

通向信道编码定理的 Turbo 码及其性能分析^{*}

Turbo Codes to Channel Coding Theory and Their Performance Analyses

吴伟陵

(北京邮电大学信息工程系, 北京 100876)^{**}

【提要】 本文综述了 Shannon 编码定理指导下信道编、译码的发展概况及趋势. 全面、系统地分析了最近引起普遍强烈关注的 Turbo 码的基本构造原理和其能够达到惊人的优异性能的原因. 指出了目前该领域一些很有理论价值与应用意义的研究方向.

关键词: 信道编码, Turbo 码, 级连码, 迭代译码

Abstract: An overview of the advances and trend in the channel coding is made under the Shannon's Coding Theory. The novel structures and astonishing performance of the Turbo codes are analyzed comprehensively and systematically. A useful direction and prediction of some hot topics on this area that are of both theoretical and practical interests are pointed out.

Key words: Channel coding, Turbo codes, Concatenated codes, Iterative decoding

一、编码定理指导下的信道编码

1948 年信息论的开创者 C. E. Shannon 在他的奠基性论文“A mathematical theory of communication”^[1]中首次提出著名的信道编码定理, 虽然人们普遍认为它是一个数学上的存在性定理, 但是它确给以后信道编码的研究指出了明确的方向.

所谓信道编码定理, 是指对每一类信道都存在着一一定的信道容量 C , 它是信道的最大极限传输能力. 只要当实际传输速率 $R < C$ 时, 就可以实现在信道中无差错的传输.

Shannon 及 A. Feinstein 给出了这一定理在分组码情况下的证明, 以后又有人将它推广至卷积码. Shannon 等在他们的证明中引用了三个基本条件:

- 1) 采用随机编、译码方式;
- 2) 编译长度 $L \rightarrow \infty$, 即分组的码组长度无限;
- 3) 译码采用最佳的极大似然译码法.

在以上三个必要条件下, Shannon 证明了在信道

中可以实现无差错传输. 后来, 1965 至 1968 年 R. G. Gallager 给出了误码率 P_e 的指数界表示形式^[2,3]:

$$P_e \leq e^{-L_1 E_1(R)} \quad (1)$$

其中: L_1 为分组码的编、译码长度; $E_1(R) > 0$ 为可靠性函数, 取决于不同的编、译码方式.

信息论诞生 50 年来, 构造好码基本上是按照 Shannon 所引用的三个基本条件的后两条, 即条件 2) 与条件 3) 为两条主线发展下来的. 对于条件 1) 一直未给予足够的重视, 其原因可能是因为随机编、译码难以产生和控制. 下面, 将首先讨论在条件 2) 与条件 3) 两条主线指导下信道编、译码的发展. 最后, 再反过来讨论实现条件 1) 的可能性.

1 信道编码的构造问题

长期以来, 由于译码的复杂度, 人们将构造信道编码的重点放在短码上, 即寻找一种可译码的结构, 使短码具有尽可能大的最小码距; 对长码而言, 其码距应尽可能接近平均码距. 在码的构造空间中, 由于高维理论的不足, 编码研究的思想多半局限于低维

^{*} 1998 年 3 月收到, 1998 年 4 月修改定稿. 本文是为纪念 C. E. Shannon “通信的数学理论”发表 50 周年而作. 国家自然科学基金重大项目 69896243 资助

^{**} Wu Weiling (Dept. of Information Engineering, Beijing University of Posts and Telecommunications, Beijing 100876)

数的短码,这时,好码要求有尽可能大的最小码距,它相对于未编码能提供一定的编码增益,但是与信道编码定理要求的相差甚远.为了获得可译的高维数的长码,人们以现有短码构造为基础提出了串接式的级连码.1966年 Forney^[4,5]首先提出利用两个确定的短码来构造长码的串接式级连码.并且采用准最佳的广义最小距离译码证明了与式(1)完全类似的结论:

$$P_e \leq e^{-L_2 E_2(R)} \quad (2)$$

式中: $E_2(R) < E_1(R)$,这是由于 $E_2(R)$ 采用的是非随机码且译码采用的是准最佳的广义最小距离译码.显然,要达到同样小的误码率 P_e 时, $L_2 > L_1$. 即其编译码的分组长要比理想的随机码与最大似然译码情况下更长才行.

Forney 的串行级连码,编、译码器实现的典型方框图如图 1、2 所示.

