国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第12卷第4期 1990年12月 Vol.12 No.4

最佳(n,2,w)二进制等重检错码的研究

肖 戎
(电子技术系)

摘 要 本文研究了最佳$(n,2,w)$二进制等重检错码的存在性问题。对于文[5]中n为偶数时所得的结论，本文给了一个简练的证明。更为重要的是，利用以上方法，作者证明了文[5]中关于n为奇数时的一个猜想。

关键词 编码，检错码，等重码
分类号 O157.4

在数字通信中，有时使用“n中取w码”作为差错控制系统中的检错码。“n中取w码”即为码长为n，每个码字的重量都为w，码字之间的最小距离为2的$(n,2,w)$码，也即二进制等重码。例如，在国内，常采用(5,2,2)码或其对偶码——(5,2,3)码。而在国际上，也常使用(7,2,3)码，(8,2,4)码或它们的对偶码。显然，这些检错码的检错性能与效率依赖于这些码的不可检错误概率，因而，如何分析这些码的不可检错误概率就是一个无论从编码学理论或从实际角度来看，都是具有重要意义的问题。

最佳检错码的存在性即是与码的不可检错误概率密切联系的一个极为重要的问题。

在二进制对称信道中，误码率$p_e \leqslant 0.5$.当$p_e=0.5$时，则信道不能传送任何信息。此时，无论发端发送任何码字，收端都以等概的形式接收所有可能错误图样中的任何一个。例如，若发端是发送$(n, 2, w)$码中的码字，则有2^n种可能的错误图样，而

1989年7月26日收稿

A Double Compression Method for Dot Matrix Graphics

Wan Liangjun
(Department of Computer Science)

Abstract

This paper describes a double compression method with characteristic block compression, and then Huffman block encoding for computer graphics in detail. The method has been implemented in the YHHT graphic software. It has been shown by applications that the method is highly efficient.

Key words computer graphics, coding, graph/dot matrix graphics, graphic compression, Huffman encoding

$(n,2,w)$码中共有$\binom{n}{w}$个码字。此时，收端译码器不能检测的错误概率为：$p_u(0.5)=2^{-n}\left(\binom{n}{w}-1\right)$。对误码率为$p_e$的二进制对称信道来说，从直觉来看，一般认为，不可检错误概率$p_u(p_e)$作为p_e的一个函数来说，应在$p_e=0.5$时达到最大值，即$p_u(p_e)\leqslant p_u(0.5)$,此处$p_e\leqslant 0.5$. 也即：当$p_e=0.5$时,具有最大的不可检错误概率。然而，事实并非如此。在文[2]中，已经证明了很多码，其中包括线性码、非线性码，它们的不可检错误概率$p_u(p_e)$随着p_e的增加，不仅不增加，反而减少。即$p_u(p_e)$并不是p_e的单调递增函数。因此，提出了以下概念：

在二进制对称信道中，误码率p_e在[0,0.5]区间内。若某一个二进制码，它的不可检错误概率$p_u(p_e)$是p_e的单调非降函数，则称此码为最佳二进制检错码。

对于给定的一个码，如何判定它是否为最佳检错码？或者说，如何判断某一类最佳检错码的存在性？这些都是迄今为止尚未完全解决的问题。近几年来，它们引起了国际、国内学者的注意。

在文[1]～[4]中，证明了绝大多数线性码,如循环码、BCH码等,除少数n个外均不是最佳检错码。文[5]证明了：在二进制对称信道的误码率$p_e\leqslant 0.5$的范围内，二进制恣性等重码是最佳检错码。对于非线性码，类似的结论不多见。在文[5]中，作者得到了以下结论：

定理 1　在二进制对称信道的误码率$p_e\leqslant 0.5$的范围内，二进制$(2b,2,w)$非线性等重码为最佳码的充分必要条件为$w=b$.

