第 22 卷第 4 期 系 统 仿 真 学 报© Vol. 22 No. 4
2010 年 4 月 Journal of System Simulation Apr., 2010

GF(2²)域上的LDPC码在深空通信中的应用研究

黎 勇[1,2]，王 琳[1]，魏琴芳[2]，徐位凯[1]
(1. 厦门大学通信工程系，厦门 361005；2. 重庆邮电大学编码技术研究所，重庆 400065)

摘 要：提出了一种**近似等效信道模型**，实现了 ***GF*(2²)域上的 *LDPC* 码在深空通信系统中的嵌入设计**。仿真结果表明：当数据帧长为 1784bits，bit error rate(*ber*)为 2×10^{-6}，采用 *FFT-BP* 译码算法，50 次迭代时，*GF*(2²)域上的 *LDPC* 码相比 *RS* 码与卷积码级联码具有 **4.8dB 的编码增益**；如果采用 *MAX-LOG-BP* 简化译码算法，10 次迭代时，前者仍然能获得约 3.8dB 的增益，且复杂度可以接受。

关键词：等效信道模型；深空通信；GF(22)域上的 LDPC 码；编码增益
中图分类号：TP391.9 **文献标识码：**A **文章编号：**1004-731X (2010) 04-0942-04

Applications of LDPC Codes on GF (2²) in Deep-space Communications

LI Yong[1,2], *WANG Lin*[1], *WEI Qin-fang*[2], *XU Wei-kai*[1]
(1. Dept. of Comm. Engineering, Xiamen University, Xiamen 361005, China;
2. Inst of Coding & Inform Tech., Chongqing Univ. of Posts &Telecomm., Chongqing 400065, China)

Abstract: *An approximate equivalent channel model* was proposed to realize the *design of LDPC codes on GF(2²) embedded in deep-space communication systems*. Simulation results show that an LDPC code on *GF*(2²) obtains *4.8 dB coding gain* compared with a serial concatenation of a RS code with a convolutional code using the FFT-BP decoding algorithm with 50 iterations, when data block size is 1784bits, ber $2*10^{-6}$. However, based on the MAX-LOG-BP simplified algorithm with 10 iterations, the former has also about 3.8 dB gain, and the complexity can be accepted.

Key words: equivalent channel model; deep-space communications; *LDPC* codes on *GF*(2²); coding gain

引 言

《中国的航天》白皮书确定了中国航天事业远期发展目标：充分发展空间技术，开发空间资源以满足国家安全以及经济建设的广泛需求，进一步增强综合国力[1]。这给我国深空通信事业的发展带来了空前的契机。

深空通信信道可视为功率受限而带宽丰裕信道，属于典型的以有效性换可靠性的传输信道。在深空通信中，由于传输距离很长，导致信号衰减非常严重，因而误码率很高。而纠错编码以牺牲一定的带宽利用率为代价，可以有效提高功率利用效率，从而提高系统的可靠性。因此，在目前的深空通信系统中，都无一例外的采用了纠错编码技术。传统的深空通信中采用 *RS* 码与卷积码的级联码作为纠错码方案。而随着 *Turbo* 码的发明[2]和 *LDPC* 码的重新兴起[3]，它们相对于 *RS* 码的巨大编码增益引起了深空通信领域研究者们的注意。

近年来，低密度奇偶校验码（*Low-Density Parity-Check* 码，简称 *LDPC* 码）[3,4]以其靠近香农限的性能及较低的译码复杂度迅速成为信道纠错编码领域的新热点。*LDPC* 码相比 *Turbo* 码具有更优异的性能，更低的译码复杂度。研究表明：在帧长为 10 的 7 次方及 *BER* 为 10 的-6 次方条件下，不规则 *LDPC* 码距香农限仅仅 0.04dB[5]，是迄今为止已知的离香农限最近的码型。同时，Davey 等发现，经过合理设计的 *GF*(*q*)上的 *LDPC* 码比二进制 *LDPC* 码具有更好的性能[6]。此外，本课题组发现 *GF*(*q*)上的 *LDPC* 码除了具有较好的纠随机错误能力外，还兼具优异的纠突发错误性能[7]。因此，本文把 *GF*(2²)上的 *LDPC* 码嵌入深空通信系统中，以期寻求到比现有的级联码更适合未来深空通信的纠错码方案。

文章结构安排如下：第二部分阐述 *GF*(*q*)上 *LDPC* 码的编译码原理；第三部分介绍 *GF*(*q*)上 *LDPC* 码嵌入深空通信系统的设计；第四部分给出仿真结果与分析；最后得到本文结论。

