

仿射簇上的码的参数^{*}

吴新文

(中国科学院数学研究所, 北京 100080)

摘要 给出了仿射簇上的码的广义 Hamming 重量的一个下界, 这类码由簇上适当的有理多项式列所定义.

关键词 仿射簇 簇上的码 广义 Hamming 重量

众所周知, 代数几何码由代数曲线上的适当的有理函数的赋值向量所定义^[1]. 可以存在性地证明存在渐近好的代数几何码超过 Gilbert-Varshamov 界^[1], 这是近年编码理论中的一个重要结果. 但是迄今为止, 这样的代数几何码的具体构造还未找到^[2]. 通过所谓的单项式的良性序列, 可以构造一类仿射曲线上的码^[3], 这种码包含 Hermite 曲线上的单点代数几何码作为特殊情形. 由良性序列定义的码是具体构造的, 而且良性序列的条件使得估计码的最小距离变得十分容易. 但是, 良性序列的条件对于估计码的最小距离并不是必要的. 本文研究一类仿射簇上的码, 它们是由良性序列定义的码的推广, 且包含重量 Reed-Muller 码^[4]和 Reed-Muller 码^[5]作为特殊情形. 将给出这类码的广义 Hamming 重量的一个估计.

广义 Hamming 重量在文献[6]中被首次定义, 但是不可约循环码的最小支撑重量的概念在较早的文献[7]中就出现了. 对于一个固定的线性码, 广义 Hamming 重量恰好就是它的最小支撑重量. 对于一个 $[n, k]$ 线性码 C , 若 $r \leq k$, 则它的第 r 个广义 Hamming 重量定义为

$$d_r(C) = \min\{|\mathcal{X}(D)| \mid D \text{ 是 } C \text{ 的 } r \text{ 维子码}\},$$

其中 $\mathcal{X}(D) = \{i \mid \exists c = (c_1, \dots, c_i, \dots, c_n) \in D, c_i \neq 0\}$ 是码 D 的支撑, $|\mathcal{X}(D)|$ 是它的支撑重量. 显然, 码 C 的第一个广义 Hamming 重量 $d_1(C)$ 恰好就是它的最小距离. 广义 Hamming 重量的许多性质, 例如对偶性, 可以在文献[6]中找到.

1 码的构造

设 T 是域 F 上的多项式环 $F[x_1, \dots, x_m]$ 的一个子集, T 的仿射零点的集合定义为

$$Z(T) = \{P \in F^m \mid f(P) = 0, \forall f \in T\}.$$

设 I 是 $F[x_1, \dots, x_m]$ 的一个理想, 则称 $V = Z(I)$ 为一个仿射簇(或简单地称为簇), 由 Hilbert 基定理^[8]可知, 域上多项式环的每个理想都是有限生成的, 故存在有限多个多项式 $f_1(x_1, \dots, x_m), \dots, f_s(x_1, \dots, x_m)$, 使得 $I = \langle f_1(x_1, \dots, x_m), \dots, f_s(x_1, \dots, x_m) \rangle$. 所以 V 是

多项式方程组 $f_1(x_1, \dots, x_m)=0, \dots, f_s(x_1, \dots, x_m)=0$ 的公共根的集合.

设 V 是 F^m 中的一个簇, V 的定位理想定义为 $\bar{I}=\{g \in F[x_1, \dots, x_m] \mid g(P)=0, \forall P \in V\}$. 显然, $\bar{I}$ 是一个理想且 $V=Z(\bar{I})$. 事实上, V 的定位理想是满足条件 $I \subseteq \bar{I}$ 和 $V=Z(\bar{I})$ 的极大理想. 因为 $V=Z(I)=Z(\bar{I})$, 在下文中, 为方便起见, 假定式 $V=Z(I)$ 中的理想 I 就是 V 的定位理想.

