

中国科学院数学研究所专刊

甲种

第6号

有限几何与不完全区组 设计的一些研究

万哲先 戴宗铎 馮緒宁 陽本傳

科学出版社

內 容 簡 介

本书是用代数方法討論了一些与数理統計有关的問題。

本书前五章討論有限域上辛几何、酉几何和正交几何中的計数定理,同时介紹了經典的計数定理。后五章則利用有限域上各种类型的几何构造結合方案和部分平衡不完全区組設計,并計算了它們的参数。

有限几何与不完全区組 設計的一些研究

万 哲 先 戴 宗 鐸 著
馮 緒 宁 阳 本 傳

*

科 学 出 版 社 出 版

北京朝陽門內大街137号

北京市书刊出版业营业許可證出字第061号

上海新华印刷厂印刷

新华书店北京发行所发行 各地新华书店經售

*

1966年7月第一版

开本:787×1092 1/16

1966年7月第一次印刷

印張:17 5/8

印數:0001—2,150

字數:899,000

統一書号:16031·2287

本社書号:3467·13-1

定价:[科七]2.40元

序

本书包括我們于 1963 年至 1964 年間在有限几何和利用有限几何来构造部分平衡不完全区組設計两方面得到的一些結果, 其中一部分結果尚未发表过。

应用有限几何来构造不完全区組設計已有二十余年的历史。北京大学的同志們于 1963 年 3 月在北京数学会代数组的学术报告会上作了“試驗設計中的代数問題”的专题报告。在报告中, 他們介绍了应用有限几何来构造不完全区組設計这一课题的发展情况, 从而引起本书前一作者的注意。当本书前一作者在这方面进行了一些初步探索之后, 其余三位作者乘在中国科学技术大学进行毕业论文的机会, 也参加到这项工作中来。

本书共分十章, 前五章討論有限几何的計数定理。在第一章里, 我們介绍了經典的計数定理, 即在 q 个元素的有限域 F_q 上的 n 維向量空間 $V_n(F_q)$ 中, m 維 ($1 \leq m \leq n$) 子空間的个数是

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}$$

这一結果。大家都知道, $V_n(F_q)$ 中 m 維子空間的全体在一般綫性群 $GL_n(F_q)$ 作用下組成一个可迁集。 $GL_n(F_q)$ 是有限域上的一类典型群, 因此, 自然要研究 $V_n(F_q)$ 中子空間在有限域上其它类型的典型群(即辛群、酉群和正交群)作用下分成的可迁集中子空間的个数。这就是本书第二、三、四、五章的主要内容。在这几章里, 我們計算了有限域上辛几何、酉几何和正交几何的各个可迁集中子空間的个数, 也計算了这几种几何中一个給定的子空間所包含的另一个可迁集中子空間的个数。我們把这些結果分別叫做有限域上辛几何、酉几何和正交几何的計数定理。

在本书后五章里, 我們利用有限域上上述各种类型的几何而构造了一些結合方案和部分平衡不完全区組設計, 并計算了它們的参数, 其中一部分参数的計算依賴于前五章得到的計数定理。这几章的一部分結果, 北京大学的同志們曾用另外的方法独立得到。在这几章里, 我們主要是选取有限域上辛几何、酉几何和正交几何中 1 維迷向(或奇异)子空間作为处理, 以及选取极大全迷向(或全奇异)子空間作为处理来构造結合方案和部分平衡不完全区組設計, 并計算了它們的参数。自然, 选取这几种几何中其它类型子空間的可迁集作为处理也可以构造結合方案和部分平衡不完全区組設計, 这样得到的結合方案和部分平衡不完全区組設計的参数計算刚刚开始(請參看万哲先[4]), 看来还有很多工作可以进行。

在整个工作进行过程中, 我們得到中国科学院数学研究所和中国科学技术大学的大力支持, 特此致謝。

北京大学的同志們曾和我們进行多次有益的討論, 特此表示感謝。

我們特別希望得到讀者的批評和指正。

万哲先 戴宗鐸 馮緒宁 阳本傳

1965 年 7 月

目 录

第一章 有限域上向量空间中的计数定理	1
§ 1. 有限域上的向量空间和一般线性群	1
§ 2. 有限域上向量空间中的计数定理	2
第二章 有限域上辛几何中的计数定理	6
§ 1. 有限域上的交错矩阵	6
§ 2. 有限域上的辛群	8
§ 3. 有限域上向量空间的子空间在辛群作用下分成的可迁集	9
§ 4. 有限域上辛几何中的计数定理	14
§ 5. 计数定理(续)	20
§ 6. 有限域上非奇异交错矩阵的个数	23
§ 7. 特征数为 2 的有限域上非奇异对称矩阵定义的群	24
第三章 有限域上酉几何中的计数定理	31
§ 1. 有限域上的埃尔米特矩阵	31
§ 2. 有限域上的酉群	33
§ 3. 有限域上向量空间的子空间在酉群作用下分成的可迁集	35
§ 4. 有限域上酉几何中的计数定理	38
§ 5. 计数定理(续)	43
§ 6. 有限域上非奇异埃尔米特矩阵的个数	47
第四章 特征数不为 2 的有限域上正交几何中的计数定理	49
§ 1. 特征数不为 2 的有限域上的对称矩阵	49
§ 2. 特征数不为 2 的有限域上的正交群	52
§ 3. 有限域上向量空间的子空间在正交群作用下分成的可迁集	54
§ 4. 证明计数定理的一些准备	60
§ 5. 计算 $n(m, 2s, s; 2\nu + \delta, \Delta)$	63
§ 6. 计算 $n(m+1, 2s+1, s, \Gamma; 2\nu + \delta, \Delta)$	67
§ 7. 计算 $n(m+2, 2s+2, s; 2\nu + \delta, \Delta)$	71
§ 8. 特征数不为 2 的有限域上正交几何中的计数定理	74
§ 9. 计数定理(续)	76
§ 10. 特征数不为 2 的有限域上非奇异对称矩阵的个数	81
第五章 特征数为 2 的有限域上正交几何中的计数定理	83
§ 1. 特征数为 2 的有限域上的同余矩阵类	83
§ 2. 特征数为 2 的有限域上的正交群	92
§ 3. 有限域上向量空间的子空间在正交群作用下分成的可迁集	95

