

第零章 符号和预备知识

本书所介绍的拟阵理论基本上是讨论在一个有限集上的数学结构。因此，除非特别声明，书中所讨论的集合均为有限集。集合族或集合类通常指的是集合的集合。由于讨论上的需要，我们有时要允许一个元素在一个集合中多次出现，这时有关的集合被称为一个可重复集合。比如 $\{a, a, b, b, b\}$ 就是一个可重复集合。

为了显而易见的原因，我们尽量采用标准的集合论的符号，同时也兼顾在拟阵文献中的习惯。当 E 是一个集合时， 2^E 和 $|E|$ 分别表示 E 中全体子集的集合族和 E 的基数。对集合 X 和 Y ，我们定义 $X - Y = \{x \in X : x \notin Y\}$ ，而当 $Y = \{e\}$ 时，我们通常用 $X - e$ 来代替较为正规的写法 $X - \{e\}$ ；类似地， $X \cap Y$ 和 $X \cup Y$ 分别表示 X 和 Y 的交与 X 和 Y 的并。并且当 $Y = \{e\}$ 时，我们也用 $X \cup e$ 和 $X \cap e$ 来分别代替 $X \cup \{e\}$ 和 $X \cap \{e\}$ 。当 $X_1, X_2, \dots, X_n$ 是两两不相交的集合时， $\bigcup_{i=1}^n X_i$ 称为一个不相交并。

在本书中，我们用 $\mathbf{N}$ 代表自然数的集合，用 $\mathbf{Z}$ ， $\mathbf{Q}$ ， $\mathbf{R}$ 和 $\mathbf{Z}_m$ 分别代表整数，有理数，实数和模 m 同余整数的集合（连同它们具有的域或加群结构），并用 $\mathbf{Z}^+$ ， $\mathbf{Q}^+$ 和 $\mathbf{R}^+$ 来分别代表非负整数，非负有理数和非负实数的集合。在本书中用到的一些不太常用的集合论的运算记号将在下面列出，而其它的记号则在需要时才引入。设 E 是一个集合， $\mathcal{A} \subseteq 2^E$ 是 E 中子集的一个族。定义

$$Upp(\mathcal{A}) = \{X \subseteq E : \text{存在 } A \in \mathcal{A} \text{ 使 } A \subseteq X\};$$

$$Low(\mathcal{A}) = \{X \subseteq E : \text{存在 } A \in \mathcal{A} \text{ 使 } X \subseteq A\};$$

$$Max(\mathcal{A}) = \{X \subseteq \mathcal{A} \text{ 对任意 } Y \in \mathcal{A}, \text{ 若 } X \subset Y, \text{ 则 } X = Y\};$$

$Min(\mathcal{A}) = \{X \subseteq A : \text{对任意 } Y \in \mathcal{A}, \text{ 若 } Y \subseteq X, \text{ 则 } X = Y\}$;

$Opp(\mathcal{A}) = \{X \subseteq E : X \notin \mathcal{A}\}$;

$Com(\mathcal{A}) = \{X \subseteq E : E - X \in \mathcal{A}\}$ 。

本书中有关矩阵的符号基本上是标准的。对一个 $n \times m$ 的矩阵 A , A 在第 i 行第 j 列的分量通常记为 $A(i, j)$ 或 a_{ij} 。若 A_1 和 A_2 分别是 $n_1 \times m_1$ 和 $n_2 \times m_2$ 的矩阵, 则矩阵 A_1 和 A_2 的直和是个 $(n_1 + n_2) \times (m_1 + m_2)$ 的矩阵:

$$A_1 \dot{+} A_2 = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}.$$

矩阵 I_r 表示 $r \times r$ 的单位矩阵, $J_{n \times m}$ 和 $O_{n \times m}$ 分别表示分量全为 1 或全为 0 的 $n \times m$ 矩阵。当 $n = m$ 时, 它们也分别记作 J_n 或 O_n 。分量全为 1 的向量记为 $\mathbf{1}$, 而分量全为 0 的向量记为 $\mathbf{0}$ 。当矩阵 A 的分量 $A(i, j) \neq 0$ 时, 我们可以通过对每个 $i' \neq i$, 把 A 的第 i 行乘以 $-A(i', j)/A(i, j)$ 再添加到第 i' 行, 然后把第 i 行乘以 $A(i, j)^{-1}$ 来得到矩阵 A' 。这时 A' 的第 j 列只有 $A'(i, j)$ 是唯一的一个非零分量, 并且 $A'(i, j) = 1$ 。我们称这个过程为把非零分量 $A(i, j)$ 化到主轴。

一般地, 对于一个域 F 和正整数 n , $V(n, F)$ 表示一个在 F 上的 n 维向量空间。通常用黑体 $\mathbf{v} = (v_1, v_2, \dots, v_n)^T$ 来表示 $V(n, F)$ 中元素。为了方便, 有时也把向量写成行向量的形式。特别地, 两个 $\mathbf{u}$ 和 $\mathbf{v}$ 的内积就记作 $\mathbf{uv}$ 或 $\mathbf{u} \cdot \mathbf{v}$ 。

域, 特别是有限域, 将在本书中反复出现。两个有限域互相同构当且仅当它们有相同的元素个数。因此我们把具有 q 个元素的有限域记作 $GF(q)$ 。每个域 F 都有一个加法单位元 0 和乘法单位元 1。若有最小的正整数 p , 使 F 中乘法单位元 1 自相加 p 次之后为 0, p 称为域 F 的特征。若这样的正整数 p 不存在, 则称 F 具有特征 0。域 F 的特征也记作 $ch(F)$ 。若有限域 F 的特征 $ch(F) = p > 0$, 则 p 一定是个质数, 并且有正整数 n , 使 $F = GF(p^n)$ 。当 $n = 1$ 时 $GF(p) = \mathbf{Z}_p$, 即由全体模 p 整数同余类在模 p 的加法和乘法下所构成的域。特别地, 当 $p = 2$ 和 3 时, 有 $GF(2) = \mathbf{Z}_2$ 和 $GF(3) = \mathbf{Z}_3$, 分别称为二元域和三元域。而四元域 $GF(4)$ 则同构于商环 $\mathbf{Z}_4[x]/(x^2 + x + 1)$ 。对每个有限域 $GF(q)$, 令 $GF(q)^* = GF(q) - \{0\}$ 。则 $GF(q)^*$ 是个关于乘法的循环群。(关于有限域的基本知识, 参见熊全淹 (1978), 吴品三 (1979), Hungerford(1974) 或其它的代数学教科书。)