V 在 F 上的坐标环定义为 $F[x_1, \dots, x_m]/I$, 以 $F[V]$ 记之. V 在 F 上的函数域定义为 $F[V]$ 的分式域, 记之为 $F(V)$. 函数域 $F(V)$ 中的元素称为 V 上的有理函数. 在下文中, 考虑 $F[x_1, \dots, x_m]$ 中的一类多项式, 此类多项式中的每一个多项式的每一项的系数都为 1, 显然, 这样一个多项式也可以视为 V 上的一个有理函数, 称它为 V 上的有理多项式.

设 V 是有限域 F_q 上的一个簇, 设它有 n 个仿射零点, 适当地排列成 $P_1, \dots, P_n$. 对于簇 V 上的任意有理多项式 h , 向量 $\mathbf{h}=(h(P_1), \dots, h(P_n))$ 称为 h 的赋值向量. 设 $\prec$ 是 V 上所有的有理多项式的集合的一个全序, 可以如下构造簇 V 上的码:

定义 1.1 设 $H=\{h_1, h_2, \dots, h_n\}$ 是 V 上的一系列有理多项式, 满足条件:

(1) $h_1 \prec h_2 \prec \dots \prec h_n$, 即 H 是一个有序列,

(2) $h_1, \dots, h_n$ 在 F_q 上线性无关.

对任意 $k, 1 \leq k \leq n$, 设 E_k 是由 $h_1, \dots, h_k$ 生成的 q 元码, C_k 是 E_k 的对偶码, 称 E_k 和 C_k 为簇 V 上的码.

显然码 E_k 和 C_k 的码长等于 n , 而 E_k 和 C_k 的维数分别为 k 和 $n-k$. 只需研究码的另一类参数, 即最小距离和广义 Hamming 重量.

2 重量分次序

注意到在上节码的定义中, 有理多项式由一个全序排成有序列, 本节将定义一种有理多项式的重量分次序.

设 R 是域 F 上的一个代数. 记由全体非负整数构成的集合为 N . 设 ρ 是一个适当定义的函数:

$$\rho: R \rightarrow N \cup \{-\infty\},$$

对任意 $f, g \in R$, 满足下列条件:

(1) $\rho(f)=-\infty$, 当且仅当 $f=0$;

(2) 对任意 $\lambda \in F$, $\rho(\lambda f)=\rho(f)$;

(3) $\rho(f+g) \leq \max\{\rho(f), \rho(g)\}$, 当 $\rho(f) \neq \rho(g)$ 时, 等号成立;

(4) $\rho(fg)=\rho(f)+\rho(g)$,

称 ρ 为 R 上的一个重量次数函数, 称 $\rho(f)$ 为 f 的重量次数 (或简单地称为 f 的重量).

文献[5]定义了序函数和重量函数. 容易看出重量次数函数是序函数和重量函数的推广.

看几个例子. 取 $R=F[x_1, \dots, x_m]$, 则 $\rho(f)=\deg f$ 是一个重量次数函数, 其中 $\deg$ 是通常意义下的多项式的次数. 设 $w_1, \dots, w_m$ 是一组固定的整数, 则 $\rho(f(x_1, \dots, x_m))=\deg f(x_1^{w_1}, \dots, x_m^{w_m})$ 也是一个重量次数函数. 考虑 F_4^2 上的平面 Hermite 曲线 $\mathcal{H}$

$$x^5 + y^4 + y = 0.$$

容易看出在 $F_q^2[x, y]/I$ 上存在一个重量次数函数 ρ , 使得 $\rho(x)=4$, $\rho(y)=5$, 而 $\rho(x^i y^j)=4i+5j$, 其中 I 为 $\mathcal{R}$ 的定位理想.

设 ρ 为多项式代数 R 上的一个重量次数函数. 考虑 R 中的所有的单项式的集合 S , 可以定义一个重量分次(字典)序 $<$ 如下:

$$x_1^{i_1}, \dots, x_m^{i_m} < x_1^{j_1}, \dots, x_m^{j_m}$$

当且仅当下列条件之一成立:

$$(1) \rho(x_1^{i_1}, \dots, x_m^{i_m}) < \rho(x_1^{j_1}, \dots, x_m^{j_m}),$$

(2) $\rho(x_1^{i_1}, \dots, x_m^{i_m}) = \rho(x_1^{j_1}, \dots, x_m^{j_m})$, 但存在 $l (1 \leq l \leq m)$, 使得对于 $l+1 \leq k \leq m$, $i_k = j_k$, 但 $i_l < j_l$.

