文章编号:1001 - 893X(2011)09 - 0027 - 08

# BIBD 循环置换矩阵的多进制 LDPC 码构造*

刘 冰[1,3],陶 伟[2,3],窦高奇[3],高 俊[3]

(1.解放军 91469 部队,北京 100841;2.海军装备研究院,北京 100161;3.海军工程大学 电子工程学院,武汉 430033)

**摘 要**:提出了基于均衡不完全区组设计(Balanced Incomplete Block Design,BIBD)的多进制准循环 LDPC(Low-Density Parity-Check)码代数构造方法。在该构造方法中提出了广义多进制位置向量的概念,并根据广义多进制位置向量和 BIBD 法对指数矩阵进行广义二维扩展,构造出具有循环置换子矩阵的多进制校验矩阵,由此得到 girth 不小于 6 的多进制 LDPC 码。仿真结果表明,采用 FFT - QSPA(基于快速傅里叶变换的多进制和积算法)对构造出的 LDPC 码进行译码,在 AWGN 信道下相比于同参数的 RS 码来说可以取得明显的编码增益,并且优于多进制 Mackay 码。

**关键词**:多进制低密度奇偶校验码;准循环;均衡不完全区组;广义多进制位置向量;二维扩展

**中图分类号**:TN911.22 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2011.09.006

# Construction of Nonbinary LDPC Codes Based on BIBD Circulant Permutation Matrices

*LIU Bing*[1,3], *TAO Wei*[2,3], *DOU Gao-qi*[3], *GAO Jun*[3]

(1. Unit 91469 of PLA, Beijing 100841, China; 2. Naval Academy of Armament, Beijing 100161, China; 3. College of Electronic Engineering, Naval University of Engineering, Wuhan 430033, China)

**Abstract**: The algebraic method for constructing nonbinary quasi-cyclic (QC) low-density parity-check (LDPC) codes based on balanced incomplete block designs (BIBD) is presented. The generalized nonbinary location vector is proposed on constructions. A nonbinary matrix, which consists of nonbinary circulant submatrices, is formed by generalized two-dimensional matrix dispersion considering the generalized nonbinary location vector and BIBD method. The codes constructed by this method have girths at least 6. Experimental results show that significant coding gains are achieved over Reed-Solomon codes of the same parameters under the Additive White Gaussian Noise (AWGN) channel with iterative decoding Fast Fourier Transform based q - ary Sum - Product Algorithm (FFT-QSPA). And a good performance is also achieved over nonbinary Mackay LDPC codes with almost the same conditions.

**Key words**: nonbinary low-density parity-check (LDPC) codes; quasi-cyclic; balanced incomplete block design; generalized nonbinary location vector; two-dimensional dispersion

## 1 引 言

均衡不完全区组设计(Balanced Incomplete Block Design, BIBD)[1-2]可用于构造多进制低密度奇偶校验(Low-Density Parity-Check,LDPC)码,其是组合数学中组合设计的一个重要问题。BIBD 构造法属结构

* **收稿日期**:2011 - 02 - 18;**修回日期**:2011 - 08 - 30
**基金项目**:国家高技术研究发展计划(863 计划)项目(2009AAJ128,2010AA7010422);国家博士后科学基金(200902671)
**Foundation Item**: The National High - tech R&D Program of China (863 Program) (2009AAJ128, 2010AA7010422); The National Science Foundation for Post - doctoral Scientists of China (200902671)

化构造法[3-6]，相比于随机化构造法[7,8]，具有特定的结构，尤其是循环或准循环(Qusic - Cyclic，QC)结构，优势在于编码实现简单，仅用简单的移位寄存器就可实现线性化的编码复杂度[9]，这对工程的实际应用具有重要的作用和意义。将二进制 LDPC 码扩展到高阶伽罗华域上形成多进制 LDPC 码[10]，一般来说，精心设计的多进制 LDPC 码具有较二进制更好的性能，特别是在中短帧长度。但是多进制 LDPC 码面临着两大难题：编码和译码的复杂度过高。对于编码来说，可以采用准循环结构的 LDPC 码，达到线性化编码的目的[9]；而对于译码来说，基于快速傅里叶变换的多进制和积算法(Fast Fourier Transform based q - ary Sum - Product Algorithm，FFT - QSPA)[11]在取得优越性能的同时，有效地降低了多进制 LDPC 码的译码复杂度。

准循环 LDPC 码作为一类非常重要的 LDPC 码分支，其构造方法汲取和借鉴了代数、几何等领域的数学理论，多角度迅速发展。Shu Lin 课题研究小组首次提出了基于有限几何[12]、有限域[13]、循环置换矩阵[14]和 BIBD[3,15]等理论的系统化二进制 LDPC 码构造方法。之后在二进制构造的基础上首次提出了基于有限几何[16]和有限域[17]的多进制准循环 LDPC 码的系统化构造方法，相比于 RS 码而言，构造出的码字在 AWGN 信道下可以取得很大的编码增益。Bassem Ammar 将 BIBD 的一种特殊子类首次运用于二进制 LDPC 码的设计中[2]，该 LDPC 码校验矩阵的构造方法采用的是 BIBD 关联矩阵。BIBD 构造多进制校验矩阵时，其元素取自 GF($p^m$)，其中 $p$ 是素数，$m$ 为正整数，但是低复杂度的 FFT - QSPA 只能对 GF($2^l$)域上构造的码字进行译码[11,18]，因此在采用 BIBD 循环置换矩阵构造多进制 LDPC 码时，两者的适用前提条件是有所区别的。针对这一问题，本文提出了基于广义多进制位置向量的广义二维扩展方法以及两类基于 BIBD 广义循环置换矩阵(Circulant Permutation Matrix，CPM)的多进制 QC LDPC 码的构造方法，该方法可取得 girth 至少为 6 的规则多进制 QC LDPC 码。通过对指数矩阵进行基于广义多进制位置向量的水平扩展和基于部分周期循环特性的垂直扩展，使得构造校验矩阵非零元素的位置和数值分别取自 GF($p^m$)和 GF($2^l$)域。提出的广义二维扩展优势在于：可适用于非 2 幂次大小循环置换子矩阵的构造和 2 的幂次大小循环置换子矩阵的拓展；构造出的多进制 LDPC 码可采用低复杂度高性能的 FFT - QSPA 译码算法。

文章的组织结构如下：第 2 节提出了基于广义多进制位置向量的广义二维扩展方法，第 3 节由上述扩展方法构造出了两类 BIBD 循环置换矩阵的多进制 LDPC 码，第 4 节通过仿真结果比较了构造出多进制 LDPC 码的性能，最后是结束语。

