一种低密度奇偶校验码的几何构造方法

汪晓光[1)] 龙沪强[2)] 张罗鸣[1)] 宫良[1)]

[1)](上海交通大学图像通信与信息处理研究所,上海 200240)

[2)](上海交通大学电子工程系,上海 200240)

摘 要 提出了一种新的 QC-LDPC 码的几何构造法,通过该方法构造出来的码字,其校验矩阵的最小环长为 8,有效地保证了码字性能。由于校验矩阵是由一系列循环子矩阵组成的,编码器的硬件结构简单。通过仿真结果表明,这种码字在具有较低的编码复杂度的同时,拥有良好的译码性能。

关键词 准循环-低密度奇偶校验 几何构造法 最小环长 低编码复杂度

中图法分类号:TN911.22 **文献标识码**:A **文章编号**:1006-8961(2008)10-2027-04

A Method for Geometric Construction of Low-density Parity-check Codes

WANG Xiao-guang[1)], LONG Hu-qiang[2)], ZHANG Luo-Ming[1)], GONG Liang[1)]

[1)](*Institute of Image Communication and Information Processing, Shanghai Jiaotong University, Shanghai* 200240)

[2)](*Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai* 200240)

Abstract A new method for geometric construction of QC-LDPC is proposed. The parity-check matrix constructed through this method has a girth more than eight, which promises good performance. Since the parity-check matrix is composed of cyclic sub-matrices, the hardware encoder is simple. Simulations show that this type of LDPC codes has remarkable performance with low encoding complexity.

Keywords QC-LDPC, geometric construction, girth, low encoding complexity

1 引 言

低密度奇偶校验(low density parity check, LDPC)码是由 Gallager 于 1962 年提出的[1],但之后并未受到足够的重视。经过了数十年的沉寂,随着计算机能力的提升和相关理论的发展(如图论,置信传播,Turbo 码等),Mackay 和 Neal 于 1996 年重新发现了 LDPC[2]。目前,LDPC 被广泛应用于各类通信系统中,如欧洲的 DVB-S2 系统以及中国的数字电视地面传输标准。

LDPC 码字的构造是研究中的一个重要方面。构造的方法有很多种,主要可以归结为两类:伪随机构造法和结构化构造法。通常在构造长码时,伪随机构造法构造出的码字性能优于后者,但是其编码的硬件复杂度较高。相对而言,结构化的 LDPC 码编码的硬件实现较为简单,并且通过合理的码字结构设计(如增加最小环长等),也能达到与伪随机构造法相当的性能。因此,结构化的 LDPC 码成为了当前信道编解码研究领域的一个热点。例如,Zhang 和 Xu 等人提出了一种利用 3 维的点阵构造的 LDPC 码,就具有良好的译码性能和较低的编码复杂度[3,4]。

本文提出了一种新的规则的准循环(quasi-cyclic, QC)LDPC 码的构造方法,其基本思想是采用了几何图形的概念,因此,可以称作几何构造法。

基金项目:国家 863 计划项目(2007AA01Z296);教育部科学技术研究重点资助项目(108140)

收稿日期:2008-07-12;**改回日期**:2008-07-30

第一作者简介:汪晓光(1984~),男。上海交通大学通信与信息系统专业硕士研究生。主要研究领域为信道编解码技术。

E-mail:wxg1984@sjtu.edu.cn

用这种方法构造出的 LDPC 码的最小环长为 8,具有出色的译码性能,并且编码器的硬件实现简单,只需要一系列的移位寄存器就能满足要求,其复杂度与码长成线性关系[5]。

2　几何构造法

(1)设要构造的规则 LDPC 码的行重和列重分别为 R 和 C,则先设置一个大小为 $C \times R$ 的点阵,我们将其称为 RC 点阵。不失一般性,选取 $C = 3$,$R = 6$,并且对每个点按顺序编号,这些点就可以表示为 $A_i(i = 1,2,\cdots,18)$,如图 1 所示。

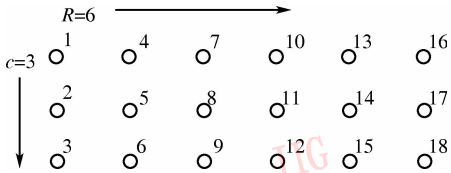

图 1　RC 点阵,$R = 6$,$C = 3$

Fig. 1　RC lattice, $R = 6$, $C = 3$

(2)任意选取 RC 点阵中的 3 个点,以其为顶点构造三角形,并将构造出的三角形定义为 RC 阵三角形(作为一种特殊情况,选取的三点可能够成一条直线,但为了表述的一般性,本文一律将其统称为 RC 阵三角形),如图 2 所示。

