低密度纠删码稳定收敛条件的证明

慕建君,贺玉成,王新梅
(西安电子科技大学综合业务网国家重点实验室,陕西西安 710071)

摘 要: 基于数学分析中著名的不动点原理,对于低密度纠删码本文证明了其删除错误译码算法稳定收敛的一充分条件.而且指出此条件优于现有的稳定收敛条件.最后对给定的度分布对证明了此译码算法能成功译码时可接受的最大损失 δ 的几个上界.

关键词: LDPC 码; 低密度纠删码; 删除错误译码算法; 稳定收敛条件
中图分类号: TN919.3 **文献标识码**: A **文章编号**: 0372-2112 (2002) 04-0530-03

A Proof of the Stability Condition for Low-Density Erasure Codes

MU Jian-jun, HE Yu-cheng, WANG Xin-mei
(National Key Lab. of ISN, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: Based on the known principle of fixed points in mathematical analysis, a sufficient convergence condition of erasure decoding algorithm for erasure codes is shown. Moreover, it is pointed out that this convergence condition is weaker than the convergence condition available. Finally, some upper bounds on the maximum tolerable loss fraction δ for which their decoding is successful are shown given a degree distribution pair.

Key words: LDPC code; low-density erasure code; erasure decoding algorithm; stability condition

1 引言

近几年来,低密度校验(Low-Density Parity Check, LDPC)码受到了人们的广泛关注[1-2].一方面,由于 LDPC 码的迭代译码算法具有低的译码复杂度[5,10];另一方面,LDPC 码可非常接近信道容量[12],这就使得 LDPC 码成为迄今为止性能最好的码.由于删除信道下 LDPC 码的分析容易些,而且这种深入分析是研究其它信道下 LDPC 码的前提.因此,本文只研究删除信道下的 LDPC 码,即低密度纠删码 (Low-Density Erasure Code),又称这种码为复损码(Loss-Resilient Code)[5].所采用的信道模型是删除信道 (Erasure Channel)[13],此信道中每个编码符号丢失的概率均为 p,且在传输中编码符号的丢失是相互独立的.把要传输的 k 比特的源数据编码为 n ($n > k$) 比特的数据后发送出去,若接收方接收到足够量的数据,则运用适当的译码方法就可恢复 k 个比特的源数据,称这种码为 (n, k) 纠删码 (Erasure Code)[4].文[2]和[5]设计了一些低密度纠删码,这些纠删码不仅能以任意接近删除信道信道容量的速率传输,而且具有线性时间的编译码算法.同时对纠删码文[5]和[7]给出了其删除错误译码算法稳定收敛的充分条件,但此条件必须要求迭代函数为严格单调递减函数.基于数学分析中著名的不动点原理,本文对低密度纠删码给出并证明了其删除错误译码算法稳定收敛的一充分条件,而且说明了此条件优于现有的稳定收敛条件.最后,对给定的度分布证明了此译码算法能成功译码时可接受的最大损失 δ 的几个上界.

收稿日期:2000-12-27;修回日期:2001-05-08
基金项目:国家自然科学基金(No. 69972035)

2 低密度纠删码算法稳定收敛性分析

LDPC 码可用一随机二部图 G 来表示, G 的一个结点集表示 LDPC 码的信息码字,并称这类结点为变量结点, G 的另一个结点集表示 LDPC 码的校验约束,并称这类结点为校验结点.定义二部图 G 的一条边的左边(右边)度数为图 G 中此边左边(右边)邻接结点的度数,并用 λ_i 和 ρ_i 分别表示 G 的左边和右边度数为 i 的边的比率,若令 $\lambda = \lambda(x) = \sum_{i\geq 2}\lambda_i x^{i-1}$ 和 $\rho = \rho(x) = \sum_{i\geq 2}\rho_i x^{i-1}$,则称偶对 (λ, ρ) 为 LDPC 码的一度分布,这时称此码是度分布为 (λ, ρ) 的 LDPC 码.文[5]给出了删除信道下 LDPC 码的一简单译码算法 (称为删除错误译码算法),并首次对纠删码的这一译码算法进行了严格分析之后,证明了其删除错误译码算法稳定收敛的一充分条件,即对于具有度分布 (λ, ρ) 的复损码及初始删除错误概率 $\delta \in (0,1)$,若对 $\forall x \in (0,1]$ 有

