

基于 Q 矩阵的 LDPC 码编码设计方法

王 哲, 栾英姿

(西安电子科技大学, 陕西 西安 710071)

摘 要:给出了 Q 矩阵的定义,在此基础上提出了一种基于 Q 矩阵的 LDPC 码编码器设计方法。此设计方案将奇偶校验矩阵 H 分解成两个子矩阵 H^p 和 H^f ,通过对这两个子矩阵分别设计,构造出 H 矩阵。其中 H^p 是上三角双对角矩阵, H^f 矩阵由 Q 矩阵按照一定的行重列重,根据某种排列规则构造而成。着重研究了 Q 排列规则,并找到了一种较好方法,使得这种编码方案得到了很好的性能。采用的这种编码方案的编码器算法具有较低的实现复杂度,为 LDPC 码编码器设计提供了很好的选择方案。

关键词:LDPC 码;奇偶校验矩阵; Q 矩阵

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2010)06-0201-04

Design of LDPC Code Based on Q - Matrix

WANG Zhe, LUAN Ying-zi

(Xidian University, Xi'an 710071, China)

Abstract: In this paper, the definition of Q matrix is introduced first, and the designation of LDPC codes based on Q matrix is proposed, which is based on Q - Matrix. In this method, the parity check matrix H is constructed by two matrixes: H^p and H^f , H^p is an upper triangular dual diagonal matrix, H^f is formed by Q matrix based on a certain principle which is the focus of this paper, a good construction principle of H^f is proposed, which improves the performances of LDPC codes. The encoder algorithm is easier to implement and it provides a good suggestion for the encoder of LDPC codes.

Key words: LDPC code; parity-check matrix; Q - Matrix

0 引言

LDPC 码(low density parity check codes)是 Gallager 于 1962 提出的一种性能接近香农极限而且可以实现的编码方案^[1]。在许多需要高可靠性的通信和数字存储系统中,有着极其广阔的应用前景。

LDPC 码是一种具有稀疏校验矩阵的线性纠错码。其校验矩阵的元素除了一小部分为 1 以外,其他绝大多数均为零。LDPC 码可以由其校验矩阵 H 来定义^[2]。对 LDPC 码编码器的研究主要分为两步:首先,研究校验矩阵的构造算法,其次,根据校验矩阵的结构来研究编码器算法。

下文介绍的基于 Q 矩阵的准规则 LDPC 码由一组循环正交 Q 矩阵构成,能根据给定的码长和码率设计校验矩阵 H ,从而使码长和码率的取值具有更大的灵活性,并且该类码字可以直接利用 H 矩阵编码,降低

了编码器的复杂度^[1]。

1 Q - 矩阵的定义及性质

定义:若 $n \times n$ 阶非对角单位方阵(n 为任意正整数)的每行每列及每条对角线(包括斜率为正负的两种情况)上均只有一个“1”,则称该矩阵为 Q 矩阵^[3]。

Q 矩阵的这种特殊结构对 LDPC 码的校验矩阵的构成具有特殊意义,如果可以找到多个 n 值相同但布局不同的 Q 矩阵,并将它们按照一定的规则排列,这样就可以构成准规则 LDPC 码的校验矩阵 H 。因而怎样寻找 n 值一定的 Q 矩阵的布局就成为这种编码方法的重要环节。这个问题可以由“皇后算法”解决。

“皇后问题”是这样描述的:由 $n \times n$ 个方块排成 n 行 n 列的正方形称为“ n ”元棋盘。若任意两个皇后位于 n 元棋盘上同一行,同一列或同一对角线,则称它们互相攻击。要求找出使 n 元棋盘上的 n 个皇后互不攻击的布局^[4]。由此可见,它与寻找 Q 矩阵的布局是等效的。

下面是 $n = 8$ 时 Q 矩阵的一种布局。

收稿日期:2009-09-09;修回日期:2009-12-30

作者简介:王 哲(1983-),女,硕士研究生,研究方向为 LDPC 码的编译码原理;栾英姿,副教授,研究方向为多载波码分多址中的关键技术。

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

其对应的矢量为(4,7,5,3,1,6,8,2),它所表示的是:该列的皇后位于哪一行,矢量中第一个元素4的意思就是第一列的皇后位于该列的第4行。

可见, Q 矩阵的每行每列是彼此正交的。并且可以看出,由一个 Q 矩阵,循环左(或右)移位一次,就可以得到一种新的布局,从而可以得出这样的结论:如果已知 n 维 Q 矩阵的一种布局,将其循环左移(或右移) n 次,就可以得到皇后矩阵的 n 种布局。并且通过证明可知,这 n 种布局彼此之间是正交的。

