# 一种基于 MDS-卷积码的 LDPC 码构造方法

乔　华, 董明科, 项海格
(北京大学卫星与无线通信实验室, 北京 100871)

摘　要: 近年来, 结构化低密度奇偶校验(LDPC)码的构造方法受到了广泛地关注. 本文提出了一种利用最大距离分割(MDS)编码构造结构化 LDPC 码的思路. 该思路将基于两个信息符号的 RS 码构造 LDPC 码的方法扩展至适用于所有的 MDS 码. 本文以具有 MDS 特性的卷积码为例详细描述该构造方法的细节, 并构造了码长从 255 比特到 4095 比特的高码率 LDPC 码. 由于卷积码的 MDS 定义不同于线性分组码, 因此本文给出了一种对卷积码截短的方法及其必要的证明. 仿真结果表明, 本文构造 MDS-Conv-LDPC 码的性能优于随机构造的 LDPC 码.

关键词: 低密度奇偶校验码; 最大距离分割码; 卷积码; 结构化构造方法
中图分类号: TN911.22　　文献标识码: A　　文章编号: 0372-2112 (2008) 01-0117-05

# Construction of LDPC Codes Based on MDS-Convolutional Codes

QIAO Hua, DONG Ming-ke, XIANG Hai-ge
*(Satellite and Wireless Communication Laboratory, Peking University, Beijing 100871, China)*

**Abstract:** A great deal of research effort has been expended in the design and construction of structured low-density parity-check (LDPC) codes. In this paper, we propose a method to construct structured LDPC codes based on maximum-distance separable (MDS) codes. The main idea of this paper is to expand the method which is based on RS codes with two information symbols[12] to all MDS codes. The details of the method are described by using MDS convolutional codes to construct LDPC codes. Since the definition of the MDS convolutional codes are different from that of linear block codes, a shorten technology is used and proved in the paper. Some LDPC codes based on the proposed method with variable code length at high rates are constructed and simulation results show their performance advantage over random construction.

**Key words:** low density parity check codes; maximum-distance separable codes; convolutional codes; structured construction

## 1 引言

低密度奇偶校验码(low density parity check codes, LDPC 码)[1]是近年来备受重视的一种信道编码[2]. 该码具有逼近香农极限的纠错性能和适合于并行计算的简单译码算法[3], 因此不断被各种新的通信标准所采纳, 如 WiMAX[4]、DVB-S2[5] 等. 这使得 LDPC 码的实际应用在不久的将来将成为现实, 也表明在未来一段相当长的时间里, LDPC 码将成为通信系统中的一种主流信道编码. 同时, 随着多媒体应用在无线通信中的兴起, 图像、视频等将成为通信中的主要业务, 与特定的信源编码相结合, 采用高码率甚至极高码率的信道编码, 能够最大限度的提高服务质量[19], 因此本文对高码率 LDPC 码的构造方法进行研究具有现实意义.

LDPC 码的构造方法一直是 LDPC 码研究的一个重点. 目前, LDPC 码的构造方法可以大致分为两类, 随机搜索的[6,7]和结构化的. 由于利用结构化的构造方法得到的 LDPC 码具有规则的结构, 能够降低系统实现的复杂度[8,9], 因此结构化的 LDPC 码具有更广泛的应用前景. 结构化的构造方法主要有有限几何方法[10]、BIBD (Balanced Incomplete Block Design) 方法[11]、只有两个信息符号的 RS 码的方法[12]以及置换矩阵方法[13~16]等. 尽管已经具有很多的结构化构造方法, 但是由于它们都局限于各自的代数结构, 能够构造的 LDPC 码参数比较有限, 因此提出更多的结构化构造方法可以为结构化 LDPC 码的参数提供更多的选择.

