线性拟等重码的检错性能*

王开弘
(重庆师范大学 数学与计算机科学学院,重庆 400047)

摘 要:线性拟等重码是一类特殊的等重码,文中利用码等价和线性拟等重与一阶R-M码的关系研究了线性拟等重码的检错性能;并证明了一类特殊的二元线性拟等重码是最佳检错码,并因此得出延长Hamming码是最佳检错码。

关键词:拟等重码;码的等价;一阶R-M码;延长Hamming码;最佳检错码
中图分类号:O157.4 **文献标识码**:A **文章编号**:1004-5694(2003)04-0061-03

Error-detecting capability for quasi-constant weight codes

WANG Kai-hong
(*Department of Mathematics & Computer Science, Chongqing Normal University, Chongqing* 400047, *P. R. China*)

Abstract: Linear quasi-constant weight code is a class of constant weight code. In this paper, the author used the point of equivalence and the first order R-M codes to prove linear codes property for error detection, and then gave the error capability of extensive Hamming codes by making use of the point of equivalence and some known results.

Key words: quasi-constant weight codes; equivalence of codes; first order R-M codes; extend Hamming codes; proper codes for error detection

0 引 言

在重传反馈差错控制通信系统中,码的不可检错概率是衡量通信系统好坏的一个重要性能指标。设C是长为n的二元码,当一个码字$a\in C$通过二元对称信道(BSC)传输,由于噪音使码字a变成C中的另一个码字b。这种情况,译码器就不能发生这种错误,从而出现不可检错概率。等重码在编码理论中占有重要地位,它在信息的传输和存储系统中有着广泛的应用。等重码的结构问题与组合学中的许多难题和猜想相联系,文献[1]研究了线性拟等重码,认为线性拟等重码具有与线性等重码相似的特殊线性码的结构,因此计算线性拟等重码的不可检错概率,有它的实际意义和理论意义。

1 预备知识

定义1 设C为二元$[n,k,d]$线性码,将C的2^k个码字按某种顺序排成2^k行,构成一个二元$2^k\times n$阶矩阵$\boldsymbol{A}$,称此矩阵$\boldsymbol{A}$为码C的码矩阵。

定义2 如果$\boldsymbol{A}$是二元线性$[n,k,d]$码C的码矩阵,如果$\boldsymbol{A}$的列向量不为零向量,并且两两不同,则称C为正则线性码。

定义3 在二元$[n,k]$线性码C中,如果$0\in C$和$1\in C$,且C中除0和1,外所有码字的重量为d,则称C为$[n,k,d]$线性弱等重量码。

定义4 在二元$[n,k]$线性码C中,如果$1\in C$,并

* 收稿日期:2002-12-26 修订日期:2003-02-27
基金项目:重庆市教委科研基金(960384)
作者简介:王开弘(1978-),女,四川双流人,硕士研究生,主要从事组合最优化、编码理论研究。

且C中除0和1外，所有码字的重量为d或n-d，则称C为$[n,k,d]$线性拟等重码。

定义5 设A_1和A_2分别是C_1和C_2的码矩阵，如果存在置换矩阵P和Q使得$A_1=PA_2Q$，那么C_1等价于C_2。

定义6 在二元对称信道中，设误码率为p，则一个二元$[n,k]$线性码的平均不可检错概率

$$p_e(p)=\sum_{i=1}^{n}A_i p^i(1-p)^{n-i}$$

其中$\{A_i\}_{i=1}^{n}$为码C的重量分布。

定义7 在二元$[n,k]$线性码C中，若任意的$0\leqslant p\leqslant 0.5$，$\frac{\mathrm{d}p_e(p)}{\mathrm{d}p}\geqslant 0$，则$C$为最佳检错码。

2 本文的主要结果

引理1 设C为$[n,k]$线性码，B_i表示重量为i的个数，$\{B_i\}_{i=1}^{n}$为码C的对偶码$C^{\perp}$的重量分布，则C为正则线性码的充要条件是$B_1=0$和$B_2=0$。