§ 4. 証明計数定理的預备知識.....	109
§ 5. 計算 $n(m+\tau, 2s+\tau, s, T; 2\nu+\delta)$	112
§ 6. 特征数为 2 的有限域上正交几何中的計数定理.....	117
§ 7. 計数定理(續).....	119
§ 8. 特征数为 2 的有限域上正則矩陣同余类的个数.....	123
第六章 利用有限域上向量空間的子空間而构造的一些部分平衡不完全区組設計	125
§ 1. 平衡不完全区組設計.....	125
§ 2. 結合方案与部分平衡不完全区組設計.....	127
§ 3. 利用有限域上向量空間的子空間而构造的多个結合类的結合方案和 PBIB 設計	132
§ 4. 取有限域上非奇异交錯矩陣的等同类作为区組而构造的 PBIB 設計	140
§ 5. 取有限域上非奇异埃尔米特矩陣的等同类作为区組而构造的 PBIB 設計	144
§ 6. 在特征数不为 2 的有限域上取非奇异对称矩陣的等同类作为区組而构造的 PBIB 設計.....	147
§ 7. 在特征数为 2 的有限域上取正則矩陣同余类的等同类作为区組而构造的 PBIB 設計	152
第七章 利用有限域上辛几何构造的一些部分平衡不完全区組設計	155
§ 1. 取 1 維子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計	155
§ 2. 在 4 維辛几何中取 2 維全迷向子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計	158
§ 3. 取极大全迷向子空間作为处理而构造的多个結合类的結合方案和 PBIB 設計	163
第八章 利用有限域上酉几何而构造的一些部分平衡不完全区組設計	179
§ 1. 取 1 維迷向子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計	179
§ 2. 在 4 維及 5 維酉几何中取 2 維全迷向子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計	182
§ 3. 取极大全迷向子空間作为处理而构造的多个結合类的結合方案和 PBIB 設計	190
第九章 利用特征数不为 2 的有限域上的正交几何而构造的一些部分平衡不完全区組設計	208
§ 1. 取 1 維迷向子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計	208
§ 2. 在 $\nu=2$ 的正交几何中取 2 維全迷向子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計.....	212
§ 3. 取极大全迷向子空間作为处理而构造的多个結合类的結合方案和 PBIB 設計	220
第十章 利用特征数为 2 的有限域上的正交几何而构造的一些部分平衡不完全区組設計	253
§ 1. 取 1 維奇异子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計	253
§ 2. 在 $\nu=2$ 的正交几何中取 2 維全奇异子空間作为处理而构造的两个結合类的結合方案和 PBIB 設計.....	255
§ 3. 取极大全奇异子空間作为处理而构造的多个結合类的結合方案和 PBIB 設計	257
参考文献	275

第一章

有限域上向量空間中的計數定理

§ 1. 有限域上的向量空間和一般綫性群

在这本书里，我們总用 F_q 表示 q 个元素的有限域， q 是一个素数的幂。我們用 $V_n(F_q)$ 表示由所有 n 数组

$$(x_1, x_2, \dots, x_n), x_i \in F_q, i=1, 2, \dots, n$$

的全体組成的 F_q 上的 n 維向量空間。令

$$e_1 = (1, 0, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, 0, 0, \dots, 0, 1),$$

那么 $e_1, e_2, \dots, e_n$ 組成 $V_n(F_q)$ 的一組基，即 $V_n(F_q)$ 中任一向量 $(x_1, x_2, \dots, x_n)$ 都可以表成 $e_1, e_2, \dots, e_n$ 的綫性組合：

$$(x_1, x_2, \dots, x_n) = x_1 e_1 + x_2 e_2 + \dots + x_n e_n,$$

而且表法是唯一的。自然， $V_n(F_q)$ 中任意 n 个綫性无关的向量都組成它的一組基。显然， $V_n(F_q)$ 一共有 q^n 个向量。

設 P 是 $V_n(F_q)$ 的一个 m 維子空間，記 $\dim P = m$ ；并設 $v_1, v_2, \dots, v_m$ 是 P 的一組基， $v_1, v_2, \dots, v_m$ 都是 $V_n(F_q)$ 中的向量。我們常用 $m \times n$ 矩陣