一个图 (graph) G 是个有序三元组 (V, E, ψ) , 其中 $V \neq \emptyset$, V 中的元素称为 G 的顶点 (vertex), E 与 V 不相交, E 中的元素称为边 (edge), 而 ψ 是从 E 到 $V \times V$ 中元素的有序对或无序对集合 $V \times V$ 的关联函数 (incidence function). 常常用 $V = V(G)$ 和 $E = E(G)$ 来强调它们分别是图 G 的顶点集和边集. 若 $\psi(e)$ 中元素全是 $V \times V$ 中无序对时, G 是一个无向图 (undirected graph) (或简称为图). 这时若 $\psi(e) = \{x, y\}$, 则称 x 和 y 与 e 相关联或 e 是连接 x 和 y 的边, 并且顶点 x 和 y 是边 e 的两个端点, 记为 $e = xy$; 若 $\psi(e) = (x, x)$, 则 e 是 G 在 x 处的一个环 (loop); 若有 $e_1, e_2 \in E(G)$, 使 $\psi(e_1) = \psi(e_2)$ 但 e_1 不是 G 的一个环, 则称 e_1 和 e_2 互为平行边 (parallel edges). 若 v 是图 G 中的一个顶点, 则 v 的度是 G 中与 v 相关联的边的个数, 记作 $d_G(v)$ 或 $d(v)$. 容易看出

$$\sum_{v \in V(G)} d_G(v) = 2|E(G)|.$$

若 $\psi(E)$ 中元素全是 $V \times V$ 中有序对时, G 是一个有向图 (directed graph). 这时若 $\psi(e) = (x, y)$, 则称 e 是从 x 到 y 的有向边 (directed edge), x 是 e 的尾 (tail) 或起点, 而 y 是 e 的头 (head) 或终点. 一个图或有向图可以用它们的图形来表示. 下面是图 G 和在 G 的每条边上加上方向而得到的有向图 $D(G)$ (通常称为 G 的一个定向 (orientation) 的图形表示).

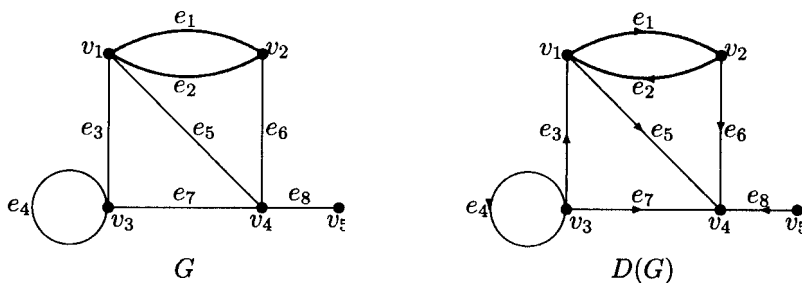


图 0.1 图 G 和 G 的一个定向 $D(G)$

在图 0.1 中, $V(G) = V(D(G)) = \{v_1, v_2, v_3, v_4, v_5\}$, $E(G) = E(D(G)) = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$. 而 $\psi_G(e_i)$ 和 $\psi_{D(G)}(e_i)$ 则分别是 G 中 e_i 所关联的一对无序的顶点, 和由 $D(G)$ 的图形中所示的由有向边 e_i 的端点所定义的有序对. 在无向图 G 和有向图 $D(G)$ 中, e_4 都是一个环. 边对 $\{e_1, e_2\}$ 在 G 中是一

对平行元,但 $\{e_1, e_2\}$ 在 $D(G)$ 中却不是一对平行元。没有环元和平行元的图称为简单图 (simple graph)。任何两个不同顶点之间都有边相连的简单图称为完全图 (complete graph)。当 $n > 1$ 是个正整数时, n 个顶点的完全图记作 K_n 。若无环图 G 的顶点集可以划分为两个非空子集 X 和 Y , 使得 X 中任何两个顶点之间无边相连, 并且 Y 中任何两个顶点之间也无边相连, 则称 G 为一个二部图 (bipartite graph), 而划分 (X, Y) 为 G 的一个顶点二部划分 (bipartition)。

设 $G = (V(G), E(G), \psi_G)$ 和 $H = (V(H), E(H), \psi_H)$ 是两个图。若 $V(H) \subseteq V(G)$, $E(H) \subseteq E(G)$, 并且 ψ_H 是 ψ_G 在 $E(H)$ 上的限制, 则称 H 是 G 的子图 (subgraph), 记为 $H \subset G$ 。若 $H \subset G$ 并且 $V(H) = V(G)$, 则称 H 为 G 的支撑子图 (spanning subgraph)。若 $H \subset G$ 但 $H \neq G$, 则称 H 为 G 的真子图 (proper subgraph), 记作 $H \subset G$ 。若 $V(H) \subseteq V(G)$ 并且若当 $e \in E(G)$ 的两个端点都在 $V(H)$ 中时, 必有 $e \in E(H)$, 则称 H 是 G 中由顶点集 $V(H)$ 导出的子图, 记作 $G[V(H)]$ 。若有 $X \subseteq E(G)$, 使得 $E(H) = X$ 并且 $v \in V(H)$ 当且仅当 v 与 X 的一条边相关联, 则称 H 是由 G 中边集 X 导出的子图, 记作 $G[X]$ 。在本书中, 通常也用 X 来代表 $G[X]$ (这时 X 既表示一个边子集, 又表示由这个边子集生成的子图)。当 G_1 和 G_2 是 G 的子图时, $G_1 \cup G_2$ 和 $G_1 \cap G_2$ 分别表示 G 中子图 $(V(G_1) \cup V(G_2), E(G_1) \cup E(G_2), \psi|_{E(G_1) \cup E(G_2)})$ 和 $(V(G_1) \cap V(G_2), E(G_1) \cap E(G_2), \psi|_{E(G_1) \cap E(G_2)})$ 。若 $S \subset V(G)$ 是个顶点子集, 则 $G - S$ 代表在 G 中把 S 中的顶点去掉, 并且同时把 G 中与 S 中顶点相关联的边也去掉而得到的子图; 若 $X \subset V(G)$ 是个边子集, 则 $G - X$ 代表在 G 中把 X 中的边去掉而得到的子图。

令 G 为一个无向图。设 $v_0, v_1, \dots, v_n \in V(G)$, $e_1, e_2, \dots, e_n \in E(G)$, 使得对每个 $i = 1, 2, \dots, n$, $e_i = v_{i-1}v_i$, 则称序列 $v_0e_1v_1e_2 \cdots v_{n-1}e_nv_n$ 为一个 (v_0, v_n) -通道 (walk)。当这个 (v_0, v_n) -通道的边集由相关联的顶点唯一确定时, 也常用顶点序列 $P = v_0v_1 \cdots v_n$ 来代表这个通道。当 $v_0 = v_n$ 时, 称 P 是个闭通道 (closed walk), 否则称 P 为一个开通道 (open walk)。若在通道 $P = v_0e_1v_1 \cdots e_nv_n$ 中, 当 $1 \leq i < j \leq n$ 时, 恒有 $e_i \neq e_j$, 则 P 是一个迹 (trail); 若当 $0 \leq i < j \leq n$ 时, $v_i \neq v_j$, 则 P 是一条 (v_0, v_n) -道路或 (v_0, v_n) -路 (path); 若 $v_0 = v_n$ 并且当 $1 \leq i < j \leq n$ 时, $v_i \neq v_j$, 则 P 是一个极小圈 (circuit) (为了和拟阵中的术语一致, 我们称闭道路为一个极小圈, 而把由极小圈的不相交并称为一个圈)。

若对任意的两个顶点 $u, v \in V(G)$, 图 G 中都存在一条 (u, v) -路, 则称 G

是个连通图 (connected graph)。图 G 的一个极大的连通子图称为 G 的一个连通分支 (connected component)； G 的连通分支的个数记为 $\omega(G)$ 。

对 G 的顶点子集 $S \subset V(G)$ ，若 $\omega(G - S) > \omega(G)$ ，或若 $G - S$ 是个无边图，则称 S 为 G 的一个点割集 (vertex-cut set)。若 $S = \{v\}$ 是个单点集，则 v 称为 G 的一个割点 (cut-vertex)。一个连通的平凡图 G 的连通度 (connectivity) 是点数最少的点割集中点的个数，记为 $\kappa(G)$ 。当 G 是平凡图 K_1 或是个不连通图时，定义 $\kappa(G) = 0$ 。

