广义 Hamming 线性等重码

樊 恽[1,3],刘宏伟[2,1]
(1. 武汉大学数学系,湖北武汉 430072;2. 华中师范大学数学系,湖北武汉 430079;3. 湖北大学数学系,湖北武汉 430062)

摘 要: 设 C 为 $[n,k]$ 线性码,本文证明:一个线性码 C 只要对于某个 r,$0<r<k$,是 r-等重线性码,那么它对于所有的 $0<r<k$ 都是 r-等重线性码.

关键词: 广义 Hamming 重量; r-等重码; 极大投射码
中图分类号: O157.4 **文献标识码**: A **文章编号**: 0372-2112 (2003) 10-1591-03

Generalized Hamming Equiweight Linear Codes

FAN Yun[1,3], LIU Hong-wei[2,1]
(1. *Dept. of Mathematics, Wuhan Univ., Wuhan, Hubei* 430072, *China*;
2. *Dept. of Mathematics, Central China Normal Univ., Wuhan, Hubei* 430079, *China*;
3. *Dept. of Mathematics, Hubei Univ., Wuhan, Hubei* 430062, *China*)

Abstract: For an [n,k] linear code, it is proved that, if it is r-equiweight for one r with $0<r<k$, then it is r-equiweight for all $0<r<k$.

Key words: generalized hamming weight; r-equiweight code; maximal projective code.

1 引言

一个码称为等距码,如果它的任意两个不同的码字之间的 Hamming 距离是一个常值. 一个码称为等重码,如果它的任意非零码字的重量是常值. 显然一个线性码是等距码当且仅当它是等重码. 文献[1]决定了所有二元线性等重码的结构,文献[2]进一步讨论了一般等距码的性质,文献[3]在文献[1]和[2]的基础上,证明了任一 q-元线性码是等距码当且仅当它单项等价于一个极大投射码的重复码.

另一方面,作为对 Hamming 重量的推广,文献[4]引入了广义 Hamming 重量和 Hamming 谱的概念,得到了许多关于它的结果;文献[5]给出了广义 Hamming 重量的广义 Plotkin 界.

可以很自然的引入广义 Hamming r-等重线性码,使得 1-等重线性码就是通常的线性等重码. 本文证明了一个线性码只要对某一个 r 是 r-等重的,那么它就对所有的 r 是 r-线性等重码;作为推论,任何 r-等重线性码单项等价于极大投射码的重复码,而且,如果它没有冗余位那么它就正好是达到广义 Plokin 界的线性码.

2 主要结果

令 F_q 总表示一个阶为 $q=p^l$ 的有限域,这里 p 是一个素数. 设 C 总表示 F_q 上的一个 $[n,k,d]$-线性码,即一个码长为 n 的维数为 k 的极小距离为 d 的 q-元码. 对任何非空集合 S,用 $|S|$ 表示集合 S 的基数.

由文献[4],对于 C 的一个线性子空间(即 C 的一个线性子码) E,称

$$w(E)=|\{1\leq i\leq n|\text{ 存在 } x=(x_1,\cdots,x_n)\in E \text{ 使得 } x_i\neq 0\}|$$

为 E 的广义 Hamming 重量,即,$w(E)$ 是线性子码 E 的有效位数;再定义

$$d_r(C)=\min\{w(E)|\ E \text{ 是 } C \text{ 的一个 } r\text{-维子空间}\}$$

称为码 C 的极小 r-重量.

显然 $d_0(C)=0$. 另一方面,$d_k(C)=w(C)$ 就是线性码 C 的有效位数. 对于其他的整数,这里 $0<r<k$,$w(E)$ 将随着 E 的不同而变化.

自然地,称码 C 是 r-等重的,如果对于 C 的任意两个 r-维子空间 E 和 E' 都有 $w(E)=w(E')$;或者等价地说,对 C 的任意 r-维子空间 E,有 $w(E)=d_r(C)$. 特别地,1-等重码就是通常的等重码,下面是本文的主要结果.