Q 矩阵的这两种性质对于文中这种编码方案有着极其重要的作用。首先,由于循环移位性,因而只需搜索到一种布局,就可以得到 n 个布局,当 n 达到一定大小时,只需找到一种布局,就能够得到构造校验矩阵所需的 Q 矩阵。其次,这 n 个布局对应的 Q 矩阵彼此正交,若将这些由一种布局循环移位所得到的布局构成一个集合,那么由这个集合中的元素按照某种规则排列构成校验矩阵,可以避免出现四环,从而提高迭代译码的性能。

Q 矩阵的获取可以由经典的皇后回溯算法实现,但是效率很低,难以满足编码的要求。文中采用一种有效的快速搜索算法实现 Q 矩阵布局的搜索,可以很好地满足码长的要求,并且具有很高的灵活性^[5~7]。

2 Q 矩阵构成 LDPC 码的方法

H 矩阵的结构对 LDPC 码的性能具有极大的影响:迭代解码的性能,若奇偶校验矩阵中存在四环,迭代解码的性能会下降。

由 Q 矩阵构成 LDPC 码 H 矩阵的思想是将 H 矩阵分解为两个子矩阵: $H = [H^p : H^d]$,其中 H^p 是一个 $(N-K) \times (N-K)$ 的方阵,称为校验位矩阵, H^d 是一个 $(N-K) \times K$ 的矩阵,称为信息位矩阵(N 为 LDPC 码的码长, K 为信息位长度)^[4]。

H^p 是双对角线形式的下三角矩阵,具有如下形式:

$$H^p = \begin{bmatrix} 1000000 \cdots \\ 1100000 \cdots \\ \cdots \cdots \cdots \\ 0000 \cdots 110 \\ 00000 \cdots 11 \end{bmatrix}$$

H^d 是由 $j \times k$ 个 n 维 Q 矩阵按一定规则构成的(其中 j 是对应 LDPC 码 H 矩阵的列重, k 为行重),故它的维数是 $jn \times kn$ 。对应 LDPC 码的码长为 $N = (j+k)n$,信息位 $K = k \times n$,码率为 $k/(j+k)$ 。这样就可以根据码长和码率设计需要的 LDPC 码,具有更大的灵活性。

由 H^p 和 H^d ,构造出校验矩阵 $H, H = [H^p : H^d]$,这样,就由 Q 矩阵构成了 LDPC 码^[3,8]。将 H 矩阵对应的码矢量 c 分解为两部分,分别为校验位 c^p 和信息位 c^d ,码字 $c = [c^p : c^d]$, H 与 c 的关系为:

$$Hc^T = [H^p H^d] \begin{bmatrix} c^p \\ c^d \end{bmatrix} = H^p c^p + H^d c^d = 0$$

$$\text{二进制情况下, } H^p c^p = H^d c^d, c^p = (H^p)^{-1} H^d c^d$$

3 Q 矩阵的排列方法

H^d 是有若干相互正交的 Q 矩阵按照一定规则排列而成的,那么如何排列这些 Q 矩阵才能得到好的性能?规则如下:第一,为了避免出现四环,构成 H^d 的这些 Q 矩阵最好是由同一个 Q 矩阵循环移位得到的。第二,为了避免出现四环,四角的 Q 矩阵不能相同^[4]。满足这两个要求的可能的排列方法有以下几种(均已行列重等于6为列,码长均为576):

1) 顺序排列法:6×6个 n 维 Q 矩阵按下标顺序排列。

$$\begin{bmatrix} Q_1 Q_2 Q_3 Q_4 Q_5 Q_6 \\ Q_7 Q_8 Q_9 Q_{10} Q_{11} Q_{12} \\ Q_{13} Q_{14} Q_{15} Q_{16} Q_{17} Q_{18} \\ Q_{19} Q_{20} Q_{21} Q_{22} Q_{23} Q_{24} \\ Q_{25} Q_{26} Q_{27} Q_{28} Q_{29} Q_{30} \\ Q_{31} Q_{32} Q_{33} Q_{34} Q_{35} Q_{36} \end{bmatrix}$$