显然重量分次序 $<$ 是一个单项式全序, 而且它可以自然地扩展成 R 中的有理多项式集合上的一个全序.

由码的定义不难发现, 由良性序列定义的码^[3] 是簇上的码的特例. 簇上的码也包含单点代数几何码以及重量 Reed Muller 码^[4] 为特例.

例 2.1(单点代数几何码) 有限域 F_q 上的平面 Hermite 曲线 $\mathcal{H}_q$ 由下列射影方程定义:

$$X^{q+1} + Y^q Z + YZ^q = 0. \quad (2.1)$$

这条曲线有 $n = q^3$ 个仿射 F_q^2 -有理点, 另外, 无穷远点 $P_\infty = (0:1:0)$ 也是它的一个有理点. 设 $D = P_1 + \dots + P_n$ 和 $G = mP_\infty$ 为曲线上的两个除子, 考虑单点代数几何码 $C_\Omega(D, mP_\infty)$. 设 $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, 则 x 和 y 以 P_∞ 为极点, 且它们的极点的重数分别是

$$\text{ord}_{P_\infty}(x) = q, \quad \text{ord}_{P_\infty}(y) = q+1,$$

可以证明

$$\mathcal{B}(m) = \{x^i y^j \mid 0 \leq i \leq q^2 - 1, 0 \leq j \leq q - 1, qi + (q+1)j \leq m\}$$

是 $L(mP_\infty)$ 的一组基. 设 $|\mathcal{B}(m)| = r$, 并记 $\mathcal{B}(m) = \{h_1, h_2, \dots, h_r\}$, 其中 $\text{ord}_{P_\infty}(h_i) < \text{ord}_{P_\infty}(h_{i+1})$, 则 $C_\Omega(D, mP_\infty)$ 定义为

$$C_\Omega(D, mP_\infty) = \{c \in F_q^n \mid c \circ h_i = 0, 1 \leq i \leq r\}, \quad (2.2)$$

其中 h_i 是 h_i 在 D 上的赋值向量.

另一方面, Hermite 曲线的仿射方程为

$$x^{q+1} + y^q + y = 0.$$

设 I 为 $\mathcal{H}_q$ 的定位理想, 容易看到在 $R = F_q^2[x, y]/I$ 上存在一个重量次数函数 ρ , 使得

$$\rho(x) = q, \quad \rho(y) = q+1, \quad \rho(x^i y^j) = qi + (q+1)j.$$

设 $<$ 为重量分次序. 取 $H = \{h_1, \dots, h_n\} = \{x^i y^j \mid 0 \leq i \leq q^2 - 1, 0 \leq j \leq q - 1\}$, 其中 $h_i < h_{i+1}$, 则 H 满足定义 1.1 中的条件(1)和(2), 所以对任意 r , $1 \leq r \leq n$, 可以定义码 C_r . 由(2.2)式看出

$$C_\Omega(D, mP_\infty) = C_r.$$

例 2.2(重量 Reed-Muller 码^[4]) 设 $\omega_1, \dots, \omega_m$ 为一组自然数, $\omega_1 \leq \omega_2 \leq \dots \leq \omega_m$. 对任意 $f(x_1, \dots, x_m) \in F_q[x_1, \dots, x_m]$, 定义 $\deg_\omega f(x_1, \dots, x_m) = \deg f(x_1^{\omega_1}, \dots, x_m^{\omega_m})$. 设 $n = q^m$, 考虑赋值映射

$$\phi: F_q[x_1, \dots, x_m] \rightarrow F_q^n,$$

其中 $\phi(f) = (\dots, f(P_i), \dots)$, P_i 取遍空间 F_q^m . 设 $V(\omega) = \{f \in F_q[x_1, \dots, x_m] \mid \deg_{\omega} f \leq \omega\}$. 重量 Reed-Muller 码 $WRM(\omega, m, q)$ 定义为