## 2 BIBD 与多进制准循环 LDPC 码构造

多进制规则 LDPC 码 C 由多进制稀疏校验矩阵 $\boldsymbol{H}$ 的零空间所定义，其具有以下结构化性质：每行的重量(非零元素的个数)为 $d_c$；每列的重量为 $d_v$；行列(RC)约束，即任何两行(或两列)之间位置相同的非零元素个数不大于 1。这样构造出来的校验矩阵是规则的，由其零空间给出的码 C 称为($d_v$，$d_c$)规则 LDPC 码。RC 约束保证了两点：由 $\boldsymbol{H}$ 的零空间给出的 LDPC 码 C 的 Tanner 图 girth 至少为 6；码的最小距离至少为 $d_v+1$。如果 $\boldsymbol{H}$ 的行与(或)列具有不同的重量，那么 $\boldsymbol{H}$ 的零空间将给出一个非规则 LDPC 码。LDPC 码的误码性能由码结构特性的诸多因素共同决定，主要因素有 Tanner 图的 girth、短环的结构、处于某一码字上短环的数量、校验矩阵的选择和码字的最小距离等。目前只能通过仿真和基本的分析来考查这些起决定作用的因素，它们之间还没有明确的结论性关系，有待进一步研究。最影响码字性能的短环是长度为 4 的环，所以这类短环在校验矩阵的构造时应予以避免，这是目前绝大多数 LDPC 码构造时首要考虑的问题，同时也满足了定义中的行列约束性质。

具有 $q$ 个元素的阿贝尔群 $G$ 的一个 BIBD 是指 $G$ 的 $n$ 个 $r$ 子集，记为 $B_1, B_2, \cdots, B_n$，称为区组(Blocks)，它们满足如下条件[1]：每个元素恰好在 $n$ 个区组中的 $k$ 个出现；任一元素对恰好在 $n$ 个区组中的 $\lambda$ 个出现；每个区组中元素的个数 $r$ 与 $X$ 中的元素总数 $q$ 相比非常小。于是，一个 BIBD 由 $n$，$v=q$，$r$，$k$ 和 $\lambda$ 5 个参数来刻画。除了用区组的表示方式外，一个 BIBD 可以用一个GF($q$)域上的 $q\times n$ 关联矩阵 $\boldsymbol{H}=[h_{i,j}]$来描述：其行对应着 $X$ 的 $q$ 个元素；其列对应着该设计的 $n$ 个区组；当且仅当第 $i$ 个元素 $x_i$ 属于第 $j$ 个区组 $B_j$ 时，$h_{i,j}\neq 0$ 且 $h_{i,j}\in$GF($q$)，否则，$h_{i,j}=0$。这个矩阵被称为设计的关联矩阵 $\boldsymbol{H}$，$\boldsymbol{H}$ 的列重和行重分别是 $r$ 和 $k$。根据 BIBD 的第 2 个条件，$\boldsymbol{H}$ 的两个行向量具有 $\lambda$ 个公共的 1 分量。如果 $\lambda$

$=1$,$\boldsymbol{H}$ 就满足了 LDPC 码定义的所有性质,于是 $\boldsymbol{H}$ 的零空间给出了一个长度为 $n$ 的$(d_v, d_c)$规则 LDPC 码,其 Tanner 图中没有长度为 4 的环。这是基于 BIBD 最直接构造 LDPC 码的方法。对于$(n, v, r, k, 1)$ BIBD 素域构造方法可查阅相关文献[1-3,15]。而本文构造的多进制校验矩阵的基矩阵是基于 Bose BIBD 理论,首先阐述下面一个定理[1]。

**定理**:令 $G=\{x^{(1)}, x^{(2)}, \cdots, x^{(q)}\}$是具有 $q$ 个元素的阿贝尔群。对于 $G$ 中的每一个元素$x^{(i)}$,重复 $f$ 次,并记为 $x_1^{(i)}, x_2^{(i)}, \cdots, x_f^{(i)}$,这样通过群 $G$ 可以得到具有$fq$ 个元素的集合 $X$。将 $fq$ 个元素分为 $q$ 组,$X$ 的 $s$ 个 $r$ 子集,记为 $B_1, B_2, \cdots, B_s$,称为区组(Blocks),它们满足如下条件:在 $s$ 个区组中的$sr$ 个元素中,$k$ 个元素属于 $q$ 组中的一组;$s$ 个区组中元素的差是对称重复的,且每一个出现 $\lambda$ 次。

通过将 $G$ 中每个元素逐个加到每一个区组 $B_1$, $B_2, \cdots, B_s$ 上,可以得到一个具有参数 $v=fq$, $n=sq$, $r$, $k$ 和 $\lambda$ 的 BIBD,这里,区组 $B_1, B_2, \cdots, B_s$ 被称为基本区组。本文校验矩阵指数矩阵的构造则是建立在基本区组上。

BIBD 构造校验矩阵中的循环阵大小都是素数的幂 $p^m$,将 BIBD 构造的校验矩阵扩展到多进制上,可直接在 GF($p^m$)域上进行,即在 BIBD 决定的位置上随机或有规律地填入 GF($p^m$)域中的非零值。但是这种方法构造出的多进制 LDPC 码只能采用 QS-PA 算法或其衍生的算法来译码,而不能采用低复杂度的 FFT – QSPA 译码算法。采用 QSPA 算法存在的缺陷是复杂度较高,不利于工程实现,但是应用 FFT – QSPA 的前提是域的阶数必须为 2 的幂,这正是构造基于 BIBD 多进制 LDPC 码时的矛盾所在。因此,本文构造的基于 BIBD 多进制 LDPC 码会涉及到 GF($p^m$)和 GF($2^l$)两个不同的域,多进制 LDPC 码校验矩阵中非零元素的位置是由 GF($p^m$)域上 BIBD 设计决定的,而非零元素的取值则是在 GF($2^l$)域上进行的。这两个域的具体关系如下:

$$(2^l-1)\cdot(r_t-1)<p^m<(2^l-1)\cdot r_t$$

其中,$l\in\mathbb{Z}$;$r_t$ 为 GF($2^l$)域中所有非零元素重复的周期数,不足一个周期的,记为一个周期,并计入 $r_t$ 中;$r_c$ 是重复周期的带分数表示,整数部分表示重复的整数周期数,分数中分母表示一个周期的长度,分子表示不足一个周期的周期长度。$l$ 的取值与 $p^m$ 的值关系如下:

$$\begin{cases} l=\lceil \mathrm{lb}(p^m+1)\rceil, & r_t=1 \\ \mathrm{lb}\left(\dfrac{p^m}{r_t}+1\right)\leqslant l<\mathrm{lb}\left(\dfrac{p^m}{r_t-1}+1\right), & r_t\geqslant 2 \end{cases} \tag{1}$$

