

基于改进型LBP译码的LDPC码稀疏校验矩阵重建

张天骐, 李春运, 吴仙越, 吴云戈

(重庆邮电大学通信与信息工程学院, 重庆 400065)

摘要: 针对LDPC码稀疏校验矩阵重建问题, 基于改进型LBP译码的思想提出了一种高误码率下的LDPC码稀疏校验矩阵重建算法。首先, 从码字矩阵中随机抽取部分比特构建码字分析矩阵, 并对其做高斯消元求对偶空间; 其次, 通过判定对偶空间向量是否稀疏, 提高了后续疑似校验向量判定的效率; 最后, 在接收码字个数不足时, 利用已知校验向量结合改进型LBP译码方法纠正错误码字, 加快LDPC码稀疏校验矩阵的重建速度, 提高重建性能。仿真结果表明, 所提算法在高误码率0.004 5的条件下, 对于IEEE 802.11n协议下的(648,324)LDPC码, 相比于现有算法, 稀疏校验矩阵重建率提升了52.16%, 可达到92.28%。

关键词: 低密度奇偶校验码; 稀疏校验矩阵; 高斯消元; 改进型LBP译码; 重建

中图分类号: TN92

文献标志码: A

DOI: 10.11959/j.issn.1000-436x.2024097

Reconstruction of LDPC code sparse check matrix based on modified LBP decoding

ZHANG Tianqi, LI Chunyun, WU Xianyue, WU Yunge

School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: In order to reconstruct the sparse check matrix of LDPC code, a sparse check matrix reconstruction algorithm for LDPC code at high BER was proposed based on modified LBP decoding. Firstly, some bits were selected randomly from the codeword matrix to construct the codeword analysis matrix, and Gaussian elimination on it was performed to find the dual space. Secondly, by determining whether the pairwise space vectors were sparse or not, it improved the efficiency of the subsequent suspected check vectors determination. Finally, in the case of insufficient received codes, the known check vectors were combined with the modified LBP decoding method to correct the wrong codes, so as to speed up the reconstruction of the sparse check matrix of LDPC code and improve the reconstruction performance. The simulation results show that the reconstruction rate of sparse check matrix of (648,324) LDPC codes in IEEE 802.11n protocol is improved by 52.16% compared with the existing algorithms, and can reach 92.28% at high BER of 0.004 5.

Keywords: LDPC, sparse check matrix, Gaussian elimination, modified LBP decoding, reconstruction

0 引言

近年来, 信道编码参数识别问题已成为研究热点。在非合作通信领域, 参数识别主要是分析截获的编码序列, 利用码字比特之间的约束关系确定编

码方式和相关参数。目前, 相关研究主要集中于分组码^[1-3]、循环码^[4-6]、卷积码^[7-9]和Turbo码^[10-11]等, 而对于低密度奇偶校验(LDPC, low-density parity-check)码^[12-14]的参数识别研究较少。

收稿日期: 2023-12-29; 修回日期: 2024-04-23

通信作者: 李春运, 1874791327@qq.com

基金项目: 重庆市自然科学基金资助项目(No.cstc2021jcyj-msxmX0836)

Foundation Item: The Natural Science Foundation of Chongqing (No.cstc2021jcyj-msxmX0836)

LDPC码是一种特殊的分组码,由于具有码长较长、校验矩阵稀疏等特点,通过传统识别算法进行参数识别会导致计算复杂度较高,难以达到预期效果。特别地,LDPC码稀疏校验矩阵重建问题一直是一个难点。为了提升后续信息破译的效率,进一步提升重建算法的容错性能具有重要的理论价值和实际意义。

公开文献中,LDPC码参数识别主要分为闭集识别和开集识别。其中,闭集识别已经取得了较多研究成果,但该识别方式需要在部分先验信息已知的情况下进行,不是真正意义上的盲识别;开集识别虽然不需要任何先验信息支持,但现有研究成果较少,且算法性能不太理想。在闭集识别研究中,文献[15]引入对数似然比(LLR, log-likelihood ratio),分别计算闭集中校验矩阵对应的LLR值,并将LLR值最大时的稀疏校验矩阵作为识别结果。但在计算LLR时进行了近似处理,会影响结果的准确性,导致算法性能变差。文献[16]提出了基于余弦符合度的识别方法,该方法将软信息的校验约束关系应用于余弦变换,降低了计算复杂度,且性能明显优于基于LLR的算法。文献[17]通过分析余弦检验函数在校验矩阵正确与错误情况下的统计特性,识别出余弦比最大值对应的校验矩阵,有效增强了识别效果。在开集识别研究中,文献[18-19]利用高斯消元法处理码字矩阵得到非稀疏校验向量,同时利用校验向量剔除含错码字,然后利用 P 阶行消元对非稀疏矩阵进行稀疏化,进而完成稀疏校验矩阵的重建。该算法对双对角线形式的矩阵具有较强实用性,但如果应用于非双对角线形式的矩阵,计算复杂度会大幅增加。文献[20]提出了基于Canteaut-Chabaud^[21]算法的随机稀疏化方法,该方法具有较好的通用性,应用于非双对角形式的矩阵也能表现出优异性能,但稀疏化过程具有一定的盲目性,导致算法复杂度较高。文献[22]利用稀疏化处理后的校验向量对LDPC译码纠错,改善了码字质量,有效提升了算法的重建性能,但是高斯消元和稀疏化过程需要大量的计算资源,导致算法计算复杂度较高。文献[23]利用对偶空间算法获取非稀疏校验向量,并用稀疏化后的校验向量对LDPC码进行软判决迭代译码,进一步提升了算法的容错性能,但在较高误码率的情况下难以获取非稀疏校验向量,且算法仍无法避免稀疏化过程,导致计算复

杂度较高。为避免稀疏化过程导致计算复杂度较高的问题,文献[24]通过随机抽取方法降低了码字空间维度,利用高斯消元可直接获取稀疏校验向量,有效解决了稀疏化引起的计算复杂度较高的问题,但在高误码率或接收码字数不足的情况下,重建性能仍有待提升。文献[25]在随机抽取的基础上,根据码字数是否充足,提出了剔除错误码字和翻转最低不可靠位相结合的算法,进一步提升了算法的容错性能,但在较高误码率情况下,需要多次迭代,逐一翻转最低不可靠位,收敛速度较慢,导致计算复杂度较高。以上开集识别算法在高误码率下的重建性能和重建速度均有待提升。

