中国科学: 信息科学 2012 年 第 42 卷 第 3 期: 343–351
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

一类基于 $B_2(\mathrm{mod}\ m)$ 序列的准循环 LDPC 码

张国华[①②*], 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, 西安 710071
② 中国空间技术研究院西安分院, 西安 710100
* 通信作者. E-mail: zhangghcast@163.com

收稿日期: 2008–08–12; 接受日期: 2011–03–31
国家重点基础研究发展计划 (批准号: 2010CB328300)、国家自然科学基金 (批准号: 61001130, 61001131) 和高等学校学科创新引智计划 (批准号: B08038) 资助项目

摘要 基于 $B_2(\mathrm{mod}\ m)$ 序列, 提出一种构造二元低密度奇偶校验 (LDPC) 码的新方法. 这类编码的校验矩阵列重为 3、行重为任意整数, 并且具有准循环 (QC) 结构. 校验矩阵对应的 Tanner 图围长至少为 8, 对应的最小距离至少为 12. 当 m 为素数时, 提出一种减少 8 环的方法, 使得 Tanner 图中 4 类可能的 8 环中两类被完全消除. 仿真结果表明, m 为素数时新 LDPC 码的译码性能优于渐进边增长 (PEG) 算法随机产生的 (准) 规则 LDPC 码. 此外, 提出一种基于邻域扩展搜索的启发式算法, 利用该算法可以获得长度接近或达到上界的 $B_2(\mathrm{mod}\ m)$ 序列.

关键词 低密度奇偶校验 (LDPC) 码 准循环 (QC) 码 循环置换矩阵 围长 迭代译码

1 引言

由于低密度奇偶校验 (low-density parity-check, LDPC) 码具有逼近 Shannon 理论极限的译码性能, 因而近十年来成为编码理论学者的主要研究课题. LDPC 的构造方法可以分为两种: 随机方法和代数方法. 在随机方法中, 1997 年 MacKay 等 [1] 提出的带约束的随机方法和 2005 年 Hu 等 [2] 提出的渐进边增长 (progressive edge-growth, PEG) 方法是目前译码性能最好的两种著名方法. PEG 方法在中短码长情况下的性能明显优于 MacKay 方法, 被认为是目前构造中短码长 LDPC 码的最好方法之一. 虽然 PEG-LDPC 码的校验矩阵通过一般的线性时间编码原理可以被裁剪成三角形结构, 从而实现线性时间编码, 但是其编码器的实现复杂度仍然很高.

在代数方法中, 2001 年 Kou 等 [3] 提出了基于有限几何 (finite-geometry, FG) 的 LDPC 码构造方法, 2007 年 Lan 等 [4] 提出了基于有限域 (finite field, FF) 的 LDPC 码构造方法. 这些方法构造的 LDPC 码可以利用反馈移位寄存器实现线性时间编码, 并且在较高的码率 (典型值 0.8~0.9) 或者较长的分组长度 (典型值 8000~60000) 条件下可以获得与理论极限十分接近的译码性能. 然而, FG 方法构造的中等码率 (0.5~0.7) 的 LDPC 码, 即使码长达到 8000~12000 比特的量级, 其性能仍然与理论限相距 4~6 dB[3]. Lan 等 [4] 利用 FF 方法构造出了两个性能优异的 0.5 码率的中短码 (长度分别为 4032 和 1890) , 但是由于使用了掩模 (masking) 矩阵和度分布对技术, 校验矩阵的描述变得比较复杂, 校验矩阵的结构变得不规则, 因而在一定程度上提高了编码器的实现复杂性. 此外, PEG-LDPC

引用格式: 张国华, 王新梅. 一类基于 $B_2(\mathrm{mod}\ m)$ 序列的准循环 LDPC 码. 中国科学: 信息科学, 2012, 42: 343–351

码、FG-LDPC 码和 FF-LDPC 码, 它们的共同特点是建立在有限几何、有限域和图论等比较高深抽象的数学基础上, 这对 LDPC 码的应用和推广带来一定困难.

本文基于一种特殊的整数序列 ——$B_2(\mathrm{mod}\ m)$ 序列, 构造了一类可以利用反馈移位寄存器实现线性时间编码的二元准循环 (quasi-cyclic, QC) LDPC 码 (本文称为 B2M-LDPC 码). 在某些参数下, B2M-LDPC 码的译码性能优于相应的 PEG-LDPC 码. 此外, 设计 B2M-LDPC 码的数学基础仅限于整数加法、乘法和取模运算, 因而在某些实用场合具有独特的竞争优势.