式中,$l\in\mathbb{Z}$,$\lceil\cdot\rceil$表示向上取整。

令 $\beta$ 是 GF($2^l$)域的本原元。$\beta^{-\infty}=0$,$\beta^0=1$,$\beta, \beta^2, \cdots, \beta^{2^l-2}$表示 GF($2^l$)域中的所有元素,并且 $\beta^{2^l-1}=1$。将基于 BIBD 区组的广义多进制位置向量定义为 $\boldsymbol{z}(i)=(z_0, z_1, \cdots, z_{p^m-1})$,其向量取值对应的是 GF($2^l$)域中的 $p^m$ 个非零元素,其中 $z_i=\beta^{i \bmod (2^l-1)}$,$i\in B_i$,而其它所有分量为 0。$B_i$ 中的元素称为循环置换矩阵的位置数,决定着校验矩阵非零值的位置。因此,$\boldsymbol{z}(i)$是 GF($2^l$)域上的 $p^m$ 重向量,其重量为 1。

令 $\delta\in B_i$ 且属于 GF($p^m$)域中的元素,则广义多进制位置向量 $\boldsymbol{z}(\delta+1)$定义为位置向量 $\boldsymbol{z}(\delta)$向右循环移一位,第 1 列到第 $p^m-1$ 列的元素右移后乘以 $\beta$,而最后一列元素则乘以 $\beta^{r_t(2^l-1)-(p^m-1)}$后得到第 1 列元素。多进制位置向量 $\boldsymbol{z}(\delta+j)$可定义为区组 $B_i$ 中某一元素依次加非零值 $j\in$GF($p^m$)后得到的一系列多进制位置向量。这样,在 GF($2^l$)域上可形成以 $\delta, \delta+1, \cdots, \delta+p^m-1$ 的位置向量为行的多进制 $p^m\times p^m$ 大小的广义循环置换矩阵 $\boldsymbol{Q}_{i,j}$。$\boldsymbol{Q}_{i,j}$可以认为是根据区组 $B_i$ 中某一元素 $\delta$ 的二维 $p^m$ 重扩展:

$$\boldsymbol{Q}_{i,j}=\mathrm{disp}(\delta)=\begin{bmatrix} \boldsymbol{z}(\delta) \\ \boldsymbol{z}(\delta+1) \\ \vdots \\ \boldsymbol{z}(\delta+p^m-1) \end{bmatrix} \tag{2}$$

二维 $p^m$ 重扩展是由垂直扩展和水平扩展两部分组成,对于某个元素 $\delta$,$\mathrm{disp}_v(\delta)=[\delta, \delta+1, \cdots, \delta+p^m-1]^{\mathrm{T}}$ 为该元素的垂直扩展,而 $\mathrm{disp}_h(\delta)=\boldsymbol{z}(\delta)$为该元素的水平扩展。根据上述基本概念和提出规则,可以对基本区组 $B_i$ 中所有元素进行广义二维 $p^m$ 重扩展得到广义多进制准循环矩阵。由于多进制校验矩阵非零值位置和数值的选取分别是建立在 GF($p^m$)和 GF($2^l$)这两个不同域中,构造出的二维 $p^m$ 重矩阵非零元素的分布具有两种情形:当 $r_t=1$ 时,在 GF($2^l$)域上只具有部分域元素循环($r_c<1$)或循环($r_c=1$)的特性;当 $r_t\geqslant 2$ 时,所有 GF($2^l$)域非零元素个数一般在矩阵中分布不均,但是当 $2^l-1=r_c p^m$ 时,非零元素分布将是均匀的。

下面将阐述通过 BIBD 构造的基矩阵扩展到

GF($2^l$)域多进制准循环校验矩阵的一般方法。假设通过 BIBD 方法构造出 $n \times r$ 的 GF($p^m$)域下指数矩阵：

$$\boldsymbol{E} = \begin{bmatrix} \boldsymbol{e}_0 \\ \boldsymbol{e}_1 \\ \vdots \\ \boldsymbol{e}_{n-1} \end{bmatrix} = \begin{bmatrix} e_{0,0} & e_{0,1} & \cdots & e_{0,r-1} \\ e_{1,0} & e_{1,1} & \cdots & e_{1,r-1} \\ \vdots & \vdots & \ddots & \vdots \\ e_{n-1,0} & e_{n-1,1} & \cdots & e_{n-1,r-1} \end{bmatrix} \tag{3}$$

式中，$e_{i,j} \in \mathrm{GF}(p^m)$，$\boldsymbol{E}$ 中的每一行是一个 BIBD 的基本区组。

$$\boldsymbol{E}_i = \mathrm{disp}_v(\boldsymbol{e}_i) = \begin{bmatrix} e_{i,0} & e_{i,1} & \cdots & e_{i,r-1} \\ e_{i,0}+1 & e_{i,1}+1 & \cdots & e_{i,r-1}+1 \\ \vdots & \vdots & \ddots & \vdots \\ e_{i,0}+p^m-1 & e_{i,1}+p^m-1 & \cdots & e_{i,r-1}+p^m-1 \end{bmatrix} \tag{4}$$

$\boldsymbol{E}_i$ 具有如下的结构特性：每一列都是GF($p^m$)中循环顺序的 $p^m$ 个元素；任意两列所有位置的元素各不相同；任意两行所有位置的元素各不相同。根据这三点特性可知，来自不同两行垂直扩展的矩阵 $\boldsymbol{E}_i$ 和$\boldsymbol{E}_j$ 不会在同一位置上具有相同的元素，这就保证了 RC 约束条件。然后将 $\boldsymbol{E}_i$ 进行水平扩展，就可构造出一个 $n \times r$ 阵列 $p^m \times p^m$ 循环置换矩阵 $\boldsymbol{Q}$：

$$\boldsymbol{Q} = \begin{bmatrix} Q_{0,0} & Q_{0,1} & \cdots & Q_{0,r-1} \\ Q_{1,0} & Q_{1,1} & \cdots & Q_{1,r-1} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{n-1,0} & Q_{n-1,1} & \cdots & Q_{n-1,r-1} \end{bmatrix} \tag{5}$$