$$\rho(1 - \delta\lambda(x)) > 1 - x \qquad (1)$$

成立,则此复损码的删除错误译码算法能以大概率成功译码.一般假定所有的校验方程都线性独立,这时复损码的码率 $R = 1 - \int\rho(x)\,dx / \int\lambda(x)\,dx$.文[7]利用新的概率分析工具对与译码过程相关联的"与或(And-Or)树"进行了分析,并得出

第 l 次迭代译码之后删除错误的比率为

$$x_l = x_l(\delta) = \delta\cdot\lambda(1-\rho(1-x_{l-1})) \quad (2)$$

其中 $x_0=\delta$, $\delta\in(0,1)$, $l\geq 1$. 而且定义度分布 (λ,ρ) 的门限 $\delta^*(\lambda,\rho)$ 为:

$$\delta^*(\lambda,\rho)=\sup\{\delta\mid 0<\delta<1, \lim_{l\to\infty}x_l(\delta)=0\}$$

且有如下引理:

引理 1[7]　设 x_l 如式(2)所定义,删除错误概率为 $\delta\in(0,1)$,即 $x_0=\delta$,对于度分布为 (λ,ρ) 的复损码有:

(a) 若 $\lim_{l\to\infty}x_l=0$,则以上删除错误译码算法能以大概率成功译码;

(b) 若对于 $\forall x\in(0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x))<x$ 成立,则有 $\lim_{l\to\infty}x_l=0$.

易证引理 1(b) 中的条件与条件(1)是等价的.

引理 2　设 $\lambda(x)$ 和 $\rho(x)$ 如上定义,$\delta\in(0,1)$,则对 $\forall x\in(0,1]$ 有 $\rho(1-\delta\lambda(x))>1-x$ 成立当且仅当对 $\forall x\in(0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x))<x$ 成立

证明　由 $\lambda(x)$ 为 $x\in(0,1]$ 上的严格单调递增函数知它的逆函数 $\lambda^{-1}(x)$ 唯一存在且为严格单调递增函数,于是有:

必要性　易见对 $\forall x\in(0,1]$, $\rho(1-\delta\lambda(x))>1-x$ 成立等价于对 $\forall t\in[0,1)$, $\rho(1-\delta\cdot\lambda(1-t))>t$ 成立,若这两个条件成立,令 $y=\delta\cdot\lambda(1-t)$ ($t=0$ 时, $y=\delta$; $t=1$ 时, $y=0$) 得 $1-t=\lambda^{-1}(y/\delta)$, $t=1-\lambda^{-1}(y/\delta)$,将此式代入 $\rho(1-\delta\lambda(1-t))>t(\forall t\in[0,1))$ 有 $\rho(1-y)>1-\lambda^{-1}(y/\delta)$,即 $\frac{y}{\delta}>\lambda(1-\rho(1-y))$,故有不等式 $\delta\cdot\lambda(1-\rho(1-y))<y$ 对于所有 $y\in(0,\delta]$ 成立.

充分性　若对 $\forall x\in(0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x))<x$ 成立,则有 $\rho(1-x)>1-\lambda^{-1}\left(\frac{x}{\delta}\right)$. 令 $u=1-\lambda^{-1}\left(\frac{x}{\delta}\right)$ ($x=0$ 时, $u=1$; $x=\delta$ 时, $u=0$),即 $x=\delta\cdot\lambda(1-u)$,将此式代入 $\rho(1-x)>1-\lambda^{-1}\left(\frac{x}{\delta}\right)$ 即得 $\rho(1-\delta\cdot\lambda(1-u))>u$, $u\in[0,1)$, 从而得 $\forall x\in(0,1]$ 有 $\rho(1-\delta\lambda(x))>1-x$ 成立.

