

基于两代树的低密度校验码校验矩阵构造方法

张菁

(长安大学 电子与控制工程学院, 西安 710061)

(jingzhang@chd.edu.cn)

摘要:针对传统的低密度校验(LDPC)码稀疏矩阵构造算法不易实现或可能得到的结果不满足条件的缺陷,给出了一种新颖的基于两代树结构的低密度校验矩阵的构造搜索算法。该算法采用人们熟悉的树型数据结构,可以较为合理地表示稀疏校验矩阵中行与列中非零元素的跳转关系。结果表明,结合蚁群算法在路径搜索方面的优势,采用这种基于两代树的搜索算法,具有算法简单、容易实现的优点。更进一步,如果考虑到非规则码的构造中外信息的引入,可以很容易地将该算法应用在非规则码的构造中。

关键词:低密度校验码;两代树结构;纠错码;和积算法;蚁群算法

中图分类号: TN911.2 **文献标志码:** A

Construction method of low density parity check code matrix based on two-generation tree structure

ZHANG Jing

(School of Electronic and Control Engineering, Chang'an University, Xi'an Shaanxi 710061, China)

Abstract: To remedy the defects of the traditional sparse matrix construction algorithm in Low Density Parity Check (LDPC) code which is hard to be fulfilled or the obtained results are not satisfactory, a new parity-check matrix searching algorithm was proposed based on two-generation tree structure. This algorithm used the data of tree structure, and could more reasonably the skipping relations of the non-zero elements in the rows and lines of the sparse check matrix. Combined with Ant Colony Algorithm (ACA) which has advantages in path-seeking, the proposed algorithm is simple and easy to realize. Furthermore, it is easy to apply the algorithm to the irregular code, when importing the outside information to the code.

Key words: Low Density Parity Check (LDPC) code; two-generation tree structure; error-correcting code; Sum-Product Algorithm (SPA); Ant Colony Algorithm (ACA)

0 引言

低密度校验(Low Density Parity Check, LDPC)码是一种线性纠错码^[1]。Gallager^[1]在其1960年的博士论文中首次提出了低密度校验码,并给出了和积算法(Sum-Product Algorithm, SPA),也就是置信传播算法(Belief Propagation Algorithm)。由于当时条件的限制,低密度校验码并未引起人们的重视。近几年,当人们在向Shannon极限前进时,重新认识到低密度校验码及其解码算法的理论上的重要性和启发意义。当前,非规则校验矩阵因为其近Shannon理论极限的良好特性而受到人们关注,其性能略好于Turbo码^[2]。

LDPC码完全由其校验矩阵决定,矩阵的结构对码的性能有决定性作用。所以,LDPC码直接可由其校验矩阵来表示,一般来说有矩阵表示和Tanner图表示^[3]。校验矩阵构造算法的数学手段包括:向量空间分析及随机置换算法、Mackey编码构造方法、组合数学中的均衡不完全区组设计(Balanced Incomplete Block Design, BIBD)^[4]、Euclid几何中的LDPC码构造方法等。

制约LDPC码应用的问题是:对于非规则的LDPC码,如果直接由校验矩阵 H 和生成矩阵 G 来进行编码和解码^[5-6],其计算量与码长 n 成平方关系;而Turbo码的编码计算量与码长成线性关系。为此,人们设计了采用相似三角形进行编

码的方法。

通过对LDPC码稀疏校验矩阵特点的研究,本文给出了一种新颖的基于两代树结构的低密度校验矩阵构造搜索算法。两代树结构^[7-8]可以较为合理地表示稀疏校验矩阵中行与列中非零元素的跳转关系。同时,对于使用面向对象编程(Object-Oriented Programming, OOP)技术来说,树型数据结构的处理已经相当为人们熟悉。结合蚁群算法^[9]在路径搜索方面的优势,本文所提出的基于两代树的搜索算法具有算法简单、容易实现的优点。更进一步,如果考虑到非规则码的构造^[10]中外信息的引入,可以很容易地将该算法应用在非规则码的构造中。

1 LDPC码的编译码特点

1.1 校验矩阵

Gallager给出了LDPC码校验矩阵 H 的属性:矩阵 H 的每一行有数量为 ρ 的“1”(行重);每一列有数量为 γ 的“1”(列重);相对于 $J \times n$ 的矩阵 H , ρ 和 γ 远小于 J 和 n ;矩阵 H 中任意两行或两列的元素中同为“1”的个数不大于1。

