低秩循环矩阵的构造方法及其关联的多元LDPC码

徐恒舟[①] 朱 海[*①] 冯 丹[②] 张 博[①] 周慢杰[①]

[①](周口师范学院网络工程学院 周口 466001)

[②](西安邮电大学通信与信息工程学院 西安 710121)

摘 要：在图像处理中，低秩矩阵的冗余信息可用于图像恢复和图像特征提取，而在迭代译码中，校验矩阵的冗余行可以加快译码收敛速度。该文研究一类易于硬件实现的低秩循环矩阵。首先将循环矩阵转换为位置集合，并基于同构理论简化了位置集合的搜索空间，从而基于比特移位方法提出了循环矩阵的构造方法。考虑非零域元素的列赋值与矩阵秩之间的关系，选取Tanner图中没有长度为4的环的循环矩阵，基于非零域元素的列赋值思想提出了不同阶数、不同码率的多元LDPC码构造方法。数值仿真结果表明，与基于PEG算法构造的二元LDPC码比较，所构造的多元LDPC码在BPSK调制方式下在误码字率10^{-5}附近有0.9 dB的增益；在与高阶调制相结合时，有更大的性能提升。此外，所构造的多元LDPC码在迭代5次与50次下的性能几乎一致，这为低时延高可靠通信提供了一种有效的候选编码方案。

关键词：LDPC码；低秩矩阵；循环矩阵；同构理论；围长

中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2021)01-0085-07

DOI: 10.11999/JEIT200351

Construction of Low-rank Circulant Matrices and Their Associated Nonbinary LDPC Codes

XU Hengzhou[①] ZHU Hai[①] FENG Dan[②] ZHANG Bo[①] ZHOU Manjie[①]

[①](*School of Network Engineering, Zhoukou Normal University, Zhoukou* 466001, *China*)

[②](*School of Communications and Information Engineering, Xi'an University of Post and Telecommunications, Xi'an* 710121, *China*)

Abstract: In image processing, the redundant information of low-rank matrices can be used for image recovery and image feature extraction, and redundant rows of the parity-check matrices can accelerate the convergence rate in iterative decoding. A class of low-rank circulant matrices with easy hardware implementation is studied. Circulant matrices are first converted into position sets, the search space of position sets is pruned based on isomorphism theory, and then construction of circulant matrices is proposed based on the bit shift method. Considering the relationship between the column assignment of non-zero field elements and the matrix rank, circulant matrices whose Tanner graphs have no cycles of length 4 are chosen, and according to the column assignment of non-zero field elements, construction of nonbinary LDPC codes over various finite fields and with different code rates is presented. Numerical simulation results show that, compared with binary LDPC codes constructed based on the PEG algorithm, the proposed nonbinary LDPC codes have 0.9 dB gain at Word Error Rate (WER) of 10^{-5} when the modulation is BPSK, and the performance gap becomes large by combining with high order modulations. Furthermore, the performance gap of the proposed codes between 5 iterations and 50 iterations is negligible, and it provides a promising coding scheme for low-latency and high-reliability communications.

收稿日期：2020-05-08；改回日期：2020-10-26；网络出版：2020-11-19

*通信作者： 朱海 zhu_sea@163.com

基金项目：国家自然科学基金(61801527, 11971311)，国家自然科学基金数学天元基金资助项目(12026230, 12026231)，河南省高等学校青年骨干教师培养计划(2018GGJS137)，河南省高等学校重点科研项目(20A510017)，河南省自然科学基金项目(202300410523)，陕西省高校科协青年人才托举计划项目(20200116)，陕西省教育厅科研计划项目(20JK0918)

Foundation Items: The National Natural Science Foundation of China (61801527,11971311), The TianYuan Special Funds of the National Natural Science Foundation of China (12026230, 12026231), The Training Program for Young Core Instructor of Henan Universities (2018GGJS137), The Key Scientific Research Projects of Henan Educational Committee (20A510017), The Natural Science Foundation of Henan (202300410523), The Project of Youth Talent Lift Program of Shaanxi Association for Science and Technology (20200116), The Scientific Research Program Funded by Shaanxi Provincial Education Department (20JK0918)

Key words: LDPC code; Low-rank matrix; Circulant matrix; Isomorphism theory; Girth