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix}$$

来代表 P 。特別，常記

$$P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix},$$

即用同一字母 P 来表示代表子空間 P 的矩陣。需要注意的是代表 m 維子空間的矩陣是秩为 m 的 $m \times n$ 矩陣。自然，两个不同的秩为 m 的 $m \times n$ 矩陣 P 和 Q 可以代表同一个 m 維子空間，只要有 $m \times m$ 非奇异矩陣 A 存在，使

$$P = AQ.$$

这时我們記 $P \sim Q$ 。显然，任一 m 維子空間都恰好含有 q^m 个向量。

設 P_1 和 P_2 是 $V_n(F_q)$ 的两个子空間。既属于 P_1 又属于 P_2 的向量的全体組成一个子空間，称为 P_1 和 P_2 的交，記作 $P_1 \cap P_2$ 。而 P_1 和 P_2 又張成一个子空間，称为 P_1 和 P_2 的联，記作 $P_1 \cup P_2$ 。我們有維數公式

$$\dim P_1 + \dim P_2 = \dim (P_1 \cap P_2) + \dim (P_1 \cup P_2).$$

我們知道, F_q 上所有 $n \times n$ 非奇异矩阵的全体对于矩阵乘法来说组成一群, 称为 F_q 上的 n 级一般线性群, 记作 $GL_n(F_q)$. $GL_n(F_q)$ 中的元素都可以看作是作用在 $V_n(F_q)$ 上的线性变换. 实际上, 设 $T \in GL_n(F_q)$, 则 T 把 $V_n(F_q)$ 中的向量 $(x_1, x_2, \dots, x_n)$ 变到 $(x_1, x_2, \dots, x_n)T$. 于是, $GL_n(F_q)$ 中的元素也可以看作是作用在 $V_n(F_q)$ 的子空间上, 即 $T \in GL_n(F_q)$ 把 m 维子空间 P (注意, P 是秩为 m 的 $m \times n$ 矩阵) 变到 PT . 显然, PT 也是 m 维子空间. 更进一步, 我們有

定理 1. 对于 $V_n(F_q)$ 中任意两个 m 维子空间 P 和 Q , 总存在一个元素 $T \in GL_n(F_q)$, 使得

$$P = QT,$$

即 $GL_n(F_q)$ 可迁地作用在一个固定维数 m 的所有 m 维子空间的集合上.

証. 实际上, 选取 $(n-m) \times n$ 矩阵 X 和 Y , 使

$$\begin{pmatrix} P \\ X \end{pmatrix} \text{ 和 } \begin{pmatrix} Q \\ Y \end{pmatrix}$$

都是非奇异 $n \times n$ 矩阵, 再令

$$T = \begin{pmatrix} Q \\ Y \end{pmatrix}^{-1} \begin{pmatrix} P \\ X \end{pmatrix}.$$

就行了.

如果用 $\mathfrak{M}(m, n)$ 表示 $V_n(F_q)$ 中所有 m 维子空间的全体组成的集合, 那么根据定理 1, $\mathfrak{M}(m, n)$ 中元素的个数 (即 $V_n(F_q)$ 中 m 维子空间的个数) 就等于 $GL_n(F_q)$ 中使 $\mathfrak{M}(m, n)$ 的一个固定元素保持不动的变换的全体所组成的子群在 $GL_n(F_q)$ 中的指数. 在下一节, 我們將用一个组合方法来计算 $\mathfrak{M}(m, n)$ 中元素的个数.

§2. 有限域上向量空间中的计数定理

我們用 $N(m, n)$ 表示 $\mathfrak{M}(m, n)$ 中元素的个数, 再用 $n(m, n)$ 表示秩为 m 的 $m \times n$ 矩阵的个数. 由于两个秩为 m 的 $m \times n$ 矩阵 P 和 Q 代表同一个 m 维子空间, 当且仅当 $m \times m$ 非奇异矩阵 A 存在, 使 $P = AQ$, 才有

$$n(m, n) = (GL_m(F_q) : 1) N(m, n),$$

其中 $GL_m(F_q) : 1$ 表示 $GL_m(F_q)$ 的阶. 因为

$$GL_m(F_q) : 1 = n(m, m),$$

所以, 要计算 $N(m, n)$, 只要计算 $n(m, n)$ 即可.

定理 2. 设 $m \leq n$, 则秩为 m 的 $m \times n$ 矩阵的个数为

$$n(m, n) = \prod_{i=n-m+1}^n (q^i - 1) q^{\frac{m(m-1)}{2}}.$$

証. 设 P 是任一秩为 m 的 $m \times n$ 矩阵. 写

$$P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix},$$

$v_1, v_2, \dots, v_m$ 是 P 的 m 个行向量. v_1 可以是 $V_n(F_q)$ 中任意一个非零向量, 因而一共有 $q^n - 1$ 种选法. 当 v_1 选定后, v_2 可以是 $V_n(F_q)$ 中任意一个不与 v_1 线性相关的向量, 因而, v_2 一共有 $q^n - q$ 种选法. 当 v_1, v_2 选定后, v_3 可以是 $V_n(F_q)$ 中任意一个不与 v_1, v_2 线性相关的向量, 而 v_1, v_2 也线性无关, 所以, v_3 一共有 $q^n - q^2$ 种选法. 如此继续下去, 最后, 当 $v_1, v_2, \dots, v_{m-1}$ 选定后, v_m 可以是 $V_n(F_q)$ 中任意一个不与 $v_1, v_2, \dots, v_{m-1}$ 线性相关的向量, 而 $v_1, v_2, \dots, v_{m-1}$ 线性无关, 所以, v_m 一共有 $q^n - q^{m-1}$ 种选法. 于是

$$\begin{aligned} n(m, n) &= (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{m-1}) \\ &= \prod_{i=n-m+1}^n (q^i - 1) q^{\frac{m(m-1)}{2}}. \end{aligned}$$

