科学・技術の研究課題への数学アプローチ

―数学モデリングの基礎と展開―

編集委員

西井 龍映（委員長）

栄 伸一郎　　岡田 勘三　　落合 啓之

小磯 深幸　　斎藤 新悟　　白井 朋之

2013年2月

About MI Lecture Note Series

The Math-for-Industry (MI) Lecture Note Series is a successor to the COE Lecture Notes, published for the 21st COE Program "Development of Dynamic Mathematics with High Functionality", sponsored by Ministry of Education, Culture, Sports, Science and technology-Japan (MEXT) (From 2003 to 2007).

The MI series reports lectures given by scholars invited under the following two programs: "Training Program of Ph.D. and new Master's in Mathematics as Required by Industry", adopted as a Support Program for Improving Gradute School Education by MEXT (from 2007 to 2009); and Education-and-Research Hub for Mathematics-for-Industry", newly adopted as a Global COE Program by MEXT (from 2008 to 2012).

July 2008
Masato Wakayama
Global COE Program "Education-and-Research Hub for Mathematics-for-Industry"
Program Leader

はじめに

九州大学マス・フォア・インダストリ研究所 (IMI) は，設立以来ようやく 2 年に至ろうとしているところです.

本書は，IMI の所員をはじめ，IMI が主催・共催する研究集会での基調講演や，毎月第 3 水曜日に定例開催している IMI Colloquium での講演をお引き受けくださったり，すでにご予定くださっている産業界の研究者の方々のご好意とご協力を得て実現したものです. テーマは各執筆者の専門と関心にもとづいて選定し，そこにある一つあるいはいくつかの課題に焦点をあて，課題解決に取り組むための数学モデリングに関する手引きを作成しました．もとより応用数学・産業数学の世界はきわめて広大であり，本書で取り上げている内容はそのなかのほんのわずかのテーマでしかありません．しかしながら，たとえ一部であろうとも，どのような数学が諸科学分野や産業に貢献しているか，また，今後貢献する可能性があるかなどを紹介することは，十分に意義深いと思われました．これが本書の出発点であり目的です．読者としては，第一に数学・数理科学に関心のある学部学生・大学院生を念頭におき，次に企業の方々，最後に教員という順序を想定して編集方針を定めました．そのため，執筆者は数学科 2, 3 年生程度の知識を仮定した原稿作りに努めることになりました.

本書は IMI 設立のための準備段階の時期より出版を計画していたものですが，言うは易く行なうは難し，の典型でありました．本書の作成のため IMI において編集委員会を設置したのは，昨年の 4 月です．西井が編集委員会委員長を務め，以下のような方針で作成作業にはいることになりました.

執筆者：【基礎編】・IMI 教員及び研究員有志（下記を参照）
【応用編】・IMI 教員（岡田（責任者），穴井）
・IMI Colloquium での講演者
・文部科学省数学連携 WS の keynote speaker 等

基礎編の内容と担当者：
【代数系】暗号などに使える代数（群・環・体，表現論）：
落合（責任者），高木，バードル，モロゾフ，若山
【幾何系】幾何解析，トポロジー，可積分系，数理物理：
小磯（責任者），梶原，佐伯，平岡
【解析系】数値解析，PDE，フーリエ解析，関数解析：
栄（責任者），木村，田上，千葉，手老
【確率統計】統計モデル，モデル選択，乱数，確率論，マルコフ連鎖，保険数理：
白井（責任者），斎藤，西井，二宮，増田
【応用数学】最適化（線形（非線形）計画，整数計画，制御など）：神山，脇
組合せ・学習理論・論理数学：溝口
物理数学：福本　　一様分布論：手塚
タンパク質複合体予測：丸山　　産業における数学史：高瀬

また，原稿のスタイルファイルの作成と取りまとめは，IMI 学術研究員の斎藤が行いました.

出来上がったものが十分に目的に沿うものかどうか，心もとない点もありますが，多くの方に手にして頂けることを願ってやみません．また，今回は試験的な取り組みと考え，これを基盤に，次年度にはさらなる内容の充実をはかってまいりたいと考えています．

本書をご覧になり拝読くださった方々には，ぜひ忌憚のないご意見やコメントをお寄せ下さいますよう，よろしくお願い申し上げます．

2013年2月10日

九州大学マス・フォア・インダストリ研究所長
若山　正人

目　次

基礎編第 5 部：応用数学

応用編

Computer Graphicsにおける運動の記述

落合　啓之

九州大学マス・フォア・インダストリ研究所

1　数学が展開されるインフラストラクチャー（集合・関数・位相）

数学では習慣的に, 扱う対象を集合を用いて表し, 関係を写像を用いて表す. これらの言葉遣いを紹介する.

1.1　集合：外延的記法と内包的記法

集合を表すには

- 要素を書き並べる方法（外延的記法）
- 条件を書き表す方法（内包的記法）

の 2 通りの方法がある.

例 1.1 曲面を表すときに, $x = x(u, v)$, $y = y(u, v)$, $z = z(u, v)$ とパラメータ表示するのは外延的記法にあたる. $f(x, y, z) = 0$ と陰関数で表すのは内包的記法である.

内包的記法では, それぞれの要素がその集合に属しているかどうかがわかりやすい. その一方で, 外延的記法では, その集合の要素を全て取ってくることがしやすい. 従って例えば, 2 つの集合 S_1, S_2 が包含関係 $S_1 \subset S_2$ を満たしていることを示すのに, S_1 が外延的記法で書かれ, S_2 が内包的記法で書かれていれば, その証明は易しい. なお, 観測によるデータにはノイズなどが含まれるため, ぴったりと等号が成立していない場合を許容する必要がある.

これらの 2 つの記法には, 長所とそれの裏返しである短所があるので, 同じ集合が両方の記法を持つことが示されると有用である.

例 1.2 例えば「方程式を解く」という行為は, 内包的記法で書かれたものを外延的に書く, という作業である. その特別な場合として, ある方程式に解がない（例えば, フェルマーの最終定理), ある条件を満たすものは一つしかない（例えば, ポアンカレ予想）などの例が挙げられる.

例 1.3 与えられたデータ集合 $D = \{(x_i, y_i) \mid i = 1, 2, \ldots, N\}$ の間に相関（法則性）を見つけて, $D \subset \{(x, y) \mid f(x, y) = 0\}$ の形に書くことは, 外延的に書かれた集合を内包的に記述することにつながっている.

1.2 関数

1.2.1 関数と写像

2 つの集合 X と Y が与えられているとする. X の各元 x に対して, Y の元 $f(x)$ がただ一つ対応しているとき, その対応付けを写像 $f\colon X \to Y$ という. 特に値の集合 Y が数値からなるとき, 写像のことをしばしば関数と呼ぶ. 関数とは写像の特別なものである.

例 1.4 飲み物の自動販売機のボタンの集合を X, 飲み物の集合を Y とすると, 押したボタンに対応して出てくる飲み物を与える対応は**写像**になる. ボタンを押せば必ず飲み物が一つ出てくる, いつボタンを押しても同じボタンに対しては同じ飲み物が出てくるという性質を抽象化したものが写像の性質である.

例 1.5 実数列 $\{a_n\}$ は, 写像 $\mathbb{N} \to \mathbb{R}$ と考えられる. 3 次元空間の N 点のデータのなす集合は, $\mathbb{R}^{3N}$ と表示されるが, 写像 $\{1, \ldots, N\} \to \mathbb{R}^3$ とも考えられるし, 写像 $\{1, \ldots, 3N\} \to \mathbb{R}$ とも考えられる.

1.2.2 平均

データ $a_1, \ldots, a_n$ に対して,

$$(a_1 + \cdots + a_n)/n$$

を平均という. この操作には, 「(交換法則と結合法則を満たすような) 加法」と, 「($1/n$ 倍するという) スカラー倍の操作」が必要である. 従って, 値が線形空間 (の部分集合) に属していることが必要である. 例えば, あるサッカーチームの成績が「勝ち, 負け, 引分」の 3 種類からなっていた場合, その成績の平均を求めるという問題には標準的な意味がつかない. 勝 $= 3$, 負 $= 0$, 分 $= 1$ という数値の割り当てを決めれば, 平均の数値を算出することができるが, この割り当てルールが妥当かどうかはまた別に議論が必要である.

また, 集められたデータが数値で表されていると, 安易に平均を考えがちであるが, 和や平均に意味がつかないことがある. 例えば, 曲面上に乗っているデータを入れ物の空間の中で平均すると, 曲面をはみ出してしまう. 従って, 何らかの工夫が必要となる. ここから曲面上で直線 (線形補間) の役割をする「測地線」「接続」の概念の必要性が生ずる. 一方で, 滑らかな短い曲線や小さい曲面片は直線や平面などの線形で十分よく近似されるので, 線形補間に十分な合理性がある. からだの動きや顔の表情などをモーションキャプチャーで集めたデータは, 高い次元 (例えば 1 万次元) の空間の中の低い次元の集合をなすと考えられるが, 大域的には非線形的であるものの局所的には線形的 (blendshape) と考えられ, これらの考え方が制作で持ちいられている.

1.3 全射, 単射

1.3.1 定義

定義 1.6 写像 $f\colon X \to Y$ に対する性質をいくつか定義する. 任意の $y \in Y$ に対して, ある $x \in X$ が存在して, $y = f(x)$ となるとき, f は全射である (surjective), あるいは, 上への写像 (onto) であるという. $x, x' \in X$ が $x \neq x'$ であれば, $f(x) = f(x')$ を満たすとき, f は単射 (injective) である, あるいは 1 対 1 の写像 (one-to-one) であるという. 全射かつ単射な写像を全単射 (bijective) という. 全単射のことを 1 対 1 写像ということもあるので注意.

例 1.7 自販機の例 1.4 を続けよう. f が**全射**であるとは, この自販機が飲み物の集合 Y を網羅していて, どの飲み物もこの自販機で買えることを意味する. f が**単射**であるとは, 異なるボタンからは異なる飲み物が出てくること, すなわち, 同じ飲み物が出てくるボタンが一つしかないことを意味する. この例で見るように, 全射であることと単射であることは異なる性質である.

全射であることと単射であることは一般には無関係（独立）である. しかし, 次の特別な場合には, 全射であることと単射であることが同値になる :

(1) X と Y が有限集合で, 元の個数が等しいとき.

(2) X と Y が線形空間で, 次元が有限で等しく, さらに $f\colon X \to Y$ が線形写像のとき.

(2') 特に A が正方行列で, 列ベクトルに対する行列のかけ算 $v \mapsto Av$ による写像のとき.

大学 1 年生の講義では, 全射や単射を学習するのと同時期に (2') の事実を学習するので, 全射と単射が密接な関係にあると印象づけられやすいが, その状況はむしろ例外的であることに注意しておきたい. なお, 無限集合や無限次元では (1)(2) のような事実は成り立たない. また, 格子（有限階数の自由 $\mathbb{Z}$ 加群）と有限次元線形空間（体上の有限階数の自由加群）は, 定義が似通っているが, 格子の場合には単射であっても全射であるとは限らない.

1.3.2 全単射と逆写像

写像が全単射であれば, 必ず逆写像が存在する. しかし, 実際に構成することは難しいことがある. これが一方向関数の肝である. 学校で学習する数学ではどちらかというと逆写像の存在と逆写像の実現可能性の差を強調しないので, 気がつきづらい. しかし, 逆行列の計算（連立方程式の解法, クラメールの公式), 逆三角関数の学習などを通じ, 一定の労力を払って練習して来ていることが, 実現性に関連している.

1.3.3 対数関数の存在

指数関数 $y = e^x$ の逆関数としての対数関数 $y = \log x$ が高校で学習できる程に易しい理由は, 指数関数の連続性あるいは単調性, および, 実数の完備性（連結性）に基づく. 例えば, 高校の教科書の巻末に掲載されている対数表や, 現代では, 数値計算ソフトが有用であるのは, x の値が十分近ければ $\log x$ の値も十分近い, という理由に基づく. 離散対数関数の場合は, (a, n

を固定して) 指数関数にあたるもの $\mathbb{Z} \ni x \mapsto (a^x \bmod n) \in \mathbb{Z}/n\mathbb{Z}$ を考えたときに, x に関する連続性がないため, 逆関数である離散対数関数の解析が微分積分学に帰着されないのである.

1.3.4 圏, 関手

集合や写像をより高度化した対象として, 圏や関手がある.

1.3.5 対応

X から Y への対応とは, 直積集合 $X \times Y$ の部分集合 C のことである. 写像 $f\colon X \to Y$ に対しては, そのグラフ $\{(x, f(x)) \mid x \in X\}$ が対応を与える. 対応 C が与えられたとき, 各点 $x \in X$ のファイバー $C_x := \{y \in Y \mid (x, y) \in C\}$ が 1 点からなることと, C が写像のグラフであることは同値である. 対応の定義は広すぎて, このままでは何の役にも立たないが, 対応（のうち特別なもの）を写像の一般化と見なすことで写像の性質を一般化できる. C_x が 2 点以上からなる場合は, 写像の行き先が 1 点に定まらず 2 点以上からなるものを許容すること, C_x が空集合になる場合は, x が写像の定義域から除外されていると考えることができる.

1.3.6 フーリエ変換

フーリエ変換も適当な関数空間同士の全単射線形写像である. ただし, もとの空間座標で表している特徴量とフーリエ変換したあとの周波数空間で表している特徴量は異なったものを表している. 従って, 近似, 打ち切り, 誤差評価をする際には, 両者の描像は同じではない. 一方から一方へ翻訳することは可能であるが, 一方で直接的であった操作が他方では間接的であったりする.

1.4 位相

近い遠いを測り, それを表すのが, 位相, 距離, ノルム, 内積, 計量, といった道具である. 位相の定義は集合系でなされるので, より漠然とした体系でつかみ所がないと感じられるかもしれない. しかし, 道具に差があるとはいえ, 精神は共通である.

1.4.1 定義

位相の特別なものが距離, 距離の特別なものがノルム, ノルムの特別なものが内積である. (なお, **ノルム**にはよい和訳がない.) 特別なものほど, より多くの構造を持つ.

距離は, 遠さを一つの実数で測定するという特徴がある. これに対して, 位相は, いわば, 有限個の実数では測定し得ないような, 多種な近さの指標を同時に表す機構であると対比できる. また, ノルムは線形構造と相性の良い距離であり, $a > 0$ 倍したもののノルムは正確に a 倍される.

1.4.2 直交性

ノルムは長さのみを測るが, 内積にはさらに角度の概念がある. 特に直角, 垂直, 垂線の概念が使えるのが大きい. 3 平方の定理が使えるし, 直交分解, 直交射影なども使える.

例 1.8 l^p 空間. $p > 1$ とし,

$$\sum_{n=1}^{\infty} |a_n|^p < \infty$$

を満たすような数列 $\{a_n\}$ の全体を l^p と書く. l^p は “完備なノルム空間であり, $p = 2$ の時, そしてそのときに限り, 内積空間である”. 関数のなす空間 L^p も同様の性質を持つ.

基底と正規直交基底, あるいは, 射影と直交射影は混同しやすく, さらに, 後者を前者で呼ぶ場合もあるが, 前者は線形空間, 後者は内積空間における概念である.

1.4.3 完備性

完備性とは, コーシー列が必ず収束するという性質である. 基礎となる空間に完備性があれば, ある要素を指定する場合に, 近似列を使うことができる. 例えば, ニュートン法, 2 分法, 折れ線法などで与えた極限が必ず存在することを保証している便利な性質である. 例えば, 円周率を $3.14\cdots$ と表すことができるように, 無限小数を使うことの根拠は実数の完備性にある. これと同じように, データ, 関数や曲線・曲面を近似的に表すことができる根拠を与える受け皿である.

なお, 完備なノルム空間を Banach 空間, 完備な内積空間を Hilbert 空間という. 名前は厳めしいが定義は自然であり, たじろぐことはない. 整数や有理数は離散的な対象であるが, 完備性を持つ受け皿として, 実数体 $\mathbb{R}$ 以外にも, 局所体 $\mathbb{Q}_p$ が用意されている [5].

2 代数系（群・環・体）

運動や対称性の記述には, 群が用いられる. 群の典型例は行列のなす集合である. 数や多項式の体系は環をなす. これらの代数系を紹介する [6].

2.1 群の定義 (静的)

集合 G に 2 項演算 $G \times G \to G$ が与えられていて, 結合法則 $(g_1 g_2) g_3 = g_1 (g_2 g_3)$, 単位元の存在, 逆元の存在を満たすとき, G とその演算の組を群という. しばしば演算を省略して, G は群である, とも言う.

例 2.1 正則行列の全体は群をなす. （行列のかけ算を演算として. ）

2.1.1 アーベル群

群で, 交換法則 $g_1g_2 = g_2g_1$ が成り立っているとき, アーベル群, 可換群などと呼ぶ. また, このとき, 演算を加法で書くことも多く, 加群とも言う.

例 2.2 $\mathbb{Z}$ や $\mathbb{Z}/n\mathbb{Z}$ で加法を演算としたときがアーベル群の例である. 絶対値 1 の複素数や 1 の冪根全体は積の演算でアーベル群となる. 楕円曲線上の点の全体は「加法」によってアーベル群をなす.

2.1.2 準同型

2 つの群 G, H に対して, 写像 $f\colon G \to H$ が $f(g_1g_2) = f(g_1)f(g_2)$ を満たすとき, (群の) 準同型であるという.

例 2.3 指数関数 e^x は加法群 $\mathbb{R}$ から乗法群 $\mathbb{R}_{>0} := \{t \in \mathbb{R} \mid t > 0\}$ への群の準同型を与える.

なお, 行列の指数関数 $\exp(A) = \sum_{n=0}^{\infty} \frac{1}{n!}A^n$ は, スカラー値の指数関数といくつもの類似の性質をみたすが, 群準同型ではない.

例 2.4 Weierstrass の $\wp$ 関数を使うと,

$$\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) \longrightarrow \{(x, y) \in \mathbb{C}^2 \mid y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\} \tag{1}$$

という加法群の同型が得られる. (左側が外延的記法, 右側が内包的記法であることに注意されたい.) また, 自然な位相のもと, 位相同型にもなる. $\mathbb{C}$ を格子 $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ で割った群の演算は複素数の加法という易しいものであるが, 楕円曲線 $y^2 = 4x^3 - g_2x - g_3$ の加法は自明ではない. また, 楕円曲線上の有理点全体は $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ の部分集合と全単射に対応しているが, $\wp$ 関数の関数としての非自明さ度合いが楕円曲線の上の対数問題の難しさに関係している.

2.2 環の乗法群

2.2.1 環の定義

集合 R 上の 2 つの演算, 加法と乗法が, 加法に関して群になる, 乗法に関する結合法則を満たす, 2 つの演算が分配法則をみたす, 時に, その集合と 2 つの演算の組を環であるという. しばしば乗法の単位元 1 が存在することを仮定し, しばしば単位元を持つ環と略称する. また, 乗法の演算が可換 $ab = ba$ のとき, 可換環であるという. (加法の単位元 0 の存在や, 加法の可換性 $a + b = b + a$ は仮定されているので改めて特筆しない習慣である.)

例 2.5 多項式環は単位元を持つ可換環である.

環においては 0 でない元が逆元を持つとは限らない. 逆元を持つような元を単元と呼び, 単元の全体を $R^\times$ と書く. 単元全体は群をなす.

例 2.6 正方行列のなす環 $M(n,\mathbb{R})$ の単元とは, 正則行列のことであり, その全体 $M(n,\mathbb{R})^\times$ を一般線形群 $GL(n,\mathbb{R})$ とよぶ.

0 でない元全体が群をなす, つまり 0 でない元がつねに逆元を持つ環を体と呼ぶ.

例 2.7 有理数体, 実数体は体である. 四元数体 $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ も 0 でない元が逆元を持つので, 体であるが, 乗法の非可換性を強調するために, 非可換体と呼ぶこともある [3].

環は群にさらに構造が付加されたもの, 一方で, 体は環の特別なものである. また, 線形空間が環の構造を持つとき, 代数と呼ぶ. 群で逆元の存在を仮定しないものを半群と呼ぶ. その他, 用途に応じた代数系は山ほどある [4]. 例えば, めんつゆは足す, かける, 割ることができるし, 布団は引く, かけることができる.

2.3 変換群：群の動的な定義

群 G と集合 X に対して, 2 項演算 $G \times X \to X$ が与えられていて, $(g_1g_2)x = g_1(g_2x)$ が成り立つとき, G が X へ作用するという.

例 2.8 座標変換群や, 一次分数変換は作用である.

例 2.9 ガロア群も根の全体に作用している.

作用の定義は, 準同型 $G \to \mathrm{Aut}(X)$ の存在と言い換えることができる. ここで, $\mathrm{Aut}(X)$ は, 集合 X 上の全単射全体が写像の合成によってなす群である. X が線形空間であり, 作用 $x \mapsto gx$ が線形写像のとき, この作用のことを表現という. 群 G が集合 X に作用するとき, 一般にはその作用は表現ではないが, X 上の関数空間は自然に表現になる.

2.4 等質空間

2.4.1 定義

作用によって X の 2 点が互いに移り合えるとき, 作用が推移的である, あるいは, X は G の等質空間であるという. 例えば, 回転群 $SO(3)$ は球面 S^2 に推移的に作用する. 等質空間の各点は同等であり, 原点のような基準となる点はない.

2.4.2 固定部分群

等質空間の点 $x \in X$ を一つ固定したとき, その点 x を固定する群の元の全体 $G_x = \{g \in G \mid gx = x\}$ は G の部分群をなす. これを, 等方的部分群, 固定部分群と呼ぶ. 等質空間 X は G/G_x という商空間としての表示を持つ. 例えば, $S^2 = SO(3)/SO(2)$. $X = G/G_x$ という表示は, 対称性の記述, 座標や距離の記述, 他の空間との比較などにしばしば有効である.

一方で, 表示（同型）が基点 x の取り方に依存することを注意しておきたい.

2.4.3 主等質空間

任意の $x, y \in X$ に対して, 点 x を点 y に写すような $g \in G$ がただ一つ存在するとき, 作用は単純推移的であるという. また, このとき, X を主語にして, X は G の主等質空間であるという. 集合として X と G は同一視できるが, G には単位元という特別な点と演算があるのに対して, X の点は平等である.

例 2.10 例えば, 3 次元ベクトル空間 $\mathbb{R}^3$ は群であり, 我々の住む 3 次元空間は, この群に関する主等質空間であるが, 我々の住む 3 次元空間で特別な原点（基点）は決まっていない. 3 次元空間において, 原点を一つ選べば, 点を座標（位置ベクトル）を使って表すことができ, さまざまな計算ができる. 一方で, 図形に関する幾何学的性質の多くは, 位置ベクトルの原点の取り方によらないので, 表示の仕方によらない.

例 2.11 原点を重心とする平面上の 3 角形全体を X とする. X には一般線形群 $GL(2, \mathbb{R})$ が単純推移的に作用する.

3 角形分割された図形を連続的に形状変形する際に, 3 角形の頂点に自然に入っている座標で補間するよりも, $GL(2, \mathbb{R})$ の中で補間することが computer graphics で提唱, 応用されている ([1] を始め, たくさんの関連研究がある）.

例 2.12 空間内の 1 つの剛体（例えばカメラ）の位置と向きの全体は, 後で述べる運動群の主等質空間である.

2.5 リー群

2.5.1 リー群

群でありしかも多様体であるものをリー群と呼ぶ. 多様体を知らない場合は, 応用上, 行列のかけ算で実現される群をリー群であると考えておいて, だいたい問題は生じない. リー群では, 線形代数も微積分も使えるという点が著しい利点である.

2.5.2 指数写像

指数写像 exp (§2.1.2) は, リー環からリー群への写像を与える.

例 2.13 例えば, 一般線形群 $GL(n, \mathbb{R})$ (例 2.6) のリー環は $\mathfrak{gl}(n, \mathbb{R}) = M(n, \mathbb{R})$ であり, $\exp\colon M(n, \mathbb{R}) \to GL(n, \mathbb{R})$ が指数写像である.

例 2.14 交代行列の全体 $\mathfrak{so}(3) = \{A \in M(3, \mathbb{R}) \mid {}^tA = -A\}$ は, 3 次の回転群 $SO(3) = \{g \in M(3, \mathbb{R}) \mid {}^tgg = I_3\}$ のリー環であり, $\exp\colon \mathfrak{so}(3) \ni A \mapsto \exp(A) \in SO(3)$ は全射である.

これらの exp は, 群準同型ではない. 2 次の回転群 $SO(2)$ の場合は, 指数写像が準同型となるがそれは例外的である.

リー環の定義は述べないが, リー群の原点での接空間であり, 特に, 線形空間である. 従って, リー環では線形補間に意味がある. 例えば, 2 つの回転の線形補間は回転ではないが, リー環で線形補間したものを指数写像で写したものは補間として意味がある.

2.5.3 dual numbers

リー環はリー群の 1 次近似である. 形式的な変数 ε を $\mathbb{R}$ に付け加えた環 $\mathbb{R}[\varepsilon]$ を考え, それをイデアル (ε^2) で割った剰余環 $\mathbb{R}[\varepsilon]/(\varepsilon^2)$ を係数として考えると, 接空間を取り出すことができる. 実際には, 形式的に $a+b\varepsilon$ という数もどきを考え, ε^2 が出てきたらその都度, 0 に置き換えて計算すれば良い.

例 2.15 例えば, $G = SO(3)$ で単位元での接空間を考える. $A \in M(3,\mathbb{R})$ とし, $g = I + \varepsilon A$ と置く. ${}^t gg = (I+\varepsilon {}^t A)(I+\varepsilon A) = I + \varepsilon({}^t A + A)$ なので, $g \in SO(3)$ と ${}^t A + A = O$ が同値である. このように接空間 $\mathfrak{so}(3)$ が得られる.

たいていの関数や図形では 1 次近似をすると打ち切り誤差が生ずるが, リー群をリー環で近似したときには, 指数写像があるので, 情報落ちなく完全にもとのデータを復元できるという特筆すべき性質がある. ただし, 復元できるのは局所な情報（の積み重ね）だけであり, 連結性 π_0, 基本群 π_1 の情報はリー環からは読み取れない. c.f., §2.6.

2.5.4 半直積

群 G の部分群 H と正規部分群 K に対して, 写像 $H \times K \ni (h,k) \mapsto hk \in G$ が全単射になるとき, G は H と K の半直積であるといい, $G = H \ltimes K$ と書く. $h \in H$, $k \in K$ に対して, $k' = h^{-1}kh$ とおけば, $kh = hk'$, $k' \in K$ となる.

例 2.16 たとえば, $H = SO(3)$, $K = \mathbb{R}^3$ としたとき, H と K はそれぞれ空間の回転と平行移動全体を表す群であり, これらを合わせた群 G が 3 次の**運動群** $SO(3) \ltimes \mathbb{R}^3$ である. 運動群は, 3 次元空間の合同変換で向きを保つものの全体である. ある回転をしてから平行移動し, さらに逆回転をすると, 一般には別の平行移動になる, ということが $K = \mathbb{R}^3$ が正規部分群であることの反映である.

2.6 単位四元数群

運動群 $SO(3) \ltimes \mathbb{R}^3$ の平行移動部分の補間は線形補間で十分であるが, 回転部分の補間には注意が必要だった. CG におけるキャラクタやカメラの制御などにも用いられる球面線形補間について述べて, この項を終わりにしよう.

長さが 1 の四元数を単位四元数と呼び, その全体を $U(1,\mathbb{H})$ と書く.

$$U(1,\mathbb{H}) = \{a + bi + cj + dk \in \mathbb{H} \mid a^2 + b^2 + c^2 + d^2 = 1\}. \tag{2}$$

$U(1,\mathbb{H})$ は多様体としては 3 次元球面 S^3 と同型であり, コンパクトなリー群である.

四元数体を複素数体上の 2 次元（右）線形空間 $\mathbb{H} = \mathbb{C} + j\mathbb{C}$ と考えて, $\mathbb{H}$ の元 $g = a + bi + cj + dk = \alpha + \beta j$ を行列表示すると, $\begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}$ となる. これらの全体は, 特殊ユニタリ群

$SU(2) = \{A \in M(2,\mathbb{C}) \mid {}^t\bar{A}A = I_2,\ \det(A) = 1\}$ と呼ばれ, $U(1,\mathbb{H}) \cong SU(2)$ という同型がある. これは CG ではあまり使わないが付記しておく.

本題に戻る. $q \in U(1,\mathbb{H})$ の共役の定める作用 $\varphi_q(z) = qzq^{-1}$ を考える ($z \in \mathbb{H}$). 四元数体は非可換なので, この写像が非自明になりうるのである. $\operatorname{Im}\mathbb{H} = \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ とする. $z \in \operatorname{Im}\mathbb{H}$ ならば, $\varphi_q(z) \in \operatorname{Im}\mathbb{H}$ である. また, $\operatorname{Im}\mathbb{H} = \mathbb{R}^3$ と同一視することによって, 写像

$$\varpi\colon U(1,\mathbb{H}) \ni q \mapsto \varphi_q \in SO(3) \tag{3}$$

ができる. この写像 ϖ は全射, 群準同型であり, 核は $\ker\varpi = \{\pm 1\}$ のように 2 つの元からなる. この写像 ϖ は $SO(3)$ の普遍被覆写像でもある.

$SO(3)$ の 2 元 g_1, g_2 の補間をすることを考える. 例えば, ある剛体（カメラ）の 2 つの位置を記述する g_1, g_2 があったとき, その間を滑らかに結ぶという問題を考える. 写像 ϖ による g_1, g_2 のリフトを q_1, q_2 とする. すなわち, $\varphi_{q_1} = g_1$, $\varphi_{q_2} = g_2$. このとき, q_1, q_2 を $U(1,\mathbb{H})$ の中でうまく補間すれば, それの ϖ による像で g_1, g_2 は補間される. $U(1,\mathbb{H})$ の中での補間としては,

- リーマン多様体 S^3 の測地線（大円）による方法
- リー環 $\operatorname{Im}\mathbb{H}$ における線形補間の指数写像による像
- 球面線形補間 (slerp)

が知られているが, これら 3 つは一致することが分かる [2, 7].

参考文献

[1] M. Alexa, D. Cohen-Or and D. Levin, As-rigid-as-possible shape interpolation. In *Proceedings of ACM SIGGRAPH* (2000), pp. 157–164.

[2] 安生健一, 単位 4 元数空間: コンピュータグラフィックス における被覆の応用, 特集「被覆の話」, 数学セミナー 2013 年 1 月号, 38–44.

[3] M. Koecher and R. Remmert, Hamilton's Quaternions, *in Numbers*, Springer-Verlag (1991), 邦訳は『数』丸善.

[4] 落合啓之, 不変式と表現論, 特集「表現論の世界」, 数理科学 2013 年 1 月号, 26–33.

[5] F. Reihardt, H. Seoder and G. Falk, カラー図解 数学事典, 共立出版, 2012.

[6] 梅田亨, 代数の考え方, 放送大学教育振興会, 2010.

[7] J. Vince, Quaternions for Computer Graphics, Springer-Verlag, 2011.

CG 表現と球面調和関数の表現論

若山　正人

九州大学マス・フォア・インダストリ研究所

1　序

調和関数とはラプラス方程式の解であり，球面調和関数とはそれを球面に制限したものである．球面調和関数は，熱伝導方程式を解くためなどに古くから物理学で用いられてきた．またそれは，たとえば水素原子の電子の軌道の記述や，さらには量子化学の分野でも必須の関数族である．Computer Graphics (CG) における研究開発現場においても，最近では球面調和関数 (Spherical Harmonics) がしばしば道具として用いられている．

球面調和関数は，いわゆるルジャンドルの陪関数を用いて表すことができ，豊かな性質をもつ特殊関数である．その理由は，i) ラプラス作用素（ラプラシアン）$\Delta := \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$ が，3 次の直交群 $O(3) = \{g \in \mathrm{Mat}_3(\mathbb{R}) \mid {}^t g g = 1\}$ で不変であること，ii) 2 次元単位球面 S^2 が $\mathbb{R}^3$ の曲面として $O(3)$ の（典型）不変式 $r^2 := x^2 + y^2 + z^2$ を用いて $r = 1$ で定義されることに由来する．実際，ラプラシアン Δ で消される多項式（調和多項式）を球面上に制限した関数たちに対して，奇麗な理論ができるのはそのためである（[4, 6] を参照）．

以下を説明しておくことは，本稿の理解に役立つだろう．直交群 $O(3)$ の部分群である 3 次の回転群 $SO(3) = \{g \in O(3) \mid \det g = 1\}$ を考える．$SO(3)$ は普通に $\mathbb{R}^3$ に（3 次元実横ベクトル）へ行列を右からかけることにより作用している．S^2 上の一点 $p_0 = (0, 0, 1)$ に対し，p_0 を固定する部分群 $K := \{g \in SO(3) \mid p_0 g = p_0\}$ は，明らかに $K = \left\{ \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \middle| \, k \in SO(2) \right\} \cong SO(2)$ である．したがって，自然な対応 $SO(3) \ni g \mapsto p_0 g \in S^2$ によって，S^2 は，$SO(3)$ の左 $SO(2)$ 剰余類がなす等質空間 $SO(2)\backslash SO(3)$（実はリーマン対称空間と呼ばれるものになっている）とみなされる．実際，この対応は明らかに全射であり，かつ

$$p_0 g = p_0 g' \iff p_0 g g'^{-1} = p_0 \iff g g'^{-1} \in SO(2) \iff SO(2)g = SO(2)g'.$$

より，単射性も従うからである．

CG において初めて球面調和関数が利用されたのは，Sloan, Kautz, Snyder による，モデルの臨場感溢れる照射の実現を目指した SIGGRAPH 2002 の論文 [10] においてである．CG における球面調和関数の応用としては，Spherical Harmonic lighting (SH-Lighting) が最初であり基本である．それは面光源からの 3 次元照射を計算する技術であり，捉えた光の反射の様子を表示し，また，グローバル・イルミネーションのイメージを構築する手法である．そのため SH-Lighting は，動きがあり臨場感溢れる陰影表現，たとえばゲーム等の開発での有用な道具を与えている．

CG における光の照射に関する表現 (Expression) を追求するにあたり，SH-Lighting のように球面調和関数が使われる理由はいくつかあるが，具体的には

- 複雑な形状をした対象の光と影をリアルタイム（計算処理）で扱うのに都合がよい
- 大域的なイルミネーション
- 点光源では実イメージを得にくい
- 対象自体の影と，反射光の記述が可能になる

などが挙げられる．

本稿では，球面調和関数が CG に使われる出発点となる事実を紹介し，さらに，CG における技術として重要となる球面調和関数たちが持つ性質の一部を，群の表現論 (Representation Theory) の立場から紹介する．ポイントとなる考え方は，たとえば周期関数のフーリエ級数展開に似ている．フーリエ級数展開とは（周期）関数を指数関数 $e^{2\pi inx}$ $(n \in \mathbb{Z})$ の一次結合として展開することであるが，この $e^{2\pi inx}$ は，加法群 $\mathbb{R}$ の 1 次元表現を定めている．しかもこの表現は 1 次元であることから“既約表現”（つまり，これ以上小さな不変部分空間は $\{0\}$ しかない）とよばれる，表現の中でも根源的なものである．本稿では，この可換な（加法）群 $\mathbb{R}$ の代わりに，積が可換でない（非可換）群 $SO(3)$ を考えることとなる．

本稿は SH-Lighting 技法の入り口を扱うが，その具体的な数学モデリングにはまだ道のりがある．しかしながら，CG 研究で重要なレンダリング方程式（e.g. [3, 9] などを参照）を（近似的に）解く際などに必要な球面調和関数の諸性質やそれを扱うテクニックが，表現論を通してみると案外簡単な事実の積み上げから理解できることを，僅かでも読者にお伝えすることができれば幸いである．

2　行列のなすリー群とそのリー環

$GL_n(\mathbb{R})$ $(GL_n(\mathbb{C}))$ を n 次の可逆な実 (複素) 行列の全体がなす群とする．以下, G で $GL_n(\mathbb{C})$ の（閉）部分群を表す．このとき G は線型リー群であるという．G の例としては，n 次実特殊線型群 $SL_n(\mathbb{R}) = \{g \in GL_n(\mathbb{R}) \mid \det g = 1\}$，直交群 $O(n) = \{g \in GL_n(\mathbb{R}) \mid {}^t gg = 1\}$，特殊直交群（回転群）$SO(n) = O(n) \cap SL_n(\mathbb{R})$ やユニタリ群 $U(n) = \{g \in GL_n(\mathbb{C}) \mid {}^t\bar{g}g = 1\}$ などがある．いま，行列の指数写像 exp を考える：

$$\exp(X) := \sum_{m=0}^{\infty} \frac{X^m}{m!} \quad (X \in \mathrm{Mat}_n(\mathbb{R})).$$

線型リー群 G に対して

$$\mathfrak{g} = \mathrm{Lie}(G) := \{X \in \mathrm{Mat}_n(\mathbb{R}) \mid \exp(tX) \in G \ (t \in \mathbb{R})\}$$

とおき G のリー環という．$\mathfrak{g}$ は $\mathrm{Mat}_n(\mathbb{R})$ の部分空間であり，$X, Y \in \mathfrak{g}$ に対しブラケット積を $[X, Y] := XY - YX$ と定めると $[X, Y] \in \mathfrak{g}$ である．行列 X を三角化すれば容易に導かれる

関係式 $\det(\exp X) = e^{\operatorname{tr} X}$ を用いれば,

$$\begin{aligned}
\operatorname{Lie}(GL_n(\mathbb{R})) &= \operatorname{Mat}_n(\mathbb{R}),\\
\operatorname{Lie}(SL_n(\mathbb{R})) &= \{X \in \operatorname{Mat}_n(\mathbb{R}) \mid \operatorname{tr} X = 0\},\\
\operatorname{Lie}(O(n)) = \operatorname{Lie}(SO(n)) &= \{X \in \operatorname{Mat}_n(\mathbb{R}) \mid {}^tX + X = 0\},\\
\operatorname{Lie}(U(n)) &= \{X \in \operatorname{Mat}_n(\mathbb{C}) \mid {}^t\bar{X} + X = 0\}
\end{aligned}$$

などがわかる．$\mathfrak{g} = \operatorname{Lie}(G)$ は多様体 G の単位元における接空間と考えられる．

3　群の表現論をすこし

V を n 次元複素ベクトル空間とする．V の可逆な線型変換の全体を $GL(V)$ と書き一般線型群と呼ぶ．V に一つの基底を定めれば，V は $\mathbb{C}^n$ と同一視できる．さらに，線型変換はその基底に関して行列表示できるので，$GL(V) = GL_n(\mathbb{C})$ である．写像の合成（あるいは行列の積により）$GL(V)$ は群である．

群 G が与えられたとする．群 G の V 上の表現とは, G から $GL(V)$ への群準同型 π (積を保つ写像) をいう．つまり, (π, V) が G の表現であるならば, $\pi(g) \in GL(V)$ であり, $\pi(gg') = \pi(g)\pi(g')$ がすべての $g, g' \in G$ に対し成り立つ．とくに，G の単位元 e に対して $\pi(g) = I_V$（V の恒等変換）であり，$\pi(g)^{-1} = \pi(g^{-1})$ である．G の表現 (π, V) が与えられたとき，G は V に作用するともいう．以下の二つの概念を定義する：

- G の 2 つの表現 (π, V) と (π', V') が同値であるとは，ある線型同型写像 $A\colon V \to V'$ が存在してすべての $g \in G$ に対して $A\pi(g) = \pi'(g)A$ が成り立つときをいう．
- （有限次元）表現 (π, V) が既約であるとは，$\{0\}$ と V を除いて V の G の作用で不変な部分空間が存在しないときをいう．

線型リー群 G の表現 (π, V) に対し，G のリー環 $\mathfrak{g}$ の表現（微分表現）が次で定義される．

$$d\pi(X) = \frac{d}{dt}\pi(\exp(tX))\bigg|_{t=0} \quad (X \in \mathfrak{g}). \tag{1}$$

ただし，リー環 $\mathfrak{g}$ のベクトル空間 V 上の表現とは，写像 $\rho\colon \mathfrak{g} \to \operatorname{End}(V)$ であって $\rho([X, Y]) = [\rho(X), \rho(Y)]$ を満たすものである．リー環の表現についても，既約性や同値性は群の場合と同様に定義される．一般に G の表現論を考えるとき，対応するリー環 $\mathfrak{g}$ の表現を考えることは重要である．$\mathfrak{g}$ に対しては線型代数がフルに使えるので都合良く，すべてではないものの，G の表現に対し多くの情報を与えるからである．

例 3.1 $G = SL_2(\mathbb{C})$ とする．複素数を係数とする 2 変数の m 次同次多項式の全体がなす空間を $\mathcal{P}_m$ とかく．明らかに $\dim \mathcal{P}_m = m + 1$ である．G の表現 $(\pi_m, \mathcal{P}_m)$ を

$$(\pi_m(g)f)(u, v) = f(au + cv, bu + dv) \quad \left(f \in \mathcal{P}_m,\ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \tag{2}$$

で定める．いま，

$$H=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad E=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix},\quad F=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix},$$

とおくと，H, E, F は，リー環 $\mathfrak{g}=\mathfrak{sl}_2(\mathbb{C})$ のベクトル空間としての基底をなし，次の交換関係をみたす：

$$[H,\,E]=2E,\quad [H,\,F]=-2F,\quad [E,\,F]=H.$$

微分表現の定義 (1) から，簡単な計算で

$$\begin{aligned} d\pi_m(H)f &= u\frac{\partial f}{\partial u}-v\frac{\partial f}{\partial v},\\ d\pi_m(E)f &= u\frac{\partial f}{\partial v},\\ d\pi_m(F)f &= v\frac{\partial f}{\partial u}\end{aligned}$$

が得られる．また，単項式 $f_j(u,v):=u^jv^{m-j}$ $(j=0,1,\dots,m)$ は明らかに $\mathcal{P}_m$ の基底をなし，

$$\begin{aligned} d\pi_m(H)f_j &= (2j-m)f_j,\\ d\pi_m(E)f_j &= (m-j)f_{j+1},\\ d\pi_m(H)f_j &= jf_{j-1}\end{aligned}$$

がわかる．このことから，

$$0 \underset{F}{\leftarrow} \mathbb{C}f_0 \underset{F}{\overset{E}{\rightleftharpoons}} \mathbb{C}f_1 \underset{F}{\overset{E}{\rightleftharpoons}} \cdots \underset{F}{\overset{E}{\rightleftharpoons}} \mathbb{C}f_{m-1} \underset{F}{\overset{E}{\rightleftharpoons}} \mathbb{C}f_m \overset{E}{\to} 0$$

となり $d\pi_m$ の既約性（自明な $\mathfrak{g}$ 不変部分空間がないこと）が示された．このことから，G の表現 $(\pi_m,\mathcal{P}_m)$ が既約であることも従う．なお，f_m を最高ウェイトベクトルとよぶ．

ところで，m 次以下の複素変数の一変数多項式の全体がなす空間 $\widetilde{P}_m$ 上への $SL_2(\mathbb{C})$ の作用 τ_m を

$$(\tau_m(g)p)(z)=(cz+d)^m p\Big(\frac{az+b}{cz+d}\Big)\quad \left(p\in\widetilde{P}_m,\ g^{-1}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\right) \tag{3}$$

で定めると，$(\tau_m,\widetilde{P}_m)$ は $(\pi_m,\mathcal{P}_m)$ と同値な表現であることが容易に示される．

例 3.2 G を 2 次の特殊ユニタリ群 $SU(2)$ とする：

$$SU(2)=\left\{g=\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\ \middle|\ |\alpha|^2+|\beta|^2=1,\ \alpha,\beta\in\mathbb{C}\right\}. \tag{4}$$

任意の $Z\in\mathfrak{sl}_2(\mathbb{C})$ は $SU(2)$ のリー環 $\mathfrak{su}_2$ の元 X, Y を用いて一意的に $Z=X+iY$ と表されるので，例 3.1 の $SL_2(\mathbb{C})$ の表現 π_m を $SU(2)$ に制限したものを ρ_m とかくと，$(\rho_m,\mathcal{P}_m)$ も既約であることがわかる．さらに，$SU(2)$ の任意の既約表現は $(\rho_m,\mathcal{P}_m)$ $(\exists m\in\mathbb{Z}_+)$ と同値であることが証明される．

例 3.3 G を線型リー群とし，$\mathfrak{g}$ をそのリー環とする．$g \in G$, $X \in \mathfrak{g}$, $t \in \mathbb{R}$ に対して，$g\exp(tX)g^{-1} = \exp(tgXg^{-1})$ が成り立つので，$gXg^{-1} \in \mathfrak{g}$ である．そこで Ad を $\mathrm{Ad}(g)X := gXg^{-1}$ と定義すると

$$\mathrm{Ad}(g)[X, Y] = [\mathrm{Ad}(g)X, \mathrm{Ad}(g)Y], \quad \mathrm{Ad}(gg') = \mathrm{Ad}(g) \circ \mathrm{Ad}(g')$$

が成り立つ．よって，$(\mathrm{Ad}, \mathfrak{g})$ は G の表現を定める．これを G の随伴表現とよぶ．Ad の微分表現が $\mathrm{ad}(X)(Y) = [X, Y]$ で与えられることは明らかである．

4 球関数の可視化

3 次元の極座標表示（球面座標）を考えよう．

$$p = (x, y, z) = (r\sin\theta\cos\phi, r\sin\theta\sin\phi, r\cos\theta), \quad r > 0,\ (\theta, \phi) \in [0, \pi] \times [0, 2\pi].$$

方程式 $r = 1$ で定まる単位球面 S^2 上の関数 $f(\theta, \phi)$ を球関数とよぶ．ここでは実数値関数のみを扱う．球関数をビジュアライズする方法について述べる：

i) 球面上の各点における値の大きさを強度と考え，それを光のスペクトル（右の帯）に対応させ，球面上に色模様を織り込む（図 1 右）．

ii) i) に加え，各点の法線方向の大きさ（値）をプロットして描く（図 1 左）．

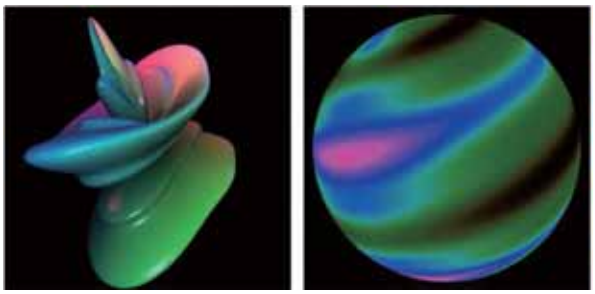


図 1：$f(\theta, \phi) = \frac{1}{4}(\cos^3 6\phi + \sin^4\theta + 1)$ の可視化 ([8]).

5 球面調和関数

$\mathbb{R}^3$ の座標を $\mathbf{x} = (x, y, z)$ と書く．3 変数 x, y, z に関する複素係数多項式の全体を $\mathcal{P}[\mathbf{x}]$ と表す．その上には，$(R(g)f)(\mathbf{x}) := f(\mathbf{x}g))$ $(f \in \mathcal{P}[\mathbf{x}],\ g \in SO(3))$ として回転群 $SO(3)$ が作用する．つまり $(R, \mathcal{P}[\mathbf{x}])$ は $SO(3)$ の表現である．$\mathcal{H}_\ell$ で ℓ 次調和多項式，すなわち ℓ 次同次なラプラス方程式の解 $(\Delta f = 0\ (f \in \mathcal{P}[\mathbf{x}]))$ 全体のなすベクトル空間を表すことにする．ℓ 次調和多項式 f を極座標 (r, θ, ϕ) で表すと，$f = r^\ell Y_\ell(\theta, \phi)$ と書ける．この，f の球面 S^2 への制限 $Y_\ell(\theta, \phi)$ を球面調和関数という．

さて，ラプラシアン Δ は，極座標を用いれば

$$\Delta = \frac{1}{r^2}\frac{\partial}{\partial r}\Big(r^2\frac{\partial}{\partial r}\Big) + \frac{1}{r^2}\Delta_{S^2},$$
$$\Delta_{S^2} := \frac{1}{\sin\theta}\frac{\partial}{\partial\theta}\Big(\sin\theta\frac{\partial}{\partial\theta}\Big) + \frac{1}{\sin^2\theta}\frac{\partial^2}{\partial\phi^2}$$

と表示される．この事実は微積分ではおなじみである．また，オイラーの次数作用素 $\mathcal{E} = x\frac{\partial}{\partial x} + y\frac{\partial}{\partial y} + z\frac{\partial}{\partial z}$ を用いると，以下のカペリ型恒等式が成り立つ ([5])：

$$r^2\Delta - \mathcal{E}(\mathcal{E}+1) = \Big(x\frac{\partial}{\partial y} - y\frac{\partial}{\partial x}\Big)^2 + \Big(y\frac{\partial}{\partial z} - z\frac{\partial}{\partial y}\Big)^2 + \Big(x\frac{\partial}{\partial z} - z\frac{\partial}{\partial x}\Big)^2 \ (= \Delta_{S^2}). \qquad (5)$$

上記の Δ の極座標表示，あるいはカペリ型恒等式 (5) から，球関数 $Y_\ell(\theta,\phi)$ が Δ_{S^2} の固有値 $-\ell(\ell+1)$ に対する固有関数であることがわかる：

$$\Delta_{S^2}Y_\ell(\theta,\phi) = -\ell(\ell+1)Y_\ell(\theta,\phi).$$

この固有関数全体がなす固有空間を $V(\Delta_{S^2}, -\ell(\ell+1))$ と表そう．このとき以下が知られている ([4, 6]).