同时，对于n为奇数的情形，[5]中提出了以下猜想：

猜想　在定理1的同样条件下，二进制$(2b+1,2,w)$非线性等重码当$b\geqslant 4$时不是最佳码。

本文对定理1给出了证明，并利用这种方法，证明了上述猜想，即证明了：

定理 2　在二进制对称信道的误码率$p_e\leqslant 0.5$的范围内，二进制$(2b+1,2,w)$非线性等重码在$b\geqslant 4$时不是最佳码。

至此，$(n,2,w)$二进制非线性等重最佳码的存在性与判定问题即获解决。

1　定理1的证明

在给出定理1的证明之前，先证明一些引理：

引理 1　在(n,d,w)二进制等重码（无论线性或非线性）中，任意两码字间的距离均为偶数。

证明　任取码中的两个码字C_1,C_2,它们之间的距离$d(C_1,C_2)=\sum_{i=1}^{n} c_{1i}\oplus c_{2i}$，此式中$c_{ij}\in GF(2)$，它是码字$C_i$的第$j$个码元，$\oplus$表示模2和，$i=1,2$，$j=1,2,\cdots,n$.

将C_1,C_2中的码元一位一位地如下对应排列起来：

$$c_{11}\ c_{12}\ c_{13}\ \cdots\cdots\ c_{1n}$$
$$c_{21}\ c_{22}\ c_{23}\ \cdots\cdots\ c_{2n}$$

记C_1，C_2中恰有a个对应的码元，使得它们的码元值等于1，即$c_{1i_j}=c_{2i_j}=1$，$j=1,2,\cdots\cdots,a$. 由于C_1的重量为w，故C_1中恰好还有$w-a$个取值为1的码元对应着C_2中码元值等于0的码元。同理，C_2中恰好还有$w-a$个取值为1的码元对应着C_1中码元值等于0的码元。除此以外，C_1，C_2中对应的码元取值都为0.

因此，$d(C_1,C_2)=(w-a)+(w-a)=2(w-a)$，为偶数。即任意两码字$C_1$，$C_2$之间的距离等于偶数。（证毕）

由引理1知，(n,d,w)二进制等重码的最小距离d必为偶数，由此不难得到：

引理2[5] 在二进制$(n,2,w)$等重码中，经过误码率为p_e的二进制对称信道传输后，收端译码器的平均不可检码字错误概率为：

$$p_u(p_e)=\sum_{i=1}^{w}\binom{w}{i}\binom{n-w}{i}p_e^{2i}(1-p_e)^{n-2i}$$

显然，从最佳码的概念可知，一个码是最佳码的充分必要条件为：$\frac{dp_u}{dp_e}\geqslant 0$，此处$p_e\leqslant 0.5$，$\frac{dp_u}{dp_e}$表示$p_u$对$p_e$的导数。由此，结合引理2，可以证明引理3：

引理3[5] 在二进制对称信道的误码率$p_e\leqslant 0.5$的范围内，二进制非线性等重码$(n,2,w)$不是最佳码的充分必要条件为：$\sum_{i=1}^{w}\binom{w}{i}\binom{n-w}{i}(4i-n)<0$.

为证定理1，我们还需要证明引理4：

引理4 记$A_{b-1}=\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)$。若$A_{b-1}<0$，则对任何单调非递增的正值函数$f(i)$，必有：$\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)<0$.

证明 记$c=\left[\frac{b+1}{2}\right]$，此处$[\cdot]$表示整数部份。则易知：对$i\geqslant c$，有$4i-2b\geqslant 0$；对$i\leqslant c-1$，有$4i-2b<0$.

记$A=\sum_{i=1}^{c-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)$，$B=\sum_{i=c}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)$，易知，$A$的和式中每一项都小于0，$B$的和式中每一项都大于0，则$A+B=A_{b-1}$.

因为$f(i)$为i的单调非递增正值函数，故知：对$i\geqslant c$，有$f(i)\leqslant f(c)$；对$i\leqslant c-1$，有$f(i)\geqslant f(c-1)$。因此，必有：

对$b-1\geqslant i\geqslant c$，有：$(4i-2b)f(i)\leqslant(4i-2b)f(c)$；

对$c-1\geqslant i\geqslant 1$，有：$(4i-2b)f(i)\leqslant(4i-2b)f(c-1)$.