最大距离分割(maximum distance separable, MDS) 特性是信道编码理论研究中不可忽视的一个重点, 被广泛应用的 RS 码等线性分组码就是具有 MDS 特性的信道编码. 文献[12]提出利用只有两个信息符号的 RS 码构造 LDPC 码也是利用了 RS 码这一特性. 本文主要的贡献在于将该方法推广到任意一个具有 MDS 特性的信道编码, 并具体分析了 MDS-卷积码[17,18]的性质, 利用它构造了不同长度的高码率 LDPC 码, 称之为 MDS-Conv-LDPC 码.

本文分为五个部分. 在随后的四个部分中, 首先回顾一下 LDPC 码的基本定义并引入正交二进制矢量的概念; 随后, MDS-卷积码的定义及其最小自由距离特性

收稿日期: 2006-12-22; 修回日期: 2007-03-30
基金项目: 预研基金(No. 9140A22030106JW02)

将被介绍; 以此为基础, 本文第四部分将给出基于 MDS-卷积码的 LDPC 码构造方法, 并对其结构进行分析; 最后, 本文将对构造出来的 MDS-Conv-LDPC 码进行误码性能的仿真, 并得出结论.

## 2 LDPC 码

作为一种线性分组码, LDPC 码的 $H$ 矩阵必须满足以下三个条件: 是一个稀疏矩阵; 任意两行至多只在同一个位置具有非零元素'1'; 任意两列至多只在同一个位置具有非零元素'1'. 通常, 上述三个条件被简称为行列约束条件[10~13].

构造 LDPC 码的过程, 就是寻找符合行列约束条件的 $H$ 矩阵的过程. 作为构造的基础, 本节首先介绍二进制正交矢量的概念[12]. 假设存在一个有限域 $F$, 其中包含 $p$ 个元素, 定义 $p$ 个长度为 $p$ 且重量为 1 的二进制矢量来表示 $F$ 中的每一个元素. 其对应关系如下所示, 其中 $\alpha$ 是有限域 $F$ 的本原元:

$$0 \rightarrow \underbrace{1000\cdots0}_{p},\ 1 \rightarrow \underbrace{0100\cdots0}_{p},\ \alpha \rightarrow \underbrace{0010\cdots0}_{p},\ \cdots,\ \alpha^{p-2} \rightarrow \underbrace{0000\cdots1}_{p}$$

通过上述具有正交特性的二进制矢量, 给定任意一个 $F$ 上长度为 $n$ 的矢量, 就可表示成为一个长度为 $np$ 的二进制矢量. 并且, 如果任意两个 $F$ 上的矢量在同一位置至多仅有一个符号相同, 那么相应的二进制矢量也至多在同一个位置上拥有非零元素'1'. 当 $p=3$ 时, 矢量的例子如下

$$\begin{matrix}[0\ 1\ \alpha] \rightarrow [100\ 010\ 001] \\ [1\ \alpha\ 0] \rightarrow [010\ 001\ 100]\end{matrix},\ p=3$$

显然, 如果有 $t$ 个 $GF(p)$ 上长度为 $n$ 的矢量, 它们两两之间至多仅在一个位置上有符号相同, 将每一个符号替换为位置矢量, 就可以将每一个 $GF(p)$ 上长度为 $n$ 的矢量表示成为一个长度为 $np$ 二进制矢量. 令这 $t$ 个二进制矢量作为 $H$ 矩阵的行, 那么得到大小为 $t\times np$ 的 $H$ 矩阵无疑是符合行列约束的. 构造 LDPC 码 $H$ 矩阵的焦点由此转化为寻找符合上述要求的矢量.

因为 MDS 码的最小码距 $d=n-k^0+1$, 其中 $n$ 为码长, $k^0$ 为信息符号数目, 所以如果选择只有两个信息符号的 MDS 码, 即 $k^0=2$, 那么该 MDS 码的最小码距就是 $n-1$, 该 MDS 码的任意两个码字之间至多仅在一个位置拥有相同的符号, 该码的所有码字都可以通过位置矢量来构造 LDPC 码的 $H$ 矩阵.