定理 5.1 球面への制限写像 $\mathcal{K}$

$$\mathcal{K}\colon \mathcal{H}_\ell \ni f \longmapsto f|_{S^2} \in V(\Delta_{S^2}, -\ell(\ell+1))$$

により，$V(\Delta_{S^2}, -\ell(\ell+1))$ は $\mathcal{H}_\ell$ に同型である． ∎

さらに次が成り立つ．

定理 5.2 $\ell = 0, 1, 2, \ldots$ とする．ℓ 次調和多項式の空間 $\mathcal{H}_\ell$ は，$(2\ell+1)$ 次元であり，回転群 $SO(3)$ の既約表現を与える．さらに，$SO(3)$ の既約表現はこれらのいずれかに同値である．

証明 概略を述べる．$\mathcal{H}_\ell$ が，$SO(3)$ の作用 $R(g)$ で不変であることは明らか．したがって，$T_\ell = R|_{\mathcal{H}_\ell}$ とおくと，$(T_\ell, \mathcal{H}_\ell)$ は $SO(3)$ の表現である．3 次元リー環 $\mathfrak{su}_2$ には，キリング形式 $B(X,Y) := \mathrm{tr}(\mathrm{ad}(X)\mathrm{ad}(Y)) = 4\,\mathrm{tr}(XY)$ から定まる内積が入る．$SU(2)$ の表現 Ad は，この内積を不変にする群 $SO(3)$ への全射準同型を与え，その核は $\{\pm e\}$ である：$SU(2)/\{\pm e\} \cong SO(3)$ (e は $SU(2)$ の単位元 (2 次の単位行列))．いま T を $SO(3)$ の既約表現であるとすると，$\sigma := T\circ\mathrm{Ad}$ は $SU(2)$ の既約表現である．したがって，例 3.2 によれば，ある m が存在して σ は ρ_m に同値である．ところが $\mathrm{Ad}(-e) = I$ であるから，m は偶数である．したがって，次元を比較すれば $\sigma_\ell := T_\ell \circ \mathrm{Ad}$ は $\rho_{2\ell}$ に同値であることがわかる．よって，T_ℓ は既約であり，さらに $SO(3)$ の既約表現（の同値類）はこれらで尽くされる． ∎

以下で述べる球面調和関数 $\mathcal{Y}_\ell^m(\theta,\phi)$ を用いると $F_\ell^m(\mathbf{x}) = r^\ell\mathcal{Y}_\ell^m(\theta,\phi)$ $(-\ell \le m \le \ell)$ は，定理 5.2 の $\mathcal{H}_\ell$ の基底を与える．ここで $\mathcal{Y}_\ell^m(\theta,\phi)$ は

$$\mathcal{Y}_\ell^m(\theta,\phi) := N_\ell^m e^{im\phi}P_\ell^m(\cos\theta) \quad (\ell\in\mathbb{N},\ -\ell\le m\le\ell).$$

であり，$\mathcal{Y}_\ell^m(\theta,\phi) \in V(\Delta_{S^2}, -\ell(\ell+1))$ より，$P_\ell^m(x)$ は ルジャンドルの陪微分方程式を満たし（定数を調整すると）以下のようにルジャンドルの陪関数で与えられることがわかる．

$$P_\ell^m(x) = \frac{(-1)^m}{2^\ell \ell!}\sqrt{(1-x^2)^m}\frac{d^{\ell+m}}{dx^{\ell+m}}(x^2-1)^\ell.$$

$P_\ell^m(x)$ は $[-1,1]$ における直交関数系である．また，$N_\ell^m e^{im\phi} = \sqrt{\frac{(2\ell+1)(1-|m|)!}{4\pi(\ell+|m|)!}}$ は規格化定数であり，これにより $\mathcal{Y}_\ell^m(\theta,\phi)$ は，S^2 の 2 乗可積分な関数のなすヒルベルト空間 $L^2(S^2) = L^2(SO(2)\backslash SO(3))$ の（測度 $dp := \sin\theta d\theta d\phi$ に関する）正規直交基底を与える：

$$\int_{S^2} \mathcal{Y}_\ell^m(p)\overline{\mathcal{Y}_{\ell'}^{m'}(p)}\,dp = \delta_{\ell,\ell'}\delta_{m,m'}.$$

なお，表現 $(T_\ell, \mathcal{H}_\ell)$ の最高ウェイトベクトルは $\mathcal{Y}_\ell^\ell(\theta,\phi)$ で与えられる．

物理学を始め，普通はこの複素数値関数を用いるが，CG においては，映像表現に直接用いることから，次のような実数値の球面調和関数 y_ℓ^m を考えることが多い：

$$y_\ell^m(\theta,\phi) := \begin{cases} \sqrt{2}\,\Re(\mathcal{Y}_\ell^m) & (m>0) \\ \sqrt{2}\,\Re(\mathcal{Y}_\ell^m) & (m<0) \\ \mathcal{Y}_\ell^0 & (m=0) \end{cases} = \begin{cases} \sqrt{2}\,N_\ell^m \cos m\phi P_\ell^m(\cos\theta) & (m>0) \\ \sqrt{2}\,N_\ell^m \sin|m|\phi P_\ell^m(\cos\theta) & (m<0) \\ N_\ell^0 P_\ell^0(\cos\theta) & (m=0). \end{cases}$$

ℓ はバンドともよばれ，ルジャンドル多項式 $P_\ell^0(t)$ の次数に一致する．なお，ルジャンドルの陪関数は以下の漸化式を満たす（よって，それらの明示式を順次計算することができる）．

$$\begin{aligned} P_m^m(x) &= (-1)^m(2m-1)!!(1-x^2)^{m/2}, \\ P_{m+1}^m(x) &= (2m+1)xP_m^m(x), \\ (\ell-m)P_\ell^m(x) &= (2\ell-1)xP_{\ell-1}^m(x) - (\ell+m-1)P_{\ell-2}^m(x). \end{aligned}$$

上記の定理5.2によれば, 球面調和関数に対する回転の作用は, バンドℓ毎に, $(2\ell+1)\times(2\ell+1)$ 行列で与えられることがわかる．また，これまでの議論により，球面調和関数という見た目には複雑な関数たちも，2 変数同次多項式（resp. 一変数多項式）という簡単な関数たちがなす空間上の $SL_2(\mathbb{C})$ の表現 $(\pi_m, \mathcal{P}_m)$ (resp. (τ_m, P_m)) を $SU(2)$ に制限した表現を考え，それを群準同型写像 Ad を通して $SU(2)$ の表現から回転群 $SO(3)$ の表現に移しただけにすぎないことがわかる．したがって，上記の漸化式も元の多項式の間の関係式から導かれるはずであり，それは実際正しい．この事実を用いて，球面調和関数を一変数の単項式を利用した計算に置き換えれば，応用上重要な計算速度の高速化に利用できると期待される．

6　球面調和関数の基底展開と復元

まず，球面調和関数をビジュアライズしてみよう．いくつかが知られているが，本稿ではもっとも標準的といわれる方法を紹介する．F を実数値球面調和関数とする．S^2 上の各点に

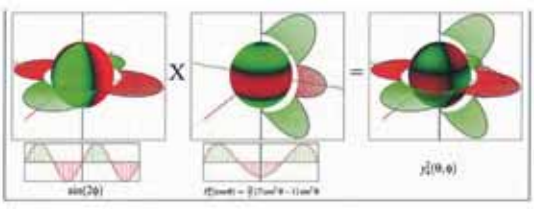


図 2：左は位相 2 の正弦波，中央は $P_4^2(\cos\theta)$，右は両者の合成 ([8]).

対し，その点での関数の絶対値を動径方向に拡大した点全体を考えると，それらは明らかに閉曲面をなす．そこで F の符号が正であるか負であるかにしたがって，その曲面上の領域を，正ならば緑，負ならば赤に色分ける．このようにして描いたものが図 2 である．

図 3 はバンド ℓ が 0〜4 までの $y_\ell^m(\theta,\phi)$ を示している．とくに，各横列は $SO(3)$ の既約表現 $(T_\ell, V(\Delta_{S^2}, -\ell(\ell+1))$ に対応している．

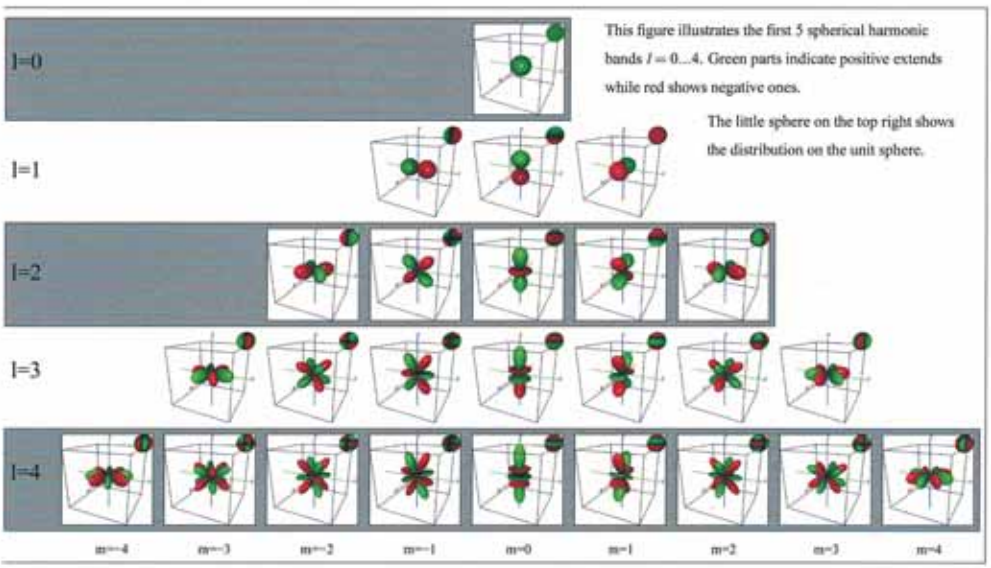


図 3：横列の図の個数 $2\ell+1$ は既約表現 T_ℓ の次元 ([8]).

実球面調和関数 $y_\ell^m(\theta,\phi)$ たちは $L^2(S^2)$ の基底をなすので，$f \in L^2(S^2)$ は $y_\ell^m(\theta,\phi)$ を用いて展開できる：

$$f(p) = \sum_{\ell=0}^{\infty} \sum_{m=-\ell}^{\ell} \widehat{f}(\ell,m) y_\ell^m(p). \tag{6}$$

ここで展開係数 $\widehat{f}(\ell,m)$ は，次のように y_ℓ^m 方向への射影で与えられる．

$$\widehat{f}(\ell,m) = \int_{S^2} f(p) y_\ell^m(p)\, dp = \int_0^{2\pi} \int_0^{\pi} f(\theta,\phi) \sin\theta\, d\theta\, d\phi.$$

関数 f があまり高い振動数をもたなければ，展開 (6) において項数を十分大きくとれば，対応する有限和は，f の良い近似を与えるはずである．各 $n \in \mathbb{N}$ に対して，以下の $f_n(p)$ は，与えられた球面上の関数 f の球面調和関数展開における和をバンドが n 以下で打ち切った関数である．

$$f(p) \approx f_n(p) := \sum_{\ell=0}^{n} \sum_{m=-\ell}^{\ell} \widehat{f}(\ell, m) y_\ell^m(p).$$

図 4 は関数 $f_n(p)$ による f の近似の様子を図示したものである．

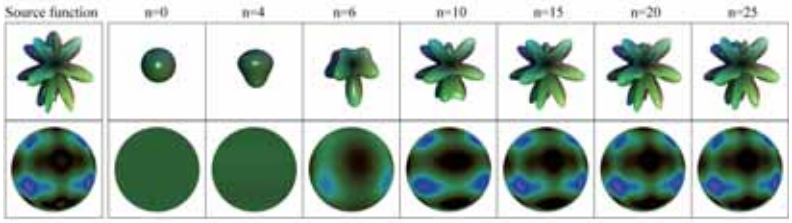


図 4：実球面調和関数基底による復元 [8]

注意 6.1 詳細は述べ得ないが，球面調和関数展開には，数値的積分を実行することが必要となる．そのための方法としては，乱数を用いたいわゆるモンテカルロ積分が用いられる．モンテカルロ法については [7] などを参照．

7　そのほか

1. 軸対称な球関数 h を考える．たとえば対称軸を z-軸にとれば，h は経度 ϕ に依存しない θ の関数となる．$y_\ell^0(\theta, \phi) = \mathcal{Y}_\ell^0(\theta, \phi) = N_\ell^0 P_\ell^0(\cos\theta)$ がその例である．このような球関数を帯球関数とよぶ．群論的にいえば，$SO(3)$ 上の両側 $SO(2)$ 不変な関数，あるいは，$S^2 = SO(2)\backslash SO(3)$ 上の右 $SO(2)$ 不変な関数である．h を帯球関数とすると h は $\cos\theta$ の，従って $[-1, 1]$ 上の関数と考えられる．そこで，与えられた球関数 f から新しい球関数を，h との合成積

$$(h * f)(x) = \int_{S^2} h(x \cdot y) f(y) dy$$

により作る．ここで $x \cdot y$ は $\mathbb{R}^3$ の内積である．合成積 $h * f$ の $y_\ell^m(\theta, \phi)$ による展開係数は，Funk-Hecke の定理（e.g. [2] を参照）により

$$\widehat{(h * f)}(\ell, m) = \sqrt{\frac{4\pi}{2\ell + 1}} h(\ell, 0) f(\ell, m)$$

となる．つまり，合成積 $h * f$ の球面調和関数展開の係数は f のそれをスケール変換するだけである．よって，f のかわりに合成積 $h * f$ を用いれば，帯関数 h をうまく選ぶことにより，高

い振動数の寄与を減らして，より早く収束する球面調和関数展開ができることになる．このことの応用については，たとえば [1] を参照．

2. 2 つの球関数の積 $c(p) = a(p)b(p)$ を考えることが必要な場合がある．たとえば，レンダリング方程式を解く場合などである．簡単のため $y_i(\theta, \phi) = y_\ell^m(\theta, \phi)$ $(i = (\ell + 1)\ell + m)$ と定める．このとき $c(p)$ の展開係数 $c_i := \int_{S^2} c(p) y_i(p)\, dp$ は，

$$\widehat{a}_{ij} = \sum_k a_k \int_{S^2} y_k(p) y_j(p) y_i(p)\, dp$$

とおくと，$c_i = \sum_j \widehat{a}_{ij} b_j$ と表される．この対称行列 $\widehat{a}_{ij}$ は多くの場合スパースである．応用例については [8] などを参照．

8　終わりに

本稿で詳細に述べることができなかった回転群の表現論については，参考文献にある日本語の書物を参考にして頂きたい．加えて CG への応用も，ほんの入り口にとどまっている．なお，CG への理論的手引きとして，論文 [3, 8, 9] は興味深く，役立つ．さらなる研究には，これらの論文に挙げられている文献を参照してもらいたい．

参考文献

[1] Ronen Basri, David W. Jacobs: Lambertian Reflectance and Linear Subspaces, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, 2003.

[2] Jacques Faraut: Analysis on Lie Groups, Cambridge Studies in Adv. Math. 110, 2008.

[3] Robin Green: Spherical Harmonic Lighting: Gritty Details, GDC 2003.

[4] 平井武，山下博：表現論入門セミナー，遊星社 2003.

[5] 黒川信重，若山正人：絶対カシミール元，岩波書店 2002.

[6] 岡本清郷：フーリエ解析の展望（すうがくぶっくす 17），朝倉書店 1997.

[7] Peter Shirley: Realistic Ray Tracing, A. K. Peters 2001.

[8] Volker Schönefeld: Spherical Harmonics, `http://heim.c-otto.de/~volker/prosem`. Seminal paper, 2005.

[9] Peter-Pike Sloan: Stupid Spherical harmonics (SH) Tricks, GDC 2008.

[10] Peter-Pike Sloan, Jan Kautz and John Snyder: Precomputed Radiance Transfer for Real-Time Rendering in Dynamic, Low-Frequency Lighting Environments, Microsoft Research and SIGGRAPH 2002.

公開鍵暗号入門

高木　剛

九州大学マス・フォア・インダストリ研究所

概 要

暗号と聞いて，人々がまず思い浮かべるのは軍事・外交で用いられる秘匿通信と考えられるが，実は，現代の暗号技術は私たちの身近なところで様々な形で利用されている．例えば，IC カードやパスポートなどの個人認証，インターネット上の電子商取引，DVD の著作権保護技術など，暗号は現代社会には無くてはならない技術となっている．現在実用化され広く普及している暗号として，第一世代の RSA 暗号と第二世代の楕円曲線暗号がある．RSA 暗号は 30 年以上前に提案された後，1990 年代のインターネット普及により暗号ソフトウェアのデファクトスタンダードとして利用されている．1985 年に発表された楕円曲線暗号は，高速に演算処理ができることを特徴とし，2000 年代から DVD プレーヤーや携帯端末など組み込みディバイスでの利用が進んでいる．このようななか，2001 年には第三世代の暗号としてペアリング暗号が提案された．ペアリング暗号は旧世代の暗号では実現が困難であったセキュリティ方式の構成を可能とするため，世界中の研究機関や企業で活発な研究開発が進んでいる．本稿では，これらの暗号に関して解説していく．

1　はじめに

情報セキュリティの安全性を支える核技術の一つとして公開鍵暗号がある．例えば，公開鍵暗号を利用したインターネットの暗号化方式 SSL は，クレジットカード番号などを安全に配送する暗号プロトコルとして実用化されている．

図 1 において，公開鍵暗号の概要に関してインターネットバンキングをもとに説明する．公開鍵暗号では，秘密鍵と公開鍵と言われる 2 種類の鍵を用意する．秘密鍵は受信者であるサーバが安全に保管し，公開鍵はネットワーク全体に公開する．クレジットカード番号を送信したい場合，公開されている公開鍵により暗号化を行い，インターネット経由で暗号文をサーバに送信する．ここでクレジットカード番号は暗号化されているため攻撃者は知ることができない．一方，秘密鍵を保持しているサーバは暗号文を復号化することができる．公開鍵暗号により，送信先のサーバの秘密鍵を配送することなく，サーバに対応する公開鍵を利用して暗号通信が可能となった．

現在最も利用されている公開鍵暗号として素因数分解の困難性を安全性の根拠にした RSA 暗号 [17] が有名である．一方，有限体上の楕円曲線における離散対数問題の困難性を安全性の根拠にした楕円曲線暗号 [15, 13] は，RSA 暗号と同程度の安全性をより短い鍵長で実現できる特徴を持つ．近年，RSA 暗号や楕円曲線暗号では実現が困難であった暗号プロトコルを実現できる方式として「ペアリング暗号」が注目を集めて世界中で活発に研究が進展している．ペアリング暗号の代表的な例として，利用者が公開鍵を ID のように自由に選択できる ID ベー

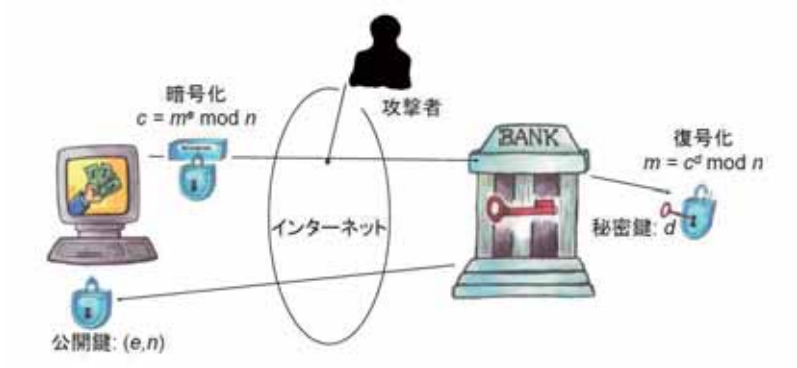


図 1：公開鍵暗号を利用したインターネットバンキング

ス暗号が知られている [18, 4]．ペアリング暗号は，楕円曲線上の離散対数問題をペアリング写像により有限体上の離散対数問題に帰着できる楕円曲線を利用して構成される．

本章では，RSA 暗号に始まり楕円曲線暗号およびペアリング暗号という形で進化してきた公開鍵暗号化方式について解説していく．特に，どのような数学的構造が公開鍵暗号に利用されており，それらが暗号の安全性や性能に与えている影響について説明する．

2 RSA 暗号

RSA 暗号は，Rivest, Shamir, Adelmann により 1978 年に発表された世界初の公開鍵暗号方式である [17]．本章では，RSA 暗号の動作原理に関して解説する．

RSA 暗号のトラップドア付き一方向関数は，整数の整除に関する基本的な性質を用いて構成される．2 個の整数 a, b に対して $a = bq + r, 0 \leq r < b$ を満たす整数 q, r が一意的に存在する．この q, r を，a を b で割った商 q と余り r と言い，$r = a \bmod b$ と書く．2 個の整数の公約数が 1 であるとき互いに素という．整数 k の余り全体の集合 $\mathbf{Z}_k = \{0, 1, 2, \ldots, k-1\}$ は環をなし，k を法とする剰余環という．剰余環 $\mathbf{Z}_k$ の元で k と互いに素となる全体は群をなし，k を法とする乗法群 $\mathbf{Z}_k^\times$ という．

RSA 暗号の安全性は素因数分解の計算量的困難性を基にしている．そのため，RSA 暗号は 2 個の素数 p, q に対して $n = pq$ を法とする乗法群 $\mathbf{Z}_n^\times$ の上で構成される．ここで，乗法群 $\mathbf{Z}_n^\times$ の位数は $(p-1)(q-1)$ となり，RSA 暗号のトラップドアは，n と互いに素な整数 m に対して $m^{(p-1)(q-1)} = 1 \bmod n$ を満たす性質 (オイラーの定理) を利用する．以下，RSA 暗号の構成方法を示す．

> **[鍵生成]** 2 個の素数 p, q を生成し $n = pq$ とする．$ed = 1 \bmod (p-1)(q-1)$ を満たす整数 e, d を生成する．公開鍵を (e, n)，秘密鍵は d とする．公開鍵 (e, n) はインターネットにおいて公開し，秘密鍵 d はサーバにおいて安全に保存する．
>
> **[暗号化]** 平文 m は剰余環 $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$ の元とする．公開鍵 (e, n) をインターネットよりダウンロードして，平文 m に対して，公開鍵 (e, n) を利用

して，暗号化 $c = m^e \bmod n$ を計算する．暗号文 c をインターネット経由でサーバに送信する．

[**復号化**] 暗号文 c と公開鍵 n に対して，秘密鍵 d を利用して，復号化 $m = c^d \bmod n$ を行う．

ここで，ある整数 h が存在して $ed = 1 + h(p-1)(q-1)$ となるため，m と n が互いに素である場合は，$c^d = m^{ed} = m^{1+h(p-1)(q-1)} = m \bmod n$ より復号化できる．また，m と n が互いに素ではない場合は，$m = 0 \bmod p$, $m = 0 \bmod q$, または $m = 0$ を満たすが，この場合も同様に復号化可能である．

2.1 RSA 暗号の安全性

RSA 暗号は素因数分解の困難性を安全性の根拠にしている．もし公開鍵 $n = pq$ が素因数分解された場合，秘密鍵 d は $d = e^{-1} \bmod (p-1)(q-1)$ により求めることが可能であり，RSA 暗号は完全に解読される．現在知られている最も高速な素因数分解アルゴリズムは数体篩法 [14] であり，n のビット長に対して準指数時間 $\mathcal{O}(\exp(((64/9)^{1/3} + o(1))(\log n^2)^{1/3}(\log\log n^2)^{2/3}))$ の計算時間が必要である．この公開鍵 n のサイズが RSA 暗号の鍵長と言われ，現在のところ 1024 ビットや 2048 ビットが選ばれることが多い．将来的には，素因数分解アルゴリズムの改良や計算機のソフトウェア/ハードウェアの進展により，より長い鍵長を選択する必要がある．RSA 暗号の安全な鍵長に関する見積もりは，CRYPTREC より詳しい報告書が出されている [9].

次に，一方向性の意味での安全性について説明する．以下，鍵長が ℓ ビットの RSA 暗号における公開鍵全体の集合を RSA_ℓ と書き，RSA 暗号の一方向性を形式的に定義する．自然数全体の集合を $\mathbf{N}$，実数全体の集合を $\mathbf{R}$ と書く．関数 $\epsilon(\ell)\colon \mathbf{N} \to \mathbf{R}$ が negligible とは，任意の整数 $\alpha > 0$ に対して，ある整数 $\ell_\alpha > 0$ が存在して，$\ell > \ell_\alpha$ を満たす全ての ℓ において $\epsilon(\ell) < 1/\ell^\alpha$ となることを言う．RSA_ℓ からランダムに選んだ公開鍵 (e, n) とランダムな暗号文 $c \in \mathbf{Z}_n$ から，平文 m を求めるアルゴリズム $\mathcal{A}$ を考える．入力サイズ ℓ の全ての多項式時間アルゴリズム $\mathcal{A}$ に対して，確率

$$\Pr\left[\begin{array}{c}(e,n) \leftarrow RSA_\ell,\ m \leftarrow \mathbf{Z}_n, \\ c \leftarrow m^e \bmod n : \mathcal{A}(e,n,c) = m\end{array}\right] < \epsilon(\ell)$$

が negligible になる場合に，RSA 暗号は一方向性の意味で安全であるという．

RSA 暗号の一方向性を破るには，公開鍵 (e, n) と暗号文 c から対応する e 乗根 $m = c^{1/e} \bmod n$ を求めることができればよい．公開鍵 n を素因数分解することなく，RSA 暗号の一方向性を解読することができるかは現在のところ不明である [7].

3 楕円曲線暗号

楕円曲線暗号は，1985 年に Miller と Koblitz により独立に発表された [15, 13]．楕円曲線暗号の安全性は，楕円曲線上の離散対数問題の困難性を基にしている．素因数分解問題の困難

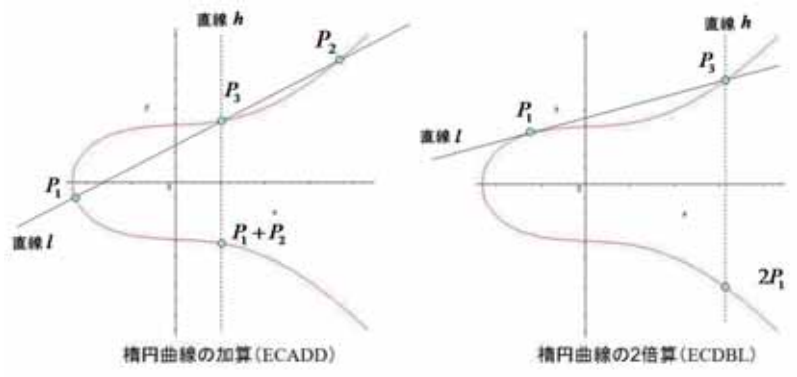


図 2：楕円曲線の加算および 2 倍算

性を基にした RSA 暗号とは異なり，鍵長に対する準指数時間の解読アルゴリズムが知られていない．そのため，楕円曲線暗号は，RSA 暗号より短い鍵長で，RSA 暗号と同等のセキュリティレベルを達成できることを特徴とする．

3.1 楕円曲線の加法公式

素数 p の位数を持つ有限体 $GF(p)$ を，$GF(p) = \{0, 1, 2, \ldots, p-1\}$ により表現する．$p > 3$ の有限体 $GF(p)$ 上の楕円曲線曲線 $E(p)$ は，

$$E(p) := \{(x, y) \in GF(p) \times GF(p) \mid y^2 = x^3 + ax + b\} \cup \{\infty\} \tag{1}$$

により定義される．ここで，$a, b \in GF(p)$ は $4a^3 + 27b^2 \neq 0$ を満たし，∞ は無限遠点と言われる $E(p)$ の元である．式 (1) の定義式をワイヤストラスの標準形とよぶ．楕円曲線 $E(p)$ は ∞ を零元として加法群をなし，点 $P = (x, y)$ の逆元は $-P = (x, -y)$ となる．Hasse-Weil の定理から $\#E(p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$ を満たし，楕円曲線 $E(p)$ の位数 $\#E(p)$ は p と同じビット長となる．ここで，t は，$E(p)$ のトレースと言われる不変量である．

楕円曲線 $E(p)$ 上の無限遠点とは異なる 2 点 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ に対して，加法 $P_1 + P_2 = (x', y')$ は次により計算される．

$$\begin{aligned} &x' = \lambda^2 - x_1 - x_2, \quad y' = \lambda(x_1 - x') - y_1, \\ &\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{for } P_1 \neq \pm P_2 \\ (3x_1^2 + a)/(2y_1) & \text{for } P_1 = P_2. \end{cases} \end{aligned} \tag{2}$$

この楕円曲線の加算 $P_1 + P_2, (P_1 \neq \pm P_2)$ を ECADD，2 倍算 $2P_1$ を ECDBL と記述する．

図 2 に，実数体上の楕円曲線 $y^2 = x^3 + 1$ を用いて，ECADD および ECDBL の説明をする．ECADD では，2 点 P_1, P_2 を通る直線 l に対して，P_1, P_2 とは異なる楕円曲線 $E(p)$ との交点 P_3 が存在する．この P_3 と無限遠点 ∞ を通る直線 (P_3 から x 軸への垂線)h に対して，P_3 とは

異なる楕円曲線 $E(p)$ との交点が加算の結果 $P_1 + P_2$ となる．同様に，ECDBL では，楕円曲線上の点 P_1 における接線 l が，楕円曲線 $E(p)$ と交わる別の点を P_3 とし，P_3 と無限遠点 ∞ を通る直線 h と交わる別の点が 2 倍算の結果 $2P_1$ となる．

3.2 楕円曲線暗号

楕円曲線 $E(p)$ を利用した公開鍵暗号方式では，小さな位数の部分群に対する攻撃を避けるために，曲線の位数が素数となる楕円曲線を利用する．式 (1) のランダムな曲線係数 $a, b \in GF(p)$ に対して楕円曲線の位数 $\#E(p)$ を求める方法として，Schoof のアルゴリズムとその改良が知られている [2, Chapter VII]．与えられた曲線位数 $\#E(p)$ および定義体の標数 p に対して，曲線係数 $a, b \in GF(p)$ を求める方法として虚数乗法がある [2, Chapter VIII]．一方，楕円曲線暗号では，a, b, p を固定した 1 本の楕円曲線を多くユーザが利用できるため，今までに報告された攻撃を考慮した上で安全となる暗号用の推奨曲線が公開されている (`http://www.secg.org/`)．

以下，楕円曲線を利用したエルガマル暗号について説明する．

> [**システムパラメータ生成**] 素数位数 ℓ の楕円曲線 $E(p)$ を生成して，その生成元を G とする．システムパラメータとして $E(p)$, G, ℓ をユーザ全体で共有する．
>
> [**公開鍵および秘密鍵生成**] 秘密鍵 $s \in \{1, 2, \ldots, \ell - 1\}$ に対して，$Q = sG$ を公開鍵とする．
>
> [**暗号化**] 平文 m を位数 ℓ のビット長以下となるビット列とする．乱数 $r \in \{1, 2, \ldots, \ell - 1\}$ を発生して，システムパラメータ G および公開鍵 Q に対して，$C_1 = rG, C_2 = rQ \in E(p)$ を計算する．C_2 の x 座標である $x(C_2)$ に対して，ビット毎の排他的論理和 $c_2 = x(C_2) \oplus m$ を計算する．(C_1, c_2) を暗号文とする．
>
> [**復号化**] 暗号文 (C_1, c_2) に対して，秘密鍵 s を利用して，$D = sC_1 \in E(p)$ を計算する．関係式 $D = sC_1 = s(rG) = r(sG) = rQ = C_2$ より，平文が $m = c_2 \oplus x(D)$ により復号化できる．

楕円曲線 $E(p)$ の生成元 G および公開鍵 Q から秘密鍵 s を求める問題は，楕円曲線 $E(p)$ の離散対数問題といわれる．エルガマル暗号の安全性は，楕円曲線 $E(p)$ の離散対数問題の困難性を基にしている．楕円曲線上の離散対数問題を解くアルゴリズムで，現在最も高速なアルゴリズムは Pollard の ρ 法である [2, 7 章]．その計算量は基礎体の位数 p のビット長に対して漸近的に指数時間 $\mathcal{O}(\sqrt{p})$ である．一方，素因数分解問題の解法は，漸近的により高速な準指数時間のアルゴリズムが知られている．RSA 暗号で利用されている 1024 ビットの素因数分解問題は，160 ビットの楕円曲線上の離散対数問題と同等の困難性があると見積もられている．このように RSA 暗号と比較して鍵長が短くなっているため，楕円曲線暗号はメモリの制限された組み込みシステム用ディバイスでの実装に向いていると言われている．

4　ペアリング暗号

ペアリング暗号の研究は，2000 年の暗号とセキュリティシンポジウム SCIS2000 において，境隆一等によって提案されたペアリング写像を利用した ID ベース暗号からスタートした [18]．その後，ペアリング写像を利用することにより，効率的なブロードキャスト暗号 [6]，キーワード検索可能暗号 [5] など，従来の公開鍵暗号では実現が難しいとされていた暗号プロトコルが次々と提案されてきている．これらのペアリング写像を利用した新しい暗号プロトコルのことを総称して，ペアリング暗号 (Pairing-Based Cryptography) と言われている．以下，ペアリング写像と ID ベース暗号について説明を行う．

4.1　ペアリング写像

本章では標数 $p > 3$ の有限体上の超特異曲線を利用した Tate ペアリングについて取り扱う．有限体 $GF(p)$ 上の超特異曲線は，$b = 0, 1$ に対して

$$E^b(p) = \{(x, y) \in GF(p) \times GF(p) \mid y^2 = x^3 + (1 - b)x + b\} \cup \{\infty\},$$

により定義される．超特異曲線 $E^b(p)$ のトレースは 0 であり，$E^b(p)$ の位数は $\#E^b(p) = p + 1$ となる．ℓ を標数 p と互いに素数であり，$\ell \mid \#E^b(p)$ を満たすとする．$\ell \mid (p^2 - 1)$ より，拡大体 $GF(p^2)$ は 1 の原始 ℓ 乗根を含む．$E^b(p)[\ell]$ を位数 ℓ の $E^b(p)$ の部分群とする．また，乗法群 $GF(p^2)^\times$ の 2 元 a_1, a_2 に対して，ある $c \in GF(p^2)^\times$ が存在して $a_1 = a_2 c^\ell$ と表現できるとき a_1, a_2 は同値であると定義する．乗法群 $GF(p^2)^\times$ において，この同値関係による商群 $GF(p^2)^\times/(GF(p^2)^\times)^\ell$ は，位数 ℓ の部分群となる．同様に，拡大体 $GF(p^2)$ 上の位数 ℓ の商群を $E^b(p^2)/\ell E^b(p^2)$ とする．ここで，Tate ペアリングは，

$$e\colon E^b(p)[\ell] \times E^b(p^2)/\ell E^b(p^2) \to GF(p^2)^\times/(GF(p^2)^\times)^\ell$$

により定義される双線形写像 e である．点 $P \in E^b(p)$ に対して，関数 $f_P^{(\ell)}(x, y)$ を，その因子 $(f_P^{(\ell)})$ が $\ell(P) - \ell(\infty)$ に同値なものとする．ここで，点 $R = (x, y) \in E^b(p^2)/\ell E^b(p^2)$ に対して，$e(P, R) = f_P^{(\ell)}(R)$ により Tate ペアリングは計算される．

次に，$i^2 = -1$ を満たす $i \in GF(p^2)$ に対して，拡大体 $GF(p^2)$ の $GF(p)$ 基底として $\{1, i\}$ を選ぶ．以下，この基底に対して曲線 $E^0(p)$ を考える (曲線 $E^1(p)$ も別の基底により同様に議論できる)．点 $Q = (x, y) \in E^0(p)$ に対して，distortion 写像を $\psi(x, y) = (-x, iy) \in E^0(p^2)$ により定義する．剰余群 $E^0(p^2)/\ell E^0(p^2)$ の点 R に対して $R = \psi(Q)$ となる点 $Q \in E^0(p)[\ell]$ が存在すため，Tate ペアリング $e(P, \psi(Q))$ は点 $P, Q \in E^0(p)[\ell]$ に対して定義できる．ここで，Tate ペアリングを剰余群 $GF(p^2)^\times/(GF(p^2)^\times)^\ell$ において一意的な値とするために，点 $P, Q \in E^0(p)$ に対して簡約 Tate ペアリングを $\hat{e}(P, Q) = e(P, \psi(Q))^{(p^2-1)/\ell}$ により定義する．簡約 Tate ペアリングは，非零整数値 a に対して双線形性

$$\hat{e}(aP, Q) = \hat{e}(P, aQ) = \hat{e}(P, Q)^a$$

を満たす．

以下に，Tateペアリングを効率的に計算する方法であるMillerアルゴリズム [16] を説明する．点 P_1, P_2 を通る直線を l，直線 l と楕円曲線の交点 P_3 と無限遠点を通る直線を h とする．これらの直線 l, h は，前節の楕円曲線上の加法公式 (図 1) で用いた．関数 $f_P^{(\ell)}$ は，点 $P_1, P_2 \in E^b(p)$ に対して

$$f_{P_1+P_2}^{(\ell)} = f_{P_1}^{(\ell)} f_{P_2}^{(\ell)} \frac{g_l}{g_h} \tag{3}$$

を満たす [3, Chapter IX]．関数 g_l, g_h は以下を因子に持つ．

$$(l) = (P_1) + (P_2) + (P_3) - 3(\infty), \quad (h) = (P_3) + (P_1 + P_2) - 2(\infty)$$

関係式 (3) により，位数 ℓ を 2 進展開することにより，$\mathcal{O}(\log p)$ 回の関数の計算によりペアリング $\hat{e}(P,Q) = (f_P^{(\ell)}(\psi(Q)))^{(p^2-1)/\ell}$ を計算することができる．Algorithm 1 に具体的な計算方法を記述する．

Algorithm 1 : Computation of Tate Pairing for $E^0(p)$

Input: $P = (x_p, y_p), Q = (x_q, y_q) \in E^0(p)[\ell], \ell = \sum_{i=0}^{t-1} \ell[i]2^i, \ell[t-1] = 1$
Output: $\hat{e}(P,Q)^{(p^2-1)/\ell} \in GF(p^2)^\times/(GF(p^2)^\times)^\ell$

1. $f \leftarrow 1$ and $V \leftarrow P$
2. **for** $i \leftarrow n-1$ **to** 0 **do**
   - 2.1. Set the lines l and h for ECDBL(T)
   - 2.2. $f \leftarrow f^2 \frac{g_l(\psi(Q))}{g_h(\psi(Q))}$ in $GF(p^2)$
   - 2.3. $T \leftarrow$ ECDBL(T) in $E^0(p)$
   - 2.4. **if** $\ell[i] = 1$ **do**
   - 2.5. Set the lines l and h for ECADD(T, P)
   - 2.6. $f \leftarrow f \frac{g_l(\psi(Q))}{g_h(\psi(Q))}$ in $GF(p^2)$
   - 2.7. $T \leftarrow$ ECADD(T, P) in $E^0(p)$
3. **return** $f^{(p^2-1)/\ell}$

Algorithm 1 の各ループは，有限体 $GF(p)$ の演算 (加算, 乗算, 逆元) を定数回行うことにより実装できるため，$\mathcal{O}((\log p)^2)$ 回のビット演算で計算できる．そのため，Millerアルゴリズムは，p のビット長に対する多項式 $\mathcal{O}((\log p)^3)$ で計算可能である．また, Millerアルゴリズムを高速化する方法として，分母 $g_h(\psi(Q))$ の計算を省略する方法，ℓ の 2 進展開におけるハミング重みを下げる方法，ヤコビアン座標を用いる方法などが知られている [12]．最近の実装結果では，ペアリング写像は同じセキュリティレベルの RSA 暗号と同じ程度の速度で実装できることが報告されている [21, 11].

4.2 ID ベース暗号

簡約 Tate ペアリング $\hat{e}$ の双線形性により，個人の公開鍵を自由なビット列をして選ぶことができる ID ベース暗号が実現できる [18, 20].

[**システムパラメータ生成**] 標数pに対して, 大きな素数位数ℓを持つ楕円曲線$E^b(p)$を生成して, 部分群$E^b(p)[\ell]$の生成元をPとする．マスター鍵$s \in \{0, 1, \ldots, \ell-1\}$を生成して，$Q = sP$とする．システムパラメータとして$\ell$, P, Qをユーザ全体で共有する．

[**公開鍵および秘密鍵**] ユーザのIDに対応する点$Q_{ID} \in E^b(p)$を生成して，ユーザの秘密鍵を$S_{ID} = sQ_{ID}$とする．

[**暗号化**] 平文mを$GF(p^2)$の元とする．乱数$r \in \{0, 1, 2, \ldots, \ell - 1\}$を発生して，システムパラメータ$P$, Qおよび公開鍵Q_{ID}に対して，$C_1 = rP \in E^b(p)$, $c_2 = m\hat{e}(Q_{ID}, Q)^r \in GF(p^2)$を計算する．$(C_1, c_2)$を暗号文とする．

[**復号化**] 暗号文(C_1, c_2)に対して，秘密鍵$S_{ID} \in E^b(p)$を利用して，復号化$m = c_2\hat{e}(S_{ID}, C_1)^{-1} \in GF(p^2)$を行う．

ここで,

$$c_2\hat{e}(S_{ID}, C_1)^{-1} = m\hat{e}(Q_{ID}, Q)^r\hat{e}(S_{ID}, C_1)^{-1} = m\hat{e}(Q_{ID}, P)^{rs}\hat{e}(Q_{ID}, P)^{-rs} = m$$

が成立つため，平文mは一意的に復号可能である．

IDベース暗号では各ユーザのIDの点Q_{ID}に対して秘密鍵S_{ID}を生成するため，RSA暗号や楕円曲線暗号と異なり，公開鍵Q_{ID}のx座標を自由なビット列 (例えば

`takagi@imi.kyushu-u.ac.jp`

など) として選ぶことが可能となる．一方，IDベース暗号と同様の構成を楕円曲線暗号で行う場合は，ユーザIDの点Q_{ID}に対して生成元Gから$Q_{ID} = sG$を満たす秘密鍵sを求める必要があり，離散対数問題を解く程度の困難性があるため実現することは難しい．

IDベース暗号の安全性は，有限体$GF(p^2)$および楕円曲線$E^b(p)$の離散対数問題の困難性を基にしている．実際，システムパラメータP, Qに対して$Q = sP$を満たすマスター鍵sを求める問題は，楕円曲線$E^b(p)$の離散対数問題である．前節の楕円曲線暗号で述べたように，この問題の解読には指数時間$\mathcal{O}(\sqrt{\ell})$が必要となり，ℓは160ビット以上とする必要がある．また，任意$R \in E^b(p)$に対して，$\hat{e}(R, Q) = \hat{e}(R, sP) = \hat{e}(R, P)^s$となるため，有限体$GF(p^2)$上の$\hat{e}(R, Q)$, $\hat{e}(R, P)$に対する離散対数問題が解読されてもマスター鍵sを求めることができる．有限体$GF(p^2)$上の離散対数問題を解読する最も高速なアルゴリズムは数体篩法であり，準指数時間$\mathcal{O}(\exp(((64/9)^{1/3} + o(1))(\log p^2)^{1/3}(\log\log p^2)^{2/3})$で計算可能である．素因数分解アルゴリズムで用いられる数体篩法と同じ計算量であり，RSA暗号と同等の安全性となる．

ペアリング写像を計算するAlgorithm 1及びその高速化版は，様々な計算プラットフォームおいて実装されている [1, 21, 11]．例えば，市販されている携帯電話においてもソフトウェア実装が行われている．BREW携帯電話 (ARM9 225MHz) では0.3秒程度 [21]，Android携帯電話では1〜2秒程度 [11] にて計算可能である．携帯電話上でもIDベース暗号は実用的な速度で実装可能である．

5 まとめ

本章では，情報セキュリティを支える基礎技術である公開鍵暗号について，RSA 暗号，楕円曲線暗号，最新のペアリング暗号までを含めて解説した．また，従来の RSA 暗号や楕円曲線暗号では実現が難しいとされていた ID ベース暗号の構成方法を説明し，ペアリング暗号を市販の携帯電話で実装した性能データを紹介した．ペアリング暗号の新しい応用技術として，効率的なブロードキャスト暗号 [6] やキーワード検索暗号 [5] などが提案されており，進展の速い研究分野である．2007 年からペアリング暗号を専門にした国際会議 Pairing-Based Cryptography [19] も開催されている．ペアリング暗号の今後の更なる研究進展が注目されている．

参考文献

[1] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase and T. Takagi, "Algorithms and Arithmetic Operators for Computing the EtaT Pairing in Characteristic Three," IEEE Transactions on Computers, Vol. 57, No. 11, pp. 1454–1468, 2008.

[2] I. Blake, G. Seroussi, N. Smart, *E*lliptic Curves in Cryptography, London Mathematical Society, Lecture Note Series 265, 1999.

[3] I. Blake, G. Seroussi, N. Smart (eds), *A*dvances in Elliptic Curve Cryptography, London Mathematical Society, Lecture Note Series 317, 2005.

[4] D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing," SIAM Journal of Computing, Vol. 32, No. 3, pp. 586–615, 2003.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, "Public Key Encryption with Keyword Search," EUROCRYPT 2004, LNCS 3027, pp. 506–522, Springer-Verlag, 2004.

[6] D. Boneh, C. Gentry and B. Waters, "Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys," CRYPTO 2005, LNCS3621, pp. 258–275, Springer-Verlag, 2005.

[7] D. Boneh and R. Venkatesan, "Breaking RSA May not be Equivalent to Factoring," EUROCRYPT'98, LNCS 1233, pp. 59–71, Springer, 1998.

[8] H. Cohen, A. Miyaji, T. Ono, "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates," ASIACRYPT 1998, LNCS 1514, pp. 51–65, Springer-Verlag, 1998.

[9] Cryptography Research and Evaluation Committees, `http://www.cryptrec.jp/`.

[10] D. Hanerson, A. Menezes and S. Vanstone, `Guide to Elliptic Curve Cryptography`, Springer, 2003.

[11] 井山政志, 清本晋作, 福島和英, 田中俊昭, 高木剛, "携帯電話におけるペアリング暗号の実装," 電子情報通信学会論文誌, Vol. J95-A, No. 7, pp. 579–587, 2012.

[12] T. Izu, T. Takagi, "Efficient Computations of the Tate Pairingfor the Large MOV Degrees," ICISC 2002, LNCS 2513, pp. 283–297, 2002.

[13] N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, Vol. 48, pp. 203–209, 1987.

[14] A.K. Lenstra and H.W. Lenstra, Jr. (eds.), *T*he Development of the Number Field Sieve, Lecture Notes in Mathematics 1554, Springer, 1993.

[15] V. Miller, “Use of Elliptic Curves in Cryptography,” CRYPTO 1985, LNCS 218, pp. 417–426, Springer-Verlag, 1985.

[16] V. Miller, “The Weil Pairing, and Its Efficient Calculation,” Journal of Cryptology, Vol. 17, No. 4, pp. 235–261, 2004.

[17] R. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, Vol. 21, No. 2, pp. 120–126, 1978.

[18] R. Sakai, K. Ohgishi and M. Kasahara, “Cryptosystems Based on Pairing,” The 2000 Symposium on Cryptography and Information Security, SCIS2000-C20, 2000.

[19] T. Takagi, T. Okamoto, E. Okamoto and T. Okamoto (Eds.), *P*airing-Based Cryptography – Pairing 2007, LNCS 4575, Springer-Verlag, 2007.

[20] 辻井重男, 笠原正雄 (篇), 暗号理論と楕円曲線, 森北出版, 2008.

[21] M. Yoshitomi, T. Takagi, S. Kiyomoto, T. Tanaka, “Efficient Implementation of the Pairing on Mobilephones using BREW”, IEICE Transaction, Vol. E91-D, No. 5, pp. 1330–1337, 2008.

Code-Based Public-Key Encryption

Kirill Morozov
Institute of Mathematics for Industry, Kyushu University

1 Introduction

The first public-key encryption (PKE) scheme based on error-correcting codes was introduced by McEliece in 1978 [28]. This scheme used Goppa codes [16, 26], a subclass of alternant codes, which has the following useful features: 1) The lower bound on the minimal distance (and hence the number of correctable errors) is known; 2) Hardness of recovering the decoding algorithm from a proper representation of the code – the meaning of this property will be explained later. In this section, we consider only irreducible Goppa codes over $\mathbb{F}_2$, and just note that working with codes over $\mathbb{F}_q$, $q > 2$ may offer some advantages [6]. There were many attempts to use different classes of codes in the McEliece-type encryption schemes, but some of them turned out to be insecure, while others are currently under evaluation – we leave this topic out of scope of this survey.

Another famous code-based PKE scheme was introduced by Niederrieter in 1986 [30]. Originally, Generalized Reed-Solomon (GRS) codes were proposed to be used, however this construction was shown insecure by Sidelnikov and Shestakov [40]. Nonetheless, when Goppa codes are employed, the security of Niederreiter PKE is equivalent to that of McEliece PKE as shown by Li et al [24]. We refer the reader to the survey by Engelbert et al for details [12].

The main advantage of the above code-based PKE's is that there is no efficient attack on this system using quantum computers [5]. This makes them candidates for postquantum PKE [33]. Although at this moment, quantum computers exist only as early prototypes, it is important to consider secure alternatives to currently used cryptographic systems (such as RSA [36]) which are not quantum-tolerant [33]. Another important advantage of these PKE is their fast encryption and decryption algorithms, that admit implementation even for embedded and memory-constraint devices, see e.g. [11, 42, 17].

The main disadvantage of both McEliece and Niederreiter PKE is relatively large public key size.

Recent research on code-based encryption proceeds in the following main directions:[1]

- Attacks on underlying assumptions: decoding attacks [7, 1], structural attacks [38, 13].
- Study on compact keys [3].
- Alternatives to Goppa codes [34].
- Efficient and compact implementations: [11, 42, 17].
- Advanced cryptographic protocols for code-based PKE [10, 27, 18].

In the rest of this presentation, I will focus on McEliece PKE.

[1] Note that this collection of references is by no means comprehensive – it only contains some of representative works on the topics in question.

2 Background

2.1 Notation

Let J be an ordered subset as follows: $\{j_1, \ldots, j_m\} = J \subseteq \{1, \ldots, n\}$, then we denote a vector $(x_{j_1}, \ldots, x_{j_m}) \in \mathbb{F}_2^m$ by x_J. Similarly, we denote by M_J the submatrix of a $(k \times n)$ matrix M consisting of the columns which correspond to the indexes of J. A concatenation of vectors $x \in \mathbb{F}_2^{n_0}$ and $y \in \mathbb{F}_2^{n_1}$ is written as $(x|y) \in \mathbb{F}_2^{n_0+n_1}$. For $x, y \in \mathbb{F}_2^m$, $x + y$ denotes a bitwise exclusive-or. We denote by $x \xleftarrow{\$} \mathcal{X}$ a uniformly random selection of an element from its domain $\mathcal{X}$.

2.2 Elements of Coding Theory

2.2.1 Linear Codes

A binary (n, k)-code $\mathcal{C}$ is a k-dimensional subspace of the vector space $\mathbb{F}_2^n$; n and k are called the *length* and the *dimension* of the code, respectively. We call $\mathcal{C}$ an (n, k, d)-code, if its so-called *minimum distance* is $d := \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} d_H(x, y)$, where d_H denotes the Hamming distance (i.e. the number of positions where x and y differ). The distance of $x \in \mathbb{F}_2^n$ to the zero-vector 0^n denoted by $w_H(x) := d_H(x, 0^n)$ is called the *weight* of x. We will write $\mathbf{0}$ to represent the zero-vector 0^n, omitting n which will be clear from the context.

For the relevant topics in coding theory we refer the reader to [37, 26].

2.2.2 Goppa Codes

In this subsection, we will follow the presentation of [12]. Let us first define a binary irreducible Goppa code of length n. Set $m = \log_2 n$. Let t be an integer – in fact, it will be an upper bound on the number of errors, which the code corrects.

Let $g(X) = \sum_{i=0}^{t} g_i X^i \in \mathbb{F}_{2^m}[X]$ be a monic polynomial of degree t called the *Goppa polynomial* and $L = (\gamma_0, \ldots, \gamma_{n-1}) \in \mathbb{F}_{2^m}^n$ called the *support*, which is a tuple of n distinct elements such that $g(\gamma_i) \neq 0$, for all $0 \leq i \leq n - 1$.

For any vector $y \in \mathbb{F}_2^n$, define the *syndrome* of y by $S_y(X) := \sum_{i=0}^{n-1} \frac{y_i}{X - \gamma_i} \mod g(X)$, where y_i denotes the i-th bit of y.

Definition 2.1. The binary Goppa code $\mathcal{G}(L, g(X))$ is the set of all vectors $y \in \mathbb{F}_2^n$ such that the identity $S_y(X) = 0$ holds in the polynomial ring $\mathbb{F}_{2^m}[X]$.

If $g(X)$ is irreducible over $\mathbb{F}_{2^m}$, then $\mathcal{G}(L, g(X))$ is called an *irreducible binary Goppa code*.

Parity-Check and Generator Matrices. A parity-check matrix of $\mathcal{G}(L, g(X))$ can be written as: $H = XYZ$, where

$$X = \begin{pmatrix} g_t & 0 & 0 & \cdots & 0 \\ g_{t-1} & g_t & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & g_3 & \cdots & g_t \end{pmatrix},$$

$$Y = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma_0 & \gamma_1 & \cdots & \gamma_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_0^{t-1} & \gamma_1^{t-1} & \cdots & \gamma_{n-1}^{t-1} \end{pmatrix},$$

and $Z = \mathrm{Diag}_n(g(\gamma_0)^{-1}, g(\gamma_1)^{-1}, \ldots, g(\gamma_{n-1})^{-1})$, where $\mathrm{Diag}_n(\cdot)$ denotes the diagonal matrix of size n with the arguments being the elements of the main diagonal. Since X is a $k \times k$ invertible matrix, it represents an equivalent code. Therefore, one may omit X, and compute $H = YZ$.

