第 51 卷 第 1 期 2002 年 1 月
1000-3290/2002/51(01)/0015-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.51,No.1,January,2002

量子 Turbo 码*

张 权 唐朝京 高 峰

(国防科技大学电子科学与工程学院,长沙 410073)

(2001 年 1 月 16 日收到;2001 年 7 月 16 日收到修改稿)

量子纠错编码技术在量子通信和量子计算领域起着非常重要的作用.构造量子纠错编码的主要方法是借鉴经典纠错编码技术,目前几乎所有经典纠错编码方案都已经被移植到量子领域中来,然而在经典编码领域纠错性能最杰出的 Turbo 码却至今没有量子对应.提出了一种利用量子寄存器网络构造量子递归系统卷积码的简单实现方案,同时利用量子 SWAP 门设计了一种高效的量子交织器门组网络方案.最后仿照经典 Turbo 码的设计原理提出串行级联的量子 Turbo 码,同时提出了可行的译码方法.量子 Turbo 码不仅丰富了量子纠错码研究的领域,同时为解释经典 Turbo 码性能优势的原因提供了可能的解决途径.

关键词:量子递归系统卷积码,量子 Turbo 码,量子纠错编码,量子信息

PACC:0365,4230,4250

1 引 言

量子通信[1,2]和量子计算[3—6]理论的提出,为未来信息技术的深入发展开辟了一个全新的领域.为了真正实现量子信息的可靠传输与处理,必须保证量子状态经过一定的时空距离后保持不变或能够正确恢复.然而,由于量子系统不可避免地受到外界环境的干扰,以及量子操作本身的不精确性,必然导致量子状态发生错误.这已经成为量子信息领域的主要障碍之一.

受到经典纠错编码技术的启发,Shor 在 1994 年提出了一种用 9 量子位编码 1 位量子信息[7],从而可以纠正任一量子位发生错误的编码方案.Shor 的方法促进了量子纠错编码理论的产生与发展.通过借鉴经典纠错编码理论,人们提出了一系列量子纠错编码方案,并且逐渐形成了量子纠错编码的理论体系[8,9,13].从原理上讲,量子纠错编码是结合了量子力学原理的经典纠错编码在 Hilbert 空间上的扩展.

目前量子纠错编码技术研究的重点集中在两个方面,首先进一步扩展和完善量子纠错编码的一般理论,为量子纠错编码的实践提供理论依据;其次将各种经典纠错编码技术移植到量子系统中来,不断丰富和扩充量子纠错编码技术.本文提出与经典 Turbo 码技术相对应的量子 Turbo 码.我们首先利用 CNOT 网络来构造量子递归系统卷积码,并证明了该码的纠错能力,然后又提出了量子交织器设计方案,最后利用这些模块来构成量子 Turbo 码.

2 经典 Turbo 码简介

作为信道编码领域中一类非常出色的编码方案,Turbo 码是对以前各种纠错编码方案的巧妙综合与发展.它吸取了传统级联码的优点,利用交织减小各成员码的相关性,同时开创性地引进了迭代译码的思想,即利用各子译码模块产生的关于译码判决可信度的外赋信息,在各子译码模块间多次迭代,逐步提高译码精度.

2.1 并行级联的 Turbo 码

并行级联 Turbo 码(parallel concatenated convolutional codes, PCCC)的编译码器结构如图 1,图 2 所示.编码器由 2 个递归系统卷积码(recursive systematic convolutional codes, RSC)和 1 个交织器构成.d_k 在输入 RSC_2 之前经交织器 int 置乱,从而消除了 Y_{1k} 和 Y_{2k} 之间的相干性.交织器的存在确保了译码过程中,用于迭代反馈的外赋信息能被各子译码模

* 国家教育部骨干教师资助项目(Turbo 码关键技术及应用研究)资助的课题.

块反复利用.两个 RSC 的输出经过打孔(punching)处理后作为校验信息(Y_k)和信息元(X_k)一起送入信道.

在译码过程中,补零后的校验信息分别输入相应译码模块 DEC_i($i=1,2$),DEC_1 输出的外赋信息经交织后送入 DEC_2,而 DEC_2 输出的外赋信息解交织后又反馈到 DEC_1,经过多次迭代后 DEC_2 的译码输出经判决后得到译码结果 $\hat{d}_k$.在译码器中,两个译码模块均采用修正的 BCJR 算法,该算法是具有软输出的最优 MAP.