在以上两个不等式两边乘上$\binom{b-1}{i}\binom{b+1}{i}$，再分别对$i$取和，即得：

$$\sum_{i=c}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)\leqslant\sum_{i=c}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(c)=f(c)\cdot B$$

及 $\sum_{i=1}^{c-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)\leqslant\sum_{i=1}^{c-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(c-1)=f(c-1)\cdot A.$

将以上两个不等式相加，即得：

$$\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)\leqslant f(c)\cdot B+f(c-1)\cdot A.$$

再由于$f(i)$单调非递增，故$f(c)\leqslant f(c-1)$，并且$f(i)$为正值函数，故$f(c-1)>0$，故知：

$$f(c)\cdot B+f(c-1)\cdot A\leqslant f(c-1)\cdot B+f(c-1)\cdot A=f(c-1)\cdot A_{b-1}<0.$$

即得：$\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)<0.$　　（证毕）

定理1的证明　充分性的证明容易，可见文[5]。现证必要性。

由引理3即知，为证定理1的必要性，我们只需证明：

$$A_w=\sum_{i=1}^{w}\binom{w}{i}\binom{2b-w}{i}(4i-2b)<0，\text{对}1\leqslant w\leqslant b-1\text{成立。}\qquad(1)$$

为此，我们先证：

$$A_{b-1}=\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)<0\qquad\text{成立。}\qquad(2)$$

事实上，记 $a_i=\binom{b-1}{i}\binom{b+1}{i}(4i-2b)$　　(3)

故 $a_{b-i}=\binom{b-1}{b-i}\binom{b+1}{b-i}(4(b-i)-2b)=\binom{b-1}{i-1}\binom{b+1}{i+1}(2b-4i)$。再将组合恒等式

$$\binom{b-1}{i-1}=\binom{b-1}{i}\frac{i}{b-i},\quad\binom{b+1}{i+1}=\binom{b+1}{i}\frac{b+1-i}{i+1}$$

代入此式，得：

$$a_{b-i}=\binom{b-1}{i}\binom{b+1}{i}\frac{i(b+1-i)(2b-4i)}{(b+i)(i+1)}$$

$$=\binom{b-1}{i}\binom{b+1}{i}\left(1-\frac{b-2i}{(b-i)(i+1)}\right)(2b-4i)\qquad(4)$$

将(3)式中的和式分成两两一组，a_i与a_{b-i}成为一组，则有

$$A_{b-1}=(a_1+a_{b-1})+(a_2+a_{b-2})+\cdots\cdots+(a_{[\frac{b-1}{2}]}+a_{b-[\frac{b-1}{2}]})$$

由(3)式与(4)式，即得

$$a_i+a_{b-i}=\binom{b-1}{i}\binom{b+1}{i}\frac{(b-2i)(4i-2b)}{(b-i)(i+1)}$$

故有：

$$A_{b-1}=\sum_{i=1}^{[\frac{b-1}{2}]}(a_i+a_{b-i})=\sum_{i=1}^{[\frac{b-1}{2}]}\binom{b-1}{i}\binom{b+1}{i}\frac{(b-2i)(4i-2b)}{(b-i)(i+1)}$$

$$=-2\sum_{i=1}^{[\frac{b-1}{2}]}\binom{b-1}{i}\binom{b+1}{i}\frac{(b-2i)^2}{(b-i)(i+1)}$$

由于此和式中每项均为正，故上式小于0.故$A_{b-1}<0$，即(2)式得证。

下面证(1)式成立。

注意组合恒等式：

$$\binom{w}{i}=\binom{b-1}{i}\frac{(w+1-i)(w+2-i)\cdots\cdots(b-1-i)}{(w+1)(w+2)\cdots\cdots(b-1)},$$

$$\binom{2b-w}{i}=\binom{b+1}{i}\frac{(b+2)(b+3)\cdots\cdots(2b-w)}{(b+2-i)(b+3-i)\cdots\cdots(2b-w-i)},$$

将此两式相乘，即得：$\binom{w}{i}\binom{2b-w}{i}=\binom{b-1}{i}\binom{b+1}{i}g(i)$

$$g(i)=\frac{(w+1-i)(w+2-i)\cdots\cdots(b-1-i)\cdot(b+2)(b+3)\cdots\cdots(2b-w)}{(w+1)(w+2)\cdots\cdots(b-1)\cdot(b+2-i)(b+3-i)\cdots\cdots(2b-w-i)}$$

故
$$A_w=\sum_{i=1}^{w}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)g(i). \qquad (5)$$

若$w\leqslant\left[\frac{b-1}{2}\right]$，则对$1\leqslant i\leqslant w$，必有$4i-2b<0$，且因为对$1\leqslant i\leqslant w$，$g(i)>0$，故(5)式的和式中每一项都小于0，故$A_w<0$.