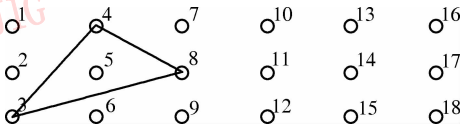

图 2　在 RC 点阵中构造三角形

Fig. 2　An example of RC triangles in RC lattice

以同样的方式,在 RC 点阵中总共构造 $R \times R = 36$ 个这样的 RC 阵三角形,并且要满足以下两个条件:

①对于点阵中的每个点,以其作为顶点的 RC 阵三角形的个数均为 R 个;

②任意两个 RC 阵三角形之间没有相同的边,即最多只有一个共同的顶点。

上述两个限制条件的目的都是在于保证构造出的校验矩阵 $\boldsymbol{H}$ 满足特定的要求,前者保证了校验矩阵的行重为 6,后者保证了校验矩阵中无 4 环。对此的具体解释将在本节的最后给出。

(3)对于一个 RC 阵三角形,可以将其每个顶点 $A_i(i = 1,2,\cdots,18)$ 扩展为一组个数为 Q 的点集 $\{a_{i1}, a_{i2}, \cdots, a_{iQ}\}$ 并对每个点按顺序编号,点 a_{ij} 的编号为 $(i-1)Q + j$。经过这样的处理,就可以将 RC 阵三角形转变为一个列数为 3 的点阵,点阵的每一列对应于 RC 阵三角形的一个顶点,如图 3 所示。不失一般性,这里选取 $Q = 136$。对每个 RC 阵三角形做同样的处理,就可以得到 $R \times R = 36$ 个这样的点阵,将其称为 Q 点阵。

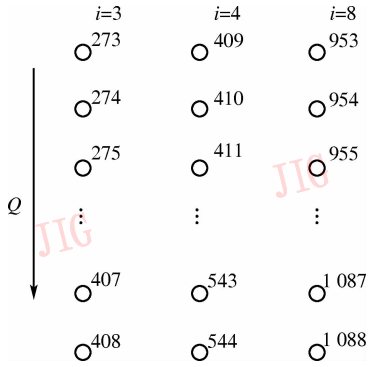

图 3　对 RC 三角形经过处理后得到的 Q 点阵

Fig. 3　Q lattice transformed from RC triangle

(4)在每个 Q 点阵中构造出一组全等三角形(为了与之前的 RC 阵三角形区别开,将其称为 Q 阵三角形),每个三角形的顶点取自不同的列,每个 Q 阵中全等三角形的个数为 Q,如图 4 所示。

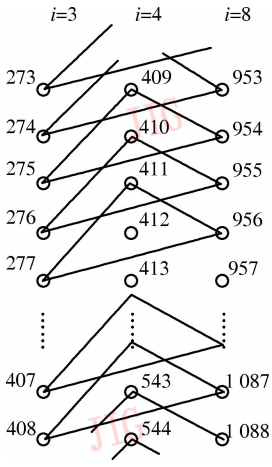

图 4　在每个 Q 点阵中构造一组全等的三角形

Fig. 4　Building congruent triangles in Q lattice

特别要指出的是,对于不同的 Q 点阵可以构造不同形状的 Q 阵三角形。这样总共 $R \times R$ 个 Q 点阵就得到了 $R \times R \times Q$ 个 Q 阵三角形。

(5)利用这些 Q 阵三角形来构造行数为 $R \times C \times Q$,列数为 $R \times R \times Q$ 的校验矩阵 $\boldsymbol{H}$。$\boldsymbol{H}$ 的每一

列代表一个 Q 阵三角形，在这一列中，将 Q 阵三角形顶点编号所对应的元素设为 1，其余元素设为 0。这样构造出的校验矩阵 $\boldsymbol{H}$ 是行重为 $R=6$，列重为 $C=3$ 的规则矩阵。

实际上，校验矩阵 $\boldsymbol{H}$ 是一个准循环矩阵，由大小为 $Q\times Q$ 的一系列子矩阵组成，这些子矩阵要么是元素全为 0 的矩阵，要么是由单位阵 $\boldsymbol{I}$ 循环移位得到的，称为置换矩阵。

如果用特定的数值来代表子矩阵，则可以得到一个比较小的矩阵，将其称为 $\boldsymbol{H}$ 矩阵的母矩阵，

$$\boldsymbol{H}_{\mathrm{M}}=\begin{bmatrix}0&0&0&0&0&0&\cdots&42&0\\0&0&0&0&0&38&\cdots&0&0\\26&83&0&0&0&0&\cdots&0&0\\0&0&0&0&0&0&\cdots&0&133\\73&0&129&0&0&0&\cdots&0&0\\0&72&136&0&0&0&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&0&0&0&135&\cdots&0&0\\0&0&0&0&0&0&\cdots&0&0\end{bmatrix}$$

