

一种改进的基于中国余定理 QC-LDPC 码设计方法

徐 华

(盐城师范学院 物理科学与电子技术学院, 江苏 盐城 224002)

摘 要: 构造了一种新的基于有限域的 QC-LDPC 码作为分量码, 与分组码和截短分组码相比, 有效改善了目标 QC-LDPC 码的性能. 首先简要描述了 QC-LDPC 码的基本定义, 接着回顾了已有的基于中国余定理 (Chinese Remainder Theory, CRT) QC-LDPC 码设计方法, 进一步阐述了采用有限域 (finite field) 方法设计构造 QC-LDPC 码的过程, 在此基础上给出了改进的基于中国余定理 QC-LDPC 码设计方法, 仿真结果表明, 基于有限域方法设计的 QC-LDPC 码性能优良, 其作为分量码应用于中国余定理的 QC-LDPC 码设计, 可以很大程度上改善构造的目标 QC-LDPC 码的性能.

关键词: 中国余定理; 有限域方法; 分组码; 截短分组码

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2014)02-0009-05

An Improved QC-LDPC Codes Construction Method Based on Chinese Remainder Theory

XU Hua

(School of Physics and Electronics Engineering, Yancheng Teachers University, Yancheng 224002, China)

Abstract: This paper proposes a novel component code, QC-LDPC code constructed by finite field method. It can improve the performance of objective QC-LDPC code effectively, when compared with the array code or shortened array code. In this paper, the background of QC-LDPC code is depicted firstly. Then, the QC-LDPC code design method based on CRT (Chinese Remainder Theory) is reviewed. Furthermore, the procedure of QC-LDPC code construction algorithm based on finite field method is given. Finally, the improved QC-LDPC code construction method based on CRT is described. Simulation results show that the finite field based QC-LDPC code can improve the performance effectively of the objective QC-LDPC code when adopted as the component code of the CRT method.

Key words: Chinese Remainder Theory; finite field method; array code; shortened array code

1 引言

采用基于中国余定理 (Chinese Remainder Theory, CRT) 的设计方法来构造 QC-LDPC (Quasi-Cyclic Low Density Parity Check) 码的校验矩阵首先由 Myung 提出^[1]; Liu 放松了相关约束条件, 作了进一步的推广, 给出了一种改进的设计方法^[2]; 文献[1-2]中都是将分组码 (array code)^[3]作为分量码.

分组码的构造简单, 但是由于其 H 矩阵中存在大量的环长为 4 的最短长度环 (即 4girth), 因此性能与其他 QC-LDPC 码相比并不理想, 为了改善分组码的性能, Milenkovic 提出了通过删除分组码中校验矩阵某些特定的列来改善码的性能^[4], 此时得到的分组码称为截短分组码 (shortened array code).

Jiang 将截短分组码引入到基于中国余定理的 QC-LDPC 码设计中^[5], 即考虑分组码和截短分组

收稿日期: 2013-04-27; 修回日期: 2013-06-18

基金项目: 国家自然科学基金(11175152); 江苏省高校自然科学研究项目(13KJB510038)

码作为中国余定理设计方法中的分量码,获得了具有较大 girth 的 QC-LDPC 码,AWGN 信道下的仿真表明构造的目标 QC-LDPC 码性能,与采用分组码作为分量码相比有了进一步改善。

文献[6-8]提出了基于有限域 (Finite Field) 的 QC-LDPC 码设计方法,包括二元 QC-LDPC 码和多元 QC-LDPC 码的设计,表明了 QC-LDPC 码的良好性能,部分 QC-LDPC 码的性能即使在长码长时也超出了随机构造的 LDPC 码,说明了有限域方法设计准循环 LDPC 码的巨大潜力。

本文将基于有限域方法构造的 QC-LDPC 码引入到了基于中国余定理的设计中,与传统的分量码、截短分组码相比,目标 QC-LDPC 码的性能有较大提高。

2 基于有限域方法 QC-LDPC 码设计

2.1 QC-LDPC 码基本原理

QC-LDPC 码的校验矩阵由若干个循环移位子矩阵或者零矩阵来组成,如式(1)所示。

$$\mathbf{H} = \begin{bmatrix} P^{a_{00}} & P^{a_{01}} & \cdots & P^{a_{0,N-1}} \\ P^{a_{10}} & P^{a_{11}} & \cdots & P^{a_{1,N-1}} \\ \vdots & \vdots & \ddots & \vdots \\ P^{a_{M-1,0}} & P^{a_{M-1,1}} & \cdots & P^{a_{M-1,N-1}} \end{bmatrix}_{M \times N} \quad (1)$$

