LDPC 码的最小汉明距离估算

肖 [illegible][1]，王 琳[1]，罗智勇[2]

(1. 厦门大学通信工程系，厦门 361005；2. 信息产业部第七五零厂，广州 510656)

摘 要：低密度奇偶校验码 (LDPC) 是一种优秀的线性分组奇偶校验码。在简要阐述 LDPC 码原理上，给出了一种叫“最小码字搜索法”的算法来估算 LDPC 码的最小汉明距离。并用相应的实例给予验证，显示了该方法的正确性与实用性，对分析与优化 LDPC 码设计具有重要参考价值。

关键词：低密度奇偶校验码；最小汉明距离

中图分类号：TP301.6　　**文献标识码**：A　　**文章编号**：1009 - 2552(2005)01 - 0004 - 03

Computation of the minimum distance of low - density parity - check codes

XIAO Min[1]，WANG Lin[1]，LUO Zhi-yong[2]

(1. Department of Communication Engineering, Xiamen University, Xiamen 361005, China;
2. The 750th Factory of Ministry of Information Industry, Guangzhou 510656, China)

Abstract: Low - density parity - check (LDPC) codes are a good liner block parity codes. In this paper, the fundamental of LDPC codes are introduced briefly first. Then an algorithm called the minimum - weight codeword searching is discussed, which can be used to compute the minimum distance of LDPC codes. The effectiveness and the practicability of the algorithm are demonstrated by some examples. It is significant for us to analyze and optimize the design of LDPC codes.

Key words: low - density parity - check codes; minimum distance

0 引言

LDPC 码(low - density parity check codes)是一种基于稀疏矩阵的奇偶校验码。Gallager 于 1962 年首先发明了这种码，故又称 Gallager 码。由于当时的计算机处理能力与相关理论的薄弱，这种优秀的码型没有在科学界引起足够的重视。1996 年 D. MacKay 从现代编码理论观点出发，证明利用迭代译码的 LDPC 码具有逼近香农限的性能[1]。2000 年发现不规则 LDPC 码甚至可以距离香农限只有 0.0045dB[2]。

目前有多种典型的方法来构造好的 LDPC 码，如何评判所构造码的好坏，一般的方法是把构造出来的码组通过仿真，算出在一定信噪比下传送一定信息量时的误码率，根据信噪比 —误码率曲线来判断码组性能的好坏。但是，实际上 LDPC 码是一种线性码，线性码组的纠错能力还可以用最小汉明距离 (即为 d_{min}) 来表示。然而，LDPC 码的 d_{min} 的计算是一个 NP 完全问题，也就是说计算 LDPC 的 d_{min} 的时间复杂度不能用一个多项式来表示。所以一直没有一个有效的方法来精确计算 LDPC 码的 d_{min}。文中给出一种叫“最小码字搜索法”的算法来估算 LDPC 码的 d_{min}，估算出的值是 d_{min} 的上限，但是已经比较接近 d_{min}，同时也用信噪比 —误码率曲线来验证了该算法的正确。这对分析 LDPC 码纠错性能具有重要参考意义。

1 LDPC 码

LDPC 码是一种线性纠错码。通常，一种线性分

收稿日期：2004 - 07 - 14

基金项目：国家“863”计划项目(2001AA123061)；国家自然科学基金项目(60272005)资助

作者简介：肖[illegible](1982 -)，女，硕士研究生，2004 年毕业于厦门大学电子工程系，主要研究方向为移动通信系统，高效纠错编码技术。

组码是由其生成矩阵 G 表示,而 LDPC 码却常由其校验矩阵 H 表示。这是因为 LDPC 码的 H 矩阵具有非常稀疏的形式:绝大多数的矩阵元素都是 0,只有很少数量的 1。Gallager 在 1963 年时定义的 (n, j, k) LDPC 码是码长为 n 的规则的 LDPC 码,在它的校验矩阵 H 中,每一行和列中 1 的数目是固定的,其中每一列 1 的个数是 j,每一行的个数是 $k(k \geq 3)$。如图 1 所示,就是一个规则的 $(12,3,4)$ LDPC 码的校验矩阵。