$\boldsymbol{H}_{\mathrm{M}}$ 矩阵中的每个元素代表的均是一个大小为 $Q\times Q$ 的子矩阵，元素“$\boldsymbol{0}$”代表的是全零矩阵，而非零元素代表的是置换矩阵，其数值大小为循环移位次数加一，取值范围是从“1”到“Q”。根据选取的参数 $R=3$，$C=6$，得到的 $\boldsymbol{H}_{\mathrm{M}}$ 是一个大小为 18×36，行重为 6，列重为 3 的规则矩阵。

在这里，给出对构造步骤(2)里面的两个限定条件的解释。实际上，母矩阵 $\boldsymbol{H}_{\mathrm{M}}$ 中的每一行对应于 RC 点阵中的一个点，每一列对应的是一个 RC 阵三角形，而列中的三个非零元素对应于三角形的 3 个顶点。条件①的作用在于确保 $\boldsymbol{H}_{\mathrm{M}}$ 中每行的非零元素的个数为 R，这样也就确保了校验矩阵 $\boldsymbol{H}$ 的行重为 R，满足了度分布的要求。而条件②则保证了 $\boldsymbol{H}_{\mathrm{M}}$ 中任意两列之间最多只有一个位置上同时出现非零元素，避免了 4 环的存在，也进一步排除了校验矩阵 $\boldsymbol{H}$ 中 4 环存在的可能性。

3 改进最小环长

由于 LDPC 译码时信息传播的特点，校验矩阵中的小环会对译码性能产生较大的影响，因此，构造时总是希望最小环长尽可能的大[6,7]。通过上述几何方法构造出来的校验矩阵，避免了 4 环的存在，使得译码性能不会受到因 4 环带来的恶劣影响。通过对步骤(4)中 Q 阵三角形的构造给出某种限定，可以去掉校验矩阵 $\boldsymbol{H}$ 中的 6 环，得到最小环长为 8 的矩阵，提高译码性能。

对于 Q 阵三角形，将其某两个顶点所在行的行数差，定义为这两个点相互之间的斜率，记为 $Slope$。斜率是存在方向性的，其大小的变化范围为 $-(Q-1)$ 到 $Q-1$ 之间。由于 Q 阵中的所有三角形是全等三角形，所以它们顶点的斜率都是相同的，可以用 i 的值来标记。如图 5 所示，$Slope_{m\to n}=-5$，$Slope_{n\to k}=2$，$Slope_{k\to m}=3$。3 个斜率之间满足如下关系：

$$Slope_{m\to n}+Slope_{n\to k}+Slope_{k\to m}=0 \tag{1}$$

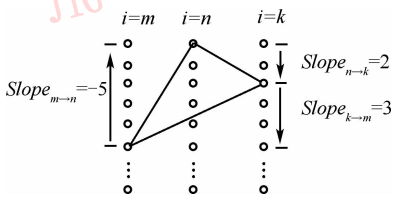

图 5 Q 阵三角形顶点间的斜率

Fig. 5 Slopes of vertexes in Q triangles

为了避免生成的校验矩阵中 6 环的存在，需要对 Q 阵三角形顶点间的斜率给出一定的限制条件：当有 3 列($i=a$，$i=b$，$i=c$)分别两两存在于 3 个 Q 点阵时，其斜率之间的关系只要满足式(2)给的条件，就可以避免校验矩阵 $\boldsymbol{H}$ 中存在 6 环，反之，则会导致 $\boldsymbol{H}$ 中出现 6 环。

$$Slope_{a\to b}+Slope_{b\to c}+Slope_{c\to a}\neq 0 \tag{2}$$

如图 6 所示，$i=2$ 的列和 $i=18$ 的列同时存在于(a)所示的 Q 点阵中，斜率 $Slope_{2\to 18}=-3$；$i=18$ 的列和 $i=13$ 的列同时存在于图 6(b)所示的 Q 点阵中，斜率 $Slope_{18\to 13}=9$；$i=13$ 的列和 $i=2$ 的列同

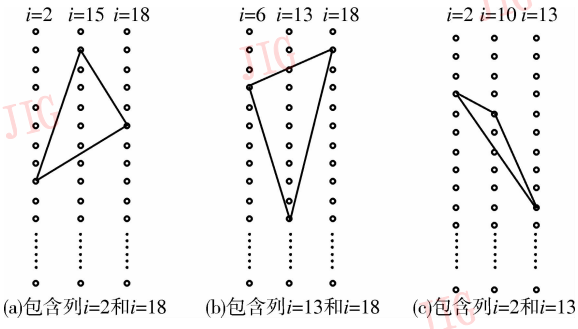

图 6 会导致六环存在的例子

Fig. 6 A example leading to girth 6

时存在于图6(c)所示的 Q 点阵中,斜率 $Slope_{13\to 2} = -6$。三者之间的关系为

$$Slope_{2\to 18} + Slope_{18\to 13} + Slope_{13\to 2} = (-3) + 9 + (-6) = 0 \quad (3)$$

