第 17 卷 第 5 期　　电 子 科 学 学 刊　　Vol. 17 No. 5
1995 年 9 月　　JOURNAL OF ELECTRONICS　　Sept. 1995

等距码的几点注记*

符方伟　　沈世镒
(南开大学数学系　天津　300071)

摘要　设 $Q(n,d)$ 为码长为 n，任意两个不同码字之间的 Hamming 距离为 d 的二元等距码所能达到的最大码字数，本文确定了 $Q(n,d)$ 的一些精确值，并且给出了最优等距码的一些性质.

关键词　等距码，Hadamard 矩阵，区组设计，Plotkin 界，Grey-Rankin 界

1 引言

确定 $Q(n,d)$ 的值是编码理论的一个重要问题，这方面的研究见文献[1—4]，到目前为止，这个问题尚未完全解决. 研究结果表明，这个问题与组合学中一些著名的问题相联系，由此可见这个问题的难度. 本文利用编码理论和区组设计的一些结果确定了 $Q(n,d)$ 的一些精确值，并与编码理论中其它类似问题的对应值进行了比较，同时我们给出了最优等距码的一些性质.

2 概念和记号

设 $A(n,d)$ 为码长为 n，任意两个不同码字之间的 Hamming 距离不小于 d 的二元码所能达到的最大码字数；$A(n,d,w)$ 为码长为 n，每个码字的重量为 w，且任意两个不同码字之间的 Hamming 距离不小于 d 的二元等重码所能达到的最大码字数；$E(n,d,w)$ 为码长为 n，每个码字的重量为 w，且任意两个不同码字之间的 Hamming 距离为 d 的二元等重等距码所能达到的最大码字数. 显然 $Q(n,d)\leqslant A(n,d)$. 确定 $A(n,d)$ 和 $A(n,d,w)$ 的精确值是编码理论的著名难题，称为编码理论的基本问题. 尽管信息论学者作出了巨大努力试图解决这个问题，但由于缺乏强有力的数学工具，这个问题相对来说进展缓慢.

在本文中我们用 $d_H(\cdot,\cdot)$ 表示 Hamming 距离，$w_H(\cdot)$ 表示 Hamming 重量，$|\cdot|$ 表示有限集所含元素的个数. 设 $X=\{x_1,\cdots,x_v\}$ 为一个含有 v 个元的有限集，$\mathscr{B}=\{B_1,\cdots,B_v\}$ 为 v 个 X 的子集，如果 $(X,\mathscr{B})$ 满足：(1) 每一个 B_i 所含元素个数为 k，(2) 对任意不同的 $x,y\in X$，含有 x,y 的 B_i 的个数都为 λ，则 $(X,\mathscr{B})$ 称为一个 (v,k,λ)-对称区组设计. 设 $r_{ij}=1$，若 $x_j\in B_i$，$r_{ij}=0$；若 $x_j\notin B_i$，称 $R=(r_{ij})_{v\times}$

1994-05-03 收到，1994-10-24 完稿
* 国家自然科学基金，国家教委优秀年青教师基金和回国留学人员科研基金资助项目
符方伟　男，1963 年 10 月生，副教授，博士，主要从事信息论，编码理论和密码学理论的研究和教学工作.
沈世镒　男，1939 年 4 月生，教授，博士生导师，主要从事信息论、编码理论、密码学理论和神经网络的数学理论的研究工作

为 $(X,\mathscr{B})$ 的关联矩阵. 一个 $(4t-1, 2t-1, t-1)$-对称区组设计称为 Hadamard 设计, Hadamard 设计与 Hadamard 矩阵相互一一对应. 我们知道如果存在一个 (v, k, λ)-对称区组设计, 则 $\lambda(v-1)=k(k-1)$. 对称区组设计的概念和性质详见文献[5]的第 13 章.

