围长为8的较大列重准循环低密度奇偶校验码的行重普适代数构造

张国华[①] 秦 煜[①] 娄蒙娟[①] 方 毅[*②]
[①](西安邮电大学 西安 710121)
[②](广东工业大学 广州 510006)

摘 要：适合于任意行重(即行重普适(RWU))的无小环准循环(QC)低密度奇偶校验(LDPC)短码，对于LDPC码的理论研究和工程应用具有重要意义。具有行重普适特性且消除4环6环的现有构造方法，只能针对列重为3和4的情况提供QC-LDPC短码。该文在最大公约数(GCD)框架的基础上，对于列重为5和6的情况，提出了3种具有行重普适特性且消除4环6环的构造方法。与现有的行重普适方法相比，新方法提供的码长从目前的与行重呈4次方关系锐减至与行重呈3次方关系，因而可以为QC-LDPC码的复合构造和高级优化等需要较大列重基础码的场合提供行重普适的无4环无6环短码。此外，与基于计算机搜索的对称结构QC-LDPC码相比，新码不仅无需搜索、描述复杂度更低，而且具有更好的译码性能。

关键词：低密度奇偶校验码；准循环；围长；最大公约数
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2024)07-3019-07
DOI: 10.11999/JEIT231111

Row-weight Universal Algebraic Constructions of Girth-8 Quasi-Cyclic Low-Density Parity-Check Codes with Large Column Weights

ZHANG Guohua[①] QIN Yu[①] LOU Mengjuan[①] FANG Yi[②]
[①](*Xi'an University of Posts and Telecommunications*, *Xi'an* 710121, *China*)
[②](*Guangdong University of Technology*, *Guangzhou* 510006, *China*)

Abstract: Short Quasi-Cyclic (QC) Low-Density Parity-Check (LDPC) codes without small cycles suitable for an arbitrary row weight (i.e., Row-Weight Universal (RWU)), are of great significance for both theoretical research and engineering application. Existing methods having RWU property and guaranteeing the nonexistence of 4-cycles and 6-cycles, can only offer short QC-LDPC codes for the column weights of 3 and 4. Based on the Greatest Common Divisor (GCD) framework, three new methods are proposed in this paper for the column weights of 5 and 6, which can possess RWU property and at the same time remove all 4-cycles and 6-cycles. Compared with existing methods with RWU property, the code lengths of the novel methods are sharply reduced from the fourth power of row weight to the third power of row weight. Therefore, the new methods can provide short RWU QC-LDPC codes without 4-cycles and 6-cycles for occasions where base codes with large column weights are required, such as composite constructions and advanced optimization pertaining to QC-LDPC codes. Moreover, compared with the search-based symmetric QC-LDPC codes, the new codes need no search, have lower description complexity, and exhibit better decoding performance.

Key words: Low-Density Parity-Check (LDPC) codes; Quasi-Cyclic(QC); Girth; Greatest Common Divisor (GCD)

收稿日期：2023-10-12；改回日期：2024-01-25；网络出版：2024-02-07
*通信作者： 方毅 fangyi@gdut.edu.cn
基金项目：国家自然科学基金(62322106, 62071131)，广东省国际科技合作项目(2022A0505050070)
Foundation Items: The National Natural Science Foundation of China (62322106, 62071131), International Collaborative Research Program of Guangdong Science and Technology Department (2022A0505050070)

1 引言

很长的低密度奇偶校验(Low-Density Parity-Check, LDPC) 码在迭代译码下的性能可以逼近理论极限。作为LDPC码的一个重要类别，准循环(Quasi-Cyclic, QC) LDPC码具有高度结构化的校验矩阵，大大简化了编码器和译码器的实现复杂性，因而在理论研究和工程实践中受到越来越多的关注[1–3]。目前，消除短环是使中等码长和短码长的QC-LDPC码具有优良译码性能的有效方法[4–6]。

消除QC-LDPC码的短环的方法大致可以分为两类：第1类是在一定策略下采用大规模遍历式或准遍历式搜索[7]，第2类是基于组合数学、数论等方法的确定性构造[8–11]。与依赖搜索的方法相比，确定性构造方法在具有相同或者更优译码能力的同时，还具有以下主要优势：(1)构建码的过程非常简单，不需要任何搜索过程[12,13]；(2)用于描述码校验矩阵的参数远远低于基于搜索的方法[14]；(3)通常适用于任何行重，可以提供搜索法无法获得的理论界限等深刻结论[15]；(4)作为基本模块，适合与其他方法(无论是确定性还是搜索方法)结合起来获得参数更灵活、性能更好的码[16]。

