doi:10.3969/j.issn.1000-436x.2014.03.009

针对 IRA-LDPC 码类的半随机半代数结构设计

彭立，张琦，王渤，陈涛
（华中科技大学 电信系 武汉国家光电实验室，湖北 武汉 430074）

摘 要：提出用半随机半代数结构的设计方法来构造 IRA-LDPC 码的信息位所对应的奇偶校验矩阵 $\boldsymbol{H}^d$。与现有结构化 LDPC 码相比，所给出的 $\boldsymbol{H}^d$ 矩阵的结构化紧凑表示阵列的独特优势在于：可使 $\boldsymbol{H}^d$ 矩阵中每个 1 元素的位置坐标均能用数学表达式计算得到，不仅极大地降低了随机奇偶校验矩阵对存储资源的消耗，而且还为 LDPC 编解码器的低复杂度硬件实现提供了可能性。与现有工业标准中的 LDPC 码相比，所提出的 IRA-LDPC 码在误码率与信噪比的仿真性能方面也占有优势。

关键词：不规则重复积累码（IRA 码）；低密度奇偶校验码（LDPC 码）；奇偶校验矩阵；整数模 n 剩余类；整数模 n 循环群

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2014)03-0077-08

Semi-random and semi-algebraic structural design for IRA-LDPC codes

PENG Li, ZHANG Qi, WANG Bo, CHEN Tao
(Wuhan National Laboratory for Optoelectronics, Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: A method of semi-random and semi-algebraic structure was presented for constructing the low-density parity-check matrix that corresponds to the information bits of the IRA codes. Compared with the existing structural LDPC codes, the distinct advantage of the presented compact structural array for information-bit-corresponding matrix is that the position coordinate of each 1 element in this matrix can be calculated by a determinate algebraic expression, which not only reduces the consumption of memory resource for the random parity-check matrix, but also provides the potential probability for designing low complexity hardware circuit of the LDPC encoder/decoder. In addition, compared with the existing practical LDPC codes in industrial standard, the presented IRA-LDPC code is also slight preponderance in the performance of simulation in bit error rate and signal noise ratio (BER-SNB).

Key words: irregular repeat-accumulate codes; low-density parity-check codes; parity-check matrix; residue class of integers modulo n; cyclic group of integers modulo n

1 引言

自从 1996 年低密度奇偶校验（LDPC）码[1]复出[2,3]以来，关于 LDPC 码的理论和应用研究就成为纠错码领域普遍关注的焦点之一。尽管多个无线通信工业标准采纳了计算机搜索的 LDPC 码[4~8]作为收发信机系统的主要纠错和抗噪声方案，但从减少搜索 LDPC 码对存储空间的占用量和降低编解码器硬件实现复杂度的角度出发，实用 LDPC 码的结构化设计及其性能分析方法仍然是当今及今后相当长一段时期内纠错码领域需要继续关注的研究命题[9~13,14]之一。目前，用数学方法设计的有代表性的 LDPC 码包括：基于有限几何[7]、基于有限循环群[8,9]、利用组合数学的不完全分组[10~12]、Steiner[13]和 ZHANG L[14]等设计的 LDPC 码。这些用数学方法构造的结构化 LDPC 码由于存在结构参数相互匹

收稿日期：2012-07-27；**修回日期**：2013-01-29
基金项目：国家自然科学基金资助项目（61071069）
Foundation Item: The National Natural Science Foundation of China (61071069)

配的局限性，以及性能不如随机码好，目前均未成为工业标准中被实际采纳的纠错码类。

LDPC 码定义为稀疏奇偶校验矩阵 $\boldsymbol{H}$ 的零空间，即 $\boldsymbol{H}\boldsymbol{c}^{\mathrm{T}}=\boldsymbol{0}$，其中，$\boldsymbol{c}$ 是码字序列，$\boldsymbol{H},\boldsymbol{c}\in GF(2)$，T 表示矩阵或矢量的转置运算。由定义可知：稀疏 $\boldsymbol{H}$ 矩阵可以是任意结构的，显然寻找性能优良的稀疏 $\boldsymbol{H}$ 矩阵是一个多解问题。最容易想到的构造 $\boldsymbol{H}$ 矩阵的方法是计算机随机搜索的方法[2]，纠错码领域普遍认为：随机码通常是好码[15]，但结构化的码通常有利于提高编解码器的执行速度和降低芯片面积，综合二者考虑，本文提出半随机半代数结构的设计方法。基本思路是构造一个能等效表示 $\boldsymbol{H}$ 矩阵的紧凑的框架阵列，该框架阵列受到多个结构参数相互匹配的约束，要求在结构参数满足特定约束条件的情况下，使框架阵列中的元素分布由计算机优化搜索得到；一旦框架结构确定，就能利用框架中的元素准确地计算 $\boldsymbol{H}$ 矩阵中 1 元素的位置坐标。由于采用了框架约束，有可能出现性能好的 LDPC 码不在框架约束范围内的情况，因此，可以说这种半随机半代数结构的设计方法通常为次优方法。

从实用的角度考虑，首先奇偶校验矩阵应具有系统结构，即 $\boldsymbol{H}=[\boldsymbol{H}^d \quad \boldsymbol{H}^p]$，其中，$\boldsymbol{H}^d$ 是信息位对应的奇偶校验矩阵，$\boldsymbol{H}^p$ 是校验位对应的奇偶校验矩阵。其次，$\boldsymbol{H}$ 矩阵应该具有线性编码方案[16]，目前，具有线性编码方案的 LDPC 码有 2 种，一种是多个 IEEE 802 标准所采纳的 QC-LDPC 码[5,6]，其 $\boldsymbol{H}^p$ 矩阵具有近似下三角阵列矩阵的结构特征，$\boldsymbol{H}^d$ 矩阵是由单位矩阵形成的循环移位置换子矩阵所排成的阵列构成，子矩阵的排列位置和循环移位值由计算机优化搜索得到；另一种是 DVB-S2 标准所采纳的 IRA-LDPC 码结构，其 $\boldsymbol{H}^p$ 矩阵具有典型的双对角线结构特征，$\boldsymbol{H}^d$ 矩阵是计算机搜索的随机结构。本文以具有双对角线结构特征的 IRA-LDPC 码为原型，提出 $M\times K$ 维 $\boldsymbol{H}^d$ 矩阵可以用半随机半代数结构的框架阵列表示的设计方法。