由定理 2 立刻推出

定理 3. $GL_n(F_q)$ 的阶为

$$GL_n(F_q):1 = \prod_{i=1}^n (q^i - 1) q^{\frac{n(n-1)}{2}}.$$

証. 实际上,

$$GL_n(F_q):1 = n(m, n).$$

定理 4. 設 $m \leq n$. $V_n(F_q)$ 中 m 維子空間的个数为

$$N(m, n) = \frac{\prod_{i=n-m+1}^n (q^i - 1)}{\prod_{i=1}^m (q^i - 1)}.$$

証. 实际上

$$N(m, n) = \frac{n(m, n)}{GL_m(F_q):1}.$$

系理 1. 設 $1 \leq k \leq m \leq n$. 如果用 $N(k, m, n)$ 表示在 $V_n(F_q)$ 中給定的一个 m 維子空間中 k 維子空間的个数, 那么

$$N(k, m, n) = N(k, m) = \frac{\prod_{i=m-k+1}^m (q^i - 1)}{\prod_{i=1}^k (q^i - 1)}.$$

系理 2. 設 $1 \leq k \leq m \leq n$, 那么包含 $V_n(F_q)$ 中一个固定的 k 維子空間的 m 維子空間的个数等于

$$\frac{\prod_{i=n-m+1}^{n-k} (q^i - 1)}{\prod_{i=1}^{m-k} (q^i - 1)}.$$

証. 实际上, 如果用 N 表示包含 $V_n(F_q)$ 中一个固定的 k 維子空間的 m 維子空間的个数, 那么

$$N(m, n) \cdot N(k, m) = N(k, n) \cdot N.$$

于是

1) 我們在本书中約定, 如果連乘积符号 $\prod_{i \in \mathfrak{M}} N_i$ 中的 $\mathfrak{M}$ 是空集, 那么 $\prod_{i \in \mathfrak{M}} N_i = 1$. 同样, 我們約定, 如果 $\mathfrak{M}$ 是空集, 那么 $\sum_{i \in \mathfrak{M}} N_i = 0$.

$$N = \frac{N(m, n)N(k, m)}{N(k, n)} = \frac{\prod_{i=n-m+1}^n (q^i - 1)}{\prod_{i=1}^m (q^i - 1)} \cdot \frac{\prod_{i=m-k+1}^m (q^i - 1)}{\prod_{i=1}^k (q^i - 1)} \cdot \frac{\prod_{i=1}^k (q^i - 1)}{\prod_{i=n-k+1}^n (q^i - 1)}$$

$$= \frac{\prod_{i=n-m+1}^{n-k} (q^i - 1)}{\prod_{i=1}^{m-k} (q^i - 1)}.$$

最后, 我們証明定理 2 的一个推广.

定理 5. 設 $0 \leq r \leq \min(m, n)$, 那么秩为 r 的 $m \times n$ 矩陣的个数为

$$n(r, m \times n) = \frac{\prod_{i=m-r+1}^m (q^i - 1) \cdot \prod_{i=n-r+1}^n (q^i - 1)}{\prod_{i=1}^r (q^i - 1)} q^{\frac{r(r-1)}{2}}.$$

証. 我們用 $\mathfrak{M}(r, m \times n)$ 表示秩为 r 的 $m \times n$ 矩陣的集合, 再用 $GL_m(F_q) \times GL_n(F_q)$ 表示 $GL_m(F_q)$ 和 $GL_n(F_q)$ 的直积. 对于任意 $(A, B) \in GL_m(F_q) \times GL_n(F_q)$, 即 $A \in GL_m(F_q)$, $B \in GL_n(F_q)$, 映射

$$X \rightarrow AXB \quad (X \in \mathfrak{M}(r, m \times n))$$

是 $\mathfrak{M}(r, m \times n)$ 的一个置换. 由于对任意 $X \in \mathfrak{M}(r, m \times n)$, 总有 $A \in GL_m(F_q)$ 和 $B \in GL_n(F_q)$ 使

$$AXB = \begin{pmatrix} I^{(r)} & O \\ O & O^{(m-r, n-r)} \end{pmatrix} \begin{matrix} r & n-r \\ r & n-r \end{matrix} \quad ^{1)}$$

所以 $GL_m(F_q) \times GL_n(F_q)$ 可迁地作用在 $\mathfrak{M}(r, m \times n)$ 上. 于是, $\mathfrak{M}(r, m \times n)$ 中元素的个数 $N(r, m \times n)$ 就等于 $GL_m(F_q) \times GL_n(F_q)$ 中使

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

保持不动的变换所组成的子群 $\mathfrak{S}$ 在 $GL_m(F_q) \times GL_n(F_q)$ 中的指数 $GL_n(F_q) \times GL_m(F_q)$: $\mathfrak{S}$.

設 $(A, B) \in \mathfrak{S}$, $A \in GL_m(F_q)$, $B \in GL_n(F_q)$. 将 A 和 B 写成分块矩陣

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22}^{(m-r)} \end{pmatrix} \begin{matrix} r & m-r \\ r & m-r \end{matrix}, \quad B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22}^{(n-r)} \end{pmatrix} \begin{matrix} r & n-r \\ r & n-r \end{matrix},$$

那么从

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \begin{pmatrix} I^{(r)} & O \\ O & O \end{pmatrix} \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} I^{(r)} & O \\ O & O \end{pmatrix}$$

推出

$$A_{11}B_{11} = I^{(r)}, A_{21} = 0, B_{12} = 0.$$

¹⁾ 我們在本书中約定, 分块矩陣的右側和下方所注的数字或文字是用来表示它的分块方式的.

