

基于 BIBD 和循环置换矩阵的 LDPC 码

焦新泉, 陈建军, 单彦虎

(中北大学电子测试技术国家重点实验室, 太原 030051)

摘 要: 提出一种基于平衡不完全区组设计(BIBD)和循环置换矩阵的准循环低密度校验码(LDPC)构造方法。根据实际需求, 利用 BIBD 构造相应的模板矩阵, 用适合的循环置换矩阵进行扩展。采用该方法构造的 LDPC 码具有良好的结构和灵活性, 该方法在一定范围内可快速方便构造出某一特定码长或码率的准循环 LDPC 码。仿真结果证明, 准循环 LDPC 码在高斯白噪声信道上采用迭代译码时, 具有较优的纠错性能及较低的错误平层。

关键词: 平衡不完全区组设计; 准循环低密度校验码; 循环置换矩阵; 模板矩阵; 有限域

LDPC Code Based on Balanced Incomplete Block Design and Cycle Permutation Matrix

JIAO Xin-quan, CHEN Jian-jun, SHAN Yan-hu

(National Key Laboratory for Electronic Measurement Technology, North University of China, Taiyuan 030051, China)

【Abstract】 A method to construct a flexible length or rate of quasi-cyclic Low Density Parity Check(LDPC) codes based on Balanced Incomplete Block Design(BIBD) and cycle permutation matrix is proposed. Based on actual demand, the corresponding template matrix is constructed by BIBD method. The template matrix is extended by the appropriate cycle permutation matrix. The quasi-cyclic LDPC codes constructed by the proposed method have a good structure and flexibility. This method improves the efficiency of construction good codes which meet the needs of a practical application. Simulations show that quasi-cyclic LDPC codes constructed by the proposed method perform well over AWGN channels with iterative decoding and have a lower error floor.

【Key words】 Balanced Incomplete Block Design(BIBD); quasi-cyclic Low Density Parity Check(LDPC) code; cycle permutation matrix; template matrix; finite field

DOI: 10.3969/j.issn.1000-3428.2012.02.095

1 概述

低密度校验(Low Density Parity Check, LDPC)码是当前信息编码研究的热点, 已在深空通信、卫星通信、光纤通信、磁/光存储、ADSL、无线局域网等领域得到应用, 并被视为未来最有发展潜力的一类编码。LDPC 码由 Gallager 等^[1]在 1962 年提出, 在相当长的时间里一直被忽视。直到 1995 年, Mackay 和 Neal^[2-3]的重新发现, 才引起人们的重视。自此, 人们对 LDPC 码从设计、构造、结构分析、编码、译码、性能分析和应用等方面进行了大量研究。其中, 准循环 LDPC 码是一类结构化 LDPC 码, 由于其奇偶校验矩阵的独特结构, 能够利用反馈移位寄存器实现线性复杂度的编码, 因此被广泛应用。

由于准循环 LDPC 码在实际应用中只需要存储校验矩阵的指数矩阵, 大大节约了存储空间, 因此近年来关于准循环码的构造获得了大量关注和研究。文献[4-5]构造了基于置换矩阵的准循环 LDPC 码, 文献[6-7]构造了基于有限域的准循环 LDPC 码, 文献[8]构造了基于欧式几何的准循环 LDPC 码, 文献[9-11]对准循环 LDPC 码子阵的选择和分布作了优化。这些方法都构造出了某类码长和码率的准循环 LDPC 码, 在码长和码率的选择上还不够灵活。本文将平衡不完全区组设计(Balanced Incomplete Block Design, BIBD)和循环置换矩阵 2 种构造方法相结合, 提出了一种一定范围内不同码率和码长准循环 LDPC 码的构造方法, 所构造出的码的围长大于等于 6。

2 平衡不完全区组设计

以下给出一类平衡不完全区组设计方法。对于正整数 t , $12t+1$ 可表示为素数的幂次方。存在含有 $12t+1$ 个元素的有限域 $GF(12t+1)$, 令 x 为其本原元且满足:

$$x^{4t}-1=x^c \quad (1)$$

其中, c 为小于 $12t+1$ 的奇整数。可以设计一个具有如下参数的 BIBD: $m=12t+1$, $n=t(12t+1)$, $\gamma=4$, $\rho=4t$, $\lambda=1$ 。首先构造 t 个集合:

$$B_i = \{0, x^{2i}, x^{2i+4t}, x^{2i+8t}\} \quad (2)$$

其中, $0 \leq i < t$ 。

对于每个集合, 将 $GF(12t+1)$ 中的每个元素与该集合相加得到 $12t+1$ 个集合, 共可得到 $t(12t+1)$ 个集合, 将这些集合看作 BIBD 的区组, 有限域中的元素看作 BIBD 中集合的元素。故该 BIBD 对应的邻接矩阵 Q 为行重 $\rho=4t$ 、列重 $\gamma=4$ 且 $\lambda=1$ 的 $(12t+1) \times t(12t+1)$ 阶矩阵。其中, Q 由 t 个 $(12t+1) \times (12t+1)$ 阶循环矩阵按行排列而成, 形如:

$$Q = [Q_0 \quad Q_1 \quad \cdots \quad Q_{t-1}] \quad (3)$$

其中, Q_i 是由 B_i 生成的 $(12t+1) \times (12t+1)$ 阶循环矩阵。由于所构造的平衡不完全区组中 $\lambda=1$, 任意 2 个区组的公共元素的

基金项目: 国家自然科学基金资助项目(60871041)

作者简介: 焦新泉(1978—), 男, 讲师、硕士; 主研方向: 信息编码, 遥测存储; 陈建军, 讲师、博士研究生; 单彦虎, 博士研究生

收稿日期: 2011-11-21 **E-mail:** jiaoxinquan@nuc.edu.cn

个数不超过 1, 因此基于该 BIBD 可以构造出围长至少为 6 的 LDPC 码。

3 基于 BIBD 和循环置换矩阵的 LDPC 码构造

循环置换矩阵 P 是满足以下 2 个条件的方阵:

(1) 矩阵 P 每行每列只有一个元素为 1, 其他元素均为 0。

(2) 矩阵 P 每一行是其上面一行向右(左)循环移动 1 位, 第 1 行是其最后一行向右(左)循环移动 1 位。

准循环 LDPC 码校验矩阵的典型特点是其由相同大小的子方阵组成, 子方阵可以是循环置换矩阵或全零矩阵。令:

$$H = \begin{pmatrix} P_{a_{0,0}} & P_{a_{0,1}} & \cdots & P_{a_{0,n-1}} \\ P_{a_{1,0}} & P_{a_{1,1}} & \cdots & P_{a_{1,n-1}} \\ \vdots & \vdots & & \vdots \\ P_{a_{m-1,0}} & P_{a_{m-1,1}} & \cdots & P_{a_{m-1,n-1}} \end{pmatrix} \quad (4)$$

其中, $P_{a_{i,j}}$ ($0 \leq i < m, 0 \leq j < n$) 为 $p \times p$ 循环置换矩阵或全零矩阵, 若 H 满足 RC-约束条件, 则 H 为一个准循环低密度校验码的校验矩阵, H^T 也可作为准循环 LDPC 码的校验矩阵。

如果将准循环 LDPC 码校验矩阵中所包含的循环置换矩阵用“1”代替、全零矩阵用“0”代替, 则构成 2 阶有限域 $GF(2)$ 上的一个矩阵, 本文称为模板矩阵 T 。

$$T = \begin{pmatrix} 1 & 1 & \cdots & 0 & 1 \\ 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad (5)$$

本文以 BIBD 构造准循环 LDPC 码校验矩阵的模板矩阵。由于循环置换矩阵 P 的每行每列只有一个元素为 1, 其他元素均为 0, 因此在模板矩阵基础上经过循环置换矩阵 P 和全零矩阵扩展所得到的 LDPC 码的围长大于等于直接由模板矩阵作为校验矩阵所得到的 LDPC 码的围长。

在构造码长为 n 、码率为 R 的准循环 LDPC 码时, 先用前面提到的 BIBD 方法构造模板矩阵。码率 R 与 t 的关系为:

$$t = 1/(1-R) \quad (6)$$

其中, t 为正整数, 是 $1/(1-R)$ 的近似值。

如果 t 的个位数非 2 和 7 ($t=2$ 除外), 则 $12t+1$ 可表示为素数的幂次方, 存在含有 $12t+1$ 个元素的有限域 $GF(12t+1)$, 就可构造出一个行重 $\rho=4t$ 、列重 $\gamma=4$ 且 $\lambda=1$ 的 $(12t+1) \times t(12t+1)$ 阶模板矩阵 T 。

码长 n 与循环置换矩阵 P 的阶数 p 的关系为:

$$n = t(12t+1)p \quad (7)$$

可得出: $p = n/t(12t+1)$ 。

用阶数为 p 的循环置换矩阵(单位矩阵 I 为特例)和全零矩阵填充模板矩阵 T , 即可得到码长为 n 、码率为 R 、围长大于等于 6 的准循环 LDPC 码。