对正整数 k ，若 $\kappa(G) \geq k$ ，则称 G 是个 k -连通图 (k -connected graph)。图 G 中的极大 2-连通子图也称为 G 的块 (block)。关于 k -连通图的特征，有下面著名的 Menger 定理：一个顶点数大于 k 的图 G 是 k -连通的充分必要条件是对 G 中的任意两个不同的顶点 u 和 v ， G 都有至少 k 条 (u, v) -路 $P_1, P_2, \dots, P_k$ ，使得当 $1 \leq i < j \leq k$ 时， $V(P_i) \cap V(P_j) = \{u, v\}$ (Bondy 和 Murty 1976)。

对 G 的边子集 $X \subseteq E(G)$ ，若 $\omega(G - X) > \omega(G)$ ，则称 X 为 G 的一个边割集 (edge-cut set)。若 $X = \{e\}$ ，则 e 称为 G 的一条割边 (cut-edge)。一个非平凡的连通图的边连通度 (edge-connectivity) 是边数最少的边割集中边的个数，记作 $\kappa'(G)$ 。当 G 是平凡图和不连通图时，定义 $\kappa'(G) = 0$ 。

对正整数 k ，若 $\kappa'(G) \geq k$ ，则称 G 是个 k -边连通图 (k -edge-connected graph)。关于 k -边连通图的特征，也有相应的 Menger 定理：一个图 G 是 k -边连通的充分必要条件是对 G 中的任意两个不同的顶点 u 和 v ， G 都有至少 k 条 (u, v) -路 $P_1, P_2, \dots, P_k$ ，使得当 $1 \leq i < j \leq k$ 时， $E(P_i) \cap E(P_j) = \emptyset$ (Bondy 和 Murty 1976)。

(关于图论的基本知识可参见田丰、马仲蕃 (1987)，Bondy 和 Murty (1976) 或其它的图论教科书。我们在这里需要强调说明的是：一般图论教科书中的圈 (cycle) 在本书中将被称为极小圈 (circuit)，而本书中的圈指的是极小圈的一个不相交并。)

第一章 拟阵的基本概念与例子

拟阵理论主要是研究定义在一个集合的子集合上的抽象相关关系。具有这种关系的例子可以在不同的数学分支中找到。比如说在线性代数中，一个线性空间中向量子集所具有的线性相关关系；又如在图论中，一个图 G 中由边集生成有圈子图所确定的相关关系。确定集合 E 上的一个拟阵就是指出 E 中所有相关的子集，等价地，我们也可指出 E 中全体不是相关的子集。不是相关的子集通常也称为独立集。一个拟阵可以有許多不同但是等价的定义方法。在这一章里，我们首先从线性代数和图论中得到关于拟阵的独立集抽象，并由此得到定义拟阵的独立集公理。然后从独立集公理出发，进一步介绍拟阵的一些其他等价公理，它们的相互关系和例子，以及拟阵的一些表示方式。

1.1 独立集公理

设 F 是一个域，我们用 $V(n, F)$ 表示域 F 上的全体 n 维向量组成的线性空间。在线性代数和图论中，我们注意到如下的两个例子。

(1.1.1) 设 $E \subseteq V(n, F)$ 是一个向量子集。若 $X \subset E$ 是 E 中的一个线性无关向量组，则 X 的任意子集 Y 也是一个线性无关向量组。当 $X_1, X_2 \subseteq E$ 是 E 中的两个线性无关向量组并且 $|X_1| < |X_2|$ 时，则 X_1 不是 $X_1 \cup X_2$ 中的极大线性无关向量组。因而有向量 $x \in X_2 - X_1$ ，使得 $X_1 \cup x$ 也是 E 中的一个线性无关向量组。

(1.1.2) 设 G 是一个图，其边集为 $E = E(G)$ 。当 $X \subset E$ 是 G 的一个无圈子图（即不含有极小圈的子图），则 X 的任意子集 Y 也是 G 的一个无圈子图。当

$X_1, X_2 \subseteq E$ 是 G 中的两个无圈子图并且 $|X_1| < |X_2|$ 时 则在 G 的子图 $X_1 \cup X_2$ 中, X_1 也不是 $X_1 \cup X_2$ 的极大无圈子图。因而有 $e \in X_2 - X_1$, 使得 $X_1 \cup e$ 也是 G 中的一个无圈子图。

以上的两个例子反映了两种在不同结构上的一种关系。但这个关系在这两个不同的例子中却有共同的性质。把这些共同的性质抽象出来, 就得到了拟阵的定义。

(1.1.3) 一个拟阵(matroid) M 是一个有序对 $(E, \mathcal{I})$, 其中 E 是一个有限集合, $\mathcal{I} \subset 2^E$ 是 E 中子集的集合, 它们满足以下的公理:

(I1) $\emptyset \in \mathcal{I}$.

(I2) 若 $I \in \mathcal{I}$, 及 $I' \subseteq I$, 则 $I' \in \mathcal{I}$.

(I3) 若 $I_1, I_2 \in \mathcal{I}$ 且 $|I_1| < |I_2|$, 则存在 $e \in I_2 - I_1$ 使得 $I_1 \cup e \in \mathcal{I}$.

集合 $\mathcal{I}$ 中的元素称为拟阵 M 的独立集(independent set)。因此公理 (I1)-(I3) 称为拟阵的独立集公理。拟阵 M 通常也记作 $M = M(E, \mathcal{I})$ 以强调这是一个在 E 上以 $\mathcal{I}$ 中元素为独立集的拟阵。类似地 我们用 $E = E(M)$ 和 $\mathcal{I} = \mathcal{I}(M)$ 来强调 $E(M)$ 是 M 的元素集合而 $\mathcal{I}(M)$ 是 M 的独立集集合。当 $I \in \mathcal{I}(M)$, 并且 $|I| = k$ 时, 也称 I 是 M 的一个 k -独立集 (k -independent subset)。条件 (I1) 保证 $\mathcal{I}$ 不空, 由此 (I1) 可以用 “ $\mathcal{I}$ 含有至少一个 E 中的子集合” 来代替, 但不能用 (I2) 独立地导出。条件 (I3) 称为独立扩充公理。它表示任何一个 M 中的任何两极大独立集都有相同的基数。

从例子 (1.1.1) 与 (1.1.2), 我们可以得到如下的两个结论。

(1.1.4) 设 A 是域 F 上的一个 $n \times m$ 矩阵。又设 A 的列向量的标号集合为 $E = E(A)$ 。定义 $\mathcal{I} \subset 2^E$ 为这样的集合: $X \in \mathcal{I}$ 当且仅当由 X 所标记的列向量在向量空间 $V(n, F)$ 中线性无关。那么 $(E, \mathcal{I})$ 是一个拟阵。

这个拟阵称为 A 的向量拟阵 (vector matroid), 记作 $M[A]$ 。为了强调这是域 F 上的向量相关关系, 我们也采用 $M_F[A]$ 的记号。若 F 是 q 个元素的域, 则也用 $M_q[A]$ 来表示 $M_F[A]$ 。