2 B2M-LDPC 码的构造方法

设 m, L 是正整数. 本文研究的校验矩阵 $\boldsymbol{H}$ 具有式 (1) 所描述的结构.

$$\boldsymbol{H}=\left[\begin{array}{cccc}\boldsymbol{H}_0 & \boldsymbol{0} & \cdots & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{H}_1 & \cdots & \boldsymbol{0}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{H}_{L-1}\\ \hline \boldsymbol{I}_1 & \boldsymbol{I}_1 & \cdots & \boldsymbol{I}_1\end{array}\right], \tag{1}$$

其中, $\boldsymbol{H}_i(0\leqslant i\leqslant L-1)$ 是一个 $2\times L$ 的阵列, 阵列中的每个元素是一个 $m\times m$ 的循环置换矩阵, 因此 $\boldsymbol{H}_i$ 可以看作是一个 $2m\times Lm$ 的矩阵. $\boldsymbol{0}$ 是一个 $2m\times Lm$ 的全零矩阵, $\boldsymbol{I}_1$ 是一个 $Lm\times Lm$ 的单位方阵, 其对角线上的元素均为 1, 其他位置上的元素均为 0. 可见 $\boldsymbol{H}$ 是一个 $3Lm\times L^2m$ 的矩阵, 列重为 3, 行重为 L, 对应 LDPC 码的设计码率为 $1-3/L$, 码长为 L^2m.

不失一般性, $\boldsymbol{H}_i$ 可以表示为

$$\boldsymbol{H}_i=\left[\begin{array}{cccc}\boldsymbol{I}(\beta_{i,1}) & \boldsymbol{I}(\beta_{i,2}) & \cdots & \boldsymbol{I}(\beta_{i,L})\\ \boldsymbol{I}(\alpha_{i,1}+\beta_{i,1}) & \boldsymbol{I}(\alpha_{i,2}+\beta_{i,2}) & \cdots & \boldsymbol{I}(\alpha_{i,L}+\beta_{i,L})\end{array}\right], \tag{2}$$

其中, $\boldsymbol{I}(v)$ 是一个 $m\times m$ 的循环置换矩阵, 定义与文献 [5] 完全一致: 即对于 $0\leqslant r\leqslant m-1$, 第 r 行第 $r+v(\mathrm{mod}\ m)$ 列位置上的元素为 1, 其他位置上的元素均为 0.

引理 1 若 $\boldsymbol{H}_i$ 对应的 Tanner 图不含 4 环, 则 $\boldsymbol{H}$ 对应的 Tanner 图围长至少为 8; 若以 $\boldsymbol{H}_i$ 为校验矩阵的码具有最小距离 $d_{\boldsymbol{H}_i}$, 则以 $\boldsymbol{H}$ 为校验矩阵码具有最小距离 $d_{\boldsymbol{H}}\geqslant 2\min_{0\leqslant i<L}(d_{\boldsymbol{H}_i})$.

证明 由 $\boldsymbol{H}$ 的结构立即可证引理 1.

注 1 文献 [6] 中的校验矩阵 $\boldsymbol{H}^3_{\mathrm{SPC}}$ 在形式上与上述校验矩阵 $\boldsymbol{H}$ 类似; 但是, $\boldsymbol{H}$ 中的 $\boldsymbol{H}_i$ 是由循环置换矩阵构成的阵列, 而 $\boldsymbol{H}^3_{\mathrm{SPC}}$ 中的 $\boldsymbol{H}^2_{\mathrm{SPC}}$ 则不是. 令 $m=L$, 且 $\boldsymbol{H}_0=\boldsymbol{H}_1=\cdots=\boldsymbol{H}_{L-1}=\boldsymbol{H}^2_{\mathrm{SPC}}$, 且 $\boldsymbol{H}^2_{\mathrm{SPC}}$ 如式 (3) 所描述, 则 $\boldsymbol{H}$ 在形式上退化为 $\boldsymbol{H}^3_{\mathrm{SPC}}$.

$$\boldsymbol{H}^2_{\mathrm{SPC}}=\left[\begin{array}{cccc}\boldsymbol{H}_{\mathrm{SPC}} & \boldsymbol{0} & \cdots & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{H}_{\mathrm{SPC}} & \cdots & \boldsymbol{0}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{H}_{\mathrm{SPC}}\\ \hline \boldsymbol{I}_2 & \boldsymbol{I}_2 & \cdots & \boldsymbol{I}_2\end{array}\right], \tag{3}$$

其中, $\boldsymbol{H}_{\mathrm{SPC}}$ 和 $\mathbf{0}$ 分别是 $1\times L$ 的全 1 矩阵和全 0 矩阵, $\boldsymbol{I}_2$ 是一个 $L\times L$ 的单位方阵, 其对角线上的元素均为 1, 其他位置上的元素均为 0. 可见, $\boldsymbol{H}_{\mathrm{SPC}}^2$ 是一个 $2L\times L^2$ 的矩阵, $\boldsymbol{H}_{\mathrm{SPC}}^3$ 是一个 $3L^2\times L^3$ 的矩阵. $\boldsymbol{H}_{\mathrm{SPC}}^3$ 对应的 LDPC 码的设计码率为 $1-3/L$, 码长为 L^3. 文献 [6] 的研究结果表明, 虽然 $\boldsymbol{H}_{\mathrm{SPC}}^3$ 对应的 Tanner 图围长为 8, 对应 LDPC 码最小距离为 8, 但是译码性能却不理想. 本文的研究目标是, 根据式 (1) 所述结构设计一类校验矩阵, 它所对应的 LDPC 码具有优异的译码性能.

根据引理 1, 提高 $d_{\boldsymbol{H}}$ 的一个有效方法是尽量提高 $d_{\boldsymbol{H}_i}$. 然而, $d_{\boldsymbol{H}_i}$ 有一个上限.