文献[12]利用 RS 码的 MDS 特性, 得到了一系列符合上述要求的 $GF(2^p)$ 上的矢量, 并利用它们构造得到了性能优异的 LDPC 码. 类似地, 本文将利用具有 MDS 特性的卷积码获得一些符合上述要求的矢量, 并利用它们构造 LDPC 码.

## 3 MDS-卷积码

本文所讨论的卷积码与广泛使用的二进制卷积码不同, 它们都基于 $GF(p)$, 其中 $p$ 大于 2. 设存在一个 $GF(p)$ 上码率为 $k/n$ 的卷积码, 其半无限生成矩阵为 $G$ 如图 1 所示, 其中每一个子矩阵 $G_i$ 的大小为 $k\times n$:

$$G=\begin{bmatrix} G_0 & G_1 & \cdots & G_v & 0 & \cdots \\ 0 & G_0 & G_1 & \cdots & G_v & 0 \\ \vdots & 0 & \ddots & \ddots & \cdots & \ddots \end{bmatrix}$$

图 1 卷积码的半无限生成矩阵

定义该卷积码的最小自由距离[18]为:

$$d_{free} := \min\{wt(v) \mid v=uG\}$$

其中 $wt(v)$ 表示码矢 $v$ 的重量, 等于 $v$ 中非零码元的个数。$u=[u_0\,u_1\cdots]$, $u_i$ 是一个 $GF(p)$ 上的 $k$ 维行向量, 并且 $u_0$ 不为 0。

取 $G$ 的前 $(j+1)n$ 列, 得到如图 2 所示的生成矩阵 $G_j^c$. 将这个截短卷积码的最小自由距离表示为 $d_j^c$, 可以得到下面的三个定理[18].

$$G_j^c=\begin{bmatrix} G_0 & G_1 & \cdots & G_j \\ & G_0 & \cdots & G_{j-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{bmatrix}$$

图 2 截短后的生成矩阵

**定理 1**[18] 取不同截短参数 $j$, 得到不同长度的截短卷积码, 其自由距离 $d_0^c \leqslant d_1^c \leqslant \cdots \leqslant d_\infty^c$, 并且 $d_\infty^c = d_{free}$. (证明见附录 A)

**定理 2**[18] 对于 $GF(p)$ 上, 码率为 $k/n$ 的卷积码 $C$, 取任意非负整数 $j$ 对其进行截短, 得到截短卷积码的最小自由距离 $d_j^c \leqslant (n-k)(j+1)+1$. (证明见附录 B)

**定义**[18] 如果 $GF(p)$ 上码率为 $k/n$ 的卷积码 $C$ 截短得到截短卷积码 $C_j$, 并且 $d_j^c=(n-k)(j+1)+1$, 则称该卷积码在截短参数 $j$ 时满足 MDS 条件.

如果一个卷积码在截短参数 $j$ 时满足 MDS 条件, 那么它满足下述定理.

**定理 3**[18] $GF(p)$ 上一个码率为 $k/n$ 的卷积码在截短参数 $j$ 时满足 MDS 条件, 那么从 $G_j^c$ 的每 $n$ 列中取出 $k$ 列, 组成一个大小为 $(j+1)k\times(j+1)k$ 的方阵, 该方阵的行列式一定不等于 0(证明见附录 C).

## 4 构造方法

在本文的第二个部分已经提到, 为了构造 LDPC 码, 就必须寻找两两之间至多仅在一个位置上有相同符号的多进制矢量. 任意一个具有 MDS 特性的线性分组码, 如果它们的信息符号数目为 2, 则它包含的所有码矢都满足上述条件. 本小节就根据具有 MDS 特性的卷积码来构造具有上述特征的矢量, 用于构造 LDPC 码.

### 4.1 构造的准备

在给出具体的构造方法之前, 首先给出定理 4 及其

证明. 利用定理4 可以将任意满足 MDS 条件的卷积码进行截短, 得到符合MDS 条件的线性分组码, 从而得到用于构造 LDPC 码的多进制矢量.