在 Berrou 等人的报告中,码率为 $R=1/2$,采用 256×256 的交织器,进行 18 次迭代译码,结果显示,当归一化信噪比 $\frac{E_b}{N_0}\geqslant0.7$dB 时,误比特率 $BER\leqslant10^{-5}$,此结果与 Shannon 的理论极限非常接近.

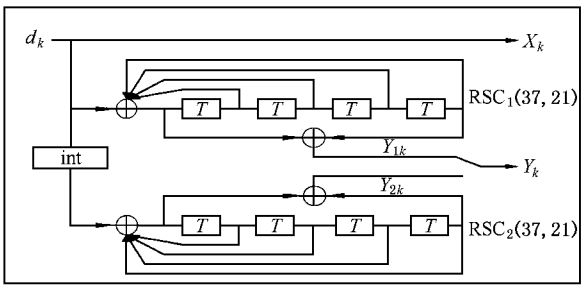

图 1 经典 Turbo 码编码器
(int 为交织器模块;RSC_i 为子码的编码模块)

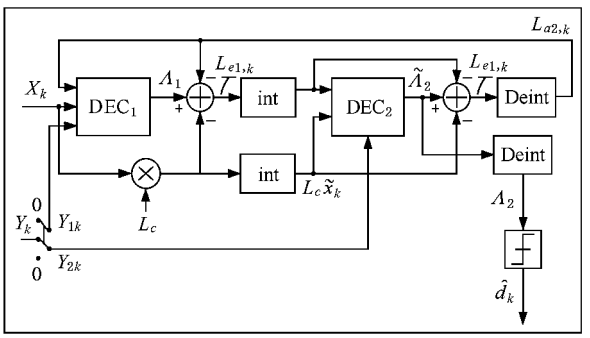

图 2 经典 Turbo 码译码器
(Deint 为解交织器;DEC_i 为子码的译码模块)

2.2 串行级联的 Turbo 码

串行级联的 Turbo 码同样采用两个 RSC 和一个交织器构成.信息元 d_k 输入 RSC_1 产生编码信息 X_{2k}和校验信息 Y_{2k},Y_{2k} 经打孔处理后与 X_{2k} 一起送入交织器,经交织后的信息又送入 RSC_2 进行编码,得到编码信息 X_{1k}和校验信息 Y_{1k},同样地,Y_{1k} 经打孔后与 X_{1k} 一起送入信道.译码器的构造与并行级联的情况相似,区别在于 DEC_1 的译码结果(而非外赋信息)直接输入 DEC_2,而 DEC_2 仍反馈外赋信息给 DEC_1.此外,对某些特定类型的纠缠态信号,由于可以实现几乎完美的量子克隆[10],有可能按照并行级联的方案实现量子 Turbo 码.

串行级联 Turbo 码在信噪比较高时($\frac{E_b}{N_0}\geqslant2$dB),比并行级联方案具有更加稳定的译码输出,即解决了译码结果的涨落问题,收敛速度也较快.当信噪比较小时,其性能要逊于并行方案,实验结果表明,当 $BER=10^{-5}$时,$\frac{E_b}{N_0}\geqslant1.5$dB,较并行级联的 Turbo 码损失了约 0.8dB 的编码增益.

3 串行级联量子 Turbo 码

在经典纠错编码领域,由 Berrou 等人提出的 Turbo 码技术以其优异的性能凌驾于所有其他编码方案[11].但是,由于量子不可克隆定理的限制,基于并行级联思想的 Turbo 码一直没有被移植到量子系统中来.其实在 Turbo 码设计中,串行级联的方案已经被证实具有和并行级联相似的信噪比性能[12],这启发我们仿照 Turbo 码的串行级联方案来构造一种串行级联的量子 Turbo 码.在该方案中,外码采用 $[[N_1,1,m_1]]$的量子卷积码,其输出经交织后送入内码,$[[N_2,1,m_2]]$,最后的编码输出为 $[[N_1N_2,1]]$.

