マトロイド理論

@bd_gfngfn

2015 年 10 月 13 日

目次

はじめに

この文書はおおよそ D. J. A. Welsh, *Matroid Theory* の流れに基づいてマトロイドの理論を追ったものである．記法は，*Matroid Theory* で用いられているものにはできるだけ従っているが，見通しをよくするために独自に拡張したり全く新しく定めたものもある．また用語の日本語訳に於いてもこの文書で独自に定めた表現がある．例えば “circuit” は単に「サーキット」と訳されることが多いが，この文書では「周」と訳している．このほか数式表現における量化と論理演算は，別行立てでは論理式に近い形式表現で，文中では自然言語によってそれぞれ表すようにしている．

1 準備

1.1 集合に関して

この文書で扱う集合はおおかた有限集合である．したがって，集合について必要以上に公理的に見ることはせず，比較的素朴に扱う方針をとる．X が Y の部分集合であることを $X \subseteq Y$ と書き，しばしば Y が X を包むと言い表す．X の部分集合全体すなわち X の冪集合は $\mathfrak{P}X$ と書く．$X \subseteq Y$ かつ $X \neq Y$ であることを $X \subsetneq Y$ と書き，しばしば Y が X を真に包むと言い表す．X と Y の和集合は $X \cup Y$，X と Y の直積は $X \times Y$ と書く．なお，集合 S と述語 P を用いた集合の内包記法 $\{x \in S \mid P(x)\}$ は分出公理を意識したものである．しばしば左側にも写像 f を用いて $\{f(x) \mid P(x)\}$ のように書くが，これは $\{y \in \operatorname{cod} f \mid \exists x \in \operatorname{dom} f.\, (y = f(x) \ \wedge \ P(x))\}$ の略記である．

定義 1.1.1 共通部分

集合 A，B に対し，$A \cap B \coloneqq \{x \in A \mid x \in B\}$ を A と B の**共通部分** (intersection) と呼ぶ[*1]．

定義 1.1.2 差，対称差

集合 A，B に対し，$A \setminus B \coloneqq \{x \in A \mid x \notin B\}$ を A と B の**差** (difference) 或いは**差集合**と呼ぶ．また，$A \triangle B \coloneqq (A \setminus B) \cup (B \setminus A)$ を A と B の**対称差** (symmetric difference) と呼ぶ．

定義 1.1.3 二項関係

集合 A と B に対し，$R \subseteq A \times B$ を A と B の上の**二項関係** (binary relation) と呼ぶ．特に $R \subseteq A \times A$ を A 上の二項関係と呼ぶ．また，$a \in A$ と $b \in B$ に対して二項関係 $R \subseteq A \times B$ が $(a, b) \in R$ を満たすとき，これを $a\, R\, b$ と中置演算子に見せかけた糖衣構文で書く．

定義 1.1.4 写像

集合 A，B，二項関係 $f \subseteq A \times B$ が

$$\forall a \in A.\ \ \exists b \in B.\ \ a\ f\ b$$
$$\forall a \in A.\ \ \forall b_1 \forall b_2 \in B.\, \big((a\ f\ b_1 \ \wedge \ a\ f\ b_2) \Rightarrow \ b_1 = b_2\big)$$

を共に満たすとき，すなわち任意の $a \in A$ に対して $a\ f\ b$ なる $b \in B$ が一意的に存在するとき，f を A から B への**写像** (map) と呼ぶ．A を f の**定義域** (domain of definition) 或いは**始域** (domain)，B を f の**値域** (range) 或いは**終域** (codomain) と呼び，f が A から B への写像であることを $f\colon A \to B$ と書く．また，写像 $f\colon A \to B$ と $a \in A$ に対して一意的に存在する $a\ f\ b$ なる $b \in B$ を $f(a)$ と書く．

定義 1.1.5 写像の制限

写像 $f\colon A \to B$ と $X \subseteq A$ に対し，

[*1] 稀に共通部分のことを積集合と呼ぶことがあるが，直積との混同を避けるため使わないことにする．また，和集合も直和との混同を避けてか**合併** (union) と呼んだりする．

$$\begin{array}{rccc} f|_X\colon & X & \longrightarrow & B \\ & \cup & & \cup \\ & x & \longmapsto & f(x) \end{array}$$

で定義される $f|_X$ を f の X への**制限**と呼ぶ.

定義 1.1.6 像，逆像

写像 $f\colon A \to B$ と集合 $X \subseteq A$ に対して $f[X] \coloneqq \{y \in B \mid \exists x \in X.\ y = f(x)\}$ を f による X の**像** (image) と呼ぶ．また，写像 $f\colon A \to B$ と集合 $Y \subseteq B$ に対して $f^{-1}[Y] \coloneqq \{x \in A \mid f(x) \in Y\}$ を f による Y の**逆像** (inverse image) と呼ぶ.

定義 極大・極小集合全体の記法

集合族 $\mathscr{F}$ に対し，

$$\begin{aligned} \operatorname{maxl}\mathscr{F} &\coloneqq \{X \in \mathscr{F} \mid \forall Y \in \mathscr{F}.\ (Y \supseteq X \Rightarrow Y = X)\} \\ \operatorname{minl}\mathscr{F} &\coloneqq \{X \in \mathscr{F} \mid \forall Y \in \mathscr{F}.\ (Y \subseteq X \Rightarrow Y = X)\} \end{aligned}$$

で $\operatorname{maxl}\mathscr{F}$，$\operatorname{minl}\mathscr{F}$ を定める.

補足 同一の性質を持った集合族 $\mathscr{F}$ の元のうち包含関係に関して極大であるもの全体が $\operatorname{maxl}\mathscr{F}$，極小であるもの全体が $\operatorname{minl}\mathscr{F}$ である.

1.2 グラフに関して

有限個の**頂点** (vertex) と，それらの頂点のうち順序の区別なくまた重複を許して 2 個を結ぶ有限本の**辺** (edge) からなる図形的構造を**無向グラフ** (undirected graph) と呼ぶ．“頂点と辺をどのように配置するか”については考慮に入れる場合と入れない場合があるが，入れない場合，“代数的には”次のように定義される.

定義 1.2.1 無向グラフ

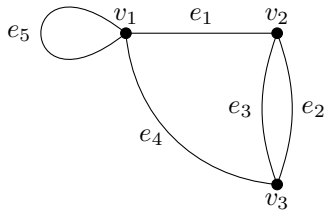
有限集合 V，E と写像 $\partial\colon E \to \mathfrak{P}V$ が

$$\forall e \in E.\ \ 1 \leq \left|\partial(e)\right| \leq 2$$

を満たすとき，$G = (V, E; \partial)$ を**無向グラフ** (undirected graph) 或いは単に**グラフ** (graph) と呼び，V を G の**頂点集合** (vertex set)，E を G の**辺集合** (set of edges) と呼ぶ．また $e \in E$ に対して $v \in V$ が $v \in \partial(e)$ を満たすとき，v を e の**端点** (endpoint) と呼ぶ．なお， ∂ を意識しなくてよい場合は $G = (V, E; \partial)$ を $G = (V, E)$ と略記する.

定義 1.2.2 隣接性

グラフ $G = (V, E; \partial)$ に於いて $e \in E$ が $\left|\partial(e)\right| = 2$ を満たして $\partial(e) = \{u, v\}$ であるとき，e は u と v を**結ぶ** (joint) という．また，$u \neq v$ なる $u, v \in V$ に対し，$\partial(e) = \{u, v\}$ なる $e \in E$ が存在するとき，u と v は**隣接している** (adjacent) という.



$$
\begin{aligned}
V &= \{v_1, v_2, v_3\} \\
E &= \{e_1, e_2, e_3, e_4, e_5\} \\
\partial(e_1) &= \{v_1, v_2\} \\
\partial(e_2) = \partial(e_3) &= \{v_2, v_3\} \\
\partial(e_4) &= \{v_1, v_3\} \\
\partial(e_5) &= \{v_1\}
\end{aligned}
$$

図 1.1　グラフの例

定義 1.2.3 ループ，並行性

グラフ $G = (V, E; \partial)$ に於いて $e \in E$ が $\left|\partial(e)\right| = 1$ を満たすとき，e を**ループ** (loop) と呼ぶ．また，$e_1, e_2 \in E$ が $\partial(e_1) = \partial(e_2)$ かつ $\left|\partial(e_1)\right| = \left|\partial(e_2)\right| = 2$ を満たすとき，e_1 と e_2 は**並行している** (parallel) という．

例　グラフの例としては図 1.1 のようなものが挙げられる．e_2 と e_3 は並行しており，e_5 はループである．

定義 1.2.4 多重グラフ，単純グラフ

グラフ $G = (V, E; \partial)$ が $\forall e \in E.\ \left|\partial(e)\right| = 2$ を満たすとき，G を**多重グラフ** (multigraph) と呼ぶ．さらに，多重グラフ $G = (V, E; \partial)$ の ∂ が単射であるとき，G を**単純グラフ** (simple graph) と呼ぶ．

補足　要するに多重グラフとはループを持たないグラフ，単純グラフとはループを持たずどの 2 辺も並行しないグラフである．また，単純グラフでは ∂ の単射性より V の 2 元部分集合全体 $\binom{V}{2}$ を用いて $E \subseteq \binom{V}{2}$，$\partial = \mathrm{id}_E$ としてよい．こうすることで端点に u と v を持つ辺 e は $e = \{u, v\}$ と表せる．端点の順序は区別しないから，組 $(u, v) \in V \times V$ ではなく非順序対 $\{u, v\} \in \binom{V}{2}$ であることに注意されたい．勿論 $\binom{V}{2}$ から $V \times V$ への単射が存在するから $E \subseteq V \times V$ と“広めにとっておく”こともできるが，この場合 $u \neq v$ なる $u, v \in V$ に対して $(u, v) \in E$ ならば $(v, u) \notin E$ でなければならないから，扱いが煩雑になる．

定義 1.2.5 頂点の次数

グラフ $G = (V, E; \partial)$ に於いて，$v \in V$ に対して

$$\deg_G v \coloneqq \left|\left\{e \in E \;\middle|\; \left|\partial(e)\right| = 2 \ \wedge\ v \in \partial(e)\right\}\right| + 2 \cdot \left|\left\{e \in E \;\middle|\; \left|\partial(e)\right| = 1 \ \wedge\ v \in \partial(e)\right\}\right|$$

で定義される $\deg_G v$ を v の**次数** (degree) と呼ぶ．$\deg_G v = 0$ なる $v \in V$ は**孤立している** (isolated) という．また，グラフ $G = (V, E; \partial)$ が任意の $u, v \in V$ に対して $\deg_G u = \deg_G v$ を満たすとき，すなわちすべての頂点の次数が相等しいとき，G を**正則グラフ** (regular graph) と呼ぶ．

補足　特に $G = (V, E; \partial)$ が多重グラフのときはループがないので，$v \in V$ の次数は

$$\deg_G v = \left|\left\{e \in E \;\middle|\; v \in \partial(e)\right\}\right|$$

である．

例　図 1.1 の各頂点の次数は $\deg_G v_1 = 4$，$\deg_G v_2 = 3$，$\deg_G v_3 = 3$．

定義 1.2.6 完全グラフ

$|V| = n$ なる単純グラフ $G = (V, E; \partial)$ に対して $E \cong \binom{V}{2}$ であるとき，すなわち任意の 2 点に対してそれらを結ぶ辺がただ 1 つ存在するとき，G を**完全グラフ** (complete graph) と呼び，K_n と書く．

定義 1.2.7 安定性

単純グラフ $G = (V, E; \partial)$ に於いて $U \subseteq V$ が

$$\forall u \forall v \in U.\ \ \forall e \in E.\ \ \partial(e) \neq \{u, v\}$$

を満たすとき，すなわち U のどの 2 元も隣接しないとき，U を G の**安定集合** (stable set) と呼ぶ[*2]．

定義 1.2.8 二部グラフ

単純グラフ $G = (V, E; \partial)$ に対し，或る $V_1 \subseteq V$ が存在して V_1 と $V \setminus V_1$ が共に非空な安定集合であるとき，G を**二部グラフ** (bipartite graph) と呼ぶ．G が二部グラフで特に上のような V_1 を明示したいとき，$V_2 := V \setminus V_1$ として $G = \Delta(V_1, V_2; E; \partial)$，或いは ∂ を省略して $G = \Delta(V_1, V_2; E)$ と書く．

補足 二部グラフは，或る $V_1 \subseteq V$ が存在して任意の $e \in E$ に対して $\left|\partial(e) \cap V_1\right| = 1$ が成り立つような単純グラフでもある．上の定義との同値性は直感的にも明らかであり，こちらを定義としてもよい．

定義 1.2.9 完全二部グラフ

$|V_1| = n_1$，$|V_2| = n_2$ なる二部グラフ $G = \Delta(V_1, V_2; E; \partial)$ が任意の $v_1 \in V_1$ に対して $\deg_G v_1 = n_2$ かつ任意の $v_2 \in V_2$ に対して $\deg_G v_2 = n_1$ を満たすとき，G を**完全二部グラフ** (complete bipartite graph) と呼び，K_{n_1, n_2} と書く．

定義 1.2.10 道

グラフ $G = (V, E; \partial)$ と $n \in \mathbf{N}$ に対し，頂点の列と辺の列の組 $P = \left((v_i)_{i=0}^n, (e_i)_{i=1}^n\right) \in V^{n+1} \times E^n$ が

$$\forall i \in [\![n]\!].\ \ \partial(e_i) = \{v_{i-1}, v_i\}$$
$$\forall i \forall j \in [\![n]\!].\ (i \neq j\ \Rightarrow\ e_i \neq e_j)$$

を満たすとき，P を v_0 と v_n を**繋ぐ** (connect) **長さ** (length) n の**道** (path) と呼ぶ．また，このとき v_0 を P の**始点** (initial vertex)，v_n を P の**終点** (terminal ventex) と呼ぶ．

補足 定義より，道には同一の辺が複数回現れることはないが，頂点は重複してもよい．また，始点と終点は区別する．その他，特に $v \in V$ に対して v と v を繋ぐ長さ 0 の道 $\left((v), ()\right)$ も定義されていることに注意されたい．

定義 1.2.11 連結性，連結成分

グラフ $G = (V, E)$ に対し，V 上の二項関係 $\sim$ を，u と v を繋ぐ道が G に存在するときに $u \sim v$ が成り立つものと定義する．この $\sim$ は明らかに同値関係であり，V の $\sim$ による同値類の各元を G の**連結成分** (connected components) と呼ぶ．また，任意の $u, v \in V$ に対して $u \sim v$ が成り立つとき，G は**連結である** (connected) という．連結でないことは**非連結である** (disconnected) という．

[*2] 安定集合を独立集合と呼ぶこともあるが，これはマトロイドに関して使用する全く異なる用語と重複するので避ける．

定義 1.2.12 部分グラフ，全域部分グラフ，部分グラフの生成

グラフ $G = (V, E; \partial)$ と $V' \subseteq V$ と $E' \subseteq E$ に対して $G' = \left(V', E'; \partial|_{E'}\right)$ がグラフをなすとき，G' を G の**部分グラフ** (subgraph) と呼ぶ．∂ を意識しなくてよい場合は，単に (V', E') を G の部分グラフと呼ぶ．また，辺集合がもとのグラフ G の辺集合 V と一致する部分グラフを G の**全域部分グラフ** (spanning subgraph) と呼ぶ．さらに，辺部分集合 $E' \subseteq E$ に対して

$$\mathrm{V}(E') \coloneqq \left\{v \in V \;\middle|\; \exists e \in E'.\ \ v \in \partial(e)\right\}$$

で頂点部分集合が定義される部分グラフ $\left(\mathrm{V}(E'), E'\right)$ を，E' が**生成する** (generate) G の部分グラフと呼び，頂点部分集合 $V' \subseteq V$ に対して G から V' の元を端点にもつ辺を除いた，頂点集合を V' とする部分グラフを $G \setminus V'$ と書く．すなわち

$$G \setminus V' \coloneqq \left(V', \left\{e \in E \;\middle|\; \forall v \in V'.\ \ v \notin \partial(e)\right\}\right)$$

である．

定義 1.2.13 多重連結性，関節点

グラフ $G = (V, E)$ と $n \in \mathbf{N}^+$ に対し，任意の $|U| < n$ なる $U \subseteq V$ に対して $G \setminus U$ が連結であるとき，G は n-**連結** (-connected) であるという．また，連結なグラフ $G = (V, E)$ に対し，$v \in V$ が $G \setminus \{v\}$ を非連結にするとき，v を G の**関節点** (cut vertex) と呼ぶ．

定義 1.2.14 閉路

グラフ $G = (V, E; \partial)$ と $n \in \mathbf{N}^+$ に対し，$C = \left((v_i)_{i=0}^{n-1}, (e_i)_{i=0}^{n-1}\right) \in V^n \times E^n$ が

$$\begin{aligned}
\forall i \forall j \in [\![0, n-1]\!].\ &\left(i \neq j \ \Rightarrow\ v_i \neq v_j\right) \\
\forall i \forall j \in [\![0, n-1]\!].\ &\left(i \neq j \ \Rightarrow\ e_i \neq e_j\right) \\
\forall i \in [\![0, n-1]\!].\ \ &\partial(e_i) = \left\{v_i, v_{(i+1) \bmod n}\right\}
\end{aligned}$$

を満たすとき，C を G の**閉路** (cycle) と呼ぶ．或いは，C からつくられる G の部分グラフ $\left(\{v_i\}_{i=0}^{n-1}, \{e_i\}_{i=0}^{n-1}\right)$ も単に閉路と呼ぶ．

補足　道と異なり，閉路では辺だけでなく頂点も重複を許容しない．

定義 1.2.15 森，木，全域森，全域木

閉路を持たないグラフを**森** (forest) と呼び，特に連結な森を**木** (tree) と呼ぶ．また，グラフ G の全域部分グラフ T が森であるとき，T を G の**全域森** (spanning forest) と呼び，特に T が連結であるとき，T を G の**全域木** (spanning tree) と呼ぶ．

2 マトロイドの基礎

2.1 マトロイドに関する基礎的概念の定義

定義 2.1.1 マトロイド，独立性，従属性

有限集合 S と部分集合族 $\mathscr{I} \subseteq \mathfrak{P}S$ が

(I1) $\quad \varnothing \in \mathscr{I}$

(I2) $\quad \forall X \in \mathscr{I}.\ \forall Y \subseteq X.\ Y \in \mathscr{I}$

