

基于多重置换阵的满秩结构化 LDPC 码构造方法

陈智雄, 苑津莎

(华北电力大学电气与电子工程学院, 河北保定 071003)

摘要: 在多重置换阵的基础上, 提出一种适用基于网络编码的协作中继策略的结构化 LDPC 码构造方法. 首先定义了多重置换阵的概念, 提出并证明了该方阵在秩和消元等方面的重要性质; 给出具体的构造步骤, 构造了列重为 3 和围长至少为 6 的满秩 LDPC 码; 分析了该 LDPC 码的生成矩阵, 具有稀疏和结构化的特点, 适用基于网络编码的协作中继系统中进行联合网络编码和迭代译码. 仿真结果表明, 在相同码长、2/3 码率和准循环矩阵 Y 结构条件下, 相比阵列 LDPC 码、近似双对角形式的 LDPC 码和三对角形式的 LDPC 码, 新构造的 LDPC 码具有相对较好的译码性能.

关键词: 网络编码; 结构化 LDPC 码; 多重置换阵; 满秩

中图分类号: TN919 **文献标识码:** A **文章编号:** 0372-2112 (2012)02-0313-06

电子学报 URL: <http://www.ejournal.org.cn> **DOI:** 10.3969/j.issn.0372-2112.2012.02.017

Construction of Structure LDPC Codes with Full Rank Based on Multi-Permutation Matrix

CHEN Zhi-xiong, YUAN Jin-sha

(School of Electrical and Electronic Engineering, North China Electric Power University, Baoding, Hebei 071003, China)

Abstract: Based on multi-permutation matrix, a constructing method for structure LDPC codes suitable for cooperative relaying joint with network coding is proposed. Multi-permutation is defined firstly, and then some important characteristic is summarized and proved. Detail process to construct full rank LDPC codes with column-weight-3 and girth-6 is given. It is analyzed that the generation matrix of proposed LDPC codes with structure and spare feature is suitable for joint encoding and iterative decoding in cooperative relaying with network coding. Compared to array LDPC codes, LDPC codes with dual diagonal and triple diagonal structure, which are the same 2/3 code rate, code length and quasi-cyclic matrix Y structure, simulation results show favorable decoding performance of LDPC codes proposed in the paper.

Key words: network coding; structure LDPC codes; multi-permutation; full rank

1 引言

网络编码在提高通信系统吞吐量的同时, 还可以获得分集增益^[1,2]. 协作中继技术中可同时使用信道编码和网络编码, 在降低系统复杂度的同时充分发挥这两种编码方法的优点^[3~5]; 通过 LDPC 码等信道编码方法来降低系统误码率从而提高系统通信的可靠性, 通过网络编码来获取分集增益并提高系统的吞吐量.

由于 LDPC 码优异的译码性能, 基于 LDPC 码的协作中继技术成为重要的研究内容^[6,7]. 雷维嘉等^[6]较早提出一种基于 LDPC 编码的协作通信方式, 通过不同的用户发送码字的不同部分, 实现虚拟的多发送天线, 获

得发送分集增益并提高系统性能. 文献[7]中构造了一种适用于中继协作通信的非正规 LDPC 系统码, 并将该码应用于协作中继系统进行联合迭代译码. 随着网络编码研究的深入进行, 针对联合 LDPC 码和网络编码的协作中继技术的研究也逐渐展开. Y Li 等^[3,4]针对联合 LDPC 码-网络编码的两用户协作中继系统, 推导了系统容量限和译码门限, 分别采用 EXIT 图和高斯近似算法来分析和优化 LDPC 码节点的度分布. 对于多用户协作中继系统, 文献[5]中提出一种基于自适应网络编码的中继策略, 使用低密度生成矩阵码 (LDGM 码) 和下三角形式的 LDPC 码作为信道编码方案. LDGM 码属于特殊的 LDPC 码, 具有系统形式的校验矩阵和稀疏的生成矩

阵,该码具有较低的编译码存储资源和线性编码复杂度.系统形式的校验矩阵使得 LDGM 码的译码性能较差,具有很大的差错平底.下三角形 LDPC 码的译码性能要好于 LDGM 码,但是生成矩阵不是稀疏的,中继节点按照生成矩阵进行网络编码时需要接收大部分甚至所有源节点的信息,产生较大的用户间干扰和编码延时,限制了该码的实用性. IEEE 802.16e 和 IEEE 802.11n 等标准中的 LDPC 码具有近似双对角的形式,它们在联合 LDPC 码和网络编码的协作中继系统中的应用也存在同样的问题.显然非稀疏的生成矩阵使得联合网络编码的复杂度过高,是限制 LDPC 码在基于网络编码的协作中继中应用的重要因素.

