QC-LDPC码的置换矩阵循环移位次数设计

彭 立,朱光喜
(华中科技大学电子与信息工程系,湖北武汉 430074)

摘 要: 本文提出了一种循环移位次数的代数设计方法,该方法可用来构造基于置换矩阵的QC-LDPC码的稀疏奇偶校验矩阵 $\boldsymbol{H}$.这个方法的基本思路是:将构造 $q\times t$ 置换阵列 $\boldsymbol{H}$ 矩阵的问题转化为构造 $q\times t$ 下标矩阵 $S(\boldsymbol{H})=[a_{i,j}]$ 的问题,然后根据 Fosserier 的充分必要条件,设计出能消除小围长(girth)的下标计算表达式 $a_{i,j}=f(q,t,n)$.由该方法构造的 $\boldsymbol{H}$ 矩阵能消除4环长,围长至少是6.

关键词: 低密度奇偶校验码(LDPC码);稀疏奇偶校验矩阵;下标矩阵;围长(girth)
中图分类号: TN919 **文献标识码:** A **文章编号:** 0372-2112 (2010) 04-0786-05

Shift Value Design of Permutation Matrices for QC-LDPC Codes

PENG Li, ZHU Guang-xi
(*Department of Electronics and Information Engineering in Huazhong University of Science and Technology, Hubei, Wuhan* 430074, *China*)

Abstract: This paper presents an algebraic method for designing circulant-shift values of permutation matrices in an array sparse parity-chick matrix which defines the QC-LDPC codes. The basic ideal is that the problem of constructing an array $\boldsymbol{H}$-matrix by the permutation matrix can be converted into the problem of constructing a subscript matrix, and then all elements (subscript values) in this subscript matrix, i.e., the circulant-shift values of all permutation matrices in the array $\boldsymbol{H}$-matrix, can be computed by a well-desinged sequence expression which is a function of the row and column weight of $\boldsymbol{H}$-matrix and the dimension of permutation matrix and can be formed by the necessary and sufficient condition of Fossorier. The $\boldsymbol{H}$-matrix formed by this method can eliminate the cycle 4 and can form at least girth 6.

Key words: low-density parity-check codes; sparse parity-check matrix; subscript matrix; girth.

1 引言

在LDPC码的研究进程中,稀疏奇偶校验矩阵 $\boldsymbol{H}$ 的分块子矩阵阵列结构形成了一类极有研究价值的码类:基于循环置换阵列矩阵的QC-LDPC码类[1~2],该码类目前受到纠错码领域普遍关注.对于LDPC码的 $\boldsymbol{H}$ 矩阵,一个重要的约束条件是:在 $\boldsymbol{H}$ 矩阵或其对应的Tanner图中不存在较小的环线或至少不存在4环线.这里给出最小环线的专门术语:称为围长(即girth[3]).围长的含义是在给定的Tanner图(也称二分图)中,形成最小闭合环路的边数.围长在 $\boldsymbol{H}$ 矩阵中的等效描述是:在 $\boldsymbol{H}$ 矩阵中用水平线连接同行的任意两个1元素,用垂直线连接同列的任意两个1元素,将这些水平线和垂直线相互连接形成的闭合环路称为环线,其中构成的最小闭合环路称为围长.每个确定的 $\boldsymbol{H}$ 矩阵必定存在最小环路,因此必定存在围长,同时还存在大于围长的许多环线.在完全由置换子矩阵构成的阵列 $\boldsymbol{H}$ 矩阵中,围长的确定与置换矩阵的循环移位次数有关[2].

最早出现的规则LDPC码的 $\boldsymbol{H}$ 阵列结构是Gallager在博士论文的附录中提出的[4].此后,Fan于2000年构造了阵列码[5],在他设计的 $\boldsymbol{H}$ 阵列中,子矩阵的循环移位数按 $a_{ij}=\{(i-1)(j-1):i=0,1,2,\cdots q-1,j=0,1,2,\cdots n-1\}$ 的规律排列,这个结构中存在4环线.同年,Tanner提出基于有限循环群理论的阵列 $\boldsymbol{H}$ 矩阵[1],其循环移位次数按 $a_{ij}=\{\alpha^{j-1}\beta^{i-1}:i=1,2,\cdots,q,j=1,2,\cdots,t\}$ 的规律排列,其中要求 q,t,α,β,n 均取素数,他们相互之间必须满足下列关系:α 是 $O(\alpha)=t$ 次单位原根,即 $\alpha^t=1$(模 n),β 是 $O(\beta)=q$ 次单位原根,即 $\beta^q=1$(模 n).在这样严格的参数限制条件下,Tanner构造出一个不包含4、6、8和10环线的 3×5 的 $\boldsymbol{H}$ 矩阵,它是目前唯一被构造出来的围长至少是12的完全由置换子矩阵构成的阵列 $\boldsymbol{H}$ 矩阵,但它的严格的结构参数限制,使码率的取值范围较小.Fossorier为实现 $\boldsymbol{H}$ 矩阵Tanner图不含 $2i$ 围长的结构设计,推导出了具有普遍指导意义的(也是本文要用到的)充分必要条件[2].根据这个充分必要条件,他首次发现在基于完全置换矩阵的规则阵列 $\boldsymbol{H}$ 矩阵中围长不会超过12的普遍规律.他以推导的充分必要条件为约束,用计算机搜索的方法生成了包含6