(I3) $\quad \forall U \forall V \in \mathscr{I}.\ \big(|U| = |V| + 1 \Rightarrow \exists x \in U \setminus V.\ V \cup \{x\} \in \mathscr{I}\big)$

を満たすとき，$M = \big(S, \mathscr{I}\big)$ を**マトロイド** (matroid) と呼ぶ．また，このとき $X \in \mathscr{I}$ なる $X \subseteq S$ は M に於いて**独立である** (independent) といい，$X \notin \mathscr{I}$ なる $X \subseteq S$ は M に於いて**従属である** (dependent) という．

定義 2.1.2 基，基族

マトロイド $M = \big(S, \mathscr{I}\big)$ に於いて独立な集合のうち，包含関係に関して極大であるものを M の**基** (base) と呼ぶ．また M の基全体からなる集合，すなわち

$$\begin{aligned}\mathscr{B}(M) &:= \max \mathscr{I} \\ &= \big\{B \in \mathscr{I} \,\big|\, \forall X \in \mathscr{I}.\ (X \supseteq B \Rightarrow X = B)\big\}\end{aligned}$$

で定義される $\mathscr{B}(M)$ を M の**基族** (base family) と呼ぶ．

定義 2.1.3 周，周族

マトロイド $M = \big(S, \mathscr{I}\big)$ に於いて従属な集合のうち，包含関係に関して極小であるものを M の**周** (circuit) と呼ぶ．また M の周全体からなる集合，すなわち

$$\begin{aligned}\mathscr{C}(M) &:= \min\big(\mathfrak{P}S \setminus \mathscr{I}\big) \\ &= \big\{C \in \mathfrak{P}S \setminus \mathscr{I} \,\big|\, \forall Y \in \mathfrak{P}S \setminus \mathscr{I}.\ (Y \subseteq C \Rightarrow Y = C)\big\}\end{aligned}$$

で定義される $\mathscr{C}(M)$ を M の**周族** (circuit family) と呼ぶ．

定義 2.1.4 階数函数

マトロイド $M = \big(S, \mathscr{I}\big)$ に対し，

$$\begin{array}{rccc} \rho\colon & \mathfrak{P}S & \longrightarrow & \mathbf{N} \\ & \cup & & \cup \\ & A & \longmapsto & \max\big\{|X| \,\big|\, X \subseteq A \ \wedge\ X \in \mathscr{I}\big\} \end{array}$$

を M の**階数函数** (rank function) と呼ぶ．また $A \subseteq S$ に対して $\rho(A)$ を M に於ける A の**階数** (rank) と呼ぶ．特に $\rho(S)$ は M の**階数** (rank) と呼び，しばしば $\rho(M)$ と書く．

補足　A に包まれる独立集合のうち最も大きいものの大きさを A の階数と定めている．また，いかなる $A \subseteq S$ に対しても $\varnothing \subseteq A$ かつ $\varnothing \in \mathscr{I}$ が成り立つので $0 = |\varnothing| \in \left\{ |X| \,\middle|\, X \subseteq A \ \wedge\ X \in \mathscr{I} \right\}$ であり，$\rho(A)$ が問題なく定義される．

定義 2.1.5 平坦性，部分空間

マトロイド $M = \big(S, \mathscr{I}\big)$ と $F \subseteq S$ が

$$\forall x \in S \setminus F.\ \ \rho\big(F \cup \{x\}\big) = \rho(F) + 1$$

を満たすとき，F は M に於いて**平坦である** (flat) という．或いは F を M の**部分空間** (subspace) と呼ぶ．また M に於いて平坦な集合全体を $\operatorname{Flat} M$ と書くことにする．すなわち

$$\operatorname{Flat} M \coloneqq \left\{ F \subseteq S \,\middle|\, \forall x \in S \setminus F.\ \ \rho\big(F \cup \{x\}\big) = \rho(F) + 1 \right\}$$

である．

補足　感覚的に言えば“外のどんな元を追加しても階数が 1 増えてしまうような集合”が平坦集合である．

定義 2.1.6 元の部分空間に対する従属性

マトロイド $M = \big(S, \mathscr{I}\big)$ と $A \subseteq S$，$x \in S$ が $\rho\big(A \cup \{x\}\big) = \rho(A)$ を満たすとき，x は A に**従属する** (depend) といい，$x \sim A$ と書く．

定義 2.1.7 閉包，閉包演算

マトロイド $M = \big(S, \mathscr{I}\big)$ に対して

$$\begin{array}{rccc} \sigma\colon & \mathfrak{P}S & \longrightarrow & \mathfrak{P}S \\ & \cup & & \cup \\ & A & \longmapsto & \{x \in S \mid x \sim A\} \end{array}$$

で定義される σ を，M に於ける **閉包演算子** (closure operator) と呼ぶ．また $A \subseteq S$ に対して $\sigma(A)$ を A の**閉包** (closure) と呼ぶ．

補足　以降，マトロイド $M = \big(S, \mathscr{I}\big)$ に M の基族 $\mathscr{B}$，階数函数 ρ，閉包演算子 σ，周族 $\mathscr{C}$ を加えた組をも単にマトロイドと呼び，$M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ と書いてよいことにする．

2.2 マトロイドの公理

前節で定義したマトロイドに関する基礎的概念である基族，階数函数，閉包演算子，周族それぞれに対して，公理のように扱われる定理を掲げる．これらの証明がひとまずの目標であり，以降の章で順次示していくことにする．

定理 2.2.1 基公理

S を有限集合とする．$\mathscr{B} \subseteq \mathfrak{P}S$ が或る S 上のマトロイドの基族であるための必要十分条件は

(B0) $\mathscr{B} \neq \varnothing$

(B1) $\forall B_1 \forall B_2 \in \mathscr{B}.\ \forall x \in B_1 \setminus B_2.\ \exists y \in B_2 \setminus B_1.\ \big(B_1 \cup \{y\}\big) \setminus \{x\} \in \mathscr{B}$

である．

定理 2.2.2 階数公理

S を有限集合とする．$\rho\colon\ \mathfrak{P}S \to \mathbf{N}$ が或る S 上のマトロイドの階数函数であるための必要十分条件は

(R1) $\rho(\varnothing) = 0$

(R2) $\forall X \subseteq S.\ \forall y \in S.\ \rho(X) \leq \rho\big(X \cup \{y\}\big) \leq \rho(X) + 1$

(R3) $\forall X \subseteq S.\ \forall y \forall z \in S.\ \Big(\rho\big(X \cup \{y\}\big) = \rho\big(X \cup \{z\}\big) = \rho(X)\ \Rightarrow\ \rho\big(X \cup \{y\} \cup \{z\}\big) = \rho(X)\Big)$

である．

定理 2.2.3 階数公理別版

S を有限集合とする．$\rho\colon\ \mathfrak{P}S \to \mathbf{N}$ が或る S 上のマトロイドの階数函数であるための必要十分条件は

(R1′) $\forall X \subseteq S.\ 0 \leq \rho(X) \leq |X|$

(R2′) $\forall X \forall Y \subseteq S.\ \big(X \subseteq Y\ \Rightarrow\ \rho(X) \leq \rho(Y)\big)$

(R3′) $\forall X \forall Y \subseteq S.\ \rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$

である．

定理 2.2.4 閉包公理

S を有限集合とする．$\sigma\colon\ \mathfrak{P}S \to \mathfrak{P}S$ が或る S 上のマトロイドの閉包演算子であるための必要十分条件は

(S1) $\forall X \subseteq S.\ X \subseteq \sigma(X)$

(S2) $\forall X \forall Y \subseteq S.\ \big(X \subseteq Y\ \Rightarrow\ \sigma(X) \subseteq \sigma(Y)\big)$

(S3) $\forall X \subseteq S.\ \sigma(X) = \sigma\big(\sigma(X)\big)$

(S4) $\forall X \subseteq S.\ \forall x \forall y \in S.\ \Big(\big(y \notin \sigma(X)\ \wedge\ y \in \sigma\big(X \cup \{x\}\big)\big)\ \Rightarrow\ x \in \sigma\big(X \cup \{y\}\big)\Big)$

である．

定理 2.2.5 周公理

S を有限集合とする．$\mathscr{C}$ が或る S 上のマトロイドの周族であるための必要十分条件は

(C1) $\quad \forall C_1 \forall C_2 \in \mathscr{C}.\, \big(C_1 \neq C_2 \;\Rightarrow\; C_1 \not\subseteq C_2\big)$

(C2) $\quad \forall C_1 \forall C_2 \in \mathscr{C}.\, \Big(C_1 \neq C_2 \;\Rightarrow\; \forall z \in C_1 \cap C_2.\;\; \exists C_3 \in \mathscr{C}.\;\; C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}\Big)$

である．

補足　まだ証明は与えていないが，これらが必要条件だけでなく十分条件でもあることは注目に値する．これらが成り立つことで，マトロイドは基族 $\mathscr{B}$，階数函数 ρ，閉包演算子 σ，周 $\mathscr{C}$ のうちどれかひとつからでも構成できるということがわかる．

2.3 様々なマトロイド

定義 2.3.1 同型

マトロイド $M_1 = (S_1, \mathscr{I}_1)$，$M_2 = (S_2, \mathscr{I}_2)$ に対し，

$$\exists \phi : S_1 \cong S_2.\, \Big(\forall X \subseteq S_1.\, \big(X \in \mathscr{I}_1 \;\Leftrightarrow\; \phi[X] \in \mathscr{I}_2\big) \;\wedge\; \forall Y \subseteq S_2.\, \big(\phi^{-1}[Y] \in \mathscr{I}_1 \;\Leftrightarrow\; Y \in \mathscr{I}_2\big)\Big)$$

が成り立つとき，M_1 と M_2 は**同型である** (isomorphic) といい，このときの全単射 ϕ を**同型写像** (isomorphism) と呼ぶ．

定義 2.3.2 自由マトロイド

有限集合 S に対して $\big(S, \mathfrak{P}S; \{S\}, |-|, \mathrm{id}_S, \varnothing\big)$ を**自由マトロイド** (free matroid) と呼ぶ．

定義 2.3.3 一様マトロイド

$n, k \in \mathbf{N}$ は $k \leq n$ を満たすとし，S を $|S| = n$ なる集合とする．

$$\begin{aligned}
\mathscr{I} &:= \big\{X \subseteq S \;\big|\; |X| \leq k\big\} \\
\mathscr{B} &= \big\{X \subseteq S \;\big|\; |X| = k\big\} \\
\mathscr{C} &= \big\{X \subseteq S \;\big|\; |X| = k+1\big\}
\end{aligned}$$

$$\begin{array}{ccc}
\rho\colon & \mathfrak{P}S & \longrightarrow \mathbf{N} \\
& \cup & \cup \\
& A & \longmapsto \begin{cases} |A| & \big(\text{if } |A| \leq k\big) \\ k & (\text{otherwise}) \end{cases}
\end{array}
\qquad
\begin{array}{ccc}
\sigma\colon & \mathfrak{P}S & \longrightarrow \mathfrak{P}S \\
& \cup & \cup \\
& A & \longmapsto \begin{cases} A & \big(\text{if } |A| < k\big) \\ S & (\text{otherwise}) \end{cases}
\end{array}$$

からなるマトロイド $U_{k,n} = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$，およびこれに同型なマトロイドを**一様マトロイド** (uniform matroid) と呼ぶ．

定理 2.3.4 ベクトル空間によるマトロイド

$(V,+,\cdot)$ を体 $(K,+,\cdot)$ 上のベクトル空間とし，$S \in \mathfrak{P}_\omega V$ とする．また S の部分集合のうち $(V,+,\cdot)$ 上線型独立であるもの全体を $\mathscr{I}$ とすると，$M=(S,\mathscr{I})$ はマトロイドである．

証明　$\mathscr{I}$ が (I1)，(I2) を満たすことは明らかなので，以降 (I3) について背理法で示す．線型独立な集合 X と Y が $|X|=|Y|+1$ を満たすとすると，$X\setminus Y\neq\varnothing$ である．いま仮に任意の $x\in X\setminus Y$ に対して $Y\cup\{x\}$ が線型従属であるとすると，Y は線型独立であるから $X\cup Y$ が生成する部分空間 W の基底集合である．このとき，$X\subseteq W$ も線形独立であり，$X\subseteq E$ なる基底集合 E が存在する．この E は $|E|\geq|X|>|Y|$ を満たすが，同一の部分空間の基底集合がすべて大きさが相等しいことによる $|Y|=|E|$ と矛盾．したがって或る $x\in X\setminus Y$ が存在して $Y\cup\{x\}$ は線型独立である．■

定義 2.3.5 ベクトル的マトロイド

ベクトル空間 $(V,+,\cdot)$ から定理 2.3.4 のようにして得られるマトロイド $M=(S,\mathscr{I})$，およびこれに同型なマトロイドを**ベクトル的マトロイド** (vectorial matroid) と呼ぶ．

補足　ベクトル空間 $(V,+,\cdot)$ によるベクトル的マトロイド $M=(S,\mathscr{I})$ に於いて，基族 $\mathscr{B}$ は S が生成する部分空間の基底集合で S に包まれるもの全体，$X\subseteq S$ の階数は X の張る空間の次元，すなわち $\rho(X)=\dim X$ である．また M の平坦集合はベクトル空間 $(V,+,\cdot)$ の部分空間であり，X の閉包は X の元の線型結合で表せるもの全体，すなわち X が生成する部分空間である．「平坦集合」という名前は，$\dim V=3$ のベクトル空間 $(V,+,\cdot)$ によるベクトル的マトロイド $(S,\mathscr{I})$ で $\rho(F)=\dim F=2$ なる平坦集合 F は，その元がひとつの平面上に乗っており，また $S\setminus F$ の元を追加するとその平面性が損なわれる，という具体的イメージを反映したものである．平坦集合を部分空間と呼ぶことがあるのも，やはりこのベクトル空間からのアナロジーである．

定理 2.3.6 無向グラフによるマトロイド

無向グラフ $G=(V,E)$ に対し，$S:=E$，また G の閉路を持たない E の部分集合全体を $\mathscr{I}$ とすると，$(S,\mathscr{I})$ はマトロイドをなす．

証明　(I1)，(I2) は明らかであるから，(I3) を示す．閉路を持たない辺集合 X と Y が $|X|=|Y|+1$ を満たすとする．このとき，$X\setminus Y\neq\varnothing$ である．いま仮に任意の $e\in X\setminus Y$ に対して $Y\cup\{e\}$ が閉路を持つとすると，Y は $X\cup Y$ が生成する G の部分グラフの全域森である．一方で X も閉路を持たないから $X\cup Y$ が生成する G の部分グラフの部分森であるが，この部分森は $|X|>|Y|$ より全域森よりも大きく，矛盾．ゆえに，或る $e\in X\setminus Y$ が存在して $Y\cup\{e\}$ は閉路を持たない．■

定義 2.3.7 閉路マトロイド

無向グラフ $G=(V,E)$ に対し，定理 2.3.6 により得られる $M=(E,\mathscr{I})$ を G の**閉路マトロイド** (cycle matroid) と呼ぶ．

補足　結局，閉路マトロイドでの独立集合とは G の部分森をなす辺集合である．したがって基とは G の全域森をなす辺集合である[*3]．さらに周とは G の閉路をなす辺集合であり，「周」(“circuit”) という名称も，この閉路からのアナロジーである．

例　K_3 の閉路マトロイドは $E \coloneqq \{e_1, e_2, e_3\}$，$\mathscr{I} \coloneqq \big\{\{\}, \{e_1\}, \{e_2\}, \{e_3\}, \{e_1, e_2\}, \{e_2, e_3\}, \{e_3, e_1\}\big\}$ なる $\big(E, \mathscr{I}\big)$ で，これは一様マトロイド $U_{2,3}$ に等しい．

定義 2.3.8 代数独立性

$\big(F, +, \cdot\big)$ を体とする．$\big(F, +, \cdot\big)$ の拡大体 $\big(K, +, \cdot\big)$ および $\{x_1, \ldots, x_k\} \subseteq K$ に対し，F の元を係数とする或る多項式 f が存在して $f(x_1, \ldots, x_k) = 0$ を満たすとき，$\{x_1, \ldots, x_k\}$ は $\big(F, +, \cdot\big)$ 上**代数独立である** (algebraically independent) という．

定義 2.3.9 アフィン従属性

$\{x_1, \ldots, x_r\} \in \mathfrak{P}_\omega \mathbf{R}^d$ に対し，$x \in \mathbf{R}^d$ が

$$\exists (\lambda_i)_{i=1}^r \in \mathbf{R}^r.\ \ x = \sum_{i=1}^r \lambda_i x_i$$

を満たすとき，x は $\{x_1, \ldots, x_r\}$ に**アフィン従属する** (affinely depend) という．また，$X \subseteq \mathbf{R}^d$ の任意の元 x が $X \setminus \{x\}$ にアフィン従属しないとき，X は**アフィン独立である** (affinely independent) という．

定理 2.3.10

体 $\big(F, +, \cdot\big)$ と $\big(F, +, \cdot\big)$ の拡大体 $\big(K, +, \cdot\big)$ に対して $S \in \mathfrak{P}_\omega K$ とし，$\big(F, +, \cdot\big)$ 上代数独立な S の部分集合全体を $\mathscr{I}$ とおくと，$\big(S, \mathscr{I}\big)$ はマトロイドをなす．

定義 2.3.11 可換群に於ける独立性，従属性

$\big(J, +\big)$ を，単位元 0_J を除くすべての元が位数 0 である可換群とする．$\{x_1, \ldots, x_n\} \subseteq J$ と $g \in J$ に対し，

$$\exists m \in \mathbf{Z} \setminus \{0\}.\ \ \exists (k_i)_{i=1}^n \in \mathbf{Z}^n.\ \ mg = k_1 x_1 + \cdots + k_n x_n$$

が成り立つとき，g は $\{x_1, \ldots, x_n\}$ に**従属する** (depend) という．また，$Y \subseteq J$ の任意の元 y が $Y \setminus \{y\}$ に従属しないとき，Y は**独立である** (independent) という．このとき，有限部分集合 $S \subseteq J$ に対し，S の部分集合で独立なもの全体を $\mathscr{I}$ とおくと，$M = \big(S, \mathscr{I}\big)$ はマトロイドをなす．

2.4 ループと並行

最初に独立集合族，基族，階数函数，閉包演算子，周についての扱いに慣れる意図も込めて，ループと並行という概念について触れておく．

[*3] ただし，基 $B \subseteq E$ に対して或る G の全域森が存在してその辺集合が B と一致することは言えるが，B が全域森を生成するとは限らない．G が次数 0 の頂点を持つかもしれないからである．

