平成7年度(第17回)数学入門公開講座テキスト(京都大学数理解析研究所, 平成7年8月7日～8月11日開催)

数学入門公開講座

平成7年8月7日（月）から8月11日（金）まで

京都大学数理解析研究所

講師及び内容

1．p 進数と整数論（6時間15分）

京都大学数理解析研究所・助手　辻　　雄

p 進数（p は素数）は、今世紀の初頭 K. Hensel によって導入されたもので、実数が少数展開できるように、p 進数は $\sum_{n=n_0}^{\infty} a_n p^n$（$a_n = 0, 1, \cdots, p-1$, n_0 はある整数）という展開を持つ。実数の世界ではこの無限和は収束しないが、p 進数の世界では収束する。有理数に関する問題、例えば不定方程式、を考えるとき、p 進数で同じ問題を解いてみることによって、もとの有理数の場合も解けることが多く、現在では整数論における基本的な手法となっている。この講義では、p 進数の概念およびその基本的な性質について述べた後、関連する整数論の問題を幾つか紹介する予定である。

2．微分方程式とその応用（6時間15分）

京都大学数理解析研究所・助手　谷口　雅治

微分方程式は様々な自然現象をよりよく記述し得る有用な道具の一つである。化学や生物学におけるある種の形態形成過程においては一様にみえる初期状態から不均一な空間パターンが自律的に生じる現象が知られている。この現象を説明するモデルとして反応拡散方程式をもちいたチューリングの拡散不安定性の仮説が知られている。

本講義ではこの仮説を中心に話題を展開する予定です。

3．マトロイド理論とアルゴリズム（6時間15分）

京都大学数理解析研究所・助手　岩田　覚

マトロイドとは、ベクトル集合の線形独立性・線形従属性の組合せ論的側面を抽象化して得られたものであるが、効率的に解くことのできる組合せ最適化問題を統一的に扱う枠組として、工学的にも極めて重要な概念である。本講座では、多くの具体例を織り交ぜながら、マトロイドに関する最適化問題が効率的に解ける仕組みについて解説する。

時　間　割

時間＼日	8月7日(月)	8日(火)	9日(水)	10日(木)	11日(金)
10：30～11：45	辻	辻	辻	辻	辻
11：45～13：00	休　憩				
13：00～14：15	谷口	谷口	谷口	谷口	谷口
14：15～14：45	休　憩				
14：45～16：00	岩田	岩田	岩田	岩田	岩田

平成7年度(第17回)数学入門公開講座テキスト(京都大学数理解析研究所, 平成7年8月7日～8月11日開催)

マトロイド理論とアルゴリズム

京都大学数理解析研究所・助　手　　岩　田　　覚

1995, AUGUST 7,8,9,10,11,　　14:45 ~ 16:00

マトロイド理論とアルゴリズム

岩田 覚

マトロイドは, 線型空間内のベクトル集合の一次独立・従属といった概念の組合せ論的な側面を抽象化して得られる公理系を満たすものとして定義されている. したがって, その具体例は身近なところにも沢山ある. 本講座では, それらの具体例に触れながら, マトロイドに関する理論のうち, 特に, 効率的なアルゴリズムの設計に関連した話題を取り上げる予定である.

1 マトロイド

有限集合 E とその部分集合族 $\mathcal{I}$ が以下の (I0)–(I2) を満たすとき, $(E,\mathcal{I})$ はマトロイドと呼ばれる.

(I0) $\emptyset \in \mathcal{I}$.

(I1) $I \subseteq J \in \mathcal{I} \Rightarrow I \in \mathcal{I}$.

(I2) $I, J \in \mathcal{I}$, $|I| < |J| \Rightarrow \exists e \in J - I$: $I \cup \{e\} \in \mathcal{I}$.

マトロイド $\mathbf{M} = (E, \mathcal{I})$ において, E を $\mathbf{M}$ の台集合, $\mathcal{I}$ を独立集合族という. 独立集合族 $\mathcal{I}$ の元 $I \in \mathcal{I}$ は, $\mathbf{M}$ の独立集合と呼ばれる.

独立集合のうちで極大なものを基と呼ぶ. 基の族を $\mathcal{B}$ と書き, $\mathbf{M}$ の基族と呼ぶ. 基族 $\mathcal{B}$ は以下の (B0)–(B1) を満たす.

(B0) $\mathcal{B} \neq \emptyset$.