于是

$$\mathfrak{S}:1 = (GL_r(F_q):1) (GL_{m-r}(F_q):1) (GL_{n-r}(F_q):1) q^{r(m-r)+r(n-r)}.$$

因此

$$\begin{aligned} n(r, m \times n) &= GL_m(F_q) \times GL_n(F_q) : \mathfrak{S} \\ &= \frac{(GL_m(F_q):1) (GL_n(F_q):1)}{\mathfrak{S}:1} \\ &= \frac{\prod_{i=m-r+1}^m (q^i - 1) \cdot \prod_{i=n-r+1}^n (q^i - 1)}{\prod_{i=1}^r (q^i - 1)} q^{\frac{r(r-1)}{2}}. \end{aligned}$$

系理. 設 $0 \leq r \leq n$, 那么秩为 r 的 $n \times n$ 矩陣的个数为

$$n(r, n \times n) = \frac{\prod_{i=n-r+1}^n (q^i - 1)^2}{\prod_{i=1}^r (q^i - 1)} q^{\frac{r(r-1)}{2}}.$$

第二章

有限域上辛几何中的计数定理

§1. 有限域上的交错矩阵

在这一章里, 我們仍然用 F_q 表示 q 个元素的有限域, q 是一个素数的幂. 設 K 是 F_q 上的一个 $n \times n$ 矩阵. 如果 $K' = -K$, 那么 K 叫做斜对称矩阵; K 叫做交错矩阵, 如果除了 $K' = -K$ 之外, 还要求 K 的主对角线上的元素都是 0. 当 F_q 的特征数 $\neq 2$ 时, 斜对称矩阵都是交错矩阵. 但是, 当 F_q 的特征数 $= 2$ 时, 确有不是交错矩阵的斜对称矩阵存在.

我們注意, 如果 K 是 F_q 上的 $n \times n$ 交错矩阵, 那么对任意 $x \in V_n(F_q)$, 都有 $xKx' = 0$. 反之, 設 K 是 F_q 上的 $n \times n$ 矩阵, 如果对任意 $x \in V_n(F_q)$ 都有 $xKx' = 0$, 那么 K 一定是交错矩阵. 事实上, 設 $K = (k_{ij})_{1 \leq i, j \leq n}$, 从 $e_i K e_i' = 0$ 推出 $k_{ii} = 0 (1 \leq i \leq n)$, 再从 $(e_i + e_j) K (e_i + e_j)' = 0$ 推出 $k_{ij} + k_{ji} = 0$, 即 $k_{ij} = -k_{ji}$, 于是 K 是交错矩阵.

設 K_1 和 K_2 都是 F_q 上的 $n \times n$ 矩阵. 如果有 F_q 上的 $n \times n$ 非奇异矩阵 Q , 使 $QK_1Q' = K_2$, 我們就說 K_1 和 K_2 合同. 显然, 合同的矩阵有相同的秩, 又, 与斜对称矩阵合同的矩阵一定是斜对称的. 再根据上一段的注記可知, 与交错矩阵合同的矩阵一定是交错的.

在这一节里, 我們要研究交错矩阵在合同之下的标准形.

定理 1. 設 K 是 F_q 上的 $n \times n$ 交错矩阵, 那么 K 的秩一定是偶数. 設 K 的秩是 2ν , 那么 K 一定合同于

$$\begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & & & & \\ & & 0 & 1 & & 0 \\ & & -1 & 0 & \ddots & \\ & \nu \uparrow & & & 0 & 1 \\ & & & & -1 & 0 \\ 0 & & & & & 0 & \ddots & 0 \end{pmatrix},$$

因而也合同于

$$\begin{pmatrix} 0 & I^{(\nu)} & 0 \\ -I^{(\nu)} & 0 & 0 \\ 0 & 0 & O^{(n-2\nu)} \end{pmatrix}.$$

証. 对 n 行使归纳法証之. 当 $n=1$ 时, $K=(0)$, 本定理自然成立. 其次, 考察 $n=2$ 的情形, 这时

$$K = \begin{pmatrix} 0 & k_{12} \\ -k_{12} & 0 \end{pmatrix}.$$

如果 $k_{12}=0$, 本定理自然成立; 否则 K 合同于

$$\begin{pmatrix} 1 & 0 \\ 0 & k_{12}^{-1} \end{pmatrix} K \begin{pmatrix} 1 & 0 \\ 0 & k_{12}^{-1} \end{pmatrix}' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

此时本定理也成立.

今设 $n>2$, 并设本定理对 $m<n$ 都成立. 设

$$K = \begin{pmatrix} 0 & k_{12} & k_{13} & \cdots & k_{1n} \\ -k_{12} & 0 & k_{23} & \cdots & k_{2n} \\ -k_{13} & -k_{23} & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & k_{n-1n} \\ -k_{1n} & -k_{2n} & \cdots & -k_{n-1n} & 0 \end{pmatrix}.$$