收稿日期:2008-11-11;修回日期:2009-09-18
基金项目:国家自然科学基金(No.60572050)

围长和8围长的完全由置换矩阵构成的阵列 $\boldsymbol{H}$ 矩阵,其置换矩阵的循环移位次数按 $a_{ij}=\{\alpha^{j-1}\beta^{i-1}:i=1,2,\cdots,q,j=1,2,\cdots,t\}$ 的规律排列,但没有向Tanner那样将 α 和 β 限制为 t 和 q 的单位原根.在 Olgica Milenkovic[6] 的设计方案中,每个循环移位次数的位置由行索引和列索引决定,在列索引满足等差数列的约束条件下,用多元线性齐次方程(文中称为循环控制方程)来描述行索引与矩阵围长的关系,他还提供了循环控制方程与6、8和10围长的对应关系列表和某些6和8围长的结构示意图.

本文的研究内容组织如下:第2部分描述关于QC-LDPC码研究的相关知识,包括阵列 $\boldsymbol{H}$ 矩阵的一般表示形式和约束条件,引出下标矩阵的定义,介绍 Fossorier 的充分必要条件;第3部分是本文的主要研究内容,提出用下标计算表达式设计下标矩阵的方法.根据Fossorier的充分必要条件,证明了下标矩阵的围长特征,给出了下标矩阵的设计实例.第4部分是全文总结和对未来工作的展望.

2　$\boldsymbol{H}$ 矩阵与下标矩阵

2.1　阵列 $\boldsymbol{H}$ 矩阵的结构形式与约束条件

低密度奇偶校验码定义为稀疏奇偶校验矩阵 $\boldsymbol{H}$ 的零空间,因此,研究 LDPC 码的结构问题实际上就是研究 $\boldsymbol{H}$ 矩阵的代数构造方法.这里首先给出需要研究的 $\boldsymbol{H}$ 矩阵的约束条件和基本模型.文献[8]根据 Gallager 的博士论文[4]总结出了规则 $\boldsymbol{H}$ 矩阵应满足的基本约束条件,现重新归纳如下:

(1)设每列含1元素的个数(即列重量,也是 Tanner 图变量节点的度数)为 d_v,一般有 $d_v\geqslant 2$,对于个别码结构,如基于 IRA 结构[10]的 LDPC 码及其它们的变形结构,容许 $d_v=1$.

(2)每行含1元素的个数(即行重量,也是 Tanner 图校验节点的度数)为 d_c,一般有 $d_c\geqslant d_v\geqslant 3$.

(3)任何两列之间同为1的行数(称为重叠数)不超过1,即 $\boldsymbol{H}$ 矩阵中不含四角为1的小方阵[8],也即Tanner图中无4环线.在[4]中将这个约束条件加强为:随着 N 的增加,由规则 LDPC 码的度分布对序列 $\lambda(x)=x^{d_v-1}$ 和 $\rho(x)=x^{d_c-1}$ 所构造的 $\boldsymbol{H}$ 矩阵或 Tanner 图不包含长度为 $2l(N)$ 的环线,其中

$$l(N):=\frac{\ln N-\ln\dfrac{d_vd_c-d_v-d_c}{2d_c}}{\ln[(d_v-1)(d_c-1)]}$$

要求 $l(N)$ 尽可能的大.

(4) d_v 和 d_c 均远小于码字长度 N 和校验方程数 M $(=Nd_v/d_c)$,且当 $N\to\infty$ 时,$d_v/N=d_c/M\to 0$,表明奇偶校验矩阵 $\boldsymbol{H}$ 足够稀疏.