1 *GF*(*q*)上 LDPC 码的编译码原理

1.1 编码原理

多进制 *LDPC* 码的二部图类似于二进制 *LDPC* 码，只是变量节点有 *q* 种取值，并且校验节点的结构约束更复杂。本文中，首先生成二进制 *LDPC* 码校验矩阵，然后把校验矩阵中的 1 随机的用{1，2，……，*q*-1}中的元素替换。令 $q=2^p$，这样我们可以用 *p* 位二进制比特来传输一个 *q* 进制符号。编码方式与二进制 *LDPC* 码类似，只是现在所有运算遵循的是 *GF*(*q*)上的运算规则。*GF*(*q*)上的加法和乘法见[8]，例如 *GF*(2²)的加法乘法见表 1。

收稿日期：2008-08-06 **修回日期：**2008-11-14
基金项目：国家自然科学基金 (60972053)；教育部新世纪优秀人才支持计划项目 (NCET-04-0601)
作者简介：黎勇(1982-)，男，重庆人，博士生，研究方向为高效纠错编译码技术和迭代检测技术；**王琳**(1963-)，男，重庆人，教授，博导，研究方向为宽带无线数字通信。

表 1　$GF(2^2)$的加法和乘法

⊕	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

⊗	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

当 H 是一个大的稀疏矩阵时，我们通过高斯消去得到生成矩阵 G，进而生成码字。

1.2 译码原理

定义 $\boldsymbol{x}$ 的元素为噪声符号，$\boldsymbol{z}$ 的元素为校验符号。令 $N(m):=\{n: H_{mn}\neq 0\}$为参加校验 m 的噪声变量集合。译码的问题是寻找最可能的向量 $\boldsymbol{x}$ 满足 $H\boldsymbol{x}=\boldsymbol{z}$，$\boldsymbol{x}$ 的似然值取决于信道模型。令 $M(n):=\{m: H_{mn}\neq 0\}$为噪声变量 n 参与的校验集合。稀疏校验矩阵 H_{mn} 中的非零元素为 a，$a\in GF(q)$。我们用 q_{mn}^a 表示从除去校验 m 外其余校验得到的 $\boldsymbol{x}$ 的第 n 位取 a 的概率。r_{mn}^a 表示 $\boldsymbol{x}$ 的第 n 位为 a 时，校验 m 被满足的概率。其它变量点的分布由概率 $\{q_{mn'}^a := n'\in N(m)\setminus n, a\in GF(q)\}$ 得到。r_{mn}^a 的值为

$$r_{mn}^a=\sum_{\boldsymbol{x}:x_n}\delta\Big(\sum_{n'\in N(m)}H_{mn'}x_{n'}=z_m\Big)\prod_{j\in N(m)\setminus n}q_{m_j}^{x_j} \tag{1}$$

假如 *LDPC* 码采用经典的 *BP* 算法译码，其复杂度为 $o(q^2)$。而采用傅立叶变换译码可以降低译码的复杂性[9]。因为式(1)表示 q_{mj}^a 的卷积，求和可以用 q_{mj}^a 的傅立叶变换的乘积代替，$j\in N(m)\setminus n$，然后作一个傅立叶反变换。$GF(2)$上的函数 f 的傅立叶变换 F 为 $F^0=f^0+f^1$，$F^0=f^0-f^1$。在 $GF(2^p)$上的傅立叶变换可看做是 p 维空间上的一系列二进制变换，因此在 $GF(2^2)$上有：

$$\begin{aligned}F^0&=[f^0+f^1]+[f^2+f^3]\\F^1&=[f^0-f^1]+[f^2-f^3]\\F^2&=[f^0+f^1]-[f^2+f^3]\\F^3&=[f^0-f^1]-[f^2-f^3]\end{aligned} \tag{2}$$

同理可以得到傅立叶反变换，只是要除以 2^p。

令 $(Q_{mj}^0,\cdots,Q_{mj}^{q-1})$ 表示向量 $(q_{mj}^0,\cdots,q_{mj}^{q-1})$ 的傅立叶变换，现在 r_{mn}^a 是 $((\prod_{j\in N(m)\setminus n}Q_{mj}^0),\cdots,(\prod_{j\in N(m)\setminus n}Q_{mj}^{q-1}))$ 的傅立叶反变换的第 a 个分量。