(B1) $B, B' \in \mathcal{B}$, $e \in B - B' \Rightarrow \exists e' \in B' - B$: $(B - \{e\}) \cup \{e'\} \in \mathcal{B}$.

基はすべて元の数が等しい. この数をマトロイド $\mathbf{M}$ の階数という.

任意の部分集合 $X \subseteq E$ に対して,

$$\rho(X) = \max\{|X \cap I| \mid I \in \mathcal{I}\}$$

と定義する. この関数 ρ がマトロイド $\mathbf{M}$ の階数関数である. 階数関数 ρ は以下の (R0)–(R3) を満たしている.

(R0) $\rho(\emptyset) = 0$.

(R1) $\forall X \subseteq E$: $\rho(X) \leq |X|$.

(R2) $X \subseteq Y \Rightarrow \rho(X) \leq \rho(Y)$.

(R3) $\forall X, Y \subseteq E$: $\rho(X) + \rho(Y) \geq \rho(X \cap Y) + \rho(X \cup Y)$.

特に, (R3) は, 劣モジュラ性と呼ばれる性質で, マトロイドに関する効率的なアルゴリズムが正しく働くための仕掛けとして, 本質的な役割を果たしている.

ここでは, (I0)–(I2) によって, マトロイドを定義したが, (B0)–(B1) を満たす基族 $\mathcal{B}$ から, マトロイドを定義することもできる. この場合, 独立集合は, 基の部分集合として定義される. 同様に, (R0)–(R3) を満たす階数関数によって, マトロイドを定義することも可能である. 独立集合族は,

$$\mathcal{I} = \{I \mid \rho(I) = |I|\}$$

によって定められる.

独立でない E の部分集合は従属であると言われ, 極小な従属集合はサーキットと呼ばれる. 各部分集合 $X \subseteq E$ に対して,

$$\mathrm{cl}(X) = \{e \mid \rho(X) = \rho(X \cup \{e\})\}$$

と定義する. この関数 cl は閉包関数と呼ばれる. 任意の独立集合 $I \in \mathcal{I}$ と元 $e \in \mathrm{cl}(I) - I$ に対して, $I \cup \{e\}$ に含まれるサーキットが唯一つ存在する. これを基本サーキットと呼び, $C(I|e)$ と書くことにする.

以下に代表的なマトロイドの例を挙げる. それぞれについて, 基, 階数関数, サーキット, 閉包関数が何に対応するか考えてみよう.

行列的マトロイド 行列 A の列集合を E とし, 一次独立な列ベクトル集合に対応する列部分集合の全体を $\mathcal{I}$ とする. このとき, $(E,\mathcal{I})$ は (I0)-(I2) を満たし, マトロイドになる. このようにして得ることのできるマトロイドを行列的マトロイドと呼ぶ.

グラフ的マトロイド 点集合 V, 枝集合 E を持つグラフ $G=(V,E)$ を考える. 枝集合の部分集合のうち, 閉路を含まないものの全体を $\mathcal{I}$ とすると, $\mathbf{M}(G)=(E,\mathcal{I})$ は (I0)-(I2) を満たし, マトロイドになる. このようにして得ることのできるマトロイドをグラフ的マトロイドと呼ぶ.

横断マトロイド 点集合 U,V, 枝集合 A からなる 2 部グラフ $G=(U,V;A)$ を考える. 端点を共有しない枝部分集合をマッチングという. 点集合 U の部分集合で, マッチングの U における端点集合となり得るものの全体を $\mathcal{I}$ とする. このとき, $(U,\mathcal{I})$ は (I0)-(I2) を満たし, マトロイドになる. こうして得られるマトロイド $(U,\mathcal{I})$ を横断マトロイドと呼ぶ.

2 貪欲算法

マトロイド $\mathbf{M}=(E,\mathcal{I})$ の各要素 $e \in E$ に 非負の "重み" $w(e)$ が与えられているとしよう. このとき, 重み最大の独立集合, すなわち, $w(I)=\sum_{e\in I} w(e)$ を最大にする独立集合 $I \in \mathcal{I}$ を求めることを考える.

もっとも素朴なアプローチは, 各要素を重みの大きい順に持って来て, 独立性を壊さない範囲で, 付け加えていくことだろう. アルゴリズムとして記述すると, 次のようになる.

1. $I \leftarrow \emptyset$; $Q \leftarrow E$;

2. $Q=\emptyset$ となるまで, 以下の (a)-(b) を繰り返す.

