围长至少为 8 的 QC-LDPC 码的新构造：一种显式框架

张国华[1,2]，王新梅[1]
（1.西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西西安 710071；
2.中国空间技术研究院西安分院，陕西西安 710100）

摘 要： 构造围长较大的校验矩阵，是提高二进制和多进制 QC-LDPC 码译码性能的一种有效手段.本文提出一种不需要借助于任何计算机搜索步骤，能够直接构造出围长至少为 8 的 QC-LDPC 码的显式构造框架.该框架所构造的 QC-LDPC 码不仅满足围长至少为 8 的条件，而且还具有循环置换矩阵（CPM）尺寸可以连续变化的优点.该框架可以分为两个步骤：第一步是在无穷大 CPM 尺寸条件下利用确定性方法构造一个围长至少为 8 的校验矩阵；第二步是根据本文新发现的一个围长性质，从该校验矩阵的移位矩阵直接精确地计算出 CPM 尺寸连续变化的紧致下界.

关键词： 低密度奇偶校验码；准循环；围长；显式构造
中图分类号： TN911.22 **文献标识码：** A **文章编号：** 0372-2112 (2012)02-0331-07
电子学报 URL： http://www.ejournal.org.cn **DOI：** 10.3969/j.issn.0372-2112.2012.02.020

Novel Constructions of QC-LDPC Codes with Girth at Least Eight: An Explicit Framework

ZHANG Guo-hua[1,2], WANG Xin-mei[1]
(1. *State Key Lab of Integrated Service Networks, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *China Academy of Space Technology (Xi'an), Xi'an, Shaanxi* 710100, *China*)

Abstract: Enabling the parity-check matrices to have a large girth is an efficient method to improve the decoding performance for many binary and non-binary QC-LDPC codes. A new explicit framework to construct QC-LDPC codes with girth at least eight is proposed, without any computer search procedures. The QC-LDPC codes constructed by the framework not only have a girth at least eight, but also possess an advantage of consecutive cyclic permutation matrix (CPM) sizes. The framework includes two steps: first, a parity-check matrix is explicitly constructed with a girth at least eight under an infinite CPM size; second, the tight lower bound of consecutive CPM sizes is precisely calculated directly from the corresponding shift matrix of the parity-check matrix, by employing a new girth property discovered by this paper.

Key words: low-density parity-check (LDPC) codes; quasi-cyclic (QC); girth; explicit construction

1 引言

使 Tanner 图具有较大的围长，是提高二进制和多进制 QC-LDPC 码译码性能的一个有效途径[1~19].目前，围长至少 8 的 QC-LDPC 码的设计方法主要有三类.第一类是基于计算机搜索或检测的方法，例如平衡环路[4]、控制方程[6]、循环差族[9]、爬山算法[10]、有限域和欧氏几何[14]、二维网格[15]、有限多项式环[16]、列差[17]、超图[18]等.这类方法将构造问题转变为受若干约束条件限制的计算机搜索或检测算法，可以比较灵活地获得满足各种约束条件的码型.但是，这类方法存在两个不足：第一，计算机搜索所花费的时间通常较长；第二，由于没有研究存在性问题，算法存在失败的可能性（即始终无法找到满足约束条件的可行解）.第二类是完全确定性的方法，例如最早序列[2]、群结构[5]、Hoey 序列[7]、三维循环网格[11]、文献[12,13]提出的两种方法、文献[20,21]提出的两种方法.这类方法可以用显式方式直接构造出校验矩阵，并且其围长特性已经过严格的理论证明.这

收稿日期：2011-03-25；修回日期：2011-10-14
基金项目：国家 973 重点基础研究发展计划（No.2010CB328300）；国家自然科学基金（No.U0635003，No.61001131）；高等学校学科创新引智计划（No.B08038）

类方法不需要任何计算机搜索操作,也不存在构造失败的可能性.第三类是大围长 QC-LDPC 码构造的一些通用理论:例如基于中国剩余定理的方法[3]、一种适用于围长至少为 8 的 QC-LDPC 码的行重扩展方法[8]、基于部分积的方法[19]、码长连续取值的下界[22,23]等.利用这类方法可以在已知码的基础上非常简单地构造出新码.由于发现第二类和第三类方法的难度比较大,因此目前属于这两类方法的具体成果还较为罕见.

本文的研究对象是第二类方法.在第二类方法中,群结构法[5]可以构造围长为 12 的 QC-LDPC 码,但是列重只能为 3,行重只能为 5;Hoey 序列[7]可以构造出围长为 12 的 QC-LDPC 码,但是列重只能为 2;三维循环网格方法[11]可以构造围长为 8 和 10 的 QC-LDPC 码,但是列重只能为 3,行重只能为素数.这在一定程度上限制了它们的实际应用。本文对围长限定为"至少为 8",在这种条件下人们已经发现了一些行重可以任意取值,列重可以为 3[2,12,20]也可以为 4[13,21]的确定性构造方法.

本文的创新点是:提出了一种构造围长至少为 8 的 QC-LDPC 码的显式构造框架.不同与已有的具体构造方法,该框架的显著优点是提供了构造围长至少为 8 的 QC-LDPC 码的一个系统化方法:通过不同的参数配置,该框架在原则上可以演变出无数种具体的构造方法.作为例子,我们从该框架非常简洁地推导出了第二类方法中的四种已有方法[12,13,20,21],并极大地简化了原有方法各自非常复杂的围长性质证明.该框架还自然地推导出了两种已知方法[12,13]所没有发现的新围长性质.此外,应用该框架我们还推导出一种构造围长至少为 8 的 QC-LDPC 码的新确定性方法;进一步的理论分析表明,这种新方法所构造的 QC-LDPC 码的围长事实上至少为 10.