We have

$$y \in \mathcal{G}(L, g(X)) \text{ if and only if } Hy^T = 0. \tag{1}$$

The entries of H are elements of the extension field $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. In order to obtain the binary form of H, we use a representation of $\mathbb{F}_{2^m}$ as a vector space over $\mathbb{F}_2$. Then, we write H as a $mt \times n$ matrix over $\mathbb{F}_2$.

Now, we need to compute the generator matrix G of the code $\mathcal{G}$. It follows by (1) that the Goppa code consists of the vectors belonging to the kernel (or the null space) of H. Therefore, a generator matrix G will consist of the basis vectors of such the kernel.

Since H is an $mt \times n$ matrix, G is $k \times n$ with $k \geq n - mt$, defining the (n, k) Goppa code.

Error Correction. For any codeword $y \in \mathcal{G}(L, g(X)) \setminus \mathbf{0}$, the following relation holds [12]: $w_H(\mathbf{y}) \geq 2 \deg g(X) + 1$. We have $\deg g(X) = t$, therefore the code $\mathcal{G}$ corrects up to t errors.

As the decoding algorithm $\mathsf{Dec}_{\mathcal{G}}$ used for decryption, we will employ the algorithm by Patterson [32]. We refer the reader to [12] for further details.

2.3 Security Assumptions

Definition 2.2 (General Decoding (G-SD) Problem).
Input: $G \xleftarrow{\$} \mathbb{F}_2^{k \times n}$, $c \xleftarrow{\$} \mathbb{F}_2^n$ and $0 < t \in \mathbb{N}$.
Decide: If there exists $x \in \mathbb{F}_2^k$ such that $e = xG + c$ and $w_H(e) \leq t$.

This problem was shown to be NP-complete by Berlekamp et al [4].

The following two problems use the quantities defined in Section 3. No polynomial-time algorithm is known for solving them [12, 14, 7].

Definition 2.3 (McEliece Problem).
Input: A McEliece public key (G^{pub}, t), where $G^{\mathrm{pub}} \in \mathbb{F}_2^{k \times n}$, $0 < t \in \mathbb{N}$;
and a McEliece ciphertext $c \in \mathbb{F}_2^n$.
Output: $m \in \mathbb{F}_2^k$ such that $d_H(mG^{\mathrm{pub}}, c) = t$.

Definition 2.4 (Goppa Code Distinguishing (GD) Problem).
Input: $G \in \mathbb{F}_2^{k \times n}$.
Decide: Is G a parity-check matrix of an (n, k) irreducible Goppa code, or of a random (n, k)-code?

A major step for solving the above problem was made by Faugère et al [13] by introducing a distinguisher for *high rate* Goppa codes, however this distinguisher does not work for typical parameters of the McEliece PKE. Nonetheless, it shows that the above assumption must be used in security proofs with extra care, to say the least.

3 McEliece Cryptosystem

The McEliece PKE consists of the following triplet of algorithms $(\mathcal{K}, \mathcal{E}, \mathcal{D})$:

- System parameters: $n, k, t \in \mathbb{N}$.
- Key generation algorithm $\mathcal{K}$: On input n, k, t, generate the following matrices:
  - $G \in \mathbb{F}_2^{k \times n}$ – the generator matrix of an irreducible binary Goppa code correcting up to t errors. Its decoding algorithm is denoted as $\mathsf{Dec}_{\mathcal{G}}$.
  - $S \in \mathbb{F}_2^{k \times k}$ – a random non-singular matrix.
  - $P \in \mathbb{F}_2^{n \times n}$ – a random permutation matrix (of size n).
  - $G^{\text{pub}} = SGP \in \mathbb{F}_2^{k \times n}$.

  Output the public key $pk = (G^{\text{pub}}, t)$ and the secret key $sk = (S, G, P, \mathsf{Dec}_{\mathcal{G}})$.
- Encryption algorithm $\mathcal{E}$: On input a plaintext $m \in \mathbb{F}_2^k$ and the public key pk, choose a vector $e \in \mathbb{F}_2^n$ of weight t at random, and output the ciphertext

$$c = mG^{\text{pub}} + e.$$

- Decryption algorithm $\mathcal{D}$: On input c and the secret key sk, calculate:
  - $cP^{-1} = (mS)G + eP^{-1}$.
  - $mSG = \mathsf{Dec}_{\mathcal{G}}(cP^{-1})$.
  - Let $J \subseteq \{1, \ldots, n\}$ be s.t. G_J is invertible. Output $m = (mSG)_J (G_J)^{-1} S^{-1}$.

It is easy to check that the decryption algorithm correctly recovers the plaintext: Since in the first step of decryption, the permuted error vector eP^{-1} is again of weight t, the decoding algorithm $\mathsf{Dec}_{\mathcal{G}}$ successfully corrects these errors in the next step.

3.1 Security Analysis

Let us discuss two major types of attacks against McEliece PKE.

Decoding Attack. For the parameter sizes related to McEliece PKE, the best algorithm is the *information-set decoding* [22, 23, 41, 8, 35, 7, 1]. The time complexity of this algorithm is sub-exponential and for the relevant parameters can be (conservatively) lower-bounded by the following expression [12]: $O(n^3)2^{-t \log_2(1-k/n)}$.

Structural Attack. If we employ the irreducible binary Goppa codes, then up to date, there is no efficient algorithm which can extract the secret key from the public key in the McEliece or the Niederreiter cryptosystems as long as the so-called weak keys [25] are avoided. Moreover, there is no algorithm which can efficiently distinguish the matrices defined by the McEliece public keys and the same size generator matrices of random codes, for the typical parameters. The time complexity of the currently best algorithm [9] is still sub-exponential.

Equivalent security (bits)	85	112	129
Code length n	1652	2440	2798
Code dimension k	1203	1877	2088
Weight of error vector t	42	50	62
Public key size (Kbytes)	66	129	181

Table 1: Examples of Parameter Sets for the McEliece PKE ([29]).

Intuitively this algorithm works as follows: enumerate Goppa polynomials and verify whether each corresponding code and the code generated by G^{pub} are "permutation equivalent" or not by using the *support splitting algorithm* [38], which results in a $n^t(1 + o(1))$-time algorithm.

A formal security proof of the McEliece PKE can be found in [39]. For details on the attacks described above and their countermeasures, we refer the reader to the surveys in [19, 12].

Some parameter sets along with their estimated security levels computed in [29] are provided in Table 1.

4 Secure Conversions for McEliece PKE

4.1 Chosen Plaintext Security

The *semantic security* (also called *indistinguishability under chosen plaintext attacks or IND-CPA*) defined by Goldwasser and Micali [15] is a security notion for public-key encryption. Its intuitive meaning is that a ciphertext does not leak any useful information about the plaintext except for its length. More precisely, suppose that the attacker is allowed to pick any pair of plaintexts. Then given a ciphertext, she must not be able to find out, which one was encrypted.

Nojima et al [31] show that the McEliece encryption with a random padding of the plaintext (which is multi-bit) is IND-CPA secure under hardness of the learning parities with noise (LPN) problem[2] and GD problem. A little more formally, the Randomized McEliece encryption is constructed in the same way as described above, except that the ciphertext $c = (r|m)G^{\text{pub}} + e$, where $r \xleftarrow{\$} \{0,1\}^{k_0}$, $m \in \{0,1\}^{k_1}$, $k = k_0 + k_1$. A particular choice of k_0 and k_1 is discussed in [31]. A similar padding will provide IND-CPA security for Niederreiter PKE as well [31].

4.2 Chosen Ciphertext Security

In some cases, a limited access to *decryption* algorithm is available to an attacker. It may sound somewhat counter-intuitive, but one can imagine some mailing service that automatically decrypts the received correspondence, and the adversary having access to the results of decryption. The point here is that the result of decryption must not reveal any additional

[2]See e.g. [20] for a formal definition of LPN problem – it is similar to G-SD problem except that in the error vector e, each bit has Bernoulli distribution with fixed p, $0 < p < 0.5$.

information (for instance, nothing about the secret key), apart from the decrypted message(s) themselves.

Public-key encryption is *indistinguishable against the adaptive chosen ciphertetxt attack (IND-CCA2)*, if in the IND-CPA scenario described in the previous chapter, the attacker is allowed to access the decryption algorithm (but not the secret key). Naturally, the attacker is allowed to request decryption of any plaintext, except those to be distinguished.

An IND-CCA2 conversion for the McEliece PKE in the random oracle model was presented by Kobara and Imai [21]. The random oracle model [2] assumes cryptographic hash functions to behave like random functions, hereby simplifying security proofs. Recently, IND-CCA2 conversions that do not use random oracles were presented for McEliece PKE [10] and for Niederreiter PKE [27].

5 Conclusion

We presented a summary of the McEliece public-key encryption scheme which is based on error-correcting codes by Goppa. We described major attacks on this system, secure parameters set, and conversions enhancing its security.

Current research trends in PKE based on error-correcting codes include studies on compact keys, related cryptographic protocols and fast implementations.

References

[1] A. Becker, A. Joux, A. May, and A. Meurer: Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding. EUROCRYPT 2012: 520–536.

[2] M. Bellare and P. Rogaway: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. ACM Conference on Computer and Communications Security 1993: 62–73.

[3] T. Berger, P. Cayrel, P. Gaborit, and A. Otmani: Reducing Key Length of the McEliece Cryptosystem. AFRICACRYPT 2009: 77–97.

[4] E. Berlekamp, R. McEliece, and H. van Tilborg: On the inherent intractability of certain coding problems. IEEE Trans. on Inf. Theory 24, 1978: 384–386.

[5] D. J. Bernstein: Grover vs. McEliece. PQCrypto 2010: 73–80.

[6] D. J. Bernstein, T. Lange, and C. Peters. Wild McEliece. Selected Areas in Cryptography 2010: 143–158.

[7] D. J. Bernstein, T. Lange, and C. Peters: Smaller Decoding Exponents: Ball-Collision Decoding. CRYPTO 2011: 743–760.

[8] A. Canteaut and F. Chabaud: A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH-codes of length 511. IEEE Transactions on Information Theory 44, 1998: 367–378.

[9] N. Courtois, M. Finiasz, and N. Sendrier: How to achieve a McEliece-based Digital Signature Scheme. ASIACRYPT 2001: 157–174.

[10] N. Döttling, R. Dowsley, J. Müller-Quade, and A. Nascimento: A CCA2 Secure Variant of the McEliece Cryptosystem. IEEE Transactions on Information Theory 58(10), 2012: 6672–6680.

[11] T. Eisenbarth, T. Güeysu, S. Heyse, and C. Paar: MicroEliece: McEliece for Embedded Devices", CHES 2009: 49–64.
[12] D. Engelbert, R. Overbeck and A. Schmidt: A Summary of McEliece-Type Cryptosystems and their Security, Journal of Mathematical Cryptology, vol. 1, Walter de Gruyter, 2007: 151–199.
[13] J. Faugère, A. Gauthier-Umaña, V. Otmani, L. Perret, and J. Tillich: A Distinguisher for High Rate McEliece Cryptosystems. Information Theory Workshop (ITW) 2011: 282–286.
[14] M. Finiasz and N. Sendrier: Security Bounds for the Design of Code-Based Cryptosystems. ASIACRYPT 2009: 88–105.
[15] S. Goldwasser and S. Micali: Probabilistic Encryption. Journal of Computer and System Sciences 28, :270–299 (1984).
[16] V. Goppa: A new class of linear error-correcting code (in Russian). Problemy Peredachi Informacii 6, Sept. 1970: 24–30.
[17] S. Heyse: Low-Reiter: Niederreiter Encryption Scheme for Embedded Microcontrollers. PQCrypto 2010: 165–181.
[18] R. Hu, K. Morozov, and T. Takagi: Proof of Plaintext Knowledge for Code-Based Public-Key Encryption Revisited (Short Paper), *To appear in* AsiaCCS 2013.
[19] G. Kabatiansky, E. Krouk and S. Semenov: Error Correcting Codes and Security for Data Networks. Wiley, 2005.
[20] J. Katz and J. Shin: Parallel and Concurrent Security of the HB and HB$^+$ Protocols. EUROCRYPT 2006: 73–87.
[21] K. Kobara and H. Imai: Semantically Secure McEliece Public-Key Cryptosystems – Conversions for McEliece PKC. PKC 2001: 19–35.
[22] P. Lee and E. Brickell: An observation on the security of McEliece's public key cryptosystem. EUROCRYPT 1988: 275–280.
[23] J. Leon: A probabilistic algorithm for computing minimum weights of large error-correcting codes. IEEE Transactions on Information Theory 34, 1988: 1354–1359.
[24] Y. Li, R. Deng, and X. Wang: The Equivalence of McEliece's and Niederreiter's Public-Key Cryptosystems. IEEE Transactions on Information Theory 40, 1994: 271–273.
[25] P. Loidreau and N. Sendrier: Weak keys in the McEliece public-key cryptosystem, IEEE Transactions on Information Theory 47(3), 2001: 1207–1211.
[26] F. MacWilliams and N. Sloane: The Theory of Error-Correcting Codes. North-Holland Amsterdam, 1992.
[27] K. Mathew, S. Vasant, S. Venkatesan, and C. Rangan: An Efficient IND-CCA2 Secure Variant of the Niederreiter Encryption Scheme in the Standard Model. ACISP 2012: 166–179.
[28] R. McEliece: A Public-Key Cryptosystem Based on Algebraic Coding Theory. Deep Space Network Progress Report, 1978.
[29] R. Niebuhr, M. Meziani, S. Bulygin, and J. Buchmann: Selecting parameters for secure McEliece-based cryptosystems. International Journal of Information Security 11(3), 2012: 137–147.
[30] H. Niederreiter. Knapsack-type Cryptosystems and Algebraic Coding Theory. Problems of Control and Information Theory 15(2), 1986: 159–166.
[31] R. Nojima, H. Imai, K. Kobara, and K. Morozov: Semantic security for the McEliece

cryptosystem without random oracles. Designs Codes and Cryptography 49 (1-3), 2008: 289–305.
[32] N. Patterson: The algebraic decoding of Goppa codes. IEEE Transactions on Information Theory 21, 1975: 203–207.
[33] R. Perlner and D. Cooper: Quantum resistant public key cryptography: a survey. IDtrust 2009: 85–93.
[34] E. Persichetti: Compact McEliece keys based on quasi-dyadic Srivastava codes. Journal of Mathematical Cryptology 6(2), 2012: 149–169.
[35] C. Peters: Information-Set Decoding for Linear Codes over F_q. PQCrypto 2010: 81–94.
[36] R. Rivest, A. Shamir, and L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communication of ACM 21(2), 1978: 120–126.
[37] R. Roth: Introduction to coding theory. Cambridge University Press, 2006.
[38] N. Sendrier: Finding the Permutation Between Equivalent Linear Codes: The Support Splitting Algorithm. IEEE Transactions on Information Theory 46(4), 2000: 1193–1203.
[39] N. Sendrier: On the security of the McEliece public-key cryptosystem. Information, Coding and Mathematics – Proceedings of Workshop honoring Prof. Bob McEliece on his 60th birthday, Kluwer, 2002: 141-163.
[40] V. Sidelnikov and S. Shestakov: On the Insecurity of Cryptosystem Based on Generalized Reed-Solomon Codes. Discrete Mathematics and Applications 2(4), 1992: 439–444.
[41] J. Stern: A method for finding codewords of small weight. Coding Theory and Applications 388, 1989: 106–133.
[42] F. Strenzke: A Smart Card Implementation of the McEliece PKC. WISTP 2010: 47–59.

Integers factorization using elliptic curve method (ECM)

Cristian Virdol

Institute of Mathematics for Industry, Kyushu University

1 Elliptic curve method (ECM)

Let n be a positive integer. We describe Lenstra elliptic curve factorization method to find a nontrivial factor of n (i.e. a positive divisor of n distinct from 1 and n; of course such a factor exists only when n is not a prime number). The method has the following steps:

1. Choose an arbitrary elliptic curve E over $\mathbb{Z}/n\mathbb{Z}$, given by an equation of the form $y^2 = x^3 + ax + b \pmod n$, and a non-trivial point P on E. The easiest way to do this is to choose first a point $P = (x, y)$ with arbitrary non-zero coordinates x, $y \pmod n$, then choose a random non-zero $a \pmod n$, and then define $b := y^2 - x^3 - ax \pmod n$.

2. One then computes some multiples $kP = P + \cdots + P$ (k times) of the point P using the standard addition rule on our elliptic curve E: given two points $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ on the E, their sum is

$$R = P + Q = (x_R, y_R),$$

with

$$x_R = s^2 - x_P - x_Q,$$

and

$$y_R = -y_P - s(x_R - x_P),$$

where

$$s = (y_P - y_Q)/(x_P - x_Q)$$

is the *slope* of the line connecting P and Q. Hence these formulas contain the *slope* of the line connecting P and Q, and thus involve divisions between residue classes modulo n, which can be performed using the standard Euclidean algorithm. In particular, a division by some $v \pmod n$ involves the calculation of the greatest common divisor $\gcd(v, n)$. If the slope is of the form u/v with $\gcd(u, n) = 1$, then $v = 0 \pmod n$ means that the result of the addition will be the point at infinity: ∞ on E. However, if $\gcd(v, n) \neq 1, n$, then the addition will not produce a meaningful point on E, which shows that E is not a group $\pmod n$, but, more importantly that $\gcd(v, n)$ is a non-trivial factor of n.

3. So one computes eP on $E \pmod n$, where e is product of many small numbers: let's say, a product of small primes raised to small powers, as in the usual $p - 1$ algorithm, or $B! = 1 \cdot \cdots \cdot B$ for some small B. This can be done efficiently, one small factor at a time. Let's say, to obtain $B!P$, first compute $2P$, then $3(2P)$, then $4(3!P)$, etc. In order for the addition $B!P$ to be performed in reasonable time, one, of course, has to choose B sufficiently small.

4. We distinguish the following three cases:

A. If we were able to finish all the above calculations without encountering non-invertible elements (mod n), then we need to try again with some other E and P.

B. If we found $kP = \infty$ at some stage, then again we should start over with a new E and P.

C. If we encountered at some stage a $\gcd(v, n) \neq 1, n$, then we are done, because $\gcd(v, n)$ is a nontrivial factor of n.

The time complexity of ECM depends only on the size of the smallest prime factor p of n and can be represented by $L_p[\frac{1}{2}, \sqrt{2}] = O(e^{(\sqrt{2}+o(1))\sqrt{(\ln p)(\ln \ln p)}})$.

2 The reason why the ECM works

With the same notations as above, assume that p and q are two distinct prime divisors of n. Then $y^2 = x^3 + ax + b \pmod{n}$ implies the same equation also modulo p and modulo q. These two new smaller elliptic curves with the usual addition are now genuine groups. If these groups have N_p and N_q elements, respectively, then for any point P on the original curve we have $N_pP = \infty$ and $N_qP = \infty$. By Lagrange's theorem, if k is minimal positive integer such that $kP = \infty$ on the curve modulo p (or mod q), then $k \mid N_p$ (or $k \mid N_q$). From Hasse's theorem we know that

$$|p + 1 - N_p| < |2\sqrt{p}|,$$

and

$$|q + 1 - N_q| < |2\sqrt{q}|.$$

When the elliptic curve is chosen randomly, then N_p and N_q are random numbers close to $p+1$ and $q+1$, respectively. Therefore it is unlikely that most of the prime factors of N_p and N_q are the same, and it is quite likely that while computing eP, we will encounter some kP that is ∞ modulo p but not modulo q, or vice versa. When this is the case, kP does not exist on the original curve, and in the computations we found some v with either $\gcd(v, p) = p$ or $\gcd(v, q) = q$, but not both. This means that $\gcd(v, n)$ is a non-trivial factor of n.

ECM is a major improvement of the older $p - 1$ algorithm. The $p - 1$ algorithm finds prime factors p such that $p - 1$ is b-powersmooth for small values of b. For any e, a multiple of $p - 1$, and any a relatively prime to p, by Fermat's little theorem we have $a^e \equiv 1 \pmod{p}$. Then $\gcd(a^e - 1, n)$ is likely to produce a factor of n. However, the algorithm does not work when $p - 1$ has large prime factors, as is the case for numbers containing strong primes, for example.

ECM avoids this obstacle by considering the group of a random elliptic curve over the finite field $\mathbb{F}_p$ with p elements, rather than considering the multiplicative group of $\mathbb{F}_p$ which always has order $p-1$. As we said above, the order of the group of an elliptic curve E over $\mathbb{F}_p$ varies (quite randomly) between $p+1-2\sqrt{p}$ and $p+1+2\sqrt{p}$ by Hasse's theorem, and is likely to be smooth for some elliptic curves. Although there is no proof that a smooth group order will be found in the Hasse-interval, by using heuristic probabilistic methods, the Sato-Tate conjecture proved by Taylor and his collaborators (see [3] and §3 below for a sketch of the proof), the Canfield-Erdős-Pomerance theorem with suitably optimized parameter choices,

and the L-notation, we can expect to try $L[\sqrt{2}/2, \sqrt{2}]$ curves before getting a smooth group order. We remark that this heuristic estimate is actually very reliable in practice.

3 Sato-Tate conjecture

Again, as we said, the order of an elliptic curve E over $\mathbb{F}_p$ varies (quite randomly) between $p+1-2\sqrt{p}$ and $p+1+2\sqrt{p}$ by Hasse's theorem. In this section we will see what means "quite randomly". This description is given by Sato-Tate conjecture which was proved recently by Taylor and his collaborators (see [3]). Below we will state this conjecture and outline the main ideas of the proof. Let E be an elliptic curve given by $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. Let p be a prime number, and let N_p be the number of the elements of E mod p. As we said in §2 above, from Hasse's theorem we know that

$$|p + 1 - N_p| < |2\sqrt{p}|,$$

and hence there exists a unique θ_p, with $0 \leq \theta_p \leq \pi$ such that

$$p + 1 - N_p = 2\sqrt{p}\cos\theta_p.$$

Assume now that E has no complex multiplication. Then Sato-Tate conjecture predicts that for every two real numbers α and β for which $0 \leq \alpha \leq \beta \leq \pi$, we have

$$\lim_{N\to\infty} \frac{|\{p \leq N \mid \alpha \leq \theta_p \leq \beta\}|}{|\{p \leq N\}|} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta\, d\theta.$$

As we mentioned, Sato-Tate conjecture was prove by Taylor and his collaborators in [3] combined with other supporting articles.

3.1 Sketch of the proof of Sato-Tate conjecture

We define

$$a_p := p + 1 - N_p.$$

Then from Hasse's theorem we know that

$$|a_p| < 2\sqrt{p}.$$

Hence the quadratic polynomial

$$X^2 - a_p X + p$$

has two complex (no real) roots $\alpha_p p^{1/2}$ and $\beta_p p^{1/2}$, with $\alpha_p\beta_p = 1$ and $|\alpha_p| = |\beta_p| = 1$. For m a positive integer define the m-th symmetric L-function

$$L(s, \mathrm{Sym}^m E) := \prod_p \prod_{j=0}^{m} (1 - \alpha_p^j \beta_p^{m-j} p^{-s})^{-1}.$$

This product converges absolutely for $\mathrm{Re}(s) > 1$ (here $\mathrm{Re}(s)$ represents the real part of the complex number s). In [7], Serre showed that if for all positive integers m, $L(s, \mathrm{Sym}^m E)$

extends to $\mathrm{Re}(s) \geq 1$ and does not vanish there, then the Sato-Tate conjecture is true. In [6], Murty showed that the non-vanishing assumption is unnecessary. Thus, the Sato-Tate conjecture was reduced to proving the analytic continuation of $L(s, \mathrm{Sym}^m E)$ to the region $\mathrm{Re}(s) \geq 1$, for all positive integers m.

In 1970, Langlands [5] outlined a method of attacking the problem of analytic continuation. He suggested the existence of an automorphic representation π_m attached to $\mathrm{GL}(m+1)/\mathbb{Q}$, such that

$$L(s, \pi_m) = L(s, \mathrm{Sym}^m E),$$

where $L(s, \pi_m)$ is the automorphic L-function attached to π_m (the equality between the above L-functions is actually up to finitely many Euler factors). When $m = 1$, this is the Shimura-Taniyama conjecture which was proved by Wiles and others (see [8] and [1] and which implies the celebrated Fermat's Last Theorem. Langlands' functoriality conjecture predicts that the symmetric powers of π_1 are automorphic. This was proved for some small values of m (see [2] for a survey of the present state of knowledge). If the Langlands conjecture about the existence of π_m is true, then by the theory of automorphic representations, one immediately has analytic continuation of $L(s, \mathrm{Sym}^m E)$ to the entire complex plane and by the result of Murty [6], the non-vanishing on the line $\mathrm{Re}(s) = 1$ follows and the Sato-Tate conjecture follows. The non-vanishing of the L-function on the line $\mathrm{Re}(s) = 1$ can also be deduced from a celebrated result of Jacquet and Shalika [4] who showed that for any automorphic representation π, we have $L(s, \pi) \neq 0$, for $\mathrm{Re}(s) = 1$.

What Taylor and his collaborators prove in [3] is not the automorphy of $L(s, \mathrm{Sym}^m E)$ (or of $\mathrm{Sym}^m E$), but rather its potential automorphy. This fact, combined with other results in the analytic theory of automorphic L-functions, leads to the Sato-Tate conjecture. More exactly, Taylor's main theorem is: let K be a totally real field (i.e. K has the property that all of its embeddings into $\mathbb{C}$ factor through $\mathbb{R}$) and E/K an elliptic curve. Then for any odd natural number m, there exists a finite, totally real Galois extension L/K such that $\mathrm{Sym}^m E$ becomes automorphic over L. (One can also choose an L that will work simultaneously for any finite set of odd positive numbers m.) From this using Brauer's induction theorem combined with some tricks he is able to prove Sato-Tate conjecture for any elliptic curve E defined over any totally real number field K. We remark that Sato-Tate conjecture could be formulated also for abelian varieties and automorphic representations, and some of these questions are still open problems!

References

[1] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over **Q**: wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001), 843–939.

[2] J. Cogdell, H. Kim and R. Murty, Lectures on automorphic L-functions, Fields Institute Lecture Notes, Am. Math. Soc., Providence.

[3] M. Harris, N. Shepherd-Barron and R. Taylor, A family of Calabi-Yau varieties and potential automorphy, Annals of Math. **171** (2010), 779–813.

[4] H. Jacquet, J. Shalika, A non-vanishing theorem for zeta functions of GL_n, Inventiones Math. **38**(1) (1976/77) 1–16.

[5] R. P. Langlands, Problems in the theory of automorphic forms, in Lectures in Modern Analysis and Applications; Lecture Notes in Math. **170** Springer-Verlag, 18–86.
[6] K. V. Murty, On the Sato-Tate conjecture, in Number theory related to Fermat's last theorem (Cambridge, Mass.); 1982 Progress in Math. **26** 195–205 (Boston: Birkhauser).
[7] J-P. Serre, Abelian l-adic representations and elliptic curves, Research Notes in Mathematics 7 (Massachusetts: A. K. Peters, Wellesley).
[8] A. Wiles, Modular elliptic curves and Fermat's last theorem, Annals of Mathematics **141**, (1995), 443–551.

等周問題型変分問題の幾何—シャボン玉の数理解析—

小磯　深幸
九州大学マス・フォア・インダストリ研究所

1　はじめに

最も基本的な等周問題は，「平面内の同じ長さの閉曲線で囲まれる領域の中で，面積最大のものを求める」という問題であろう．答えは円である．この問題は，「平面内の同じ面積を囲む閉曲線の中で，長さが最小のものを求める」ことと同値である．次元を1つ上げると，「3次元ユークリッド空間内の同じ体積を囲む閉曲面の中で，面積最小のものを求めよ」となり，答えはもちろん球面である．

さて，自然界には，このように，「同じ体積を囲む閉曲面の中でのエネルギー極小解」を実現していると説明できる物質や現象が数多くある．その代表は，シャボン玉 (エネルギーは表面張力で，表面積に比例する) と水滴 (エネルギーは，表面張力＋重力) であろう．結晶のように表面の法線方向に依存するエネルギーを考える必要がある場合や，さまざまな境界条件が問題を複雑にする場合もある．

さて，このような，与えられた境界条件や付加的条件のもとで，「与えられたエネルギー汎関数の臨界点 (エネルギー汎関数の第1変分 $= 0$ のもの) を求めよ」という問題は，変分問題と呼ばれる．またその解は，エネルギー汎関数の第2変分が非負の時に，安定であるといわれる．特に，エネルギー最小解や極小解は安定であり，安定性について研究することは，理論・応用の両観点から重要である．

本稿では，まず，「同じ体積を囲む曲面の中での面積の臨界点」である平均曲率一定曲面の変分問題の解としての特徴付け (§3)，安定性の判定法 (§4)，体積または平均曲率をパラメータとした時の解の分岐の存在定理，分岐前後の解の安定性の判定法 (§5) について述べる．いわゆる pitchfork 分岐が現れ，エネルギー汎関数やその境界条件の持つ対称性よりも低い対称性しか持たない解が安定であり，高い対称性を持つ解が不安定になるという，「対称性の崩壊」現象が生じるための条件も定式化される．そして，これらの結果を簡単な自由境界問題に対して応用する (§6)．最後に，面積汎関数よりも一般の「非等方的表面エネルギー」に対する臨界点について言及する (§7)．

2　平均曲率の定義と例

まず，3次元ユークリッド空間 $\mathbf{R}^3$ 内の滑らかな曲面に対するパラメータ表示を与える．Σ を2次元の向き付け可能でコンパクトかつ連結な (境界を持つかもしれない) C^∞ 級多様体と

し，$X = (x^1, x^2, x^3)\colon \Sigma \to \mathbf{R}^3$ をはめ込み，$\nu = (\nu^1, \nu^2, \nu^3)\colon \Sigma \to S^2 := \{\nu = (\nu^1, \nu^2, \nu^3) \in \mathbf{R}^3\,;\, |\nu| = 1\}$ を X に沿う単位法ベクトル場とする．Σ の局所座標を (u^1, u^2) で表す．$\mathbf{R}^3$ のベクトル $\mathbf{u}$, $\mathbf{v}$ の標準的な内積を $\langle \mathbf{u}, \mathbf{v} \rangle$ で表す．

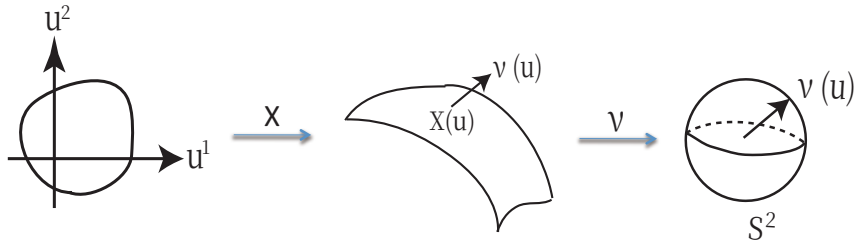


図 1：曲面とその単位法ベクトル ν

X の第 1 基本形式 ds^2, 第 2 基本形式 II は，

$$ds^2 = g_{ij}du^i du^j, \qquad \Big(g_{ij} := \langle X_i, X_j \rangle,\ X_i := \partial X/\partial u^i\Big),$$
$$\mathrm{II} = h_{ij}du^i du^j, \qquad \Big(h_{ij} := \langle \nu, X_{ij} \rangle = -\langle \nu_i, X_j \rangle,\ X_{ij} := \partial^2 X/\partial u^i \partial u^j\Big)$$

によって定義される．$(g^{ij}) := (g_{ij})^{-1}$ とおく．X の平均曲率 H, Gauss 曲率 K は，

$$H = h_{ij}g^{ij}/2, \qquad K = \det(h_{ij})/\det(g_{ij})$$

により定義される．$H\nu$ を X の平均曲率ベクトルという．方程式 “H = 定数” は (非線形) 楕円型となり，最大値原理が適用できる等の利点がある．

注意 2.1 上では，Einstein の規約を使っている．すなわち，同じ添字が上下に出てくるときには，その添字についての和を取ることを意味する．たとえば，$g_{ij}du^i du^j = \sum_{i,j=1}^{2} g_{ij}du^i du^j$.

例 2.2 平均曲率一定の回転面は，Delaunay 曲面と呼ばれる．弧長 s で表示された滑らかな曲線 $\Gamma\colon (x(s), z(s))$ $(x \geq 0)$ を z 軸の周りに回転して得られる回転面の平均曲率は $H = (x''z' - x'z'' - x^{-1}z')/2$ である．したがって，Delaunay 曲面は (合同を除き) 二助変数族を成す．

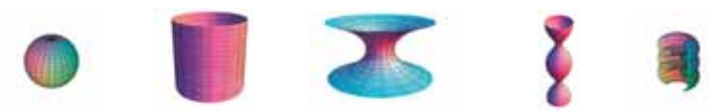


図 2：Delaunay 曲面．左から，球面，円柱，懸垂曲面，unduloid，nodoid.

3　平均曲率一定曲面の変分問題の解としての特徴付けと安定性に関する定義

はめ込み $X\colon \Sigma \to \mathbf{R}^3$ に対し，X の面積 $A(X)$ と体積 $V(X)$ を次で定義する．

$$A(X) = \int_\Sigma d\Sigma, \quad V(X) = \frac{1}{3}\int_\Sigma \langle X, \nu\rangle \, d\Sigma.$$

ここで，$d\Sigma := \sqrt{\det(g_{ij})}\, du^1 du^2$ は X の面積要素である．

注意 3.1 $V(X)$ は，曲面 $X(\Sigma)$ と $\mathbf{R}^3$ の原点が作る錐状領域の代数的体積である．$X(\Sigma)$ が自己交差を持たない向き付け可能な閉曲面の時は，ν を $X(\Sigma)$ が囲む領域 Ω から見て外向きにとると，$V(X)$ は Ω の体積と一致する．

$X_\epsilon = X + (\xi + f\nu)\epsilon + \mathcal{O}(\epsilon^2)$ を X の境界を固定する変分とする．すなわち, $X_*\colon \Sigma \times (-\epsilon_0, \epsilon_0) \to \mathbf{R}^3$ は C^∞ 級写像で,

$$X_0(w) = X(w), \quad \forall w \in \Sigma, \qquad X_\epsilon(\zeta) = X(\zeta), \quad \forall \zeta \in \partial\Sigma$$

を満たす．また，$f \in C_0^\infty(\Sigma)$ であり，ξ は変分ベクトル場 $\delta X := (\partial X_\epsilon/\partial\epsilon)_{\epsilon=0} = \xi + f\nu$ の接成分であって，共に $\partial\Sigma$ 上 0 である．

補題 3.2 A と V の第 1 変分は次で与えられる．

$$\delta A := \frac{d}{d\epsilon} A(X_\epsilon)|_{\epsilon=0} = -2\int_\Sigma Hf \, d\Sigma, \qquad \delta V = \int_\Sigma f \, d\Sigma. \tag{1}$$

注意 3.3 したがって，曲面 X の平均曲率ベクトル $H\nu$ の方向への変分 $X_\epsilon = X + \epsilon H\nu$ は，面積を減少させる．時間変化に伴って平均曲率ベクトル方向へ曲面を変形する「平均曲率流」方程式も応用の多い重要な概念である．

次の補題は，体積を保つ変分を考える上で重要である．証明には、陰関数定理を用いる。

補題 3.4 $\displaystyle\int_\Sigma f \, d\Sigma = 0$ を満たす任意の $f \in C_0^\infty(\Sigma)$ に対し，X の境界を固定し体積を保つ変分 $X_\epsilon = X + (f\epsilon + \mathcal{O}(\epsilon^2))\nu$ が存在する．

補題 3.2 を用いて，次が示せる．

定理 3.5 $X\colon \Sigma \to \mathbf{R}^3$ ははめ込みとし，その平均曲率を H で表す．

$$H_0 := (A(X))^{-1}\int_\Sigma H \, d\Sigma$$

とおく．このとき，次の (i)–(iii) は同値である．

(i) X の平均曲率は定数 H_0 である．

(ii) X の体積を保ち境界を固定する任意の変分に対し，面積汎関数 A の第 1 変分 $= 0$.

(iii) X の境界を固定する任意の変分に対し，汎関数 $A + 2H_0V$ の第 1 変分 $= 0$.

次の命題も重要である．証明は，たとえば，[7, pp.150–151] にある．

命題 3.6 $X\colon \Sigma \to \mathbf{R}^3$ ははめ込みとする．$X_\epsilon = X + (\xi^i X_i + f\nu)\epsilon + \mathcal{O}(\epsilon^2)$ を X の変分とする．このとき，平均曲率 H の第 1 変分は次で与えられる．

$$\delta H = L[f]/2 + \xi^i H_i. \tag{2}$$

ただしここで，L は自己共役作用素 $L[f] := \Delta f + \|d\nu\|^2 f$ である．特に X が平均曲率一定のときは，$\delta H = L[f]/2$ が成り立つ．

注意 3.7 $\Delta f = g^{ij} f_{ij} + \sqrt{g}^{-1}(\sqrt{g} g^{ij})_i f_j$, $g := \det(g_{ij})$. $\|d\nu\|^2 = 4H^2 - 2K$.

命題 3.8 X は平均曲率一定 $= H_0$ とする．X の体積を保ち境界を固定する変分に対し，面積汎関数 A の第 2 変分は

$$\delta^2 A := \frac{d^2}{d\epsilon^2} A(X_\epsilon)|_{\epsilon=0} = -\int_\Sigma f L[f]\, d\Sigma, \quad f := \langle \delta X, \nu \rangle \tag{3}$$

となる．ここで，δX は変分ベクトル場である．X の境界を固定する任意の変分に対する汎関数 $A + 2H_0 V$ の第 2 変分も，(3) で与えられる：

$$\delta^2 (A + 2H_0 V) = -\int_\Sigma f L[f]\, d\Sigma, \quad f := \langle \delta X, \nu \rangle. \tag{4}$$

証明 $X_\epsilon = X + \epsilon(\xi + f\nu) + \mathcal{O}(\epsilon^2)$ は，X の体積を保ち境界を固定する変分とすると，

$$\delta A = \delta A + 2H_0 \delta V = -2\int_\Sigma (H - H_0) f\, d\Sigma.$$

故に，

$$\delta^2 A = -2\int_\Sigma (\delta(H - H_0)) f\, d\Sigma - 2\int_\Sigma (H - H_0)\delta(f\, d\Sigma).$$

$\epsilon = 0$ のとき $H \equiv H_0$ であることと命題 3.6 より (3) が従う．(4) も同様に示せる． ∎

$$I(f) := -\int_\Sigma f L[f]\, d\Sigma$$

とおく．X の安定性を次で定義する．

定義 3.9 X は平均曲率一定とする．X の体積を保ち境界を固定する任意の変分に対して $\delta^2 A \geq 0$ が成立する時，X は安定であるといい，安定でない時，不安定であるという．

補題 3.4 と命題 3.8 から，次がわかる．

補題 3.10

$$F_0 := \left\{ f \in C_0^\infty(\Sigma)\ ;\ \int_\Sigma f\, d\Sigma = 0 \right\}$$

とおくと，X が安定 $\Longleftrightarrow I(f) \geq 0,\ \forall f \in F_0$.

注意 3.11 $X\colon \Sigma \to \mathbf{R}^3$ が安定ならば，任意の $\Sigma_1 \subset \Sigma$ に対し，$X|_{\Sigma_1}$ は安定である．

平均曲率一定曲面の安定性を判定するためには，次の補題が有用である．

補題 3.12 X は平均曲率一定 $= H$ とする．$L[\nu^j] = 0$, $L[\langle E_j \times X, \nu\rangle] = 0$, $(j = 1,2,3)$, $L[\langle X, \nu\rangle] = -2H$ が成り立つ．ここで，$E_1 := (1,0,0)$, $E_2 := (0,1,0)$, $E_3 := (0,0,1)$.

証明 はめ込み $X\colon \Sigma \to \mathbf{R}^3$ の変分 $X_\epsilon = X + \epsilon f\nu + \mathcal{O}(\epsilon^2)$ に対し，$2\delta H = L[f]$ であった．$\mathbf{R}^3$ の定ベクトル v に対し，平行移動 $X_\epsilon = X + \epsilon v$ によって平均曲率 H は変化しないことから，第 1 式を得る．同様に，回転 $X_\epsilon = X + \epsilon E_j \times X + \mathcal{O}(\epsilon^2)$ によって H が不変であることから，第 2 式を得る．また，相似変換 $X_\epsilon = (1+\epsilon)X$ によって H が $1/(1+\epsilon)$ 倍になることから，第 3 式を得る． ∎

4 平均曲率一定曲面の安定性の判定法

$X\colon \Sigma \to \mathbf{R}^3$ は平均曲率一定 $= H$ とする．X の安定性の判定条件について述べるために，面積汎関数の第 2 変分に付随する次の固有値問題を考える．

$$L[u] = -\lambda u, \qquad u \in C_0^\infty(\Sigma). \tag{5}$$

(5) の固有値はすべて実数であり，可算無限個の単調非減少列を成す．それらを $\lambda_1 < \lambda_2 \le \lambda_3 \le \cdots$ と表す．負の固有値の個数 (重複度も数える) を X の Morse 指数といい，$\mathrm{Ind}(X)$ で表す．$\mathrm{Ind}(X)$ は，境界を固定し，汎関数 $A + 2HV$ を減少させる変分ベクトル場の成す空間の次元である．したがって，(5) の固有値だけから X の安定性を判定することはできないが，下に述べるような判定法が知られている．

一方，体積を保つ変分に対する面積の第 2 変分に付随する固有値問題が次のように定式化される．

$$L[u] + c = -\tilde{\lambda} u \text{ on } \Sigma,\ \exists c \in \mathbf{R}, \qquad u \in F_0 - \{0\} \tag{6}$$

この問題の固有値は $\tilde{\lambda}_1 \le \tilde{\lambda}_2 \le \tilde{\lambda}_2 \le \cdots$ と書ける．ここで，$u \in F_0$ なる条件は，u が X の体積を保ち境界を固定する変分ベクトル場の法成分となるための条件である．

補題 4.1 (i) X が安定であることと $\tilde{\lambda}_1 \ge 0$ は同値である．
(ii) $\lambda_1 < \tilde{\lambda}_1 \le \lambda_2$ が成り立つ．

一般に，(6) の固有値の評価は (5) の固有値の評価よりも難しい．そのため，(5) を用いた平均曲率一定曲面の安定性の判定法を以下に与える．

以下では，Σ から $\mathbf{R}^3$ へのはめ込みの一助変数族 $\{X_t\}_t$ に対し，次の記号を用いる．

$$H(t) := X_t \text{ の平均曲率}, \qquad V(t) := X_t \text{ が囲む 3 次元体積},$$
$$L_t := X_t \text{ に付随する自己共役作用素}$$

まず，やや幾何的に見える判定法を述べる．

定理 4.2 (安定性の判定 [8], [12], [3]) X は平均曲率一定とする．
(I) $\lambda_1 \geq 0$ ならば，X は安定である．
(II) $\lambda_1 < 0 \leq \lambda_2$ とする．X の境界を保つ変分 X_t で，$H'(0) =$ 定数 $\neq 0$ なるものが存在する時，
(i) $H'(0)V'(0) \geq 0$ ならば，X は安定である．
(ii) $H'(0)V'(0) < 0$ ならば，X は不安定である．
このような変分が存在しないならば，X は不安定である．
(III) $\lambda_2 < 0$ ならば，X は不安定である．

次に，解析的に見える判定法を述べる．

$$E := \{u \in C_0^\infty(\Sigma)\ ;\ L[u] = 0\}$$

とおく．(5) が零固有値を持つ時は，E は零固有値に属する固有空間である．$L^2(\Sigma)$ における E の直交補空間を $E^\perp$ で表す．ただし，$L^2(\Sigma)$ は，内積 $(u,v)_{L^2} = \displaystyle\int_\Sigma uv\, d\Sigma$ による $C^\infty(\Sigma)$ の完備化である．また，$H_0^1(\Sigma)$ を，内積 $(u,v)_{H^1} = \displaystyle\int_\Sigma (uv + \nabla u \nabla v)\, d\Sigma$ による $C_0^\infty(\Sigma)$ の完備化とする．

固有値 λ_j に属する固有関数 $\varphi_j \in C_0^\infty(\Sigma)$ を $L^2(\Sigma)$ の正規直交系を成すようにとることができる．さらに，次が成立する．

$$\lambda_1 = I(\varphi_1) = \min\left\{ I(u)\ ;\ u \in H_0^1(\Sigma) \text{ かつ } \int_\Sigma u^2\, d\Sigma = 1 \right\}, \tag{7}$$

$$\lambda_j = I(\varphi_j) = \min\left\{ I(u)\ ;\ u \in H_0^1(\Sigma),\ \int_\Sigma u^2\, d\Sigma = 1,\ \int_\Sigma u\varphi_k\, d\Sigma = 0,\ \forall k \in \{1,\dots,j-1\} \right\},\quad j = 2,3,\dots. \tag{8}$$

次の定理は，定理 4.2 と本質的には同じものである．

定理 4.3 (安定性の判定 [8], [12], [3]) $X\colon \Sigma \to \mathbf{R}^3$ は平均曲率一定とする．
(I) $\lambda_1 \geq 0$ ならば，X は安定である．
(II) $\lambda_1 < 0 < \lambda_2$ ならば，$L[u] = 1$ を満たす関数 $u \in C_0^\infty(\Sigma)$ が一意的に存在して，次の (II-1), (II-2) が成り立つ．
(II-1) $\int_\Sigma u\, d\Sigma \geq 0$ ならば，X は安定である．
(II-2) $\int_\Sigma u\, d\Sigma < 0$ ならば，X は不安定である．
(III) $\lambda_2 = 0$ ならば，次の (III-A), (III-B) が成り立つ．
(III-A) $\int_\Sigma u\, d\Sigma \neq 0$ なる $u \in E$ が存在するならば，X は不安定である．
(III-B) 任意の $u \in E$ に対して $\int_\Sigma u\, d\Sigma = 0$ が成立するならば，$L[u] = 1$ を満たす関数 $u \in E^\perp \cap C_0^\infty(\Sigma)$ が一意的に存在して，次の (III-B1), (III-B2) が成り立つ．
(III-B1) $\int_\Sigma u\, d\Sigma \geq 0$ ならば，X は安定である．
(III-B2) $\int_\Sigma u\, d\Sigma < 0$ ならば，X は不安定である．
(IV) $\lambda_2 < 0$ ならば，X は不安定である．

定理 4.2, 4.3 は，より一般の，またさまざまな境界条件 (固定境界，自由境界，部分的自由境界) を持つ条件付き変分問題に対する定理として述べることも可能である．

注意 4.4 $X\colon \Sigma \to \mathbf{R}^3$ は平均曲率一定とする．$\forall w \in \Sigma$ に対し，w の十分小さい閉近傍 U をとれば，$\lambda_1(U) > 0$ であり，したがって，$X|_U$ は安定である．

例 4.5 (i) 球面は安定である．
(ii) 半径 r の円柱の表面を考える．長さが $2\pi r$ 以下ならば，安定である．それよりも大きい部分は不安定である．
(iii) unduloid の neck から次の neck までは安定である．それよりも小さい部分も安定である．それよりも大きい部分は不安定である．
(iv) 円柱に十分近い unduloid については，bulge から次の bulge までは安定である．
(v) くびれの大きい unduloid については，bulge から次の bulge までは不安定である．

5 解の分岐と安定性

平均曲率一定曲面の安定性を判定するために，その分岐の状況を調べることが時として有効である．本節では，与えられた境界値を持つ平均曲率一定曲面族に対する分岐の存在条件，及び，分岐前後の曲面の安定性の判定法を紹介する．

与えられた境界条件を満たす平均曲率一定曲面は，平均曲率 H または体積 V をパラメータとする変分問題の一助変数族の解として特徴付けられる．しかしながら，たとえば H をパラメータとした時，一般に，H と解の対応は 1 対 1 ではない．H が増加 (あるいは減少) する時，対応する解の族が，ある $H = H_0$ において分岐するという現象が起こることがある．H の代わりに V をパラメータとしてとった場合も同様である．

陰関数定理を用いることにより，次の結果が示せる．

定理 5.1 (平均曲率一定曲面族の存在と一意性 [3]) $X\colon \Sigma \to \mathbf{R}^3$ は平均曲率一定とする．次の (i) または (ii) が成り立つと仮定する．

(i) $E = \{0\}$.　　(ii) $\dim E = 1$ かつ $\displaystyle\int_\Sigma e\, d\Sigma \neq 0,\ \forall e \in E - \{0\}$.

この時，X の近傍で，平均曲率一定はめ込みの一助変数族 $\{X_t\}$ ($X_t\colon \Sigma \to \mathbf{R}^3$, $X_0 = X$, $X_t|_{\partial\Sigma} = X|_{\partial\Sigma}$) が，($\Sigma$ の微分同相を除き) 一意的に存在する．

したがって，この時は解の分岐は起こらない．λ_1 に属する固有空間の次元は 1 で固有関数は定符号だから，$\lambda_1 = 0$ ならば (ii) が満たされる．したがって，解の分岐が起こる可能性があるのは，$\lambda_k = 0$ ($\exists k \geq 2$) の時のみである．

固有値問題 (5) が重複度 1 の零固有値を持つ場合には，解の分岐の存在についての次の結果が成り立つ．証明は，本質的には，陰関数定理の応用である．

定理 5.2 (分岐の存在と一意性 [6]) $X_t = X + \varphi(t)\nu\colon \Sigma \to \mathbf{R}^3$, ($t \in I = (-\epsilon, \epsilon) \subset \mathbf{R}$), は平均曲率一定はめ込みの一助変数族で，$t$ について微分可能，$X = X_0$，$X|_{\partial\Sigma} = X_t|_{\partial\Sigma}$ なるものとする．次の (i), (ii) を仮定する．

(i) $H'(0) \neq 0$.

(ii) $E = \{ae\,;\, a \in \mathbf{R}\}$, $\quad \exists e \in (C_0^\infty(\Sigma) - \{0\})$.