定義 2.4.1 ループ，並行

マトロイド $M = \big(S, \mathscr{I}\big)$ に対し，$x \in S$ が $\{x\} \notin \mathscr{I}$ を満たす，すなわち $\{x\}$ が従属であるとき，x を M のループ (loop) と呼び，$\circlearrowleft_M x$ と書くことにする．また $x, y \in S$ が $\{x\} \in \mathscr{I}$ かつ $\big\{y\big\} \in \mathscr{I}$ かつ $\big\{x, y\big\} \notin \mathscr{I}$ を満たすとき，x と y は M に於いて並行している (parallel) といい，$x \underset{M}{\parallel} y$ と書くことにする．

閉路マトロイドでは，ループはもとのグラフでのループ，並行性はもとのグラフでの並行性に相当し，マトロイドに於けるループと並行性の名前はこれに基づいている．$\big(K, +, \cdot\big)$ 上ベクトル空間 $\big(V, +, \cdot\big)$ からつくられるベクトル的マトロイド $\big(S, \mathscr{I}\big)$ は，V の零元を $\mathbf{0}$ として，$0 \in S$ のとき S のループは $\mathbf{0}$ のみであり，$\mathbf{0} \notin S$ のとき S はループをもたない．$\boldsymbol{x}, \boldsymbol{y} \in S$ が並行するとは，$\boldsymbol{y} = a\boldsymbol{x}$ なる $a \in K \setminus \{0\}$ が存在することに相当する．

補題 2.4.2 従属集合を包む集合の従属性

マトロイド $M = \big(S, \mathscr{I}\big)$ に対し，

$$\forall X \forall Y \subseteq S. \Big(\big(X \notin \mathscr{I} \ \wedge \ X \subseteq Y\big) \Rightarrow \ Y \notin \mathscr{I}\Big)$$

が成り立つ．すなわち，従属集合を包む任意の集合は従属集合である．

証明　従属集合 $X \in \mathfrak{P}S \setminus \mathscr{I}$ に対し，$Y \subseteq S$ が $X \subseteq Y$ を満たすとする．いま仮に $Y \in \mathscr{I}$ とすると，$X \subseteq Y$ と (I2) より $X \in \mathscr{I}$ が成り立ち矛盾．ゆえに $Y \in \mathfrak{P}S \setminus \mathscr{I}$，すなわち Y は従属集合．　■

定理 2.4.3 ループに関する簡単な定理

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，以下がそれぞれ成り立つ．

(1) ループであることと 1 元集合の階数が 0 であることは同値：　$\forall x \in S. \Big(\circlearrowleft_M x \ \Leftrightarrow \ \rho\big(\{x\}\big) = 0\Big)$

(2) ループであることと空集合の閉包に含まれることは同値：　$\forall x \in S. \Big(\circlearrowleft_M x \ \Leftrightarrow \ x \in \sigma(\varnothing)\Big)$

(3) ループを含む集合は従属：　$\forall A \subseteq S. \Big(\big(\exists x \in A. \ \ \circlearrowleft_M x\big) \Rightarrow \ A \notin \mathscr{I}\Big)$

(4) 任意の集合の閉包は任意のループを含む：　$\forall x \in S. \Big(\circlearrowleft_M x \ \Rightarrow \ \forall A \subseteq S. \ \ x \in \sigma(A)\Big)$

(5) ループであることと 1 元集合が周であることは同値：　$\forall x \in S. \Big(\circlearrowleft_M x \ \Leftrightarrow \ \{x\} \in \mathscr{C}\Big)$

(6) ループであることとどの基にも含まれないことは同値：　$\forall x \in S. \Big(\circlearrowleft_M x \ \Leftrightarrow \ \forall B \in \mathscr{B}. \ \ x \notin B\Big)$

証明

[(1)]　$x \in S$ に対して $\circlearrowleft_M x$ すなわち $\{x\} \notin \mathscr{I}$ と仮定すると，(I1) より $\{x\}$ に包まれる独立集合は $\varnothing$ のみであるから，$\rho\big(\{x\}\big) = \max\Big\{|X| \ \Big| \ X \subseteq \{x\} \ \wedge \ X \in \mathscr{I}\Big\} = |\varnothing| = 0$ である．逆に $x \in S$ が $\rho\big(\{x\}\big) = 0$ を満たすとする．仮に $\{x\} \in \mathscr{I}$ ならば $\rho(x) \geq \big|\{x\}\big| = 1$ であるから矛盾し，したがって $\{x\} \notin \mathscr{I}$，すなわ

ち $\circlearrowleft_M x$ である．■

[(2)]　$\circlearrowleft_M x$ と仮定すると，(1) より $\rho\big(\{x\}\big) = 0$ であるから $\rho\big(\varnothing \cup \{x\}\big) = \rho\big(\{x\}\big) = 0 = \rho(\varnothing)$．ゆえに $x \sim \varnothing$，すなわち $x \in \sigma(\varnothing)$．逆に $x \in \sigma(\varnothing)$ とすると $x \sim \varnothing$ であるから $\rho\big(\{x\}\big) = \rho\big(\varnothing \cup \{x\}\big) = \rho(\varnothing) = 0$ が成り立ち，やはり (1) より $\circlearrowleft_M x$．■

[(3)]　$A \subseteq S$ とする．$\circlearrowleft_M x$ なる $x \in A$ が存在するとき，この x は $\{x\} \notin \mathscr{I}$ を満たすから，補題 2.4.2 より $A \notin \mathscr{I}$．■

[(4)]　$\circlearrowleft_M x$ なる $x \in S$ および $A \subseteq S$ に対して，ρ の定義より $|X| = \rho\big(A \cup \{x\}\big)$ かつ $X \subseteq A \cup \{x\}$ なる $X \in \mathscr{I}$ が存在する．仮にこの X が $x \in X$ を満たすとすると $\{x\} \subseteq X$ と (I2) より $\{x\} \in \mathscr{I}$ が成り立ち矛盾するから，$x \notin X$ である．したがって $X \subseteq A$ であり，$|X| \leq \rho(A)$．ここで仮に $|X| < \rho(A)$ が成り立つとすると，或る $Y \in \mathscr{I}$ が存在して $|X| < |Y|$ かつ $Y \subseteq A$ であるが，この Y は $Y \subseteq A \cup \{x\}$ を満たすから $|Y| \leq \rho\big(A \cup \{x\}\big) = |X|$ が成り立ち矛盾．ゆえに $\rho\big(A \cup \{x\}\big) = |X| = \rho(A)$ すなわち $x \sim A$ であり，$x \in \sigma(A)$．■

[(5)]　(I1) : $\varnothing \in \mathscr{I}$ と周族の定義 $\mathscr{C} := \mathrm{minl}\,\big(\mathfrak{P}S \setminus \mathscr{I}\big)$ より明らか．■

[(6)]　いま仮に或る $x \in S$ と $B \in \mathscr{B}$ が存在して $\circlearrowleft_M x$ かつ $x \in B$ を満たすとすると，$\{x\} \subseteq B$ と (I2) より $\{x\} \in \mathscr{I}$ となり矛盾．よって $\circlearrowleft_M x$ なる $x \in S$ に対しては任意の $B \in \mathscr{B}$ が $x \notin B$ を満たす．一方，$x \in S$ に対して $\neg\big(\circlearrowleft_M x\big)$ とすると $\{x\} \in \mathscr{I}$ であるから，基の極大性より $\{x\} \subseteq B$ なる $B \in \mathscr{B}$ が存在する．これの対偶をとって，$x \in S$ に対して任意の $B \in \mathscr{B}$ が $x \notin B$ を満たすならば $\circlearrowleft_M x$ である．■

定理 2.4.4　並行に関する簡単な定理

マトロイド $M = \big(S, \mathscr{I}, \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，以下がそれぞれ成り立つ．

(1) 相異なる 2 元が並行であることとその 2 元からなる集合が周であることは同値：

$$\forall x \forall y \in S.\ \Big(x \underset{M}{\parallel} y \ \Leftrightarrow\ \big\{x, y\big\} \in \mathscr{C}\Big)$$

(2) 並行性は“非反射的な推移律”を満たす：

$$\forall x \forall y \forall z \in S.\ \Big(\big(x \underset{M}{\parallel} y \ \wedge\ y \underset{M}{\parallel} z \ \wedge\ x \neq z\big) \Rightarrow\ x \underset{M}{\parallel} z\Big)$$

(3)

$$\forall x \forall y \in S.\ \Big(x \neq y \ \Rightarrow\ \Big(x \underset{M}{\parallel} y \ \Leftrightarrow\ x \in \sigma\big(\{y\}\big) \ \wedge\ y \in \sigma\big(\{x\}\big) \ \wedge\ \neg\big(\circlearrowleft_M x\big) \ \wedge\ \neg\big(\circlearrowleft_M y\big)\Big)\Big)$$

証明

[(1)]　周の極小性より明らか．■

[(2)]　$x \underset{M}{\parallel} y$ かつ $y \underset{M}{\parallel} z$ かつ $x \neq z$ とすると，$\{x\} \in \mathscr{I}$，$\{y\} \in \mathscr{I}$，$\{z\} \in \mathscr{I}$．ここで仮に $\{x,z\} \in \mathscr{I}$ であるとすると，$x \neq z$ より $\big|\{x,z\}\big| = \big|\{y\}\big| + 1$ が成り立つから，(I3) より $\{x,y\} \in \mathscr{I}$ または $\{x,z\} \in \mathscr{I}$ が成り立つが，これは仮定に矛盾．ゆえに $\{x,z\} \notin \mathscr{I}$ であり，結局 $x \underset{M}{\parallel} z$ が成り立つ．　■

[(3)]　$\{x\} \in \mathscr{I}$ かつ $\{y\} \in \mathscr{I}$ かつ $x \neq y$ なる $x, y \in S$ に対して，$\{x,y\} \notin \mathscr{I}$ と $x \in \sigma\big(\{y\}\big)$ かつ $y \in \sigma\big(\{x\}\big)$ が同値であることを示せばよい．まず $\{x,y\} \notin \mathscr{I}$ とすると，$\{x\} \in \mathscr{I}$ かつ $\{y\} \in \mathscr{I}$ より $\rho\big(\{x,y\}\big) = \big|\{x\}\big| = \big|\{y\}\big|$ であり，また $\rho\big(\{x\}\big) = \big|\{x\}\big|$，$\rho\big(\{y\}\big) = \big|\{y\}\big|$ であるから，$\rho\big(\{x\} \cup \{y\}\big) = \rho\big(\{x,y\}\big) = \rho\big(\{x\}\big)$ すなわち $x \sim \{y\}$ が成り立ち，$x \in \sigma\big(\{y\}\big)$．$y \in \sigma\big(\{x\}\big)$ も同様．逆に $x \in \sigma\big(\{y\}\big)$ かつ $y \in \sigma\big(\{x\}\big)$ とすると $x \sim \{y\}$ であるから $\rho\big(\{x,y\}\big) = \rho\big(\{y\}\big) = \big|\{y\}\big| = 1$．このとき仮に $\{x,y\} \in \mathscr{I}$ とすると $1 = \rho\big(\{x,y\}\big) \geq \big|\{x,y\}\big| = 2$ より矛盾するから，$\{x,y\} \notin \mathscr{I}$ が成り立つ．　■

2.5 独立集合と基に関する性質

これまでは“代数系らしい姿”のマトロイドを見てきたが，ここでイメージを掴むためにマトロイドを具体的に描いてみよう．マトロイド $M = (S, \mathscr{I})$ に対し，半順序系 $(\mathfrak{P}S, \subseteq)$ の Hasse 図を描き，独立か従属かによって S の各部分集合に相当する各点を塗り分けることを考える．簡単な例として，ここでは $|S| = 3$ なる S に対してマトロイドを描くことにしよう．S の各元を a，b，c と表すと，$(\mathfrak{P}S, \subseteq)$ の Hasse 図は図 2.1(a) のようになる．大きさの相等しい S の部分集合は横一列に並んでいることに注目してほしい．これを図 2.1(b) のように個々の要素を無視して構造のみ描くことにする．

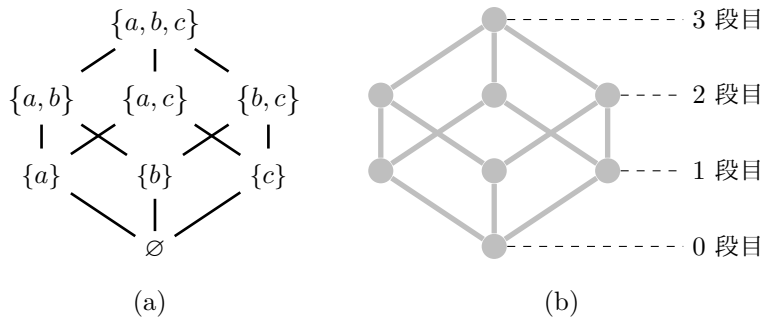


図 2.1　冪集合の包含関係を半順序とする Hasse 図

独立集合に対応する点を黒色，従属集合に対応する点を灰色で塗ることにしよう．ここで独立集合の公理を思い返すと

(I1)　$\varnothing \in \mathscr{I}$

(I2)　$\forall X \in \mathscr{I}.\ \forall Y \subseteq X.\ Y \in \mathscr{I}$

(I3)　$\forall U \forall V \in \mathscr{I}.\ \big(|U| = |V| + 1 \ \Rightarrow\ \exists x \in U \setminus V.\ V \cup \{x\} \in \mathscr{I}\big)$

であった．最下点を「0 段目」とし，また下に降りて辿り着ける点を「下位」，上に登って辿り着ける点を「上位」と表現することにして，各公理を“Hasse 図でのことば”に直すと，

- (I1)：　最下点は黒色

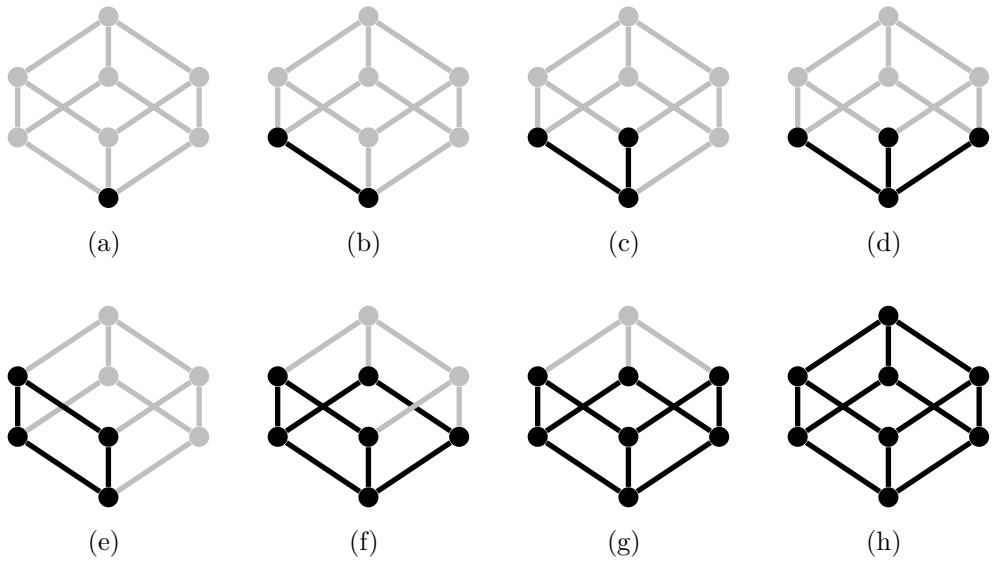


図 2.2　Hasse 図で表現された大きさ 3 の集合上のマトロイド

- (I2)：　黒色の点の子孫はすべて黒色
- (I3)：　黒色の点 V と V より 1 段高い位置の黒色の点 U に対して，V から 1 段上位の或る黒色の点 W があり，U と W から共通に下位だが V の下位ではない点が 1 段目にある

となる．これに基づけば，大きさ 3 の集合上のマトロイドは，同型を除いて図 2.2 の 8 種類である．

図 2.2(a) は一様マトロイド $U_{3,0}$，図 2.2(d) は $U_{3,1}$，図 2.2(g) は $U_{3,2}$，図 2.2(h) は $U_{3,3}$ であり自由マトロイドである．

ところで独立集合族の公理のうち (I3) だけは他に比べて複雑で直感的に捉えにくいが，$|U| = |V| + 1$ なる U，V，すなわち大きさが 1 異なる独立集合の組に限らず，$|X| < |Y|$ なる X，Y，すなわち単に大きさが異なる独立集合の組にまで“(I3) のような公理”を一般化することができる．これが次に述べる**増強定理** (augmentation theorem) である．

定理 2.5.1 増強定理

マトロイド $M = (S, \mathscr{I})$ に対し，

$$\forall X \forall Y \in \mathscr{I}.\ \Big(|X| < |Y| \ \Rightarrow\ \exists Z \subseteq Y \setminus X.\ \big(X \cup Z \in \mathscr{I} \ \wedge\ |X \cup Z| = |Y|\big)\Big)$$

が成り立つ．

証明　$|X| < |Y|$ なる $X, Y \in \mathscr{I}$ を考える．$X \cup Z \in \mathscr{I}$ なる $Z \subseteq Y \setminus X$ のうち，$|X \cup Z|$ を最大化する Z

を Z_0 とおく．いま $|X \cup Z_0| < |Y|$ であると仮定すると，(I2) より $Y_0 \in \mathscr{I}$ かつ $|Y_0| = |X \cup Z_0| + 1$ なる $Y_0 \subseteq Y$ が存在する．この Y_0 をとると (I3) より $(X \cup Z_0) \cup \{y\} \in \mathscr{I}$ なる $y \in Y_0 \setminus (X \cup Z_0)$ が存在するが，この y は $\left|X \cup \left(Z_0 \cup \{y\}\right)\right| > |X \cup Z_0|$ を満たすから，Z_0 のとり方に反する．よって $|X \cup Z_0| \geq |Y|$ である．$X \cup Z_0 \subseteq Y$ より $|X \cup Z_0| \leq |Y|$ であるから，結局 $|X \cup Z_0| = |Y|$ が成り立つ． ■