矩阵 H 的密度 r 定义为矩阵 H 中“1”的数量和整个 H 中的总的条目的比,即: $r = \rho/n = \gamma/J$ 。由于 ρ 和 γ 远小于 J 和 n ,所以称为稀疏矩阵或是低密度的矩阵。如果 $\rho/n = \gamma/J$ 则称为规则LDPC码,否则称为非规则LDPC码。一般来说,

$r < 0.5$ 就可以认为是稀疏矩阵,如果随着矩阵 H 的条目的增加,矩阵 H 的密度 r 不断减小,就称 H 为非常稀疏的。由上所述,一个长度为 n 的 LDPC 码可以表示为: (n, γ, ρ) 。

1.2 线性分组码的向量空间分析

有两个元素 0 和 1 的有限域称为伽罗华域 $GF(2)$ 。设有一个长度为 k 的由 0 和 1 构成的信息序列 $u = \{u_0, u_1, \dots, u_{k-1}\}$, 如果将其通过某种算法映射为长为 $n (n > k)$ 的序列 $c = \{c_0, c_1, \dots, c_{n-1}\}$, 同时满足 $c_k = b_0 c_i + b_1 c_j$ 也属于码字时,称 (n, k) 为线性分组码。可以看到,有限域的性质使得上述条件是能够得到满足的。

向量 $c = \{c_0, c_1, \dots, c_{n-1}\}$ 的全体有 2^n 个,它构成一个 $GF(2)$ 域上的 n 维空间 S 。同时,向量 $u = \{u_0, u_1, \dots, u_{k-1}\}$ 的全体有 2^k 个,它应当是 S 空间的一个 K 维子空间 C 。编码的过程就是将 u 映射到某一个 c 上,即: $c = Tu$, 这里 T 是某种变换,它可以由矩阵 G 表示,得到: $c = uG$, G 称为生成矩阵。这里将 u 写成行向量,则 G 是一个 $k \times n$ 的矩阵。将 G 的每一行写成向量的形式,则这 K 个向量都是 n 维向量。有如下关系:

$$c = u_0 g_0 + u_1 g_1 + \dots + u_{k-1} g_{k-1} = [u_1, u_2, \dots, u_{k-1}] \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{pmatrix}$$

这时, K 个 n 维向量 $\langle g_0, g_1, \dots, g_{k-1} \rangle$ 构成 K 维子空间 C 的一组基。通过初等变换, G 可以变为系统矩阵形式: $G_{k \times n} = [I_{k \times k} | P_{k \times (n-k)}]$, $I_{k \times k}$ 为单位阵, $P_{k \times (n-k)}$ 为校验阵。由系统生成矩阵 G 生成的码字称为系统线性分组码。

对于由 K 个 n 维向量 $\langle g_0, g_1, \dots, g_{k-1} \rangle$ 张成的空间 $C = \text{span}(g_0, g_1, \dots, g_{k-1})$, 我们需要找到它的零空间 C^\perp (这时,零空间 C^\perp 必然是 $n - k$ 维的), 零空间 C^\perp 的 $n - k$ 个线性无关向量组 $\langle h_0, h_1, \dots, h_{(n-k)-1} \rangle$ 构成零空间 C^\perp 的一组基。由零

空间的性质,对于 $\forall c \in C$ 有 $cH^T = 0$, 其中 $H = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{(n-k)-1} \end{bmatrix}$ 就

称为校验矩阵。因为对 C 空间中所有码字都有 $cH^T = 0$, 所以有 $GH^T = 0$ 。

如果已经构造出校验矩阵 H , 通过高斯消去法可以将矩阵 H 变为如下形式: $H = [I | P]$, 则对应的生成矩阵 $G = [P^T | I]$ 。

我们知道,二进制序列的模 2 和、模 2 差、异或这三种运算是等价的。设任意两个码字 $\forall c_i, c_j \in C$, 其汉明距离为 $d(c_i, c_j) = \text{weigh}(c_i - c_j)$, 同时在 $GF(2)$ 域中加法运算封闭, 所以 $c_i - c_j = c_k \in C$, 得到: $d(c_i, c_j) = \text{weigh}(c_k)$ 。如果对该式两边都取最小值, 则可以知道码空间的最小汉明距离等于最小码重, 即: $d_{\min}(c_i, c_j) = w_{\min}(c_k)$ 。