不规则重复积累（IRA）码[17]由 Hui J 在其博士论文中提出，它是一类 $\boldsymbol{H}^p$ 矩阵具有双对角线结构特征的 LDPC 码，本文将其称为 IRA-LDPC 码。$\boldsymbol{H}^d$ 矩阵中 1 元素的分布由参数 $(f_1,\cdots,f_\psi,u)$ 确定，其中，$f_\psi\geqslant 0$ 表示 $\boldsymbol{H}^d$ 矩阵中列重量为 ψ 的列在 K 列中所占的比例，且有 $\sum f_\psi=1$；u 是正整数，表示行重量的值，即 $\boldsymbol{H}^d$ 矩阵是等行重量的。由此可知，一共有 $K\sum_{\psi=1}^{v}\psi f_\psi$ 个 1 元素在 $\boldsymbol{H}^d$ 矩阵中随机分布，随着码长增加（相应的 K 增加），在 $\boldsymbol{H}^d$ 矩阵中寻找性能优良的 1 元素的随机分布将是十分困难的。另一方面，关于 IRA-LDPC 码 $\boldsymbol{H}^d$ 矩阵的完全代数结构设计，公开发表的研究论文较少。为此，本文提出用半随机半代数结构的等效阵列来表征 $\boldsymbol{H}^d$ 矩阵的设计是有理论和实用价值的，它将搜索 $\boldsymbol{H}$ 矩阵中所有 1 元素的最优分布的复杂问题简化为搜索框架阵列中元素的次优分布问题，使 $\boldsymbol{H}$ 矩阵的搜索范围和计算量有很大程度的降低，同时又保留了随机性所带来的性能优良的优点，很显然本文提出的 LDPC 码构造方法是一种性能与复杂度折中的方案。

2 数学基础和新概念定义

同余[18]：设 2 个整数 a_1 和 a_2 被同一个正整数 n 除时，有相同的余数 r，即 $a_1=q_1n+r$，$a_2=q_2n+r$，$0\leqslant r<n$，则称 a_1、a_2 关于模 n 同余，并有 $a_1\equiv a_2(\mathrm{mod}\,n)$。

剩余类[18]：由同余概念可对全体整数进行分类，把余数相同的归为一类。即由表达式 $a=qn+r$ 可将余数同为 r 的整数进行分类，每一类构成一个集合 $\overline{r}=\{a\,|\,a=r(\mathrm{mod}\,n)\}$。所有整数可划分为 n 个这样的集合，也称为 n 个剩余类。显然，任意整数必属于 n 个剩余类中的一个。

定义 1 剩余类数对：从表达式 $a=qn+r$ 中提取 2 个正整数 r 和 q，构成数偶对 $(r \quad q)_n$，称为关于模 n 的剩余类数对。数对 $(r \quad q)_n$ 通过 $a=qn+r$ 映射成 a，表示以模 n 划分剩余类，在剩余类 $\overline{r}$ 中的第 q 个元素的值是 a。

例如，设模数 $n=5$，$(r \quad q)_n=(2 \quad 3)_5$ 表示剩余类 $\overline{r}=\overline{2}$ 中的第 3 个元素为 $a=17=3\times5+2$，又如，$(r \quad q)_n=(3 \quad 0)_5$ 表示剩余类 $\overline{r}=\overline{3}$ 中的第 0 个元素为 $a=3=0\times5+3$。

定义 2 剩余类数对阵列：设 $\boldsymbol{D}$ 表示一个 $m\times k$ 维的阵列，它由关于模 m 的剩余类数对 $(r \quad q)_m$ 或空集($\varnothing$) 2 种元素构成，为不产生歧义，以下将关于模 m 的剩余类数对 $(r \quad q)_m$ 简称剩余类数对 $(r \quad q)$。$\boldsymbol{D}$ 阵列中规定每行放置数量相等的 u 个剩余类数对，每列的剩余类数对数量可不等，分别为 $v_0,v_1,\cdots,v_{k-1}$。因此，在阵列 $\boldsymbol{D}$ 中，剩余类数对的总

数为 $m\times u=\sum_{\delta=0}^{k-1}v_\delta$ 个。

循环群[18]：由一个单独元素的一切幂次所构成的群称为循环群，该元素称为循环群的生成元。若群中元素个数有限称之为有限循环群，反之则称无限循环群。设 g 为有限域 $GF(n)$ 的某个生成元，则有限域 $GF(n)$ 中除 0 之外的所有元素都包含在由 g 生成的有限循环群 $\{g^0=1,g^1,g^2,\cdots,g^{n-1}\}$ 中。

3　基于剩余类数对阵列的 IRA-LDPC 码结构设计

设 $\boldsymbol{H}$ 表示 IRA-LDPC 码的稀疏奇偶校验矩阵，维数为 $M\times N$，可分解为 $\boldsymbol{H}=[\boldsymbol{H}^d\quad \boldsymbol{H}^p]$ 的系统形式，其中，$\boldsymbol{H}^p$ 是校验位对应的 $M\times M$ 维矩阵，具有双对角线结构；$\boldsymbol{H}^d$ 是信息位对应的 $M\times K$ 维矩阵，本文的主要任务是设计 $\boldsymbol{H}^d$ 矩阵，也就是确定 1 元素在 $\boldsymbol{H}^d$ 矩阵中的位置分布和数量。基本方法是将 $\boldsymbol{H}^d$ 矩阵的结构设计转换为类似于剩余类数对阵列 $\boldsymbol{D}$ 的结构设计。为此，需要引入几个结构参数，并对从 $\boldsymbol{H}^d$ 矩阵到剩余类数对阵列 $\boldsymbol{D}$ 的映射做下列规定。

结构 1　$\boldsymbol{H}^d$ 矩阵的紧凑表示形式——剩余类数对阵列 $\boldsymbol{D}_H$

1) 将 $\boldsymbol{H}^d$ 矩阵按列分解成 k 个子矩阵，即 $\boldsymbol{H}^d=[\boldsymbol{H}_0^d,\cdots,\boldsymbol{H}_\delta^d,\cdots,\boldsymbol{H}_{k-1}^d]$，$\delta=0,1,\cdots,k-1$，每个子矩阵包含 L 列，其中，$K=kL$。

