关于等重码不可检错误概率的界

夏树涛, 江 勇
(清华大学深圳研究生院, 广东深圳 518055)

摘 要: 本文研究了二元等重码不可检错误概率 (UEP)的界. 首先, 我们通过研究二元等重码的对偶距离分布及其性质, 给出二元等重码 UEP的一个新的下界, 该下界改进了 Fu-Klöve-Wei的最新结果; 然后, 我们指出 2003年 Fu-Klöve-Wei关于二元等重码 UEP上界的某些结果有错误, 我们随后给出更正后的结果, 即二元等重码 UEP的平均值和一个上界.

关键词: 二元等重码; 不可检错误概率 (UEP); 距离分布; 对偶距离分布
中图分类号: TN911.2 文献标识码: A 文章编号: 0372-2112 (2006) 05-0944-03

Bounds of Undetected Error Probability for Binary Constant Weight Codes

XIA Shu-tao, JIANG Yong
(Graduate School at Shenzhen, Tsinghua University, Shenzhen, Guangdong 518055, China)

Abstract Bounds of undetected error probability (UEP) for binary constant weight codes (BCWCs) are studied in this paper. Firstly, by using the dual distance distribution and its properties for BCWC, we obtain a new lower bound of UEP for BCWC which improves the best known corresponding results by Fu-Klöve-Wei. We point out that there are mistakes in results of Fu-Klöve-Wei in 2003 which discussed the upper bounds, and a new upper bound of UEP for BCWC are obtained.

Key words binary constant weight codes; undetected error probability (UEP); distance distribution; dual distance distribution

1 引言

在自动重复请求(ARQ)差错控制系统中, 检错码的不可检错误概率 (UEP)是最重要的性能指标之一. 二元等重码在编码理论中占有重要地位, 被广泛应用于各种数字通信系统. 关于二元等重码的不可检错误概率, 目前已有一些研究 (参见文[1~4]), 其中文[4]是近年来比较重要的一篇论文.

令 $V_n=\{0,1\}^n$ 是二元 n维向量空间, $d_H(\cdot,\cdot)$表示向量之间的 (Hamming) 距离, $\omega_H(\cdot)$表示向量的 (Hamming)重量. 设 $C\subseteq V_n$ 是一个二元 (n,M)码, C 的距离分布 A_i和对偶距离分布 B_i定义为: 对 $i=0,1,\cdots,n$,

$$A_i=\frac{1}{M}\left|\{(a,b)\mid a,b\in C, d_H(a,b)=i\}\right| \tag{1}$$

$$B_i=\frac{1}{M^2}\sum_{u\in V_n}\left[\sum_{c\in C}(-1)^{\langle u,c\rangle}\right]^2 \tag{2}$$

其中$\langle\cdot,\cdot\rangle$表示向量之间的内积. 在二元对称信道 (BSC)中, 设误码率为 p ($0\leqslant p\leqslant 1/2$), 由文[1]或文[4]知, C作为一个检错码其 UEP为:

$$\begin{aligned}P_{ue}(C,p)&=\frac{1}{M}\sum_{a\in C}\sum_{\substack{b\in C\\ b\neq a}}p^{d_H(a,b)}(1-p)^{n-d_H(a,b)}\\&=\sum_{i=1}^{n}A_ip^i(1-p)^{n-i}\\&=\frac{M}{2^n}\sum_{i=0}^{n}B_i(1-2p)^i-(1-p)^n\end{aligned} \tag{3}$$

令 $V_{n,\omega}$为 V_n中所有重量为 ω的向量的集合, $V_{n,\omega}$的包含 M个元的子集称为二元 (n,M,ω)等重码. 从现在开始, 我们假定 C是一个二元 (n,M,ω)等重码, 下面的结果来自文[4]定理 7.

