

准循环 LDPC 码最小汉明距离的计算与校验矩阵的改善

李韵姣, 叶 凡, 任俊彦

(复旦大学 专用集成电路与系统国家重点实验室, 上海 201203)

摘 要: 基于线性代数的基本原理和线性分组码的结构特点, 提出了能准确计算 QC LDPC 码最小汉明距离的方法, 并对计算复杂度进行估计; 然后针对 QC LDPC 码的结构特点, 对其校验矩阵进行改善, 以增大码字的最小汉明距离, 从而得到更好的译码性能. 其中, 计算最小汉明距离的方法同样适用于普通的线性分组码.

关键词: 低密度奇偶校验码; 校验矩阵; 最小汉明距离; 准循环; 误码率

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2010)06-0118-04

Computation and Reformation of the Minimum Distance and Check Array of QC LDPC Codes

LI Yun-jiao, YE Fan, REN Jun-yan

(State Key Laboratory of ASIC and System, Micro/Nanoelectronics Science and
Technology Innovation Platform, Fudan University, Shanghai 201203, China)

Abstract: Based on the principles of linear algebra and linear block codes, a method is proposed to calculate the minimum distance of a group of QC LDPC codes as well as other kinds of linear block codes. A estimation of time complexity is stated too. A method of generating larger minimum distance by reforming the check array is given for QC LDPC codes based on its special structure.

Key words: LDPC codes; check array; minimum distance; quasi-cyclic; Bit error rate

1 引言

低密度奇偶校验码 (Low-Density Parity-Check codes, LDPC codes) 是一种性能逼近香农限的优秀线性分组码, 在码长较长时, 其性能超过了 Turbo 码^[1]. 此外, LDPC 码的译码采用了具有线性复杂度的“和-乘积”算法 (SPA), 译码复杂度大大低于 Turbo 码. LDPC 码的优异性能及其在信息传输中的良好应用前景已经引起学术界和信息产业界的高度重视. 然而编码器的复杂度始终是制约 LDPC 码发展的主要因素, 因此产生了准循环奇偶校验码 (Quasi-Cyclic LDPC codes, QC LDPC codes) 等有利于编码电路硬件实现的构造方式^[2-3].

QC LDPC 码属于线性分组码, 而线性分组码的

最小汉明距离是反映该组码性能好坏的最根本因素^[4]. 文中针对线性分组码的结构特点, 提出了计算最小汉明距离的方法, 并根据 QC LDPC 码的结构特征对其校验矩阵进行改善, 使得由此矩阵确定的 QC LDPC 码的最小汉明距离尽量大, 以得到更好的译码性能.

2 QC LDPC 码简介

2.1 LDPC 码简介

LDPC 码是一类特殊的线性分组码, 其校验矩阵 H 中绝大多数元素为 0, 只有极少数的 1, 即 H 是稀疏矩阵. 校验矩阵的稀疏性使得译码复杂度得到降低, 实现更为简单. LDPC 码是由其校验矩阵唯一确定的. 一个 (n, j, k) 规则的 LDPC 码的校验矩

阵每一行和每一列都含有固定个数的 1,且个数分别为 k 和 j . 例如一个 $(12,3,4)$ LDPC 码的校验矩阵:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (1)$$

线性分组码的生成矩阵 G 与校验矩阵 H 满足 $HG^T = 0$,通常将 H 用高斯消元法化简为 $H = (I | P)$ 的形式,其中 I 为单位阵,则 $G = (P^T | I)^T$. 然而 H 的稀疏性并不能保证 G 的稀疏性,因此给编码电路带来很多困难. 编码电路的复杂度往往与码长成指数关系.