以构造相对稀疏和结构化的生成矩阵为目标,论文提出一种适用于联合网络和信道编码协作中继技术的 LDPC 码的构造方法.构造的 LDPC 码的校验矩阵具有满秩、列重为 3 和围长至少为 6 的特点.

2 多重置换阵的定义及其性质

已知 $q \times q$ 的單位置换阵 $\mathbf{P}(a_i)$ 是指将 $q \times q$ 的單位阵向上循环移动 a_i 次后得到的方阵.定义重数为 w 的多重置换阵 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 为:将 w 个偏移数为 a_i 的單位置换阵 $\mathbf{P}(a_i)$ 在二元域上加和生成的方阵,其中 $0 \leq a_1 < a_2 < \dots < a_w < q$.显然多重置换阵的重数 w 等于自身的列重.例如,式(1)为重数 $w = 3$ 的 5×5 多重置换阵 $\mathbf{P}_3(0, 1, \dots, 4)$.

$$\mathbf{P}_3(0, 1, 4) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \quad (1)$$

定义 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 第 1 个行向量对应二元域上的多项式为多重置换阵的生成多项式,并用 $X^{a_1} + X^{a_2} + \dots + X^{a_w}$ 表示.提取 X^{a_1} ,将 $X^{a_1} + X^{a_2} + \dots + X^{a_w}$ 转换成 $X^{a_1}(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1})$ 的形式,称 $1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}$ 为 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 的根多项式.式(1)中 $\mathbf{P}_3(0, 1, \dots, 4)$ 的生成多项式和根多项式都为 $1 + X + X^4$.

因为多重置换阵的各个行向量满足循环移位的关系,所以 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 中的每个行向量都可以表示成多项式 $X^i(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1})$ (模 $X^q + 1$) 的形式,其中 i 为整数, $0 \leq i < q$,模 $X^q + 1$ 相当于 $X^q + 1 = 0$,即 $X^q = 1$.

研究发现,多重置换阵在秩、构造和消元等方面具有以下几个重要性质.

性质 1 重数为偶数的多重置换阵必然不是满秩的.

证明 由定义可知,重数为偶数的多重置换阵的每个列向量中有偶数个元素“1”.采用模二运算,将置换阵中除第 1 个行向量外的其它行向量都加和到第 1 个行向量上,则第 1 个行向量将变成全零向量.可知此多重置换阵的各个行向量是线性相关的,即必然不是满秩的.(证明完毕)

根据性质 1,为了更好地控制校验矩阵的秩并设计 LDPC 码的码率,构造基于多重置换阵的满秩 LDPC 码,最好选用重数为奇数的多重置换阵,有如下性质:

性质 2 重数为奇数的 $q \times q$ 多重置换阵 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 是满秩方阵的充要条件是根多项式 $1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}$ 不能整除多项式 $X^q + 1$ (模 $X^q + 1$).

证明

(1)先用反证法证明必要条件.

假设多项式 $1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}$ 能整除 $X^q + 1$,定义 $Q(X)$ 是次数不超过 $q - 1$ 的多项式且满足 $Q(X)(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}) = X^q + 1$.

因为可用 $X^i(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1})$ 表示 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 中任意行向量对应的多项式,其中 $0 \leq i \leq q - 1$.根据模 $X^q + 1$ 的定义 $X^q = 1$,可知 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 存在着一些行向量,这些行向量的模二和为零向量,即 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 不是满秩的,与 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 是满秩的已知条件相矛盾,所以多项式 $1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}$ 能整除 $X^q + 1$ 的假设不成立.

(2)再证充分条件.

若根多项式 $1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}$ 不能整除 $X^q + 1$,则假设不存在最高次数小于 q 的 $Q(X)$ 使 $Q(X)(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}) = X^q + 1$.已知 $X^i(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1})$ 表示 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 中行向量对应的多项式,其中 $0 \leq i \leq q - 1$.可知不存在一组不全为零的二元域上的数 k_0, k_2, \dots, k_{q-1} ,使得

$$\begin{aligned} & \left(\sum_{i=0}^{q-1} k_i \cdot X^i \right) \cdot \left(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1} \right) \\ &= Q(x)(1 + X^{a_2 - a_1} + \dots + X^{a_w - a_1}) \\ &= X^q + 1 \\ &= 0 \end{aligned}$$

根据定义, $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 中行向量是非线性相关的,即 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 是满秩的. (证明完毕)

根据性质 2,存在满秩且重数为奇数的多重置换阵.采用性质 2 的条件来构造满秩多重置换阵,避免了使用消元方法验证矩阵是否满秩带来的复杂运算量,但是仍然需要进行多项式的除法运算.下面提出更简便的方法来确定满秩多重置换阵的每个偏移数,给出以下的性质.

