# 无小环大列重 QC-LDPC 短码的显式构造

张国华[1],孙爱晶[1],倪孟迪[1],方 毅[2*]
(1. 西安邮电大学通信与信息工程学院,陕西西安 710121;2. 广东工业大学信息工程学院,广东广州 510000)

**摘 要:** 针对列重较大的无 4 环且无 6 环的准循环(Quasi-Cyclic,QC)低密度奇偶校验(Low-Density Parity-Check,LDPC)码,本文提出了三种新的显式构造方法. 新方法的指数矩阵由两个整数序列完全定义,其中第一个序列是从 0 开始且公差为 1 的等差序列,第二个序列是由符合最大公约数约束的整数组成的特殊序列. 对于现有显式方法只能提供较大循环块尺寸的多种行重类型,新显式构造方法在这些行重类型下均获得了相当小的循环块尺寸,从而将最小循环块尺寸降低到大约只有原来的一半. 与近期提出的基于搜索的对称结构法相比,新的显式构造方法具有类似或更优的译码性能、极低的描述复杂度且不需要计算机搜索.

**关键词:** 循环块;环;最大公约数;低密度奇偶校验码;准循环
**基金项目:** 国家自然科学基金(No.62322106,No.62071131);广东省国际科技合作项目(No.2022A0505050070)
**中图分类号:** TN911.22;TN927 **文献标识码:** A **文章编号:** 0372-2112(2024)06-1862-07
**电子学报 URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20230300

# Explicit Constructions of Short QC-LDPC Codes Free of Small Cycles and with Large Column Weight

ZHANG Guo-hua[1], SUN Ai-jing[1], NI Meng-di[1], FANG Yi[2*]
(1. *School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi* 710121, *China*;
2. *School of Information Engineering, Guangdong University of Technology, Guangzhou, Guangdong* 510000, *China*)

**Abstract:** Three new explicit constructions are proposed for quasi-cyclic (QC) low-density parity-check (LDPC) codes free of 4-cycles and 6-cycles with large column weights. The exponent matrices for these new methods are completely defined by two sequences of integers. The first sequence is an arithmetic sequence starting from zero with the common difference being one, and the second is a special sequence composed of integers satisfying the greatest-common-divisor (GCD) constraint. The new methods can produce rather small circulant sizes for many categories of row weights, while the existing explicit methods can only provide relatively large circulant sizes, thus the up-to-date smallest circulant sizes being nearly halved. Compared with the recently proposed symmetrical construction which relies upon extensive search, the new explicit constructions have similar or better decoding performance, possess extremely low description complexity and need no computer search.

**Key words:** circulant; cycle; greatest common divisor; low-density parity-check code; quasi-cyclic
**Foundation Item(s):** National Natural Science Foundation of China (No.62322106, No.62071131);International Collaborative Research Programof Guangdong Science and Technology Department (No.2022A0505050070)

## 1 引言

低密度奇偶校验(Low-Density Parity-Check,LDPC)码是一种译码性能可以接近理论极限的信道编码. 作为一类特殊的 LDPC 码,准循环(Quasi-Cyclic,QC)-LDPC 码[1,2]的编码器和译码器实现复杂度可以大大降低,因此目前得到学术界和工业界的广泛研究和应用. QC-LDPC 码的主要优化途径之一,是消除其 Tanner 图中的小环(cycle)[3~6]. QC-LDPC 码的校验矩阵是一个 $J$ 行 $L$ 列的矩阵,矩阵中的每个元素是一个循环块(circulant). 一般而言,循环块的尺寸越小,QC-LDPC 码的小环越难消除. 因此,如何构建无小环且循环块尺寸尽可能小的 QC-LDPC 码,是目前 QC-LDPC 码构造领域的一

收稿日期:2023-04-04;修回日期:2023-10-14;责任编辑:李勇锋
*通讯作者:方毅

个重要研究方向. QC-LDPC码中可能出现的环的最小长度是4(记为4环),其次是6(记为6环). 当$L$是素数时,基于阵列码的QC-LDPC码已经达到了无4环情况下的最小循环块尺寸[1];因此,如何在无4环且无6环即围长(girth)至少为8的前提下获得循环块尺寸尽可能小的QC-LDPC码,是目前QC-LDPC码构造领域的前沿和难点.

QC-LDPC码的构造方法大致可分为搜索法[5,6]和数学公式法[7~13]. 与搜索法相比,数学公式法可以提供较深刻的理论结果;此外,在某些参数下数学公式法也可以提供与搜索法相比拟的小循环块尺寸. 因此,如何利用数学公式法构造无4环无6环且循环块尺寸尽量小的QC-LDPC码是一个非常有挑战性的理论难题. 对于$J$=3的情况,目前能产生最短的无4环无6环QC-LDPC码的数学公式法是整数网格方法[3]和数列移序及反序法[7];这些方法所提供的最小循环块尺寸大致是$L^2/2$. 对于$J$=4的情况,能获得最短无4环无6环QC-LDPC码的数学公式法是文献[8]中的方法;该方法所提供的最小循环块尺寸大致是$3L^2/4$. 因为$J$=5的情况便于结合掩膜(masking)等通用技巧,所以列重为5的QC-LDPC短码的构造问题近年来吸引了国内外学者的浓厚兴趣. M Karimi提出的构造方法[9]可以获得的最小循环块尺寸约为$L^3$,基于最大公约数理论的构造方法[10]可以取得的最小循环块尺寸约为$2L^2$. 2023年J Wang等人提出的构造方法[11]对于$L$满足$L(\mathrm{mod}\ 6)=2$或者4的情况获得的最小循环块尺寸降低到大约$L^2$.