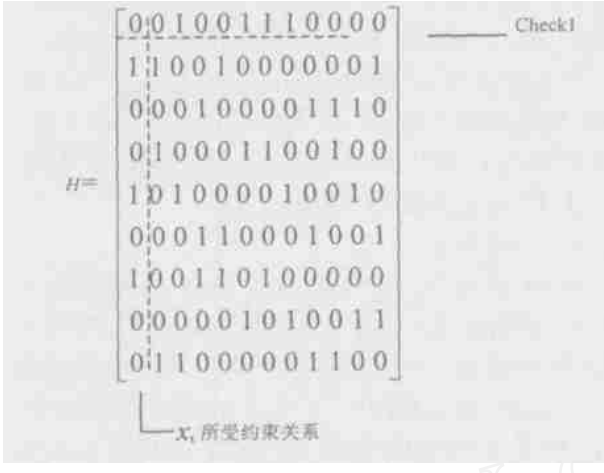

图 1 $(12,3,4)$ LDPC 码的校验矩阵

根据 H 矩阵的定义可知,矩阵的每一行是一个校验方程 (check);矩阵的每一列表示该列所对应的变量(variable)受到哪些 check 的约束。图 1 的例子中,第一行即为:$x_3 \oplus x_6 \oplus x_7 \oplus x_8 = 0$,$\oplus$ 表示模 2 加,第一列表示 variablex_1 受到 check2,check5,check7 的约束。

不规则 LDPC 码的每个变量点所受约束的个数不一样,每个校验方程约束的变量点的个数也是不一样的。这就使其 H 矩阵每一行的 1 个数不同,每一列的 1 个数也不同。

2 LDPC 码最小汉明距离的估算

2.1 LDPC 码的最小汉明距离问题

解决线性码的最小汉明距离问题就是要找到与一个特定的 H 矩阵相对应的码组的最小汉明距离 $d_{\min}$。线性码的最小汉明距离与该码组的纠错能力 $[(d_{\min}-1)/2]$ 有关,所以在编码理论中最小汉明距离问题是一个基本的问题。如果能够把它计算出来,就可以用来判别码组纠错能力的好坏。

而对于 LDPC 码的最小汉明距离的计算更有其特殊的意义。目前有多种典型的方法来构造好的 LDPC 码,有:随机构造法、几何构造法、PEG(progressive - edge - growth)方法等等。这些好的码在实验室的大量仿真中都有很好的性能,误码率达到 10^{-5} 到 10^{-7},但是对于目前仿真还不能达到的更低的误码率的估计,只能用联合界限的渐进算法来从理论上估计,而这一方法要用到码字的最小汉明距离 $d_{\min}$。

不幸的是,LDPC 码最小汉明距离的精确计算是一个 NP 完全问题,也就是说计算 LDPC 码的最小汉明距离的时间复杂度不能用一个多项式来表示[3 ～ 4]。在无法精确地知道 LDPC 码 $d_{\min}$ 的情况下,对 $d_{\min}$ 的估算就显得具有重要实用价值。在下文中,阐述了一种叫“最小码字搜索法”的方法来估算 LDPC 码的 $d_{\min}$。以便用联合界限的渐进算法估计 LDPC 码误码率上下限,从性能上分析与优化 LDPC 码设计。

2.2 最小码字搜索法

2.2.1 基本思想

线性分组码的最小汉明距离可以等于非 0 码的最小码重。“最小码字搜索法”的主要思想是:在传输中给全 0 的码字增加适当的噪声,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。当然,同样的噪声只传送一次,所找到的码字不一定是最小码重的码字,于是就继续发送全 0 的码字,叠加不同的噪声后再译码、搜索。随着重复次数的增加,找到的小码重的码字就越多,这些码字中包含最小码重的码字的可能性就越大。最后从找到的码字中确定一个最小的码重,作为 LDPC 码的最小汉明距离的估计值。这个方法的关键是噪声的控制,要使得译码器既然不会译出全 0 的码字,也不会译出码重太大的码字。

