科学通报 2010 年 第 55 卷 第 22 期：2257 ~ 2262
论 文 www.scichina.com csb.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS

围长至少为 10 的 QC-LDPC 码连续码长的紧致下界

张国华[①②], 王菊花[②], 李学远[①], 王新梅[①]

① 西安电子科技大学综合业务网国家重点实验室, 西安 710071;
② 中国空间技术研究院西安分院, 西安 710100
E-mail: zhangghcast@163.com

2010-01-20 收稿, 2010-04-01 接受
国家重点基础研究发展计划(2010CB328300)、国家自然科学基金(U0635003)和高等学校学科创新引智计划(B08038)资助

摘要 对于围长至少为 10 的任意(3, L)QC-LDPC 码, 提出了连续码长的紧致下界. 当码长大于下界时围长至少为 10, 当码长等于下界时围长小于 10. 研究结论对于大围长 QC-LDPC 码的存在性研究、基于中国剩余定理的大围长 LDPC 码构造、具有纠错能力保证的 LDPC 码构造等问题具有重要应用价值.

关键词
低密度奇偶校验码
准循环
围长
连续

消除短环是提高低密度奇偶校验(LDPC)码译码性能的一个重要手段. 目前消除 4 环和 6 环的研究成果已经比较丰富[1~7], 因此如何消除 8 环和更长的环已成为 LDPC 码构造研究的热点之一. LDPC 码由校验矩阵完全定义. 若校验矩阵的列重和行重分别为 R 和 L, 则相应的 LDPC 码称为(R,L)LDPC 码; 若校验矩阵是一个由循环置换矩阵构成的阵列, 则相应的 LDPC 码称为准循环(QC-)LDPC 码. 本文将围长至少为 g 记为 girth-g^+, 将围长恰好为 g 记为 girth-g. 采用各种思路, 人们目前已经开发出一些构造 girth- 10^+(3, L)LDPC 码的方法. 这些巧妙的思路包括: 容许斜率对[8]、二次置换多项式[9]、平衡环路[10]、控制方程[11]、网格[12]、三维循环网格[13]、邻接矩阵理论[14]和爬山算法[15]. 虽然这些方法可以构造各种性能优异的 girth-10^+(3, L) LDPC 码, 但是所构造的 LDPC 码码长是固定的, 当码长需要调整时必须重新执行构造算法. 明显不同于上述方法的一种技术路线, 是构造码长可以连续变化的 LDPC 码. 最近, 文献[16]基于有限多项式环理论构造出一种码长可以连续变化的 girth-10^+(3,L) QC-LDPC 码, 当码长大于某个下界时这类码的围长至少为 10; 然而, 该方法要求移位矩阵必须满足某种严格的规则, 因此文献[16]提出的下界对于码长连续变化的一般 QC-LDPC 码设计不具有普适性.

本文的创新点是, 通过研究任意移位矩阵所定义的 girth-10^+(3, L)QC-LDPC 码, 发现了一般 girth-10^+(3, L)QC-LDPC 码的连续码长的紧致下界: 当码长大于该下界时, 利用同一个移位矩阵产生的(3, L)QC-LDPC 码的围长至少为 10; 当码长等于该下界时(3, L)QC-LDPC 码的围长小于 10. 本文提出的新下界对于码长连续变化的 girth-10^+(3, L)QC-LDPC 码设计具有普遍指导意义, 文献[16]发现的下界只是本文新下界的一个特例.

近年来, 人们在密码的基本数学理论[17,18]、伪随机序列设计[19,20]、密码系统设计[21~24]、密码分析与攻击[25~28]等方面取得了重要研究成果. 最近, 周亮等人[29]发现大围长 LDPC 码在密码学中具有重要应用前景. 因此, 本文的研究结果对于密码领域也具有重要参考价值.

因为环长与校验矩阵的定义域(二元或多元)无关, 因此虽然下文的讨论限定为二元情形, 但是结论同样适用于多元 LDPC 码.

1 连续码长的紧致下界

码长为 N=XL 的(3, L) QC-LDPC 码的校验矩阵

英文版见: Zhang G H, Wang J H, Li X Y, et al. Tight lower bound of consecutive lengths for QC-LDPC codes with girth at least ten. Chinese Sci Bull, 2010, 55, doi: 10.1007/s11434-010-4049-8

$\boldsymbol{H}_X$ 可以表示为[30]:

$$\boldsymbol{H}_X=\begin{bmatrix} \boldsymbol{I}(0) & \boldsymbol{I}(0) & \cdots & \boldsymbol{I}(0) \\ \boldsymbol{I}(p_{1,0}) & \boldsymbol{I}(p_{1,1}) & \cdots & \boldsymbol{I}(p_{1,L-1}) \\ \boldsymbol{I}(p_{2,0}) & \boldsymbol{I}(p_{2,1}) & \cdots & \boldsymbol{I}(p_{2,L-1}) \end{bmatrix}, \quad (1)$$

其中 $\boldsymbol{I}(p)$ 表示一个由移位值 p 定义的 $X\times X$ 循环置换矩阵: 对于 $0\leqslant r\leqslant X-1$, 第 r 行、第 $(r+p) \bmod X$ 列的元素为 1, 其余元素均为 0.

