

Constructions of Quasi-Cyclic LDPC Codes Based on Some Partially Balanced Incomplete Block Designs

YAN Tingsu, TANG Yuansheng

School of Mathematical Science, Yangzhou, China

e-mail: yts365@yahoo.com.cn, ystang@yzu.edu.cn

Abstract: In this paper, we construct partially balanced incomplete block designs (PBIBD) based on finite fields, and use them to construct regular low-density parity-check (LDPC) codes. The constructed LDPC codes are free of 4-cycles and with high flexibility for the choosing of the code rate. In addition, we can construct QC-LDPC codes with girth at least 8. In particular, they can also be quasi-cyclic. Simulation results show that some of our codes can have slightly better performance than random regular LDPC codes over AWGN channel.

Keywords: PBIBD; quasi-cyclic LDPC codes; girth; sum-product decoding

基于一些部分平衡不完全区组设计拟循环 LDPC 码的构造

颜廷苏, 唐元生

扬州大学数学科学学院, 扬州, 中国, 225002

e-mail: yts365@yahoo.com.cn, ystang@yzu.edu.cn

【摘要】通过构造部分平衡不完全区组设计, 得到一类低密度校验 (LDPC) 码, 其最小环长 (girth) 至少为 6, 码率的选取具有很大的灵活性, 而且可以具有拟循环结构, 进一步, 我们也利用其构造了 girth 至少为 8 的拟循环 LDPC 码。计算机仿真结果表明, 在加性高斯白噪声信道中与随机码相比, 我们构造的一些码具有更好的译码性能。

【关键词】部分平衡不完全区组设计; 拟循环低密度校验码; 围长; 和积译码

1 引言

LDPC 码首先由 Gallager^[1,2]于 1962 年提出, 在相当长的时间里一直被忽视。直到 1995 年, Mackay 和 Neal^[3,4]的重新发现, 才引起人们的重视。LDPC 码具有非常好的纠错性能, 可以非常接近香农界, 特别是对于随机或伪随机构造的较长的非规则的 LDPC 码^[5,6], 有人甚至构造出了离香农界 0.0045dB 的 LDPC 码^[6]。但随机码的编码复杂度较高, 不利于硬件实现。而拟循环 LDPC 码, 可以在线性时间内用简单线性移位寄存器在线性复杂度条件下完成编码, 而且, 只需要存储校验矩阵的指数矩阵, 大大节约了存储空间。因此, 近年来关于拟循环码

^[7]的构造获得了大量关注。Yu Kou 和 Shu Lin 等人在 [8] 中利用有限几何方法构造出了 LDPC 码, 并在该文的末尾指出, 利用平衡不完全区组设计 (BIBD) 构造 LDPC 码是一个很好的方向。B. Honary 等人^[9-11]利用 Bose^[12]构造的几类 BIBD, 构造出了性能非常好的拟循环 LDPC 码。

本文中, 我们通过构造两类部分平衡不完全区组设计 (PBIBD), 同样得到了一些 girth 大于等于 6 的正则 LDPC 码, 而且可以具有拟循环结构。进一步, 我们也构造了 girth 至少为 8 的 QC-LDPC 码。

本文余下的部分安排如下: 在第二部分我们给出一些基本概念。在第三部分我们构造了两类部分平衡不完全区组设计。在第四部分我们说明了利用部分平衡不完全区组设计来构造正则 LDPC 码的方法。最后我们将所构造的码与 Mackay 的随机码进行了纠错性能方面的比较。

基金项目: 国家自然科学基金 (60473018); 江苏省自然科学基金 (BK2008208); 教育部科学技术研究重点项目 (208045); 东南大学移动通信国家重点实验室开放课题 (W200819)。

2 基本定义

我们首先给出部分平衡不完全区组设计(PBIBD)的定义,这方面的介绍可参考[12,13].

定义 2.1 设 X 为一个 q 元集合, Λ 为一个非负整数的集合. 如果 X 的 n 个 g 元子集 $B_1, B_2, \dots, B_n$, 称为区组, 满足以下条件:

(1) X 中的任意一个元素恰好出现在 r 个区组中;

(2) X 中的任意一个元素对在区组中出现的次数是 Λ 中的一个整数;

则称它们为一个部分平衡不完全区组设计, 记为 PBIBD(q, n, r, g, Λ). 若 Λ 中仅含有一个正整数, 即 $\Lambda = \{\lambda\}$, 则称其为平衡不完全区组设计, 记为 BIBD(q, n, r, g, λ).