2.2.2 噪声的选择

为了适应该搜索法,利用了两种噪声:突发错误噪声和信息位反转噪声。

突发错误噪声是 Berrou 等人提出的[5],最早是用于计算 Turbo 码的最小汉明距离的。由于这种噪声的加入,使得送入译码器的已调制的全 0 码字的形式为 $Y = (-1, -1, \cdots -1, -1 + A, -1, \cdots -1, -1)$ (假设 $X = (-1, \cdots, -1)$ 是全 0 码字调制以后的表示),A_i 是一个正整数,i 是产生突发错误的位置。这种噪声的特点是:A_i 只加在 i 这个位置。只要把 A_i 的大小或位置作适当调整,使得译码器能够较快地搜索到小码重的码字,再从这些小码重的码字中找到最小的那个,目的就达到了。

对于信息位反转噪声,顾名思义,假设发送的码字为 $X = (-1, \cdots, -1)$,则第 i 位发生信息位反转之后,接收到的码字的第 i 位就为 1。

需要指出的是突发错误噪声和信息匣反转噪声都是人为的噪声,现实当中并不存在,是为了一些算法才被设计出来的。这两种噪声还可以进一步地推广,即可以在多个信息位上增加突发错误或信息位反转。

2.2.3 “最小码字搜索”译码算法

“最小码字搜索”译码算法是 Fossorier 的 IRB (iterative reliability - based) 算法[6]的一种派生。每一次搜索时,先经过和积算法把每个信息 bit 的后验概率算出来,按照概率的大小找到最可能确定下来几个的信息 bit,作为一个基(basis),再由这个基生成一系列的后备码字,最后用校验方程来检验后备码字,排除不满足校验方程的码字。而“最小码字搜索”译码器和 IRB 译码器的不同点在于:前者的目的是要找到最小码重的码字,而后者的目的是要找到最有可能是发送码字的码字。

“最小码字搜索”译码的每次搜索步骤如下:

(1) 通过和积算法[7]算出每个信息 bit 的后验概率。

(2) 按照后验概率的情况找到 N^e 个最不能确定的信息 bit,并把这几个 bit 对应的 H 矩阵中的列置换到 H 矩阵的最左边。剩下的 $n - N^e$ 个信息 bit 就根据它们的后验概率判决为 0 或 1,并保存下来,作为基。

(3) 对 H 矩阵最左边的 N^e 列进行高斯消去,产生一个近似的上三角矩阵的形式,将在高斯消去过程中遇到的非独立的 N^d 列置换到右边,而左边剩下是 $N^e - N^d$ 个的独立列,如图 2 所示。

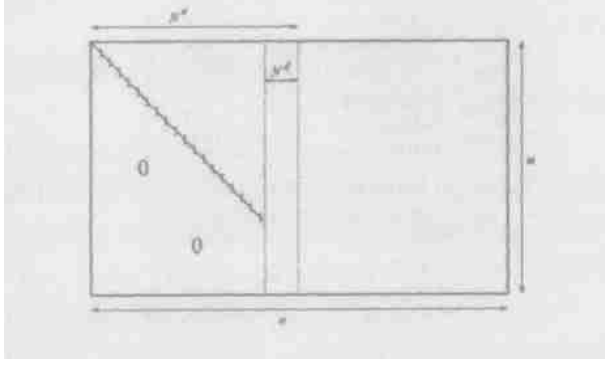

图 2 变换之后的 H 矩阵

(4) 对 N^d 个非独立的列所对应的信息 bit 进行 0 或 1 的组合,对每一次的组合,检验一下 $N^e - N^d + 1, \cdots, m$ 这几个校验方程。如果其中任何一个方程不满足,则排除这一组合。如果都满足,则按照递归的方法根据方程:$N^e - N^d$, $N^e - N^d - 1, \cdots, 1$ 推算出剩下的 $N^e - N^d$ 个信息 bit,再与前面的 $n - N^e$ 个信息 bit 一起进行校验,排除不满足方程的组合。这样就可以找到满足校验方程的小码重的码字。