1 引言

5G标准化的基础功能阶段已经完成，而标准化的下一阶段主要面向物联网/垂直行业应用场景，提供支撑未来10年信息社会的无线通信传输方案[1]。这里，标准化主要包括两方面：高可靠低时延通信业务(Ultra Reliable &Low Latency Communication, URLLC)和大规模机器通信(massive Machine Type Communication, mMTC)[2]。与5G不同的是，6G的“万物随心”愿景需要同时满足实时性、可靠性、吞吐量和海量连接的需求，这将对新一代无线通信网络提出全新的挑战[1]。本文主要讨论低时延高可靠通信的信道编码技术。这些通信业务主要面向以机器通信为代表的物联网，具有小数据包、低功耗、海量连接、强突发性等特点，需要编译码速度快、抗突发能力强和码长较短的信道编码方案。时延和可靠性指标通常一起考虑，指的是在一定正确传输概率下通信系统的最大传输时延。对信道编码而言，就是要求编译码处理时延较低，并消除译码算法所产生的错误平层。结合软输出迭代译码，LDPC码是一种有竞争力的实用信道编码技术。研究表明[3]，在中短码长下，与相同比特长度下的二元LDPC码相比，多元LDPC码有以下优势：(1)有更多(1～1.3 dB)的编码增益；(2)有更强的抗突发错误能力；(3)更易于与高阶调制相结合。近年来，在迭代译码框架下，多元LDPC码译码复杂度高的问题也得到了有效的解决[4–8]，这为多元LDPC码的应用奠定了坚实的基础。而在迭代译码中，LDPC码校验矩阵的冗余行可以加快译码收敛速度[9]，从而有效地减少译码时延。此外，在图像处理中，自然图像的数据矩阵通常都是低秩或者近似低秩的[10]。也就是说，这些矩阵的每行(或列)均可由其他的行(或列)线性表示，从而包含了大量的冗余信息。基于这些冗余信息可以去除图像的噪声信息，并恢复出正确的图像信息，还可以恢复错误的图像信息[11]。然而，关于低秩矩阵构造的研究相对较少。综上，研究低秩矩阵(或者冗余行较多的矩阵[12])的构造方法是十分有意义的。

循环矩阵具有循环移位性质，很容易基于线性移位寄存器进行硬件实现。因此，本文主要研究低秩循环矩阵的构造方法。这里的循环矩阵指的是一个大小为$L\times L$的方阵，它的每一行是上一行的右(或左)循环移位，第1行是最后一行的右(或左)循环移位；它的每一列是它左边一列的向下(或上)循环移位，第1列是最后一列的向下(或上)循环移位。显然，循环矩阵的行重和列重是相同的。分别基于欧氏几何和Reed–Solomon码，文献[13]给出了这类循环矩阵的构造方法；文献[14]则利用2维的最大距离可分(Maximum Distance Separable, MDS)码构造了一些循环矩阵，但这些代数方法所得到的循环矩阵数量有限。基于循环码和同构理论，文献[15]给出了循环矩阵的计算机穷搜索方法。但是，随着矩阵大小和行(或列)重的增大，搜索空间会急剧增大，寻找和确定不同构类将变得异常困难。此外，文献[16]研究了循环矩阵的秩性质，并基于本原多项式给出了满秩循环矩阵的构造方法。

本文首先利用同构理论降低了循环矩阵的搜索空间，然后利用求秩算法搜索得到不同秩的循环矩阵。与文献[15]不同的是，本文利用计算秩的方式直接寻找不同秩的循环矩阵，而不再寻找并划分循环矩阵的同构类。进一步地，本文研究了循环矩阵Tanner图中长度为4的环(简记为4-环)结构，并提出确定4-环的算法，还给出了非零元赋值方法，从而提出了围长至少为6的多元LDPC码构造方法。数值仿真结果表明，在加性高斯白噪声(Additive White Gaussian Noise, AWGN)信道中，所构造的多元LDPC码有很好的迭代译码性能，并且在迭代5次与50次下的性能曲线几乎重叠。

2 基于同构理论的低秩循环矩阵构造方法

2.1 循环矩阵及其同构理论

这里，将本文考虑的循环矩阵$\boldsymbol{C}=[c_{i,j}]_{L\times L}$记为一个行(或列)重为$m$、大小为$L\times L$的二元矩阵。由于循环矩阵$\boldsymbol{C}$的循环移位特性，我们只需标记循环矩阵$\boldsymbol{C}$的第1行非零元素位置即可。不妨设非零元素位置集合为$S=\{s_1,s_2,\cdots,s_m\}$，其中，对于$1\le i<j\le m, 0\le s_i<s_j\le L-1$。因此，循环矩阵$\boldsymbol{C}$的构造等价于第1行非零元素位置集合$S$的设计。

循环矩阵$\boldsymbol{C}$的Tanner图是一个二部图(bipartite graph)[17]。Tanner图中的节点被划分为两类：变量节点(Variable Node, VN)(或编码比特节点)和校验节点(Check Node, CN)(或约束节点)，分别用VN和CN来表示。Tanner图中的线只连接不同类型的节点。循环矩阵$\boldsymbol{C}$的Tanner图可以这样得到：当$\boldsymbol{C}$中的元素$c_{i,j}$为1时，第i个校验节点(CN i)和第j个变量节点(VN j)相连接；否则它们之间没有线相连。循环矩阵$\boldsymbol{C}$的Tanner图中最短环的长度称为围长(girth)。如果两个循环矩阵的Tanner图是同构的，则称这两个循环矩阵也是同构的。根据文献[15]