2 新提出的显式构造框架

根据文献[1],(J,L) QC-LDPC 码的校验矩阵可以规范化地表示为:

$$\boldsymbol{H}(X)=\begin{bmatrix}\boldsymbol{I}(0) & \boldsymbol{I}(0) & \cdots & \boldsymbol{I}(0)\\ \boldsymbol{I}(0) & \boldsymbol{I}(p_{1,1}) & \cdots & \boldsymbol{I}(p_{1,L-1})\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{I}(0) & \boldsymbol{I}(p_{J-1,1}) & \cdots & \boldsymbol{I}(p_{J-1,L-1})\end{bmatrix} \tag{1}$$

其中,J 和 L 分别为校验矩阵的列重和行重,$\boldsymbol{I}(p)$是受移位值 p 控制的一个 $X\times X$ 的循环置换矩阵(CPM),具体定义见文献[1].与 $\boldsymbol{H}(X)$对应的移位矩阵 $\boldsymbol{S}_H(X)$可以表示为:

$$\boldsymbol{S}_H(X)=\begin{bmatrix}0 & 0 & \cdots & 0\\ 0 & p_{1,1} & \cdots & p_{1,L-1}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & p_{J-1,1} & \cdots & p_{J-1,L-1}\end{bmatrix} \tag{2}$$

2.1 CPM 尺寸无穷大时一种围长至少为 8 的校验矩阵

在构造大围长 QC-LDPC 码时,已有方法通常都是在特定的有限 CPM 尺寸 X 下,利用文献[1]中的模 X 等式来检测校验矩阵中是否会出现某个长度的环,当所有模 X 等式都不成立时就找到了满足围长条件的校验矩阵.本节将采取一种明显不同的方式来构造校验矩阵:先假定 CPM 尺寸为无穷大(即 $X=\infty$),然后构造出满足围长条件的移位矩阵,最后通过理论分析的方法得出该移位矩阵所适用的 CPM 尺寸范围.

在 $X=\infty$时构造移位矩阵有两个好处:第一,文献[1]中的模 P 等式可以转变为通常意义下的一般等式;在本节引理 1 的证明中可以看到,这样做有助于得到具有较强理论价值的结果.第二,一般等式成立时模 X 等式必然成立,反之则不然;所以,$X=\infty$时选择较小的移位值就可以破坏等式的成立条件,我们举一个例子来说明这一点的重要作用.假设 $J=3$ 且移位矩阵 $\boldsymbol{S}_H(X)$的第 2 行移位值是第 1 行移位值的 3 倍.当 $X=1213$ 时文献[6]根据围长为 12 的条件,采用贪婪搜索得到了第 1 行的前 7 个移位值:0,1,7,29,96,148,324。在 $X=\infty$时我们采用同样的方法得到了第 1 行前 7 个移位值:0,1,7,29,96,148,261.可见,$X=\infty$时 $p_{1,6}=261$ 比 $X=1213$ 时 $p_{1,6}=324$ 要小很多.根据文献[23]可知:采用第一种移位矩阵时,对于任意 $X>648$ 得到的(3,7)QC-LDPC 码的围长都为 12;而采用第二种移位矩阵时,对于任意 $X>522$ 得到的(3,7)QC-LDPC 码的围长都为 12.这说明:$X=\infty$时可以设计出 CPM 连续取值范围更大的大围长 QC-LDPC 码.

下面开始本节的主要内容.我们研究一种特殊类型的移位矩阵:该移位矩阵为 4 行 L 列,且第 3 行移位值为第 1、2 行移位值之和,如式(3)所示.

$$\boldsymbol{S}(X)=\begin{bmatrix}0 & 0 & \cdots & 0\\ 0 & p_{1,1} & \cdots & p_{1,L-1}\\ 0 & p_{2,1} & \cdots & p_{2,L-1}\\ 0 & p_{1,1}+p_{2,1} & \cdots & p_{1,L-1}+p_{2,L-1}\end{bmatrix} \tag{3}$$

为了便于分析 $\boldsymbol{S}(X)$的围长性质,引入定义 1.

定义 1 $\boldsymbol{S}(X;i,j,k)$为 $\boldsymbol{S}(X)$的第 i,j,k 行$(0\leqslant i,j,k\leqslant 3)$所构成的移位矩阵.

本文新提出的显式构造框架的第一个步骤,建立在引理 1 的基础上.

引理 1 假设 $p_{1,1},p_{1,2},\cdots,p_{1,L-1}$是严格递增的 $L-1$ 个正整数,且对于任意 $1\leqslant n\leqslant L-1$,$p_{2,n}\geqslant p_{2,n-1}+1+\max\{p_{1,n},p_{1,L-1}-p_{1,n-1}\}$,则 $\boldsymbol{S}(\infty;0,1,2)$的围长至少为 8.

证明 根据引理 1 的题设条件,显然 $\boldsymbol{S}(\infty;0,1,2)$

中不含 4 – 环.下面证明 $\boldsymbol{S}(\infty;0,1,2)$中不含 6 – 环.设 r,s,t 满足 $0\leqslant r,s,t<L;r\neq s,s\neq t,r>t$.则 $S(\infty;0,1,2)$中可能出现的 6 – 环模式只有图 1 所示的两种.

①若 $\boldsymbol{S}(\infty;0,1,2)$中包含图 1 模式 a 所示的 6-环,则 $p_{1,r}-p_{2,r}+p_{2,t}-0+0-p_{1,s}=0$,即 $p_{2,r}-p_{2,t}=p_{1,r}-p_{1,s}$.而 $p_{2,r}-p_{2,t}\geqslant 1+\max\{p_{1,r},p_{1,L-1}-p_{1,t}\}\geqslant 1+p_{1,r}>p_{1,r}-p_{1,s}$.矛盾.