$$WRM(\omega, m, q) = \phi(V(\omega)). \quad (2.3)$$

设 $I = (0)$ 为 $F_q[x_1, \dots, x_m]$ 的零理想, 则 $V = Z(I) = F_q^m$, 而 $\rho = \deg_{\omega}$ 是 $F_q^m[x_1, \dots, x_m]$ 上的一个重量次数函数. 取 $H = \{h_1, h_2, \dots\} = \{x_1^{i_1}, \dots, x_m^{i_m} \mid 0 \leq i_k \leq q-1, k=1, \dots, m\}$, 其中 $h_i < h_{i+1}$, 则 H 满足定义 1.1 中的条件 (1) 和 (2), 所以可以定义码 E_k . 设 $|\{h_i \in H \mid \rho(h_i) \leq \omega\}| = k$, 则由 (2.3) 式有

$$WRM(\omega, m, q) = E_k.$$

因为重量 Reed-Muller 码是 Reed-Muller 码^[5]的推广, 所以簇上的码也包含 Reed-Muller 码为特例. 事实上, 在上例中若取 $\omega_1 = \omega_2 = \dots = \omega_m = 1$, 就得到通常的 Reed-Muller 码.

3 码的参数估计

假定 $V = Z(I)$ 是 F_q^m 中的一个簇, 设它有 n 个仿射零点. 设 ρ 是 $R = F_q^m[x_1, \dots, x_m]/I$ 上的一个重量次数函数. 设 $H = \{h_1, \dots, h_n\}$ 是 V 上一列有理多项式, 满足定义 1.1 中的条件 (1) 和 (2) 以及条件

$$(3) \quad h_1 = 1, \quad \rho(h_1) < \rho(h_2) < \dots < \rho(h_n).$$

本节研究码 E_k 的广义 Hamming 重量.

设 $\{h_i \mid i=1, \dots, k\} \subseteq H$ 为 V 上的一列有理多项式. 对 $r \leq k$, 记 $D_{\{h_1, h_2, \dots, h_r\}}$ 为方程组 $h_1 = h_2 = \dots = h_r = 0$ 在 F_q^m 中的根的个数, 要求这些根同时是 V 的仿射零点. 设 $[h_{i_{\mu}}]$ 表示 $h_1, h_2, \dots, h_{i_{\mu}-1}, h_{i_{\mu}}$ 的任意一个线性组合, 使得 $h_{i_{\mu}}$ 的系数为 1, 即

$$[h_{i_{\mu}}] = h_{i_{\mu}} + \sum_{j=1}^{i_{\mu}-1} \alpha_j h_j,$$

其中系数 $\alpha_j (j=1, \dots, i_{\mu}-1)$ 为 F_q 中的任意元素. 定义

$$D_r^{(k)} = \max\{D_{\{[h_{i_1}], \dots, [h_{i_r}]\}} \mid i_1, \dots, i_r \leq k\}.$$

定理 3.1 对任意 $r, 1 \leq r \leq k$, 有

$$d_r(E_k) = n - D_r^{(k)}.$$

证 由码的定义和广义 Hamming 重量的定义直接得到.

引理 3.1 设 $Q_1, \dots, Q_t$ 是 F_q^m 中的 t 个不同的点, $b_1, \dots, b_t$ 为 F_q 中的任意 t 个元素, 则存在多项式 $p \in F_q^m[x_1, \dots, x_m]$, 使得 $p(Q_i) = b_i, i=1, \dots, t$.

证 设 $Q = (a_1, \dots, a_m)$ 为 F_q^m 中的一个点, 取 $p_Q = \prod_{i=1}^m [1 - (x_i - a_i)^{q-1}]$, 则有: 当 $P = Q$ 时, $p_Q(P) = 1$; 当 $P \neq Q$ 时, $p_Q(P) = 0$. 称 p_Q 为 Q 点处的指标多项式. 设 p_{Q_i} 是 $Q_i (i=1, \dots, t)$ 点处的指标多项式. 取

$$p(x_1, \dots, x_m) = \sum_{i=1}^t b_i p_{Q_i}(x_1, \dots, x_m),$$

则 $p(x_1, \dots, x_m)$ 为满足引理的多项式.