在空间遥控链路、卫星导航电文、无线传感网络、机器类通信等场合都需要使用短数据包，QC-LDPC短码可以为这些场合提供有力的数据可靠性保证。使用确定性方法构造无小环码的挑战主要在于如何使码长尽量短。目前，对于列重J为3[4,17]和4[16]的情况，人们已经提出了几种适用于任意行重L (称为行重普适)的短码长无小环码的确定性构造方法。然而，对于列重大于等于5的情况，目前仅有两种具有行重普适特性的确定性方法，它们提供的码长都很大。文献[18]对于列重为5和6的情况所能给出最小码长分别是$L[L^2(L-1)+1]$和$L[(L^2+1)(L-1)+1]$。列重为5时，文献[15]在行重为奇数和偶数时给出的最小码长分别是$L(3L^3/4+L^2/4-7L/4+7/4)$和$L(3L^3/4+L^2/4-2L+2)$；列重为6时，文献[15]在行重为奇数和偶数时给出的最小码长分别是$L(3L^3/4+L^2/4-3L/4+3/4)$和$L(3L^3/4+L^2/4-L+1)$。可见，无论列重为5还是6，现有两种方法的最小码长分别按L^4和$0.75\times L^4$规模变化。

本文在最大公约数(Greatest Common Divisor, GCD)框架[19]基础上，提供了3种具有行重普适性质的确定性构造方法。第1种可以构造出列重为5的无4环无6环的码，最小码长为$L[(3L+1)(L-1)+1]$；后两种可以构造出列重为6的无4环无6环的码，最小码长为$L[(4L+2)(L-1)+1]$。列重为5时，本文方法将原有的码长从L^4或$0.75\times L^4$的规模降到$3L^3$的规模；列重为6时，本文方法将原有的码长从L^4或$0.75\times L^4$的规模降低到$4L^3$的规模。因此，新的行重普适确定性方法可以显著地缩短现有同类方法所能提供的码长，为本领域的理论研究和工程实践提供高性能短码。

本文组织结构如下：第2节介绍了QC-LDPC码和GCD方法的基本概念与性质。第3节描述了本文的第1个新构造方法及理论性结果和规律性发现。第4节阐述了本文的第2个和第3个新构造方法及理论性结果和规律性发现。第5节通过仿真展示了所提3种新码的优秀译码性能。第6节总结全文。

2 QC-LDPC码的基本概念

(J,L)-LDPC码是一种具有稀疏校验矩阵的线性分组码，其校验矩阵每行有L个非零元素，每列有J个非零元素。(J,L)-QC-LDPC码是一类特殊的LDPC码，它的校验矩阵由一个$J\times L$的指数矩阵$\boldsymbol{E}$和循环块尺寸P共同确定，其中的循环块都是循环置换矩阵，循环块的每行都是前一行右移后的结果。具体来说，$\boldsymbol{E}$中的每个元素都对应一个$P\times P$的循环块，表示第1行中唯一非零元素出现的位置。LDPC码的环长是大于等于4的偶数。对于QC-LDPC码，利用$\boldsymbol{E}$可以有效地检测出长度为$2l$ (用“$2l$ 环”表示)的环[20]。围长(girth)是最短环的长度；因此，一个不含4环和6环的QC-LDPC码的围长至少为8。本文研究一类特殊的QC-LDPC码，其指数矩阵可以表示成$\boldsymbol{E}=\boldsymbol{S}_2^{\mathrm{T}}\cdot\boldsymbol{S}_1$，其中$\boldsymbol{S}_1=[0,1,\cdots,L-1]$，$\boldsymbol{S}_2$是一个含有$J$个元素的整数序列。根据GCD方法[21]可知：

引理1 设$\boldsymbol{S}_2=[a_0,a_1,\cdots,a_{J-1}]$，其中的$J$个整数依次递增。如果对所有3元组$[a_i,a_j,a_k]$不等式(GCD约束)$(a_k-a_i)/\gcd(a_k-a_i,a_j-a_i)\geq L$都成立，则对于任意$P\geq(a_{J-1}-a_0)(L-1)+1$，指数矩阵$\boldsymbol{E}$都可以生成围长为8的QC-LDPC码。

根据文献[5]的4环方程，引理2显然成立。

引理2 设a为任意正整数。若循环块尺寸$P\geq a(L-1)+1$，则$\boldsymbol{S}_2=[0,a]$对应的Tanner图无4环。

根据文献[5]的环路方程，以下关于序列$\boldsymbol{S}_2$的变换显然成立。

等价变换(S)：对于任意的循环块尺寸，序列$[a_0,a_1,\cdots,a_{n-1}]$和序列$[a_0-a_0,a_1-a_0,\cdots,a_{n-1}-a_0]$生成两个围长相同的QC-LDPC码。

等价变换(R)：对于任意的循环块尺寸，序列$[a_0,a_1,\cdots,a_{n-1}]$和序列$[a_{n-1}-a_{n-1},a_{n-1}-a_{n-2},\cdots,a_{n-1}-a_0]$生成两个围长相同的QC-LDPC码。

等价变换(D)：对于任意的循环块尺寸，序列

$[a_0,a_1,\cdots,a_{n-1}]$和序列$[xa_0,xa_1,\cdots,xa_{n-1}]$生成两个围长相同的QC-LDPC码，其中$x$是与$P$互素的任意正整数。

此外，以下引理可以简化本文证明过程。

引理3　设a和b是正整数，c是非负整数。若a,b和c满足$(L+c)|b$且$\gcd(a,L+c)=1$，则$\boldsymbol{S}_2=[0,a,b]$在循环块尺寸P满足$(L+c)|P$时所对应的Tanner图不含6环。