(5) 计算生成的合法码字的码重并记录下来,把找到的最小码重值跟 d_{min} 比较,若小于 d_{min},则把它赋给 d_{min}。

(6) 改变叠加噪声的位置,重复以上步骤。理论上叠加噪声的位置可以从 0 一直到 $n - 1$, d_{min} 的值随着时间的增加会不断地更新,但是只要你觉得所求得的 d_{min} 已经满足要求,就可以中止程序运行。

需要指出的是,如果叠加的噪声是信息位反转噪声,则叠加噪声的这一位不参与和积算法的计算,并硬判决为 1。同时 N^e 的值需要调整,使得 N^d 的值不会太大,一般来说, $N^d = 6 \sim 10$。

2.2.4 估算例子

寻找到帧长为 500,1000,3000 的规则(3,6)LDPC 码各一组,三者的性能如图 3 所示。再利用“最小码字搜索”算法对这三个码组的最小汉明距离进行估算,算法是用 C ++ 语言实现的,估算结果如下:帧长为 500 的码组的 d_{min} 为 22,帧长为 1000 的码组的 d_{min} 为 54,帧长为 3000 的码组的 d_{min} 为 200。

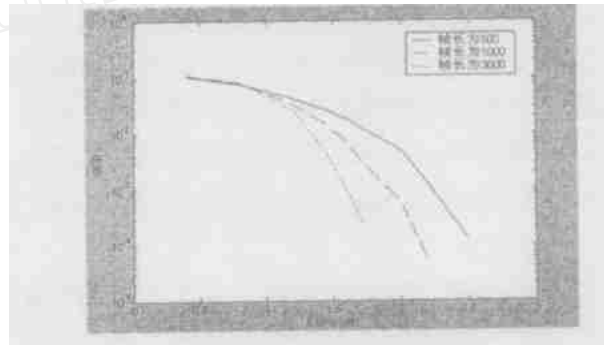

图 3 LDPC 码的性能比较

3 结束语

LDPC 码以其优秀的性能吸引着越来越多人的关注,对 LDPC 码的最小汉明距离的研究有助于对其性能进行评判和优化。由于精确计算 LDPC 码的最小汉明距离是一个 NP 完全问题,所以本文给出一种叫“最小码字搜索法”的算法来估算 LDPC 码的最小汉明距离。这种方法的主要思想是:给全 0 的码字加适当小的噪声,让译码器把收到的码字当成小码重的码字来译码,从而寻找一个最接近全 0 的码字,这个码字的码重就最接近该码组的最小汉明距离。实验结果表明该方法可以有效地估计出 LDPC 码的最小汉明距离,这对分析和优化 LDPC 码设计具有重要作用。

(下转第 71 页)

lc.bind(ldapVersion ,loginDN ,password)

lc.add(newentry) ;

5.4 LDAP 的安全模型

LDAP 的安全模型主要是基于绑定操作的,如图 3。绑定操作的不同使得安全机制有所不同。一般有匿名、基本认证、SASL 认证三种方式。SASL 认证是提供的在 SSL 和 TLS 安全通道基础上进行的身份认证,包括数字证书的认证。SSL/ TLS 是基于 PKI 安全技术,在 Internet 上广泛采用的安全服务。通过 SASL 方式绑定,LDAP 客户端应用调用在服务器上的 SASL 协议驱动器,接着该驱动器连接由 SASL 机制所说明的验证系统来获取用户的验证信息,可以实现对客户端身份和服务器端身份的双向验证,结合 PKI 认证机制使用。

图 3 SASL 安全机制示意图

6 结束语

LDAP 服务以其高效性、可扩展性、灵活性等方面的强大优势在信息安全、科学计算、网络管理、电子政务管理等方面广泛应用。本文主要讲述了 LDAP 在统一身份认证系统中的基本应用,对于统一身份认证系统的设计与实现,这些是不够的,在实际研究中还将进行大量的程序开发和技术结合等工作。

参 考 文 献:

[1] Yeong W ,Howes T ,Kille S. Lightweight Directory Access Protocol [S]. RFC1777. 1995.