为了构造量子 Turbo 码,首先需要设计量子递归系统卷积码(quantum recursive systematic convolutional codes,QRSC)和量子交织器(quantum interleaver, QI)等关键模块.QRSC 是量子卷积码(quantum convolutional codes,QCC)的一种,它采用递归编码的方式,增加码字的约束.目前关于 QCC 已经有文章论及[14,15],然而都只是给出编码的思路,本文则提出了用基本量子逻辑门来构造 QRSC 的实现方案.此外,我们还用基本的量子操作实现了 QI.

3.1 量子卷积码

在经典纠错编码中,卷积码以其较高的编码效率和快速高效的译码算法受到编码界的广泛重视.

受此启发,Chau 在 1997 年提出了量子卷积码的构造方案[14].他利用分组码(quantum block codes, QBC)来构造 QCC,然后又提出仿造经典卷积码构造 QCC 的方法.

利用 QBC 构造的 QCC 本质上是经过移位的 QBC,原理上和 QBC 相同,也没有充分利用量子系统的纠缠特性.而第二种方法则可以构造比较纯粹的 QCC.我们在 Chau 的方法上,结合量子移位寄存器(quantum shift register, QSR)来设计 QCC 编码器.

Berrou 所采用的 RSC 编码器的变换函数为

$$G(x) = \left[1, \frac{g_2(x)}{g_1(x)}\right], \tag{1}$$

当输入信息序列 $m(x)$,相应的编码输出为

$$c(x) = m(x)G(x) = \left[m(x), \frac{m(x)g_2(x)}{g_1(x)}\right], \tag{2}$$

可见,实现 QCC 的关键是找到计算 $\frac{m(x)g_2(x)}{g_1(x)}$ 的 QSR 网络.

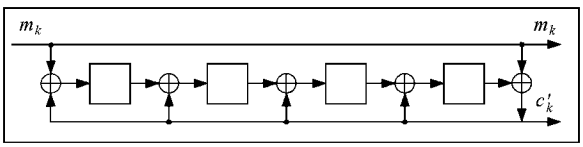

图 3　经典 $c(x) = m(x)\left[1, \frac{g_2(x)}{g_1(x)}\right]$ 运算电路

仍以 RSC(37,21)码为例,$g_2(x) = 1 + x^4$,$g_1(x) = 1 + x + x^2 + x^3 + x^4$,其经典运算电路如图 3 所示.仿此,可以用 CNOT 量子门构造相应的量子 RSC 编码器,如图 4 所示.

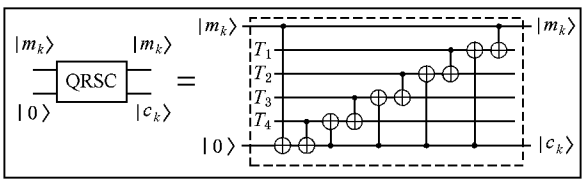

图 4　量子 RSC(37,21)编码器

对于连续的量子信息序列

$|m\rangle = |m_1, m_2, \cdots, m_i, \cdots\rangle$, $m_i \in \mathrm{GF}(2)$,先扩展为 $|m'\rangle = |m_1, 0, m_2, 0, \cdots, m_i, 0, \cdots\rangle$,再输入上述 QRSC 编码器,得到编码信息序列为 $|c\rangle = |m_1, c_1, m_2, c_2, \cdots, m_i, c_i, \cdots\rangle$.图中 $T_i(i = 1,2,3,4)$ 为量子寄存器,其初态为 $|0000\rangle$.

该编码器的运算过程可以用如下迭代式表示:

$$\begin{aligned} c_k &= m_k + T_{4,k-1}, \\ T_{4,k} &= c_k + T_{4,k-1} + T_{3,k-1}, \\ T_{3,k} &= c_k + T_{3,k-1} + T_{2,k-1}, \\ T_{2,k} &= c_k + T_{2,k-1} + T_{1,k-1}, \\ T_{1,k} &= c_k + T_{1,k-1} + m_k, \end{aligned} \tag{3}$$