性质 3 如果本原多项式 $B(X)$ 的次数为 m ,总项

数 w 为奇数,则由 $B(X)$ 每项的幂次数 $a_i (1 \leq i \leq w, 0 \leq a_1 < a_2 < \dots < a_w, a_w = m)$ 确定的 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 必然是满秩的,只要 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 的维数为 $q \times q$, 且 q 和 m 满足 $1 \leq q < 2^m - 1$.

证明 根据本原多项式定义,若 m 次不可约多项式 $B(X)$ 能整除的 $X^n + 1$ 的最小正整数为 $n = 2^m - 1$, 则称 $B(X)$ 为本原多项式. 可知,项数为 w 且次数为 m 的本原多项式 $B(X)$ 能整除多项式 $X^{2^m-1} + 1$, 但是不能整除任何次数小于 $2^m - 1$ 的多项式 $X^n + 1 (1 \leq n < 2^m - 1)$.

若多重置换阵的维数为 $q \times q$, 满足 $1 \leq q < 2^m - 1$, 且令 w 为奇数,则由性质 2 可知,因为满足: m 次本原多项式 $B(X)$ 不能整除 $X^q + 1$, 所以由 $B(X)$ 的 w 个项的幂次数 $a_i (1 \leq i \leq w, 0 \leq a_1 < a_2 < \dots < a_w, a_w = m)$ 确定的 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 必然满秩. (证明完毕)

性质 3 为构造满秩多重置换阵提供了重要的方法依据. 实际构造满秩多重置换阵时可直接使用本原多项式的幂指数来确定相关的偏移数. 只要维数 q 和本原多项式的次数 m 满足: $1 \leq q < 2^m - 1$.

性质 4 如果维数为 $q \times q$ 的多重置换阵 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 是满秩的,令 \mathbf{P}_w^{-1} 为它的逆矩阵, $\mathbf{P}(A)$ (A 为正整数, $A < q$) 为 $q \times q$ 置换阵,则矩阵 $[\mathbf{P}_w(a_1, a_2, \dots, a_w) | \mathbf{P}(A)]$ 进行高斯消元后生成的矩阵 $[\mathbf{P}(0) | \mathbf{Q}]$ 中, 方阵 \mathbf{Q} 、 \mathbf{P}_w^{-1} 和 $\mathbf{P}(A)$ 之间的关系满足: $\mathbf{Q} = \mathbf{P}_w^{-1} \mathbf{P}(A)$.

证明 因为 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 满秩可逆,则存在 k 个初等方阵 $\mathbf{R}_1, \mathbf{R}_2, \dots, \mathbf{R}_k$, 使得 $\mathbf{P}_w(a_1, a_2, \dots, a_w) = \mathbf{R}_1 \mathbf{R}_2 \dots \mathbf{R}_k$. 假设 \mathbf{R}_i^{-1} 为初等方阵 \mathbf{R}_i 的逆矩阵, 则有:

$$\mathbf{R}_k^{-1} \dots \mathbf{R}_1^{-1} \mathbf{P}_w(a_1, a_2, \dots, a_w) = \mathbf{P}(0) \quad (2)$$

及

$$\mathbf{R}_k^{-1} \mathbf{R}_{k-1}^{-1} \dots \mathbf{R}_1^{-1} \mathbf{P}(0) = \mathbf{P}_w^{-1} \mathbf{P}(0) \quad (3)$$

式(3)的两边同时右乘 $\mathbf{P}(A)$, 有

$$\mathbf{R}_k^{-1} \mathbf{R}_{k-1}^{-1} \dots \mathbf{R}_1^{-1} \mathbf{P}(A) = \mathbf{P}_w^{-1} \mathbf{P}(A) \quad (4)$$

式(2)表明 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 经过一系列的初等变换可转化为 $\mathbf{P}(0)$; 根据式(4), $\mathbf{P}(A)$ 经过同一系列的变换即可变成矩阵 $\mathbf{P}_w^{-1} \mathbf{P}(A)$. 如果采用分块矩阵的形式表示, 将式(2)和式(4)合并, 则:

$$\begin{aligned} & \mathbf{R}_k^{-1} \mathbf{R}_{k-1}^{-1} \dots \mathbf{R}_1^{-1} [\mathbf{P}_w(a_1, a_2, \dots, a_w) | \mathbf{P}(A)] \\ & = [\mathbf{P}(0) | \mathbf{P}_w^{-1} \mathbf{P}(A)] \end{aligned} \quad (5)$$

显然方阵 \mathbf{Q} 、 \mathbf{P}_w^{-1} 和 $\mathbf{P}(A)$ 的关系满足:

$$\mathbf{Q} = \mathbf{P}_w^{-1} \mathbf{P}(A) \quad (\text{证明完毕})$$

根据性质 4, 如果对满秩的多重置换阵 $\mathbf{P}_w(a_1, a_2, \dots, a_w)$ 进行高斯消元, 则处于相同行分组的单位置换阵在消元后生成的方阵满足循环移位关系. 性质 4 主要用于分析新构造的 LDPC 码的生成矩阵.