证明　设i,j,k是3个不同的整数，满足$0\le i,j,k\le L-1$。若$[0,a,b]$对应的6环存在，那么该环可表示为$(0-aj)+(ai-bi)+(bk-0)=0(\mathrm{mod}P)$，整理后得到$a(i-j)+b(k-i)=nx(L+c)$，其中$x$和$n$为某两个整数。由于$(L+c)|b$和$\gcd(a,L+c)=1$，因此$(L+c)|(i-j)$，这显然是不可能的。证毕。

3　列重为5时的新构造

新QC-LDPC码的构造思路如下。显然，$\boldsymbol{S}_2$包含J个整数。本文假设这J个整数满足3个条件：(1)每个整数可以写成$aL+b$的形式，其中a和b都是不超过某个门限值且与L无关的固定的非负整数；(2) J个整数依次递增，且第1个整数设定为0；(3)对于某个连续取值区间内的所有L，序列$\boldsymbol{S}_2$中任意3个依次递增的元素都满足GCD约束。

当门限设定为4时，本文发现一种新的构造方法，可以证明该方法适用于任意行重L。

定理1　取$\boldsymbol{S}_2=[0,2,2L+1,3L,3L+1]$。令$\boldsymbol{E}=\boldsymbol{S}_2^{\mathrm{T}}\cdot[0,1,\cdots,L-1]$，则$\boldsymbol{E}$在任意$P>(3L+1)(L-1)$时对应的Tanner图围长为8。

证明　$\boldsymbol{S}_2$共包括$(5\times4\times3)/(3\times2\times1)=10$个不同的3元组，如表1第2列所示。对原始3元组进行等价变换后得到表1第3列。表1最后一列表明了特定3元组的GCD指标。以情况7为例，原始3元组$[2,2L+1,3L]$利用等价变换(S)和等价变换(R)后可简化为$[0,L-1,3L-2]$，因此简化后的3元组表示为(S)(R)$[0,L-1,3L-2]$。GCD指标是指3元组$[a_i,a_j,a_k]$代入$(a_k-a_i)/\gcd(a_k-a_i,a_j-a_i)$后输出的值。由表1可知：所有3元组的GCD指标都不小于L，因此所有3元组都满足GCD约束。证毕。

由定理1可知，当循环块尺寸P大于$(3L+1)(L-1)$时，QC-LDPC码的Tanner图围长就可以达到8；但当循环块尺寸P不满足该条件时，围长就不能确保达到8了。尽管如此，通过计算机验证分析发现：以下规律对于$5\le L\le100$之间的任何L都是成立的。本文猜测这种规律对于任何L都成立。

规律1(a)　在如下的行重L和循环块尺寸P的组合下，定理1中$\boldsymbol{E}$对应的Tanner图的围长是8：

(1)$\mathrm{mod}(L,6)=0$时，$P=2L^2+4L$；
(2)$\mathrm{mod}(L,6)=1$时，$P=2L^2-L$；
(3)$\mathrm{mod}(L,6)=2$时，$P=2L^2$；
(4)$\mathrm{mod}(L,6)=3$时，$P=2L^2+L$；
(5)$\mathrm{mod}(L,6)=4$时，$P=2L^2+2L$；
(6)$\mathrm{mod}(L,6)=5$时，$P=2L^2+3L$。

特别地，以下性质1表明：规律1(a)中的情况(4)对于满足前提条件的所有L都是成立的。

性质1　对于任何满足$\mathrm{mod}(L,6)=3$的L，当$P=2L^2+L$时$\boldsymbol{E}$对应的Tanner图的围长是8。

证明　4环共有10种情况，如表2所示。利用等价性质(S)、等价性质(D)和引理2后，只剩3种情况需单独证明。其次，6环也共有10种情况，如表3所示。利用等价性质(S)、等价性质(R)、引理1和引理3后，也只剩3种情况需单独证明，具体证明方法与文献[20]类似，因篇幅所限略去。证毕。

更进一步地，通过计算机验证(由于计算量大，仅验证了$5\le L\le70$的所有L取值)发现：

规律1(b)　除了$L=5$之外，规律1(a)中的循环块尺寸是规律1(a)所述的指数矩阵和L取值条件下能够满足girth-8性质的最小循环块尺寸。

表 1　定理1中的新构造所涉及3元组及其GCD指标

序号	原始3元组	简化后的3元组	GCD指标
1	$[0,2,2L+1]$	-	$2L+1$
2	$[0,2,3L]$	-	$\ge3L/2$
3	$[0,2,3L+1]$	-	$\ge(3L+1)/2$
4	$[0,2L+1,3L]$	(R)$[0,L-1,3L]$	$\ge L$
5	$[0,2L+1,3L+1]$	(R)$[0,L,3L+1]$	$3L+1$
6	$[0,3L,3L+1]$	(R)$[0,1,3L+1]$	$3L+1$
7	$[2,2L+1,3L]$	(S)(R)$[0,L-1,3L-2]$	$3L-2$
8	$[2,2L+1,3L+1]$	(S)(R)$[0,L,3L-1]$	$3L-1$
9	$[2,3L,3L+1]$	(S)(R)$[0,1,3L-1]$	$3L-1$
10	$[2L+1,3L,3L+1]$	(S)(R)$[0,1,L]$	L