为解决上述问题,重建LDPC码稀疏校验矩阵,本文提出了一种高误码率下的LDPC码稀疏校验矩阵重建算法。该算法首先利用随机抽取和高斯消元法获取码字的对偶空间。其次,在稀疏对偶空间为非零空间时,进行疑似校验向量的判定,能够有效避免由于出现大量非稀疏对偶空间向量,而需要不断重新进行随机抽取、高斯消元和校验关系判定等操作,提高了疑似校验向量判定的效率。最后,在码字数充足时,利用已获取的稀疏校验向量将不满足校验关系的错误码字剔除;在码字数不足时,利用已获取的稀疏校验向量集合结合改进型分层置信传播(LBP, layered belief propagation)译码^[26]方法纠正错误码字,从而改善码字质量,加快稀疏校验矩阵的重建速度。

1 问题描述

在非合作通信中,LDPC开集识别问题主要集中在码长、码率和码字起点的识别,以及稀疏校验矩阵重建等。其中,根据截获码字实现LDPC码稀疏校验矩阵重建是本文的研究重点。

本文主要研究二进制 (n, k) LDPC码, n 为码长, k 为信息位长度。假设 \mathbf{h}_j 为LDPC码稀疏校验矩阵 \mathbf{H} 的第 j 行稀疏校验向量,则码字 \mathbf{c}_i 满足校验关系

$$\mathbf{c}_i \mathbf{h}_j^T = 0 \quad (1)$$

对码字序列进行二进制相移键控(BPSK, binary phase shift keying)调制,将1映射为-1,0映射为+1,并经过均值为0、方差为 σ^2 的加性白高斯噪声(AWGN, additive white Gaussian noise)信道,可得软判决码字序列 $\mathbf{r}_i = (r_{i,1}, r_{i,2}, \dots, r_{i,n})$,即

$$r_{ij} = 1 - 2c_{ij} + n_{ij} \quad (2)$$

进一步,对序列 \mathbf{r}_i 进行硬判决,可得码字序列

$\mathbf{u}_i = (u_{i,1}, u_{i,2}, \dots, u_{i,n})$ 。

现有研究中, LDPC 码稀疏校验矩阵重建算法均基于码字与校验矩阵之间的校验约束关系。校验向量稀疏是指其汉明重量远小于码长 n 。设 $\text{wt}(\mathbf{h}_j)$ 表示第 j 行校验向量 \mathbf{h}_j 的汉明重量, 若 $\frac{\text{wt}(\mathbf{h}_j)}{n} \leq 0.03$, 则判定 \mathbf{h}_j 为稀疏校验向量。其中, 校验向量获取方法介绍如下。

假设接收的码字序列为 $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_N)$, N 为其中包含的码字个数, 随机抽取 n 个码字排成 n 阶码字矩阵 $\mathbf{U}_{n \times n}$, 即

$$\mathbf{U}_{n \times n} = \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,n} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n,1} & u_{n,2} & \cdots & u_{n,n} \end{bmatrix} \quad (3)$$

其中, u_{ij} 为矩阵 $\mathbf{U}_{n \times n}$ 中的码字比特。对码字矩阵进行高斯消元, 可得

$$\mathbf{L} = \mathbf{R}_{n \times n} \mathbf{U}_{n \times n} = \begin{bmatrix} \mathbf{I}_{k' \times k'} & \mathbf{P}_{k' \times (n-k')} \\ \mathbf{0}_{(n-k') \times k'} & \mathbf{Q}_{(n-k') \times (n-k')} \end{bmatrix} \quad (4)$$

其中, $\mathbf{R}_{n \times n}$ 为初等行变换矩阵, $\mathbf{I}_{k' \times k'}$ 为 $k' \times k'$ 单位矩阵, $\mathbf{0}_{(n-k') \times k'}$ 为 $(n-k') \times k'$ 维全零矩阵。在无误码条件下, 式(4)中 $k' = k$ 且 $\mathbf{Q}_{(n-k') \times (n-k')}$ 为全

零矩阵, $\begin{bmatrix} \mathbf{P}_{k' \times (n-k')} \\ \mathbf{I}_{(n-k') \times (n-k')} \end{bmatrix}$ 中所有向量均为校验向量;

若存在误码, 则部分线性关系被破坏, 此时 $k' > k$

且 $\mathbf{Q}_{(n-k') \times (n-k')}$ 为稀疏矩阵, $\begin{bmatrix} \mathbf{P}_{k' \times (n-k')} \\ \mathbf{I}_{(n-k') \times (n-k')} \end{bmatrix}$ 中只有

部分向量为校验向量; 极端情况下, $k' = n$, \mathbf{L} 为行满秩矩阵, 无法获取校验向量。

文献[24]算法通过从码字矩阵中随机抽取部分码字比特, 降低码字空间维度, 并利用高斯消元法处理码字空间, 直接获取稀疏校验向量。但当误码率较高时, 高斯消元会导致误码扩散, 如果不改善码字质量, 将会导致算法失效, 无法获取校验向量。

为解决上述问题, 文献[25]提出了剔除错误码字和翻转最低不可靠位相结合的重建算法。该算法能够有效提高码字中无误码码组的比例, 但翻转最低不可靠位每次只能修改一个错误比特, 收敛速度较慢。当误码率较高时, 每个错误码字中包含的错误比特较多, 若不能快速降低错误比例, 则每次抽取到错误比特的概率依然较高, 导致高斯消元无法获取新增校验向量。因此, 在码字个数不足时, 可

使用改进型 LBP 译码方法纠正错误码字, 从而快速改善码字质量, 加快算法的重建速度。

2 LDPC 稀疏校验矩阵重建算法

针对上述问题, 本文提出了一种能够重建 LDPC 码稀疏校验矩阵的算法。当稀疏对偶空间为非零空间时, 对疑似校验向量进行判定, 从而提高稀疏校验向量获取的有效性。在码字个数充足时, 利用已获取的稀疏校验向量将不满足校验关系的错误码字剔除; 在码字个数不足时, 利用已获取的稀疏校验向量集合对码字进行软判决译码, 并纠正错误码字, 从而快速改善码字质量, 以期在后续迭代中获取更多校验向量。

2.1 稀疏校验向量获取

校验矩阵 \mathbf{H} 的每一行对应一个校验方程 $\mathbf{c}_i \mathbf{h}_j^T = 0$, 因此获取稀疏校验向量的实质就是求解线性方程组的过程。在随机抽取的过程中, 校验比特的位置未知, 一次随机抽取无法包含所有校验比特, 故需要反复进行多次随机抽取。假设某一稀疏校验向量为 \mathbf{h}' , 其非零元素个数为 wt (一般不超过 10), 随机抽取的码字比特个数为 s , 则抽取的样本集合中包含的元素个数为 C_n^s , 而随机抽取的比特中有 wt 个是校验比特的情况共有 $C_{n-\text{wt}}^s$ 种, 则该校验向量中所有校验比特在一次随机抽取中都被抽到的概率为

$$P_2 = \frac{C_{n-\text{wt}}^s}{C_n^s} = \prod_{i=0}^{\text{wt}-1} \frac{s-i}{n-i} \quad (5)$$