其中加法都定义在 GF(2)上.由此可得

$$c_k = \sum_{i=0}^{3} m_{k-i} + T_{1,k-4}. \tag{4}$$

在译码过程中,可以认为 $T_{1,k-4}$ 的值已经在前期的译码阶段正确恢复,则对于连续的 4 个编码量子位 $m_k, c_k, m_{k+1}, c_{k+1}$,考虑 $\langle i_{\mathrm{enc}} | \varepsilon'^{\dagger}\varepsilon | i_{\mathrm{enc}}\rangle$ 对于错误 ε 和 ε',最不利的情况是发生在不同的量子位,因此

$$\begin{aligned} m_{2k} &= m'_{2k}, \\ \sum_{i=0}^{3} m_{2k-i} &= \sum_{i=0}^{3} m'_{2k-i}, \\ m_{2k+1} &= m'_{2k+1}, \\ \sum_{i=0}^{3} m_{2k+1-i} &= \sum_{i=0}^{3} m'_{2k+1-i} \end{aligned} \tag{5}$$

中至少有两个等式成立.

任取(5)式中两个,将 m' 视为常量,可求解得对 $\forall k, m_k = m'_k$,有

$$\langle i'_{\mathrm{enc}} | \varepsilon'^{\dagger}\varepsilon | i_{\mathrm{enc}}\rangle = \delta_{i',i}\delta_{\varepsilon',\varepsilon}.$$

根据文献[9]可知,该码可以纠正连续 4 个量子信息位中的 1 位比特型翻转错误.

为使编码器在完成一组信息编码后回到初始态,可以在码组的结束部分添加尾随序列 $|n_0\rangle$,使得 $g_1(x) | [x^{\deg n_0(x)+1}m(x) + n_0(x)]$.也可以在完成指定长度的信息编码后将 $T_i(i = 1,2,3,4)$ 强行置 0.这样,可以截断码组之间的纠缠,使译码误差不至于发散.

在本文中,QRSC 假设输入的量子信息位属于 GF(2),为了保证可操作性,通常制备量子信息时都使之处于系统的本征态,所以这一假设在多数情况下是合理的.本文的结论可以通过适当的修改[16]使之适用于一般的量子信息输入 $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

此外,我们的 QRSC 只考虑了量子翻转型错误(bit flipping),而位相错误(phase dumping)可以通过 Hadamard 变换转化为量子翻转错误,因此在实际编码中,可以仿照 Shor 的方法[6]进行扩展,从而实现纠正任何错误类型的 QRSC.

3.2　量子交织器

对于 K 位量子信息序列 $|m(x)\rangle = |\sum_{i=0}^{k-1} m_i x^i\rangle$,

定义伪随机的一一映射 $f_r: Z_k \to Z_k$，则交织后的序列为 $|m'(x)\rangle = \hat{f}_r |m(x)\rangle = |\sum_{i=0}^{k-1} m_i x^{f_r(i)}\rangle$，其中算子 $\hat{f}_r$ 由 f_r 定义，可以证明 $\hat{f}_r$ 是幺正的.

交织器的物理实现比较直接，利用量子置换(SWAP)操作可以实现两个量子位的交织，因此可以用若干个 SWAP 操作来构造量子交织器. 图 5 给出了实现 6 量子位 $\begin{pmatrix}1&2&3&4&5&6\\4&1&2&6&3&5\end{pmatrix}$ 交织的网络.

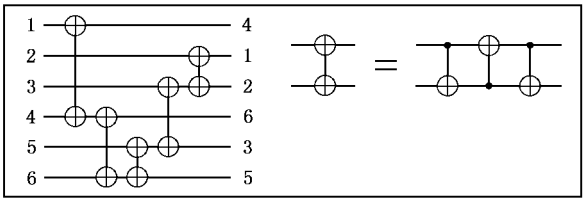

图 5 量子交织器

观察 SWAP 操作在交织器中的位置，发现与量子交织器的适当重排列 $\begin{pmatrix}1&4&6&5&3&2\\4&6&5&3&2&1\end{pmatrix}$ 相关. 因此可以证明，实现一个 $K(K\geqslant 2)$ 位量子交织器最多需要 $K-1$ 个量子 SWAP 操作.