②若 $\boldsymbol{S}(\infty;0,1,2)$中包含图 1 模式 b 所示的 6-环,则 $0-p_{2,r}+p_{2,t}-p_{1,t}+p_{1,s}-0=0$,即 $p_{2,r}-p_{2,t}=p_{1,s}-p_{1,t}$.而 $p_{2,r}-p_{2,t}\geqslant 1+\max\{p_{1,r},p_{1,L-1}-p_{1,t}\}\geqslant 1+p_{1,L-1}-p_{1,t}>p_{1,s}-p_{1,t}$.矛盾.

我们发现,无论 X 是一个有限正整数还是无穷大,$\boldsymbol{S}(X)$中 6-环的出现都存在引理 2 描述的规律性.

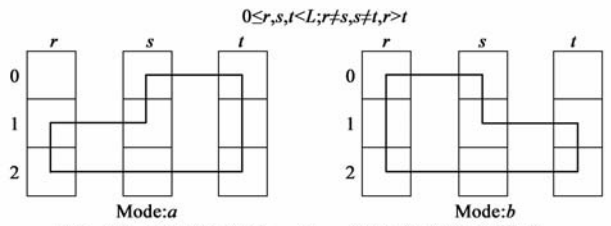


图1　$S(\infty;0,1,2)$中经过$p_{2,r}$和$p_{2,t}$的两种可能6-环模式

引理 2　若 $\boldsymbol{S}(X;0,1,2)$无 6-环,则 $\boldsymbol{S}(X;1,2,3)$也无 6-环;若 $S(X;0,1,3)$无 6-环,则 $\boldsymbol{S}(X;0,2,3)$也无 6-环.

证明　设 r,s,t 满足 $0\leqslant r,s,t<L;r\neq s,s\neq t,t\neq r$.

①若 $\boldsymbol{S}(X;1,2,3)$存在 6-环,则存在 3 个整数 r,s,t 满足 $p_{2,r}-p_{3,r}+p_{3,t}-p_{1,t}+p_{1,s}-p_{2,s}\equiv 0(\bmod X)$.由于第 3 行移位值是第 1、2 行移位值之和,所以有 $0-p_{1,r}+p_{1,s}-p_{2,s}+p_{2,t}-0\equiv 0(\bmod X)$,这说明 $S(X;0,1,2)$存在 6-环.与题设矛盾.

②若 $\boldsymbol{S}(X;0,2,3)$存在 6-环,则存在 3 个整数 r,s,t 满足 $p_{2,r}-p_{3,r}+p_{3,t}-0+0-p_{2,s}\equiv 0(\bmod X)$.由于第 3 行移位值是第 1、2 行移位值之和,所以有 $0-p_{1,r}+p_{1,s}-p_{3,s}+p_{3,t}-0\equiv 0(\bmod X)$,这说明 $S(X;0,1,3)$存在 6-环.与题设矛盾.

由引理 1、2 立即可得定理 1.

定理 1　假设 $p_{1,1},p_{1,2},\cdots,p_{1,L-1}$是严格递增的 $L-1$ 个正整数,且对于任意 $1\leqslant n\leqslant L-1$ $p_{2,n}\geqslant p_{2,n-1}+1+\max\{p_{1,n},p_{1,L-1}-p_{1,n-1}\}$,则 $\mathrm{girth}(S(\infty))\geqslant 8$.

定理 1 充分概括了本文新提出的显式构造框架第一个步骤的方法和结果.根据定理 1,可以在无穷大 CPM 尺寸条件下以完全确定的方式构造一个围长至少为 8、列重为 4 行重为 L 的校验矩阵.

2.2　CPM 尺寸连续变化的紧致下界

CPM 尺寸可以连续变化的 QC-LDPC 码,对于自适应链路系统具有较大的应用价值[16],对于大围长 QC-LDPC 码的存在性和基于中国剩余定理的大围长 QC-LDPC 码构造等问题都具有较重要的理论价值[22].

本节设 $J\geqslant 3$.为研究 CPM 尺寸连续变化问题的方便,本节考察 QC-LDPC 码校验矩阵的非规范化形式,如式(4)所示.式(1)描述的规范化形式是式(4)的特例.

$$\boldsymbol{H}'(X)=\begin{bmatrix}\boldsymbol{I}(p_{0,0}) & \boldsymbol{I}(p_{0,1}) & \cdots & \boldsymbol{I}(p_{0,L-1})\\ \boldsymbol{I}(p_{1,0}) & \boldsymbol{I}(p_{1,1}) & \cdots & \boldsymbol{I}(p_{1,L-1})\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{I}(p_{J-1,0}) & \boldsymbol{I}(p_{J-1,1}) & \cdots & \boldsymbol{I}(p_{J-1,L-1})\end{bmatrix}\tag{4}$$

与 $\boldsymbol{H}'(X)$对应的移位矩阵可以表示为

$$\boldsymbol{U}(X)=\begin{bmatrix}p_{0,0} & p_{0,1} & \cdots & p_{0,L-1}\\ p_{1,0} & p_{1,1} & \cdots & p_{1,L-1}\\ \vdots & \vdots & \ddots & \vdots\\ p_{J-1,0} & p_{J-1,1} & \cdots & p_{J-1,L-1}\end{bmatrix}\tag{5}$$

给定一个围长至少为 10 的$(3,L)$ QC-LDPC 码,人们研究了(移位矩阵不变,围长至少为 10 时)CPM 尺寸连续变化的下界[16,22].那么,给定一个围长至少为 8 的 QC-LDPC 码,(移位矩阵不变,围长至少为 8 时)是否也存在 CPM 尺寸连续变化的下界?我们使用数学语言将该问题归结为:

问题 1　假设 $\mathrm{girth}(\boldsymbol{U}(\infty))\geqslant 8$.问:满足条件"对于任意 $X\geqslant Q$ 均有 $\mathrm{girth}(\boldsymbol{U}(X))\geqslant 8$"的最小 Q 值是多少?