二维 $p^m$ 重扩展 disp($e_{i,j}$)可以理解为将 $\boldsymbol{E}$ 中的一个元素 $e_{i,j}$ 扩展成一个循环置换矩阵$\boldsymbol{Q}_{i,j}$，对于任一整数对($d_v$, $d_c$)，其中 $1 \leqslant d_v \leqslant n$，$1 \leqslant d_c \leqslant r$，令 $\boldsymbol{Q}(d_v, d_c)$是 $\boldsymbol{Q}$ 的 $d_v \times d_c$ 子阵列，则 $\boldsymbol{Q}(d_v, d_c)$就是一个 GF($2^l$)域上的 $d_v p^m \times d_c p^m$ 矩阵，同时也满足 RC 约束，其零空间给出的就是长度为 $d_c p^m$ 的多进制 CPM – BIBD – LDPC 码。其码率至少为 $1 - d_v/d_c$，girth 至少为 6。令 $\boldsymbol{H} = \boldsymbol{Q}^{\mathrm{T}}$，则 $\boldsymbol{H}$ 是一个 $r \times n$ 阵列 $p^m \times p^m$ 循环置换矩阵。对于任一整数对($d_v$, $d_c$)，其中 $1 \leqslant d_v \leqslant r$，$1 \leqslant d_c \leqslant n$，令 $\boldsymbol{H}(d_v, d_c)$是 $\boldsymbol{H}$ 的 $d_v \times d_c$ 子阵列，则 $\boldsymbol{H}(d_v, d_c)$同样可表述为一个 GF($2^l$)域上的 $d_v p^m \times d_c p^m$ 矩阵，同时也满足 RC 约束，其零空间给出的就是长度为 $d_c p^m$ 的多进制 CPM – BIBD – LDPC 码。其行重为 $d_c$，列重为 $d_v$，码率至少为 $1 - d_v/d_c$，$\boldsymbol{H}$ 满足 RC 约束，因此，girth 至少也为 6。

## 3 BIBD 循环置换矩阵多进制 LDPC 码

### 3.1 第 1 类 CPM – BIBD – LDPC 码

令 $t$ 是满足 $12t + 1 = p^m$ 的一个正整数，其中 $p$ 是一个素数，$m$ 是一个正整数，也就是说，$12t + 1$ 是一个素数的幂。假设 GF($12t + 1$)域有一个本原元 $\alpha$ 满足 $\alpha^{4t} - 1 = \alpha^c$，其中 $c$ 是一个小于 $p^m$ 的正奇数，表 1 给出了部分 $t$、$12t + 1$ 及所对应的全部 $\alpha$ 和 $c$ 的取值表，以使在素域 GF($12t + 1$)中存在满足 $\alpha^{4t} - 1 = \alpha^c$ 的本原元 $\alpha$，其中本原元 $\alpha$ 是用实数来表示的。

**表 1 在素域 GF($12t + 1$)中本原元 $\alpha$ 满足 $\alpha^{4t} - 1 = \alpha^c$ 时参数的取值**

Table 1 A list of parameters that the prime field GF($12t + 1$) has a primitive element $\alpha$ such that the condition $\alpha^{4t} - 1 = \alpha^c$ holds

| $t$ | $12t + 1$ | ($\alpha$, $c$) |
|---|---|---|
| 1 | 13 | (11,7) (7,9) (6,3) (2,1) |
| 6 | 73 | (68, 69) (62, 51) (60, 27) (59, 9) (58, 51) (53, 9) (47, 15) (45, 69) (44, 27) (42, 27) (40, 33) (39, 45) (34, 9) (33, 69) (31, 63) (29,63) (28, 33) (26, 51) (20, 45) (15, 15) (14,45) (13,63) (11,15) (5,33) |
| 8 | 97 | (92, 75) (90, 21) (87, 41) (84, 3) (83, 59) (82,77) (80, 83) (76, 95) (74, 71) (71, 65) (68, 87) (60, 81) (59, 9) (58, 5) (57, 93) (56,63) (41, 15) (40, 45) (39, 53) (38, 57) (37,33) (29, 39) (26, 17) (23, 23) (21, 47) (17,35) (15, 29) (14, 11) (13, 51) (10, 89) (7,69) (5,27) |
| 9 | 109 | (103,17) (99, 5) (98, 85) (96, 47) (95, 77) (91, 19) (85, 95) (79, 79) (72, 7) (70, 13) (69,11) (67, 43) (65, 55) (62, 91) (59, 103) (58,53) (57, 89) (56, 29) (53, 83) (52, 35) (51,107) (50, 49) (47, 37) (44, 1) (42, 97) (40,65) (39, 67) (37, 61) (30, 25) (24, 41) (18,73) (14, 23) (13, 101) (11, 31) (10, 59) (6,71) |
| 15 | 181 | (179,103) (171,19) (163,41) (160,83) (158,101) (157,167) (153,29) (140,71) (134,91) (131,151) (128,79) (127,7) (124,143) (123,127) (118,49) (115,107) (112,67) (105,89) (104,149) (103,113) (98,163) (97,31) (96,133) (91,137) (90,47) (85,43) (84,121) (83,73) (78,23) (77,59) (76,179) (69,157) (66,17) (63,139) (58,37) (57,53) (54,97) (53,169) (50,61) (47,1) (41,161) (28,119) (24,77) (23,11) (21,173) (18,131) (10,109) (2,13) |

于是，对于具有 $q = 12t + 1$ 个元素集合 $G$ 中每个元素重复$f = 1$ 次得到集合 $X$，存在一个 BIBD，它具有 $n = t(12t + 1)$个区组，每个区组由 $r = 4$ 个元

素组成,每个元素恰好在 $k=4t$ 个区组中出现,每个元素对恰好在 $\lambda=1$ 个区组中出现。用 GF$(12t+1)$ 域的元素 $\alpha^{-\infty}=0,\alpha^0=1,\alpha,\alpha^2,\cdots,\alpha^{12t-1}$来表示集合 $X$ 的 $12t+1=p^m$ 个元素。于是,$X$ 的 BIBD 可由下述 $t$ 个基本区组完全确定:

$$B_i=\{0,\alpha^{2i},\alpha^{2i+4t},\alpha^{2i+8t}\} \tag{6}$$

式中,$0\leqslant i<t$。

对于给定的第 1 类 BIBD 的每一个基本区组,可形成一个 $t\times 4$ 的基矩阵 $\boldsymbol{E}^{(1)}$:

$$\boldsymbol{E}^{(1)}=\begin{bmatrix}e_0\\e_1\\\vdots\\e_{t-1}\end{bmatrix}=\begin{bmatrix}0&\alpha^0&\alpha^{4t}&\alpha^{8t}\\0&\alpha^2&\alpha^{2+4t}&\alpha^{2+8t}\\\vdots&\vdots&\vdots&\vdots\\0&\alpha^{2(t-1)}&\alpha^{2(t-1)+4t}&\alpha^{2(t-1)+8t}\end{bmatrix} \tag{7}$$