3 基于多重置换阵的 LDPC 码构造方法

基于单位置换阵和三重置换阵, 提出一种结构化 LDPC 码的构造方法, 该方法构造的 LDPC 码校验矩阵 $\mathbf{H}(q, I, J) = [\mathbf{H}_{mz} \mathbf{Y}]$ 是满秩的, 共 qJ 列, qI 行 (q, I 和 J 均为大于 3 的正整数), 从而构造的 LDPC 码的码长为 qJ , 码率为 $(J-I)/J$.

矩阵 $\mathbf{H}(q, I, J) = [\mathbf{H}_{mz} \mathbf{Y}]$ 由两个部分构成: 列重为 3 且围长为 6 的满秩准循环方阵 \mathbf{H}_{mz} 和列重为 3 且围长为 8 的准循环矩阵 \mathbf{Y} . 其中 \mathbf{H}_{mz} 包含 qI 列和 qI 行, 由 I^2 个 $q \times q$ 的循环移位方阵构成; \mathbf{Y} 包含 $(J-I) \times q$ 列和 qI 行, 由 $I \times (J-I)$ 个 $q \times q$ 的循环移位方阵构成. 定义基矩阵为将准循环矩阵中的零阵用“0”代替, 非零方阵用“1”表示后得到的矩阵.

首先, 构造满秩方阵 \mathbf{H}_{mz} , 包括以下几个要求和步骤:

(1) 方阵 \mathbf{H}_{mz} 由列重为 3 且围长为 6 的满秩多重置换阵 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 和全零方阵 \mathbf{O} 组合而成, 且 \mathbf{H}_{mz} 的基矩阵是维数为 $I \times I$ 的单位阵 $\mathbf{P}(0)$, 即 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 中的下标满足 $i = j$, 且 $1 \leq i \leq I, 1 \leq j \leq I$.

(2) 由性质 3, $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 中偏移数 $a_{i,j}, b_{i,j}$ 和 $c_{i,j}$ 满足下述条件: 由 $a_{i,j}, b_{i,j}$ 和 $c_{i,j}$ 确定的二元域多项式 $1 + X^{AB_{i,j}} + X^{AC_{i,j}}$ 不能整除 $X^q + 1$, 其中 $AB_{i,j} = b_{i,j} - a_{i,j}$, $AC_{i,j} = c_{i,j} - a_{i,j}$. 由性质 2 和步骤(1)可知, 这个要求保证方阵 \mathbf{H}_{mz} 是满秩的.

(3) 针对置换阵 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$, 令 $AB_{i,j} = b_{i,j} - a_{i,j}$, $BC_{i,j} = c_{i,j} - b_{i,j}$, $CA_{i,j} = q - AB_{i,j} - BC_{i,j}$, 则该置换阵不包含长度为 4 的小环的充分条件是: ① $AB_{i,j}, BC_{i,j}$ 和 $CA_{i,j}$ 互不相等; ② $AB_{i,j} + BC_{i,j} \neq CA_{i,j}$, $BC_{i,j} + CA_{i,j} \neq AB_{i,j}$ 和 $CA_{i,j} + AB_{i,j} \neq BC_{i,j}$. 保证 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 的围长至少为 6.

(4) 满秩置换阵 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 的偏移数 $a_{i,j}, b_{i,j}$ 和 $c_{i,j}$ 确定的二元域上多项式 $1 + X^{AB_{i,j}} + X^{AC_{i,j}}$ 都不相同或者部分相同, 其中 $AB_{i,j} = b_{i,j} - a_{i,j}$, $AC_{i,j} = c_{i,j} - a_{i,j}$. 这个条件是为了增加 \mathbf{H}_{mz} 中多重置换阵的随机性, 保证结构化 LDPC 码具有较好的译码性能.

下面证明根据条件(3)构造的三重置换阵 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 的围长至少为 6.