引理 2 $d_{\boldsymbol{H}_i}\leqslant 6$.

证明 根据文献 [5] 定理 2.5, $\boldsymbol{H}_i$ 对应的 Tanner 图围长至多为 12. 又根据文献 [7] 引理 3.7, $d_{\boldsymbol{H}_i}$ 等于 $\boldsymbol{H}_i$ 对应的 Tanner 图围长的一半. 因此 $d_{\boldsymbol{H}_i}$ 至多为 6. 证毕.

如何设计 $\boldsymbol{H}_i$, 才能使相应的 $d_{\boldsymbol{H}_i}$ 达到最大值 6? 为了回答这一问题, 我们首先引入 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列的概念 [8]. $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列是 $\boldsymbol{Z}_m=\{0,1,\ldots,m-1\}$ 的一个子集, 在该子集中任意两个元素 (可以相同) 之和 (模 m) 互不相同. 数学上严格的定义如下:

定义 1 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列 $\boldsymbol{A}=\{\alpha_1,\alpha_2,\ldots,\alpha_k\}$ 是 $\boldsymbol{Z}_m=\{0,1,\ldots,m-1\}$ 的一个子集, 对于任意 $x\in\boldsymbol{Z}_m$ 均满足 $r_{\boldsymbol{A}}(x)=|\{(a,b):a,b\in\boldsymbol{A},a\leqslant b,x=a+b(\mathrm{mod}\ m)\}|\leqslant 1$.

引理 3 对于任意 $0\leqslant i\leqslant L-1$, $d_{\boldsymbol{H}_i}=6$ 当且仅当 $\{\alpha_{i,1},\alpha_{i,2},\ldots,\alpha_{i,L}\}$ 是 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列.

证明 根据文献 [5] 推论 2.1 和定理 2.5, $\boldsymbol{H}_i$ 对应的 Tanner 图围长只可能是 4, 8, 12. 根据文献 [5] 关系式 (4) , $\boldsymbol{H}_i$ 不含 4 环的充要条件是 (a):

$$\alpha_{i,I}\neq\alpha_{i,J}(\mathrm{mod}\,m)\quad(I\neq J,1\leqslant I,J\leqslant L).$$

根据文献 [5] 关系式 (4) , 校验矩阵 $\boldsymbol{H}_i$ 不含 8 环的充要条件是 (b):

$$\alpha_{i,J}+\alpha_{i,R}\neq\alpha_{i,I}+\alpha_{i,K}(\mathrm{mod}\,m)\quad(I\neq J,J\neq K,K\neq R,R\neq I,1\leqslant I,J,K,R\leqslant L).$$

在条件 (b) 中令 $I=K,J=R$, 则有 $2\alpha_{i,J}\neq 2\alpha_{i,I}(\mathrm{mod}\,m)$, 由此可知条件 (b) 蕴含条件 (a) .

所以, 校验矩阵 $\boldsymbol{H}_i$ 不含 4 环和 8 环 (即围长为 12, $d_{\boldsymbol{H}_i}=6$) 的充要条件是 (b) . 根据定义 1, 条件 (b) 与 "$\{\alpha_{i,1},\alpha_{i,2},\ldots,\alpha_{i,L}\}$ 构成 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列" 这一条件等价. 证毕.

注 2 文献 [9] 在研究围长为 12 的多元 LDPC 码时曾指出了条件 (b) , 但是没有揭示出条件 (b) 与 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列之间的等价关系. 另外, 对于如何选择满足条件 (b) 的序列, 文献 [9] 得出了一个错误结论, 我们将在第 3 节的注 3 中加以说明.

引理 3 建立了 $d_{\boldsymbol{H}_i}$ 达到最大值和 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列之间的关系, 由此可以得到本文的第一个重要结果.

定理 1 给定一个长度为 L 的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列, 则可以构造一个校验矩阵 $\boldsymbol{H}$, 具有以下性质: 1) 维数为 $3Lm\times L^2m$; 2) 列重为 3, 行重为 L; 3) 对应的 Tanner 图围长至少为 8; 4) 对应的 LDPC 码设计码率为 $1-3/L$, 码长为 L^2m; 5) 对应的 LDPC 码的最小距离至少为 12.

3 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列的性质及设计方法

3.1 性质

根据第 2 节的讨论, 校验矩阵 $\boldsymbol{H}$ 的构造问题被转化为 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列的设计问题. 首先介绍一些 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列的基本性质, 这些性质对于序列设计十分有益.

性质 1 设 $\boldsymbol{A}$ 是 $B_2(\mathrm{mod}\ m)$ 序列, D 是满足 $\gcd(D,m)=1$ 的任意整数, T 是任意整数, 则 $\boldsymbol{A}'=\{D\alpha+T:\alpha\in\boldsymbol{A}\}$ 也是 $B_2(\mathrm{mod}\ m)$ 序列. 其中 D 和 T 分别称为扩张因子和平移因子.

定义 2[9] Hoey 序列是一个由非负整数组成的无限集合 $\boldsymbol{H}_{\mathrm{oey}}=\{h_0,h_1,h_2,\ldots\}$, 其中 h_i 是使序列保持严格递增且每两项元素 (可以相同) 之和两两不同的最小非负整数.