この時，L_t の単純実固有値 $\lambda(t)$ で，$\lambda(0) = 0$ であり t について微分可能なものが 0 の近くで一意的に存在する．そこで，

(iii) $\lambda'(0) \neq 0$

と仮定する．開区間 $\hat{I}$ $(0 \in \hat{I} \subset \mathbf{R})$ と C^1 級関数 $\zeta\colon \hat{I} \to E^\perp$, $\hat{H}\colon \hat{I} \to \mathbf{R}$ で以下を満たすものが存在する．$\zeta(0) = 0$ であり，$Y_s := X + (se + s\zeta(s))\nu$ は平均曲率一定 $= \hat{H}(s)$．さらに，X の近傍で，X と同じ境界値を持つ平均曲率一定はめ込みは，$\{X_t\,;\, t \in I\}$ と $\{Y_s\,;\, s \in \hat{I}\}$ のみであり，$\{X_t\,;\, t \in I\} \cap \{Y_s\,;\, s \in \hat{I}\} = \{X\}$ である．

注意 5.3 X の変分 Y_s の変分ベクトル場は e で，$\displaystyle\int_\Sigma e\, d\Sigma = 0$ が成り立つ．これより，X_t が対称性を持つ時，Y_s は X_t と同じ対称性を持たない可能性が高い．

注意 5.4 固有値問題 (5) の零固有値の重複度が 2 以上の場合でも，対称性の高い解のみに制限することにより，定理 5.2 が適用できる場合がある．

定理 5.2 と同様の結果で，平均曲率の代わりに体積を用いたものが，Patnaik [9] によって得られている．これらの結果と Crandall-Rabinowitz [2] の結果の一般化，及び，定理 4.2 を用いることにより，分岐前後の固有値の評価を与える次の 2 つの定理が得られる．

定理 5.5 (分岐前後の固有値 [6]) X, X_t, Y_s は定理 5.2 と同じとする．分岐前後の λ の値について，H をパラメータとして，スーパークリティカルピッチフォーク分岐 (supercritical pitchfork bifurcation)，サブクリティカルピッチフォーク分岐 (subcritical pitchfork bifurcation)，trancendental 分岐の三種類が起こり得る (下図で，U は $\lambda < 0$ なる CMC 曲面の族，S は $\lambda > 0$ なる CMC 曲面の族を表す．図の左から，サブクリティカルピッチフォーク分岐，スーパークリティカルピッチフォーク分岐，trancendental 分岐)．

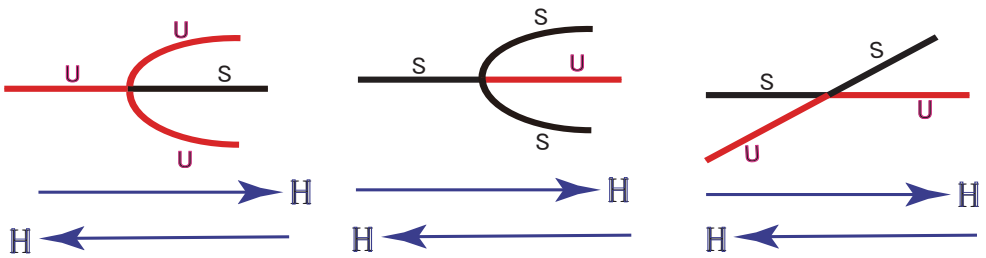


図 3 : サブクリティカルピッチフォーク分岐，スーパークリティカルピッチフォーク分岐，trancendental 分岐

定理 5.6 (分岐前後の安定性 [6]) X, X_t は定理 5.2 と同じとする．$H'(0)V'(0) \neq 0$, $\lambda_2(0) = 0$, $\dim E = 1$, $\lambda_2'(0) \neq 0$ とする．この時，定理 5.2 より，X からの分岐 Y_s が存在する．

(a) $H'(0)V'(0) < 0$ ならば，X, Y_s は不安定である．

(b) $H'(0)V'(0) > 0$ ならば，分岐前後の安定性について，V をパラメータとして，スーパークリティカルピッチフォーク分岐 (supercritical pitchfork bifurcation)，サブクリティカルピッチフォーク分岐 (subcritical pitchfork bifurcation)，trancendental 分岐の三種類が起こり得る (下図．左からサブクリティカルピッチフォーク分岐，スーパークリティカルピッチフォーク分岐，trancendental 分岐．S は安定解の族，U は不安定な解の族を表す)．

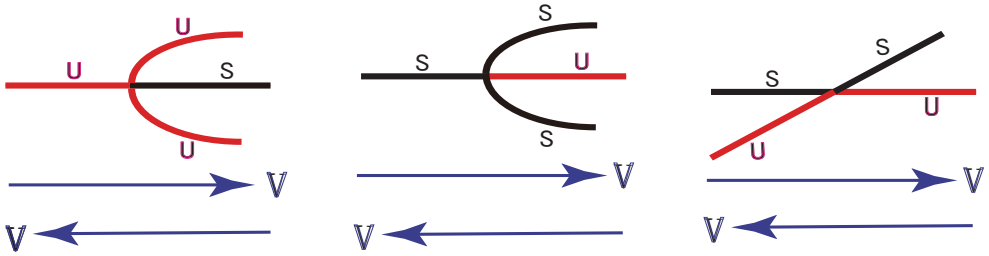


図 4：サブクリティカルピッチフォーク分岐，スーパークリティカルピッチフォーク分岐，trancendental 分岐

注意 5.7 注意 5.3 と同様に，X_t が対称性を持つ時，Y_s は X_t と同じ対称性を持たない可能性が高い．対称性の高い安定解が，対称性の低い安定解と対称性の高い不安定解に分岐するという興味深い現象が成り立つための条件が，定理 5.6 により得られた．

6 二つの平行な平面に自由境界を持つ平均曲率一定曲面の安定性への応用

上述の議論において境界条件を修正することにより，自由境界問題に対する解の安定性や分岐についての結果が得られる．この節では，自由境界問題の簡単な例をあげる．

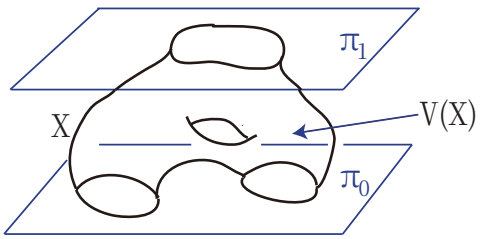


図 5：自由境界問題 (§6)

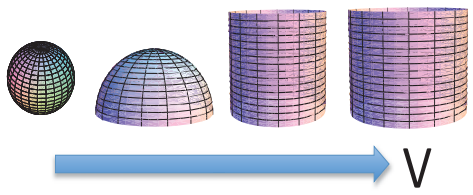


図 6：自由境界問題 (§6) の安定解: 球面，半球面，円柱.

Π_0, Π_1 を，$\mathbf{R}^3$ 内の，距離 h だけ離れた平行な二平面とし，$\Pi := \Pi_0 \cup \Pi_1$ とおく．Π が囲む閉領域を Ω とする．Π 上に自由境界をもち Ω に含まれる曲面の，体積を保つ変分に対する臨界点は，境界上で Π と直交する平均曲率一定曲面となる．自己交差を持たない曲面のみに問題を制限すると，最大値原理により，解は回転面であることが示せる．したがって，解はすべてわかる (cf. 例 2.2)．その中で，球面と半球面は安定である．円柱については，その半径を r とすると，$h \leq \pi r$ の時に限り安定である．それら以外の安定解の候補は，unduloid の半周期のみであることが示せる．unduloid の半周期は，そのどれもが，$h = \pi r$ を満たす円柱からの分岐により得られ，定理 5.6 を繰り返し適用することにより，すべて不安定であることが示せる．すなわち，安定解は，球面，半球面，$h \leq \pi r$ を満たす円柱のみである．この結果自体は [1], [12] によってすでに得られているものであり，[5] もこれを含む結果を [1], [12] とは異なる方法で得ているが，定理 5.6 を用いることにより，より簡明な別証明が得られるということである．なお，体積が十分大きい時は安定解は円柱のみであり，体積が十分小さい時は安定解は球面及び半球面である．体積によっては，球面，半球面，円柱の内の二種または三種の安定解が存在する．

7　汎関数の一般化 — 非等方的表面エネルギー —

§3 以降で展開した議論は，$\mathbf{R}^{n+1}$ 内の超曲面に対する，より一般のエネルギー汎関数に対しても一般化される．エネルギー汎関数の第 2 変分に付随する線形作用素が 2 階楕円型自己共役作用素であれば十分であると思われるが，たとえば，以下で紹介する非等方的表面エネルギー汎関数に対して一般化される．

γ を，$S^n = \{\nu \in \mathbf{R}^{n+1} \,;\, |\nu| = 1\}$ 上で定義された正値 C^∞ 級関数とする．$\mathbf{R}^{n+1}$ にはめ込まれた向き付け可能な超曲面 (以下では超曲面という) $X\colon \Sigma = \Sigma^n \to \mathbf{R}^{n+1}$ に対し，

$$\mathcal{F}(X) := \int_\Sigma \gamma(\nu)\, d\Sigma \tag{9}$$

とおく．ここで，$\nu = (\nu_1, \nu_2, \cdots, \nu_{n+1})\colon \Sigma \to S^n$ は X の単位法ベクトル場である．汎関数 $\mathcal{F}$ は非等方的表面エネルギーのモデルとしてしばしば利用される ([13], [14])．

$\mathbf{R}^{n+1}$ 内の同じ $(n+1)$ 次元体積 V を囲む閉超曲面の中で，$\mathcal{F}$ の最小解 $W(V)$ が (平行移動を除き) ただ一つ存在し，凸である ([11])．すなわち，$W(V)$ は汎関数 $\mathcal{F}$ に対する等周問題の

解である．体積 $V_0 := (n+1)^{-1}\displaystyle\int_{S^n} \gamma(\nu)\, dS^n$ に対するエネルギー最小解 $W(V_0)$ を Wulff 図形と呼び，W で表す．$W(V)$ は W に相似である．特に $\gamma \equiv 1$ のときは，$\mathcal{F}$ は X の n 次元体積であり，W は単位球面 S^n である．

以下，W は滑らかな狭義凸超曲面であると仮定する (凸性条件)．この時，W は，$\chi(\nu) = D\gamma(\nu) + \gamma(\nu)\nu$ により定義される埋め込み $\chi\colon S^n \to \mathbf{R}^{n+1}$ の像と一致する．

超曲面 X が囲む $(n+1)$ 次元体積を保つ変分に対する汎関数 $\mathcal{F}$ の Euler-Lagrange 方程式は

$$\mathrm{div}_\Sigma D\gamma - nH\gamma = \text{定数} \tag{10}$$

となる．ここで，H は X の平均曲率であり，$D\gamma$ は $\mathbf{R}^{n+1}$ での平行移動により，X に沿う接ベクトル場とみなしている．そこで，X の非等方的平均曲率 (anisotropic mean curvature) Λ を次のように定義する (cf. [10], [4])．

$$\Lambda := -\mathrm{div}_\Sigma D\gamma + nH\gamma.$$

Λ が定数のとき，X を非等方的平均曲率一定超曲面 (CAMC 超曲面) と呼ぶ．特に $\gamma \equiv 1$ の時は $\Lambda = nH$ である．また，Wulff 図形の (外向き法ベクトルに対する) 非等方的平均曲率は $-n$ である．凸性条件により，方程式 "$\Lambda =$ 定数" は楕円型となる．

§3 以降で展開した議論は，CAMC 超曲面に対してもそのまま一般化される．また，§6 の自由境界問題については，γ の与え方によっては unduloid 型の安定解が存在することが示せる．

参考文献

[1] M. Athanassenas, *A variational problem for constant mean curvature surfaces with free boundary*, J. Reine Angew. Math. **377** (1987), 97–107.

[2] M. G. Crandall and P. H. Rabinowitz, *Bifurcation, perturbation of simple eigenvalues, and linearized stability*, Arch. Rat. Mech. Anal. **52** (1973), 161–180.

[3] M. Koiso, *Deformation and stability of surfaces with constant mean curvature*, Tohoku Math. J. (2) **54** (2002), 145–159.

[4] M. Koiso and B. Palmer, *Geometry and stability of surfaces with constant anisotropic mean curvature*, Indiana Univ. Math. J. **54** (2005), 1817–1852.

[5] M. Koiso and B. Palmer, *Stability of anisotropic capillary surfaces between two parallel planes*, Calculus of Variations and Partial Differential Equations **25** (2006), 275–298.

[6] M. Koiso, B. Palmer and P. Piccione, in preparation.

[7] 小磯憲史, 変分問題, 共立出版, 1998.

[8] J. H. Maddocks, *Stability and folds,* Arch. Rat. Mech. Anal. **99** (1987), 301–328.

[9] U. Patnaik, *Volume constrained Douglas problem and the stability of liquid bridges between two coaxial tubes*, Dissertation, University of Toledo, USA, 1994.

[10] R. C. Reilly, *The relative differential geometry of nonparametric hypersurfaces*, Duke Math. J. **43** (1976), 705–721.

[11] J. E. Taylor, *Crystalline variational problems*, Bull. Amer. Math. Soc. **84** (1978), 568–588.

[12] T. I. Vogel, *Stability of a liquid drop trapped between two parallel planes*, SIAM J. Appl. Math. **47** (1987), 516–525.

[13] W. L. Winterbottom, *Equilibrium shape of a small particle in contact with a foreign substrate*, Acta Metallurgica **15** (1967), 303–310.

[14] G. Wulff, *Zur Frage der Geschwindigkeit des Wachsthums und der Auflösung der Krystallflächen*, Zeitschrift für Krystallographie und Mineralogie **34** (1901), 449–530.

平面曲線の等周変形の離散モデルと離散可積分系

梶原　健司

九州大学マス・フォア・インダストリ研究所

1　平面曲線とその等周変形

1.1　平面曲線と Frenet の公式

$\gamma(x) = \begin{bmatrix} X(x) \\ Y(x) \end{bmatrix} \in \mathbb{R}^2$ を弧長パラメータ表示された曲線，x は（曲線上の適当な点から計った）弧長とする．x が弧長であることから $dx = \sqrt{(dX)^2 + (dY)^2}$ すなわち

$$|\gamma'| = \sqrt{\left(\frac{dX}{dx}\right)^2 + \left(\frac{dY}{dx}\right)^2} = 1 \tag{1}$$

が成り立つ．ここで $'$ は x に関する微分である．γ の接線ベクトル T を $T = \gamma'$ で定義すると，(1) より $|T| = 1$ であるから

$$T = \gamma' = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} \tag{2}$$

とパラメータ表示ができる．$\theta = \theta(x)$ は接線ベクトル T の X 軸から正の向きに計った角度という意味をもち，角函数と呼ばれる．法線ベクトル N を

$$N = R\left(\frac{\pi}{2}\right) T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} T, \quad R(\phi) = \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{bmatrix} \tag{3}$$

で定義する（図 1）．$\langle \cdot, \cdot \rangle$ をユークリッド内積とすると，(1) より $\langle T, T \rangle = 1$ であるからこれを x で微分すると $\langle T', T \rangle = 0$, すなわち T と T' は直交することがわかる．これより

$$T' = \kappa N = \begin{bmatrix} 0 & -\kappa \\ \kappa & 0 \end{bmatrix} T \tag{4}$$

となる $\kappa = \kappa(x)$ が存在する．κ を曲率と呼ぶ．(2) の両辺を x で微分して (4) と比較すると，ただちに $\kappa = \theta'$ であることがわかる．このことから θ はポテンシャル函数とも呼ばれる．ここで Frenet 標構 Φ を $\Phi = [T, N]$ で定義すると，$\Phi \in \mathrm{SO}(2)$ は曲線の各点に付随した $\mathbb{R}^2$ の正規直交基底であり，(3), (4) から

$$\Phi' = \Phi U, \quad U = \begin{bmatrix} 0 & -\kappa \\ \kappa & 0 \end{bmatrix} \tag{5}$$

が従うことがただちにわかる．(5) を Frenet の公式と呼ぶ．

1.2 平面曲線の等周変形と mKdV 方程式

曲線 $\gamma(x)$ や付随する量が変形パラメータ t に依存しているものとし，全ての t に対して

$$|\gamma'(x,t)| = 1 \tag{6}$$

すなわち弧長が変化しない（曲線が伸縮しない）変形を考えることにする．このような変形を等周変形，(6) を等周条件と呼ぶ．Φ が $\mathbb{R}^2$ の正規直交基底であることに注意して

$$\frac{\partial \gamma}{\partial t} = g(x,t)T + f(x,t)N \tag{7}$$

と表し，$\langle \gamma', \gamma' \rangle = 1$ の両辺を t で微分して (7) を用いると，簡単な計算で Φ に関して

$$\frac{\partial \Phi}{\partial t} = \Phi V, \quad V = \begin{bmatrix} 0 & -(f' + \kappa g) \\ f' + \kappa g & \end{bmatrix}, \quad g' = \kappa f \tag{8}$$

が成り立つことがわかる．Φ に関する線形偏微分方程式系 (5), (8) の両立条件 $\Phi_{xt} = \Phi_{tx}$ より U, V は

$$\frac{\partial U}{\partial t} - \frac{\partial V}{\partial x} + UV - VU = 0 \tag{9}$$

に従う．(9) を成分毎に書き下すと，κ は

$$\kappa_t = f_{xx} + \kappa_x g + \kappa^2 f, \quad g_x = \kappa f \tag{10}$$

を満たさなければならないことがわかる．ここで，特に f, g を

$$f = -\kappa_x, \quad g = -\frac{\kappa^2}{2} \tag{11}$$

と選ぶと，(10) より

$$\kappa_t + \frac{3}{2}\kappa^2 \kappa_x + \kappa_{xxx} = 0 \tag{12}$$

もしくは θ に関して

$$\theta_t + \frac{1}{2}(\theta_x)^3 + \theta_{xxx} = 0 \tag{13}$$

が成り立つ．(12), (13) はそれぞれ modified Korteweg-de Vries (mKdV) 方程式，ポテンシャル mKdV 方程式と呼ばれる典型的な可積分系である．すなわち，（ポテンシャル）mKdV 方程式はユークリッド平面上の曲線の等周変形を記述することがわかった [1].

2 離散曲線とその等周変形

2.1 離散曲線と離散 Frenet の公式

上記の離散モデルを考えよう．$\gamma_n \in \mathbb{R}^2$ $(n \in \mathbb{Z})$ が与えられた $a_n \in \mathbb{R}$ に関して

$$\left| \frac{\gamma_{n+1} - \gamma_n}{a_n} \right| = 1 \tag{14}$$

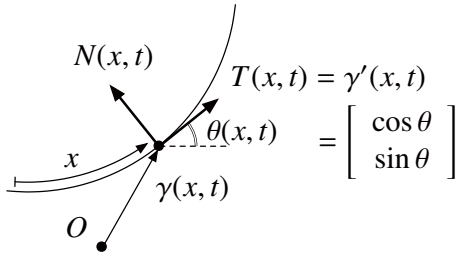


図 1：連続曲線

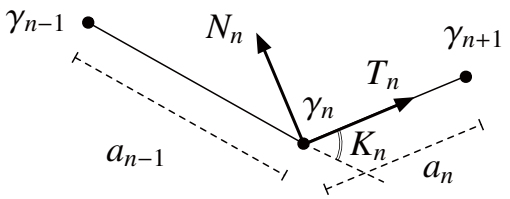


図 2：離散曲線

を満たすとき，γ_n を平面離散曲線と呼ぶ．(14) より

$$\frac{\gamma_{n+1}-\gamma_n}{a_n}=\begin{bmatrix}\cos\Psi_n\\ \sin\Psi_n\end{bmatrix} \tag{15}$$

とパラメータ表示されるが，Ψ_n は「セグメント」$\gamma_n\gamma_{n+1}$ の X 軸から正の向きに計った角度に他ならず，これも連続曲線の場合と同様に角函数と呼ぶことにする．さて，二つの隣接するセグメント $\gamma_{n-1}\gamma_n$, $\gamma_n\gamma_{n+1}$ の間の正の向きに計った角度を K_n とすると，

$$\frac{\gamma_{n+1}-\gamma_n}{a_n}=R(K_n)\frac{\gamma_n-\gamma_{n-1}}{a_{n-1}},\quad K_n=\Psi_n-\Psi_{n-1} \tag{16}$$

が成り立つ（図 2）．離散 Frenet 標構 $\Phi_n\in\mathrm{SO}(2)$ を

$$\Phi_n=[T_n,N_n],\quad T_n=\frac{\gamma_{n+1}-\gamma_n}{a_n},\quad N_n=R\left(\frac{\pi}{2}\right)T_n \tag{17}$$

で定義すると，

$$\Phi_{n+1}=\Phi_n\begin{bmatrix}\cos\Psi_n & -\sin\Psi_n\\ \sin\Psi_n & \cos\Psi_n\end{bmatrix} \tag{18}$$

が従う．(16) または (18) を離散 Frenet の公式と呼ぶ.

2.2 離散曲線の離散的等周変形

離散曲線の離散的な等周変形で，連続極限で 1 章で述べた mKdV 方程式による連続曲線の等周変形に帰着するものを考える [5, 7]．$m\in\mathbb{Z}$ を離散時間，γ_n^m を $\gamma_n=\gamma_n^0$ の等周変形，すなわち，すべての m に対して

$$\left|\frac{\gamma_{n+1}^m-\gamma_n^m}{a_n}\right|=1 \tag{19}$$

（セグメントの長さは m によらず一定）を満たすものとする．特に，等距離条件

$$\left|\frac{\gamma_{n+1}^{m+1}-\gamma_{n+1}^m}{b_m}\right|=\left|\frac{\gamma_n^{m+1}-\gamma_n^m}{b_m}\right|=1 \tag{20}$$

で特徴付けられる変形を考えることにする．ここで b_m は任意に与えた m だけの函数．このとき，図 3 のようにセグメント $\gamma_n^m\gamma_{n+1}^m$ と $\gamma_n^m\gamma_n^{m+1}$ のなす角を W_n^m とおくと，

$$\frac{\gamma_n^{m+1}-\gamma_n^m}{b_m}=\cos W_n^m\ T_n^m+\sin W_n^m\ N_n^m=\begin{bmatrix}\cos W_n^m & -\sin W_n^m\\ \sin W_n^m & \cos W_n^m\end{bmatrix}T_n^m \tag{21}$$

または離散 Frenet 標構 Φ_n^m について

$$\Phi_n^{m+1}=\Phi_n^m\times \begin{bmatrix}1+\frac{b_m}{a_n}\{\cos(W_{n+1}^m+K_{n+1}^m)-\cos K_n^m\} & -\frac{b_m}{a_n}\{\cos(W_{n+1}^m+K_{n+1}^m)-\sin K_n^m\}\\ \frac{b_m}{a_n}\{\cos(W_{n+1}^m+K_{n+1}^m)-\sin K_n^m\} & 1+\frac{b_m}{a_n}\{\cos(W_{n+1}^m+K_{n+1}^m)-\cos K_n^m\}\end{bmatrix} \tag{22}$$

が成り立つ．ここで，等周条件 (19)，および (18) と (22) の両立条件 $((\Phi_{n+1})^{m+1}=(\Phi^{m+1})_{n+1})$ より，少し煩雑な計算のあと，

$$\tan\frac{W_{n+1}^m+K_{n+1}^m}{2}=\frac{b_m+a_n}{b_m-a_n}\tan\frac{K_n^m}{2},\quad K_n^{m+1}-K_{n+1}^m=W_{n+1}^m-W_{n-1}^m \tag{23}$$

がそれぞれ得られる．第 2 式よりポテンシャル函数 θ_n^m を

$$K_n^m=\frac{\theta_{n+1}^m-\theta_{n-1}^m}{2},\quad W_n^m=\frac{\theta_n^{m+1}-\theta_{n+1}^m}{2},\quad \Psi_n^m=\frac{\theta_{n+1}^m+\theta_n^m}{2} \tag{24}$$

で導入すると，第 1 式より離散ポテンシャル mKdV 方程式が従う [3]：

$$\tan\frac{\theta_{n+1}^{m+1}-\theta_n^m}{2}=\frac{b_m+a_n}{b_m-a_n}\tan\frac{\theta_n^{m+1}-\theta_{n+1}^m}{2} \tag{25}$$

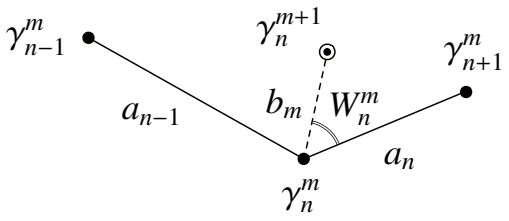


図 3：離散曲線の等周変形

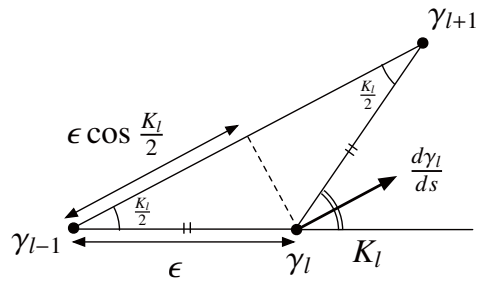


図 4：離散曲線の接線流

2.3 離散曲線の連続的等周変形

$\gamma_l\in\mathbb{R}^2$ $(l\in\mathbb{Z})$ をセグメント長 ϵ (定数)，角函数 Ψ_l の離散曲線，すなわち，

$$\left|\frac{\gamma_{l+1}-\gamma_l}{\epsilon}\right|=1,\quad \frac{\gamma_{l+1}-\gamma_l}{\epsilon}=\begin{bmatrix}\cos\Psi_n\\ \sin\Psi_n\end{bmatrix}, \tag{26}$$

$$\frac{\gamma_{l+1}-\gamma_l}{\epsilon}=R(K_l)\frac{\gamma_l-\gamma_{l-1}}{\epsilon} \tag{27}$$

が成り立っているものとする．s を連続的な変形パラメータとし，次の変形を考える [4, 6].

$$\frac{d}{ds}\gamma_l = \frac{1}{\cos\frac{K_l}{2}} R\left(-\frac{K_l}{2}\right)\frac{\gamma_{l+1}-\gamma_l}{\epsilon} \tag{28}$$

図 4 より，これは γ_l をベクトル $\gamma_{l+1}-\gamma_{l-1}$（点接ベクトル）と平行な方向に動かす変形であり，接線流と呼ばれる．(26) が全ての s について成り立つという要請（等周条件），および (27), (28) の両立条件からポテンシャル函数 θ_l と半離散ポテンシャル mKdV 方程式が得られる [2] :

$$\Psi_l = \frac{\theta_{l+1}+\theta_l}{2}, \quad K_l = \frac{\theta_{l+1}-\theta_{l-1}}{2}, \tag{29}$$

$$\frac{d\theta_l}{ds} = \frac{2}{\epsilon}\tan\frac{\theta_{l+1}-\theta_{l-1}}{4} \tag{30}$$

2.4 連続極限

離散ポテンシャル mKdV 方程式 (25) から半離散ポテンシャル mKdV 方程式 (30)，ポテンシャル mKdV 方程式 (13) は，それぞれ次のような極限操作で得られる [2, 3, 6].

(25)⟶(30)

$$\begin{gathered} a_n = a \text{ (const.)}, \quad b_m = b \text{ (const.)}, \quad \delta = \frac{a+b}{2}, \quad \epsilon = \frac{a-b}{2}, \\ \frac{s}{\delta} = n+m, \quad l = n-m, \quad \delta \to 0 \end{gathered} \tag{31}$$

(30)⟶(13)

$$x = \epsilon l + s, \quad t = -\frac{\epsilon^2}{6}s, \quad \epsilon \to 0 \tag{32}$$

なお，方程式だけでなく角函数や Frenet 標構，さらに曲線そのものについても上記の極限移行が成立する．計算は単に変数変換を施した後に，極限を取るパラメータについてテイラー展開すればよい．なお，変形を支配する方程式が可積分系であるということを用いて，曲線の変形のさまざまな厳密解が τ 函数を用いて明示的に得られる．詳細は [5, 6] を参照すること．

参考文献

[1] 井ノ口順一，「曲線とソリトン」（朝倉書店，2010 年）

[2] R. Hirota, Exact N-soliton solution of nonlinear lumped self-dual network equation, J. Phys. Soc. Jpn. **35**(1973) 289–294.

[3] R. Hirota, Discretization of the potential modified KdV equation, J. Phys. Soc. Jpn. **67**(1998) 2234–2236.

[4] T. Hoffmann（安藤央 訳），曲線や曲面に関する離散微分幾何学，若山正人編「可視化の技術と現代幾何学」，岩波書店 (2010)，133–181.

[5] J. Inoguchi, K. Kajiwara, N. Matsuura and Y. Ohta, Motion and Bäcklund transformations of discrete plane curves, Kyushu J. Math. **66**(2012), 303–324.

[6] J. Inoguchi, K. Kajiwara, N. Matsuura and Y. Ohta, Explicit solutions to the semi-discrete modified KdV equation and motion of discrete plane curves, J. Phys. A: Math. Theoret. **45**(2012) 045206.

[7] N. Matsuura, Discrete KdV and discrete modified KdV equations arising from motions of discrete planar curves, Int. Math. Res. Notices **2012**(2012), 1681–1698.

パーシステントホモロジー群
―離散データのトポロジカル解析―

平岡　裕章

九州大学マス・フォア・インダストリ研究所

1　はじめに

近年離散データのトポロジカル解析手法としてパーシステントホモロジー群が注目されている [2, 5]．ここではパーシステントホモロジー群の幾何学的側面と代数的側面について解説をおこない，タンパク質構造解析への具体的な応用例を紹介する．なお本稿の内容に関するより詳細な解説は [4] を参照されたい．

2　単体複体フィルトレーション

2.1　脈体

$X \subset \mathbb{R}^N$ が有限個の部分集合の集まり $\Phi = \{B_i \subset \mathbb{R}^N \mid i = 1, \ldots, m\}$ で被覆されているとする：

$$X = \bigcup_{i=1}^{m} B_i.$$

このとき頂点集合を $V = \{1, \ldots, m\}$，単体の集まりを

$$\Sigma = \left\{ \{i_0, \ldots, i_k\} \;\middle|\; \bigcap_{j=0}^{k} B_{i_j} \neq \emptyset \right\}$$

で定めると，これは抽象単体複体になる．この抽象単体複体を Φ の脈体とよび $\mathcal{N}(\Phi)$ で表す．X の被覆が凸閉集合で与えられる場合は次の関係が成り立つ．

定理 2.1（脈体定理） $X \subset \mathbb{R}^N$ が有限個の凸閉集合の集まり $\Phi = \{B_i \mid i = 1, \ldots, m\}$ で被覆

$$X = \bigcup_{i=1}^{m} B_i$$

されているとする．このとき X と脈体 $\mathcal{N}(\Phi)$ はホモトピー同型となる．

2.2 Čech 複体

$\mathbb{R}^N$ 内の有限個の点の集まり $P = \{x_i \in \mathbb{R}^N \mid i = 1, \ldots, m\}$ に対して，点 x_i を中心とし半径 r の球 $B_r(x_i) = \{x \in \mathbb{R}^N \mid \|x - x_i\| \leq r\}$ を配置する．ここで $\|x\|$ はユークリッドノルムを表す．これらの球の集まり $\Phi = \{B_r(x_i) \mid x_i \in P\}$ についての脈体 $\mathcal{N}(\Phi)$ を Čech 複体とよび，$\mathcal{C}(P, r)$ で表す．球は凸閉集合なので，脈体定理よりホモトピー同型

$$X_r = \bigcup_{i=1}^{m} B_r(x_i) \simeq \mathcal{C}(P, r)$$

を得る．図 1 に Čech 複体の例を示す．

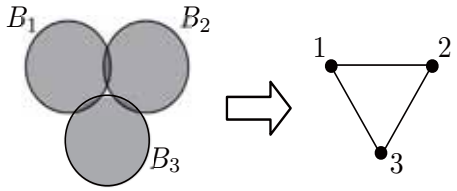


図 1：Čech 複体の例

Čech 複体に k 単体 $\{i_0, \ldots, i_k\}$ が存在する必要十分条件は，$\bigcap_{j=0}^{k} B_r(x_{i_j}) \neq \emptyset$ である．この条件は，球の半径を r より大きい r' に置き換えても成り立つ．すなわち

$$\bigcap_{j=0}^{k} B_r(x_{i_j}) \neq \emptyset \Longrightarrow \bigcap_{j=0}^{k} B_{r'}(x_{i_j}) \neq \emptyset, \quad r < r'.$$

よって半径 r が定める Čech 複体に現れる単体は，r より大きな半径 r' が定める Čech 複体に全て含まれる．よって以下の包含関係が成立する：

$$\mathcal{C}(P, r) \subset \mathcal{C}(P, r').$$

これにより r の増大列 $r_1 < \cdots < r_i < \cdots < r_T$ に対して Čech 複体のフィルトレーション

$$\mathcal{C}(P, r_1) \subset \cdots \subset \mathcal{C}(P, r_i) \subset \cdots \subset \mathcal{C}(P, r_T)$$

を得る．

ここまでは全ての点に同じ半径の球を配置して脈体を構成していたが，脈体定理を適用する際には各点で異なる半径を与えても構わない．すなわち P 内の各点 x_i に半径 r_i の球 $B_{r_i}(x_i)$ を配置し，その脈体を考えることで $\bigcup_{i=1}^{m} B_{r_i}(x_i)$ とホモトピー同型な単体複体が得られる．この単体複体を重み付き Čech 複体とよび $\mathcal{C}(P, R)$ で表す．ここで R は各点での半径の集まり $R = \{r_i \mid i = 1, \ldots, m\}$ を表す．

2.3 アルファ複体

有限個の点の集まり $P = \{x_i \in \mathbb{R}^N \mid i = 1, \ldots, m\}$ に対して，各点 x_i に領域

$$V_i = \{x \in \mathbb{R}^N \mid \|x - x_i\| \leq \|x - x_j\|,\ 1 \leq j \leq m,\ j \neq i\}$$

を割り当てる．すると $\mathbb{R}^N$ はこれらの領域の和集合として表せる：

$$\mathbb{R}^N = \bigcup_{i=1}^{m} V_i. \tag{1}$$

領域 V_i をボロノイ領域とよび，ボロノイ領域による $\mathbb{R}^N$ の分割 (1) をボロノイ図とよぶ．

ドロネー複体はボロノイ図の脈体として定められる．すなわち (1) で与えられる被覆 $\Phi = \{V_i \mid i = 1, \ldots, m\}$ に対して，そのドロネー複体 $\mathcal{D}(P)$ を $\mathcal{D}(P) = \mathcal{N}(\Phi)$ で定める．よってドロネー複体 $\mathcal{D}(P)$ に k 単体 $\{i_0, \ldots, i_k\}$ が存在する必要十分条件は

$$\bigcap_{j=0}^{k} V_{i_j} \neq \emptyset$$

であり，さらにこの条件は，

$$\|x - x_{i_0}\| = \cdots = \|x - x_{i_k}\| \text{ となる } x \in \mathbb{R}^N \text{ が存在する，}$$

と同値である．図 2 は，$\mathbb{R}^2$ 内の 5 点が定めるボロノイ図と，そのドロネー複体の例を示してある．

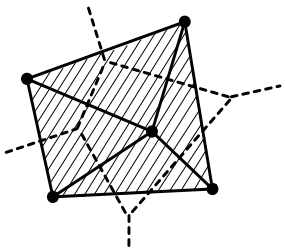


図 2：ボロノイ図（点線）とそのドロネー複体（実線）

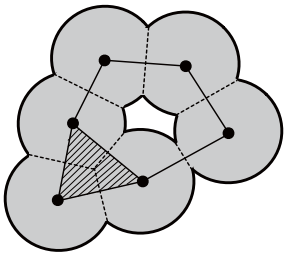


図 3：アルファ複体の例

ここでアルファ複体を導入する．m 個の半径 r の球からなる和集合

$$X_r = \bigcup_{i=1}^{m} B_r(x_i), \quad x_i \in P$$

を考える．P が定める各ボロノイ領域 V_i と，球 $B_r(x_i)$ の共通部分を $W_i = B_r(x_i) \cap V_i$ とおく．すると W_i は凸集合の共通部分なので凸集合となり，球 $B_r(x_i)$ をボロノイ領域 V_i に制限した図形を与える．また

$$\Psi = \{W_i \mid i = 1, \ldots, m\}$$

が X_r の被覆

$$X_r = \bigcup_{i=1}^{m} W_i$$

を与えることも容易にわかる．

球の集まり $\{B_r(x_i) \mid i = 1, \ldots, m\}$ のアルファ複体 $\alpha(P, r)$ は，Ψ に対する脈体

$$\alpha(P, r) = \mathcal{N}(\Psi)$$

として定義される．図 3 は 6 個の球の集まりからなるアルファ複体の例である．

W_i は凸閉集合であり X_r の被覆を与えていることから，脈体定理 2.1 より X_r と $\alpha(P, r)$ はホモトピー同型

$$X_r \simeq \alpha(P, r)$$

である．

包含関係 $W_i \subset B_r(x_i)$ より，アルファ複体 $\alpha(P, r)$ は Čech 複体 $\mathcal{C}(P, r)$ の部分複体である．また $W_i \subset V_i$ より，アルファ複体 $\alpha(P, r)$ はドロネー複体 $\mathcal{D}(P)$ の部分複体でもある．P が一般の位置にある[1]場合は，ドロネー複体 $\mathcal{D}(P)$ の次元は N 以下であり，よってアルファ複体 $\alpha(P, r)$ の次元も N 以下になる．

ここで Čech 複体も X_r とホモトピー同型な単体複体であったが，一般には N より大きな次元の単体が現れることに注意する．すなわち P が一般の位置にある場合，アルファ複体は X_r とホモトピー同型な単体複体を，次元が N 以下の単体で構成できる点において Čech 複体とは異なる．

また Čech 複体のときと同様に，半径の増大列 $r_1 < \cdots < r_i < \cdots < r_T$ からアルファ複体のフィルトレーション

$$\alpha(P, r_1) \subset \cdots \subset \alpha(P, r_i) \subset \cdots \subset \alpha(P, r_T)$$

も得られる．各点で半径が異なる球を配置させる重み付きアルファ複体も同様に定義される．

3　パーシステントホモロジー群

単体複体 K^t, $t = 0, 1, \ldots,$ のフィルトレーション

$$\mathbb{K}\colon K^0 \subset K^1 \subset \cdots \subset K^t \subset \cdots \tag{2}$$

を考える．ここで，フィルトレーション内の単体複体 K^t を指定する添字 t を時刻とよぶことにする．フィルトレーション $\mathbb{K}$ は，ある非負整数 Θ が存在し，$K^j = K^\Theta$, $j \geq \Theta$, が成り立つとき，有限型であるという．またこの性質を満たす Θ の最小値を，フィルトレーションの飽和時刻とよぶことにする．以下では有限型フィルトレーションのみ考察する．

[1] $\mathbb{R}^N$ 内の $N+2$ 個の点 $x_1, \ldots, x_{N+2}$ は，それらから等距離にある点が存在しないとき一般の位置にあるという．また P 内の全ての $N+2$ 個の点が一般の位置にあるとき，P は一般の位置にあるという．

フィルトレーション (2) に対して，$K = \bigcup_{t\geq 0} K^t$ とする．また時刻 t での単体複体 K^t の，k 次元単体の集まりを K_k^t と表す．さらに K 内の単体 σ が時刻 t で発生したとき，つまり

$$\sigma \in K^t \setminus K^{t-1}$$

のとき，$T(\sigma) = t$ と表すことにする．

各次元 k ごとに，$\mathbb{Z}_2$ 係数ベクトル空間

$$C_k(K^t) = \sum_{\sigma \in K_k^t} \mathbb{Z}_2 \sigma$$

を用意する．さらにこれらの直和

$$C_k(\mathbb{K}) = \bigoplus_{t\geq 0} C_k(K^t) = \{(c_0, c_1, \ldots, c_t, \ldots) \mid c_t \in C_k(K^t)\}$$

に，次の x の作用

$$x \cdot (c_0, c_1, \ldots) = (0, c_0, c_1, \ldots)$$

を導入する．すると $C_k(\mathbb{K})$ は次数付き $\mathbb{Z}_2[x]$ 加群となる．この次数付き $\mathbb{Z}_2[x]$ 加群 $C_k(\mathbb{K})$ を，フィルトレーション $\mathbb{K}$ に対する k 鎖群とよぶ．また斉次部分 $C_k(K^t)$ から $C_k(\mathbb{K})$ への包含写像 $i_t \colon C_k(K^t) \to C_k(\mathbb{K})$,

$$i_t(\sigma) = (c_0, c_1, \ldots), \quad c_i = \begin{cases} \sigma, & i = t, \\ 0, & i \neq t \end{cases}$$

を導入しておく．

ここで k 鎖群 $C_k(\mathbb{K})$ は

$$\Xi_k = \left\{ e_\sigma = i_{T(\sigma)}(\sigma) \mid \sigma \in K_k \right\}$$

を基底とする自由 $\mathbb{Z}_2[x]$ 加群になることが確かめられる．そこで境界作用素 $\partial_k \colon C_k(\mathbb{K}) \to C_{k-1}(\mathbb{K})$ を，基底 Ξ_k をもちいて

$$\partial_k(e_\sigma) = \sum_{i=0}^{k} \left(x^{T(\sigma) - T(\sigma_i)} \right) e_{\sigma_i}, \quad \sigma \in K_k$$

で定める．ここで k 単体 $\sigma = \{v_0 \cdots v_k\} \in K_k$ の面を $\sigma_i = \{v_0 \cdots \hat{v}_i \cdots v_k\}$（$v_i$ を除く）で表している．

この定義において，単体 σ の面 σ_i に対しては，$T(\sigma_i) \leq T(\sigma)$ であることに注意しておく．またここで導入した境界作用素は，$\partial_{k-1} \circ \partial_k = 0$ を満たす次数付き準同型写像 $\partial_k(C_k(K^t)) \subset C_{k-1}(K^t)$ となる．

ここで k 鎖群 $C_k(\mathbb{K})$ に対して，2 つの斉次部分加群を導入する：

$$Z_k(\mathbb{K}) = \operatorname{Ker} \partial_k,$$
$$B_k(\mathbb{K}) = \operatorname{Im} \partial_{k+1}.$$

$Z_k(\mathbb{K})$, $B_k(\mathbb{K})$ は斉次部分加群なので，$Z_k(K^t) = Z_k(\mathbb{K}) \cap C_k(K^t)$, $B_k(K^t) = B_k(\mathbb{K}) \cap C_k(K^t)$ とすると，

$$Z_k(\mathbb{K}) = \bigoplus_{t\geq 0} Z_k(K^t),$$
$$B_k(\mathbb{K}) = \bigoplus_{t\geq 0} B_k(K^t)$$

が成り立つ．

単体複体のフィルトレーションに対して，そのパーシステントホモロジー群は次で与えられる．

定義 3.1 単体複体の有限型フィルトレーション

$$\mathbb{K}\colon K^0 \subset K^1 \subset \cdots \subset K^t \subset \cdots$$

に対して

$$PH_k(\mathbb{K}) = Z_k(\mathbb{K})/B_k(\mathbb{K})$$

を，k 次パーシステントホモロジー群とよぶ．

パーシステントホモロジー群の詳細については文献 [2, 5] などを参照されたい．まず $Z_k(\mathbb{K})$, $B_k(\mathbb{K})$ は斉次部分加群なので，パーシステントホモロジー群は次数付き $\mathbb{Z}_2[x]$ 加群として

$$PH_k(\mathbb{K}) = \bigoplus_{t\geq 0} Z_k(K^t)/B_k(K^t) = \bigoplus_{t\geq 0} H_k(K^t)$$

となる．ここで x の $PH_k(\mathbb{K})$ への作用は，包含写像 $C_k(K^t) \to C_k(K^{t+1})$ が誘導する準同型写像

$$\varphi_t^{t+1}\colon H_k(K^t) \to H_k(K^{t+1})$$

を用いて

$$x \cdot [z] = \varphi_t^{t+1}([z]), \quad [z] \in H_k(K^t)$$

で与えられる．

また $\mathbb{Z}_2[x]$ は単項イデアル整域なので，パーシステントホモロジー群 $PH_k(\mathbb{K})$ は次の形に一意的に表せる：

$$PH_k(\mathbb{K}) \simeq \bigoplus_{i=1}^{s} \left((x^{d_i}) \Big/ (x^{d_i+l_i}) \right) \oplus \bigoplus_{i=s+1}^{s+r} (x^{d_i}) \tag{3}$$

この表示において，最初の s 個の直和成分は，時刻 d_i で発生し $d_i + l_i$ で消滅するホモロジー類を表している．また次の r 個の直和成分は，時刻 d_i で発生しフィルトレーションの飽和時刻まで存続するホモロジー類を表している．

定義 3.2 パーシステントホモロジー群 (3) に対して

$$I_i = \begin{cases} [d_i, d_i + l_i)\,, & i = 1, \ldots, s, \\ [d_i, \Theta]\,, & i = s+1, \ldots, s+r \end{cases}$$

をパーシステント区間とよぶ．ここで Θ はフィルトレーション (2) の飽和時刻である．また d_i をパーシステント区間 I_i の発生時刻，$d_i + l_i$ を消滅時刻とよぶ．

パーシステント区間 I_i に対して，$I_i(b)$ で区間の下限 (birth)，$I_i(d)$ で区間の上限 (death) を表すことにする．

定義 3.3 パーシステントホモロジー群 (3) に対して

$$PD_k(\mathbb{K}) = \{(I_i(b), I_i(d)) \in \mathbb{R} \times \mathbb{R} \mid i = 1, \ldots, s+r\}$$

を k 次パーシステント図とよぶ．

ここでパーシステント図 $PD_k(\mathbb{K})$ 内の全ての点は，対角線より上側にくることに注意しておく．また定義より，対角線付近の点はパーシステント区間が短いため，発生してからすぐに消滅，もしくは飽和するホモロジー類に対応する．一方で対角線から離れたところにある点は，長く存続するホモロジー類を表すことになる．

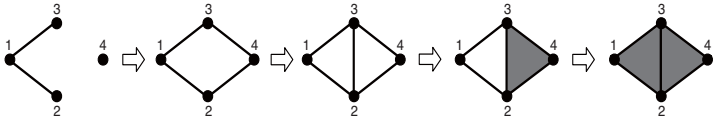


図 4：フィルトレーション $\mathbb{K}$．飽和時刻 $\Theta = 4$.

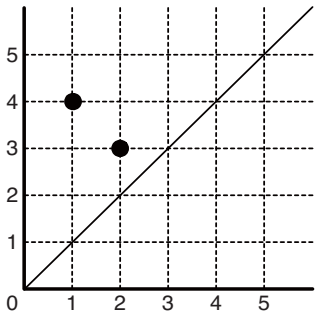


図 5：図 4 で与えられるフィルトレーション $\mathbb{K}$ の 1 次パーシステント図 $PD_1(\mathbb{K})$

例えば図 4 のフィルトレーション $\mathbb{K}$ が定めるパーシステント図 $PD_1(\mathbb{K})$ は，図 5 で与えられる．

4　タンパク質の立体構造解析への応用

タンパク質は生命活動を営む上で必須の物質であり，細胞内で繰り広げられている様々な働きはタンパク質を基本ユニットとして展開される．生体内に現れるタンパク質は，20 種類のアミノ酸を 1 次元的に並べたものを，3 次元空間内で折りたたんだ構造をとる．

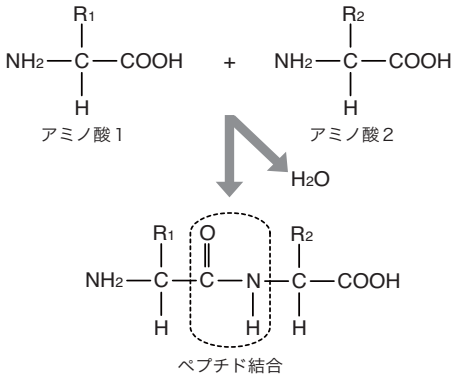


図 6：ペプチド結合．R_1 や R_2 はアミノ酸の側鎖を表す．

ここで，アミノ酸は共通の基本構造に加えられる側鎖の違いによって分類される．またアミノ酸の 1 次元的な構造は，隣り合うアミノ酸とのペプチド結合によって与えられる（図 6 参照）

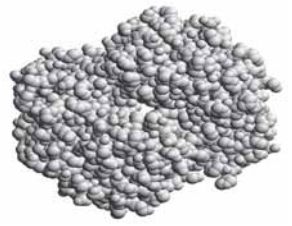


図 7：ヘモグロビン (1BUW)

各原子にはファンデルワールス半径が定められている．これはそれぞれの原子の原子核を中心に，電子が存在する密度に応じて定められた原子の仮想的な半径である．この半径が定める球として原子を表現したものを，ファンデルワールス球とよぶ．よって各原子の 3 次元空間での中心座標がわかれば，タンパク質をファンデルワールス球の和集合として表現できることになる．ここでタンパク質を構成している原子の空間座標は，X 線結晶解析技術の発達によって詳細に調べられており，そのデータは Protein Data Bank (PDB) [6] に保存され一般公開されている．図 7 は，タンパク質の一つであるヘモグロビン (PDB ID: 1BUW) のファンデルワールス球体モデルを，PDB データから描画させたものである．

これより各タンパク質を，重み付き Čech 複体やアルファ複体で表現することができる．また半径増大列に対応するフィルトレーションを構成することで（図 8 を参照），トポロジカルな量の履歴やロバスト性を調べることが可能となる．

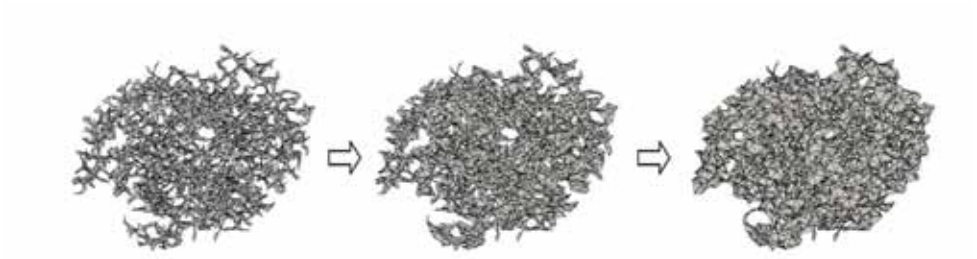


図 8：ヘモグロビン (1BUW) の Čech 複体フィルトレーション

例えば PDB ID が 1OVA で与えられるオボアルブミンを例に挙げ，そのパーシステント図を見てみよう．ここでフィルトレーションは重み付きアルファ複体で与える．またファンデルワールス球の半径を調節するパラメータ w を，各 i 番目の原子半径ごとに

$$r_i(w) = \sqrt{r_i^2 + w}$$

で導入する．ここで $w = 0$ に対応する r_i はファンデルワールス半径とする．このときパラメータ w を区間 $[0, 20]$ の間で動かした 1, 2 次パーシステント図は，それぞれ図 9 と図 10 で与えられる．また比較のため，これらのベッチ数のプロットを図 11 と図 12 にのせてある．

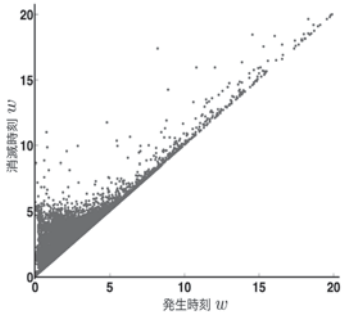


図 9：1OVA の 1 次パーシステント図

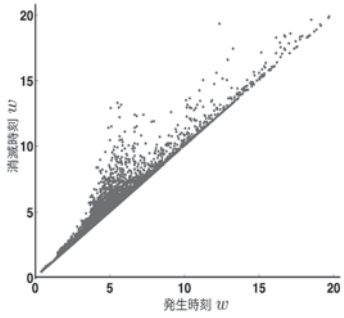


図 10：1OVA の 2 次パーシステント図

パーシステント図を見てわかるように，対角線付近に多くの生成元が存在している．これらの対角線付近の生成元は，発生してから消滅するまでのパラメータ幅が短いため，フィルトレーション内に現れるトポロジカルなノイズと見なせる．また比較的対角線から離れたところに位置する生成元は発生してから消滅するまでのパラメータ幅が長いため，パラメータ変化に対してロバストな生成元に対応する．つまりフィルトレーション過程に現れるこのようなトポロジカルなノイズやロバストな生成元を，パーシステント図は区別することができる．ベッチ数のプロットからなる図 11 と図 12 からは，このような情報は手に入らないことに注意しておく．

ではパーシステントホモロジー群を用いて，タンパク質の物性について調べてみよう．タンパク質は生体内で多種多様な働きをしており，その機能と立体構造は密接に関係している．

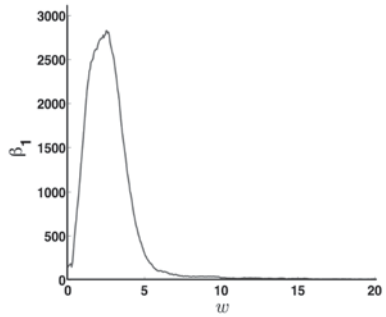


図 11 : 1OVA の 1 次ベッチ数のプロット

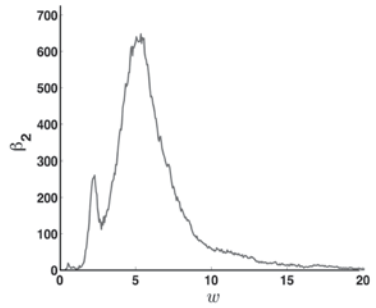


図 12 : 1OVA の 2 次ベッチ数のプロット

例えば，立体構造を大きく変形させることで，別の分子を取り込む働きをするタンパク質もある．このようなタンパク質の場合，立体構造を変形させる為にはある程度柔らかい構造を取る必要がある．このようにタンパク質の柔さや固さといった物性を知ることは，機能発現を調べる際の重要な手がかりとなりうる．

このタンパク質の柔らかさを測る指標の 1 つに圧縮率とよばれるものがある．タンパク質の圧縮率を実験的に求めることで，立体構造とゆらぎや機能との関係を調べることが可能である（詳しくは文献 [1] を参照）．しかし圧縮率を実験で測定するにはそれなりの実験装置が必要であり，もう少し手軽に圧縮率を調べることができれば望ましい．例えば PDB には膨大なタンパク質の立体構造に関するデータが蓄えられているので，これらのデータを利用して圧縮率と相関をもつ指標を得られないだろうか．そこでパーシステントホモロジー群の立場からこの問題を考えてみる．

タンパク質の圧縮率は，その内部に存在する空洞に関係していると予想されている．さらに物理・化学的背景から，圧縮率に影響を及ぼすと思われる幾つかの幾何構造（原子の疎配置性など）もある．論文 [3] では，これらを反映させた量をパーシステント図から取り出し定量化を試みた．その結果を図 13 に示す．

ここでの数値計算結果との比較には，文献 [1] 内にある実験から圧縮率が求まっているタンパク質を用いている．図 13 から見てとれるように，多くのタンパク質がパーシステント図から導出した定量化 C_P と線型相関の関係にある．これより，ここで行ったパーシステント図を用いた圧縮率の定量化 C_P は，ある程度幾何構造と圧縮率の関係を抽出できているものと思われる．

参考文献

[1] 月向邦彦，硬い蛋白質と軟らかい蛋白質—圧縮率から見た構造のゆらぎ—，蛋白質　核酸　酵素, Vol. 41, 2025–2036.