如果 $K=0$, 本定理自然成立. 设 $K \neq 0$, 不妨设 $k_{12} \neq 0$, 否则 K 必合同于一个交错矩阵, 它的 $(1, 2)$ 位置元素不为 0. 实际上, 如 $k_{ij} \neq 0$, 而 $i < j$, 那么, 将 K 的第一行与第 i 行对调, 并将第一列与第 i 列对调, 就得到一个与 K 合同的矩阵 K_1 , 它的 $(1, j)$ 位置元素不为 0. 再将 K_1 的第二行与第 j 行对调, 并将第二列与第 j 列对调, 就得到一个与 K_1 合同的矩阵, 它的 $(1, 2)$ 位置元素不为 0. 更进一步, 无妨设 $k_{12}=1$. 实际上, 如果 K 的 $(1, 2)$ 位置的元素不为 0, 那么, K 合同于

$$\begin{pmatrix} 1 & & \\ & k_{12}^{-1} & \\ & & I^{(n-2)} \end{pmatrix} K \begin{pmatrix} 1 & & \\ & k_{12}^{-1} & \\ & & I^{(n-2)} \end{pmatrix},$$

而它的 $(1, 2)$ 位置的元素为 1. 于是, K 合同于

$$\begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ k_{23} & -k_{13} & 1 & & \\ \vdots & \vdots & & \ddots & \\ k_{2n} & -k_{1n} & 0 & & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & k_{13} & \cdots & k_{1n} \\ -1 & 0 & k_{23} & \cdots & k_{2n} \\ -k_{13} & -k_{23} & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & k_{n-1n} \\ -k_{1n} & -k_{2n} & \cdots & -k_{n-1n} & 0 \end{pmatrix} \begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ k_{23} & -k_{13} & 1 & & \\ \vdots & \vdots & & \ddots & \\ k_{2n} & -k_{1n} & 0 & & 1 \end{pmatrix}' \\ = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & K_0 & \\ 0 & 0 & & & \end{pmatrix},$$

其中 K_0 是 $(n-2) \times (n-2)$ 交错矩阵. 根据归纳法假设, K_0 合同于

$$QK_0Q' = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & 0 & 1 & \\ & & -1 & 0 & \\ \nu-1 \uparrow & & & \ddots & 0 & 1 \\ & & & & -1 & 0 \\ & 0 & & & & \ddots & 0 \end{pmatrix}.$$

因此, K 合同于

$$\begin{pmatrix} I^{(2)} & \\ & Q \end{pmatrix} K \begin{pmatrix} I^{(2)} & \\ & Q \end{pmatrix}' = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & 0 & 1 & \\ & & -1 & 0 & \\ \nu \uparrow & & & \ddots & 0 & 1 \\ & & & & -1 & 0 \\ & 0 & & & & \ddots & 0 \end{pmatrix}.$$

这时 K 的秩是 2ν .

显然, K 也合同于

$$\begin{pmatrix} O & I^{(\nu)} \\ -I^{(\nu)} & O \\ & & O_{(n-2\nu)} \end{pmatrix}.$$

它叫做秩为 2ν 的 $n \times n$ 交错矩阵的合同标准形, 而 ν 是 K 的指数.

系理 1. F_q 上两个 $n \times n$ 交错矩阵是合同的, 当且仅当它们有相同的秩.

系理 2. 设 K 是 F_q 上 $n \times n$ 非奇异交错矩阵, 那么 $n=2\nu$ 一定是偶数, 而 K 一定合同于

$$\begin{pmatrix} O & I^{(\nu)} \\ -I^{(\nu)} & O \end{pmatrix}.$$

§2. 有限域上的辛群

从这一节起, 我们假定 $n=2\nu$ 是偶数并设 K 是 F_q 上的 $2\nu \times 2\nu$ 非奇异交错矩阵. F_q 上的 $2\nu \times 2\nu$ 矩阵 T 称为对于 K 来说的辛矩阵, 如果

$$TKT' = K.$$

容易证明, F_q 上所有对于 K 来说的 $2\nu \times 2\nu$ 辛矩阵的集合, 对于矩阵乘法组成一群, 叫做 F_q 上对于 K 来说的 2ν 级辛群, 记作 $Sp_{2\nu}(F_q, K)$.

设 K_1 和 K_2 是两个 $2\nu \times 2\nu$ 非奇异交错矩阵. 根据定理 1 的系理 1, 存在 $2\nu \times 2\nu$ 非奇异矩阵 Q , 使得 $QK_1Q' = K_2$. 如果 $T \in Sp_{2\nu}(F_q, K_1)$, 即 $TK_1T' = K_1$, 那么

$QTQ^{-1} \in Sp_{2\nu}(F_q, K_2)$. 实际上,

$$(QTQ^{-1})K_2(QTQ^{-1})' = QTQ^{-1}K_2Q'^{-1}T'Q' = QTQ^{-1}K_1T'Q' = QK_1Q' = K_2.$$

更进一步,

$$T \rightarrow QTQ^{-1}$$

是从 $Sp_{2\nu}(F_q, K_1)$ 映到 $Sp_{2\nu}(F_q, K_2)$ 上的一个同构映射. 因此, $Sp_{2\nu}(F_q, K_1)$ 与 $Sp_{2\nu}(F_q, K_2)$ 同构. 从而, 在讨论辛群时, 不失普遍性, 可以取任一固定的非奇异交错矩阵 K , 而研究 $Sp_{2\nu}(F_q, K)$.

从现在开始, 我们取

$$K = \begin{pmatrix} O & I^{(\nu)} \\ -I^{(\nu)} & O \end{pmatrix},$$

并将 K 定义的辛群简记作 $Sp_{2\nu}(F_q)$.