定义 2.2 设 X 为 q 元有限域, 区组 $A_1, A_2, \dots, A_k$ 为 X 的 k 个 g 元子集. 若一个部分平衡不完全区组设计可表示为 $A_i + x$, $i=1, \dots, k$, $x \in X$, 则称 $A_1, A_2, \dots, A_k$ 为此部分平衡不完全区组设计的基区组.

在平衡不完全区组设计中, 若 $\lambda=1$, 则 X 的每对元素恰好出现在一个区组中. 在[9,10,11]中 B.Honary 等人利用 BIBD 的这种特殊性质构造了性能很好的 LDPC 码. 我们还注意到, 当 $\Lambda = \{0,1\}$ 时, 这样的 PBIBD(q, n, r, g, Λ) 也可用来构造 Tanner 图中 girth 大于 4 的 LDPC 码.

一个 PBIBD 可由其关联矩阵表示, 设 $X = \{x_1, x_2, \dots, x_9\}$, 下面的区组: $\{x_1, x_2, x_3\}$, $\{x_2, x_7, x_4\}$, $\{x_3, x_9, x_5\}$, $\{x_1, x_8, x_6\}$, $\{x_2, x_9, x_6\}$, $\{x_7, x_8, x_9\}$, $\{x_1, x_7, x_5\}$, $\{x_3, x_8, x_4\}$, $\{x_4, x_5, x_6\}$, 构成一个 PBIBD($9, 9, 3, 3, \{0,1\}$), 它的关联矩阵如下:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

3 部分平衡不完全区组设计的构造

本节中, 我们将给出两类部分平衡不完全区组设计, 定理 3.2 的证明与定理 3.1 类似, 故省.

定理 3.1 设 $p \geq 5$ 为素数, e 为满足 $p^e \equiv 1 \pmod{8}$ 的一个正整数, 令 $t = (p^e - 1)/8$. 设 $S \subseteq \{0, 1, \dots, 2t-1\}$, α 为 $GF(p^e)$ 的一个本原元, 并且使 $\alpha^{2t} + 1 = \alpha^h$ 成立的 h 满足

$$h \not\equiv 0 \pmod{2t} \quad (1)$$

如果存在正整数 L 使得对于 S 中互异的 i 和 j 皆有

$$L(i-j) \not\equiv 0, \pm h \pmod{2t} \quad (2)$$

则

$$\{\alpha^{Li}, \alpha^{2t+Li}, \alpha^{4t+Li}\}, i \in S \quad (3)$$

为一个 PBIBD($8t+1, (8t+1)s, 3s, 3, \{0,1\}$) 的基区组, 其中 $s = |S|$.

证明: 首先我们证明任意两个区组的公共元素的个数不超过 1. 若其不然, 则必有 $i, j \in S, \beta, \beta' \in GF(p^e)$ 使得

$(i, \beta) \neq (j, \beta')$ 以及下面的方程组成立:

$$\begin{cases} \beta + \alpha^{Li+2tu} = \beta' + \alpha^{Lj+2tv}, \\ \beta + \alpha^{Li+2tu'} = \beta' + \alpha^{Lj+2tv'}, \end{cases}$$

其中 $u, u', v, v' \in \{0, 1, 2\}, u > u', v \neq v'$. 根据

$$0 = \alpha^{8t} - 1 = (\alpha^{4t} - 1)(\alpha^{4t} + 1),$$

$$\alpha^{4t} - 1 = (\alpha^{2t} - 1)(\alpha^{2t} + 1),$$

易知

$$\alpha^{4t} + 1 = 0, \quad (4)$$

$$\alpha^{4t} - 1 = (\alpha^{2t} - 1)\alpha^h \quad (5)$$

如果前面的方程组成立, 则可得 $\alpha^{L(i-j)+2t(u'-v')}(\alpha^{2t(u-u')} - 1) = \alpha^{2t(v-v')} - 1$. 由(4),(5)可知, 当

$$(u-u', v-v') \in \{(1, 2), (1, -2), (2, 1), (2, -1)\}$$

时, 有

$$L(i-j) + 2t(u'-v') \equiv 2t-h, \pm h \pmod{8t}$$

而由(1),(2)知这不可能成立. 当

$$(u-u', v-v') \in \{(1, 1), (2, 2), (1, -1), (2, -2)\}$$

时, 由(4),(5)知,

$$L(i-j) + 2t(u'-v') \equiv 0 \pmod{8t} \quad (6)$$

进一步,若 $i=j$, 则可得 $u'=v'$, 进而有 $\beta=\beta'$, 这与 $(i,\beta)\neq(j,\beta')$ 矛盾。而当 $i\neq j$ 时, (6)与(2)是矛盾的。