[2] G. Carlsson, Topology and Data, Bulletin AMS, Vol. 46, 255–308 (2009).

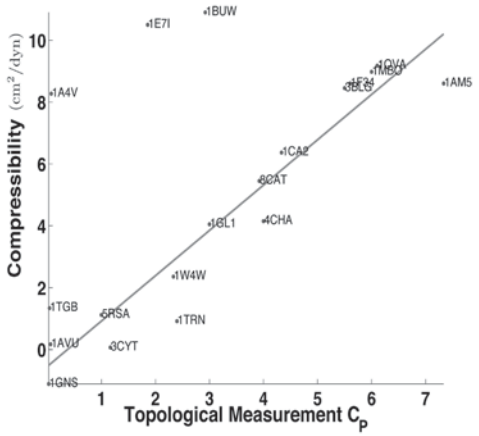


図 13 : パーシステント図から得られる定量化 C_P と圧縮率の関係．各タンパク質の圧縮率は論文 [1] の値を用いており，数値計算で使用した PDB ID はプロットの横に記入してある．

[3] M. Gameiro, Y. Hiraoka, S. Izumi, M. Kramar, K. Mischaikow, and V. Nanda, Topological Measurement of Protein Compressibility via Persistence Diagrams, 九州大学 IMI プレプリント.

[4] 平岡裕章，タンパク質構造とトポロジー：パーシステントホモロジー群入門，シリーズ「現象を解明する数学」，共立出版（近刊）.

[5] A. Zomorodian and G. Carlsson, Computing Persistent Homology, Discrete Comput. Geom. Vol. 33, 249–274 (2005).

[6] PDB, `http://www.rcsb.org/pdb/`

可微分写像の特異点論とデータ可視化

佐伯　修
九州大学マス・フォア・インダストリ研究所

1　序文

一般に，科学的なシミュレーションや実験により得られるデータは，ユークリッド空間の間の写像 $f\colon \mathbb{R}^n \to \mathbb{R}^p$ の離散サンプル点の集まりとして定式化できることが多い．本稿ではこうしたデータ，特に大規模なデータの特徴を，微分位相幾何学に基づいて解析し，データの可視化に役立てる技術について，特にそのために必要となる，可微分写像の特異点論における基礎的な事項を中心に解説する．

なお本文章の内容の一部は，高橋成雄氏（東京大学大学院新領域創成科学研究科）との共同研究の結果であり，一部の資料は高橋氏からご提供いただいたものである．高橋氏にはこの場を借りて感謝申し上げたい．

以下，M を n 次元 C^∞ 級多様体，N を p 次元 C^∞ 級多様体とし，$n \geq p \geq 1$ と仮定する．多様体論に不慣れな読者は，M, N はそれぞれ $\mathbb{R}^n$, $\mathbb{R}^p$ の開集合であると思って読み進めていただいて問題ない．そして，$f\colon M \to N$ を可微分写像（より正確には C^∞ 級，すなわち無限回微分可能な写像）とする．

2　関数とレベル集合

序文のような写像のデータ解析については，まずスカラー関数の場合，すなわち $p = 1$ で $N = \mathbb{R}$ の場合が非常に良く研究されている．実際この場合は，技術的にあまり複雑なことは要求されず，種々の現実的場面で役立つことが知られている．この節ではこうしたスカラー関数 $f\colon M \to \mathbb{R}$ の場合について解説する．

スカラー関数の特徴解析には，次で定義されるレベル集合が重要な働きをする．

定義 2.1 値 $c \in \mathbb{R}$ に対して，

$$f^{-1}(c) = \{x \in M \mid f(x) = c\}$$

を**レベル集合**（もしくは，等値集合，等値線，等値面，isoline, isosurface 等々）という．

一般にレベル集合は $n-1$ 次元となる ($n = \dim M$)．ただし，多様体になるとは限らない．たとえば地上の標高データであれば，$n = 2$ であってレベル集合は等高線となる．

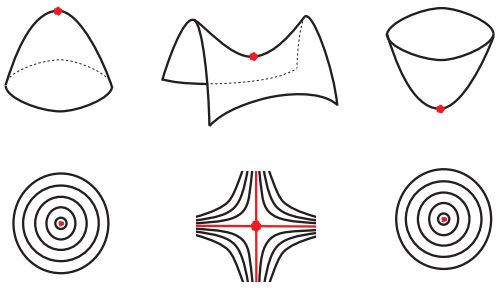


図 1：特徴的な等高線

さて，たとえばそうした地上の標高データが与えられたとき，そのデータの特徴を読み取るためには何が重要であろうか？ 等高線が重要であることはもちろんであるが，中に特徴的な等高線があることに気づくであろう．それは頂上，峠，谷底に相当する（図 1 参照）．

これらの特徴的等高線での（標高の）値を少し変化させると，等高線が生成・消滅したり，あるいは併合・分離したりする．つまり，等高線の形が変化するところが，データの特徴を把握する際に重要である．

こうした情報を集約するために，以下の概念が非常に良く用いられる．

定義 2.2 (Reeb [11]) レベル集合の各連結成分を 1 点につぶしてできる図形（グラフ）を **Reeb グラフ**という（状況によっては contour tree, volume skeleton tree, topological volume skeleton, level-set graph, Stein 分解，等々とも呼ばれる）．図 2 参照．数学的に厳密には，定義域 M の商空間としての位相を入れた位相空間であるが，実際には一般的なスカラー関数 f の Reeb グラフは，頂点と辺からなるグラフとなることが知られている．

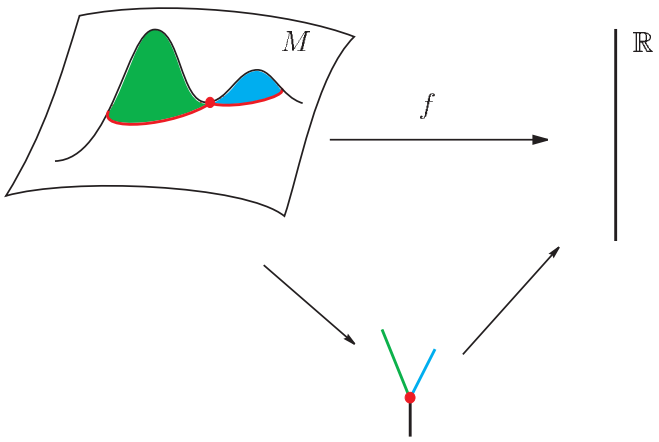


図 2：Reeb グラフの例

こうしたグラフは，標高データの場合に等高線の形の変化を表現する道具[13]として非常に多くの研究がなされていると共に，様々な応用も試されている．

与えられたデータからReebグラフを求めるアルゴリズムは，定義域の次元nが$n=2,3,4$のときには既に確立している（たとえば[1, 4, 10]参照）．

さて，ここで重要な点は，Reebグラフの頂点が，ちょうどレベル集合の形が変わるところに対応していることである．データの大局的特徴を捉えるには，こうした頂点が重要な役割を担う．これは図1のような点に対応している．これらは以下のように定式化できる．

定義 2.3 (1) 可微分関数$f\colon M\to\mathbb{R}$を考える．点$x\in M$であって，（xのまわりの局所座標について）そこでのfの1階の偏微分係数がすべて消える点をfの**臨界点**（または**特異点**）という．またその点でのfの値を**臨界値**という．

(2) 臨界点xで，fの2階の偏微分係数からなる$n\times n$対称行列

$$\left(\frac{\partial^2 f}{\partial x_i\partial x_j}(x)\right)_{i,j}$$

が正則行列のとき，臨界点xは**非退化**であるという（ここで$(x_1,x_2,\dots,x_n)$は，点xのまわりの局所座標である）．

なお，どんな関数も，ほんの少し摂動すれば，臨界点はすべて非退化として良いことが知られている（たとえば[6, 7]参照）．

微分位相幾何では以下の定理が基本的である．

定理 2.4（Morseの補題） 非退化な臨界点のまわりで，fは適当な局所座標により

$$f=\pm x_1^2\pm x_2^2\pm\cdots\pm x_n^2+c$$

と書ける（cは定数で，臨界値に相当する）．

上の2次式で，マイナスの符号の個数を，臨界点の**指数**という．臨界点のトポロジーは指数で決定される．すなわち，レベル集合の変化は臨界点の近くでのみ起こるが，その変化は上の2次式で完全に記述できるのである．（たとえば次元が$n=2$のときは，指数は2, 1, 0の3種類であって，それぞれの臨界点の近くでのレベル集合は図1で尽きている．）こうした意味で，レベル集合の変化を追うためにMorseの補題は基本的なのである．

たとえば$n=3$で，Mが3次元ユークリッド空間の開集合のとき，レベル集合（等値面）の臨界値前後での大局的な変化は，その面が外に向かって値が大きくなるのか，小さくなるのか，つまりその面によって隠される部分の値の大小まで込めて，数学的に分類することが可能である（[14, 15]参照）．こうした分類は，3次元データの可視化において大変重要である．

具体例として，たとえば[3]では，陽子と水素原子の衝突における電子密度関数のシミュレーションデータにこうした手法を適用している．これは時空間データであり$n=4$に相当するが，実際には時刻Tを止めたときの3次元データの解析を行い，その時刻Tを変化させることで，Reebグラフの変化を抽出し，特徴的な時刻を探している．これにより，衝突の際の電子分布の変化の様子とその特徴が，単なる動画による通常の可視化によるよりも，良くつかめることが解説されている．

3　可微分写像の特異点と特異ファイバー

ではいよいよ一般の可微分写像 $f\colon M \to N$ で，$n = \dim M \geq p = \dim N \geq 1$ で $p = 1$ とは限らない場合を考えよう．$N = \mathbb{R}^p$ の場合は，p 個の成分関数を並べて，

$$f = (f_1, f_2, \ldots, f_p)$$

と書けるので，f は p 値関数（もしくは多値関数）とも呼べる．この場合は p 個の関数それぞれについて前節で述べたような解析をすることはもちろん可能である．しかし，それでは各成分関数間の関係はおろか，データの全体像も見えてこないことが多い．

そこでここでは成分関数それぞれを考えてからそれらの間の関係を探る，といった指針を捨て，1つのまとまった写像 f を考える，という立場に立ってデータ解析をしてゆこう．

定義 3.1 点 $c \in N$ に対して，

$$f^{-1}(c) = \{x \in M \mid f(x) = c\}$$

を，f の**ファイバー**という．（ときにはレベル集合ともいう．）

たとえば，$n = 3$ とし，M を海水，$f\colon M \to \mathbb{R}^2$ を，$f =$（水温，塩分濃度）として得られる写像としよう．すると，状況は図3のようになる．

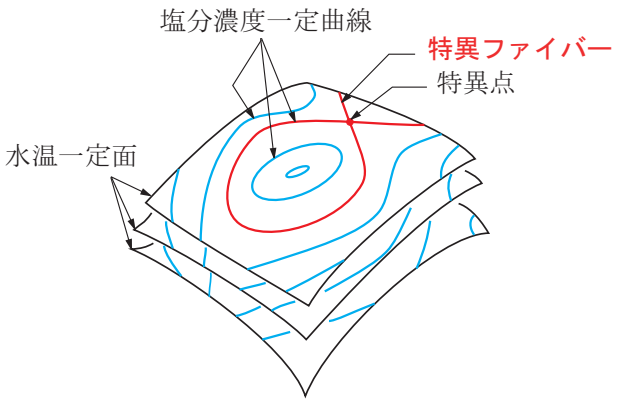


図3：2値関数のファイバーの例

なお，特異点を含むファイバーを特異ファイバーと呼ぶが（詳細は後述），これが多値関数データの特徴抽出において重要な役割を果たすことが，スカラー関数の場合の類似として容易に想像できよう．

定義 3.2 可微分写像 $f\colon M \to N$ を考える．M の点 x に対して，x と $f(x)$ のまわりの局所座標を選ぶ．このとき，$df_x\colon \mathbb{R}^n \to \mathbb{R}^p$ を，f の**ヤコビ行列**（f の成分関数の点 x での1階の偏微分係数を並べてできる，実 $p \times n$ 行列）から定まる線形写像とする．これを f の，点 x での

微分という．そして，$\operatorname{rank} df_x < p$ となる M の点 x を f の**特異点**という．（この定義は局所座標の選び方に依存しないことが容易に証明できる．）特異点全体の集合

$$J(f) = \{x \in M \mid \operatorname{rank} df_x < p\}$$

を f の**ヤコビ集合**（もしくは**特異点集合**）という．さらに，特異点の f による像を**特異値**，特異点を含むファイバーを**特異ファイバー**という．

一般にヤコビ集合 $J(f)$ は $p-1$ 次元となることが知られている．

さて，$p=1$ の場合，すなわちスカラー関数の場合には Morse の補題があり，それによりレベル集合の変化が非常によく理解できた．しかしながら一般の $p \geq 2$ に対しては，そうした補題は特別な場合を除き知られていない．というよりむしろ，一般には不可能であることが数学的に示されている（詳細は [5, 8] 等を参照）．

ここではそうした Morse の補題に類似の定理が成り立つ場合について解説する．具体的には $p=2,3$ の場合である．

まず $p=2$ の場合を見てみよう．簡単のため $n=2$ とする．すると，“一般的な写像” の特異点には，**折り目**と**カスプ**の 2 種類しかないことが古典的に知られている（[9, 16] 等参照）．それぞれ，局所座標を用いて

$$(x,y) \mapsto (x,y^2), \qquad (x,y) \mapsto (x,-xy+y^3)$$

と表される特異点である（図 4 参照）．

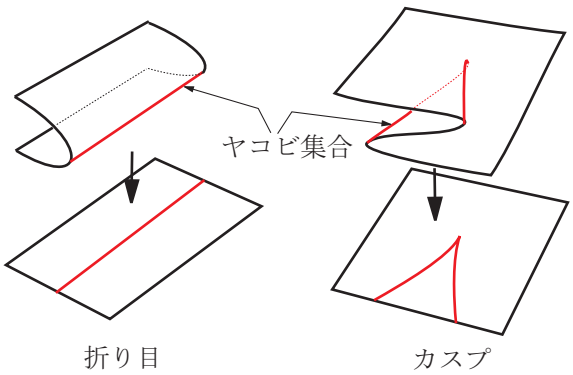


図 4：折り目とカスプ

なお，上のような分類は定義域の次元が $n \geq 3$ の場合にも同様に可能である．ただし，Morse の補題のときのように，指数によっていくつか異なるものが登場する．

たとえば可微分写像 $f\colon M \to N$ について，$p = \dim N = 2$ で，$\dim M = n \geq 3$ が奇数と仮定しよう．すると各折り目特異点に**指数** λ が定義できる $(\lambda = 0, 1, \ldots, (n-1)/2)$．ヤコビ集合の中で，どの点がカスプかというのは，理論的にはもちろん分かるはずであるが，データ相手にカスプを同定するためには工夫が必要である．たとえばカスプは，上述の指数が変化すると

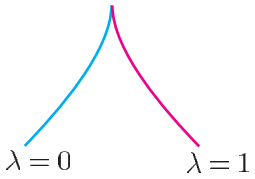


図 5：カスプ近くの折り目特異点の指数（$n = 3$ の場合）

ころとして特徴付けられる（図 5 参照）．なお，折り目特異点の指数を計算することはそれほど（アルゴリズム的に）難しくはない．

Edelsbrunner–Harer [2] は，可微分写像を区分的線形写像で近似し，そのヤコビ集合を求めるアルゴリズムを提唱した．理論的にはそれで求められるはずであるが，実データに対して適用すると，曲線となるべき部分がギザギザになってしまうなど，一般にきれいに出力されない．図 6 は，この抽出アルゴリズムを組み合わせて計算された特異ファイバーの例を示しており，2 つのスカラー関数の逆像の共通部分であるファイバーが，その関数値の変化に応じて位相的な変化を起こしている様子が見て取れる．（それぞれ，定義域 $\mathbb{R}^3$ と値域 $\mathbb{R}^2$ がペアになっており，$\mathbb{R}^2$ の黒い点に対応する特異ファイバーが $\mathbb{R}^3$ で赤い曲線として描かれている．左のペアは 1 つの連結成分が生成・消滅する場合を，右のペアは 2 つの連結成分が併合・分岐する場合を表している．）しかしながら，この特異ファイバーの抽出手法は，解析関数の事例では適切な微分位相幾何特徴をもたらすが，実際のボリュームデータなどに適用すると，ノイズや離散データの扱いのために，定義域の多くが特異ファイバーとして覆い尽くされてしまうなどの問題が存在する．

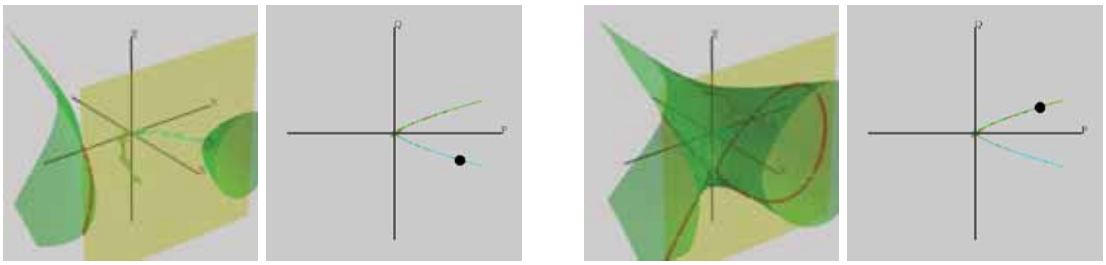


図 6：3 次元から 2 次元への写像の特異ファイバーの例

さらに，特異点や特異ファイバーがどこにあるかは分かっても，各特異点や特異ファイバーの型は不明である．微分位相幾何学における可微分写像の特異点論を用いれば，そうした特異点や特異ファイバーの型の同定がある程度可能になり，大規模データの解析，及び可視化に大きく貢献できる可能性がある．

4　可視化のために

多値関数データの可視化のためには，

(1) ヤコビ集合の特定
(2) 各特異点の型の特定
(3) ヤコビ集合像の特定
(4) ヤコビ集合像が仕切る値域多様体の各領域上のファイバーの特定

が必要である．特に上記 (4) のためには，特異ファイバーと，その近くでのファイバーの変化を特定することが不可欠となる．$\dim M = n = 3$, $N = \mathbb{R}^2$ のときの写像 $f\colon M \to \mathbb{R}^2$ について，ファイバー変化の一例を図 7 に示す（赤線がヤコビ集合像を表し，それで仕切られた各領域上のファイバーが黒で，ヤコビ集合像の交点以外の点上のファイバーが青で，交点上のファイバーが緑で，それぞれ描かれている）．

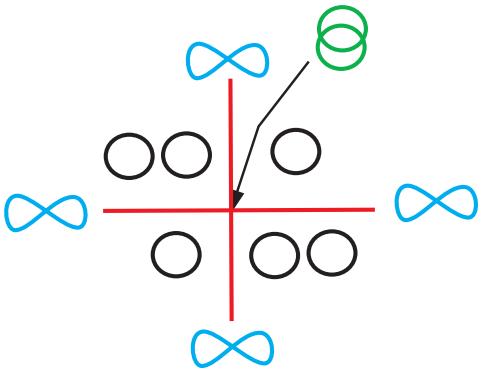


図 7：3 次元から 2 次元への写像のファイバー変化の一例

図 7 を見てもわかるように，ファイバーには，その複雑度に応じて階層構造がある．正確には，ファイバーの「型」$\mathcal{F}$ に対して，

$$\mathcal{F}(f) = \{y \in N \mid \text{ファイバー } f^{-1}(y) \text{ が } \mathcal{F} \text{ 型}\}$$

という値域多様体 N 内の部分集合を考え，

$$\kappa = \dim N - \dim \mathcal{F}(f)$$

を，ファイバーの型 $\mathcal{F}$ の**余次元**という．$n = 3$, $p = 2$ のときに現れるファイバーの余次元の例を図 8 に示す．

では次に $n = 4$, $p = 3$ の場合を見てみよう（詳細は [12] を参照）．これはたとえば，時空間上で与えられたデータの 3 つ組の解析に相当する．まず，“一般的な写像” $f\colon M \to N$ ($\dim M = 4$, $\dim N = 3$) のヤコビ集合像は，N 内の特異点を持った曲面となって現れる．その各点の近くでの様子は図 9 のように分類される．

たとえば図 9 の (5) のような点の近くでのファイバー変化は，何種類かあるが，そのうちの一つは図 10 のようになる．

そして，$n = 4$, $p = 3$ の場合の特異ファイバーのリストは図 11 のようになる．

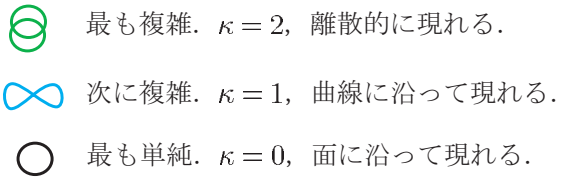


図 8：3 次元から 2 次元への写像に現れるファイバーの例とその余次元

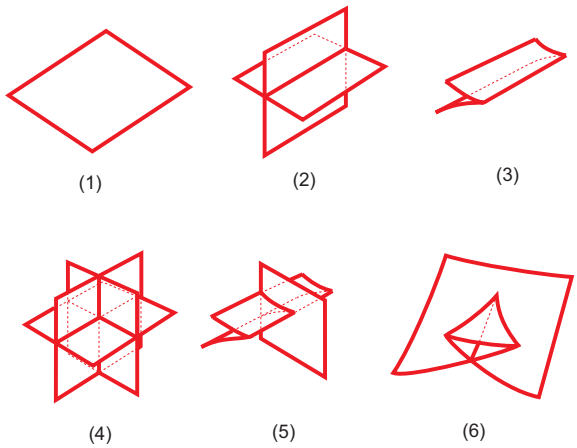


図 9：4 次元から 3 次元への写像のヤコビ集合像の局所形

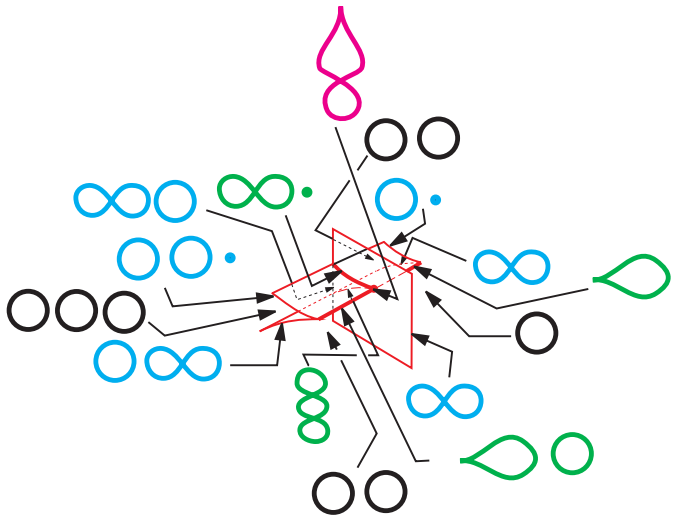


図 10：4 次元から 3 次元への写像のファイバー変化の一例

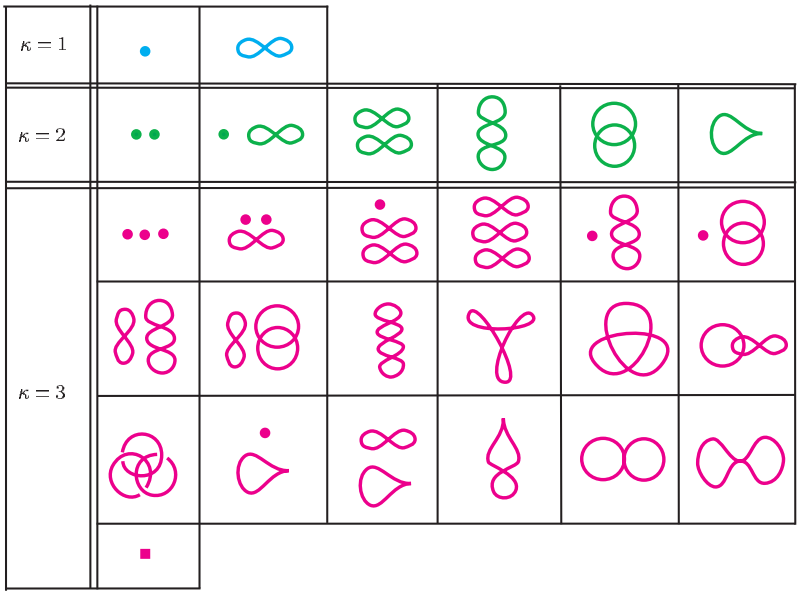


図 11 : 4 次元から 3 次元への写像に現れる特異ファイバーのリスト

こうしたリストを用いれば，データ解析において，特徴的なファイバーとその型を抽出することが可能となり，データの可視化に貢献できることが大いに期待される．

応用の可能性の例としては，たとえば CT スキャンデータがある．CT スキャンは，ある方向に関する断層画像を積み重ねることで，3 次元データを計測する．その際，複数の方向からの断層画像群を計測することで，取得したい 3 次元データの復元精度を上げることが考えられる．1 方向だけ考えれば Reeb グラフを構築することに相当するので，こうして 2 つ（以上）の方向を考え，Reeb グラフの合成表現，あるいは特異ファイバーのつながりを表すグラフを構築すれば，1 方向だけ考えていたのでは見えなかった特徴も抽出できるであろう．

さて，こうして見てきた微分位相幾何特徴抽出手法は，通常ではハンドリングできないほどの膨大な取得データに内在する重要な特徴を，少ないデータ量で効率的に画像として表現できる特長を持っている．もちろん，視覚情報の（情報）帯域が数値データなどの文字情報に比べると格段に広いのもご利益の一つである．こうした手法が今後，データ解析において大活躍することになるであろうと期待される所以である．

参考文献

[1] H. Carr, J. Snoeyink, and U. Axen, Computing contour trees in all dimensions, Computational Geometry: Theory and Applications **24** (2003), 75–94.

[2] H. Edelsbrunner and J. Harer, Jacobi sets of multiple Morse functions, Foundations of computational mathematics: Minneapolis, 2002, pp. 37–57, London Math. Soc. Lecture Note Ser., Vol. 312, Cambridge Univ. Press, Cambridge, 2004.

[3] I. Fujishiro, R. Otsuka, S. Takahashi, and Y. Takeshima, T-Map: A topological approach to visual exploration of time-varying volume data, in "High-Performance Computing" (Eds. J. Labarta, K. Joe, and T. Sato), pp. 176–190, Lecture Notes in Computer Science, Vol. 4759, Springer, Berlin, Heidelberg, 2008.

[4] X. Ge, I. Safa, M. Belkin, and Y. Wang, Data skeletonization via Reeb graphs, Twenty-Fifth Annual Conference on Neural Information Processing Systems 2011, pp. 837–845.

[5] J.N. Mather, Stability of C^∞ mappings. VI: The nice dimensions, Proc. Liverpool Singularities–Symposium, I (1969/70), pp. 207–253, Lecture Notes in Math., Vol. 192, Springer, Berlin, 1971.

[6] 松本幸夫，Morse 理論の基礎，岩波書店，2005.

[7] J. Milnor, Morse theory. Based on lecture notes by M. Spivak and R. Wells, Ann. of Math. Studies, No. 51, Princeton Univ. Press, Princeton, N.J., 1963.

[8] 西村尚史，福田拓生，特異点と分岐，特異点の数理 2，共立出版，2002.

[9] 野口広，福田拓生，復刊 初等カタストロフィー，共立出版，2002.

[10] V. Pascucci, G. Scorzelli, P.-T. Bremer, and A. Mascarenhas, Robust on-line computation of Reeb graphs: Simplicity and speed, ACM Trans. Graph. **26**, no. 3, (2007), Article 58, 58.1–58.9.

[11] G. Reeb, Sur les points singuliers d'une forme de Pfaff complètement intégrable ou d'une fonction numérique, C. R. Acad. Sci. Paris **222** (1946), 847–849.

[12] O. Saeki, Topology of singular fibers of differentiable maps, Lecture Notes in Math., Vol. 1854, Springer–Verlag, Berlin, 2004.

[13] S. Takahashi, T. Ikeda, Y. Shinagawa, T.L. Kunii, and M. Ueda, Algorithms for extracting correct critical points and constructing topological graphs from discrete geographical elevation data, Computer Graphics Forum **14** (1995), 181–192.

[14] S. Takahashi, Y. Takeshima, and I. Fujishiro, Topological volume skeletonization and its application to transfer function design, Graphical Models **66** (2004), 24–49.

[15] Y. Takeshima, S. Takahashi, I. Fujishiro, and G.M. Nielson, Introducing topological attributes for objective-based visualization of simulated datasets, in "Proc. Volume Graphics 2005", pp. 137–145, 2005.

[16] H. Whitney, On singularities of mappings of euclidean spaces. I. Mappings of the plane into the plane, Ann. of Math. (2) **62** (1955), 374–410.

パターン形成問題の数理解析

栄　伸一郎

九州大学マス・フォア・インダストリ研究所

1　自然界に見られる形

自然界には色々な形がありますが, それらがどのくらい理論的に理解出来るかを考えてみることにしましょう．ところで, 一口に形といいましても, 大きくは宇宙における星や銀河の集まりが表す形から, 小さくは原子や電子の分布の表す形まで色々ありまして, それぞれの分野で宇宙論あり, 量子論ありで対応する理論というものがあります．ここでは我々の日常身の回りで目にすることが出来る程度の大きさのものを対象とすることにします．例えば, 雪の結晶や樹脂状結晶の形, 炎の形, しま馬や豹などの動物の表皮模様, ある種の化学反応に見られる螺旋模様などを挙げることが出来ます（図 1, 2, 3, 4 など）．この他にも身の回りにはさまざまな形が存在しています．それでは, このような形というものはどのようにして生じてくるので

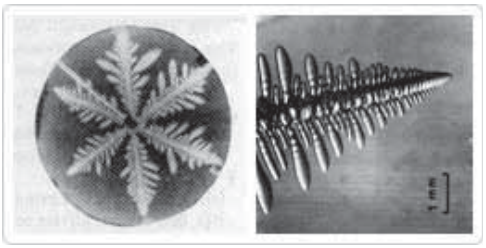


図 1：雪の結晶（左）及び樹枝状結晶（右）（[3] より）

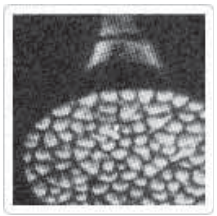


図 2：炎（[1] より）

しょうか．何か理論的に分かることがないでしょうか．ここでは一つのアプローチの仕方を紹介することにします．

図 3：動物の表皮模様（[2] より）

図 4：ある酸化還元反応に見られる螺旋模様（[3] より）

さて, 形の形成ということを理論的に解析したい訳ですが, 上に挙げたような現象はそれぞれ皆メカニズムが異なっています．例えば雪の結晶や樹枝状結晶の形成は物性の問題に属するでしょうし, しま馬や豹の表皮模様の形成は生物学に属することでしょう．従って, それらをひとまとめにして議論することは殆ど不可能ですし, 仮に出来たとしても, ものすごく一般的な話になってしまう恐れがあります．そこで, ここでは具体的なテーマを一つ絞って紹介したいと思います.

ここで具体的な話に入る前に, そもそも形とはどのように認識されるのかということをはっきりさせておこうと思います．最初に挙げた幾つかの例からわかりますように, それぞれの形は全てある 2 つの異なった状態の領域と領域の境界として表現されています．例えば雪の結晶は 6 角形の美しい形をしていますが, 氷と水の境界がそのような形をしている訳です．また, 表皮模様であれば色素の多い場所と少ない場所の境界の形が動物特有の模様を表している訳です．そこで, その境界付近に注目してみましょう．境界の近傍では, その境界を挟んで 2 つの異なった状態が隣り合っている訳で, ある状態の領域から別の状態の領域にその境界を越えて進んでみると, 途中でどちらの状態ともいえない所があるはずです．雪の結晶であれば, その境界付近では氷とも水ともいえない, どろどろした状態があることでしょう．表皮模様であれば, 色素の量が中途半端で色が付いているともいないともいえるような状態があることでしょう．もし, そのような中途半端な状態の領域がかなり広い範囲にあるなら, もはや形は, はっきりとは認識出来ないことになります．このように考えると, ある形がちゃんと認識されるためには境界付近に分布する中途半端な領域が非常に狭く, 境界がある程度はっきりしていることが必要であるとわかります．最後にまとめとして, 形の認識に関して標語的に述べておきますと, 次のようになります．“ある 2 つの異なった状態の領域があってそれらの領域の境界が十

分狭いとき, 形は境界の形状として認識される.”

2　形の理論的取り扱い

前節で, 形を扱うにはその境界の成す形状を解析すればいいということがわかりました. それでは, 境界自身はどのように扱うかというと, 境界は幅はあっても十分狭いため, 理想化として幅 0 と思ってしまうというのが一つの方法です. 従って, もし形を平面上で考えているなら, 対応する境界は曲線ということになります. これ以外にも, 幅は十分狭いが 0 ではないとして扱う方法もあり, 理論的には大変重要なのですが, ここでは幅を 0 として扱う方法のみ紹介することにします.

それでは, 理論的取り扱いがほぼ完成している例の中から, 最も単純そうな現象を一つ紹介することにしましょう.

今, 平面上に微小な磁性体的な素子が均一に隙間なく敷き詰められていて, 一つ一つの素子は真上か真下を向くのが落ち着いた状態であるとします. 一方, これらの素子は互いに隣り合って密に敷き詰められているため, 磁場の相互作用から, それぞれの素子は自身の周辺の素子の状態の影響を受けると考えられます. 影響の受け方としてはここでは最も単純なものの一つである, 周辺と同じ向きになろうとする, という影響の受け方をすると仮定します. ここで, 磁性体的としたのは, もし磁性体なら, 隣同士上下ペアになるのが一番落ち着いた状態ということになって, 上の仮定は少しおかしくなります. しかし, 上下ペアが落ち着いた状態とすると話がかなり難しくなりますので, 上のように仮定することにしました. ただし, 磁性体そのものの性質とは異なりますので, 磁性体的と表現したわけです.

さて, 話をわかり易くするために, 素子が上を向いていると黒く, 下を向いていると白く見えるとします. このときこの平面を上から見て, 黒または白の領域がどのような形になるかを考えてみましょう.

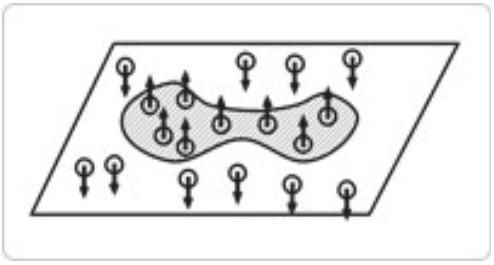


図 5：平面上に敷き詰められた素子

まず, 一つ一つの素子の上, または下を向く向き易さが同じでないとしましょう. 例えば上にはるかに向き易いとします. このときは, 途中どのような経過を辿るにせよ, 最終的には全ての素子は上を向き, 平面全体が黒くなってしまうだろうという予想が付くと思います. そこで最後の仮定として, 素子間の相互作用を考えないときの単独の素子が上または下を向く向き

易さは全く同じであるとします．このように仮定すると直感はほとんど働かなくなり, 理論的考察が重要になります.

最後に各素子は限りなく小さいとし, 連続的に分布しているとして扱うことにします．初期の状態が図 6 のようであったとします．このとき黒と白の境界（Γ とする）はどのように時間

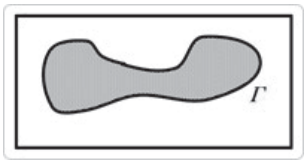


図 6：初期の形

変化するでしょうか．上述の基本的な状況設定に幾つかの仮定を加えることにより, 1980 年以降の研究を通して Γ の運動に関し次のことがわかっています：

結果 1 “曲線 Γ は

$$V = -\kappa \tag{1}$$

に従って運動する．ここで, V は Γ の外側法線方向に進む速度, κ は Γ の曲率である.”

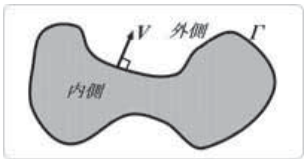


図 7：Γ の運動

(1) に従った運動を“曲率流”と言います.

この運動方程式に対して説明をしておきましょう．まず, V についてですが, Γ の外側方向ということで, Γ の内側, 外側を予め決めておかねばなりません．ここでは黒い領域の方を Γ の内側ということに決めます．従って V は Γ で囲まれた黒い方の領域から白い方の領域に向かって, Γ に垂直な方向に Γ が進む速さということになります.

次に曲率 κ ですが, Γ 上の点 P を一つ決め, その点において Γ に接するような円のうちで最大のもの（それ以上半径を大きくすると Γ からはみ出す部分が出来てしまうような円, 最大接円）を描きます．このような円は唯一つに決まりますが, その円の半径を r とし, $k = 1/r$ とします．最大接円が Γ の内部に描けるとき $\kappa = k$ とおき, 最大接円が Γ の外部に描けるとき $\kappa = -k$ とおいたものを点 P における Γ の曲率と定義します．例として, Γ が点 P の周りで直線だと, 無限に大きい接円が描けてしまうので, $r = \infty$, すなわち $\kappa = 0$ ということになります.

曲率の幾何学的な意味を簡単に説明しておきましょう．曲率とは曲線 Γ が内部の方向にどの程度曲がっているかを示す量で, 内部の方向に急な曲がり方をしている程, 接円の半径が小さく

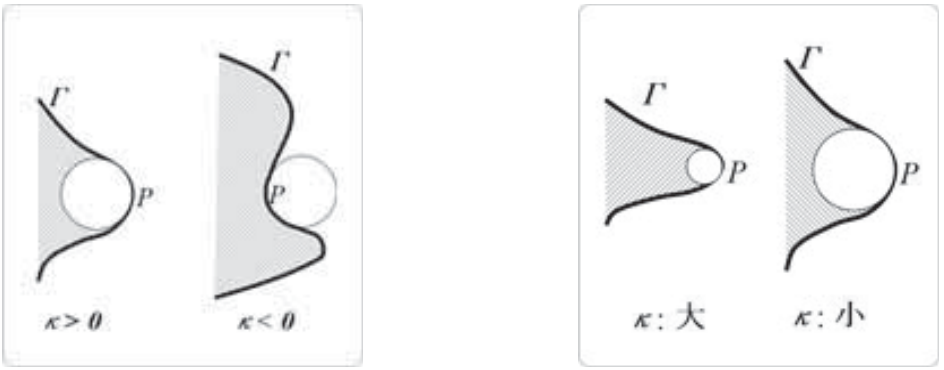


図 8：曲率 κ の正負, および曲率 κ の大小

なりますから曲率 κ は正の大きな値をとることになります．一方, 外側に急に曲がる程, 接円は Γ の外部に小さく描けますから曲率 κ は負で大きな値をとることになります．従って, Γ の運動が (1) であるということは, 例えば外側に出っ張ったような点では $\kappa > 0$ より, $V = -\kappa < 0$ となり, 曲線 Γ はそのような点においては内側に向かって運動することになりますし, 逆に内側に出っ張った点では $V = -\kappa > 0$ となり, Γ は外側に向かって運動することになります．こ

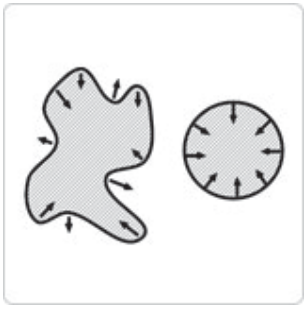


図 9：曲線 Γ の運動

のことは, Γ はその形の凹凸がなくなるように運動しているということを意味します．従ってだんだん円周に近い形になっていきます．また, Γ が一端, 円周に近い形になったなら, Γ 上至る所の点で曲率 κ は正ですから（円の内側が黒い領域だとして), どんどん内側に縮んで最後にはなくなってしまうということも理解出来ると思います．このように最初の黒と白の領域の関係で, 最終的にどの色が全体を占めるのかが分かるわけです.

実は (1) の運動に関してはもっと詳しいことがわかっています．それは, (1) に従って運動する曲線は, 必ずその弧長が時間と共に短くなっていくというものです．これによると, もし領域の形が図のようなひょうたん型をしていたとすると, 長さが極小になる場所で運動は止まり, 静止するということもわかります.

ここまでは, 各素子の上または下を向く向き易さは全く同じであるという仮定の下での話でした．しかし現実世界においてそのような理想的な状況はあり得ません．それを踏まえて, 少

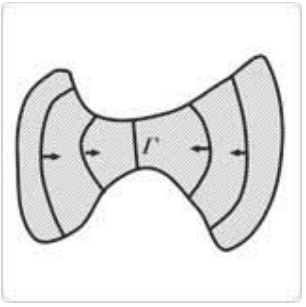


図 10：ひょうたん型領域における Γ の運動

しだけ現実的な設定として, 各素子の上下への向き方が少しだけ異なるという状況を考えてみることにします．このとき (1) に対応する式は

$$V = -\kappa + c \tag{2}$$

という式に変わります．これも曲率流方程式と呼びます．c は上下の向きやすさの違いの大きさに応じて決まる定数であり, 向きやすさが完全に同じ場合は $c = 0$ であったわけです．

以降, 仮に上の方が下の方より少しだけ向きやすかったとして話を進めてみましょう．前に上を向いている状態が黒く, 下を向いている状態が白く見えるとして, V は黒の領域から白の領域に, その境界 Γ が進む速さを表しているとしました．今, 上の方が少しだけ向きやすいわけですから, 黒の領域の方が拡がりやすい, すなわち $c > 0$ と仮定してよいことがわかります．Γ の運動を表す式が (2) となったとたんに, (1) に対して成り立っていた, 凹凸がなくなっていくなどの多くの結果は成り立たなくなります．そこで最も簡単な状況として, Γ の初期の形が完全な円周であったとしましょう．このとき, 時間がたっても円周の形状をしていることがわかっています．そこで時刻 t のときの円周の半径を $r(t)$ として, (2) を $r(t)$ の式で表してみると,

$$\frac{dr}{dt} = -\frac{1}{r} + c \tag{3}$$

となることが簡単な計算からわかります (読者の方の演習としましょう)．これは r の微分方程式であり, 実際に解くことができますが, ここでは次のように考えてみましょう．まず $r^* = 1/c$ と置きます．このとき, もし初期の円周の半径 $r(0) = r_0$ がこの r^* に等しければ, (3) の右辺がちょうど 0 ですから $\frac{dr}{dt} = 0$, すなわち半径 $r(t)$ はずっと r^* のまま変化しないことになります．このような特別な状態を“平衡状態”といいます．

次に $r_0 < r^*$ であったとします．このとき $\frac{1}{r_0} > c$ となりますから $\frac{dr}{dt} < 0$, すなわち半径 $r(t)$ は時間とともに減少します．いったん減少すると $\frac{1}{r}$ は c より更に小さくなり, $r(t)$ は益々減少することになります．結果として有限時間で $r(t) = 0$, すなわち消滅してしまうことがわかります．

逆に $r_0 > c$ であれば上記の議論と同様に, 今度は $r(t)$ はどんどん増加することがわかります．こうして初期半径 r_0 が r^* より大きいか小さいかで成長するか消滅するかが別れることになります．このような半径のことを“臨界半径”と呼び, 凝固現象などで, 最初にできた小さな氷片がその後成長するか消えてしまうかの説明に大変有効であることがわかっています．

(1) や (2) といった形の曲率流という運動は至る所に顔を出すことが知られています. 例えば, 2 種の生物が互いに競合関係にあり, その生物的力が対等のとき, 各種の占める領域同士の境界は曲率流 (1) の方程式に従って運動することがわかっています.

最初に紹介した, さまざまな形, 例えば氷と水の境界や動物の表皮の色素の境界など, 現象のメカニズムは全然異なるものの, いずれも境界の曲率が関係した形の方程式でその運動が記述出来ることがわかっており, 計算機シミュレーション等により, 現象に近いパターンが再現出来ることが知られています.

このように, 物の形を調べるのにその輪郭のみに注目し, 輪郭の運動を支配する方程式を導出し, 形の理論的解析を進めていこうという方法は, ようやく最近可能になったばかりです. この研究により, これまでわかっていなかった多くの問題が, 幾何的量と関連づけられることにより解決されつつあることを述べて終わりとします.

参考文献

[1] B. Lewis and G. von Elbe, Combustion, Flames and Explosions of Gases, Academic Press, 1961.

[2] J. D. Murray, Mathematical Biology, Biomathematics vol. 19, Springer-Verlag, 1989.

[3] P. Pelce, Dynamics of Curved Fronts, Perspectives in Physics, Academic Press, 1988.

[4] A. R. Winfree, When Time Breaks Down, Princeton University Press, 1986.

生物の輸送ネットワークモデルとその応用

手老　篤史

九州大学マス・フォア・インダストリ研究所

1　イントロ

道路や鉄道といった輸送ネットワークは製作・維持に多くのコストがかかるが我々の生活に欠かせないものであり, 現在, 日本でも多くの道路網や鉄道網が整備され続けている. 鉄道網では利用客が多い路線は乗客の運賃により増線・増便され, 利用者が少ない路線は減便・廃線となる. このような都市における輸送ネットワークは人口分布などに対応して最適な形状が変化する為, 製作開始時に計画した最適なネットワークが必ずしも運用時に最適であるとは限らない. 加えて事故や災害のようなアクシデントにより輸送ネットワークが断線する場合があるが, 事故・災害時には負傷者や物資の輸送が必要であるため, 輸送ネットワークは短期・長期にかかわらず予期できない状況変化への対応が求められる. このため様々な手法を試行錯誤し, 実際に実験することにより最適な都市計画法を模索する必要がある. だが, そのためには多くのコスト・年月を必要とするため現実的ではない.

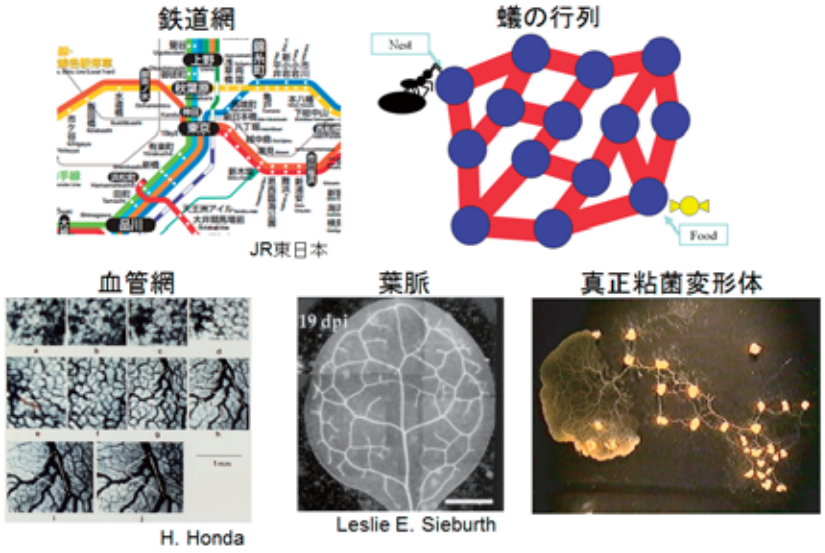


図 1：生物の作る適応的輸送ネットワーク

一方で人間以外の生物も集団で輸送ネットワークを作る場合がある. 例えば蟻は餌を巣に持ち帰るときにフェロモンを散布し, 後の蟻がその道を選択しやすくする. この結果, 蟻は効率的な経路の上に行列を作成する. また同様に個々の生物の内部にも輸送ネットワークが存在する. 例えば人間をはじめとした多くの生物は体内に血管網を持ち, 体内に適切に栄養分や酸素を行き渡らせる. この血管網の形成では血流と血管のずり応力により血管は成長する. 他にも植物では葉脈が葉の各所に水分や養分を輸送する役割を持っており, オーキシンという化学物質が葉脈形成に大きな影響を与えているといわれている [1].

このようなネットワークはどれも利用されている経路が発達し, 利用されていない経路が減衰・消滅するという適応的な性質によりネットワークが構築される. ここでは適応的なネットワーク全般に応用可能な理論を説明する. また, それにより長い年月の自然淘汰を生き延びることを可能にした生物ネットワークと人間の鉄道網を比較し, 最適なネットワークについて考察した結果を解説する.

2　粘菌の管ネットワーク

このような適応的なネットワークを持つ生物として真正粘菌変形体（以下, 粘菌とする）がいる. 粘菌は餌に接触するとその餌の周りに集まり栄養分を吸収する. また同時に 2 つ以上の餌に接触するとそれぞれの餌に集まりながらその間を管状の構造を持ったもので繋ぐ（図 2）. また, 粘菌は内部に核を多数持つが, それらを仕切る細胞膜や細胞壁が無いため単細胞生物である. 粘菌はこのように 1 つの細胞に多数の核を持つため, 個と集団の両方の性質を持つ. 例えば 1 個体の粘菌をナイフ等で物理的に切断すると切り離されたそれぞれが個体として振る舞い, 2 つの粘菌が接触すると 1 個体に合体する. この性質により粘菌は自在に形をコントロールできるため, 適応ネットワークを理解する良いモデル生物となっている.