2) 从每个子矩阵 $\boldsymbol{H}_0^d,\cdots,\boldsymbol{H}_\delta^d,\cdots,\boldsymbol{H}_{k-1}^d$ 中抽取第一列 $\boldsymbol{h}_0,\cdots,\boldsymbol{h}_\delta,\cdots,\boldsymbol{h}_{k-1}$，形成一个新矩阵 $\boldsymbol{H}_e=[\boldsymbol{h}_0,\cdots,\boldsymbol{h}_\delta,\cdots,\boldsymbol{h}_{k-1}]$，称为 $\boldsymbol{H}^d$ 的第一列抽取矩阵，或简称为抽取矩阵。规定列矢量 $\boldsymbol{h}_0,\cdots,\boldsymbol{h}_\delta,\cdots,\boldsymbol{h}_{k-1}$ 的重量分别为 $v_0,\cdots,v_\delta,\cdots,v_{k-1}$。每个列矢量 $\boldsymbol{h}_0,\cdots,\boldsymbol{h}_\delta,\cdots,\boldsymbol{h}_{k-1}$ 分别循环下移 m bit，得到各子矩阵 $\boldsymbol{H}_0^d,\cdots,\boldsymbol{H}_\delta^d,\cdots,\boldsymbol{H}_{k-1}^d$ 的第二列，一直操作下去，直到第 $L-1$ 列循环下移 m bit，得到第 L 列。由此，将抽取矩阵 $\boldsymbol{H}_e$ 还原成 $\boldsymbol{H}^d$ 矩阵，其中，$M=mL$。

3) 将抽取矩阵 $\boldsymbol{H}_e$ 中的 1 元素用剩余类数对取代，0 元素用空集($\varnothing$)取代，即构成 $\boldsymbol{H}^d$ 矩阵的紧凑的等效表示形式——剩余类数对阵列 $\boldsymbol{D}_H$。

$$\boldsymbol{D}_H=\begin{bmatrix}(r_{0,0}\ \ q_{0,0}) & (r_{0,1}\ \ q_{0,1}) & \cdots & (r_{0,\delta}\ \ q_{0,\delta}) & \cdots & (r_{0,k-1}\ \ q_{0,k-1})\\ (r_{1,0}\ \ q_{1,0}) & (r_{1,1}\ \ q_{1,1}) & \cdots & (r_{1,\delta}\ \ q_{1,\delta}) & \cdots & (r_{1,k-1}\ \ q_{1,k-1})\\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots\\ (r_{\theta,0}\ \ q_{\theta,0}) & (r_{\theta,1}\ \ q_{\theta,1}) & \cdots & (r_{\theta,\delta}\ \ q_{\theta,\delta}) & \cdots & (r_{\theta,k-1}\ \ q_{\theta,k-1})\\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots\\ (r_{m-1,0}\ \ q_{m-1,0}) & (r_{m-1,1}\ \ q_{m-1,1}) & \cdots & (r_{m-1,\delta}\ \ q_{m-1,\delta}) & \cdots & (r_{m-1,k-1}\ \ q_{m-1,k-1})\end{bmatrix}\overset{probable}{=\!=}\begin{bmatrix}\ddots & \cdots & & & \cdots & \iddots\\ \vdots & \varnothing & & \vdots & \varnothing & \vdots\\ & \cdots & (r_{\psi,\gamma}\ \ q_{\psi,\gamma}) & \cdots & & \\ \vdots & \varnothing & & \vdots & \varnothing & \vdots\\ \iddots & \cdots & & & \cdots & \ddots\end{bmatrix}\tag{1}$$

其中，对 $\theta=0,1,\cdots,m-1$ 和 $\delta=0,1,\cdots,k-1$，有 $(r_{\theta,\delta}\ \ q_{\theta,\delta})\in\{\varnothing\}\cup\{(r_{\psi,\gamma}\ \ q_{\psi,\gamma})\,|\,\psi=0,1,\cdots,v_\delta-1,\ \gamma=0,\ 1,\cdots,u-1\}$。

1) 规定 $m+1$ 是素数，$L(=K/k=M/m)$ 是 K 和 M 的公因数。如果 $\boldsymbol{D}_H$ 存在，那么 $\boldsymbol{D}_H$ 中每行剩余类数对的数量相等，意味着 $\boldsymbol{H}^d$ 矩阵有等行重量 u；$\boldsymbol{D}_H$ 中每列剩余类数对的数量为 v_δ，$\delta=0,1,\cdots,k-1$，相当于 $\boldsymbol{H}^d$ 矩阵的每个子矩阵 $\boldsymbol{H}_0^d,\cdots,\boldsymbol{H}_\delta^d,\cdots,\boldsymbol{H}_{k-1}^d$ 有相等的列重量 v_δ。$\boldsymbol{D}_H$ 中有 $m\times u=\sum_{\delta=0}^{k-1}v_\delta$ 个剩余类数对，$\boldsymbol{H}^d$ 矩阵中有 $L\cdot m\cdot u=L\cdot\sum_{\delta=0}^{k-1}v_\delta$ 个 1 元素。

关于结构 1 的几点讨论。

1) 由结构 1 构造出的 $\boldsymbol{H}=[\boldsymbol{H}^d\quad \boldsymbol{H}^p]$ 矩阵所定义的 LDPC 码被称为基于剩余类数对的 IRA-LDPC 码，它的码率为 $R=K/N=k/(k+m)$。为了简化结构，可以规定一种特殊情况，即 $\boldsymbol{H}^d$ 矩阵只有 2 种列重量 $v_{\min}=3$ 和 $3<v_{\max}<m$。根据结构 1 中所规定的参数匹配关系，可以推知 $\boldsymbol{H}=[\boldsymbol{H}^d\quad \boldsymbol{H}^p]$ 矩阵的校验节点和变量节点所对应的度分布对分别为 $\rho=\frac{1}{M}x^u+\frac{M-1}{M}x^{u+1}$，$\lambda=\frac{1}{N}+\frac{M-1}{N}x+\frac{\varepsilon K}{N}x^2+\frac{(1-\varepsilon)K}{N}x^{v_{\max}-1}$，其中，$0<\varepsilon<1$ 表示重量为 3 的列在 K 列中所占的比例。显然，当 M 和 K 参数确定后，码长和码率也就确定了。在 M、K 和 $\boldsymbol{D}_H$ 阵列的约束条件下，可利用密度进化算法[19]搜索最优的度分布对，也就是搜索在阈值最优情况下的参数 u、$v_{\max}$ 和 ε。可以看出，基于密度进化算法的最优度分布对只给出了列重量和行重量的分布，解决了优化码的存在问题；但没有给出 1 元素在 $\boldsymbol{H}^d$ 矩阵中的具体位置分布。因此，对实用 LDPC 码来说，利用密度进化算法搜索最优度分布对存在局限性，即不能给出确定结构的 $\boldsymbol{H}$ (或 $\boldsymbol{H}^d$)矩阵。如果采用逐