4 仿真结果

用本文提出的方法构造了 2 个准循环 LDPC 码, 与用 Mackay 方法构造的随机码作了仿真结果比较。仿真在加性高斯白噪声(AWGN)信道上进行, 采用 BPSK 调制及 SPA 译码。这些码采用 SPA 译码时都收敛得很快, 在仿真中用了 50 次迭代。选用的第 1 个码是码长为 6 123、码率约为 0.92 的一个(6 123, 5 652)准循环低密度校验码。

由已知码率根据式(6)可得出参数 $t=13$, 在有限域 $GF(12t+1)$ (即有限域 $GF(157)$)上按本文方法先构造出一个 157×2041 的模板矩阵 T 。然后通过式(7)得出 $p=3$ 。最后用

阶数为 3 的循环置换矩阵(这里用单位矩阵 I)和全零矩阵填充模板矩阵 T , 得到一个列重 $\gamma=4$ 的(6 123, 5 652)准循环低密度校验码。将这个码标记为 BP(6 123, 5 652)。在误码率为 10^{-6} 时, BP(6 123, 5 652)与香农限仅有约 1.2 dB 的差距。用 BP(6 123, 5 652)与有相同码长、码率、列重的随机 Mackay 码进行对比仿真实验。从图 1 可以看出, 用本文方法构造出的码在误码率 BER 上具有与随机码一样的优异纠错性能。由于这些码的列重为 4, 因此都具有较好的极小距离, 图中, E_b/N_0 是每个 bit 上的能量与干扰功率谱密度的比值。

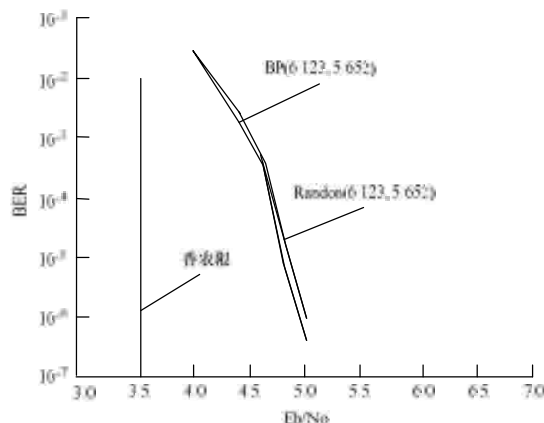


图 1 BP(6 123, 5 652) QC-LDPC 码的纠错性能

仿真中选用的第 2 个码是码长为 9 264、码率为 0.94 的一个(9 264, 8 685)准循环低密度校验码。构造方法与第 1 个码的方法相同。将这个码标记为 BP(9 264, 8 685)。在误码率为 10^{-6} 时, BP(9 264, 8 685)与香农限仅有约 0.9 dB 的差距。从图 2 可以看出, BP(9 264, 8 685)同样具有与随机 Mackay 码几乎完全相同的性能。没有估计所构造的低密度校验码的错误平层, 但是从仿真结果可以看到, 采用本文方法构造的低密度校验码的错误平层在 10^{-8} 以下。

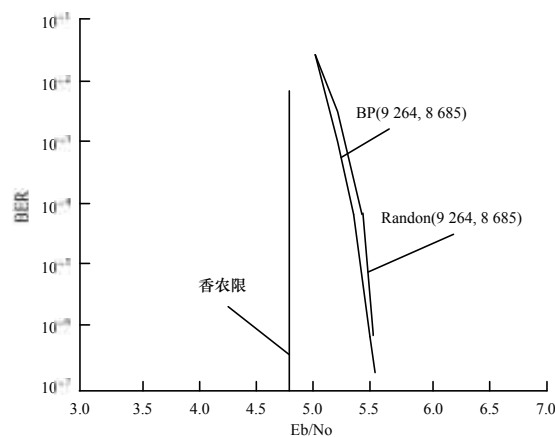


图 2 BP(9 264, 8 685) QC-LDPC 码的纠错性能

5 结束语

代数构造的准循环低密度校验码具有编码及译码较为简单、易于实现等优点。本文给出了一种在一定范围内可快速方便构造出某一特定码长或码率的准循环低密度校验码的方法。在纠错码的实际应用过程中提高了针对某一实际应用需求构造好码的效率。仿真结果证明, 所构造的这一类准循环低密度校验码在加性高斯白噪声信道上采用迭代译码时具有优良的纠错性能, 并具有较低的错误平层。

(下转第 287 页)