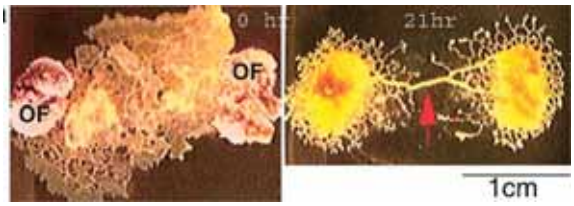


図 2：餌の周りに集まる粘菌

3　粘菌の迷路解き

ここではまず, ネットワークトポロジーを決定する重要な境界となっている粘菌の迷路解き現象について紹介する [2]. 本実験は中垣俊之氏（現はこだて未来大学教授）によって行われた. まず初期状態として寒天培地の上に OHP シートで迷路を作成する（図 3a）. ここで, 寒天は湿気を含んでいるため粘菌にとっては侵入可能な迷路の「通路」になるのに対し, OHP シー

トは乾燥しているため粘菌は侵入不可能な迷路の「壁」となる. 次に迷路のスタートとゴールにあたる箇所に 2 つの餌を配置する. すると粘菌は餌の周りに集まり, 迷路の通路上に管状の構造を持ったネットワーク（以下, 管とする）を形成する. 次に, 行き止まり上の管が消失し (図 3b), 最終的には条件にもよるが迷路の最短経路上にのみ管が残る（図 3c).

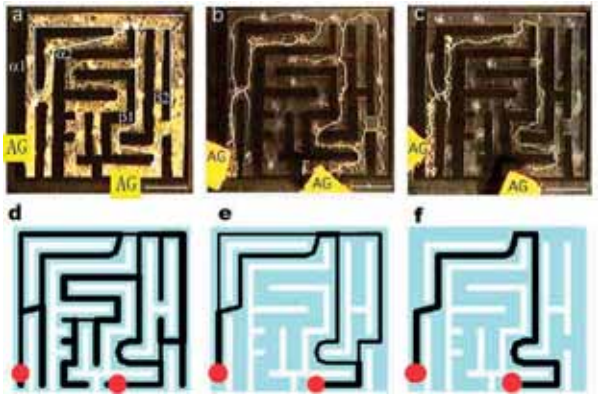


図 3 : (a-c) 粘菌の迷路解き. (d-f) 数理モデルによる数値計算結果

4　数理モデル

脳の無い粘菌はどのようなメカニズムで迷路を解くのだろうか. ここでは迷路を離散グラフで表記し, 数理モデルを用いてそのメカニズムを説明する. 迷路の交差点や行き止まりをノード N_i であらわし, それらを繋ぐ迷路の通路をリンク E_{ij} であらわす. ここで, N_1, N_2 は餌を置いた点とする. 各ノード N_i は変数 p_i をもち, これは各時間において粘菌の管が内部の原形質を押す力をあらわす. また, 各リンク E_{ij} は変数 L_{ij}, $a_{ij}(t)$, $Q_{ij}(t)$ をもつ. L_{ij} はリンクの物理的な長さをあらわし, $a_{ij}(t)$ は管の太さを, $Q_{ij}(t)$ は流量をあらわす.

ここでは管内の原形質流動は非圧縮性ニュートン流体が円管を流れているとしてポワズイユ流を仮定する.

$$Q_{ij} = \frac{\pi a_{ij}^4}{8\kappa} \frac{p_i - p_j}{L_{ij}} \tag{1}$$

ここで κ は原形質の粘性であり, 定数である. 次に $D_{ij}(t) = \frac{\pi a_{ij}^4}{8\kappa}$ とおくと以下が成り立つ

$$Q_{ij} = \frac{D_{ij}}{L_{ij}}(p_i - p_j) \tag{2}$$

ここで $D_{ij}(t)$ は管の太さ a_{ij} に対して単調増加な関数であり, リンクの重みを表す.

また, 各ノード N_i に流れこんでくる原形質の量と流れ出す原形質の量は等しいことから次の式が成り立つ.

$$\sum_j Q_{ij} + I_i = 0 \tag{3}$$

$I_i(t)$ は餌の周りに集まった粘菌から管ネットワークに流れ込む原形質の量をあらわし, 餌に繋がっていないノード N_i $(i \neq 1, 2)$ では $I_i = 0$ である.

なお, ここでは抵抗として $R_{ij} = \frac{L_{ij}}{D_{ij}}$ とおくことにより, (2) 式, (3) 式はそれぞれ電気回路におけるオームの法則・キルヒホッフの法則と同様になる.

次に経路の成長について考える. 粘菌の管はその内部を通る原形質量が多いと太さがより成長し, 少ないと減衰・消滅する性質がある. ここでは $D_{ij}(t) = \frac{\pi a_{ij}^4}{8\kappa}$ とおいているため, リンクの重み $D_{ij}(t)$ が流量 $Q_{ij}(t)$ に応じて変化する.

$$\frac{d}{dt} D_{ij} = f(|Q_{ij}|) - r D_{ij}. \tag{4}$$

ここで $f(q)$ は $f(q) = 0$ を満たし, q に対して単調増加な関数とする. $f(q)$ の関数によって最終的なネットワークの形状は異なる.

5 $f(q) = |q|^\mu$ の数値計算結果

ここでは前節で述べた数理モデルの典型的な数値計算結果として $f(q) = |q|^\mu$ の場合の数値計算結果を紹介する（図 4）. $\mu < 1$ の場合はほとんど全てのネットワークにおいて経路が残るのに対し（図 4a), $\mu > 1$ の場合は初期値やネットワーク形状に対して 1 つの経路が選ばれる. このように $\mu = 1$ のパラメータを境界としてネットワークのトポロジーは大きく変化する [3]. この $\mu = 1$ の場合では最短経路でのみ管が残り, 粘菌の迷路解きの実験が再現できる（図 3d-f）[4]. このとき最短経路上にのみ管が残ることは数学的にも証明されている [5, 6].

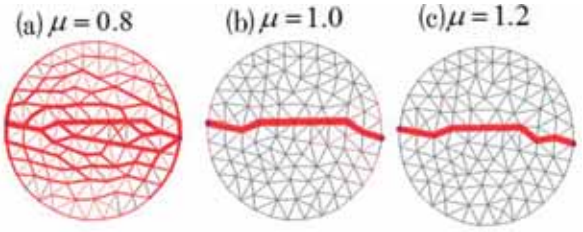


図 4 : $f(q) = |q|^\mu$ の数値計算結果.

6 ネットワークのリスク分散

一方で粘菌は流量が多い管を作らず, 流量が増えてくると何本かの管を残すことが知られている（図 5a,b）[7]. もし, 多すぎる流量を持つ太い管を作ればアクシデントによりその管が切断されたときに粘菌は大きな被害を受ける. このことから粘菌には自発的にリスク分散を行うメカニズムが内包されているといえる. この現象は管の成長法則である $f(q)$ に S 字型の関数を用いることで再現できる（ここでは $f(q) = \frac{|q|^3}{1+|q|^3}$ としている）.

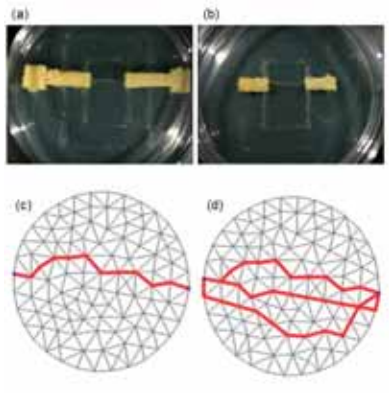


図 5 : 粘菌ネットワークのリスク分散に対する実験. (a), (b) はどちらも同量の粘菌を用いているが, (a) の方が餌が大きい. すると餌の周りに粘菌が集まった結果, 集合間を流動する粘菌は (b) の方が多くなり, 最終的な管の本数は変化する. (c), (d) は数値計算結果. 餌周辺からの流量 I_i を大きくすることにより, 最終的な管の本数が増加する.

7　多点の最短ネットワーク

次に 3 点以上の点を結ぶ最適ネットワークについて解説する. これまでに述べたように粘菌は流量が少ない場合に疎なネットワークを作る. この性質を用いて多点間の最短ネットワークを求めた結果が図 6 である. このアルゴリズムの解は必ずしも正解とはならないが, 短時間である程度の精度を持った解が得られる [8].

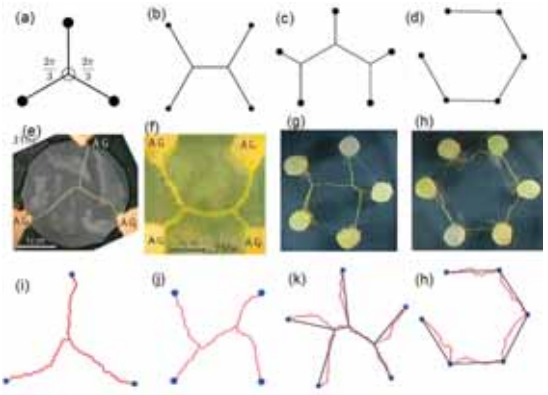


図 6 : 正多角形上の頂点を結ぶ最短ネットワーク (a-d) と粘菌の解 (e-h) と数値計算結果 (i-h). 実験・数値計算共に正解とは異なるネットワークトポロジーが得られる可能性があるが, 誤差は少なく短時間で解が得られる.

8　多点の最適ネットワーク

ここでは3点以上のリスク分散も考慮したネットワークを考える. 粘菌は流量が増えてくると複雑なネットワークを構成する（図 7d-f）. この数理モデルでも流量 $I_j(t)$ を大きくすることにより, 複雑なネットワークが得られる（図 7g-i）.

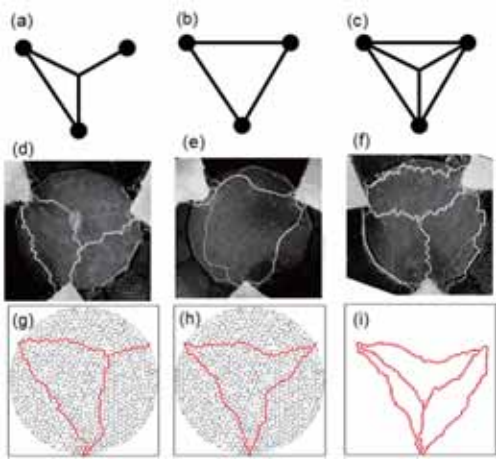


図 7 : 3 点の最適ネットワーク. 流量が増えるにしたがって, リスク分散が行われるかわりにネットワークの総距離が増加する.

9　生物による最適ネットワークの比較

最後に粘菌のネットワークと実際の人間の鉄道ネットワークを比べた結果を紹介する [9]. 図 8g は実際の関東圏の鉄道網. 図 8a–f は関東の形状に作った培地に粘菌が広がる様子を撮影した結果. 図 8g, h はシミュレーション結果. 実際の鉄道網と同様に利用者数が増えるに従って最終的なネットワーク形状が密になる.

10　まとめ

本稿では粘菌の作るネットワークの数理モデルを基に, さまざまな適応ネットワークに応用可能なネットワーク理論を提唱した. このように様々な分野・生物のネットワークを統一的に理解することができることこそが数学の利点ということができるだろう.

謝辞

本研究において実験データを提供してくださった共同研究者の中垣俊之氏（はこだて未来大学), 高木清二氏（北海道大学), 三枝徹氏（九州大学）ならびに数理モデルに関して相談に

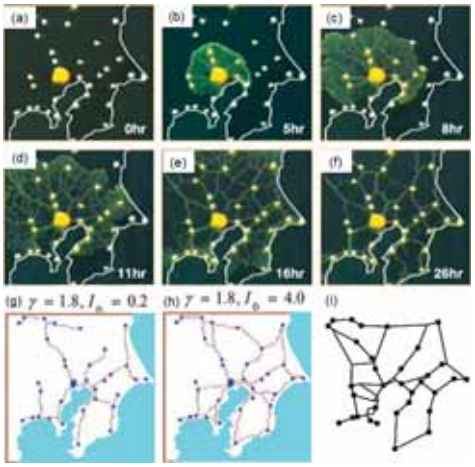


図 8：(a–f) 粘菌が提案する関東の鉄道網. (g, h) 数値計算結果. (i) 実際の関東の鉄道網.

のってくださった小林亮氏（広島大学）に感謝いたします.

参考文献

[1] L. E. Sieburth, Auxin Is Required for Leaf Vein Pattern in Arabidopsis, Plant Physiology, December 1999, Vol. 121, pp. 1179–1190

[2] T. Nakagaki, H. Yamada, A. Tóth, “Maze-solving by an amoeboid organism” Nature Vol. 407 (2000), 470

[3] A. Tero, R. Kobayashi, T. Nakagaki, A mathematical model for adaptive transport network in path finding by the true slime mold. J. Theor. Biol, ELSEVIER 244 (2007) 553–564

[4] A. Tero, R. Kobayashi, T. Nakagaki, Physarum solver: a biologically inspired method of road-network navigation, Physica A, ELSEVIER 363 (2006) 115–119 (2006)

[5] Tomoyuki Miyaji, Isamu Ohnishi, Physarum can solve the shortest path problem on riemannian surface mathematically rigorously. International Journal of Pure and Applied Mathematics. Volume 47 No. 3 2008, 353–369

[6] V. Bonifaci, K. Mehlhorn, G. Varma, Physarum can compute shortest paths. Journal of Theoretical Biology, 309 (2012), pp. 121–133

[7] T. Nakagaki, T. Saigusa, A. Tero, R. Kobayashi Effects of amount of food on path selection in the transport network of an amoeboid organism. Topological Aspects of Critical Systems and Networks, World Scientific 2007/07 p. 94–100

[8] A. Tero, K. Toyabe, K. Yumiki, R. Kobayashi, T. Nakagaki, A method inspired by Physarum for solving the Steiner problem. International Journal of Unconventional Computing. 6, 109–123, 2010

[9] A. Tero, S. Takagi, T. Saigusa, K. Ito, D. P. Bebber, M. D. Fricker, K. Yumiki, R. Kobayashi, T. Nakagaki, Rules for Biologically Inspired Adaptive Network Design. Science 2010/1/22 Vol. 327, No. 5964 P. 439–442

微分方程式に対するくりこみ群の方法

千葉　逸人
九州大学マス・フォア・インダストリ研究所

1　導入

自然科学における様々な現象は微分方程式を使ってモデル化されるため，微分方程式の解析は数学の研究としても応用上の観点からも非常に重要である．ところがよく知られているように，ほとんどの非線形微分方程式は具体的に解を書き下すことはできない．そこで，摂動論—近似解を構成すること—が重要になってくる．自然科学に現れる微分方程式の中には，性質がよく分かっている方程式の摂動として与えられる方程式が少なくない．例えば十分小さい摩擦のもとに運動する剛体の運動方程式は，摩擦のまったくない運動からのわずかな摂動だと思うことができる．もし摩擦のまったくない運動が解析可能でありその性質がよく分かっているなら，摩擦がある場合の運動も，摩擦が十分小さい限りにおいてはそれなりに解析可能であると期待できる．具体的にそのような解析手法を提供する理論を摂動論，あるいは摂動法と呼ぶ．

もう少し問題設定を明確にしよう．次のような n 次元の常微分方程式系を考えよう．

$$\frac{dx}{dt} = f(x) + \varepsilon g(t, x, \varepsilon), \quad x \in \mathbb{R}^n. \tag{1}$$

ここで $\varepsilon > 0$ は微小なパラメータであり，上の例では摩擦の大きさに相当している．ε が 0 のとき，すなわち摂動のない方程式 $dx/dt = f(x)$ が厳密に解けるという仮定のもと，式 (1) についての何らかの有効な情報を得るのが目標である．

ε が十分小さいのだから，解 $x(t)$ を ε についてのべき級数の形で求めようとするのは自然なアイデアだろう．すなわち，$x(t)$ が

$$x(t) = x_0(t) + \varepsilon x_1(t) + \varepsilon^2 x_2(t) + \cdots \tag{2}$$

のように展開できると仮定して，$x_0, x_1, \ldots$ を逐次求めていくのである．実際，このべき級数を与えられた方程式に代入すれば，$x_0, x_1, \ldots$ が満たすべき微分方程式が得られるから，それらを逐次解いていけば $x(t)$ を ε についてのべき級数として求めることができる．このようにして解を構成する方法を**素朴な摂動法**という．

ところがこの素朴な摂動法にはいくつかの欠点がある．もし全ての i に対して $x_i(t)$ を計算することができたなら，式 (2) は式 (1) の厳密解を与えるかもしれない．ところが $x_0, x_1, \ldots$ は逐次的に計算していくため，現実的には全ての（無限個の）x_i を計算することは不可能である．したがって我々はこの操作をどこか有限のところ，例えば m 次の部分で打ち切って，

$$\hat{x}(t) = x_0(t) + \varepsilon x_1(t) + \cdots + \varepsilon^m x_m(t) \tag{3}$$

という形の近似解で満足するほかない．ではこの式は，どれくらい厳密解をよく近似しているだろうか．打ち切った部分は ε^{m+1} くらいの大きさだから，ε が小さければ十分良い近似を与えていると期待するかもしれない．ところが次の簡単な例から分かるように，必ずしも厳密解の定性的な性質を捉えているとは言えないのである．

今，与えられた方程式の厳密解が $x(t) = \sin(\varepsilon t)$ で与えられるとしよう．このような問題に対して素朴な摂動法を用いると，

$$\hat{x}(t) = \varepsilon t - \frac{1}{3!}(\varepsilon t)^3 + \frac{1}{5!}(\varepsilon t)^5 + \cdots \tag{4}$$

のようなべき級数解を得るであろう．すなわち厳密解を ε で展開したものである．この級数を有限のところで打ち切ると，右辺は t についての多項式になってしまう．厳密解 $x(t) = \sin(\varepsilon t)$ は t について周期関数であるにもかかわず，打ち切り形は t について発散してしまうのである！周期運動は我々が正しく理解すべき最も基本的な現象であるから，それが捉えられないとなれば，素朴な摂動法は欠陥品であると言わざるを得ない．

このように，微分方程式に対して素朴な摂動法を用いると，方程式の厳密解の性質の如何にかかわらずに t についての多項式が現れることがしばしばある．この t についての多項式の項を**永年項**という．永年項は，素朴な摂動法で作った“近似解”の近似の精度を破綻させる．そのため，永年項をうまく処理して正しい近似解を構成するための理論が必要となる．そのような手法はこれまでに数多く提案されており，総称して**特異摂動法**と言うことが多い．本稿では，**くりこみ群の方法**と呼ばれる特異摂動法を紹介したい．これは Chen, Goldenfeld, Oono [2] によって 90 年代に提案された方法であり，Chiba [1] によってその数学的な正当化がなされた．くりこみ群の方法は，それまでに知られていた他の特異摂動法，たとえば多重尺度法，平均化法，中心多様体理論などを特別な場合として含んでおり，最も統一的で適用範囲の広い摂動法であると考えられる．また，常微分方程式だけでなく偏微分方程式にも適用可能であり，様々なタイプの方程式に対して形式的な計算だけで近似解を構成できる．本稿では，比較的簡単なクラスの常微分方程式に対してくりこみ群の方法を使った近似解の構成法を紹介しよう．

2　具体例

くりこみ群の方法を用いた近似解の構成法を，簡単な具体例を使って解説しよう．

例 2.1 次のような 2 階の微分方程式

$$\ddot{x} + x + \varepsilon x^3 = 0,\ \ x \in \mathbb{R} \tag{5}$$

を考える．ここでドット $(\dot{})$ は時間微分を表す．まずはこの方程式に対して素朴な摂動法を適用し，具体的に永年項を求めてみよう．そのため，$x(t) = x_0(t) + \varepsilon x_1(t) + O(\varepsilon^2)$ とおいて方程式に代入すると

$$\ddot{x}_0 + \varepsilon\ddot{x}_1 + x_0 + \varepsilon x_1 + \varepsilon(x_0 + \varepsilon x_1)^3 + O(\varepsilon^2) = 0$$

を得る．これを整理して，両辺で ε^0 の係数と ε^1 の係数を比較すると

$$\ddot{x}_0 + x_0 = 0, \tag{6}$$
$$\ddot{x}_1 + x_1 = -x_0^3 \tag{7}$$

という x_0 と x_1 についての微分方程式を得る．x_0 についての方程式はまさに式 (5) において $\varepsilon = 0$ とおいた方程式であり，非摂動系の方程式という．式 (6) は厳密に解けて，$A \in \mathbb{C}$ を初期条件から定まる任意定数として

$$x_0(t) = Ae^{it} + \overline{A}e^{-it} \tag{8}$$

が一般解である．この x_0 を式 (7) に代入すると

$$\ddot{x}_1 + x_1 = -(A^3e^{3it} + 3|A|^2Ae^{it} + 3|A|^2\overline{A}e^{-it} + \overline{A}^3e^{-3it})$$

を得る．これは非斉次形の線形方程式であるから厳密に解くことができて，解は

$$x_1(t) = \frac{A^3}{8}e^{3it} + \frac{3i}{2}|A|^2Ate^{it} + \text{c.c.} \tag{9}$$

で与えられることが分かる．ここで c.c. はそれより前の項の複素共役 (complex conjugate) を意味する．初項は t について周期的であるが，2 項目が t について発散する永年項である．この永年項のため，我々が構成した

$$x(t) = x_0(t) + \varepsilon x_1(t) = Ae^{it} + \varepsilon\left(\frac{A^3}{8}e^{3it} + \frac{3i}{2}|A|^2Ate^{it}\right) + \text{c.c.} \tag{10}$$

はもとの方程式の厳密解を正しく近似しない．そこで，ちょっとした細工を施してこの永年項を除去し，正しい近似解を構成しよう．ここからがくりこみ群の方法である．

まず，ダミーのパラメータ τ を導入し，式 (10) を形式的に

$$x(t;\tau) = Ae^{it} + \varepsilon\left(\frac{A^3}{8}e^{3it} + \frac{3i}{2}|A|^2A(t-\tau)e^{it}\right) + \varepsilon\frac{3i}{2}|A|^2A\tau e^{it} + \text{c.c.} \tag{11}$$

と書き直してみる．永年項 t を $t-\tau$ に置き換え，つじつま合わせのための項を最後に加えている．このつじつま合わせの項を，定数 A の中に“くりこんで”みる．すなわち，$A = A(\tau)$ は未定の τ の関数であり，上式は

$$x(t;\tau) = A(\tau)e^{it} + \varepsilon\left(\frac{A(\tau)^3}{8}e^{3it} + \frac{3i}{2}|A(\tau)|^2A(\tau)(t-\tau)e^{it}\right) + \text{c.c.} \tag{12}$$

と変形できると仮定しよう．$A(\tau)$ はどのような関数であろうか．厳密解 $x(t)$ は，我々が勝手に導入したダミーパラメータ τ に依存しないはずだから，$x(t;\tau)$ を τ で微分すると 0 にならなければならない．そこで

$$\left.\frac{dx}{d\tau}\right|_{\tau=t}(t;\tau) = 0 \tag{13}$$

という条件を課す．式 (12) に対して具体的にこれを計算してみると，

$$\frac{dA}{dt} = \varepsilon\frac{3i}{2}|A|^2A + O(\varepsilon^2)$$

という A についての微分方程式が得られる．これを**くりこみ群方程式**と呼ぶ．また，ε について高次の項を打ち切ったもの

$$\frac{dA}{dt} = \varepsilon\frac{3i}{2}|A|^2A \tag{14}$$

を**1 次のくりこみ群方程式**と呼ぼう．

この形式的な操作の背景は次のようなものである．t の多項式を含む永年項は $t \to \infty$ で発散して近似の精度を破綻させる．そこでパラメータ τ を導入して t を $t-\tau$ で置き換え，t が大きくなると τ も同時に大きくなると仮定する．すると $t-\tau$ は有界に留まってくれる．勝手に t を $t-\tau$ に置き換えたことに対するつじつま合わせとして，本来定数であった A は τ についての何かの関数だと見なされ，それはくりこみ群方程式を解くことで得られるのである．

式 (14) は a を任意定数として

$$A(t) = \frac{1}{2}a\exp i\left(\frac{3\varepsilon}{8}a^2t\right) \tag{15}$$

のように解くことができる．この $A(t)$ を式 (12) に代入し，$\tau = t$ とおけば，望むべき近似解を得る．すなわち

$$x(t) = \frac{1}{2}a\exp i\left(t+\frac{3\varepsilon}{8}a^2t\right) + \frac{\varepsilon}{8}\cdot\frac{1}{8}a^3\exp i\left(3t+\frac{9\varepsilon}{8}a^2t\right) + \text{c.c.} \tag{16}$$

が精度の良い近似解を与える．

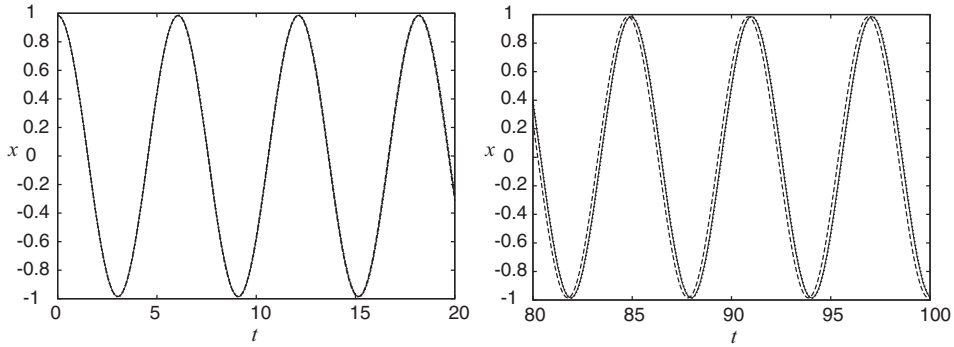


図 1 : 普通の線が式 (5) の厳密解，破線が 1 次のくりこみ群方程式を用いて構成した近似解 (16)，点線は（この記事では紹介しなかったが）2 次のくりこみ群方程式を用いて構成した近似解を表す．1 次の近似解も十分に良い近似解だが，2 次の近似解は厳密解とほとんど重なっていて区別がつかない．

3　問題設定

一般的な問題設定をして，それからくりこみ群の方法の主定理を述べよう．$\mathbb{R}^n$ 上の常微分方程式の摂動問題

$$\dot{x} = f(x) + \varepsilon g(t,x), \quad x \in \mathbb{R}^n \tag{17}$$

を考える．次のような仮定を設ける：

(A1) 非摂動系 $\dot{x} = f(x)$ について，初期条件 $x(0) = y$ を満たす解を $\varphi_t(y)$ と表すとき，$\varphi_t(y)$ は t についての周期関数である．

(A2) g は t について周期関数である．

応用上は，前節の例のように式 (17) は線形方程式の摂動であることが多い．すなわち，ある行列 F があって $f(x) = Fx$ と書ける問題である．このときは，$\varphi_t(y) = e^{Ft}y$ であり，仮定 (A1) は，行列 F の全ての固有値が虚軸上に存在することを意味する．これらの仮定は様々なやり方で弱めることができるが，本稿では簡単のためこのような仮定をおいた．より一般的な理論は [1] を参照されたい．

まず，式 (17) に対するくりこみ群方程式を導出しよう．そのために $x = x_0 + \varepsilon x_1 + \cdots$ と展開して代入すると，ε の 0 次と 1 次の部分からそれぞれ

$$\dot{x}_0 = f(x_0), \quad \dot{x}_1 = Df(x_0)x_1 + g(t,x_0)$$

という方程式を得る．ここで Df は f の Jacobi 行列である．前者の解を $x_0 = \varphi_t(y)$ と書く約束であった．これを x_1 の方程式に代入すると

$$\dot{x}_1 = Df(\varphi_t(y))x_1 + g(t,\varphi_t(y))$$

を得る．$f(x) = Fx$ の場合は単に $Df(\varphi_t(y))x_1 = Fx_1$ である．いずれにせよこれは x_1 について非斉次形の線形方程式なので，例えば定数変化法を用いるなどして具体的に解くことができて，解は

$$x_1 = D\varphi_t(y) \int (D\varphi_t(y))^{-1} g(t,\varphi_t(y))\, dt$$

で与えられることが分かる．ここで，周期性の仮定から，被積分関数は

$$(D\varphi_t(y))^{-1} g(t,\varphi_t(y)) = (\text{定数}) + (\text{周期関数})$$

のように，t について定数部分と周期的な部分から成ることに注意しよう．これを積分すると，定数部分の積分は t についての 1 次多項式となるが，周期的な部分は積分しても周期的である：

$$\int (D\varphi_t(y))^{-1} g(t,\varphi_t(y))\, dt = (\text{定数}) \cdot t + (\text{周期関数}).$$

よって，被積分関数の定数項から永年項が生じることが分かる．具体的にはこの定数項は

$$R_1(y) := \lim_{t\to\infty} \frac{1}{t} \int (D\varphi_t(y))^{-1} g(t,\varphi_t(y))\, dt$$

で与えられる．t で割って $t \to \infty$ とすれば周期的な部分は 0 に収束して，(定数) $\cdot\, t$ の係数だけが生き残ることが分かるだろう．これは y についての関数なので $R_1(y)$ とおいた．

x_1 から永年項を除いた部分を

$$h_t^{(1)}(y) = D\varphi_t(y) \int ((D\varphi_t(y))^{-1} g(t, \varphi_t(y)) - R_1(y))\, dt$$

とおく．以上より，1 次までの素朴な摂動解は

$$\begin{aligned} x(t) &= x_0 + \varepsilon x_1 \\ &= \varphi_t(y) + \varepsilon D\varphi_t(y) \int (D\varphi_t(y))^{-1} g(t, \varphi_t(y))\, dt \\ &= \varphi_t(y) + \varepsilon D\varphi_t(y) \int \left((D\varphi_t(y))^{-1} g(t, \varphi_t(y)) - R_1(y) + R_1(y) \right) dt \\ &= \varphi_t(y) + \varepsilon D\varphi_t(y) R_1(y) t + \varepsilon h_t^{(1)}(y) \end{aligned}$$

で与えられることが分かり，永年項を具体的に $D\varphi_t(y)R_1(y)t$ と書き下すことができた．

さて，くりこみ群の方法を用いて永年項を除去しよう．そのためにダミーパラメータ τ を導入し，多項式 t を $t - \tau$ に置き換える．そのつじつま合わせとして，本来定数であった y を τ についての未知の関数 $y = y(\tau)$ だと解釈する：

$$x(t;\tau) = \varphi_t(y(\tau)) + \varepsilon D\varphi_t(y(\tau)) R_1(y(\tau)) \cdot (t - \tau) + \varepsilon h_t^{(1)}(y(\tau)). \tag{18}$$

この式はダミー τ に依存しないはずだから，

$$\left. \frac{dx}{d\tau} \right|_{\tau=t} = 0$$

という条件を課す．合成関数の微分法に注意すると，式 (18) から

$$0 = \left. \frac{dx}{d\tau} \right|_{\tau=t} = D\varphi_t(y(t)) \frac{dy}{dt} - \varepsilon D\varphi_t(y(t)) R_1(y(t)) + \varepsilon D h_t^{(1)}(y(t)) \frac{dy}{dt}$$

を得る．これを dy/dt について整理すると

$$\frac{dy}{dt} = \varepsilon R_1(y(t)) + O(\varepsilon^2) \tag{19}$$

を得るので，2 次以上の項を打ち切ったもの

$$\frac{dy}{dt} = \varepsilon R_1(y) \tag{20}$$

が 1 次のくりこみ群方程式である．この解を $y(t)$ とし，式 (18) に代入して $\tau = t$ とおけば 1 次までの近似解

$$\hat{x}(t) = \varphi_t(y(t)) + \varepsilon h_t^{(1)}(y(t)) + O(\varepsilon^2) \tag{21}$$

を得る．以上の手続きは，より高次の近似解を構成するために逐次進めることができるが，本稿では 1 次までしか扱わない．

4　主定理

以上で近似解の計算法は分かったが，もちろん数学的には問題は山積みである．示さなければならないことは
(i) くりこみ群の方法で構成した近似解は，どれくらいの近似の精度になっていて，どれくらい長い時間有効なのか．
(ii) 周期軌道の存在のような，もとの方程式の定性的な性質について言えることはあるか．
(iii) くりこみ群方程式を解くことはもとの問題を解くことよりも簡単なのか．

(i) について調べることは当然必要なのだが，後で分かるように，くりこみ群の方法で構成した近似解は時刻 $t \sim O(1/\varepsilon)$ のタイムスケールまで有効である．ε が十分小さければこれは十分に長い時間となるのだが，一般には $t \to \infty$ まで正しい近似解は作れないことに注意しよう．(ii) について，応用上は単に近似の精度のみならず，周期解の存在のような定性的な性質も知ることが大事である．ところが，我々の構成した近似解は，いかに近似の精度がよくとも厳密解からわずかにずれているのだから，たとえ厳密解が周期解であっても，近似解は周期的でなく，したがって周期解の存在が予言できないかもしれない．(iii) について，近似解はくりこみ群方程式を解くことで得られるのだから，くりこみ群方程式がもとの方程式よりも簡単でなければ，くりこみ群の方法を適用する意味がない．以下でくりこみ群の方法に関する主定理のいくつかを紹介し，上記の問題が全て解決されることをみていく．以下ではくりこみ群方程式とは全て 1 次のくりこみ群方程式を意味するものとする．より高次のくりこみ群方程式について，および定理の証明については [1] を参照せよ．

定理 4.1（誤差評価）. $\hat{x}(t)$ をくりこみ群の方法を用いて構成した近似解（すなわち式 (21)），$x(t)$ を $x(0) = \hat{x}(0)$ を満たす (17) の厳密解とするとき，ある定数 $C, T > 0$ が存在して

$$\|x(t) - \hat{x}(t)\| < C\varepsilon$$

が時間区間 $0 \le t \le T/\varepsilon$ において成り立つ．

この意味において，くりこみ群の方法は確かに近似解を与えるのである．なお，m 次のくりこみ群方程式を用いた場合には右辺の誤差が $C\varepsilon^m$ になる．$t \to \infty$ では近似の精度が破綻することに注意しよう．ただし，次の定理の意味においては $t \to \infty$ の漸近挙動を記述できる場合もある．以下では説明の簡単のため，式 (17) において g が t に依存しない自励系の方程式のみを扱う．

定理 4.2（不変多様体の存在）. くりこみ群方程式 $\dot{y} = \varepsilon R_1(y)$ は法双曲型不変多様体 M を持つとせよ．このとき，もとの方程式 (17) も M と微分同相な不変多様体 M_ε を M の ε-近傍に持ち，それらの安定性は一致する．

法双曲型不変多様体とは，大雑把に言えば指数的に吸引，あるいは反発するような不変多様体のことを言うが，正確な定義は力学系理論の教科書を参照してほしい．応用上は M が安定な周期軌道の場合が重要であるが，この場合について定理を述べ直すとつぎのようになる．

定理 4.3（周期軌道の存在）. くりこみ群方程式 $\dot{y} = \varepsilon R_1(y)$ が漸近安定な周期軌道を持つとき，もとの方程式 (17) も漸近安定な周期軌道を持つ.

これらの定理は，くりこみ群方程式によりもとの方程式の定性的な性質を捉えることができることを意味する．特に漸近安定な不変多様体の近傍では $t \to \infty$ における解の挙動が分かることになる．次の定理でも簡単のため自励系（g が t に依存しない）について述べる.

定理 4.4（対称性）. (i) 方程式 (17) が Lie 群 H の作用で不変であるとき，くりこみ群方程式もまた H の作用で不変である.
(ii) くりこみ群方程式は f の流れ φ_t の作用で不変である．すなわち

$$R_1(\varphi_t(y)) = D\varphi_t(y)R_1(y)$$

が成り立つ.

この定理より，くりこみ群方程式はもとの方程式が持つ対称性よりも 1 つ多い対称性を持つことが分かる．すなわち，くりこみ群方程式はもとの方程式よりもより可積分系に近く，解析が容易なのである.

最後に，定理 4.3 の簡単な適用例を紹介して終わることにする.

例 4.5 次の方程式を考える.

$$\begin{cases} \dot{x} = y + \varepsilon(x - x^3) \\ \dot{y} = -x, \quad 0 < \varepsilon \ll 1. \end{cases} \tag{22}$$

例 2.1 と同様，これは摂動を受けた調和振動子である．途中の計算は省くが，くりこみ群方程式は

$$\dot{A} = \frac{\varepsilon}{2}(A - 3A|A|^2)$$

で与えられる．周期軌道の存在を示すために，この方程式をわざわざ解く必要はない．力学系理論の初歩的な知識から，これが漸近安定な周期解 $|A| = 1/\sqrt{3}$（半径 $1/\sqrt{3}$ の円）を持つことが簡単に分かる．したがって定理 4.3 より，方程式 (22) も，（半径）$= 1/\sqrt{3} + O(\varepsilon)$ の安定な周期解を持つことが分かる.

参考文献

[1] H. Chiba, Extension and unification of singular perturbation methods for ODEs based on the renormalization group method, SIAM j. on Appl. Dyn.Syst., Vol. 8, 1066–1115 (2009).

[2] L. Y. Chen, N. Goldenfeld, Y. Oono, Renormalization group and singular perturbations: Multiple scales, boundary layers, and reductive perturbation theory, Phys. Rev. E 54, (1996), 376–394 .

フェーズフィールド法による亀裂進展現象の数理モデリング

高石　武史*　　木村　正人†

*広島国際学院大学　情報デザイン学部
†九州大学マス・フォア・インダストリ研究所

1　亀裂進展現象とその数理モデル

物体内の亀裂やひびは，様々な分野において現れ，多様な観点からの研究がされている．例えば，微細な精密機器や部品から，車体や建物，巨大構造物に加え，地面や地殻など，様々な場所とスケールで発生し，材質に入った微小な亀裂の進展は，構造全体の破壊につながることから重要視されてきた．特に，亀裂の進展が引き起こす物体や構造物の破壊を防止するための破壊基準などが工学的な要請からも重要な問題とされ，亀裂を持つ弾性体の変形や，亀裂の進展防止や破壊制御に関する研究の多くは，偏微分方程式で記述された弾性体方程式を基礎に数学的な成果が挙げられ，歴史的に，亀裂問題において数学の果たして来た役割は少なくない．一例としては，応力拡大係数やJ積分によるエネルギー解放率の見積もりなどが挙げられる．

一方で，亀裂の経路予測や亀裂の時間発展現象を記述する閉じた形での偏微分方程式モデルについては，あまり研究が進んでおらず，数学的な解析の難しさの一因となっている．但し，破壊現象の数値シミュレーション自体は近年離散モデルを用いて多く試みられており，例えば，有限要素法による構造計算に亀裂先端の特異性を組み込んだ拡張有限要素法 (X-FEM, [17]) による亀裂進展モデルや，広い意味でのバネ・質点モデルである剛体バネモデル (RBSM, [11])，個別要素法 (DEM, [6, 18]) やその精密化である粒子離散化有限要素法 (PDS-FEM, [9, 10]) などが挙げられる．これらの手法についての比較などは，[23] を参照されたい．上記のモデルは，離散化された世界での亀裂進展モデルなので，数値シミュレーションには適している反面，数学的には未知の部分が多く残されている．

本稿では，筆者らによって最近提案された亀裂進展現象のフェーズフィールドモデルを紹介し，その考察を行う．このモデルは，閉じた偏微分方程式系で記述された連続モデルであり，亀裂進展現象の数学解析という観点から重要なアプローチではないかと考えている．またその数値シミュレーションにおいても，有限要素法や差分法などの既存の数値解析手法がそのまま適用できるという利点もある．

亀裂進展問題の数値計算において，現実的な数値計算を行うためにはいくつかの難点がある．一つ目は，破壊先端への応力集中により現れる特異性である．亀裂進展の古典的理論においては材質の変位 u の勾配が亀裂先端部で無限大になるために，数値的な扱いが難しくなる．二つ目は，亀裂の進展する方向の陽的な決定方法の欠如である．亀裂が進展する度に全ての方向への亀裂進展を評価した上で，一番エネルギーの小さい方向を選択することになると，評価する方向の選び方や数値計算上の負荷が問題になる．三つ目は，新たな亀裂の発生や亀裂の枝

分かれ（サブクラック）を数値的にどう扱うかである．エネルギーの評価のためには亀裂の発生場所を特定する必要があり，先端部以外からの亀裂の発生をすべてチェックするのは困難である．四つ目は，亀裂進展に伴って生じる新しい境界面に対する計算メッシュの切り直しの必要性である．亀裂面を境界として計算する場合には亀裂の進展とともに計算領域の形状が変化してしまう．そのため，新しい形状に合わせたメッシュを切り直して計算を再開する必要があり，数値計算上大きな負荷になる．これらの点を解決するために，前述のような様々な数値計算モデルが開発されているが，完全な決定版である数理モデルが確立されているとは言い難い．本稿で紹介するフェーズフィールドモデルでは，上記の難点が解決されている．

我々は，亀裂の位置を表現するフェーズフィールドを導入することによって，亀裂の進展方向の選択や，亀裂の進展に伴う新しい境界面の設定等の，数値計算上の難点を排した数理モデルを導出した [20, 21]．この数理モデルは板状弾性体のモード III（面外ずれ変形モード）における亀裂進展を時間発展方程式として記述するものである．このモデル方程式は Francfort-Marigo [7] によって提案された亀裂進展モデルに正則化されたエネルギーを用い，その勾配流としてモデルが導出される．類似の試みとして，Bourdin ら [3, 4] や Buliga [5] はこのエネルギーを最小化することによって亀裂進展現象の数値計算を行っている．

2 節ではこの時間発展方程式の導出とその性質について述べ，3 節ではこの方程式で亀裂進展現象が再現できることを実際の数値計算結果で示す．特に，二本の初期亀裂が先端位置の関係により，サブクラックを含む様々な亀裂へと進展していく様子を再現することができることを示し，このモデルが有用であることを検証する．

本研究の一部は JSPS 科研費 00268666 の助成を受けて実施されました．

2　モデルの導出とエネルギーの評価

板状物質の微小変位による亀裂の進展は，面内で亀裂に垂直方向の変位により割れていく場合（モード I），面内で亀裂に平行方向の変位により割れていく場合（モード II），面に垂直方向の変位により割れていく場合（モード III），及びそれらの混成モードに分類できる．ここでは，亀裂を含んだ平面が面に垂直方向の変位で割れていく（モード III）場合について扱うものとする．面に水平な方向に直交座標 $x = (x_1, x_2) \in \mathbb{R}^2$ をとり，面に垂直な方向に座標 x_3 をとる．板状物質は厚さ一定の等方弾性体として，区分的に滑らかな境界 Γ を持つ 2 次元領域 Ω がそれを表すものとする．

図 1 のように，領域 Ω 内の亀裂は曲線 $\Sigma \subset \Omega$ として表現できる．但し，Σ は Ω 内の端点を含む曲線とする．平板の変位が面に垂直な x_3 方向のみに限定されると仮定し，その x_3 方向の変位を $u(x) \in \mathbb{R}$, $x \in \Omega \setminus \Sigma$ と書く．

平板面にかかる垂直方向の外部負荷を $f(x)$ $(x \in \Omega)$，長さ正の境界 Γ_D で与えられた x_3 方向の変位を $g(x)$ とし，境界 $\Gamma_N = \Gamma \setminus \Gamma_D$ は自由端で，簡単のため外部からの荷重はかかっていないものとする．Γ_N で荷重がかかっている場合の取扱いについては，[21] を参照のこと．

亀裂の進展が非常にゆっくりであるとし，時刻 t を止める毎に力の釣り合いが成立すると仮定する．このとき，変位 u は次の外部力を含む弾性ポテンシャルエネルギーを最小にする

$v \in V(g, \Omega \setminus \Sigma) := \{v \in H^1(\Omega \setminus \Sigma);\ v = g \text{ on } \Gamma_D\}$ として与えられる．

$$E_1(v, \Sigma) = \frac{\mu}{2} \int_{\Omega \setminus \Sigma} |\nabla v|^2 \, dx - \int_\Omega fv \, dx \qquad (v \in V(g, \Omega \setminus \Sigma)),$$

ここで，$H^1(\Omega \setminus \Sigma)$ は $\Omega \setminus \Sigma$ 上の Sobolev 空間を表し，ある $\tilde{g} \in H^1(\Omega)$ があって，$g = \tilde{g}|_{\Gamma_D}$ であるものとする．パラメータ $\mu > 0$ は Lamé 定数のひとつである剛性率を表す．

変位 u は次の力の釣り合いの式を満たす．

$$\begin{cases} -\mu \Delta u = f & \text{in } \Omega \setminus \Sigma \\ u = g & \text{on } \Gamma_D \\ \dfrac{\partial u}{\partial n} = 0 & \text{on } \Gamma_N \\ \dfrac{\partial u^\pm}{\partial n} = 0 & \text{on } \Sigma^\pm, \end{cases} \tag{1}$$

$\frac{\partial}{\partial n}$ は，亀裂を除いた領域 $(\Omega \setminus \Sigma)$ の境界における外向き法線微分を表している．亀裂 Σ の両側をそれぞれ Σ^+, Σ^- と表し，各々の外向き法線微分を $\frac{\partial u^+}{\partial n}, \frac{\partial u^-}{\partial n}$ と書いた．

Griffith [8] は亀裂を含む物体のエネルギー収支に着目し，準静的なエネルギーバランスから，新たな亀裂面を作るために要するエネルギーと亀裂進展によって解放されるエネルギーの関係（Griffith の破壊規準）を導いた．

Griffith の理論をさらに発展させる形で，Francfort-Marigo [7] は次のようなエネルギーを提案した：

$$\begin{cases} E(\Sigma) = E_1(u, \Sigma) + E_2(\Sigma) \\ E_1(u, \Sigma) = \min\limits_{v \in V(g, \Omega \setminus \Sigma)} E_1(v, \Sigma) \qquad (u \in V(g, \Omega \setminus \Sigma)) \\ E_2(\Sigma) := \displaystyle\int_\Sigma \gamma(x) \, ds \end{cases} \tag{2}$$

ここで E_2 は破壊表面エネルギーを表し，$\gamma(x) > 0$ は $x \in \Omega$ において与えられた物質の破壊靭性値 (fracture toughness) である．[7] において，彼らはこのエネルギーを用いて亀裂進展の数理モデルを提案し，その詳細について調べた．

ここに現れた系の全エネルギー E を時間依存 Ginzburg-Landau (TDGL) 理論における自由エネルギーとして見ると，フェーズフィールドモデルの手法（[16] など）により，時間発展方程式が導かれる．

ここで，亀裂の形状を表現するにあたり，亀裂部分に引かれたラインマーカーのような役割を果たすものとして，フェーズフィールド $z(x, t)$ を導入する．この関数は $0 \le z \le 1$ を満たし，亀裂近傍では $z \approx 1$，それ以外の点では $z \approx 0$ となるように設定する．また，一度発生した亀裂は修復しないものとする．

さらに，破壊先端への応力集中により現れる特異性を解決するために空間正則化パラメータ $\epsilon > 0$ を導入し，亀裂の幅を $O(\epsilon)$ となるような平滑化を行う．Ambrosio-Tortorellio のアイデア [2] を利用し，次のような正則化された弾性エネルギー $\mathcal{E}_1(u, z)$ と亀裂表面エネルギー $\mathcal{E}_2(z)$

を用いる．

$$\begin{cases} \mathcal{E}(u,z) := \mathcal{E}_1(u,z) + \mathcal{E}_2(z) \\ \mathcal{E}_1(u,z) := \dfrac{\mu}{2}\displaystyle\int_\Omega (1-z)^2 |\nabla u|^2 \, dx - \int_\Omega fu \, dx \\ \mathcal{E}_2(z) := \dfrac{1}{2}\displaystyle\int_\Omega \gamma(x) \left(\epsilon |\nabla z|^2 + \frac{1}{\epsilon} z^2 \right) dx \end{cases} \tag{3}$$

$\epsilon \to 0$ とすることによってこのエネルギーは (2) に Γ-収束することが知られている [2].

ここでは，体積力 f や境界上の変位 g は非常にゆっくり変化するものとし，u と z は比較的短い時間で準平衡状態へと近づいていくものとする．TDGL 理論（及びフェーズフィールドモデルの手法）では，平衡状態に近い系のダイナミクスを自由エネルギーの勾配流によって記述している（例えば [16] など）．一般に，自由エネルギー $F(u)$ においてその勾配流は適当な時定数 α を用いて $\alpha \frac{\partial u}{\partial t} = -\frac{\delta F}{\delta u}$ と表される．ここで，$\frac{\delta F}{\delta u}$ は第 1 変分を表す．

今考えている系のエネルギー勾配を計算する．Γ_D 上で $u = g$，Γ_N 上で $\frac{\partial u}{\partial n} = 0$ とし，まず変数 u について (3) 式を元にエネルギーの第 1 変分をとる．任意の $\xi \in V(0,\Omega)$ に対し，

$$\left.\frac{d}{d\rho}\mathcal{E}(u+\rho\xi, z)\right|_{\rho=0} = \left.\frac{d}{d\rho}\mathcal{E}_1(u+\rho\xi, z)\right|_{\rho=0} = -\mu \int_\Omega \operatorname{div}\left((1-z)^2 \nabla u\right) \xi \, dx \tag{4}$$

が得られる．ここで，境界条件を用いて部分積分を行っている．これより，変位 u に関するエネルギーの勾配流は次のようになる．

$$\alpha_1 \frac{\partial u}{\partial t} = \mu \ \operatorname{div}\left((1-z)^2 \nabla u\right) + f \tag{5}$$

ここで，式 (1) における準静的仮定より $\alpha_1 = 0$ であるが，$\alpha_1 = 0$ の場合には $z = 1$ の場合に楕円型方程式が退化することがあり，より一般に，$0 < \alpha_1 \ll 1$ とすることによって数値計算上不都合が起きないようにすることができる．

同様に Γ 上で $\frac{\partial z}{\partial n} = 0$ とし，フェーズフィールド z に関するエネルギーの勾配流を考えると，

$$\left.\frac{d}{d\rho}\mathcal{E}_1(u, z+\rho\zeta)\right|_{\rho=0} = -\mu \int_\Omega (1-z)|\nabla u|^2 \zeta \, dx$$

$$\left.\frac{d}{d\rho}\mathcal{E}_2(z+\rho\zeta)\right|_{\rho=0} = -\int_\Omega \left\{ \epsilon \ \operatorname{div}\left(\gamma(x)\nabla z\right) - \frac{\gamma(x)}{\epsilon} z \right\} \zeta \, dx$$

より，適当な時定数 $\alpha_2 > 0$ を用いて，変位 z に関するエネルギーの勾配流は次の時間発展方程式で表される．

$$\alpha_2 \frac{\partial z}{\partial t} = \epsilon \ \operatorname{div}\left(\gamma(x)\nabla z\right) - \frac{\gamma(x)}{\epsilon} z + \mu |\nabla u|^2 (1-z) \tag{6}$$

ただし，このままでは一度入った亀裂が修復される可能性があるので，非修復の条件 $\frac{\partial z}{\partial t} \geq 0$ を満たすように，$\alpha_2 \frac{\partial z}{\partial t} = (\cdots)_+$ と変更する．ここで，$(a)_+ = \max(a, 0)$ である．

上記の内容をまとめると，(5) と (6) より，亀裂進展を記述する次のようなフェーズフィールド方程式が得られる:

$$
\begin{cases}
\alpha_1 \dfrac{\partial u}{\partial t} = \mu \operatorname{div}\left((1-z)^2 \nabla u\right) + f(x,t) & x \in \Omega,\ t > 0 \\
\alpha_2 \dfrac{\partial z}{\partial t} = \left(\epsilon \operatorname{div}\left(\gamma(x)\nabla z\right) - \dfrac{\gamma(x)}{\epsilon} z + \mu |\nabla u|^2 (1-z)\right)_+ & x \in \Omega,\ t > 0 \\
u = g(x,t) & x \in \Gamma_D,\ t > 0 \\
\dfrac{\partial u}{\partial n} = 0 & x \in \Gamma_N,\ t > 0 \\
\dfrac{\partial z}{\partial n} = 0 & x \in \Gamma,\ t > 0 \\
u(x,0) = u_0(x) & x \in \Omega\ (\alpha_1 = 0 \text{ の場合は不要}) \\
z(x,0) = z_0(x) \in [0,1] & x \in \Omega
\end{cases}
\tag{7}
$$

第 2 式では亀裂が修復しないための条件を課しているが，この様な形の時間発展方程式は通常，二重非線形発展方程式（[22] など）の枠組みで取り扱われる．最近，赤木・木村によって，$u_t = (\Delta u + f(x,t))_+$ の形の単独発展方程式について，離散勾配流の手法を用いて，解の一意存在などの数学的結果が得られている [1].