详细的译码步骤如下：

A.初始化

令 q_{mn}^a 的初始值为 f_n^a，即根据信道模型得到的 $x_n=a$ 的似然值。

B.傅立叶变换(FT)

$$Q_{mn}^a=FT[q_{mn}^0,\cdots,q_{mn}^{q-1}] \tag{3}$$

C.傅立叶反变换(IFT) (更新 r_{mn}^a)

$$r_{mn}^a=IFT[(\prod_{j\in N(m)\setminus n}Q_{mn}^0),\cdots,(\prod_{j\in N(m)\setminus n}Q_{mn}^{q-1})] \tag{4}$$

D. 更新 q_{mn}^a

$$q_{mn}^a=\alpha_{mn}f_n^a\prod_{j\in M(n)\setminus m}r_{jn}^a \tag{5}$$

选取 α_{mn}^a 使 $\sum_{a=0}^{q-1}q_{mn}^a=1$。

E. 计算 q_n^a

$$q_n^a=\alpha_n f_n^a\prod_{j\in M(n)}r_{jn}^a \tag{6}$$

选取 α_n 使 $\sum_{a=0}^{q-1}q_n^a=1$。

令 $\hat{x}_n=\arg\max_a\ q_n^a$ (7)

如果 $H\hat{x}=z$，则表示已确定一个合法码字，译码终止。否则在(3)和(7)之间迭代译码。如果达到预设最大译码次数仍然没有找到合法的码字，则宣布译码失败。

2　GF(q)上LDPC码嵌入深空通信系统的设计

在目前深空通信系统中，采用的信道编码技术是 *RS* 码与卷积码的级联码方案。其中，*RS* 码采用 Berlekamp-Massey 硬判决译码，卷积码采用 Vitebi 硬判决译码。SPW4.8 上的深空通信链路如图 1 所示。它主要包括信源，外码编译码器，交织器，内码编译码器，上下采样滤波器和 TWT 放大管。滤波器的冲激响应如图 2 所示。因为在深空通信信道里面引入了上采样滤波器、TWT 放大管、下采样滤波器，译码器的先验概率不能再采用 *AWGN* 信道里的计算公式。我们首先来分析在深空通信中该如何实现概率译码。

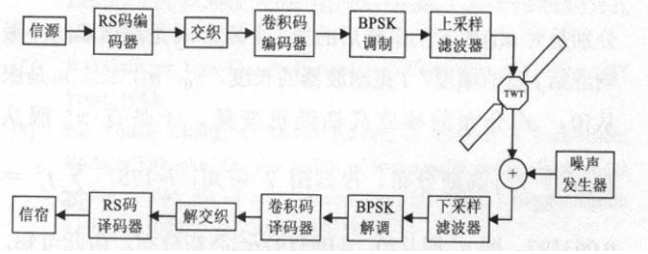

图 1　深空通信链路系统框图

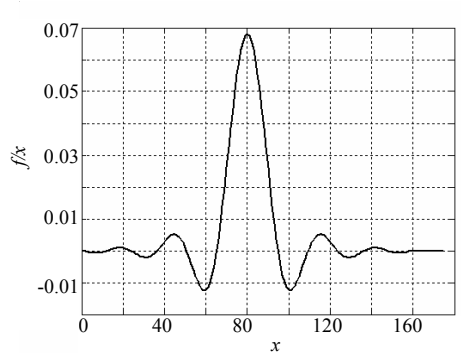

图 2　滤波器的冲激响应

信道等效处理：

A. 先对 TWT 模块进行简化

TWT 模块的输入输出满足等式：

$I\_out = I\_in\cdot A\cdot\cos\phi$。其中 I_in 是输入，I_out 是输出。

$$A=\frac{\alpha_r k}{1+\beta_r k^2|I\_in|}$$

$$\phi=\frac{\alpha_\varphi k^2|I\_in|}{1+\beta_\varphi k^2|I\_in|}-\frac{\alpha_\varphi k^2}{1+\beta_\varphi k^2}$$

这里，我们选取$\alpha_\varphi = 4.0033$, $\beta_\varphi = 9.1040$, $\alpha_r = 2.1587$, $\beta_r = 1.1517$[10], $k > 0$。

$$\because -\frac{\alpha_\varphi k^2}{1+\beta_\varphi k^2} < -\frac{\alpha_\varphi k^2}{\beta_\varphi k^2} = -\frac{\alpha_\varphi}{\beta_\varphi} < \phi < \frac{\alpha_\varphi k^2 |I\_in|}{\beta_\varphi k^2 |I\_in|} = \frac{\alpha_\varphi}{\beta_\varphi}$$