通过广义二维 $12t+1$ 重扩展后可得多进制的 $(12t+1)\times(12t+1)$广义循环置换矩阵的 $t\times 4$ 阵列:

$$\boldsymbol{Q}^{(1)}=\begin{bmatrix}Q_{0,0}&Q_{0,1}&\cdots&Q_{0,3}\\Q_{1,0}&Q_{1,1}&\cdots&Q_{1,3}\\\vdots&\vdots&\ddots&\vdots\\Q_{t-1,0}&Q_{t-1,1}&\cdots&Q_{t-1,3}\end{bmatrix} \tag{8}$$

令 $\boldsymbol{H}^{(1)}$是$\boldsymbol{Q}^{(1)}$的转置,即:

$$\boldsymbol{H}^{(1)}=[\boldsymbol{Q}^{(1)}]^{\mathrm{T}}=\begin{bmatrix}H_{0,0}&H_{0,1}&\cdots&H_{0,t-1}\\H_{1,0}&H_{1,1}&\cdots&H_{1,t-1}\\H_{2,0}&H_{2,1}&\cdots&H_{2,t-1}\\H_{3,0}&H_{3,1}&\cdots&H_{3,t-1}\end{bmatrix} \tag{9}$$

可以很清楚地看出,$\boldsymbol{Q}^{(1)}$ 和 $\boldsymbol{H}^{(1)}$ 分别是具有 $(12t+1)\times(12t+1)$的多进制循环置换矩阵的 $t\times 4$ 和 $4\times t$ 阵列,对于每一个子矩阵 $\boldsymbol{Q}_{j,i}$($\boldsymbol{H}_{i,j}$)都是 $(12t+1)\times(12t+1)$的多进制循环置换矩阵,行重(列重)和列重(行重)分别为 4 和 $t$。由于对 $\boldsymbol{Q}^{(1)}(d_v,d_c)$和$\boldsymbol{H}^{(1)}(d_v,d_c)$的分析是一致的,只是 $d_v$ 和 $d_c$ 的取值范围不同。下面以$\boldsymbol{H}^{(1)}$为例,对于 $1\leqslant d_v\leqslant 4,1\leqslant d_c\leqslant t$,令$\boldsymbol{H}^{(1)}(d_v,d_c)$是$\boldsymbol{H}^{(1)}$的 $d_v\times d_c$ 子阵列,则$\boldsymbol{H}^{(1)}(d_v,d_c)$是 $d_v(12t+1)\times d_c(12t+1)$ 的多进制矩阵,$d_v$、$d_c$ 恰为矩阵的列重和行重,$H^{(1)}(d_v,d_c)$的零空间给出了一个$(d_v,d_c)$的规则多进制 CPM – BIBD – LDPC 码。码长为 $N=d_c(12t+1)$,最小距离至少为 $d_v+1$,码率至少为 $1-d_v/d_c$。

### 3.2　第 2 类 CPM – BIBD – LDPC 码

令 $t$ 是满足 $20t+1=p^m$ 的一个正整数,其中 $p$ 是一个素数。假设 GF$(20t+1)$域有一个本原元 $\alpha$ 满足 $\alpha^{4t}+1=\alpha^c$,其中 $c$ 是一个小于 $p^m$ 的正奇数。表 2 给出了部分 $t$、$20t+1$ 及所对应的全部 $\alpha$ 和 $c$ 的取值表,以使在素域 GF$(20t+1)$中存在满足 $\alpha^{4t}-1=\alpha^c$ 的本原元$\alpha$。

**表 2　在素域 GF$(20t+1)$中本原元 $\alpha$ 满足 $\alpha^{4t}+1=\alpha^c$ 时参数的取值**

Table 2 A list of parameters that the prime field GF$(20t+1)$ has a primitive element $\alpha$ such that the condition $\alpha^{4t}+1=\alpha^c$ holds

| $t$ | $20t+1$ | $(\alpha,c)$ |
|---|---|---|
| 2 | 41 | (35,23) (34,25) (30,31) (29,7) (28,33) (26,17) (24,21) (22,15) (19,35) (17,1) (15,37) (13,13) (12,27) (11,11) (7,5) (6,3) |
| 3 | 61 | (59,53) (55,55) (54,29) (51,47) (44,35) (43,37) (35,13) (31,49) (30,19) (26,43) (18,7) (17,5) (10,17) (7,59) (6,25) (2,23) |
| 12 | 241 | (234,77) (228,5) (227,67) (210,107) (207,17) (206,71) (204,163) (202,41) (199,223) (195,205) (190,143) (189,145) (186,73) (185,167) (179,217) (175,55) (173,7) (172,211) (171,181) (170,131) (167,173) (163,31) (157,233) (155,101) (149,95) (146,133) (142,121) (137,35) (132,185) (131,203) (129,37) (127,115) (114,235) (112,157) (110,83) (109,65) (104,155) (99,1) (95,13) (92,215) (86,221) (84,113) (78,151) (74,53) (71,11) (70,61) (69,91) (68,127) (66,175) (62,97) (56,47) (55,193) (52,25) (51,23) (46,85) (42,103) (39,161) (37,43) (35,191) (34,137) (31,227) (14,187) (13,125) (7,197) |
| 14 | 281 | (278,33) (270,23) (269,193) (268,153) (266,153) (262,213) (260,93) (259,43) (258,23) (257,263) (255,143) (254,73) (251,23) (240,253) (239,113) (237,53) (235,153) (233,83) (230,173) (229,123) (227,53) (226,183) (210,243) (207,123) (206,183) (205,93) (199,73) (198,143) (197,263) (194,223) (190,223) (187,23) (186,93) (185,93) (184,213) (178,173) (177,253) (176,113) (174,103) (173,43) (171,33) (166,13) (164,3) (161,103) (159,103) (154,83) (150,143) (148,193) (133,53) (131,3) (127,223) (122,243) (120,243) (117,143) (115,153) (110,173) (108,183) (107,243) (105,253) (104,113) (103,33) (97,73) (96,233) (95,233) (94,163) (91,83) (87,83) (84,123) (83,3) (82,213) (76,233) (75,43) (74,263) (71,103) (55,43) (54,193) (52,263) (51,33) (48,223) (46,13) (44,193) (42,253) (41,113) (30,163) (27,213) (26,3) (24,123) (23,163) (22,183) (21,233) (19,73) (15,13) (13,13) (12,53) (11,163) (3,173) |