定理 1 设 C 是一个 q-元 $[n,k]$-线性码. 如果存在 r 满足 $0<r<k$ 使得 C 是 r-等重码,那么 C 对任何 s 满足 $0<s<k$ 都是 s-等重码.

在证明主要结果之前,给出两个显然的推论.

按定义,一个线性码 C 称为是投射码,如果 C 的生成矩阵的任意两列线性无关,进一步,k 维线性码 C 称为极大投射码是指它是一个投射码并且在相同维数的投射码中它的码长达到极大. 极大投射码的码长必须等于 $(q^k-1)/(q-1)$;并且

收稿日期:2002-05-15;修回日期:2002-09-10
基金项目:国家"973"计划项目(No. G19990751)

除了 $k=1$ 这种特殊情况以外,这样一个码就是 Hamming 码的对偶码,参看文[6, p36].

以码 C 的所有码字为行向量的矩阵 C 称为码的码矩阵;把码矩阵 C 并排重复 s 次,再并排或不并排一个零矩阵,得矩阵$(C, \cdots, C, 0)$,对应的码称为码 C 的重复码. 结合文[3]的定理 1(1),从本文定理 1 马上得如下推论.

推论 1 如果 k 维线性码 C 对某个 $r, 0<r<k$,是 r-等重码,则 C 单项等价于极大投射码的重复码.

另一方面,结合文献[5]给出的广义 Plotkin 界和文[3]的定理 1(2),本文定理 1 的另一显然推论如下.

推论 2 设 C 是$[n, k]$线性码,并设 $n'=w(C)$ 为 C 的有效位数. 下面三条彼此等价:

(a) 存在一个 $r, 0<r<k$,使得 $d_r(C)=n\,q^{k-r}(q^r-1)/(q^k-1)$;

(b) 对任何 $r, 0<r<k$,都有 $d_r(C)=n\,q^{k-r}(q^r-1)/(q^k-1)$;

(c) C 等价于一个无冗余位的极大投射码的重复码.

以下证明定理 1,证明的主要工具是定义在投射空间上的重值函数[7].

对于 F_q 上的任何 k-维向量空间 U,它的所有非零子空间按照子空间的包含关系构成投射空间 $PG(U)$. 为方便,记 $PG^r(U)$ 为 U 的所有 r-维子空间构成的集合;特别的 $PG^1(U)$ 是 U 的所有 1-维子空间构成的集合. 那么易得$|PG^r(U)|=s_r(q^k)$;这里

$$s_r(q^k)=\frac{(q^k-1)(q^k-q)\cdots(q^k-q^{r-1})}{(q^r-1)(q^r-q)\cdots(q^r-q^{r-1})}$$

特别的,$|PG^1(U)|=(q^k-1)/(q-1)$. 对任意的 $0\neq u\in U$,由 u 生成的子空间$\langle u\rangle$是 $PG^1(U)$ 的一个元素. 对 U 的一个子空间 V,显然 $PG^r(V)\subset PG^r(U)$ 对任意 $r\leq \dim V$. 特别的,$PG^1(V)\subset PG^1(U)$.

设 $m: PG^1(U)\to N$ 是从 $PG^1(U)$ 到非负整数集合 N 的一个函数. 用 $m^r: PG^r(U)\to N$ 记由函数 m 诱导出来的定义在 $PG^r(U)$ 上的非负整值函数,即,

$$m^r(V)=\sum_{L\in PG^1(V)} m(L),\quad \forall V\in PG^r(U). \tag{1}$$

设 C 是一个 q-元$[n, k]$-线性码;令 G 是 C 的一个生成矩阵. 将 G 分成 n 列:$G=(G_1, \cdots, G_n)$;则 G 的每一个非零列 G_i 对应了 $PG^1(F_q^k)$ 中的一个元素$\langle G_i\rangle\in PG^1(F_q^k)$,从而由 G 可以定义如下的一个函数:$m_G: PG^1(F_q^k)\to N$,这里

$$m_G(L)=|\{i\mid 1\leq i\leq n, G_i\neq 0, \langle G_i\rangle=L\}|,\quad \forall L\in PG^1(F_q^k). \tag{2}$$