中的定理2，下面不加证明地给出循环矩阵的同构定理。

定理1(循环矩阵的同构理论)：令$\boldsymbol{C}_1$和$\boldsymbol{C}_2$为两个行(或列)重为m、大小为$L\times L$的二元循环矩阵，它们的第1行非零位置集合分别记为$S_1=\{s_{1,1},s_{1,2},\cdots,s_{1,m}\}$和$S_2=\{s_{2,1},s_{2,2},\cdots,s_{2,m}\}$。如果循环矩阵$\boldsymbol{C}_2$可由$\boldsymbol{C}_1$按下面至少一个条件得到，则称$\boldsymbol{C}_1$同构于$\boldsymbol{C}_2$，记为$\boldsymbol{C}_1\cong\boldsymbol{C}_2$。

条件1　对于实数$c\in\{0,1,\cdots,L-1\}$，集合S_2的全部元素均可由集合S_1的全部元素加上一个c得到，即，对于$1\le i\le m, s_{2,i}=s_{1,i}+c\,(\mathrm{mod}\ L)$。

条件2　假设实数$c\in\{1,2,\cdots,L-1\}$，且与L互素。集合S_2的全部元素与集合S_1的全部元素满足如下等式关系：对于$1\le i\le m, s_{2,i}=c\cdot s_{1,i}\,(\mathrm{mod}\ L)$。

2.2 基于同构理论的低秩循环矩阵构造方法

由上节可知，给定循环矩阵$\boldsymbol{C}$的行数L和行(或列)重m，构造循环矩阵$\boldsymbol{C}$等价于设计第1行的非零元素位置集合$S=\{s_1,s_2,\cdots,s_m\}$，即一个基(cardinality)为m的集合。因此，本节主要构造一个基为m的位置集合$S=\{s_1,s_2,\cdots,s_m\}$，其中，对于$1\le i<j\le m, 0\le s_i<s_j\le L-1$。

由集合S中元素的个数与取值范围可知，位置集合S的总个数为

$$C_L^m=\frac{L!}{m!\cdot(L-m)!}\tag{1}$$

由定理1的条件1可知，任意一个位置集合S均同构于一个包含0元素的位置集合S_-，即

$$\begin{aligned}S&=\{s_1,s_2,\cdots,s_m\}\cong S_-=\{s_1-s_1\\&=0,s_2-s_1,\cdots,s_m-s_1\}\end{aligned}\tag{2}$$

注意，集合S_-中的减法运算是在模L下进行的。因此，可以直接将位置集合S中的元素s_1设为0，由位置集合的不可重复性可知，位置集合S的总个数减少为

$$C_{L-1}^{m-1}=\frac{(L-1)!}{(m-1)!\cdot(L-m)!}\tag{3}$$

这样有效地降低了位置集合S的搜索空间。假设集合S_-中的元素(s_2-s_1)与L互素，由数论知识可知，则存在一个数n，使得$(s_2-s_1)\cdot n=1\,(\mathrm{mod}\ L)$。那么，由定理1的条件2可知，集合$S_-$同构于一个包含0元素和1元素的位置集合$S_*$，即

$$\begin{aligned}S_-&=\{0,s_2-s_1,s_3-s_1,\cdots,s_m-s_1\}\\&\cong S_*=\{0,(s_2-s_1)\cdot n=1,\\&\quad(s_3-s_1)\cdot n,\cdots,(s_m-s_1)\cdot n\}\end{aligned}\tag{4}$$

注意，集合S_*中的乘法运算是在模L下进行的。这种情况下，可以直接将位置集合S中的元素s_1设为0，元素s_2设为1，由位置集合的不可重复性可知，位置集合S的总个数减少为

$$C_{L-2}^{m-2}=\frac{(L-2)!}{(m-2)!\,(L-m)!}\tag{5}$$

这样可以进一步降低位置集合S的搜索空间。由于实际的需求，我们只需构造具有特定秩的循环矩阵。由循环矩阵的大小可知，循环矩阵秩的最小值为1，最大值为L。由于本文主要关注低秩矩阵，为了减少搜索空间，这里设置一个阈值R，只需寻找秩小于R的循环矩阵。

由上可知，循环矩阵的穷搜索等价于位置集合S的穷搜索，而位置集合可以简化为一个包含零元素且共有m个元素的集合。因此，循环矩阵搜索其实就是如何产出组合序列的问题。目前，比特移位方法是一种产生组合序列的有效算法。下面给出一个构造低秩循环矩阵的搜索算法，即表1中的算法1。