相应地, 移位矩阵 $\boldsymbol{S}$ 可以表示为

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

其中, 对于 $1\leqslant u\leqslant 2$, $1\leqslant v\leqslant L-1$, $p_{u,v}\in\{0,1,\cdots,X-1\}$, $p_{u,0}=0$. 式(2)中各元素为正整数的限定不失一般性, 因为负整数对 X 取模后可以变成正整数.

$\boldsymbol{H}_X$ 由 $\boldsymbol{S}$ 和 X 唯一确定. 本文使用符号 $g(\boldsymbol{H}_X)$ 表示 $\boldsymbol{H}_X$ 的围长.

引理 1: 假设对于某个特定整数 Q, $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$. 则对于任意 $P\geqslant 2\max\{\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D}\}+1$, 有 $g(\boldsymbol{H}_{\mathrm{P}})\geqslant 10$. 其中, $\mathrm{A}=\max_v p_{1,v}$, $\mathrm{B}=\max_v p_{2,v}$, $\mathrm{C}=\max_v p_{2,v}-p_{1,v}$, $\mathrm{D}=\max_v p_{1,v}-p_{2,v}$.

证明: 为证明引理 1, 需要证明 $\boldsymbol{H}_P$(或者等价地证明 $\boldsymbol{S}$)中不存在 4–, 6–, 8–环. 证明思路如下: 第一步, 假设 $\boldsymbol{S}$ 中存在 t–环(t=4, 6 或 8), 则根据文献[30]中式(4)可以写出一个模 P 等式; 第二步, 通过对模 P 等式进行简单变换, 使其等式左右两侧非负, 这样只要证明 P 既大于等式左侧又大于等式右侧, 模 P 等式就可以简化为不含模运算的等式; 第三步, 由于等式对任意整数取模仍然成立, 因此可以得到一个模 Q 等式. 第四步, 模 Q 等式表明 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在 t–环, 从而与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 的前提条件矛盾.

在证明之前, 首先分析 $\boldsymbol{S}$ 中所有可能的 4–, 6–, 8–环的类型. 根据文献[30], 4–环只可能出现在 $\boldsymbol{S}$ 的任意两行元素中, 6–环只可能出现在 $\boldsymbol{S}$ 的三行元素中, 8–环只可能出现在 $\boldsymbol{S}$ 的任意两行元素中或三行元素中.

情形 A: 4–环

(A.1) $\boldsymbol{S}$ 第 0 行和第 1 行中的 4–环: 假设在 $\boldsymbol{S}$ 第 0 行和第 1 行中存在 4–环, 则存在两个整数 $i\neq j$ 满足

$$(0-p_{1,i})+(p_{1,j}-0)=0(\mathrm{mod}\,P). \quad (3)$$

因为 $P>\mathrm{A}$, 所以式(3)可以简化为 $p_{1,i}=p_{1,j}$. 因此

$$(0-p_{1,i})+(p_{1,j}-0)=0(\mathrm{mod}\,\mathrm{Q}), \quad (4)$$

式(4)表明 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 4–环, 这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

(A.2) $\boldsymbol{S}$ 第 0 行和第 2 行中的 4–环: 类似地可以证明, 因为 $P>\mathrm{B}$ 所以在 $\boldsymbol{S}$ 第 0 行和第 2 行中不存在 4–环.

(A.3) $\boldsymbol{S}$ 第 1 行和第 2 行中的 4–环: 假设在 $\boldsymbol{S}$ 第 1 行和第 2 行中存在 4–环, 则存在两个整数 $i\neq j$ 满足

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})=0(\mathrm{mod}\,P). \quad (5)$$

因为 $P>\max\{2\mathrm{A},2\mathrm{B}\}\geqslant \mathrm{A}+\mathrm{B}$, 所以式(5)可以简化为

$$p_{1,i}+p_{2,j}=p_{1,j}+p_{2,i}, \quad (6)$$

因此

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})=0(\mathrm{mod}\,\mathrm{Q}). \quad (7)$$

式(7)表明 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 4–环, 这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