[2] Wahl M ,Howes T ,Kille S. Lightweight Directory Access Protocol (v3) [S]. RFC 2251. 1997.

[3] Smith M. Definition of the Inetorgperson LDAP Object Class [S]. RFC2798. 2000.

[4] 王燕,谢金宝. Linux 下基于 Web 的目录服务系统的设计与实现[J]. 计算机应用工程,2000 ,(1).

[5] 于剑. LDAP 目录服务在 Web 开发中的应用[J]. 计算机应用,2003 ,(10).

[6] 钟小平,张金石. 网络服务器配置与应用[M]. 北京:人民邮电出版社,2004. 1.

责任编辑:杨立民

(上接第 14 页)两个信噪比为 20dB 的等功率信号,分别从 45 和 °入射到八元半波等距线性天线阵列上时,MUSIC 算法的角度分辨率明显要高于 Capon 最小方差算法。但 MUSIC 算法仍有许多的限制,其中要求信号不相关,其实在很多实际情况中阵列会接收到来自不同方向上的相干信号,这就会使 MUSIC 算法的性能显著下降。此外,受多径的影响也较为严重。

3 结束语

本文针对基于时间(TDOA)的定位方法在实现中的同步问题,提出了一种利用自适应阵列的基于方位角的定位方法,避免了同步要求而带来的问题。同时,自适应阵列作为自适应数字波束形成器,能获取高精度的 MS 方位角信息。此外,应用自适应阵列还可以实现扇区划分,提高了系统容量和接收信号的强度。

参 考 文 献:

[1] 范平志,等. 蜂窝网无限定位[M]. 北京:电子工业出版社,2002. 12.

[2] Litva J ,Lo T K. Digital Beamforming in Wireless Communication[M]. Artech House Publisher ,1996.

[3] Feuerstein. Phased - Array Smart Antennas Increase Capacity in CDMA Networks[J]. Wireless Design ,1999.

[4] 无线通信中的智能天线 IS - 95 和第 3 代 CDMA 应用[M]. 马凉,等译. 北京:机械工业出版社,2002. 8:187 - 200.

责任编辑:杨立民

(上接第 6 页)

参 考 文 献:

[1] MacKay D J C and Neal R M. Near Shannon limit performance of low density parity check codes[J]. Electronics Lett. ,1996 ,32(18) :1645 - 1646.

[2] Chung S Y, Forney J G D, Richardson T, and Urbanke R. On the design of low - density parity - check codes within 0. 0045 dB of the Shannon limit[J]. IEEE Commun. Lett. , 2001 ,5(2) :58 - 60.

[3] Vardy A. The intractability of computing the minimum distance of a code[J]. IEEE Trans. Inform. Theory, 1977 ,43(11) :1757 - 1766.

[4] http :// www. inference. phy. cam. ac. uk/ mackay/ MINDIST- ECC. html [DB/ OL].

[5] Berrou C and Vaton S. Computing the minimum distance of linear codes by the error impulse method[J]. in Proc. IEEE Intl. Symp. Inform. Theory, Lausanne, witzerland, 2002 ,(7).

[6] Fossorier M P C. Iterative reliability - based decoding of low - density parity - check codes[J]. IEEE J. Select. Areas Commun. , 2001 ,19 (5) :908 - 917.

[7] Kschischang Frank R, Frey Brendan J ,Hans - Andrea Loeliger. Factor Graphs and the Sum - Product Algorithm[J]. IEEE Trans. Inform Theory ,2001 ,47(2).

责任编辑:李光辉