为了证明算法1的有效性，表2给出部分低秩循环矩阵的搜索结果。

3 基于低秩循环矩阵的多元LDPC码构造

3.1 循环矩阵的4-环结构

短环，尤其是4-环，会降低LDPC码的迭代译码性能[18]。因此，本节分析循环矩阵的4-环结构，并给出一种确定循环矩阵4-环的方法。

由文献[15]可知，循环矩阵$\boldsymbol{C}$中的4-环由4个元

表 1　算法1：秩小于R的循环矩阵搜索算法

输入：阈值R，循环矩阵的行(或列)数L，行(或列)重m。

输出：位置集合S及其秩。

(1) **repeat**

(2) 基于比特移位方法按照组合顺序产生位置集合$S=\{s_1\,(=0),s_2,s_3,\cdots,s_m\}$，其中对于$1<l\le m$，$s_{l-1}<s_l$和$0<s_l<L$；

(3) 根据位置集合S生成大小为$L\times L$的二元循环矩阵$\boldsymbol{C}$；

(4) 计算循环矩阵$\boldsymbol{C}$的秩r；

(5) 如果r小于R，存储位置集合S，并记录它的秩为r，并打印输出集合S和秩r(注意，如果多个位置集合的秩相同，则只存储第1个位置集合，其他不再存储)；

(6) **until** (全部找到秩从1到R的位置集合，或$s_m-s_1=m-2$)

表 2 基于算法1搜索的部分循环矩阵

行/列数	行/列重	秩	位置集合	行/列数	行/列重	秩	位置集合
9	3	3	{0, 3, 6}	30	4	10	{0, 5, 15, 20}
12	3	4	{0, 4, 8}	32	4	8	{0, 8, 16, 24}
15	3	5	{0, 5, 10}	36	4	9	{0, 9, 18, 27}
18	3	6	{0, 6, 12}	40	4	10	{0, 10, 20, 30}
21	3	7	{0, 7, 14}	42	4	14	{0, 7, 21, 28}
24	3	8	{0, 8, 16}	44	4	11	{0, 11, 22, 33}
27	3	9	{0, 9, 18}	48	4	12	{0, 12, 24, 36}
30	3	10	{0, 10, 20}	25	5	5	{0, 5, 10, 15, 20}
33	3	11	{0, 11, 22}	30	5	6	{0, 6, 12, 18, 24}
39	3	13	{0, 13, 26}	35	5	7	{0, 7, 14, 21, 28}
42	3	14	{0, 14, 28}	40	5	8	{0, 8, 16, 24, 32}
45	3	15	{0, 15, 30}	45	5	9	{0, 9, 18, 27, 36}
48	3	16	{0, 16, 32}	50	5	10	{0, 10, 20, 30, 40}
8	4	2	{0, 2, 4, 6}	39	6	12	{0, 1, 13, 14, 26, 27}
12	4	3	{0, 3, 6, 9}	42	6	7	{0, 7, 14, 21, 28, 35}
16	4	4	{0, 4, 8, 12}	42	6	12	{0, 2, 14, 16, 28, 30}
18	4	6	{0, 3, 9, 12}	45	6	10	{0, 5, 15, 20, 30, 35}
20	4	5	{0, 5, 10, 15}	45	6	12	{0, 3, 15, 18, 30, 33}
24	4	6	{0, 6, 12, 18}	48	6	8	{0, 8, 16, 24, 32, 40}
27	4	7	{0, 7, 14, 21}	48	6	12	{0, 4, 16, 20, 32, 36}

素1组成，它们分布在矩阵$\boldsymbol{C}$中的两行两列，其结构见图1。由循环矩阵与位置集合$S=\{s_1,s_2,\cdots,s_m\}$之间的关系可知，这4个元素1的行列坐标可以简记为 $(a,s_i+a),(b,s_k+b),(b,s_l+b),(a,s_j+a)$ ， 其中，$0\le a<b\le L-1,1\le i<j\le m,1\le k<l\le m$。注意，上式括号里的加法运算是基于模$L$下进行的。显然，图1中这条4-环存在的充分必要条件为

$$s_i-s_j=s_k-s_l\,(\mathrm{mod}\ L) \tag{6}$$

或者

$$(s_i-s_j)+(s_l-s_k)=0\,(\mathrm{mod}\ L) \tag{7}$$

由于$i\ne j,k\ne l,(i,j)\ne(k,l)$，所以式(6)，式(7)是否成立与两个数有关，即$(s_i-s_j)$和$(s_l-s_k)$。注意，这两个数是在模$L$下得到的正数。基于此，这里根据位置集合$S$定义一个新的概念“差集”。

定义1(位置集合的差集)：令循环矩阵$\boldsymbol{C}$的位置集合为$S=\{s_1,s_2,\cdots,s_m\}$，且循环矩阵$\boldsymbol{C}$的行(或列)数为L。位置集合S的差集为$D=\{d\in Z_L|d=s_i-s_j\,(\mathrm{mod}\ L),1\le i\le m,1\le j\le m,i\ne j\}$。

显然，差集也是一个集合。理论上，该集合的基为$C_m^2=0.5m(m-1)$。由于集合的不可重复性，如果差集D的元素个数小于C_m^2，则说明差集中至少有两个元素是相等的，这也意味着式(6)是成立