情形 B: S 第 0, 1, 2 行中的 6–环

假设在 $\boldsymbol{S}$ 第 0, 1, 2 行中存在 6–环(如图 1(a)所示), 则存在 3 个整数 $i,j,k(i\neq j;j\neq k;k\neq i)$ 满足

$$(0-p_{1,j})+(p_{1,i}-p_{2,i})+(p_{2,k}-0)=0(\mathrm{mod}\,P), \quad (8)$$

因为 $P>\max\{2\mathrm{A},2\mathrm{B}\}\geqslant \mathrm{A}+\mathrm{B}$, 所以式(8)可以简化为

$$p_{1,i}+p_{2,k}=p_{1,j}+p_{2,i}, \quad (9)$$

因此

$$(0-p_{1,j})+(p_{1,i}-p_{2,i})+(p_{2,k}-0)=0(\mathrm{mod}\,\mathrm{Q}), \quad (10)$$

式(10)表明, 在 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 6–环, 这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

情形 C: 8–环

(C.1): $\boldsymbol{S}$ 任意两行中的 8–环

(C.1.1) $\boldsymbol{S}$ 第 0 行和第 1 行中的 8–环: 假设在 $\boldsymbol{S}$ 第 0, 1 行中存在 8–环, 则存在 4 个整数 $i,j,k,l(i\neq j;j\neq k;k\neq l;l\neq i)$ 满足

$$(0-p_{1,i})+(p_{1,j}-0)+(0-p_{1,k})+(p_{1,l}-0)=0(\mathrm{mod}\,P). \quad (11)$$

因为 $P>2\mathrm{A}$, 式(11)可以简化为

$$p_{1,j}+p_{1,l}=p_{1,i}+p_{1,k}, \quad (12)$$

因此

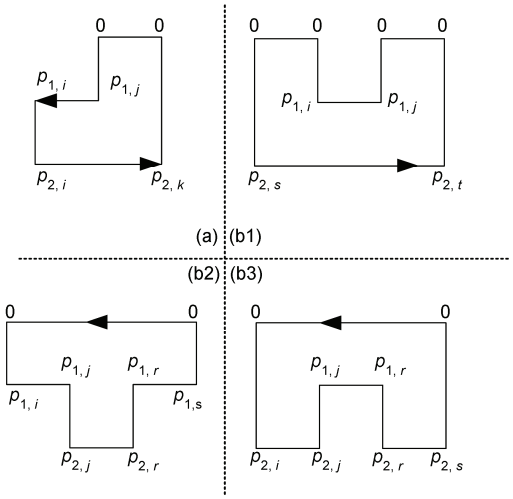

图 1　在移位矩阵 $\boldsymbol{S}$ 的三行元素中可能出现的全体 6–环和 8–环

$$(0-p_{1,i})+(p_{1,j}-0)+(0-p_{1,k})+(p_{1,l}-0)=0(\mathrm{mod\,Q}),\ (13)$$

式(13)表明，在 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 8–环，这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

(C.1.2) $\boldsymbol{S}$ 第 0 行和第 2 行中的 8–环: 类似地可以证明, 因为 $P>2\mathrm{B}$ 所以在 $\boldsymbol{S}$ 第 0 行和第 2 行中不存在 8–环.

(C.1.3) $\boldsymbol{S}$ 第 1 行和第 2 行中的 8–环: 假设在 $\boldsymbol{S}$ 第 1, 2 行中存在 8–环, 则存在 4 个整数 $i,j,k,l(i\neq j;\ j\neq k;k\neq l;l\neq i)$ 满足

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=0(\mathrm{mod}\,P).\ (14)$$

定义 $D_x=(p_{1,x}-p_{2,x}),x\in\{i,j,k,l\}$. 按照 D_i,D_j,D_k,D_l 各自取值是否非负，一共有 16 种组合情况. 为使行文简洁, 我们只分析 6 种典型情况, 其余 10 种情况可做类似分析.

(C.1.3.0) 当 $D_i\geqslant 0,D_j\geqslant 0,D_k\geqslant 0,D_l\geqslant 0$ 时: 因为 $P>2\mathrm{D}$，所以式(14)可以简化为

$$(p_{1,i}-p_{2,i})+(p_{1,k}-p_{2,k})=(p_{1,j}-p_{2,j})+(p_{1,l}-p_{2,l}).\ (15.0)$$

(C.1.3.1) 当 $D_i\geqslant 0,D_j\geqslant 0,D_k\geqslant 0,D_l<0$ 时: 因为 $P>\mathrm{C}+2\mathrm{D}$，所以式(14)可以简化为

$$(p_{1,i}-p_{2,i})+(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=(p_{1,j}-p_{2,j}).\ (15.1)$$

(C.1.3.2) 当 $D_i\geqslant 0,D_j\geqslant 0,D_k<0,D_l<0$ 时: 因为 $P>\mathrm{C}+\mathrm{D}$，所以式(14)可以简化为

$$(p_{1,i}-p_{2,i})+(p_{2,l}-p_{1,l})=(p_{1,j}-p_{2,j})+(p_{2,k}-p_{1,k}).\ (15.2)$$