このモデルにおいてはもはや数値計算上困難になる点は無い．計算領域が固定されていることから，亀裂領域が表現できるようにメッシュサイズに留意すれば既存の数値計算手法を利用して亀裂進展現象を解析することができる．次節ではこのモデル方程式を用いて実際の数値計算を行い，亀裂進展現象が再現できることを示す.

3　数値計算結果

3.1　数値計算スキーム

ここで行った数値計算はアダプティブメッシュ有限要素法で行なっている．ここでは，アダプティブメッシュ有限要素法ライブラリ ALBERTA [19] を利用した反応拡散方程式系ソルバー [12, 13] を使用した．正則化パラメータ ε を導入しているものの，実際の数値計算では亀裂の両側での値のジャンプが大きいため，効率的に数値計算を行うためにアダプティブメッシュを用いた．数値計算法の詳細は [20] を参照のこと.

ここでは (7) を時間方向に陰的に離散化したものを，各時間ステップで P1 要素のアダプティブメッシュ FEM によって解き，時間刻みはアダプティブに可変とした [12, 13]．また，メッシュ再分割は z について評価して行っている.

以下では初期亀裂 $z_0(x)$ についていくつかの場合を計算した．実際の数値計算においては，亀裂が進展を始める時刻近くで最小メッシュサイズはほぼ下がりきり（図 4 の $t \sim 0.5$），その後メッシュ数が増大していく．メッシュ数は亀裂が反対側の境界まで届いた時刻近くでほぼ飽和している（図 4 の $t \sim 1.1$）．反応拡散方程式での場合 [12, 13] と同じように，メッシュサイズを調整しながら亀裂進展現象が計算できていることがわかる.

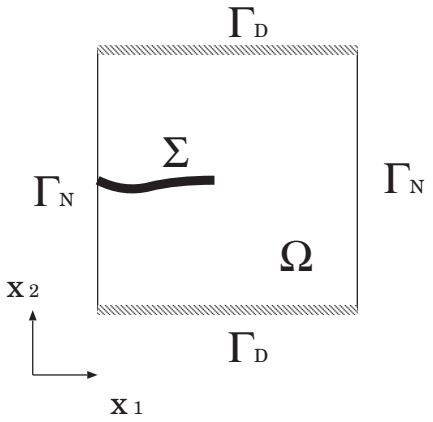


図 1：数値計算に用いた空間領域.

3.2　破壊靭性値が一様な場合

以下の数値計算では (7) においてパラメータを $\varepsilon = 10^{-3}$, $\alpha_1 = 0$, $\alpha_2 = 10^{-3}$, $\gamma = 0.5$ とし，計算領域は図 1 のように，$\Omega = (-1,1) \times (-1,1)$，ディリクレ境界として $\Gamma_D = \{(x_1, x_2) \mid x_1 \in (-1,1),\ x_2 = \pm 1\}$ を設定した．境界 Γ_D における変位 u は $g(x,t) = 10x_2 t$ $(x \in \Gamma_D,\ t \geq 0)$ として与えた.

まず，板の中央に 1 本の亀裂が入っている場合に亀裂が進展していく様子が再現できることを確認する．$\zeta_0(x) := e^{-(x_2/\delta)^2}(1 + e^{x_1/\delta})^{-1}$ $(\delta = 0.1)$ とおき，初期亀裂 $z_0(x)$ を $z_0(x) := \zeta_0(x_1 + 0.5, x_2)$ として与えると図 2 のように亀裂の進展が再現される．図の上段は変位 u の鳥瞰図，中段は変位 u の値の分布を最大値と最小値で正規化し濃淡で表している．時間とともに亀裂が進展していき，最終的に破断している様子が見える．図の下段はフェーズフィールド z の値の分布を，$z = 0$ が黒，$z = 1$ が白となるように濃淡で表しており，時刻の進展とともに亀裂領域（$z \approx 1$：白い部分）が伸びていく様子を示している．参考のためにどの図も右端にグレースケールを表示させている.

ここでは $t \sim 0.5$ から亀裂が伸び初め，$t \sim 1.1$ で反対側の境界まで届いている．この計算においてアダプティブメッシュがどのように働いているかを示したのが図 3 と図 4 で，最小メッシュサイズ $h \sim 0.003$ くらいで数値計算可能であることがわかる.

このモデルでは，準静的な条件下でのエネルギーの減少により亀裂が進展することが仮定されている．従って，数値計算で正しく亀裂進展現象がとらえられているかどうかはそのエネルギーの時間発展を調べることで，ある程度検証可能である．今度は，$t = 0$ で亀裂を与え，境界条件を固定して計算を行なった．ここでは，境界 Γ_D における変位 u は $g(x,t) = 5x_2$ $(x \in \Gamma_D,\ t \geq 0)$ として与え，$t = 0$ で板の中央に 1 本の亀裂が入っているとした.

やはり，時間とともに亀裂が進展していくのだが，境界条件を固定しているためそのスピードは次第に遅くなっていく．この亀裂進展の数値計算結果において各時刻のエネルギーを計算すると，亀裂の進展共に弾性エネルギー $\mathcal{E}_1$ は減少，亀裂表面エネルギー $\mathcal{E}_2$ は増加しているが，系全体のエネルギー $\mathcal{E} = \mathcal{E}_1 + \mathcal{E}_2$ は少しづつ減少していることが確認できる（図 5）．ま

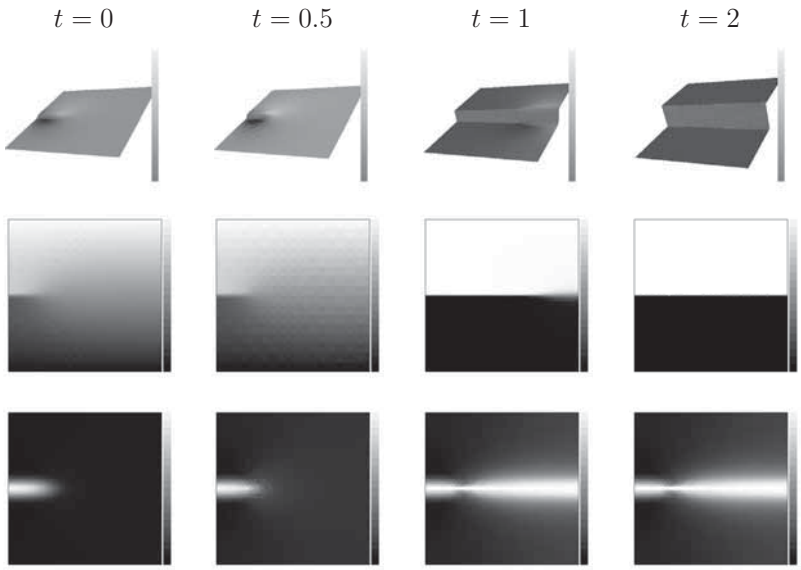


図 2 : u の鳥瞰図（上），u（中）および z（下）の値．1 本の亀裂が進展するようす．変位の大きさを明度で表している．左から右にむかって時間が進み、最後は破断している．

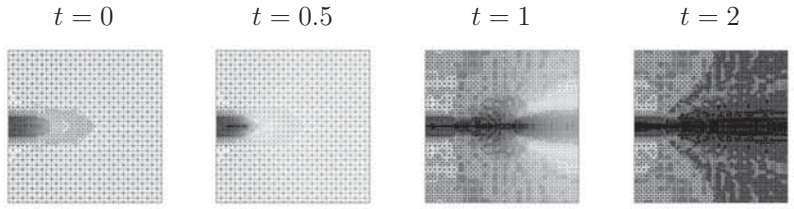


図 3 : 亀裂進展シミュレーションにおけるアダプティブメッシュ有限要素法の様子

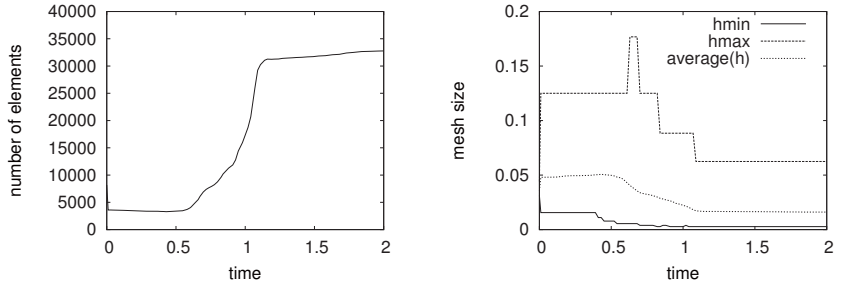


図 4 : アダプティブ有限要素法における要素数（左）とメッシュサイズ（右）の時間発展

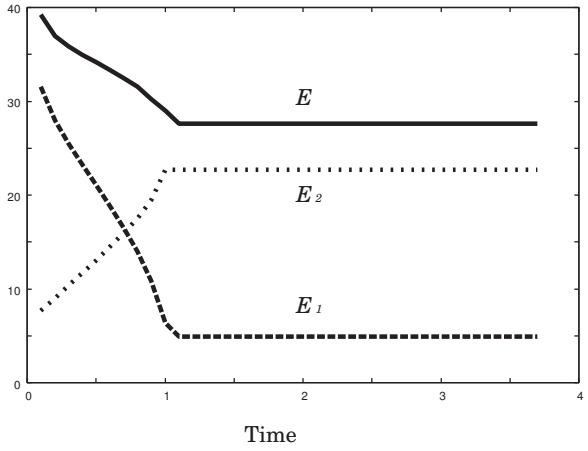


図 5：エネルギー $\mathcal{E}$, $\mathcal{E}_1$, $\mathcal{E}_2$ の時間発展.

た，ここで得られたエネルギーの時間変化を元に，亀裂によるエネルギー解放率などを計算することができる.

3.3　破壊靭性値が空間分布を持つ場合

次に，破壊靭性値が空間分布を持つ場合について，境界上の変位を時間とともに変化させることで亀裂がどのように進んでいくかを調べた．モード III 亀裂進展のフェーズフィールドモデル (7) において境界 Γ_D における変位 u を $g(x,t) = 10x_2t$ $(x \in \Gamma_D, t \geq 0)$ とし，破壊靭性値としてストライプパターン $\gamma(x) = 0.5(1 + 0.2\cos 10(x + y))$ を与えた．亀裂は破壊靭性値の小さいところを通って，枝分かれしつつ進展する様子が見て取れる（図 6）.

4　まとめ

亀裂進展現象は実験的には再現性の難しいものであり，それを数値計算で再現するためにも多くの困難がある．解決法として多くの手法が開発されているが，その結果亀裂進展の数値計算には特別な計算手法が必要と考えられている．本論文ではフェーズフィールドを用いた PDE モデルを導出することにより，方程式から現象の理解を深めることが可能になったばかりでなく，X-FEM などの特別な数値計算手法を用いずに計算機シミュレーションを行うことが可能である.

今回，モデルの導出に用いた手法は非常に明解なものであるため，モード III 亀裂進展のみならず，モード I, II を含む平板内の 2 次元弾性体や，全てのモードを含む 3 次元弾性体モデルへの拡張も可能である．また，バネ質点系を用いた離散弾性体モデルにおける破壊現象の同様のフェーズフィールドモデル構築の試みも行われている．これらの最近の拡張・進展については [15] および [14] を参照されたい.

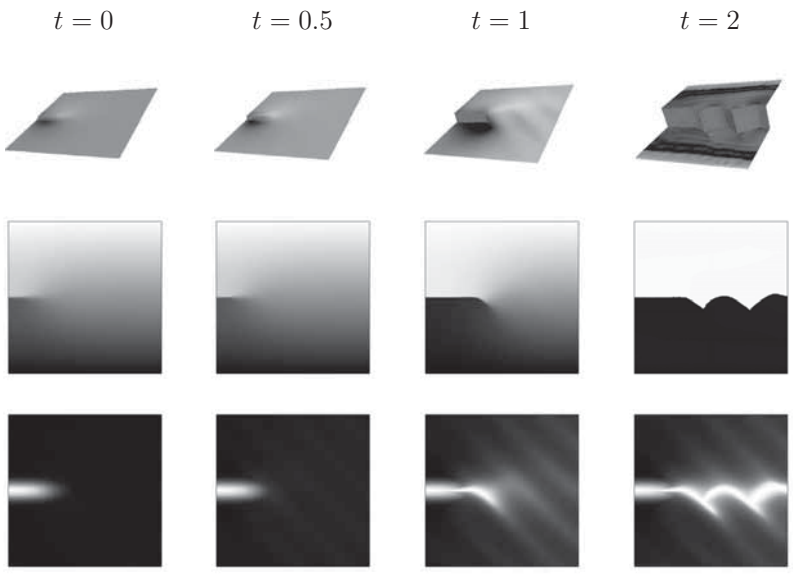


図 6 : $\gamma(x) = 0.5(1 + 0.2\cos 10(x + y))$ の場合の u の鳥瞰図（上），u（中）および z（下）の値の時間変化.

参考文献

[1] G. Akagi and M. Kimura, Existence and uniqueness of solutions to irreversible diffusion equations.（仮題，準備中）

[2] L. Ambrosio and V. M. Tortorelli, On the approximation of free discontinuity problems, Boll. Un. Mat. Ital. (7) 6-B, (1992) 105–123.

[3] B. Bourdin, Numerical implementation of the variational formulation of brittle fracture. Interfaces Free Bound., **9** (2007), 411–430.

[4] B. Bourdin, G. A. Francfort and J.-J. Marigo, Numerical experiments in revisited brittle fracture. J. Mech. Phys. Solids, **48** No. 4, (2000), 797–826.

[5] M. Buliga, Energy minimizing brittle crack propagation. J. Elasticity, **52** No. 3 (1998/99), 201–238.

[6] P. A. Cundall, A computer model for simulating progressive large scale movements in blocky rock systems, in: Proceedings of the Symposium of the International Society for Rock Mechanics, Nancy, **2** (1971), 129–136.

[7] G. A. Francfort and J.-J. Marigo, Revisiting brittle fracture as an energy minimization problem. J. Mech. Phys. Solids, **46** (1998), 1319–1342.

[8] A. A. Griffith, The phenomenon of rupture and flow in solids. Phil. Trans. Royal Soc. London, **A221** (1920), 163–198.

[9] M. Hori, K. Oguni and H. Sakaguchi, Proposal of FEM implemented with particle discretization for analysis of failure phenomena, J. Mech. Phys. Solids, **53** (2005), 681–703.

[10] T. Ichimura, M. Hori and M. L. L. Wijerathne, Linear finite elements with orthogonal discontinuous basis functions for explicit earthquake ground motion modeling, Int. J. Numer. Meth. Engng **86** (2011), 286–300.

[11] T. Kawai, New discrete models and their application to seismic response analysis, Nuclear Engineering and Design **48** (1978), 207-229.

[12] M. Kimura, H. Komura, M. Mimura, H. Miyoshi, T. Takaishi, and D. Ueyama, Adaptive mesh finite element method for pattern dynamics in reaction-diffusion systems. in: Proc. of the Czech-Japanese Seminar in Applied Mathematics 2005, COE Lecture Note Vol.3, Faculty of Mathematics, Kyushu University ISSN1881-4042 (2006), 56–68.

[13] M. Kimura, H. Komura, M. Mimura, H. Miyoshi, T. Takaishi, and D. Ueyama, Quantitative study of adaptive mesh FEM with localization index of pattern, in: Proc. of the Czech-Japanese Seminar in Applied Mathematics 2006, COE Lecture Note Vol. 6, Faculty of Mathematics, Kyushu University ISSN1881-4042 (2007), 114–136.

[14] M. Kimura and H. Notsu, Energy consistent fracture model on symmetric spring-block system. (preprint)

[15] M. Kimura and T. Takaishi, Phase field models for crack propagation. Theoretical and Applied Mechanics Japan, Vol. 59 (2011) pp. 85–90.

[16] R. Kobayashi, Modeling and numerical simulations of dendritic crystal growth. Physica D, **63** (1993), 410–423.

[17] N. Moës, J. Dolbow and T. Belytschko, A finite element method for crack growth without remeshing. Int. J. Numer. Meth. Engng **46** (1999), 131–150.

[18] A. Munjiza, The Combined Finite-Discrete Element Method, Wiley, 2004.

[19] A. Schmidt and K. G. Siebert, Design of Adaptive Finite Element Software. The Finite Element Toolbox ALBERTA, Lecture Notes in Computational Science and Engineering, 42. Springer-Verlag, Berlin, 2005.

[20] 高石武史: モード III 亀裂進展のフェーズフィールドモデルとその数値計算, 日本応用数理学会 論文誌 **19** (2009), 351–369.

[21] T. Takaishi and M. Kimura, Phase field model for mode III crack growth, Kybernetika **45** (2009), 605–614.

[22] A. Visintin, *Models of phase transitions.* Birkhauser (1996).

[23] M. L. L. Wijerathne, K. Oguni and M. Hori, Numerical analysis of growing crack problems using particle discretization scheme, Int. J. Numer. Meth. Engng **80** (2009), 46–73.

有限要素法による数値解析

田上　大助

九州大学マス・フォア・インダストリ研究所

1　はじめに

計算機を用いた数値シミュレーションによって, 水の流れや熱の伝達など自然界や産業界で見られる様々な現象を理解する試みは盛んに行われている; 例えば図 1 は, あるガラス溶融炉の温度分布の数値シミュレーションの様子である [10]. これら様々な現象理解の試みと, 近年

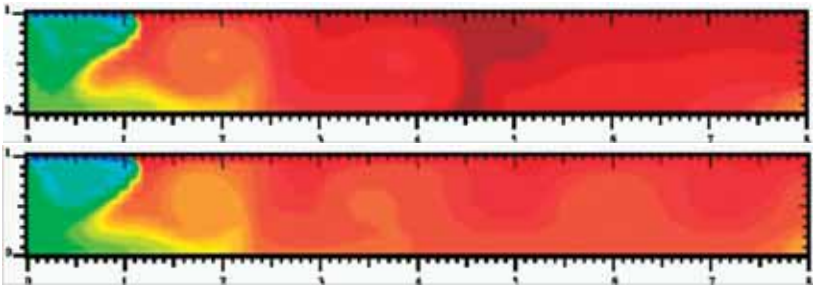


図 1: 有限要素法を用いた溶融炉の温度分布の数値シミュレーション例. 炉内部の電流の有無によって温度分布が異なっている様子を表している.

の計算機環境の目覚ましい発展を受け, 数値シミュレーションは理論, 実験に続く, 現象理解のための第三の手段として広く認知されている.

数値シミュレーションでは, まず現象を物理法則に基づいて微分方程式で記述する**数理モデル化**を行い, 次に微分方程式を計算機で扱うことのできる近似方程式に置き換える**離散化**を行い, 最後に近似方程式の解法を計算機に実装し目的とする現象を再現する**数値計算**を行う. 数値計算によって得られる近似的な現象の振る舞いが, 実際の現象をどの程度再現出来ているかを検討することは重要である. 例えば, 与えられた速度で波が伝搬する様子を数値シミュレーションした場合, 離散化の手法によっては, 必要となる離散化パラメータの選択を誤ると波の伝搬を正しく再現出来ずに近似解が振動することが良く知られている; 次頁の図 2 参照.

ここでは, **有限要素法 (Finite Element Method; FEM)** を用いた時間変化の無い定常状態における温度分布の数値シミュレーションを取り上げ, 離散化の方法を解説し, 近似方程式の信頼性評価に数学の力が役立つ例を見ることにする.

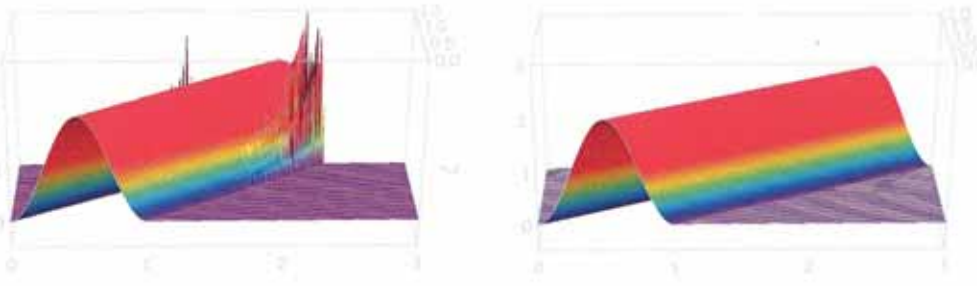


図 2: 前進差分法を用いた波の伝搬の数値シミュレーションの様子. 左図では離散化パラメータの選択を誤っているため, 本来は起こり得ない振動が生じていることが分かる.

2 Poisson 方程式

話を簡単にするために, 温度分布を考える領域 Ω が図 3 に示すような 2 次元凸多角形であり, 多角形 Ω の境界を成すそれぞれの辺が $\Gamma_0 \neq \emptyset$, $\Gamma_0 \cap \Gamma_1 = \emptyset$ を満たす 2 つの部分境界 Γ_0, Γ_1 のいずれかに含まれる場合を考えよう. また Γ_1 に含まれる辺上の外向き単位法線を $\boldsymbol{n}$ とする. ここで, 領域 Ω における場の温度を u, 領域 Ω で与えられる外部熱源を f, 境界 Γ_0 で与えられる境界温度を g とする. 場の温度 u が時間に依存しない定常状態に達した時, 次の Poisson 方程式と呼ばれる偏微分方程式を満たしていると考えることができる:

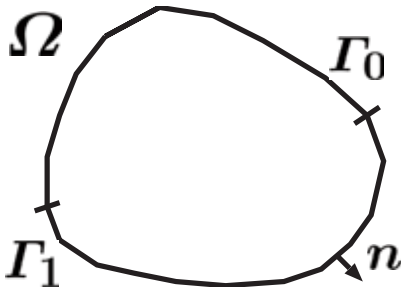


図 3: 2 次元の場合の領域 Ω の例.

$$\begin{cases} -\Delta u = f & (\boldsymbol{x} \in \Omega), \quad (1a) \\ u = g & (\boldsymbol{x} \in \Gamma_0), \quad (1b) \\ \dfrac{\partial u}{\partial n} = 0 & (\boldsymbol{x} \in \Gamma_1). \quad (1c) \end{cases}$$

式 (1a), (1b), および (1c) は, 熱量保存から導かれる場の支配方程式, 温度指定の境界条件, および断熱の境界条件をそれぞれ表わしている. 定常状態に達するまでを含めた温度分布を定める方程式の取扱いについては, 例えばスタンリー・ファーロウ [6] などが良い入門書である.

次に, 方程式 (1) に対する弱形式を構成するために必要な関数空間を準備する. $L^2(\Omega)$ を Ω 上で定義された 2 乗可積分な実数値関数からなる関数空間, 自然数 k に対して $H^k(\Omega)$ を Ω 上で定義された k 階微分までが $L^2(\Omega)$ である実数値関数からなる関数空間とする. また $\|.\|_{H^k(\Omega)}$ および $\|.\|_{L^2(\Omega)}$ で, $H^k(\Omega)$ および $L^2(\Omega)$ のノルムを, $|.|_{H^k(\Omega)}$ で $H^k(\Omega)$ のセミノルムをそれぞれ表わす. 以下では関数 g に対して, $\widetilde{g} \in H^1(\Omega)$ かつ $\widetilde{g} = g$ $(x \in \Gamma_0)$ を満たす領域 Ω への拡張 $\widetilde{g}$ が存在すると仮定する. この時, V を "Γ_0 上の境界値が 0 に等しい" 関数全体, $V(g)$ を

“Γ_0 上の境界値が g に等しい” 関数全体を表すとする:

$$V := \{v \in H^1(\Omega);\ v = 0,\ x \in \Gamma_0\}, \tag{2}$$

$$V(g) := \{v \in H^1(\Omega);\ v = g,\ x \in \Gamma_0\} \quad (= V + g). \tag{3}$$

この時, 方程式 (1) に対応する式

$$\int_\Omega \nabla u \cdot \nabla v\, dx = \int_\Omega f v\, dx \qquad (\forall v \in V) \tag{4}$$

を満たす $u \in V(g)$ を求める方程式を考えることができる. 方程式 (1) では 2 階微分が必要となるのに対して, 式 (4) では微分の階数が一つ弱い 1 階微分が必要となる. このことから, 式 (4) を**弱形式**, その解を**弱解**と呼ぶ. 方程式 (1) と弱形式 (4) は, 解が十分に滑らかな場合には同値である.

定理 2.1 $u \in H^2(\Omega)$ が方程式 (1) の解ならば $u \in H^2(\Omega)$ は弱形式 (4) の解でもある. また逆も成り立つ.

また方程式 (1) で課された境界条件のうち, (1b) は弱形式 (4) において解を探す空間の中で明示する必要がある. 一方で, (1c) は弱形式 (4) では陽に現われずに方程式そのものに自然に取り込まれている. このことから (1b) を**本質境界条件**, (1c) を**自然境界条件**と呼ぶ.

このように, 着目する現象を定める方程式を弱形式の形で表わすことが, 有限要素法を用いた数値シミュレーションの第一歩となる.

3 有限要素法

前節で考えた弱形式 (4) で用いる V を適当な有限次元部分空間で置き換え, その中から解を探すことが有限要素法の基本的な発想である. まず最初に, 有限次元部分空間を構成するための準備をしよう. 図 4 に示すように, 領域 Ω に対して N_E 個の閉 3 角形 K_j $(j = 1, \ldots, N_E)$ からなる 3 角形分割 $\mathscr{T}_h$ を考える:

$$\mathscr{T}_h := \{K_j;\ j = 1, \ldots, N_E\}.$$

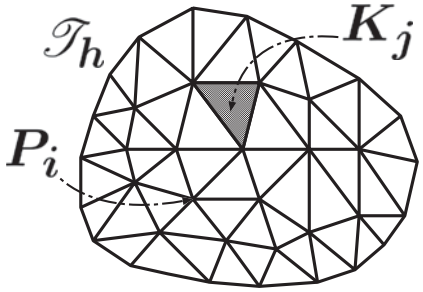


図 4: 3 角形分割 $\mathscr{T}_h$ の例

ここで h は離散化パラメータと呼ばれる正定数で, 分割を成す閉 3 角形の辺長の最大値とする. また K_j を構成する N_P 個の頂点全体を $\mathscr{N}_h := \{P_i;\ i = 1, \ldots, N_P\}$ とする. それぞれの 3 角形 K_j を要素, 頂点 P_i を節点とも呼ぶ. 3 角形分割は, 以下の条件を満足する必要がある:

(a) 3 角形分割 $\mathscr{T}_h$ が領域 Ω を再現出来なければならない:

$$\bigcup_{j=1}^{N_E} K_j = \overline{\Omega}. \tag{5}$$

(b) 異なる 3 角形 (の内点集合) は重ならない:

$$\operatorname{int} K_i \cap \operatorname{int} K_j = \emptyset \quad (i, j = 1, \ldots, N_E,\ i \neq j). \tag{6}$$

(c) 異なる 3 角形の共通部分は, 辺全体か, 頂点か, 空集合か, のいずれかである.
(d) 3 角形と境界との共通部分は, Γ_0 のみに含まれるか, Γ_1 のみに含まれるか, 空集合か, のいずれかである.

図 5 に, それぞれの条件で許容されない 3 角形分割の例を示している. 式 (5) は領域 Ω が多角

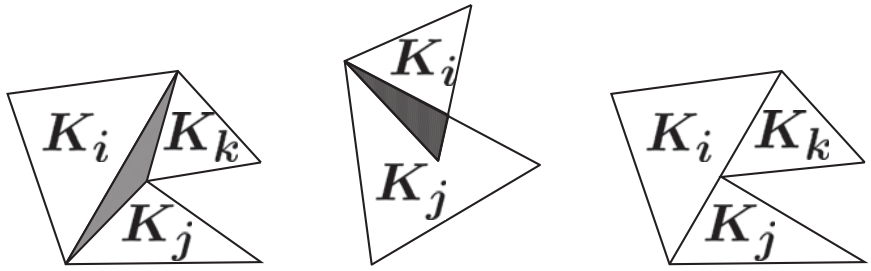


図 5: 許容されない 3 角形分割の例. 左から (a) 3 角形の間に隙間があり考える領域を埋め尽くせていない; (b) 3 角形が重なっている; (c) 3 角形の辺上に他の 3 角形の頂点がある.

形でない場合, 例えばより一般の滑らかな境界を持つ領域の場合にはもはや成り立たない. しかし多角形でないより一般の領域の場合でも, 例えば領域 Ω を多角形で近似した領域 Ω_h を用いることで有限要素法を構成することができ, その数学的正当化も行われている. そこでここでは話を簡単にするために, 最初から考える領域が多角形であると仮定している.

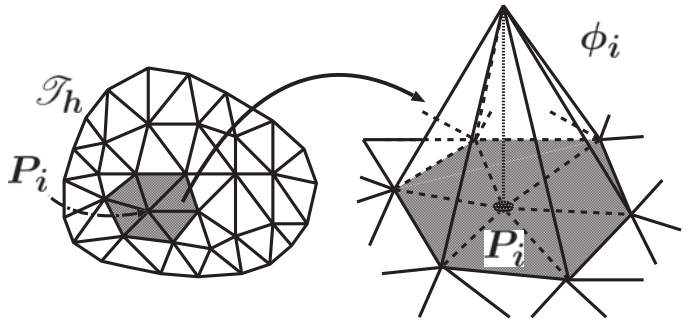


図 6: 頂点 P_i に対応する区分的 1 次多項式を用いた基底関数 ϕ_i.

次に, 図 6 に示すような 3 角形の頂点 P_i に関連付けた区分的 1 次多項式 ϕ_i で

$$\phi_i(P_j) = \delta_{ij}, \quad \phi_i|_{K_k} \in \mathscr{P}_1(K_k) \qquad (i, j = 1, \ldots, N_P,\ k = 1, \ldots, N_E) \tag{7}$$

を満たす関数を考える．ここに $\mathscr{P}_1(K_k)$ は K_k 上で高々 1 次の多項式全体を表わす．この時，$\{\phi_i;\ i=1,\ldots,N_P\}$ によって張られる有限次元空間

$$X_h := \{v_h \in \mathscr{C}^0(\overline{\Omega});\ v_h|_{K_j} \in \mathscr{P}_1(K_j),\ j=1,\ldots,N_E\} = \langle \phi_1,\ldots,\phi_{N_P}\rangle \tag{8}$$

を考える．これは $H^1(\Omega)$ を近似する有限次元の空間 (**有限要素空間**) である．有限次元空間 X_h は，3 角形分割上で区分的 1 次多項式を利用していることから $\boldsymbol{P_1}$ **要素**と呼ぶ．

以下では境界温度 g が Γ_0 上で連続であると仮定する．この時，V_h, $V_h(g)$ を近似する有限次元の空間を

$$V_h := \{v_h \in X_h;\ v_h|_{\Gamma_0} = 0\}, \tag{9}$$

$$V_h(g) := \{v_h \in X_h;\ v_h(P) = g(P),\ \forall P \in \mathscr{N}_h \cap \Gamma_0\} \tag{10}$$

とし，弱形式 (4) に対して，

$$\int_\Omega \nabla u_h \cdot \nabla v_h\, dx = \int_\Omega f v_h\, dx \qquad (\forall v_h \in V_h) \tag{11}$$

を満たす $u_h \in V_h(g)$ を求める方程式を考える．方程式 (11) は，設定した有限要素空間 (ここでは P_1 要素) から近似解を探すことから，**有限要素方程式**，**有限要素問題**などと呼ばれる．

さらに，有限要素方程式 (11) から実際の数値シミュレーションで用いる連立 1 次方程式を導出しよう．今，$\mathscr{N}_h$ の番号付けを並べ替えて

$$\{P_i;\ i=1,\ldots,N\} = \mathscr{N}_h \cap \big(\Omega \cup (\Gamma_1 \backslash \overline{\Gamma}_0)\big) \qquad \text{(内点, 自然境界条件を課す頂点)},$$

$$\{P_i;\ i=N+1,\ldots,N_P\} = \mathscr{N}_h \cap \Gamma_0 \qquad \text{(本質境界条件を課す頂点)}$$

とする．ここで Γ_0 と Γ_1 の境界にある多角形の頂点は後者に含むことに注意する．この時，$\{\phi_i;\ i=1,\ldots,N\}$ が V_h の基底で，$\dim V_h = N$ となる．したがって V_h, $V_h(g)$ は，

$$V_h := \{v_h \in X_h;\ v_h|_{\Gamma_0} = 0\} = \langle \phi_1,\ldots,\phi_N\rangle, \tag{12}$$

$$V_h(g) := \left\{u_h \in X_h;\ u_h = \sum_{j=1}^{N} u_j\phi_j + \sum_{j=N+1}^{N_p} g(P_j)\phi_j\right\} \tag{13}$$

と表わすこともできる．ただし $u_j = u_h(P_j)$ $(j=1,\ldots,N)$ である．線形性から有限要素方程式 (11) は

$$\int_\Omega \nabla u_h \cdot \nabla \phi_i\, dx = \int_\Omega f\phi_i\, dx \qquad (i=1,\ldots,N) \tag{14}$$

と同値である．有限要素方程式 (11), (14) において解を探す空間は $V_h(g)$ であるから，有限要素解は

$$u_h = \sum_{j=1}^{N_p} u_h(P_j)\phi_j = \sum_{j=1}^{N} u_j\phi_j + \sum_{j=N+1}^{N_p} g(P_j)\phi_j \tag{15}$$

と表わすことができる. これを弱形式 (14) に代入すると

$$\mathbf{A}\mathbf{u} = \mathbf{b} \tag{16}$$

と連立 1 次方程式が導かれる. ただし

$$\begin{aligned}
&\mathbf{A} = (a_{ij}) : \ n \text{ 次元正方行列},\\
&\mathbf{u} = (u_1, \ldots, u_N)^T, \quad \mathbf{b} = (b_1, \ldots, b_N)^T : \ n \text{ 次元列ベクトル},\\
&a_{ij} = \int_\Omega \nabla\phi_j \cdot \nabla\phi_i \, dx \qquad (i, j = 1, \ldots, N),\\
&b_i = \int_\Omega f\phi_i \, dx - \sum_{j=N+1}^{N_p} g(P_j) \int_\Omega \nabla\phi_j \cdot \nabla\phi_i \, dx \qquad (i = 1, \ldots, N)
\end{aligned}$$

である.

実際の数値シミュレーションでは, 連立 1 次方程式 (16) を計算機上で解くことで得られる $\mathbf{u}$ を式 (15) に代入することで, 近似解 u_h を構成する. 連立 1 次方程式を計算機上で解くための解法には様々なものがある. 例えば藤野–張 [2], 杉原–室田 [7] などに詳しい. また計算機上での様々な効率を考慮した連立 1 次方程式を解くためのライブラリーが多く開発されている. 実際に数値シミュレーションを行う際には, これらのライブラリーを利用して得られた連立 1 次方程式を解くことが多い. 例えば直接解法のライブラリである SuperLU [8], 反復解法のライブラリである LIS [5] をはじめ, 他にも多くのライブラリが開発されている.

4 抽象的変分問題と誤差評価

前節までで, 定常状態にある温度分布を有限要素法によって数値シミュレーションする手順の概略を述べた. 本節では, 連立 1 次方程式 (16) を解くことで得られた有限要素解 (15) が元の Poisson 方程式 (4) の解を “どの程度近似できているか” を数学的に評価する手法について触れる. ここでは頁数の関係から評価手法の概略のみに触れる. 例えば Ciarlet [1], Girault–Raviart [3], 菊地 [4], 田端 [9] などの文献から, 有限要素法の数学的な評価についてより深い議論を知ることができる.

4.1 抽象的変分問題

以下 V を実 Hilbert 空間とし, $\|\,.\,\|_V$ をそのノルムとする. また V' を V に対応する双対空間とする.

定義 4.1 (双 1 次形式, 強圧性) 写像 $a\colon V \times V \to \mathbb{R}$ が各成分について線形の時, $V \times V$ 上の双 1 次形式であるという. また, ある正定数 α が存在して

$$\alpha\|v\|_V^2 \le a(v, v) \qquad (\forall v \in V) \tag{17}$$

が満たされる時, 双 1 次形式 a は強圧的であるという.

補題 4.2 $V \times V$ 上の双 1 次形式 a が直積空間 $V \times V$ から $\mathbb{R}$ への連続写像であることと, ある正定数 a_0 が存在して

$$|a(u,v)| \leq a_0 \|u\|_V \|v\|_V \qquad (\forall u, v \in V) \tag{18}$$

が成り立つことは同値である.

定理 4.3 (Lax–Milgram の定理) a を $V \times V$ 上の連続かつ強圧的な双 1 次形式とする. その時, 任意の $\ell \in V'$ に対し

$$a(u,v) = \ell(v) \qquad (\forall v \in V) \tag{19}$$

を満たす $u \in V$ は一意に存在する. 更に, この ℓ から u への対応は V' から V への同型写像であり,

$$\|u\|_V \leq \frac{1}{\alpha} \|\ell\|_{V'}. \tag{20}$$

が成り立つ.

V_h を V の閉部分空間とする. 式 (19) で V を V_h で置き換え,

$$a(u_h, v_h) = \ell(v_h) \qquad (\forall v_h \in V_h) \tag{21}$$

を満たす $u_h \in V_h$ を探す方程式を考える. この時, 再び Lax–Milgram の定理を用いれば, 方程式 (21) の解が存在して一意であることを示すことができる. ここで V の閉部分空間 V_h が何らかの意味で V に “近い” ならば, 方程式 (21) の解 u_h は方程式 (19) の解 u の “良い近似” になっていると予想される. このことは, 次の Céa の補題によって示されている.

定理 4.4 (Céa の補題) a を $V \times V$ 上の連続かつ強圧的な双 1 次形式とする. 方程式 (19) および方程式 (21) の解をそれぞれ u, u_h とすると,

$$\|u - u_h\|_V \leq \frac{a_0}{\alpha} \inf_{v_h \in V_h} \|u - v_h\|_V \tag{22}$$

が成り立つ. ただし, a_0 および α はそれぞれ式 (17) および (18) で定まる正定数である.

正定数 a_0 および α が V_h によらないことに注意すると, 不等式 (22) の右辺は **V_h の元による u の最良近似における誤差**を表している. すなわち, この定理は u_h が u に “どれくらい近い” かは, 閉部分空間 V_h の選択に依存していることを表わしている.

証明 双 1 次形式 a の強圧性と連続性から, 任意の $v_h \in V_h$ に対し,

$$\begin{aligned}
\alpha \|u - u_h\|_V^2 &\leq a(u - u_h, u - u_h) \\
&= a(u - u_h, u - v_h) + a(u, v_h - u_h) - a(u_h, v_h - u_h) \\
&= a(u - u_h, u - v_h) + \ell(v_h - u_h) - \ell(v_h - u_h) \\
&\leq a_0 \|u - u_h\|_V \|u - v_h\|_V
\end{aligned}$$

より $\alpha \|u - u_h\|_V \leq a_0 \|u - v_h\|_V$ を得る. 従って v_h の任意性より, 式 (22) が成り立つ. ∎

4.2 有限要素方程式の解の誤差評価

弱形式 (4) の解の一意存在や, 弱形式 (11) の解の収束性が, 前節で示した抽象的変分問題の枠組みを用いて示されることを見ていこう. まず

$$V := \left\{ v \in H^1(\Omega);\ v = 0,\ x \in \Gamma_0 \right\} \tag{23}$$

と定める. このようにして定めた V は (実) Hilbert 空間である. また

$$a(u,v) := \int_\Omega \nabla u \cdot \nabla v \, dx, \qquad \|v\| := a(v,v)^{1/2} \qquad (\forall u, v \in H^1(\Omega))$$

とする. この時, $\|\,.\,\|$ は V において $H^1(\Omega)$ のノルムと同値なノルムになる: ある正定数 c_1, c_2 $(c_1 \le c_2)$ が存在して

$$c_1 \|v\|_{H^1(\Omega)} \le \|v\| \le c_2 \|v\|_{H^1(\Omega)} \qquad (\forall v \in V)$$

が成り立つ. 左側の不等号は Poincaré の不等式と呼ばれている. したがって V のノルムとして $\|\,.\,\|$ を採用すると, V はこのノルムにより Banach 空間になる. また $a(\,.\,,\,.\,)$ を内積とする Hilbert 空間になる.

ここで $w := u - \widetilde{g}$ とおくと, 弱形式 (4) は

$$\int_\Omega \nabla w \cdot \nabla v \, dx = \int_\Omega f v \, dx - \int_\Omega \nabla \widetilde{g} \cdot \nabla v \, dx \qquad (\forall v \in V) \tag{24}$$

を満たす $w \in V$ を求めることと同値である. Lax–Milgram の定理を用いれば, 弱形式 (24) の一意可解性が, すなわち弱形式 (4) の一意可解性が示される.

定理 4.5 $f \in L^2(\Omega)$ の時, 弱形式 (4) の解は一意的に存在する.

証明 弱形式 (24) の一意可解性を示せば十分である.

$$\ell(v) := \int_\Omega f v \, dx - \int_\Omega \nabla \widetilde{g} \cdot \nabla v \, dx$$

は V 上の線形汎関数であり, Schwarz の不等式とノルムの同値性とから

$$|\ell(v)| \le c \left(\|f\|_{L^2(\Omega)} + \|\widetilde{g}\|_{H^1(\Omega)} \right) \|v\|, \qquad \forall v \in V$$

となる正の定数 c が存在する. したがって $\ell \in V'$ である. 再び Schwarz の不等式とノルムの同値性とから

$$a(u,v) := \int_\Omega \nabla u \cdot \nabla v \, dx$$

は V 上の連続かつ強圧的な双 1 次形式であることがわかる. 以上のことから弱形式 (24) に Lax–Milgram の定理が適用できるので, $w \in V$ が一意的に存在することが分かる. ∎

次に弱形式 (11) の解の収束性について考えよう. 以下では簡単のために, ある定数 g_D が存在して $g = g_D$ $(\forall x \in \Gamma_0)$, すなわち g は Γ_0 上で定数であると仮定する. この時,

$$\widetilde{g} = g_D, \quad \nabla\widetilde{g} = 0 \qquad (\forall x \in \Omega) \tag{25}$$

ととれることに注意しよう. 式 (9) で定めた V_h は V の閉部分空間であるから, Céa の補題を用いれば次の評価を得ることができる:

定理 4.6 3 角形分割 $\mathscr{T}_h$ の取り方によらないある定数 $c > 0$ が存在して

$$\|u - u_h\|_{H^1(\Omega)} \leq c \inf_{v_h \in X_h} \|u - v_h\|_{H^1(\Omega)}. \tag{26}$$

が成り立つ.

証明 $w_h := u_h - \widetilde{g}$ とおくと, 弱形式 (11) は

$$a(w_h, v_h) = \ell(v_h) \left(= \int_\Omega f v_h \, dx \right) \qquad (\forall v_h \in V_h)$$

を満たす $w_h \in V_h$ を求めることと同値である. よって式 (25) に注意すれば Céa の補題より, $V \times V$ 上における a の連続性と強圧性によって定まる 3 角形分割によらないある正定数 c が存在して

$$\|u - u_h\| = \|w - w_h\| \leq c \inf_{v_h \in V_h} \|w - v_h\| = c \inf_{v_h \in X_h} \|u - v_h\|$$

が成り立つ. ∎

今, $h \downarrow 0$ となる 3 角形分割の列 $\left\{\mathscr{T}_h\right\}_{h\downarrow 0}$ が与えられたとする. 3 角形が “潰れていない” ために以下の条件を課す:

定義 4.7 (3 角形分割列の正則性) ある正定数 σ が存在して,

$$\frac{\rho(K)}{\mathrm{diam}(K)} \geq \sigma \qquad (\forall K \in \mathscr{T}_h, \ \forall h) \tag{27}$$

が成り立つ時, 3 角形分割列 $\left\{\mathscr{T}_h\right\}_{h\downarrow 0}$ は正則であるという. ここに, $\rho(K)$ は 3 角形 K の内接円の半径, $\mathrm{diam}(K)$ は 3 角形 K の辺長の最大値である.

例えば 3 角形分割列の場合, それぞれの 3 角形の内角を θ とした時, ある正定数 θ_0 が存在して

$$\theta \geq \theta_0 \qquad (\forall K \in \mathscr{T}_h, \ \forall h) \tag{28}$$

が成り立っていれば, 条件 (27) が満たされることが分かっている. 条件 (28) は**最小角条件**と呼ばれる.

さらに弱形式 (4) の解 u が $u \in H^2(\Omega)$ を満たし, 3 角形分割列が正則であるとする. この時 P_1 要素に関して, ある正定数 c が存在して

$$\|v - v_h\|_{H^k(\Omega)} \leq c h^{2-k} |v|_{H^2(\Omega)} \qquad (\forall v \in H^2(\Omega), \ k = 0, 1) \tag{29}$$

が成り立つことが示せる. ただし v_h は v に対する X_h での補間関数で, $v_h := \sum_{j=1}^{N} v(P_j)\phi_j$ である. すなわち, 式 (26) の右辺は h に関して 1 次の収束次数を持つ. これより Poisson 方程式の弱形式 (4) の解 u と, P_1 要素を用いた有限要素方程式 (11) による近似解 u_h の間に以下の誤差評価が成り立つ.

定理 4.8 $\{\mathcal{T}_h\}_{h\downarrow 0}$ を正則な 3 角形分割列とし, $\{u_h\}_{h\downarrow 0}$ を対応する有限要素方程式 (11) の解とする. また弱形式 (4) の解 u が $H^2(\Omega)$ を満たしているとする. この時, h に依存しないある正定数 c が存在して

$$\|u - u_h\|_{H^1(\Omega)} \leq c\,h \qquad (h > 0)$$

が成り立つ.

5 おわりに

有限要素法を用いた時間変化の無い定常状態における温度分布の数値シミュレーションを取り上げ, 離散化の方法を解説し, 近似方程式の誤差評価を示した. 興味を持たれた方は, [1, 3, 4, 9] などの文献を通して理解をより深めて欲しい. さらにここでは取り上げることができなかったが, 解説した例を元に実際の数値シミュレーションにも取り組んで頂ければ幸いである.

参考文献

[1] Ciarlet, P.-G.: The Finite Element Method for Elliptic Problems, SIAM Classics in Applied Mathematics, No. 40, SIAM, 2002.

[2] 藤野清次, 張紹良: 反復法の数理, 応用数値計算ライブラリ, 朝倉書店, 1996.

[3] Girault, V. and Raviart, P.-A.: Finite Element Methods for Navier-Stokes Equations, Theory and Algorithms, Springer Series in Computational Mathematics, Vol. 5 Springer, 1986.

[4] 菊地文雄: 有限要素法の数理, 数学的基礎と誤差解析, 計算力学と CAE シリーズ 13, 培風館, 1994.

[5] Lis web site: ⟨`http://www.ssisc.org/lis/`⟩

[6] スタンリー・ファーロウ著, 伊理正夫, 伊理由美訳: 偏微分方程式: 科学者・技術者のための使い方と解き方, 新版, 朝倉書店, 1996.

[7] 杉原正顯, 室田一雄: 線形計算の数理, 岩波数学叢書, 岩波書店, 2009.

[8] SuperLU web site: ⟨`http://crd-legacy.lbl.gov/~xiaoye/SuperLU/`⟩

[9] 田端正久: 偏微分方程式の数値解析, 岩波書店, 2010.

[10] Tagami, D. and Tabata, M.: Numerical Computations of a Melting Glass Convection in the Furnace, Proc. The Seventh China-Japan Seminar on Numerical Mathematics (Shi, Z.-C. and Okamoto, H. eds.), Science Press, 2006, pp. 149–160.