$\boldsymbol{C}=$

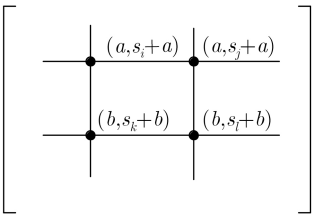

图 1 循环矩阵$\boldsymbol{C}$中的4-环结构

的。或者，当差集D中的两个元素相加在模L下等于零时，式(7)是成立的。这也对应着一条4-环的存在。这就说明循环矩阵$\boldsymbol{C}$至少存在一条4-环。基于此，这里给出一种检验循环矩阵$\boldsymbol{C}$中4-环是否存在的算法，即表3中的算法2。

根据算法1和算法2，可以得到一些不包含4-环的低秩循环矩阵位置集合。为了证明算法2的有效性，表4给出一些位置集合，其对应的循环矩阵Tanner图中没有4-环。

3.2 多元LDPC码的构造方法

本文主要研究多元LDPC码的构造方法。基于算法1和算法2，可以得到一个大小为$L\times L$的二元循环矩阵$\boldsymbol{C}$，其Tanner图的围长至少为6。为了构造多元矩阵，还需要将循环矩阵$\boldsymbol{C}$中的非零元素1替换为有限域GF(q)上的非零域元素。值得注意的是，在替换过程中，还得保证所得到的多元矩阵

表 3　算法2：检验循环矩阵$\boldsymbol{C}$中是否存在4-环的算法

输入：循环矩阵$\boldsymbol{C}$的位置集合$S=\{s_1,s_2,\cdots,s_m\}$，循环矩阵的行(或列)数L；

输出：是否存在4-环。

(1) 根据位置集合$S=\{s_1,s_2,\cdots,s_m\}$得到差集$D=\{d\in Z_L|d=s_i-s_j\,(\mathrm{mod}\,L),1\le i\le m,1\le j\le m,i\ne j\}$；

(2) 计算差集D中元素的个数，或者检查集合$E=\{e|e=d_i+d_j\,(\mathrm{mod}\,L),i\ne j,d_i\in D,d_j\in D,\}$中是否有零元素；

(3) 如果差集D中元素的个数小于C_m^2，或者集合E中有零元素，直接输出“存在4-环”；否则，输出“不存在4-环”。

表 4　不包含4-环的循环矩阵位置集合

行/列数	行/列重	秩	位置集合	行/列数	行/列重	秩	位置集合
7	3	4	{0, 1, 3}	39	5	27	{0, 1, 5, 8, 25}
14	3	8	{0, 2, 6}	42	5	20	{0, 2, 8, 28, 32}
21	3	12	{0, 3, 9}	45	5	35	{0, 1, 3, 10, 15}
49	3	28	{0, 7, 21}	63	5	30	{0, 3, 12, 42, 48}
56	3	32	{0, 8, 24}	93	5	48	{0, 3, 9, 21, 45}
60	3	44	{0, 4, 16}	45	6	28	{0, 1, 3, 12, 19, 40}
63	3	36	{0, 9, 27}	48	6	39	{0, 1, 3, 7, 12, 33}
70	3	40	{0, 10, 30}	60	6	39	{0, 1, 5, 28, 49, 52}
84	3	48	{0, 12, 36}	63	6	32	{0, 1, 3, 7, 15, 31}
91	3	52	{0, 13, 39}	65	6	48	{0, 1, 3, 30, 43, 51}
15	4	8	{0, 1, 3, 7}	84	6	60	{0, 1, 5, 8, 21, 40}
21	4	14	{0, 1, 3, 8}	85	6	60	{0, 1, 5, 21, 62, 79}
30	4	16	{0, 2, 6, 14}	90	6	56	{0, 2, 6, 24, 38, 80}
45	4	24	{0, 3, 9, 21}	51	7	43	{0, 1, 3, 9, 21, 37, 47}
75	4	40	{0, 5, 15, 35}	57	7	39	{0, 1, 3, 13, 36, 43, 52}
90	4	48	{0, 6, 18, 42}	62	7	47	{0, 1, 3, 10, 14, 39, 57}
91	4	75	{0, 1, 6, 17}	63	7	39	{0, 1, 3, 18, 34, 54, 58}
21	5	10	{0, 1, 4, 14, 16}	63	8	26	{0, 1, 3, 7, 15, 20, 31, 41}
31	5	16	{0, 1, 3, 7, 15}	85	8	48	{0, 1, 3, 7, 15, 31, 42, 63}

不是满秩的。通常情况下，直接将矩阵$\boldsymbol{C}$中的非零元素1随机替换成非零域元素，那么所得到的多元矩阵基本上全是满秩的。因此，本文采用文献[19]的非零域元素赋值方法，基于一个二元循环矩阵，可以得到一套域阶数、码率均灵活可变的多元LDPC码。不妨假设二元循环矩阵$\boldsymbol{C}$的秩为R，那么，本文所提出的多元LDPC码的可选择码率为$1-R,1-R-1/L,1-R-2/L,1-R-3/L,\cdots,0$。下面简单介绍两种非零域元素的赋值方法。