   (a) Q の中で, 重み最大の要素を e とする; $Q \leftarrow Q-\{e\}$;

   (b) もし $I \cup \{e\} \in \mathcal{I}$ であれば, $I \leftarrow I \cup \{e\}$.

実際, この単純なアルゴリズムで, 正しい答が見つかってしまう. すなわち, アルゴリズム終了時の I が最大重みの独立集合である.

このアルゴリズムは, 貪欲算法と呼ばれている. 行列のランクを Gauss 消去法で求めるのは, この貪欲算法の特殊な場合と解釈することもできる.

3 双対マトロイド

マトロイド $\mathbf{M} = (E, \mathcal{I})$ の基族 $\mathcal{B}$ に対して,

$$\mathcal{B}^* = \{E - B \mid B \in \mathcal{B}\}$$

とすると, $\mathcal{B}^*$ も (B0)–(B1) を満たす. すなわち, $\mathcal{B}$ を基族とする E 上のマトロイド $\mathbf{M}^*$ が定まる. このマトロイド $\mathbf{M}^*$ を $\mathbf{M}$ の双対マトロイドと呼ぶ. 双対マトロイド $\mathbf{M}^*$ の階数関数は ρ^* は, $\mathbf{M}$ の階数関数 ρ を用いて,

$$\rho^*(X) = |X| + \rho(E - X) - \rho(E)$$

と表される.

双対マトロイド $\mathbf{M}^*$ におけるサーキットを, $\mathbf{M}$ のコサーキットと呼ぶ. コサーキットはすべての基と空でない交わりを持っている. グラフ的マトロイドのコサーキットはグラフのカットセットに対応している.

行列的マトロイドの双対マトロイドは, 行列的マトロイドになる. すなわち, マトロイドが行列的であるという性質は, 双対に関して閉じている. これに対し, グラフ的マトロイドや横断マトロイドは, 双対に関して閉じてはいない. グラフ的マトロイド $\mathbf{M}(G)$ の双対マトロイド $\mathbf{M}^*(G)$ は, グラフ G が平面的であるとき, すなわち, 枝を交差させることなく G を平面に埋め込むことのできるとき, かつそのときに限って, グラフ的になることが知られている.

4 簡約・縮約・マイナー

マトロイド $\mathbf{M} = (E, \mathcal{I})$ と部分集合 $F \subseteq E$ に対して,

$$\mathcal{I}^F = \{I \mid I \subseteq F, I \in \mathcal{I}\}$$

は, 明らかに (I0)–(I2) を満たし, F を台集合とするマトロイド $(F, \mathcal{I}^F)$ を定める. このマトロイド $(F, \mathcal{I}^F)$ を, $\mathbf{M}$ の F への簡約といい, $\mathbf{M} \cdot F$ と表す.

続いて, 部分集合 $D \subseteq E$ による縮約を考えよう. 部分集合 $X \subseteq E - D$ に対して,

$$\rho_D(X) = \rho(X \cup D) - \rho(D)$$

とすると, 関数 ρ_D は (R0)–(R3) を満たす. すなわち, ρ_D を階数関数とする $E - D$ 上のマトロイド $\mathbf{M}/D$ が定まる. このマトロイド $\mathbf{M}/D$ を $\mathbf{M}$ の D による縮約と呼ぶ.

簡約と縮約とは互いに双対的な関係にある. すなわち, $F = E - D$ とすると,

$$\mathbf{M}/D = (\mathbf{M}^* \cdot F)^*$$

が成立している.

与えられたマトロイドに簡約と縮約とを繰り返して得られるマトロイドを $\mathbf{M}$ のマイナーと呼ぶ. マトロイドに関する様々な性質が, マイナーをに関して閉じている. 例えば, 行列的マトロイドのマイナーは, 常に行列的であるし, グラフ的マトロイドのマイナーも, 常にグラフ的である. この種の性質を, その禁止マイナーによって, 特徴づけるといった結果が沢山知られている. 代表的なものとして, グラフ G が平面的であるための必要十分条件が, $\mathbf{M}(G)$ がマイナーとして, $\mathbf{M}(K_5)$ および $\mathbf{M}(K_{3,3})$ を持たないことであるという Kuratowski の定理がある. ここで, K_5 は点の数が 5 の完全グラフであり, $K_{3,3}$ は両側の点の数がともに 3 の完全 2 部グラフである. なお, 横断マトロイドのマイナーは, 必ずしも横断マトロイドになるとは限らないことに注意する.