3.3 量子卷积码概率译码算法

在经典卷积码最大概率译码算法中，关键任务是计算

$$\Lambda(d_k) = \log \frac{P_r(d_k = 1 \mid R_N)}{P_r(d_k = 0 \mid R_N)},$$

此方法要求掌握所有接收码字的信息. 在量子系统中，这存在一个明显的障碍：为了获得接收码字的全部信息需要对码字进行不可逆的测量，这会使系统发生态塌缩，从而彻底丢失编码信息. 因此只能采用间接测量的方法. 在二元对称信道中，最大后验概率等效于最小汉明距离. 量子编码的汉明距离可以用满足 $\langle \bar{i} | \varepsilon | \bar{j} \rangle \neq C\delta_{ij}$ (C 为常数)的 Pauli 算子 ε 的最小重量表示[1] 所以在译码过程中，首先计算 $k-1$ 时刻到 k 时刻所有可能的状态转换及其相应的编码输出，同时恢复各量子寄存器 $T_{1,2,3,4}$ 的状态. 比较各种可能的输出与接收码字间的差别可以得到各种可能的错样，这些错样对应于 Pauli 算子群代数中的算子，可以称为错样算子. 通常一种错样所对应的 Pauli 算子构成 Pauli 算子群的子群，因此错样算子在态空间中的表示是可约的. 又由于 Pauli 算子群是可交换的，因此错样算子的表示可以分解为不可约表示的直和. 每个不可约表示对应一种量子错误，其中具有最小维数的不可约表示称为最简不可约表示. 译码时，将最简不可约表示对应的错误作为译码的依据. 当一种错样具有两种以上相当的最简不可约表示时，任取其中之一作为结果. 对各种错样按照其相应最简不可约表示的维数和重数赋予不同的置信系数作为本级译码输出.

该方法是经典软判决 Viterbi 算法在量子系统中的对应，与 Chau 所提出的 QVA 算法[15] 相比，在两个方面作了改进：其一，将错样转化为 Pauli 算子群代数上的算子，利用 Pauli 群的表示论结构进行译码，提高了算法的可操作性；其二，对各种错样赋予不同概率作为译码的软输出，有利于实现软判决迭代译码. 因此我们将此算法称为软输出量子 Viterbi 算法(soft output quantum viterbi algorithm，SOQVA).

3.4 串行级联量子 Turbo 码编译码器

利用上述各种模块，可以非常方便地构造出串行级联的量子 Turbo 码(Serial concatenated quantum turbo coding，SCQTC)的编译码器. 在译码端，$\mathrm{SOQVA}_{1,2}$ 的量子寄存器初始状态均为 $|0000\rangle$. 设 SOQVA_1 接收到量子信息序列 $|\bar{i}'\rangle = |i'_0 i'_1 \cdots i'_5\rangle$. 首先，$\mathrm{SOQVA}_1$ 根据每种可能的输入及寄存器的状态计算寄存器状态变化和相应的输出估计 $|\bar{j}'\rangle = |j'_0 j'_1 \cdots j'_5\rangle$，比较 $|\bar{i}'\rangle$ 和 $|\bar{j}'\rangle$ 得到各种可能的错样，将最小错样所对应的译码估计 $|\bar{j}'\rangle = |j_0 j_1 \cdots j_5\rangle$ 用 QI^{-1} 解交织后

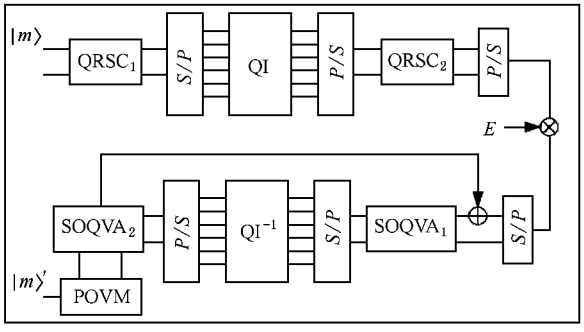

图 6 串行级联的量子 Turbo 码编译码器
(QRSC_i 为量子递归系统卷积码；SOQVA_i 为软输出量子 Viterbi 译码器；QI 为量子交织器；POVM 为广义测量)

[1] Pauli 算子 ε 的重量是指 ε 中非平凡 Pauli 矩阵($\sigma_x, \sigma_y, \sigma_z$)的个数.

输入 $SOQVA_2$ 进行相似的译码过程,同时 $SOQVA_2$ 需对各种可能的错样赋予加权系数后反馈给 $SOQVA_1$ 以调整译码估计 $|\bar{j}\rangle$.当满足联合的译码误差最小时,迭代结束.最后由 $SOQVA_2$ 对译码信息进行测量并输出译码结果 $|m\rangle'$.