本文要研究的稀疏奇偶校验矩阵 $\boldsymbol{H}$ 是 $q\times t$ 的阵列结构,具有如下表示形式:

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{H}_{a_{11}} & \boldsymbol{H}_{a_{12}} & \cdots & \boldsymbol{H}_{a_{1j}} & \cdots & \boldsymbol{H}_{a_{1t}}\\ \boldsymbol{H}_{a_{21}} & \boldsymbol{H}_{a_{22}} & \cdots & \boldsymbol{H}_{a_{2j}} & \cdots & \boldsymbol{H}_{a_{2t}}\\ \vdots & \vdots & \ddots & \vdots & & \vdots\\ \boldsymbol{H}_{a_{i1}} & \boldsymbol{H}_{a_{i2}} & \cdots & \boldsymbol{H}_{a_{ij}} & \cdots & \boldsymbol{H}_{a_{it}}\\ \vdots & \vdots & & \vdots & \ddots & \vdots\\ \boldsymbol{H}_{a_{q1}} & \boldsymbol{H}_{a_{q2}} & \cdots & \boldsymbol{H}_{a_{qj}} & \cdots & \boldsymbol{H}_{a_{qt}}\end{bmatrix}\tag{1}$$

其中,$\boldsymbol{H}_{a_{ij}}$ 表示在 $\boldsymbol{H}$ 矩阵的分块阵列中第 i 行第 j 列的置换子矩阵,下标 $a_{ij}\in Z$ 表示阵列矩阵中第 i 行第 j 列子矩阵的循环移位次数,其中大写字母 Z 表示整数,正整数表示循环左移,负整数表示循环右移,0表示没有进行循环移位的原始置换矩阵,$1\leqslant i\leqslant q$,$1\leqslant j\leqslant t$.$\boldsymbol{H}$ 矩阵的维数(尺寸大小)是 $qn\times tn=M\times N$,n 是子矩阵维数.

2.2　下标矩阵的定义

观察(1)式的 $\boldsymbol{H}$ 矩阵阵列结构,将每个子矩阵的下标值单独提取出来,组成如下的下标矩阵.

定义1[下标矩阵]　构造一个 $q\times t$ 的矩阵

$$S(\boldsymbol{H})=\begin{bmatrix}a_{q_1,t_1} & a_{q_1,t_2} & \cdots & a_{q_1,t_j} & \cdots & a_{q_1,t}\\ a_{q_2,t_1} & a_{q_2,t_2} & \cdots & a_{q_2,t_j} & \cdots & a_{q_2,t}\\ \vdots & \vdots & \ddots & \vdots & & \vdots\\ a_{q_i,t_1} & a_{q_i,t_2} & \cdots & a_{q_i,t_j} & \cdots & a_{q_i,t}\\ \vdots & \vdots & & \vdots & \ddots & \vdots\\ a_{q,t_1} & a_{q,t_2} & \cdots & a_{q,t_j} & \cdots & a_{q,t}\end{bmatrix}(\bmod n)\tag{2}$$

其中,$a_{q_i,t_j}\in Z$ 表示 $\boldsymbol{H}$ 阵列中置换矩阵的循环移位次数,它与式(1)中置换矩阵的下标值 $a_{ij}\in Z$ 有相同的含义.a_{q_i,t_j} 的每一个值均需取模 n 运算,n 是置换矩阵的尺寸.行索引 $i=1,2,\cdots q$,列索引 $j=1,2,\cdots,t$,任意行号 $q_i\in[1,q]$,任意列号 $t_j\in[1,t]$,q 和 t 表示阵列的行数和列数,$q_{\max}$ 和 $t_{\max}$ 分别表示最大列重量和最大行重量.称(2)式的 $S(\boldsymbol{H})=[a_{q_i,t_j}]$ 矩阵为(1)式 $\boldsymbol{H}$ 阵列矩阵的下标矩阵. □

在某些文献中下标矩阵被定义为指数矩阵,那是因为置换集是由 I 单位置换矩阵构成的,这时下标矩阵和指数矩阵等效.对于文献[9]的 Q 置换矩阵,则只能采用下标矩阵的概念.如果 $\boldsymbol{H}$ 矩阵完全由置换矩阵构成,那么下标矩阵称为整数下标矩阵;如果 $\boldsymbol{H}$ 矩阵由部分置换矩阵和部分全零矩阵构成,那么下标矩阵称为稀疏下标矩阵.本文主要研究整数下标矩阵的结构设计.

2.3　具有大围长的规则下标矩阵的充分必要条件

设计规则下标矩阵应使围长(girth)尽可能的大(见 $\boldsymbol{H}$ 矩阵约束条件3),下面首先给出构造没有 $2i$ 围长的

规则下标矩阵的充分必要条件.