渐减小信噪比，使误码率尽可能小的优化搜索方法，搜索满足结构参数的 $\boldsymbol{D}_H$ 阵列，不仅可以确定参数值 u、$v_{\max}$ 和 ε，还可以得到所有 1 元素在 $\boldsymbol{H}^d$ 矩阵中的位置分布，本文第 5 节描述了这种搜索方法。

2) 解释结构 1 中的下标索引：$\psi=0,1,\cdots,v_\delta-1$ 是阵列 $\boldsymbol{D}_H$ 中每一列剩余类数对的数量索引，也是 $\boldsymbol{H}^d$ 矩阵的子矩阵 $\boldsymbol{H}_0^d,\cdots,\boldsymbol{H}_\delta^d,\cdots,\boldsymbol{H}_{k-1}^d$ 的列重量索引，每个子矩阵的列重量相等；$\gamma=0,1,\cdots,u-1$ 是阵列 $\boldsymbol{D}_H$ 中每一行剩余类数对的数量索引，也是 $\boldsymbol{H}^d$ 矩阵的行重量索引，阵列 $\boldsymbol{D}_H$ 的每一行有相同数量的剩余类数对，$\boldsymbol{H}^d$ 是等行重量的；$\theta=0,1,\cdots,m-1$ 是 $\boldsymbol{D}_H$ 阵列的行索引；$\delta=0,1,\cdots,k-1$ 是 $\boldsymbol{D}_H$ 阵列的列索引，也是 $\boldsymbol{H}^d$ 矩阵的子矩阵的数量索引。数对 $(r_{\psi,\gamma}\quad q_{\psi,\gamma})$ 是准确的剩余类数对，但数对 $(r_{\theta,\delta}\quad q_{\theta,\delta})$ 不一定是剩余类数对，它也可能是空集 $\varnothing$。仅当索引 ψ 和索引 θ 指向同一个“1”元素的行位置，索引 γ 和索引 δ 指向这个“1”元素的列位置时，数对 $(r_{\theta,\delta}\quad q_{\theta,\delta})$ 才表示剩余类数对，即有 $(r_{\theta,\delta}\quad q_{\theta,\delta})=(r_{\psi,\gamma}\quad q_{\psi,\gamma})$。

3) 由于 $\boldsymbol{H}^d$ 矩阵可以用紧凑 $\boldsymbol{D}_H$ 阵列表示，使 $\boldsymbol{H}$ 矩阵的围线结构可以用代数的方法进行分析，主要考虑两方面的问题，其一是在 $\boldsymbol{H}^d$ 的任意一列中不能出现连续的 2 个 1 元素，以避免与双对角线结构 $\boldsymbol{H}^d$ 矩阵形成 4 围线；其二是在 $\boldsymbol{H}^d$ 矩阵内部不能出现 4 围线。由于篇幅所限，本文只限于讨论 $\boldsymbol{H}^d$ 矩阵的结构设计，关于 $\boldsymbol{H}=[\boldsymbol{H}^d\quad \boldsymbol{H}^p]$ 矩阵中围线的结构特征问题将专门撰文进行讨论。

4) 将 $\boldsymbol{H}^d$ 矩阵用紧凑的 $\boldsymbol{D}_H$ 阵列表示，带来的最直接好处是：如果 $\boldsymbol{D}_H$ 阵列存在，那么 $\boldsymbol{D}_H$ 阵列中的剩余类数对可以唯一地确定 $\boldsymbol{H}^d$ 矩阵中每个 1 元素的位置坐标。首先计算在抽取矩阵 $\boldsymbol{H}_e$ 中每个 1 元素所在列的行坐标，设 $a_{\psi,\delta}$ 表示 $\boldsymbol{D}_H$ 阵列中第 δ 列第 ψ 个剩余类数对所在行的位置值，也就是 $\boldsymbol{H}_e$ 矩阵中第 δ 列第 ψ 个 1 元素的行坐标，根据剩余类数对的定义，这个行坐标的值计算如下

$$a_{\psi,\delta}=r_{\psi,\delta}+m\cdot q_{\psi,\delta}\pmod M \tag{2}$$

由式(2)可计算出 $\boldsymbol{H}_e$ 矩阵中所有 1 元素的位置坐标。将 $\boldsymbol{H}_e$ 矩阵的每一列循环下移 m bit，进行 L 次操作，即可得到 $\boldsymbol{H}^d$ 矩阵。此外，式(2)也可以扩展到对整个 $\boldsymbol{H}^d$ 矩阵中的 1 元素的位置坐标进行计算，也就是 $\boldsymbol{H}^d$ 矩阵的第 δ 个子矩阵 $\boldsymbol{H}_\delta^d$ 的第 τ ($\tau=0,1,\cdots,L-1$)列第 ψ 个 1 元素的行坐标计算为

$$a_{\psi,\delta}^{\tau}=r_{\psi,\delta}+m\cdot q_{\psi,\delta}+m\tau\pmod M \tag{3}$$

由式(2)和式(3)可知，要确定 $\boldsymbol{H}_{\mathrm{e}}$ 和 $\boldsymbol{H}^d$ 矩阵中每个“1”元素的位置坐标，就需要知道数对 $(r_{\psi,\delta}\quad q_{\psi,\delta})$。当索引 δ 和索引 γ 指向同一个“1”元素的位置时，有 $(r_{\psi,\delta}\quad q_{\psi,\delta})=(r_{\psi,\gamma}\quad q_{\psi,\gamma})$。

剩下的问题是如何计算 $\boldsymbol{D}_H$ 阵列中每个剩余类数对 $(r_{\psi,\gamma}\quad q_{\psi,\gamma})$ 的 2 个元素 $r_{\psi,\gamma}$ 和 $q_{\psi,\gamma}$。

4 剩余类数对中元素的计算方法

本节讨论式(1)中剩余类数对 $(r_{\psi,\gamma}\quad q_{\psi,\gamma})$ 的两组元素 $r_{\psi,\gamma}$ 和 $q_{\psi,\gamma}$ 的设计方法，$\psi=0,1,\cdots,v_\delta-1$，$\gamma=0,1,\cdots,u-1$。