表 2　性质1所涉及的2元组及无4环的原因

序号	原始2元组	化简后的2元组	原因
1	$[0,2]$	-	引理2
2	$[0,2L+1]$	-	引理2
3*	$[0,3L]$	-	需证明
4	$[0,3L+1]$	(D)$[0,1]$	引理2
5	$[2,2L+1]$	(S)$[0,2L-1]$	引理2
6*	$[2,3L]$	(S)$[0,3L-2]$	需证明
7*	$[2,3L+1]$	(S)$[0,3L-1]$	需证明
8	$[2L+1,3L]$	(S)$[0,L-1]$	引理2
9	$[2L+1,3L+1]$	(S)$[0,L]$	引理2
10	$[3L,3L+1]$	(S)$[0,1]$	同序号4

例如，当$\mathrm{mod}(L,6)=0$时，使定理1中$\boldsymbol{E}$满足girth-8性质的最小循环块尺寸P恰好是$2L^2+4L$。本文猜测规律1(b)对于任何L都成立。

4 列重为6时的新构造

当列重$J=6$时仍将门限设定为4，本文找到了两种新的构造方法，它们同样适用于任意行重L。

定理2 取$\boldsymbol{S}_2=[0,1,2L,2L+2,4L+1,4L+2]$。令$\boldsymbol{E}=\boldsymbol{S}_2^{\mathrm{T}}\cdot[0,1,\cdots,L-1]$，则$\boldsymbol{E}$在任意$P>(4L+2)(L-1)$时对应的Tanner图围长为8。

证明 序列$\boldsymbol{S}_2$共包括$(6\times5\times4)/(3\times2\times1)=20$个不同的3元组，如表4中的第2列所示。对原始3元组进行等价变换后得到表4的第3列。表4最后一列表明了特定3元组的GCD指标。由表4可知：所有3元组的GCD指标都不小于L，因此所有3元组都满足GCD约束。 证毕。

定理2指出，当循环块尺寸P大于$(4L+2)(L-1)$时，QC-LDPC码的Tanner图围长达到8；当循环块尺寸P不满足这个关系时，围长就不能保证达到8了。但是，通过计算机验证分析发现：以下规律对于$6\le L\le100$之间的任何L都是成立的。本文猜测这种规律对于任何L都成立。

规律2(a) 在如下的行重L和循环块尺寸P的组合下，定理2中$\boldsymbol{E}$所对应的Tanner图的围长是8：

(1)$\mathrm{mod}(L,6)=0$时，$P=2L^2+2L$；

(2)$\mathrm{mod}(L,6)=1$时，$P=2L^2$；

(3)$\mathrm{mod}(L,6)=2$时，$P=2L^2+3L+3$；

(4)$\mathrm{mod}(L,6)=3$时，$P=2L^2+L+2$；

(5)$\mathrm{mod}(L,6)=4$时，$P=2L^2+2L$；

(6)$\mathrm{mod}(L,6)=5$时，$P=2L^2$。

特别地，以下性质2表明：规律2(a)中的情况(1)对于满足前提条件的所有L都是成立的。

性质2 对于任何满足$\mathrm{mod}(L,6)=0$的L，当$P=2L^2+2L$时$\boldsymbol{E}$对应的Tanner图的围长是8。

表 3 性质1所涉及的3元组及无6环的原因

序号	原始3元组	简化后的3元组	原因
1	$[0,2,2L+1]$	-	引理1
2	$[0,2,3L]$	-	引理3
3*	$[0,2,3L+1]$	-	需证明
4	$[0,2L+1,3L]$	(R)$[0,L-1,3L]$	引理3
5	$[0,2L+1,3L+1]$	(R)$[0,L,3L+1]$	引理3
6	$[0,3L,3L+1]$	(R)$[0,1,3L+1]$	引理3
7*	$[2,2L+1,3L]$	(S)(R)$[0,L-1,3L-2]$	需证明
8	$[2,2L+1,3L+1]$	(S)(R)$[0,L,3L-1]$	引理3
9*	$[2,3L,3L+1]$	(S)(R)$[0,1,3L-1]$	需证明
10	$[2L+1,3L,3L+1]$	(S)(R)$[0,1,L]$	引理1

