有限域上酉空间中子空间的不变量

万 哲 先

(中国科学院系统科学研究所,北京 100080)

关键词 酉空间、酉群、不变量

设 $\mathbf{F}_{q^2}$ 是含 q^2 个元素的有限域,这里 q 是一个素数的幂. 设

$$a \longmapsto \bar{a} = a^q, \tag{1}$$

$\mathbf{F}_{q^2}$ 的对合自同构,它的固定子域是 $\mathbf{F}_q$. $\mathbf{F}_{q^2}$ 上的 $n \times n$ 矩阵 H 叫做厄米特矩阵,如果

$$\bar{H}^T = H,$$

这里 $\bar{H}$ 表示将 H 的每个位置上的元素都用它在对合自同构(1)下的像来代替而得到的矩阵,而 $\bar{H}^T$ 表示 $\bar{H}$ 的转置矩阵. 两个 $n \times n$ 厄米特矩阵 H_1 和 H_2 叫做合同,如果 $\mathbf{F}_{q^2}$ 上有 $n \times n$ 非奇异矩阵 P,使 $H_1 = PH_2\bar{P}^T$. 熟知[1], $\mathbf{F}_{q^2}$ 上的 $n \times n$ 厄米特矩阵 H 一定和以下形状的一个矩阵合同:

$$\begin{pmatrix} I^{(r)} & \\ & 0^{(n-r)} \end{pmatrix},$$

这里 r 是 H 的秩. 因此两个 $n \times n$ 厄米特矩阵合同,当且仅当它们的秩相等.

设 H 是个 $n \times n$ 非奇异厄米特矩阵,定义

$$U_n(\mathbf{F}_{q^2}, H) = \{T : \mathbf{F}_{q^2} \text{ 上的 } n \times n \text{ 矩阵} \mid TH\bar{T}^T = H\}.$$

熟知[1], $U_n(\mathbf{F}_{q^2}, H)$ 对于矩阵乘法来说组成一群,叫做 $\mathbf{F}_{q^2}$ 上对于 H 的 n 级酉群,设 H_1 和 H_2 是两个 $n \times n$ 非奇异厄米特矩阵,并假设有 $n \times n$ 非奇异矩阵 P 使 $H_1 = PH_2\bar{P}^T$. 那么映射 $T \to P^{-1}TP$ 就是把 $U_n(\mathbf{F}_{q^2}, H_1)$ 映到 $U_n(\mathbf{F}_{q^2}, H_2)$ 之上的同构映射,因此只要讨论 $U_n(\mathbf{F}_{q^2}, I^{(n)})$ 就行了,下面我们把它简记作 $U_n(\mathbf{F}_{q^2})$.

设 $V_n(\mathbf{F}_{q^2})$ 是 $\mathbf{F}_{q^2}$ 上的 n 维行向量空间. 设 P 是 $V_n(\mathbf{F}_{q^2})$ 的一个 m 维子空间. 如果一个 $m \times n$ 矩阵的 m 个行向量组成 P 的一组基,就说它是子空间 P 的一个矩阵表示,并且仍用 P 来代表这个矩阵.

显然,映射

$$V_n(\mathbf{F}_{q^2}) \times U_n(\mathbf{F}_{q^2} \to V_n(\mathbf{F}_{q^2}),$$

$$((x_1, x_2, \cdots, x_n), T) \longmapsto (x_1, x_2, \cdots, x_n)T$$

是群 $U_n(\mathbf{F}_q)$ 在 $V_n(\mathbf{F}_{q^2})$ 上的一个群作用. $V_n(\mathbf{F}_{q^2})$ 带着这个作用就叫做 $\mathbf{F}_{q^2}$ 上的 n 维酉空间. 这个作用还诱导出 $V_n(\mathbf{F}_{q^2})$ 的子空间上的一个作用,使得 $T \in U_n(\mathbf{F}_{q^2})$ 将 $V_n(\mathbf{F}_{q^2})$ 的子空间 P 映到 PT. 熟知[2,3],两个子空间 P_1 和 P_2 在 $U_n(\mathbf{F}_{q^2})$ 的作用下可迁,当且仅当 $P_1\bar{P}_1^T$ 和 $P_2\bar{P}_2^T$ 合同. 因此子空间 P 的维数和矩阵 $P\bar{P}^T$ 的秩是 P 的一组全系不变量. 我们说子空间 P 是 (m, r) 型的,如果 $\dim P = m$ 而 $\operatorname{rank} P\bar{P}^T = r$.

本文 1990 年 9 月 21 日收到.

定理 1 $\mathbf{F}_{q^2}$ 上的 n 维酉空间中(m,r)型子空间存在，当且仅当

$$2r \leqslant 2m \leqslant n + r. \tag{2}$$

证 先假设条件(2)成立. 考察从 $\mathbf{F}_{q^2}^*$ 到 $\mathbf{F}_q^*$ 中的映射 $\varphi:\lambda \to \lambda\bar{\lambda}$. 显然，这是个群同态，它的核 $\ker\varphi = \{\lambda \in \mathbf{F}_{q^2}^* | \lambda\bar{\lambda} = \lambda^{q+1} = 1\}$ 的阶 $\leqslant q+1$，它的像 $\mathrm{Im}\varphi$ 是 $\mathbf{F}_q^*$ 的子群，因而 $\mathrm{Im}\varphi$ 的阶 $\leqslant q-1$. 可是

$$q^2 - 1 = |\mathbf{F}_{q^2}^*| = |\ker\varphi||\mathrm{Im}\varphi| \leqslant (q+1)(q-1) = q^2 - 1,$$