这个充分必要条件最初由 Fossorier 在文[2]中提出.设在 $\boldsymbol{H}=[h_{x,y}]$的矩阵中,在元素值为 $h_{x,y}=1$ 的 $2i$ 个位置上,定义了一个长度为 $2i$ 的环线,这个 $2i$ 环线一定满足如下两个约束条件:(1) 环线的两个连续位置只能通过交替地改变行号和列号才能得到;(2)除了环线的第一个和最后一个位置外,所有的位置都是不同的.这意味着任何环线的两个连续位置都属于不同的循环移位置换矩阵,这两个置换矩阵可能在同一行上,也可能在同一列上.因此,可以认为一个长度为 $2i$ 的环线与一组循环移位置换矩阵相关联:

$$\boldsymbol{H}_{a_{q_0,t_0}},\boldsymbol{H}_{a_{q_1,t_0}},\boldsymbol{H}_{a_{q_1,t_1}},\cdots,\boldsymbol{H}_{a_{q_i,t_{i-1}}},\boldsymbol{H}_{a_{q_i,t_i}},\boldsymbol{H}_{a_{q_0,t_i}},\boldsymbol{H}_{a_{q_0,t_0}} \tag{3}$$

根据从 $\boldsymbol{H}_{a_{q_{k-1},t_{k-1}}}$ 到 $\boldsymbol{H}_{a_{q_k,t_k}}$ 必经过 $\boldsymbol{H}_{a_{q_k,t_{k-1}}}$,即先改变行后改变列的规则(或从 $\boldsymbol{H}_{a_{q_{k-1},t_{k-1}}}$ 到 $\boldsymbol{H}_{a_{q_k,t_k}}$ 必经过 $\boldsymbol{H}_{a_{q_{k-1},t_k}}$,即先改变列后改变行的规则),$\boldsymbol{H}$ 矩阵中长度为 $2i$ 的任意环线能用一个下标序列表示:

$$a_{q_0,t_0},a_{q_0,t_1},a_{q_1,t_1},\cdots,a_{q_i,t_{i-1}},a_{q_i,t_i},a_{q_0,t_i},a_{q_0,t_0} \tag{4}$$

也可表示成行号和列号的一个序列对:

$$\begin{aligned}&(q_0,t_0);(q_0,t_1);(q_1,t_1);\cdots;(q_i,t_{i-1});\\&(q_i,t_i);(q_0,t_i);(q_0,t_0)\end{aligned} \tag{5}$$

从式(3)到式(5),对 $1\leqslant k\leqslant i$,均有 $q_k\neq q_{k-1}$和 $t_k\neq t_{k-1}$.

定义 2[下标差] 从式(2)下标矩阵的任意一行 q_k 上,任意取两个元素 a_{q_k,t_x} 和 a_{q_k,t_y},其中 $q_k\in[1,q]$,$t_x,t_y\in[1,t]$,$t_x\neq t_y$,$x\neq y$,$x,y=1,2,3,\cdots t$,t_x 和 t_y 是下标矩阵第 q_k 行上不同的两个列序号.如果设

$$\Delta_{t_x,t_y}(q_k)=a_{q_k,t_x}-a_{q_k,t_y} \tag{6}$$

那么,称 $\Delta\in Z$ 为下标矩阵任意行上任意两个下标值之差,简称为下标差. □

在式(4)中,的 $2i$ 个下标值构成的序列也可表示成 i 个下标差构成序列:

$$\Delta_{t_0,t_1}(q_0),\Delta_{t_1,t_2}(q_1),\cdots,\Delta_{t_{i-2},t_{i-1}}(q_{i-2}),\Delta_{t_{i-1},t_0}(q_{i-1}) \tag{7}$$

根据式(4~6)和(7),可以推知:当且仅当下式成立时,$\boldsymbol{H}$ 矩阵包含长度为 $2i$ 的环线.

$$\sum_{k=0}^{i-1}\Delta_{t_k,t_{k+1}}(q_k)=\sum_{k=0}^{i-1}a_{q_k,t_k}-a_{q_k,t_{k+1}}=0$$

其中 $t_0=t_i$,$q_k\neq q_{k-1}$,$t_k\neq t_{k-1}$.

上面推理实际上给出了下面定理的完整证明过程,它与文献[2]中给出的用来描述 $\boldsymbol{H}$ 矩阵不包含长度为 $2i$ 环线的充分必要条件的定理是等效的[2],这里将其扩展到下标矩阵中.