表 4 定理2中的新构造所涉及3元组及其GCD指标

序号	原始3元组	化简后的3元组	GCD指标
1	$[0,1,2L]$	-	$2L$
2	$[0,1,2L+2]$	-	$2L+2$
3	$[0,1,4L+1]$	-	$4L+1$
4	$[0,1,4L+2]$	-	$4L+2$
5	$[0,2L,2L+2]$	(R)$[0,2,2L+2]$	$L+1$
6	$[0,2L,4L+1]$	-	$4L+1$
7	$[0,2L,4L+2]$	-	$2L+1$
8	$[0,2L+2,4L+1]$	(R)$[0,2L-1,4L+1]$	$\ge(4L+1)/3$
9	$[0,2L+2,4L+2]$	(R)$[0,2L,4L+2]$	同序号7
10	$[0,4L+1,4L+2]$	(R)$[0,1,4L+2]$	同序号4
11	$[1,2L,2L+2]$	(S)(R)$[0,2,2L+1]$	$2L+1$
12	$[1,2L,4L+1]$	(S)$[0,2L-1,4L]$	$4L$
13	$[1,2L,4L+2]$	(S)$[0,2L-1,4L+1]$	同序号8
14	$[1,2L+2,4L+1]$	(S)(R)$[0,2L-1,4L]$	同序号12
15	$[1,2L+2,4L+2]$	(S)(R)$[0,2L,4L+1]$	同序号6
16	$[1,4L+1,4L+2]$	(S)(R)$[0,1,4L+1]$	同序号3
17	$[2L,2L+2,4L+1]$	(S) $[0,2,2L+1]$	同序号11
18	$[2L,2L+2,4L+2]$	(S) $[0,2,2L+2]$	同序号5
19	$[2L,4L+1,4L+2]$	(S)(R)$[0,1,2L+2]$	同序号2
20	$[2L+2,4L+1,4L+2]$	(S)(R)$[0,1,2L]$	同序号1

证明 证明方法与性质1类似，略去。

更进一步地，通过计算机验证(在区间$6\le L\le70$内的所有L)发现：

规律2(b) 规律2(a)中的循环块尺寸是规律2(a)所述的指数矩阵和L取值条件下能够满足girth-8性质的最小循环块尺寸。

例如，当$\mathrm{mod}(L,6)=0$时，使定理2中$\boldsymbol{E}$满足girth-8性质的最小循环块尺寸P恰好是$2L^2+2L$。本文猜测规律2(b)对于任何L都成立。

定理3 取$\boldsymbol{S}_2=[0,L,L+1,3L+1,3L+2,4L+2]$。令$\boldsymbol{E}=\boldsymbol{S}_2^{\mathrm{T}}\cdot[0,1,\cdots,L-1]$，则$\boldsymbol{E}$在任意$P>(4L+2)(L-1)$时对应的Tanner图围长为8。

证明 序列$\boldsymbol{S}_2$共包括$(6\times5\times4)/(3\times2\times1)=20$个不同的3元组，如表5中的第2列所示。对原始3元组进行等价变换后得到表5的第3列。表5最后一列表明了特定3元组的GCD指标。由表5可知：所有3元组的GCD指标都不小于L，因此所有3元组都满足GCD约束。 证毕。

定理3指出，当循环块尺寸P大于$(4L+2)\cdot(L-1)$时，对应QC-LDPC码的Tanner图围长达到8；当循环块尺寸P不满足这个关系时，围长就不能保证达到8了。但是，通过计算机验证分析发现：以下规律对于$6\le L\le100$之间的任何L都是成立的。本文猜测这种规律对于任何L都成立。

表 5　定理3中的新构造所涉及3元组及其GCD指标

序号	原始3元组	化简后的3元组	GCD指标
1	$[0, L, L+1]$	(R)$[0, 1, L+1]$	$L+1$
2	$[0, L, 3L+1]$	-	$3L+1$
3	$[0, L, 3L+2]$	-	$\geq (3L+2)/2$
4	$[0, L, 4L+2]$	-	$\geq 2L+1$
5	$[0, L+1, 3L+1]$	-	$\geq (3L+1)/2$
6	$[0, L+1, 3L+2]$	-	$3L+2$
7	$[0, L+1, 4L+2]$	-	$\geq 2L+1$
8	$[0, 3L+1, 3L+2]$	(R)$[0, 1, 3L+2]$	$3L+2$
9	$[0, 3L+1, 4L+2]$	(R)$[0, L+1, 4L+2]$	同序号7
10	$[0, 3L+2, 4L+2]$	(R)$[0, L, 4L+2]$	同序号4
11	$[L, L+1, 3L+1]$	(S)$[0, 1, 2L+1]$	$2L+1$
12	$[L, L+1, 3L+2]$	(S)$[0, 1, 2L+2]$	$2L+2$
13	$[L, L+1, 4L+2]$	(S)$[0, 1, 3L+2]$	同序号8
14	$[L, 3L+1, 3L+2]$	(S)(R)$[0, 1, 2L+2]$	同序号12
15	$[L, 3L+1, 4L+2]$	(S)(R)$[0, L+1, 3L+2]$	同序号6
16	$[L, 3L+2, 4L+2]$	(S)(R)$[0, L, 3L+2]$	同序号3
17	$[L+1, 3L+1, 3L+2]$	(S)(R)$[0, 1, 2L+1]$	同序号11
18	$[L+1, 3L+1, 4L+2]$	(S)(R)$[0, L+1, 3L+1]$	同序号5
19	$[L+1, 3L+2, 4L+2]$	(S)(R)$[0, L, 3L+1]$	同序号2
20	$[3L+1, 3L+2, 4L+2]$	(S)$[0, 1, L+1]$	同序号1