**定理4**　对码率为 $1/n$, $j=1$ 时满足 MDS 条件的卷积码进行截短, 得到子阵 $G_1^c$; 将 $G_1^c$ 的前 $n-1$ 列删除, 得到的 $2\times(n+1)$ 矩阵 $G'$ 是码长为 $n+1$, 只有两个信息符号, 并且最小码距为 $n$ 的线性分组码生成矩阵.

证明　首先证明, 矩阵 $G_1^c$ 对应的线性分组码是一个最小码重为 $n$ 的线性分组码.

已知 $G_1^c=\begin{bmatrix} G_0 & G_1 \\ 0 & G_0 \end{bmatrix}$, 其中 $G_i$ 是 $1\times n$ 矩阵, 设输入的信息矢量 $\boldsymbol{u}=[u_0\ u_1]$, 其最小自由距离 $d_j^c=(n-k)(j+1)+1=2n-1$. 又根据最小自由距离的定义可得 $wt(uG_1^c)\geqslant 2n-1$, 其中 $u_0$ 不为 0.

若将 $G_1^c$ 看作是一个线性分组码 $B$ 的生成矩阵, 则 $u_0$ 可以为 0. 将 $B$ 所有的码矢分为两个部分, 信息矢量 $u=[u_0\ u_1]$ 中 $u_0\neq 0$ 的部分与 $u_0=0$ 的部分. 根据最小自由距离的定义可知, 所有 $u_0\neq 0$ 对应的所有码矢重量不小于 $2n-1$. 下面来分析 $u_0=0$ 那部分的码矢重量.

$u_0=0$ 时对应的码矢可以写作$[0\ u_1G_0]$, 其中前面的0 表示一个长度为 $n$ 的 0 向量. 显然该码矢的重量不大于 $n$. 又根据定理3 可知, 从 $G_1^c$ 中每 $n$ 列中挑出 1 列组成的 $2\times 2$ 方阵行列式不等于 0. 即子矩阵 $G_0$ 中不存在全 0 列. 此刻 $u_1\neq 0$, 所以 $u_1G_0$ 是一个重量为 $n$ 的向量, 即 $u_0=0$ 时非零码矢重量都等于 $n$.

综上可得矩阵 $G_1^c$ 对应的线性分组码最小码重为 $n$.

然后证明, 将 $G_1^c$ 去掉前 $n-1$ 列之后, 得到的是一个码长为 $n+1$, 只有两个信息符号, 并且最小码距为 $n$ 的线性分组码生成矩阵.

将矩阵 $G_1^c$ 的前 $n-1$ 列删去, 得到的是一个大小为 $2\times(n+1)$ 矩阵 $G'$. 该矩阵对应的线性分组码的码矢可以由矩阵 $G_1^c$ 生成的线性分组码码矢截短前 $n$-1 个码元得到.

类似地, 输入信息矢量 $u=[u_0\ u_1]$, 将所有码矢分为 $u_0=0$ 与 $u_0\neq 0$ 两个部分进行分析. $u_0\neq 0$ 时, 截短前线性分组码码矢重量不小于 $2n-1$, 去掉其中任意 $n-1$ 个码元后, 码矢重量一定不小于 $n$.

$u_0=0$ 时, 截短前, 码矢重量等于 $n$, 并且前 $n$ 个码元都是 0, 因此去掉前面 $n-1$ 个码元之后, 得到的码矢重量依然为 $n$.

综上, 将 $G_1^c$ 的前 $n-1$ 列删除, 得到的 $2\times(n+1)$ 矩阵 $G'$ 是码长为 $n+1$, 只有两个信息符号, 并且最小码距为 $n$ 的线性分组码生成矩阵. 证毕.