式中,每个子矩阵的大小为 $L \times L$, $P^{a_{ij}}$ 指将单位阵移位 a_{ij} ($0 \leq i < M, 0 \leq j < N$) 获得的循环移位子矩阵,而指数 a_{ij} 组成的矩阵称为指数矩阵,如式(2)所示。

$$\mathbf{E}(\mathbf{H}) = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0,N-1} \\ a_{10} & a_{11} & \cdots & a_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M-1,0} & a_{M-1,1} & \cdots & a_{M-1,N-1} \end{bmatrix}_{M \times N} \quad (2)$$

需要说明的是每个非零子矩阵的每行、每列均只有一个“1”,而非零子矩阵是由单位矩阵移位得到,因此指数矩阵中的元素 $a_{ij} \in \{0, 1, \dots, L-1\}$,即在该范围的整数空间中寻找合适的移位参数。

2.2 基于有限域方法 QC-LDPC 码设计

矩阵扩展及定位矢量表达是 QC-LDPC 有限域设计方法的关键^[6]。

考虑有限域 $GF(q)$ 以及相应的本原元素 α , $GF(q)$ 中 $q-1$ 个非零元素可以由 α^i 表示,而 α^i 的定位矢量可以表示为 $z(\alpha^i) = (z_0, z_1, z_2, \dots, z_{q-2})$,其中第 i 个元素是 1,其余是 0,该矢量的所有元素对应

着 $GF(q)$ 的 $(q-1)$ 个非零元素。

图 1 所示为采用有限域方法构造 QC-LDPC 码的 $\mathbf{H}$ 矩阵的过程。

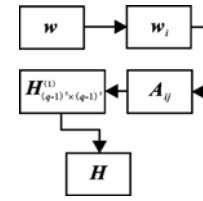


图 1 有限域方法构造 $\mathbf{H}$ 矩阵的过程

有限域 $GF(q)$ 中 $(q-1) \times (q-1)$ 大小的矩阵 $\mathbf{W}$ 可由下式表示。

$$\mathbf{W} = \begin{bmatrix} w_0 \\ w_1 \\ \vdots \\ w_{q-2} \end{bmatrix} = \begin{bmatrix} \alpha^0 - 1 & \alpha - 1 & \cdots & \alpha^{q-2} - 1 \\ \alpha - 1 & \alpha^2 - 1 & \cdots & \alpha^{q-1} - 1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-2} - 1 & \alpha^{q-1} - 1 & \cdots & \alpha^{2(q-1)} - 1 \end{bmatrix} \quad (3)$$

在式(3)的基础上,可以获得 $\mathbf{W}_i$,它是式(3)第 i 行的垂直矩阵扩展,如下式所示。

$$\mathbf{W}_i = \begin{bmatrix} w_i \\ \alpha w_i \\ \vdots \\ \alpha^{q-2} w_i \end{bmatrix} \quad (4)$$

进一步, $\mathbf{A}_{ij}$ 由 $w_{ij}, \alpha w_{ij}, \dots, \alpha^{q-2} w_{ij}$ 的定位矢量表示, w_{ij} 为零时,则 $\mathbf{A}_{ij}$ 为零矩阵,而 w_{ij} 取非零值时,则 $\mathbf{A}_{ij}$ 为循环移位矩阵。

在得到 $\mathbf{A}_{ij}$ 后,在此基础上可以如式(5)所示,构造出大小为 $(q-1)^2 \times (q-1)^2$ 的 $\mathbf{H}^{(1)}$ 矩阵,其中的每个元素为大小 $(q-1) \times (q-1)$ 的零矩阵或者循环移位矩阵。

$$\mathbf{H}^{(1)} = \begin{bmatrix} \mathbf{A}_{00} & \mathbf{A}_{01} & \cdots & \mathbf{A}_{0,q-2} \\ \mathbf{A}_{10} & \mathbf{A}_{11} & \cdots & \mathbf{A}_{1,q-2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{q-2,0} & \mathbf{A}_{q-2,1} & \cdots & \mathbf{A}_{q-2,q-2} \end{bmatrix} \quad (5)$$