性质 2 Hoey 序列中不大于 $(m-1)/2$ 的全体元素构成的序列是 $B_2(\mathrm{mod}\ m)$ 序列.

证明 根据定义 1 和定义 2 容易证明性质 1 和性质 2.

性质 3[10,11] 设 $\boldsymbol{A}$ 是 $B_2(\mathrm{mod}\ m)$ 序列, 用 $|\boldsymbol{A}|$ 表示 $\boldsymbol{A}$ 的长度, 则有 $|\boldsymbol{A}|(|\boldsymbol{A}|-1)\leqslant m-1$.

注 3 文献 [9] 利用 Hoey 序列 (0, 1, 3, 7, 12, 20, 30, 44, 65, 80, 96, 122, ...) 前 12 项构造了一个 128 元 [1524, 1271] UQ-LDPC 码, 然而 Tanner 图的围长并没有达到声称的最大值 12 (实际只达到 8). 产生这一问题的原因是, Hoey 序列前 12 项不可能满足条件 (b) , 因为根据性质 3 可知长度大于 11 的 $B_2(\mathrm{mod}\ 127)$ 序列不存在. 文献 [9] 利用 Hoey 序列前 8 项构造了一个 64 元 [504, 379]UQ-LDPC 码, Tanner 图的围长也没有达到声称的最大值 12. 根据性质 2, Hoey 序列中所有不大于 31 的元素可以保证构成一个 $B_2(\mathrm{mod}\ 63)$ 序列. 由于元素 44 不满足性质 2 所规定的条件, 因此不能保证构成 $B_2(\mathrm{mod}\ 63)$ 序列. 事实上, 由于 20+44=0+1 (mod 63), 因此 Hoey 序列的前 8 项不是 $B_2(\mathrm{mod}\ 63)$ 序列.

3.2 设计方法

设 p 是素数, q 是素数幂. 当 $m=q^2+q+1, q^2-1$ 或 p^2-p 时, 可以利用 3 种著名的代数方法 [10] (Ruzsa 构造法、Bose 构造法和 Singer 构造法) 构造出长度达到性质 3 所述上界的 $B_2(\mathrm{mod}\ m)$ 序列. 然而, 代数方法在参数 m 的取值上十分受限. 此外, 后两种方法涉及非常复杂的有限域运算, 因此对实用而言代数方法不是最合适的方法. 本文首先介绍一种产生 $B_2(\mathrm{mod}\ m)$ 序列的穷举法, 然后提出一种新的启发式搜索算法. 第一种方法适用于 m 较小 (例如至多为 64) 的情形, 第二种方法适用于 m 不太大 (例如至多为 127) 的情形. 根据定理 1 的性质 4), 本文新构造的 LDPC 码的码长为 L^2m, 再根据性质 3 有 $L^2m\approx m^2$. 因此, m 取 127 时相应的码长约为 16000. 本文目标是设计短码长和中等码长的 LDPC 码, 因此这两种方法完全可以满足应用需要.

(1) 穷举法. 对于较小的 m, 获取 $B_2(\mathrm{mod}\ m)$ 序列的一种平凡方法是采用穷举搜索：罗列出全部序列, 然后逐一判别该序列是否是 $B_2(\mathrm{mod}\ m)$ 序列. 利用性质 1 穷举搜索法的搜索速度可以显著提高.

对于 $m\leqslant 64$, 使用穷举法搜索 $B_2(\mathrm{mod}\ m)$ 序列, 搜索到的序列长度都达到了性质 3 所述的上界 $(22,32\sim 34,43\sim 47,58\sim 62$ 除外, 在这 14 个取值下上界比实际最大长度大 1) .

(2) 邻域扩展搜索法. 获取 $B_2(\mathrm{mod}\ m)$ 序列的另一种思路是采用随机搜索. 为了加快随机搜索的速度, 我们引入邻域扩展搜索 (neighbor and extension search, NES) 的概念. 设 $\boldsymbol{A}$ 是一个长度为 $n-1$ 的 $B_2(\mathrm{mod}\ m)$ 序列. 对 $\boldsymbol{A}$ 进行邻域搜索是指, 在集合 $\{\boldsymbol{\Lambda}|n-2\leqslant|\boldsymbol{\Lambda}\cap\boldsymbol{A}|\}$ 中找出全部 $B_2(\mathrm{mod}\ m)$ 序列. 可见, 邻域搜索的结果中包括 $\boldsymbol{A}$ 本身. 对 $\boldsymbol{A}$ 进行扩展搜索是指, 在序列集合 $\{\boldsymbol{A}\cap\beta|\beta\in\boldsymbol{Z}_m,\beta\notin\boldsymbol{A}\}$ 中找出全部 $B_2(\mathrm{mod}\ m)$ 序列. 对 $\boldsymbol{A}$ 实施 NES 操作是指, 先对 $\boldsymbol{A}$ 进行邻域搜索, 然后对所得的全体序列进行扩展搜索. 显然, 对 $\boldsymbol{A}$ 实施 NES 操作后可能得到若干条长度为 n 的 $B_2(\mathrm{mod}\ m)$ 序列, 也可能一个都得不到 (此时 NES 失效) .