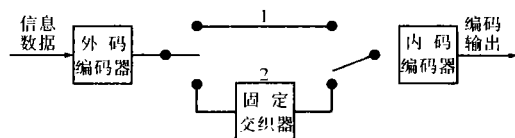


图 1 串行级连码编码器框图

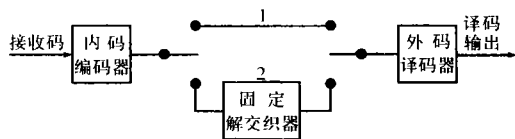


图 2 串行级连码译码器框图

由上述框图可见,串行级连码是采用两个确定短码作为内、外码串接而成,其性能也是两个短码性能函数的串接,即希望通过对外码的译码纠正内码尚未能纠正的差错.由于这一革新思想的引入,给信道编码,特别是长码的性能带来了很大程度上的改

善.这类串行级连码很快地就应用于无需追求传输效率的深空通信,并取得了巨大的成功.它在采用最大似然的软判决译码以后,其误码率几乎达到逼近理想 Shannon 限的优异性能^[6],如图 3 所示.图中:① Shannon 理论限;② 伽利略号采用的实验:内码(4,1,15)卷积码,外码(255,223)RS 码;③ 旅行者号(1986 年):内码(2,1,7)卷积码,外码(255,223)RS 码;④ 未编码的 PSK 调制.

上述的优异性能是在远离信道容量的条件下,即 $R/C \ll 1$ 时取得的.一旦 $R/C \rightarrow 1$,即处于渐近状态,以上优异性能将很快丢失.这是目前所有已知短码存在的固有特点.即使由这类短码串行级连构成长码,其渐近状态的组合性能仍然是由被串接的内、外两个短码的性能所决定,所以在采用确定的短码来构造长码时其性能仍存在着一个渐近状态不可逾越的鸿沟.

2 最佳译码问题

信道编码理论与实践主要是围绕编码与译码两个方面展开的.条件 2) 主要侧重于编码构造问题,条件 3) 则主要侧重于译码的准则、算法与实现问题,条件 1) 则同时涉及编、译码的方法与原则问题.

从工程实现角度,编码构造远比译码简单得多.只要编码规则与方法一旦确定,实现比较简单,其实现复杂度一般仅为 $O(k)$, 或 $O(n-k)$, 其中, k 为信息位数, n 为码长.译码则复杂得多.首先是准则与算法问题,从理论上讲,在白噪声信道条件下,实现译码差错概率最小的最佳译码方法早已解决.它就是最大后验概率译码,若在码字等概率发送的条件下(比如满足强对称信道、对称信道以及准对称信道条件下),它就等效为著名的最大似然译码,进一步对于二进制对称信道它还可以等效为简单的最小汉明距离译码.工程上要实现这类最佳译码,比如最常用的最大似然译码却相当复杂,其译码复杂度一般应 $O(2^k)$ 或 $O(2^{n-k})$. 可见从译码角度看,要实现中等长度以上的译码几乎是不可能的.直至目前为止,能真正达到最佳译码性能的仅仅只有一种 Viterbi 译码,它是一种最大似然译码.而且仅仅适合于约束长度较小的卷积码和短或低纠错能力的分组码.事实上,早在七十年代, Berlekamp 等人已证明了一般线性码的译码问题是一个 NPC 问题^[7]. 因此人们将注意力和研究方向转移到寻找接近最大似然译码性能,而在工程实现上却要简单得多的准最佳、次最

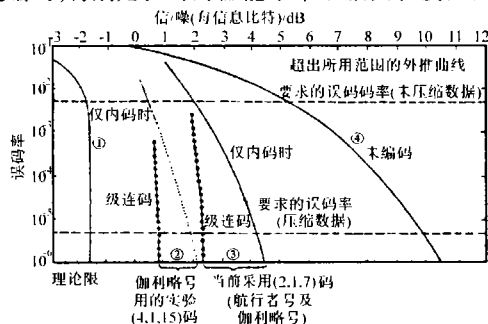


图 3 深空通信中的信道编码性能

佳各类译码算法上。

几十年来,在寻找较为实用化的准最佳、次最佳的译码算法中,大致可以划分为两个方面:一个是以追求每个码元译码错误概率最小为目标的逐位软判决译码算法;另一个则是以追求每个码字(组)错误概率最小为目标的逐组软判决译码算法。

逐位软判决译码算法,起源于 1963 年 Massey 提出的适用于大数逻辑可以译码的最大后验概率译码^[8],它实质上是一种门限译码。在硬判决时就是大数逻辑译码。在这类译码算法中特别要提出的是在后面 Turbo 码译码中将要采用的 Bahl 等人提出的计算每位码元最大后验概率的迭代算法,又称 BCJR 算法^[9](它由四个作者名字的第一个字母构成)。这种算法的特点亦即与其它最大似然算法不同之处在于它是一种递推迭代算法,且每个符号的运算量不随总码长而变化,因此计算速度很快。这一算法当时提出后并没有受到人们足够的重视,直至 1993 年 Berrou 等人在 Turbo 码的译码中采用,才重新广泛引起人们的注意和兴趣。