设 C 为一个 n 长二元码, 且对任意不同的码字 a,b, $d \leqslant d_H(a,b) \leqslant n-d$, 则由编码理论中的 Grey-Rankin 界 (参见文献 [6], P.544, 问题 18 的证明提示) 知 $|C| \leqslant 4d(n-d)/[4d(n-d)-n(n-1)]$, $(n-\sqrt{n})/2 < d \leqslant n/2$

3 关于 $Q(n,d)$ 的一些结果

推论 1 $Q(n,d)=E(n,d,d)+1$, $d \neq 0$.

证明 设 C 为一个达到 $Q(n,d)$ 的等距码, 取 $a \in C$, 将 $a+C=\{a+c: c \in C\}$ 去掉零向量后构成一个等重等距码 C^*; 每一个码字的 Hamming 重量为 d, 任意两个不同码字的 Hamming 距离为 d, 则 $E(n,d,d) \geqslant |C^*| = |C|-1 = Q(n,d)-1$.

反过来, 设 C_1 为一个达到 $E(n,d,d)$ 的二元等重等距码, 则将 C_1 添加一个零向量后构成一个等距码 C_2; 任意两个不同码字的 Hamming 距离为 d, 故 $Q(n,d) \leqslant |C_2| = |C_1|+1 = E(n,d,d)+1$, 则 $Q(n,d)=E(n,d,d)+1$. 证毕

由推论 1 知除了 $d=0, n$ 外, $Q(n,d)$ 只有当 d 为偶数时才有意义.

推论 2 当 $d \leqslant n < 2d$, d 为偶数时, $Q(n,d) \leqslant 2[d/(2d-n)]$, 且如果某些相应的 Hadamard 矩阵存在, 则等号成立. 这里 $[x]$ 表示不超过 x 的最大整数.

证明 由 $Q(n,d) \leqslant A(n,d)$ 和 Plotkin 界知不等式成立. 由文献[6]知当 d 为偶数时, 通过某些相应的 Hadamard 矩阵构造的且达到 Plotkin 界的码实际上是等距码. 证毕

二元 $[2^m-1, m, 2^{m-1}]$ 极长码是一个等距码, 它达到了推论 2 的界.

推论 3 如果存在 $4t$ 阶 Hadamard 矩阵, 则 $Q(4t,2t)=4t, E(4t,2t,2t)=4t-1$.

证明 由 Grey-Rankin 界知 $Q(4t,2t) \leqslant 4t$. 如果存在 $4t$ 阶 Hadamard 矩阵, 则存在 $4t$ 阶规范的 Hadamard 矩阵; 将这个规范的 Hadamard 矩阵中的 -1 变成 0, 则得到一个 $4t \times 4t$ 阶 (0,1)-矩阵. 由 Hadamard 矩阵的性质知这个 (0,1)-矩阵的行向量构成一个等距码, 则 $Q(4t,2t) \geqslant 4t$, 故 $Q(4t,2t)=4t$. 由推论 1 知 $E(4t,2t,2t)=4t-1$. 证毕

推论 3 是一个有趣的结论, 我们知道如果存在 $4t$ 阶 Hadamard 矩阵, 则 $A(4t,2t)=8t$, $A(4t,2t,2t)=8t-2$, 这说明 $Q(n,d)$ 与 $A(n,d)$; $E(n,d,w)$ 与 $A(n,d,w)$ 是不全相同的. 推论 3 可以推广成下面的定理.

定理 1 (1) 如果 $n \neq 4t-1$, 则 $Q(n,2t) \leqslant n$, 且如果存在一个 (v,k,λ)-对称区组设计, $v \neq 4(k-\lambda)-1$, 则 $Q(v,2(k-\lambda))=v$.

(2) $Q(4t-1,2t) \leqslant 4t$, 且等号成立的充要条件为存在 $4t$ 阶 Hadamard 矩阵.

为了证明定理 1, 我们先证明下面的引理.

引理 1 若存在一个二元 n 长等距码 C, $|C| \geqslant n+1$, 且任意两个不同码字的 Hamming 距离为 $2t$, 则 $n=4t-1$, 且存在 $4t$ 阶 Hadamard 矩阵.