1.3 Tanner 图及置信传播算法

下面考虑一个 $(10, 2, 4)$ 线性分组码的校验矩阵:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}; \rho = 4, \gamma = 2$$

矩阵中每一行代表一个校验方程,一共有 5 个校验方程。在这

个例子中,码 $c = \{c_0, c_1, \dots, c_9\}$, 长度 $n = 10$, 用第一列表示 c_0 这一位在第一个和第二个校验方程中出现, 第二列表示 c_1 这一位在第一个和第三个校验方程中出现。根据 $cH^T = 0$ 可以得到 5 个校验方程:

$$c_0 h_{1,1} + c_1 h_{1,2} + \dots + c_9 h_{1,10} = 0$$

$$c_0 h_{2,1} + c_1 h_{2,2} + \dots + c_9 h_{2,10} = 0$$

$$c_0 h_{3,1} + c_1 h_{3,2} + \dots + c_9 h_{3,10} = 0$$

$$c_0 h_{4,1} + c_1 h_{4,2} + \dots + c_9 h_{4,10} = 0$$

$$c_0 h_{5,1} + c_1 h_{5,2} + \dots + c_9 h_{5,10} = 0$$

c_0, c_1, \dots, c_9 分别称为信息节点,它代表校验矩阵中的一列。校验矩阵的一行称为校验节点(用 f_0, f_1, \dots, f_4 表示)。这样,我们得到 10 个信息节点和 5 个校验节点。根据校验矩阵中“1”的位置关系,可以确定信息节点和校验节点之间的连接关系。如,校验矩阵 H 的第一行第二列为“1”,则 c_1 和 f_0 之间有一条连线。以此类推,得到的有向图称为 Tanner 图。如图 1 所示。

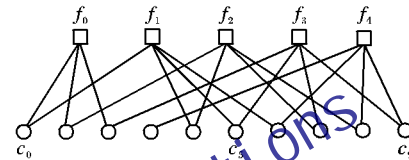


图 1 Tanner 图

在 Tanner 图中,每个节点连接的边的数量称为该节点的度。节点的度是否相同决定是规则码还是非规则码。

Gallager 给出的置信传播译码算法的主要思想是:由于信息位同时出现在若干个校验方程中,所以,如果包含某信息位的几个校验方程不成立(不为零),则修改该信息位,再重新计算所有校验方程;如果这时所有校验方程都成立,则译码结束。否则重复上述步骤,如果迭代次数超过某个规定值,则宣布译码失败。

具体算法包括四个步骤^[4]。

- 1) 初始化:对特定信道预先设置信息位的先验概率。
- 2) 横向步骤:由信息节点的先验概率按置信传播算法得出各校验节点的后验概率。
- 3) 纵向步骤:由校验节点的后验概率推算出信息节点的后验概率。

4) 对信息节点的后验概率做硬判决,将判决结果代入方程 $z = rH^T = (sG + n)H^T = nH^T$ 进行错误图案 z 的检验,如果 $z = 0$ 则译码完毕,否则重复步骤 2) ~ 4); 如果迭代次数超过某个值,则译码失败。

影响 SPA 效果的一个重要因素是周期为 4 的环的存在。

2 校验矩阵和两代树结构

树是我们熟悉的数据结构,基本的树结构由父节点和若干子节点构成。常用的树结构是单亲树,即子节点只有一个父节点。一般来说,树结构中的节点具有邻代同质的特征,也就是说父节点和子节点除了遗传、继承关系外没有其他的差异。如果这种同质的特征只表现在隔代的祖节点和孙节点上,则这样的树结构称为两代树。为了说明这一点请参考图 2 和图 3。

我们可以清楚地地在两代树结构中发现隔代同质的性质。隔代同质的性质可以使我们将两代树结构和校验矩阵(首先我们讨论规则矩阵)中“1”元素的排列关系对应起来。如图 4 所示。如果从 $(1, 1)$ 位置出发,先行转移再列转移,转移时只

转移到“1”元素,那么,可以得到如图5所示的两代树结构。

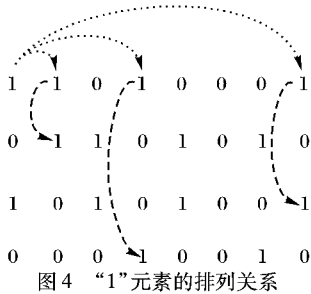
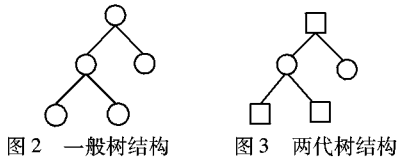