在准最佳、次最佳译码研究上另一个方向是研究逐字(组)软判决译码。Forney 首次提出的广义最小距离译码^[4],即迭代纠错译码就是系统的最先研究的逐字(组)软判决译码。1972 年,Chase 在广义最小距离译码思想的基础上提出了著名的三类 Chase 算法^[10]。分组码逐字(组)软判决译码的另一研究方向是基于网格(Trellis)图上的 Viterbi 译码的研究,由于这一类与 Turbo 码目前关系不大,就不再赘述。

3 关于随机码

自从 C.E.Shannon 引用长随机序列的渐近等分割的 A.E.P 特性以及在其基础上的随机编、译码思想用于证明他的三个编码定理以来,人们一直认为它不过是为了证明三个编码定理而采用的一种数学方法和手段,因此并未给予足够的重视。实际上,随机化思想是 Shannon 理论的精华,它不仅在理论上体现在整个 Shannon 理论中,而且,它也是构造长的理想信道编码的方向,这一点将从 Turbo 码中得到体现。有关这一部分内容,我们将留到在后面讨论。

二、Turbo 码的基本构造

在 1993 年 ICC 国际会议上两位任教于法国不列颠通信大学的教授与他们的缅甸籍博士生 C.

Berrou, A. Glavieux 和 P. Thitimajshiwa, 首先提出了一种称之为 Turbo 码的编、译码方案^[11](在英文中前缀 Turbo 带有涡轮驱动的含义),其编、译码基本结构如图 4、5 所示。

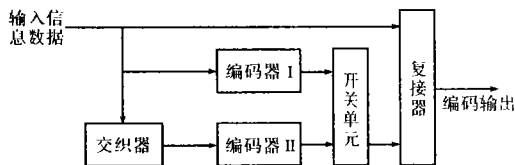


图 4 Turbo 码编码原理图

从上述编码器可以看出,编码是由三部分组成:直接输入复接器、经水平编码器 I 再经开关电路送入复接器以及经垂直编码器 II 再经开关电路送入复接器。其中经水平编码器 I 的水平码与经垂直编码器 II 的垂直码又可分别称为 Turbo 码的分量码,又称为二维分量码。显然从二维很自然地可以推广到多维。作为分量码既可以是卷积码,也可以是分组码;其码型既可以相同,也可以不同;既可以是单一的码也可由级连产生的码。原则上讲,分量码既可采用系统码形式也可采用非系统码形式,但考虑到码的整体速率,研究更多的是用系统作为分量码。

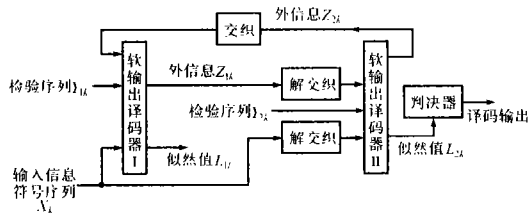


图 5 Turbo 码译码原理图

在译码中,判决是按照最大似然比进行的。而计算似然比的算法,是采用了修正的 BCJR 算法,它实质上可归结为软输入/软输出的反馈递推迭代译码算法,图 4 中两个软输出译码器 I、II 之间是依靠反馈附加的外信息建立相互联系的。其原理后面将作进一步介绍。Berrou 论文仅是一个按上述框图进行计算机仿真的研究,仿真结果表明,当归一化位噪比 $E_b/N_0 \geq 0.7\text{dB}$ 时, $\text{BER} \leq 10^{-5}$,这一结果是在交织器大小为: $256 \times 256 = 65536$ 情况下,以及进行 18 次迭代以后获得的。这一超乎寻常的优异性能立即引起编码界的强烈反响。

Turbo 码为什么会取得如此超乎寻常的接近 Shannon 限的优异性能,至今还是一个谜。其主要原因之一是由于提出 Turbo 码的三个作者并不是从理

论角度研究与探讨 Turbo 码,而仅是从工程上从计算机仿真角度提出并得出上述优异性能的.因此很多人认为 Turbo 码缺乏理论基础,而且至今也未找到有效的理论分析与解释方法,因此对其性能与结论产生怀疑是很自然的.但是,后来又经过不少人重复性研究后发现 Turbo 码决非巧合,它的确存在着巨大的潜力,它的性能是目前最好的,尚没有一种信道编码与其能抗衡,与其优异性能相比拟.因此,目前人们将注意力更多地从怀疑转向揭示这一新思想的实质,完善其理论体系,以便更好地指导 Turbo 码的发展和应用.