定理 1[阵列 $\boldsymbol{H}$ 矩阵和对应下标矩阵中不包含长度为 $2i$ 环线的充分必要条件] 关于式(1)描述的阵列 $\boldsymbol{H}$ 矩阵和式(2)描述的下标矩阵 $S(\boldsymbol{H})$,其对应的 Tanner 图至少包含 $2(i+1)$围长的充分必要条件是:

$$\sum_{k=0}^{m-1}\Delta_{t_k,t_{k+1}}(q_k)\neq 0\pmod n \tag{8}$$

其中对所有的 m,有 $2\leqslant m\leqslant i$,对所有的 q_k 和 q_{k+1},有 $0\leqslant q_k,q_{k+1}\leqslant q-1$,对所有的 t_k 和 t_{k+1},有 $0\leqslant t_k,t_{k+1}\leqslant t-1$,并且 $t_0=t_m$,$q_k\neq q_{k+1}$,$t_k\neq t_{k+1}$. □

定理 1 实际提供了设计下标矩阵的基本原则,它的一种等效描述是:在式(2)的下标矩阵中,如果任意 k 行上由任意 $2i$ 个下标值形成的 $i(i\geqslant k)$个下标差之模 2 和不等于 0,那么这个 $\boldsymbol{H}$ 矩阵的 Tanner 图中一定不存在长度为 $2i$ 的围长,它的围长至少是 $2(i+1)$,反之,如果 i 个下标差之代数和等于 0,那么 i 个下标差的模 2 和一定为零,$\boldsymbol{H}$ 矩阵的 Tanner 图中存在长度为 $2i$ 的围长.需要注意的是任意 i 个下标差值的数量是大于等于实际选定的行数 k 的,如果 i 等于选定的行数,那么平均每一行取一个下标差,称为异行下标差;如果 i 大于选定的行数,其中某些行会出现两个以上的下标差,被称为同行下标差.

3 规则下标矩阵的围长设计

设计整数下标矩阵的关键问题是下标值如何取值以及如何分布才能消除小围长的问题,或者说在无小围长的约束条件下,如何设计循环移位次数的问题.对于完全由置换矩阵构成的规则 $\boldsymbol{H}$ 矩阵,在它的任意 2×3或3×2的子矩阵阵列中,不可避免的存在 12 围长[2,6].因此,在整数下标矩阵的设计过程中,只需考虑如何消除 4、6、8 和 10 围长的情况.目前,针对整数下标矩阵中下标值(也就是循环移位次数)的设计,正如引言中所描述的,除了 Tanner 基于有限循环群的代数方法能消除 4、6、8 和 10 围长[1]以外(基于严格的参数限制),大多数文献[6,7]都是在定理 1 的约束条件下,由计算机优化搜索来完成.这里提出一种完全不同的构造整数下标矩阵的基本方法:首先根据定理 1 的下标差代数和为零的充分必要条件,设计出实用的下标值计算表达式,再由下标值计算表达式确定整数下标矩阵中的每个元素,最终构造出 $q\times t$ 的整数下标矩阵.

定理 2[下标值计算定理] 如果式(2)的 $q\times t$ 整数下标矩阵的每个下标值 a_{ij}可由下列表达式计算确定 a_{ij} =

$$\begin{cases}j-1 & ,\ 当\ i=1\ 和\ 1\leqslant j\leqslant t\\ t+(i-1)(i-2)/2+(2i+j-2)(j-1)/2\pmod n & \\ \qquad ,\ 当\ 2\leqslant i\leqslant q\ 和\ 1\leqslant j\leqslant t\end{cases} \tag{9}$$

那么在这个下标矩阵中,下列结论成立:

(1)q 个异行下标差(或 q 条异行水平线)不会构成 $2q$ 围长.

(2)当 $q>3, t\geqslant q$ 时,整数下标矩阵中仅存在同行下标差构成的 6、8、10 和 12 环线,但不存在 4 环线,即围长为 6. □

证明 (1)根据定理 1 和式(9)的下标值计算表达式,写出 q 个下标差之代数和的一般通式

$$\begin{aligned}
&\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}+\cdots+\Delta_{q_{q-1}}=\sum_{k=0}^{q-1}\Delta_{t_k,t_{k+1}}(q_k)\\
&=\Delta_{t_0,t_1}(q_0)+\Delta_{t_1,t_2}(q_1)+\Delta_{t_2,t_3}(q_2)+\cdots+\Delta_{t_{q-1},t_0}(q_{q-1})\\
&=a_{q_0,t_0}-a_{q_0,t_1}+a_{q_1,t_1}-a_{q_1,t_2}+a_{q_2,t_2}-a_{q_2,t_3}+\cdots+a_{q_5,t_5}-a_{q_5,t_0}\\
&=q_1(t_1-t_2)+q_2(t_2-t_3)+\cdots+q_{q-1}(t_{q-1}-t_0)\\
&\quad+(t_1-t_0)(t_1+t_0-5)/2\\
&=t_2(q_2-q_1)+t_3(q_3-q_2)+\cdots+t_{q-1}(q_{q-1}-q_{q-2})\\
&\quad+t_1q_1-q_{q-1}t_0+(t_1-t_0)(t_1+t_0-5)/2 \qquad (10)
\end{aligned}$$