定理 1[4] 若 C为一个二元 (n,M,ω)等重码, 则

$$P_{ue}(C,p)\geqslant\frac{M}{\binom{n}{\omega}}\left[\sum_{i=1}^{\omega}\binom{\omega}{i}\binom{n-\omega}{i}p^{2i}(1-p)^{n-2i}\right]-\left[1-\frac{M}{\binom{n}{\omega}}\right](1-p)^n \tag{4}$$

2 一个改进的下界

设 $\omega\leqslant n/2$, 易知 $V_{n,\omega}$的距离分布和 UEP分别为

收稿日期: 2004-03-08; 修回日期: 2006-02-06
基金项目: 国家自然科学基金 (No. 60402031, No. 60503053); 广东省自然科学基金 (No. 34308)

$D_j = \binom{\omega}{i}\binom{n-\omega}{i}$, 若 $j = 2i$ 且 $i = 0, 1, \cdots, \omega$; $D_j = 0$ 对其他 j.

(5)

$$P_{ue}(V_{n,\omega}, p) = \sum_{i=1}^{\omega}\binom{\omega}{i}\binom{n-\omega}{i}p^{2i}(1-p)^{n-2i} \quad (6)$$

由文[3]知, $V_{n,\omega}$的对偶距离分布为 $D_i = [K_i(\omega)]^2\binom{n}{i}$, $i = 0, 1, \cdots, n$, 其中 $K_\omega(x)$为 Krawtchouk 多项式, 由下式给出:

$$K_\omega(x) = \sum_{j=0}^{\omega}(-1)^j\binom{x}{j}\binom{n-x}{\omega-j} \quad (7)$$

设 C是一个二元(n, M, ω)等重码, 其中 $\omega \leqslant n/2$, 令 A_k和 B_k为 C的距离分布和对偶距离分布, 由非线性码的 MacWilliams恒等式知(参见文[5]),

$$B_k = \frac{1}{M}\sum_{i=0}^{n}K_k(i)A_i, \quad A_k = \frac{M}{2^n}\sum_{i=0}^{n}K_k(i)B_i, \quad k = 0, 1, \cdots, n$$

(8)

由 C的等重特性易知, $A_i = 0$若 i为奇数或 $i > 2\omega$, 结合式(7)得,

$$B_k = \frac{1}{M}\sum_{i=0}^{\omega}K_k(2i)A_{2i} = \frac{1}{M}\sum_{i=0}^{\omega}K_{n-k}(2i)A_{2i} = B_{n-k} \quad (9)$$

引理 1[5]　$B_k \geqslant 0$, $B_0 = 1$, $\sum_{k=0}^{n}B_k = 2^n/M$. 特别地, $\sum_{k=0}^{n}D_k = 2^n\binom{n}{\omega}$.

引理 2[4]　$B_k \geqslant D_k = [K_k(\omega)]^2\binom{n}{k}$. 特别地, $B_1 \geqslant D_1 = (n-2\omega)^2/n$.

由式(3)和引理 1得,

$$\begin{aligned}P_{ue}(C, p) &= \frac{M}{2^n}\Big[\sum_{i=0}^{n}B_i(1-2p)^i\Big] - (1-p)^n\\ &= \frac{M}{2^n}\Big\{\sum_{i=0}^{n}B_i[(1-2p)^i - (1-2p)^{n-1}] + \frac{2^n}{M}(1-2p)^{n-1}\Big\} - (1-p)^n.\end{aligned}$$

由引理 1和式(9)知, $B_n = B_0 = 1 = D_0 = D_n$. 又因为 $B_i \geqslant D_i$(引理 2)和 $(1-2p)^i - (1-2p)^{n-1} \geqslant 0$, $i = 0, 1, \cdots, n-2$, 所以