即 $-\frac{\alpha_\varphi}{\beta_\varphi} < \phi < \frac{\alpha_\varphi}{\beta_\varphi}$。则有 $\cos(\frac{\alpha_\varphi}{\beta_\varphi}) < \cos\phi < \cos(0)$。

又$\because \cos(\frac{\alpha_\varphi}{\beta_\varphi}) \approx 1$

$\therefore \cos\phi \approx 1$ 即 $I\_out = I\_in \cdot A$。又因为 $A = \frac{\alpha_r k}{1+\beta_r k^2 |I\_in|} > 0$

所以 TWT 模块可以认为仅仅起一个衰减幅度的作用。

B. 噪声等效

由于噪声通过下采样滤波器，进行的是线性变换。因此我们可将噪声等效到下采样滤波器输出端。通过发送训练序列发现：编码后的码字经过 *BPSK* 调制以后，再经过上采样滤波器，TWT，下采样滤波器，得到的输出相比 *BPSK* 调制后的输出仅仅在幅度上发生了衰减，而且这种衰减是缓变的，可以用一个衰减常量α来近似。采用均方值近似，求得α=0.645。高斯噪声过程为 $n(t)$，等效噪声记为 $n'(t)$。结合下采样滤波器的工作原理则有：$n'_i = \sum_{j=0}^{l} f_j \cdot n_j$。其中 n_i，n'_i 分别是对 $n(t)$和 $n'(t)$采样后的第 i 个元素，f_j是滤波器的冲激响应第 j 点的幅度，l 是滤波器的长度。n_0，n_1，…，n_l是服从[0，σ^2]分布的独立高斯随机变量。于是有 n'_i 服从 $[0, \sigma^2 \sum_{j=0}^{l} f_j^2]$ 高斯分布。根据图 2 可知，l=175，$\sum_{j=0}^{l} f_j^2 =$ 0.063197。即 n'_i服从[0，$0.063197\sigma^2$]高斯分布。由此可知，下采样滤波器起到了抑制噪声的作用。等效后的模型如图 3 所示。

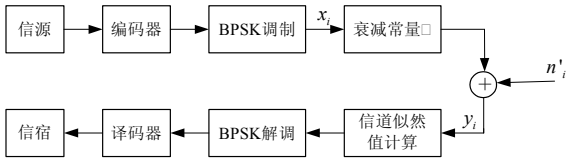

图 3 深空通信系统等效模型框图

现在信道数学模型就变得简单易处理了，信道的输入输出关系为

$y_i = \alpha x_i + n'_i$。

所以初始后验概率计算式为：

$$\frac{p(x_i = +1/y_i)}{p(x_i = -1/y_i)} = \exp(2*0.645*y_i / 0.063197\sigma^2)$$

这样，根据上述的等效模型，就可以实现 *LDPC* 码在深空通信系统中的概率译码。

3 仿真结果及分析

深空通信中采用的纠错码方案的一个工业标准是(255, 223)*RS* 码和(2,1,3)反馈系统卷积码（码长为 4080bits）的级联码（后文简记为 *SCRSCC* 码）。由于深空通信信道(自由空间段)是一种理想的信道，与 *AWGN* 信道非常相似。所以我们有必要先研究一下该级联码与 $GF(2^2)$上的 *LDPC* 码在 *AWGN* 信道下的性能差异。尽管仿真仅针对 $GF(2^2)$域，但相关算法很容易推广到 $GF(2^p)(p>2)$上[11]。文中 $GF(2^2)$上的 *LDPC* 码采用 *PEG* 算法[12]构造(后文简记为 *PQLDPC* 码)。

图 4 比较了基于 *FFT-BP* 译码算法，不同迭代次数的 *PQLDPC* 码和 *SCRSCC* 码在 *AWGN* 信道下的性能。由图可知：在 $ber = 10^{-5}$ 时，采用 30 或 50 次迭代，*PQLDPC* 码比 *SCRSCC* 码好约 4.3dB，即便只采用 10 次迭代，*PQLDPC* 码仍然能获得约 3.9dB 的增益。