得到 $(q-1)^2 \times (q-1)^2$ 的 $\mathbf{H}^{(1)}$ 矩阵后,可以根据具体的码长、码率要求在其中选择相应的行和列构造出 QC-LDPC 码的 $\mathbf{H}$ 矩阵。

需要说明的是有限域方法构造的 QC-LDPC 码的 $\mathbf{H}$ 矩阵中最短长度环的环长最少是 6 (6girth),即已经消除了严重影响 LDPC 码性能的长度为 4 的最短长度环 (4girth),其他有限域设计方法的细节

可参见文献[6].

3 改进的中国余定理 QC-LDPC 码设计方法

传统的中国余定理设计方法一般是采用分组码(array code)或者截短分组码(shortened array code)作为分量码,构造出的目标 QC-LDPC 码由于其 $\mathbf{H}$ 矩阵的短长度环的分布(girth distribution)要优于分量码,因此其性能也优于分量码的性能.

分组码的构造较简单,但是其 $\mathbf{H}$ 矩阵中往往存在较多的长度为 4 的短长度环(4 girth),而 4girth 的存在会使得相应 QC-LDPC 码的性能有较大的影响.

有限域方法设计的 QC-LDPC 码性能比分组码及截短分组码要好的多,作为分量码,构造出的目标 QC-LDPC 码性能将有较大的改善.

在给出所提的改进方法之前,首先给出以下的定理.

定理 1 考虑有 T 个分量码,每个分量码 $\mathbf{H}$ 矩阵的 girth(最短长度环)定义为 $\{g_t, t = 1, 2, \dots, T\}$,目标码的 girth 定义为 g_{obj} ,则有,

$$g_{\text{obj}} \geq \max(g_t, t = 1, 2, \dots, T) \quad (6)$$

由该定理可知,中国余定理设计获得的目标码的 girth 至少和分量码中的最大 girth 相等,因此目标码的性能要优于分量码.

为了更好地描述所提方法,仍然考虑有 T 个分量码,分别为 $C_1, C_2, \dots, C_T$,每个分量码的 $\mathbf{H}$ 矩阵由循环置换矩阵组成,各自的循环置换矩阵的大小对应为 $L_1, L_2, \dots, L_T$,则对应的目标码的子矩阵大小为 $L = L_1 \cdot L_2 \cdots L_T$,需要说明的是,各个分量码的循环置换矩阵的大小各自不相等,且应该为质数(prime),在构造过程中,需要依据设计的目标码长和目标码率的要求,来选择具体分量码的个数以及各个分量码的子矩阵大小,设采用有限域方法设计的分量码为 T_F 个,而作为分量码的分组码个数为 T_A .

在此基础上,具体步骤如下:

(1) 依据事先确定的 T_F 个分量码的子矩阵大小,按照图 1 所示的过程采用有限域方法分别构造 T_F 个分量码的指数矩阵;

(2) 依据事先确定的 T_A 个分组码的大小,分别构造各个分组码作为其他的分量码的指数矩阵;

(3) 如果各个分量码的指数矩阵 $s_{jq}^t \neq \infty$,则可以得到如式(7)所示得到目标码指数矩阵中的各个

元素:

$$s_{jq} = \sum_{t=1}^T s_{jq}^t A_t \bar{L}_t \bmod L \quad (7)$$

式中, $\bar{L}_t = L/L_t, A_t \bar{L}_t \equiv 1 \bmod L_t$. 而如果 $s_{jq}^t = \infty$,则 $s_{jq} = \infty$. 需要说明的是,此处的 $s_{jq}^t = \infty$ 指分量码的指数矩阵中的元素为零(即对应着 $\mathbf{H}$ 矩阵中的零矩阵).

(4) 获得 s_{jq} 后,即可以得到相应目标 QC-LDPC 码的指数矩阵.

(5) 按照式(1)构造出目标 QC-LDPC 码的 $\mathbf{H}$ 矩阵. 如果指数矩阵中有元素 $s_{jq} = \infty$,则该位置由零矩阵来替换,非零元素则由移位参数为 s_{jq} 的循环移位矩阵作为子矩阵替换.