证明 根据置换阵 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 的定义, 每行共包含三个, 这三个“1”构成三种不同长度的线段. 例如, 第 1 行的“1”元素构成长度为 $b_{i,j} - a_{i,j}$ 的短线段 (线段中间没有“1”元素)、长度为 $c_{i,j} - b_{i,j}$ 的短线段和长度为 $c_{i,j} - a_{i,j}$ 的长线段 (线段中间还有其他“1”元素). 则 $\mathbf{P}_3(a_{i,j}, b_{i,j}, c_{i,j})$ 只包含三种长度的短线段, 长度分别为 $AB_{i,j} = b_{i,j} - a_{i,j}$, $BC_{i,j} = c_{i,j} - b_{i,j}$, $CA_{i,j} = Z -$

$AB_{i,j} - BC_{i,j}$; 还包含三种长度的长线段, 长度分别为 $AB_{i,j} + BC_{i,j}$, $BC_{i,j} + CA_{i,j}$ 和 $CA_{i,j} + AB_{i,j}$. 因为多重置换阵中各行满足循环移位的关系, 所以 $P_3(a_{i,j}, b_{i,j}, c_{i,j})$ 中所有线段的长度只有上述六种情况.

首先令 $AB_{i,j}$ 、 $BC_{i,j}$ 和 $CA_{i,j}$ 互不相等, 那么根据长线段的构成关系, 长线段的长度必然也互不相等. 再根据短线段和长线段的位置关系, 令两条基本短线段的长度和与相应基本长线段的长度各不相等, 即 $AB_{i,j} + BC_{i,j} \neq CA_{i,j}$, $BC_{i,j} + CA_{i,j} \neq AB_{i,j}$ 和 $CA_{i,j} + AB_{i,j} \neq BC_{i,j}$. 从而 $P_3(a_{i,j}, b_{i,j}, c_{i,j})$ 中所有线段的长度都不相等, 这些线段将无法构成矩形图案(小四环), 即矩阵中不存在小四环, 围长至少为 6. (证明完毕)

最后构造围长为 8 列重为 3 的矩阵 Y : 由 $3 \times (J-1)$ 单位置换阵和 $(I-3) \times (J-1)$ 个零阵 O 构成, 它的基矩阵每列包含 3 个元素“1”; Y 不包含小四环和小六环. 因为根据条件(3), 多重置换阵不包含小四环, 且位于 H_{mz} 基矩阵的对角线, 显然 $H(q, I, J) = [H_{mz}Y]$ 的围长至少为 6. 矩阵 Y 的列分组按照从左到右的顺序逐个生成, 每个列分组包含 3 个单位置换阵, 并且构造时应尽量保持 Y 中每个行分组的单位置换阵数相等.

为了验证构造方法的正确性和有效性, 按照提出的方法, 构造了一个结构化 LDPC 码的满秩校验矩阵 $H(q, I, J) = [H_{mz}Y]$, 码长为 1944, 码率为 2/3.

首先按照提出的 4 个要求和步骤, 结合性质 3 中的方法, 选用本原多项式来确定三重置换阵的偏移数, 构造 6 个满秩的三重置换阵 $P_3(a_{i,j}, b_{i,j}, c_{i,j})$, 如下所示:

$$\begin{aligned} P_3(0, 3, 7) \quad (i=j=1), \quad P_3(0, 4, 9) \quad (i=j=2), \\ P_3(0, 3, 10) \quad (i=j=3), \quad P_3(0, 2, 11) \quad (i=j=4), \\ P_3(0, 1, 15) \quad (i=j=5), \quad P_3(0, 3, 17) \quad (i=j=6). \end{aligned}$$

接着构造列重为 3 且围长为 8 的准循环矩阵 Y . Y 共包含 12 个列分组, 按照从左到右的顺序依次生成, 每个行分组中单位置换阵的个数都为 6. 根据构造方法, 一种可能的 Y 如式(6)所示.

$$Y = \begin{pmatrix} P(0) & P(0) & P(0) & O & O & P(0) \\ O & O & O & P(10) & P(0) & O \\ P(12) & O & P(16) & O & O & O \\ O & P(8) & O & P(24) & P(27) & P(30) \\ O & P(20) & O & P(28) & O & P(35) \\ P(17) & O & P(25) & O & P(35) & O \\ O & O & P(0) & O & O & P(0) \\ P(13) & O & P(15) & P(9) & P(17) & O \\ P(19) & P(26) & O & P(30) & O & P(34) \\ O & P(38) & O & O & P(45) & O \\ O & P(44) & O & P(52) & O & P(70) \\ P(45) & O & P(19) & O & P(65) & O \end{pmatrix} \quad (6)$$

其中 $P(a_{i,r})$ 为单位置换阵, O 表示全零方阵. 将 Y 第 i 个行分组的 $P(a_{i,r})$ 和 O 统称为循环移位方阵 $P_1^{i,r}$. 显然构造的 Y 中每个行分组包含的单位置换阵的数量不超过 6, 其中 i 和 r 为正整数, $1 \leq i \leq 6, 1 \leq r \leq 12$.