根据上述思路, 可以设计以下算法 (记为 NES1) .

算法 1 (NES1)

OK=0;
while OK 为 0
flag=0;
while flag 为 0
随机产生由 $n-1$ 个互异整数组成的序列 $\boldsymbol{A}$, 整数在区间 [0, $m-1$] 取值.
若 $\boldsymbol{A}$ 是 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列, 则置 flag=1.
end
对 $\boldsymbol{A}$ 进行 NES 操作, 所得序列集记录在 BUF 中.
若 BUF 至少包含一条序列, 则搜索成功, OK=1.
end
删除 BUF 中重复出现的序列, 结果记录在 BUFO 中.
输出 BUFO;

设 $\boldsymbol{A}$ 和 $\boldsymbol{A}^+$ 分别是长度为 $n-1$ 和 n 的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列, 其满足 $|\boldsymbol{A}\cap\boldsymbol{A}^+|\geqslant n-2$. 则算法 1 在 $\boldsymbol{A}$ 基础上必然可以找到 $\boldsymbol{A}^+$. 由于 $\boldsymbol{A}$ 是随机产生的, 因此该算法可以在整个解空间实现快速搜索.

通过重复执行算法 NES1, 可以在长度为 $n-1$ 的序列基础上搜索长度为 n+1 的序列. 该算法记为 NES2.

算法 2 (NES2)

OK=0;
while OK 为 0
利用算法 1 求出 BUFO, 设其中包含 R 个长度为 n 的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列.
for i=1:R
对第 i 个序列进行 NES 操作, 所得序列集记录在 BUF 中.
若 BUF 至少包含一条序列, 则搜索成功, 跳出 for 循环, OK=1;
end
end

设 $\boldsymbol{A}$ 和 $\boldsymbol{A}^+$ 分别是长度为 $n-1$ 和 $n+1$ 的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列, 且满足 $|\boldsymbol{A}\cap\boldsymbol{A}^+|\geqslant n-3$. 则算法 2 在 $\boldsymbol{A}$ 基础上必然可以找到 $\boldsymbol{A}^+$.

对于 $64<m\leqslant 127$, 采用 NES 算法搜索 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列. 在 $m=65\sim 73, 80, 85\sim 91, 107\sim 110$ 和 120 下, NES 算法都找到了长度达上界的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列, 在其他参数下 NES 算法找到的序列长度比上界小 1. 根据 Shearer 发布的网页结果 (http://www.research.ibm.com/people/s/shearer/mgrule.htm), 这是可以达到的最好结果.

4 减少 8 环和低重量码字的方法

由式 (1) 所述校验矩阵 $\boldsymbol{H}$ 的结构易知, 若存在 $i,j(i\neq j, 0\leqslant i,j\leqslant L-1)$ 使得 $\boldsymbol{H}_i=\boldsymbol{H}_j$ 成立, 则 $\boldsymbol{H}$ 对应的 Tanner 中必然存在大量 8 环, 并且 $\boldsymbol{H}$ 对应的 LDPC 码中必然存在大量重量为 12 的码字. 因此, 为了消除这种十分明显的 8 环和低重量码字, $\boldsymbol{H}_i(0\leqslant i\leqslant L-1)$ 应该互不相同.

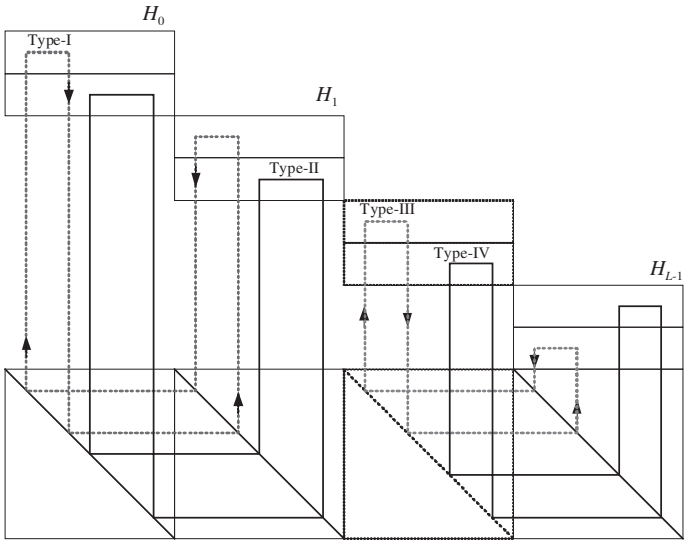

图 1　校验矩阵中 4 种可能的 8 环类型

Figure 1　Four possible types of 8-cycles in the parity-check matrix

设 $0<\beta_0<\beta_1<\cdots<\beta_{L-1}<m$ 且与 m 互素, $\{\alpha_1<\alpha_2<\cdots<\alpha_L\}$ 是一个 $B_2(\mathrm{mod}\ m)$ 序列. 对于 $0\leqslant i\leqslant L-1$ 和 $1\leqslant J\leqslant L$, 令 $\beta_{i,J}=\beta_i J$, $\alpha_{i,J}=\beta_i\alpha_J$. 则式 (2) 可以表示为

$$\boldsymbol{H}_i=\begin{bmatrix}\boldsymbol{I}(\beta_i 1) & \boldsymbol{I}(\beta_i 2) & \cdots & \boldsymbol{I}(\beta_i L)\\ \boldsymbol{I}(\beta_i(\alpha_1+1)) & \boldsymbol{I}(\beta_i(\alpha_2+2)) & \cdots & \boldsymbol{I}(\beta_i(\alpha_L+L))\end{bmatrix}. \tag{4}$$

由式 (4) 可知 $\boldsymbol{H}_i(0\leqslant i\leqslant L-1)$ 两两不同, 根据性质 1 和引理 3 可知 $\boldsymbol{H}_i$ 均满足 $d_{\mathbf{H}_i}=6$.