证明 先证必要性(⇒)：由于C为正则线性码，则C的码矩阵的列向量不为零向量，且两两不同，则从C的码矩阵找出一个$k\times n$阶矩阵，此子矩阵为线性码C的生成矩阵G，故G的列向量也不为零。否则，由于码C的码矩阵是由G生成的，若G有一列向量为零，则C的码矩阵必有一列向量为零，这与已知矛盾。G中也无两两相同的列，否则C的码矩阵将有两两相同的列，而由于C的生成矩阵是其对偶码$C^{\perp}$的一致校验矩阵，故C的对偶码$C^{\perp}$的一致校验矩阵的列向量不为零向量，且两两不同，则C的最小距离>2，故C的最小重量$\geqslant 3$，从而$B_1=0$；$B_2=0$。

再证充分性(⇐)：由于$B_1=0$；$B_2=0$，则C的对偶码$C^{\perp}$的最小重量不小于3，则$C^{\perp}$的最小距离大于2，故对偶码$C^{\perp}$的一致校验矩阵H列向量中无零向量，且两两不同，即$(C^{\perp})^{\perp}=C$的生成矩阵列向量无零向量，且两两不同，则C的码矩阵也无零向量，且两两不同，由定义2知，C为正则码。

引理2 若C_1和C_2为线性码，A_1和A_2分别是C_1和C_2的码矩阵，且C_1等价于C_2，则C_1和C_2的重量分布相同。

证明 由于C_1等价于C_2，则存在置换矩阵P和Q使$A_1=PA_2Q$，也就是经过适当的行或列置换之后，可以将C_2变为C_1，而对于A_2的任意一行(即C_2的任意一个码字)进行置换时，其中码元为1的个数并未改变，即每个码字C的重量未变；又由于A_2进行列置换时，对于A_2的任意一列码元的1的个数也未改变，即对A_2列置换时，C_2中每一码字的重量未变，C_1和C_2均为线性码，则相同重量的码字数也未变，即C_1和C_2的重量分布相同。

注 在一些文献中，有类似引理1和引理2的结果，但本文中证法与其它文献不同。

定理1 C_1和C_2是线性码，若C_1和C_2等价，则C_1和C_2的不可检错概率相同。

证明 因为C_1和C_2等价，则由引理2可知：C_1和C_2的重量分布相同；由定义6可知：C_1和C_2不可检错概率相同。

推论1 C_1和C_2是线性码，且C_1和C_2等价，若C_1是检错好码，则C_2也是检错好码。

引理3[1] 若C为二元正则$[n,k,d]$线性弱等重码，则C等价于一阶R-M码RM$(k-1,1)$

引理4[2] 若C是检错好码，则$C^{\perp}$也是检错好码。

引理5 C为二元$[n,k]$线性码，$\{A_i\}_{i=1}^{n}$和$\{B_i\}_{i=1}^{n}$分别为C和$C^{\perp}$的重量分布，则

$$\sum_{i=1}^{n}iA_i=2^{k-1}(n-B_1)$$

定理2 设C为$[n,k]$正则线性码，且C的重量为偶数，则C是最佳检错码。

证明 由于码C是偶重码，则可设重量分布为$\{A_{2i}\}_{i=0}^{[n/2]}$，又由于C是$[n,k]$正则线性码，则C的对偶码中没有重量为1的码，故$B_1=0$。由引理5可知：

$$\sum_{i=0}^{[n/2]}2iA_{2i}=2^{k-1}n$$

码C的不可检错概率为：

$$p_e(p)=\sum_{i=1}^{[n/2]}A_{2i}p^{2i}(1-p)^{n-2i}$$

$$f(p)\triangleq\frac{\mathrm{d}p_e(p)}{\mathrm{d}p}=\sum_{i=1}^{[n/2]}A_{2i}[2ip^{2i-1}(1-p)^{n-2i}-(n-2i)p^{2i}(1-p)^{n-2i-1}]=$$

