

准循环多进制 LDPC 码构造

杨 民^① 张文彦^② 钟 杰^{*②} 吴 杰^②

^①(同方电子科技有限公司 九江 332000)

^②(浙江大学信息与通信工程研究所 杭州 310027)

摘 要: 该文研究准循环多进制 LDPC 码的构造, 给出多进制 LDPC 码的设计流程和构造方法。详细讨论了多进制 LDPC 码的性能影响因素, 综合考虑了环长和环的连通性对性能的影响, 研究了母矩阵扩展中偏移因子的选择以及 $GF(q)$ 上非零元素替代。同时提出了次优解的搜索方法, 以降低搜索复杂度。最后, 将提出的方法用于不同阶数下 LDPC 码的构造。仿真结果表明, 通过新方法构造得到的多进制 LDPC 码与二进制码相比, 在 BPSK 调制方式下在误帧率 10^{-4} 附近有 0.2 dB 的性能提升; 在有限域阶数与调制阶数匹配的情况下, 有更大的性能提升。与相近码长, 相同码率的多进制循环码相比, 该文构造得到的多进制 LDPC 码在误帧率 10^{-4} 附近有 0.25 dB 的性能提升。

关键词: 多进制 LDPC; 码构造; 环长; 满秩条件

中图分类号: TN911.22

文献标识码: A

文章编号: 1009-5896(2013)02-0297-06

DOI: 10.3724/SP.J.1146.2012.00403

Construction of Non-binary QC-LDPC Codes

Yang Min^① Zhang Wen-yan^② Zhong Jie^② Wu Jie^②

^①(Tong Fang Electronic Technology Co., Ltd., Jiujiang 332000, China)

^②(Institute of Information and Communication Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: The construction of non-binary quasi-cyclic low-density parity-check codes are investigated. Important factors that influence the performance of non-binary LDPC codes are discussed in detail. The circle length and connectivity are taken into account in the construction. The selection of shift values to extend the mother matrix and the replacement of non-zero elements over $GF(q)$ for the parity check matrix are studied. Meanwhile, a suboptimum method with lower complexity is proposed to search for the solution according to the new formula. The method is applied to the construction of non-binary LDPC codes over different Galois fields. Simulation results show that the codes constructed by this method outperform the corresponding binary codes by 0.2 dB at FER around 10^{-4} on the BPSK AWGN channel. The performance gap is larger when the order of the Galois field equals the order of the modulation. Compared with non-binary cycle code with the same code rate and approximate code length, the constructed non-binary LDPC code gets an improvement of 0.25 dB at FER around 10^{-4} .

Key words: Non-binary LDPC; Code construction; Girth; Full Rank Condition (FRC)

1 引言

LDPC 码是一种具有接近香农极限的优秀信道编解码方案。文献[1]引入了多进制 LDPC 码, 并且给出了相应的译码算法。与二进制 LDPC 码相比, 多进制 LDPC 码具有更好的性能, 且具有更好的抗突发错误能力。同时准循环结构的 LDPC 码具有更低的实现复杂度, 因此吸引了广泛的研究。文献[2]研究了准循环矩阵中环的形成条件。文献[3]对环的

连通性进行了研究, 提出了 ACE(Approximate Circle EMD(Extrinsic Message Degree))作为另外一个重要的性能影响因素。除此之外, 多进制 LDPC 码的校验矩阵还需要考虑 $GF(q)$ 上非零元素的替代。文献[4]研究了多进制 LDPC 码校验矩阵的二进制表示, 提出了行满秩条件 FRC(Full Rank Condition)用于非零元素的替代。针对特殊结构, 文献[5-7]研究了基于有限域的准循环多进制 LDPC 码的构造方法。文献[8,9]研究了基于代数几何的准循环多进制 LDPC 码的构造方法。文献[10,11]研究了环形图结构的多进制 QC-LDPC 码的构造。