5 合併マトロイド

マトロイド $\mathbf{M}_1 = (E, \mathcal{I}_1)$ と $\mathbf{M}_2 = (E, \mathcal{I}_2)$ に対して,

$$\mathcal{I}_{1\vee 2} = \{I_1 \cup I_2 \mid I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}$$

と定義すると, $(E, \mathcal{I}_{1\vee 2})$ は (I0)–(I2) を満たし, マトロイドになる. このことは, 以下の様にして示すことができる. 定義より, (I0)–(I1) は自明なので, 専ら (I2) に注目する. また, マトロイド $\mathbf{M}_h$ における 階数関数, 基本サーキット, 閉包関数をそれぞれ, ρ_h, C_h, cl_h で表す $(h = 1, 2)$.

互いに素な $I_1 \in \mathcal{I}_1$ と $I_2 \in \mathcal{I}_2$ によって, $I = I_1 \cup I_2 \in \mathcal{I}_{1\vee 2}$ が得られているとしよう. 任意の部分集合 $Y \subseteq E$ に対して,

$$|I| = |I_1 \cap Y| + |I_2 \cap Y| + |I - Y| \leq \rho_1(Y) + \rho_2(Y) + |E - Y| \qquad (1)$$

が成立することに注意しておく.

有向グラフ $H = (E \cup \{t\}, A_1 \cup A_2)$ を

$$\begin{aligned} A_1 &= \{(i,j) \mid i \in \mathrm{cl}_1(I_1) - I_1,\ j \in C_1(I_1|i)\} \cup \{(i,t) \mid i \in E - \mathrm{cl}_1(I_1)\} \\ A_2 &= \{(i,j) \mid i \in \mathrm{cl}_2(I_2) - I_2,\ j \in C_2(I_2|i)\} \cup \{(i,t) \mid i \in E - \mathrm{cl}_2(I_2)\} \end{aligned}$$

によって定義する. この有向グラフ H 上で $S = E - I$ を出発し, A_1 の枝と A_2 の枝を交互に使う有向道を考える. その様な有向道で t に至るものが存在しないならば, S から到達可能な点集合を R とする. このとき, $|I_1 \cap R| = \rho_1(R)$, $|I_2 \cap R| = \rho_2(R)$ が成立し, $I \supseteq E - R$ より, $|I| = \rho_1(R) + \rho_2(R) - |E - R|$ を得る. ここで, (1) より, $|J| > |I|$ となるような $J \in \mathcal{I}_{1\vee 2}$ が存在し得ないことがわかる.

一方, t に至るものが存在するならば, それらのうちで枝数最小の P を用いて,

$$\begin{aligned} I'_1 &= (I_1 - \{\partial^- a \mid a \in P \cap A_1\}) \cup \{\partial^+ a \mid a \in P \cap A_1\} \\ I'_2 &= (I_2 - \{\partial^- a \mid a \in P \cap A_2\}) \cup \{\partial^+ a \mid a \in P \cap A_2\} \end{aligned}$$

とする. ただし, $\partial^+ a$ と $\partial^- a$ は, それぞれ, 枝 a の始点と終点を表す. 有向道 P の始点を s とすると, $I' = I'_1 \cup I'_2 = I \cup \{s\}$ となっている. さらに, $I'_1 \in \mathcal{I}_1$, $I'_2 \in \mathcal{I}_2$ を示すことができ, その結果として, $I' \in \mathcal{I}_{1\vee 2}$ を得る.

マトロイド $(E, \mathcal{I}_{1\vee 2})$ を $\mathbf{M}_1$ と $\mathbf{M}_2$ の合併マトロイドと呼び, $\mathbf{M}_1 \vee \mathbf{M}_2$ と書き表す. 上の議論が, $\mathbf{M}_1 \vee \mathbf{M}_2$ の階数関数を求めるアルゴリズムをも

与えていることに注意する. 実際, 合併マトロイドの階数関数 $\rho_{1\vee 2}$ は,

$$\rho_{1\vee 2}(X) = \min\{p(Y) \mid Y \subseteq X\} + |X|$$

と表される. ただし,

$$p(Y) = \rho_1(Y) + \rho_2(Y) - |Y|$$

である. 関数 p の劣モジュラ性より, その最小値を達成するものの全体は集合の包含関係に関する分配束をなす. 上の手続きで現れた R はこの分配束の最小元にあたる. 最大元を D とし, $E_- = R$, $E_0 = D - R$, $E_+ = E - D$ によって, 台集合 E の分割 $(E_+; E_0; E_-)$ を定める. これを, $\mathbf{M}_1 \vee \mathbf{M}_2$ に関する基本三分割と呼ぼう.