需要说明的是,据上述定理式(6)所示,获得的目标 QC-LDPC 码的 girth 至少与分量码中的最大的 girth 相等,保证了构造的新 QC-LDPC 码的良好性能.

4 数值仿真和分析

仿真中考虑 AWGN (Additive White Gaussian Noise) 信道,采用 BPSK (Binary Phase Shifting Keying) 调制,LDPC 码译码采用 BP (Belief Propagation) 译码算法,最大的译码迭代次数设为 50 次.

为了便于说明和仿真,设共有两个分量码 C_1 和 C_2 ,即 $T=2$,而本文所提方法构造的目标 QC-LDPC 码,由于采用有限域方法构造的 QC-LDPC 码和分组码作为分量码,因此称为 FFAR (Finite Field + ARray) 码.

在构造 FFAR 码时,第一个分量码为有限域方法构造的(3,6)QC-LDPC 码,其对应的每个子矩阵大小为 $L_1=31$. 该分量码采用在 $\text{GF}(32)$ 中构造,即 $q=32$,按照图 1 的构造过程,可构造大小为 $31^2 \times 31^2$ 的 $\mathbf{H}^{(1)}$ 矩阵,再将其转换为相应指数矩阵,选择第 2 行到第 4 行(因为第一行中有零矩阵)、第 1 列到第 6 列,即可得到列重为 3、行重为 6 的 QC-LDPC 码的指数矩阵,再将其转换为相应的 $\mathbf{H}$ 矩阵. 第二个分量码为(3,6)分组码,由于分组码的子矩阵大小必须为质数^[3],因此其子矩阵的大小取 $L_2=11$.

表 1 所示为有限域方法构造的分量码的指数矩阵,表 2 所示为作为第二个分量码的分组码指数矩阵,表 3 所示为通过本文所提方法得到的目标 QC-LDPC 码的指数矩阵.

其中表 1 指数矩阵对应的子矩阵大小为 $L_1=31$,

则其中每个元素按照模 31 来计算获得;表 2 指数矩阵对应的子矩阵大小为 $L_2=11$,则其中每个元素按照模 11 来计算;而目标 QC-LDPC 码的指数矩阵大小为 $L=341$,则其中元素按照模 341 来计算获得。

在表 3 给出的指数矩阵基础上,根据式(1)即可以构造出相应的 $\mathbf{H}$ 矩阵. FFAR 码长为 $341 \times 6 = 2\,046$.

为了便于比较,还在仿真中采用了传统的截短分组码 (Shortened Array code) 和分组码作为分量码,构造的目标 QC-LDPC 码称为 SHAR (SHortened array + ARray) 码。

表 4 为行重为 6,列重为 3 的(3,6)截短分组码的指数矩阵,其中截取的分组码的列数如表 4 中第一行所示为第{0,3,4,7,9,12}列^[4],其中子矩阵大小为 $L_1=41$ (据文献[4],为了便于和 FFAR 码比较,取最接近 31 的子矩阵大小 $L_1=41$).

SHAR 码构造时另一个分量码即为分组码如表 5 所示,子矩阵大小为 $L_2=7$. 表 6 为 SHAR 码的指数矩阵,其子矩阵大小为 $L=41 \times 7 = 287$. SHAR 码的码长为 $287 \times 6 = 1\,722$.

表 1 有限域方法构造的指数矩阵 ($L_1=31$)

	0	1	2	3	4	5
0	18	5	29	10	2	27
1	5	29	10	2	27	22
2	29	10	2	27	22	20

表 2 (3,6)分组码的指数矩阵 ($L_2=7$)

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	8	10

表 3 FFAR 码的指数矩阵 ($L=341$)

	0	1	2	3	4	5
0	297	253	308	165	33	275
1	253	122	134	157	213	115
2	308	134	312	182	239	175

表 4 截短分组码的指数矩阵 ($L_1=41$)

	0	3	4	7	9	12
0	0	0	0	0	0	0
1	0	3	4	7	9	12
2	0	6	8	14	18	24

表 5 分组码的指数矩阵 ($L_2=7$)

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6	1	3

表 6 SHAR 码的指数矩阵 ($L=287$)

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	85	86	171	214	12
2	0	170	172	55	141	24