(C.1.3.3) 当 $D_i\geqslant 0,D_j<0,D_k\geqslant 0,D_l<0$ 时: 因为 $P>2(\mathrm{C}+\mathrm{D})$，所以式(14)可以简化为

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+(p_{1,k}-p_{2,k})+(p_{2,l}-p_{1,l})=0.\ (15.3)$$

(C.1.3.4) 当 $D_i\geqslant 0,D_j<0,D_k<0,D_l<0$ 时: 因为 $P>2\mathrm{C}+\mathrm{D}$，所以式(14)可以简化为

$$(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+(p_{2,l}-p_{1,l})=(p_{2,k}-p_{1,k}).\ (15.4)$$

(C.1.3.5) 当 $D_i<0,D_j<0,D_k<0,D_l<0$ 时: 因为 $P>2\mathrm{C}$，所以式(14)可以简化为

$$(p_{2,i}-p_{1,i})+(p_{2,k}-p_{1,k})=(p_{2,j}-p_{1,j})+(p_{2,l}-p_{1,l}).\ (15.5)$$

因此, 无论出现那种组合情形, 均有

$$\begin{aligned}&(p_{1,i}-p_{2,i})+(p_{2,j}-p_{1,j})+(p_{1,k}-p_{2,k})\\&+(p_{2,l}-p_{1,l})=0(\mathrm{mod\,Q}).\end{aligned}\ (16)$$

式 (16) 表明，在 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 8–环，这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

(C.2): $\boldsymbol{S}$ 三行中的 8–环

假设在 $\boldsymbol{S}$ 第 0, 1, 2 行中存在 8–环, 则该 8–环必为图 1(b1~b3)所示的 3 种 8–环模式之一(原因见附录 1).

(C.2.1)假设 8–环以模式(b1)出现, 则存在 4 个整数 $i,s,t,j(i\neq s;s\neq t;t\neq j;j\neq i)$ 满足

$$(p_{1,i}-0)+(0-p_{2,s})+(p_{2,t}-0)+(0-p_{1,j})=0(\mathrm{mod}\,P),\ (17)$$

因为 $P>\mathrm{A}+\mathrm{B}$，所以式(17)可以简化为 $p_{1,i}+p_{2,t}=p_{2,s}+p_{1,j}$，因此

$$(p_{1,i}-0)+(0-p_{2,s})+(p_{2,t}-0)+(0-p_{1,j})=0(\mathrm{mod\,Q}).\ (18)$$

式 (18) 表明，在 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 8–环，这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

(C.2.2) 假设 8–环以模式(b2)出现, 则存在 4 个整数 $i,j,r,s(i\neq j;j\neq r;r\neq s;s\neq i)$ 满足

$$\begin{aligned}&(0-p_{1,i})+(p_{1,j}-p_{2,j})+(p_{2,r}-p_{1,r})\\&+(p_{1,s}-0)=0(\mathrm{mod}\,P).\end{aligned}\ (19)$$

定义 $D_x=(p_{1,x}-p_{2,x}),x\in\{j,r\}$. 按照 D_j,D_r 各自取值是否非负，一共有 4 种组合情况. 下面对这 4 种情形分别分析.

(C.2.2.0)当 $D_j\geqslant 0,D_r\geqslant 0$ 时: 因为 $P>\mathrm{A}+\mathrm{D}$，式(19)可以简化为

$$(p_{1,j}-p_{2,j})+p_{1,s}=p_{1,i}+(p_{1,r}-p_{2,r}), \quad (20.0)$$

(C.2.2.1) 当 $D_j\geqslant 0, D_r<0$ 时: 因为 $P>\mathrm{A}+\mathrm{C}+\mathrm{D}$, 式(19)可以简化为

$$(p_{1,j}-p_{2,j})+(p_{2,r}-p_{1,r})+p_{1,s}=p_{1,i}, \quad (20.1)$$

(C.2.2.2) 当 $D_j<0, D_r\geqslant 0$ 时, 因为 $P>\mathrm{A}+\mathrm{C}+\mathrm{D}$, 式(19)可以简化为

$$p_{1,s}=p_{1,i}+(p_{2,j}-p_{1,j})+(p_{1,r}-p_{2,r}), \quad (20.2)$$

(C.2.2.3) 当 $D_j<0, D_r<0$ 时: 因为 $P>\mathrm{A}+\mathrm{C}$, 式(19)可以简化为

$$(p_{2,r}-p_{1,r})+p_{1,s}=p_{1,i}+(p_{2,j}-p_{1,j}), \quad (20.3)$$

因此, 无论出现哪种组合情形, 均有

$$\begin{aligned}&(0-p_{1,i})+(p_{1,j}-p_{2,j})+(p_{2,r}-p_{1,r})\\&+(p_{1,s}-0)=0(\mathrm{mod}\,\mathrm{Q}).\end{aligned} \quad (21)$$

式(21)表明, 在 $\boldsymbol{H}_{\mathrm{Q}}$ 中存在一个 8–环, 这与 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 矛盾.