本文提出三种新的显式构造方法,对于$L$的所有其他取值情形首次获得了低至约$L^2$的循环块尺寸. 此外,在三种新构造方法中,两种方法所产生的新QC-LDPC码的性能显著优于现有的典型搜索方法,即对称结构QC-LDPC码[5];另一种新方法产生的新QC-LDPC码的性能与现有典型搜索方法几乎相同. 与已有的典型搜索方法相比,本文提出的新构造方法有两个优势:第一,具有非常低的描述复杂度;第二,构造过程不需要计算机搜索.

## 2　预备知识

为了便于理解,本文避免使用"矩阵同构"[14]这种在数学上较为繁琐的描述,而是采用"环特性相同"这种更简单的描述方式. 在本文中,环特性相同的两个QC-LDPC码是指,第一个码的Tanner图中的$2n$环可以与第二个码的Tanner图中的$2n$环建立对应关系.

QC-LDPC码的校验矩阵可以使用指数矩阵$\boldsymbol{E}$和循环块尺寸$P$共同确定. 本文涉及的循环块都是循环置换矩阵(Circulant Permutation Matrix,CPM),即重量为1的循环块. 因此一个$J$行$L$列的指数矩阵$\boldsymbol{E}$对应于一个$(J,L)$-规则QC-LDPC码,其中$J$是校验矩阵的列重,$L$是校验矩阵的行重. 本文研究的指数矩阵$\boldsymbol{E}$可以表示为两个序列的乘积,即$\boldsymbol{E}=\boldsymbol{S}_2^{\mathrm{T}}\boldsymbol{S}_1$,其中$\boldsymbol{S}_2$是一个包含$J$个整数的序列,$\boldsymbol{S}_1$是从0到$L-1$递增且步进为1的等差序列,符号T表示转置. 这种指数矩阵所对应的QC-LDPC码的围长最大可以达到8[10].

设$a_1,a_2,\cdots,a_n$和$b$都是整数. 根据Fossorier的环路方程[1],以下两个性质显然成立.

**性质1**　由$\boldsymbol{S}_2=[a_1,a_2,\cdots,a_n]$和$\boldsymbol{S}_2'=[b+a_1,b+a_2,\cdots,b+a_n]$定义的两个QC-LDPC码的环特性相同.

**性质2**　若$\gcd(b,P)=1$,则$\boldsymbol{S}_2=[ba_1,ba_2,\cdots,ba_n]$和$\boldsymbol{S}_2'=[a_1,a_2,\cdots,a_n]$定义的两个QC-LDPC码的环特性相同.

根据性质2(令$b=-1$)和性质1(令$b=a_n$)可知,如下性质成立.

**性质3**　$\boldsymbol{S}_2=[a_1,a_2,\cdots,a_n]$和$\boldsymbol{S}_2'=[a_n-a_1,a_n-a_2,\cdots,a_n-a_n]$定义的两个QC-LDPC码的环特性相同.

在下文表格中,使用性质3的位置以符号"R"标记.

此外,根据Fossorier的4环方程可知如下性质成立.

**性质4**　设$a$是正整数. 当循环块尺寸$P\geqslant a(L-1)+1$时,$\boldsymbol{S}_2=[0,a]$对应的Tanner图无4环.

根据GCD方法[4]可知如下性质成立.

**性质5**　设$a$和$b$是满足$b>a$和$b/\gcd(b,a)\geqslant L$的正整数. 当$P\geqslant b(L-1)+1$时$\boldsymbol{S}_2=[0,a,b]$对应的Tanner图无6环.

对于可分解为两个因子的循环块尺寸,以下结论成立.

**性质6**　设$x$和$y$是两个正整数,$z$是非负整数. 如果(1)$y$是$L+z$的整数倍,并且(2)$\gcd(x,L+z)=1$,则$\boldsymbol{S}_2=[0,x,y]$和循环块尺寸$P=m(L+z)$所对应的Tanner图无6环,其中$m$是正整数.

**证明**　如果存在6环,则该环可以表示为$(xi-yi)+(yk-0)+(0-xj)=0\ (\mathrm{mod}P)$,其中$i,j$和$k$是满足$0\leqslant i,j,k<L$的三个不同整数. 该式可表示为$y(k-i)+x(i-j)=nm(L+z)$,其中$n$是整数. 因为$y$是$L+z$的整数倍,所以可知$x(i-j)$也是$L+z$的整数倍. 但由于$\gcd(x,L+z)=1$,因此$(i-j)$是$L+z$的整数倍. 这是不可能的,因为$0<|i-j|<L$. 证毕.