由式(5)可知, 随机抽取比特个数 s 越大, P_2 越大, 得到校验向量就越容易, 但同时也会增大对偶空间的维度, 不利于稀疏向量的获取。极端情况下, $s = n$, 算法将无法直接获取稀疏形式的校验向量, 因此 s 的取值不宜过大。为兼顾对偶空间维度和 P_2 , 一般根据 LDPC 码率来选择, 设码率为 R , 则每次抽取比特个数 $s = nR$ 。接下来, 讨论最小随机抽取次数的确定问题。

假设随机抽取次数为 iter_{col} , 则在 iter_{col} 次随机抽取中, 包含所有校验比特的次数 Z 服从二项分布

$$Z \sim B(\text{iter}_{\text{col}}, P_2) \quad (6)$$

当随机抽取次数较大时, 由康莫弗-拉普拉斯定理可得

$$\frac{Z - \text{iter}_{\text{col}} P_2}{\sqrt{\text{iter}_{\text{col}} P_2 (1 - P_2)}} \sim N(0, 1) \quad (7)$$

若某事件发生的概率超过99.75%，则认为是一大概率事件。要保证至少有一次随机抽取的比特中包含所有校验比特， iter_{col} 应满足

$$P\left[\frac{Z-1}{\sqrt{\text{iter}_{\text{col}}P_2(1-P_2)}} \geq 0\right] \geq 0.9975 \quad (8)$$

求解式(8)可得最小随机抽取次数为

$$(\text{iter}_{\text{col}})_{\min} = \frac{P_1 + \sqrt{P_1^2 - 4}}{2P_2} \quad (9)$$

$$P_1 = 2 + 2.81^2(1 - P_2) \quad (10)$$

基于高斯消元的校验向量重建算法的具体步骤如算法1所示。

算法1 基于高斯消元的校验向量重建算法

初始化参数 $s = nR$ ，迭代消元次数 iter_{row} ，重建的稀疏校验矩阵 \mathbf{H}_{res} ，设 $i_1 = 0$ 。

1) 将截获的LDPC硬判决码字序列 $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_N)$ 构造成硬判决码字矩阵 $\mathbf{U}_{N \times n}$ ，其中 N 为码字个数。

2) 从 $\mathbf{U}_{N \times n}$ 中随机抽取 s 列数据，构成新的码字矩阵 $\mathbf{U}'_{N \times s}$ 。

3) 从 $\mathbf{U}'_{N \times s}$ 中随机抽取 s 行数据，构成方阵 $\mathbf{V}_{s \times s}$ ，对 $\mathbf{V}_{s \times s}$ 做高斯消元将其转换为式(4)形式，并得出其对偶空间基向量。若对偶空间为非零空间，则转至步骤4)；否则， $i_1 = i_1 + 1$ ，重复步骤3)，直到 $i_1 > \text{iter}_{\text{row}}$ 。

4) 根据对偶空间基向量遍历整个解空间，计算解空间向量的码重与LDPC码长的比值 $\frac{\text{wt}(\mathbf{h}')}{n}$ ，寻找稀疏向量，构成稀疏对偶空间。若稀疏对偶空间为非零空间，则转至步骤5)；否则， $i_1 = i_1 + 1$ ，转至步骤3)，直到 $i_1 > \text{iter}_{\text{row}}$ 。

5) 计算稀疏对偶空间中所有向量 \mathbf{h}' 对应的统计量 t (通过校验关系的码字数和不通过个数之差) 和判决门限 T ，若 $t \geq T$ 且 \mathbf{h}' 与 \mathbf{H}_{res} 中所有向量之间线性不相关，则将该稀疏向量保存到稀疏校验矩阵 \mathbf{H}_{res} 。

6) 若 \mathbf{H}_{res} 中有新增校验向量或 $i_1 > \text{iter}_{\text{row}}$ ，则结束运算，输出 \mathbf{H}_{res} ；否则， $i_1 = i_1 + 1$ ，返回步骤3)。

步骤4)中，在获取对偶空间后没有直接进行校验向量判定，而是先对解空间向量进行稀疏性判定，能够进一步保证算法获取的校验向量具有稀疏

性质，提高疑似校验向量判定的效率。

考虑2种假设条件： H_0 表示向量 \mathbf{h}' 不是校验向量； H_1 表示向量 \mathbf{h}' 是校验向量。若信道误码率为 p_e ，向量 \mathbf{h}' 的码重为 $\text{wt}_{\mathbf{h}'}$ ，则在 H_0 下，码字校验关系成立的概率随机，即 $P_{H_0} = 0.5$ ；在 H_1 下，校验关系仍成立的概率为

$$P_{H_1} = \sum_{i=0}^{\lfloor \frac{\text{wt}_{\mathbf{h}'}}{2} \rfloor} C_{\text{wt}_{\mathbf{h}'}}^{2i} p_e^{2i} (1-p_e)^{\text{wt}_{\mathbf{h}'}-2i} \quad (11)$$

在 H_0 下，统计量 t 服从均值 $\mu_0 = 0$ 、方差 $\sigma_0^2 = N$ 的正态分布；在 H_1 下，统计量 t 服从均值 $\mu_1 = N(2P_{H_1} - 1)$ 、方差 $\sigma_1^2 = 4NP_{H_1}(1 - P_{H_1})$ 的正态分布，通过计算可得最小错误判决门限 T 为

$$T \approx \frac{\mu_0\sigma_1 + \mu_1\sigma_0}{\sigma_0 + \sigma_1} \quad (12)$$

2.2 改进型LBP译码

在误码率较高的情况下，对随机抽取算法构造的新码字矩阵做高斯消元会引起严重的误码扩散，导致算法失效，无法获取校验向量，故需要在迭代过程中改善码字质量。在接收码字数充足 ($N > n$) 的条件下，只需要利用剔除错误码字的方法将不满足校验关系的含错码组剔除即可。而在接收码字数不足 ($N \leq n$) 时，使用剔除错误码字会导致数据量降低，无法再利用高斯消元法求对偶空间。因此，在码字数不足时，采用下面介绍的改进型LBP译码方法纠正错误码字。

若信号接收端得到的软判决码字序列为 $\mathbf{r}_i = (r_{i,1}, r_{i,2}, \dots, r_{i,n})$ ，在噪声功率为 σ^2 的AWGN信道条件下，其对应的LLR为

$$L(c_{i,j}|r_{i,j}) = \ln \frac{P_r(c_{i,j} = 0|r_{i,j})}{P_r(c_{i,j} = 1|r_{i,j})} \quad (13)$$

后验概率 $P_r(c_{i,j} = 0|r_{i,j})$ 和 $P_r(c_{i,j} = 1|r_{i,j})$ 的表达式分别为

$$P_r(c_{i,j} = 0|r_{i,j}) = \frac{1}{1 + e^{\frac{2r_{i,j}}{\sigma^2}}} \quad (14)$$

$$P_r(c_{i,j} = 1|r_{i,j}) = \frac{1}{1 + e^{-\frac{2r_{i,j}}{\sigma^2}}} \quad (15)$$