(C.2.3): 采用与(C.2.2)类似的分析, 可以证明不存在模式(b3)所示的 8–环.

根据情形 A-C 的分析, 可知对于任意整数 $P\geqslant 2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})+1$ 均有 $g(\boldsymbol{H}_P)\geqslant 10$.

证毕.

注 1: 文献[16]提出了一种码长连续变化的 girth-10^{+}(3,L)QC-LDPC 码, 根据该文献式(5), 其移位矩阵 $\boldsymbol{S}$ 可以表示为

$$\boldsymbol{S}=\begin{bmatrix}0 & 0 & \cdots & 0\\ l_0 & l_1 & \cdots & l_{L-1}\\ 3l_0 & 3l_1 & \cdots & 3l_{L-1}\end{bmatrix}. \quad (22)$$

通过等价变换, 式(22)可以转变为与式(2)定义一致的形式:

$$\boldsymbol{S}=\begin{bmatrix}0 & 0 & \cdots & 0\\ 0 & l_1-l_0 & \cdots & l_{L-1}-l_0\\ 0 & 3(l_1-l_0) & \cdots & 3(l_{L-1}-l_0)\end{bmatrix}. \quad (23)$$

虽然文献[16]没有明确定义, 但在是根据该文献, 定理 2 的证明和表 1 可知: $l_{L-1}-l_0$ 是 $\boldsymbol{S}$ 第 1 行中的最大值, 因此 $\mathrm{A}=l_{L-1}-l_0$, $\mathrm{B}=3(l_{L-1}-l_0)$, $\mathrm{C}=2(l_{L-1}-l_0)$, $\mathrm{D}=0$. 根据引理 1, 若 $\boldsymbol{S}$ 对于某个特定的整数 Q, 满足 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$, 则对于任意整数 $P\geqslant 2\times 3\times(l_{L-1}-l_0)+1$, 有 $g(\boldsymbol{H}_P)\geqslant 10$. 由此可见, 文献[16]中式(9)]给出的下界只是本文引理 1 的一个特例.

当 $P<2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})+1$ 时, $g(\boldsymbol{H}_P)\geqslant 10$ 是否可以继续成立? 对于 $P=2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})$, 我们有

引理 2: $g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})})<10$.

证明: 我们首先考虑 $g(\boldsymbol{H}_{2\mathrm{A}})$ 和 $g(\boldsymbol{H}_{2\mathrm{B}})$ 的取值. 设 $p_{1,x}=\mathrm{A}$. 令 $P=2\mathrm{A}$, 则有

$$(0-0)+(p_{1,x}-0)+(0-0)+(p_{1,x}-0)=0(\mathrm{mod}\,P). \quad (24)$$

对于 $\boldsymbol{H}_{2\mathrm{A}}$, 式(24)描述了一个出现在 $\boldsymbol{S}$ 第 0 行和第 1 行中的 8–环. 这表明 $g(\boldsymbol{H}_{2\mathrm{A}})<10$. 同理可证 $g(\boldsymbol{H}_{2\mathrm{B}})<10$. 现在考虑 $g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})})$, 分 3 种情况证明. 第一种情况: 若移位矩阵 $\boldsymbol{S}$ 第 2 行与第 1 行对应移位值的差同时非负, 即 $p_{2,v}-p_{1,v}\geqslant 0(0\leqslant v\leqslant L-1)$, 则 $\mathrm{D}=0$, $\mathrm{C}+\mathrm{D}=\mathrm{C}+0<\mathrm{B}$. 因此, $g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})})=g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B})})<10$. 第二种情况: 若移位矩阵 $\boldsymbol{S}$ 第 1 行与第 2 行对应移位值的差同时非负, 即 $p_{1,v}-p_{2,v}\geqslant 0(0\leqslant v\leqslant L-1)$, 则 $\mathrm{C}=0$, $\mathrm{C}+\mathrm{D}=0+\mathrm{D}<\mathrm{A}$. 因此 $g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})})=g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B})})<10$. 第三种情况: 若 $\boldsymbol{S}$ 第 2 行与第 1 行对应移位值的差中既包含正整数又包含负整数(显然, 此时 C,D 均为正整数), 则定义两个非空集合 $\boldsymbol{X}:=\{x\,|\,p_{2,x}-p_{1,x}=\mathrm{C}, x\in\{0,\cdots,L-1\}\}$ $\boldsymbol{Y}:=\{y\,|\,p_{1,y}-p_{2,y}=\mathrm{D}, y\in\{0,\cdots,L-1\}\}$. 在式(14)中令 $i=k\in\boldsymbol{Y}$, $j=l\in\boldsymbol{X}$, 则式(14)成为

$$\mathrm{D}+\mathrm{C}+\mathrm{D}+\mathrm{C}=0(\mathrm{mod}\,P). \quad (25)$$

对于 $\boldsymbol{H}_{2(\mathrm{C}+\mathrm{D})}$, 式(25)描述了一个出现在 $\boldsymbol{S}$ 第 1 行和第 2 行中的 8–环. 这表明 $g(\boldsymbol{H}_{2\mathrm{C}+2\mathrm{D}})<10$. 因此对于该情形, 同样有 $g(\boldsymbol{H}_{2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})})<10$.