$r_{\psi,\gamma}$ 以剩余类数对第一个元素的形式分布在 $m\times k$ 的 $\boldsymbol{D}_H$ 阵列中。在 $\boldsymbol{D}_H$ 阵列中一共有 $m\times u$ 个剩余类数对，因此，需要设计 $m\times u$ 个 $r_{\psi,\gamma}$ 值。本文用有限循环群的生成元来设计 $r_{\psi,\gamma}$ 值。设 $m+1$ 是素数，在有限域 $G(m+1)$ 上，存在 $m+1$ 阶循环群。$m+1$ 阶循环群中有 $\varphi(m+1)=m$ 个生成元（其中，$\varphi(\cdot)$ 为欧拉函数），则从中选取 u 个生成元（$1\leqslant u\leqslant\varphi(m+1)$），用 $g_0,g_1,\cdots,g_{u-1}$ 表示，并有 $g_\gamma^{m+1}=1$。将 $\theta+1=1,2,\cdots,m$ 作为幂指数，作用于每个生成元 $g_0,g_1,\cdots,g_{u-1}$，可以得到每一个生成元 g_γ 的 m 个值。因此，每一个 $r_{\psi,\gamma}$ 的值计算如下

$$r_{\psi,\gamma}=r_{\theta,\gamma}=[(g_\gamma)^{\theta+1}-1]\pmod{(m+1)} \tag{4}$$

由式(4)可知，$r_{\psi,\gamma}$ 的取值范围为 $r_{\psi,\gamma}\in\{0,1,\cdots,m-1\}$，在 $\boldsymbol{D}_H$ 阵列中每一行的 $r_{\psi,\gamma}$ 值是相同的，即第一行的 u 个 $r_{\psi,\gamma}$ 取值均为 0，最后一行的 u 个 $r_{\psi,\gamma}$ 取值均为 $m-1$。对于 $\theta=0,1,\cdots,m-1$ 和 $\gamma=0,1,\cdots,u-1$，将式(4)计算出来的 $r_{\psi,\gamma}$ 值按 θ 行索引 γ 列索引的方式排列，得到如下的 $m\times u$ 个 $r_{\psi,\gamma}$ 值，用 $\left[r_{\psi,\gamma}\right]=\left[r_{\theta,\gamma}\right]_{m\times u}$ 表示，即

$$\left[r_{\psi,\gamma}\right]=\left[r_{\theta,\gamma}\right]_{m\times u}=\begin{bmatrix} g_0^1-1 & g_1^1-1 & \cdots & g_{u-1}^1-1\\ g_0^2-1 & g_1^2-1 & \cdots & g_{u-1}^2-1\\ \vdots & \vdots & \ddots & \vdots\\ g_0^m-1 & g_1^m-1 & \cdots & g_{u-1}^m-1 \end{bmatrix}\pmod{(m+1)} \tag{5}$$

注意，在 $\boldsymbol{D}_H$ 阵列中有 $m\times u$ 个剩余类数对 $(r_{\psi,\gamma}\quad q_{\psi,\gamma})$ 对应的 $m\times u$ 个 $r_{\psi,\gamma}$ 值，在式(5)中这 $m\times u$ 个 $r_{\psi,\gamma}$ 值是按 θ 行 γ 列布置，所以 $r_{\psi,\gamma}$ 和 $r_{\theta,\gamma}$ 是一一对应的。在式(5)的 $\left[r_{\theta,\gamma}\right]_{m\times u}$ 中，元素的特点是：对大于 m 的值，减 1 后取 $\mathrm{mod}(m+1)$，保证每个 $r_{\psi,\gamma}$ 值不超过 $m-1$。在式(5)的矩阵中，一共有 m 个不同的元素，每个元素在 $0,1,\cdots,m-1$ 中取值，$0,1,\cdots,m-1$ 中的每个值在 $\left[r_{\theta,\gamma}\right]_{m\times u}$ 中重复出现 u 次。生成式(5)中的 $\left[r_{\theta,\gamma}\right]_{m\times u}$ 矩阵的目的是为下面 $q_{\psi,\gamma}$ 的设计提供方便。

若剩余类数对的第一个元素 $r_{\psi,\gamma}$ 按式(4)计算，按式(5)排列，则该剩余类数对的 $m\times u$ 个 $\left[q_{\psi,\gamma}\right]=\left[q_{\theta,\gamma}\right]_{m\times u}$ 值中的每一个值 $q_{\psi,\gamma}=q_{\theta,\gamma}$，由下列递归表达式计算。

$$q_{\psi,\gamma}=q_{\theta,\gamma}=\begin{cases}[u+(r_{\theta,\gamma}+3)(r_{\theta,\gamma}+2)/2](\mathrm{mod}\,L),\\ \gamma=0,\theta=0,1,\cdots,m-1\\ [q_{\theta,\gamma-1}+\gamma+r_{\theta,\gamma}+3](\mathrm{mod}\,L),\\ \gamma=1,2,\cdots,u-1,\theta=0,1,\cdots,m-1\end{cases}\tag{6}$$

从式(5)中取出一个 $r_{\theta,\gamma}$ 值，就能由式(6)计算出一个 $q_{\theta,\gamma}$ 值。注意式(6)中第 1 个表达式的 u 值由第 5 节的优化搜索确定；第 2 个表达式有递归特征。

到此为止，完成了 $m\times u$ 个剩余类数对的设计。剩下的问题是：这 $m\times u$ 个剩余类数对在 $\boldsymbol{D}_H$ 阵列中如何排列，才能使本文设计的 $\boldsymbol{H}=[\boldsymbol{H}^d\quad\boldsymbol{H}^p]$ 矩阵所定义的 IRA-LDPC 码达到性能最优。第 5 节的优化搜索算法回答了这个问题。

5　剩余类数对阵列的最优搜索与数字仿真

首先根据结构 1 为 $\boldsymbol{H}^d$ 矩阵设计一个紧凑的 $\boldsymbol{D}_H$ 阵列表示框架；然后用计算机搜索结构参数相互匹配的所有 $\boldsymbol{D}_H$ 阵列，形成一个 $\boldsymbol{D}_H$ 阵列的集合；最后在有限的 $\boldsymbol{D}_H$ 阵列集合中搜索误码率—信噪比尽可能小的 $\boldsymbol{D}_H$ 阵列。

如果给定码长 $N=K+M$，码率 $R=K/N$，那么 $\boldsymbol{D}_H$ 阵列的各结构参数之间的匹配应满足下列条件：

1) L 是 K 和 M 的公因数，在 L 存在的条件下，$m+1$ 必须取素数，且 L、m、k 3 个参数满足 $L=K/k=M/m$。

2) 从有限域 $G(m+1)$ 上的所有 $\varphi(m)$ 个生成元 $g_0,g_1,\cdots$，中选取 u 个生成元 $g_0,g_1,\cdots,g_{u-1}$。