引理 3.2 设 $f_1, \dots, f_k$ 为多项式且它们不属于 I , 记 $\langle f_1, \dots, f_k \rangle$ 为 $f_1, \dots, f_k$ 生成的理想, 则

$$D_{\{f_1, \dots, f_k\}} \leq \dim(R / \langle f_1, \dots, f_k \rangle).$$

证 设 $D_{\{f_1, \dots, f_k\}} = t$ 且 $\{Q_1, \dots, Q_t\}$ 为 $f_1, \dots, f_k$ 的公共零点的集合, 其中每个 Q_μ 也是 I 的仿射零点. $R / \langle f_1, \dots, f_k \rangle$ 是 F_q 上的一个线性空间. 设 $\dim(R / \langle f_1, \dots, f_k \rangle) = l$, 且 $\{p_\nu(x_1, \dots, x_m) \mid \nu = 1, \dots, l\}$ 为 $R / \langle f_1, \dots, f_k \rangle$ 的一组基. 每一个 $p(x_1, \dots, x_m) \in R / \langle f_1, \dots, f_k \rangle$ 可以唯一地表成 $p = \sum_{\nu=1}^l a_\nu p_\nu$. 所以 $R / \langle f_1, \dots, f_k \rangle$ 中的每个元素 p 唯一地对应着 F_q^l 中的一个向量 $a = (a_1, \dots, a_l)^T$.

设 $b = (b_1, \dots, b_t)^T$, 其中 $b_\mu = p(Q_\mu)$, $\mu = 1, \dots, t$, 则有线性关系 $b = Pa$, 其中 P 是一个 $t \times l$ 矩阵 $(P_{\mu\nu})$, $P_{\mu\nu} = p_\nu(Q_\mu)$, $\mu = 1, \dots, t$, $\nu = 1, \dots, l$, 而 $a = (a_1, \dots, a_l)^T$. 所以, 存在线性映射

$$P: F_q^l \rightarrow F_q^t, \quad (a_1, \dots, a_l)^T \mapsto (b_1, \dots, b_t)^T = (P_{\mu\nu})(a_1, \dots, a_l)^T. \quad (3.1)$$

由引理 3.1, 对任意 $(b_1, \dots, b_t)^T \in F_q^t$, 存在多项式 $p'(x_1, \dots, x_m) \in F_q[x_1, \dots, x_m]$, 使得 $p'(Q_\mu) = b_\mu$, $\mu = 1, \dots, t$. 由于 I 中每个多项式以及 $\langle f_1, \dots, f_k \rangle$ 中的每个多项式都以 $Q_1, \dots, Q_t$ 为零点, 所以 $p'(x_1, \dots, x_m)$ 投影到 $R / \langle f_1, \dots, f_k \rangle$ 中的一个多项式 $p(x_1, \dots, x_m)$, 使得 $p(Q_\mu) = p'(Q_\mu) = b_\mu$. 所以, 对任意 b , 存在元素 $p \in R / \langle f_1, \dots, f_k \rangle$, 其中 p 对应着 a , 使得 $Pa = b$. 这说明映射 (3.1) 式是一个满射. 所以 $t \leq l$, 即

$$D_{\{f_1, \dots, f_k\}} \leq \dim(R / \langle f_1, \dots, f_k \rangle).$$

引理 3.3 向量空间 $F_q[x_1, \dots, x_m] / I$ 的维数等于 n , 即 V 的仿射零点的个数. 特别地, H 构成 $F_q[x_1, \dots, x_m] / I$ 的一组基.