按照上述方法排列 Q 矩阵得到 H 矩阵,仿真结果如图1所示,可见这种排列方法性能很差,分析原因,可能是由于所有的 Q 矩阵都是由同一个原始的 Q 矩

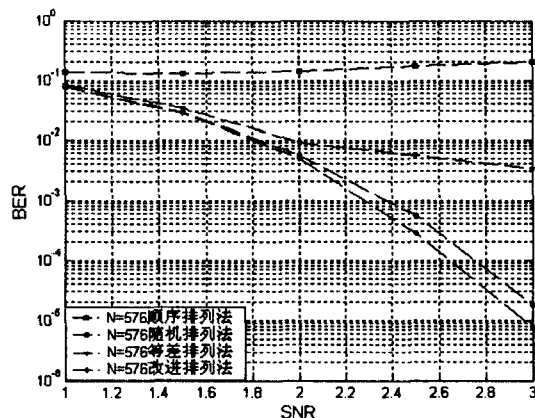


图1 码长576时四种排列方法性能对比图

阵循环移位得到的,相邻编号的 Q 矩阵是彼此循环一位得到的,这导致性能很差,应该尽量让这些 Q 矩阵分散开来,因而考虑到下面的第二种排列方法。

2) 随机排列法: 6×6 个 n 维 Q 矩阵根据下标顺序随机排列。

这种方法用到 36 个 Q (用到 Q 的个数根据行重和列重得到),它们是在 N 一定时,由同一个 Q 矩阵循环移位产生的。

$$\begin{bmatrix} Q_{10} & Q_{29} & Q_9 & Q_{11} & Q_{27} & Q_{30} \\ Q_{17} & Q_{33} & Q_{24} & Q_{40} & Q_{46} & Q_{14} \\ Q_{21} & Q_{42} & Q_7 & Q_1 & Q_{12} & Q_{19} \\ Q_{36} & Q_{38} & Q_{32} & Q_{43} & Q_2 & Q_6 \\ Q_{15} & Q_{20} & Q_8 & Q_{41} & Q_{25} & Q_{44} \\ Q_{35} & Q_{31} & Q_{26} & Q_{18} & Q_3 & Q_{48} \end{bmatrix}$$

按照上述方法排列 Q 矩阵得到 H 矩阵,性能有很大的提高,可以作为一种方案,但是这种排列方法缺少规律性,实际操作的过程中难以实现。最好能找到一种排列方法,既能保证 Q 矩阵分散开来,又使排列方案有规律可循,因而想到下面的排列方案。

3) 变换公差为等差数列排列法: 6×6 个 n 维 Q 矩阵根据下标顺序按等差数列排列,但每行的公差都不相同。每列都以 Q_1 开始,第一行的公差是 0,所以第一行都是 Q_1 ,第二行公差是 2,第三行公差是 3,以此类推,公差之间必须满足互为素数^[4]。

$$\begin{bmatrix} Q_1 & Q_1 & Q_1 & Q_1 & Q_1 & Q_1 \\ Q_1 & Q_2 & Q_4 & Q_6 & Q_8 & Q_{10} \\ Q_1 & Q_3 & Q_6 & Q_9 & Q_{12} & Q_{15} \\ Q_1 & Q_5 & Q_{10} & Q_{15} & Q_{20} & Q_{25} \\ Q_1 & Q_7 & Q_{14} & Q_{21} & Q_{28} & Q_{35} \\ Q_1 & Q_{11} & Q_{22} & Q_{33} & Q_{44} & Q_{55} \end{bmatrix}$$

按照上述方法排列 Q 矩阵得到 H 矩阵,性能不是特别理想,没有随机排列性能好,但是规律性比较强。分析原因,从尽量让相邻的 Q 矩阵分散这个规律入手,上述排列法中的 Q_1 过多,可能影响性能。因此得到下面第四种排列法。

4) 在第三种排列方法的基础上,提出一种改进的排列方法,即去掉第一行和第一列元素完全相同的矩阵 Q_1 ,排列方法如下:

$$\begin{bmatrix} Q_2 & Q_4 & Q_6 & Q_8 & Q_{10} & Q_{12} \\ Q_3 & Q_6 & Q_9 & Q_{12} & Q_{15} & Q_{18} \\ Q_5 & Q_{10} & Q_{15} & Q_{20} & Q_{25} & Q_{30} \\ Q_7 & Q_{14} & Q_{21} & Q_{27} & Q_{35} & Q_{42} \\ Q_{11} & Q_{22} & Q_{33} & Q_{44} & Q_{55} & Q_{66} \\ Q_{13} & Q_{26} & Q_{39} & Q_{52} & Q_{65} & Q_{78} \end{bmatrix}$$