由性质6的证明过程可知:性质6中的$x$和$y$可互换;这有助于简化下文的证明过程.

在后文可以看到,性质1~6可以大大简化本文的论证过程. 对于本文提出的每种新构造方法,需要论证的4环情形和6环情况都由原来的10种减少到至多1种. 本文的论证还用到以下性质.

**性质7**[11] 设$a$和$b$是满足$2a\leqslant b$的两个正整数. 设$i,j$和$k$是大于等于0且小于$L$的三个不同整数. 则$|(i-j)a+(k-i)b|\leqslant -a+(L-1)b$.

## 3 新构造

在大量随机试探和对规律梳理总结的基础上,本节提出了三种可以产生围长为8的QC-LDPC码的新构造法.

### 3.1 构造1

**定理1** $\mathrm{mod}(L,6)=1$和3时,令$\boldsymbol{S}_2=[0,4,L+8,2L,2L+8]$和$P=L(L+4)$. 则对应的Tanner图无4环和6环.

**证明** 首先考虑4环. 根据4环与$\boldsymbol{S}_2$中哪两个元素相关联来分类,共有10种情况,如表1所示. 表1中数据的含义以最后一行举例说明. 原始二元组"[2L,2L+8]"表示该4环与$\boldsymbol{S}_2$的最后两个元素相关联,即该4环出现在指数矩阵$\boldsymbol{E}$最后两行对应的Tanner子图中. "(-2L)[0,8]"表示[2L,2L+8]中每个元素减去2L得到变形后的二元组[0,8];"(/8)[0,1]"表示二元组[0,8]中每个元素除以8得到变形后的二元组[0,1]. 由表1可知:在所有10种4环中除情况2之外的9种情况均无4环. 这是由于$P=L(L+4)>(L+5)(L-1)$,所以根据性质4,当$a\leqslant L+5$时$\boldsymbol{S}_2=[0,a]$对应的Tanner图无4环. 情况2无4环的证明如下.

情况2:如果存在这种4环,则有$(L+8)(j-i)=nL(L+4)$,其中$0\leqslant i<j<L$. LHS=$(L+4)(j-i)+4(j-i)$,RHS=$nL(L+4)$. 由此可知,$4(j-i)$含有因子$L+4$. 因为$\gcd(L+4,4)=\gcd(L,4)$且$L$是奇数,所以$\gcd(L+4,4)=1$. 因此,只可能是$(j-i)$含有因子$L+4$. 因为$0<j-i<L$,所以$(j-i)$不可能含有因子$L+4$,矛盾.

其次,考虑6环情况. 根据6环与$\boldsymbol{S}_2$中的哪三个元素相关联来分类,共有10种情况,如表2所示. 这10种6环不可能出现的原因如表2最后一列所示. 证毕.

### 3.2 构造2

**定理2** $\mathrm{mod}(L,6)=0$时,令$\boldsymbol{S}_2=[0,1,L+2,L+5,2L+7]$和$P=L^2+4L+7$. 则对应的Tanner图无4环和6环.

**证明**

首先考虑4环. 如表3所示,在所有的10种4环中,除情况4之外的9种情况均无4环. 情况4的证明过程与构造1情况2类似,因此略去.

其次,考虑6环情况. 根据6环与$\boldsymbol{S}_2$中的哪三个元素相关联来分类,共有10种情况,如表4所示. 除了情况3,剩余的9种6环不可能出现的原因如表4最后一列所示.

情况3:如果存在这种6环,则$(0-j)+[i-(2L+7)i]+[(2L+7)k-0]=n(L^2+4L+7)$,其中$i,j$和$k$是满足$0\leqslant i,j,k<L$的三个不同整数. 上式可以表示为$(i-j)+(2L+7)(k-i)=n(L^2+4L+7)$. 根据性质7,$|\mathrm{LHS}|\leqslant(2L+7)(L-1)-1=2L^2+5L-8<2(L^2+4L+7)$,因此$n$只可能等于0,1和-1.

(1) 当$n=0$时,上式可以表示为$(i-j)+(2L+7)(k-i)=0$,由此可知$2L+7|(i-j)$. 因为$0<|i-j|<L$,所以不可能.

(2) 当$n=1$时,上式可表示为$(i-j)+(2L+7)(k-i)=L^2+4L+7$. 即$2(L+3)(k-i)+(k-j-4)=(L+1)(L+3)$. 由此可知,$L+3|(k-j-4)$. 因为$0\leqslant|k-j-4|\leqslant L+3$,所以只可能$k-j=4$或者$k-j=-(L-1)$. 当$k-j=4$时上式简化为$2(k-i)=(L+1)$,因为左侧是偶数而右侧是奇数,所以不可能. 当$k-j=-(L-1)$时上式简化为$2(k-i)-1=(L+1)$,即$k-i=L/2+1$. 由此可知$j-i=3L/2$,这是不可能的.

(3) $n=-1$的证明过程与$n=1$类似,因此略去. 证毕.

