极大距离可分码的存在范围研究*

陈 勤**

(杭州电子工业学院计算机科学与技术系 杭州 310037)

【摘要】 引进了 F_2 上矩阵的行间距和极小行间距概念，给出了极小行间距的一些基本性质，证明了极小行间距的两个重要定理。给出了 $V_n(F_2)$中 Hamming 极小距离的两个重要结论，得到了二元线性码（n，k）中存在极大距离可分码的一个必要条件：当 $k\geq 3$ 时，$n\leq 3(k-1)$；当 $k\geq 5$ 并且 n 能被 3 整除时，$n<3(k-1)$。同时给出了 q 元线性码（n, k）中存在极大距离可分码的一个必要条件。

关 键 词 行间距； 极小行间距； Hamming 距离； Hamming 极小距离； 线性码； 极大距离可分码

中图分类号 TN911.22

数字信息在传送过程中可能会受到种种干扰（自然界存在的电磁源以及其他无线电系统发射的信号等），这样接收到的数字信息可能不是信息源发送的数字信息。为了使信息源发送的数字信息能正确地传送到接收者，常常采用抗干扰编码技术，在数字信息传送之前先进行一次抗干扰编码，然后再发送抗干扰编码后的数字信息。

纠错码是抗干扰编码中的一种，而人们希望设计纠错能力强的纠错编码。当 n 和 k 给定时，码长 n 而信息位个数等于 k 的线性码中极大距离可分码是纠错能力最大的码，因此对于给定的 n 和 k，常用极大距离可分码作为纠错码。由此可知，极大距离可分码的存在范围研究是十分必要的，这样可避免盲目选择 n 和 k 来设计事实上不存在的极大距离可分码。

1 基本引理

定义 1 设 F_2 上矩阵 $A=(a_{ij})_{m\times n}$，$d_{\text{row}}(A,i,j)=\sum_{k=1}^{n}(a_{ik}\oplus a_{jk})$，则称 $d_{\text{row}}(A,i,j)$ 为矩阵 A 中第 i 行与第 j 行间的行间距。其中，$\oplus$ 为模加；$\sum$ 为按整数求和。

引理 1 设 F_2 上矩阵 $A=(a_{ij})_{m\times n}$，矩阵 $B=(b_{ij})_{m\times n}$ 为 A 中某一列元素取反，其余元素不变，则 $\forall 1\leq i(j\leq m$ 有 $d_{\text{row}}(B,i,j)=d_{\text{row}}(A,i,j)$。

证明 根据题意，不妨假设 A 中第 k 列 $(1\leq k\leq n)$ 取反，即 $b_{ik}=a_{ik}\oplus 1(i=1,2,\cdots,m)$，。$b_{ij}=a_{ij}(j\neq k;1\leq i\leq m;j=1,2,\cdots,n)$。于是 $\forall 1\leq i\leq j\leq m$ 有

$$d_{\text{row}}(B,i,j)=\sum_{p=1}^{n}(b_{ip}\oplus b_{jp})=\sum_{p=1,p\neq k}^{n}(b_{ip}\oplus b_{jp})+(b_{ik}\oplus b_{jk})=\sum_{p=1,p\neq k}^{n}(a_{ip}\oplus a_{jp})+(a_{ik}\oplus 1\oplus a_{jk}\oplus 1)=$$

$$\sum_{p=1,p\neq k}^{n}(a_{ip}\oplus a_{jp})+(a_{ik}\oplus a_{jk})=\sum_{p=1}^{n}(a_{ip}\oplus a_{jp})=d_{\text{row}}(A,i,j)$$

推论 1 设 F_2 上的矩阵 $A=(a_{ij})_{m\times n}$，F_2 上矩阵 B 为 A 中任意若干列元素取反，其余元素不变，则 $\forall 1\leq i<j\leq m$ 有 $d_{\text{row}}=(B,i,j)=d_{\text{row}}(A,i,j)$。

引理 2 设 F_2 上矩阵 $A=(a_{ij})_{m\times n}$，F_2 上矩阵 B 和 A 经任意列置换后的矩阵，则 $\forall 1\leq i\leq(j\leq m)$ 有 $d_{\text{row}}(B,i,j)=d_{\text{row}}(A,i,j)$。

引理 2 的证明参见文献[1]。

推论 2 设 F_2 上矩阵 $A=(a_{ij})_{m\times n}$，F_2 上矩阵 B 为 A 经任意若干列元素取反和任意列置换后的矩阵，则 $\forall 1\leq i(j\leq m)$ 有 $d_{\text{row}}(B,i,j)=d_{\text{row}}(A,i,j)$。