于是,对于具有 $q=20t+1$ 个元素的集合 $X$,存

在一个 BIBD,它有 $n = t(20t+1)$个区组,每个区组由 $r=5$ 个元素组成,每个元素恰好在 $k=5t$ 个区组中出现,每个元素对恰好在 $\lambda=1$ 区组中出现。用 GF($20t+1$)域的元素 $\alpha^{-\infty}=0, \alpha^0=1, \alpha, \alpha^2, \cdots, \alpha^{20t-1}$来表示集合 $X$ 的 $20t+1=p^m$ 个元素。于是,$X$ 的 BIBD 由下述 $t$ 个基本区组完全确定:

$$B_i = \{\alpha^{2i}, \alpha^{2i+4t}, \alpha^{2i+8t}, \alpha^{2i+12t}, \alpha^{2i+16t}\} \quad (10)$$

式中,$0 \leqslant i < t$。

对于给定的第 2 类 BIBD 的每一个基本区组,可形成一个 $t \times 4$ 的基矩阵$\boldsymbol{E}^{(2)}$:

$$\boldsymbol{E}^{(2)} = \begin{bmatrix} \boldsymbol{e}_0 \\ \boldsymbol{e}_1 \\ \vdots \\ \boldsymbol{e}_{t-1} \end{bmatrix} = \begin{bmatrix} \alpha^0 & \alpha^{4t} & \alpha^{8t} & \alpha^{12t} & \alpha^{16t} \\ \alpha^2 & \alpha^{2+4t} & \alpha^{2+8t} & \alpha^{2+12t} & \alpha^{2+16t} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{2(t-1)} & \alpha^{2(t-1)+4t} & \alpha^{2(t-1)+8t} & \alpha^{2(t-1)+12t} & \alpha^{2(t-1)+16t} \end{bmatrix} \quad (11)$$

$\boldsymbol{E}^{(2)}$的垂直扩展其实是通过将 GF($p^m$)中的每个元素逐个加到这 $t$ 个基本区组的每一个上而得到 BIBD 的所有 $n=t(20t+1)$个区组。通过广义二维 $20t+1$ 重扩展后可得到具有$(20t+1)\times(20t+1)$广义多进制循环置换矩阵的 $t \times 5$ 阵列$\boldsymbol{Q}^{(2)}$,令$\boldsymbol{H}^{(2)} = [\boldsymbol{Q}^{(2)}]^{\mathrm{T}}$,$\boldsymbol{Q}^{(2)}$和$\boldsymbol{H}^{(2)}$都可作为多进制 LDPC 码的校验矩阵。同样,对于$\boldsymbol{H}^{(2)}$,$1 \leqslant d_v \leqslant 5$,$1 \leqslant d_c \leqslant t$,而对于$\boldsymbol{Q}^{(2)}$,$1 \leqslant d_v \leqslant t$,$1 \leqslant d_c \leqslant 5$,$\boldsymbol{H}^{(2)}(d_v, d_c)$和$\boldsymbol{Q}^{(2)}(d_v, d_c)$分别是$\boldsymbol{H}^{(2)}$和$\boldsymbol{Q}^{(2)}$中 $d_v \times d_c$ 大小的子阵列,其零空间也给出了一个$(d_v, d_c)$的规则多进制 CPM – BIBD – LDPC 码。码长为 $N = d_c(20t+1)$,最小距离至少为 $d_v+1$,码率至少为 $1-d_v/d_c$。

## 4 仿真结果及性能分析

本节给出两类由 BIBD 构造出的多进制 CPM – BIBD – LDPC 码采用 FFT – QSPA 译码时的性能,并与相同比特长度的 RS 码和多进制 Mackay LDPC 码进行比较。所有仿真中的信号均采用 BPSK 调制,且在双边功率谱密度为 $N_0/2$ 的加性高斯白噪声(Additive White Gaussian Noise, AWGN)信道中传输。FFT – QSPA 算法的最大迭代次数设置为 50。

对于第 1 类多进制 CPM – BIBD – LDPC 码,取 $t=6$,该设计具有如下参数:$v=q=73$,$n=438$,$r=4$,$k=48$ 和 $\lambda=1$,这样可以得到一个 $6\times4$ 的基矩阵$\boldsymbol{E}^{(1)}$。为了设计一列重 $d_v=3$、行重 $d_c=6$ 的多进制 LDPC 码,首先只取$\boldsymbol{E}^{(1)}$中的前 $6\times3$ 矩阵作为构造多进制 CPM – BIBD – LDPC 码的基矩阵$\boldsymbol{E}^{(1)}(3,6)$:

$$\boldsymbol{E}^{(1)}(3,6) = \begin{bmatrix} 0 & 1 & 8 \\ 0 & 25 & 54 \\ 0 & 41 & 36 \\ 0 & 3 & 24 \\ 0 & 2 & 16 \\ 0 & 50 & 35 \end{bmatrix} \quad (12)$$

对$\boldsymbol{E}^{(1)}(3,6)$进行广义二维扩展的矩阵经转置后可得$\boldsymbol{H}^{(1)}(3,6)$,它是一个由 $3\times6$ 的 $73\times73$ 的广义循环置换矩阵所构成校验矩阵,其非零值的位置和数值分别建立在 GF(73)和 GF($2^7$)域上。由构造出的$\boldsymbol{H}^{(1)}(3,6)$的零空间将给出一个码率为0.504 6 的 128 – ary (438,221) CPM – BIBD – LDPC 码。采用 FFT – QSPA 译码算法,该码的性能如图 1 所示。为了便于比较,我们也给出了同比特长度 RS 码的 BM 算法的误码性能。在 FER 为 $10^{-4}$处,相对于 GF($2^9$)域上采用 BM 算法的(340,172) RS 码来说,取得了大约3.80 dB的编码增益。