为了研究问题 1,引入定义 2 和定义 3.

定义 2　对于 $0\leqslant J_1<J$ 和 $0\leqslant J_2<J(J_1\neq J_2)$,定义第 J_1 行与第 J_2 行的差向量为

$$D_{J_1,J_2}:=\{p_{J_1,0}-p_{J_2,0},p_{J_1,1}-p_{J_2,1},\cdots,p_{J_1,L-1}-p_{J_2,L-1}\}\tag{6}$$

令 $0\leqslant i<j<k<J;0\leqslant r,s,t<L(r\neq s,s\neq t,t\neq r)$.在定义 2 基础上引入 3 个符号.

定义 3　$T_{i,j,k}:=\max(D_{i,j})+\max(D_{j,k})+\max(D_{k,i})$,$T'_{i,j,k}:=\max(D_{j,i})+\max(D_{k,j})+\max(D_{i,k})$,$Q_{i,j,k}:=\max(T_{i,j,k},T'_{i,j,k})+1$.

性质 1　$T_{i,j,k}\geqslant 0,T'_{i,j,k}\geqslant 0$.

证明　根据定义 2,显然有 $\max(D_{J_1,J_2})=-\min(D_{J_2,J_1})$.又因为 $\max(D_{i,j})+\max(D_{j,k})\geqslant\max(D_{i,k})\geqslant min(D_{i,k})$,所以 $T_{i,j,k}\geqslant 0$.同理,$T'_{i,j,k}\geqslant 0$.

本文新提出的显式构造框架的第二个步骤,建立在引理 3 的基础上.

引理 3　若 $\mathrm{girth}(\boldsymbol{U}(\infty;i,j,k))\geqslant 8$,则对于任意 $X\geqslant Q_{i,j,k}$均有 $\mathrm{girth}(\boldsymbol{U}(X;i,j,k))\geqslant 8$,而 $\mathrm{girth}(\boldsymbol{U}(Q_{i,j,k}-1;i,j,k))<8$.

证明　①首先,证明 $\boldsymbol{U}(X;i,j,k)$不含 4-环.假设

在第 i,j 行,第 r,s 列中存在一个 4-环,则

$$p_{i,r}-p_{j,r}+p_{j,s}-p_{i,s}\equiv 0(\bmod X) \tag{7}$$

记式(7)左侧表达式为 $LH7$,则 $LH7=(p_{i,r}-p_{j,r})+(p_{j,s}-p_{k,s})+(p_{k,s}-p_{i,s})$. $LH7$ 的取值范围是: $-T'_{i,j,k}\leqslant LH7\leqslant T_{i,j,k}$. 由于 $\boldsymbol{U}(\infty;i,j,k)$无 4-环,所以 $LH7\neq 0$. 因此,$0<|LH7|\leqslant\max(T_{i,j,k},T'_{i,j,k})<Q_{i,j,k}\leqslant X$. 与式(7)矛盾.

②其次,证明 $U(X;i,j,k)$不含 6-环. 假设在第 i,j,k 行,第 r,s,t 列中存在一个 6-环,则

$$p_{i,r}-p_{j,r}+p_{j,s}-p_{k,s}+p_{k,t}-p_{i,t}\equiv 0(\bmod X) \tag{8}$$

记式(8)左侧表达式为 $LH8$,则 $LH8$ 的取值范围是: $-T'_{i,j,k}\leqslant LH8\leqslant T_{i,j,k}$. 由于 $\boldsymbol{U}(\infty;i,j,k)$无 6-环,所以 $LH8\neq 0$. 因此,$0<|LH8|\leqslant\max(T_{i,j,k},T'_{i,j,k})<Q_{i,j,k}\leqslant X$. 与式(8)矛盾.

③最后,证明 $\boldsymbol{U}(Q_{i,j,k}-1;i,j,k)$存在长度小于 8 的环.

假设 $\max(D_{i,j})$,$\max(D_{j,k})$,$\max(D_{k,i})$分别出现在第 r,s,t 列. 显然,$r=s=t$ 是不可能的.

若 r,s,t 互不相同,则出现图 2 中 $a1$ 所示的 6-环:

$$\begin{aligned}T_{i,j,k}&=(p_{i,r}-p_{j,r})+(p_{j,s}-p_{k,s})+(p_{k,t}-p_{i,t})\\&\equiv 0(\bmod\ T_{i,j,k})\end{aligned}$$

若 $r=s,s\neq t$,则出现图 2 中 $a2$ 所示的 4-环:

$$\begin{aligned}T_{i,j,k}&=(p_{i,r}-p_{j,r})+(p_{j,s}-p_{k,s})+(p_{k,t}-p_{i,t})\\&=(p_{i,r}-p_{k,r})+(p_{k,t}-p_{i,t})\\&\equiv 0\ (\bmod\ T_{i,j,k}).\end{aligned}$$