由于 $\boldsymbol{H}_i$ 不含 8 环, 根据 $\boldsymbol{H}$ 的结构可知 $\boldsymbol{H}$ 中只可能出现 4 种类型的 8 环, 如图 1 所示.

引理 4　当 m 为素数时, 利用式 (4) 配置 $\boldsymbol{H}_i(0\leqslant i\leqslant L-1)$, 则校验矩阵 $\boldsymbol{H}$ 中的 Type-I 型 8 环可以完全消除.

证明　出现 Type-I 型 8 环的条件是, 存在两个子矩阵 $\boldsymbol{H}_I,\boldsymbol{H}_J(0\leqslant I<J\leqslant L-1)$ 满足

$$\beta_I Q-\beta_I P=\beta_J Q-\beta_J P(\mathrm{mod}\ m)\ (0\leqslant P<Q\leqslant L-1), \tag{5}$$

即 $(\beta_J-\beta_I)(Q-P)=0(\mathrm{mod}\ m)$. 由于 m 是素数, 且 $0<\beta_J-\beta_I<m, 0<Q-P<m$, 所以式 (5) 不可能成立.

引理 5　当 m 为素数且满足 $\alpha_L-\alpha_1\leqslant m-L$ 时, 利用式 (4) 配置 $\boldsymbol{H}_i(0\leqslant i\leqslant L-1)$, 则校验矩阵 $\boldsymbol{H}$ 中的 Type-II 型 8 环可以完全消除.

证明　出现 Type-II 型 8 环的条件是, 存在两个子矩阵 $\boldsymbol{H}_I,\boldsymbol{H}_J(0\leqslant I<J\leqslant L-1)$ 满足

$$\beta_I(\alpha_P+Q)-\beta_I(\alpha_Q+P)=\beta_J(\alpha_P+Q)-\beta_J(\alpha_Q+P)(\mathrm{mod}\ m)(0\leqslant P<Q\leqslant L-1), \tag{6}$$

即 $(\beta_J-\beta_I)\{(\alpha_Q-\alpha_P)+(Q-P)\}=0(\mathrm{mod}\ m)$.

因为 $\alpha_Q-\alpha_P\leqslant\alpha_L-\alpha_1\leqslant m-L<m-(Q-P)$, 所以 $(\alpha_Q-\alpha_P)+(Q-P)<m$, 因此式 (6) 不可能成立.

表 1 两个 B2M-LDPC 码的参数

Table 1 Parameters of the two B2M-LDPC codes

code#	m	$\{\alpha_1,\alpha_2,\ldots,\alpha_L\}$	$\{\beta_0,\beta_1,\ldots,\beta_{L-1}\}$	(n,k)	Girth	Code rate
1	31	{0,1,3,8,12,18}	{19,23,25,26,27,29}	(1116,565)	8	0.5063
2	67	{0,1,3,7,12,20,30,46}	{1,2,4,8,13,21,31,47}	(4288,2689)	8	0.6271

引理 6 对于任意长度为 L 的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列 $\boldsymbol{A}=\{\alpha_1<\alpha_2<\cdots<\alpha_L\}$, 都存在一个 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列 $\boldsymbol{A}'=\{\alpha'_1<\alpha'_2<\cdots<\alpha'_L\}$ 满足 $\alpha'_L-\alpha'_1\leqslant m-L$.

证明 在所有差值 $d_1=\alpha_2-\alpha_1, d_2=\alpha_3-\alpha_2,\ldots,d_{L-1}=\alpha_L-\alpha_{L-1}$ 和 $d_L=m+\alpha_1-\alpha_L$ 中, 一定存在某个差值 $d_k(1\leqslant k\leqslant L)$ 满足 $d_k\geqslant L$, 否则 $m=\sum_{i=1}^{L}d_i\leqslant L(L-1)\leqslant m-1$, 矛盾.

令 $D=m-1$, $T=\alpha_k$, 定义 $\boldsymbol{A}'=(D\{\alpha_k,\alpha_{k-1},\ldots,\alpha_1,\alpha_L,\alpha_{L-1},\ldots,\alpha_{k+1}\}+T)\ \mathrm{mod}\ m$. 由性质 1 可知 $\boldsymbol{A}'$ 是 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列. 经过化简可得

$$\begin{aligned}\boldsymbol{A}'&=\{0,\alpha_k-\alpha_{k-1},\ldots,\alpha_k-\alpha_1,m+\alpha_k-\alpha_L,m+\alpha_k-\alpha_{L-1},\ldots,m+\alpha_k-\alpha_{k+1}\}\\&:=\{\alpha'_1,\alpha'_2,\ldots,\alpha'_L\}\end{aligned}$$

容易看出, $\boldsymbol{A}'$ 满足 $\alpha'_1<\alpha'_2<\cdots<\alpha'_L$, 并且 $\alpha'_L-\alpha'_1=(m+\alpha_k-\alpha_{k+1})-0\leqslant m-L$.