2.2 QC LDPC 码

准循环 LDPC 码(QC LDPC codes)是一种允许低复杂度编码结构 LDPC 码^[5]. 其校验矩阵是由多个相同大小的稀疏循环矩阵构成的矩阵,具有如下形式:

$$H_{qc} = \begin{bmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,t} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,t} \\ \vdots & \vdots & & \vdots \\ A_{c,1} & A_{c,2} & \cdots & A_{c,t} \end{bmatrix} \quad (2)$$

其中 c 和 t 为正整数,且 $c < t$; A_{ij} 为 $b \times b$ 的循环阵. 所谓循环阵,是指这样一个方阵,其中每一行都是上一行的循环右移,并且第一行是最后一行的循环右移. 对于这样的循环阵,每一列也都是它前一列的循环下移,并且第一列是最后一列的循环下移.

QC LDPC 码是一个由稀疏循环矩阵构成的校验矩阵的零空间. 由约束条件 $HG^T = 0$ 计算得到的生成矩阵 G 也同样具有准循环的特性,这样就可以用简单的移位寄存器和累加器进行编码,其复杂度与该码的生成矩阵的规模成线性关系. 参考文献[2]给出了编码电路结构.

3 最小汉明距离的计算

与所有线性分组码一样,QC LDPC 码的最小汉明距离仍然是判断其译码性能的一个重要参考标准. 对于最小距离为 $d_{\min}$ 的一组线性分组码,有如下定理:

定理 1 若纠错码的最小距离为 $d_{\min}$,那么有如下三个结论的任何一个结论成立:

(1) 可以检测出任意小于等于 $l = d_{\min} - 1$ 个差错.

(2) 可以纠正任意小于等于 $t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$ 个差错.

(3) 可以检测出任意小于等于 l 同时纠正小于等于 t 个差错,其中 l 和 t 满足

$$\begin{cases} l + t \leq d_{\min} - 1 \\ t < l \end{cases}$$

可以看出,最小汉明距离对于线性分组码的性能有着重要影响.

对于最小汉明距离的计算,一些文献给出了估算方法,例如最小码字搜索法^[4,6],其基本思想是,在传输过程中给一个全 0 的码字叠加适当的噪声,让译码器把收到的码字当成小码重的码字来译码,然后算出这些码的码重,从中搜索最小码重的码字. 这种方法中对噪声的控制要求比较严格,而且得到的是估计值. 下面将提出一种精确计算最小汉明距离的方法,并且在得到一组码的最小汉明距离的同时,也可以得到与其相关的矩阵的列的位置信息,调整这些列的位置,可以有效增加最小汉明距离.

根据线性分组码的结构及线性代数的基本原理,可以推出以下推论:

推论 1 一组线性分组码的最小汉明距离为 d 的充分必要条件是,这组码的校验矩阵 H 中必存在 d 列,使得由这 d 列构成的子矩阵中,每行“1”的个数都为偶数或 0;且不存在任何 $s < d$ 列,使得由这 s 列构成的子矩阵中,每行“1”的个数都为偶数或 0.

证明:

(1) 充分性

令校验矩阵

$$H = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} \quad (3)$$

在其对应的码字集合中,取两个码字 C_i 和 C_j , 其中

$$C_i = (C_{i1}, C_{i2}, \cdots, C_{in}) \quad (4)$$

$$C_j = (C_{j1}, C_{j2}, \cdots, C_{jn}) \quad (5)$$

假定 C_i 与 C_j 之间的距离就是最小码距 d ,并且假定 C_i 与 C_j 在同一位置具有不同比特值的码段,即产生码距的码段为 $C_{i,r1}, C_{i,r2}, \cdots, C_{i,rd}$ 和 $C_{j,r1}, C_{j,r2}, \cdots, C_{j,rd}$, 其中

$$\sum_{k=1}^d r_k = d \quad (6)$$

由于 C_i, C_j 都满足校验方程


```

11000000 10010000 00000110
01100000 01001000 00000011
00110000 00100100 10000001
00011000 00010010 11000000
00001100 00001001 01100000
00000110 10000100 00110000
00000011 01000010 00011000
10000001 00100001 00001100];

```

经计算得 $d = 6$, 其中由第 1、3、9、14、22、23 列组成的子矩阵的每一行含有 1 的个数都为偶数或 0。实际上由于 H_1 矩阵的准循环特性, 第 2、4、10、15、23、24 等由以上各列循环移位得到的列组成的子矩阵, 每一行都含有偶数个 1 或 0。