若 $r\neq s,s=t$,则出现图 2 中 $a3$ 所示的 4-环:

$$\begin{aligned}T_{i,j,k}&=(p_{i,r}-p_{j,r})+(p_{j,s}-p_{k,s})+(p_{k,t}-p_{i,t})\\&=(p_{i,r}-p_{j,r})+(p_{j,s}-p_{i,s})\\&\equiv 0\ (\bmod\ T_{i,j,k}).\end{aligned}$$

若 $r=t,t\neq s$,则出现图 2 中 $a4$ 所示的 4-环:

$$\begin{aligned}T_{i,j,k}&=(p_{i,r}-p_{j,r})+(p_{j,s}-p_{k,s})+(p_{k,t}-p_{i,t})\\&=(p_{k,r}-p_{j,r})+(p_{j,s}-p_{k,s})\\&\equiv 0\ (\bmod\ T_{i,j,k}).\end{aligned}$$

总之,$\text{girth}(\boldsymbol{U}(T_{i,j,k};i,j,k)<8$. 同理可证 $\text{girth}(\boldsymbol{U}(T'_{i,j,k};i,j,k)<8$. 因此,有 $\boldsymbol{U}(Q_{i,j,k}-1;i,j,k)$的围长小于 8.

由引理 3 立即可得定理 2.

定理 2 令 $Q=\max\limits_{0\leqslant i<j<k<J}\{Q_{i,j,k}\}$. 若 $\text{girth}(\boldsymbol{U}(\infty))\geqslant 8$,则对于任意 $X\geqslant Q$ 均有 $\text{girth}(\boldsymbol{U}(X))\geqslant 8$,而 $\text{girth}(\boldsymbol{U}(Q-1))<8$.

定理 2 充分概括了本文新提出的显式构造框架第二个步骤的方法和结论. 根据定理 2,可以从移位矩阵直接精确计算出 CPM 尺寸连续变化的紧致下界. 我们将在第 3 节看到定理 2 的具体应用.

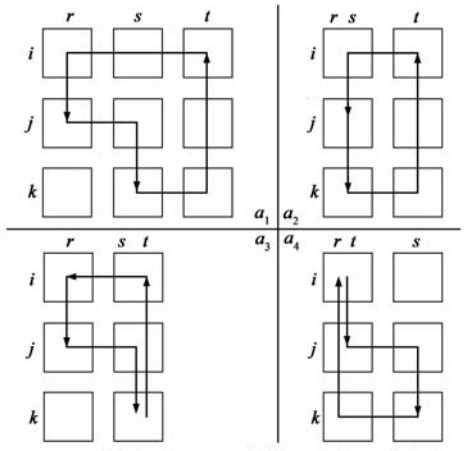


图2 $X=T_{i,j,k}$时必然出现a_1-a_4中的一种小环(长度小于8)

3 由框架导出四种已知的确定性方法

利用确定性方法,文献[20,21]分别构造了一类(3,L)QC-LDPC 码和一类(4,L)QC-LDPC 码,并证明:它们的 CPM 尺寸可以(在一个门限之上)连续变化,并且围长均为 8. 通过对移位矩阵直接赋值,文献[12,13]分别构造了一类多进制(3,L)QC-LDPC 码和一类多进制(4,L)QC-LDPC 码,并证明对于特定的某个 CPM 取值,它们的围长均为 8.

下面,本文从新框架的视角对这四种已有方法进行深入分析.

设 INT(Y)表示不小于 Y 的最小整数. 令 $p_{1,n}=n(1\leqslant n\leqslant L-1)$,则定理 1 中的条件 $p_{2,n}\geqslant p_{2,n-1}+1+\max\{p_{1,n},p_{1,L-1}-p_{1,n-1}\}$转变为 $p_{2,n}\geqslant p_{2,n-1}+\max\{n+1,L-n+1\}$.

下面讨论两种特殊情况.

①$p_{2,n}=p_{2,n-1}+\max\{n+1,L-n+1\}$. 该情形对应于文献[20,21]提出的构造方法,该方法与中国剩余定理结合在一起设计出了性能优良的二进制 QC-LDPC 码.

推论 1 对于任意 $X\geqslant 3L^2/4$,$\text{girth}(\boldsymbol{S}(X;0,1,2))=8$,$X=\text{INT}(3L^2/4)-1$ 时 $\text{girth}(\boldsymbol{S}(X;0,1,2))<8$.

推论 2 对于任意 $X\geqslant 3L^2/4+L-1$,$\text{girth}(\boldsymbol{S}(X))=8$,而 $X=\text{INT}(3L^2/4)+L-2$ 时 $\text{girth}(\boldsymbol{S}(X))<8$.

证明 由定理 1 可知 $\text{girth}(\boldsymbol{S}(\infty))\geqslant 8$,根据 $p_{1,n}$的赋值方式,$S(\infty)$的第 0 行和第 1 行中存在子矩阵[0 0 0;0 1 2],这显然会导致 8-环,因此 $\text{girth}(\boldsymbol{S}(\infty))=8$,$\text{girth}(\boldsymbol{S}(\infty;0,1,2))=8$. 根据定理 2,$T_{0,1,2}=0+0+p_{2,L-1}=p_{2,L-1}$,$T'_{0,1,2}=(L-1)+\{p_{2,L-1}-(L-1)\}+0=p_{2,L-1}$,而

$$p_{2,L-1}=\sum_{n=1}^{L-1}\max\{n+1,L-n+1\}=\text{INT}(3L^2/4)-1 \tag{9}$$

所以,$Q_{0,1,2}=\max(T_{0,1,2},T'_{0,1,2})+1=\mathrm{INT}(3L^2/4)$.