按照上述方法排列 Q 矩阵得到 H 矩阵,性能很理想。这种排列方法规律性强,同时具备很好的性能,故文中采用这种排列方法来生成 H 矩阵,实现编码器。

图 1 是上文研究的四种排列方法得到的仿真图,由图可见,改进方法的性能最好。

图 2 是码长分别为 576, 1056, 1536 和 2304 四种情况下,采用改进排列方法构造 Q 矩阵 LDPC 码得到的仿真图,可见码长为 2304 时,信噪比约为 2.2dB 时,误码率已达 10^{-6} 。

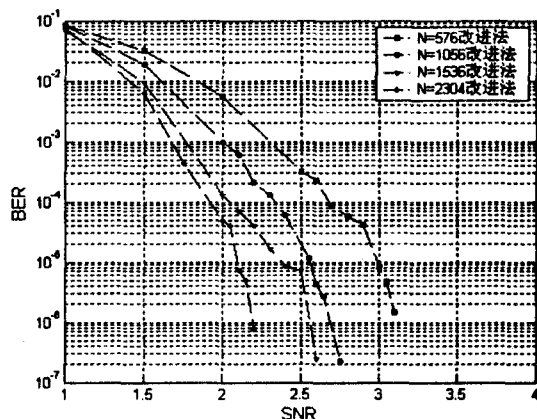


图 2 改进法四种码长性能对比图

综上所述,可得出构造 H^d 矩阵的最佳方案,即先找到 N 维 Q 矩阵的一种布局,通过循环移位,得到 N 种不同的布局,把这些 Q 矩阵按照改进的构造法就得到信息位矩阵 H^d 。

接下来的问题是:当 Q 矩阵的维数较大时,通过快速搜索算法,可以得到多种原始 Q 矩阵,只需将其中的一种布局循环移位若干次,当维数 N 足够大时,就可以得到构成 H^d 所需的 Q 矩阵。那么,选择哪种布局作为原始 Q 矩阵进行循环移位,得到若干个相互正交的 Q 矩阵构造 H^d 矩阵?在所有 Q 矩阵中一定存在最优的原始 Q 矩阵,选择最优原始 Q 矩阵与否对性能影响是否会很大?如果是,那就有必要找到最优的原始 Q 矩阵;如果不是,那么就可以使用 Q 矩阵的快速搜索算法随机地找到一种布局作为原始 Q 矩阵的布局来构成 H 矩阵。

首先通过快速搜索算法,随机地得到四种原始 Q 矩阵,分别对它们进行循环移位,构成 H 矩阵,仿真结果如图 3 和图 4 所示,码长为 576 和 1056。

由图 3 和图 4 可见,当信噪比较小时,原始 Q 矩阵不同的情况下,误码率差别很小,随着信噪比的增加,误码率出现抖动(码长为 576 时,信噪比超过 2.5dB 时出现抖动;码长 1056 时,信噪比超过 2dB 就出现抖动)。说明原始 Q 矩阵不同,对编码器性能有一定的影响。码长越长,对抖动越敏感。多种原始 Q 矩阵中一定