设 $T \in Sp_{2\nu}(F_q)$. 将 T 写作分块矩阵

$$T = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

其中 A, B, C, D 都是 $\nu \times \nu$ 矩阵, 那么 $TKT' = K$ 当且仅当

$$AB' - BA' = 0, CD' - DC' = 0, AD' - BC' = I. \quad (1)$$

今后经常要用到这几个公式. 利用这几个公式, 不难看出下面几种形状的元素都属于 $Sp_{2\nu}(F_q)$:

$$(i) \quad \begin{pmatrix} A & O \\ O & A'^{-1} \end{pmatrix},$$

其中 $A \in GL_\nu(F_q)$.

$$(ii) \quad \begin{pmatrix} I & Q \\ & I \end{pmatrix}, \begin{pmatrix} I & \\ Q & I \end{pmatrix},$$

其中 Q 是 $\nu \times \nu$ 矩阵而且满足 $Q' = Q$.

$$(iii) \quad \begin{pmatrix} J & I-J \\ -(I-J) & J \end{pmatrix},$$

其中 J 是 $\nu \times \nu$ 对角形矩阵, 而且满足 $J^2 = J$.

§3. 有限域上向量空间的子空间在辛群作用下分成的可迁集

设 P 是 $V_{2\nu}(F_q)$ 的秩为 m 的子空间. 我们约定, 用同一符号 P 来表示代表子空间 P 的秩为 m 的 $m \times 2\nu$ 矩阵. 容易证明, PKP' 是 $m \times m$ 交错矩阵. 根据定理 1, PKP' 的秩是偶数. 设 PKP' 的秩是 $2s$, 自然有 $s \leq \nu$ 及 $2s \leq m$. 这时我们把 P 叫做指数 s 的 m 维子空间, 也把 (m, s) 叫做 P 的类型. 特别, 如果 $PKP' = 0$, 则 P 叫做 m 维全迷向子空间; 如果 PKP' 是非奇异的, 这时 $m = 2s$ 一定是偶数, P 叫做 $2s$ 维非迷向子空间.

$V_{2\nu}(F_q)$ 中两个向量 x 和 y 叫做正交的, 如果 $xKy' = 0$. 显然, 如果 $xKy' = 0$, 那么 $yKx' = 0$. 自然每个向量都与它自己正交, 即每个向量都是迷向的. 设 P 是 $V_{2\nu}(F_q)$ 的一个 m 维子空间, 用 P^* 表示与 P 中每个向量都正交的 $V_{2\nu}(F_q)$ 中所有向量的集合. 显

然, P^* 是 $2\nu - m$ 維子空間, 称 P^* 为 P 的共軛子空間.

定理 2. 子空間 P 是全迷向的, 当且仅当 $P \subseteq P^*$; P 是非迷向的, 当且仅当 $P \cap P^* = (0)$.

証. 第一个断言是显然的, 現在証明第二个断言. 注意

$$\begin{pmatrix} P \\ P^* \end{pmatrix} K \begin{pmatrix} P \\ P^* \end{pmatrix}' = \begin{pmatrix} PKP' & O \\ O & P^* K P^* \end{pmatrix}.$$

如果 $P \cap P^* = (0)$, 那么

$$\begin{pmatrix} P \\ P^* \end{pmatrix}$$

是 $2\nu \times 2\nu$ 非奇异矩陣. 于是 PKP' 非奇异, 即 P 非迷向. 反之, 如果有 $\alpha \in P \cap P^*$ 而 $\alpha \neq 0$, 設 P 是 m 維的, 那么有 $1 \times m$ 矩陣 $\xi \neq 0$, 使得 $\alpha = \xi P$. 于是 $\xi PKP' = \alpha K P' = 0$. 因之 PKP' 奇异, 即 P 不是非迷向的.

因为 $Sp_{2\nu}(F_q)$ 是 $GL_{2\nu}(F_q)$ 的子群, 而 $GL_{2\nu}(F_q)$ 可以看作是 $V_{2\nu}(F_q)$ 上的变换群, 所以, $Sp_{2\nu}(F_q)$ 也可以看作是 $V_{2\nu}(F_q)$ 上的变换群. 我們来研究 $V_{2\nu}(F_q)$ 的子空間在 $Sp_{2\nu}(F_q)$ 作用下的可迁性. 首先, 我們証明

引理 1. 設 P 是指数 s 的 m 維子空間, $s \leq \nu$ 而 $2s \leq m$, 那么存在一个 $m \times m$ 非奇异矩陣 Q 和一个 $(2\nu - m) \times 2\nu$ 矩陣 Z 使得

$$\begin{pmatrix} QP \\ Z \end{pmatrix} K \begin{pmatrix} QP \\ Z \end{pmatrix}' = \begin{pmatrix} O & I^{(s)} & & & \\ -I^{(s)} & O & & & \\ & & O & I^{(m-2s)} & \\ & & -I^{(m-2s)} & O & \\ & & & & O & I^{(\sigma)} \\ & & & & -I^{(\sigma)} & O \end{pmatrix}$$

其中 $\sigma = \nu + s - m$. 因此 $m - 2s \leq \nu - s$, 即 $\sigma = \nu + s - m \geq 0$.