1998 年 10 月 6 日收稿

* 电子部预研基金资助项目

** 男 36 岁 硕士 副教授

2　两个重要定理

定义 2　设 F_2 上矩阵 $A=(a_{ij})_{m\times n}, d_{\text{row}}(A,\min)=\min\limits_{1\le i<j\le m}\{d_{\text{row}}(A,i,j)\}$，则称 $d_{\text{row}}(A,\min)$ 为矩阵 A 的极小行间距。

定理 1　设 $A=(a_{ij})_{m\times n}$ 为 F_2 上的矩阵，$m\ge 3$，则 $d_{\text{row}}(A,\min)\le\dfrac{2n}{3}$。

证明　引进几个记号：t_{ij} 表示 i 与第 j 行对应位相同部分的个数；f_{ij} 表示第 i 行与第 j 行对应位不同部分的个数；$t_{(ij,pk,1)}$ 表示第 p 行与第 k 行对应位相同部分中，第 i 行与第 j 行对应位相同部分的个数；$f_{(ij,pk,1)}$ 表示第 p 行与第 k 行对应位相同部分中，第 i 行与第 j 行对应位不相同部分的个数；$f_{(ij,pk,0)}$ 表示第 p 行与第 k 行对应位不相同部分中，第 i 行与第 j 行对应位相同部分的个数；$t_{(ij,pk,0)}$ 表示第 p 行与第 k 行对应位不相同部分中，第 i 行与第 j 行对应位不相同部分的个数。显然

$$t_{12}+f_{12}=n\qquad t_{13}+f_{13}=n\qquad t_{23}+f_{23}=n \tag{1}$$

设 $d_{\text{row}}(A,\min)>\dfrac{2}{3}$，则根据 $d_{\text{row}}(A,\min)$ 定义知

$$f_{12}>\frac{2n}{3}\qquad f_{13}>\frac{2n}{3}\qquad f_{23}>\frac{2n}{3} \tag{2}$$

由式(1)与式(2)知

$$t_{12}<\frac{n}{3}\qquad t_{13}<\frac{n}{3}\qquad t_{23}<\frac{n}{3} \tag{3}$$

另外由约定的记号知

$$t_{(23,12,1)}+f_{(23,12,1)}=t_{12},\qquad t_{(23,12,0)}+f_{(23,12,0)}=f_{12} \tag{4}$$

故由式(4)知

$$f_{(23,12,1)}\le t_{12}<\frac{n}{3}$$

由此可见 $f_{(23,12,0)}>\dfrac{n}{3}$，否则若 $f_{(23,12,0)}\le\dfrac{n}{3}$，则 $f_{23}=f_{(23,12,1)}+f_{(23,12,0)}<\dfrac{n}{3}+\dfrac{n}{3}=\dfrac{2n}{3}$，与式（2）矛盾。

由 $f_{(23,12,0)}$ 的约定知，$f_{(23,12,0)}$ 所代表的对应位部分，既表示第 1 行与第 2 行对应位不同，也表示第 2 行与第 3 行对应位不同，故由 $a_{ij}\in\{0,1\}$ 知这一对应部分的对应位第 1 行与第 3 行相同。因此 $t_{13}\ge f_{(23,12,0)}>\dfrac{n}{3}$，与式（3）矛盾。命题成立。

定理 2　设 $A=(a_{ij})_{m\times n}$ 为 F_2 上的矩阵，$m\ge 5, n=0 \bmod 3$，则 $d_{\text{row}}(A,\min)<\dfrac{2n}{3}$。

证明　根据定理 1，$d_{\text{row}}(A,\min)<\dfrac{2n}{3}$，所以只要证明 $d_{\text{row}}(A,\min)<\dfrac{2n}{3}$ 不成立。

假设 $d_{\text{row}}(A,\min)<\dfrac{2n}{3}$，因 $n\equiv 0 \bmod 3$，故可设 $n=3t$ (t 为自然数)。

根据 $d_{\text{row}}(A,\min)$ 的定义知：$d_{\text{row}}(A,\min)=\min\limits_{1\le i\le j\le m}\{d_{\text{row}}(A,i,j)\}=\dfrac{2n}{3}=2t$，即矩阵 A 中任意不同的二行至少有 $2t$ 个对应位不同，最多有 t 个对应位相同。

1）先证明 $\forall 1\le i\le j\le m$，有 $d_{\text{row}}(A,i,j)=2t$。

假设有二行(不妨设第 1 行与第 2 行)多于 $2t$ 个对应位不同，则 $t_{12}<t, f_{12}>2t$。因为 $\forall 1\le i<j\le m$ 有 $d_{\text{row}}(A,i,j)=2t$，所以 $t_{13}\le t$、$t_{23}\le t$、$t_{3,}\le t(i>3$ 时）、$f_{13}\ge 2t$、$f_{23}\ge 2t$。于是 $t_{(23,12,0)}+f_{(23,12,0)}=f_{12}>2t$，故 $t_{(23,12,0)}$ 与 $f_{(23,12,0)}$ 中至少有一个大于 t:

(1) 若 $t_{(23,12,0)}>t$，则 $t_{23}=t_{(23,12,0)}+t_{(23,12,1)}\ge t_{(23,12,0)}>t$，与假设矛盾；

(2) 若 $t_{(23,12,0)}>t$，则 $t_{13}=t_{(23,12,0)}+t_{(23,12,1)}\ge f_{(23,12,0)}>t$，与假设矛盾。

故 $\forall 1\le i\le j\le m$ 有 $d_{\text{row}}(A,i,j)=2t$。由此可知，若 $d_{\text{row}}(A,\min)=\dfrac{2n}{3}$，则不同行间正好有 $2t$ 个对应

位不同，正好有 t 个对应位相同。

2） 以下证明满足 $d_{\text{row}}(A,i,j)=2t(1\le i<j\le m)$ 的矩阵是不存在的。

将每行从左至右等分为三个相等的段，每个段均由 t 个位组成，依次称为第 1 段、第 2 段、第 3 段，并引进记号：

(1) $b_{(i,j,0)}$ 表示第 i 行中第 j 段 0 出现的个数 $(1\le i\le m;\ 1\le j\le 3)$；

(2) $b_{(i,j,1)}$ 表示第 i 行中第 $j1$ 段出现的个数 $(1\le i\le m;\ 1\le j\le 3)$。

若满足要求的矩阵 A 存在，则根据推论述不妨假设 A 的第 1 行元素全为 0（否则，对第 1 行中不为 0 的列取反）。即 $b_{(1,1,0)}=b_{(1,2,0)}=b_{(1,3,0)}=t$，根据引理 2 这里假设 $b_{(2,1,0)}=t$，从而 $b_{(2,2,1,)}=b_{(2,3,1)}=t$，由约定的记号及已得到的结论知

$$b_{(i,1,0)}+b_{(i,2,0)}+b_{(i,3,0)}=t \qquad b_{(i,1,0)}+b_{(i,1,1)}=t$$

所以 $\forall i\ge 3$，有

$$f_{2i}=f_{(2i,12,1)}+f_{(2i,12,0)}=b_{(i,1,1)}+b_{(i,2,0)}+b_{(i,3,0)}=2t$$

于是 $\forall i\ge 3$

$$b_{(i,1,1)}+2b_{(i,1,0)}+b_{(i,3,0)}=2t$$

由上可知 $\forall i\ge 3$ 时，$b_{(i,1,0)}=0$。故 $\forall i\ge 3$ 时，有 $b_{((i,1,1)}=t$。

同理根据列置换不影响 $d_{\text{row}}(A,i,j)$ 的值这一性质，这里假设 $b_{(3,2,0)}=t$（这不影响矩阵存在性的证明），故 $b_{(3,1,1)}=b_{(3,2,0)}=b_{(3,3,1)}=t$。所以 $\forall i>3$ 时,有

$$t_{3i}=b_{(i,1,1)}+b_{(i,2,0)}+b_{(i,3,1)}=t+b_{(i,2,0)}+b_{(i,3,1)}$$

因此，当 $\forall i>3$ 时，有 $b_{(i,2,1)}=b_{(i,3,0)}=t$。这说明从第 4 行开始都是一样的，即当 $\forall 4\le i<j\le m$ 时，有：$d_{\text{row}}(A,i,j)=0$，因 $m\ge 5$，显然与假设矛盾。故满足 $d_{\text{row}}(A,i,j)=2t(1\le i\le j\le m)$ 条件的矩阵是不存在的。命题成立。

3 极大距离可分码的存在范围

定义 3 设 a,b 是 $V_n(F_q)$ 中的向量，记 $a=(a_1,a_2,\cdots,a_m)$，$b=(b_1,b_2,\cdots,b_n)$，$\rho(a,b)$ 为 a 和 b 的相应位置不相等的个数，则称 $\rho(a,b)$ 为 a 和 b 之间的 Hamming 距离，简称距离。

定义 4 设 $\rho_{\min}=\min\{\rho(a,b)\mid a,b\in V_n(F_q),\ a\ne b\}$，则称 $\rho_{\min}$ 为 $V_n(F_q)$ 上的 Hamming 极小距离，简称极小距离。

推论 3 设 $V_n(F_2)$ 中至少含有 3 个互不相同的向量，则 $\rho_{\min}\le\dfrac{2n}{3}$。

证明 设 a_1、a_2、a_3 为 $V_n(F_2)$ 中 3 个互不相同的向量，分别以 a_1、a_2、a_3 的 n 个分量作为 F_2 上矩阵 A 的第 1、2、3 行，则矩阵 A 为 F_2 上 $3\times n$ 矩阵，由定理 1 知 $d_{\text{row}}(A,\min)\le\dfrac{2n}{3}$，于是由定义 2 及定义 4 易知 $V_n(F_2)$ 上的极小距离 $\rho_{\min}\le\dfrac{2n}{3}$。