(1.1.5) 设 G 是一个图, $E = E(G)$ 是 G 的边集。定义 $\mathcal{I} \subset 2^E$ 为这样的集合: $X \in \mathcal{I}$ 当且仅当 X (作为 G 的子图) 不含有极小圈。那么 $(E, \mathcal{I})$ 是一个拟阵。这个拟阵通常称为 G 的圈拟阵 (cycle matroid), 记作 $M(G)$ 。

以下是两个具体的例子:

(1.1.6) 考虑实数域 $\mathbf{R}$ 上的矩阵

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

令 a_i ($1 \leq i \leq 4$) 代表 A 的第 i 个列向量的标号；又令 $E_1 = \{a_1, a_2, a_3, a_4\}$ 为 A 的列向量的标号集合。要确定所有独立集的集族 $\mathcal{I}$ ，我们要找出所有的子集 $I \subseteq E_1$ ，使得由 I 中元素所标号的向量组在 $V(3, \mathbf{R})$ 中线性无关。从线性代数中我们知道，任何一个线性无关向量组都被一个极大线性无关向量组所包含。因此我们只要找出 A 的列向量中的全体极大线性无关向量组。不难看出， A 的全体极大线性无关向量组由 E_1 的这些子集所标号

$$\{a_1, a_2, a_3\}, \{a_1, a_2, a_4\}, \{a_2, a_3, a_4\}.$$

因而

$$\mathcal{I} = \text{Low}\{\{a_1, a_2, a_3\}, \{a_1, a_2, a_4\}, \{a_2, a_3, a_4\}\}.$$

(1.1.7) 考虑图 G

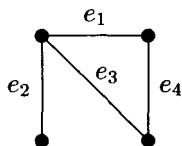


图 1.1 例 (1.1.7) 的图

其边集为 $E_2 = \{e_1, e_2, e_3, e_4\}$ 。我们要确定所有无圈子图的边集的集族 $\mathcal{I}$ 。由于每一个无圈子图都是一个支撑树的子图，因此我们只要找出 G 的所有的支撑树。不难看出 G 的全体支撑树对应的边子集是

$$\{e_1, e_2, e_3\}, \{e_1, e_2, e_4\}, \{e_2, e_3, e_4\},$$

因此，

$$\mathcal{I} = \text{Low}\{\{e_1, e_2, e_3\}, \{e_1, e_2, e_4\}, \{e_2, e_3, e_4\}\}.$$

进一步的观察可以看出，(1.1.6) 与 (1.1.7) 这两个例子，除了一个从矩阵出发得到，另一个从图得到以外，它们有互相对应的独立子集族。因而它们的独立结构没有什么本质的区别，为此我们有如下的定义。

(1.1.8) 对于给定的两个拟阵 $M_1(E_1, \mathcal{I}_1)$ 和 $M_2(E_2, \mathcal{I}_2)$, 若映射 $\phi: E_1 \rightarrow E_2$ 满足以下的条件:

- (i) $\phi: E_1 \rightarrow E_2$ 是一个一一对应,
- (ii) 对任意子集 $X \subseteq E_1$, $X \in \mathcal{I}_1$ 当且仅当 $\phi(X) \in \mathcal{I}_2$.

则称 $\phi: E_1 \rightarrow E_2$ 为从 M_1 到 M_2 的一个同构。若这样的 ϕ 存在, 称 M_1 与 M_2 同构, 记作 $M_1 \cong M_2$ 。对每个拟阵 M , 易见全体从 M 到 M 的同构在映射的复合下构成一个群 $\text{Aut}(M)$ (称为 M 的自同构群)。

作为例子, 若 A 是 (1.1.6) 中的矩阵而 G 是 (1.1.7) 中的图, 则 $M[A] \cong M(G)$, 其同构映射就是 $\phi(a_i) = e_i, (1 \leq i \leq 4)$ 。

设 M 是个拟阵。若存在某个域 F , 及域 F 上的一个矩阵 A 使得 $M \cong M_F[A]$, 则称 M 是个 F -可线性表示拟阵 (F -representable matroid), 或 (在不强调 F 的时候) 称 M 为一个可线性表示拟阵 (representable matroid) (也常简称为 F -可表示拟阵或可表示拟阵); 而矩阵 A 则称为 M 的一个 F -线性表示 (F -representation) (或简称为 F -表示), 有时也称 A 为 M 在 F 上的一个坐标化 (F -coordinatization)。若存在某个图 G , 使得 $M \cong M(G)$, 则称 M 为可图拟阵 (graphic matroid)。

除向量拟阵和可图拟阵外, 均匀拟阵 (见本章习题 (1.1)) 也是常常遇到的拟阵。此外, 还可以通过拟阵的限制 (也称为删除运算和直和运算 (见本章习题 (1.4) 和 (1.5))) 来构造得到新的拟阵的例子。我们用下面关于可图拟阵的讨论来结束这一节。

设 M 是个可图拟阵, 则有某个图 G , 使得 $M = M(G)$ 。若 G 不是连通的, 可设 $G_1, G_2, \dots, G_s$ 是 G 的连通分支。取 $v_i \in V(G_i), i = 1, 2, \dots, s$ 。把各个 v_i 合在一起构成一个新的顶点 v' 我们就从 G 得到一个新的图 G' 。注意到 G' 是连通图, $E(G') = E(G)$, 且边集 $X \subseteq E(G')$ 是 G' 中的无圈图当且仅当 $X \subseteq E(G)$ 是 G 中的无圈图。因此我们得到下面的结论。

(1.1.9) 若 M 是可图拟阵, 则恒存在连通图 G , 使得 $M \cong M(G)$ 。

(1.1.10) 对任意域 F , 若拟阵 M 是可图的, 则 M 也是 F -可线性表示的。

证明 因 M 是可图的, 则有图 G 使得 $M = M(G)$ 。记 $m = |E(M)|$ 。由于 F 是一个域, 可设 F 的乘法单位元是 1, 加法单位元是 0。令 $n = |V(G)|$ 。不妨设 $n > 0$ 。

对 $i = 1, 2, \dots, n$, 令 $\mathbf{e}_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$ 为 $V(n, F)$ 中的向量, 其第 i 个分量是 1, 而其他分量是 0。我们用以下的算法来构造 M 的一个 F -表示。

(1.1.11) (可图拟阵 M 的一个 F -表示的构造)

第 1 步 记 $V(G) = \{v_1, v_2, \dots, v_n\}$ 。

第 2 步 作映射 $\phi: E(G) \rightarrow V(n, F)$, 其定义如下:

对每一条边 $e = v_i v_j \in E(G)$ (不妨设 $i \leq j$), 令 $\phi(e) = \mathbf{e}_j - \mathbf{e}_i$ 。

第 3 步 作域 F 上 $n \times m$ 矩阵 A , A 的列由 $E(M)$ 中的元素标号。对每个 $e \in M$, A 中第 e 列的列向量是 $\phi(e)$ 。

设 $X \subset E$ 。我们只要证明: X 生成 G 中的一个无圈子图当且仅当 $\{\phi(e) : e \in X\}$ 是 $V(n, F)$ 中的一个线性无关向量组。如果我们能够证明这一点, 则第 3 步所得矩阵 A 就是 M 的一个 F -表示。

