Turbo 码有效自由距离 d_2 上限的证明 [1]

陈献光 王 进

(解放军广州通信学院电子技术教研室 广州 510502)

摘 要 Turbo 码是一种新的纠错码，具有十分突出的纠错能力。Turbo 码编码器由两个或两个以上的分量码编码器和交织器并行级联而成。S. Benedetto 和 G. Montersi(1996) 中提出了设计 Turbo 码的新参数——有效自由距离 d_2(Effective Free Distance)。D. Divsalar 和 R. J. McEliece(1996) 给出了有效自由距离的两个上限，但未给出证明。本文从理论上对 d_2 的两个上限进行证明。

关键词 Turbo 码，级联码，信道编码

中图号 TN911.22

1 引 言

1993 年 Berrou 等人提出了一种新的信道编码—— Turbo 码 [1]，它又称为并行级联卷积码 (Parallel Concatenation of Convolutional Code)。由于 Turbo 码在接近 Shannon 极限的信噪比下仍能够获得较低的误码率 $(10^{-2}-10^{-3})$，所以在近几年引起了编码界的广泛兴趣，并成为编码研究领域最新的发展方向之一。Turbo 码编码器由两个或两个以上分量编码器和一个或一个以上交织器并行级联而成。因此，Turbo 码的设计主要就是如何选择分量编码器和交织器，使整个 Turbo 码的性能达到最优。从最终目标来看，人们不仅想找到一个好码，更想发现满足什么条件的码才能提供好的性能。显然，码设计必然建立在性能分析的基础上，但目前对这种码的性能分析还不够完全。Benedetto 等人给出一类 Turbo 码的平均性能，并提出了设计 Turbo 码的新参数——有效自由距离 d_2。文献 [2] 给出了有效自由距离的两个上限，但未给出证明。

在本文中，我们将对有效自由距离 d_2 的上限从理论上给予证明。文中第二部分介绍有效自由距离的定义及上限。第三部分给出证明 d_2 的上限所需的知识和定理。第四部分对 d_2 的上限进行证明。第五部分是本文的结束语。

2 有效自由距离 d_2 及其上限

文献 [2] 中给出了设计 Turbo 码的一些基本原则，给出了在 AWGN 信道中 Turbo 码比特差错率 P_b 的上限

$$P_b \leq \sum_{k=1}^{\lfloor N/2 \rfloor} 2k \binom{2k}{k} N^{-1} \cdot \left. \frac{(H^{2+2z_{\min}})^k}{(1-H^{z_{\min}-2})^{2k}} \right|_{H=e^{-R_c E_b/N_0}} \tag{1}$$

其中 $z_{\min}$ 为输入信息序列重量为 2 时，输出序列校验比特的最小重量。定义 (1) 式中 H 的最小指数为 Turbo 码的有效自由距离，即

$$d_2 = 2 + 2z_{\min} \tag{2}$$

文献 [2] 中对有效自由距离进行了分析，并以定理形式给出了 d_2 的两个上限。

定理 1 对二进制 (r,k,m) 卷积码，有

$$d_2 \leq \min(\lceil 2^m/k \rceil r, 2r + \lfloor (2^{m-1}r)/k \rfloor) \tag{3}$$

定理 2 对二进制 $(r,1,m)$ 卷积码，有

$$d_2 \leq (2+2^{m-1})r, \quad m \geq 2 \tag{4}$$

[1] 1998-11-02 收到，1999-06-04 定稿

当且仅当生成矩阵形式为 $G(D)=[P_1(D)/Q(D),\cdots,P_r(D)/Q(D)]$ 时等式成立。其中 $Q(D)$ 为 m 阶本原多项式，$P_1(D),\cdots,P_r(D)$ 为 m 阶多项式。$P_j(D)$ 常数项为 $1(j=1,\cdots,m)$，且 $P_j(D)\neq Q_j(D)$。

3 预备知识及定理

在证明 d_2 的上限之前，先介绍证明时所需的有关定理和推论。因篇幅所限，有些定理直接给出，而不加证明。

一个 (r,k,m) 二进制卷积码可由矩阵 A, B, C 和 D 的线性运算所决定，矩阵为

$$A:m\times m;\quad B:k\times m$$
$$C:m\times r;\quad D:k\times r$$

k 维输入矢量序列 $u_0,u_1,\cdots$，输入至编码器，经 m 维状态矢量变换，产生 r 维输出矢量序列 $x_0,x_1,\cdots$，即有

$$s_{j+1}=s_jA+u_jB,\ x_j=s_jC+u_jD,\quad j=0,1\cdots \tag{5}$$

初始状态 $s_0=0$。

引理 1 2^m 个零输入支路的总输出重量最多为 2^{m-1}，当且仅当矩阵 C 每列至少有一非零项等式成立。

定理 3 设 $(i,t_i)\neq(j,t_j)$，输入序列码重为 2 的码径满足

$$b_iA^{t_i}=b_jA^{t_j} \tag{6}$$

其中 b_i, b_j 为 B 中第 i, j 行，t_i 和 t_j 为非负整数。

证明 生成有限码径重量为 2 的输入序列形式为 $(e_i,0,\cdots,0,e_j,0,\cdots,0)$ 或者 $(e_i+e_j,0,\cdots,0)$。