同理可证 $Q_{0,1,3}=Q_{0,2,3}=\mathrm{INT}(3L^2/4)+L-1$,$Q_{1,2,3}=\mathrm{INT}(3L^2/4)$.所以,$Q=\max\{Q_{0,1,2},Q_{0,1,3},Q_{0,2,3},Q_{1,2,3}\}=\mathrm{INT}(3L^2/4)+L-1$.

推论 1 完全包含了文献[20]中发现的围长特性和 CPM 连续取值门限,推论 2 完全包含了文献[21]中发现的围长特性和 CPM 连续取值门限.

②$p_{2,n}=p_{2,n-1}+L$.该情形对应于文献[12,13]提出的构造方法,该方法设计出了性能优良的多进制 QC-LDPC 码.

推论 3　对于任意 $X\geqslant L(L-1)+1$,$\mathrm{girth}(\boldsymbol{S}(X;1,2,3))=8$;而当 $X=L(L-1)$时 $\mathrm{girth}(\boldsymbol{S}(X;1,2,3))<8$.

推论 4　对于任意 $X\geqslant L^2$,$\mathrm{girth}(\boldsymbol{S}(X))=8$;而当 $X=L^2-1$ 时 $\mathrm{girth}(\boldsymbol{S}(X))<8$.

证明　因为 $L\geqslant\max\{n+1,L-n+1\}$,所以 $p_{2,n}\geqslant p_{2,n-1}+\max\{n+1,L-n+1\}$.因此,由定理 1 可知 $\mathrm{girth}(\boldsymbol{S}(\infty))\geqslant 8$.根据 $p_{1,n}$和$p_{2,n}$的赋值方式,$\boldsymbol{S}(\infty)$的第 1 行和第 2 行中存在子矩阵$\begin{bmatrix}0&1&2;0&L&2L\end{bmatrix}$,这显然会导致 8-环,因此 $\mathrm{girth}(\boldsymbol{S}(\infty))=8$,$\mathrm{girth}(\boldsymbol{S}(\infty;1,2,3))=8$.根据定理 2,$T_{0,1,2}=0+0+p_{2,L-1}=(L-1)L$,$T'_{0,1,2}=(L-1)+\{(L-1)L-(L-1)\}+0=(L-1)L$,所以 $Q_{0,1,2}=\max(T_{0,1,2},T'_{0,1,2})+1=(L-1)L+1$.同理可证,$Q_{0,1,3}=Q_{0,2,3}=L^2$,$Q_{1,2,3}=(L-1)L+1$.所以,$Q=\max\{Q_{0,1,2},Q_{0,1,3},Q_{0,2,3},Q_{1,2,3}\}=L^2$。

推论 3~4 不仅包含了文献[12,13]发现的全部围长特性,而且得出了更丰富和深刻的新结论.例如,文献[12,13]没有研究 CPM 尺寸的连续变化问题,而推论 3 和推论 4 非常简洁地推导出了针对该问题的新结论;文献[12,13]假定 $X+1$ 为素数幂,而推论 3 和推论 4 对于 X 的取值类型没有进行任何限制.

4　由框架导出的一种新方法

第 3 节的四种方法均定义 $p_{1,n}=n(1\leqslant n\leqslant L-1)$.本节改变 $p_{1,n}$的赋值方法,利用本文提出的显式构造框架设计了一种新的 QC-LDPC 码构造方法.新的赋值方法需要用到 Golomb 尺的概念.

定义 4　Golomb 尺[24]:Golomb 尺是一个整数集合 $a_0<a_1<\cdots<a_{L-1}$,其中差值 $a_r-a_s(r\neq s)$互不相同.

关于 Golomb 尺构造方法的综述可以参考文献[25].下面介绍一种代数构造方法.

Ruzsa 构造法[25]:设 p 为素数,g 为有限域 $GF(p)$的本原元,则集合

$$\boldsymbol{R}(p,g)=pa+(p-1)g^a \bmod p(p-1),1\leqslant a\leqslant p-1 \tag{10}$$

构成一个 Golomb 尺.

定理 3　设 $0=p_{1,0}<p_{1,1}<\cdots<p_{1,L-1}$是一个 Golomb 尺.若

$$p_{2,1}\geqslant p_{1,L-1}+p_{1,1}+1 \tag{11}$$

且对于 $2\leqslant y\leqslant L-1$ 有

$$p_{2,y}\geqslant 2p_{2,y-1}+p_{1,y}-p_{1,y-1}+1 \tag{12}$$

则 $\boldsymbol{S}(\infty)$的围长至少为 8.

证明　根据定理 1,显然有 $\mathrm{girth}(\boldsymbol{S}(\infty))\geqslant 8$.

注 1:事实上,可以证明满足定理 3 条件的移位值不会在 $\boldsymbol{S}(\infty;0,1,2)$中产生 8-环(证明见附录).因此,根据定理 3 得出的 $\boldsymbol{S}(\infty;0,1,2)$可以构造出围长至少为 10 的$(3,L)$QC-LDPC 码.