设 X 是 G 中的一个无圈图。我们对 $|X|$ 用归纳法来证明结论。若 $|X| \leq 1$, 由第 2 步, 因为 X 是个无圈子图, 所以对应的向量集或是空集, 或是由一个非零向量组成的集合, 因而在 $V(n, F)$ 中线性无关。当 $|X| \geq 2$, 由于 X 无圈, 存在 $e' = v_i v_j \in X$, 使得 v_j 在 X 中是个度为 1 的顶点。不妨设 $j > i$, 则 $\phi(e')$ 的第 j 个分量是 1, 并且对任意的 $e \in X - e'$, $\phi(e)$ 的第 j 个分量均为 0。若 $\{\phi(e) : e \in X\}$ 在 $V(n, F)$ 中线性相关, 则在 F 中有不全为 0 的元素 α_e , 使

$$\sum_{e \in X} \alpha_e \phi(e) = 0.$$

由于 $e' \in X$, 上式可写成

$$\alpha_{e'} \phi(e') + \sum_{e \in X - e'} \alpha_e \phi(e) = 0.$$

比较等式两边的第 j 个分量, 可知 $\alpha_{e'} = 0$ 。于是有 $\sum_{e \in X - e'} \alpha_e \phi(e) = 0$ 。由于 $X - e'$ 是 G 中的无圈图, 根据归纳假设, $\{\phi(e) : e \in X - e'\}$ 在 $V(n, F)$ 中线性无关。因此对任意的 $e \in X - e'$, 都有 $\alpha_e = 0$, 这与 α_e 的选择矛盾。从而 $\{\phi(e) : e \in X\}$ 是 $V(n, F)$ 中的一个线性无关向量组。

设 $\{\phi(e) : e \in X\}$ 是 $V(n, F)$ 中的一个线性无关向量组, 我们用反证法来证明 X 是 G 中的无圈子图。若不然, 则有 $X = \{e_1, e_2, \dots, e_s\}$ 使得 $v_{i_1} e_1 v_{i_2} e_2 \dots$

$v_{i_s} e_s v_{i_1}$ 是 X 中的一个极小圈 这里 $e_j = v_{i_j} v_{i_{j+1}}$ ($1 \leq i \leq s-1$) 及 $v_{i_{s+1}} = v_{i_1}$.
令

$$\alpha_j = \begin{cases} 1, & \text{若 } i_{j+1} \geq i_j, \\ -1, & \text{若 } i_{j+1} < i_j. \end{cases}$$

则

$$\sum_{j=1}^s \alpha_j \phi(e_j) = 0.$$

这与 $\{\phi(e) : e \in X\}$ 在 $V(n, F)$ 中线性的假设矛盾。所以 X 是 G 中的无圈子图。 $\square$

习题

(1.1) 设 $n > r > 0$ 为两个整数, E 是个 n -元集. 令

$$\mathcal{I} = \{X \subseteq E : |X| \leq r\}.$$

则 $(E, \mathcal{I})$ 是个拟阵 (这种拟阵称为均匀拟阵 (uniform matroid), 记作 $U_{r,n}$).

(1.2) 证明 $(E, \mathcal{I})$ 是个拟阵当且仅当 $\mathcal{I}$ 满足 (I2) 和下面的两个条件:

(I1)' $\mathcal{I}$ 不空.

(I3)' 若 $I_1, I_2 \in \mathcal{I}$ 且 $|I_2| = |I_1| + 1$, 则恒有 $e \in I_2 - I_1$, 使 $I_1 \cup e \in \mathcal{I}$.

(1.3) 证明 $(E, \mathcal{I})$ 是个拟阵当且仅当 $\mathcal{I}$ 满足 (I1), (I2) 和下面的条件:

(I3)'' 对任意 $X \subseteq E$, 若 $I_1, I_2 \in \text{Max}\{I \subseteq X : I \in \mathcal{I}\}$, 则 $|I_1| = |I_2|$.

(1.4) 设 $M(E, \mathcal{I})$ 是个拟阵, $X \subseteq E$. 令 $\mathcal{I}_X = \{I \subseteq X : I \in \mathcal{I}\}$, 则 $(X, \mathcal{I}_X)$ 是个拟阵. (这个拟阵称为 M 在 X 上的限制(restriction), 记作 $M|X$. 由于 $M|X$ 也可看作是从 M 中把 $E - X$ 删除的拟阵 因此 $M|X$ 也记作 $M - (E - X)$, 称为 M 的一个删削或删除(deletion).)

(1.5) 设 $M_1(E_1, \mathcal{I}_1), M_2(E_2, \mathcal{I}_2)$ 是两个拟阵满足 $E_1 \cap E_2 = \emptyset$. 定义 $E = E_1 \cup E_2$ 及 $\mathcal{I} = \{I_1 \cup I_2 : I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}$. 则 $M(E, \mathcal{I})$ 是个拟阵, 称为 M_1 与 M_2 的直和 (direct sum), 记作 $M = M_1 \oplus M_2$. 并证明 $M_1 \oplus M_2 \cong M_2 \oplus M_1$.

(1.6) 设 $M(E, \mathcal{I})$ 是个拟阵.

(i) 若 $B_1, B_2 \in \text{Max}(\mathcal{I})$, 则 $|B_1| = |B_2|$.

(ii) 若 $B \in \text{Max}(\mathcal{I})$, $I \in \mathcal{I}$ 满足 $|I| = |B|$, 则 $I \in \text{Max}(\mathcal{I})$.

1.2 极小圈公理

设 $M(E, \mathcal{I})$ 是一个拟阵。若子集 $X \in \text{Opp}(\mathcal{I}) = 2^E - \mathcal{I}$, 则 X 称为 M 的一个相关集 (dependent set)。极小的相关集叫做极小圈 (circuit)。令 $\mathcal{C}(M)$ 表示由拟阵 M 的全体极小圈组成的集合, 则有 $\mathcal{C}(M) = \text{Min}(\text{Opp}(\mathcal{I}))$ 。当 $C \in \mathcal{C}(M)$, 并且 $|C| = k$ 时, 我们称 C 为 M 的一个 k -极小圈 (k -circuit), k 为 C 的长度 (length)。

(1.2.1) 设 $M(E, \mathcal{I})$ 是一个拟阵, $\mathcal{C} = \mathcal{C}(M)$, 则 $\mathcal{C}$ 满足下列性质:

(C1) $\emptyset \notin \mathcal{C}$ 。

(C2) 若 $C_1, C_2 \in \mathcal{C}$ 且 $C_1 \subseteq C_2$, 则 $C_1 = C_2$ 。

(C3) 若 $C_1 \neq C_2, C_1, C_2 \in \mathcal{C}$ 并且存在 $e \in C_1 \cap C_2$, 则恒有 $C_3 \in \mathcal{C}$ 满足 $C_3 \subseteq (C_1 \cup C_2) - e$ 。

证明 因为 $M(E, \mathcal{I})$ 是拟阵, $\mathcal{I}$ 满足独立集公理 (I1)–(I3)。根据 (I1), $\emptyset \in \mathcal{I}$, 故 $\emptyset \notin \mathcal{C}$ 。

若 $C_1, C_2 \in \mathcal{C}$ 且 $C_1 \subseteq C_2$, 因为 $C_1 \in 2^E - \mathcal{I}$ 而 C_2 是 $2^E - \mathcal{I}$ 中的极小元, 所以一定有 $C_1 = C_2$ 。