证 记 $V = \{P_1, \dots, P_n\}$. 假设 $\dim(F_q[x_1, \dots, x_m] / I) = l$. 和引理 3.2 的证明类似, $F_q[x_1, \dots, x_m] / I$ 中的每个元素 $p(x_1, \dots, x_m)$ 唯一地对应着 F_q^l 中的一个向量 $(a_1, \dots, a_l)^T$, 而且存在线性映射

$$P: F_q^l \rightarrow F_q^n, \quad (a_1, \dots, a_l)^T \mapsto (b_1, \dots, b_n)^T, \quad (3.2)$$

其中 $b_\mu = p(P_\mu)$, $\mu = 1, \dots, n$, P 是一个满射.

设 $p'(x_1, \dots, x_m)$ 为 $F_q[x_1, \dots, x_m]$ 中的多项式, 它投影到 $F_q[x_1, \dots, x_m] / I$ 中的元素 $p(x_1, \dots, x_m)$. 如果 $(b_1, \dots, b_n)^T = 0$, 即 $p(P_1) = p(P_2) = \dots = p(P_n) = 0$, 则 $p'(P_1) = \dots = p'(P_n) = 0$. 所以 $p'(x_1, \dots, x_m) \in I$, 因为 I 为 V 的定位理想. 这说明 $p(x_1, \dots, x_m) = 0$, 即 $(a_1, \dots, a_n)^T = 0$. 所以 P 是一个单射. 从而 $\dim(F_q[x_1, \dots, x_m] / I) = n$.

因为 $h_1, \dots, h_n$ 在 I 的零点上的赋值向量 $h_1, \dots, h_n$ 线性无关, 所以, 作为 $F_q[x_1, \dots, x_m] / I$ 中的元素, $h_1, \dots, h_n$ 线性无关. 所以 H 是 $F_q[x_1, \dots, x_m] / I$ 的一组基.

定理 3.2 对任意 $h_i \in H$, 有

$$D_{\{h_i\}} \leq \rho(h_i).$$

证 记 R 中的元素的重量集合为 $W = \rho(R) = \{\rho_1, \rho_2, \dots\}$, 假设 $\rho_1 < \rho_2 < \dots$. 理想 $\langle [h_i] \rangle$ 中的元素的重量集合为 $\rho(\langle [h_i] \rangle) = \{\rho(h) \mid h \in \langle [h_i] \rangle\} = \{\rho([h_i]g) \mid g \in R\} = \{\rho([h_i]) + \rho(g) \mid g \in R\} = \rho([h_i]) + W = \rho(h_i) + W$, 其中等式 $\rho([h_i]) = \rho(h_i)$ 根据 $[h_i]$ 的定义以及条件 $\rho(h_1) < \dots < \rho(h_n)$ 得到.

考虑集合 $\mathcal{B} = \{f_\mu \in R \mid \rho(f_\mu) = \rho_\mu \in W\}$. 可以证明 $\mathcal{B}$ 中的任意有限多个元素线性无关. 事实上, 如果 $f_{\mu_1}, \dots, f_{\mu_l} (\mu_1 < \dots < \mu_l)$ 线性相关, 不失一般性, 假设 $f_{\mu_l} = a_{l-1}f_{\mu_{l-1}} + \dots + a_1f_{\mu_1}$, 其中 $a_{l-1} \neq 0$, 则 $\rho(f_{\mu_l}) = \rho(f_{\mu_{l-1}})$. 但这是不可能的, 因为对 $\mu \neq \nu$, 有 $\rho(f_\mu) \neq \rho(f_\nu)$. 另一方面, $\rho(H) \subseteq \rho(\mathcal{B}) = W$. 所以, $|H| \leq |\mathcal{B}|$. 由引理 3.3, 知 $\dim R = |H| \leq |\mathcal{B}|$. 所以 $\mathcal{B}$ 是 R 的一组基. 因为 $\langle [h_i] \rangle = \{g[h_i] \mid g \in R\} = [h_i]R$. 类似地可以证明 $\mathcal{C} = \{f_\mu \in \langle [h_i] \rangle \mid \rho(f_\mu) \in \rho(h_i) + W\}$ 是 $\langle [h_i] \rangle$ 的一组基. 进一步, 由于 $\langle [h_i] \rangle$ 是 R 的子空间, 可以假设 $\mathcal{B}$ 是 $\mathcal{C}$ 的扩张 (子空间的基可以扩张成整个空间的一组基), 即 $\mathcal{C} \subseteq \mathcal{B}$. 因此, 所有的 f_μ 对 $\langle [h_i] \rangle$ 的剩余类的集合构成 $R/\langle [h_i] \rangle$ 的一组基, 其中 $\rho(f_\mu) \in W - (\rho(h_i) + W)$. 所以 $R/\langle [h_i] \rangle$ 的维数小于或等于 $W - (\rho(h_i) + W)$ 的元素个数.