証. 根据定理 1, 存在 $m \times m$ 非奇异矩陣 Q , 使

$$Q(PKP')Q' = \begin{pmatrix} O & I^{(s)} & O \\ -I^{(s)} & O & O \\ O & O & O^{(m-2s)} \end{pmatrix}.$$

設 Z_1 是 $(2\nu - m) \times 2m$ 矩陣, 使得

$$\begin{pmatrix} QP \\ Z_1 \end{pmatrix}$$

是非奇异的. 于是可設

$$\begin{pmatrix} QP \\ Z_1 \end{pmatrix} K \begin{pmatrix} QP \\ Z_1 \end{pmatrix}' = \begin{pmatrix} O & I^{(s)} & O & K_{14} \\ -I^{(s)} & O & O & K_{24} \\ O & O & O^{(m-2s)} & K_{34} \\ -K'_{14} & -K'_{24} & -K'_{34} & K_{44} \end{pmatrix},$$

其中 K_{44} 是 $(2\nu - m) \times (2\nu - m)$ 交錯矩陣, 那么

$$\begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ K'_{24} & -K'_{14} & O & I^{(2\nu-m)} \end{pmatrix} \begin{pmatrix} O & I^{(s)} & O & K_{14} \\ -I^{(s)} & O & O & K_{24} \\ O & O & O^{(m-2s)} & K_{34} \\ -K'_{14} & -K'_{24} & -K'_{34} & K_{44} \end{pmatrix} \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ K'_{24} & -K'_{14} & O & I^{(2\nu-m)} \end{pmatrix}' \\
= \begin{pmatrix} O & I^{(s)} & O & O \\ -I^{(s)} & O & O & O \\ O & O & O & K_{34} \\ O & O & -K'_{34} & K_{44} \end{pmatrix}.$$

但需注意, 其中 K_{44} 应该是 $K_{44} + K'_{24}K_{14} - K'_{14}K_{24}$, 只是为了书写简单起见, 仍将它记作 K_{44} . 因为 K 非奇异, 所以 K_{34} 的秩是 $m-2s$; 于是 $m-2s \leq 2\nu-m$ 而且有 $(2\nu-m) \times (2\nu-m)$ 非奇异矩阵 B 使

$$K_{34}B' = (I^{(m-2s)}, O^{(m-2s, 2\sigma)}).$$

那么

$$\begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & B \end{pmatrix} \begin{pmatrix} O & I^{(s)} & & \\ -I^{(s)} & O & & \\ & & O & K_{34} \\ & & -K'_{34} & K_{44} \end{pmatrix} \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & B \end{pmatrix}' \\
= \begin{pmatrix} O & I^{(s)} & & \\ -I^{(s)} & O & & \\ & & O & I^{(m-2s)} & O \\ & & -I^{(m-2s)} & K_{44} & K_{45} \\ & & O & -K'_{45} & K_{55} \end{pmatrix},$$

其中 K_{44} 是 $(m-2s) \times (m-2s)$ 交错矩阵, K_{55} 是 $2\sigma \times 2\sigma$ 交错矩阵. 设 T 是将 K_{44} 的主对角线以下的元素都换上 0 之后得到的矩阵, 那么

$$K_{44} = T - T'.$$

因此

$$\begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & -T & I^{(m-2s)} \\ & & K'_{45} & I^{(2\sigma)} \end{pmatrix} \begin{pmatrix} O & I^{(s)} & & \\ -I^{(s)} & O & & \\ & & O & I^{(m-2s)} \\ & & -I^{(m-2s)} & K_{44} & K_{45} \\ & & & -K'_{45} & K_{55} \end{pmatrix} \\
\times \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & -T & I^{(m-2s)} \\ & & K'_{45} & I^{(2\sigma)} \end{pmatrix}' = \begin{pmatrix} O & I^{(s)} & & \\ -I^{(s)} & O & & \\ & & O & I^{(m-2s)} \\ & & -I^{(m-2s)} & O & O \\ & & & O & K_{55} \end{pmatrix}.$$

因为 K 是非奇异的, 所以 K_{55} 是非奇异交错矩阵. 于是, 根据定理 1 的系理 2, 有 $2\sigma \times 2\sigma$ 非奇异矩阵 R 存在, 使得

$$RK_{55}R' = \begin{pmatrix} O & I^{(\sigma)} \\ -I^{(\sigma)} & O \end{pmatrix}.$$

因此

$$\begin{aligned} & \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & I^{(m-2s)} \\ & & & & R \end{pmatrix} \begin{pmatrix} O & I^{(s)} \\ -I^{(s)} & O \\ & & O & I^{(m-2s)} \\ & & -I^{(m-2s)} & O \\ & & & & K_{55} \end{pmatrix} \\ & \quad \times \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & I^{(m-2s)} \\ & & & & R \end{pmatrix}' \\ & = \begin{pmatrix} O & I^{(s)} \\ -I^{(s)} & O \\ & & O & I^{(m-2s)} \\ & & -I^{(m-2s)} & O \\ & & & & O & I^{(\sigma)} \\ & & & & -I^{(\sigma)} & O \end{pmatrix}. \end{aligned}$$

可以记

$$\begin{aligned} & \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & I^{(m-2s)} \\ & & & & R \end{pmatrix} \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & -I^{(m-2s)} \\ & & & & K'_{45} \\ & & & & & I \end{pmatrix} \\ & \quad \times \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & B \end{pmatrix} \begin{pmatrix} I^{(s)} & & & \\ & I^{(s)} & & \\ & & I^{(m-2s)} & \\ & & & K'_{24} \quad -K'_{14} \\ & & & & I^{(2\nu-m)} \end{pmatrix} \\ & = \begin{pmatrix} I^{(m)} \\ L_1 & L_2^{(2\nu-m)} \end{pmatrix}. \end{aligned}$$

令

$$\begin{pmatrix} I^{(m)} \\ L_1 & L_2^{(2\nu-m)} \end{pmatrix} \begin{pmatrix} QP \\ Z_1 \end{pmatrix} = \begin{pmatrix} QP \\ Z \end{pmatrix},$$