将式(14)和式(15)代入式(13)可得

$$L(c_{i,j}|r_{i,j}) = \frac{2r_{i,j}}{\sigma^2} \quad (16)$$

假设已获取的 LDPC 稀疏校验向量集合为 \mathbf{H}_{res} , 译码输出结果为 $\hat{\mathbf{c}}_l = (\hat{c}_{i,1}, \hat{c}_{i,2}, \dots, \hat{c}_{i,m})$, 当前迭代次数为 l 。用 F_u 表示变量节点 u 的后验概率信息, $F_{u,v}^{(l)}$ 表示第 l 次迭代过程中由变量节点 u 传递给校验节点 v 的信息, $G_{v,u}^{(l)}$ 表示由校验节点 v 传递给变量节点 u 的信息, $d(u)$ 表示与节点 u 相邻的校验节点集合, $d(u) \setminus v$ 表示除 v 外与 u 相邻的校验节点集合, $d(v)$ 表示与节点 v 相邻的变量节点集合, $d(v) \setminus u$ 表示除 u 外与 v 相邻的变量节点集合, 则改进型 LBP 译码算法如算法 2 所示。

算法 2 改进型 LBP 译码算法

初始化变量节点信息 $F_u^{(0)} = L(c_{i,j} | r_{i,j}) = \frac{2r_{i,j}}{\sigma^2}$,

校验节点传递给变量节点的信息 $G_{v,u}^{(0)} = 0$, 最大迭代次数 iter_{max} , $i_2 = 0$ 。

1) 计算变量节点传递给校验节点的信息 $F_{u,v}^{(l)} = F_u^{(l-1)} - G_{v,u}^{(l-1)}$ 。

2) 计算校验节点传递给变量节点的信息 $G_{v,u}^{(l)} =$

$$\prod_{k \in d(v) \setminus u} \text{sign}(F_{k,v}^{(l)}) \min_{k \in d(v) \setminus u} (|F_{k,v}^{(l)}|) \alpha。$$

3) 计算变量节点后验概率信息 $F_u^{(l)} = F_{u,v}^{(l)} + G_{v,u}^{(l)}$, 若 $F_u^{(l)} < 0$, 则 $\hat{c}_{i,j} = 1$; 否则 $\hat{c}_{i,j} = 0$ 。

4) 若 $\mathbf{H}_{\text{res}} \hat{\mathbf{c}}^T = 0$ 或 $i_2 > \text{iter}_{\text{max}}$, 则结束运算, 输出译码结果; 否则, $i_2 = i_2 + 1$, 转至步骤 1) 继续进行译码。

由于近似计算会导致校验节点公式的幅度变大, 步骤 2) 中引入了参数校正因子 $\alpha \in (0,1)$ (本文中设置 $\alpha = 0.75$), 能够平衡近似计算造成的性能损失。

通过上述改进型 LBP 译码算法, 可以在码字数不足的情况下, 同时对多个错误比特进行纠正, 加快码字质量改善的速度, 从而加快稀疏校验矩阵的重建速度。

2.3 LDPC 稀疏校验矩阵重建

本文算法首先利用随机抽取和高斯消元法获取稀疏校验向量, 然后利用剔除错误码字和改进型 LBP 译码方法纠正错误码字, 加快算法重建速度。LDPC 稀疏校验矩阵重建算法如算法 3 所示。

算法 3 LDPC 稀疏校验矩阵重建算法

初始化 $i_3 = 0$ 。

1) 将接收的软判决序列 $\mathbf{r} = (r_1, r_2, \dots, r_N)$ 构成软判决码字矩阵 $\mathbf{R}_{N \times n}$ 。

2) 计算最小随机抽取次数 $(\text{iter}_{\text{col}})_{\text{min}}$ 。

3) 使用算法 1 处理接收的 LDPC 硬判决码字序列, 获取稀疏校验矩阵 \mathbf{H}_{res} , 同时 $i_3 = i_3 + 1$ 。

4) 若 \mathbf{H}_{res} 中有新增校验向量 \mathbf{h}' , 则利用 \mathbf{h}' 获取原始硬判决码字矩阵中错误码字索引, 否则重复步骤 3), 直到 $i_3 > (\text{iter}_{\text{col}})_{\text{min}}$ 。

5) 判断码字数是否充足, 若 $N > n$, 转至步骤 6); 否则转至步骤 7)。

6) 根据错误码字索引, 剔除硬判决码字矩阵中的错误码字, 并更新对应的软判决码字矩阵。

7) 使用 \mathbf{H}_{res} 和算法 2 对错误码字对应的软判决序列进行译码, 并根据译码结果纠正错误码字, 更新码字矩阵。

8) 若 $i_3 > (\text{iter}_{\text{col}})_{\text{min}}$ 或 \mathbf{H}_{res} 的维度为 $n-k$, 则输出稀疏校验矩阵 \mathbf{H}_{res} , 否则返回步骤 3), 直到 $i_3 > (\text{iter}_{\text{col}})_{\text{min}}$ 。

2.4 算法复杂度分析

文献[25]在每次迭代中利用已得到的校验向量改善码字质量, 加快了算法迭代收敛速度。不妨设随机抽取的码字比特个数为 s , 随机抽取次数为 iter_{col} , 迭代消元次数为 iter_{row} , 则文献[25]在极端情况下的最大计算量为 $O(\text{iter}_{\text{col}} \text{iter}_{\text{row}} s^3)$ 。

本文算法在文献[25]的基础上, 在获取校验向量时, 通过判定对偶空间向量是否稀疏, 降低了后续疑似校验向量判定的次数。在码字数不足时, 改进型 LBP 译码方法能更快改善码字质量, 从而加快迭代收敛速度, 故在任何情况下, 本文算法的迭代次数都不大于文献[25]算法。若译码迭代次数为 iter_{max} (本文中设置 $\text{iter}_{\text{max}} = 5$), 所用校验向量集合有 M 个元素, 则在每次迭代中其计算复杂度为 $O(\text{iter}_{\text{max}} M)$, 远小于迭代中高斯消元的计算复杂度为 $O(s^3)$, 可忽略不计。故本文算法复杂度在任何情况下均不大于文献[25]算法。