基于有限域和代数几何的构造方法比较简单,

2012-04-09 收到, 2012-11-06 改回

国家自然科学基金(61001133)资助课题

*通信作者: 钟杰 zhongjie@zju.edu.cn

但是适用于高码率 LDPC 码的构造。基于环形图结构构造的多进制 LDPC 码适用于 $q \geq 64$ 的情况^[12]。本文在上述研究的基础上,提出了一种新的构造方法,用于 $q \leq 16$ 的中等码率多进制 LDPC 码的构造。同时提出了搜索偏移因子和非零元素的方法,可以大大降低构造复杂度。两者相结合可以方便地根据码的参数构造得到相应的校验矩阵。本文的主要内容和章节安排如下。第 2 节简单介绍了准循环多进制 LDPC 码的基本结构和表示方法;第 3 节分析了多进制 LDPC 码的性能影响因素,推导得到构造的基本准则;第 4 节详细描述了准循环多进制 LDPC 码构造算法;第 5 节给出了仿真结果,最后进行了总结。

2 准循环多进制 LDPC 码简介

考虑定义在 $\text{GF}(q)$ 上的多进制 LDPC 码, q 为质数的幂次方。 α 是有限域的本原元,且有 $\alpha^{q-1} = 1$ 。 $\text{GF}(q)$ 中的元素都可以用 α 的幂次方表示,分别为 $\{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\}$ 。多进制 LDPC 码的校验矩阵 \mathbf{H} 由 $\text{GF}(q)$ 上的元素组成,有效码字 \mathbf{c} 满足

$$\mathbf{H} \cdot \mathbf{c}^T = \mathbf{0} \quad (1)$$

多进制 LDPC 码的构造思路是首先通过母矩阵扩展得到二进制 LDPC 码的校验矩阵 \mathbf{H}_b , 然后将校验矩阵中 ‘1’ 的位置用 $\text{GF}(q)$ 上的非零元素替代,得到多进制 LDPC 码的校验矩阵 \mathbf{H}_q 。准循环 LDPC 码的母矩阵表示为

$$\mathbf{P} = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n-1} & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n-1} & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ p_{m,1} & p_{m,2} & \cdots & p_{m,n-1} & p_{m,n} \end{bmatrix} \quad (2)$$

在 \mathbf{P} 中, $p_{i,j} = -1$ 的位置表示对应位置由 $s \times s$ 的全零矩阵替代, $p_{i,j}$ 为非负的位置表示对应位置由循环右移 p 位的 $s \times s$ 的单位矩阵替代,从而得到二进制校验矩阵 \mathbf{H}_b 。然后将 \mathbf{H}_b 上 ‘1’ 的位置用 $\text{GF}(q)$ 上的非零元素替代,得到 \mathbf{H}_q 。 \mathbf{H}_b 的构造主要考虑的是环长的影响,尽可能消除短环。 \mathbf{H}_q 上非零元素的选择主要考虑的是进一步消除 \mathbf{H}_b 上短环的影响。

3 准循环多进制 LDPC 码的构造影响因素

3.1 码距

多进制 LDPC 码为线性分组码,其纠错性能受最小码距影响。对于 $\text{GF}(q)$ 上码长为 N , 信息位长度为 K 的多进制 LDPC 码(K 比较大),其最小码距 d 满足普洛特金限:

$$d \leq \frac{Nq^K(q-1)}{(q^K-1)q} \approx \frac{N(q-1)}{q} \quad (3)$$

多进制 LDPC 码的码距主要由环长和环的连通性决定,校验矩阵中 $\text{GF}(q)$ 元素的替代对码距也有一定的影响。

3.2 环长与环的连通性

定理 1 假设 $(p_1, p_2, \dots, p_{2t})$ 是 \mathbf{H} 矩阵上一个长度为 $2t$ 的环上的元素,定义

$$w = \frac{s}{\text{gcd} \left\{ \text{mod} \left[\sum_{i=1}^{2t} (-1)^{i+1} p_i, s \right], s \right\}} \quad (4)$$