### 4.2　构造步骤

令卷积码 $C$ 是$j=1$时达到 MDS 条件的 $GF(p)$上, 码率为 $1/n$ 的卷积码, 其截短卷积码的生成矩阵 $G_1^c$ 大小为 $2\times 2n$, 将其前 $n-1$ 列去掉, 得到一个大小为 $2\times(n+1)$的 $GF(p)$上的矩阵 $G'$. 根据定理 4 有, 它是一个码长为 $n+1$, 只有两个信息符号, 并且最小码距为 $n$ 的线性分组码的生成矩阵. 令该线性分组码为 $B$, 总共包含了 $p^2$ 个码矢, 每个码矢的重量大于等于 $n$.

从 $B$ 中任取一个重量为$n+1$ 的码矢 $c_0$, 令 $GF(p)$ 上每一个元素与之相乘, 得到包含 $c_0$ 和全零码矢在内的 $p$ 个码矢, 将它们表示成为码矢集合 $C^0$. 再将其中每个码矢的码元用正交二进制矢量替换, 得到 $p$ 个长度为$(n+1)p$ 的二进制矢量. 令每一个矢量为一列, 得到一个稀疏矩阵 $H^0$, 它的大小为$(n+1)p\times p$, 并且行重量为 1, 列重量为 $n+1$.

再任取一个 $C^0$ 以外的码矢 $c^1$, 将它与 $C^0$ 中的每一个码矢相加, 得到包含 $c_1$ 在内的 $p$ 个码矢, 它们组成一个集合称为 $C^1$, 并且该集合中的每一个码矢都与 $C^0$ 中的不相同. 同样可以得到一个大小为$(n+1)p\times p$ 的稀疏矩阵$H$1, 行重量为 1, 列重量为 $n+1$. 以此类推, 可以将线性分组码 $B$ 的所有$p^2$ 个码矢分解为 $p$ 个码矢子集, 得到 $p$ 个大小为$(n+1)p\times p$, 行重量为 1, 列重量为 $n+1$ 的稀疏矩阵. 从 $p$ 个稀疏矩阵$H_i$ 中任取 $t$ 个, 组成一个大小为$(n+1)p\times tp$ 的矩阵$H$, 如下所示:

$$H=\begin{bmatrix} H_0 & H_1 & H_2 & \cdots & H_t \end{bmatrix}$$

$H$ 符合行列约束, 并且列重量为 $n+1$, 行重量为 $t$, 它对应一个长度为 $tp$, 码率大于 $1-(n+1)/t$ 的规则 LDPC 码. 将 $H$ 转置, 可以得到一个列重量为 $t$, 行重量为 $n+1$ 的符合行列约束的稀疏矩阵 $H^t$, 它对应一个长度为$(n+1)p$, 码率大于 $1-t/(n+1)$ 的规则 LDPC 码. 具体选择哪一种 $H$ 矩阵, 可以根据 $t$、MDS-卷积码的参数 $n$ 以及需要构造的 LDPC 码码率来确定.

## 5　仿真及结论

本节对利用本文提出来的方法构造得到的 MDS-Conv-LDPC 码进行仿真, 仿真在 AWGN 信道下进行, 最大迭代译码次数为 50 次, 累计错误 50 个码矢时仿真停

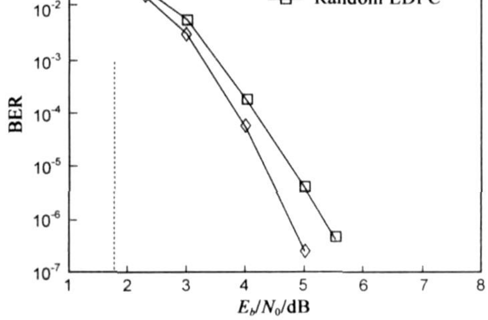


图 3　误比特仿真曲线 1

止. 与 MDS-Conv-LDPC 码进行性能对比的随机 LDPC 码的产生办法采用文献[2]的方法 1A.