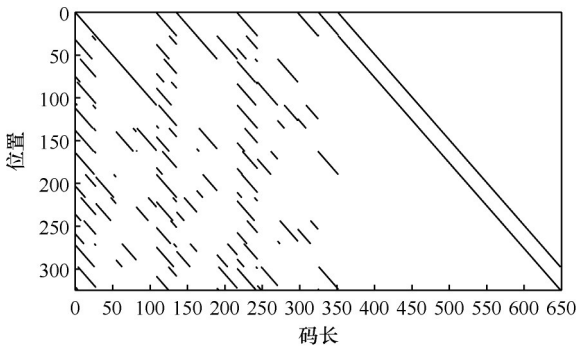
3 仿真实验及性能分析

本节仿真实验以 IEEE 802.11n 协议下 LDPC 码为例, 首先验证本文算法对稀疏校验矩阵的重建效果, 其次分别在不同迭代消元次数、不同码长、不同码率、不同截获码字数、不同抽取次数情况下, 与现有算法重建性能进行对比。为了区别

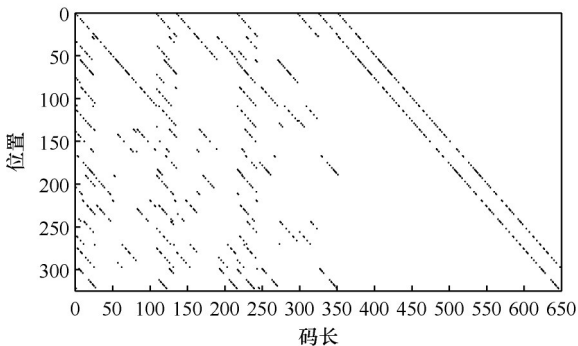
于本文算法, 根据文献[24]和文献[25]算法的特点, 将其分别命名为随机抽取算法和比特翻转算法。

3.1 算法重建性能验证

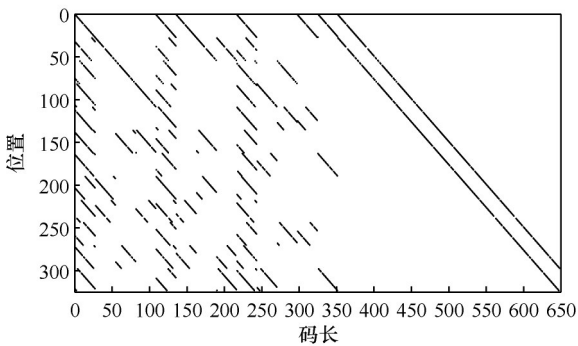
本实验采用 IEEE 802.11n 协议中码长为 648、码率为 $\frac{1}{2}$ 的 LDPC 码, 假设截获的码字个数为 3 000, 误码率为 0.004 5, 校验向量最大码重为 10, 迭代消元次数为 20 次, 分别用比特翻转算法和本文算法进行稀疏校验矩阵重建, 重建结果(重新排列后)如图 1 所示。



(a) IEEE802.11n协议下定义的(648,324)LDPC码稀疏校验矩阵



(b) 比特翻转算法的重建结果(重新排列后)



(c) 本文算法的重建结果(重新排列后)

图1 本文算法与比特翻转算法的重建结果

观察图 1(b)可得, 比特翻转算法在误码率为 0.004 5 时, 重建的稀疏校验矩阵中包含 130 个校验

向量, 重建率为 40.12%。由图 1(c)可知, 本文算法重建的稀疏校验矩阵中包含 299 个校验向量, 重建率为 92.28%, 更接近图 1(a)所示的真实稀疏校验矩阵。由此可得, 本文算法在较高误码率条件下能够更好地实现 LDPC 码稀疏校验矩阵重建。

3.2 不同迭代消元次数下性能对比

本实验采用 IEEE 802.11n 协议中码长为 648、码率为 $\frac{1}{2}$ 的 LDPC 码, 假设截获的码字个数为 3 000, 误码率取值范围为 0.000 5~0.006 5, 校验向量最大码重为 10, 迭代消元次数分别为 5、10、20 次。定义重建率为重建的稀疏校验向量个数与真实稀疏校验矩阵的秩之比。图 2 为本文算法与比特翻转算法在不同误码率和迭代消元次数下的稀疏校验矩阵重建率。

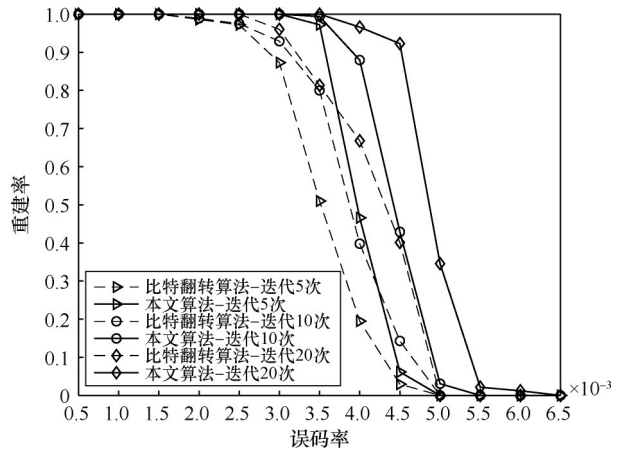


图2 本文算法与比特翻转算法在不同误码率和迭代消元次数下的稀疏校验矩阵重建率

由图 2 可得, 随着迭代消元次数的增加, 2 种算法的稀疏校验矩阵重建性能均得到有效提升。这主要是因为增加迭代消元次数能抽取到更多具有相同校验关系的码字, 且抽取的码字中无误码比例也会提高, 进而增加了高斯消元获取的稀疏校验向量个数。在不同迭代消元次数下, 本文算法的稀疏校验矩阵重建率均高于比特翻转算法, 且本文算法在误码率为 0.004 5 的条件下, 重建率仍能达到 92.28%, 相比于比特翻转算法, 提升了约 50%。这主要是因为本文算法先判定对偶空间向量是否具有稀疏性质, 再从稀疏对偶空间中筛选和判定疑似校验向量, 避免了出现非稀疏校验向量而导致算法提前终止迭代消元, 无法获取稀疏校验向量的问题。因此, 在相同条件下, 本文算法能获取更多稀疏校验向量。

3.3 不同码长下性能对比

本实验采用 IEEE 802.11n 协议中码率为 $\frac{1}{2}$ 的 LDPC 码，假设截获的码字个数为 3 000，码长分别为 648、1 296、1 944，误码率取值范围为 0.000 5~0.006 5，校验向量最大码重为 10，迭代消元次数为 20 次。图 3 为本文算法与比特翻转算法在不同误码率和码长下的稀疏校验矩阵重建率对比。