補足　増強定理から (I3) が得られるのは明らかであり，結局 (I3) と増強定理は同値ということになる．

先ほど大きさ 3 の台集合を持つマトロイドを考えて図 2.2 を描いたとき，Hasse 図の上で「頂上の黒い点がどれも同じ高さになる」ことが (I3) から要請されるのを感じただろうか．「頂上の黒い点」とは極大な独立集合すなわち基に相当する点であるから，「頂上の黒い点がどれも同じ高さになる」ということは，“普通のマトロイドでのことば”に直せば基の大きさはどれも相等しいということになる．実際，それは次に示すように増強定理の系として証明できる．

系 2.5.2

マトロイド M の基はどれも相等しい大きさを持ち，その大きさは M の階数である．

証明　$M = (S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C})$ とおく．いま仮に或る $B_1, B_2 \in \mathscr{B}$ に対して $|B_1| \neq |B_2|$ とする．$|B_1| < |B_2|$ として一般性を失わないのでこう定める．このとき，定理 2.5.1 : 増強定理より $|B_1 \cup Z| = |B_2|$ かつ $B_1 \cup Z \in \mathscr{I}$ なる $Z \subseteq B_2 \setminus B_1$ が存在する．この Z に対して基 $B_1 \cup Z$ は $B_1 \cup Z \supsetneq B_1$ を満たし，基 B_1 の極大性に反する．よって $\forall B_1 \forall B_2 \in \mathscr{B}.\ |B_1| = |B_2|$ である．また，階数函数 ρ の定義および基族の定義 $\mathscr{B} := \mathrm{maxl}\,\mathscr{I}$ より

$$\begin{aligned}\rho(M) &= \rho(S)\\ &= \max\left\{|X| \;\middle|\; X \subseteq S \ \wedge\ X \in \mathscr{I}\right\}\\ &= \max\left\{|X| \;\middle|\; X \in \mathscr{B}\right\}\end{aligned}$$

であるから，結局 $\forall B \in \mathscr{B}.\ \rho(M) = |B|$ である． ■

ただし，注意としては「頂上の高さが揃っている」だけでは (I3) が成り立つとは限らない．例えば $|S| = 4$ に対する集合族の Hasse 図として図 2.3 がある．これは「頂上の高さが揃っている」が，図中のように U と V をとると (I3) を満たすような黒色の点 $W = V \cup \{x\}$ が存在しないので，マトロイドではない．

さて，あらかじめ掲げておいた基公理の [⇐] を示す準備をしておこう．したがって以下の各補題で扱う $\mathscr{B}$ はマトロイドの基族ではなく，単なる集合族であることに注意されたい．

まずは (B1) の“入れ替え”を“1 ステップから多ステップ”に拡張してみる．

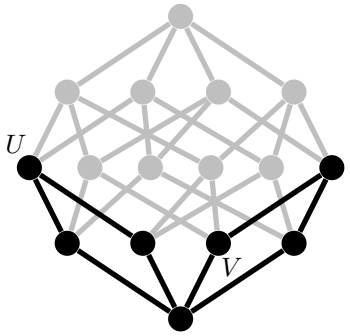


図 2.3　「頂上の高さが揃っている」がマトロイドではない集合族

補題 2.5.3 (B1) の拡張

有限集合 S と集合族 $\mathscr{B} \subseteq \mathfrak{P}S$ が (B1) を満たすならば，

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \ \forall X \subseteq B_1 \setminus B_2.\ \ \exists Y \subseteq B_2 \setminus B_1.\ \Big(|Y| = |X| \ \wedge\ \big(B_1 \setminus X\big) \cup Y \in \mathscr{B}\Big)$$

が成り立つ．

証明　$B_1, B_2 \in \mathscr{B}$ を任意にとり，$X \subseteq B_1 \setminus B_2$ とする．X の大きさ $|X|$ に関する帰納法により示す．

- $|X| = 0$ のとき，$X = \varnothing$ であり $Y = \varnothing$ が満たすので明らか．
- $|X| \geq 1$ のとき，$x \in X$ がとれる．$\big|X \setminus \{x\}\big| < |X|$ であるから，帰納法の仮定より或る $Y' \subseteq B_2 \setminus B_1$ が存在して $|Y'| = \big|X \setminus \{x\}\big|$ かつ $\Big(B_1 \setminus \big(X \setminus \{x\}\big)\Big) \cup Y' \in \mathscr{B}$ が成り立つ．この Y' を用いて $B_3 \coloneqq \Big(B_1 \setminus \big(X \setminus \{x\}\big)\Big) \cup Y'$ とすると，$x \in B_3 \setminus B_2$ であるから，(B1) より或る $y \in B_2 \setminus B_3$ が存在して $\big(B_3 \setminus \{x\}\big) \cup \{y\} \in \mathscr{B}$ を満たす．ここで $Y \coloneqq Y' \cup \{y\}$ とすると，$Y' \subseteq B_2 \setminus B_1$ と $y \in B_2 \setminus B_3 \subseteq B_2 \setminus B_1$ より $Y \subseteq B_2 \setminus B_1$ である．また

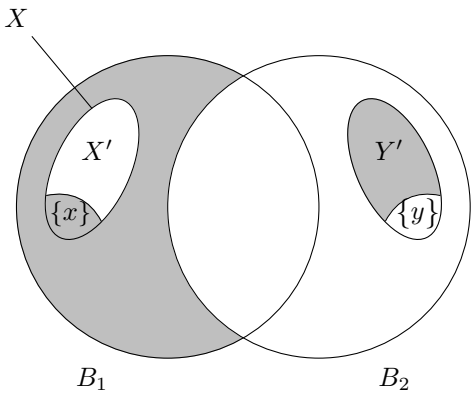
  $$\big(B_3 \setminus \{x\}\big) \cup \{y\} = \Big(\big(B_1 \setminus X\big) \cup Y'\Big) \cup \{y\} = \big(B_1 \setminus X\big) \cup Y$$

  より $\big(B_1 \setminus X\big) \cup Y \in \mathscr{B}$ が成り立ち，さらに

  $$\begin{aligned} |Y| &= \big|Y' \cup \{y\}\big| \\ &= |Y'| + 1 \\ &= \big|X \setminus \{x\}\big| + 1 \\ &= |X| - 1 + 1 = |X| \end{aligned}$$

  より $|Y| = |X|$ である．ゆえに，或る $Y \subseteq B_2 \setminus B_1$ が存在して $|Y| = |X|$ かつ $\big(B_1 \setminus X\big) \cup Y \in \mathscr{B}$ を満たす．

以上より示された．　■



灰色部分が B_3 である．

上で示した (B1) の拡張は，さらにもう少し便利に拡張できる．

補題 2.5.4 (B1) の拡張 2

有限集合 S と集合族 $\mathscr{B} \subseteq \mathfrak{P}S$ が (B1) を満たすならば，

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \forall X \subseteq B_1.\ \exists Y \subseteq B_2.\ \Big(|Y| = |X| \ \wedge\ \big(B_1 \setminus X\big) \cup Y \in \mathscr{B} \\ \wedge\ X \cap B_1 \cap B_2 = Y \cap B_1 \cap B_2\Big)$$

が成り立つ．

証明　$B_1, B_2 \in \mathscr{B}$ を任意にとり，$X \subseteq B_1$ とする．$Z \coloneqq X \cap (B_1 \cap B_2)$，$X' \coloneqq \cap\big(B_1 \setminus B_2\big)$ とおくと，$Z \cup X' = X$，$Z \cap X' = \varnothing$ である．このとき，$X' \subseteq B_1 \setminus B_2$ であるから，補題 2.5.3 より或る $Y' \subseteq B_2 \setminus B_1$ が存在して $|Y'| = |X'|$ かつ $\big(B_1 \setminus X'\big) \cup Y' \in \mathscr{B}$ を満たす．この Y' を用いて $Y \coloneqq Y' \cup Z$ とすると，$Y' \subseteq B_2 \setminus B_1$，$Z \subseteq B_1 \cap B_2$ より $Y \subseteq B_2$．また，$X' \cap Z = \varnothing$，$Y' \cap Z = \varnothing$，$X' \cap Y' = \varnothing$ より

$$\begin{aligned}\big(B_1 \setminus X\big) \cup Y &= \big(B_1 \setminus (X' \cup Z)\big) \cup (Y' \cup Z) \\ &= \big(B_1 \setminus X'\big) \cup Y'\end{aligned}$$

より，$\big(B_1 \setminus X\big) \cup Y \in \mathscr{B}$．さらに

$$\begin{aligned}|Y| &= |Y'| + |Z| \\ &= |X'| + |Z| = |X|\end{aligned}$$

より $|Y| = |X|$ である．ゆえに，$|Y| = |X|$ かつ $\big(B_1 \setminus X\big) \cup Y \in \mathscr{B}$ なる $Y \subseteq B_2$ が存在する．　■

補題 2.5.5

有限集合 S と集合族 $\mathscr{B} \subseteq \mathfrak{P}S$ が (B1) を満たすならば，

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \big(B_1 \neq B_2 \ \Rightarrow\ B_1 \not\subseteq B_2\big)$$

が成り立つ．すなわち，$\mathscr{B}$ のどの 2 元も一方が他方を真に包むことはない．

証明　今仮に或る B_1, B_2 が $B_1 \subsetneq B_2$ を満たすとすると，$x \in B_2 \setminus B_1$ がとれるので，(B1) より或る $y \in B_1 \setminus B_2$ が存在して $\big(B_2 \setminus \{x\}\big) \cup \{y\} \in \mathscr{B}$ が成り立つが，$B_1 \setminus B_2 = \varnothing$ より矛盾である．　■

補題 2.5.6

有限集合 S と集合族 $\mathscr{B} \subseteq \mathfrak{P}S$ が (B1) を満たすならば，

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \ |B_1| = |B_2|$$

が成り立つ．すなわち $\mathscr{B}$ の元はすべて大きさが相等しい．

証明　今仮に或る $B_1, B_2 \in \mathscr{B}$ が存在して $|B_1| > |B_2|$ を満たしたとする．このとき，$B_1 \subseteq B_1$ と補題 2.5.4 より，或る $Y \subseteq B_2$ が存在して $|Y| = |B_1|$ かつ $\big(B_2 \setminus B_1\big) \cup Y \in \mathscr{B}$ を満たすが，この Y をとると $Y \subseteq B_2$ より

$$|B_1| = |Y| \leq |B_2| < |B_1|$$

が成り立ち矛盾．したがって $|B_1| > |B_2|$ なる $B_1, B_2 \in \mathscr{B}$ は存在せず，$B_1, B_2 \in \mathscr{B}$ に対して $|B_1| \leq |B_2|$．同時に $|B_1| \geq |B_2|$ でもあるから，結局 $|B_1| = |B_2|$ が成り立つ．　■

定理 再掲：基公理

S を有限集合とする．$\mathscr{B} \subseteq \mathfrak{P}S$ が或る S 上のマトロイドの基族であるための必要十分条件は

(B0)　$\mathscr{B} \neq \varnothing$

(B1)　$\forall B_1 \forall B_2 \in \mathscr{B}.\ \forall x \in B_1 \setminus B_2.\ \exists y \in B_2 \setminus B_1.\ \big(B_1 \cup \{y\}\big) \setminus \{x\} \in \mathscr{B}$

である．

証明

[⇒]　マトロイド $M = \big(S, \mathscr{I}\big)$ に対し，M の基族 $\mathscr{B}$ が (B0) および (B1) を満たすことを示す．まず (I1) より $\varnothing \in \mathscr{I}$ であるから，$\mathscr{B} := \operatorname{maxl} \mathscr{I} \neq \varnothing$ すなわち (B0) が成り立つ．

また $B_1, B_2 \in \mathscr{B}$ とし，$x \in B_2 \setminus B_1$ をとると，系 2.5.2 より $|B_1| = |B_2|$．したがって $\big|B_1 \setminus \{x\}\big| + 1 = |B_1| = |B_2|$ であり，(I3) を（$U := B_2$，$V := B_1 \setminus \{x\}$ として）適用すると，或る $y \in B_2 \setminus \big(B_1 \setminus \{x\}\big)$ が存

在して $\big(B_1 \setminus \{x\}\big) \cup \{y\} \in \mathscr{B}$ となる．$x \in B_2 \setminus B_1$ より $B_2 \setminus \big(B_1 \setminus \{x\}\big) = B_2 \setminus B_1$，$y \in B_2 \setminus B_1$ に対して $\big(B_1 \setminus \{x\}\big) \cup \{y\} = \big(B_1 \cup \{y\}\big) \setminus \{x\}$ であるから，結局

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \ \forall x \in B_1 \setminus B_2.\ \ \exists y \in B_2 \setminus B_1.\ \ \big(B_1 \cup \{y\}\big) \setminus \{x\} \in \mathscr{B}$$

すなわち (B1) が成り立つ． ■

[⇐]　$\mathscr{B} \subseteq \mathfrak{P}S$ が (B0) および (B1) を満たすとする．この $\mathscr{B}$ に対して

$$\mathscr{I} \coloneqq \{X \subseteq S \mid \exists B \in \mathscr{B}.\ \ X \subseteq B\}$$

で定めた $(S, \mathscr{I})$ が (I1)，(I2)，(I3) をすべて満たし，$\mathscr{B}$ を基族とするマトロイドであることを示す．まず (B0) より $\mathscr{B} \neq \varnothing$ であるから $\varnothing \subseteq B$ なる $B \in \mathscr{B}$ が存在し，したがって $\varnothing \in \mathscr{I}$ すなわち (I1) が成り立つ．また (I2) は $\mathscr{I}$ の定義より明らかに成り立つ．以降は (I3) を示す．$|U| = |V| + 1$ なる $U, V \in \mathscr{I}$ をとると，$\mathscr{I}$ の定義より $U \subseteq B_1$，$V \subseteq B_2$ なる $B_1, B_2 \in \mathscr{B}$ が存在する．この $B_1, B_2 \in \mathscr{B}$ をとると，補題 2.5.6 より $|B_1| = |B_2|$ であり，したがって

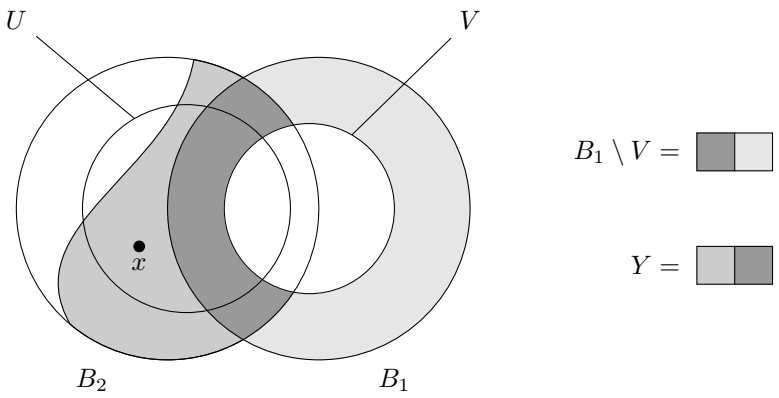
$$\begin{aligned} \big|B_1 \setminus B_2\big| &= |B_1| - |B_1 \cap B_2| \\ &= |B_2| - |B_1 \cap B_2| = \big|B_2 \setminus B_1\big| \end{aligned}$$

より $\big|B_1 \setminus B_2\big| = \big|B_2 \setminus B_1\big|$ である．このとき，補題 2.5.4 と $B_1 \setminus V \subseteq B_1$ より，或る $Y \subseteq B_2$ が存在して $|Y| = \big|B_1 \setminus V\big|$ かつ $\big(B_1 \setminus \big(B_1 \setminus V\big)\big) \cup Y \in \mathscr{B}$ を満たす．すなわちこの Y をとると $|Y| = |B_1| - |V|$ かつ $V \cup Y \in \mathscr{B}$ が成り立つ．ここで $Y \subseteq B_2$，$B_2 \setminus U \subseteq B_2$ だが，

$$\begin{aligned} |Y| &= |B_1| - |V| \\ &= |B_2| - \big(|U| - 1\big) \\ &> |B_2| - |U| = \big|B_2 \setminus U\big| \end{aligned}$$

であるから $Y \not\subseteq B_2 \setminus U$ が成り立ち，したがって $Y \cap U \neq \varnothing$ であり $x \in Y \cap U$ がとれる．$Y \cap U \subseteq U \setminus V$ より $x \in U \setminus V$ であり，また $V \cup \{x\} \subseteq V \cup Y$ かつ $V \cup Y \in \mathscr{B}$ であるから，$\mathscr{I}$ の定義より $V \cup \{x\} \in \mathscr{I}$ が成り立つ．ゆえに，任意の $|U| = |V| + 1$ なる $U, V \in \mathscr{I}$ に対して或る $x \in U \setminus V$ が存在して $V \cup \{x\} \in \mathscr{I}$ を満たし，(I3) が成り立つ．

以上より，$M = (S, \mathscr{I})$ は (I1)，(I2)，(I3) をいずれも満たし，マトロイドである．M の基族が $\mathscr{B}$ であることは，$\mathscr{I}$ の定義と補題 2.5.5 より明らかである． ■



基公理の [⇒] が示されたから，基公理の [⇐] を証明するための準備で示した (B1) から導かれる諸性質は，そのままマトロイドの性質であることがわかる．以下に系として掲げておく．

系 2.5.7 (B1) の拡張

マトロイド $M = (S, \mathscr{I})$ と M の基族 $\mathscr{B}$ に対して

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \ \forall X \subseteq B_1 \setminus B_2.\ \ \exists Y \subseteq B_2 \setminus B_1.\ \Big(|Y| = |X| \ \wedge\ \big(B_1 \setminus X\big) \cup Y \in \mathscr{B}\Big)$$

が成り立つ．

証明　基公理と補題 2.5.7 から明らかである． ■

系 2.5.8 (B1) の拡張 2

マトロイド $M = (S, \mathscr{I})$ と M の基族 $\mathscr{B}$ に対して

$$\forall B_1 \forall B_2 \in \mathscr{B}.\ \ \forall X \subseteq B_1.\ \ \exists Y \subseteq B_2.\ \Big(|Y| = |X| \ \wedge\ \big(B_1 \setminus X\big) \cup Y \in \mathscr{B}\Big)$$

が成り立つ．

証明　基公理と補題 2.5.8 から明らかである． ■

以上により基公理を示すことができたのだが，以降で独立集合族を規定する同値な公理を少し見てみよう．

定義 2.5.9 公理 (I3′)

有限集合 S と $\mathscr{I} \subseteq \mathfrak{P}S$ に対し，

(I3′)　$$\forall A \subseteq S.\ \ \forall Y_1 \forall Y_2 \in \operatorname{maxl}\big\{Y \subseteq A \,\big|\, Y \in \mathscr{I}\big\}.\ \ |Y_1| = |Y_2|$$