方法1　将二元循环矩阵C中每一列的所有非零元素1替换为有限域GF(q)上的同一个非零域元素，这里的非零域元素是随机选取的。这样，就可以得到一个GF(q)上的矩阵C_q。由文献[19]的定理1可知，二元循环矩阵$\boldsymbol{C}$与多元矩阵$\boldsymbol{C}_q$有相同的秩。因此，矩阵$\boldsymbol{C}_q$的零空间给出了一组码率为($1-R$)、码长为L的q元LDPC码。

方法2　将二元循环矩阵$\boldsymbol{C}$中某一列(或一些列)的非零元素1替换为有限域GF(q)上的不相同非零域元素(要求不相同)，而剩余的每一列的非零元素1替换为有限域GF(q)上的同一个非零域元素，这里的非零域元素是随机选取的。这样，就可以得到一个GF(q)上的矩阵$\boldsymbol{C}_q$。通常，随着矩阵$\boldsymbol{C}_q$列中有不同非零域元素的列数逐渐增加，矩阵$\boldsymbol{C}_q$的秩会逐一增加，直到满秩。因此，矩阵$\boldsymbol{C}_q$的零空间可以定义一组码率可变的q元LDPC码。

3.3　仿真结果

下面的仿真参数为AWGN信道和BPSK调制。二元LDPC码的译码算法为和积算法(SPA)，而多元LDPC码的译码算法为基于快速傅里叶变换(Fast Fourier Transform, FFT)的多元和积算法(Q-ary Sum-Product Algorithm, QSPA)。选用的高阶调制为QPSK, 8PSK和64-QAM调制。

考虑一个行(或列)数为31、行(或列)重为5的循环矩阵。根据表4，可以找到一个没有4-环的循环

矩阵，它的位置集合为{0, 1, 3, 7, 15}、秩为16。根据3.2节的方法1，可以构造一组码长为31、码率为15/31的q元LDPC码。根据方法2，可以得到一组码长为31、码率可变的q元LDPC码，其可选择的码率有{15/31, 14/31, 13/31, 12/31, 11/31, 10/31, 9/31, 8/31, 7/31, 6/31, 5/31, 4/31, 3/31, 2/31, 1/31}。根据方法1，选择有限域GF(64)，可以得到一个64元(31, 15)LDPC码。图2给出了该码在采用迭代1次、3次和50次的QSPA下的误码字率(Word Error Rate, WER)性能。为了在相同码参数(等效比特码长和码率)下比较，这里基于PEG算法构造了一个二元(186, 90)LDPC码[20]。图2也给出了该码在采用迭代50次的SPA下的误码字率性能和码长为186 bit、码率为15/31的有限长性能限(PPV Bound)[21]。可以看出，当迭代次数为50和误码字率等于10^{-5}时，所构造的64元(31, 15)LDPC码比二元(186, 90)LDPC码约有0.9 dB的编码增益。此外，还可以看出所构造的64元(31, 15)LDPC码在迭代3次和50次之间的性能差距很小；当误码字率等于10^{-5}时，所构造的64元(31, 15)LDPC码离有限长性能限约1 dB。图3给出了所构造的64元(31, 15)LDPC码和二元(186, 90)LDPC码在高阶调制下的误码字率性能。可以看出，随着调制阶数的增大，所构造的多元码与二元码的性能差距也变大，而且所构造的多元码在迭代5次和50次的性能曲线几乎重叠。根据方法1，选择有限域GF(4), GF(32)和GF(128)，可以得到3个(31, 15)多元LDPC码。图4给出了这3个码在迭代5次和50次的QSPA下的误码字率性能。由图4可知，所构造的多元LDPC码有较好的译码性能，并且在误码字率10^{-6}处没有出现错误平层。此外，所提出的多元LDPC码只需迭代5次就可以达到迭代50次的译码性能。