4 增大最小汉明距离的方法

对于上面给出的 H_1 矩阵, 如果打破第 1、3、9、14、22、23 列所构成的子矩阵所满足的每行具有偶数或 0 个 1 的条件, 并保证没有个数更少的列组成的子矩阵满足这个条件, 那么由 H_1 确定的一组 QC LDPC 码的最小汉明距离将大于 6。

根据线性代数中向量的线性相关定理, 只需将这些列中的某一段进行调整, 即可打破这个条件。为了保持原矩阵的密度和码率不做太大的改变, 以便于比较, 仅对原矩阵中的个别子循环矩阵进行循环移位。这里对 H_1 矩阵中的 A_{21} 子矩阵循环右移一次, 得到新的 H_2 矩阵:

$H_2 =$

```

[10110000 01010000 11000000
01011000 00101000 01100000
00101100 00010100 00110000
00010110 00001010 00011000
00001011 00000101 00001100
10000101 10000010 00000110
11000010 01000001 00000011
01100001 10100000 10000001

```

```

01100000 10010000 00000110
00110000 01001000 00000011
00011000 00100100 10000001
00001100 00010010 11000000
00000110 00001001 01100000
00000011 10000100 00110000
10000001 01000010 00011000
11000000 00100001 00001100];

```

经过 matlab 计算, 得到最小汉明距离 $d = 8$, 产生最小距离的列位置为: 1, 2, 3, 5, 13, 14, 15, 19 以

及由这些列循环移位得到的其他列。

对 H_1 和 H_2 矩阵确定的 QC LDPC 码进行译码性能比较, 对于全零的码字叠加随机错误, 采用硬判决译码, 其译码结果如表 1 所示。

表 1 不同最小汉明距离 QC LDPC 码的译码性能比较

错误个数	是否成功译码		平均迭代次数(总数 20)	
	H_1	H_2	H_1	H_2
1	是	是	1	1
2	否	是	20	2
3	否	是	20	2

为演示方便, 所选 H_1 和 H_2 矩阵的规模较小, 且不具有严格的低密度的性质, 但可以粗略看出最小距离增大后, 译码性能得到了改善。

对于更大规模的矩阵, 比较结果如图 1 所示。其中 H_1 矩阵通过上述方法计算得出的最小汉明距离为 16。 H_2 由 H_1 多次调整得到, 调整方法为上文所述的对 H_1 的子循环矩阵进行移位, 并避免产生更小的码距。最终得到的 H_2 所对应 QC LDPC 码的最小距离为 21。

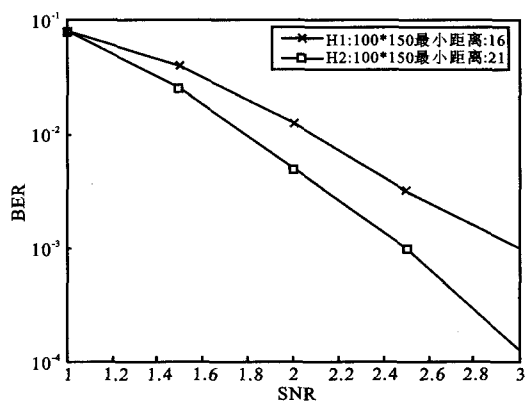


图 1 相同规模不同最小汉明距离的 QC LDPC 码译码性能比较

可以看出, 在对已有校验矩阵进行分析计算得到其对应码组的最小汉明距离以及相关的列的位置后, 可以采用如下的方法对校验矩阵进行调整: 将产生最小距离的列所在的子循环矩阵进行尝试性的多次循环移位, 并保证没有造成更小的汉明距离的产生。此方法可以有效增加最小汉明距离, 使误码率得到降低。

5 结束语

文中对线性分组码提出了一种准确计算最小汉

(下转第 127 页)

优化方案分支方向预测器实现较复杂,但是分支方向预测准确率比 mgshare 预测器和 bimodal 预测器都高;采用优化的 BTB,硬件实现存储器和比较逻辑面积大幅降低,分支方向预测和分支目标地址预测实现分配合理.和参考方案比较,整体实现面积小、功耗低,整个分支处理单元预测准确率高^[6].