我们来证明 (C3)。设 $C_1 \neq C_2, C_1, C_2 \in \mathcal{C}$ 并且 $e \in C_1 \cap C_2$ 。要证明 (C3), 只要证明 $C_1 \cup C_2 - e \in 2^E - \mathcal{I}$ 。若 $C_1 \cup C_2 - e \in \mathcal{I}$, 则 $C_1 \cup C_2 - e$ 是包含于 $C_1 \cup C_2$ 中的一个独立集。由于 $C_1 \neq C_2$, 存在 $e_1 \in C_1 - C_2$ 。因 $C_1 \in \mathcal{C}$, $C_1 - e_1$ 也是包含于 $C_1 \cup C_2$ 的一个独立集。据公理 (I3) 独立集 $C_1 - e_1$ 可扩充为一个包含于 $C_1 \cup C_2$ 的极大独立集 I 。由于 $C_2 \in \mathcal{C}(M)$, C_2 不能是 I 的子集 故必有 $e_2 \in C_2 - I$ 因而有 $I \subseteq (C_1 - e_1) \cup (C_2 - e_2)$ 。这样, $|I| \leq |C_1 \cup C_2| - 2$ 。根据假设, $C_1 \cup C_2 - e \in \mathcal{I}$ 且 $|C_1 \cup C_2 - e| = |C_1 \cup C_2| - 1 > |I|$ 。于是据公理 (I3), I 不可能是包含于 $C_1 \cup C_2$ 的极大独立集。这个矛盾说明 $C_1 \cup C_2 - e \notin \mathcal{I}$ 。□

命题 (1.2.1) 中的性质 (C1)–(C3) 可以唯一地确定拟阵 M 的结构。

(1.2.2) 设 E 是一个集合 并设 $\mathcal{C} \subset 2^E$ 是个满足条件 (C1)–(C3) 的子集合族, 则必有 E 上的拟阵 M 使得 $\mathcal{C} = \mathcal{C}(M)$ 。

证明 若有这样的 M 存在, E 中什么样的子集会在 $\mathcal{I}(M)$ 中呢? 按照定义,

$\mathcal{I}(M)$ 中的元素一定不能包含任何 $\mathcal{C}$ 中的元素作为子集。从这点出发, 定义

$$\mathcal{I} = Opp(Upp(\mathcal{C})).$$

我们希望能够证明 $\mathcal{I}$ 满足公理 (I1)–(I3)。

根据 (C1), $\emptyset \notin \mathcal{C}$, 于是 $\emptyset \in \mathcal{I}$ 。若 $I \in \mathcal{I}$ 并且 $I' \subset I$, 则据 $Upp(\mathcal{C})$ 的定义, I' 不能在 $Upp(\mathcal{C})$ 中。由此也有 $I' \in \mathcal{I}$ 。

我们用反证法来证明 $\mathcal{I}$ 也满足 (I3)。若不然, 则存在一个子集对 (I_1, I_2) , 满足 $I_1, I_2 \in \mathcal{I}$, 并且 $|I_2| > |I_1|$ 但对任意的 $e \in I_2 - I_1$, 都有 $I_1 \cup e \notin \mathcal{I}$ 。考虑子集 $I_1 \cup I_2$ 。注意到存在这样的子集 I , 满足 $I \in \mathcal{I}, I \subseteq I_1 \cup I_2$ 并且 $|I_1| < |I|$ (I_2 就是其中之一)。在这些子集中我们选取一个 $I_3 \in \mathcal{I}$ 满足 $I_3 \subseteq I_1 \cup I_2$, $|I_1| < |I_3|$ 并且 $|I_1 - I_3|$ 最小。

从 I_1 的选取可知 $I_1 - I_3 \neq \emptyset$ 。取定一个元素 $e \in I_1 - I_3$ 。对任意的 $f \in I_3 - I_1$, 令 $I_f = (I_3 \cup e) - f$ 。由于 $|I_1 - I_f| < |I_1 - I_3|$ 且 $I_f \subseteq I_1 \cup I_2$, 必有 $I_f \notin \mathcal{I}$, 否则与 I_3 的选取矛盾。因而 I_f 含有一个子集 $C_f \in \mathcal{C}$ 。由于 $I_3 \in \mathcal{I}$, 必有 $e \in C_f$ 。

先取 $g \in I_3 - I_1$, 得到 C_g 。若 $C_g \cap (I_3 - I_1) = \emptyset$, 则 $C_g \subseteq I_g \cap I_1 \subseteq (I_1 \cap (I_3 \cup e)) - g \subseteq I_1$, 与 $I_1 \in \mathcal{I}$ 的假设矛盾。于是又可取 $h \in C_g \cap (I_3 - I_1)$, 并得到 C_h 。注意到 $e \in C_g \cap C_h$ 并且 $C_g, C_h \in \mathcal{C}$ 。由于 $\mathcal{C}$ 满足 (C3), 故存在 $C \in \mathcal{C}$, 满足 $C \subseteq C_g \cup C_h - e \subseteq (I_3 \cup e) - e = I_3$, 这与 $I_3 \in \mathcal{I}$ 的假定矛盾。这说明 $\mathcal{I}$ 一定满足 (I3)。

由于 $\mathcal{I}$ 满足独立集公理 (I1)–(I3), 所以存在一个定义在 E 上的拟阵 M , 使得 $\mathcal{I} = \mathcal{I}(M)$ 。

下面我们来证明 对这样得到的拟阵 M , 必有 $\mathcal{C} = \mathcal{C}(M)$ 。先来证明 $\mathcal{C}(M) \subseteq \mathcal{C}$ 。取 $C \in \mathcal{C}(M)$ 。若 $C \in \mathcal{C}(M)$, 则由极小圈的定义, $C \notin \mathcal{I}(M)$ 但对任一元素 $e \in C, C - e \in \mathcal{I}(M)$ 。由于 $C \notin \mathcal{I}(M)$, C 含有一个子集 $C' \in \mathcal{C}$; 但是任何 C 的真子集都在 $\mathcal{I}(M)$ 中, 因此必有 $C = C' \in \mathcal{C}$ 。这就证明了 $\mathcal{C}(M) \subseteq \mathcal{C}$ 。注意到这个证明是可逆的。把这证明倒过去, 就可以证明 $\mathcal{C} \subseteq \mathcal{C}(M)$ 。于是 $\mathcal{C} = \mathcal{C}(M)$ 得证。□

设 M 是一个拟阵, $C \in \mathcal{C}(M)$ 。若 $C = \{e\}$, 则 e 称为 M 的一个环 (或环元) (loop); 若 $C = \{e_1, e_2\}$, 则称 e_1 与 e_2 互为平行元素 (parallel elements) 或者说 e_1 平行于 e_2 。若拟阵 M 不含有环及平行元素, 则称 M 是个简单拟阵 (simple

matroid)。一个简单拟阵也称为一个组合几何 (combinatorial geometry)。

(1.2.3) 设 $M(E, \mathcal{I})$ 是一个拟阵, $I \in \mathcal{I}$ 且 $e \in E - I$, 则或者 $I \cup e \in \mathcal{I}$, 或者 $I \cup e$ 含有唯一的一个极小圈 $C \in \mathcal{C}(M)$, 使得 $e \in C \subset I \cup e$ 。

证 明 设 $I \cup e \notin \mathcal{I}$, 则据极小圈定义, 必有 $C \in \mathcal{C}(M)$ 使得 $C \subset I \cup e$ 。