**表1 构造1的10种4环**

| 情况 | 原始二元组 | 变形 | 无4环原因 |
|---|---|---|---|
| 1 | [0,4] | (/4) [0,1] | 性质4 |
| 2* | [0,L+8] | — | 需证明 |
| 3 | [0,2L] | (/2) [0,L] | 性质4 |
| 4 | [0,2L+8] | (/2) [0,L+4] | 性质4 |
| 5 | [4,L+8] | (-4) [0,L+4] | 性质4 |
| 6 | [4,2L] | (/2) [2,L]<br>(-2) [0,L-2] | 性质4 |
| 7 | [4,2L+8] | (/2) [2,L+4]<br>(-2) [0,L+2] | 性质4 |
| 8 | [L+8,2L] | (-(L+8)) [0,L-8] | 性质4 |
| 9 | [L+8,2L+8] | (-(L+8)) [0,L] | 性质4 |
| 10 | [2L,2L+8] | (-2L) [0,8]<br>(/8) [0,1] | 性质4 |

**表2 构造1的10种6环**

| 情况 | 原始三元组 | 变形 | 无6环原因 |
|---|---|---|---|
| 1 | [0,4,L+8] | (R) [0,L+4,L+8] | 性质6(L奇数) |
| 2 | [0,4,2L] | (/2) [0,2,L] | 性质6(L奇数) |
| 3 | [0,4,2L+8] | (/2) [0,2,L+4] | 性质6(L奇数) |
| 4 | [0,L+8,2L] | (R) [0,L-8,2L] | 性质6(L奇数) |
| 5 | [0,L+8,2L+8] | (R) [0,L,2L+8] | 性质6(L奇数) |
| 6 | [0,2L,2L+8] | (R) [0,8,2L+8]<br>(/2) [0,4,L+4] | 性质6(L奇数) |
| 7 | [4,L+8,2L] | (-4) [0,L+4,2L-4] | 性质6(L=1,3mod6) |
| 8 | [4,L+8,2L+8] | (-4) [0,L+4,2L+4]<br>(R) [0,L,2L+4] | 性质6(L奇数) |
| 9 | [4,2L,2L+8] | (-4) [0,2L-4,2L+4]<br>(/2) [0,L-2,L+2] | 性质5 (L奇数) |
| 10 | [L+8,2L,2L+8] | (-(L+8)) [0,L-8,L]<br>(R) [0,8,L] | 性质6(L奇数) |

### 3.3 构造3

**定理3** $\mathrm{mod}(L,6)=5$时,令$\boldsymbol{S}_2=[0,3,L+2,L+3,2L+$

**表3　构造2的10种4环**

| 情况 | 原始二元组 | 变形 | 无4环原因 |
|---|---|---|---|
| 1 | [0,1] | — | 性质4 |
| 2 | [0,$L$+2] | — | 性质4 |
| 3 | [0,$L$+5] | — | 性质4 |
| 4* | [0,2$L$+7] | — | 需证明 |
| 5 | [1,$L$+2] | (−1) [0,$L$+1] | 性质4 |
| 6 | [1,$L$+5] | (−1) [0,$L$+4] | 性质4 |
| 7 | [1,2$L$+7] | (−1) [0,2$L$+6](/2) [0,$L$+3] | 性质4 |
| 8 | [$L$+2,$L$+5] | (−($L$+2)) [0,3] | 性质4 |
| 9 | [$L$+2,2$L$+7] | (−($L$+2)) [0,$L$+5] | 性质4 |
| 10 | [$L$+5,2$L$+7] | (−($L$+5)) [0,$L$+2] | 性质4 |

**表4　构造2的10种6环**

| 情况 | 原始三元组 | 变形 | 无6环原因 |
|---|---|---|---|
| 1 | [0,1,$L$+2] | — | 性质5($L$任意) |
| 2 | [0,1,$L$+5] | — | 性质5($L$任意) |
| 3* | [0,1,2$L$+7] | — | 需证明 |
| 4 | [0,$L$+2,$L$+5] | (R) [0,3,$L$+5] | 性质5($L$≠1,4mod6) |
| 5 | [0,$L$+2,2$L$+7] | (*($L$+2)) [0,−3,3$L$]<br>(/3) [0,−1,$L$]<br>(+1) [0,1,$L$+1] | 性质5<br>($L$≠1,4mod6) |
| 6 | [0,$L$+5,2$L$+7] | (R) [0,$L$+2,2$L$+7] | 同情况5 |
| 7 | [1,$L$+2,$L$+5] | (−1) [0,$L$+1,$L$+4] | 性质5($L$≠2,5 mod 6) |
| 8 | [1,$L$+2,2$L$+7] | (−1) [0,$L$+1,2$L$+6]<br>(*($L$+1)) [0,−2$L$−6,−8]<br>(/(−2)) [0,4,$L$+3] | 性质5<br>($L$偶数) |
| 9 | [1,$L$+5,2$L$+7] | (−1) [0,$L$+4,2$L$+6]<br>(/2) [0,$L$/2+2,$L$+3] | 性质5<br>($L$偶数) |
| 10 | [$L$+2,$L$+5,2$L$+7] | (−($L$+2)) [0,3,$L$+5] | 同情况4 |

7]和$P=(L+2)^2$. 则对应的Tanner图无4环和6环.