注 2: 虽然 $P<2\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})$ 时, $g(\boldsymbol{H}_P)\geqslant 10$ 也有可能成立, 但在大多数情况下围长都达不到 10, 通过计算机分析我们没有发现围长变化的任何规律.

根据引理 1~2 可以得到本文的主要结论:

定理 1: 假设对于某个特定整数 Q, $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 成立. 则 $2L\max(\mathrm{A},\mathrm{B},\mathrm{C}+\mathrm{D})$ 是一个紧致下界, 当码长大于该下界时总有 $g(\boldsymbol{H}_P)\geqslant 10$, 当码长等于该下界时 $g(\boldsymbol{H}_P)<10$. 其中, A, B, C, D 分别为移位矩阵 $\boldsymbol{S}$ 的第 1 行最大值、第 2 行最大值、第 2 行与第 1 行之差的最大值、第 1 行与第 2 行之差的最大值.

2 紧致下界的应用场景举例

2.1 Girth-10$^+$ (3,L) QC-LDPC 码的存在性分析

Girth-10$^+$(3,L) QC-LDPC 码的存在性是一个难度非常大的研究课题. 通过定理 1, 该存在性问题可以采用间接方式进行研究. 根据定理 1, 若可以找到一个 $3\times L$ 的移位矩阵 $\boldsymbol{S}$ 使 $g(\boldsymbol{H}_{\mathrm{Q}})\geqslant 10$ 对于某个整数 Q 成立, 则所有码长为 $N=PL(P\geqslant 2\max\{\mathrm{A,B,C+D}\}+1)$ 的 girth-10$^+$ (3,L) QC-LDPC 码的存在性问题就能全部获得解决.

例 1: 本文作者设计了一种基于模拟退火算法的搜索方法(另文发表), 利用此算法找到一个 3×6 的移位矩阵 $\boldsymbol{S}$, 如式(26)所示. 不难验证, 对于整数 Q=129, $g(\boldsymbol{H}_{\mathrm{Q}})$=10. 根据定理 1, 由于 $\max\{\mathrm{A,B,C+D}\}=\mathrm{B}=90$, 因此对于所有码长 $N=6P\geqslant 6(180+1)=1086$, 有 $g(\boldsymbol{H}_P)\geqslant 10$.

$$\boldsymbol{S}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 3 & 7 & 18 & 26\\ 0 & 10 & 24 & 44 & 77 & 90\end{bmatrix}. \tag{26}$$

例 2: 不难验证, 式(27)所示的 3×6 的移位矩阵 $\boldsymbol{S}$ 对于整数 Q=97 满足 $g(\boldsymbol{H}_{\mathrm{Q}})=10$. 根据定理 1, 由于 $\max\{\mathrm{A,B,C+D}\}=\mathrm{C+D}=134$, 因此对于所有码长 $N=6P\geqslant 6(268+1)=1614$, 有 $g(\boldsymbol{H}_P)\geqslant 10$.

$$\boldsymbol{S}=\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0\\ 0 & 35 & 64 & 51 & 8 & 79\\ 0 & 96 & 73 & 90 & 94 & 31\end{bmatrix}. \tag{27}$$

对于 girth-10$^+$(3,6)QC-LDPC 码, 例 1 和例 2 给出的连续码长最小值分别是 1086 和 1614, 这比文献[16]给出的连续码长最小值(2058)要小得多. 这是由于定理 1 没有对移位矩阵的形式进行任何限定, 因此我们可以在更大范围内寻找合适的移位矩阵.

2.2 基于中国剩余定理的大围长 LDPC 码的构造

利用中国剩余定理可以根据若干码长较短的分量码构造出一个码长较长的新码, 新码的围长至少等于(通常很容易大于)所有分量码的最大围长[31]. 文献[31,32]分别将原始阵列码和大围长的缩短阵列码作为分量码, 结合中国剩余定理构造出了一些围长为 6 和围长大于 6 的 QC-LDPC 码. 在基于中国剩余定理的构造方法中, 所有分量码的循环置换矩阵尺寸 P 值必须互素. 由于阵列码的 P 值只能为素数, 因此这两种方法所构造的 QC-LDPC 码在码长取值方面很不灵活. 如果使用码长允许连续变化的大围长 QC-LDPC 码作为一个分量码, 则利用中国剩余定理就可以构造出围长大且码长灵活的 QC-LDPC 码. 将定理 1 与一些大围长 LDPC 码的搜索构造法[10,14,15]结合在一起, 可以很容易构造出一大批码长连续变化的大围长 QC-LDPC 码. 因此, 定理 1 在基于中国剩余定理的大围长 LDPC 码构造中具有重要用途.