根据引理 4~6 和定理 1, 可以得到本文的第二个重要结果.

定理 2 设 m 为素数. 给定一个长度为 L 的 $\mathrm{B}_2(\mathrm{mod}\ m)$ 序列, 则可以构造一个满足定理 1 性质的校验矩阵 $\boldsymbol{H}$, 并且其中的 Type-I 型 8 环和 Type-II 型 8 环可以完全消除.

5 例子和仿真

本节研究 B2M-LDPC 码的译码性能, 并与 PEG-LDPC 码的性能进行比较. 我们构造了两个 B2M-LDPC 码, 它们的码长和码率基本覆盖本文的研究范围, 其他具体参数如表 1 所示. 由表 1 可知, m 和 $\{\alpha_1,\alpha_2,\ldots,\alpha_L\}$ 满足引理 4 和引理 5 的条件.

对于 code 1, 我们选择 (1008, 504)PEG-LDPC 码 [12] 作为比较对象. 对于 code 2, 我们根据 PEG 算法构造了一个 (4288, 2689)PEG-LDPC 码, 该码对应的校验矩阵维数为 1599×4288, 列重为 3, 行重为 7 (31 行, 占 1.94%), 8 (1465 行, 占 91.62%) 和 9 (103 行, 占 6.44%), 校验矩阵对应的 Tanner 图围长为 10. 仿真条件：迭代译码算法为 SPA 算法, 最大迭代次数设定为 80, 信道模型为 AWGN, 调制方式为 BPSK. 为了保证仿真数据的可靠性, 每个仿真点是在捕获到至少 100 个错误帧后计算得出的.

图 2 描绘了 code 1 的误比特率和误帧率仿真结果. 在 BER=10^{-5} 时, code 1 的译码性能距离 1/2 码率的 Shannon 限 (0.18 dB) 仅为 2.3 dB, 对于码长约为 1000 的规则 LDPC 短码而言, 这是很好的性能. 在 BLER=10^{-4} 时, code 1 的误帧率相对于 PEG 码的性能改善超过了 0.1 dB. code 1 码与 PEG 码的长度差异很小 (108 bits) , 因此长度差异对译码性能的影响十分有限. code 1 在仿真中没有出现不可检测错误, 因此其最小距离可能比定理 1 所述的下界 12 要大很多, 这或许是其性能得以提高的主要因素.

图 3 描绘了 code 2 的误比特率和误帧率仿真结果. 在 BER=10^{-5} 时 code 2 的译码性能距离 5/8 码率的 Shannon 限 (0.80 dB) 仅为 1.4 dB. code 2 的误比特率和误帧率性能略优于 PEG 码. 在 Eb/No= 2.4 dB 时, code 2 和 PEG 码的误帧率分别约为 4.0×10^{-6} 和 1.0×10^{-5}. 在 PEG 码的仿真中出现了不

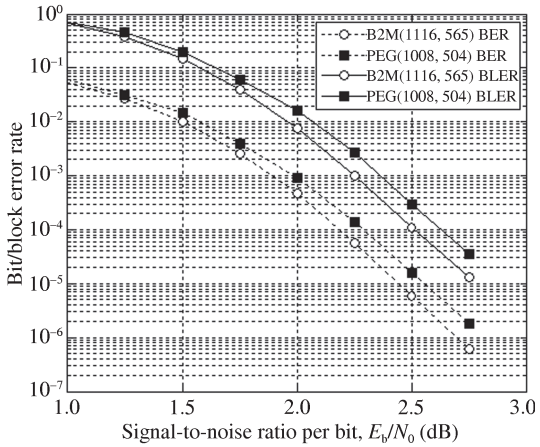

图 2　Code 1 的误比特率和误帧率仿真结果

Figure 2　Simulation results of the bit (block) error rate for code 1

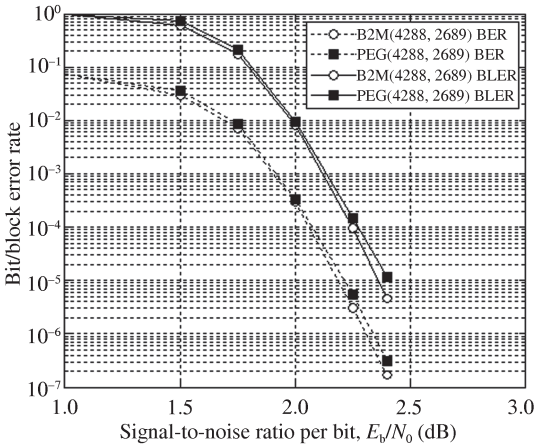

图 3　Code 2 的误比特率和误帧率仿真结果

Figure 3　Simulation results of the bit (block) error rate for code 2

可检测错误, 并出现了重量为 14 的码字. 在 code 2 的仿真中没有出现不可检测错误, 因此 code 2 具有较大的最小距离可能是使误帧率性能提高的主要原因.