**证明**　首先考虑4环. 如表5所示,在所有的10种4环中,除情况4之外的9种情况均无4环. 情况4的证明过程与构造1情况2类似,因此略去. 其次,考虑6环情况. 根据6环与$\boldsymbol{S}_2$中的哪三个元素相关联来分类,共有10种情况,如表6所示. 除了情况6,剩余的9种6环不可能出现的原因如表6最后一列所示. 情况6的证明过程与构造2情况3类似,因此略去. 证毕.

根据定理1~3和文献[11]的定理7,可得以下推论.

**推论1**　对于任意$L$,可以使$(5,L)$-规则QC-LDPC码的围长至少为8的最小循环块尺寸满足$P\leqslant L^2+4L+7$.

关于无4环无6环$(5,L)$-规则QC-LDPC码的最小循环块尺寸,目前的最小上界是$P\leqslant(2L+3)(L-1)+1$[10]. 由此可见,推论1将原来的大约为$2L^2$的循环块尺寸降低了大约一半.

**表5　构造3的10种4环**

| 情况 | 原始二元组 | 变形 | 无4环原因 |
|---|---|---|---|
| 1 | [0,3] | — | 性质4 |
| 2 | [0,$L$+2] | — | 性质4 |
| 3 | [0,$L$+3] | — | 性质4 |
| 4* | [0,2$L$+7] | — | 需证明 |
| 5 | [3,$L$+2] | (−3) [0,$L$−1] | 性质4 |
| 6 | [3,$L$+3] | (−3) [0,$L$] | 性质4 |
| 7 | [3,2$L$+7] | (−3) [0,2$L$+4](/2) [0,$L$+2] | 性质4 |
| 8 | [$L$+2,$L$+3] | (−($L$+2)) [0,1] | 性质4 |
| 9 | [$L$+2,2$L$+7] | (−($L$+2)) [0,$L$+5] | 性质4 |
| 10 | [$L$+3,2$L$+7] | (−($L$+3)) [0,$L$+4] | 性质4 |

**表6　构造3的10种6环**

| 情况 | 原始三元组 | 变形 | 无6环原因 |
|---|---|---|---|
| 1 | [0,3,$L$+2] | — | 性质5($L$≠1,4 mod 6) |
| 2 | [0,3,$L$+3] | — | 性质5($L$≠0,3 mod 6) |
| 3 | [0,3,2$L$+7] | (R) [0,2$L$+4,2$L$+7] | 性质6 ($L$≠1,4 mod 6) |
| 4 | [0,$L$+2,$L$+3] | (R) [0,1,$L$+3] | 性质5($L$任意) |
| 5 | [0,$L$+2,2$L$+7] | — | 性质6 ($L$≠1,4 mod 6) |
| 6* | [0,$L$+3,2$L$+7] | — | 需证明 |
| 7 | [3,$L$+2,$L$+3] | (−3) [0,$L$−1,$L$] | 性质5($L$任意) |
| 8 | [3,$L$+2,2$L$+7] | (−3) [0,$L$−1,2$L$+4] | 性质6 ($L$≠1,4 mod 6) |
| 9 | [3,$L$+3,2$L$+7] | (−3) [0,$L$,2$L$+4] | 性质6 ($L$奇数) |
| 10 | [$L$+2,$L$+3,2$L$+7] | (−($L$+2)) [0,1,$L$+5] | 性质5($L$任意) |

## 4　性能仿真

本节对比新构造的QC-LDPC码与已知QC-LDPC码的译码性能. 以下用四个例子来考察新码知的译码性能,这四个例子覆盖了新提出的三种构造方法所对应的四种$L$取值情形. 仿真条件为AWGN信道,BPSK调制和SPA(Sum-Product Algorithm)译码(最多50次迭代).

为了衡量新码的性能,本文采用的对比基准QC-LDPC码包括:(1)文献[11]中的码;(2)基于行列随机选取的阵列码[1];(3)基于随机搜索的对称结构码[5]. 由于基准方法(2)的指数矩阵和新方法的指数矩阵都有很强结构,且基准方法(2)基于搜索,因此当$L$较大时基准方法(2)很难搜到符合围长条件的码. 此外,基准方法(1)在多数行重情况下得到的码都太长[11],无法与新码对比性能. 因此,在以下仿真对比中,仅在具有类似码长时采用基准方法(1),仅在$L$较小时采用基准方法(2). 由于基准方法(3)的指数矩阵结构性较弱,因此通过较长时间搜索都找到了与新码长度相同的对比码.