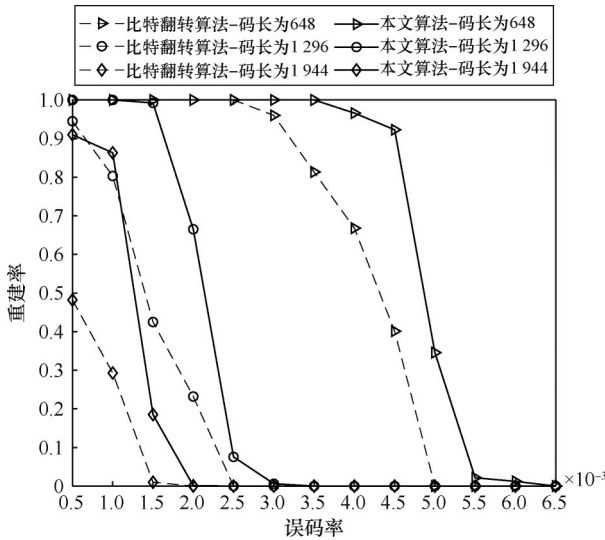


图 3 本文算法与比特翻转算法在不同误码率和码长下的稀疏校验矩阵重建率对比

观察图 3 可知，在误码率相同时，LDPC 码的码长越长，稀疏校验矩阵的重建率越低。这主要是因为码长越长，每次随机抽取的码字比特个数越多，错误码字比特的比例就越高。因此，高斯消元过程中误码扩散现象会加剧，进而导致稀疏校验矩阵的重建率大幅下降。在误码率为 0.001 5 时，对于码长为 1 296、码率为 $\frac{1}{2}$ 的 LDPC 码，本文算法的重建率相比于比特翻转算法提升了约 60%。这主要是因为本文算法在迭代消元过程中能获取更多稀疏校验向量，所以在利用校验向量集合回校码字时，能剔除更多错误码字，加速改善码字质量，从而提高稀疏校验矩阵重建率和重建速度。

3.4 不同码率下性能对比

本实验采用 IEEE 802.11n 协议中码长为 648 的 LDPC 码，假设截获的码字个数为 3 000，码率分别为 $\frac{1}{2}$ 、 $\frac{2}{3}$ 、 $\frac{3}{4}$ ，误码率取值范围为 0.000 5~0.006 5，校验向量最大码重为 10，迭代消元次数为 20 次。

图 4 为本文算法与比特翻转算法在不同误码率和码率下的稀疏校验矩阵重建率对比。

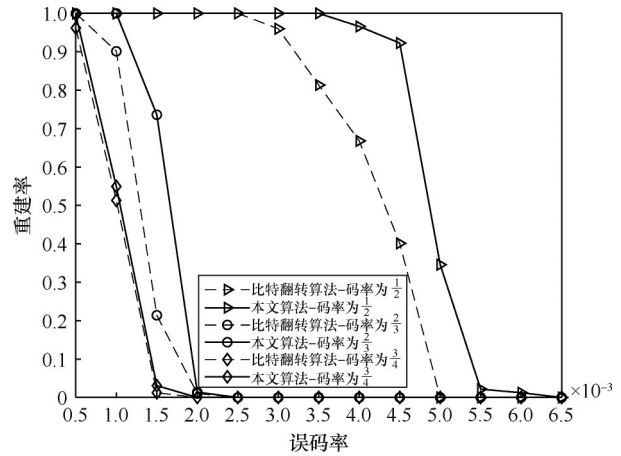


图 4 本文算法与比特翻转算法在不同误码率和码率下的稀疏校验矩阵重建率对比

观察图 4 可知，当误码率相同时，LDPC 码的码率越高，稀疏校验矩阵重建率越低。这是因为升高码率会导致稀疏校验向量的汉明重量增加，随机抽取到校验比特的概率就会降低，进而导致稀疏校验矩阵的重建率降低。在误码率为 0.004 5 的条件下，对于码长为 648、码率为 $\frac{1}{2}$ 的 LDPC 码，本文算法的重建率相比于比特翻转算法提升了约 50%，具有更强的容错性能。这同样是因为本文算法在每次迭代过程中能剔除更多错误码字。但当码率较高时，本文算法在迭代消元过程中同样无法获取较多稀疏校验向量，因此重建性能相对于比特翻转算法提升不明显。

3.5 不同码字个数下性能对比

本实验采用 IEEE 802.11n 协议中码长为 648、码率为 $\frac{1}{2}$ 的 LDPC 码，校验向量最大码重为 10，迭代消元次数为 10 次。在码字个数充足的情况下，设误码率为 0.003 5，截获的码字个数取值范围为 648~1 250，步长为 50，本文算法与比特翻转算法在不同码字个数下的重建率如图 5 所示。

分析图 5 可知，增加码字个数能有效提升 2 种算法的稀疏校验矩阵重建率。这主要是因为随着接收码字的个数增加，具有相同校验关系的码字数量会越来越多，那么随机抽取的码字具有相同校验关系的概率也会增大，利用高斯消元法获取的稀疏校验向量个数就会增加。在误码率为 0.003 5 时，本

文算法的稀疏校验矩阵重建率在不同码字个数下均高于比特翻转算法。这主要是因为本文算法在码字个数充足时,能一次性剔除更多错误码字,且在后续码字个数不足时,改进型 LBP 译码方法能表现出更加优异的纠错性能。

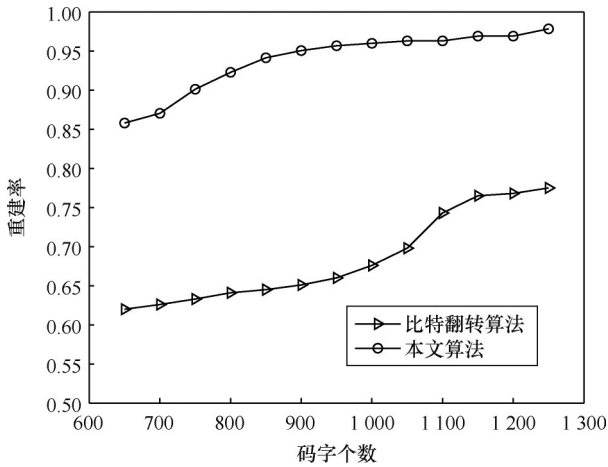


图5 本文算法与比特翻转算法在不同码字个数下的重建率 (码字个数充足)

在码字个数不足的情况下,设误码率为0.002 5,截获的码字个数取值范围为324~648,步长为50,随机抽取算法、比特翻转算法与本文算法在不同码字个数下的稀疏校验矩阵重建率如图6所示。

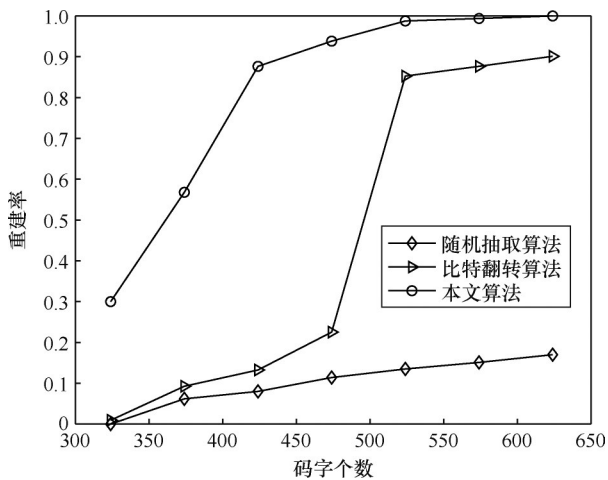


图6 随机抽取算法、比特翻转算法与本文算法在不同码字个数下的稀疏校验矩阵重建率(码字个数不足)