若$w>\left[\frac{b-1}{2}\right]$，令$f(i)=\begin{cases}g(i) & \text{对}1\leqslant i\leqslant w\\ g(w) & \text{对}w<i\leqslant b-1,\end{cases}$ 则易知$f(i)$为$[1,\ b-1]$区间上的单调非递增正值函数。由$f(i)$的定义及(5)式，故有

$$A_w=\sum_{i=1}^{w}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)$$

由于对$i\geqslant w$，必有$4i-2b>0$，且$f(i)$为正值函数，故有

$$\sum_{i=1}^{w}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)\leqslant\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)$$

即：$A_w\leqslant\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b+1}{i}(4i-2b)f(i)$

再由引理4及(2)式，即知此和式小于0，即得$A_w<0$.

综合以上两种情况，即证明了(1)式，即证明了定理1. (证毕)

2 定理2的证明

为证定理2，先证如下引理。

引理5 记 $B_{b-1}=\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4i-2b+1)$，$b\geqslant5$. 若$B_{b-1}<0$，则

$$\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1}<-2.$$

证明　记 $e=\left[\frac{2b-1}{4}\right]+1$，此处 $[\cdot]$ 为整数部份。则对 $1\leqslant j\leqslant e-1$，有 $4j-2b+1<0$；对 $e\leqslant j\leqslant b-1$，有 $4j-2b+1>0$.

记：$E=\sum_{j=1}^{e-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)$，$F=\sum_{j=e}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)$

故显然：E 中和式的每一项都小于 0，F 的和式中每项均大于 0．且由于 $\frac{1}{j+1}$ 为 j 的单调递减正函数，故易知：

$$\sum_{j=1}^{e-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1}\leqslant\sum_{j=1}^{e-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{e}=\frac{E}{e}$$

$$\sum_{j=e}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1}\leqslant\sum_{j=e}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{e+1}=\frac{F}{e+1}$$

由于 $b\geqslant 5$，故这两个不等式中至少有一个式子中的不等号成立。故将这两个不等式相加后，则得：

$$\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1}<\frac{E}{e}+\frac{F}{e+1}=\frac{e(E+F)+E}{e(e+1)}\qquad(6)$$

由于 $B_{b-1}<0$，且 B_{b-1} 显然为整数，故 $B_{b-1}\leqslant -1$．而 $B_{b-1}=E+F$，故 $E+F\leqslant -1$．又因为

$$e=\left[\frac{2b-1}{4}\right]+1,$$

$$E=\sum_{j=1}^{e-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)<\binom{b-1}{1}\binom{b}{1}(5-2b)=(b-1)(5-2b)b<-2e^2-e,$$

故由(6)式得知：

$$\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1}<\frac{-e-2e^2-e}{e(e+1)}=-2$$

即得引理 5 的结论。　　（证毕）

同引理 4，引理 5 的证明类似，我们可证得引理 6：

引理 6　记 $B_{b-1}=\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)$，$b\geqslant 5$．若 $B_{b-1}<0$，则：对任何单调非递增的正值函数 $f(i)$，必有：$\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)\cdot f(j)<0$.

证明　（略）。

还需要证明引理 7：

引理 7　记 $B_b=\sum_{i=1}^{b}\binom{b}{i}\binom{b+1}{i}(4i-2b-1)$，则对 $b\geqslant 4$，必有 $B_b<0$.

证明　我们对 b 用归纳法来证。

$b=4$ 时，$B_4=\sum_{i=1}^{4}\binom{4}{i}\binom{5}{i}(4i-9)=-4<0$

设$b-1$时成立，即$B_{b-1}=\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b}{i}(4i-2b+1)<0$ (7)

对 b 时：因$\binom{b}{i}=\binom{b-1}{i}+\binom{b-1}{i-1}$，$\binom{b+1}{i}=\binom{b}{i}+\binom{b}{i-1}$，

故有：

$$B_b=\sum_{i=1}^{b}\binom{b-1}{i}\binom{b}{i}(4i-2b-1)+\sum_{i=1}^{b}\binom{b-1}{i}\binom{b}{i-1}(4i-2b-1)$$
$$+\sum_{i=1}^{b}\binom{b-1}{i-1}\binom{b}{i}(4i-2b-1)+\sum_{i=1}^{b}\binom{b-1}{i-1}\binom{b}{i-1}(4i-2b-1) \quad (8)$$