**例1**　(新构造方法1):选择$L$=9. 新构造方法1所定义的指数矩阵为$\boldsymbol{E}=[0,4,L+8,2L,2L+8]^{\mathrm{T}}[0,1,\cdots,L-$

1],循环块尺寸为 $P=L(L+4)=117$. 该指数矩阵和循环块尺寸定义了一个码长为 $PL=1\,053$、信息位长度为512、码率为512/1 053≈0.486(设计码率为0.444)、围长为8的(5,9)-规则码. 选择三种已有方法作为对比基准,分别是:(1)文献[11]中对应的码,其指数矩阵为 $\boldsymbol{E}=[0,2,L,2L+1,2L+2]^{\mathrm{T}}[0,1,\cdots,L-1]$、循环块尺寸 $P=2L^2-2L+1=145$;(2)基于行列随机选取的阵列码[1],其指数矩阵为 $\boldsymbol{E}=[15,37,73,82,104]^{\mathrm{T}}[19,33,36,39,73,79,84,88,113]$、循环块尺寸 $P=119$;(3)基于随机搜索的对称结构码[5],其循环块尺寸为117. 这三种对比基准码的围长都是8. 图1描绘了新码和三种已有码的误比特率(Bit Error Rate,BER)和误分组率(Block Error Rate,BLER)曲线. 由图1可见,新码的性能显著优于基准码(2)和基准码(3),也优于基准码(1). 需要指出的是,虽然基准码(1)比新码长很多,但是其性能却明显不如新码.

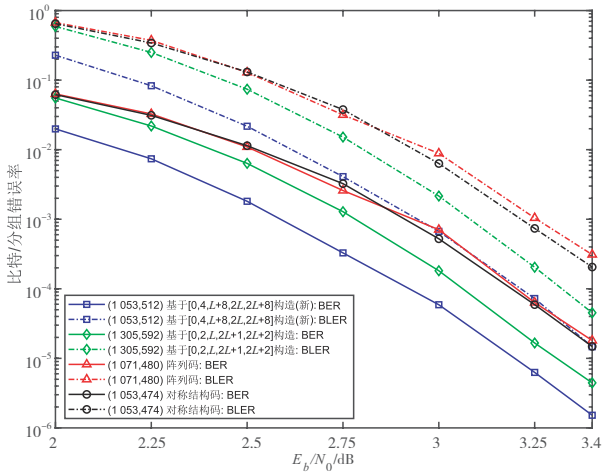


图1 新构造1与三种已有方法的译码性能对比($L=9$)

**例2** (新构造方法1):选择 $L=13$. 新构造方法1所定义的指数矩阵为 $\boldsymbol{E}=[0,4,L+8,2L,2L+8]^{\mathrm{T}}[0,1,\cdots,L-1]$,循环块尺寸为 $P=L(L+4)=221$. 该指数矩阵和循环块尺寸定义了一个码长为 $PL=2\,873$、信息位长度为1 828、码率为1 828/2 873≈0.636(设计码率为0.615)、围长为8的(5,13)-规则码. 为了进行性能对比,利用随机搜索构建了一个围长为8的对称结构码[5],该码的循环块尺寸也是221. 图2描绘了新码和对称结构码的BER和BLER曲线. 可见,新码的性能显著地优于对称结构码. 在图2中,新码还与一种基于有限域的码[15](记为LLLA码)进行了对比. 可见,新码的译码性能明显优于这种基于有限域的码. 该有限域码的具体参数为:GF(223),本原元 $a=3$,根据文献[15]所述方法随机产生两个以本原元为底的指数序列:$\boldsymbol{R}=[14,46,82,83,184]$ 和 $\boldsymbol{S}=[0,7,23,35,44,48,67,75,79,103,190,192,200]$. 最后,这两个序列根据规则 $a^{e(i,j)}=a^{r(i)}+a^{s(j)}$ 产生一个5行13列的指数矩阵 $\boldsymbol{E}$,而循环块尺寸为有限域的大小减1,即等于222.

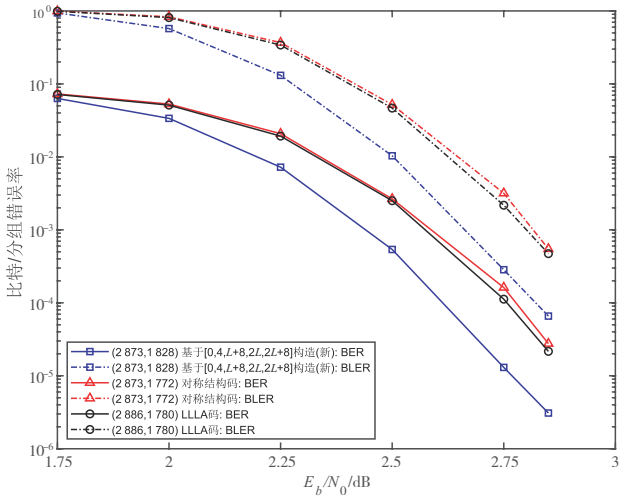


图2 新构造1与两种已有方法的译码性能对比($L=13$)