异行表示所有的行序号都不同,即 $q_1\neq q_2\neq\cdots\neq q_{q-2}\neq q_{q-1}$;由于 t_0 和 t_1 表示第一列和第二列的两个列号,始终有 $t_1-t_0=1$ 和 $t_1+t_0\neq 5$,表达式(10)中包含 5/2 的非整数项,即 q 个下标差之代数和不可能是整数,这时即使 n 取任意正整数,都不可能成为式(10)计算结果的倍数,所以式(10)中 q 个下标差之模 n 和一定不为零,即 $\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}+\cdots+\Delta_{q_{q-1}}\neq 0$(模 n),那么 $\boldsymbol{H}$ 矩阵中一定不存在长度为 $2q$ 的由异行水平线构成的围长,问题(1)得证.

(2)先证明不存在 4 环线,只要任意两行的两个下标差之模 n 和不为 0,即可.设 x,y 是正整数,表示任意两行;α,β 是正整数,表示任意两列.根据定理 1,写出任意两个下标差之代数和的一般表达式为

$$\begin{aligned}
&\Delta_{q_x}+\Delta_{q_y}=\sum_{k=0}^{1}\Delta_{t_k,t_{k+1}}(q_k)=\Delta_{t_\alpha,t_\beta}(q_x)+\Delta_{t_\beta,t_\alpha}(q_y)\\
&=a_{q_x,t_\alpha}-a_{q_x,t_\beta}+a_{q_y,t_\beta}-a_{q_y,t_\alpha}=a_{x,\alpha}-a_{x,\beta}+a_{y,\beta}-a_{y,\alpha}
\end{aligned}$$

设 $x=1$,即考虑第一行和其它任意一行的情况,由下标计算表达式(10)可得 $\Delta_{q_x}+\Delta_{q_y}=y(\beta-\alpha)+(\beta+\alpha-5/2)(\beta-\alpha)$,已知 α,β 是正整数,并且一个下标差至少需要两列才能产生,必定有 $\alpha\neq\beta$,可推知 $\Delta_{q_x}+\Delta_{q_y}\neq 0$,即两个下标差之代数和不为零.再设 $x\neq y\neq 1$,即考虑除第一行外的其它任意两行的情况,由式(10)可得 $\Delta_{q_x}+\Delta_{q_y}=(y-x)(\beta-\alpha)$,由于 4 围长必在不同的两行和不同的两列上产生,必有 $\alpha\neq\beta, x\neq y$,所以 $\Delta_{q_x}+\Delta_{q_y}\neq 0$ 成立.又由于式(9)算出的 a_{ij} 是单调增数列,即在下标矩阵中总有后面的值大于前面的值,下面的值大于上面的值,下标差总是正值,所以不会出现 $\Delta_{q_x}+\Delta_{q_y}$ 的代数和不为零,而模 n 和为零的情况,所以始终有 $\Delta_{q_x}+\Delta_{q_y}\neq 0(\mathrm{mod}\,n)$.综上所述,在由式(9)下标计算表达式构成的下标矩阵中一定不存在 4 环线.

下面只需验证由式(9)下标计算表达式所构成的下标矩阵中 3,4 和 5 个下标差的代数和为零,即可表明存在 6、8 和 10 环线.设 q_0,q_1,q_2,q_3,q_4 是正整数,表示任意五行,t_0,t_1,t_2,t_3,t_4 是正整数,表示任意五列.根据式(10)一般下标计算表达式,写出五个下标差代数和的一般形式

$$\begin{aligned}
&\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}+\Delta_{q_3}+\Delta_{q_4}\\
&=t_0(q_0-q_4)+t_1(q_1-q_0)+t_2(q_2-q_1)+t_3(q_3-q_2)\\
&\quad+t_4(q_4-q_3)\\
&=q_0(t_0-t_1)+q_1(t_1-t_2)+q_2(t_2-t_3)+q_3(t_3-t_4)\\
&\quad+q_4(t_4-t_0)
\end{aligned}$$

当 $q_0=q_2=q_4$ 和 $t_1=t_2, t_3=t_4$ 时,有 $\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}+\Delta_{q_3}+\Delta_{q_4}=0$,五个下标差的代数和为 0,表明 $\boldsymbol{H}$ 阵列中存在 10 环线,其中 $q_0=q_2=q_4$ 表示三个下标差出现在同一行上.