在数学分析中有著名的不动点定理:

定理 1[14]　设函数 $f(x)$ 满足:

(a) $-\infty<a\leq f(x)\leq b<+\infty$ ($a\leq x\leq b$);

(b) 存在 $k\in(0,1)$ 使得对所有 $x,y\in[a,b]$ 有 $|f(x)-f(y)|\leq k|x-y|$ 成立.

设 $x_1\in[a,b]$,并定义序列 $\{x_n\}: x_{n+1}=f(x_n)$ ($n=1,2,\cdots$),则有 $\lim_{n\to\infty}x_n$ 存在,且若令 $\lim_{n\to\infty}x_n=x^*$,则 x^* 是 $[a,b]$ 中满足 $f(x)=x$ 的唯一元素.

根据不动点定理可得如下结论.

定理 2　(低密度纠删码稳定收敛的充分条件)

设 $\lambda(x)$ 和 $\rho(x)$ 为一随机二部图的度分布,$\delta\in(0,1)$,对整数 $l\geq 1$,定义 $x_l=\delta\cdot\lambda(1-\rho(1-x_{l-1}))$, $x_0=\delta$,若 $\delta<\frac{1}{\lambda'(0)\rho'(1)}$,则存在 $\xi=\xi(\lambda,\rho,\delta)$, $\xi>0$,使得对于所有 $x_l\leq\xi$ ($l=0,1,\cdots$) 有 $\lim_{l\to\infty}x_l=0$.

证明　若令 $f(x)=\delta\cdot\lambda(1-\rho(1-x))$,则有

$$x_l=f(x_{l-1})=\delta\cdot\lambda(1-\rho(1-x_{l-1}))$$

其中 $x_0=\delta$ ($l=1,2,\cdots$),即得序列 $\{x_l\}$ ($l=0,1,\cdots$). 将 $\delta\lambda(1-\rho(1-x_{l-1}))$ 在 $x=0$ 点展开为泰勒级数得

$$x_l=\delta\lambda'(0)\rho'(1)x_{l-1}+O(x_{l-1}^2)$$

若 $\delta<\frac{1}{\lambda'(0)\rho'(1)}$,即 $\delta\lambda'(0)\rho'(1)<1$,则存在一充分小的常数 $\xi(\lambda,\rho,\delta)>0$ 使得对于所有的 $x_l\leq\xi$ ($l=0,1,\cdots$) 存在常数 $k(0<k<1)$ 有

$$\begin{aligned}|x_{l_1}-x_{l_2}|&=|f(x_{l_1-1})-f(x_{l_2-1})|\leq|\delta\lambda'(0)\rho'(1)||x_{l_1-1}-x_{l_2-1}|\\&\quad+O(|x_{l_1-1}+x_{l_2-1}||x_{l_1-1}-x_{l_2-1}|)\\&\leq k|x_{l_1-1}-x_{l_2-1}|\end{aligned}$$

其中 x_{l_1} 和 x_{l_2} 为 $[0,\xi]$ 中的任意两个元素.

即存在充分小的 $\xi>0$,使得对于所有的 $x_l\leq\xi$ ($l=0,1,\cdots$) $f(x)$ 满足以下条件:

(a) $-\infty<0<f(x)\leq\delta\leq\xi<+\infty$ ($0\leq x\leq\xi$);

(b) 存在常数 $k(0<k<1)$,使得对任意的 $x_{l_1},x_{l_2}\in[0,\xi]$ 有 $|f(x_{l_1})-f(x_{l_2})|\leq k|x_{l_1}-x_{l_2}|$.

