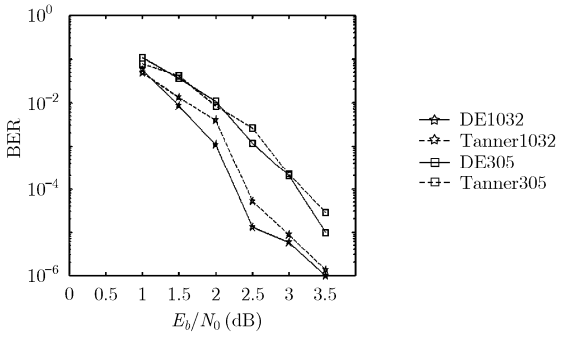

图 1 DE 码和 Tanner 码的 BER 性能比较

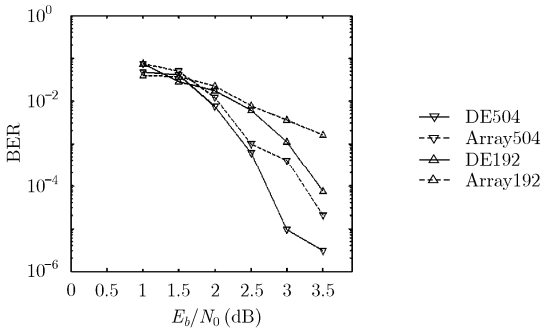

图 2 DE 码和 Array 码的 BER 性能比较

码长进一步增加后，girth 对于译码算法的性能影响也会越来越小[2]，因此中短码长情况下利用文中方法可以构造好 girth 分布的 QC LDPC 码，因而在中短码长约束条件下有较好应用前景；而当码长较长时，可以考虑随机构造方法，两者可以互相补充。

5 结束语

本文提出了一种新的 QC LDPC 码构造方法，它以优化 girth 分布为目标，利用差分进化技术来并行搜索具有好 girth 分布的移位参数矩阵，进而构造出好 girth 分布的 H 矩阵，通过仿真给出了相应的 4 种典型码长和码率参数的 QC LDPC 码的移位参数矩阵，最后从最小距离和 BER 性能两个方面对于本文所提方法构造的 QC LDPC 码，DE 码，进行了评价，并分别和 Tanner 码及 Array 码进行了比较。仿真结果表明，GirthOpt-DE 算法构造的 QC LDPC 码在最小距离和 BER 性能两方面均优于目前代表性方法构造出的 QC LDPC 码：Tanner 码和 Array 码。但是如何从理论上进一步地探讨或者证明本文的搜索结果是否是最优的，是需要进一步考虑的问题。

参 考 文 献

[1] Tanner R M, Sridhara D, and Sridhara A, *et al.*. LDPC block and convolutional codes based on circulant matrices[J]. *IEEE Trans. on Inform. Theory*, 2004, 50(12): 2966–2984.

[2] Fossorier M. Quasi-cyclic low-density parity-check codes from circulant permutation matrices[J]. *IEEE Trans. on Inform. Theory* , 2004, 50(8): 1788–1793.

[3] Fan J L. Array codes as low-density parity-check codes[C]. In Proc. 2nd Int. symp. turbo codes and related topics, brest, France, sept. 4-7, 2000: 553–556.

[4] Yoshida K, Brockman J, and Costello D, *et al.*. VLSI implementation of quasi cyclic LDPC codes[C]. In Proc.2004 Int. Symp. Information Theory and its Application, Italy, Oct.10-13, 2004: 551–556.

[5] Chen Z G and Bates S. Construction of low-density parity-check convolutional codes through progressive edge-growth [J]. *IEEE Communications Letters*, 2005, 9(12): 1058–1060.

[6] Ko Y J and Kim J H. Girth conditioning for construction of short block length irregular LDPC codes [J]. *Electronics Letters*, 2004, 40(3): 187–188.

[7] Milenkovic O. Shortened array codes of large girth[J]. *IEEE Trans. on Inform. Theory*, 2006, 52(8): 3707–3722.

[8] Mao Y M and Banihashemi A H. A heuristic search for good low-denstiy parity-check codes at short block lengths[C].In IEEE ICC2001, St.-Petersburg, Russia, June 11-15, 2001: 41–44.

[9] Hu X Y and Fossorier M. On the computation of the minimum distance of low-density parity-check codes [C]. In IEEE ICC2004, Paris, France, June 20-24, 2004: 767–771.

徐　华：　男，1975 年生，博士生，讲师，研究方向为 LDPC 码结构设计及应用.

徐澄圻：　男，1942 年生，教授，博士生导师，研究方向为 MIMO、纠错编码等现代通信中信号与信息处理的相关理论与应用研究.