需要说明,表 1~表 6 中的第一列和第一行分别为各自的列索引号和行索引号. 各个表中的指数矩阵元素“0”指单位阵,即移位参数为 0,而不是零矩阵。

图 2 所示为 FFAR 码和 SHAR 码在 AWGN 信道中的误比特率 (Bit Error Rate, BER) 性能。

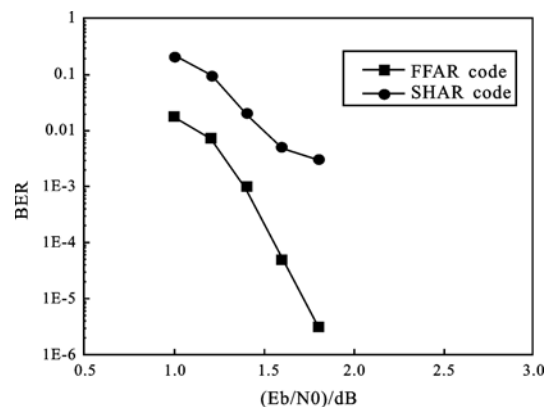


图 2 FFAR 码和 SHAR 码的 BER 性能比较

从图 2 中可以看出,FFAR 码的 BER 性能要明显优于 SHAR 码,有限域方法构造的 QC-LDPC 码性能优异,其“error floor”很低^[6],某些场合甚至超出了随机构造的 LDPC 码性能,因此将其引入到中国余定理设计方法中作为分量码,能够很好改善目标 QC-LDPC 码的性能,有限域方法构造的 QC-LDPC 码 $\mathbf{H}$ 矩阵的最短长度环至少为 6girth (即环长为 6),而分组码的 $\mathbf{H}$ 矩阵中存在着较多的 4girth。

5 结束语

本文构造了基于有限域的 QC-LDPC 码,并将其引入到基于中国余定理的设计方法中. 在中国余定理设计中,有限域方法作为分量码,与已有的分量码,分组码和截短分组码相比,有效改善了目标 QC-LDPC 码的性能,且在接近 10^{-6} 时也没有出现明显的“error floor”. 本文提出的设计方法,不需要优化搜索,构造速度快,性能优异,且适合于硬件实现,在未来移动通信、无线传感网等场合有着很好的应用潜力。

参考文献:

- [1] Myung S, Yang K. A combining method of quasi-cy-

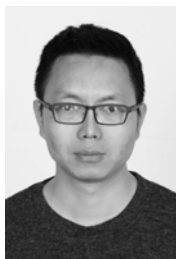
- clic LDPC codes by the chinese remainder theorem[J]. IEEE Communications Letters, 2005(9):823-825.
- [2] Liu Y, Wang X, Chen R, et al. Generalized combining method for design of quasi-cyclic LDPC codes [J]. IEEE Communications Letters, 2004(12):392-394.
- [3] Fan J L. Array codes as low-density parity-check codes [C]// Proc. 2nd Int. symp. turbo Codes and related topics. Brest, France, 2000(4-7):553-556.
- [4] Milenkovic O, Kashyap N, Leyba D. Shortened array codes of large girth[J]. IEEE Trans. Inf. Theory, 2006(52):3707-3722.
- [5] Jiang X, Lee M. Large girth quasi-cyclic LDPC codes based on the chinese remainder theorem[J]. IEEE Communications Letters, 2009(13):342-344.
- [6] Lan L, Zen L, Tai Y Y, et al. Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach[J]. IEEE Trans. Inform. Theory, 2007,53(7):2429-2458.
- [7] Kang J, Huang Q, Zhang L, et al. Quasi-cyclic LDPC codes: an algebraic construction [J]. IEEE Trans. Commun, 2010,58(5):1383-1396.
- [8] Zhang L, Lin S, Ghaffar K A. Quasi-cyclic LDPC codes on cyclic subgroups of finite fields[J]. IEEE Trans. Commun. , 2011,59(9):2330-2336.

作者简介:

徐 华 (1975—), 博士, 副教授. 研究方向为信道编码、协作通信及压缩感知等.

(上接第8页)

作者简介:



孙 斌 男, (1974—), 博士, 讲师. 研究方向为网络流量工程、排队论在计算机网络中的应用.



许 炜 男, (1984—), 博士. 研究方向为网络控制、RFID、物联网在工业中的投资应用分析.