**例3** (新构造方法2):选择 $L=12$. 新构造方法2所定义的指数矩阵为 $\boldsymbol{E}=[0,1,L+2,L+5,2L+7]^{\mathrm{T}}[0,1,\cdots,L-1]$,循环块尺寸为 $P=L^2+4L+7=199$. 该指数矩阵和循环块尺寸定义了一个码长为 $PL=2\,388$、信息位长度为1 397、码率为1 397/2 388≈0.585(设计码率为0.583)、围长为8的(5,12)-规则码. 为作性能对比,采用随机搜索构建了一个围长为8的对称结构码[5],该码的循环块尺寸也是199. 图3描绘了新码和对称结构码的BER和BLER曲线. 可见,新码的性能与对称结构码几乎一致. 然而,与对称结构码相比,新码有两点优势:(1)新码的构造过程非常简单,不需要搜索;(2)新码的描述复杂度非常低,只需要6个参数(序列 $\boldsymbol{S}_2$ 中的5个数值和循环块尺寸 $P$),而对称结构码需要使用多达 $5L/2=30$ 个参数用于描述指数矩阵和一个参数指定循环块尺寸 $P$.

**例4** (新构造方法3):选择 $L=11$. 新构造方法3所定义的指数矩阵为 $\boldsymbol{E}=[0,3,L+2,L+3,2L+7]^{\mathrm{T}}[0,1,\cdots,L-1]$,循环块尺寸为 $P=(L+2)^2=169$. 该指数矩阵和循环块尺寸定义了一个码长为 $PL=1\,859$、信息位长度为1 042、码率为1 042/1 859≈0.561(设计码率为0.545)、围长为8的(5,11)-规则码. 为作性能对比,采用随机搜索构建了一个围长为8的对称结构码[5],该码的循环块尺寸也是169. 图4描绘了新码和对称结构码的BER和BLER曲线. 可见,新码的性能明显优于对称结构码. 为了说明较大列重的无小环QC-LDPC码可以结合掩膜(masking)技术获得性能更好的码,图4也描绘了新码和对称结构码分别与掩膜结合后的译码性能. 本例采用的掩膜矩阵是5行11列的0-1矩阵:$[\boldsymbol{g}^{(0)},\boldsymbol{g}^{(1)},\cdots,\boldsymbol{g}^{(4)},\boldsymbol{h}^{(0)},\boldsymbol{h}^{(1)},\cdots,\boldsymbol{h}^{(4)},\boldsymbol{g}^{(0)}]$,其中 $\boldsymbol{g}=[0\,0\,1\,1\,1]^{\mathrm{T}}$,$\boldsymbol{h}=[0\,1\,0\,1\,1]^{\mathrm{T}}$,$\boldsymbol{g}^{(i)}$ 表示

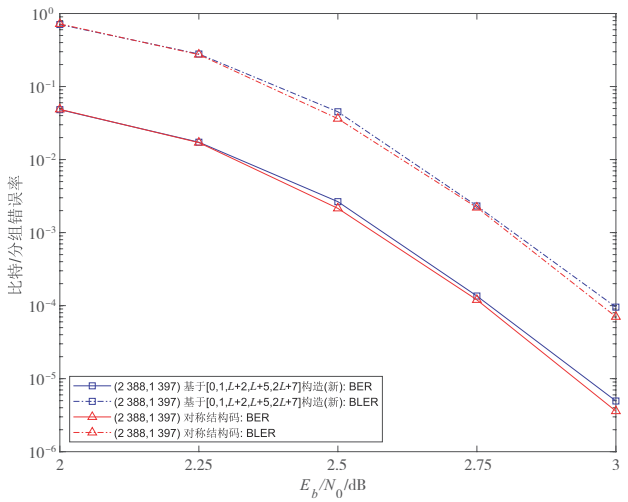


图3　新构造2与对称构造法的译码性能对比($L$=12)

对列向量$\boldsymbol{g}$向下循环移位$i$次. 由图4可见:(1)掩膜后码的性能与未掩膜码相比在BER=$1\times10^{-6}$时有超过0.5 dB的增益;(2)掩膜后的新码性能略优于掩码后的对称结构码. 同样地,与掩膜后的对称结构码相比,掩膜后的新码同样具有低描述复杂度和不需要搜索这两点优势.

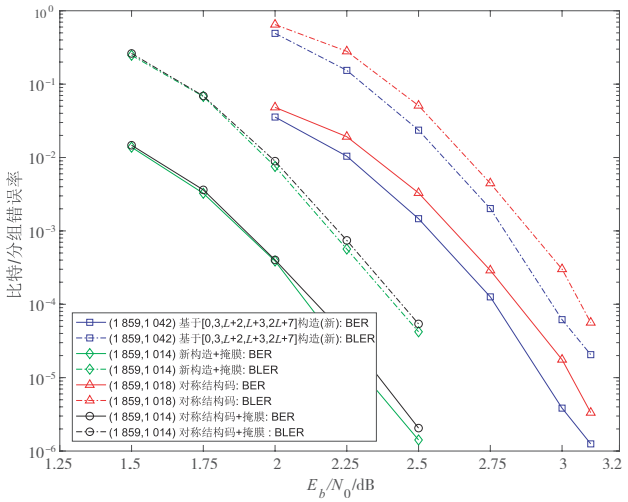


图4　新构造3与对称构造法(结合掩膜)的译码性能对比($L$=11)

## 5　结束语

本文针对列重为5的QC-LDPC短码,提出了三种围长为8的显式构造方法. 译码仿真表明:新码的性能等同于或明显优于现有的基于搜索的对称结构法. 新方法还有两个突出优点:(1)描述复杂度非常低;(2)不需要搜索过程,直接利用简单的数学公式即可直接定义围长为8的QC-LDPC码. 此外,本文利用新构造方法还得出了这类QC-LDPC码的最小循环块尺寸的新上界,仅约为目前最好上界的一半.