其并不满足式(2)给出的条件,将会导致校验矩阵中 6 环的存在。

为了避免 6 环,在构造 Q 阵三角形时,需要对顶点间的斜率大小进行适当选取,以满足式(2)给出的条件,这样构造出来的校验矩阵的最小环长为 8,进一步提高了码字性能。

4　仿真分析

为了验证码字的性能,需要对上述几何法构造出的码字进行仿真,仿真信道采用的是 AWGN 信道,调制方式为 BPSK 调制。并将其与 Mackay 给出的相同码长、相同度分布的 LDPC 码进行比较。

仿真选取的码字度分布为(3,6),码长为4 896,信息位个数为 2 448,译码最大迭代次数为 50 次,仿真结果如图 7 所示。从仿真结果可以看出,本文提出的用几何方法构造的 QC-LDPC 码性能略好于 Mackay 码,原因在于 Mackay 码仅是避免了校验矩阵中四环的存在,而几何构造法进一步去除了 6 环,使得码字具有更好的译码性能。

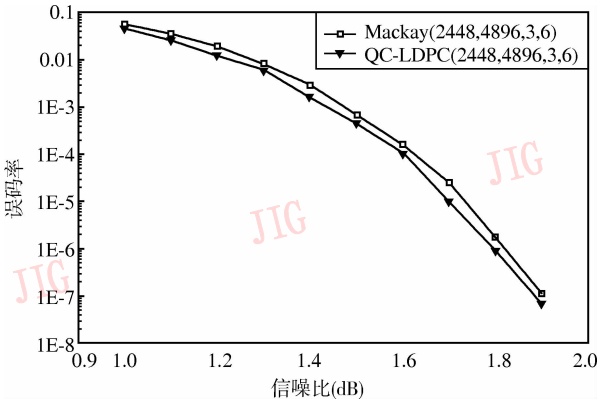

图 7　QC-LDPC 与 Mackay 码的性能比较

Fig. 7　Performance comparison between QC-LDPC and Mackay

5　结　论

本文提出了一种新的 LDPC 码的几何构造法,相比于文献[3]、[4]、8]中采用直线的方法,增加了构造的灵活性,也扩大了码字性能提升的空间。事实上,本文提出的几何构造法,同样适用于构造其他度分布的规则 QC-LDPC 码,只是要作相应的一些变化。例如,构造列重为 4 的码字时,不是通过构造三角形,而是通过构造四边形来生成校验矩阵。

同时,通过给出的限定条件,保证了校验矩阵的最小环长为 8,提升了性能。通过仿真发现,用该种方法构造出来的码字有良好的译码性能,并且由于校验矩阵是由一些循环子矩阵组成的,编码时只需由一系列的移位寄存器就能实现,编码器结构简单,因此,这种码有较强的实用性,在宽带无线视频传输中有着良好的应用前景。

参考文献(References)

1　Gallager R G. Low-density parity-check codes [J]. IEEE Transactions on Information Theory, 1962, **8**(1): 21 ~ 28.

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

3　Zhang F, Xu Y, Mao X, *et al*. High girth LDPC codes construction based on combinatorial design [A]. In: Proceedings of Vehicular Technology Conference[C], Stockholm, Sweden, 2005, 591 ~ 594.

4　Xu Y, Wei G. On the construction of quasi-systematic block-circulant LDPC codes [J]. IEEE Communications. Letters, 2007, **11**(1), 886 ~ 888.

5　Li Zong-wang, Chen Lei, Zeng Ling-qi, *et al*. Efficient encoding of quasi-cyclic low-density parity-check codes [J]. IEEE Transactions on Communications, 2006, **54**, (1): 71 ~ 81.

6　Yang Lei, Liu Hiu, Shi Richard. Cycle elimination method to construct VLSI oriented LDPC codes [A]. In: Proceedings of Vehicular Technology Conference[C], Stockholm, Sweden, 2005: 522 ~ 526.

7　Zhong Hao, Zhang Tong. Block-LDPC: A practical LDPC coding system design approach [J]. IEEE Transactions on Circuits and Systems, 2005, **52**, (4): 766 ~ 775.

8　Vasic B, Milenkovic O. Combinatorial constructions of low-density parity-check codes for iterative decoding[J]. IEEE Transactions on Information Theory. 2004, **50**(6): 1156 ~ 1176