合併マトロイド $\mathbf{M}_1 \vee \mathbf{M}_2$ の双対マトロイドの階数関数 ${\rho_{1\vee 2}}^*$ が,

$${\rho_{1\vee 2}}^*(X) = \min\{p(Y) \mid Y \subseteq E - X\} - \min\{p(Z) \mid Z \subseteq E\}$$

となることにより, $\mathbf{M}_1 \vee \mathbf{M}_2$ の任意の基が $E_0 \cup E_+$ を含むことがわかる. 一方, 双対マトロイドの合併, すなわち, ${\mathbf{M}_1}^* \vee {\mathbf{M}_2}^*$ の全ての基は, $E_0 \cup E_-$ を含む.

6　応用 — Shannon のスイッチング・ゲーム

最後に, マトロイドの応用例として, Shannon のスイッチング・ゲームと呼ばれるグラフ上のゲームを紹介しよう. このゲームに関する問題は, 当初, グラフの言葉で提起されたが, マトロイド理論を用いることによって, 初めて解決された. 勿論, グラフの言葉に焼き直して初等的に説明することも可能だが, マトロイド理論によって, 見通しが良くなり, 問題の解決に結びついたといえよう.

グラフ $G = (V, E)$ とその上の 2 点 $u, v \in V$ が与えられているものとしよう. 二人のプレーヤー, 甲と乙が交互にグラフの枝集合に自分のラベルをつけていく. 既にラベルの付けられた枝にラベルをつけることはできない. 甲は, 自分のラベルのついた枝で u と v とを結ぶことを目的とする. 乙の目的は, これを妨害することである.

グラフ G に特別な枝 $a^* = (u, v)$ を付け加えてできるグラフ を $G' = (V, E \cup \{a^*\})$ とする. グラフ的マトロイド $\mathrm{M}(G')$ と自分自身との合併 $\mathrm{M}(G') \vee \mathrm{M}(G')$ に関する基本三分割 $(E_-; E_0; E_+)$ を考える. このとき, 以下の事実が知られている.

(i) $a^* \in E_-$ ならば, 甲に必勝法がある.

(ii) $a^* \in E_+$ ならば, 乙に必勝法がある.

(iii) $a^* \in E_0$ ならば, 先手に必勝法がある.

グラフ G と u, v とが与えられたときに, 上の (i)-(iii) のどれに相当するかを効率的に判定することもできる. 図 1 にグラフの例を載せておく. それぞれのグラフは (i)-(iii) のどれに当たるのだろうか? また, 必勝法は, どのようなものだろうか?

参考文献

[1] 伊理・藤重・大山: グラフ・ネットワーク・マトロイド, 産業図書, 東京, 1986.

[2] E. L. Lawler: *Combinatorial Optimization — Networks and Matroids*, Holt, Reinhart and Winston, New York, 1976.

[3] D. J. A. Welsh: *Matroid Theory*, Academic Press, London, 1976.