で公理 (I3′) を定める．

定理 2.5.10 独立集合族の公理の代替

有限集合 S と $\mathscr{I} \subseteq \mathfrak{P}S$ に対し，$\mathscr{I}$ が (I1)，(I2)，(I3) をすべて満たすことと，$\mathscr{I}$ が (I1)，(I2)，(I3′) をすべて満たすこととは同値である．

証明

[⇒]　(I1)，(I2)，(I3) から (I3′) を背理法により示す．或る $A \subseteq S$ と $Y_1, Y_2 \in \operatorname{maxl}\big\{Y \subseteq A \,\big|\, Y \in \mathscr{I}\big\}$ が存在して $|Y_1| \neq |Y_2|$ が成り立つと仮定する．$|Y_1| < |Y_2|$ として一般性を失わないのでこう定める．定理

2.5.1 : 増強定理より，$Z \subseteq Y_2 \setminus Y_1$ で $|Y_1 \cup Z| = |Y_2|$ かつ $Y_1 \cup Z \in \mathscr{I}$ を満たすものが存在する．この Z をとると $Z \neq \varnothing$ および $Z \subseteq Y_2 \subseteq A$ が成り立つので $Y_1 \cup Z \in \{Y \subseteq A \mid Y \in \mathscr{I}\}$ かつ $Y_1 \subsetneq Y_1 \cup Z$ であり，これは Y_1 の極大性に反し矛盾である． ■

[⇐]　(I1)，(I2)，(I3′) から (I3) を示す．$|U| = |V| + 1$ なる $U, V \in \mathscr{I}$ をとり，$A \coloneqq U \cup V$ とする．このとき，$U \subseteq X_1$，$V \subseteq X_2$ なる $X_1, X_2 \in \operatorname{maxl}\{X \subseteq A \mid X \in \mathscr{I}\}$ が存在する．この X_1，X_2 は (I3′) より $|X_1| = |X_2|$ を満たす．$|X_2| = |X_1| \geq |U| = |V| + 1$ より $|V| < |X_2|$ であるから $V \subsetneq X_2$．したがって $X_2 \setminus V \neq \varnothing$ であり，$x \in X_2 \setminus V$ がとれる．この x は $V \cup \{x\} \subseteq X_2$ を満たすから，$X_2 \in \mathscr{I}$ と (I2) より $V \cup \{x\} \in \mathscr{I}$．ところで $X_2 \subseteq A = U \cup V$ だったので $X_2 \setminus V \subseteq U \setminus V$ が成り立ち，x は $x \in U \setminus V$ を満たす．

ゆえに，$|U| = |V| + 1$ なる任意の $U, V \in \mathscr{I}$ に対して $x \in U \setminus V$ が存在して $V \cup \{x\} \in \mathscr{I}$ を満たす．すなわち (I3) が成り立つ． ■

2.6 階数函数に関する性質

まずは階数公理の [⇒] を示す準備として，マトロイドの階数函数がもつ諸性質を示しておこう．

補題 2.6.1 独立性と最大階数性の一致

マトロイド $M = (S, \mathscr{I})$ と M の階数函数 ρ に対し，$\forall A \subseteq S.\ \big(A \in \mathscr{I} \ \Leftrightarrow\ \rho(A) = |A|\big)$ が成り立つ．

証明　階数函数 ρ の定義からほぼ自明：　$A \in \mathscr{I}$ とすると，$\rho(A) = \max\big\{|X| \,\big|\, X \subseteq A \ \wedge\ X \in \mathscr{I}\big\} = |A|$ である．逆に $\rho(A) = |A|$ とすると $|A| = |X|$ かつ $X \in \mathscr{I}$ なる $X \subseteq A$ が存在するが，$|A| = |X|$ なる $X \subseteq A$ は A のみであるから $A \in \mathscr{I}$ である． ■

補題 2.6.2 階数函数の単調増加性

マトロイド $M = (S, \mathscr{I})$ と M の階数函数 ρ に対し，

$$\forall A \forall B \subseteq S.\ \big(A \subseteq B \ \Rightarrow\ \rho(A) \leq \rho(B)\big)$$

が成り立つ．

証明　感覚的にもほぼ明らかである：　$A \subseteq B$ なる $A, B \subseteq S$ をとると

$$\big\{|X| \,\big|\, X \subseteq A \ \wedge\ X \in \mathscr{I}\big\} \subseteq \big\{|X| \,\big|\, X \subseteq B \ \wedge\ X \in \mathscr{I}\big\}$$

であるから，$\rho(A) \leq \rho(B)$ が成り立つ． ■

補題 2.6.3

マトロイド $M = \big(S, \mathscr{I}\big)$ と M の階数函数 ρ に対し，$\forall x \in S.\ \forall A \subseteq S.\ \rho\big(A \cup \{x\}\big) \leq \rho(A) + 1$ が成り立つ．

証明　まず $x \in A$ のときは自明であるから，以降 $x \in S \setminus A$ のときを考える．ρ の定義より $|Y| = \rho\big(A \cup \{x\}\big)$ かつ $Y \subseteq A \cup \{x\}$ かつ $Y \in \mathscr{I}$ なる Y が存在するのでこの Y をとる．

- $x \notin Y$ のとき，$Y \subseteq A$ かつ $Y \in \mathscr{I}$ であるから

$$\begin{aligned}\rho\big(A \cup \{x\}\big) &= |Y| \\ &\leq \max\big\{|X| \,\big|\, X \subseteq A \ \wedge\ X \in \mathscr{I}\big\} \\ &= \rho(A)\end{aligned}$$

  であり，一方補題 2.6.2 より $\rho(A) \leq \rho\big(A \cup \{x\}\big)$ であるから，結局 $\rho\big(A \cup \{x\}\big) = \rho(A)$ が成り立ち，$\rho\big(A \cup \{x\}\big) \leq \rho(A) + 1$．■

- $x \in Y$ のとき，$x \notin Z$ なる $Z \subseteq A$ を用いて $Y = Z \cup \{x\}$ と書ける．このとき $Y \in \mathscr{I}$ と (I2) より $Z \in \mathscr{I}$ であるから，Z は $Z \subseteq A$ かつ $Z \in \mathscr{I}$ を満たし，

$$\begin{aligned}\rho(A) &= \max\big\{|X| \,\big|\, X \subseteq A \ \wedge\ X \in \mathscr{I}\big\} \\ &\geq |Z| \\ &= |Y| - 1 \\ &= \rho\big(A \cup \{x\}\big) - 1\end{aligned}$$

  が成り立つ．すなわち $\rho\big(A \cup \{x\}\big) \leq \rho(A) + 1$ である．■

続いて階数公理の $[\Leftarrow]$ を示すために，(R1)，(R2)，(R3) から導かれる諸性質を示しておこう．

補題 2.6.4

有限集合 S と函数 $\rho\colon\ \mathfrak{P}S \to \mathbf{N}$ が (R1)，(R2) を満たすならば，

$$\forall X \subseteq S.\ \ 0 \leq \rho(X) \leq |X|$$

が成り立つ．

証明　集合 X の大きさ $|X| \in \mathbf{N}$ に関する帰納法による．

- $|X| = 0$ のとき，$X = \varnothing$ であり，(R1) より $\rho(\varnothing) = 0$ であるから明らか．

- $|X| \geq 1$ のとき，$x \in X$ をとると，帰納法の仮定より $0 \leq \rho\big(X \setminus \{x\}\big) \leq \big|X \setminus \{x\}\big|$．したがって (R2)

より

$$\begin{aligned}\rho(X) &= \rho\Big(\big(X \setminus \{x\}\big) \cup \{x\}\Big) \\ &\geq \rho\big(X \setminus \{x\}\big) \\ &\geq 0\end{aligned}$$

であり $0 \leq \rho(X)$. また，やはり (R2) より

$$\begin{aligned}\rho(X) &= \rho\Big(\big(X \setminus \{x\}\big) \cup \{x\}\Big) \\ &\leq \rho\big(X \setminus \{x\}\big) + 1 \\ &\leq \big|X \setminus \{x\}\big| + 1 \\ &= \big(|X| - 1\big) + 1 = |X|\end{aligned}$$

であり $\rho(X) \leq |X|$ が成り立つ．ゆえに $0 \leq \rho(X) \leq |X|$.

以上より，任意の $X \subseteq S$ に対して $0 \leq \rho(X) \leq |X|$ が成り立つ． ■

補足 上の証明を平易に書けば，$X = \{x_1, \ldots, x_m\}$ とおいて

$$\begin{aligned}\rho(X) &= \rho\Big(\big\{x_1, \ldots, x_{m-1}\big\} \cup \big\{x_m\big\}\Big) \\ &\geq \rho\Big(\big\{x_1, \ldots, x_{m-1}\big\}\Big) \\ &\vdots \\ &\geq \rho\big(\{x_1\}\big) \\ &\geq \rho(\varnothing) = 0\end{aligned}$$

および

$$\begin{aligned}\rho(X) &= \rho\Big(\big\{x_1, \ldots, x_{m-1}\big\} \cup \big\{x_m\big\}\Big) \\ &\leq \rho\Big(\big\{x_1, \ldots, x_{m-1}\big\}\Big) + 1 \\ &\vdots \\ &\leq \rho\big(\{x_1\}\big) + (m-1) \\ &\leq \rho(\varnothing) + 1 + (m-1) = m = |X|\end{aligned}$$

ということになる．簡潔な場合はこのような有限回の操作を中略する書き方でも良いが，手続きが複雑なものは中略の部分でその妥当性が不明瞭になるおそれがあるので，できるだけ帰納法で書くことにする．

補題 2.6.5

有限集合 S と $\rho\colon\ \mathfrak{P}S \to \mathbf{N}$ が (R2) を満たすならば，

$$\forall X \forall Z \subseteq S.\ \ \rho(X \cup Z) \leq \rho(X) + |Z|$$

が成り立つ．

証明　Z の大きさ $|Z|$ に関する帰納法による．

- $|Z| = 0$ のとき，$Z = \varnothing$ より $\rho(X \cup Z) = \rho(X) \leq \rho(X) + |Z|$ であり明らか．
- $|Z| \geq 1$ のとき，$z \in Z$ がとれる．$\bigl|Z \setminus \{z\}\bigr| < |Z|$ であるから，帰納法の仮定より

  $$\rho\Bigl(X \cup \bigl(Z \setminus \{z\}\bigr)\Bigr) \leq \rho(X) + \bigl|Z \setminus \{z\}\bigr| = \rho(X) + |Z| - 1$$

  が成り立つ．ここで (R2) より

  $$\begin{aligned}\rho(X \cup Z) &= \rho\Bigl(X \cup \bigl(Z \setminus \{z\}\bigr) \cup \{z\}\Bigr) \\ &\leq \rho\Bigl(X \cup \bigl(Z \setminus \{z\}\bigr)\Bigr) + 1 \\ &\leq \bigl(\rho(X) + |Z| - 1\bigr) + 1 \\ &= \rho(X) + |Z|\end{aligned}$$

  であり，ゆえに $\rho(X \cup Z) \leq \rho(X) + |Z|$.

以上より，任意の $X, Z \subseteq S$ に対して $\rho(X \cup Z) \leq \rho(X) + |Z|$. ■

補題 2.6.6

有限集合 S と $\rho\colon \mathfrak{P}S \to \mathbf{N}$ が (R3) を満たすならば，

$$\forall X \forall Y \subseteq S.\ \Bigl(\bigl(\forall y \in Y.\ \ \rho\bigl(X \cup \{y\}\bigr) = \rho(X)\bigr) \Rightarrow\ \rho(X \cup Y) = \rho(X)\Bigr)$$

が成り立つ．

証明　Y の大きさ $|Y|$ に関する帰納法による．

- $|Y| = 0$ のとき，$Y = \varnothing$ であり，明らかに成り立つ．
- $|Y| = 1$ のとき，$Y = \{y\}$ とおけることから明らかに成り立つ．
- $|Y| \geq 2$ のとき，$a \neq b$ なる $a, b \in Y$ がとれる．任意の $y \in Y$ に対して $\rho\bigl(X \cup \{y\}\bigr) = \rho(X)$ が成り立つとすると，$\bigl|Y \setminus \{a, b\}\bigr| < |Y|$ かつ任意の $y \in Y \setminus \{a, b\}$ に対して $\rho\bigl(X \cup \{y\}\bigr) = \rho(X)$ であるから，帰納法の仮定より

  $$\rho\Bigl(X \cup \bigl(Y \setminus \{a, b\}\bigr)\Bigr) = \rho(X)$$

  が成り立つ．$Z \coloneqq X \cup \bigl(Y \setminus \{a, b\}\bigr)$ とすると $\rho(Z) = \rho(X)$．$Y \setminus \{a\}$ および $Y \setminus \{b\}$ についても同様に帰納法の仮定より

  $$\begin{aligned}\rho\Bigl(X \cup \bigl(Y \setminus \{a\}\bigr)\Bigr) &= \rho(X) \\ \rho\Bigl(X \cup \bigl(Y \setminus \{b\}\bigr)\Bigr) &= \rho(X)\end{aligned}$$

が成り立つ．このとき

$$\rho\big(Z\cup\{a\}\big)=\rho\Big(X\cup\big(Y\setminus\{b\}\big)\Big)=\rho(X)=\rho(Z)$$
$$\rho\big(Z\cup\{b\}\big)=\rho\Big(X\cup\big(Y\setminus\{a\}\big)\Big)=\rho(X)=\rho(Z)$$

であるから，(R3) より $\rho\big(Z\cup\{a\}\cup\{b\}\big)=\rho(Z)$，すなわち $\rho(X\cup Y)=\rho(X)$ が成り立つ．

以上より示された． ■

……

補足 上の補題の証明でやっていることはなにやらわかりづらいが，実際に“大きさの小さい方から示していく”ことを試すと実感が湧く．任意の $y_1\in Y$ に対して $\rho\big(X\cup\{y_1\}\big)=\rho(X)$ が成り立つとすると，勿論任意の $y_1,y_2\in Y$ に対して

$$\rho\big(X\cup\{y_1\}\big)=\rho\big(X\cup\{y_2\}\big)=\rho(X)$$

であるから，(R3) より

$$\rho\big(X\cup\{y_1\}\cup\{y_2\}\big)=\rho(X)$$

が成り立つ．これも $y_1,y_2\in Y$ は任意であったから，さらに任意の $y_1,y_2,y_3\in Y$ に対して

$$\rho\big(X\cup\{y_1\}\cup\{y_2\}\big)=\rho\big(X\cup\{y_1\}\cup\{y_3\}\big)=\rho(X)=\rho\big(X\cup\{y_1\}\big)$$

が成り立ち，やはり (R3) より

$$\rho\Big(\big(X\cup\{y_1\}\big)\cup\{y_2\}\cup\{y_3\}\Big)=\rho\big(X\cup\{y_1\}\big)=\rho(X)$$

となる．こうして“ひとつずつ増やしていく”ことにより，$m:=|Y|$ とするとやがて任意の $y_1,\dots,y_m\in Y$ に対して $\rho\big(X\cup\{y_1\}\cup\cdots\cup\{y_m\}\big)=\rho(X)$ に到達し，$y_1,\dots,y_m$ に Y の相異なる元をあてることで $\rho(X\cup Y)=\rho(X)$ が示せるのである．

さて，これで階数公理を示す準備ができたので，実際に以下で示してみよう．

定理 再掲：階数公理

S を有限集合とする．$\rho\colon\mathfrak{P}S\to\mathbf{N}$ が或る S 上のマトロイドの階数函数であるための必要十分条件は

(R1) $\rho(\varnothing)=0$

(R2) $\forall X\subseteq S.\ \forall y\in S.\ \rho(X)\le\rho\big(X\cup\{y\}\big)\le\rho(X)+1$

(R3) $\forall X\subseteq S.\ \forall y\forall z\in S.\ \Big(\rho\big(X\cup\{y\}\big)=\rho\big(X\cup\{z\}\big)=\rho(X)\ \Rightarrow\ \rho\big(X\cup\{y\}\cup\{z\}\big)=\rho(X)\Big)$

である．

証明

[⇒]　(I1)，(I2)，(I3) を満たす $M = \big(S, \mathscr{I}\big)$ に対し，M の階数函数 ρ が (R1)，(R2)，(R3) を満たすことを示す．(R1) は (I1) より $\rho(\varnothing) = \big\{|X| \,\big|\, X \subseteq \varnothing \ \wedge\ X \in \mathscr{I}\big\} = |\varnothing| = 0$ と簡単に示せる．(R2) も，$X \subseteq S$ と $y \in S$ に対して補題 2.6.2 より $\rho(X) \leq \rho\big(X \cup \{y\}\big)$，補題 2.6.3 より $\rho\big(X \cup \{y\}\big) \leq \rho(X) + 1$ であるから容易である．以降 (R3) を背理法により示す．

いま仮に $\rho\big(X \cup \{y\}\big) = \rho\big(X \cup \{z\}\big) = \rho(X)$ かつ $\rho\big(X \cup \{y\} \cup \{z\}\big) \neq \rho(X)$ なる $X \subseteq S$ と $y, z \in S$ が存在するとする．$X \subseteq X \cup \{y\} \cup \{z\}$ と補題 2.6.2：階数函数の単調性より $\rho(X) \leq \rho\big(X \cup \{y\} \cup \{z\}\big)$ であるから，結局 $\rho\big(X \cup \{y\} \cup \{z\}\big) > \rho(X)$ が成り立つ．このとき，階数函数 ρ の定義より $\rho(X) = |Y|$ かつ $Y \subseteq X$ なる $Y \in \mathscr{I}$ と，$\rho\big(X \cup \{y\} \cup \{z\}\big) = |Z|$ かつ $Z \subseteq X \cup \{y\} \cup \{z\}$ なる $Z \in \mathscr{I}$ がそれぞれ存在する．この Y と Z は仮定 $\rho\big(X \cup \{y\} \cup \{z\}\big) > \rho(X)$ より $|Z| > |Y|$ を満たし，定理 2.5.1：増強定理より，或る $W \subseteq Z \setminus Y$ が存在して $Y \cup W \in \mathscr{I}$ かつ $|Y \cup W| = |Z|$ が成り立つ．この W が仮に $y \notin W$ かつ $z \notin W$ を満たしたとすると，$Y \cup W \subseteq X$ かつ $Y \cup W \in \mathscr{I}$ より

$$|Z| = |Y \cup W| \leq \max\big\{|A| \,\big|\, A \subseteq X \ \wedge\ A \in \mathscr{I}\big\} = \rho(X) = |Y| < |Z|$$