存在最优,如何找到最优的布局,还需要进一步研究。

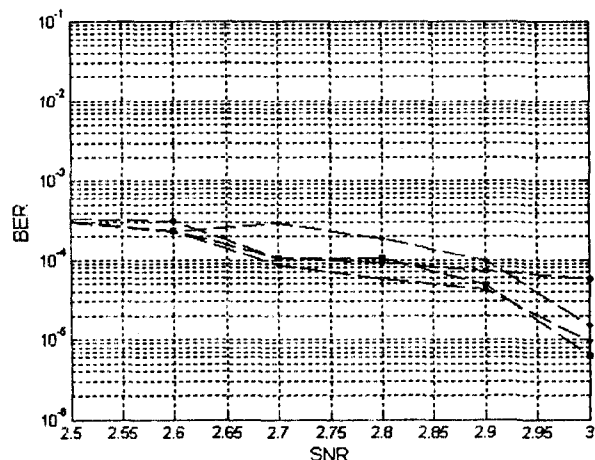


图 3 码长 576 时不同原始 Q 矩阵性能对比

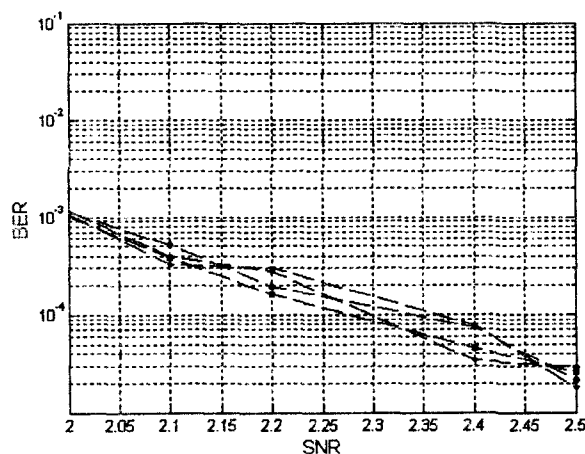


图 4 码长 1056 时不同原始 Q 矩阵性能对比

4 结束语

文中介绍的由 Q 矩阵构成 LDPC 码的方法,不需

要生成 G 矩阵,只需由 H 矩阵就可以进行编码。其中 H^d 矩阵的构成,即 Q 矩阵的排列规则对整个 LDPC 码的性能有重要的影响。通过顺序排列、随机排列、变换公差等差数列排列法,以及其改进排列法这四种排列方法的对比,总结出了一定的排列规律并得到了较好的性能。文中只给出了一种相对较好的排列方案,如何排列这些正交的 Q 矩阵得到最优的布局并且分析是否最优布局对编码器性能的影响,是未来一个很好的研究方向。

参考文献:

- [1] Gallager R. Low Density Parity Check Codes[D]. Cambridge, MA:Massachusetts Institute of Technology,1960.
- [2] 孙韶辉,慕建君,王新梅. 低密度校验码研究及其新进展[J]. 西安电子科技大学学报,2001,28(3):393-397.
- [3] 彭立,朱光喜. Q -矩阵准规则 LDPC 码编码器计方案的研究[J]. 计算机工程与科学,2005,27(6):81-82.
- [4] 彭立,朱光喜. 基于 Q -矩阵的 LDPC 码编码器设计[J]. 电子学报,2005,33(10):1734-1739.
- [5] Susic R, Gu Jun. Fast Search Algorithms for the Q -queens Problem[J]. IEEE Transactions System, Man, and Cybernetics, 1991,21(6):1572-1576.
- [6] Susic R, Gu Jun. Efficient Local Search Conflict Minimization: A case Study of the n -Queens Problem[J]. IEEE Transactions on Knowledge and Data Engineering, 1994, 6(5):661-668.
- [7] 王哲,栾英姿. N 皇后问题的快速搜索算法[J]. 计算机技术与发展,2009,19(6):72-75.
- [8] 彭立,朱光喜. 不同置换矩阵对基于分块 H 矩阵的 LDPC 码性能的影响[J]. Chinese Journal of Computers, 2008, 31(5):783-954.

(上接第 195 页)

处理框架[J]. 计算机技术与发展,2009,19(8):74-79.

- [5] 萧荣兴,苏伟仁,许育嘉. RFID 技术运作的神经中枢——RFID 中间件[J]. 信息与电脑,2005,19(9):35-37.
- [6] Hoag J E, Thompson C W. Architecting RFID middleware[J]. Internet Computing, 2006,10(5):88-92.

(上接第 200 页)

应用研讨会(SPCA06). 中国新疆乌鲁木齐:[出版者不详],2006:306-310.

- [4] 贾雯,贺栋. 面向服务的开发方式在普适计算领域中的应用[J]. 计算机应用与软件,2008,25(8):123-125.
- [5] 郭朝珍,林志虹,郭昆. 协同综合预报 IGDSS 通用模型的研究与应用[J]. 通信学报,2006,27(11):42-47.
- [6] 刘少林. 台风综合预报群决策支持系统的研究与实现[D]. 福州:福州大学,2009.

- [7] 蒋邵岗,谭杰. RFID 中间件数据处理与过滤方法的研究[J]. 计算机应用,2008,28(10):2613-2615.
- [8] 饶涛涛,邹继军,郑勇芸. 现场总线 CAN 原理与应用技术[M]. 北京:北京航空航天大学出版社,2007:18-20.

- [7] 王伟,张正兰. 基于 J2ME 平台的手机实时监视系统的设计[J]. 计算机技术与发展,2007,17(12):182-186.
- [8] 任晓尘,孙涌. 基于 J2ME/J2EE 移动预约挂号系统的设计与实现[J]. 计算机技术与发展,2006,16(12):187-189.
- [9] 张俊妍,陈启买. SOAP 协议性能与安全的研究进展[J]. 计算机技术与发展,2009,19(6):163-166.
- [10] 赵阳. 基于 Web Service 的群体决策支持系统的研究[D]. 南京:南京理工大学,2008.