## 参考文献

[1] FOSSORIER M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices[J]. IEEE Transactions on Information Theory, 2004, 50(8): 1788-1793.

[2] KIM I, SONG H Y. Some new constructions of girth-8 QC-LDPC codes for future GNSS[J]. IEEE Communications Letters, 2021, 25(12): 3780-3784.

[3] VASIC B, PEDAGANI K, IVKOVIC M. High-rate girth-eight low-density parity-check codes on rectangular integer lattices[J]. IEEE Transactions on Communications, 2004, 52(8): 1248-1252.

[4] ZHANG G H, SUN R, WANG X M. Construction of girth-eight QC-LDPC codes from greatest common divisor[J]. IEEE Communications Letters, 2013, 17(2): 369-372.

[5] TASDIGHI A, BANIHASHEMI A H, SADEGHI M R. Symmetrical constructions for regular girth-8 QC-LDPC codes[J]. IEEE Transactions on Communications, 2017, 65 (1): 14-22.

[6] KHARIN A, DRYAKHLOV A, MIROKHIN E, et al. An approach to the generation of regular QC-LDPC codes with girth 8[C]//2020 9th Mediterranean Conference on Embedded Computing (MECO). Piscataway: IEEE, 2020: 1-4.

[7] ZHANG G H, SUN R, WANG X M. Several explicit constructions for (3, L) QC-LDPC codes with girth at least eight[J]. IEEE Communications Letters, 2013, 17(9): 1822-1825.

[8] 张国华, 孙蓉, 王新梅. 围长为8的QC-LDPC码的显式构造及其在CRT方法中的应用[J]. 通信学报, 2012, 33(3): 171-176.
ZHANG G H, SUN R, WANG X M. Explicit construction of girth-eight QC-LDPC codes and its application in CRT method[J]. Journal on Communications, 2012, 33(3): 171-176. (in Chinese)

[9] KARIMI M, BANIHASHEMI A H. On the girth of quasi-cyclic protograph LDPC codes[J]. IEEE Transactions on Information Theory, 2013, 59(7): 4542-4552.

[10] ZHANG J H, ZHANG G H. Deterministic girth-eight QC-LDPC codes with large column weight[J]. IEEE Communications Letters, 2014, 18(4): 656-659.

[11] WANG J H, ZHANG J H, ZHOU Q, et al. Full-length row-multiplier QC-LDPC codes with girth eight and short circulant sizes[J]. IEEE Access, 2023,11: 22250-22265.

[12] ZHANG Y, DA X Y. Construction of girth-eight QC-LDPC codes from arithmetic progression sequence with

large column weight[J]. Electronics Letters, 2015, 51(16): 1257-1259.

[13] 张轶, 达新宇, 苏一栋. 任意列重大围长QC-LDPC码的确定性构造[J]. 电子学报, 2016, 44(8): 1814-1819.
ZHANG Y, DA X Y, SU Y D. Deterministic construction of QC-LDPC codes for any column weight with a large girth[J]. Acta Electronica Sinica, 2016, 44(8): 1814-1819. (in Chinese)

[14] DERRIEN A, BOUTILLON E, CERQUEUS A. Additive, structural, and multiplicative transformations for the construction of quasi-cyclic LDPC matrices[J]. IEEE Transactions on Communications, 2019, 67(4): 2647-2659.

[15] LI J, LIU K, LIN S, et al. Quasi-cyclic LDPC codes on two arbitrary sets of a finite field[C]//2014 IEEE International Symposium on Information Theory. Piscataway: IEEE, 2014: 2454-2458.

## 作者简介

**张国华** 男, 1977年生于山西临汾. 博士, 研究员, 硕士生导师. 主要研究方向为信道编码.
E-mail: zhangghcast@163.com

**孙爱晶** 女, 1971年生于甘肃庆阳. 西安邮电大学通信与信息工程学院教授, 硕士生导师. 主要研究方向为物联网技术及应用.
E-mail: sunaijing@xupt.edu.cn

**倪孟迪** 女, 1999年生于四川成都. 西安邮电大学通信与信息工程学院硕士研究生, 主要研究方向为LDPC码的构造和译码.
E-mail: ni_mengdi@163.com

**方 毅** 男, 1986年生于浙江义乌. 博士, 广东工业大学信息工程学院教授, 博士生导师. 主要研究方向为面向通信与存储系统的信道编码. 中国电子学会会员编号: E190028682M.
E-mail: fangyi@gdut.edu.cn