这样我们就证明了任意两个区组的公共元素的个数不超过 1。此外,由域的性质易知每个元素恰好出现在 $3s$ 个区组中。因此 (3) 是一个 PBIBD($8t+1,(8t+1)s,3s,3,\{0,1\}$) 的基区组。

定理 3.2 设 $p\neq 2,5$ 为素数, e 为满足 $p^e\equiv 1(\bmod 18)$ 的一个正整数,令 $t=(p^e-1)/18$ 。设 $S\subseteq\{0,1,\dots,3t-1\}$, α 为 $\text{GF}(p^e)$ 的一个本原元, h 为使 $\alpha^{6t}-1=\alpha^h$ 成立的某个正整数,如果存在正整数 L 使得对于 S 中互异的 i 和 j 皆有 $L(i-j)\not\equiv 0,\pm h(\bmod 3t)$, 则

$$\{0,\alpha^{Li},\alpha^{6t+Li},\alpha^{12t+Li}\}, i\in S$$

为一 PBIBD($18t+1,(18t+1)s,4s,4,\{0,1\}$) 的基区组,其中 $s=|S|$ 。

4 PBIBD-LDPC 码的构造

基于 PBIBD 可以构造 PBIBD-LDPC 码,方法与[9,10,11]中基于 BIBD 构造 BIBD-LDPC 码相似。以定理 2.1 为例,由基区组(3)可得二元关联矩阵 $H=(H_0,H_1,\dots,H_{s-1})$,其中 H_i 为基区组中第 $i+1$ 个基区组 B_i 所得到的 $p^e\times p^e$ 阶方阵, H_i 的第 j 列向量为 B_i 中的元素与 $\text{GF}(p^e)$ 中的第 j 个元素相加所得区组 $B_{i,j}$ 的位置向量,即若 $B_{i,j}$ 中有一个元素为 $\text{GF}(p^e)$ 的第 k 个元素,则此列向量的第 k 个位置为 1,其余位置都为 0。

这样就得到了一个稀疏的二元矩阵 H , 它的解空间给出了一个 LDPC 码,且 $e=1$ 时, LDPC 码是逆循环的。由于任意两个区组的公共元素的个数不超过 1,这保证了 H 的 Tanner 图中没有长为 4 的圈,从而它的 Girth 至少为 6。由于每个 P_i 相当于 3 个循环置换矩阵的和,因此里面存在大量长为 6 的圈。

更进一步,我们可以构造 Girth 至少为 8 的拟循环 LDPC 码,仍以定理 2.1 为例,先用前面的方法得到 $H=(H_0,H_1,\dots,H_{s-1})$, 由于列重为 3, $P_i, 0\leq i\leq s-1$ 的行重列重都为 3,对 H_i 进行列划分,得到 $3p^e\times p^e$ 阶矩阵 $Q_i=(Q_{i,1},Q_{i,2},Q_{i,3})^T$, 其中 $Q_{i,j}, 1\leq j\leq 3$ 为行重列重都为 1 的循环置换矩阵,结合[7]中的定理 2.1,适当选取 S ,可使构造的码 Girth 至少为 8。

5 计算机仿真与分析

在加性高斯白噪声信道中,我们采用和积译码算法进行译码,最大迭代次数为 100,所有的随机码均由 Neal 和 Mackay 的软件包^[14]生成。

Girth=6 的 QC-LDPC 码的构造。

例 5.1: 由定理 3.1,取 $8t+1=8\times 50+1=401^1$ 。取 $\text{GF}(401)$ 的本原元 $\alpha=3$, 则 $h=63$ 。

取 $S=\{0,1,2,3,4,5,6,7\}$, $L=2$, 此时,我们可得一 PBIBD, 它的关联矩阵由 8 个 401×401 的循环矩阵 $H_0,H_1,\dots,H_7$ 构成,为 $H=(H_0,H_1,\dots,H_7)$, 它的解空间给出一个(2807,3208) QC-LDPC 码,列重为 3,行重为 24,码率为 0.875。其在误码率为 10^{-5} 时,距离香农界约 1.1dB,而在相同误码率的条件下,参数相似的随机码距离香农界 1.05dB,它们之间非常接近。

例 5.2: 由定理 3.2,取 $18t+1=18\times 22+1=397$ 。取本原元 $\alpha=20$,则 $h=364$ 。取 $S=\{0,1,2,3,4,5,6,7\}$, $L=3$, 此时,我们可得一 PBIBD, 其关联矩阵的解空间给出一个(2279,3176) QC-LDPC 码,列重为 4,行重为 32,码率为 0.875。在误码率为 10^{-5} 时,距离香农界约 1.0dB。