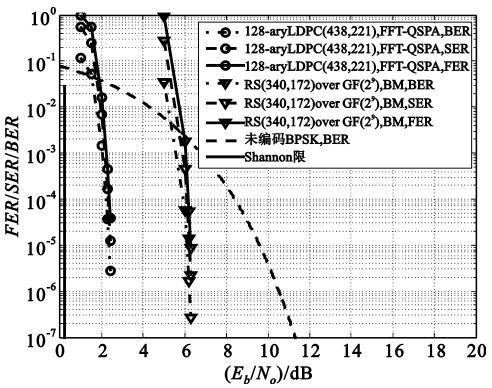


图 1 采用 FFT – QSPA 译码的 128 – ary (438,221) CPM – BIBD – LDPC 码和采用 BM 算法 GF($2^9$)域的(340,172) RS 码的误码性能

Fig.1 Error performances of the 128 – ary (438,221) BIBD – QC – LDPC code decoded with the FFT – QSPA and the (340,172) RS code over GF($2^9$) decoded with the BM algorithm

为了构造出不同的 $2^l$ 进制的 LDPC 码,根据式(1)可知,当 $l=7$ 时,$r_t=1$,$r_c=\frac{73}{127}$;当 $l=6$ 时,$r_t=2$,$r_c=1\frac{10}{63}$;当 $l=5$ 时,$r_t=3$,$r_c=2\frac{11}{31}$。因此,可以据此构造出 128 – ary、64 – ary、32 – ary CPM – BIBD – LDPC 码。如图 2 所示,首先我们将 128 – ary CPM – BIBD – LDPC 码与几乎同码率的 128 – ary Mackay LDPC 码作一比较,相比于 Mackay LDPC 码,在 FER 为 $10^{-4}$处取得了大约0.14 dB的编码增益,因而本文提出的多进制 CPM – BIBD – LDPC 码具有更好的误

码性能。通过对不同进制的 LDPC 码比较可以看出,随着进制数的减少,误码性能也相对变好,但是这种性能的差距不大,进制数的减少同时也能降低译码的复杂度。这种现象 Mackay 也曾指出[19]:随着域阶数的增加,其误码性能并不总是单调提升,这一现象的产生与校验矩阵的构造密切相关。

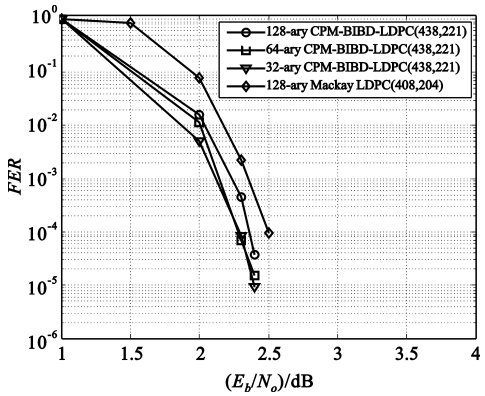


图 2　不同进制数下的(438,221) CPM – BIBD – LDPC 码和 128 – ary Mackay LDPC 码的性能比较

Fig.2 Performances comparison of (438,221) CPM – BIBD – LDPC codes over different Galois fields and a 128 – ary Mackay LDPC code

图 3 给出了 4 种 LDPC 码的平均迭代次数曲线图,其反映了如下 3 点:构造出的多进制 LDPC 码具有很好的收敛特性;随着进制数的减少,其收敛越快,但是之间的差距并不大;相比于 Mackay LDPC 码,本文构造的 LDPC 码误码性能和收敛特性更为优越。

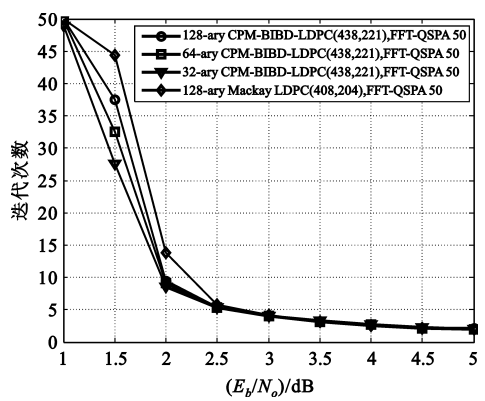


图 3　采用 FFT – QSPA 译码不同进制数下 CPM – BIBD – LDPC 码和 Mackay LDPC 码的平均迭代次数

Fig.3 Average numbers of iterations for decoding CPM – BIBD – LDPC codes over different Galois fields and a Mackay LDPC code with the FFT – QSPA

对于第 2 类多进制 CPM – BIBD – LDPC 码,取 $t=3$,这样可以得到一个 $3\times5$ 的基矩阵 $\boldsymbol{E}^{(2)}$:

$$\boldsymbol{E}^{(2)}(3,5)=\begin{bmatrix}1 & 9 & 20 & 58 & 34\\ 4 & 36 & 19 & 49 & 14\\ 16 & 22 & 15 & 13 & 56\end{bmatrix} \tag{13}$$

利用第 2 节提出的二维扩展方法可设计出一个 $183\times305$ 的多进制校验矩阵 $\boldsymbol{Q}^{(2)}(3,5)$,其列重和行重分别是 3 和 5。$\boldsymbol{Q}^{(2)}(3,5)$的零空间给出一个码率为0.406 6的 64 – ary (305,124) CPM – BIBD – LDPC 码。该 LDPC 码的 FFT – QSPA 和 RS 码的 BM 算法的误码性能和迭代性能如图 4 所示。与上述分析类似,在 BER 为 $10^{-4}$处,相对于 GF($2^8$)上采用 BM 算法的(229,93) RS 码来说,取得了大约3.90 dB的编码增益。

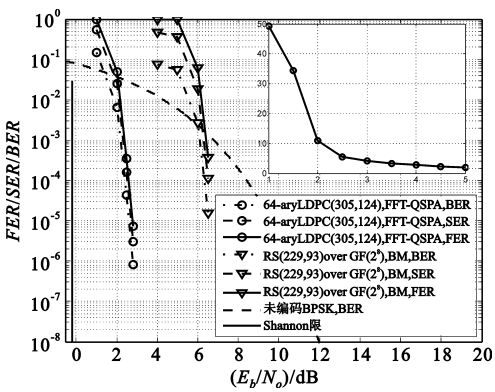


图 4　采用 FFT – QSPA 译码的 64 – ary (305,124) CPM – BIBD – LDPC 码和采用 BM 算法 GF($2^8$)域的(229,93) RS 码的误码性能和迭代性能

Fig.4 Error performances and iteration characteristic of the 64 – ary (305,124) CPM – BIBD – LDPC code decoded with the FFT – QSPA and the (229,93) RS code over GF($2^8$) decoded with the BM algorithm