设 $C' \neq C$, $C' \in \mathcal{C}(M)$, 且 $e \in C' \subset I \cup e$ 。因为 $I \in \mathcal{I}$, 所以 $e \in C'$ 。由于 $e \in C \cap C'$, 根据 (C3), 存在 $C'' \in \mathcal{C}(M)$, 使得 $C'' \subseteq C \cup C' - e \subseteq I$, 这与 $I \in \mathcal{I}$ 的假设矛盾。因此 C 是唯一的。□

极小圈公理中的 (C3) 称为极小圈消去公理 (circuit elimination)。应用 (C3) 和其他极小圈公理我们可以得到较强的强极小圈消去公理及其他形式的极小圈性质 (见本节习题)。

(1.2.4) 设 M 是个拟阵, 则 $\mathcal{C} = \mathcal{C}(M)$ 满足以下的强极小圈消去公理 (strong circuit elimination) :

(C3)' 设 $C_1, C_2 \in \mathcal{C}$ 。若有 $e \in C_1 \cap C_2$ 及 $f \in C_2 - C_1$, 则必有 $C_3 \in \mathcal{C}$ 使得 $f \in C_3 \subseteq (C_1 \cup C_2) - e$ 。

证明 用反证法, 设 (C3)' 不真。则对给定的 M , 存在 $C_1, C_2 \in \mathcal{C}(M)$ 及元素 $e \in C_1 \cap C_2, f \in C_2 - C_1$, 但 M 中不存在 (C3)' 所要求的 C_3 。我们称这样的 (C_1, C_2) 为一个反例对。选取反例对 (C_1, C_2) 使得 $|C_1 \cup C_2|$ 尽可能的小。

从 (C3) 可知有 $C_3 \subseteq C_1 \cup C_2 - e$ 。根据 (C2) 不可能有 $C_3 \subseteq C_2 - e$ 。因此必有 $g \in C_3 \cap (C_1 - C_2)$ 。现在我们来考虑极小圈 C_1 和 C_3 。注意到 $g \in C_1 \cap C_3$, $e \in C_1 - C_3$ 且 $C_1 \cup C_3 \subseteq C_1 \cup C_2 - f$ 。根据我们选取 (C_1, C_2) 的原则, C_1 和 C_3 不是一对反例对。从而有 $C_4 \in \mathcal{C}(M)$, 满足 $e \in C_4 \subseteq C_1 \cup C_3 - g$ 。再来考察 C_2 和 C_4 。注意到 $e \in C_2 \cap C_4, C_4 \subseteq C_1 \cup C_3 - g \subseteq C_1 \cup C_2 - \{g, f\}$, 故 $f \in C_2 - C_4$ 。由于 $g \in C_1 - C_2$ 且 $g \notin C_4$, 可知 $C_4 \cup C_2 \subseteq C_1 \cup C_2 - g$ 。同理据 (C_1, C_2) 的选取, (C_2, C_4) 不是反例对, 故有 $C_5 \in \mathcal{C}(M)$, 使得

$$f \in C_5 \subseteq C_2 \cup C_4 - e \subseteq C_1 \cup C_2 - \{g, e\},$$

这与 (C_1, C_2) 是个反例对的假设矛盾。□

习题

(2.1) 设 G 是一个图, 满足 $E(G) \neq \emptyset$. 又设 $\mathcal{C}^*$ 是 G 中全体极小边割集的集合族. 证明集合族 $\mathcal{C}^*$ 满足极小圈公理 (C1), (C2) 和 (C3). (从而有 $E(G)$ 上的一个拟阵 $M^*(G)$, 其极小圈族为 $\mathcal{C}^*$. $M^*(G)$ 称为图 G 的余圈拟阵 (cocycle matroid).)

(2.2) 设 $C_1, C_2 \in \mathcal{C}(M)$ 且满足 $E(M) = C_1 \cup C_2$ 及 $C_1 - C_2 = \{e\}$. 若有 $C_3 \in \mathcal{C}(M)$, 证明或者 $C_3 = C_1$, 或者 $C_2 - C_1 \subseteq C_3$.

(2.3) 设 $M(E, \mathcal{I})$ 是拟阵. 试证明下列命题:

(i) (极小圈传递性质) 设 $C_1, C_2 \in \mathcal{C}(M)$ 且有 $e_1 \in C_1 - C_2, e_2 \in C_2 - C_1$ 及 $C_1 \cap C_2 \neq \emptyset$. 则存在 $C_3 \in \mathcal{C}(M)$, 使得 $e_1, e_2 \in C_3 \subseteq C_1 \cup C_2$.

(ii) 对任意 $e_1, e_2 \in E$, 定义 $e_1 \sim e_2$ 当且仅当 $e_1 = e_2$ 或存在 $C \in \mathcal{C}(M)$, 使得 $e_1, e_2 \in C$. 证明 $\sim$ 是 E 上的一个等价关系.

(iii) 若 $M = M(G)$ 是某个图 G 的圈拟阵, 那么在 (ii) 中定义的等价关系 $\sim$ 所确定的等价类对应于 G 的什么子图? (参见第三章习题 (1.8)).

(2.4) 设 $M(E, \mathcal{I})$ 是拟阵. 对任意 $e_1, e_2 \in E$, 定义 $e_1 \sim e_2$ 当且仅当 $e_1 = e_2$ 或 $\{e_1, e_2\} \in \mathcal{C}(M)$.

(i) 证明 $\sim$ 是 E 上的一个等价关系.

(ii) 记 $\tilde{E}$ 为由 $\sim$ 所确定的全体等价类的集合. 对每个子集合 $X \subseteq E$, 令 $\tilde{X} \subset \tilde{E}$ 为 X 中元素所在的等价类作成的 $\tilde{E}$ 中的子集. 证明若 $X_1 = X_2$ 且 $|X_1| = |X_2|$, 则 $X_1 \in \mathcal{I}$ 当且仅当 $X_2 \in \mathcal{I}$.

(iii) 设

$$\mathcal{I}' = \{X \subseteq E : X \in \mathcal{I}\}.$$

证明 $\mathcal{I}'$ 满足独立集公理 (I1), (I2) 和 (I3).

(iv) 给出一个拟阵 M , 我们进行以下的算法:

(第一步) 找出 M 的一个环 e , 把 M 换为 $M - e$.

(第二步) 找出 M 的一对平行元素 e_1, e_2 , 把 M 换为 $M - e_2$.

(第三步) 重复 (第一步) 和 (第二步) 直到所处理的拟阵 M 是个简单拟阵.

令 M' 记拟阵 M 经过此算法而得到的简单拟阵, 并称为 M 的简单化拟阵 (simplification of M). 证明若 M 是个无环的拟阵, 则在 E 上以 $\mathcal{I}'$ (见本习题之 (iii)) 为独立集的拟阵同构于 M' . (从而 M 在同构意义下是唯一的.)

(2.5) 设 $\mathcal{D}$ 是 E 上的一个集合族. 找出并证明 $\mathcal{D}$ 是 E 上某个拟阵 M 之全体相关子集合的充分必要条件.

(2.6) 设 M_1 和 M_2 是两个在 E 上的拟阵. 举例说明 $(E, \mathcal{I}(M_1) \cap \mathcal{I}(M_2))$ 不一定是个拟阵.

(2.7) 设 X 是 $E(M)$ 的一个子集, 则 $\mathcal{C}(M|X) = \{C \in \mathcal{C}(M) : C \subseteq X\}$ (参看本章习题 (1.4)).