(8)式右端第一个和式$=\sum_{i=1}^{b}\binom{b-1}{i}\binom{b}{i}(4i-2b+1-2)$

$$=\sum_{i=1}^{b}\binom{b-1}{i}\binom{b}{i}(4i-2b+1)-2\sum_{i=1}^{b}\binom{b-1}{i}\binom{b}{i}$$
$$=\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b}{i}(4i-2b+1)-2\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b}{i}$$
$$=B_{b-1}-2\sum_{i=1}^{b-1}\binom{b-1}{i}\binom{b}{i}$$

(8)式右端第四个和式$=\sum_{j=0}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+3)$

$$=\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+3)+3-2b$$
$$=\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1+2)+3-2b$$
$$=\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)+2\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}+3-2b$$
$$=B_{b-1}+2\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}+3-2b$$

把这两式代入(8)式，即得：

$$B_b=2B_{b-1}+3-2b+\sum_{i=1}^{b}\left(\binom{b-1}{i}\binom{b}{i-1}+\binom{b-1}{i-1}\binom{b}{i}\right)(4i-2b-1) \quad (9)$$

令$i=b-j$，则

(9)式右端的和式$=\sum_{j=0}^{b-1}\left(\binom{b-1}{b-j}\binom{b}{b-j-1}+\binom{b-1}{b-j-1}\binom{b}{b-j}\right)(2b-4j-1)$

$$=2b-1+\sum_{j=1}^{b-1}\left(\binom{b-1}{b-j}\binom{b}{b-j-1}\right.$$

$$+\binom{b-1}{b-j-1}\binom{b}{b-j}\Big)(2b-4j-1)$$

$$=2b-1+\sum_{j=1}^{b-1}\Big(\binom{b-1}{j-1}\binom{b}{j+1}+\binom{b-1}{j}\binom{b}{j}\Big)(2b-4j-1)$$

$$=2b-1+\sum_{j=1}^{b-1}\binom{b-1}{j-1}\binom{b}{j+1}(2b-4j-1)-B_{b-1}$$

故由(9)式，有：

$$B_b=B_{b-1}+2-\sum_{j=1}^{b-1}\binom{b-1}{j-1}\binom{b}{j+1}(4j-2b+1) \tag{10}$$

将$\binom{b-1}{j-1}\binom{b}{j+1}=\binom{b-1}{j}\binom{b}{j}\frac{j}{j+1}$代入(10)式，得：

$$B_b=B_{b-1}+2-\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}\Big(1-\frac{1}{j+1}\Big)(4j-2b+1)$$

$$=B_{b-1}+2-\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}(4j-2b+1)+\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1}$$

$$=2+\sum_{j=1}^{b-1}\binom{b-1}{j}\binom{b}{j}\frac{4j-2b+1}{j+1} \tag{11}$$

由归纳假设，知$B_{b-1}<0$，则由引理5知，(11)式中的和式小于－2．由于(11)式，得知$B_b<0$．故由归纳法原理知引理7得证。

定理2的证明　由引理3知，要证定理2，只需证对任何$w\geqslant 1$，有

$$\sum_{i=1}^{w}\binom{w}{i}\binom{2b+1-w}{i}(4i-2b-1)<0 \qquad \text{对}b\geqslant 4\text{成立} \tag{12}$$

以下分几种情形讨论：

(1) 若$w\leqslant\frac{2b+1}{4}$，则显知对$1\leqslant i\leqslant w$，必有$4i-2b-1<0$．故(12)式的和式中每一项都小于0，故(12)式成立。

(2) 若$b-1\geqslant w>\frac{2b+1}{4}$。注意两个恒等式：

$$\binom{w}{i}=\binom{b}{i}\frac{(b-i)(b-i-1)\cdots\cdots(w-i+1)}{b(b-1)\cdots\cdots(w+1)}$$

$$\binom{2b+1-w}{i}=\binom{b+1}{i}\frac{(2b+1-w)(2b-w)\cdots\cdots(b+2)}{(2b+1-w-i)(2b-w-i)\cdots\cdots(b+2-i)}$$

则

$$(12)\text{式左边和式}=\sum_{i=1}^{w}\binom{b}{i}\binom{b+1}{i}(4i-2b-1)\cdot g(i)$$

此处

$$g(i)=\frac{(b-i)(b-i-1)\cdots\cdots(w-i+1)\cdot(2b+1-w)(2b-w)\cdots\cdots(b+2)}{b(b-1)\cdots\cdots(w+1)\cdot(2b+1-w-i)(2b-w-i)\cdots\cdots(b+2-i)}$$