下面我们举一个例子来说明新构造方法.令 $p=7$,$g=3$.容易验证,g 的所有幂次对 7 取模可以生成 $GF(7)$中的所有非零元素$\{1,2,3,4,5,6\}$,因此 $g=3$ 是 $GF(7)$的一个本原元.根据式(10)得到一个 Golomb 尺:$\boldsymbol{R}(7,3)=\{25,26,15,10,23,6\}$.根据 Golomb 尺的移位不变性[25],$R(7,3)$各项减去 6 并排序,得到的集合$\{0,4,9,17,19,20\}$仍然是一个 Golomb 尺.在该例中,我们选择定理 3 中式(11)和式(12)取等号的赋值方式,则得到式(13)所示的移位矩阵 $\boldsymbol{S}(X)$.根据定理 3,$\boldsymbol{S}(\infty)$的围长至少为 8.因此,$\boldsymbol{S}(\infty;0,1,2)$的围长也至少为 8.其实,由附录的证明可知 $\boldsymbol{S}(\infty;0,1,2)$的围长至少为 10.根据紧致下界[22]可知:对于任意整数 $X\geqslant 2\times 492+1$,$S(X;0,1,2)$的围长至少为 10.

$$\boldsymbol{S}(X)=\begin{bmatrix}0&0&0&0&0&0\\0&4&9&17&19&20\\0&25&56&121&245&492\\0&29&65&138&264&512\end{bmatrix} \tag{13}$$

本节的研究结果说明:基于新提出的显式构造框架可以开发出新的构造方法;该框架本身并不限制 QC-LDPC 码的围长只能等于 8,在满足定理 1 的基础上对移位值进行恰当配置(例如定理 3)也可以得到围长超过 8 的 QC-DLPC 码的确定性构造方法.

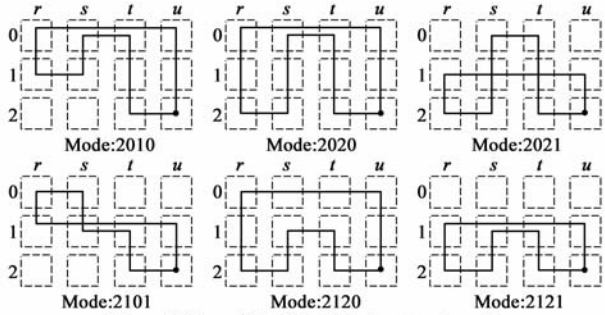
5　结论

本文提出了一种构造围长至少为 8 的 QC-LDPC 码的显式框架.该框架的突出特点是:(1)不需要任何计算机搜索步骤;(2)构造的 QC-LDPC 码不仅围长至少为 8,而且还具有 CPM 尺寸连续变化的优点.本文提出的显式框架是一种系统化的确定性构造方法,利用它可以推导出许多具体的已知或新的确定性构造方法.因此,新提出的框架对于围长至少为 8 的二进制和多进制 QC-LDPC 码的具体构造方法有重要的指导意义和参考价值.与 QC-LDPC 码的一些理论文献[5,20,22,23,26~28]一样,本文的目的是获得对于 QC-LDPC 码构造具有一定指导意义的新理论成果.对于译码性能的计算机

仿真等问题,将在后续论文中作进一步研究.

附录

证明 根据 Golomb 尺的定义,在 $\boldsymbol{S}(\infty)$的第 0 行和第 1 行移位值之间不会产生 8-环.下面证明:在第 2 行中依次添加移位值 $p_{2,u}(1\leqslant u\leqslant L-1)$后,$\boldsymbol{S}(\infty;0,1,2)$中都不会产生经过 $p_{2,u}$的 8-环,因此最终的 $\boldsymbol{S}(\infty;0,1,2)$中也没有 8-环.为了分析方便,定义模式 $2ABC$ 为:以 $p_{2,u}$为出发点,按照 8-环的顺时针方向追溯,构成 8-环的 4 条横线依次出现第 2 行、第 A 行、第 B 行和第 C 行.通过分析易知:经过 $p_{2,u}$的可能 8-环只有图(A)所示的 6 种模式(黑点表示 $p_{2,u}$).



图A 经过$p_{2,u}$的可能8-环($r\neq s,s\neq t,t\neq u,u\neq r$)

假设存在图 A 模式 2010 所示的 8-环,则存在等式 $0-p_{1,r}+p_{1,s}-0+0-p_{2,t}+p_{2,u}-0=0$.

若 $u>1$,则 $p_{2,u}=p_{2,t}+p_{1,r}-p_{1,s}\leqslant p_{2,u-1}+p_{1,L-1}-0$,与式(12)矛盾.若 $u=1$,则根据 $r\neq u$,$s\neq r$,$t\neq s$,$t\neq u$ 的条件,t 只能取 0,此时 r 和 s 可以分别取 $L-1$ 和 1.所以,$p_{2,1}=p_{2,0}+p_{1,r}-p_{1,s}\leqslant 0+p_{1,L-1}-p_{1,1}$,与式(11)矛盾.

同理可证(受篇幅所限,具体证明过程此处略去),图 A 中的其他 5 种环也不可能存在.总之,在第 2 行中添加移位值 $p_{2,u}(1\leqslant u\leqslant L-1)$后,$\boldsymbol{S}(\infty;0,1,2)$中不会产生经过 $p_{2,u}$的 8-环.证毕.

参考文献

[1] MPC Fossorier. Quasi-cyclic low-density parity-check codes from circulant permutation matrices[J]. IEEE Trans Inf Theory, 2004, 50(8): 1788 – 1793.

[2] B Vasic, K Pedagani, M Ivkovic. High-rate girth-eight low-density parity-check codes on rectangular integer lattices[J]. IEEE Trans Commun, 2004, 52(8): 1248 – 1252.

[3] S Myung, K Yang. A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem[J]. IEEE Commun Letters, 2005, 9(9): 823 – 825.

[4] ME O'Sullivan. Algebraic construction of sparse matrices with large girth[J]. IEEE Trans Inform Theory, 2006, 52(2): 718 – 727.

[5] S Kim, J S No H Chung, et al. On the girth of Tanner (3,5) quasi-cyclic LDPC codes[J]. IEEE Trans Inf Theory, 2006, 52(4): 1739 – 1744.

[6] O Milenkovic, N Kashyap, D Leyba. Shortened array codes of large girth[J]. IEEE Trans Inf Theory, 2006, 52(8): 3707 – 3722.