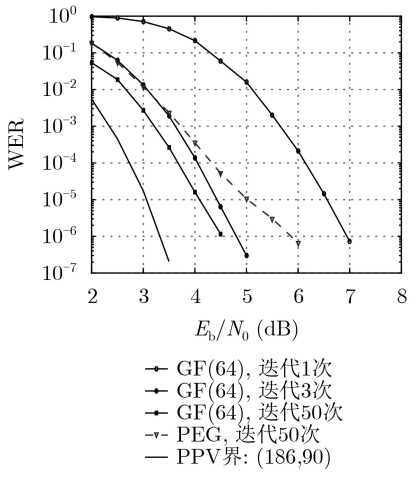

图 2 GF(64)上的(31, 15)LDPC码和基于PEG算法构造的二元(186, 90)LDPC码在不同迭代次数下的误码字率性能比较

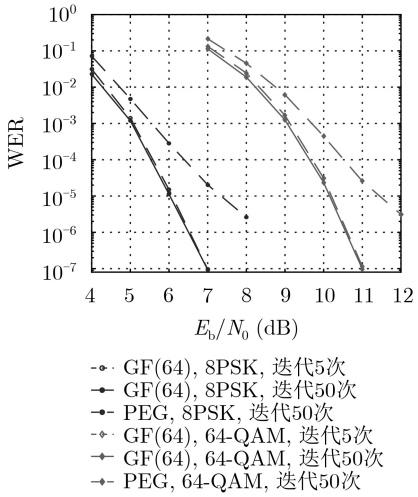

图 3 GF(64)上的(31, 15)LDPC码和基于PEG算法构造的二元(186, 90)LDPC码在高阶调制下的误码字率性能比较

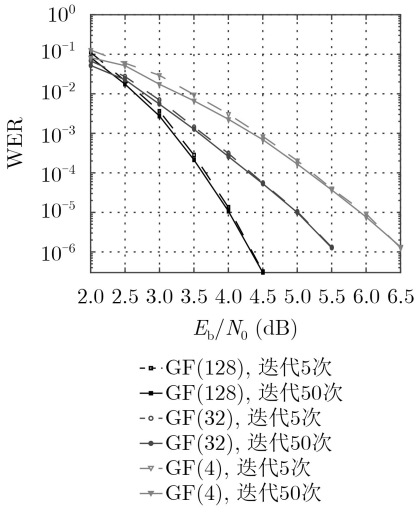

图 4 GF(4), GF(32)和GF(128)上的(31, 15)LDPC码在迭代5次和50次下的误码字率性能

4 结束语

本文研究了一类低秩循环矩阵的构造方法。首先将循环矩阵的构造转化为非零元素位置集合的设计，并基于位置集合的同构理论提出了低秩循环矩阵的搜索算法。进一步地，分析了循环矩阵的4-环结构，得到了围长至少为6的循环矩阵。基于此，利用非零域元素的两种赋值方法，提出了多元LDPC码的构造方法。AWGN信道上的数值仿真结果表明，所构造的多元LDPC码有较好的译码性能，并且只需迭代5次就能达到迭代50次的译码性能。这为低时延高可靠无线通信提供了一种有效的候选编码方案。为了进一步提升这类码的性能，如何优化它们的非零域元素是值得研究的。

参 考 文 献

[1] 赵亚军, 郁光辉, 徐汉青. 6G移动通信网络: 愿景、挑战与关

键技术[J]. 中国科学: 信息科学, 2019, 49(8): 963–987. doi: 10.1360/N112019-00033.
ZHAO Yajun, YU Guanghui, and XU Hanqing. 6G mobile communication networks: Vision, challenges, and key technologies[J]. *Scientia Sinica Informationis*, 2019, 49(8): 963–987. doi: 10.1360/N112019-00033.

[2] LIU Yanfang, OLMOS P M, and MITCHELL D G M. Generalized LDPC codes for ultra reliable low latency communication in 5G and beyond[J]. *IEEE Access*, 2018, 6: 72002–72014. doi: 10.1109/ACCESS.2018.2880997.

[3] CHEN Chao, BAI Baoming, SHI Guangming, *et al*. Nonbinary LDPC codes on cages: Structural property and code optimization[J]. *IEEE Transactions on Communications*, 2015, 63(2): 364–375. doi: 10.1109/TCOMM.2014.2387341.

[4] ZHU Min, GUO Quan, BAI Baoming, *et al*. Reliability-based joint detection-decoding algorithm for nonbinary LDPC-coded modulation systems[J]. *IEEE Transactions on Communications*, 2016, 64(1): 2–14. doi: 10.1109/TCOMM.2015.2487454.

[5] WANG Shuai, HUANG Qin, and WANG Zulin. Symbol flipping decoding algorithms based on prediction for non-binary LDPC codes[J]. *IEEE Transactions on Communications*, 2017, 65(5): 1913–1924. doi: 10.1109/TCOMM.2017.2677438.

[6] HUANG Qin, SONG Liyuan, and WANG Zulin. Set message-passing decoding algorithms for regular non-binary LDPC codes[J]. *IEEE Transactions on Communications*, 2017, 65(12): 5110–5122. doi: 10.1109/TCOMM.2017.2746101.

[7] ZHANG Mu, CAI Kui, HUANG Qin, *et al*. On bit-level decoding of nonbinary LDPC codes[J]. *IEEE Transactions on Communications*, 2018, 66(9): 3736–3748. doi: 10.1109/TCOMM.2018.2827994.

[8] WIJEKOON V B, VITERBO E, HONG Yi, *et al*. A novel graph expansion and a decoding algorithm for NB-LDPC codes[J]. *IEEE Transactions on Communications*, 2020, 68(3): 1358–1369. doi: 10.1109/TCOMM.2019.2961884.