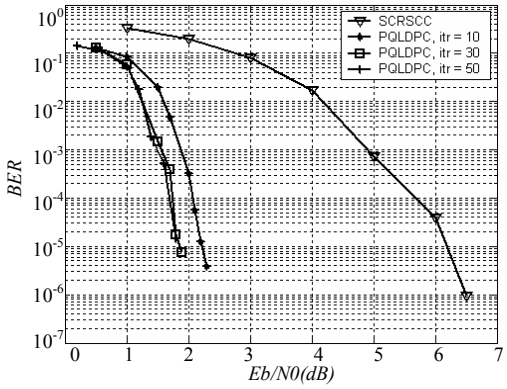

图 4 *PQLDPC* 与 *SCRSCC* 码在 *AWGN* 信道下的比较结果。码率为 0.43725。

图 5 比较了 *PQLDPC* 码与 *SCRSCC* 码在深空通信链路中的误比特率性能(迭代次数同上)。鉴于 *FFT-BP* 译码算法有较多的乘法运算，同时还研究了基于 *MAX-LOG-BP* 简化译码算法的 *PQLDPC* 码在深空通信链路中的性能。由图可知：在 $ber = 2\times10^{-6}$ 条件下，*PQLDPC* 码采用 *FFT-BP* 译码算法，50 次迭代时相比原系统的 *SCRSCC* 码约有 4.8dB 的编码增益，并且无论采用 *FFT-BP* 算法还是 *MAX-LOG-BP* 简化译码算法，30 次迭代和 50 次的性能均几乎完全一致。采用 *MAX-LOG-BP 算法*，10 次迭代时，*PQLDPC* 码仍然有 3.8dB 的增益，这为进一步实现译码性能和复杂度的平衡提供了参考。

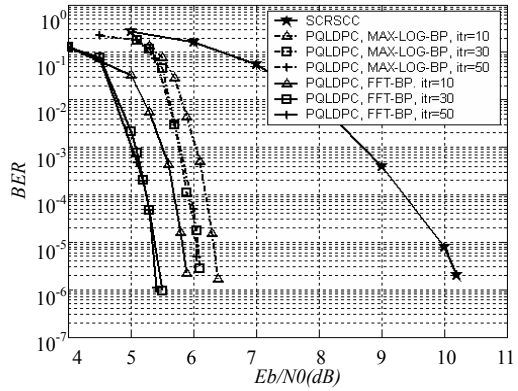

图 5 *PQLDPC* 码与 *SCRSCC* 码在深空通信链路中的比较结果。码率为 0.437255。

译码复杂度分析:

PQLDPC 码和 *SCRSCC* 码的译码复杂度（将 *RS* 码与卷积码分开列出）对比结果如表 2 所示。其中 n_l ,R_c ,w_c , w_r 分别表示 *PQLDPC* 码的码长，码率，列重和行重；n_{rs}, t 分别表示 *RS* 码的码长和能够纠正的错误个数；n_0，k_0，m 分别表示卷积码的码长，信息位长度和输入存储，编码器输入端的信息序列长度为 n_{cc}。

以文中仿真的 $GF(2^2)$上的规则（3，6）*PQLDPC* 码为例，*FFT-BP* 译码算法每次迭代共需 260160 次乘法、146930 次加法、6120 次比较和 55104 次查表；*MAX-LOG-BP* 算法每次迭代共需 817340 次加法、743900 次比较和 1363800 次查表（**注：本文是根据算法公式计算的运算次数，实际中通过合理的安排可以进一步降低复杂度，还可通过并行计算进一步加快运算速度**）；而采用传统的 *RS* 码与 *CC* 码的级联码，则需要有限域 $GF(2^8)$上的 13264 次乘法、9424 次加法，和实数域上的 32640 次加法和 16320 次比较。在有限域上，加法通过异或运算完成，一次乘法包含 3 次查表、一次实数加法、一次模运算。由于有限域阶数越高，其对应的乘法加法运算愈加复杂，因此，基于 *MAX-LOG-BP* 算法的 $GF(2^2)$上的 *PQLDPC* 码每次迭代所需的运算次数比传统级联码可比拟，但由于前者采用了迭代译码从而使得复杂度相比采用硬判决译码的传统级联码更高。