由不动点定理 1 知 $\lim_{n\to\infty}x_n$ 存在,且若令 $\lim_{n\to\infty}x_n=x^*$,则 x^* 是 $[0,\xi]$ 中满足 $f(x)=x$ 的唯一元素,但易知 $x=0$ 是 $f(x)=x$ 的一个不动点,所以 $x^*=0$,即得 $\lim_{n\to\infty}x_n=0$.

注　若对 $\forall x\in(0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x))<x$,其中 $\delta\in(0,1)$,则由文[11]得 $\delta\leq\frac{1}{\lambda'(0)\rho'(1)}$,但反过来 $\delta\leq\frac{1}{\lambda'(0)\rho'(1)}$ 成立时并不能保证对 $\forall x\in(0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x))<x$ ($\delta\in(0,1)$) 成立. 因此,定理 2 的稳定收敛条件弱于引理 1(b) 所给的稳定收敛条件.

3　可接受的最大损失 δ 的上界

现在以引理 2 中的两个条件为工具给出以上删除错误译码算法成功译码时可接受的最大损失 δ 的几个上界.

引理 3[12]　设 G 是度分布为 $\lambda(x)$ 和 $\rho(x)$ 的随机二部图,则 G 的左边和右边结点的平均度数 a_L 和 a_R 分别为 $a_L=1/\int_0^1\lambda(x)\,dx$ 和 $a_R=1/\int_0^1\rho(x)\,dx$.

由引理 2 可得如下上界.

定理 3　设 $\lambda(x)$ 和 $\rho(x)$ 为一随机二部图的度分布,a_L 和 a_R 分别为二部图 G 左边和右边结点的平均度数 ($\delta\in(0,1)$),若对 $\forall x\in(0,1]$ 有 $\rho(1-\delta\lambda(x))>1-x$ (或对 $\forall x\in(0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x))<x$),则有:

(a) $\delta\leq\delta^*(\lambda,\delta)\leq a_L/a_R$;

(b) $\delta\leq\delta^*(\lambda,\rho)\leq\frac{a_L}{a_R}(1-(1-\delta)^{a_R})$;

(c) $\delta\leq\delta^*(\lambda,\rho)\leq\frac{1}{\lambda'(0)\rho'(1)}$.

证明　由 $\lambda(x)$ 和 $\rho(x)$ 均为 $[0,1]$ 上的严格单调递增函数知,它们的逆函数 $\lambda^{-1}(x)$ 和 $\rho^{-1}(x)$ 也都唯一存在且均为严格单调递增函数,于是结合 $\delta^*(\lambda,\rho)$ 的定义有:

(a) 已知条件等价于对所有的 $x\in(0,1]$ 不等式 $1-\delta\lambda(x)>\rho^{-1}(1-x)$ 成立. 对上式两边从 0 到 1 求积分得 $1-\delta$

$\int\lambda(x)\,dx \geq \int\rho^{-1}(1-x)\,dx = 1 - \int\rho(x)\,dx$. 结合引理 3 得 $\delta \leq \delta^*(\lambda,\delta) \leq a_L/a_R$.

(b) 若对 $\forall x \in (0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x)) < x$ 成立, 则由文[11]知 $\delta \leq \frac{a_L}{a_R}(1-(1-\delta)^{a_R})$ 成立. 根据 $\delta^*(\lambda,\rho)$ 的定义易得 $\delta \leq \delta^*(\lambda,\rho) \leq \frac{a_L}{a_R}(1-(1-\delta)^{a_R})$.

(c) 若对 $\forall x \in (0,\delta]$ 有 $\delta\cdot\lambda(1-\rho(1-x)) < x$ 成立, 其中 $\delta \in (0,1)$, 则由文[11]得 $\delta \leq 1/\lambda'(0)\rho'(1)$, 因此 $\delta \leq \delta^*(\lambda,\rho) \leq 1/\lambda'(0)\rho'(1)$.