## 5　结束语

多进制码的优势在于应对突发噪声和混合类型噪声比二进制码更为有效,多进制码中的 RS 码广泛应用于随机噪声、突发噪声和干扰同时存在的通信系统或数据存储系统中,而目前多进制 LDPC 码的研究呈现上升趋势,表现出了具有替代 RS 码的潜能。本文提出了基于 BIBD 循环置换矩阵的多进制 LDPC 码构造方法,多进制校验矩阵中非零元素位置的确定源于对基本区组的选择,而非零元素数值的选取则是建立在提出的广义多进制位置向量的基础上。在这种规则下构造出的多进制 LDPC 码具有 QC 特性,编译码复杂度低,其 Tanner 图没有长度为 4 的环路,提出的构造方法可适用于所有素数大小的循环置换子矩阵组成的多进制校验矩阵,具有

很大的灵活性和可扩展性。仿真结果表明,在采用低复杂度 FFT – QSPA 译码时具有很好的纠错性能和良好的收敛特性,在几乎相同的比特长度上,本文构造的多进制 LDPC 码比 RS 码和多进制 Mackay LDPC 码具有更好的性能。

## 参考文献:


[1] Bose R C. On the construction of balanced incomplete design [J]. Annals of Eugenics, 1939, 9(1): 353 – 399.

[2] Ammar B, Honary B, Kou Y, et al. Construction of low – density parity – check codes based on balanced incomplete block designs[J]. IEEE Transactions on Information Theory, 2004, 50(6): 1257 – 1268.

[3] Lan L, Tai Y Y, Lin S, et al. New constructions of quasi – cyclic LDPC codes based on special classes of BIBD's for the AWGN and binary erasure channels[J]. IEEE Transactions on Communications, 2008, 56(1): 39 – 48.

[4] Zhou B, Kang J, Song S, et al. Construction of non – binary quasi – cyclic LDPC codes by arrays and array dispersions [J]. IEEE Transactions on Communications, 2009, 57(6): 1652 – 1662.

[5] Chen C, Bai B, Wang X. Construction of nonbinary quasi – cyclic LDPC cycle codes based on singer perfect difference set [J]. IEEE Communications Letters, 2010, 14(2): 181 – 183.

[6] Kang J, Huang Q, Zhang L, et al. Quasi – cyclic LDPC codes: An algebraic construction[J]. IEEE Transactions on Communications, 2010, 58(5): 1383 – 1396.

[7] Chen X, Men A, Yang B, et al. Construction of LDPC codes over GF(q) with modified progressive edge growth[J]. Journal of China Universities of Posts and Telecommunications, 2009, 16(5): 103 – 106.

[8] Shebl S, El – Fishawy N, Elazm A A, et al. A random construction of LDPC codes using a sub – optimal search algorithm[C]// Proceedings of 2009 National Conference on National Radio Science. New Cairo, Egypt: IEEE, 2009: 1 – 10.

[9] Li Z, Chen L, Zeng L, et al. Efficient encoding of quasi – cyclic low – density parity – check codes[J]. IEEE Transactions on Communications, 2006, 54(1): 71 – 81.

[10] Song S, Zhou B, Lin S, et al. A unified approach to the construction of binary and nonbinary quasi – cyclic LDPC codes based on finite fields[J]. IEEE Transactions on Communications, 2009, 57(1): 84 – 93.

[11] Barnault L, Declercq D. Fast decoding algorithm for LDPC over GF($2^q$)[C]//Proceedings of 2003 IEEE Information Theory Workshop. Paris, France: IEEE, 2003: 70 – 73.

[12] Kou Y, Lin S, Fossorier M P C. Low – density parity – check codes based on finite geometries: A rediscovery and new results[J]. IEEE Transactions on Information Theory, 2001, 47(7): 2711 – 2736.

[13] Lan L, Zeng L, Tai Y Y, et al. Construction of quasi – cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach[J]. IEEE Transactions on Information Theory, 2007, 53(7): 2429 – 2458.

[14] Fossorier M P C. Quasi – cyclic low – density parity – check codes from circulant permutation matrices[J]. IEEE Transactions on Information Theory, 2004, 50(8): 1788 – 1793.

[15] Djordjevic I B. Quantum LDPC codes from balanced incomplete block designs[J]. IEEE Communications Letters, 2008, 12(5): 389 – 391.

[16] Zeng L, Lan L, Tai Y Y, et al. Construction of nonbinary cyclic, quasi – cyclic and regular LDPC codes: A finite geometry approach[J]. IEEE Transactions on Communications, 2008, 56(3): 378 – 387.

[17] Zeng L, Lan L, Tai Y Y, et al. Constructions of nonbinary quasi – cyclic LDPC codes: A finite field approach[J]. IEEE Transactions on Communications, 2008, 56(4): 545 – 554.

[18] Voicila A, Declercq D, Verdier F, et al. Low – complexity decoding for non – binary LDPC codes in high order fields [J]. IEEE Transactions on Communications, 2010, 58(5): 1365 – 1375.

[19] Davey M C, MacKay D. Low – density parity check codes over GF(q)[J]. IEEE Communications Letters, 1998, 2(6): 165 – 167.


## 作者简介:


**刘　冰**(1984—),男,江西南昌人,博士,工程师,主要研究方向为差错控制编码和数字通信信号处理;

LIU Bing was born in Nanchang, Jiangxi Province, in 1984. He is now an engineer with the Ph.D. degree. His research interests include error control coding and signal processing for digital communications.

Email: liubing5275093@hotmail.com

**陶　伟**(1974—),男,黑龙江哈尔滨人,博士研究生,工程师,主要研究方向为差错控制编码和无线数据传输;

TAO Wei was born in Harbin, Heilongjiang Province, in 1974. He is now an engineer and currently working toward the Ph.D. degree. His research interests include error control coding and wireless data transmission.

Email: alantao0451@yahoo.com.cn

**窦高奇**(1981—),男,山西长治人,博士,讲师,主要研究方向为差错控制编码和数字通信信号处理;

DOU Gao – qi was born in Changzhi, Shanxi Province, in 1981. He is now a lecturer with the Ph.D. degree. His research interests include error control coding and signal processing for digital communications.

Email: gqdou0917@163.com

**高　俊**(1957—),男,江苏泰兴人,1989 年获博士学位,现为教授、博士生导师,主要研究方向为信道编码和数字通信。

GAO Jun was born in Taixing, Jiangsu Province, in 1957. He received the Ph.D. degree from Beijing Institute of Technology in 1989. He is now a professor and also the Ph.D. supervisor. His research interests include error control coding and digital communications.

Email: gaojunnj@163.com