となって矛盾するので，$y \in W$ または $z \in W$ である．$y \in W$ として一般性を失わないのでこう定める．このとき，$W \subseteq Z \setminus Y$ より $y \notin Y$．また，$Y \cup W \in \mathscr{I}$，$Y \cup \{y\} \subseteq Y \cup W$，(I2) より $Y \cup \{y\} \in \mathscr{I}$ であり，補題 2.6.1 より

$$\begin{aligned}\rho\big(Y \cup \{y\}\big) &= \big|Y \cup \{y\}\big| \\ &= |Y| + 1 \\ &= \rho(X) + 1\end{aligned}$$

が成り立つ．一方補題 2.6.2：階数函数の単調性より

$$\rho\big(Y \cup \{y\}\big) \leq \rho\big(X \cup \{y\}\big)$$

であり，結局 $\rho(X) + 1 \leq \rho\big(X \cup \{y\}\big)$ が成り立ち $\rho(X) = \rho\big(X \cup \{y\}\big)$ に矛盾．

ゆえに，任意の $X \subseteq S$ と $y, z \in S$ に対して，$\rho\big(X \cup \{y\}\big) = \rho\big(X \cup \{z\}\big) = \rho(X)$ ならば $\rho\big(X \cup \{y\} \cup \{z\}\big) = \rho(X)$ である．すなわち (R3) が成り立つ．■

[⇐]　(R1)，(R2)，(R3) を満たす ρ に対し，

$$\mathscr{I} := \big\{X \subseteq S \,\big|\, \rho(X) = |X|\big\}$$

で定めた $\big(S, \mathscr{I}\big)$ が (I1)，(I2)，(I3) を満たし，ρ を階数函数とするマトロイドであることを示す．

まず (R1) より $\rho(\varnothing) = 0 = |\varnothing|$ であるから $\varnothing \in \mathscr{I}$ すなわち (I1) が成り立つ．

次に (I2) を背理法で示す．仮に $X \in \mathscr{I}$ に対して或る $Y \subseteq X$ が存在して $Y \notin \mathscr{I}$ を満たすとする．このとき $\mathscr{I}$ の定義より $\rho(Y) \neq |Y|$．補題 2.6.4 より $\rho(Y) \leq |Y|$ であるから，結局 $\rho(Y) < |Y|$．このとき，補題 2.6.5 より $\rho\big(Y \cup \big(X \setminus Y\big)\big) \leq \rho(Y) + \big|X \setminus Y\big|$ であり，

$$\begin{aligned}\rho(X) &= \rho\big(Y \cup \big(X \setminus Y\big)\big) \\ &\leq \rho(Y) + \big|X \setminus Y\big| \\ &< |Y| + \big|X \setminus Y\big| = |X|\end{aligned}$$

より $\rho(X) < |X|$，すなわち $X \notin \mathscr{I}$ が成り立ち矛盾．よって任意の $X, Y \subseteq S$ に対して $Y \subseteq X$ かつ $X \in \mathscr{I}$ ならば $Y \in \mathscr{I}$ であり，(I2) が成り立つ．

最後に (I3) を背理法により示す．いま仮に或る $U, V \in \mathscr{I}$ が $|U| = |V| + 1$ かつ任意の $z \in U \setminus V$ に対して $V \cup \{z\} \notin \mathscr{I}$ を満たすとする．すなわち $z \in U \setminus V$ を任意に選ぶと $\rho\big(V \cup \{z\}\big) \neq \big|V \cup \{z\}\big| = |V| + 1$ である．これに加えて (R2) より $\rho(V) \leq \rho\big(V \cup \{z\}\big) \leq \rho(V) + 1$，また $V \in \mathscr{I}$ より $|V| = \rho(V)$ であるから，結局 $\rho\big(V \cup \{z\}\big) = \rho(V)$ が成り立つ．以上より

$$\forall z \in U \setminus V.\ \ \rho\big(V \cup \{z\}\big) = \rho(V)$$

であるから，補題 2.6.6 より $\rho\big(V \cup \big(U \setminus V\big)\big) = \rho(V)$ が成り立つ．すなわち $\rho(U \cup V) = |V|$ である．ここで $U \subseteq U \cup V$ と補題 2.6.4 より $\rho(U) \leq \rho(U \cup V)$ であり，また $U \in \mathscr{I}$ より $|U| = \rho(U)$ であるから，したがって

$$\begin{aligned} |V| + 1 &= |U| \\ &= \rho(U) \\ &\leq \rho(U \cup V) = |V| \end{aligned}$$

が成り立ち矛盾．ゆえに任意の $|U| = |V|+1$ なる $U, V \in \mathscr{I}$ に対して或る $z \in U \setminus V$ が存在して $V \cup \{z\} \in \mathscr{I}$ を満たし，(I3) が成り立つ．

以上より，(R1)，(R2)，(R3) を満たす ρ に対して $\mathscr{I} \coloneqq \big\{X \subseteq S \,\big|\, \rho(X) = |X|\big\}$ で定めた $M = (S, \mathscr{I})$ はマトロイドである．M の階数函数を r とおくと，$A \subseteq S$ に対して

$$r(A) \coloneqq \big\{|X| \,\big|\, X \subseteq A \ \wedge\ X \in \mathscr{I}\big\}$$

である．$|X| = r(A)$ かつ $X \subseteq A$ なる $X \in \mathscr{I}$ が存在し，$\mathscr{I}$ の定義より $\rho(X) = |X| = r(A)$．ここで任意に $w \in A \setminus X$ を選ぶ．仮に $X \cup \{w\} \in \mathscr{I}$ であるとすると X の極大性に矛盾，すなわち $X \cup \{w\} \subseteq A$ かつ $X \cup \{w\} \in \mathscr{I}$ より

$$\begin{aligned} |X| &< \big|X \cup \{w\}\big| \\ &\leq \max\big\{|Y| \,\big|\, Y \subseteq A \ \wedge\ Y \in \mathscr{I}\big\} \\ &= r(A) = |X| \end{aligned}$$

となって矛盾するので，$X \cup \{w\} \notin \mathscr{I}$ が成り立つ．よって $\rho\big(X \cup \{w\}\big) \neq \big|X \cup \{w\}\big|$ であり，やはり $|X| = \rho(X)$ と (R2) より $\rho\big(X \cup \{w\}\big) = \rho(X)$．$w \in A \setminus X$ は任意であったから，補題 2.6.6 より $\rho(A) = \rho\big(X \cup \big(A \setminus X\big)\big) = \rho(X)$ が成り立つ．以上より $\rho(A) = \rho(X) = r(A)$ であり，任意の $A \subseteq S$ に対して $\rho(A) = r(A)$ であるから $\rho = r$，すなわち ρ は M の階数函数である． ■

ところで，最初に階数公理 (R1)，(R2)，(R3) と並べて階数公理の別版 (R1′)，(R2′)，(R3′) を挙げた．階数公理は $x \in S$ などと“S の元の階層”にも直接言及しているのに対して，別版は“S の階層”で完結した表現である．特に (R3′) は**劣モジュラ律** (submodularity) と呼ばれる重要な性質である．以下でその同値性を示そう．

定理 再掲：階数公理別版

S を有限集合とする．$\rho\colon \mathfrak{P}S \to \mathbf{N}$ が或る S 上のマトロイドの階数函数であるための必要十分条件は

(R1′) $\forall X \subseteq S.\ \ 0 \leq \rho(X) \leq |X|$

(R2′) $\forall X \forall Y \subseteq S.\ \big(X \subseteq Y \ \Rightarrow\ \rho(X) \leq \rho(Y)\big)$

(R3′) $\forall X \forall Y \subseteq S.\ \ \rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$

である．

証明

[⇒]　(R1′) および (R2′) はそれぞれ補題 2.6.4 と補題 2.6.2 で既に示したので，以降はマトロイド $M = (S, \mathscr{I})$ の階数函数 ρ が (R3′) を満たすことを示す．

$X, Y \subseteq S$ とする．ρ の定義より $|P| = \rho(X \cap Y)$ かつ $P \subseteq X \cap Y$ なる $P \in \mathscr{I}$ と $\big|Q\big| = \rho(X \cup Y)$ かつ $Q \subseteq X \cup Y$ なる $Q \in \mathscr{I}$ がそれぞれ存在するので，これらの $P, Q \in \mathscr{I}$ をとる．このとき，$X \cap Y \subseteq X \cup Y$ と補題 2.6.2：階数函数の単調性より $\rho(X \cap Y) \leq \rho(X \cup Y)$ であり，したがって $|P| \leq \big|Q\big|$.

- $|P| = \big|Q\big|$ のとき，$P \in \mathscr{I}$，$P \subseteq X$，$P \subseteq Y$ より $|P| \leq \rho(X)$，$|P| \leq \rho(Y)$ である．したがって

  $$\rho(X \cap Y) + \rho(X \cup Y) = |P| + \big|Q\big| = |P| + |P| \leq \rho(X) + \rho(Y)$$

  が成り立つ．

- $|P| < \big|Q\big|$ のとき，定理 2.5.1：増強定理より，或る $Z \subseteq Q \setminus P$ が存在して $|P \cup Z| = \big|Q\big|$ かつ $P \cup Z \in \mathscr{I}$ が成り立つから，この Z を用いて $W \coloneqq P \cup Z$ と定める．$P \subseteq W \cap (X \cap Y)$ であるが，ここで仮に $P \subsetneq W \cap (X \cap Y)$ であるとすると，$W \in \mathscr{I}$ から (I2) より $W \cap (X \cap Y) \in \mathscr{I}$ であり，$W \cap (X \cap Y) \subseteq X \cap Y$ より P の極大性に反して矛盾，すなわち

  $$\begin{aligned} |P| &< \big|W \cap (X \cap Y)\big| \\ &\leq \rho(X \cap Y) = |P| \end{aligned}$$

  により矛盾する．したがって $P = W \cap (X \cap Y)$ である．ここで $U \coloneqq W \cap \big(X \setminus Y\big)$, $V \coloneqq W \cap \big(Y \setminus X\big)$ と定めると，$U \cap P = \varnothing$，$V \cap P = \varnothing$，$U \cap V = \varnothing$，$Q = U \cup P \cup V$ であるから

  $$\begin{aligned} |U \cup P| + |V \cup P| &= |U| + |P| + |V| + |P| \\ &= \big|Q\big| + |P| \\ &= \rho(X \cup Y) + \rho(X \cap Y) \end{aligned}$$

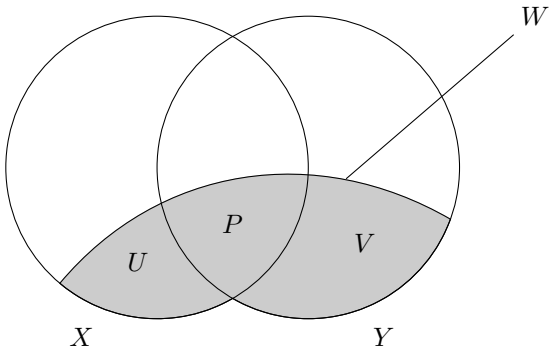
  が成り立つ．さらに $U \cup P \subseteq Q$，$V \cup P \subseteq Q$ から (I2) より $U \cup P \in \mathscr{I}$，$V \cup P \in \mathscr{I}$ であり，$U \cup P \subseteq X$ および $V \cup P \subseteq Y$ より

  $$|U \cup P| \leq \rho(X) \qquad\qquad |V \cup P| \leq \rho(Y)$$

  であるから，結局

  $$\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$$

が成り立つ．



以上より，任意の $X, Y \subseteq S$ に対して $\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$ が成り立つ． ■

[⇐]　階数公理より，(R1′)，(R2′)，(R3′) を満たす ρ が (R1)，(R2)，(R3) を満たすことを示せば十分である．まず (R1′) より $0 \leq \rho(\varnothing) \leq |\varnothing| = 0$ であり，$\rho(\varnothing) = 0$，すなわち (R1) が成り立つ．次に (R2) を示す．$X \subseteq S$，$y \in S$ を任意にとると，$X \subseteq X \cup \{y\}$ と (R2′) より $\rho(X) \leq \rho\big(X \cup \{y\}\big)$．

- $X \cap \{y\} \neq \varnothing$ のとき，$y \in X$ より $X \cup \{y\} = X$ であり，$\rho\big(X \cup \{y\}\big) = \rho(X) \leq \rho(X) + 1$．
- $X \cap \{y\} = \varnothing$ のとき，$y \notin X$ であり，(R3′) および既に示した (R1) より

$$\begin{aligned} \rho(X) + \rho\big(\{y\}\big) &\geq \rho\big(X \cup \{y\}\big) + \rho\big(X \cap \{y\}\big) \\ &= \rho\big(X \cup \{y\}\big) + \rho(\varnothing) \\ &= \rho\big(X \cup \{y\}\big) \end{aligned}$$

が成り立つ．(R1′) より $0 \leq \rho\big(\{y\}\big) \leq \big|\{y\}\big| = 1$ であるから，結局

$$\rho\big(X \cup \{y\}\big) \leq \rho(X) + \rho\big(\{y\}\big) \leq \rho(X) + 1$$

が成り立つ．

以上より，任意の $X \subseteq S$ と $y \in S$ に対して $\rho(X) \leq \rho\big(X \cup \{y\}\big) \leq \rho(X) + 1$ であり，(R2) が成り立つ．最後に (R3) を示す．

- $x \in X$ のとき，$X \cup \{x\} = X$ であるから，$\rho\big(X \cup \{x\}\big) = \rho\big(X \cup \{y\}\big) = \rho(X)$ とすると即座に $\rho\Big(\big(X \cup \{x\}\big) \cup \{y\}\Big) = \rho\big(X \cup \{y\}\big) = \rho(X)$ が成り立ち，明らか．
- $y \in X$ のとき，上と同様に明らか．
- $x \notin X$ かつ $y \notin X$ のとき，$\rho\big(X \cup \{x\}\big) = \rho\big(X \cup \{y\}\big) = \rho(X)$ とすると，まず $X \subseteq X \cup \{x\} \cup \{y\}$

と (R2′) より $\rho(X) \leq \rho\big(X \cup \{x\} \cup \{y\}\big)$ が成り立つ．一方，(R3′) より

$$\begin{aligned}\rho(X) + \rho(X) &= \rho\big(X \cup \{x\}\big) + \rho\big(X \cup \{y\}\big) \\ &\geq \rho\Big(\big(X \cup \{x\}\big) \cup \big(X \cup \{y\}\big)\Big) + \rho\Big(\big(X \cup \{x\}\big) \cap \big(X \cup \{y\}\big)\Big) \\ &= \rho\big(X \cup \{x\} \cup \{y\}\big) + \rho(X)\end{aligned}$$

であり，$\rho(X) \geq \rho\big(X \cup \{x\} \cup \{y\}\big)$ が成り立つから，結局 $\rho\big(X \cup \{x\} \cup \{y\}\big) = \rho(X)$ である．

以上より，(R3) が成り立つ． ■

2.7 平坦集合と閉包演算子に関する性質

補題 2.7.1 閉包演算子の増大性

マトロイド $M = (S, \mathscr{I})$，M の閉包演算子 σ に対し，$\forall A \subseteq S.\ \ A \subseteq \sigma(A)$ が成り立つ．

証明　M の階数函数を ρ とおき，$A \subseteq S$ とする．

$x \in A$ とすると $A \cup \{x\} = A$ より $\rho\big(A \cup \{x\}\big) = \rho(A)$，すなわち $x \sim A$ であるから $x \in \sigma(A)$ が成り立つ．ゆえに $A \subseteq \sigma(A)$ である． ■

補題 2.7.2

マトロイド $M = (S, \mathscr{I})$ に対して $\forall F \in \operatorname{Flat} M.\ \ \forall x \in S.\, (x \sim F \ \Rightarrow\ x \in F)$ が成り立つ．

証明　平坦集合 $F \in \operatorname{Flat} M$ に対して $x \sim F$ なる $x \in S$ をとると，従属性の定義より $\rho\big(F \cup \{x\}\big) = \rho(F)$．ここで仮に $x \in S \setminus F$ とすると，平坦性の定義より $\rho\big(F \cup \{x\}\big) = \rho(F) + 1$ となり矛盾する．したがって $x \in F$ である． ■

補足　“元ならば従属”は一般に成り立つが，平坦集合ではさらに“従属ならば元”が成り立つ．つまり平坦集合 F に対しては F に従属な元全体と F 自身が一致するのである．

補題 2.7.3 閉包の平坦性

マトロイド $M = (S, \mathscr{I})$ と M の閉包演算子 σ に対し，$\forall A \subseteq S.\ \ \sigma(A) \in \operatorname{Flat} M$ が成り立つ．

証明　M の階数函数を ρ とおき，$A \subseteq S$ とする．

$x \in S \setminus \sigma(A)$ を任意にとると $\sigma(A)$ の定義より $x \not\sim A$，すなわち $\rho\big(A \cup \{x\}\big) \neq \rho(A)$ である．また補題 2.6.2：階数函数の単調増加性より $\rho(A) \leq \rho\big(A \cup \{x\}\big)$ であり，$\rho(A) + 1 \leq \rho\big(A \cup \{x\}\big)$ が成り立つ．一方補題 2.6.3 より $\rho\big(A \cup \{x\}\big) \leq \rho(A) + 1$ も成り立つから，結局 $\rho\big(A \cup \{x\}\big) = \rho(A) + 1$ である．

ゆえに $\forall x \in S \setminus \sigma(A).\ \ \rho\big(A \cup \{x\}\big) = \rho(A) + 1$，すなわち $\sigma(A) \in \operatorname{Flat} M$． ■

系 2.7.4 平坦性と閉包演算による不動性の一致

マトロイド $M = \big(S, \mathscr{I}\big)$ と M の閉包演算子 σ に対し，

$$\forall A \subseteq S.\ \big(A \in \operatorname{Flat} M \ \Leftrightarrow\ A = \sigma(A)\big)$$

が成り立つ．

証明　$A \subseteq S$ とする．$A \in \operatorname{Flat} M$ とすると，補題 2.7.2 より任意の $x \in S$ に対して $x \in A$ と $x \sim A$ が同値であるから，$\sigma(A) = \{x \in S \mid x \sim A\} = \{x \in S \mid x \in A\} = A$ となる．逆に $\sigma(A) = A$ とすると，補題 2.7.3：閉包の平坦性より $\sigma(A) \in \operatorname{Flat} M$ であり，したがって $A \in \operatorname{Flat} M$ である． ■