因此 φ 是满射. 特别，$\mathbf{F}_{q^2}$ 有一个元素 λ 使 $\lambda\bar{\lambda} + 1 = 0$. 那么在条件(2)成立的前提下，

$$\begin{matrix} \begin{pmatrix} I^{(r)} & 0 & 0 & 0 \\ 0 & I^{(m-r)} & \lambda I^{(m-r)} & 0 \end{pmatrix} \begin{matrix} r \\ m-r \end{matrix} \\ \begin{matrix} r & m-r & m-r & n-m \end{matrix} \end{matrix}$$

就是 $V_n(\mathbf{F}_{q^2})$ 中的 (m,r) 型子空间. 这证明了条件(2)的充分性.

反过来，假设 P 是 $V_n(\mathbf{F}_{q^2})$ 中的 (m,r) 型子空间，那么有一个 $m \times m$ 非奇异矩阵 Q，使

$$Q(P\bar{P}^T)\bar{Q}^T = \begin{pmatrix} I^{(r)} & \\ & 0^{(m-r)} \end{pmatrix},$$

于是 $r \leqslant m$. 总有一个 $(n-m) \times n$ 矩阵 Z，使

$$\begin{pmatrix} Q & P \\ Z & \end{pmatrix} \tag{3}$$

是 $n \times n$ 非奇异矩阵. 我们可以写

$$\begin{pmatrix} Q & P \\ Z & \end{pmatrix}\begin{pmatrix} \overline{Q} & P \\ Z & \end{pmatrix}^T = \begin{matrix} \begin{pmatrix} I & & H_{13} \\ & 0 & H_{23} \\ \bar{H}_{13}^T & \bar{H}_{23}^T & H_{33} \end{pmatrix} \begin{matrix} r \\ m-r \\ n-m \end{matrix} \\ \begin{matrix} r & m-r & n-m \end{matrix} \end{matrix},$$

这里 H_{33} 是个 $(n-m) \times (n-m)$ 厄米特矩阵. 我们有

$$\begin{aligned} &\begin{pmatrix} I & & \\ & I & \\ -\bar{H}_{13}^T & & I \end{pmatrix}\begin{pmatrix} I & & H_{13} \\ & 0 & H_{23} \\ \bar{H}_{13}^T & \bar{H}_{23}^T & H_{33} \end{pmatrix}\begin{pmatrix} I & & \\ & I & \\ -\bar{H}_{13}^T & & I \end{pmatrix}^T \\ &= \begin{matrix} \begin{pmatrix} I & 0 & 0 \\ 0 & 0 & H_{23} \\ 0 & \bar{H}_{23}^T & H_{33} - \bar{H}_{13}^T H_{13} \end{pmatrix} \begin{matrix} r \\ m-r \\ n-m \end{matrix} \\ \begin{matrix} r & m-r & n-m \end{matrix} \end{matrix}, \end{aligned} \tag{4}$$

因为(3)式是非奇异矩阵，所以(4)式也是非奇异矩阵. 因此 $\mathrm{rank}H_{23} = m - r$. 可是 H_{23} 是 $(m-r) \times (n-m)$ 矩阵，所以 $m - r \leqslant n - m$，于是 $2m \leqslant n + r$. 将这个不等式和上面得到的不等式 $r \leqslant m$ 合并，就得到 $2r \leqslant 2m \leqslant n + r$. 这证明了条件(2)的必要性.

定理 2 $V_n(\mathbf{F}_{q^2})$ 的子空间在 $U_n(\mathbf{F}_{q^2})$ 的作用下所分成的可迁集的个数等于

$$\begin{cases} ([n/2]+1)^2, & \text{如果 } n \text{ 是偶数}, \\ ([n/2]+1)([n/2]+2), & \text{如果 } n \text{ 是奇数}. \end{cases}$$

证 根据定理 1，$V_n(\mathbf{F}_{q^2})$ 的子空间在 $U_n(\mathbf{F}_{q^2})$ 的作用下所分成的可迁集的个数等于非负整数对 (m, r) 适合条件 $2r \leqslant 2m \leqslant n + r$ 的个数. 但条件 (2) 等价于 $2m - n \leqslant r \leqslant m$. 对于任一给定的 m 使 $0 \leqslant m \leqslant n$，如果 $2m \leqslant n$，则 r 可以取 $m+1$ 个值：$0, 1, \cdots, m$；如

果 $2m > n$，则 r 可以取 $n-m+1$ 个值 $2m-n, 2m-n+1, \cdots, m$。因此适合条件 $2r \leqslant 2m \leqslant n+r$ 的非负整数对 (m,r) 的个数等于

$$\sum_{m=0}^{[n/2]}(m+1)+\sum_{m=[n/2]+1}^{n}(n-m+1)=\begin{cases}([n/2]+1)^2, & \text{如果 } n \text{ 是偶数;}\\ ([n/2]+1)([n/2]+2), & \text{如果 } n \text{ 是奇数。}\end{cases}$$

参 考 文 献

[1] Dickson, L. E., *Linear Groups*, Teubner, 1900.

[2] Dieadonné, J., *Sur les Groupes Classiques*, Hermann, 1948.

[3] 华罗庚、万哲先，典型群，上海科技出版社，1963.