由图可以看出,我们构造的 QC-LDPC 码与参数相似的 Mackay 随机码相比,有着非常接近,甚至稍好的译码性能。但我们的码有明确的结构,由于 $e=1$,它是拟循环的。

Girth ≥ 8 的 QC-LDPC 码的构造。

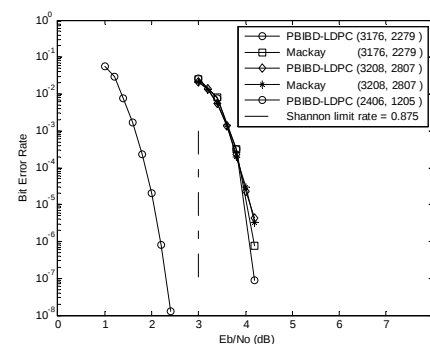


Figure 1. The error performance of codes

图 1. 码的纠错性能

例 5.3: 在例 5.1 中我们取 $S=\{0,1,3,4,6,9\}$, 得一关联矩阵 H , 它由 6 个 401×401 的循环矩阵构成,再将其中的每个循环矩阵进行列划分,得一新的 H , 它由 3×6 个 401×401 的循环置换矩阵构成,它

的解空间给出一个(1205,2406) QC-LDPC 码, 其 girth 至少为 8, 在信噪比为 2.4dB 时, 误比特率达到了 10^{-8} 数量级, 有较低的错误平层(error floor)。

6 结束语

B.Honary 等人利用 Bose^[12]构造的 BIBD, 构造了性能很好的 BIBD-LDPC 码, 我们通过构造 PBIBD, 同样获得了译码性能较好的码, 可保证其 girth 至少为 6 或 8, 仿真表明, 其译码性能很好。

References (参考文献)

- [1] GALLAGER Robert G. Low density parity check codes[J], IRE Transactions on Information Theory, Jan 1962, 8(1), P21-28.
- [2] GALLAGER Robert G. Low density parity check codes[D]. Cambridge, MA:MIT Press, 1963.
- [3] MACKAY David J. C., NEAL R. M. Near Shannon limit performance of low density parity check codes [J], Electronics Letters, 1996, 32(18), P1645-1646.
- [4] MACKAY David J.C. Good error-correcting codes based on very sparse Matrices [J], IEEE Transactions on Information Theory, 1999, 45(2), P399-431.
- [5] CHUNG Sae-Young, FORNEY G. David Jr., RICHARDSON Thomas J. *et al.* Design of capability approaching irregular low density parity check codes [J], IEEE Transactions on Information Theory, 2001, 47(2), P619-637.
- [6] CHUNG Sae-Young, FORNEY G. David Jr., RICHARDSON Thomas J. *et al.* On the design of low density parity check codes within 0.0045dB of the Shannon limit [J], IEEE Communications Letters, 2001, 5(2), P58-60.
- [7] FOSSORIER Marc P. C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices [J], IEEE Transactions on Information Theory, 2004, 50(8), P1788-1793.
- [8] KOU Yu, LIN Shu, FOSSORIER Marc P. C. Low density parity check codes based on finite geometries : A rediscovery and new results [J]. IEEE Transactions on Information Theory, 2001, 47(7), P2711-2736.
- [9] HONARY B., MOINIAN A., AMMAR B. Construction of well-structured quasi-cyclic low-density parity check codes [J], IEE Proc.-Communications, 2005, 152(6), P1081-1085.
- [10] LAN Lan, YING Yu Tai, SHU Lin *et al.* New Constructions Quasi-cyclic LDPC Codes Based on Two classes of balanced incomplete block designs :for AWGN and binary erasure channels AAEC[M] LNCS3857, Berlin Heidelberg: Springer-Verlag, 2006. 275-284.
- [11] LAN Lan, YIN Yu Tai, BEHSHAD Memari *et al.* New Constructions Quasi-cyclic LDPC Codes Based on Special Classes of BIBD's for the AWGN and Binary Erasure Channels [J], IEEE Transactions on Communications, 2008, 56(1), P39-48.
- [12] LE Pan, CHEN Zhi Jingsen, Principle and Applications of Combinatorics Coding[M]. Shanghai scientific & Technical Publishers, 1995.
靳蕃, 陈志, 组合编码原理及应用[M], 上海科学技术出版社, 1995.
- [13] VAN Lint J. H., WILSON R. M. A Course in Combinatorics[M]. Machinery Industry Press, 2004.
- [14] NEAL Radford M., MACKAY David J. C. LDPC-2006-08 [Online]<http://www.cs.toronto.edu/~radford/ftp/LDPC-2006-02-08/index.html>, 2009.