规律3(a)　在如下的行重L和循环块尺寸P的组合下，定理3中$\boldsymbol{E}$所对应的Tanner图的围长是8：

(1a)$\mathrm{mod}(L,12)=0$时，$P=2L^2+5L/2+1$；

(1b)$\mathrm{mod}(L,12)=6$时，$P=2L^2+3L+1$；

(2)$\mathrm{mod}(L,6)=1$时，$P=2L^2+L$；

(3a)$\mathrm{mod}(L,12)=2$时，$P=2L^2+9L/2+2$；

(3b)$\mathrm{mod}(L,12)=8$时，$P=2L^2+5L+1$；

(4)$\mathrm{mod}(L,6)=3$时，$P=2L^2+3L$；

(5a)$\mathrm{mod}(L,12)=4$时，$P=2L^2+3L+1$；

(5b)$\mathrm{mod}(L,12)=10$时，$P=2L^2+L/2$；

(6)$\mathrm{mod}(L,6)=5$时，$P=2L^2+L$。

特别地，以下性质3表明：规律3(a)中的情况(1b)对于满足前提条件的所有L都是成立的。需要指出：规律3(a)情况(1b)中的L取值($\mathrm{mod}(L,12)=6$)是性质3中L取值($\mathrm{mod}(L,6)=0$)的特例。

性质3　对于任何满足$\mathrm{mod}(L,6)=0$的L，当$P=2L^2+3L+1$时$\boldsymbol{E}$对应Tanner图的围长是8。

证明　证明方法与性质1类似，略去。

更进一步地，通过计算机验证(在区间$6\leq L\leq 70$内的所有L)发现：

规律3(b)　规律3(a)中的循环块尺寸是规律3(a)所述的指数矩阵和L取值条件下能够满足girth-8性质的最小循环块尺寸。

例如，当$\mathrm{mod}(L,12)=0$时，使定理3中$\boldsymbol{E}$满足girth-8性质的最小循环块尺寸P恰好是$2L^2+5L/2+1$。本文猜测规律3(b)对于任何L都成立。

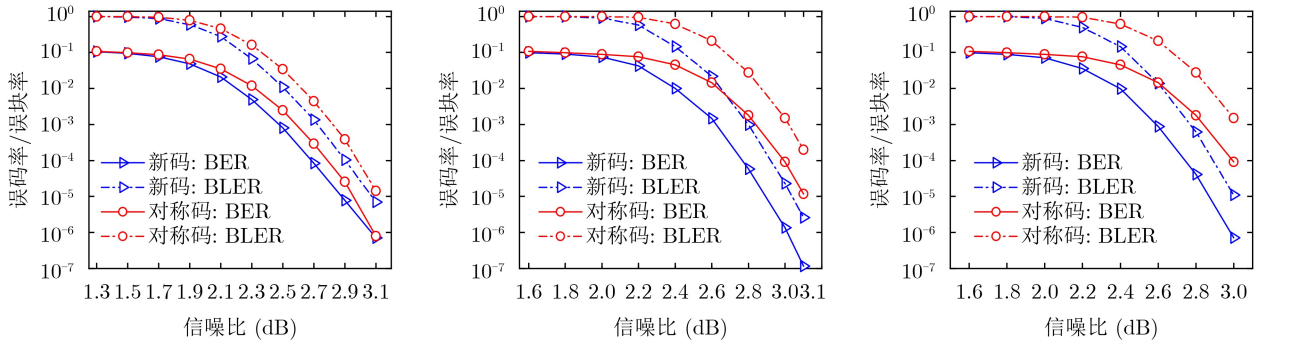
5　性能仿真

本节对第3节和第4节提出的新QC-LDPC码的性能进行仿真。仿真条件为：BPSK调制，AWGN信道、最大迭代次数为50的和积译码算法(Sum-Product Algorithm, SPA)。采用近期提出的基于搜索的对称结构girth-8 QC-LDPC码作为比对基准。

例1：令行重L为10。根据本文定理1，令$\boldsymbol{S}_2=[0,2,2L+1,3L,3L+1]$，设$\boldsymbol{E}_1=\boldsymbol{S}_2^{\mathrm{T}}\cdot[0,1,\cdots,9]$为构造的指数矩阵。根据规律1(a)(5)，该指数矩阵在循环块尺寸P为$2L^2+2L=220$时对应于一个围长为8的(5,10)-规则QC-LDPC码，记为C1，其码长为2 200，信息位长度为1 128，码率为0.512 7。在相同的循环块尺寸下，通过计算机搜索可以找到一个围长为8的(5,10)-规则QC-LDPC码，其指数矩阵(左右对称)的左半部分如式(1)所示，码长为2 200，信息位长度为1 104，码率为0.501 8。新码C1与已有的对称结构码的性能对比如图1(a)所示。由图1(a)可以看出：虽然新码C1的码率略高于对称结构码，但是在低信噪比区(小于3.1 dB)时新码C1的误码率和误块率性能仍然显著地优于现有的对称结构码。

$$\boldsymbol{E}_{\mathrm{SYM1}}=\begin{bmatrix}179&199&27&200&139\\21&61&120&210&212\\34&213&210&106&31\\92&211&144&7&186\\166&86&41&57&118\end{bmatrix}\tag{1}$$