图 3 所示的是利用 $GF(2^4)$ 上, $n=4$, $k=1$, 生成多项式矩阵为

$$[1+\alpha D+D^2 \quad \alpha^3+\alpha D+D^2 \quad \alpha^3+\alpha^6 D+D^2 \quad \alpha^8+\alpha D]$$

的 MDS 卷积码构造得到的(255, 197)MDS-Conv-LDPC 码与同样参数随机 LDPC 码的性能比较曲线, 从曲线可以看出, 在误码率为 $10^{-6}$时, MDS-Conv-LDPC 码距离香农极限约为 3dB, 优于随机的 LDPC 码 0.5dB. 该码具有规则的结构, 并且码率接近 0.8, 码长仅有 255 比特, 非常适合对时延敏感的高速语音通信的需要.

图 4 所示的是利用 $GF(2^6)$ 上的, $n=3$, $k=1$, 生成多项式矩阵为

$$[1+\alpha^{57}D+\alpha^{62}D^2 \quad \alpha+\alpha^{44}D+\alpha^{54}D^2 \quad 1+\alpha^{17}D+\alpha^{21}D^2]$$

的 MDS 卷积码构造得到的(4095, 3854) MDS-Conv-LDPC 码与相同参数的随机 LDPC 码的性能比较曲线, 从曲线可以看出, 在误码率为 $10^{-6}$时, MDS-Conv-LDPC 码距离香农极限约为 1dB, 优于随机的 LDPC 码 0.3dB. 该码同样具有很高的码率, 码长中等, 也非常适合对于时延敏感的视频通信或者图像传输业务.

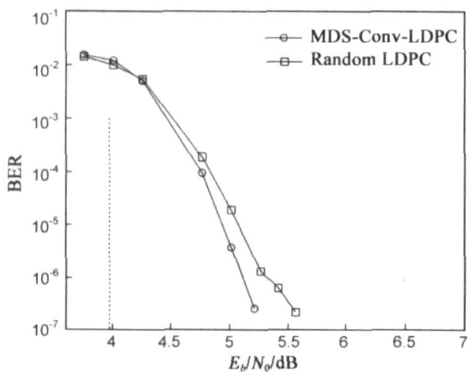


图 4　误比特仿真曲线 2

图 5 所示的则是利用参数为 $n=2$, $k=1$, 分别基于 GF(17)、GF(23)、GF(25), 生成多项式矩阵分别为

$$[1+7D+13D^2+2D^3+D^4+4D^5+14D^6 \quad 1],$$

$$[1+5D+10D^2+10D^3+5D^4+D^5 \quad 1],$$

$$[1+\alpha D+\alpha^6 D^2+\alpha^9 D^3+\alpha^6 D^4+\alpha D^5+D^6 \quad 1]$$

的 MDS 卷积码构造得到的参数为(288, 239), (528, 461)和(1023, 934)的 MDS-Conv-LDPC 码的性能仿真曲线. 从曲线可以看到, 在误码率为 $10^{-6}$时, 它们分别距离香农极限 2.9dB、2.6dB 和 2.7dB.

具有 MDS 特性的信道编码非常多, 利用它们的这一特性, 可以构造出许多结构化的 MDS-LDPC 码. 通过上面的仿真结果表明, MDS-LDPC 码的参数比较灵活, 性能也非常优异. 利用具有 MDS 特性的卷积码, 可以构造出一系列好的 MDS-Conv-LDPC 码. 寻找更多的具有 MDS 特性的信道编码, 利用它们来构造不同参数的 LDPC 码, 并对其进行结构上的分析, 将是下一步深入研究的方向之一.