则在扩展后矩阵中,存在长度为 $w \times 2t$ 的环,环的数量为 s/w 。

定理 1 由文献[2]中的定理推导得到。根据环的形成条件,精心选择 \mathbf{H} 中的偏移值,可以使扩展后的矩阵 \mathbf{H}_b 中环长尽可能大。扩展后矩阵中环的个数为 s/w , 通过统计母矩阵中的环,然后计算环上元素的值,由此计算得到扩展后矩阵 \mathbf{H}_b 上环的分布情况。

环的连通性一般通过停止集衡量。停止集 S_v 表示 v 个变量节点组成的集合,与这个集合相连的子图中不存在任何度为 1 的校验节点。停止集被认为是二进制删除信道中译码失败的主要因素。外部信息度(EMD)是一个变量节点集中外部校验节点的个数。对于停止集,它的外部信息度为 0。一个外部信息度大的集合需要添加更多的变量节点才能形成停止集,因此得到的停止集更大。对于变量节点度大于 2 的矩阵,停止集是在环的基础上形成的。因此外部信息度小的短环在构造中是需要避免的。我们选择环的近似外部信息度(Approximate Circle EMD, ACE)作为衡量环的连通性的标准。假设 C_{2t} 表示一个长度为 $2t$ 的环,则 C_{2t} 的 ACE^[3] 的计算方法为

$$\sum_{j=1}^{j=2t} (d_{v_j} - 2) \quad (5)$$

3.3 行满秩条件

即使精心选择母矩阵中的偏移因子,扩展后的矩阵中仍然存在短环。因此需要通过 $\text{GF}(q)$ 上非零元素的选择,进一步消除短环的影响。矩阵中形成环的部分通过行列调整都可以构成一个方阵。式(6)所示为长度为 $2t$ 的环组成的方阵:

$$\mathbf{C}_d = \begin{pmatrix} \beta_2 & \beta_3 & 0 & \cdots & \cdots & 0 \\ 0 & \beta_4 & \beta_5 & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ 0 & \cdots & \cdots & & \beta_{2t-2} & \beta_{2t-1} \\ \beta_1 & 0 & \cdots & \cdots & 0 & \beta_{2t} \end{pmatrix} \quad (6)$$

如果 \mathbf{C}_d 线性相关则存在一组非零系数 \mathbf{T} , 使得

$C_d \cdot T = 0$ 。由此可能存在一个码字 $c' = \{0, \dots, 0, T, 0, \dots, 0\}$ ，满足 $H_q \cdot c' = 0$ 。由此引入低重量码字，等价于小的码距，带来比较高的误码平层。因此需要通过 $GF(q)$ 上非零元素的选择避免这个情况出现。矩阵 C_d 线性无关的条件是 $\det(C_d) \neq 0$ ，因此有如下所示行满秩条件 (Full Rank Condition, FRC)^[4]：

$$\prod_{i=1}^l \beta_{2i-1} \neq \prod_{i=1}^l \beta_{2i} \quad (7)$$

由于 $GF(q)$ 上的元素可以用本原元的幂次方表示，此时形成环的矩阵可以表示为

$$C_d = \begin{pmatrix} \alpha^{r_2} & \alpha^{r_3} & 0 & \dots & \dots & 0 \\ 0 & \alpha^{r_1} & \alpha^{r_5} & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ 0 & \dots & \dots & & \alpha^{r_{2l-2}} & \alpha^{r_{2l-1}} \\ \alpha^{r_1} & 0 & \dots & \dots & 0 & \alpha^{r_{2l}} \end{pmatrix} \quad (8)$$

满秩条件中 $GF(q)$ 上的乘法可以通过本原元幂的加法表示，新的满秩条件为

$$\text{mod} \left[\sum_{i=1}^{2l} (-1)^{i+1} r_i, q-1 \right] \neq 0 \quad (9)$$

通过对上面条件的变换，将环的形成条件与满秩条件统一起来。此时可以用相同的方法统一考虑二者的影响。

4 准循环多进制 LDPC 码的构造算法

多进制 LDPC 码的构造步骤主要根据度分布，通过 PEG^[9] 算法构造母矩阵。然后根据环的形成条件和环的连通性确定偏移因子，得到扩展后的二进制 LDPC 矩阵 H_b 。最后根据环的满秩条件确定 H_b 上 ‘1’ 的位置 $GF(q)$ 非零元素的替代值，从而得到校验矩阵 H 。