[7] X Ge, S Xia. Structured non-binary LDPC codes with large girth[J]. IEE Electronics Letters, 2007, 43(22): 1220 – 1221.

[8] M Wataru, M Yoshikuni, Y Hideo. A study on QC-LDPC codes with girth 8 or 10 for broadband[J]. IEICE Technical Report, 2007, 27: 31 – 35.

[9] F Masaya, S Shojira. A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8 [J]. IEICE Trans Fundamentals, 2007, E90-A(5): 1055 – 1061.

[10] Y Wang, J-S Yedidia, S-C Draper. Construction of high-girth QC-LDPC codes[A]. 5th International Symposium on Turbo Codes and Related Topics[C]. Lausanne, Switzerland, 2008. 180 – 185.

[11] F Zhang, X Mao, W Zhou, et al. Girth-10 LDPC codes based on 3-D cyclic lattices[J]. IEEE Trans Vehicular Technology, 2008, 57(2): 1049 – 1060.

[12] K Liu, Z Fei, J Kuang. Novel algebraic constructions of nonbinary structured LDPC codes over finite fields[A]. Proc 68th IEEE VTC Fall[C]. Calgary, Alberta, Canada, 2008. 1 – 5.

[13] K Liu, Z Fei, J Kuang. Three algebraic methods for constructing nonbinary LDPC codes based on finite fields[A]. Proc 19th IEEE PIMRC[C]. Cannes, French Riviera, France, 2008. 1 – 5.

[14] X Jiang, MH Lee. Large girth non-binary LDPC codes based on finite fields and Euclidean geometries[J]. IEEE Signal Processing Letters, 2009, 16(6): 521 – 524.

[15] X Tao, W Liu, X Zou. On the construction of low-density parity-check codes with girth 10[J]. Int J Electron Commun (AEÜ), 2009, 63: 689 – 694.

[16] 刘磊,周武旸.码长连续变化的 QC-LDPC 码的设计[J].电子与信息学报,2009,31(10):2523 – 2526.
Liu Lei, Zhou Wu-yang. Design of QC-LDPC code with continuously variable length[J]. Journal of Electronics & Information Technology, 2009, 31(10): 2523 – 2526. (in Chinese)

[17] 张伟,朱光喜,彭立,等.大围长结构化 LDPC 码构造方法[J].计算机科学,2009,36(11):109 – 112.
Zhang Wei, Zhu Guang-xi, Peng Li, et al. Design of structured LDPC codes with large girth[J]. Computer Science, 2009, 36(11): 109 – 112. (in Chinese)

[18] I-E Bocharova, F Hug, R Johannesson, et al. New low-density parity-check codes with large girth based on hypergraphs[A]. ISIT 2010[C]. Austin, Texas, USA, 2010. 13 – 18.

[19] M Esmaeilia, MH Tadayonb, TA Gulliver. Low-complexity

girth-8 high-rate moderate length QC LDPC codes[J]. Int J Electron Commun (AEÜ),2010,64:360 – 365.

[20] 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.
Zhang Guo-hua, 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. (in Chinese)

[21] 张国华. 大围长结构化 LDPC 码的构造研究[D]. 陕西西安:西安电子科技大学,2010.6.
Zhang Guo-hua. Research on the construction of structured low-density parity-check codes with large girth[D]. Xi′an, Shaanxi: Xidian University,2010.6. (in Chinese)

[22] Zhang Guo-hua, Wang Ju-hua, Li Xue-yuan, et al. Tight lower bound of consecutive lengths for QC-LDPC codes with girth at least ten[J]. Chinese Science Bulletin, 2011, 56(12): 1272 – 1277.

[23] 张国华,王新梅. 围长为 12 的 QC-LDPC 码连续码长的紧致下界[J]. 科学通报,2011,56(19):1578 – 1582.
Zhang Guo-hua, Wang Xin-mei, Tight lower bound of consecutive lengths for QC-LDPC codes with girth twelve[J]. Chinese Science Bulletin, 2011, 56(19): 1578 – 1582. (in Chinese)

[24] JB Shearer. Some new disjoint Golomb rulers[J]. IEEE Trans Inf Theory,1998,44(7):3151 – 3153.

[25] A Dimitromanolakis. Analysis of the Golomb ruler and the Sidon set problems, and determination of large, near-optimal Golomb rulers[D]. Technical University of Crete,2002.

[26] 彭立,朱光喜. QC-LDPC 码的置换矩阵循环移位次数设计[J]. 电子学报,2010,38(4):786 – 790.
Peng Li, Zhu Guang-xi. Shift value design of permutation matrices for QC-LDPC codes[J]. Acta Electronica Sinica,2010, 38(4):786 – 790. (in Chinese)

[27] K Lally. Explicit construction of type-II QC LDPC codes with girth at least 6[A]. ISIT2007[C]. Nice, France, 2007. 2371 – 2375.

[28] S. Kim, J-S No, H Chung, et al. Quasi-cyclic low-density parity-check codes with girth larger than 12[J]. IEEE Trans Inf Theory,2007,53(8):2885 – 2891.

作者简介

张国华　男,1977 年生于山西临汾. 1999 年,2002 年和 2010 年分别在山东大学、中国空间技术研究院(西安分院)、西安电子科技大学获得理学学士、工学硕士和工学博士学位. 现在为中国空间技术研究院(西安分院)高级工程师,主要从事信道编码理论和 ATM 交换方面的研究.
E-mail: zhangghcast@163.com

王新梅　男,1937 生于浙江浦江. 西安电子科技大学教授、博士生导师,主要研究方向为信道编码理论、密码学.