例2：令行重L为12。根据本文定理2，令$\boldsymbol{S}_2=[0,1,2L,2L+2,4L+1,4L+2]$，设指数矩阵$\boldsymbol{E}_2=\boldsymbol{S}_2^{\mathrm{T}}\cdot[0,1,\cdots,11]$。可以验证，该指数矩阵在循环块尺寸$P$为$2L^2+3L+1=325$时对应于一个围长为8的(6,12)-规则QC-LDPC码，记为C2，其码长为3 900，信息位长度为2 051，码率为0.525 9。类似地，根据本文定理3，令$\boldsymbol{S}_2=[0,L,L+1,3L+1,3L+2,4L+2]$，设指数矩阵$\boldsymbol{E}_3=\boldsymbol{S}_2^{\mathrm{T}}\cdot[0,1,\cdots,11]$。可以验证，该指数矩阵在相同的循环块尺寸下也对应于一个围长为8的(6,12)-规则QC-LDPC码，记为C3，其码长为3 900，信息位长度为2 063，码率为0.528 9。在相同的循环块尺寸下，通过计算机搜索可以找到一个围长为8的(6,12)-规则QC-LDPC码，其指数矩阵(左右对称)的左半部分如式(2)所示，码长为3 900，信息位长度为1 955，码率为0.501 3。新码C2、新码C3与已有的对称结构码的性能对比



(a) 新码C1与对称结构码的译码性能对比 (b) 新码C2与对称结构码的译码性能对比 (c) 新码C3与对称结构码的译码性能对比

图 1 新码与对称结构码的译码性能对比

分别如图1(b)和图1(c)所示。由图1(b)和图1(c)可以看出：虽然新码C2和新码C3的码率略高于对称结构码，但是新码C2和新码C3的误码率和误块率性能仍然显著地优于现有的对称结构码。

$$\boldsymbol{E}_{\mathrm{SYM2}}=\begin{bmatrix}205&31&90&177&311&313\\51&315&311&157&260&46\\137&297&257&311&213&303\\246&241&127&55&89&15\\31&308&244&45&81&48\\214&210&264&1&288&268\end{bmatrix} \tag{2}$$

若不考虑指数矩阵的结构特征，在行重和列重相同的情况下，新码与对称结构等现有QC-LDPC码具有相同的编译码复杂度。但是，与对称结构码相比，新码具有更强的结构特征，因此新码在降低编译码复杂度上有更大潜力。如何具体地利用这种结构特征来降低复杂度，有待进一步深入研究。

6 结论

本文基于GCD方法提出了3种围长为8的QC-LDPC码。3种新码适用于任意行重L，比现有的适于任意L的构造方法可以提供更小的循环块尺寸。与基于搜索的对称结构girth-8 QC-LDPC码相比，新码有3个优点：(1)只需描述$\boldsymbol{S}_2$序列的J个整数即可完全确定指数矩阵，因此具有更低的描述复杂度；(2)构造过程完全代数化，不需要任何搜索过程；(3)在AWGN信道下具有更好的译码性能。

参 考 文 献

[1] ZHANG Lintao and WANG Juhua. Construction of QC-LDPC codes from Sidon sequence using permutation and segmentation[J]. *IEEE Communications Letters*, 2022, 26(8): 1710–1714. doi: 10.1109/LCOMM.2022.3177511.

[2] AMIRZADE F, SADEGHI M R, and PANARIO D. Construction of protograph-based LDPC codes with chordless short cycles[J]. *IEEE Transactions on Information Theory*, 2024, 70(1): 51–74. doi: 10.1109/TIT.2023.3307583.

[3] SMARANDACHE R and MITCHELL D G M. A unifying framework to construct QC-LDPC Tanner graphs of desired girth[J]. *IEEE Transactions on Information Theory*, 2022, 68(9): 5802–5822. doi: 10.1109/TIT.2022.3170331.

[4] VASIC B, PEDAGANI K, and 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. doi: 10.1109/TCOMM.2004.833037.

[5] FOSSORIER M P C. Quasic-cyclic low-density parity-check codes from circulant permutation matrices[J]. *IEEE Transactions on Information Theory*, 2004, 50(8): 1788–1793. doi: 10.1109/TIT.2004.831841.

[6] BOCHAROVA I E, KUDRYASHOV B D, OVSYANNIKOV E P, *et al*. Design and analysis of NB QC-LDPC codes over small alphabets[J]. *IEEE Transactions on Communications*, 2022, 70(5): 2964–2976. doi: 10.1109/TCOMM.2022.3160176.

[7] TASDIGHI A, BANIHASHEMI A H, and SADEGHI M R. Symmetrical constructions for regular girth-8 QC-LDPC codes[J]. *IEEE Transactions on Communications*, 2017, 65(1): 14–22. doi: 10.1109/TCOMM.2016.2617335.