4 结束语

基于数学分析中著名的不动点原理, 本文对于低密度纠删码给出并证明了其删除错误译码算法稳定收敛的一充分条件, 且此条件不必要求迭代函数在整个区间 $x \in (0,\delta]$ 上为严格单调递减函数, 所以此条件优于现有的稳定收敛条件. 最后, 对给定的度分布给出了此译码算法能成功译码时可接受的最大损失 δ 的几个上界. 对 LDPC 码本文的译码算法稳定收敛条件是在删除信道下而得出的, 如何寻找高斯加性噪声信道和二进对称信道等其它信道下其译码算法稳定收敛的条件仍然是一个值得研究的重要问题. 另外, 可利用最优化理论的知识研究寻找最优度分布 (λ,ρ) 的方法, 从而构造良好性能的 LDPC 码, 这也是构造基于二部图的纠删码的非常重要的问题.

参考文献:

[1] R G Gallager. Low Density Parity Check Codes [M]. Cambridge, Massachusetts: MIT Press, 1963.

[2] D Spielman. Linear-time encodable and decodale error-correcting codes [J]. IEEE Trans on Inform Theory, 1996, 42(6): 1723 - 1731.

[3] N Alon, M Luby. A linear time erasure-resilient code with nearly optimal recovery [J]. IEEE Trans on Information Theory, 1996, 42(6): 1732 - 1736.

[4] I Rizzo. Effective erasure codes for reliable computer communication protocols [J]. ACM Computer Communication Review, 1997, 27(2): 24 - 36.

[5] M Luby, M Mitzenmacher, A Shokrollahi, D Spieman, V Stemann. Practical loss-resilient codes [A]. Proc. of the 29th ACM Symposium on Theory of Computing [C]. 1997. 150 - 159.

[6] D J C MacKay, R M Neal. Near shannon limit performance of low density parity check codes [J]. Electronics Letters, 1997, 33(6): 457 - 458.

[7] M Luby, M Mitzenmacher, A Shokrollahi. Analysis of random processes via and-or tree evaluation [A]. In Proceedings of the 9th Annual ACM-SIAM Symposium on Discrete Algorithms [C]. 1998. 364 - 373.

[8] M G Luby, M Mitzenmacher, M A Shokrollahi, D A Spielman. Analysis of low-density parity check codes and improved designs using irregular graphs [A]. Proc. of the 30th ACM Symposium on Theory of Computing [C]. 1998. 249 - 258.

[9] M G Luby, M Mitzenmacher, M A Shokrollahi, D A Spielman. Improved low-density parity check codes using irregular graphs and belief propagation [A]. Proceedings 1998 IEEE International Symposium on Information Theory [C]. 1998.

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

[11] M A Shokrollahi. New sequences of linear-time erasure codes approaching the channel capacity [A]. Proceedings of the 13th conference on Applied Algebra, Error Correcting Codes, and Cryptography [C]. Springer Verlag: 1999.

[12] 慕建君, 孙韶辉, 王新梅. 关于线性时间复损码的研究 [J]. 电子学报, 2002, 30(1): 122 - 125.

[13] P Elias. Coding for two noisy channels [A]. Information Theory, Third London Symposium [C]. 1955. 61 - 67.

[14] Walter Rudin. Principles of Mathematical Analysis [M]. New York: McGraw-Hill, 1976.

作者简介:

慕建君 男, 1965 年生于陕西吴堡, 1997 年获西安电子科技大学应用数学专业硕士学位并留校任教, 现为该校通信与电子系统专业在职博士研究生, 目前的研究兴趣为编码、信息论与应用数学.

贺玉成 男, 1989 年毕业于西安电子科技大学, 获通信与电子系统工学硕士学位, 现为该校博士研究生, 1999～2000 年在日本静冈大学进行学习和研究, 目前的研究方向是 LDPC 码、Turbo 码及编码调制技术.

王新梅 男, 西安电子科技大学教授, 博士生导师, 中国电子学会会士, 长期从事信息论、编码和密码学的教学与研究.