另一方面, $0 = \rho(h_i) \in W$; 且对任意 $\rho_\mu = \rho(f) \in W$ 及 $\rho_\nu = \rho(g) \in W$, 有 $\rho_\mu + \rho_\nu = \rho(fg) \in W$. 所以 $W - (\rho(h_i) + W)$ 的元素个数至多为 $\rho(h_i)$. 这说明 $\dim(R/\langle [h_i] \rangle) \leq \rho(h_i)$. 由引理 3.2, $D(\langle [h_i] \rangle) \leq \dim(R/\langle [h_i] \rangle)$. 因此,

$$D(\langle [h_i] \rangle) \leq \rho(h_i).$$

下列推论给出簇上的码的最小距离的一个下界.

推论 3.1 码 E_k 的最小距离至少为 $n - \rho(h_k)$, 即

$$d(E_k) \geq n - \rho(h_k).$$

设 λ 为一条代数曲线, λ 的第 r 个度数定义为^[9]

$$\gamma_r = \min\{\deg A \mid A \text{ 为曲线 } \lambda \text{ 的除子且 } \dim A \geq r\}.$$

在下面的讨论中, 考虑这样的曲线: 它有 n 个仿射零点 $P_1, \dots, P_n$, 还有一个有理点 P 在无穷远处. 设 $H = \{h_1, \dots, h_n\}$ 为一列有理多项式, 每个 h_i 以 P 为其唯一的极点.

定理 3.3 对 $1 \leq k \leq n$, $r \leq k$,

$$D_r^{(k)} \leq \rho_k - \gamma_r,$$

其中 $\rho_k = \rho(h_k)$.

证 设 $N = D_r^{(k)} = D(\langle [h_1], \dots, [h_r] \rangle)$, 其中 $N \leq n$. 由定义, 方程组 $[h_1] = \dots = [h_r] = 0$ 有 N 个不同的根, 不失一般性, 设它们为 $P_1, \dots, P_N$. 设 $D = P_1 + \dots + P_N$, D 是曲线 λ 上的一个除子. 令 $G = mP$, 考虑空间 $L(G) = \{A \mid A \text{ 为 } \lambda \text{ 上的除子且 } A + G \geq 0\}$.

对每一个函数 $[h_j]$, $1 \leq j \leq r$, 考虑它的主除子 $([h_j]) = ([h_j])_0 - ([h_j])_\infty$, 其中 $([h_j])_0$ 和 $([h_j])_\infty$ 分别为 $[h_j]$ 的零点部分和极点部分. 由定理 3.2, $\deg([h_j])_0 = D(\langle [h_j] \rangle) \leq \rho(h_j) \leq \rho(h_k)$, 因为 $i_j \leq k$. 又因为 $\deg([h_j])_\infty = \deg([h_j])_0$, 所以 $\deg([h_j])_\infty \leq \rho(h_j) \leq \rho(h_k)$, 这说明函数 $[h_j]$ 在 P 点处的极点的重数不超过 $\rho(h_k)$, 所以

$$[h_j] \in L(\rho(h_j)P) \subseteq L(\rho(h_k)P).$$

另一方面, $P_1, \dots, P_N$ 为 $[h_i]$ 的零点, 所以存在有效除子 Q_j , 即满足 $Q_j \geq 0$ 的除子, 使得

$$([h_i]) + \rho(h_i)P = D + Q_j.$$

所以,

$$([h_i]) = D + Q_j + (\rho(h_k) - \rho(h_i))P - \rho(h_k)P,$$

其中 $(\rho(h_k) - \rho(h_i))P \geq 0$, 令 $Q'_j = Q_j + (\rho(h_k) - \rho(h_i))P$, 则有

$$([h_i]) = D + Q'_j - \rho(h_k)P,$$

其中 $Q'_j \geq 0$.