一般情况下，校验矩阵 H 是否满秩由母矩阵结构、偏移因子和非零位置替代值共同决定。而当母矩阵满足某些特定结构或者度分布特性，如采用 eIRA 结构^[13] 或者 $d_p=2$ 的满秩矩阵时，扩展得到的 H 矩阵一定是满秩的，码率也由母矩阵的大小唯一确定。下面将对准循环多进制 LDPC 码的构造算法展开进行讨论。图 1 所示为该构造算法的简要流程。

4.1 母矩阵构造

由于经过迭代译码之后变量节点度越小的点越不可靠，因此需要优先考虑度小的变量节点，尽量避免度小的变量节点之间形成短环。在构造过程中按照度的大小从小到大进行排序，通过 PEG (Progressive Edge Growth) 算法逐步添加到母矩阵中进行构造。PEG 算法是贪婪算法，每次添加的边，都使当前添加的变量节点局部环长最大。

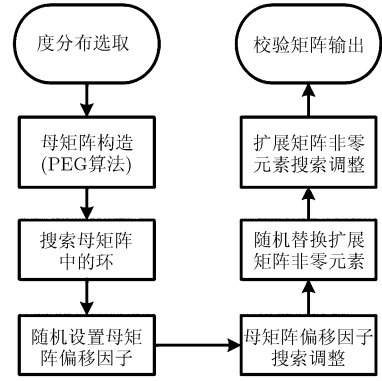


图 1 构造算法简要流程

4.2 母矩阵扩展

通过逐个添加变量节点的方式，根据扩展后矩阵中环的形成条件和环的连通性逐列确定偏移因子。对于新添加的变量节点，首先搜索与已添加变量节点在母矩阵中形成的短环，得到环的集合，然后建立方程组确定偏移因子，从而得到扩展矩阵 H_b 。

4.2.1 搜索图中的环

为了找到母矩阵中的环，我们把母矩阵展开为树的形式。在 PEG 算法中，通过建立最小生成树找到图中最短的环。然而最小生成树并不能帮助找到图中所有的环，因此我们采用了一个新的方法。假设 Q^l 为第 l 层中所有节点的集合， Q^{l+1} 表示图中与 Q^l 中的节点相连的所有节点的集合。如果在集合 Q^l 中存在相同的节点，同时它们在树中的父节点不同，那么母矩阵中存在一个长度为 $2l$ 的环。

环的搜索复杂度随着环的层数增加几何级数增长，同时对性能影响比较大的主要是短环，因此不需要设置太大的展开层数。文献[14]给出了规则 LDPC 码 (d_c, d_v) 中最小环长的下界。

$$t = \frac{\lg(m \times d_c - m \times d_c / d_v - m + 1)}{\lg(d_v - 1)(d_c - 1)} - 1 \quad (10)$$

$$g = (\lfloor t \rfloor + 2) \times 2 \quad (11)$$

其中 m 为码长， d_c 为校验节点度， d_v 为变量节点度， $\lfloor \cdot \rfloor$ 为下取整操作。

令搜索的层数 $L_t \geq g/2+1$ 。在复杂度允许的范围内适当增大 L_t 的值，最小为 $g/2+1$ 。

下面以变量节点 V_j 为例，说明如何搜索得到与它有关的环。

- (1) 初始化： $l = 0, Q^l = \{V_j\}$ ；
- (2) 寻找所有与 Q^l 相连的节点，加入队列 Q^{l+1} 中，记录各自的父节点信息； $l = l + 1$ ；
- (3) 如果 $l \leq L_t$ ，则返回步骤(2)，否则跳出，完

成了环的搜索过程。

步骤(2)中,如果 Q^l 中元素同时满足下面 3 个条件,则形成了一个当前变量节点相关的环:

- (a)在同一层存在相同的节点;
- (b)它们的父节点不同;
- (c)它们在第 1 层中祖先节点不同。

条件(a)保证了环的存在,条件(b)和条件(c)保证了形成的环起止于根节点。

当满足这些条件的节点存在时,在树中回溯它们的祖先节点,并记录在一个链表上,从而得到与 V_j 有关的长度小于 $2L_t$ 的所有环,记为 Ψ_j 。同时计算环的 ACE。

4.2.2 偏移值的搜索 找到图中所有长度小于 $2L_t$ 的环后,根据环的形成条件建立相应的方程组。令 V_j 为当前连接到图 G_c 的变量节点,它的度为 d_{V_j} , $B_j = [b_1, b_2, \dots, b_{d_{V_j}}]$ 是偏移矩阵中与 V_j 有关的元素的集合。 B_j 中的每一个元素的取值范围是 $[0, s-1]$ 内的整数,记为 $B_j \in X^{d_{V_j}}$ 。 B_j 中的所有元素初始化为 0,建立的方程组与 B_j 的两个元素有关。根据 $\sum_{i=1}^{2t} (-1)^{i+1} p_i$, 建立起所有环对应的方程组集合 E 。由于要同时考虑环长和环的连通性,在偏移因子的搜索时首先确保没有 4 环,然后考虑 ACE 与环长的一半之和作为度量,以此减少小的停止集出现的概率。

偏移因子的穷举搜索可以得到方程组最优解,但是搜索空间的大小随着变量节点的度和单位矩阵大小的增加呈几何级数增长。在两者比较大的时候,穷举搜索复杂度太高,因此考虑随机构造得到一个偏移矩阵,然后使用次优的贪婪算法进行搜索。

将集合 B_j 分为 $d_{V_j}(d_{V_j}-1)/2$ 组,每组包含两个不同的元素,表示为

$$CLU = \{(b_m, b_n) \mid m \neq n, m \in [1, d_{V_j}], n \in [1, d_{V_j}]\} \quad (12)$$

然后建立对应的方程组集合,集合中的每一个方程组都与 CLU 中元素有关。贪婪算法的具体步骤如下:

- (1)初始化 k 为 1;
- (2)将集合 E 中所有的与 b_k 有关方程合并到集合 E_k 中;
- (3)遍历 0 到 $s-1$ 区间内的所有值,将集合中 $\max \min(ACE + G/2)$ 的值作为解输出,同时更新 E_k 中所有的方程。 k 自增 1。如果 $k > d_{V_j}$, 那么跳至步骤(4), 否则跳至步骤(2);
- (4)更新 B_j 中的元素。

4.3 非零元素替代

通过前面的方法得到了扩展后二进制矩阵后,根据满秩条件式(8),进行非零元素的替代。由于扩

展后的矩阵中部分变量节点所在的环比较长,可能不在搜索的环长范围内,因此我们首先通过随机替代的方式初始化多进制 LDPC 码的校验矩阵 H_q 信息位部分,然后在校验位部分对应的位置填 1。接着搜索扩展后的矩阵 H_b 中的短环,根据 $\sum_{i=1}^{2l} (-1)^{i+1} r_i$ 建立对应的方程组集合 E^q 。最后通过贪婪算法搜索得到相应的非零元素进行调整。令 $R_j = (r_1, r_2, \dots, r_{d_{V_j}^q})$ 是 H_q 中与 V_j^q 有关的元素的集合。 R_j 中的每一个元素的取值范围是 $[0, q-2]$ 内的整数。将集合 R_j 分为 $d_{V_j^q}(d_{V_j^q}-1)/2$ 组,每组包含两个不同的元素,表示为

$$CLU_R = \{(r_m, r_n) \mid m \neq n, m \in [1, d_{V_j^q}], n \in [1, d_{V_j^q}]\} \quad (13)$$

然后建立对应的方程组集合,集合中的每一个方程组都与 CLU_R 中元素有关。非零元素替代的具体步骤如下:

- (1)初始化 k 为 1;
- (2)将集合 E^q 中所有的与 r_k 有关方程合并到集合 E_k^q 中;
- (3)遍历 0 到 $q-2$ 区间内的所有值,将集合中 $\sum_{i=1}^{2l} (-1)^{i+1} r_i \neq 0$, 或者等于零的个数最少的值作为解输出,同时更新 E_k 中所有的方程。 k 自增 1。如果 $k > d_{V_j^q}$, 那么跳至步骤(3), 否则跳至步骤(1);
- (4)更新 R_j 中的元素。

得到对应的元素后,转换到对应的 $GF(q)$ 元素上,得到最终的多进制 LDPC 码校验矩阵。

5 仿真结果与分析

在这一节中,我们利用前面描述的方法构造了 $GF(8)$, $GF(16)$ 域上的 LDPC 码,等效比特码长 1152, 码率 1/2, 母矩阵大小为 16×32 。同时构造了相同参数的二进制 LDPC 码进行比较。这些 LDPC 码的校验矩阵均为 eIRA 结构^[13]。表 1 所示为对应的构造参数。

图 2 表示了当码长比特数一定时, GF 域的阶数 q 与最小码距 d 的上界的对应关系(码长归一化到 1 bit)。从图中可以看出,当码长比特数不变时, q 越大, LDPC 码最小码距的上界越小,因而越容易出现误码平台。根据普洛特金限,构造得到的 $GF(2)$ 上的 LDPC 码的最小码距上界约为 576, $GF(8)$ 上的

表 1 LDPC 码构造参数

有限域	GF(2)	GF(8)	GF(16)
码长	1152	384	288
s	36	12	9

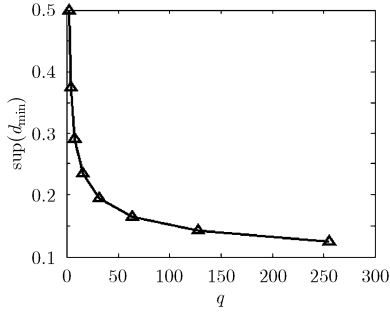


图 2 q 与 $\text{sup}(d_{\min})$ 对应关系图

LDPC 码的最小码距上界约为 336, GF(16)上的 LDPC 码的最小码距上界约为 213。

利用参考文献[15]中给出的对应参数下优化后的度分布, 构造母矩阵:

GF(2)上度分布为

$$\lambda(x) = 0.2655x + 0.2389x^2 + 0.4956x^6 \quad (14)$$

$$\rho(x) = 0.9292x^6 + 0.0708x^7 \quad (15)$$

GF(8)上度分布为

$$\lambda(x) = 0.4545x + 0.1023x^2 + 0.2727x^3 + 0.1705x^4 \quad (16)$$

$$\rho(x) = 0.4545x^4 + 0.5455x^5 \quad (17)$$

GF(16)上度分布为

$$\lambda(x) = 0.64x + 0.24x^2 + 0.0533x^3 + 0.0667x^4 \quad (18)$$

$$\rho(x) = 0.2667x^3 + 0.7333x^4 \quad (19)$$

仿真环境为 AWGN 信道, 采用的译码算法为 BP 译码算法^[1], 迭代次数 50 次。通过 PEG 算法, 根据式(13)~式(18)给出的度分布构造得到对应的母矩阵。然后根据环的形成条件式(4)得到对应的二进制矩阵。最后根据行满秩条件进行非零元素的替代, 从而得到多进制矩阵。