图4 “1”元素的排列关系

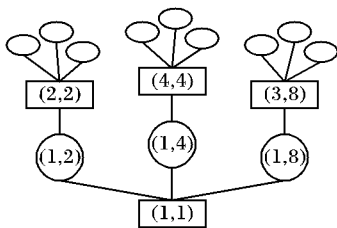


图5 两代树结构

从图4中可以得到几个结论。

结论1 如果对两元组 (a, b) , a 称为行号, b 称为列号, 那么邻代之间行号、列号交替不变。

结论2 引用 Tanner 图中关于节点度的概念, 这里树节点的分支数目也称为度, 则隔代节点的度必然相同。

结论3 相对行号, 列号的最大值, 节点的度很小。

结论4 如果某节点的列号为 b , 其后第三代子节点中也有行号为 b 的子节点, 则该矩阵中必存在周期为4的环。

实际上, 上述四个结论同 Gallager 关于稀疏矩阵的要求是等价的^[1]。四个结论以两代树数据结构为描述的对象。规定了两代树的性质为实现两代树生成算法, 并最终转换为稀疏矩阵提供了基础。

3 两代树结构搜索算法

实现两代树结构搜索算法首先应使算法满足两代树的四个结论, 其次还应补充如下两个结论。

结论5 两代树所表示的稀疏矩阵的最小环周期为非相邻节点之间具有相同行号或列号的节点之间深度差的最小值。

结论6 从 $(1, 1)$ 点出发分别(先生成一棵再生成另一棵)按行、列生成两个深度为环的周期的两代树则可以穷尽稀疏矩阵的所有“1”。

有了上面的六个结论, 算法可以归结为已知树结构(因为首先要确定行重和列重, 这样就确定了两代树节点的度, 而最小环周期决定树的深度), 将两元组 (a, b) 分别填在每个节点上, 在满足一定两元组约束关系的条件下, 即可将两代树转变为低密度校验矩阵 H 。

算法首先需要解决的问题是: 根据结论1, 邻代之间在确定了行号(列号)的情况下如何确定列号(行号)。一个解决办法是随机选择的方式, 但是已经选择的行号或列号不能再选, 因此算法需要实现一定的记忆功能。并且, 对于分支的选择存在随机性, 为此, 仿照蚁群算法^[7]中随机路径选择和信息素释放的处理方法来解决这个问题。得到如图6所示的选

号器结构。

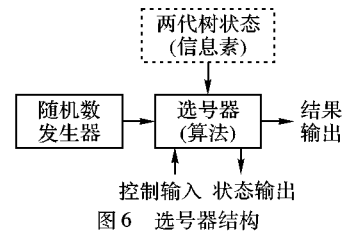


图6 选号器结构

下面给出具体的算法流程。

1) 初始化: 按照所要求的稀疏矩阵的性质(见前述), 生成两个(分别按行、列生成)空的两代树结构 tg_tree1 和 tg_tree2 (行重、列重 ρ 和 γ 、最小周期 p), 根节点两元组设置为 $(1, 1)$, 初始化信息素空间为空。

STAGE1: 生成 tg_tree1 。

2) 向选号器要 $\gamma - 1$ 个数, 以本节点行号及 $\gamma - 1$ 个数构成 $\gamma - 1$ 个两元组赋给下一代节点, 并释放信息素(更新树状态空间结构)。

3) 向选号器要 $\rho - 1$ 个数, 以本节点列号及 $\rho - 1$ 个数构成 $\rho - 1$ 个两元组赋给下一代节点。

4) 重复2) ~ 3), 直到选号器输出异常状态。

异常状态的处理:

异常状态包括以下两种可能: ①选号失败, 无可码资源, 本次搜索失败; ②算法结束, 树生成完毕, 在 STAGE1 的基础上执行 STAGE2。

STAGE2:

5) 向选号器要 $\rho - 1$ 个数, 以本节点列号及 $\rho - 1$ 个数构成 $\rho - 1$ 个两元组赋给下一代节点。

6) 向选号器要 $\gamma - 1$ 个数, 以本节点行号及 $\gamma - 1$ 个数构成 $\gamma - 1$ 个两元组赋给下一代节点, 并释放信息素(更新树状态空间结构)。