3) u 是 $\boldsymbol{D}_H$ 阵列中每行的剩余类数对的数量，也是 $\boldsymbol{H}^d$ 矩阵的行重量，要求 $\boldsymbol{H}^d$ 矩阵的行重量相等。

4) $\boldsymbol{D}_H$ 每列剩余类数对的数量有 2 种分布，或者说 $\boldsymbol{H}^d$ 矩阵的列重量有 2 种分布，即 $v_{\min}=3$ 和 $3<v_{\max}<m$。

5) K_1 表示列重量为 $v_{\min}=3$ 的列在 $\boldsymbol{H}^d$ 矩阵的 K 列中所占的列数，K_2 表示列重量为 $v_{\max}$ 的列在 $\boldsymbol{H}^d$ 矩阵的 K 列中所占的列数，则 $K_1+K_2=K$，且 $K_1v_{\min}+K_2v_{\max}=Mu$。

从上述对 $\boldsymbol{D}_H$ 阵列结构参数的要求可以看出，L、m、k、u、$v_{\max}$、K_1、K_2 和 $g_0,g_1,\cdots,g_{u-1}$ 均可取多种不同的值，所有这些参数按上述 5 个条件的不同变化而相互匹配，能形成 $\boldsymbol{D}_H$ 阵列的一个集合。于是优化搜索算法可以这样描述：在 $\boldsymbol{D}_H$ 阵列的集合之内，寻找信噪比尽可能低的最优 $\boldsymbol{D}_H$ 阵列，使误码率保持在 10^{-5} 以下。

根据上述搜索方法，采用 IEEE 802.16e 标准中的已知参数，即码率 $R=1/2$ 和 4 种码长 N=576、960、1 536、2 304，搜索到 4 个 $\boldsymbol{D}_H$ 阵列，表 1 给出了这 4 种基于剩余类数对的 IRA-LDPC 码的结构参数。采用 DVB-S2 标准中的已知参数，即码长 N=64 800 和码率为 R=1/4、1/3、2/5、1/2、3/5、2/3、3/4、4/5、5/6、8/9、9/10，搜索出 11 个 $\boldsymbol{D}_H$ 阵列，表 2 给出了这 11 种基于剩余类数对的 IRA-LDPC 码的结构参数（由于篇幅所限，这里省略了上述 15 个 $\boldsymbol{D}_H$ 阵列的结构演示，但这并不影响对本文半随机半结构化设计的理解）。按照表 1 的结构参数，图 1 给出了 2 种码结构的信噪比与误码率的性能仿真曲线。实际的仿真实验表明：与不同码长和不同码率的 IEEE 802.16e 标准中所采纳的 QC-LDPC 码的仿真性能（虚线）相比，本文提出的基于剩余类数对的 IRA-LDPC 码的仿真性能（实线）在 10^{-5} 误码率时均有 0.1~0.3 dB 的性能优势。限于篇幅，图 1 只给出了 1/2 码率 4 种码长(N=576、960、1 536、2 304)的性能比较曲线。根据表 2 提供的结构参数，图 2 和图 3 给出了 DVB-S2 标准中 IRA-LDPC 码与基于剩余类数对的 IRA-LDPC 码的误码率与信噪比的性能仿真曲线。从两幅图中可以看出，对于码长 N=64 800 和 11 个不同码率，在 10^{-5} 误码率时，本文提出的基于剩余类数对的 IRA-LDPC 码的性能（实线）略优于或相当于 DVB-S2 标准中的 LDPC

表 1 利用 IEEE 802.16e 标准中 LDPC 码的已知参数搜索相应的 IRA-LDPC 码的结构参数

IEEE 802.16e 标准中 LDPC 码的已知参数			基于剩余类数对的 IRA-LDPC 码在性能最优情况下搜索出来的结构参数						
N	R	$M=K$	$m=k$	L	u	K_1	$v_{\max}$	K_2	$g_0,g_1,\cdots,g_{u-1}$
576	1/2	288	16	18	5	144	7	144	3,5,6,7,10
960	1/2	480	16	30	5	240	7	240	3,5,6,7,10
1 536	1/2	768	16	48	5	576	11	192	3,5,6,7,10
2 304	1/2	1 152	16	72	6	576	9	576	3,5,6,7,10,11

表 2 利用 DVB-S2 标准中 LDPC 码的已知参数搜索相应的 IRA-LDPC 码的结构参数(N=64 800)

DVB-S2 标准中 LDPC 已知参数			基于剩余类数对的 IRA-LDPC 码在性能最优情况下搜索出来的结构参数						
R	K	M	$m\times k$	L	u	K_1	$v_{\max}$	K_2	$g_0,g_1,\cdots,g_{u-1}$
1/4	16 200	48 600	36×12	1 350	3	8 100	15	8 100	2,5,13
1/3	21 600	43 200	60×30	720	3	14 400	12	7 200	2,6,7
2/5	25 920	38 880	60×40	648	5	18 144	18	7 776	2,6,7,10,17
1/2	32 400	32 400	432×432	75	6	21 600	12	10 800	5,7,10,14,15,19
3/5	38 880	25 920	36×54	720	8	28 800	12	10 080	2,5,13,15,17,18,19,20
2/3	43 200	21 600	36×72	600	8	38 400	12	4 800	2,5,13,15,17,18,19,20
3/4	48 600	16 200	40×102	405	12	38 880	8	9 720	6,7,11,12,13,15,17,19,22,24,26,28
4/5	51 840	12 960	240×960	54	21	40 176	13	11 664	7,13,14,31,34,35,37,39,42,46,51,52,55,56,62,66,68,69,70,71
5/6	54 000	10 800	1 200×6 000	9	29	44 550	19	9 450	11,17,22,26,29,31,33,34,37,39,46,52,65,69,71,73,77,78,82,88,92,94,101,106,113,115,116,119,123
8/9	57 600	7 200	96×768	75	25	55 200	6	2 400	5,7,10,13,14,15,17,21,23,26,29,37,38,39,40,41,56,57,58,59,60,68,71,74,76
9/10	58 320	6 480	108×972	60	28	56 160	6	2 160	6,10,11,13,14,18,24,30,37,39,40,42,44,47,50,51,52,53,56,57,58,59,62,65,67,69,70,72