对 $0<r<k$ 它诱导函数 $m_G^r: PG^r(F_q^k)\to N$,这里

$$m_G^r(V)=\sum_{L\in PG^1(V)} m_G(L),\quad \forall V\in PG^r(F_q^k). \tag{3}$$

虽然这个函数并不唯一地被码 C 决定,但不妨碍我们的讨论,因为如果 G 是 C 的另一个生成矩阵,则存在一个 $k\times k$ 的可逆矩阵 Q 使得 $G'=QG$,并且 Q 诱导投射空间 $PG^1(F_q^k)$ 上的一个保序的双射 T_Q,从而由 G 决定的函数 m_G 满足 $m_{G'}=m_G\circ T_Q$.

下面是本文的关键引理.

引理 1 设 U 是 F_q 上的 k-维线性空间. 则函数 $m: PG^1(U)\to N$ 是常值函数当且仅当它诱导的函数 $m^{k-1}: PG^{k-1}(U)\to N$ 是常值函数.

证明 必要性是显然的. 为证明充分性,可设 $U=F_q^k$,设 m^{k-1}是常值函数,通过等距码的已知结果来证明 m 是常值函数. 对 $L\in PG^1(U)$,若 $m(L)>0$ 就令 $u_L\in U=F_q^k$ 使得$\langle u_L\rangle=L$,以这些 u_L 为列向量并使每 u_L 重复 $m(L)$ 次构造矩阵 G;则 G 是 $k\times n$ 矩阵这里 $n=\sum_{L\in PG^1(U)} m(L)$,并且由它决定的函数 $m_G=m$. 首先断言集合 $R=\{u_L\mid m(L)>0\}$生成 $U=F_q^k$;因为如果 R 不生成 U,则存在 U 的两个超平面 W 和 W' 使得 $R\subseteq W$ 但 $R\not\subseteq W'$;从而显然可得 $m^{k-1}(W)>m^{k-1}(W')$,这与 m^{k-1}是常值函数矛盾. 由此断言知 G 的秩为 k. 于是以 G 为生成矩阵得线性码 C. 对 C 的任一非零码字 c 存在惟一非零 $y\in U$ 使得 $c=yG$,这里 y 写成列向量;那么由线性代数(参看文[3])知 c 的 Hamming 重量为

$$w(c)=w(yG)=n-m_G^{k-1}(\langle y^{\perp}\rangle) \tag{4}$$

其中 $y^{\perp}$记 y 的在 $U=F_q^k$ 的典型内积之下的正交子空间,故 $y^{\perp}$为 U 的 $k-1$ 维子空间. 但由假设,$m_G^{k-1}=m^{k-1}$是常值函数,所以 C 是等距线性码. 那么由文[3]的定理 1,码 C 的生成矩阵 G 的列向量中每个 u_L 重复次数彼此相等. 即 $m=m^1$ 是常值函数.

最后,定理 1 将从下述结果推出.

定理 2 设 U 是 F_q 上的 k-维向量空间,并且 $m: PG^1(U)\to N$ 是一个函数,而 $m^r: PG^r(U)\to N$ 是由 m 诱导的函数. 则下面两条等价:

(a) 存在一个 $r, 0<r<k$,使得函数 $m^r: PG^r(U)\to N$ 是常值函数.

(b) 对任意 $r, 0<r<k$,函数 $m^r: PG^r(U)\to N$ 是常值函数.