補題 2.7.5

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，

$$\forall B \in \mathscr{B}.\ \ \forall x \in S.\ \ x \sim B$$

が成り立つ．

証明　$B \in \mathscr{B}$，$x \in S$ とする．

- $x \in B$ のとき，自明である．
- $x \notin B$ のとき，今仮に $\rho\big(B \cup (x)\big) \neq \rho(B)$ とすると，(R2) より $\rho(B) \leq \rho\big(B \cup (x)\big) \leq \rho(B) + 1$ であるから $\rho\big(B \cup \{x\}\big) = \rho(B) + 1$ が成り立つ．ここで $B \in \mathscr{I}$ と補題 2.6.1 より $\rho(B) = |B|$ であるから

$$\begin{aligned} \rho\big(B \cup \{x\}\big) &= \rho(B) + 1 \\ &= |B| + 1 = \big|B \cup \{x\}\big| \end{aligned}$$

  より $\rho\big(B \cup \{x\}\big) = \big|B \cup \{x\}\big|$ が成り立ち，再び補題 2.6.1 より $B \cup \{x\} \in \mathscr{I}$ であるが，これは B の極大性に反するので矛盾．したがって $\rho\big(B \cup (x)\big) = \rho(B)$ であり，$x \sim B$．

以上より，任意の基 $B \in \mathscr{B}$ と $x \in S$ に対して $x \sim B$ が成り立つ． ■

補題 2.7.6

マトロイド $M = \big(S, \mathscr{I}\big)$ に対し，

$$\forall X \forall Y \subseteq S.\ \ \forall z \in S. \Big((x \sim X\ \wedge\ X \subseteq Y) \Rightarrow\ x \sim Y \Big)$$

が成り立つ．

証明　M の階数函数を ρ とおき，$X \subseteq Y$ なる $X, Y \subseteq S$ と $z \in S$ を任意にとる．

- $z \in Y$ のとき，自明である．
- $z \notin Y$ のとき，$z \notin X$ であり，また $z \sim X$ より $\rho\big(X \cup \{z\}\big) = \rho(X)$ であるから，(R3′) より

$$\begin{aligned} \rho(X) + \rho(Y) &= \rho\big(X \cup \{z\}\big) + \rho(Y) \\ &\geq \rho\Big(Y \cap \big(X \cup \{z\}\big)\Big) + \rho\Big(Y \cup \big(X \cup \{z\}\big)\Big) \\ &= \rho(X) + \rho\big(Y \cup \{z\}\big) \end{aligned}$$

が成り立ち，すなわち $\rho(Y) \geq \rho\big(Y \cup \{z\}\big)$ である．一方 (R2′) より $\rho(Y) \leq \rho\big(Y \cup \{z\}\big)$ であるから，結局 $\rho(Y) = \rho\big(Y \cup \{z\}\big)$ であり，すなわち $z \sim Y$．

以上より示された． ■

補題 2.7.7 閉包演算子の単調性

マトロイド $M = \big(S, \mathscr{I}\big)$ と M の閉包演算子 σ に対して

$$\forall A \forall B \subseteq S. \big(A \subseteq B\ \Rightarrow\ \sigma(A) \subseteq \sigma(B) \big)$$

が成り立つ．

証明　$A, B \subseteq S$ が $A \subseteq B$ を満たすとする．このとき $x \in \sigma(A)$ を任意にとると，$x \sim A$ であるから補題 2.7.6 より $x \sim B$ である．すなわち $x \in \sigma(B)$ が成り立つ．ゆえに $\sigma(A) \subseteq \sigma(B)$ である． ■

補題 2.7.8

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対して

$$\forall A \subseteq S.\ \ \forall X \subseteq A. \Big(\big(|X| = \rho(A)\ \wedge\ X \in \mathscr{I}\big) \Rightarrow\ \sigma(X) = \sigma(A) \Big)$$

が成り立つ．すなわち，部分集合のうちで極大な独立集合の閉包は，もとの集合の閉包と一致する．

証明　背理法による．$A \subseteq S$ に対し，$X \subseteq A$ が $|X| = \rho(A)$ かつ $X \in \mathscr{I}$ を満たすとする．補題 2.6.1 より

$|X| = \rho(X)$ である．いま仮に $\sigma(X) \neq \sigma(A)$ が成り立つとすると，$X \subseteq A$ と補題 2.7.7 より $\sigma(X) \subseteq \sigma(A)$ より，$\sigma(X) \subsetneq \sigma(A)$ である．このとき $\sigma(A) \setminus \sigma(X) \neq \varnothing$ より $y \in \sigma(A) \setminus \sigma(X)$ がとれる．この y は $y \in \sigma(A)$ より $y \sim A$ を満たし，従属性の定義より $\rho\big(A \cup \{y\}\big) = \rho(A)$ が成り立つ．同様に $y \notin \sigma(X)$ より $\rho\big(X \cup \{y\}\big) \neq \rho(X)$ であり，階数公理の (R2) より結局 $\rho\big(X \cup \{y\}\big) = \rho(X) + 1$．以上より

$$\begin{aligned}\rho\big(X \cup \{y\}\big) &= \rho(X) + 1 \\ &= |X| + 1 \\ &= \rho(A) + 1 \\ &= \rho\big(A \cup \{y\}\big) + 1 > \rho\big(A \cup \{y\}\big)\end{aligned}$$

であり $\rho\big(X \cup \{y\}\big) > \rho\big(A \cup \{y\}\big)$ が成り立つが，これは $X \cup \{y\} \subseteq A \cup \{y\}$ と補題 2.6.2 : 階数函数の単調性から導かれる $\rho\big(X \cup \{y\}\big) \leq \rho\big(A \cup \{y\}\big)$ と矛盾する．したがって $\sigma(X) = \sigma(A)$ が成り立つ． ■

補題 2.7.9 部分集合との階数の一致による閉包の一致

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，

$$\forall A \subseteq S.\ \ \forall X \subseteq A.\ \big(\rho(X) = \rho(A)\ \Rightarrow\ \sigma(X) = \sigma(A)\big)$$

が成り立つ．

証明　$A \subseteq S$ とし，$X \subseteq A$ が $\rho(X) = \rho(A)$ を満たすとする．ρ の定義より $|Y| = \rho(X)$ かつ $Y \subseteq X$ なる $Y \in \mathscr{I}$ が存在する．この Y は $\rho(X) = \rho(A)$ より $|Y| = \rho(A)$ も満たす．したがって補題 2.7.8 より $\sigma(Y) = \sigma(X)$ かつ $\sigma(Y) = \sigma(A)$ が成り立ち，$\sigma(X) = \sigma(A)$ である． ■

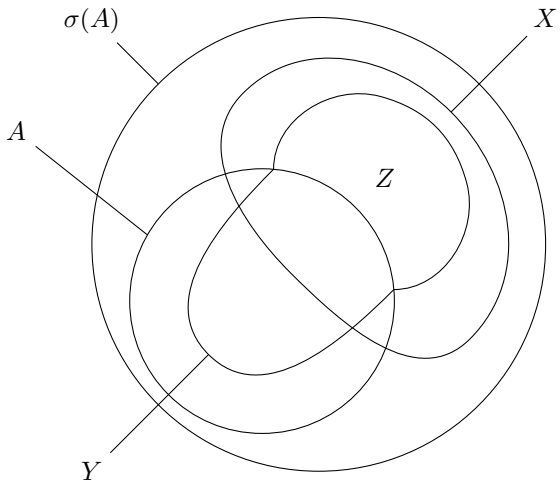
補題 2.7.10 閉包演算による階数の保存

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，

$$\forall A \subseteq S.\ \ \rho\big(\sigma(A)\big) = \rho(A)$$

が成り立つ．

証明　背理法による．$A \subseteq S$ とする．いま仮に $\rho\big(\sigma(A)\big) \neq \rho(A)$ が成り立つとすると，補題 2.7.1 : $A \subseteq \sigma(A)$ と補題 2.6.2 : 階数函数の単調性より $\rho\big(\sigma(A)\big) \geq \rho(A)$ であるから，結局 $\rho\big(\sigma(A)\big) > \rho(A)$ である．ρ の定義より，$|X| = \rho\big(\sigma(A)\big)$ かつ $X \subseteq \sigma(A)$ なる $X \in \mathscr{I}$ と $|Y| = \rho(A)$ かつ $Y \subseteq A$ なる $Y \in \mathscr{I}$ がそれぞれ存在するから，この $X, Y \in \mathscr{I}$ は $|X| > |Y|$ を満たす．このとき，定理 2.5.1 : 増強定理より，或る $Z \subseteq X \setminus Y$ が存在して $|Y \cup Z| = |X|$ かつ $Y \cup Z \in \mathscr{I}$ が成り立つ．この Z をとると $Z \neq \varnothing$ であるから，$z \in Z$ がとれる．$Y \cup \{z\} \subseteq Y \cup Z$ と (I2) より $Y \cup \{z\} \in \mathscr{I}$ であり，$\rho\big(Y \cup \{z\}\big) = \big|Y \cup \{z\}\big| = |Y| + 1 \neq |Y|$ より $z \notin \sigma(Y)$ が成り立つ．補題 2.7.8 より $\sigma(Y) = \sigma(A)$ であり，$z \notin \sigma(A)$ であるが，これは $z \in Z$ かつ $Z \subseteq \sigma(A)$ より $z \in \sigma(A)$ であることに矛盾．ゆえに $\rho\big(\sigma(A)\big) = \rho(A)$ が成り立つ． ■



.....

系 2.7.11 閉包演算子の合成に関する冪等律

マトロイド $M = \big(S, \mathscr{I}\big)$ と M の閉包演算子 σ に対し，

$$\forall A \subseteq S.\ \ \sigma\big(\sigma(A)\big) = \sigma(A)$$

が成り立つ．すなわち，$\sigma \circ \sigma = \sigma$ である．

証明　補題 2.7.10 と補題 2.7.9 より明らかである． ■

.....

次の補題は閉包公理の [⇐] を示すための準備である．σ は閉包演算子ではなく単なる (S1)，(S2)，(S3)，(S4) を満たす写像であることに注意.

補題 2.7.12

有限集合 S と (S1)，(S2)，(S3)，(S4) を満たす $\sigma\colon\ \mathfrak{P}S \to \mathfrak{P}S$ に対して

$$\mathscr{I} \coloneqq \Big\{ A \subseteq S \ \Big|\ \forall x \in A.\ \ x \notin \sigma\big(A \setminus \{x\}\big) \Big\}$$

で $\mathscr{I}$ を定めると，

$$\forall I \in \mathscr{I}.\ \ \forall A \subseteq S.\ \big(|A| < |I| \ \Rightarrow\ I \not\subseteq \sigma(A)\big)$$

が成り立つ．

証明　$I \in \mathscr{I}$，$A \subseteq S$ が $|A| < |I|$ を満たすとする．$\big|A \setminus I\big|$ に関する帰納法による．

- $\big|A \setminus I\big| = 0$ のとき，$A \subseteq I$ であるから，$|A| < |I|$ より $A \subsetneq I$ が成り立ち，$x \in I \setminus A$ がとれる．この

x は $A \subseteq I \setminus \{x\}$ を満たすから (S2) より $\sigma(A) \subseteq \sigma\big(I \setminus \{x\}\big)$ であり，また $x \in I$，$I \in \mathscr{I}$ と $\mathscr{I}$ の定義より $x \notin \sigma\big(I \setminus \{x\}\big)$ であるから $x \notin \sigma(A)$ が成り立つ．したがって $x \in I \setminus \sigma(A)$ であり，$I \not\subseteq \sigma(A)$ が成り立つ．

- $\big|A \backslash I\big| \geq 1$ のとき，$y \in A \backslash I$ がとれて，$\Big|\big(A \backslash \{y\}\big) \backslash I\Big| < \big|A \backslash I\big|$ から帰納法の仮定より $I \not\subseteq \sigma\big(A \backslash \{y\}\big)$，すなわち $x \in I \setminus \sigma\big(A \setminus \{y\}\big)$ がとれる．
  - $x \notin \sigma(A)$ のとき，$x \in I \setminus \sigma(A)$ より $I \not\subseteq \sigma(A)$.
  - $x \in \sigma(A)$ のとき，$x \notin \sigma\big(A \setminus \{y\}\big)$ かつ $x \in \sigma(A) = \sigma\Big(\big(A \setminus \{y\}\big) \cup \{y\}\Big)$ から (S4) より $y \in \sigma\Big(\big(A \setminus \{y\}\big) \cup \{x\}\Big)$．(S1) および (S2) より $A \setminus \{y\} \subseteq \sigma\Big(\big(A \setminus \{y\}\big) \cup \{x\}\Big)$ であるから，結局 $A \subseteq \sigma\Big(\big(A \backslash \{y\}\big) \cup \{x\}\Big)$ が成り立つ．ここでさらに (S2) と (S3) より $\sigma(A) \subseteq \sigma\Big(\big(A \backslash \{y\}\big) \cup \{x\}\Big)$ が成り立つ．また，$\Big|\Big(\big(A \backslash \{y\}\big) \cup \{x\}\Big) \backslash I\Big| < \big|A \backslash I\big|$ から帰納法の仮定より $I \not\subseteq \sigma\Big(\big(A \backslash \{y\}\big) \cup \{x\}\Big)$ が成り立ち，したがって $I \not\subseteq \sigma(A)$ である．

  よっていずれの場合も $I \not\subseteq \sigma(A)$ が成り立つ．

以上より示された． ■

これで準備が整ったので，閉包公理を示すことにする．

定理 再掲：閉包公理

S を有限集合とする．$\sigma\colon\ \mathfrak{P}S \to \mathfrak{P}S$ が或る S 上のマトロイドの閉包演算子であるための必要十分条件は

(S1) $\quad \forall X \subseteq S.\ \ X \subseteq \sigma(X)$

(S2) $\quad \forall X \forall Y \subseteq S.\ \big(X \subseteq Y\ \Rightarrow\ \sigma(X) \subseteq \sigma(Y)\big)$

(S3) $\quad \forall X \subseteq S.\ \ \sigma(X) = \sigma\big(\sigma(X)\big)$

(S4) $\quad \forall X \subseteq S.\ \ \forall x \forall y \in S.\ \Big(\big(y \notin \sigma(X)\ \wedge\ y \in \sigma\big(X \cup \{x\}\big)\big)\ \Rightarrow\ x \in \sigma\big(X \cup \{y\}\big)\Big)$

である．

証明

[⇒]　マトロイド $M = (S, \mathscr{I})$ の閉包演算子 σ が (S1)，(S2)，(S3)，(S4) をすべて満たすことを示す．(S1) は補題 2.7.1 : 閉包演算子の増大性で，(S2) は補題 2.7.7 : 閉包演算子の単調性で，(S3) は系 2.7.11 : 閉包演算子の冪等律でそれぞれ既に示しているから，以降では (S4) を背理法により示す．

$y \notin \sigma(X)$ かつ $y \in \sigma\big(X \cup \{x\}\big)$ なる $X \subseteq S$ と $x, y \in S$ が，仮に $x \notin \sigma\big(X \cup \{y\}\big)$ を満たすとする．$y \notin \sigma(X)$ および (R2) より

$$\rho\big(X \cup \{y\}\big) = \rho(X) + 1$$

が，$y \in \sigma\big(X \cup \{x\}\big)$ より

$$\rho\big(X \cup \{x\} \cup \{y\}\big) = \rho\big(X \cup \{x\}\big)$$

が，$x \notin \sigma\big(X \cup \{y\}\big)$ および (R2) より

$$\rho\big(X \cup \{x\} \cup \{y\}\big) = \rho\big(X \cup \{y\}\big) + 1$$

がそれぞれ成り立つ．以上より

$$\begin{aligned}\rho\big(X \cup \{x\}\big) &= \rho\big(X \cup \{x\} \cup \{y\}\big) \\ &= \rho\big(X \cup \{y\}\big) + 1 \\ &= \rho(X) + 2\end{aligned}$$

であり $\rho\big(X \cup \{x\}\big) = \rho(X) + 2$ が成り立つが，これは (R2) に矛盾．ゆえに $x \in \sigma\big(X \cup \{y\}\big)$ である． ■

[⇐] (S1)，(S2)，(S3)，(S4) をすべて満たす有限集合 S と $\sigma\colon \mathfrak{P}S \to \mathfrak{P}S$ に対して

$$\mathscr{I} \coloneqq \Big\{A \subseteq S \;\Big|\; \forall x \in A.\ \ x \notin \sigma\big(A \setminus \{x\}\big)\Big\}$$

で定めた $\mathscr{I}$ が (I1)，(I2)，(I3) を満たすことを示す．

まず $\mathscr{I}$ の定義より $\varnothing \in \mathscr{I}$ であり，(I1) が成り立つ．

次に (I2) を背理法により示す．今仮に或る $X \in \mathscr{I}$ と $Y \subseteq X$ が $Y \notin \mathscr{I}$ を満たすとすると，$\mathscr{I}$ の定義より或る $y \in Y$ が存在して $y \in \sigma\big(Y \setminus \{y\}\big)$ である．$Y \setminus \{y\} \subseteq X \setminus \{y\}$ と (S2) より $\sigma\big(Y \setminus \{y\}\big) \subseteq \sigma\big(X \setminus \{y\}\big)$ であり，したがって $y \in \sigma\big(X \setminus \{y\}\big)$ が成り立つが，これは $X \in \mathscr{I}$ に矛盾．ゆえに任意の $X \in \mathscr{I}$ と $Y \subseteq X$ に対して $Y \in \mathscr{I}$ であり，(I2) が成り立つ．

最後に (I3) を示す．$X, Y \in \mathscr{I}$ が $|X| = |Y| + 1$ を満たすとすると，補題 2.7.12 より $X \not\subseteq \sigma(Y)$，すなわち $x \in X \setminus \sigma(Y)$ がとれる．この x は $x \notin \sigma(Y) = \sigma\Big(\big(Y \cup \{x\}\big) \setminus \{x\}\Big)$ を満たし，また $Y \in \mathscr{I}$ であるから，任意に $z \in Y \cup \{x\}$ をとると $z \notin \sigma\big(Y \setminus \{z\}\big)$ が成り立つ．このとき，(S4) の対偶

$$\forall X \subseteq S.\ \ \forall y \forall z \in S.\ \Big(x \notin \sigma\big(X \cup \{y\}\big) \ \Rightarrow\ y \in \sigma(X) \ \vee\ y \notin \sigma\big(X \cup \{x\}\big)\Big)$$