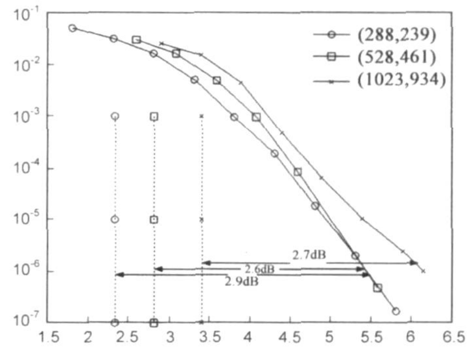


图 5　误比特仿真曲线 3

## 附录 A

选择不同的 $j$ 对同一个卷积码生成矩阵 $G$ 进行截取之后, 不同截短长度的卷积码等价于从同一个半无限长的卷积码编码码流中截取不同的长度的编码符号. 截取长度短的截断卷积码是截取长度长的截断卷积码的一部分.

$$\underbrace{\underbrace{\underbrace{c_1, c_2, c_3, \cdots, c_n}_{j=0}, c_{n+1}, c_{n+2}, \cdots, c_{2n-1}, c_{2n}}_{j=1}, c_{2n+1}, \cdots, c_{in}}_{j=i-1}, c_{in+1}, \cdots$$

取 $j$ 分别等于 $i-1$ 与 $i$ 的两个截短卷积码, 前者的每一个码矢包含 $in$ 个码元, 并且这 $in$ 个码元都是后者某一些码矢的前 $in$ 个码元. 根据最小自由距离的定义可知, 最小自由距离由具有最小重量的码矢决定. 因此, 对于 $j=i$ 的截短卷积码而言, 它包含的最小重量码矢不会小于前 $in$ 个码元中的最小重量. 因此有 $d_0^c \leqslant d_1^c \leqslant \cdots \leqslant d_\infty^c$. 当 $j$ 趋于无穷时, 截短卷积码就等价于原始的卷积码, 因此 $d_\infty^c = d_{free}$. 证毕.

## 附录 B

对于参数为 $j$ 的截短卷积码, 其生成矩阵 $G_j^c$ 也可看作是一个长度为 $(j+1)n$, 信息符号数目为 $(j+1)k$ 的线性分组码 B 的生成矩阵. 根据线性分组码最小码距的性质可知, 该线性分组码的最小码距 $d_{\min} \leqslant (n-k)(j+1)+1$, 即该码的最小重量不大于 $(n-k)(j+1)+1$. 又由于参数为 $j$ 的截短卷积码是线性分组码 B 的一个子集, 而 $d_{free}$ 定义为截短卷积码的最小重量, 因此得到结论 $d_j^c \leqslant (n-k)(j+1)+1$. 证毕.

## 附录 C

令 $\boldsymbol{u}=[u_0, u_1, \cdots]$, 且 $u_0$ 不为 0 表示截短卷积码的输入信息符号矢量, 由于它的最小自由距离 $d_j^c=(n-k)(j+1)+1$, 即 $\boldsymbol{u}G_j^c$ 得到的编码码矢至多只有 $k(j+1)-1$ 个 0, 这 $k(j+1)-1$ 个 0 对应了 $k(j+1)-1$ 个方

程,它存在非零解的充要条件是其行列式等于 0. 又由于每 $n$ 列中抽取 $k$ 列, 同时 $u_0$ 不为 0. 利用反证法, 假设每 $n$ 列中任取 $k$ 列组成的 $(j+1)k*(j+1)k$ 方阵的行列式等于 0, 那么就存在一个 $u_0$ 不为 0 的信息矢量 $u$, 使得 $\boldsymbol{u}G_j^c$ 中至少有 $k(j+1)$ 个码元为 0, 这导致截短卷积码的最小自由距离 $d_j^c<(n-k)(j+1)+1$, 与条件矛盾, 证毕.

参考文献:


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

[2] D J C MacKay, R M Neal. Near Shannon limit performance of low-density parity-check codes[J]. Elec Lett, 1996. 1645-1645.

[3] S K Chung, G D Forney, T Richardson. On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit[J]. IEEE Comm Lett, 2001. 58-60.

[4] IEEE Std. 802 16e, IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layer for Combined Fixed and Mobile Operation in Licensed Bands[S]. Feb. 2006.

[5] ETSI EN 302 307, Second Generation Framing Structure, Channel Coding and Modulation System for Broadcasting, Interactive Services, News Gathering and Other Broadband Satellite Applications[S]. Jan. 2004.