2.3 具有纠错能力保证的 LDPC 码的构造

虽然 LDPC 码在 SPA 等迭代译码算法下具有优异性能, 但是一般并不像传统纠错码类(例如 Golay 码、BCH 码)那样具有纠错能力保证, 即保证可以纠正不多于 n 比特的任意错误. 最近, 文献[33]研究了列重为 3、具有纠错能力保证的 LDPC 码的性质, 发现只要列重为 3 的 LDPC 码具有围长 $g\geqslant 10$, 这种码就可以利用 Gallager-A 算法经过 $g/2$ 次迭代纠正不多于 $g/2-1$ 比特的任意错误. 由于 Gallager-A 算法比 SPA 等迭代译码算法简单得多, 因此具有纠错能力保证的 LDPC 码在特定场合具有重要应用价值. 显然, 利用本文研究成果可以很容易地构造出码长(在一个门限以上)允许任意取值、具有纠错能力保证(4 比特)的 QC-LDPC 码.

3 结语

本文发现并证明了一般 girth-10$^+$(3, L)QC-LDPC 码的一个重要新性质: 给定一个 girth-10$^+$(3, L)QC-LDPC 码, 使用其移位矩阵和任意的循环置换矩阵尺寸 P(P 大于一个由移位矩阵决定的门限)得到的 QC-LDPC 码围长至少为 10. 本文还证明了该门限是一个最优门限, 当 P 等于该门限时 QC-LDPC 码的围长一定小于 10. 值得进一步研究的问题包括: (1) 利用定理 1, 对本文提出的三种应用场景进行深入研究. (2) QC-LDPC 码的最大围长是 12[30], 因此利用本文证明引理 1 的方法对连续码长的 girth-12(3, L) QC-LDPC 码进行探讨, 也是一个非常有意义的研究课题.