5 结束语

分支处理单元由分支方向预测器和分支目标地址预测单元两部分组成,文中通过理论分析、实验论证说明了这两大部分各种实现方案的优缺点,并分别进行了优化设计.进一步综合数学推导的结论和实验得到的结论,提出了自己的分支预测单元:comb 分支方向预测器和优化的 BTB 结构.为了显示该设计的优越性,同时实现了一种简单的分支处理单元的参考模型: gshare 预测器^[7]和 BTB.在搭建的 VCS 仿真平台下进行仿真验证,并用 Power Compiler 进行功耗分析;用 Design Compiler 对分支处理单元进行了综合,其中时钟约束在 100MHz,并用 Primetime 进行了静态时序分析.结果表明,该设计相比参考模型具有面积小、功耗低及预测准确率高的特点.

参考文献:

- [1] Smith J E. A study of branch prediction strategies[C]// Minneapolis: Proceedings of the 8th Annual International

Symposium on Computer Architecture. Widely, 1981:135-148.

- [2] Yeh T, Patt Y. Two-level adaptive branch prediction [C]// Proceedings of the 24th Annual ACM/IEEE International Symposium and Workshop on Microarchitecture. USA:Ann Arbor, 1991:51-61.
- [3] Scott M, McFaring. Combining branch predictors[R]. California, Technical Report TN-36, Digital Western Research Laboratory, 1993.
- [4] Perleberg C, Smith A J. Branch target buffer design and optimization[J]. IEEE Transactions on Computers, 1993 (23):396-412.
- [5] Brian K Bray, Flynn M J. Strategies for branch target buffers[M]. New York:ACM,1991.
- [6] 汪永威,樊晓桢,黄小平. 32 位 RISC 微处理器中分支预测器的硬件实现[J]. 计算机应用与研究,2008(2):419-422.
- [7] 武萌,沈海斌. 一种 gshare 分支预测器的低功耗设计方法[J]. 微电子学与计算机,2007,24(3):200-206.

作者简介:

鄢国丰 男,(1984-),硕士研究生.研究方向为计算机系统结构、专用集成电路设计.

张盛兵 男,(1968-),教授.研究方向为 VLSI 系统设计、计算机系统结构、电子设计自动化.

黄小平 男,(1980-),博士研究生.研究方向为计算机系统结构、专用集成电路设计、VLSI 系统设计.

(上接第 121 页)

明距离的方法,并针对 QC LDPC 码校验矩阵的准循环结构特点提出改善校验矩阵的方法,使最小汉明距离得到增加,从而提高了 QC LDPC 码的译码性能.对于分析和优化 QC LDPC 码具有一定的意义.

参考文献:

- [1] Robert G Gallager. Low density parity check codes[J]. IRE Transon. Inform. Theory, 1962,8(1):21-28.
- [2] Zongwang Li, Lei Chen, Lingqi Zeng, et al. Efficient encoding of quasi-cyclic low-density parity-check codes [J]. IEEE Transaciton On Communications, 2006, 54 (1):71-81.

- [3] Tomas J Richardson, Rudiger L Urbanke. Efficient encoding of low-density parity-check codes [J]. IEEE Transaciton on Communications Theory, 2001,47(2):638-656.
- [4] Xiaoyu Hu, Fossorier M P C, Evangelos E. On the computation of the minimum distance of low-density parity-check codes[J]. IEEE International Conference on Communications, 2004(2):767-771.
- [5] Shu Lin, Lei Chen, Jun Xu, et al. Near shannon limit quasi-cyclic low-density parity-check codes[J]. IEEE Globecom, 2003:2030-2035.
- [6] 肖旻,王琳,罗智勇. LDPC 码的最小汉明距离估算. 信息技术,2005(1):4-6.