4 基于多重置换阵 LDPC 码的生成矩阵

下面以新构造的校验矩阵 $H(108, 6, 18)$ 为例来分析对应生成矩阵 $G(108, 12, 18)$ 的特点. 不失一般性, 其它基于多重置换阵的 LDPC 码的生成矩阵可使用相同的方法来分析. $G(108, 12, 18)$ 的结构如式(7)所示:

$$G(108, 12, 18) = [G_I | G_S] = \begin{bmatrix} P(0) & O & \cdots & O & Q_{1,1} & Q_{1,2} & \cdots & Q_{1,6} \\ O & P(0) & \cdots & O & Q_{2,1} & Q_{2,2} & \cdots & Q_{2,6} \\ O & O & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ O & O & \cdots & P(0) & Q_{12,1} & Q_{12,2} & \cdots & Q_{12,6} \end{bmatrix} \quad (7)$$

其中 $Q_{r,i}$ 为 108×108 的循环移位方阵; r 和 i 均为正整数, 且 $1 \leq i \leq 6, 1 \leq r \leq 12$.

设 $P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j})$ 为满秩置换阵 $P_3(a_{i,j}, b_{i,j}, c_{i,j})$ 的逆矩阵. $G(108, 12, 18)$ 的结构和特点包括以下几个方面:

(1) $G(108, 12, 18)$ 具有准循环形式^[8], 由 12×18 个方阵组成(包括零方阵和多重置换阵), 分为 12 个行分组和 18 个列分组.

(2) $H(108, 6, 18) = [H_{mz}Y]$ 高斯消元后变成 $[I | W]$ 的形式, 则根据校验矩阵和生成矩阵的关系, W 和 G_S 互为转置的关系. 若 $P_1^{i,r}$ 为全零方阵 O , 对它进行初等变换结果仍是 O , 则有两个结论: $Q_{r,i}$ 也是 O , 也满足 $Q_{r,i}^T = P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j}) \times P_1^{i,r}$; 与 Y 第 i 个行分组中 O 的个数相等, G_S 第 i 个列分组 G_i 共包含 6 个 O , 即 $G(108, 12, 18)$ 是相对稀疏的.

若 $P_1^{i,r}$ 为单位置换阵 $P(a_{i,r})$, 由性质 4 可知, $Q_{r,i}^T = P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j}) \times P_1^{i,r}$.

综上, $Q_{r,i}$ 、 $P_1^{i,r}$ 和 $P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j})$ 满足 $Q_{r,i}^T = P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j}) \times P_1^{i,r}$.

(3) 由 $Q_{r,i}^T = P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j}) \times P_1^{i,r}$, 若 $P_1^{i,r}$ 为 $P(a_{i,r})$, 则 $Q_{r,i}$ 也是非零方阵, 且可由 $P_3^{-1}(a_{i,j}, b_{i,j}, c_{i,j})$ 循环移动 $a_{i,r}$ 位后转置得到, 即 G_i 中的非零方阵 $Q_{r,i}$ 之间满足循环移位关系, 这些非全零方阵可共用一个生成器(方阵的第一个行向量). 因为 G_S 共有六个列分组, 编码器只需存储生成矩阵的 6 个生成器即可, 而一般准循环 LDPC 码(比如近似双对角形式)的生成矩阵不是稀疏的, 需要存储 6×12 个生成器, 可见新构造的

LDPC 码可降低编码器的硬件复杂度。

(4)协作中继系统中的中继节点根据 LDPC 码的生成矩阵进行联合网络编码时,是在信息分组的基础上进行的,即源节点在广播时隙中发送的信息是长度至少为 108 位的分组.系统中共有 6 个中继节点,每个中继节点对应 G_s 中的每个列分组.第 i 个中继节点进行编码时,选择 G_i 中非零方阵对应的源节点的信息分组 M_i 进行联合编码。

根据第(2)条结论,易知 G_i 只包含 6 个非全零方阵,计算第 i 个校验分组 C_i 不需要所有 12 个源节点的信息,只需要其中 6 个节点的信息.可见采用新构造的 LDPC 码进行联合编码可减少编码时延和干扰。

5 性能仿真与分析

在二进制相移键控调制和加性高斯白噪声信道下,对新构造的 LDPC 码和另外几种结构化 LDPC 码进行译码性能仿真和分析对比.仿真中所有的 LDPC 码都采用迭代次数为 50 的置信传播 BP 译码算法。

定义新构造的基于不同多重置换阵的 LDPC 码为 M-P LDPC 码.仿真中构造了上三角形式的阵列 LDPC 码^[9]、采用相同三重置换阵 $P_3(a_{i,j}, b_{i,j}, c_{i,j})$ 的结构化 LDPC 码、近似双对角的准循环 LDPC 码和三对角线形式的准循环 LDPC 码.它们的校验矩阵 $H(q, I, J) = [H_{mz} Y]$ 由两个部分构成:满秩准循环方阵 H_{mz} 和围长为 8 且列重为 3 的准循环矩阵 Y .近似双对角的 LDPC 码和三对角线 LDPC 码中的满秩方阵 H_{mz} 分别如式(8)和式(9)所示,显然这两个 LDPC 码都是非规则码.由于都是满秩的,因此构造的 LDPC 码的码长都是 qJ ,码率都是 $(J-I)/J$.