$$\begin{aligned}P_{ue}(C, p) &\geqslant \frac{M}{2^n}\Big\{\sum_{i=0}^{n}D_i[(1-2p)^i - (1-2p)^{n-1}] + \frac{2^n}{M}(1-2p)^{n-1}\Big\} - (1-p)^n\\ &= \frac{M}{2^n}\Big[\sum_{i=0}^{n}D_i(1-2p)^i - \frac{2^n}{\binom{n}{\omega}}(1-2p)^{n-1} + \frac{2^n}{M}(1-2p)^{n-1}\Big] - (1-p)^n\\ &= \frac{M}{\binom{n}{\omega}}\Big[\frac{\binom{n}{\omega}}{2^n}\sum_{i=0}^{n}D_i(1-2p)^i - (1-p)^n\Big] - \Big[1-\frac{M}{\binom{n}{\omega}}\Big](1-p)^n + \Big[1-\frac{M}{\binom{n}{\omega}}\Big](1-2p)^{n-1}\\ &\xlongequal{(3)} \frac{M}{\binom{n}{\omega}}P_{ue}(V_{n,\omega}, p) - \Big[1-\frac{M}{\binom{n}{\omega}}\Big](1-p)^n + \Big[1-\frac{M}{\binom{n}{\omega}}\Big](1-2p)^{n-1}\\ &\xlongequal{(6)} \frac{M}{\binom{n}{\omega}}\Big[\sum_{i=1}^{\omega}\binom{\omega}{i}\binom{n-\omega}{i}p^{2i}(1-p)^{n-2i}\Big] + \Big[1-\frac{M}{\binom{n}{\omega}}\Big][(1-2p)^{n-1} - (1-p)^n].\end{aligned}$$

因此, 我们得到以下定理.

定理 2　设 C是一个二元(n, M, ω)等重码, 则

$$P_{ue}(C, p) \geqslant \frac{M}{\binom{n}{\omega}}\Big[\sum_{i=1}^{\omega}\binom{\omega}{i}\binom{n-\omega}{i}p^{2i}(1-p)^{n-2i}\Big] + \Big[1-\frac{M}{\binom{n}{\omega}}\Big][(1-2p)^{n-1} - (1-p)^n]$$

与定理 1的下界比较, 易知定理 2的下界改进值为 $\Big[1-\frac{M}{\binom{n}{\omega}}\Big](1-2p)^{n-1}$, 所以定理 2的结果优于定理 1. 下面, 我们用文[4]中的例子比较一下.

设 $C_1 = \{(110), (101)\}$, 则 $n = 3$, $\omega = 2$, $M = 2$

定理 1下界: $\frac{4}{3}p^2(1-p) - \frac{1}{3}(1-p)^3$,

定理 2下界: $\frac{4}{3}p^2(1-p) - \frac{1}{3}(1-p)^3 + \frac{1}{3}(1-2p)^2$.

设 $C_2 = \{(11000), (01100), (00110), (00011)\}$, 则 $n = 5$, $\omega = 2$, $M = 4$

定理 1下界: $\frac{12}{5}p^2(1-p)^3 + \frac{6}{5}p^4(1-p) - \frac{3}{5}(1-p)^5$,

定理 2下界: $\frac{12}{5}p^2(1-p)^3 + \frac{6}{5}p^4(1-p) - \frac{3}{5}(1-p)^5 + \frac{3}{5}(1-2p)^4$.

3 一个上界

设 $P_{ue}(n, M, \omega, p)$表示所有二元(n, M, ω)等重码的$P_{ue}(C, p)$的最小值, $\mathscr{C}(n, M, \omega)$为所有二元$(n, M, \omega)$等重码的集合, $\mathscr{C}(n, M, \omega)$中码的平均不可检错误概率为

$$\bar{P}_{ue}(n, M, \omega, p) = \frac{1}{|\mathscr{C}(n, M, \omega)|} \sum_{C \in C(n, M, \omega)} P_{ue}(C, p)$$

文[4]定理 5给出

$$\bar{P}_{ue}(n, M, \omega, p) = \frac{(M-1)\binom{n}{\omega}}{\left[\binom{n}{\omega} - M + 1\right]\left[\binom{n}{\omega} - M + 2\right]} \cdot \sum_{i=1}^{\omega} \binom{\omega}{i}\binom{n-\omega}{i} p^{2i}(1-p)^{n-2i} \quad (10)$$