证明 显然只须证明,如果 $m^r: PG^r(U)\to N$ 是常值函数,则 $m: PG^1(U)\to N$ 是常值函数. 由上面的引理 1,对 U 的任何维数为 $r+1$ 的子空间 V,限制函数 $m|_{PG^1(V)}: PG^1(V)\to N$ 是一个常值函数. 因为 $r+1\geq 2$,对任何 $L, L'\in PG^1(U)$ 能够找到 U 的维数为 $r+1$ 的子空间 V 和 V' 使得 $L\in PG^1(V)$ 且 $L'\in PG^1(V')$,并且 $PG^1(V)\cap PG^1(V')\neq 0$;从而存在 $L''\in PG^1(V)\cap PG^1(V')$;于是得到 $m(L)=m(L'')=m(L')$.

定理 1 的证明 令 G 是线性码 C 的生成矩阵,并把 G 按列写出 $G=(G_1, \cdots, G_n)$;设 $m_G: PG(F_q^k)\to N$ 是由 G 决定的函数,见式(2),(3). 设 D 是 C 的任意一个 r 维线性子码. 那么存在 F_q^k 的惟一一个 r 维子空间 V 使得 $D=\{yG\mid y\in V\}$. 类似于式(4),由内积计算知 $w(D)=n-|\{i\mid 1\leq i\leq n, yG_i=0\quad \forall y\in V\}|$,即

$$w(D)=n-m_G^{k-r}(V^{\perp}) \tag{5}$$

其中 $V^{\perp}$是 V 在 F_q^k 的典型内积之下的正交子空间,故 $V^{\perp}$为 F_q^k 的 $k-r$ 维子空间. 如果 C 是 r-等重码,那么由式(5)知 m_G 诱导的函数 $m_G^{k-r}: PG^{k-r}(F_q^k)\to N$ 是常值函数;于是由定理 2 得知对任意 s 满足 $0<s<k$ 都可断言函数 $m_G^{k-s}: PG^{k-s}(F_q^k)$

$\to N$ 是常值函数;所以仍由式(5)(它对一切 $0 < r < k$ 都成立),得到 C 是 s-等重码.

参考文献:

[1] 杨义先,胡正名. 线性等重码的结构分析[J]. 电子学报,1990,18(6):1 - 8.

[2] 符方伟,夏树涛. 等距码的对偶距离分布及其性质[J]. 通信学报,1998,19(2):1 - 5.

[3] 樊恽,刘宏伟. 线性等距码与极大投射码[J]. 通信学报,2001,22(6):48 - 52.

[4] V K Wei. Generalized Hamming weights for linear codes [J]. IEEE Trans. Inform. Theory, Sept. 1991, 37:1412 - 1418.

[5] G Cohen, S, Litsyn, G Zemor. Upper bounds on generalized distances [J]. IEEE Trans. Inform. Theory, Nov. 1994. 2090 - 2092.

[6] J H Van LINT. Introduction to Coding Theory [M]. GTM86, New York: Springer-Verlag, 1982.

[7] H G Scaathun. Duality and weights of liner codes and projective multi-sets [R]. Report No 211, May, 2001, ISSN 0333 - 3590, University of Bergen, Norway.

作者简介:

樊　恽　男,1946 年 3 月生于湖北省武汉市,教授,博士生导师;1978 年入武汉大学数学系读研究生,1981 - 1989 年在武汉大学数学系任讲师,副教授,1989 - 1995 年在湖北大学任副教授,教授,数学系主任,1996 年至今在武汉大学数学系工作;从 1986 年至今任美国《数学评论》评论员;发表论文 50 余篇,主编、参与编撰著作 5 本;研究方向:代数、组合、编码、算法等.

刘宏伟　男,1969 年 12 月生于湖北广水市,讲师,博士;1992 年毕业于湖北大学数学系,2000 年于武汉大学获得理学硕士学位,2000 年 9 月至 2003 年 6 武汉大学数学系攻读博士学位;目前在华中师范大学数学与统计学院工作,发表论文 6 篇;研究方向:群表示论、编码、算法等.