对第一种形式，相应的状态序列为

$$\mathbf{0}\xrightarrow{e_i}b_i\xrightarrow{0}b_iA\cdots\xrightarrow{0}b_iA^{t-1}\xrightarrow{e_j}b_iA^t+b_j\cdots\xrightarrow{0}(b_iA^t+b_j)A^s=\mathbf{0}.$$

从上面可知，$b_iA^{t+s}=b_jA^s$。

对第二种形式，状态序列为

$$\mathbf{0}\xrightarrow{e_i+e_j}b_i+b_j\xrightarrow{0}\cdots\xrightarrow{0}(b_i+b_j)A^t=\mathbf{0}$$

这等同于 $b_iA^t=b_jA^t$。

证毕

定理 4 设 b_i 和 b_j 为矩阵 B 的行，且 (6) 式成立，则有

$$d_2\leq r\times(\max(t_i,t_j)+1);\quad (i,t_i)\neq(j,t_j)$$

证明 从定理 3 可知，长度为 $\max(t_i,t_j)+1$，输入码重为 2 的码径是存在的。显然，这个码径的输出重量不能超过 $r\times(\max(t_i,t_j)+1)$。 证毕

推论 1 对 $d_1<\infty$ 的 (r,k,m) 卷积码，有 $d_2\leq\lceil 2^m/k\rceil r$。

定理 5 如矩阵 A 是非奇异的，有 $d_2\leq 2r+\lceil(2^{m-1}r)/k\rceil$。

定理 6 如矩阵 A 是奇异的，则有 $d_2\leq(1+\lceil(2^{m-1}/k\rceil)r$。

证明 $\{b_1,\cdots,b_k\}$ 是 B 的行向量，b_iA^j 有 kL 个状态，$i=1,\cdots,k;\ j=1,\cdots,L$。每一状态以 A 为行空间。由于 A 是奇异的，行空间最多含有 $2^{m-1}-1$ 个非零元素。如 $kL\geq 2^{m-1}$，

信格原理表明其中两个状态一定相等，也就是说 $b_iA^s = b_jA^t$, $(\max(s,t) \le L)$, 于是由定理 5，知 $d_2 \le (L+1)r$，取 $L = \lceil 2^{m-1}/k \rceil$，可得定理 6。　　证毕

推论 2　若矩阵 A 是奇异的，则有 $d_2 \le 2r + \lfloor (2^{m-1}r)/k \rfloor$。

定理 7　设 A 是非奇异且非降幂的 $m \times m$ 矩阵，特征多项式为 $Q(D) = 1 - q_1D - \cdots - q_mD^m$，而 b 和 c 为任意 m 维矢量，则有理函数 $F_b(D) = b(I_m - DA)^{-1}c$ 具有 $P_{b,c}(D)/Q(D)$ 的形式。其中 $P_{b,c}(D)$ 为小于 $m-1$ 阶的多项式。$P_{b,c}(D)$ 的常数项为 bc, D^{m-1} 的系数为 $q_mbA^{-1}c$。

4 d_2 上限的证明

从推论 1 知，对 (r,k,m) 卷积码有

$$d_2 \le \lceil 2^m/k \rceil r \tag{7}$$

当 A 为非奇异时，由定理 5 可得

$$d_2 \le 2r + \lfloor (2^{m-1}r)/k \rfloor \tag{8}$$

由推论 2 可知，A 为奇异时，(7) 式同样成立，因此对任意 (r,k,m) 卷积码，(7) 式和 (8) 式都是成立的。这就证明了定理 1。

注意到当 $k=1$ 时，(4) 式是 (3) 式中的第二项因子，因此 (4) 式的等式成立必须有 $\lceil 2^m/k \rceil r \ge 2r + \lfloor 2^{m-1}r/k \rfloor$。因 $k=1$，上式可简化为 $2^{m-1} \ge 2$, 即 $m \ge 2$。

由定理 6 可知，$k=1$ 时，有 $d_2 \le (1+2^{m-1}) \cdot r$。这说明如 $d_2 = (2+2^{m-1}) \cdot r$，反馈矩阵一定是非奇异的。也可以说，对 $(r,1,m)$ 卷积码，使 $d_2 = (2+2^{m-1}) \cdot r$ 的必要条件是 $m \ge 2$ 和 A 是非奇异的。