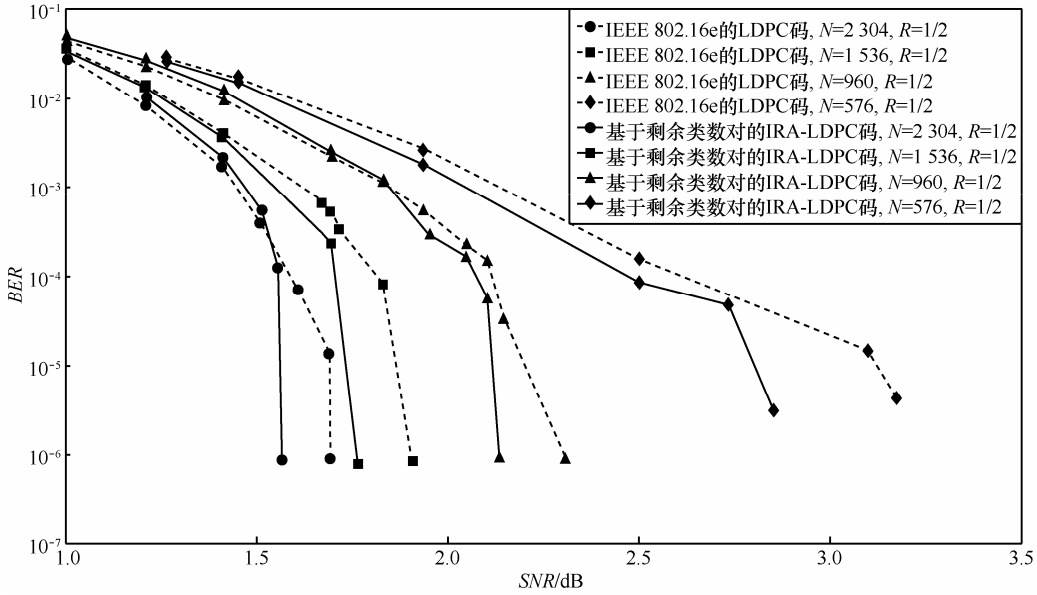

图 1 相同码率不同码长 IEEE 802.16e 中 LDPC 码与基于剩余类数对的 IRA-LDPC 码的性能比较

码的性能（虚线）。对于 N=16 200 码长和相应的 10 种码率也有同样的结论。

图 2 给出了码率不大于 1/2 的仿真情况，针对低率码，基于剩余类数对的 IRA-LDPC 码比 DVB-LDPC

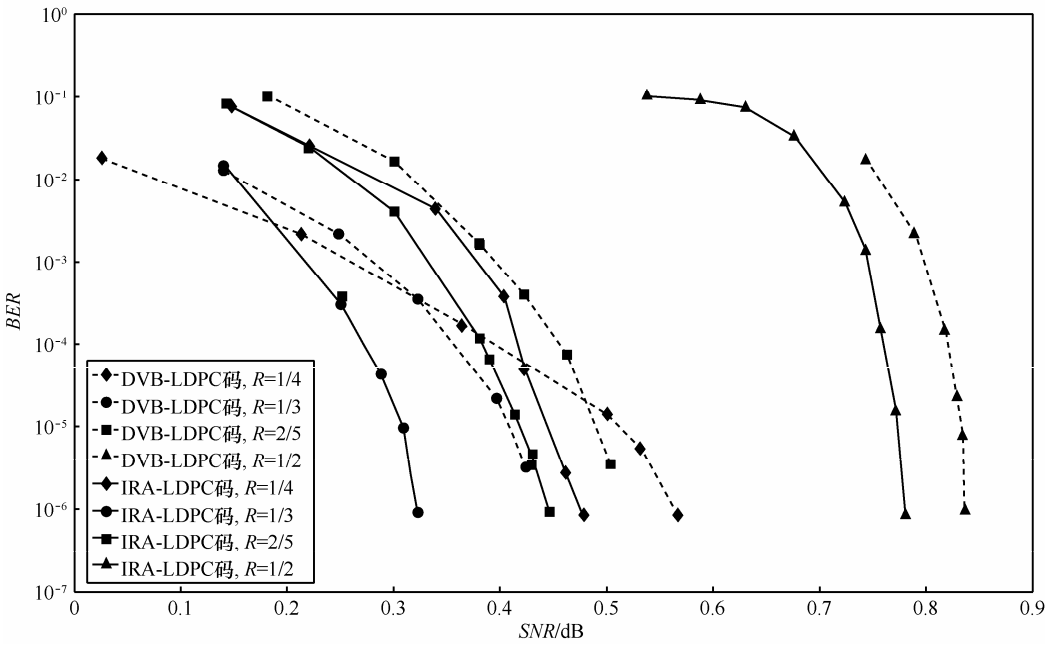

图 2　码率不大于 1/2 的 DVB-LDPC 码与剩余类数对 IRA-LDPC 码的性能比较

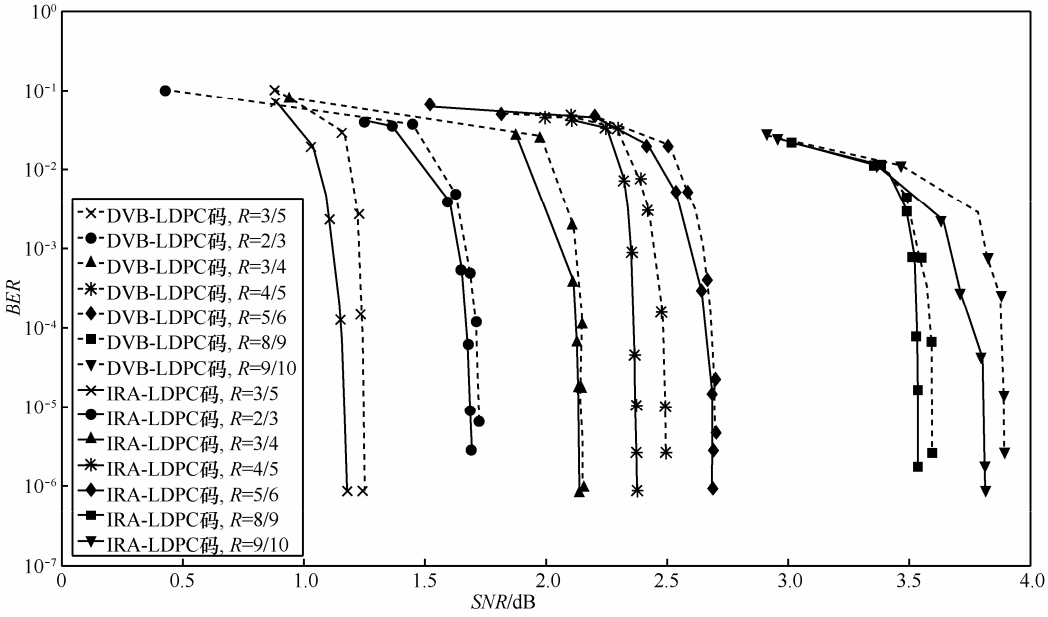

图 3　码率大于 1/2 的 DVB-LDPC 码与剩余类数对 IRA-LDPC 码的性能比较

码有大约 0.1 dB 的优势。对于 2 种结构，码率较低的 1/4 率（2 条星号表示的曲线）IRA-LDPC 码的性能不如码率较高的 1/3 率（2 条圆点表示的曲线）和 2/5 率（2 条方块表示的曲线）IRA-LDPC 码的性能。图 3 给出了码率大于 1/2 的情况，对某些码率，如 3/5、4/5、9/10 码率，在10^{-5} 误码率时，基于剩余类数对的 IRA-LDPC 码优于 DVB-LDPC 码大约 0.1 dB；对其余高率码，二者性能几乎相当。