を用いると $x \notin \sigma(Y) = \sigma\Big(\big(Y \setminus \{z\}\big) \cup \{z\}\Big)$ より $z \in \sigma\big(Y \setminus \{z\}\big)$ または $z \notin \sigma\Big(\big(Y \setminus \{z\}\big) \cup \{x\}\Big)$ が成り立つが，前者は既に掲げた $z \notin \sigma\big(Y \setminus \{z\}\big)$ に反するから，$z \notin \sigma\Big(\big(Y \setminus \{z\}\big) \cup \{x\}\Big)$ が成り立つことになる．$\big(Y \setminus \{x\}\big) \cup \{z\} \subseteq \big(Y \setminus \{z\}\big) \cup \{x\}$ と (S2) より $\sigma\Big(\big(Y \setminus \{x\}\big) \cup \{z\}\Big) \subseteq \sigma\Big(\big(Y \setminus \{z\}\big) \cup \{x\}\Big)$ が成り立ち，したがって $z \notin \sigma\Big(\big(Y \setminus \{x\}\big) \cup \{z\}\Big)$．$z \in Y \cup \{x\}$ は任意であったので，

$$\forall z \in Y \cup \{x\}.\ \ z \notin \sigma\Big(\big(Y \setminus \{x\}\big) \cup \{z\}\Big)$$

が成り立ち，したがって $Y \cup \{x\} \in \mathscr{I}$ である．ゆえに，$|X| = |Y| + 1$ なる $X, Y \in \mathscr{I}$ に対し，或る $x \in Y \setminus X$ が存在して $Y \cup \{x\} \in \mathscr{I}$ を満たし，(I3) が成り立つ．

以上より $(S, \mathscr{I})$ はマトロイドである． ■

定理 2.7.13 閉包の平坦集合としての最小性

マトロイド $M = (S, \mathscr{I})$，M の閉包演算子 σ，$A \subseteq S$ に対して，$\sigma(A)$ は A を部分集合とする最小の平坦集合である．すなわち $\mathscr{F}_A \coloneqq \{F \in \operatorname{Flat} M \mid A \subseteq F\}$ として $\operatorname{minl} \mathscr{F}_A = \{\sigma(A)\}$ である．

証明　まず $\sigma(A) \in \mathscr{F}_A$ を示す．補題 2.7.1 : 閉包演算子の増大性より $A \subseteq \sigma(A)$ が成り立つ．また補題 2.7.3 より $\sigma(A) \in \operatorname{Flat} M$ が成り立つ．ゆえに $\sigma(A) \in \mathscr{F}_A$．

次に任意の $X \in \mathscr{F}_A$ に対して $\sigma(A) \subseteq X$ が成り立つことを示す．$X \in \mathscr{F}_A$ をとると $A \subseteq X$ かつ $X \in \operatorname{Flat} M$ である．ここで $x \in \sigma(A)$ とすると $x \sim A$ であり，$x \sim A$ および $A \subseteq X$ から補題 2.7.6 より $x \sim X$．そして $x \sim X$ と補題 2.7.2 より $x \in X$ が成り立つ．したがって $\sigma(A) \subseteq X$ である．

以上より $\sigma(A)$ は $\mathscr{F}_A$ の包含関係に関する最小元であり，$\operatorname{minl} \mathscr{F}_A = \{\sigma(A)\}$ である．■

補題 2.7.14 平坦集合同士の共通部分の平坦性

マトロイド $M = (S, \mathscr{I})$ に対し，

$$\forall X \forall Y \in \operatorname{Flat} M.\ \ X \cap Y \in \operatorname{Flat} M$$

が成り立つ．さらに，一般に

$$\forall \mathscr{A} \subseteq \operatorname{Flat} M.\ \ \bigcap \mathscr{A} \in \operatorname{Flat} M$$

が成り立つ．

証明　$X, Y \in \operatorname{Flat} M$ とする．平坦性より $\sigma(X) = X$ および $\sigma(Y) = Y$ である．$X \cap Y \subseteq X$ と (S2) より $\sigma(X \cap Y) \subseteq \sigma(X)$，同様に $\sigma(X \cap Y) \subseteq \sigma(Y)$ であるから，$\sigma(X \cap Y) \subseteq \sigma(X) \cap \sigma(Y)$ が成り立つ．したがって (S1) より

$$\begin{aligned} X \cap Y &\subseteq \sigma(X \cap Y) \\ &\subseteq \sigma(X) \cap \sigma(Y) = X \cap Y \end{aligned}$$

であり，$X \cap Y = \sigma(X \cap Y)$ が成り立つ．一般の場合もほぼ同様. ■

補題 2.7.15 共通部分としての閉包

マトロイド $M = (S, \mathscr{I})$ に対し，

$$\forall A \subseteq S.\ \ \sigma(A) = \bigcap \{F \in \operatorname{Flat} M \mid A \subseteq F\}$$

が成り立つ．すなわち，任意の $A \subseteq S$ に対して $\sigma(A)$ は A を包むすべての平坦集合の共通部分である．

証明　$A \subseteq S$ とし，$\mathscr{F}_A \coloneqq \{F \in \operatorname{Flat} M \mid A \subseteq F\}$ とおく．(S1) : $A \subseteq \sigma(A)$ および補題 2.7.3 : 閉包の平坦

性より $\sigma(A) \in \mathscr{F}_A$ であり，$\bigcap \mathscr{F}_A \subseteq \sigma(A)$ は明らか．

$x \in \sigma(A)$ とすると $x \sim A$ および $A \subseteq \bigcap \mathscr{F}_A$ から補題 2.7.6 より $x \sim \bigcap \mathscr{F}_A$ すなわち $x \in \sigma\Big(\bigcap \mathscr{F}_A\Big)$ であるが，補題 2.7.14 より $\bigcap \mathscr{F}_A \in \operatorname{Flat} M$ であり，さらに系 2.7.4 より $\mathscr{F}\Big(\bigcap \mathscr{F}_A\Big) = \bigcap \mathscr{F}_A$ であるから結局 $x \in \bigcap \mathscr{F}_A$ である．したがって $\sigma(A) \subseteq \bigcap \mathscr{F}_A$．

以上より，$\sigma(A) = \bigcap \mathscr{F}_A$ が成り立つ． ■

2.8 周に関する性質

補題 2.8.1 周の簡単な性質

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，以下がそれぞれ成り立つ．

(1) 従属集合は或る周を包む：$\forall A \in \mathfrak{P}S \setminus \mathscr{I}.\ \exists C \in \mathscr{C}.\ C \subseteq A$

(2) 周の真部分集合はすべて独立：$\forall C \in \mathscr{C}.\ \forall x \in C.\ C \setminus \{x\} \in \mathscr{I}$

(3) 周の階数は大きさより 1 小さい：$\forall C \in \mathscr{C}.\ \rho(C) = |C| - 1$

(4) $\forall C \in \mathscr{C}.\ |C| \leq \rho(S) + 1$

(5) 周が存在しないことと基が S のみであることは同値：$\mathscr{C} = \varnothing \Leftrightarrow \mathscr{B} = \{S\}$

(6) 相異なる周の一方が他方を真に包むことはない：$\forall C_1 \forall C_2 \in \mathscr{C}.\ \big(C_1 \subseteq C_2 \Rightarrow C_1 = C_2\big)$

証明 いずれも自明である． ■

補題 2.8.2

マトロイド $M = \big(S, \mathscr{I}\big)$ と M の周族 $\mathscr{C}$ に対し，

$$\forall C_1 \forall C_2 \in \mathscr{C}.\ \Big(C_1 \neq C_2 \Rightarrow \forall z \in C_1 \cap C_2.\ \exists C_3 \in \mathscr{C}.\ C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}\Big)$$

が成り立つ．

証明 背理法による．すなわち，或る $C_1 \neq C_2$ なる $C_1, C_2 \in \mathscr{C}$ と或る $z \in C_1 \cap C_2$ に対して，$C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}$ なる $C_3 \in \mathscr{C}$ が存在しないと仮定する．補題 2.8.1(1) の対偶より $(C_1 \cup C_2) \setminus \{z\} \in \mathscr{I}$ であ

るから，

$$\begin{aligned}\rho\big((C_1 \cup C_2) \setminus \{z\}\big) &= \big|(C_1 \cup C_2) \setminus \{z\}\big| \\ &= |C_1 \cup C_2| - 1\end{aligned}$$

が成り立つ．また $C_1, C_2 \in \mathscr{C}$ と補題 2.8.1(3) より $\rho(C_1) = |C_1| - 1$ および $\rho(C_2) = |C_2| - 1$ であり，(R3′)：劣モジュラ律より

$$\begin{aligned}\rho(C_1 \cup C_2) + \rho(C_1 \cap C_2) &\leq \rho(C_1) + \rho(C_2) \\ &= |C_1| + |C_2| - 2 \\ &= |C_1 \cup C_2| + |C_1 \cap C_2| - 2\end{aligned}$$

が成り立つ．ここで (R2′) より $\rho(C_1 \cup C_2) \geq \rho\big((C_1 \cup C_2) \setminus \{z\}\big) = |C_1 \cup C_2| - 1$ であるから

$$\begin{aligned}\rho(C_1 \cap C_2) &\leq |C_1 \cup C_2| + |C_1 \cap C_2| - 2 - \rho(C_1 \cup C_2) \\ &\leq |C_1 \cup C_2| + |C_1 \cap C_2| - 2 - \big(|C_1 \cup C_2| - 1\big) \\ &= |C_1 \cap C_2| - 1\end{aligned}$$

より $\rho(C_1 \cap C_2) < |C_1 \cap C_2|$ となるが，$C_1 \neq C_2$ より $C_1 \cap C_2 \subsetneq C_1$ であり，補題 2.8.1(2) より $C_1 \cap C_2 \in \mathscr{I}$，すなわち $\rho(C_1 \cap C_2) = |C_1 \cap C_2|$ が成り立つので矛盾である．ゆえに，任意の $C_1 \neq C_2$ なる $C_1, C_2 \in \mathscr{C}$ と $z \in C_1 \cap C_2$ に対し，$C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}$ なる $C_3 \in \mathscr{C}$ が存在する． ■

補題 2.8.3

マトロイド $M = (S, \mathscr{I})$ と M の周族 $\mathscr{C}$ に対し，

$$\forall A \in \mathscr{I}.\ \forall x \in S.\ \Big|\big\{C \in \mathscr{C} \bigm| C \subseteq A \cup \{x\}\big\}\Big| \leq 1$$

が成り立つ．すなわち，任意の $A \in \mathscr{I}$ と $x \in S$ に対して，$A \cup \{x\}$ に包まれる周は高々 1 つである．

証明　今仮に $A \in \mathscr{I}$，$x \in S$ とし，$C_1 \neq C_2$ なる $C_1, C_2 \in \mathscr{C}$ が $C_1 \in A \cup \{x\}$，$C_2 \in A \cup \{x\}$ を満たすとする．このとき $C_1 \cup C_2 \in A \cup \{x\}$ である．また $x \notin C_1$ と仮定すると $C_1 \subseteq A$ であり，(I2) より $C_1 \in \mathscr{I}$ となって矛盾するので $x \in C_1$，同様に $x \in C_2$ も成り立つ．したがって $x \in C_1 \cap C_2$ であり，補題 2.8.2 より $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$ なる $C_3 \in \mathscr{C}$ が存在する．この C_3 は $(C_1 \cup C_2) \setminus \{x\} \subseteq A$ より $C_3 \subseteq A$ を満たし，(I2) より $C_3 \in \mathscr{I}$ となって矛盾．ゆえに $A \cup \{x\}$ に包まれる周は高々 1 つである． ■

系 2.8.4

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に対し，

$$\forall B \in \mathscr{B}.\ \forall x \in S \setminus B.\ \exists! C \in \mathscr{C}.\ C \subseteq B \cup \{x\}$$

が成り立つ．すなわち，任意の基 $B \in \mathscr{B}$ と $x \in S \setminus B$ に対して $B \cup \{x\}$ に包まれる周が一意的に存在する．

証明　$B \in \mathscr{B}$，$x \in S \setminus B$ に対し，$B \subsetneq B \cup \{x\}$ と B の極大性より $B \cup \{x\} \in \mathscr{I}$ であり，補題 2.8.1(1) より $C \subseteq B \cup \{x\}$ なる $C \in \mathscr{C}$ が存在するが，このような C は補題 2.8.3 より一意的である．■

定義 2.8.5 基本周

マトロイド $M = \big(S, \mathscr{I}; \mathscr{B}, \rho, \sigma, \mathscr{C}\big)$ に於いて，基 $B \in \mathscr{B}$ および $x \in S \setminus B$ に対して一意的に存在する $C \subseteq B \cup \{x\}$ なる周 $C \in \mathscr{C}$ を，x と B による**基本周** (fundamental circuit) と呼び，$\mathrm{C}\big(x, B\big)$ と書く．

ところで，補題 2.8.2 はさらに強い主張にすることができる．それが次の**強周公理** (strong circuit axiom) である．

定理 2.8.6 強周公理

マトロイド $M = \big(S, \mathscr{I}\big)$ と M の周族 $\mathscr{C}$ に対し，

$$\forall C_1 \forall C_2 \in \mathscr{C}.\ \Big(C_1 \neq C_2\ \Rightarrow\ \forall x \in C_1 \cap C_2.\ \forall y \in C_1 \setminus C_2.\ \exists C_0 \in \mathscr{C}.\ \big(y \in C_0\ \wedge\ C_0 \subseteq (C_1 \cup C_2) \setminus \{x\}\big)\Big)$$

が成り立つ．

証明　今仮に或る $C_1 \neq C_2$ なる $C_1, C_2 \in \mathscr{C}$ と $x \in C_1 \cap C_2$，$y \in C_1 \setminus C_2$ が存在して，$y \in C_3$ かつ $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$ なる C_3 が存在しないとする．その中でも $C_1 \cup C_2$ が極小となるようなものを選ぶ．このとき，補題 2.8.2 より $y \notin C_3$ かつ $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$ なる $C_3 \in \mathscr{C}$ が存在する．この C_3 は周の極小性より $C_3 \setminus C_1 \neq \varnothing$ を満たすから $C_3 \cap \big(C_2 \setminus C_1\big) \neq \varnothing$ を満たし，したがって $z \in C_3 \cap \big(C_2 \setminus C_1\big)$ がとれる．

このとき $z \in C_2 \cap C_3$，$x \in C_2 \setminus C_3$ であり，また $y \in C_1$ かつ $y \in C_2 \cup C_3$ より $C_2 \cup C_3 \subsetneq C_1 \cup C_2$．$C_1 \cup C_2$ の選び方より，$C_2 \cup C_3$ に対しては或る $C_4 \in \mathscr{C}$ が存在して $x \in C_4$ かつ $C_4 \subseteq (C_2 \cup C_3) \setminus \{z\}$ を満たす．

さらに，$x \in C_1 \cap C_4$，$y \in C_1 \setminus C_4$ であり，また $z \in C_2$ かつ $z \notin C_1 \cup C_4$ より $C_1 \cup C_4 \subsetneq C_1 \cup C_2$．やはり $C_1 \cup C_2$ の選び方より，或る $C_5 \in \mathscr{C}$ が存在して $y \in C_5$ かつ $C_5 \subseteq (C_1 \cup C_4) \setminus \{x\}$ が成り立つ．

ところが $C_1 \cup C_4 \subsetneq C_1 \cup C_2$ より，この C_5 は $y \in C_5$ かつ $C_5 \subseteq (C_1 \cup C_2) \setminus \{x\}$ を満たし，矛盾．■

さて，周公理を示そう．

定理 2.8.7 周公理

S を有限集合とする．$\mathscr{C}$ が或る S 上のマトロイドの周族であるための必要十分条件は

(C1) $\quad \forall C_1 \forall C_2 \in \mathscr{C}.\, \big(C_1 \neq C_2 \;\Rightarrow\; C_1 \not\subseteq C_2\big)$

(C2) $\quad \forall C_1 \forall C_2 \in \mathscr{C}.\, \Big(C_1 \neq C_2 \;\Rightarrow\; \forall z \in C_1 \cap C_2.\;\; \exists C_3 \in \mathscr{C}.\;\; C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}\Big)$

である．

証明

[⇒] 補題 2.8.1(6) および補題 2.8.2 で既に示した． ■

[⇐] (C1)，(C2) を満たす $\mathscr{C} \subseteq \mathfrak{P}S$ に対し，

$$\begin{array}{rccc} \rho\colon & \mathfrak{P}S & \longrightarrow & \mathbf{N} \\ & \cup & & \cup \\ & A & \longmapsto & |A| - \Big|\big\{a \in A \;\big|\; \exists C \in \mathscr{C}.\, (a \in C \;\wedge\; C \subseteq A)\big\}\Big| \end{array}$$

で定義した ρ が (R1)，(R2)，(R3) を満たすことを示せば，階数公理より十分である．

まず (R1) : $\rho(\varnothing) = 0$ は明らか．

次に (R2) : $\forall X \subseteq S.\;\; \forall y \in S.\;\; \rho(X) \leq \rho\big(X \cup \{y\}\big) \leq \rho(X) + 1$ を示す．$X \subseteq S$ と $y \in S$ に対し，

- $y \in X$ のとき，自明．
- $y \notin X$ のとき，

$$\rho\big(X \cup \{y\}\big) = \big|X \cup \{y\}\big| - \Big|\big\{a \in X \cup \{y\} \;\big|\; \exists C \in \mathscr{C}.\, \big(a \in C \;\wedge\; C \subseteq X \cup \{y\}\big)\big\}\Big|$$

であるから！要加筆！

最後に (R3) を示す．$X \subseteq S$ が $\rho\big(X \cup \{y\}\big) = \rho\big(X \cup \{z\}\big) = \rho(X)$ を満たすとすると，ρ の定義より $y \in C_1$ かつ $C_1 \subseteq X \cup \{y\}$ なる $C_1 \in \mathscr{C}$ と $z \in C_2$ かつ $C_2 \subseteq X \cup \{z\}$ なる $C_2 \in \mathscr{C}$ が存在する．したがって $\rho\big(X \cup \{y\} \cup \{z\}\big) = \rho(X)$ が成り立つ． ！要加筆！

以上より，ρ は (R1)，(R2)，(R3) を満たす． ！要加筆！ ■