推论 4 设 $V_n(F_q)$ 中至少含有 5 个互不相同的向量，则 $\rho_{\min}<\dfrac{2n}{3}$。

推论 4 的证明与推论 3 的证明相类似。

定义 5 设 σ 是从 $V_k(F_q)$ 映入 $V_k(F_q)$ 的一个一一映射 $\sigma:V_k(F_q)\to V_n(F_q),C=\sigma(V_k(F_q))$。若 C 是 $V_n(F_q)$ 的子空间，则称 C 是个 q 元 (n,k) 线性码。

定义 6 设有一 (n,k) 线性码，它的极小距离 $\rho_{\min}$ 达到极大值 $n-k+1$，则称这个 (n,k) 线性码是极大距离可分码。

定义 3 至定义 6 及相关内容参见文献[2,3]，文献[4]对线性码的极小距离作了研究。

推论 5 设 (n,k) 为一个二元线性码，$\rho_{\min}$ 达到极大值 $n-k+1$, 则 $n<3(k-1)$。

证明 由推论 3 易知 $n-k+1\le\dfrac{2}{3}n$，即 $3n-3k+3\le 2n$, 故 $n\le 3(k-1)$。

推论 6　设 (n,k) 为一个二元线性码，ρ_{min} 达到极大值 $n-k+1, n\equiv 0 \bmod 3$, 则 $n<3(k-1)$。

推论 6 的证明与推论 5 的证明类似。

由推论 5、6 知，对于给定的 n、k，二元线性码 (n,k) 中存在极大距离可分码的必要条件是：当 $k\geq 3$ 时，$n\leq 3(k-1)$；当 $k\geq 5, n\equiv 0 \bmod$ 时，$n<3(k-1)$。

上述结论不难加以推广，以下是推广后的主要结论：

推论 7　设 (n,k) 为一 q 元线性码，ρ_{min} 达到极大值 $n-k+1$，则 $\dfrac{n\leq 3(k-1)}{\log_2 q}$（这里 x 表示不小于 x 的最小整数）。

证明　先对 q 元线性码 (n,k) 中每一元素 $a_{ij}\in\{0,1,\cdots,q\}$ 用二进制进行自然编码，则 a_{ij} 编码后的长度均为 $\log_2 q$，于是由推论 5 易知命题成立。

推论 8　设 (n,k) 为一 q 元线性码，ρ_{min} 达到极大值 $n-k+1$, $n\equiv 0 \bmod 3$，则 $\dfrac{n\leq 3(k-1)}{\log_2 q}$。

推论 8 的证明与推论 7 的证明类似。于是可知，对于给定的 n、k，q 元线性码 (n,k) 中存在极大距离可分码的必要条件是：当 $k\geq 3$ 时，$\dfrac{n\leq 3(k-1)}{\log_2 q}$；当 $k\geq 5$, $n\equiv 0 \bmod 3$ 时，$\dfrac{n\leq 3(k-1)}{\log_2 q}$。

4　结 束 语

本文给出了 F_2 上极小行间距的两个上界定理，基于这两个定理得到了 q 元线性码 (n,k) 中存在极大距离可分码的一个必要条件。

文中得到的两个上界是否是最小上界，上界范围内是否一定存在极大距离可分码及存在时如何进行设计，这些问题还需作进一步地研究。

参 考 文 献

1　叶又新. 扩散码及其密码学用途. 通信学报，1997，18(9)：19~25

2　万哲先. 代数与编码. 北京：科学出版社，1976

3　肖国镇，卿斯汉. 编码理论.北京：科学出版社；1993

4　冯登国. 线性码和 Walsh 谱. 通信保密，1994，58（2）：60~62

Research on Existent Range of Maximum Distance Isolated Code

Chen Qin

(Department of Computer Science and Technology, Hangzhou Institute of Electronic Engineering　Hangzhou　310037)

Abstract　In this paper, row distance and minimum row distance of matrix on F_2 are presented, and some properties about row distance are given. Two important theorems are proved. According to these theorems, a necessary codition is obtained whether there is a maximum distance isolated code among 2-order (n,k) linear codes:n is smaller than or egual to $3(k-1)$ when k is bigger than or egual to 3,n is smaller than $3(k-1)$ when k is bigger than or egual to 5 and n can be dibided by 3.In this paper a necessary condition is also given whether there is a maximum distance isolated code among q-order (n,k) linear codes.

Key words　row distance;　minmum row distance;　Hamming distance;　Hamming minimum distance;　linear code;　maximum distance isolated code