$$\sum_{i=1}^{[n/2]}A_{2i}p^{2i-1}(1-p)^{n-2i-1}[2i(1-p)-(n-2i)p]=$$

$$\sum_{i=1}^{[n/2]}A_{2i}\left(\frac{p}{1-p}\right)^{2i-1}(1-p)^{n-2}(2i-np)=$$

$$(1-p)^{n-2}\sum_{i=1}^{[n/2]}A_{2i}\left(\frac{p}{1-p}\right)^{2i-1}(2i-np)$$

当 $p=1/2$ 时,则

$$f(\frac{1}{2})=(\frac{1}{2})^{n-2}\sum_{i=1}^{[n/2]}A_{2i}(2i-\frac{1}{2}n)=$$

$$(\frac{1}{2})^{n-2}\sum_{i=1}^{[n/2]}2iA_{2i}-(\sum_{i=1}^{[n/2]}A_{2i}\frac{1}{2}n)=$$

$$(\frac{1}{2})^{n-2}[2^{k-1}n-\frac{1}{2}(2^k-1)]=$$

$$(\frac{1}{2})^{n-2}[2^{k-1}(n-1)+\frac{1}{2}]>0$$

当 $0\leqslant p\leqslant 1/2$ 时,容易验证 $f(p)$ 为减函数,从而

$$f(p)\underset{=}{\Delta}\frac{\mathrm{d}p_e(p)}{\mathrm{d}p}>0$$

从而 C 为最佳检错码。

推论 2 延长 Hamming 码是最佳检错码。

证明 根据延长 Hamming 码的定义可知延长 Hamming 码是偶重码,且一阶 R-M 码 RM(m,r),$m>r+1$ 的最小距离为 $2^{m-r}>2$,故延长 Hamming 码是正则线性码。由定理 2 可知:延长 Hamming 是最佳检错码。

注 此结论和文献[3]中的结论相同,但本文证法不同。

定理 3 C 为二元正则$[n,k,d]$线性弱等重码,则 C 为最佳检错码。

证明 由于延长 Hamming 码是最佳检错码,又因为一阶 R-M 码 RM$(k-1,1)$是延长 Hamming 码的对偶码,由引理 4 可知:一阶 R-M 码是最佳检错码,又由引理 3 可知,C 也是最佳检错码。

引理 6[1] 设 C 为二元正则$[n,k]$线性拟等重码,$n\neq 2d$,如果 $2^{k-1}-1$ 为素数,则 C 等价于一阶 R-M 码 RM$(k-1,1)$删除第一个分量后得可到线性码 RM$^*(k-1,1)$。

引理 7[2] 一阶 R-M 码 RM$(k-1,1)$删除第一个分量后得到的线性码 RM$^*(k-1,1)$是最佳检错码。

定理 C 为二元正则$[n,k,d]$线性等重码,$n\neq 2d$ 且 $2^{k-1}-1$ 为素数,则 C 为最佳检错码。

证明 由引理 6,7 及推论 1 就能得出结论。

3 结束语

本文证明了一类线性码是最佳检错码,并利用等价的观点研究了一类特殊的线性码——线性拟等重码的不可检错概率。由于线性拟等重码的特殊结构,我们可直接用它的重量分布,计算出它的不可检错概率,但本文意在用等价的观点得出线性拟等重码是最佳检错码。从而得出一些关于线性码等价的一些结果,同样我们可以用此等价的观点推广到非线性等重码上去。但一些不能确定是否是最佳检错码的等重码,如非线性等重码(24,6,12);(38,8,17);(40,10,20);(13,4,6);(14,4,7)等码[4,5],还有待于进一步研究。

参考文献:

[1] 符方伟,沈世镒. 线性拟等重码的结构分析[J]. 电子学报,1997,25(1) :114-116.

[2] 杨义先,林须端. 编码密码学[M]. 北京:北京邮电大学出版社,1992.

[3] WOLF J K. MICHELSON A H. On the probability of undetected error for linear block codes[J]. IEEE Trans on Com,1982,30(2):317-324.

[4] 符方伟,夏树涛. 二元非线性等重码的检错性能[J],科学通报, 1997 ,42(4):343-347.

[5] 罗文俊. 二元非线性等重码的检错性能[J],科学通报,2000,45(13):1441-1446.

[6] 谢安国,邓小艳,吉庆兵. 非线性等重检错好码的存在性的进一步分析[J]. 重庆邮电学院学报(自然科学版),2002,14(3):44-47.

(编辑:龙能芬)