[8] 张国华, 王新梅. 围长至少为8的QC-LDPC码的新构造: 一种显式框架[J]. 电子学报, 2012, 40(2): 331–337. doi: 10.3969/j.issn.0372-2112.2012.02.020.

ZHANG Guohua and WANG Xinmei. Novel constructions of QC-LDPC codes with girth at least eight: an explicit framework[J]. *Acta Electronica Sinica*, 2012, 40(2): 331–337. doi: 10.3969/j.issn.0372-2112.2012.02.020.

[9] ZHANG Jianhua and ZHANG Guohua. Deterministic girth-eight QC-LDPC codes with large column weight[J]. *IEEE Communications Letters*, 2014, 18(4): 656–659. doi: 10.1109/LCOMM.2014.030114.132853.

[10] MAJDZADE M and GHOLAMI M. On the class of high-rate QC-LDPC codes with girth 8 from sequences satisfied in GCD condition[J]. *IEEE Communications Letters*, 2020, 24(7): 1391–1394. doi: 10.1109/LCOMM.2020.2983019.

[11] TAO Xiongfei, CHEN Xin, and WANG Bifang. On the

construction of QC-LDPC codes based on integer sequence with low error floor[J]. *IEEE Communications Letters*, 2022, 26(10): 2267–2271. doi: 10.1109/LCOMM.2022.3187435.

[12] 张轶, 达新宇, 苏一栋. 利用等差数列构造大围长准循环低密度奇偶校验码[J]. 电子与信息学报, 2015, 37(2): 394–398. doi: 10.11999/JEIT140538.
ZHANG Yi, DA Xinyu, and SU Yidong. Construction of quasi-cyclic low-density parity-check codes with a large girth based on arithmetic progression[J]. *Journal of Electronics & Information Technology*, 2015, 37(2): 394–398. doi: 10.11999/JEIT140538.

[13] 张国华, 陈超, 杨洋, 等. Girth-8 (3, L)-规则QC-LDPC码的一种确定性构造方法[J]. 电子与信息学报, 2010, 32(5): 1152–1156. doi: 10.3724/SP.J.1146.2009.00838.
ZHANG Guohua, CHEN Chao, YANG Yang, *et al*. Girth-8 (3, L)-regular QC-LDPC codes based on novel deterministic design technique[J]. *Journal of Electronics & Information Technology*, 2010, 32(5): 1152–1156. doi: 10.3724/SP.J.1146.2009.00838.

[14] ZHANG Guohua, HU Yulin, FANG Yi, *et al*. Relation between GCD constraint and full-length row-multiplier QC-LDPC codes with girth eight[J]. *IEEE Communications Letters*, 2021, 25(9): 2820–2823. doi: 10.1109/LCOMM.2021.3096386.

[15] ZHANG Yi and DA Xinyu. Construction of girth-eight QC-LDPC codes from arithmetic progression sequence with large column weight[J]. *Electronics Letters*, 2015, 51(16): 1257–1259. doi: 10.1049/el.2015.0389.

[16] 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. doi: 1000-436X(2012)03-0171-06.
ZHANG Guohua, SUN Rong, and WANG Xinmei. Explicit construction of girth-eight QC-LDPC codes and its application in CRT method[J]. *Journal on Communications*, 2012, 33(3): 171–176. doi: 1000-436X(2012)03-0171-06.

[17] ZHANG Guohua, SUN Rong, and WANG Xinmei. Several explicit constructions for (3, L) QC-LDPC codes with girth at least eight[J]. *IEEE Communications Letters*, 2013, 17(9): 1822–1825. doi: 10.1109/LCOMM.2013.070913.130966.

[18] KARIMI M and BANIHASHEMI A H. On the girth of quasi-cyclic protograph LDPC codes[J]. *IEEE Transactions on Information Theory*, 2013, 59(7): 4542–4552. doi: 10.1109/TIT.2013.2251395.

[19] ZHANG Guohua, SUN Rong, and WANG Xinmei. Construction of girth-eight QC-LDPC codes from greatest common divisor[J]. *IEEE Communications Letters*, 2013, 17(2): 369–372. doi: 10.1109/LCOMM.2012.122012.122292.

[20] WANG Juhua, ZHANG Jianhua, ZHOU Quan, *et al*. Full-length row-multiplier QC-LDPC codes with girth eight and short circulant sizes[J]. *IEEE Access*, 2023, 11: 22250–22265. doi: 10.1109/ACCESS.2023.3249464.

[21] ZHANG Guohua, FANG Yi, and LIU Yuanhua. Automatic verification of GCD constraint for construction of girth-eight QC-LDPC codes[J]. *IEEE Communications Letters*, 2019, 23(9): 1453–1456. doi: 10.1109/LCOMM.2019.2925792.

张国华：男，研究员，研究方向为信道编码理论与应用.
秦　煜：男，硕士生，研究方向为LDPC码的构造方法.
娄蒙娟：女，硕士生，研究方向为LDPC码的构造方法.
方　毅：男，教授，研究方向为通信与存储系统中的信道编码.

责任编辑：余　蓉