证明 在 C 中取 $n+1$ 个码字 $c_0, c_1, \cdots, c_n$, 令 $a_i=c_0+c_i$, $i=1,\cdots,n$. 设

$\bar{R}$ 为一个 $n \times n$ 阶(0,1)-矩阵，以 $a_i, i = 1, \cdots, n$ 为行向量，则 $\bar{R}$ 的任一个行向量的重量为 $2t$，任意两个不同行向量的 Hamming 距离为 $2t$，则任意两个不同行向量的内积为 t。故由对称区组设计的性质(文献[5]，P. 81，定理 13.1.4)知存在一个 $(n, 2t, t)$-对称区组设计，则 $t(n-1) = 2t(t-1)$，故 $n = 4t - 1$。

因为存在一个 $(4t-1, 2t, t)$-对称区组设计，而它的反设计为一个 $(4t-1, 2t-1, t-1)$-对称区组设计，即 Hadamard 设计。故存在 $4t$ 阶 Hadamard 矩阵。

定理 1 的证明　(1) 我们用反证法证明 $Q(n, 2t) \leqslant n$，$n \neq 4t - 1$。反设 $Q(n, 2t) \geqslant n + 1$，$n \neq 4t - 1$，则存在一个二元 n 长等距码满足引理 1 的条件，由引理 1 知 $n = 4t - 1$，这与条件矛盾，故假设不对，则 $Q(n, 2t) \leqslant n$，$n \neq 4t - 1$。

若存在一个 (v, k, λ)-对称区组设计，则它的关联矩阵的 v 个行向量构成一个等距码，码长为 v，任意两个不同码字的 Hamming 距离为 $2(k - \lambda)$，故 $Q(v, 2(k-\lambda)) \geqslant v$，则当 $v \neq 4(k-\lambda) - 1$ 时，$Q(v, 2(k-\lambda)) = v$。

(2) 由 Plotkin 界知 $Q(4t-1, 2t) \leqslant 4t$。如果存在 $4t$ 阶 Hadamard 矩阵，则存在一个 $(4t-1, 2t-1, t-1)$-Hadamard 设计，它的反设计为一个 $(4t-1, 2t, t)$-对称区组设计。这个反设计的关联矩阵的行向量再加上一个零向量后构成一个等距码，码长为 $4t-1$，码字个数为 $4t$，任意两个不同码字的 Hamming 距离为 $2t$，故 $Q(4t-1, 2t) \geqslant 4t$，则 $Q(4t-1, 2t) = 4t$。

反过来，如果已知 $Q(4t-1, 2t) = 4t$，则存在一个二元等距码 C，码长为 $4t-1$，码字个数为 $4t$，任意两个不同码字的 Hamming 距离为 $2t$，则由引理 1 知存在 $4t$ 阶 Hadamard 矩阵。　证毕

4　结论

本文利用编码理论和区组设计的一些结果去研究最优等距码的结构和性质，确定了等距码所能达到的最大码字数的部分精确值。确定所有最优等距码的结构和码字数仍然是编码理论中一个尚待解决的难题。

参　考　文　献

[1] Van Lint J H. Discrete Math, 1973, 6(3): 353—358.

[2] Hall J I. Discrete Math, 1977 17(1): 85—94.

[3] Hall J I, *et al*. Discrete Math, 1977, 17(1): 71—83.

[4] 杨义先. 电子学报，1993，21(7)：98—100.

[5] 魏万迪. 组合论(下册). 北京：科学出版社，1987，第 13 章第 1 节.

[6] MacWilliams F J, Sloane N J A. The Theory of Error-Correcting Codes, Third printing, North-Holland, Amsterdam: Elsevier Science Publishing Company, 1981. Chapter 17.

SOME NOTES FOR EQUIDISTAN T CODES

Fu Fangwei Shen Shiyi
(Department of Mathematics, Nankai University, Tianjin 300071)

Abstract Let $Q(n,d)$ denote the largest number of cod-words in any binary equidistant code of length n and Hamming distance d between code words, this paper determines some exact values of $Q(n,d)$, and presents several properties of optimal equidistant codes.

Key words Equidistant code, Hadamard matrix, Block design, Plotkin bound, Grey-Rankin bound