$$\begin{bmatrix} P(a_{1,1}) & P(a_{1,2}) & \cdots & O & O \\ O & P(a_{2,2}) & \cdots & O & O \\ P(a_{3,1}) & O & \cdots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & \cdots & P(a_{l-1,l-1}) & P(a_{l-1,l}) \\ P(a_{l,1}) & O & \cdots & O & P(a_{l,l}) \end{bmatrix} \quad (8)$$

$$\begin{bmatrix} P(a_{1,1}) & \cdots & O & O & O \\ P(a_{2,1}) & \ddots & \vdots & \vdots & \vdots \\ P(a_{3,1}) & \ddots & O & O & O \\ \vdots & \ddots & P(a_{l-2,l-2}) & O & O \\ O & \cdots & P(a_{l-1,l-2}) & P(a_{l-1,l-1}) & O \\ O & \cdots & P(a_{l,l-2}) & P(a_{l,l-1}) & P(a_{l,l}) \end{bmatrix} \quad (9)$$

图 1 给出了多重置换阵取不同维数时,码长 1944、码率 2/3 的 M-P LDPC 码的译码性能对比情况.三种参

数结构的 M-P LDPC 码的列重都为 3 且行重都为 9,即具有相同的节点度分布,但是参数为 $H(81, 8, 24)$ 的码字的译码性能都要好于 $H(162, 4, 12)$ 和 $H(108, 6, 18)$ 的性能.因此,对于结构化 LDPC 码来说,除了围长和度分布等因素外,构造中还要考虑置换阵维数的影响.因为不同维数的置换阵,元素“1”分布的密集度不一样,不同数量置换阵的组合最终会影响 LDPC 码校验矩阵中元素“1”分布的随机性.为了充分说明 M-P LDPC 码的译码性能,下面构造的 2/3 码率的 LDPC 码的参数都选择 $H(81, 8, 24)$ 。

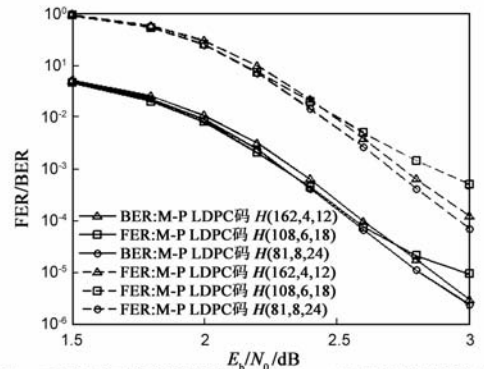


图1 三种不同参数结构的M-P LDPC码的译码性能对比

图 2 给出了五种 LDPC 码的译码性能仿真曲线,码字的参数都是 $H(81, 8, 24)$ 且是满秩的,因此码长都是 1944,码率都是 2/3.对比图中的译码性能,主要有以下结论:

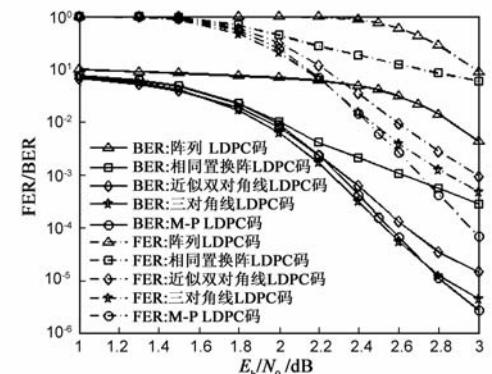


图2 五种不同形式的结构化LDPC码译码性能对比

(1)五种 LDPC 码中阵列 LDPC 码的译码性能最差,主要是因为阵列 LDPC 码中存在着大量的小六环,码字的最小距离太小;校验矩阵中大部分列重在 3 以上,其中有 2/3 的列重等于 8,列重太大且含数量较多的小六环,会使迭代计算过程的信息得不到充分更新,造成译码振荡和译码错误。

(2)采用相同三重置换阵构造的结构化 LDPC 码的译码性能比 M-P LDPC 码要差很多.主要是因为采用相同三重置换阵使得校验方阵具有类似循环码校验矩阵的循环特性,极大降低了矩阵元素分布的随机性。

(3) 由于校验矩阵中存在着大量重量为 2 的列, 近似双对角形式的 LDPC 码的译码性能比 M-P LDPC 码和三对角线形式的 LDPC 码都要差. 主要原因是大量重量为 2 的列, 会导致较小的最小码距^[10], 降低 BP 译码的性能.