图 3 所示为 GF(8)上随机替代和根据 FRC 准则

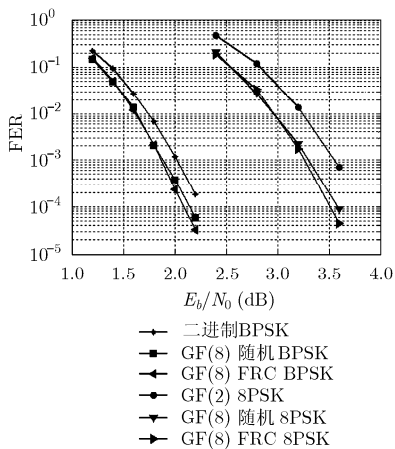


图 3 GF(2)与 GF(8) 误帧率性能比较

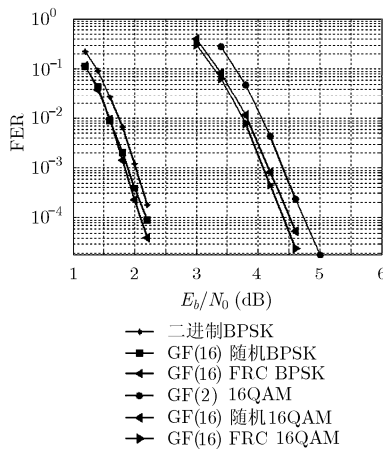


图 4 GF(2)与 GF(16) 误帧率性能比较

搜索得到的多进制 LDPC 码与二进制 LDPC 码的性能比较。从仿真结果可以看出, 根据 FRC 准则搜索得到的多进制 LDPC 码与随机替代得到的多进制 LDPC 码相比有更好的性能, 特别是在高信噪比条件下。优化后的八进制 LDPC 码与二进制 LDPC 码相比, 在 BPSK 调制方式下, 性能有 0.2 dB 的提升; 在 8PSK 调制方式下, 性能有 0.3 dB 的提升。

图 4 所示为 GF(16)上随机替代和根据 FRC 准则搜索得到的多进制 LDPC 码与二进制 LDPC 码的性能比较。从仿真结果同样可以看到, 根据 FRC 准则搜索得到的多进制 LDPC 码与随机替代得到的多进制 LDPC 码相比有更好的性能。优化后的十六进制 LDPC 码与二进制 LDPC 码相比, 在 BPSK 调制方式下, 性能有 0.2 dB 的提升; 在 16QAM 调制方式下, 性能有 0.35 dB 的提升。

图 5 所示为 GF(16)上不同的构造方法得到的码的误帧率性能比较。图中循环码为文献[4]中给出的仿真结果, 码长 1504、码率 1/2, 仿真环境为 AWGN 信道下采用 BPSK 调制, 最大迭代次数为 1000。我们用前面的方法构造得到了码长为 1536、码率 1/2 的多进制 LDPC 码, 采用相同的仿真环境, 最大迭代次数为 50 次。从仿真结果我们可以看到在 10^{-4} 附近有 0.25 dB 的性能提升。

从仿真结果看, 根据 FRC 准则进行非零元素的替代得到的多进制 LDPC 码具有更好的性能。优化后的多进制 LDPC 码与二进制 LDPC 码相比, 性能有比较大的提升。在有限域阶数与调制阶数匹配的情况下, 性能提升更明显。同时在有限域阶数比较低的情况下, 采用本文中提出的构造方法得到的多进制 LDPC 码与循环码相比具有更好的性能。

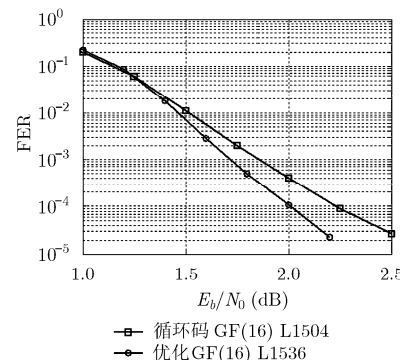


图 5 GF(16)上码率 1/2 不同构造方法得到的码的误帧率性能比较

6 结束语

本文研究了准循环多进制 LDPC 码的构造, 详细说明了准循环多进制 LDPC 码的设计流程和构造方法。在母矩阵扩展时综合考虑了环长和环的连通性对性能的影响, 进行偏移因子的选择。为了进一步减小短环对性能的影响, 降低误码平层, 我们对多进制 LDPC 码校验矩阵中 $GF(q)$ 上非零元素替代进行了研究。在前人研究的基础上, 推导得到新的替代准则。新的替代准则与偏移因子的选择具有类似的表示方法, 从而可以统一到一个框架下进行研究。在这个统一的框架下, 我们提出了次优解的搜索方法, 具有更低的复杂度。最后, 我们将提出的方法用于不同阶数下 LDPC 码的构造。仿真结果表明, 优化后的多进制 LDPC 码的性能与二进制码相比, 在 BPSK 调制方式下在误帧率 10^{-4} 附近性能有 0.2 dB 的提升; 在有限域阶数与调制阶数匹配的情况下, 性能有 0.3~0.35 dB 的提升。新的构造方法具有很好的灵活性, 并且具有比较低的构造复杂度, 可以用于不同参数的准循环多进制 LDPC 码的构造。