同理,写出四个下标差代数和的一般形式:

$$\begin{aligned}
&\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}+\Delta_{q_3}\\
&=t_0(q_0-q_4)+t_1(q_1-q_0)+t_2(q_2-q_1)+t_3(q_3-q_2)\\
&=q_0(t_0-t_1)+q_1(t_1-t_2)+q_2(t_2-t_3)+q_3(t_3-t_4)
\end{aligned}$$

当 $q_0=q_1, q_2=q_3$ 和 $t_0=t_2=t_4$ 时,有 $\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}+\Delta_{q_3}=0$,四个下标差的代数和为 0,表明 H 阵列中存在 8 环线,其中 $q_0=q_1, q_2=q_3$ 表示两个下标差同行的情况有两行.

同样,写出三个下标差代数和的一般形式

$$\begin{aligned}
&\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}=t_0(q_0-q_4)+t_1(q_1-q_0)+t_2(q_2-q_1)\\
&\quad=q_0(t_0-t_1)+q_1(t_1-t_2)+q_2(t_2-t_3)
\end{aligned}$$

当 $q_0=q_2$ 和 $t_0=t_3, t_1=t_2$ 时,有 $\Delta_{q_0}+\Delta_{q_1}+\Delta_{q_2}=0$ 三个下标差代数和为 0,表明 $\boldsymbol{H}$ 阵列中存在 6 围长.12 环线是不可避免的,不必再证.这就完成了第(2)问,下标矩阵中仅存在同行下标差构成的 6、8、10 和 12 环线,不存在 4 环线的情况. 证毕. □

例 1 根据定理 2 的式(9),设计下标矩阵实例如下:设 $q=t=3,4,5,6$,得 3×3、4×4、5×5 和 6×6 的方阵.方阵一般用于设计 1/2 码率的 LDPC 码.设 $q=3, t=10$,得到 3×10 的宽矩阵,宽矩阵一般用于设计高率 LDPC 码.设 $q=6, t=2$,得到 6×2 的高矩阵,高矩阵一般用于设计低率 LDPC 码.各种下标矩阵演示如下:

$$S(\boldsymbol{H})_{3\times 3}=\begin{bmatrix}0&1&2\\3&5&8\\4&7&11\end{bmatrix},\ S(\boldsymbol{H})_{4\times 4}=\begin{bmatrix}0&1&2&3\\4&6&9&13\\5&8&12&17\\7&11&16&22\end{bmatrix}$$

$$S(\boldsymbol{H})_{3\times 10}=\begin{bmatrix}0&1&2&3&4&5&6&7&8&9\\10&12&15&19&24&30&37&45&54&64\\11&14&18&23&29&36&44&53&63&74\end{bmatrix}$$

$$S(\boldsymbol{H})_{5\times 5}=\begin{bmatrix}0&1&2&3&4\\5&7&10&14&19\\6&9&13&18&24\\8&12&17&23&30\\11&16&22&29&37\end{bmatrix}$$

$$S(\boldsymbol{H})_{6\times 6}=\begin{bmatrix}0&1&2&3&4&5\\6&8&11&15&20&26\\7&10&14&19&25&32\\9&13&18&24&31&39\\12&17&23&30&38&47\\16&22&29&37&46&56\end{bmatrix}$$

$$S(\boldsymbol{H})_{6\times 3}=\begin{bmatrix}0&1&2\\3&5&8\\4&7&11\\6&10&15\\9&14&20\\13&19&26\end{bmatrix}$$

可以验证上述矩阵不存在 4 环线,围长至少是 6. □

在定理 2 的下标计算表达式(9)中,如果对第一行和第二行的计算序列均增加一个常数 a,$a\in Z$,即:

$$a_{ij}=\begin{cases}j-1+a & \text{,当 } i=1 \text{ 和 } 1\leqslant j\leqslant t,a\in Z\\ t+(i-1)(i-2)/2+(2i+j-2)(j-1)/2+a(\mathrm{mod}n) & \\ & \text{,当 } 2\leqslant i\leqslant q \text{ 和 } 1\leqslant j\leqslant t,a\in Z\end{cases}\tag{11}$$

当 $a>0$,所有下标值都是正整数,表示置换矩阵循环左移;当 $a<0$,某些下标值可能出现负整数,表示置换矩阵循环右移.由此可知,按式(11)设计的下标矩阵依参数 a 浮动,改变 a 值可以构成一个下标矩阵族,它们与式(9)设计的下标矩阵具有相同的围长和环线结构.