参考文献

1 Zhang G H, Wang X M. Construction of low-density parity-check codes based on frequency-hopping sequences.Chin J El, 2009, 18: 141—144
2 张国华, 王新梅. 利用双重扩展 RS 码及循环 MDS 码构造实用化的 LDPC 码. 通信学报, 2008, 29: 100—105
3 Vasic B, Pedagani K, Ivkovic M. High-rate girth-eight low-density parity-check codes on rectangular integer lattices. IEEE Trans Comm, 2004, 52: 1248—1252
4 何善宝, 赵春明, 史志华, 等. 基于稀疏二进制序列的低密度奇偶校验码. 通信学报, 2005, 26: 81—86
5 Fujisawa M, Sakata S. A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8. IEICE Trans Fund El Comm Comp Sci, 2007, E90-A: 1055—1061
6 陶雄飞, 刘卫忠, 邹雪城. 利用几何图形构造不含小环的 LDPC 码. 系统工程与电子技术, 2007, 29: 1965—1968
7 敬龙江, 林竟力, 朱维乐. 无小环的结构化低密度校验码的构造方法. 计算机学报, 2007, 30: 648—654
8 Zhang H, Moura J M F. Geometry based designs of LDPC codes. In: ICC'04, Paris, France, 2004. 762—766
9 Takeshita O Y. A compact construction for LDPC codes using permutation polynomials. In: ISIT 2006. Seattle, USA, 2006. 79—82
10 O'Sullivan M E. Algebraic construction of sparse matrices with large girth. IEEE Trans Inf Theory, 2006, 52: 718—727
11 Milenkovic O, Kashyap N, Leyba D. Shortened array codes of large girth. IEEE Trans Inf Theory, 2006, 52: 3707—3722
12 Tao X F, Kim J M, Liu W Z, et al. Improved construction of low-density parity-check codes based on lattices. In: ISITC2007, Jeonju, Korea, 2007. 208—212
13 Zhang F, Mao X H, Zhou W Y, et al. Girth-10 LDPC codes based on 3-D cyclic lattices. IEEE Trans Veh Tech, 2008, 57: 1049—1060
14 Wu X F, You X H, Zhao C M. A necessary and sufficient condition for determining the girth of quasi-cyclic LDPC codes. IEEE Trans Comm, 2008, 56: 854—857
15 Wang Y, Yedidia J S, Draper S C. Construction of high-girth QC-LDPC codes. In: 5th Int Symp Turbo Codes Rel Top, Lausanne, Switzerland, 2008. 180—185
16 刘磊, 周武旸. 码长连续变化的 QC-LDPC 码的设计. 电子与信息学报, 2009, 31: 2523—2526
17 冯登国, 裴定一. 环 Z_N 上的两种 Chrestenson 谱之间的关系. 科学通报, 1996, 41: 1808—1810
18 张文英, 武传坤, 刘祥忠. 代数免疫阶最高的 Boole 函数的构造和计数. 中国科学 F 辑: 信息科学, 2009, 39: 687—693
19 郭宝安. 一类既非 Bent 基又非线性基的二元 Bent 序列的产生与计数. 科学通报, 1991, 36: 1668—1668
20 郭宝安. 一类二值自相关序列族的构造方法. 科学通报, 1993, 38: 282—282
21 佟晓筠, 崔明根. 基于扰动的复合混沌序列密码的图像反馈加密算法. 中国科学 F 辑: 信息科学, 2009, 39: 588—597
22 陈帅, 钟先信, 巫正中. 无线传感器网络混沌分组密码研究. 中国科学 F 辑: 信息科学, 2009, 39: 357—362
23 孙琦. 一类用于实现密码体制的良好椭圆曲线. 科学通报, 1989, 34: 237—237
24 董晓蕾, 曹珍富. 基于二次域的密码系统的新设计. 中国科学 F 辑: 信息科学, 2009, 39: 526—533
25 李大兴. 破译修改的 Lu-Lee 密码体制. 科学通报, 1990, 35: 1595—1595
26 李大兴. 基于 Euclid 辗转相除法攻破一类公开钥密码体制. 科学通报, 1990, 35: 871—871
27 罗平, 周海建, 王道顺, 等. 对 RSA 公钥密码系统在 d>e 时的一种特殊情形的密码学分析. 中国科学 F 辑: 信息科学, 2009, 39: 815—821
28 韦永壮, 胡予濮. 简化 AES-192 和 AES-256 的相关密钥矩形新攻击. 中国科学 F 辑: 信息科学, 2009, 39: 246—253
29 周亮, 李胜强. 流密码与纠错码联合设计新方向—快速相关攻击译码算法研究进展. 电子科技大学学报, 2009, 38: 555—561
30 Fossorier M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. IEEE Trans Inf Theory, 2004, 50: 1788—1793
31 Liu Y H, Wang X M, Chen R W, et al. Generalized combining method for design of quasi-cyclic LDPC codes. IEEE Comm Lett, 2008, 12: 392—394
32 Jiang X Q, Lee M H. Large girth quasi-cyclic LDPC codes based on the Chinese remainder theorem. IEEE Comm Lett, 2009, 13: 342—344
33 Chilappagari S K, Nguyen D V, Vasic B, et al. Girth of the Tanner graph and error correction capability of LDPC codes. In: Proc. 46th Ann All Conf Comm, Contr Comp, Illinois USA, 2008, THC6.3: 1238—1245

补充材料

附录: $\boldsymbol{s}$ 三行中全部 8-环的分类

本文的补充材料见网络版 csb.scichina.com. 补充材料为作者提供的原始数据, 作者对其学术质量和内容负责.

附录: s 三行中全部 8–环的分类

根据文献[30]中的式(4), 构成 $2k$–环的必要条件是(1) 环经过移位矩阵 s 的 $2k$ 个元素(可以重复); (2) 环在移位矩阵 s 某一行内所经过的元素个数必须为偶数. 我们采用有序数组$(x_1, x_2, \cdots, x_k)$表示一个 $2k$–环$(x_1 \neq x_2, x_2 \neq x_3, \cdots, x_k \neq x_1)$, 其中 x_i 表示构成 $2k$–环的第 $2i$–1 和第 $2i$ 个元素经过第 x_i 行. 例如, 图 1 中 b1 模式所示的环可以表示为(0,2,0,1). 因此, 在 s 三行中出现的所有 8–环可以分别表示为

(1): (0,1,0,2); (2): (0,1,2,1); (3): (0,2,0,1); (4): (0,2,1,2);

(5): (1,0,1,2); (6): (1,0,2,0); (7): (1,2,0,2); (8): (1,2,1,0);

(9): (2,0,1,0); (10): (2,0,2,1); (11): (2,1,0,1); (12): (2,1,2,0);

以上 12 种情形可以划分为 3 个等价类: (1)(3)(6)(9); (2)(5)(8)(11); (4)(7)(10)(12). 不难看出, 每个等价类中的 4 种情况所描述的环在本质上相同, 只不过它们选择不同的起始位置(第 0 行、第 1 行或第 2 行)或不同方向(逆时针或顺时针)对环进行描述而已, 这对环的分析没有任何影响. 我们选择情形(3)(2)(4)作为每个等价类的代表, 它们分别对应于图 1 中的模式 b1, b2 和 b3.