4　讨　论

在引进量子 Turbo 码编译码设计方案的时候,我们采用了经典类比的方法,因此在形式上,我们的 SCQTC 与经典串行级联卷积码基本上相同,可以选用类似的成员码,相同的交织策略,结构几乎相同的编译码器等.这样可以利用经典 Turbo 码的设计方案非常方便构造量子 Turbo 码.然而,由于 SCQTC 受到量子约束以及量子系统所特有的物理性质,使得我们目前难以对 SCQTC 进行性能仿真,这也是目前大多数量子纠错编码技术研究的主要障碍.这并不影响 SCQTC 作为一种新颖的纠错编码技术,需要进一步深入研究.

目前关于经典 Turbo 码为什么具有如此出色的信噪比性能仍未在理论上得到解释,这在很大程度上是由于对迭代过程缺乏完善的形式化描述方法.而量子力学则具有非常严谨的形式体系,因此我们认为利用量子方法可以在分析经典 Turbo 码性能的道路上开辟一条新的思路,即利用量子力学语言来解释 Turbo 码出色性能的物理原因.信息和计算本质上都是物理的,量子信息理论作为量子理论和现代信息处理技术的交叉学科,更加充分地体现了上述特点.通信技术中的难题由掌握相当经典编码技术的物理学者来解决,这无论对量子信息还是传统通信理论,都是一件好事.总之,量子 Turbo 码不仅可以拓展量子纠错编码技术的研究领域,而且可能解决经典方法难以解决的编码理论难题.

[1] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895

[2] Bennett C H and Shor P W 1998 *IEEE Trans. Info.* **44** 2724

[3] Deutsch D 1985 *Proc. Roy. Soc. London Ser.* **400** 97

[4] Deutsch D 1989 *Proc. Roy. Soc. London Ser.* **A425** 73

[5] Grover L 1996 *Proc. 28th ACM Symp. Theo. Comp.* 212

[6] Shor P W 1994 *Proc. 35th IEEE Symp. Found. CS* 124

[7] Shor P W 1995 *Phys. Rev.* **A52** 2493

[8] Steane A M 1996 *Phys. Rev. Lett.* **77** 793

[9] Knill E and Laflamme R 1997 *Phys. Rev.* **A55** 900

[10] Gong S Q 2000 *Chin. Phys.* **9** 94

[11] Berrou C, Glavieux A and Thitimajshima P 1993 *Proc. ICC* '93 1064

[12] Berrou C and Galvieux A 1998 *IEEE Info. Theo. Soc. Newsletter* **48** 1

[13] Gottesman D 1996 *Phys. Rev.* **A54** 1862

[14] Chau H F 1997 *Phys. Rev.* **A56** 1

[15] Chau H F 1998 *Phys. Rev.* **A58** 905

[16] Shi M J *et al* 2000 *Acta Phys. Sin.* **49** 1912(in chinese)[石名俊等 2000 物理学报 **49** 1912]

Quantum Turbo codes*

Zhang Quan† Tang Chao-Jing†† Gao Feng

(*School of Electronic Science and Technology, National University of Deference Technology, Changsha* 410073, *China*)

(Received 16 January 2001; revised manuscript received 16 July 2001)

ABSTRACT

Quantum error correction coding technology is of great importance for quantum communication as well as quantum computation. Nearly all of the classical error correction coding schemes have, for the time being, been transplanted to the domain of quantum information; nevertheless, the most outstanding scheme in classical coding region, turbo code, still lacks the quantum analogy till now. We have completed a simple scheme of quantum recursive systematic convolutional code by means of quantum register network. At the same time, a kind of efficient quantum interweaver is constructed using only quantum SWAP gates. Also a serially concatenated quantum Turbo code is developed by analogy to the classical Turbo code. As limited by the quantum non – cloning theorem, the proposed quantum turbo code is serially concatenated. Quantum turbo code may not only extend the research area of quantum error correction coding technology, but also solve the puzzle in classical coding theory.

Keywords: qantum recursiue systematic codes, quantum turbo code, quantum error-correcting coding, quantum information

PACC: 0365, 4230, 4250

* Project supported in part by the state Education Ministry Funds for leading teachers (The key technology and application of Turbo codes).

†Email: mavea@cmmail.com

††Email: cjtang@nudt.edu.cn