(2.8) 设 $X \subseteq E(M)$ 并且 $X \in \mathcal{I}(M)$, 则下列命题等价:

(i) $X \in \text{Max}(\mathcal{I}(M))$;

(ii) 对每个 $e \in E(M) - X$, $X \cup e$ 含有唯一的一个极小圈 C_e 且 $e \in C_e$.

1.3 基公理

沿用线性代数中的术语, 我们称拟阵 M 中的极大独立子集为 M 的基 (base). 记 $\mathcal{B}(M)$ 为 M 中全体基的集合. 则 $\mathcal{B}(M) = \text{Max}(\mathcal{I})$. 若 E 是某个有限维线性空间 $V(n, F)$ 的子集, 则 E 中任意两个极大线性无关子集含有相同个数的元素; 若 B 是 E 中一个极大线性无关子集, 且 $x \in E - B$, 则 $B \cup x$ 含有唯一的一个极小线性相关子集. 拟阵的基也有同样的性质. 命题 (1.3.1) 是 (1.2.3) 的直接推论.

(1.3.1) 设 B 是拟阵 M 的一个基, 且 $x \in E - B$, 则 $B \cup x$ 含有一个唯一的极小圈 C . (我们称 $B \cup x$ 中这个唯一的极小圈 C 为元素 x 对应于基 B 的基本极小圈 (fundamental circuit of x with respect to B), 记作 $C_M(x, B)$ 或 $C(x, B)$.)

(1.3.2) 设 $M(E, \mathcal{I})$ 是个拟阵, 令 $\mathcal{B} = \mathcal{B}(M)$, 则 $\mathcal{B}$ 有如下性质:

(B1) $\mathcal{B}$ 至少含有一个元素 (即 M 有至少一个基).

(B2) 若 $B_1, B_2 \in \mathcal{B}$ 且 $x \in B_1 - B_2$, 则必有 $y \in B_2 - B_1$ 使得 $(B_1 - x) \cup y \in \mathcal{B}$.

证明 由于 $M(E, \mathcal{I})$ 是个拟阵, $\mathcal{I}$ 满足 (I1), 故 $\mathcal{I}$ 至少含有一个元素. 于是 $\mathcal{B} = \text{Max}(\mathcal{I})$ 也至少含有一个元素. 因而 (B1) 得证.

现在来证明 (B2). 设 $B_1, B_2 \in \mathcal{B}$ 且 $x \in B_1 - B_2$. 由基的定义, $B_1, B_2 \in \mathcal{I}$ 并且 $|B_1| = |B_2|$ (见本章习题 (1.6)(i)). 于是据 (I1), $B_1 - x \in \mathcal{I}$. 因为 $|B_1 - x| < |B_1| = |B_2|$, 所以根据 (I3), 必有 $y \in B_2 - (B_1 - x)$, 使得 $(B_1 - x) \cup y \in \mathcal{I}$. 因为 $x \notin B_2$, 所以 $x \neq y$. 从而 $y \in B_2 - B_1$, 并且 $|(B_1 - x) \cup y| = |B_1 - x| + 1 = |B_1| = |B_2|$. 由此可知必有 $(B_1 - x) \cup y \in \mathcal{B}$ (本章习题 (1.6)(ii)). $\square$

(1.3.3) 设 E 是个非空集, 又设 $\mathcal{B} \subset 2^E$ 满足条件 (B2), 则

(B3) 若 $B_1, B_2 \in \mathcal{B}$, 则 $|B_1| = |B_2|$.

证明 用反证法。设有 $B_1, B_2 \in \mathcal{B}(M)$ 并设 $|B_1| < |B_2|$ 。在这些使 (B3) 不成立的子集对中，取反例 B_1, B_2 ，满足 $|B_2| > |B_1|$ 并且 $|B_1 \cap B_2|$ 尽可能大。

由于 $|B_2| > |B_1|$ ，可取 $x \in B_2 - B_1$ 。据 (B2)，恒有 $y \in B_1 - B_2$ 使 $B_3 = (B_2 \cup y) - x \in \mathcal{B}$ 。于是从 $x \notin B_1$ 及 $y \notin B_2$ 可知， $B_2 \cap B_1 \subseteq B_3 \cap B_1 - y$ ，且 $y \in B_3 \cap B_1$ 。

因而 $|B_3 \cap B_1| \geq |B_2 \cap B_1| + 1$ 。据 B_1, B_2 的选取， B_1, B_3 不能是反例子集对，故有

$$|B_1| = |B_3| = |B_2| + 1 - 1 = |B_2|,$$

这与 B_1, B_2 是个反例子集对的假设矛盾，因而 (B3) 得证。□

定理 (1.3.2) 中的条件 (B2) 也可以有下列的形式。其证明留作习题。

(1.3.4) 设 M 是个拟阵，则 $\mathcal{B}(M)$ 满足下面的条件。

(B2)' 若 $B_1, B_2 \in \mathcal{B}(M)$ 且 $x \in B_1 - B_2$ ，则必有 $y \in B_2 - B_1$ 使得 $(B_2 - y) \cup x \in \mathcal{B}$ 。

拟阵的基完全由条件 (B1) 和 (B2) 所决定。像拟阵的独立集和极小圈一样，拟阵的基也唯一地确定了所在的拟阵。故 (B1) 和 (B2) 叫做拟阵的基公理。

(1.3.5) 设 E 是个非空集，又设 $\mathcal{B} \subset 2^E$ 满足条件 (B1) 和 (B2)。则存在拟阵 $M(E, \mathcal{I})$ ，满足 $\mathcal{B} = \mathcal{B}(M)$ 。

证明 若有这样的拟阵 M 存在，使 $\mathcal{B}(M) = \mathcal{B}$ ，则 $\mathcal{I}(M)$ 中的元素一定是 $\mathcal{B}$ 中某个成员的子集。这就启发了我们来定义： $\mathcal{I} = \text{Low}(\mathcal{B})$ 。

我们先来证明 $\mathcal{I}$ 满足独立集公理 (I1)–(I3)。易见 (I1) 可以从 (B1) 立即推得，且 (I2) 也可以从 $\mathcal{I} = \text{Low}(\mathcal{B})$ 马上得到。因而只需要证明 (I3)。

用反证法，假定有 $I_1, I_2 \in \mathcal{I}$ ，满足 $|I_1| < |I_2|$ ，但

(1.3.6) 对任意的 $e \in I_2 - I_1, I_1 \cup e \notin \mathcal{I}$ 。

因为 $\mathcal{I} = \text{Low}(\mathcal{B})$ ，恒存在 $B_1, B_2 \in \mathcal{B}$ ，满足 $I_1 \subseteq B_1, I_2 \subseteq B_2$ 。对给定的一对满足 (1.3.4) 的子集 I_1, I_2 ，选取 $B_1, B_2 \in \mathcal{B}$ ，使得 $I_1 \subseteq B_1, I_2 \subseteq B_2$ ，并且 $|B_1 \cap B_2|$ 尽可能大。我们来逐条证明以下各个断言。

(一) $|B_1| = |B_2|$ 。

由于这里的 $\mathcal{B}$ 满足 (B2)，因而据 (1.3.3)， $\mathcal{B}$ 也满足 (B3)。

(二) $B_1 - B_2 \neq \emptyset$ 。