(4) FER 译码性能方面, 对比三对角形式的 LDPC 码, M-P LDPC 码的性能最好. BER 译码性能, 当 E_b/N_0 在 1.5dB ~ 2.6dB 之间取值时, 三对角形式的 LDPC 码的 BER 性能要好一些, 合理的解释是, 它是非规则 LDPC 码, 在译码过程中存在着“波浪效应”^[11]; 当 $E_b/N_0 > 2.6$ dB 时, M-P LDPC 码的性能好于三对角形式的 LDPC 码. 综合考虑 FER/BER 的译码性能, M-P LDPC 码的译码性能是相对最好的.

6 结论

非稀疏的生成矩阵使得联合网络编码的复杂度过高, 是限制 LDPC 码在基于网络编码的协作中继中应用的关键问题. 论文提出一种适用于联合网络编码和 LDPC 码的协作中继系统的 LDPC 码的构造方法. 新 LDPC 码的校验矩阵采用满秩的多重置换阵构造, 有利于控制矩阵的秩并设计 LDPC 码的码率; 它的列重为 3, 围长至少为 6. 相比其他的 LDPC 码, 新构造的 M-P LDPC 码具有较好的译码性能.

为了将提出的 LDPC 码应用到协作中继系统中, 后续的工作包括: 针对其他码长和码率, 通过设计 LDPC 码节点的度分布和多重置换阵的维数, 优化系统的译码性能; 分析新提出的 LDPC 码在瑞利等信道下的性能; 研究基于多重置换阵的结构化 LDPC 码的高效译码器, 设计关键译码单元, 例如适用于多重置换阵的循环移位置换单元等.

参考文献

- [1] L Xiao, T E Fuja, et al. A network coding approach to cooperative diversity[J]. *IEEE Trans Info Theory*, 2007, 53(10): 3714 - 3722.
- [2] Z Ding, K K Leung, et al. On the study of network coding with diversity[J]. *IEEE Trans Wireless Comm*, 2009, 8(3): 1247 - 1259.
- [3] Y Li, G Song, L Wang. Design of joint network—Low density parity check codes based on the EXIT charts[J]. *IEEE Comm Letters*, 2009, 13(8): 600 - 602.
- [4] Y Li, G Song, L Wang. Analysis of the joint network LDPC codes over orthogonal multi-access relay channel[J]. *IEEE Comm Letters*, 2010, 14(2): 184 - 186.
- [5] X Bao, J Li. Adaptive network coded cooperation for wireless relay networks: Matching code-on-graph with network-on-graph[J]. *IEEE Trans Wireless Comm*, 2008, 7(2): 574 - 583.
- [6] 雷维嘉, 谢显中, 李广军. 一种基于 LDPC 编码的协作通信方式[J]. *电子学报*, 2007, 35(4): 712 - 715.
Lei Wei-jia, Xie Xian-zhong. A cooperative communication method based on LDPC code[J]. *Acta Electronica Sinica*, 2007, 35(4): 712 - 715. (in Chinese)
- [7] 陈婧文, 仰枫帆. 基于非正规 LDPC 码的中继协作通信及其联合迭代译码的性能研究[J]. *电子学报*, 2010, 38(7): 1534 - 1540.
Chen Jing-wen, Yang Feng-fang. Study on the irregular-LDPC-based relay cooperation and performance of joint iterative decoding[J]. *Acta Electronica Sinica*, 2010, 38(7): 1534 - 1540. (in Chinese)
- [8] Z Li, L Chen, et al. Efficient encoding of quasi-cyclic low-density parity-check codes[J]. *IEEE Trans Comm*, 2006, 54(1): 71 - 81.
- [9] S Myung, K Yang, J Kim. Quasi-cyclic LDPC codes for fast encoding[J]. *IEEE Trans Info Theory*, 2005, 51(8): 2894 - 2901
- [10] S Lin, Daniel, J Costello. *Error Control Coding, Fundamentals and Applications-Second Edition*[M]. New Jersey, America: Prentice Hall, 2004. 577 - 592.
- [11] T J Richardson, M A Shokrollahi, R L Urbanke. Design of capacity approaching irregular low-density parity-check codes[J]. *IEEE Trans Info Theory*, 2001, 47(9): 619 - 637.

作者简介



陈智雄 男, 1983 年 8 月出生于福建莆田, 2007 年、2010 年分别在哈尔滨工业大学和华北电力大学获硕士和博士学位. 现为华北电力大学电气与电子工程学院讲师. 主要研究方向为信道编码和协作通信等.

E-mail: chenxz1983@sohu.com