利用例 1 设计的 $n\times n$ 下标矩阵,可以构造具有线性编码器的类 IRA(IRA-like)结构的 LDPC 码,其中信息位对应的 $\boldsymbol{H}^d$ 矩阵用本文的下标矩阵来设计,并用文献[9]提出的 Q 置换矩阵去填充;校验位对应的矩阵 $\boldsymbol{H}^p$ 采用双对角线结构,将 $\boldsymbol{H}^d$ 和 $\boldsymbol{H}^p$ 并置在一起,形成一个新的 $\boldsymbol{H}$ 矩阵,由这个 $\boldsymbol{H}$ 矩阵定义的 LDPC 码是 IRA 码[10]的一个子类,称为 SPB-LDPC 码,它有线性复杂度的编码算法.仿真实验表明,在相同码率和码长条件下,虽然它的 girth 为 6,但比 Tanner 构造的 girth 为 12 的规则结构 LDPC 码的性能优越.表明 LDPC 码的不规则性,优于规则的但围长大的结构码.如果,在不规则结构中,考虑大围长,LDPC 码的性能会有所改善,特别是相同性能条件下,解码迭代次数有显著下降,围长的加大真正影响的是解码迭代次数.

4 结论

通常来说,对于给定的置换矩阵尺寸 n,为了使 LDPC码的 $\boldsymbol{H}$ 矩阵得到最大可能的围长,阵列 $\boldsymbol{H}$ 矩阵中置换矩阵的循环移位值的确定是必须考虑的关键问题,也是难题,本文提出用下标值计算表达式来确定循环移位值是解决问题的一种有效途径之一.文中提出的下标值计算表达式可以用来设计围长为 6 的 $\boldsymbol{H}$ 矩阵,并能消除 4 环线.后续研究将讨论如何设计稀疏下标矩阵,使由部分置换矩阵和部分全零矩阵构成的 $\boldsymbol{H}$ 阵列能达到围长大于 12.

参考文献:

[1] R M Tanner, D Sridhara, A Sridharan, et. LDPC block and convolutional codes based on circulant matrices[J]. IEEE Trans. Info. Theory, 2004, 50(10): 2966 – 2984.

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

[3] R M Tanner. A recursive approach to low complexity codes [J]. IEEE Trans. Inform. Theory, 1981, IT-27: 533 – 547.

[4] R G Gallager. Low-Density Parity-Check Codes[D]. Ph. D. thesis, Cambridge, MA: MIT Press, 1963.

[5] J L Fan. Array codes as low-density parity-check codes[A]. Proc. 2nd Int. Symp. Turbo Codes and Related Topics[C]. Brest, France, 2000. 543 – 546.

[6] Olgica Milenkovic, Navin Kashyap and David Leyba. Shortened array codes of large girth[J]. IEEE Trans. on Info. Theory, 2006, 52(8): 3707 – 3723.

[7] S H Kim, H Chung and D J Shin. Quasi-cyclic low-density parity-check codes with girth larger than 12[J]. IEEE Trans. on Info. Theory, 2007, 53(8): 2885 – 2891.

[8] Y Kou, L Shu and M P Fossorier. Low-density parity-check codes based on finite geometries: a rediscovery and new results [J]. IEEE Trans. Info. Theory, vol. 47, Nov. 2001, pp. 2711 – 2736.

[9] 彭立,朱光喜. 基于 Q – 矩阵的 LDPC 码编码器设计.[J] 电子学报, 2005, 33(10): 1734 – 1740.
Peng Li, Zhu Guang-xi. An exploit of designing encoder for LDPC codes based on Q-matrix[J]. Acta Electronica Sinica. 2005, 33(10): 1734 – 1740. (in Chinese)

[10] Jin Hui, Analysis and Design of Turbo-like Codes[D]. Ph. D. dissertation California Institute of Technology Pasadena, California.

作者简介:

彭 立 女,1984 年于华中工学院获工程学士学位,1990 年于华中理工大学获硕士学位.2009 年获华中科技大学电子与信息工程系博士学位.现为华中科技大学电子与信息工程系副教授.主要研究方向:信息论、信道编码、网络编码、无线传输技术.

E-mail: pengli@mail.hust.edu.cn