定义 $f_j = [h_i] / [h_i]$, 考虑有理函数 $f_1, \dots, f_r$. f_j 的主除子为

$$(f_j) = ([h_i]) - ([h_i]) = Q'_j - Q'_1.$$

所以, $(f_j) + Q'_1 = Q'_j \geq 0$, 这说明

$$f_j \in L(Q'_1).$$

另一方面, 由 $h_1, \dots, h_n$ 的线性无关性, 可证 $f_1, \dots, f_r$ 是线性无关的. 所以

$$\dim Q'_1 = \dim L(Q'_1) \geq r.$$

由 γ_r 的定义,

$$\deg Q'_1 \geq \gamma_r.$$

考虑 $([h_i])$ 的次数, 有

$$\deg([h_i]) = \deg(D + Q'_1 - \rho(h_k)P) =$$

$$\deg D + \deg Q'_1 - \deg(\rho(h_k)P) \geq D_r^{(k)} + \gamma_r - \rho_k.$$

另一方面, 由于任意主除子的次数为 0, 有 $\deg([h_i]) = \deg([h_i])_0 - \deg([h_i])_\infty = 0$, 所以, $0 \geq D_r^{(k)} + \gamma_r - \rho_k$, 即

$$D_r^{(k)} \leq \rho_k - \gamma_r.$$

由以上定理, 可得下列推论, 它给出码 E_k 的广义 Hamming 重量的一个下界:

推论 3.2 对于 $1 \leq r \leq k$, 有

$$d_r(E_k) \geq n - \rho_k + \gamma_r.$$

由广义 Hamming 重量的对偶性^[6], 也可以研究 C_k 的广义 Hamming 重量, 因为 C_k 是 E_k 的对偶码.

参 考 文 献

- 1 Tsfasman M A, Vladut S G, Zink T. Modular curves, Shimura curves and Goppa codes, better than the Varshamov-Gilbert bound. Math Nachr, 1982, 109: 21 ~ 28
- 2 Garcia A, Stichtenoth H. A tower of Artin-Schreier extension of function fields attaining the Drinfeld-Vladut bound. Invent Math, 1995, 121: 211 ~ 222
- 3 Feng G L, Rao T R N. Improved geometric Goppa codes Part I: Basis theory. IEEE Trans on Infor Theory, 1995, 41(6): 1 678 ~ 1 693
- 4 Sørensen A B. Weighted Reed-Muller codes and algebraic-geometric codes. IEEE Trans on Infor Theory, 1992, 38(6): 1 821 ~ 1 826
- 5 Heijnen P, Pelikaan R. Generalized Hamming weights of q -ary Reed Muller codes. IEEE Trans on Infor Theory, 1998, 44(1):

181 ~ 196

- 6 Wei V K. Generalized Hamming weights for linear codes. IEEE Trans on Infor Theory, 1991, 37(5): 1 412 ~ 1 418
- 7 Helleseth H, Kløve T, Mykkjelveit J. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$. Discrete Math, 1977, 18: 179 ~ 211
- 8 Becker T, Weispfenning V, Kredel H. Gröbner Bases——A Computational Approach to Commutative Algebra. New York: Springer-Verlag, 1993
- 9 Yang K, Kumar P V, Stichtenoth H. On the weight hierarchy of geometric Goppa codes. IEEE Trans on Infor Theory, 1994, 40(3): 913 ~ 920
- 10 Abhyankar S S. Algebraic Geometry for Scientists and Engineers. Providence: American Mathematical Society, 1990
- 11 Munuera C. On the generalized Hamming weights of geometric Goppa codes. IEEE Trans on Infor Theory, 1994, 40(6): 2 092 ~ 2 099