本文也试图在这方面做一些工作.作者认为 Turbo 码的核心是构造长序列的伪随机性的编、译码.

三、Turbo 码的性能分析

1993 年, Berrou 等人提出的 Turbo 码实际上是前人工作的巧妙综合与发展,是编码理论与实际发展的必然产物.虽然在实现的巧妙综合方法上带有一定的偶然性,但是其发展总趋势是必然的.它以巧妙综合的仿真结果取得了令人振奋的优异结论,使其译码性能几乎接近 Shannon 的信道编码定理的要求.后来人们对它进行分析的文章也很多,它们分别涉及到编码方法、交织器结构、译码算法以及码重分布和距离谱等,得出了一些很有价值的观点和结论.但是,这些分析多半是从某一个局部进行的,缺乏系统性与全局观点.

本文是在前人分析的基础上,试图着重从全局和系统的角度进行较全面的分析,本文分析的依据,完全是按信息论创始人 Shannon 等在证明信道编码定理时提出的三个必要性条件,也即是前面分析时指出的三个必要条件进行的.

1 随机性编、译码及其实现

人们一直广泛地认为随机编、译码只不过仅是 Shannon 为了证明其信道编、译码定理的存在性而引入的一种数学方法和手段,而并没有将它作为构造性能优良长码的主要方向和手段.普遍认为它是一类可望而不可及的构造方法.其实,随机化是贯穿 Shannon 理论的核心思想之一,不论是对信源与信道的分析还是信源、信道编码定理的证明,始终是其处理方法的一条主线.因此对其理论价值早有足够的

认识.但是在构造上如何发挥作用一直抱有怀疑,直到 1993 年 Berrou 等人带有一定偶然性巧妙地综合出 Turbo 码,产生了如此不可思议的好的优异性能.其根本原因是在 Berrou 的 Turbo 码实现方案中,长码构造的伪随机性是核心.在发送端,其伪随机性是通过编码器中的交织器以及并行级连方式来实现的;在接收端,则是利用具有软输入/软输出特性的带有交织器的反馈递推迭代译码来实现的.

从 Turbo 码编码器构造(图 4)可以清楚地看出: Turbo 码是数据流经三路并行级连而形成的.特别是并行中的第三路在重直编码器前加上了一个交织器,正是这个交织器及并行串接级连实现了编码器的伪随机化作用,这就是说我们可以将三路并行含交织器的结构看作一个完整统一的伪随机码编码器.按照这一观点,若将交织器设计成非固定的一组伪随机式交织器其效果将更好.

1995 年, Svirid^[12]考虑分量码线性分组码时,码字 $C = (m \parallel mP \parallel m'P)$, 其中 m 是 k 维信息矢量, P 是 $k \times r$ 的矩阵, m' 是 m 通过随机转换得到的. Svirid 指出交织器的目的在于使 Turbo 码的最小重量尽可能大,即交织器直接影响 m' 的 P 重量,起到随机化作用. mP 的汉明重量 $W(mP)$ 小时, $W(m'P)$ 应该大,反之亦然. 1996 年 S. Benedetto 和 G. Montorsi^[13]引入均匀交织器的概念,给出了 Turbo 码一个 BER 的联合上限,并指出好的交织器是存在的.这些都说明了 Turbo 码优异性能在发送端主要是由编码交织器的伪随机化带来的.

Turbo 码的译码,由图 5 清楚的显示,它是一类具有反馈结构的伪随机译码器.这是由于两个码可以交替互不影响的译码,并且还可以通过关于系统码信息位的软判决输出相互传递信息,进行递推式迭代译码;通过多次迭代使每个码元都可以得到来自序列中几乎所有码元的信息,它具体是通过迭代中反复交织反馈、去交织来实现的,这实际上就实现了译码的伪随机化.尽管图 5 中给出的是反馈式的结构,但是由于有交织环节的存在必然引起时延使得不可能有真正意义上的反馈,而是流水线式的迭代结构,如图 6 所示.

正是由于采用了这种流水线式结构,使得译码器可以由若干个(L 个)完全相同的软输入/软输出的基本译码单元构成.