由定理 3 选定输入序列码重为 2 的路径，即满足

$$b_iA^{t_i} = b_jA^{t_j} \tag{9}$$

其中 b_i 和 b_j 为 B 的行矢量。当 $k=1$ 时，B 成为一行向量，这里用 b 表示。由于 A 是非奇异的，所以 (9) 式可简化为

$$bA^t = b \tag{10}$$

如 t 是使 (10) 式成立的最小正整数，则相应的码径为

$$s_0 = \mathbf{0} \xrightarrow[d]{1} b \xrightarrow[bC]{0} bA \xrightarrow[bAC]{0} \cdots \xrightarrow[bA^{t-2}C]{0} bA^{t-1} \xrightarrow[bA^{t-1}C+d]{1} \mathbf{0}$$

该码径的输出重量为 $d_2 = |d| + |bA^{t-1}C+d| + |bC| + |bAC| + \cdots + |bA^{t-2}C|$。因 d 和 $bA^{t-1}C+d$ 都为 r 维矢量，这样有 $|d| + |bA^{t-1}C+d| \le 2r$。由于 $bC, bAC, \cdots, bA^{t-2}C$ 为零输入支路上的输出符号，从引理 1 知：$|bC| + |bAC| + \cdots + |bA^{t-2}C| \le 2^{m-1}r$。因此，当且仅当

$$\left.\begin{aligned} &d = (1,1,\cdots,1) \\ &bA^{t-1}C = (0,0,\cdots,0) \\ &|bC| + |bAC| + \cdots + |bA^{t-2}C| + |bA^{t-1}C| = 2^{m-1}r \end{aligned}\right\} \tag{11}$$

时，有 $d_2 = (2+2^{m-1})r$。

由矩阵 A、B、C 和 D 所定义的卷积码生成矩阵为

$$G(D) = b \times [D^{-1}I_m - A]^{-1} \times [c_1, \cdots, c_r] + [1, \cdots, 1] \tag{12}$$

由定理 7 和 $[D^{-1}I_m - A]^{-1} = D[I_m - DA]^{-1}$, $G(D)$ 有如下形式:

$$G(D) = \left(\frac{P_1(D)}{Q(D)}, \cdots, \frac{P_r(D)}{Q(D)}\right),$$

其中 $Q(D)$ 为 m 阶本原多项式 (也就是 A 的特征多项式) 。 $P_j(D) = DP'_j(D) + Q(D)$ ，而 $P'_j(D)$ 为小于或等于 $m-1$ 阶多项式。由定理 7 可知， $P'_j(D)$ 的 D^{m-1} 系数为 $q_m bA^{-1}c_j = 0$ ，所以 $P_j(D)$ 一定为 m 阶多项式。由于 $DP'_j(D)$ 的常数项为 0 ， $Q(D)$ 的常数项为 1 ，从而 $P_j(D)$ 的常数项也为 1 。同时，由于 $b \neq 0$ 和 $c_j \neq 0$, $P'_j(D) \neq 0$ ，进而 $P_j(D) \neq Q(D)$ ，这样就证明了定理 2 。

5 结束语

在本文中对文献 [3] 所提出的 Turbo 码有效自由距离的上限给出了证明。输入码重为 2 的输出码序列的最小距离，也即有效自由距离在很大程度上决定了 Turbo 码的性能。所以 d_2 能作为设计 Turbo 码的一个重要参数。设计 Turbo 码的任务之一就是对给定的存贮长度，找出最优的分量码。文献 [3] 给出了一些好的分量码。 Turbo 码的优良性能，目前大多数还是仿真结果，如何从理论上解释 Turbo 码的性能，还有许多研究工作。不过相信， Turbo 码可在各种恶劣条件下提供接近极限的通信能力，有望出现在未来的各种通信系统中。

参 考 文 献

[1] C. Berrou, A. Glavieux, P. Thitimasjshima, Near Shannon limit error-correcting coding and decoding, Turbo-codes(1), in Proc., IEEE Int. Conf. on Commun., Geneva, Switzerland, 1993, 1064–1070.

[2] S. Benedetto, G. Montorsi, Design of parallel concatenated convolutional codes, IEEE Trans. on Commun., 1996, 44(5), 591–600.

[3] D. Divsalar, R. J. McEliece, Effective free distance of turbo codes, Electron. Lett., 1996, 32(2), 445–446.

THE PROOF OF UPPER BOUNDS OF EFFECTIVE FREE DISTANCE FOR TURBO CODE

Chen Xianguang Wang Jin

(*PLA Quangzhou Communication Institute, Guangzhou* 510502, China)

Abstract Turbo code is a new class of error correcting and achieves almost reliable communication when SNR is very close to the Shannon-Limit. Turbo encoder consists of a parallel concatenation of two or more convolutional codes and interleaver. A new parameter effective free distance d_2 was proposed by S. Benedetto and G. Montorsi(1996) and two upper bounds on d_2 were stated without proof by D. Divsalar and R. J. McEliece (1996). This paper proofs the two upper bounds on d_2.

Key words Turbo codes, Concatenated codes, Channel coding

陈献光: 男， 1959 年生，讲师，研究兴趣为信号处理、微波通信等.

王 进: 男， 1962 年生，博士、副教授，研究兴趣为信道编码、扩频通信等.