总的来看，对低码率短码长的情况，本文提出的基于剩余类数对的 IRA-LDPC 码性能优势较多，对大码长高码率的情况，基于剩余类数对的 IRA-LDPC 码与标准中的 LDPC 码性能相当或略有优势。但基于剩余类数对的 IRA-LDPC 码还有其他优势，特别是 $\boldsymbol{H}^d$ 矩阵对存储空间的占用明显低于标准中的 LDPC 码。此外，还有结构清晰、软件搜索的计算复杂度低和具有结构化的框架等优点，其中，结构化框架的优点有利于降低编解码器的硬件描述复杂度，最终达到减小发射机和接收机系统芯

片面积的目的。

6 结束语

本文提出一种 IRA-LDPC 码的半随机半代数结构的构造方法，给出了 IRA-LDPC 码结构设计的一种新途径，使其在实用 LDPC 码的结构设计方面成为 QC-LDPC 码的竞争对手。与现有工业标准中所采纳的 LDPC 方案相比，本文所构造的基于剩余类数对的 IRA-LDPC 码具有较低的硬件实现复杂度、占用内存资源更少、性能更优等特点。本文提出的构造方法在 LDPC 的结构设计中给出了一种半随机半代数的框架结构新思路，它的未来发展还有许多工作需要进行。首先，剩余类数对阵列为 IRA-LDPC 码的围线（girth）构成提供了潜在的数学分析方法；其次，$\boldsymbol{H}^d$ 矩阵 1 元素的位置坐标可用表达式计算，有可能促成低描述复杂度编码器硬件电路的实现；最后，关于 IRA-LDPC 码低描述复杂度的解码器硬件电路和控制逻辑正在研究中。

参考文献：

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

[2] MACKAY D J C. Good error-correcting codes based on very sparse matrices[J]. IEEE Trans Info Theory, 1999, 45(3):399-431.

[3] MACKAY D J C, NEAL R M. Near Shannon limit performance of low-density parity-check codes[J]. Elect Lett, 1996, 32:1645-1646.

[4] Digital Video Broadcasting (DVB), European Standard (Telecommunications Series)[S].2005.

[5] Air Interface for Fixed and Mobile Broadband wireless Access Systems, IEEE Standard 802.16e[S]. 2006.

[6] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Pecifications: Amendment 4: Enhancements for Higher Throughputs, IEEE Standard 802.11n[S]. 2007.

[7] YU K. Finite Geometry Low Density Check Codes[D]. University of California, 2001.

[8] TANNER R M, SRIDHARA D, SRIDHARAN A, *et al*. LDPC block and convolutional codes based on circulant matrices[J]. IEEE Trans Info Theory, 2004, 50(10):2966-2984.

[9] ZHANG L, LIN S, ABDEL-GHAFFAR K, *et al*. Quasi-cyclic LDPC codes on cyclic subgroups of finite fields[J]. IEEE Trans Commun, 2011, 59(9): 2330-2336.

[10] TANG H, XU J, KOU Y, *et al*. On algebraic construction of gallager and circulant low-density parity-check codes[J]. IEEE Trans Info Theory, 2004, 50(6): 1269-1279.

[11] VASIS B, MILENKOVIC O. Combinatorial constructions of low-density parity-check codes for iterative decoding[J]. IEEE Trans Info Theory, 2004, 50(6): 1156-1172.

[12] AMMAR B, HONARY B, KOU Y, *et al*. Construction of low-density parity-check codes based on balanced incomplete block designs[J]. IEEE Trans Info Theory, 2004, 50(6): 1257-1268.

[13] FALSAFAIN H, ESMAEILI M. A new construction of structured binary regular LDPC codes based on steiner systems with parameter t>2[J]. IEEE Trans Commun, 2012, 60(1):74-80.

[14] ZHANG L, HUANG Q, LIN S, *et al*. Quasi-cyclic LDPC codes: an algebraic construction, rank analysis, and codes on latin squares[J]. IEEE Trans Commun, 2010, 58(11):3126-3139.

[15] COSTELLO D J, FORNEY G D. Channel coding: the road to channel capacity[J]. Proceedings of the IEEE, 2007, 95(6):1150-1177.

[16] RICHARDSON T, URBANKE R. Efficient encoding of low-density parity-check codes[J]. IEEE Trans Info Theory, 2001, 47(2): 638-656.

[17] HUI J. Analysis and Design of Turbo-like Codes[D]. Dissertation California Institute of Technology Pasadena, 2001.

[18] 王新梅, 肖国镇. 纠错码——原理与方法[M]. 西安: 西安电子科技大学出版社, 2001.
WANG X M, XIAO G Z. The Principle and Method Error Correcting Code[M]. Xi'an: Xidian University Press, 2001.

[19] RICHARDSON T J, SHOKROLLAHI A, URBANKE R. Design of capacity-approaching irregular low-density parity-check codes[J]. IEEE Trans Info Theory, 2001, 47(2): 619-637.

作者简介：

彭立（1968-），女，湖北武汉人，华中科技大学副教授，主要研究方向为信息论、信道编码、网络编码、无线传输技术。

张琦（1985-），男，湖北武汉人，华中科技大学硕士生，主要研究方向为纠错码、LDPC 码编码器的结构设计和 FPGA 的编解码器实现。

王渤（1988-），男，湖北咸宁人，华中科技大学硕士生，主要研究方向为纠错码、LDPC 码编码器的结构设计。

陈涛（1986-），男，湖北荆州人，华中科技大学硕士生，主要研究方向为纠错码、LDPC 码编解码器的 FPGA 实现。