1996 年, J. Hagenauer 等^[14]对存在软输入/软输

算就变成了加法运算,而加法运算则变成了

$$e^a + e^b = e^{\max(a,b) + \ln(1 + e^{-|a-b|})} \quad (4)$$

这里的对数项可用一个加法运算和一个查表运算来实现,于是总运算量为 16×2^k 次加法, 5×2^k 次求最大运算和 5×2^k 次查表。

C. 最大值运算^[18,19] 在上述对数域的算法中,似然值加法表示式中的对数分量忽略掉,使似然加法完全变成求最大值运算。这样,除了可省去大部分加法运算以外,更大的好处是省去了对信噪比的估计,使算法更稳健。

D. 软输出 Viterbi 译码(SOVA) 其运算量为标准 Viterbi 算法的两倍。

几种算法性能比较,最大值算法比标准算法稍差,而 SOVA 算法性能损失最大约 1dB。

参 考 文 献

- 1 C. E. Shannon. A mathematical theory of Communication. BSTJ, 27: 379 ~ 423, July and pp. 623 ~ 656, Dec, 1948
- 2 R. G. Gallager. A simple derivation of the coding theorem and some applications. IEEE Trans. Inform. Theory, IT-11: 3 ~ 18, Jan., 1965
- 3 R. G. Gallager. Information Theory and Reliable Communication. New York, Wiley, 1968
- 4 G. D. Forney, Jr. Concatenated Codes, Sc. D. Thesis, M. I. T., Cambridge, Mass, 1965, also, MIT Press Research Monograph 37, 1966
- 5 G. D. Forney, Jr. Generalized minimum distance decoding. IEEE Trans. Inform. Theory, 12: 125 ~ 131, 1966
- 6 王育民等. 纠错码在数字通信中的应用. 西安电子科技大学学报, 1993 年 8 月第 20 卷第 2 期
- 7 E. R. Berlekamp, R. J. McEliece and H. C. A. Van Tilborg. On the inherent intractability of certain coding problem. IEEE Trans. Inform. Theory, 24: 386 ~ 389, 1978
- 8 J. L. Massey. Threshold Decoding, Cambridge, MA: MIT Press, 1963
- 9 L. R. Bahl, J. Cocke, F. Jeinek and J. Raviv. Optimal decoding of linear codes for minimizing symbol error rate. IEEE Trans. Inform. Theory, 20: 248 ~ 287, 1997
- 10 D. Chase. A class of algorithms for decoding block codes with channels measurement information. IEEE Trans. Inform. Theory, 23: 514 ~ 517, 1976
- 11 C. Berrou, A. Glavieux and P. Thitimajshima. Near Shannon limit error-correcting coding and decoding; Turbo-codes(1). ICC'93: 1064 ~ 1074, 1993
- 12 Y. S. Svirid. Weight distributions of turbo codes. Proc. ISIT'95, 38
- 13 S. Benedetto and G. Montorsi. Unveiling turbo codes: Some results on parallel concatenated coding schemes. IEEE Trans. Inform. Theory, 42: 409 ~ 428, Mar, 1996
- 14 J. Hagenauer, E. Offer and L. Papke. Iterative decoding of binary block and convolutional codes. IEEE Trans. Inform. Theory, 42: 429 ~ 445, May, 1996
- 15 A. J. Viterbi. Error bounds for convolutional codes and an asymptotically optimal decoding algorithm. IEEE Trans. Inform. Theory, IT-13: 260 ~ 269, April 1967
- 16 H. L. Yudkin. Channel state testing information decoding. Sc. D. Thesis, Dept of Elec. Eng., MIT, 1964
- 17 P. Robertson, E. Villebrun, P. Hoeber. A comparison of optimal and suboptimal MAP decoding algorithms operating in the Log domain. ICC'95, 1995: 1009 ~ 1013
- 18 P. Jung. Novel low complexity decoder for Turbo codes. Electron. Lett, 1995, 31(2): 86 ~ 87
- 19 J. Hagenauer, P. Hoeber. A Viterbi Algorithm with soft-decision outputs and its applications. GLOBECOM'89, 1989, 1680 ~ 1687
- 20 王新梅, 马建峰, 马嘯. 软判决译码研究进展. 信息论与通信理论学术会议(论文集), 1997 年 12 月, 深圳, 23 ~ 38
- 21 叶中行, Victor Wei. Turbo 码的若干新进展. 信息论与通信理论学术会议(论文集), 1997 年 12 月, 深圳, 106 ~ 114
- 22 周世东. 关于提高移动多址信道容量的原理和方法. 清华大学博士论文, 1997. 4



吴伟陵 1938 年生, 1961 年毕业于北京邮电学院无线电系, 现任北京邮电大学教授、博士生导师, 国家自然科学基金委学科评审组成员、中国电子学会信息论分会主任委员。