由于$b-1\geqslant w>\frac{2b+1}{4}$，故对$j>w$，必有$4j-2b-1>0$. 且显然，若令：

$$f(i)=\begin{cases}g(i)，\text{对}1\leqslant i\leqslant w\\ g(w)，\text{对}w+1\leqslant i\leqslant b,\end{cases}$$

则知，$f(i)$为单调非递增的正值函数，故

$$(12)\text{式左边的和式}=\sum_{i=1}^{w}\binom{b}{i}\binom{b+1}{i}(4i-2b-1)\cdot f(i)$$

$$<\sum_{j=1}^{b}\binom{b}{j}\binom{b+1}{j}(4j-2b-1)\cdot f(j) \qquad (13)$$

由引理7，引理6即知，(13)式小于0，即已证得(12)式成立。

(3) 若$w=b$，则由引理7知，(12)式成立。

(4) 若$2b\geqslant w\geqslant b+1$，则由检错码的理论知，$(2b+1,2,w)$码与$(2b+1,2,2b+1-w)$码的性质完全相同。而对$(2b+1,2,2b+1-w)$码来说，此时$b\geqslant 2b+1-w\geqslant 1$. 故由刚证得的1,2,3三种情形知(12)式成立。

综合1,2,3,4四种情形，即知(12)式成立，即定理2得证。 (证毕)

参 考 文 献

[1] Wolf J K, Chelson A M M, Levesque A H. On the Probability of Undetected Error for Linear Block Codes. IEEE Trans. Commun., 1982, 30: 317～324

[2] Kasami T, Klove T, Lin S. Linear Block Codes for Error Detection IEEE Trans. IT, 1983, 29: 131～136

[3] Kasami T, Lin S. On the Probability of Undetected Error for the Maximum Distance Separable Codes IEEE Trans. Commun., 1984, 32: 998～10006

[4] Sommer R C. A Note Upon Another Error Detecting Code that is not Proper IEEE Trans. Commun., 1985, 33: 719～721

[5] 王新梅. 最佳$(n,2,w)$二进制等重检错码的存在性及其猜想. 中国科学 (A辑), 1987, 11: 1225～1232

A Study on the Optimum (n,2,w) Binary Constant Weight Error-detecting Codes

Xiao Rong

(Department of Electronic Technology)

Abstract

The paper discusses the existance of optimum $(n,2,w)$ binary constant

国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第12卷第4期 1990年12月 Vol.12 No.4

m序列的完备递归采样法

唐朝京 肖戎
(电子技术系)

摘 要 本文提出了m序列递归采样的概念，研究并解决了素数周期m序列的完备递归采样，对周期为合数的情况得到了一些有用的结论。

关键词 保密通信，采样，m序列
分类号 TP918.1

m序列是一类非常有用的伪随机序列，在编码、密码及通信工程中得到了广泛的应用。特别在密码学领域，将m序列进行适当变换产生密码序列是行之有效的办法。若存贮一定数量的m序列，则可以有效地增加密钥量，提高密码的抗破译能力。因此产生多个m序列的问题具有重要的意义。

产生m序列的传统方法是求GF(2)上的本原多项式，这可以直接根据本原多项式的定义来求，也可以利用各种等价的方法求得[1]，但这些方法都不很实用。目前产生m序列的最简单方法是采样法，只要采样间隔选得与序列的周期互素，就能得到一个新的m序列。但是当需要产生的m序列数量很大时，采样法也存在如下的不足之处（设级数为n，采样值为s，要求产生的m序列的个数为l）：

(1) 对每个采样值s，都要求保证$(s, 2^n-1)=1$，这一工作的计算量是不能忽略的；

(2) 为求得一个采样序列的反馈多项式，需要产生$2ns$位m序列。当l比较大时，s的值必然越来越大，则计算量也越来越大；

(3) 对于不同采样值采到的m序列，需要从中排除平移等价的序列，这个工作量为$\frac{1}{2}l(l-1)$；

(4) 不能保证在比较短的时间内采到所有的n级m序列。

针对采样方法的这些不足，作者提出了m序列递归采样和完备递归采样的概念，可

1990年3月16日收稿

weight error-detecting codes. A succinct proof is given for the conclusion made by prof. Wang xinmei (china science, vol.11, 1987) when n is even. The author also gives a proof for the conjecture of the wang xinmei's paper.

Key words code, coding error-detecting code, optimization / constant weight codes