7) 重复5) ~ 6), 直到选号器输出异常状态。

异常状态的处理:

异常状态包括以下两种可能: ①选号失败, 无可码资源, 本次搜索失败; ②算法结束, 树生成完毕, 将两棵树转换为稀疏校验矩阵 H 。

需要强调的是: 1) 选号器的输出只有在信息素无法满足请求的情况下才会启动随机数发生器; 2) 选号器输出以信息素提供的号码资源为优先, 也就是说如果在行或列跳转时, 已经存在“1”的位置则直接给出其行或列的数值, 而无需产生随机素。在蚁群算法中, 这相当于本路径已经有先头的兵蚁走过(兵蚁总是按照信息素多的路线走, 而很少自己开辟新的路径)。

4 关于非规则矩阵搜索算法的讨论

非规则 LDPC 码由于其对信道的适应性^[11], 其性能优于规则码。这相当于外信息的引入, 有助于 SPA 中对解码可信程度的提高。

本文所提出的基于两代树的搜索算法很容易移植到非规则码校验矩阵的搜索算法中, 这要求在数据结构和算法上加适当修改: 1) 两代树隔代节点的度不再相等, 但节点度的最大值仍满足结论3; 2) 树的构造采用动态树生成算法, 这一点在 OOP 中更容易实现; 3) 节点度的选择依赖外信息(信道估计给出)。

(下转第988页)

从图8中可以看出,魔方的旋转与还原时间小于椭圆曲线加解密算法,因为魔方算法的旋转主要是对矩阵求转置,而椭圆加密算法利用定义在有限域上的椭圆曲线对信息进行复杂的数学运算,所以魔方算法的执行时间较少。

从图9中可以看出,魔方旋转后的信息量只有少许增加,增加的信息为数字摘要和证书的标志;而椭圆曲线加密后的信息大量增加,数据在复杂的运算后会变大。

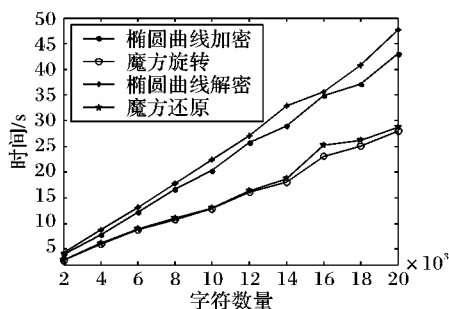


图8 时间消耗比较

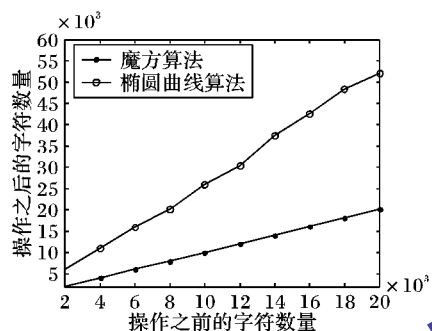


图9 信息传输量比较

4 结语

魔方算法在自动信任协商中,有许多特点:1)传输过程中没有暴露证书与资源的相关信息;2)传输效率高;3)信息传输量小。除了上述特点外,魔方算法还具有以下特征:

1)证书是用角色属性等确立的,建立证书集简单;

2)魔方与证书都只限于一次协商过程,魔方与证书都是临时的,由协商双方集中存放,故没有发现证书的网络开销;

3)将用户请求变成抽象的序列,有利于保护用户请求。

在下一步的工作中,主要是将魔方算法应用到实际的系统中,体现其优势;对魔方算法的证书与魔方颁发进行深入研究,从而设计出更合理的颁发方案。

参考文献:

- [1] 廖振松, 金海, 李赤松, 等. 自动信任协商及其发展趋势[J]. 软件学报, 2006, 17(9): 1933-1948.
- [2] 李建欣, 怀进鹏, 李先贤. 自动信任协商研究[J]. 软件学报, 2006, 17(1): 124-133.
- [3] LI JIANGTAO, LI NINGHUI. OACerts: Oblivious attribute certificates[C]// Proceedings of the Third Conference on Applied Cryptography and Network Security. New York: ACM, 2003. 108-121.
- [4] YU T, WINSLETT M. A unified scheme for resource protection in automated trust negotiation[C]// Proceedings of the 2003 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 2003: 245-257.
- [5] SEAMONS K E, WINSLETT M, YU T. Limiting the disclosure of access control policies during automated trust negotiation[C]// Network and Distributed System Security Symposium. California: IEEE Computer Society, 2001: 212-231.
- [6] WINSBOROUGH W H, LI N H. Towards practical automated trust negotiation[C]// Proceedings of the Third International Workshop on Policies for Distributed Systems and Networks. Washington, DC: IEEE Computer Society, 2002: 92-103.
- [7] FUJIT JIE, BRADSHAW R W, SEAMONS K E, et al. Hidden credentials[C]// 2nd ACM Workshop on Privacy in the Electronic Society. New York: ACM, 2003: 1-8.
- [8] 王继林, 陈晓峰, 陈德人. 无安全信道的 OSBE 方案[J]. 浙江大学学报: 工学版, 2006, 40(4): 590-593.
- [9] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairing, extended abstract[C]// Proceedings of Crypto 2001, LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229.
- [10] 陈涛, 谢阳群. 基于扩展的魔方加密算法的设计与实现[J]. 情报杂志, 2005, 24(2): 13-14, 17.
- [11] 王世卿, 张红艳. 基于数字摘要技术的 IM 系统认证方案[J]. 微机计算机信息, 2009, 25(1-3): 42-43, 70.
- [12] STINSON D R. 密码学原理与实践[M]. 3版. 冯登国, 译. 北京: 电子工业出版社, 2009.

(上接第947页)

5 结语

本文给出了一种新颖的基于两代树的 LDPC 码稀疏校验矩阵 H 的搜索算法,并在对规则码稀疏校验矩阵搜索算法的基础上,讨论了对非规则码应用本算法的可能性和优势。当前的稀疏矩阵构造算法主要分为随机置换方法和数学几何方法两大类。随机置换方法虽然简单,但是可能得到结果不满足条件,而需要重新用算法计算;数学几何方法虽然能够得到确定的结果,在理论上有支持,但算法往往不容易实现。相对于当前的稀疏矩阵构造算法,本文算法具有算法简单、利于计算机实现的优点,而且能够得到确定的结果。

参考文献:

- [1] GALLAGER R G. Low density parity-check codes [EB/OL]. [2010-06-12]. <http://www.rle.mit.edu/rgallager/documents/ldpc.pdf>.
- [2] EROZ M, SUN F-W, LEE L-N. An innovative low-density parity-check code design with near Shannon limit performance and simple implementation[J]. IEEE Transactions on Communications, 2006, 54(1): 13-17.
- [3] JIANG Y-B, ASHIKHMIN A, SHARMA N. LDPC codes for flat Rayleigh fading channels with channel side information[J]. IEEE Transactions on Communications, 2008, 56(8): 1207-1213.
- [4] 包晓燕. 低密度校验码的性能分析及量化译码[D]. 西安: 西安电子科技大学, 2006.
- [5] 詹伟, 梁俊杰. 低编码复杂度不规则准循环 LDPC 码的构造方法[J]. 计算机工程与应用, 2010, 46(28): 102-104.
- [6] 李博, 王钢, 杨洪娟, 等. 一种 LDPC 码双向图环路检测新算法[J]. 哈尔滨工业大学学报, 2010, 42(7): 1051-1055.
- [7] 曾蓉, 梁钊. 低密度校验(LDPC)码的构造及编码[J]. 重庆邮电大学学报, 2005, 17(3): 1-4.
- [8] KIENLE F, WEHN N. Low complexity stopping criterion for LDPC code decoders[C]// VTC 2005-Spring: IEEE Proceedings of the 61st Vehicular Technology Conference. Washington, DC: IEEE, 2005, 1: 606-609.
- [9] 韩国军, 刘星成. LDPC 码的信道自适应迭代译码算法[J]. 电路与系统学报, 2010, 15(1): 102-107, 101.
- [10] 陈为刚, 殷柳国, 陆建华. 非规则 LDPC 码译码改进算法及其实现[J]. 清华大学学报: 自然科学版, 2007, 47(4): 555-559.
- [11] 毛倩, 董德存, 曾小清. 一种 AWGN 信道下非规则 LDPC 码的优化方法[J]. 计算机应用, 2010, 30(2): 292-294.