[9] HUANG Qin, LIU Keke, and WANG Zulin. Low-density arrays of circulant matrices: Rank and row-redundancy, and QC-LDPC codes[C]. 2012 IEEE International Symposium on Information Theory, Cambridge, USA, 2012: 3073–3077. doi: 10.1109/ISIT.2012.6284127.

[10] 李骜, 刘鑫, 陈德运, 等. 基于低秩表示的鲁棒判别特征子空间学习模型[J]. 电子与信息学报, 2020, 42(5): 1223–1230. doi: 10.11999/JEIT190164.
LI Ao, LIU Xin, CHEN Deyun, *et al*. Robust discriminative feature subspace learning based on low rank representation[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1223–1230. doi: 10.11999/JEIT190164.

[11] 彭义刚, 索津莉, 戴琼海, 等. 从压缩传感到低秩矩阵恢复: 理论与应用[J]. 自动化学报, 2013, 39(7): 981–994. doi: 10.3724/SP.J.1004.2013.00981.
PENG Yigang, SUO Jinli, DAI Qionghai, *et al*. From compressed sensing to low-rank matrix recovery: Theory and applications[J]. *Acta Automatica Sinica*, 2013, 39(7): 981–994. doi: 10.3724/SP.J.1004.2013.00981.

[12] 陈容, 陈岚, WAHLA A H. 基于公式递推法的可变计算位宽的循环冗余校验设计与实现[J]. 电子与信息学报, 2020, 42(5): 1261–1267. doi: 10.11999/JEIT190503.
CHEN Rong, CHEN Lan, and WAHLA A H. Design and implementation of cyclic redundancy check with variable computing width based on formula recursive algorithm[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1261–1267. doi: 10.11999/JEIT190503.

[13] RYAN W E and LIN Shu. Channel Codes: Classical and Modern[M]. New York, USA: Cambridge University Press, 2009: 448–578.

[14] CHEN Chao, BAI Baoming, and WANG Xinmei. Construction of quasi-cyclic LDPC codes based on a two-dimensional MDS code[J]. *IEEE Communications Letters*, 2010, 14(5): 447–449. doi: 10.1109/LCOMM.2010.05.100008.

[15] XU Hengzhou, BAI Baoming, ZHU Min, *et al*. Construction of short-block nonbinary LDPC codes based on cyclic codes[J]. *China Communications*, 2017, 14(8): 1–9. doi: 10.1109/CC.2017.8014342.

[16] 陈智雄, 苑津莎. 基于多重置换阵的满秩结构化LDPC码构造方法[J]. 电子学报, 2012, 40(2): 313–318. doi: 10.3969/j.issn.0372-2112.2012.02.017.
CHEN Zhixiong and YUAN Jinsha. Construction of structure LDPC codes with full rank based on multi-permutation matrix[J]. *Acta Electronica Sinica*, 2012, 40(2): 313–318. doi: 10.3969/j.issn.0372-2112.2012.02.017.

[17] TANNER R. A recursive approach to low complexity codes[J]. *IEEE Transactions on Information Theory*, 1981, 27(5): 533–547. doi: 10.1109/TIT.1981.1056404.

[18] XIAO Xin, VASIĆ B, LIN Shu, *et al*. Reed-Solomon based quasi-cyclic LDPC codes: Designs, girth, cycle structure, and reduction of short cycles[J]. *IEEE Transactions on Communications*, 2019, 67(8): 5275–5286. doi: 10.1109/TCOMM.2019.2916605.

[19] XU Hengzhou, FENG Dan, SUN Cheng, *et al*. Algebraic-based nonbinary ldpc codes with flexible field orders and code rates[J]. *China Communications*, 2017, 14(4): 111–119. doi: 10.1109/CC.2017.7927569.

[20] HU Xiaoyu, ELEFTHERIOU E, and ARNOLD D M. Regular and irregular progressive edge-growth tanner graphs[J]. *IEEE Transactions on Information Theory*, 2005, 51(1): 386–398. doi: 10.1109/TIT.2004.839541.

[21] POLYANSKIY Y, POOR H V, and VERDU S. Channel coding rate in the finite blocklength regime[J]. *IEEE Transactions on Information Theory*, 2010, 56(5): 2307–2359. doi: 10.1109/TIT.2010.2043769.

徐恒舟：男，1987年生，讲师，主要研究方向为组合设计与编码理论、信息论等.
朱　海：男，1978年生，教授，主要研究方向为信道编码、云计算、无线网络技术等.
冯　丹：女，1989年生，讲师，主要研究方向为编码调制、MIMO等.
张　博：男，1982年生，副教授，主要研究方向为信息论、信道编码等.
周慢杰：女，1985年生，助教，主要研究方向为LDPC编码理论及信息教育技术等.

责任编辑：马秀强