由图6可知,在码字个数不足时,改进型 LBP 译码方法能够有效改善码字质量,提高稀疏校验矩阵的重建率,且相比于翻转最低不可靠位方法能表现出更加优异的纠错性能。当误码率为0.002 5时,本文算法在码字个数严重不足的情况下,稀疏校验

矩阵的重建率仍能达到90%以上。

3.6 不同列抽取次数下性能对比

本实验采用 IEEE 802.11n 协议中的(648,324) LDPC 码,假设截获的码字个数为3 000,迭代消元次数为20次,校验向量最大汉明重量为8,计算可得最小随机抽取次数 $(iter_{col})_{min} = 2\ 611$,实验设置随机抽取次数为 $\frac{4}{7}(iter_{col})_{min} : \frac{(iter_{col})_{min}}{7} : 2(iter_{col})_{min}$ 。当误码率为0.002 8时,随机抽取算法、比特翻转算法与本文算法在不同随机抽取次数下重建的校验向量个数如图7所示。

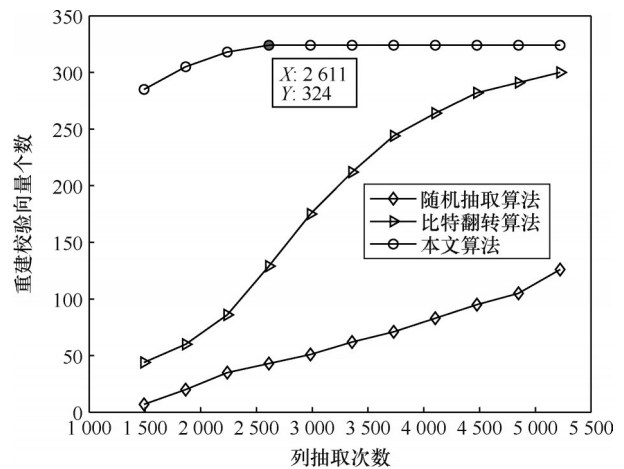


图7 不同列抽取次数下重建校验向量个数对比

观察图7可知,当列抽取次数相同时,随机抽取算法和比特翻转算法重建稀疏校验向量的数量均低于本文算法,且本文算法在列抽取次数为2 611时能够完整重建稀疏校验矩阵。当列抽取次数为理论推导的 $iter_{col} = 2\ 611$ 时,本文算法重建的稀疏校验向量个数较比特翻转算法增加约195个,重建率提升了约60%。这主要是因为本文算法应用的改进型 LBP 译码方法能加快纠正错误码字的速度,从而加快算法收敛速度,降低完成稀疏校验矩阵重建所需的列抽取次数。

4 结束语

本文算法首先利用随机抽取和高斯消元法获取码字的对偶空间,并在稀疏对偶空间中筛选和判决疑似校验向量,提高了获取稀疏校验向量的效率。其次,根据接收码字个数是否充足,采用剔除错误码字和改进型 LBP 译码的方法,改善了码字质量,进而提高了稀疏校验矩阵的重建性能。在高误码率

为 0.004 5 的条件下, 对于 IEEE 802.11n 协议下的 (648,324) LDPC 码, 本文算法的校验矩阵重建率能达到 90% 以上。相比于现有算法, 本文算法的重建速度较快、重建性能较强, 更适用于实际环境。

参考文献:

- [1] 吴昭军, 张立民, 钟兆根, 等. 基于平均余弦符合度下的本原 BCH 码盲识别[J]. 通信学报, 2020, 41(1): 15-24.
WU Z J, ZHANG L M, ZHONG Z G, et al. Blind recognition of primitive BCH code based on average cosine conformity[J]. Journal on Communications, 2020, 41(1): 15-24.
- [2] 王玉龙, 吴迪, 胡涛. 一种同型空时分组码的识别算法[J]. 电子学报, 2022, 50(11): 2754-2764.
WANG Y L, WU D, HU T. An identification algorithm for space-time block codes with the same shape[J]. Acta Electronica Sinica, 2022, 50(11): 2754-2764.
- [3] 尤红雨, 王垚, 王翔, 等. 基于码重奇偶性的扩展 BCH 码盲识别[J]. 系统工程与电子技术, 2024, 46(5): 1783-1791.
YOU H Y, WANG Y, WANG X, et al. Blind identification of extended BCH codes based on parity of code weight[J]. Systems Engineering and Electronics, 2024, 46(5): 1783-1791.
- [4] 吴昭军, 张立民, 钟兆根, 等. 一种软判决下的 RS 码识别算法[J]. 电子与信息学报, 2020, 42(9): 2150-2157.
WU Z J, ZHANG L M, ZHONG Z G, et al. Blind recognition of RS codes based on soft decision[J]. Journal of Electronics & Information Technology, 2020, 42(9): 2150-2157.
- [5] 张晓林, 李修桥, 孙溶辰. 基于快速码根检验的 RS 码综合识别算法[J]. 通信学报, 2022, 43(11): 117-126.
ZHANG X L, LI X Q, SUN R C. Comprehensive recognition algorithm of RS code based on fast code root trial[J]. Journal on Communications, 2022, 43(11): 117-126.
- [6] 张天骐, 王雪怡, 方竹, 等. 基于软判决下的校验关系的循环码参数盲识别[J]. 信号处理, 2023, 39(6): 1120-1130.
ZHANG T Q, WANG X Y, FANG Z, et al. Soft-decision based blind identification of cyclic code parameters with parity-check relation[J]. Journal of Signal Processing, 2023, 39(6): 1120-1130.
- [7] 陈增茂, 陆丽, 孙志国, 等. 基于共轭梯度求解代价函数的卷积码参数识别算法[J]. 系统工程与电子技术, 2022, 44(10): 3235-3242.
CHEN Z M, LU L, SUN Z G, et al. Parameter estimation algorithm of convolutional codes with solving cost function based on conjugate gradient[J]. Systems Engineering and Electronics, 2022, 44(10): 3235-3242.
- [8] 陶志勇, 闫明豪, 刘影. 基于时序卷积网络的信道编码闭集识别[J]. 华中科技大学学报(自然科学版), 2022, 50(3): 12-17.
TAO Z Y, YAN M H, LIU Y. Channel coding closed set recognition based on temporal convolutional network[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2022, 50(3): 12-17.
- [9] 王垚, 满欣, 尤红雨, 等. 矩阵变换特征与码序列联合学习的卷积码识别方法[J]. 国防科技大学学报, 2023, 45(5): 38-47.
WANG Y, MAN X, YOU H Y, et al. Convolutional codes recognition method based on joint learning of matrix transformation features and code sequences[J]. Journal of National University of Defense Technology, 2023, 45(5): 38-47.
- [10] 胡延平, 张天骐, 白杨柳, 等. 删余型 Turbo 码分量编码器盲识别算法[J]. 信号处理, 2021, 37(11): 2207-2215.
HU Y P, ZHANG T Q, BAI Y L, et al. A blind recognition algorithm for the component encoder of punctured turbo code[J]. Journal of Signal Processing, 2021, 37(11): 2207-2215.
- [11] 李卓伦, 韩卓茜. 利用多种纠错方式进行优化的 Turbo 码交织器识别[J]. 电子学报, 2021, 49(2): 239-247.
LI Z L, HAN Z X. An optimization method using multiple error correction for turbo-code interleaver identification[J]. Acta Electronica Sinica, 2021, 49(2): 239-247.
- [12] 刘倩, 张昊, 宋莹炯, 等. 小样本条件下基于矩阵乘法和秩分析的 LDPC 参数估计方法[J]. 电子学报, 2022, 50(5): 1075-1082.
LIU Q, ZHANG H, SONG Y J, et al. LDPC parameter estimation by matrices product and rank analysis under the condition of small sampling[J]. Acta Electronica Sinica, 2022, 50(5): 1075-1082.
- [13] 刘恒燕, 张立民, 闫文君, 等. 基于随机抽取的稀疏校验矩阵重建算法[J]. 系统工程与电子技术, 2023, 45(4): 1215-1221.
LIU H Y, ZHANG L M, YAN W J, et al. Reconstruction algorithm of sparse check matrix based on random extraction[J]. Systems Engineering and Electronics, 2023, 45(4): 1215-1221.
- [14] ZOU L Q, WU H L, LIU R, et al. A new method for LDPC blind recognition over a candidate set using kullback-leibler divergence[J]. IEEE Communications Letters, 2024, PP(99): 1-5.
- [15] XIA T, WU H C. Novel blind identification of LDPC codes using average LLR of syndrome a posteriori probability[C]//Proceedings of the 2012 12th International Conference on ITS Telecommunications. Piscataway: IEEE Press, 2012: 12-16.
- [16] WU Z J, ZHANG L M, ZHONG Z G, et al. Blind recognition of LDPC codes over candidate set[J]. IEEE Communications Letters, 2020, 24(1): 11-14.
- [17] 刘仁鑫, 张立民, 钟兆根, 等. 基于最大余弦比的 LDPC 码闭集识别[J]. 信号处理, 2020, 36(8): 1234-1242.
LIU R X, ZHANG L M, ZHONG Z G, et al. Closed set identification of LDPC codes based on maximum cosine ratio[J]. Journal of Signal Processing, 2020, 36(8): 1234-1242.
- [18] 包昕, 周磊珂, 何可, 等. 误码条件下的 LDPC 码盲识别算法[J]. 西安交通大学学报, 2015, 49(12): 53-58.
BAO X, ZHOU L K, HE K, et al. A recognition algorithm for LDPC codes of blind in a noisy environment[J]. Journal of Xi'an Jiaotong University, 2015, 49(12): 53-58.
- [19] 包昕, 周磊珂, 何可, 等. LDPC 码稀疏校验矩阵的重建方法[J]. 电子科技大学学报, 2016, 45(2): 191-196.
BAO X, ZHOU L K, HE K, et al. A method of restructuring LDPC parity-check matrix[J]. Journal of University of Electronic Science and Technology of China, 2016, 45(2): 191-196.
- [20] 于沛东, 彭华, 巩克现, 等. 基于寻找小重量码字算法的 LDPC 码盲识别[J]. 通信学报, 2017, 38(6): 108-117.
YU P D, PENG H, GONG K X, et al. LDPC code reconstruction based

on algorithm of finding low weight code-words[J]. Journal on Communications, 2017, 38(6): 108-117.

- [21] CANTEAUT A, CHABAUD F. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511[J]. IEEE Transactions on Information Theory, 1998, 44(1): 367-378.
- [22] 陈泽亮, 彭华, 巩克现, 等. 误码条件下LDPC码参数的盲估计[J]. 电子学报, 2018, 46(3): 652-658.
CHEN Z L, PENG H, GONG K X, et al. A method for blind recognition of LDPC codes in a noisy environment[J]. Acta Electronica Sinica, 2018, 46(3): 652-658.
- [23] 钟兆根, 刘仁鑫, 张立民, 等. 基于迭代译码的LDPC码稀疏校验矩阵重建[J]. 北京航空航天大学学报, 2021, 47(12): 2623-2631.
ZHONG Z G, LIU R X, ZHANG L M, et al. Reconstruction of sparse parity-check matrix of LDPC codes based on iterative decoding[J]. Journal of Beijing University of Aeronautics and Astronautics, 2021, 47(12): 2623-2631.
- [24] 吴昭军, 张立民, 钟兆根, 等. 高误码率下LDPC稀疏校验矩阵重建[J]. 通信学报, 2021, 42(3): 1-10.
WU Z J, ZHANG L M, ZHONG Z G, et al. Reconstruction of sparse check matrix for LDPC at high bit error rate[J]. Journal on Communications, 2021, 42(3): 1-10.
- [25] 王忠勇, 李正豪, 巩克现, 等. 高误码率下基于随机抽取的LDPC码校验矩阵重建[J]. 通信学报, 2023, 44(3): 128-137.
WANG Z Y, LI Z H, GONG K X, et al. Reconstruction of LDPC code check matrix based on random extraction at high bit error rate[J]. Journal on Communications, 2023, 44(3): 128-137.
- [26] 刘明山, 王亚忠, 刘珊珊. LDPC码改进型LBP译码算法研究[J]. 吉林大学学报(信息科学版), 2015, 33(4): 367-372.
LIU M S, WANG Y Z, LIU S S. Research on modified LBP decoding algorithm of LDPC codes[J]. Journal of Jilin University (Information Science Edition), 2015, 33(4): 367-372.

[作者简介]



张天骐 (1971-), 男, 四川眉山人, 博士, 重庆邮电大学教授、博士生导师, 主要研究方向为通信信号的调制解调、盲处理、语音信号处理、神经网络实现以及FPGA、VLSL实现。



李春运 (2000-), 男, 河南信阳人, 重庆邮电大学硕士生, 主要研究方向为信道编码参数盲识别。



吴仙越 (2000-), 女, 重庆人, 重庆邮电大学硕士生, 主要研究方向为扩频信号盲估计。



吴云戈 (2000-), 女, 河南许昌人, 重庆邮电大学硕士生, 主要研究方向为通信信号盲处理、深度学习。