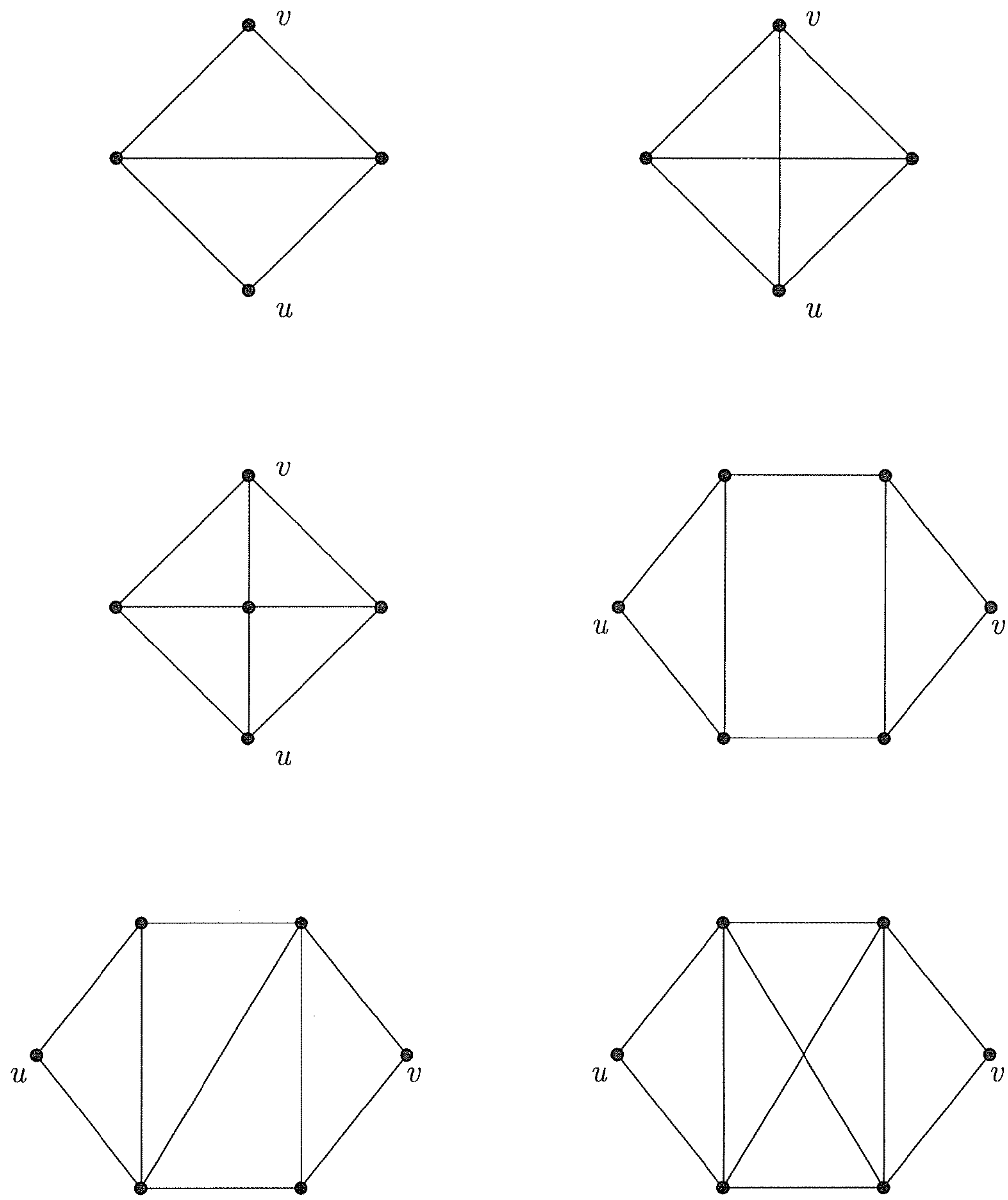

図 1. Shannon のスイッチング・ゲームの例

マトロイド理論とアルゴリズム

1995年8月10日
岩田 覚

参考文献

[1] 伊理・藤重・大山: *グラフ・ネットワーク・マトロイド*, 産業図書, 東京, 1986.

[2] 茨木: 離散最適化法とアルゴリズム, 岩波講座 応用数学, 岩波書店, 東京, 1993.

[3] 藤重: 離散数学, 岩波講座 応用数学, 岩波書店, 東京, 1993.

[4] 藤重 (編): 離散構造とアルゴリズム I, 近代科学社, 東京, 1992.

[5] 藤重 (編): 離散構造とアルゴリズム II, 近代科学社, 東京, 1993.

[6] 室田 (編): 離散構造とアルゴリズム III, 近代科学社, 東京, 1994.

[7] 室田 (編): 離散構造とアルゴリズム IV, 近代科学社, 東京, 1995.

[8] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin: *Network Flows — Theory, Algorithms, and Applications*, Prentice Hall, Englewood Cliffs, 1993.

[9] S. Fujishige: *Submodular Functions and Optimization*, North-Holland, Amsterdam, 1991.

[10] E. L. Lawler: *Combinatorial Optimization — Networks and Matroids*, Holt, Reinhart and Winston, New York, 1976.

[11] J. G. Oxley: *Matroid Theory*, Oxford University Press, Oxford, 1992.

[12] D. J. A. Welsh: *Matroid Theory*, Academic Press, London, 1976.

[13] N. White (ed.): *Theory of Matroids*, Cambridge University Press, Cambridge, 1986.

[14] N. White (ed.): *Combinatorial Geometries*, Cambridge University Press, Cambridge, 1987.

[15] N. White (ed.): *Matroid Applications*, Cambridge University Press, Cambridge, 1991.

[16] R. J. Wilson: *Introduction to Graph Theory*, 3rd ed., Longman, London, 1985. (斉藤・西関 (訳): *グラフ理論入門*, 近代科学社, 東京, 1985.)