[6] Xiao-Yu Hu, Eleftheriou E, Arnold D-M. Progressive edge-growth tanner graphs[A]. IEEE GLOBECOM'01[C]. Massachusetts: MIT Press, 2001. 25-29.

[7] X Y Hu, E Eleftheriou, D-M Arnold. Regular and irregular progressive edge-growth Tanner graphs[J]. IEEE Trans Inf Theory, 2005. 386-398.

[8] Mansour M M, Shanbhag N R. A novel design methodology for high-performance programmable decoder cores for AA-LDPC codes[A]. IEEE SIPS'03[C]. Massachusetts: MIT Press, 2003. 29-34.

[9] Karkooti M, Cavallaro J R. Semi-parallel reconfigurable architectures for real-time LDPC decoding[A]. IEEE ITCC'04[C]. Massachusetts: MIT Press, 2004. 579-585.

[10] Y Kou, S Lin, M P C Fossorier. Low-density parity-check codes based on finite geometries: A rediscovery and new results[J]. IEEE Trans Inf Theory, 2001. 2711-2736.

[11] B Ammar, B Honary, Y Kou, J Xu, S Lin. Construction of low-density parity-check codes based on balanced incomplete block designs[J]. IEEE Trans Inf Theory, 2004. 1257-1269.

[12] I Djurdjevic, Jun Xu, K Abdel-Ghaffar, Shu Lin. A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols[J]. IEEE Comm Lett, 2003. 317-319.

[13] J Xu, L Zeng, L Lan, L Chen, S Lin. Construction of low-density parity-check codes by superposition[J]. IEEE Trans Comm, 2005. 243-251.

[14] K S Kim, S H Lee, Y H Kim, J Y Ahn. Design of binary LDPC code using cyclic shift matrices[J]. Elec Lett, 2004. 325-326.

[15] Fossorier M P C. Quasicyclic low-density parity-check codes from circulant permutation matrices[J]. IEEE Trans Inf Theory, 2004. 1788-1793.

[16] Seho Myung, Kyeongcheol Yang, Jaeyoel Kim. Quasi-cyclic LDPC codes for fast encoding[J]. IEEE Trans Inf Theory, 2005. 2894-2901.

[17] J Justesen, L R Hughes. On maximum-distance-separable convolutional codes[J]. IEEE Trans Inf Theory, 1974. 288-288.

[18] H G Luerssen, J Rosenthal, R Smarandache. Strongly-MDS convolutional codes[J]. IEEE Trans Inf Theory, 2006. 584-598.

[19] 谢亮, 乔秦宝, 周统和. LDPC 和 SPIHT 联合编码用于图像压缩与保护的方法[J]. 现代电视技术, 2005, 5: 142-144.
Xie Liang, Qiao Qin-bao, Zhou Tong-he. A method on image compression and protection by LDPC and SPIHT jointly encoding scheme[J]. Advanced Television Engineering, 2005, 5: 142-144. (in Chinese)


作者简介:


乔　华　男, 1980 年生于湖北武汉, 2002 年毕业于北京大学电子学系, 获得学士学位. 现为北京大学卫星与无线通信实验室直博生. 主要研究方向为信道编码以及卫星通信网.
E-mail: qiaohua@pku.edu.cn

董明科　男, 1973 年生, 1995 年于北京理工大学电子工程系获工学学士学位, 1998 年于北京大学电子学系获硕士学位. 现在北京大学电子学系从事数字通信、信号处理、软件无线电方向研究. E-mail: mingke.dong@pku.edu.cn

项海格　男, 1941 年生于云南, 1964 年毕业于北京大学无线电电子学系无线电物理专业, 并留校任教, 现任北京大学信息科学与技术学院电子学系教授. 他主要研究领域是数字通信、信号处理、无线和卫星通信网、软件无线电以及基于芯片的通信系统(SOC).
E-mail: xianghg@pku.edu.cn