由式(10)和 $P_{ue}(n, M, \omega, p) \leqslant \bar{P}_{ue}(n, M, \omega, p)$可得文[4]推论 3,即

$$P_{ue}(n, M, \omega, p) \leqslant \frac{(M-1)\binom{n}{\omega}}{\left[\binom{n}{\omega} - M + 1\right]\left[\binom{n}{\omega} - M + 2\right]} \cdot \sum_{i=1}^{\omega} \binom{\omega}{i}\binom{n-\omega}{i} p^{2i}(1-p)^{n-2i} \quad (11)$$

上述文[4]中的结果包含错误, 理由如下: 令 $M = \binom{n}{\omega}$, 易知 $\mathscr{C}(n, M, \omega)$只包含一个码 $V_{n,\omega}$, 而且有

$$P_{ue}(V_{n,\omega}, p) = \bar{P}_{ue}(V_{n,\omega}, p) = \sum_{i=1}^{\omega} \binom{\omega}{i}\binom{n-\omega}{i} p^{2i}(1-p)^{n-2i} \quad (12)$$

显然式(10)与(12)矛盾. 事实上, 仔细分析文[4]定理 5的证明不难知道,

$$\binom{\binom{n}{\omega}}{M-2} \text{ 应该更正为 } \binom{\binom{n}{\omega} - 2}{M-2},$$

因此, 与文[4]定理 5和推论 3对应, 我们有以下结果:

定理 3

$$\bar{P}_{ue}(n, M, \omega, p) = \frac{M-1}{\binom{n}{\omega} - 1} \sum_{i=1}^{\omega} \binom{\omega}{i}\binom{n-\omega}{i} p^{2i}(1-p)^{n-2i}$$

推论 1

$$P_{ue}(n, M, \omega, p) \leqslant \frac{M-1}{\binom{n}{\omega} - 1} \sum_{i=1}^{\omega} \binom{\omega}{i}\binom{n-\omega}{i} p^{2i}(1-p)^{n-2i}$$

本文研究了二元等重码 UEP的界. 首先, 我们通过研究二元重码的对偶距离分布及其性质, 得到了 $P_{ue}(C, p)$的一个新的下界, 该下界改进了文[4]的相应结果; 然后, 我们指出文[4]在讨论 $P_{ue}(C, p)$的上界时其某些结论有错误, 我们随后给出了更正后的结果.

参考文献:

[1] Wang X M, Yang Y X. On the undetected error probability of nonlinear binary constant weight codes[J]. IEEE Trans Commu, 1994, 42(7): 2390-2394

[2] Fu F W, Xia S T. Binary nonlinear constant weight codes for error detection[J]. IEEE Trans Inform. Theory, 1998, 44(3): 1294-1299.

[3] Fu F W, Klφve T, Xia S T. On the undetected error probability of m-out-of-n codes on the binary symmetric channel [A]. Buchmann R J, *et al* Coding Theory, Cryptography and Relate Fields[C]. Springer-Verlag, 2000. 102-110.

[4] Fu F W, Klφve T, Wei V K. On the undetected error probability for binary codes[J]. IEEE Trans Inform. Theory, 2003, 49(2): 382-390.

[5] MadWilliams F J, Sloane N J A. The Theory of Error-correcting Codes[M]. New York: North-Holland, 1977.

作者简介:

夏树涛 男, 1972年出生于黑龙江省, 1997年毕业于南开大学数学学院, 获理学博士学位. 1997年 9月 ~ 1998年 9月期间在香港中文大学讯息工程系作访问学者, 现为清华大学深圳研究生院信息学部副教授, 主要从事信道编码和网络安全等方向的教学与科研工作, 目前负责或参加国家自然科学基金、973等多项课题, 在国内外学术期刊及国际会议上发表学术论文题 20余篇.

E-mail: xiasf@sz.tsinghua.edu.cn

江 勇 男, 1975年出生于四川省, 2002年毕业于清华大学计算机系, 获工学博士学位. 现为清华大学深圳研究生院信息学部副教授, 研究方向为计算机网络及其应用技术, 目前负责或参加国家自然科学基金、973等多项课题, 在国内外学术刊物和学术会议上发表论文 30余篇.