6　结束语

本文基于 $B_2(\mathrm{mod}\ m)$ 序列构造了一类二元规则 LDPC 码 (B2M-LDPC 码) , 这类 LDPC 码的校验矩阵列重为 3、行重为 L, 具有准循环结构, 因而可实现线性时间编码. 校验矩阵对应的 Tanner 图围长至少为 8, 对应的 LDPC 码最小距离至少为 12. 对于 m 为素数的情形, 提出一种消除 Tanner 图中两类 8 环的方法. 仿真结果表明, m 为素数时 B2M-LDPC 码的译码性能优于 (准) 规则 PEG-LDPC 码. B2M-LDPC 码的构造基础可以归结为 $B_2(\mathrm{mod}\ m)$ 序列的设计. 本文在介绍穷举法的基础上, 提出一种设计 $B_2(\mathrm{mod}\ m)$ 序列的新启发式算法 —— 邻域扩展搜索法. 与 PEG, FG 和 FF 方法相比, B2M-LDPC 码构造方法的最大优势在于数学基础非常简单, 仅限于整数加法、乘法和取模运算.

参考文献

1　MacKay D J C, Neal R M. Near Shannon limit performance of low density parity check codes. IEE Electron Lett, 1997, 33: 457–458

2　Hu X Y, Eleftheriou E, Arnold D M. Regular and irregular progressive edge-growth Tanner graphs. IEEE Trans Inf Theory, 2005, 51: 386–398

3　Kou Y, Lin S, Fossorier M P C. Low-density parity-check codes based on finite geometries: a rediscovery and new results. IEEE Trans Inf Theory, 2001, 47: 2711–2736

4　Lan L, Zeng L Q, Tai Y Y, et al. Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: a finite field approach. IEEE Trans Inf Theory, 2007, 53: 2429–2458

5　Fossorier M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. IEEE Trans Inf Theory, 2004, 50: 1788–1793

6　Xu J, Chen L, Zeng L Q, et al. Construction of low-density parity-check codes by superposition. IEEE Trans Commun, 2005, 53: 243–251

7 Hu X Y. Low-delay low-complexity error-correcting codes on sparse graphs. PhD Thesis. Switzerland: Swiss Federal Institute of Technology Lausanne (EPFL), 2002
8 Dimitromanolakis A. Analysis of the Golomb ruler and the Sidon set problems, and determination of large, near-optimal Golomb rulers. PhD Thesis. Chanic: Technical University of Crete, 2002
9 Ge X, Xia S T. Structured non-binary LDPC codes with large girth. IEE Electron Lett, 2007, 43: 1220–1221
10 O'Bryant K. A complete annotated bibliography of work related to Sidon sequences. Electron J Combin, 2004, 11: 1–39
11 Milenkovic O, Kashyap N, Leyba D. Shortened array codes of large girth. IEEE Trans Inf Theory, 2006, 52: 3707–3722
12 Hu X Y, Eleftheriou E, Arnold D M. Progressive edge-growth Tanner graphs. In: Proceedings of the IEEE Global Telecommun Conference, San Antonio, 2001. 995–1001

A class of quasi-cyclic LDPC codes from $\mathbf{B_2}$(mod m) sequences

ZHANG GuoHua[1,2*] & WANG XinMei[1]

1 *State Key Laboratory of Integrated Service Network, Xidian University, Xi'an* 710071, *China;*
2 *China Academy of Space Technology* (*CAST, Xi'an*), *Xi'an* 710100, *China*
*E-mail: zhangghcast@163.com

Abstract A new class of binary low-density parity-check (LDPC) codes is proposed based on B_2(mod m) sequences. The parity-check matrix of such a code has a column weight of three and a row weight of an arbitrary integer, and a quasi-cyclic structure. The parity-check matrix also has a girth at least 8, and corresponds to a code with minimal distance at least 12. When m is prime, an 8-cycles reduction method is presented to completely avoid the two types of 8-cycles within the total four types existed in the Tanner graph. Simulation results show that, for a prime integer m, the new LDPC code outperforms the random (quasi-) regular counterpart generated by the PEG algorithm. Finally, a heuristic algorithm based on a strategy called neighboring extension search is presented to search for the B_2(mod m) sequences whose lengths approach or meet the upper bound.

Keywords low-density parity-check (LDPC) codes, quasi-cyclic (QC) codes, circulant permutation matrix, girth, iterative decoding

ZHANG GuoHua was born in 1977. He received the Ph.D. degree in communication and information system from Xidian University, Xi'an in 2010. Currently, he is a Senior Engineer at China Academy of Space Technology (CAST, Xi'an). His research interests include error-control coding techniques and their application to digital communications.

WANG XinMei was born in 1937. He is currently a Professor and Ph.D. supervisor of Xidian University. His research interests include channel coding, cryptogram and telecommunication network security. He is one of the pioneer researchers in error-correction coding in China. Professor Wang is a fellow of CIC and CIE.