表 2　PQLDPC 码和 SCRSCC 码的译码复杂度比较

	运算量			
	乘法	加法	比较	查表
PQLDPC 码(FFT-BP)	$n_l w_c(w_c+2)q+(1-R_c)n_l(w_r-1)w_r q$	$2(1-R_c)n_l w_r q\log_2 q+2(q-1)\, n_l w_c$	$n_l(q-1)$	$2(1-R_c)n_l w_r q$
PQLDPC 码(MAX-LOG-BP)		$qn_l w_c^2+2(1-R_c)n_l w_r^2(q-1)^2$	$2(1-R_c)n_l w_r^2(q-1)^2$	$(1-R_c)n_l w_r^2(q-1)(4q-5)$
RS 码	$3\, n_{rs}t+4t^2$	$2\, n_{rs}t+5t^2-t$		
卷积码		$n_{cc}2^m 2^{k0}$	$n_{cc}2^m(2^{k0}-1)$	

注：对于 *RS* 码而言，其加法和乘法均是在有限域 $GF(2^p)$上进行的，对于本文中所用的（255，223）*RS* 码，$p=8$；而对于 *PQLDPC* 码和卷积码，加法和乘法都在实数域进行。

5　结论分析

本文提出了一种新的思路，通过发送训练序列和对噪声进行等效处理的方式实现了 $GF(2^2)$上的 *LDPC* 码在深空通信系统的嵌入设计和仿真分析。仿真结果表明：$GF(2^2)$上的规则（3，6）*PQLDPC* 码相比 *RS* 码与卷积码的级联码具有显著的优势：在数据帧长为 1784*bits*，$ber=2\times10^{-6}$ 条件下，基于 *FFT-BP* 译码算法，30 次迭代，其相较传统级联码可以获得 4.8dB 的增益，采用 *MAX-LOG-BP* 简化算法，10 次迭代时仍然能获得 3.8dB 的增益。并且，由于 *MAX-LOG-BP* 算法没有乘法运算，且只是在 $GF(2^2)$上进行查表运算，其算法复杂度虽依然较高，但硬件实现复杂度相对于传统级联码并不会高很多，相对于深空通信的重要战略价值，这样显著的编码增益付出相应的设备复杂度是值得的。后续我们将引入结构化校验矩阵设计方法，以及对 *MAX-LOG-BP* 简化译码算法进一步修正简化，从而在保持较优越性能前提下，继续降低 *LDPC* 码的编译码复杂度，为未来 *LDPC* 码最终应用到深空通信系统中奠定相关理论基础。

参考文献:

[1] 欧阳自远, 李春来, 邹永廖, 等. 深空探测的进展与我国深空探测的发展战略[J]. 中国航天, 2002, (12): 28-32.

[2] C Berrou, A Glavieux, P Thitimajshima. Near Shannon limit error-correcting coding and decoding: Turbo-codes (1) [C]// Proceedings of international communication conference (ICC1993). Geneva, Switzerland. USA: IEEE, 1993: 1064-1070.

[3] D J C MacKay, R M Neal. Near Shannon limit performance of Low-Density Parity-Check codes [J]. Electronics Letters (S0013-5194), 1997, 33(6): 457-458.

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

[5] Sae-Young Chung, G David Forney, Jr Thomas J Richardson, Rüdiger Urbanke. On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit [J]. IEEE Communication Letters (S1089-7798), 2001, 5(2): 58-60.

[6] M C Davey. Error-correction using Low- Density Parity-Check Codes [D]. UK: Univ. of Cambridge, 1999.

[7] Junbin Chen, Lin Wang, Yong Li. Performance Comparison between Non-binary LDPC Codes and Reed-Solomon Codes over Noise Burst Channels [C]// Proc. ICCCAS2005/IEEE, May 27-30, Hong Kong, China. USA: IEEE, 2005.

[8] 王新梅, 肖国镇. 纠错码——原理与方法 [M]. 修订版. 西安: 电子科技大学出版社, 2002.

[9] Hongxin Song, J R Cruz. Reduced- complexity Decoding of q-ary LDPC Codes for Magnetic Recording [J]. IEEE Trans. Magn. (S0018-9464), 2003, 39(3): 1081-1087.

[10] A A M Saleh. Frequency-Independent and Frequency-Dependent Nonlinear Models of TWT Amplifiers [J]. IEEE Trans. Comm. (S0090-6778), 1981, Com-29(11): 1715-1720.

[11] Yong Li, Lin Wang, Junbin Chen. The Design and Simulation of Q-ary LDPC Codes Based on the PEG Algorithm [C]// 14th IST Mobile and Wireless Communications Summit, 19-23rd, June, 2005, Dresden, Germany.

[12] X-Y Hu, E Eleftheriou, D M Arnold. Regular and Irregular Progressive Edge-Growth Tanner Graphs [J]. IEEE Trans. Inform. Theory (S0018-9448), 2005, 51(1): 386-398.