参 考 文 献

- [1] Davey M C and MacKay D J C. Low density parity check codes over $GF(q)$ [J]. *IEEE Communications Letters*, 1998, 2(6): 165-167.
- [2] Myung S, Yang K, and Kim J. Quasi-cyclic LDPC codes for fast encoding[J]. *IEEE Transactions on Information Theory*, 2005, 51(8): 2894-2901.
- [3] Tian T, Jones C R, Villasenor J D, et al.. Selective avoidance of cycles in irregular LDPC code construction[J]. *IEEE Transactions on Communications*, 2004, 52(8): 1242-1247.
- [4] Poulliat C, Fossorier M, and Declercq D. Design of regular (2, dc)-LDPC codes over $GF(q)$ using their binary images[J]. *IEEE Transactions on Communications*, 2008, 56(10): 1626-1635.
- [5] Zeng L, Lan L, Tai Y Y, et al.. Construction of nonbinary cyclic, quasi-cyclic and regular LDPC codes: a finite geometry approach[J]. *IEEE Transactions on Communications*, 2008, 56(3): 378-387.
- [6] Song S, Zhou B, Lin S, et al.. A unified approach to the construction of binary and nonbinary quasi-cyclic LDPC codes based on finite fields[J]. *IEEE Transactions on Communications*, 2009, 57(1): 84-93.
- [7] Zhou B, Kang J, Song S, et al.. Construction of non-binary quasi-cyclic LDPC codes by arrays and array dispersions[J]. *IEEE Transactions on Communications*, 2009, 57(6): 1652-1662.
- [8] Kang J, Huang Q, Zhang L, et al.. Quasi-cyclic LDPC codes: an algebraic construction[J]. *IEEE Transactions on Communications*, 2010, 58(5): 1383-1396.
- [9] Chen C, Bai B, Wang X, et al.. Nonbinary LDPC codes constructed based on a cyclic MDS code and a low-complexity nonbinary message-passing decoding algorithm[J]. *IEEE Communications Letters*, 2010, 14(3): 239-241.
- [10] Huang J, Zhou S, and Willett P. Structure, property, and design of nonbinary regular cycle codes[J]. *IEEE Transactions on Communications*, 2010, 58(4): 1060-1071.
- [11] Chen C, Bai B, and Wang X. Construction of nonbinary quasi-cyclic LDPC cycle codes based on singer perfect difference set[J]. *IEEE Communications Letters*, 2010, 14(2): 181-183.
- [12] Li G, Fair I J, and Krzymie W A. Density evolution for nonbinary LDPC codes under Gaussian approximation[J]. *IEEE Transactions on Information Theory*, 2009, 55(3): 997-1015.
- [13] Zhang Y, Ryan W E, and Li Y. Structured eIRA codes with low floors[C]. Proceedings of International Symposium on Information Theory, Adelaide, 2005: 174-178.
- [14] Hu X Y, Eleftheriou E, and Arnold D M. Regular and irregular progressive edge-growth tanner graphs[J]. *IEEE Transactions on Information Theory*, 2005, 51(1): 386-398.
- [15] Wu J, Zhao M, Zhong J, et al.. Statistical-based density evolution algorithm for nonbinary low-density parity-check codes[C]. IEEE Vehicular Technology Conference, San Francisco, 2011: 1-5.

杨 民: 男, 1975 年生, 工程师, 研究方向为短波通信与信道编码。

张文彦: 男, 1988 年生, 硕士生, 研究方向为信道编码。

钟 杰: 男, 1981 年生, 副研究员, 研究方向为无线通信。