マルコフ連鎖と混合時間

白井　朋之

九州大学マス・フォア・インダストリ研究所

マルコフ連鎖は確率過程の中でもっとも基本的かつ重要なものである．本稿では，マルコフ連鎖の基礎的な概念を例を通して紹介した後，混合時間とカットオフ現象について説明する．コンピュータ内で実現されるものを想定して，離散時間で有限集合 S に値をとる有限マルコフ連鎖のみを扱う．

1.1　マルコフ連鎖の定義

状態空間 S 上の (離散時間) 確率過程とは, 確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ 上で定義された有限集合 S に値をとる確率変数列 $\{X_t,\ t = 0, 1, \dots\}$ のことをいう．状態空間 S 上のマルコフ連鎖とは, S 上の確率過程でマルコフ性とよばれる以下の性質を持つものである : 任意の $0 \le t_1 < t_2 < \cdots < t_n < t$ と $x_0, x_1, \dots, x_n, x \in S$ に対して,

$$\mathbb{P}(X_t = x \mid X_{t_0} = x_0, X_{t_1} = x_1, \dots, X_{t_n} = x_n) = \mathbb{P}(X_t = x \mid X_{t_n} = x_n).$$

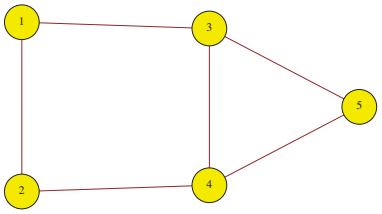
特に，マルコフ連鎖 $X = \{X_t\}$ に対して，$\mathbb{P}(X_{t+1} = y \mid X_t = x)$, $x, y \in S$ が t によらないとき，X は時間的に一様なマルコフ連鎖といい，x から y への 1 ステップの推移確率 $p(x, y) := \mathbb{P}(X_{t+1} = y \mid X_t = x)$, $x, y \in S$ により定まる $|S| \times |S|$ 行列 $P = (p(x, y))_{x,y \in S}$ を推移確率行列という．時間的に一様なマルコフ連鎖を与えることは，1 ステップの推移の確率法則，つまり推移確率行列 P を与えることと同値である．

補題 1.1 時間的に一様なマルコフ連鎖について，任意の $s, t = 0, 1, \dots$ と任意の $x, y \in S$ に対して，$\mathbb{P}(X_{t+s} = y \mid X_s = x) = P^t(x, y)$ となる．

このことより，「原理的」にはマルコフ連鎖の基本的な観測量は推移行列 P のべき乗を考えることによりすべて得られる．

1.2　マルコフ連鎖の例

例 1.2 有限グラフ上の単純ランダムウォーク (Simple random walk, SRW)．有限グラフ $G = (V, E)$ を考える．有限グラフ上の SRW とは, V を状態空間として, 各頂点 x から隣接点に等確率 $\deg(x)^{-1}$ で遷移するものとして推移確率を定義したものである．ただし, $\deg(x)$ は頂点 x の次数で，例えば，以下の図において $\deg(1) = \deg(2) = \deg(5) = 2$, $\deg(3) = \deg(4) = 3$ である．



$$P = \begin{pmatrix} 0 & 1/2 & 1/2 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 & 0 \\ 1/3 & 0 & 0 & 1/3 & 1/3 \\ 0 & 1/3 & 1/3 & 0 & 1/3 \\ 0 & 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$

例 1.3 エーレンフェストの壺のモデル. 2つの壺 A, B の中に合せて n 個の球が入っている．それぞれの玉には1から n の番号が一つずつ書いてある．ランダムに1から n までの中から数字を選んで，その番号の書いてある球を壺から取りだし別の壺に移す．このとき，壺 A の中にある球の個数に着目すると，状態空間 $S = \{0, 1, 2, \ldots, n\}$ 上のマルコフ連鎖で推移確率が

$$p(k, k-1) = \frac{k}{n}, \quad p(k, k+1) = \frac{n-k}{n} \qquad (k = 0, 1, 2, \ldots, n)$$

となるものが対応する．

例 1.4 超立方体上の SRW. $S = \{0,1\}^n$ とする．$n = 2$ のときは S は正方形の各頂点と，$n = 3$ のときは S は立方体の各頂点と同一視できる．推移確率行列は $2^n \times 2^n$ になるのでこれをすべて書き下すのは現実的でない．このような場合は，アルゴリズム的に書くとわかりやすい．$x = (x_1, \ldots, x_n) \in S$ の推移を以下で定義する：

(1) 一様ランダムに $\{1, 2, \ldots, n\}$ から座標 i を選ぶ．

(2) $x_i = 0$ ならば $x_i = 1$ に，$x_i = 1$ ならば $x_i = 0$ にアップデートする．一つの式で書けば，$x_i \mapsto 1 - x_i$ である．

例えば，$n = 5$ のときの推移の様子は以下のようになる．

$$(1,0,1,1,0) \xrightarrow{3} (1,0,0,1,0) \xrightarrow{5} (1,0,0,1,1) \xrightarrow{2} (1,1,0,1,1) \xrightarrow{3} (1,1,1,1,1) \xrightarrow{1} \cdots$$

矢印の上の数字は，ステップ (1) でランダムに選ばれる座標をあらわす．1 と 0 のかわりにアップスピンとダウンスピンをあらわす矢印に置きかえれば，

$$(\uparrow,\downarrow,\uparrow,\uparrow,\downarrow) \xrightarrow{3} (\uparrow,\downarrow,\downarrow,\uparrow,\downarrow) \xrightarrow{5} (\uparrow,\downarrow,\downarrow,\uparrow,\uparrow) \xrightarrow{2} (\uparrow,\uparrow,\downarrow,\uparrow,\uparrow) \xrightarrow{3} (\uparrow,\uparrow,\uparrow,\uparrow,\uparrow) \xrightarrow{1} \cdots$$

のようになり，磁石のモデル（イジング模型）の時間発展のようにも見なせる．

特に，X_t の1の個数 $N_t = \sum_{i=1}^n (X_t)_i$ は，例 1.3 で述べたエーレンフェストの壺と同じマルコフ連鎖を定めることがわかる．

例 1.5 q-彩色全体上のマルコフ連鎖. $G = (V, E)$ を有限グラフとする．$q > \max_{x \in S} \deg(x)$ なる自然数を固定して，写像 $c\colon V \to \{1, 2, \ldots, q\}$ を考える．これは，色の種類が q 種類あって，グラフ上の点 v を $c(v)$ と彩色することをあらわす．各点に1から q までのいずれかを割り振っていると考えてもよい．写像 c を q-彩色といい，その全体を状態空間 S とする．また，$vw \in E$ のとき，つまり v と w がグラフ上で隣接しているとき，$c(v) \neq c(w)$ となるような写像 c をプロパー q-彩色といい，その全体からなる S の部分集合を S_{proper} とあらわす．一般のグラフ G の場合には S_{proper} の個数自体はっきりしないが，このときにも，アルゴリズム的に S 上のマルコフ連鎖 $\{c_t\}$ を定義することができる：

(1) V の一点を一様ランダムに選ぶ.
(2) (1) で $v \in V$ が選ばれたとき，$A_v(c_t) = \{1, 2, \ldots, q\} \setminus \{c_t(w); vw \in E\}$ を頂点 v を彩色可能な色の集合とし，$A_v(c_t)$ から一様に色を選んで，$c_{t+1}(v)$ をその色にアップデートし，他の点の色はそのままとする.

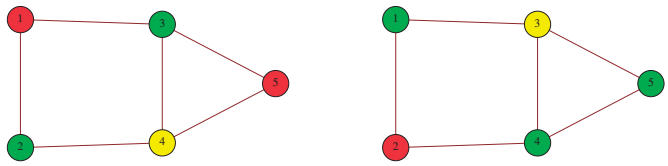


図 1 : 左はプロパー 3-彩色である．右は 3-彩色であるがプロパー 3-彩色ではない.

注意 1.6 図 1 では 3-彩色としたが，もちろん $k \geq 3$ ならば k-彩色でもある.

1.3 既約性と周期性

定義されたマルコフ連鎖が状態空間全体を行き渡るかどうかはまず考えるべき問題である.

定義 1.7 任意の $x, y \in S$ に対して，ある $t = t_{x,y}$ が存在して $\mathbb{P}(X_t = y \mid X_0 = x) > 0$ となるとき，S 上のマルコフ連鎖 X は既約 (irreducible) であるという.

定義 1.8 $\mathcal{P}(x) := \{t \geq 1 \mid \mathbb{P}(X_t = x \mid X_0 = x) > 0\}$ とおく．$\mathcal{P}(x)$ の最大公約数を状態 $x \in S$ の周期という．X が既約であるとき，各状態の周期はすべて等しいことが知られている．このとき，その値をマルコフ連鎖 X の周期といい，周期が 1 であるとき，X は非周期的 (aperiodic) であるという.

例 1.9 図 2 は，チェスのビショップとナイトの動きをあらわしたものである．状態空間 S をチェス盤の 64 個のマス目とし，推移のルールは各駒の到達可能なマス目を一様ランダムに選ぶ．図 2 のときは，ビショップの場合 $\frac{1}{13}$ の確率で推移可能なマス目を選び，ナイトの場合は $\frac{1}{8}$ でマス目を選ぶことになる．このような推移を繰り返すことにより得られるマルコフ連鎖をそれぞれランダムビショップムーブ，ランダムナイトムーブという.
(既約性) ランダムビショップムーブは既約でない．実際，推移のルールから初期位置と同じ色のマス目の上のみを動き，別の色のマス目に移る確率は 0 である．一方，ランダムナイトムーブは既約であることが示される (何故か？).
(周期性) ランダムナイトムーブは周期 2 である．実際，推移のルールから一回のジャンプでは，初期位置と違う色のマス目にしか移動できない．よって，元の場所には偶数回のジャンプの後にしか戻れない．ランダムビショップムーブは非周期的である.

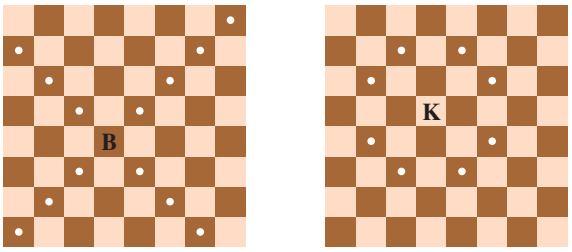


図 2：ビショップ（角）とナイト（八方桂馬）の動き方．白丸のマス目にジャンプ可能．

1.4 定常分布と可逆分布

マルコフ連鎖の $t \to \infty$ で挙動は重要である．マルコフ連鎖の無記憶性より，（ある弱い条件のもと）初期状態によらず X_t の分布は定常分布とよばれる確率分布へ収束する．

定義 1.10 S 上の確率分布 π がマルコフ連鎖 X の定常分布であるとは，

$$\sum_{x \in S} \pi(x) p(x, y) = \pi(y)$$

をみたすときをいう．また，詳細釣り合い (detailed balance) の式

$$\pi(x) p(x, y) = \pi(y) p(y, x), \quad \forall x, y \in S$$

が成り立つとき，π は可逆分布であるという．

命題 1.11 π が可逆分布ならば，定常分布である．

注意 1.12 (1) 任意の閉路 $(x_1, x_2, \ldots, x_n, x_1)$ に対して，

$$p(x_1, x_2) p(x_2, x_3) \cdots p(x_n, x_1) = p(x_1, x_n) p(x_n, x_{n-1}) \cdots p(x_2, x_1)$$

となること，つまり任意の閉路に対して右廻りと左廻りの確率が等しくなることが可逆分布が存在するための必要十分条件である．
(2) 可逆分布が存在するとき，詳細釣り合いの式によりすべての点の比が決定可能である．

例 1.13 例 1.3 のマルコフ連鎖は，$\pi(k) = \binom{n}{k} 2^{-n}$ を可逆分布として持つことが確かめられる．実際，$\tilde{\pi}(0) = 1$ として詳細釣り合いの式 $\tilde{\pi}(k) \frac{n-k}{n} = \tilde{\pi}(k+1) \frac{k+1}{n}$, $k = 0, 1, \ldots, n-1$ を解くと $\tilde{\pi}(k) = \binom{n}{k}$ が得られるので，確率分布になるように $\pi(k) = \tilde{\pi}(k) / \sum_{j=0}^{n} \tilde{\pi}(j)$ とすればよい．

例 1.14 n 点からなるサイクルグラフを C_n とあらわす．C_n 上の SRW は既約である．奇サイクルの場合は非周期的で，偶サイクルの場合は周期 2 となる．ともに一様分布が可逆分布となる．また，C_n 上のマルコフ連鎖で，各頂点での推移確率が，時計廻りに確率 p $(\neq 1/2)$，反時計廻りに確率 $q = 1 - p$ $(\neq 1/2)$ となるものを考えると，定常分布が一様分布となることはすぐに確かめられるが，注意 1.12 (1) によると可逆分布でないことがわかる．

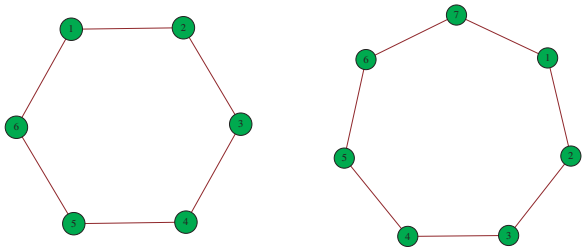


図 3：偶サイクル C_6 と奇サイクル C_7

命題 1.15 例 1.2 で扱った有限グラフ $G=(V,E)$ 上の SRW の場合，定常分布は $\pi(x)=\frac{\deg(x)}{2|E|}$ で与えられる．$\pi(x)$ は可逆分布でもある．

定理 1.16 (1) 有限マルコフ連鎖 X が既約ならば，定常分布はただ一つ存在する．
(2) 有限マルコフ連鎖 X が既約かつ非周期的のとき，初期状態が $x\in S$ のときの X_t の分布 $\mathbb{P}(X_t=\cdot\mid X_0=x)=P^t(x,\cdot)$ は $t\to\infty$ で $x\in S$ によらず定常分布 π に収束する．つまり，推移確率行列の t 乗 P^t は行列 Π に収束する．ただし，$\Pi(x,y)=\pi(y)$ $(x,y\in S)$ である．

命題 1.17 既約マルコフ連鎖の推移確率が，任意の $x,y\in S$ に対して $p(x,y)=p(y,x)$ をみたせば，一様分布 $\pi(x)=\frac{1}{|S|}$, $\forall x\in S$ は可逆分布，特に定常分布である．

例 1.18 例 1.2 のマルコフ連鎖において，命題 1.15 により $\pi=(\frac{1}{6},\frac{1}{6},\frac{1}{4},\frac{1}{4},\frac{1}{6})$ である．また既約で非周期的であるから定理 1.16 (2) により，

$$P^t=\begin{pmatrix}0&1/2&1/2&0&0\\1/2&0&0&1/2&0\\1/3&0&0&1/3&1/3\\0&1/3&1/3&0&1/3\\0&0&1/2&1/2&0\end{pmatrix}^t\to\begin{pmatrix}1/6&1/6&1/4&1/4&1/6\\1/6&1/6&1/4&1/4&1/6\\1/6&1/6&1/4&1/4&1/6\\1/6&1/6&1/4&1/4&1/6\\1/6&1/6&1/4&1/4&1/6\end{pmatrix}=\Pi\qquad(t\to\infty)$$

となることがわかる．

注意 1.19 推移確率 P の既約マルコフ連鎖で，$p(x,x)>0$ となる点が一つでも存在すれば非周期的となる．定理 1.16 (2) を用いるために，しばしばマルコフ連鎖の怠惰版 (lazy version) を用いることがある．これは，$P=(p(x,y))$ から

$$q(x,y)=\begin{cases}\frac{1}{2}p(x,y), & y\neq x\\ \frac{1}{2}+\frac{1}{2}p(x,x), & y=x\end{cases}$$

と定まる推移確率をもつマルコフ連鎖のことである．推移確率行列で書けば，$Q=\frac{1}{2}(I+P)$ であり，公平なコインを投げて表ならば P で定まるマルコフ連鎖の推移を行ない，裏ならばその場に留まる，というマルコフ連鎖をあらわす．Q の定常分布は P のものと一致し，P が周期的な場合も Q は非周期的となる．

例 1.20 既約ではないが，時間が十分経つと既約成分に落ち着く例．　$G=(V,E)$ は連結有限グラフで，$q>\max_{x\in S}\deg(x)$ とする．例 1.5 において，G の q-彩色全体を状態空間 S とするマルコフ連鎖が定義された．推移ルールのステップ (1) で選ばれた頂点にはステップ (2) で隣接点と違う色が彩色される．よって，どんな彩色からスタートしても，ステップ (1) ですべての点が少なくとも一度選ばれれば q-プロパー彩色となる．また，一度プロパー q-彩色 c に到達すれば，その後プロパー q-彩色にしか推移しない．つまり，S_{proper} は閉じている．状態空間 S 全体でのマルコフ連鎖は既約でないが，S_{proper} 上のマルコフ連鎖は既約となる．S_{proper} のような集合を S 上のマルコフ連鎖の既約成分ということもある．また，推移ルールについて少し考察すると，命題 1.17 により定常分布は S_{proper} 上の一様分布になることがわかる．

1.5　クーポンコレクターの問題

様々な問題に応用されるクーポンコレクターの問題を考える．

問題　ある会社が n 種類のクーポン（カード）をあるお菓子のおまけとして発行している．このクーポンを全種類集めたいと思っている人がいるとする．一つお菓子を買うと一枚ずつ等確率 $1/n$ でクーポンを手にする．全種類のクーポンを手に入れるためには，大体何個くらいお菓子を買えばよいか?

この問題はマルコフ連鎖 $\{X_t\}_{t\geq 0}$ の問題として定式化される．$S=\{0,1,2,\dots,n\}$ は手持ちのクーポンの種類をあらわす状態空間．k 種類のクーポンを持っている状態で新しいクーポンを得る確率は $\frac{n-k}{n}$ であるから，推移確率は

$$p(k,k)=\frac{k}{n},\quad p(k,k+1)=\frac{n-k}{n}\qquad (k\in S)$$

と与えられる．自然数に値をとる確率変数 τ_n を

$$\tau_n=\inf\{t\in\mathbb{N};X_t=n\}$$

とおくと，初めてクーポンが全種類（n 種類）集まる時間をあらわす．上の問題は確率変数 τ_n の性質を調べることと言いかえられる．例えば，以下の事実を簡単に示すことができる．

命題 1.21　(1) $E[\tau_n]=n\sum_{k=1}^{n}\frac{1}{k}\sim n\log n$. (2) $\lim_{n\to\infty}P(\tau_n\leq n\log n+cn)=e^{-e^{-c}}$ $(c\in\mathbb{R})$.

つまり，クーポンを集めるまでの平均時間は約 $n\log n$ で，$n\log n$ を越えても全種類のクーポンが集っていない確率は指数的に小さくなる．例えば，$n=100$ のとき，$E[\tau_{100}]=518.738\cdots$ である．図 5 は $n=100$ として τ_{100} を 10000 回シミュレーションした結果である．実線は，命題 1.21 (2) から得られる理論値である．

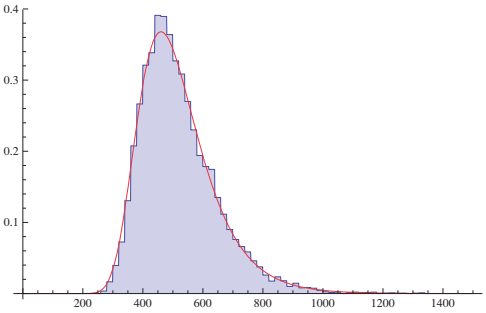


図 4：τ_{100} のヒストグラムと極限分布.

1.6 混合時間

有限マルコフ連鎖は既約かつ非周期的ならば定常分布に収束することを定理 1.16 で述べた. 以下ではその収束のスピードに関して議論する. そのために, 状態空間 S 上の確率分布の全体 $\mathcal{P}(S)$ 上に距離を導入すると便利である. 確率分布は行ベクトル $\pi = (\pi(x))_{x\in S}$ とみなす.

定義 1.22 $\mu, \nu \in \mathcal{P}(S)$ に対して,

$$\|\mu - \nu\|_{TV} = \max_{A\subset S} |\mu(A) - \nu(A)|$$

と定義される距離を全変動距離 (total variation distance) という.

全変動距離は以下のような別の表現ももつ.

命題 1.23 $0 \le \|\mu - \nu\|_{TV} \le 1$ で,

$$\begin{aligned}\|\mu - \nu\|_{TV} &= \frac{1}{2}\sum_{x\in S} |\mu(x) - \nu(x)| = \sum_{\substack{x\in S \\ \mu(x)\ge\nu(x)}} |\mu(x) - \nu(x)| \\ &= \inf\{P(X \ne Y) \mid (X, Y) \text{ は } (\mu, \nu) \text{ のカップリング}\}\end{aligned}$$

ここで, X の周辺分布が μ, Y の周辺分布が ν となるような 2 次元確率変数 (X, Y) を (μ, ν) のカップリングであるという.

注意 1.24 X が既約かつ非周期的のとき, 定理 1.16 と S が有限集合であることを考慮すると, $d(t) := \max_{x\in S} \|P^t(x, \cdot) - \pi\|_{TV} \to 0$ であると言える. さらに, $d(t)$ は単調減少（単調非増加）であることが知られている.

定義 1.25 混合時間 (mixing time) を以下のように定義する.

$$t_{\text{mix}}(\epsilon) := \inf\{t \in \mathbb{N} \mid d(t) \le \epsilon\}$$

と定義し, 特に $t_{\text{mix}} := t_{\text{mix}}(1/4)$ と定義する. $1/4$ は $1/2$ 以下ならば本質的には何でもよい.

混合時間とはマルコフ連鎖がほぼ定常分布に近づいた時間をあらわし，最近，以下の問題が色々な例で調べられている．

問題 増大する状態空間の列 $\{S_n,\ n \in \mathbb{N}\}$ と S_n 上のマルコフ連鎖 $X^{(n)} = \{X_t^{(n)}\}$ が与えられているとすると，各 $(X^{(n)}, S_n)$ に対して，$d_n(t)$ や $t_{\text{mix}}^{(n)}$ が定義される．$t_{\text{mix}}^{(n)}$ の $n \to \infty$ での挙動を調べよ．

例えば，コンピュータシミュレーションによりある集合 S の中から一様にサンプリングをしたいとき，しばしば定常分布が S 上の一様分布となるマルコフ連鎖が用いられる (Markov Chain Monte Carlo, MCMC)．十分時間が経てばマルコフ連鎖 X_t の分布は一様分布に近づいているので，十分大きい t に対する X_t をもって一様サンプリングしたことにするのである．この際，どれくらいの時間が経てば定常分布に近づいているかを見積るために上のような問題が意味を持ってくる．「X_t の分布は $t \to \infty$ で定常分布に収束する」という事実より少し詳しいことを調べることになる．

1.7 マルコフ連鎖のカップリング

定義 1.26 (1) 推移確率行列 P をもつ S 上のマルコフ連鎖で初期状態が x と y であるものの（マルコフ）カップリングとは，$S \times S$ 上のマルコフ連鎖で (X_t, Y_t) で，X_t だけに着目すると x 出発のマルコフ連鎖，Y_t だけに着目すると y 出発のマルコフ連鎖となっているものをいう．このカップリングの分布を $\mathbb{P}_{x,y}$ とあらわす．
(2)（マルコフ）カップリングのカップリング時間 τ_{couple} は，$\tau_{\text{couple}} = \inf\{t \geq 0 \mid X_t = Y_t\}$ と定義される．

例 1.27 $S = \{0, 1, 2, \ldots, n\}$ 上の反射壁をもつマルコフ連鎖を考える．つまり，$\{1, 2, \ldots, n-1\}$ では等確率 $1/2$ で隣りにジャンプし，0 では 1 に，n では $n-1$ に確率 1 でジャンプする．このマルコフ連鎖の怠惰版で出発点が x と y のものを考える．これらのカップリングは以下のようにして構成される：「コインを投げて表ならば，もう一度コインを投げて X_t を動かす．裏ならば同様のことを Y_t について行う．」一回の操作で，X_t か Y_t の一方だけを動かしている．もし，Y_t の存在を忘れて X_t にだけ着目すると，出発点が x のマルコフ連鎖の怠惰版になっていることがわかる．このカップリングの著しい性質は，$x \leq y$ ならば, 任意の t に対して $X_t \leq Y_t$ となっていることにある．よって，事象の包含関係 $\{X_t = n\} \subset \{Y_t = n\}$ より，

$$P^t(x, n) = \mathbb{P}_{x,y}(X_t = n) \leq \mathbb{P}_{x,y}(Y_t = n) = P^t(y, n)$$

がわかる．任意の時刻 t に対して，右端 n にいる確率 $P^t(x, n)$ は，初期状態 x に関して単調増大であることが示された．

1.8 マルコフ連鎖のカップリングと混合時間の評価

カップリング時間の期待値は t_{mix} の上からの評価に用いられる．

命題 1.28 $t_{\mathrm{mix}} \le 4 \max_{x,y\in S} \mathbb{E}_{x,y}[\tau_{\mathrm{couple}}]$. ただし，$\mathbb{E}_{x,y}$ は $\mathbb{P}_{x,y}$ による期待値をあらわす.

この評価から，混合時間の評価のためにはカップリング時間が小さくなるうまいカップリングを構成することが重要になる．以下 2 つの例を紹介する.

1.8.1 サイクル C_n 上のマルコフ連鎖の混合時間

例 1.14 の SRW の怠惰版 (LSRW) の混合時間を評価する．異なる初期状態から出発する LSRW のカップリング (X_t, Y_t) を以下のようにして構成する：

(1) コインを投げて表ならば X_t を推移させ，裏ならば Y_t を推移させる.

(2) $X_t = Y_t$ となった後は同じ状態を保ったまま，LSRW のルールで推移させる.

例えば，X_t のみに着目すると，C_n 上の LSRW となっていることは明らかであろう．このカップリングのカップリング時間を考えてみよう．X_t と Y_t のグラフ上の最短距離を Z_t とすると，$\{0, 1, \dots, \lfloor n/2 \rfloor\}$ 上のマルコフ連鎖となる（n の偶奇により $\lfloor n/2 \rfloor$ での動きが少しだけ違う）. よって，X_t と Y_t のカップリング時間は，Z_t が 0 へ初めて到達する時間に等しい．この時間の期待値は $O(n^2)$ であることが知られている．よって，命題 1.28 により，$t_{\mathrm{mix}} = O(n^2)$ であることがわかる.

1.8.2 超立方体上のマルコフ連鎖の混合時間

例 1.4 の怠惰版 (LSRW) の混合時間を評価してみよう．異なる初期状態から出発する LSRW のカップリング (X_t, Y_t) は以下のようにして構成される：

(1) 一様ランダムに $\{1, 2, \dots, n\}$ を選ぶ.

(2) コインを投げて表ならばその座標の値をともに 1, 裏ならばその座標の値をともに 0 とする.

以下は，$n = 5$ の場合のカップリングの例である．上段が X_t, 下段が Y_t をあらわす.

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \overset{3,\text{表}}{\to} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \overset{5,\text{表}}{\to} \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \overset{3,\text{裏}}{\to} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \overset{1,\text{表}}{\to} \cdots$$

例えば，(1) で i 座標が選ばれたとき，(2) の操作は i 座標の値が 0 でも 1 でも確率 1/2 で変化せず，確率 1/2 で違う値にアップデートされる．よって，X_t, Y_t のいずれかに着目すると，例 1.4 の怠惰版になっていることがわかる．このカップリングにより，一度 (1) で選ばれた座標の値は以後ずっと一致している．よって，カップリング時間は，初期状態 x, y のうち値の異なる座標（上の例では $\{1, 3, 4\}$）すべてが (1) で選ばれる最初の時間である．これは，1, 3, 4 をまだ手にしていないクーポンとみなすと，1.5 節のクーポンコレクターの問題で考えた τ_n よりも小さい．ゆえに，$\mathbb{E}_{x,y}[\tau_{\mathrm{couple}}] \le \mathbb{E}[\tau_n] \le n \log n + n$. よって，命題 1.28 により $t_{\mathrm{mix}} \le 4(n \log n + n)$ と評価される．実際は，もっと詳しく $t_{\mathrm{mix}} \sim \frac{1}{2} n \log n$ であることが知られている.

1.9　カットオフ現象

カットオフ現象とは，混合時間 t_{mix} の前後で $d(t)$ の値が 1 から 0 へ急激に変化する現象のことをいう．X_t の分布がある時間を過ぎると急激に定常分布に近づく現象である．

定義 1.29 幅 w_n の窓のカットオフ現象が起こるとは，$w_n = o(t_{\mathrm{mix}}^{(n)})$ かつ

$$\lim_{c\to-\infty} \liminf_{n\to\infty} d_n(t_{\mathrm{mix}}^{(n)} + cw_n) = 1, \qquad \lim_{c\to+\infty} \limsup_{n\to\infty} d_n(t_{\mathrm{mix}}^{(n)} + cw_n) = 0$$

となるときをいう．

カットオフ現象の定義は，$d_n(t)$ のグラフを $t = t_{\mathrm{mix}}^{(n)}$ の前後で w_n の幅で拡大して $n \to \infty$ とすると，階段関数となることを示している．例えば，超立方体の SRW の怠惰版では $t_{\mathrm{mix}}^{(n)} = \frac{1}{2} n \log n$ で幅 n の窓のカットオフ現象が起きる．一方，C_n 上の単純ランダムウォークではカットオフ現象は起きないことが知られている．

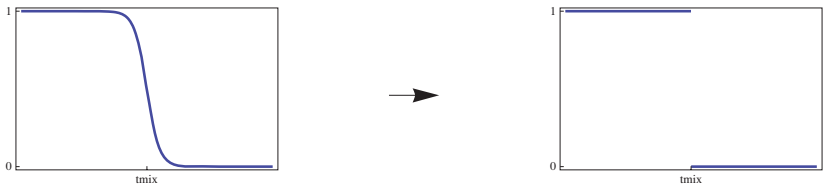


図 5：カットオフ現象のイメージ．$d_n(t)$ のグラフ．

1.10　最後に

マルコフ連鎖と混合時間の基本概念について述べた．紙幅の関係で t_{mix} の評価はカップリングの方法による上からの評価についてのみ説明したが，下からの評価も含めて様々な評価の方法が知られている．詳しくは参考文献 [2] をお薦めする．確率論のテキストとしては例えば [1] などが参考になる．

参考文献

[1] R. Durrett, *Probability: theory and examples*, Fourth edition, Cambridge University Press, Cambridge, 2010.

[2] D. A. Levin, Y. Peres and E. L. Wilmer, *Markov Chains and Mixing Times*, Amer. Math. Soc., providence, RI, 2009.

確率論の数理ファイナンス・保険数理への応用

斎藤　新悟

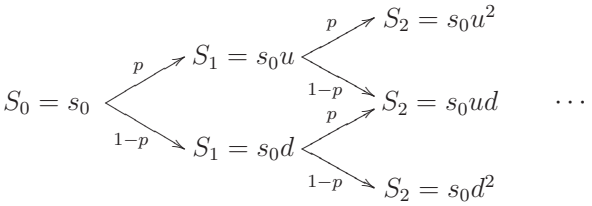
九州大学マス・フォア・インダストリ研究所

本稿では確率論の数理ファイナンスおよび保険数理への応用例を取り扱う．第1節では，**二項モデル** (binomial model) または **CRR モデル** (CRR model, Cox-Ross-Rubinstein model) と呼ばれる，金融派生商品の価格付けの離散的なモデルについて述べる．第2節では，生命保険数理において生存・死亡などの状況を Markov 過程を用いて記述する方法について概観する．どちらについてもごく基本的な事項にとどめているので，より詳しくは末尾の参考文献などを参照．

1　二項モデルにおける金融派生商品の価格付け

1.1　設定

一定の利率 $r > 0$ を持つ安全資産と，時刻 $t \in \{0, 1, \dots, T\}$ での価格が S_t であるような株が存在する市場を考え，S_t は次のように変化すると仮定する：時刻 0 における株価 S_0 は定数 $s_0 > 0$ であり，時刻が 1 だけ経過するごとに株価は上昇して u 倍になるか下降して d 倍になるかのいずれかがそれぞれ確率 p, $1-p$ で独立に起こる $(0 < d < 1 + r < u,\ 0 < p < 1)$.



確率空間の言葉を用いると，次で与えられる確率空間 $(\Omega, \mathcal{F}, P)$ が背後にあると考えられる：$\Omega = \{\pm 1\}^T = \{\omega = (\omega_1, \dots, \omega_T) \mid \omega_1, \dots, \omega_T = \pm 1\}$ で，$\mathcal{F}$ は Ω のべき集合であり，確率測度 P は各 $\omega = (\omega_1, \dots, \omega_T) \in \Omega$ に対して

$$P(\{\omega\}) = p^{\#\{i=1,\dots,T \mid \omega_i = 1\}} (1-p)^{\#\{i=1,\dots,T \mid \omega_i = -1\}}$$

を満たすようなものである．$t = 0, \dots, T$ に対して，$\mathcal{F}$ の部分 σ 加法族 $\mathcal{F}_t$ を

$$\mathcal{F}_t = \left\{ \{\omega = (\omega_1, \dots, \omega_T) \in \Omega \mid (\omega_1, \dots, \omega_t) \in A\} \;\middle|\; A \subset \{\pm 1\}^t \right\}$$

で定義する．特に $\mathcal{F}_0 = \{\emptyset, \Omega\}$, $\mathcal{F}_T = \mathcal{F}$ である．$\mathcal{F}_t$ は時刻 t までの情報を表し，確率変数が $\mathcal{F}_t$ 可測であることは各 $\omega = (\omega_1, \dots, \omega_T) \in \Omega$ での値が $\varphi(\omega_1, \dots, \omega_t)$ と書けることと同値である．

1.2 金融派生商品の価格付け

二項モデルでは，**金融派生商品** (derivative) は満期時刻 T におけるペイオフを表す確率変数 X としてモデル化され，特に S_T の関数として $X = f(S_T)$ と書けるものが主要な興味の対象である．例えば $X = \max\{k - S_T, 0\}$ は行使価格 k のヨーロピアン・プット・オプションを表し，$X = \max\{S_T - k, 0\}$ は行使価格 k のヨーロピアン・コール・オプションを表す．本節の目標はこのような金融派生商品の価格を求めることである．

まず，金融派生商品の価格を定義するために投資戦略の概念を定義する．

定義 1.1 次の条件を満たす確率変数の列 $\theta = (\alpha_1, \beta_1, \ldots, \alpha_T, \beta_T)$ を**自己資金調達投資戦略** (self-financing strategy) と呼ぶ：

- 任意の $t = 1, \ldots, T$ に対して α_t, β_t は $\mathcal{F}_{t-1}$ 可測．
- 任意の $t = 1, \ldots, T-1$ に対して $\alpha_t(1+r)^t + \beta_t S_t = \alpha_{t+1}(1+r)^t + \beta_{t+1} S_t$ が成立する．

自己資金調達投資戦略 θ の時刻 t における**価値** (value) を

$$V_t(\theta) = \alpha_t(1+r)^t + \beta_t S_t = \alpha_{t+1}(1+r)^t + \beta_{t+1} S_t$$

で定義する．ただし，$t = 0$ のときは $V_0(\theta) = \alpha_1(1+r)^0 + \beta_0 S_0 = \alpha_1 + \beta_0 s_0$ と定義し，$t = T$ のときは $V_T(\theta) = \alpha_T(1+r)^T + \beta_T S_T$ と定義する．

注意 1.2 α_t, β_t はそれぞれ時刻 $t-1$ から t までの間の安全資産・株の保有量を表している．$V_t(\theta)$ は $\mathcal{F}_t$ 可測な確率変数である．

定義 1.3 確率変数 X に対して，$V_T(\theta) = X$ を満たす自己資金調達投資戦略 θ を X の**複製戦略** (replicating strategy) と呼ぶ．X の複製戦略 θ に対して，$V_t(\theta)$ を時刻 t における X の**価格** (price) と呼ぶ $(t = 0, \ldots, T)$．

注意 1.4 X の価格は株価が上昇する確率 p には依存しない．

ここでの価格の定義が well-defined であることは次の定理によって保証される：

定理 1.5 任意の確率変数 X に対して複製戦略はただ 1 つ存在する．

証明 複製戦略を $\theta = (\alpha_1, \beta_1, \ldots, \alpha_T, \beta_T)$ とおくと，可測性より $\alpha_t = \alpha_t(\omega_1, \ldots, \omega_{t-1})$, $\beta_t = \beta_t(\omega_1, \ldots, \omega_{t-1})$ と書ける．このとき θ が満たすべき条件は，

$$\begin{cases} \alpha_T(\omega_1, \ldots, \omega_{T-1})(1+r)^T + \beta_T(\omega_1, \ldots, \omega_{T-1}) S_{T-1}(\omega_1, \ldots, \omega_{T-1}) u = X(\omega_1, \ldots, \omega_{T-1}, 1), \\ \alpha_T(\omega_1, \ldots, \omega_{T-1})(1+r)^T + \beta_T(\omega_1, \ldots, \omega_{T-1}) S_{T-1}(\omega_1, \ldots, \omega_{T-1}) d = X(\omega_1, \ldots, \omega_{T-1}, -1) \end{cases}$$

かつ $t = 1, \ldots, T$ に対して

$$\begin{cases} \alpha_t(\omega_1, \ldots, \omega_{t-1})(1+r)^t + \beta_t(\omega_1, \ldots, \omega_{t-1}) S_{t-1}(\omega_1, \ldots, \omega_{t-1}) u \\ \qquad = \alpha_{t+1}(\omega_1, \ldots, \omega_{t-1}, 1)(1+r)^t + \beta_{t+1}(\omega_1, \ldots, \omega_{t-1}, 1) S_{t-1}(\omega_1, \ldots, \omega_{t-1}) u, \\ \alpha_t(\omega_1, \ldots, \omega_{t-1})(1+r)^t + \beta_t(\omega_1, \ldots, \omega_{t-1}) S_{t-1}(\omega_1, \ldots, \omega_{t-1}) d \\ \qquad = \alpha_{t+1}(\omega_1, \ldots, \omega_{t-1}, -1)(1+r)^t + \beta_{t+1}(\omega_1, \ldots, \omega_{t-1}, -1) S_{t-1}(\omega_1, \ldots, \omega_{t-1}) d \end{cases}$$

が成立することなので，帰納的に $\alpha_T, \beta_T, \ldots, \alpha_1, \beta_1$ が一意的に定まる． ∎

リスク中立確率の概念を用いると，X の価格を簡単に計算することができる．

定義 1.6 $q \in (0,1)$ を方程式

$$qu + (1-q)d = 1 + r$$

の解すなわち $q = (1+r-d)/(u-d)$ とする．$(\Omega, \mathcal{F})$ 上の確率測度 Q であって，各 $\omega = (\omega_1, \ldots, \omega_T) \in \Omega$ に対して

$$Q(\{\omega\}) = q^{\#\{i=1,\ldots,T|\omega_i=1\}}(1-q)^{\#\{i=1,\ldots,T|\omega_i=-1\}}$$

を満たすものを**リスク中立確率** (risk-neutral probability) または**同値マルチンゲール測度** (equivalent martingale measure) と呼ぶ．

命題 1.7 θ を自己資本調達投資戦略とし，$0 \leqq s \leqq t \leqq T$ とすると，

$$V_s(\theta) = \frac{1}{(1+r)^{t-s}} E_Q[V_t(\theta)|\mathcal{F}_s]$$

すなわち任意の $\omega_1, \ldots, \omega_s = \pm 1$ に対して次が成立する：

$$V_s(\theta)(\omega_1, \ldots, \omega_s) = \frac{1}{(1+r)^{t-s}} \sum_{\omega_{s+1},\ldots,\omega_t=\pm 1} q^{\#\{i=s+1,\ldots,t|\omega_i=1\}}(1-q)^{\#\{i=s+1,\ldots,t|\omega_i=-1\}} V_t(\theta)(\omega_1, \ldots, \omega_t).$$

証明　s を固定して t についての帰納法で証明する．$t = s$ のとき右辺は

$$\frac{1}{(1+r)^0} q^0 (1-q)^0 V_s(\theta)(\omega_1, \ldots, \omega_s) = V_s(\theta)(\omega_1, \ldots, \omega_s)$$

となるのでよい．t のときに成立すると仮定する．任意の $\omega_{s+1}, \ldots, \omega_t = \pm 1$ に対して

$$\begin{aligned} V_{t+1}(\theta)(\omega_1, \ldots, \omega_t, 1) &= \alpha_{t+1}(\omega_1, \ldots, \omega_t)(1+r)^{t+1} + \beta_{t+1}(\omega_1, \ldots, \omega_t) S_t(\omega_1, \ldots, \omega_t) u, \\ V_{t+1}(\theta)(\omega_1, \ldots, \omega_t, -1) &= \alpha_{t+1}(\omega_1, \ldots, \omega_t)(1+r)^{t+1} + \beta_{t+1}(\omega_1, \ldots, \omega_t) S_t(\omega_1, \ldots, \omega_t) d \end{aligned}$$

より

$$\begin{aligned} &qV_{t+1}(\theta)(\omega_1, \ldots, \omega_t, 1) + (1-q)V_{t+1}(\theta)(\omega_1, \ldots, \omega_t, -1) \\ &\quad = \alpha_{t+1}(\omega_1, \ldots, \omega_t)(1+r)^{t+1} + \beta_{t+1}(\omega_1, \ldots, \omega_t) S_t(\omega_1, \ldots, \omega_t)\big(qu + (1-q)d\big) \\ &\quad = (1+r)\big(\alpha_{t+1}(\omega_1, \ldots, \omega_t)(1+r)^t + \beta_{t+1}(\omega_1, \ldots, \omega_t) S_t(\omega_1, \ldots, \omega_t)\big) \\ &\quad = (1+r)V_t(\theta) \end{aligned}$$

が成立する．よって，$t+1$ のときの命題の式の右辺は

$$\begin{aligned}
&\frac{1}{(1+r)^{t+1-s}} \sum_{\omega_{s+1},\dots,\omega_{t+1}=\pm 1} q^{\#\{i=s+1,\dots,t+1|\omega_i=1\}}(1-q)^{\#\{i=s+1,\dots,t+1|\omega_i=-1\}} V_{t+1}(\theta)(\omega_1,\dots,\omega_{t+1}) \\
&= \frac{1}{(1+r)^{t+1-s}} \sum_{\omega_{s+1},\dots,\omega_t=\pm 1} \Big(q^{\#\{i=s+1,\dots,t|\omega_i=1\}+1}(1-q)^{\#\{i=s+1,\dots,t|\omega_i=-1\}} V_{t+1}(\theta)(\omega_1,\dots,\omega_t,1) \\
&\qquad\qquad + q^{\#\{i=s+1,\dots,t|\omega_i=1\}}(1-q)^{\#\{i=s+1,\dots,t|\omega_i=-1\}+1} V_{t+1}(\theta)(\omega_1,\dots,\omega_t,-1) \Big) \\
&= \frac{1}{(1+r)^{t+1-s}} \sum_{\omega_{s+1},\dots,\omega_t=\pm 1} \Big(q^{\#\{i=s+1,\dots,t|\omega_i=1\}}(1-q)^{\#\{i=s+1,\dots,t|\omega_i=-1\}} \\
&\qquad\qquad \times \big(q V_{t+1}(\theta)(\omega_1,\dots,\omega_t,1) + (1-q) V_{t+1}(\theta)(\omega_1,\dots,\omega_t,-1) \big) \Big) \\
&= \frac{1}{(1+r)^{t-s}} \sum_{\omega_{s+1},\dots,\omega_t=\pm 1} q^{\#\{i=s+1,\dots,t|\omega_i=1\}}(1-q)^{\#\{i=s+1,\dots,t|\omega_i=-1\}} V_t(\theta) \\
&= V_s(\theta)(\omega_1,\dots,\omega_s)
\end{aligned}$$

となり確かに $t+1$ のときも成立することが分かる． ∎

注意 1.8 命題 1.7 は確率測度 Q に関して $\big(V_t(\theta)/(1+r)^t\big)_{t=0,\dots,T}$ がマルチンゲールであることを示している．これが Q が同値マルチンゲール測度と呼ばれる由来である．

定理 1.9 確率変数 X の時刻 0 における価格は次で与えられる：

$$\frac{1}{(1+r)^T} E_Q[X] = \frac{1}{(1+r)^T} \sum_{\omega=(\omega_1,\dots,\omega_T)\in\Omega} q^{\#\{i=1,\dots,T|\omega_i=1\}}(1-q)^{\#\{i=1,\dots,T|\omega_i=-1\}} X(\omega).$$

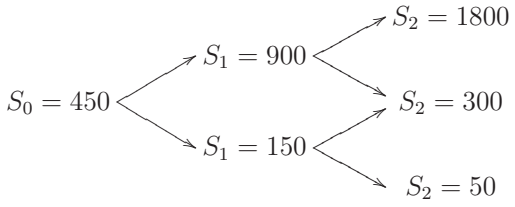
特に $X = f(S_T)$ の形で表される場合は次で与えられる：

$$\frac{1}{(1+r)^T} \sum_{k=0}^{T} \binom{T}{k} q^k (1-q)^{T-k} f(s_0 u^k d^{T-k}).$$

証明 命題 1.7 で $s=0$, $t=T$ とすればよい． ∎

1.3 例

$T=2$, $r=0.5$, $u=2$, $d=1/3$, $s_0=450$ とする（p は不要なので特に指定しない）と，株価の変化は次のように表される：



このとき，満期時刻 2，行使価格 375 のヨーロピアン・プット・オプションの時刻 0 における価格を求める．このオプションの満期でのペイオフは次で与えられる：

$$X = \max\{375 - S_2, 0\} = \begin{cases} 0 & (S_2 = 1800), \\ 75 & (S_2 = 300), \\ 325 & (S_2 = 50). \end{cases}$$

定理 1.5 の証明に従って X の複製戦略 $\theta = (\alpha_1, \beta_1, \alpha_2, \beta_2)$ を求めよう．まず α_2, β_2 は

$$\begin{cases} 1.5^2\alpha_2(1) + 1800\beta_2(1) = 0, \\ 1.5^2\alpha_2(1) + 300\beta_2(1) = 75, \end{cases} \qquad \begin{cases} 1.5^2\alpha_2(-1) + 300\beta_2(-1) = 75, \\ 1.5^2\alpha_2(-1) + 50\beta_2(-1) = 325 \end{cases}$$

から $\alpha_2(1) = 40$, $\beta_2(1) = -1/20$, $\alpha_2(-1) = 500/3$, $\beta_2(-1) = -1$ と求められる．次に α_1, β_1 は

$$\begin{cases} 1.5\alpha_1 + 900\beta_1 = 1.5\alpha_2(1) + 900\beta_2(1) = 1.5 \cdot 40 + 900 \cdot (-1/20) = 15, \\ 1.5\alpha_1 + 150\beta_1 = 1.5\alpha_2(-1) + 150\beta_2(-1) = 1.5 \cdot 500/3 + 150 \cdot (-1) = 100 \end{cases}$$

から $\alpha_1 = 78$, $\beta_1 = -17/150$ と求められる．よって時刻 0 における X の価格は

$$V_0(\theta) = \alpha_1 + 450\beta_1 = 78 + 450 \cdot (-17/150) = 27$$

である．

一方，リスク中立確率を求めると

$$2q + \frac{1}{3}(1 - q) = 1.5$$

より $q = 0.7$ となるので，定理 1.9 より時刻 0 における X の価格は

$$\frac{1}{1.5^2}\left(\binom{2}{0} \cdot 0.7^2 \cdot 0 + \binom{2}{1} \cdot 0.7 \cdot 0.3 \cdot 75 + \binom{2}{2} \cdot 0.3^2 \cdot 325\right) = 27$$

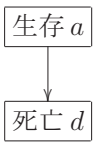
となり，上で求めたものと一致する．

2　Markov 過程による生存・死亡状況の記述

$(X_x)_{x \geqq 0}$ を連続時間 Markov 過程とする．状態空間は各小節で定められる有限集合であり，X_x は人の x 歳における状態（生存・死亡など）を表す．

2.1　生存・死亡

状態空間を $\{a, d\}$ とし（a は生存 (alive) を表し，d は死亡 (dead) を表す），推移は次の方向にのみ起こりうると仮定する：



$x, t \geqq 0$ に対して推移確率を

$$ {}_tp_x = P(X_{x+t} = a \mid X_x = a), \qquad {}_tq_x = P(X_{x+t} = d \mid X_x = a) $$

と書き，これらが微分方程式

$$ \frac{d}{dt}\begin{pmatrix} {}_tp_x & {}_tq_x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} {}_tp_x & {}_tq_x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -\mu_{x+t} & \mu_{x+t} \\ 0 & 0 \end{pmatrix} $$

を満たすと仮定する．μ_x を年齢 x における**死力** (force of mortality) と呼ぶ.

命題 2.1 任意の $x, t \geqq 0$ に対して次が成立する：

$$ {}_tp_x = \exp\left(-\int_0^t \mu_{x+s}\, ds\right), \qquad {}_tq_x = 1 - {}_tp_x. $$

証明　微分方程式と ${}_0p_x = 1$, ${}_0q_x = 0$ から容易に従う. ∎

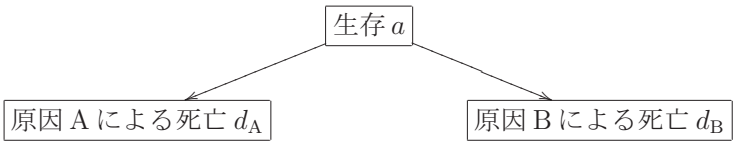
例 2.2 $\mu_{x+t} = \mu_x/(1 - \mu_x t)$ $(0 \leqq t \leqq 1)$ の場合，$0 \leqq t \leqq 1$ に対して

$$ {}_tp_x = \exp\left(-\int_0^t \frac{\mu_x}{1 - \mu_x s}\, ds\right) = 1 - \mu_x t, \qquad {}_tq_x = 1 - {}_tp_x = \mu_x t $$

となる．これは $0 \leqq t \leqq 1$ において一様に死亡が発生する状況を表しており，このとき $\mu_x = {}_1q_x$ が成立する.

2.2　多重脱退

状態空間を $\{a, d_{\mathrm{A}}, d_{\mathrm{B}}\}$ とし（d_{A}, d_{B} はそれぞれ原因 A, B による死亡を表す），推移は次の方向にのみ起こりうると仮定する：



$x, t \geqq 0$ に対して推移確率を

$$ {}_tp_x = P(X_{x+t} = a \mid X_x = a), \quad {}_tq_x^{\mathrm{A}} = P(X_{x+t} = d_{\mathrm{A}} \mid X_x = a), \quad {}_tq_x^{\mathrm{B}} = P(X_{x+t} = d_{\mathrm{B}} \mid X_x = a) $$

と書き，これらが微分方程式

$$ \frac{d}{dt}\begin{pmatrix} {}_tp_x & {}_tq_x^{\mathrm{A}} & {}_tq_x^{\mathrm{B}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} {}_tp_x & {}_tq_x^{\mathrm{A}} & {}_tq_x^{\mathrm{B}} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} -\mu_{x+t}^{\mathrm{A}} - \mu_{x+t}^{\mathrm{B}} & \mu_{x+t}^{\mathrm{A}} & \mu_{x+t}^{\mathrm{B}} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} $$

を満たすと仮定する.

命題 2.3 任意の $x, t \geqq 0$ に対して次が成立する：

$$ {}_tp_x = \exp\left(-\int_0^t (\mu^{\mathrm{A}}_{x+s} + \mu^{\mathrm{B}}_{x+s})\, ds\right), \quad {}_tq^{\mathrm{A}}_x = \int_0^t {}_sp_x \mu^{\mathrm{A}}_{x+s}\, ds, \quad {}_tq^{\mathrm{B}}_x = \int_0^t {}_sp_x \mu^{\mathrm{B}}_{x+s}\, ds. $$

証明 容易である. ∎

A, B の片方の原因が存在しない場合の死亡率を**絶対死亡率** (absolute probability of death) と呼び,

$$ {}_tq^{\mathrm{A}*}_x = 1 - \exp\left(-\int_0^t \mu^{\mathrm{A}}_{x+s}\, ds\right), \qquad {}_tq^{\mathrm{B}*}_x = 1 - \exp\left(-\int_0^t \mu^{\mathrm{B}}_{x+s}\, ds\right) $$

で定義される. 死亡が一様に発生するという仮定の下で, 死亡率は絶対死亡率から次のようにして簡単に求めることができる：

命題 2.4 $0 \leqq t \leqq 1$ に対して $\mu^{\mathrm{A}}_{x+t} = \mu^{\mathrm{A}}_x/(1-\mu^{\mathrm{A}}_x t)$, $\mu^{\mathrm{B}}_{x+t} = \mu^{\mathrm{A}}_x/(1-\mu^{\mathrm{B}}_x t)$ が成立すると仮定すると, 次が成立する：

$$ q^{\mathrm{A}}_x = q^{\mathrm{A}*}_x\left(1 - \frac{q^{\mathrm{B}*}_x}{2}\right), \qquad q^{\mathrm{B}}_x = q^{\mathrm{B}*}_x\left(1 - \frac{q^{\mathrm{A}*}_x}{2}\right). $$

ただし q^{A}_x などは ${}_1q^{\mathrm{A}}_x$ などの略記である.

証明 どちらも同様なので q^{A}_x についてのみ証明する. $0 \leqq t \leqq 1$ に対して

$$ {}_tp_x = \exp\left(-\int_0^t \left(\frac{\mu^{\mathrm{A}}_x}{1-\mu^{\mathrm{A}}_x s} + \frac{\mu^{\mathrm{B}}_x}{1-\mu^{\mathrm{B}}_x s}\right) ds\right) = (1-\mu^{\mathrm{A}}_x t)(1-\mu^{\mathrm{B}}_x t) $$

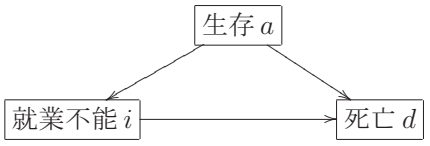
なので

$$ q^{\mathrm{A}}_x = \int_0^1 (1-\mu^{\mathrm{A}}_x s)(1-\mu^{\mathrm{B}}_x s)\frac{\mu^{\mathrm{A}}_x}{1-\mu^{\mathrm{A}}_x s}\, ds = \mu^{\mathrm{A}}_x\left(1 - \frac{\mu^{\mathrm{B}}_x}{2}\right) $$

となり, 例 2.2 より $\mu^{\mathrm{A}}_x = q^{\mathrm{A}*}_x$, $\mu^{\mathrm{B}}_x = q^{\mathrm{B}*}_x$ なので命題が従う. ∎

2.3 死亡・就業不能

状態空間を $\{a, i, d\}$ とし（i は就業不能 (invalid) を表す), 推移は次の方向にのみ起こりうると仮定する：



$x, t \geqq 0$ に対して推移確率を

$$ {}_tp^{aa}_x = P(X_{x+t} = a \mid X_x = a), \quad {}_tp^{ai}_x = P(X_{x+t} = i \mid X_x = a), \quad {}_tq^{a}_x = P(X_{x+t} = d \mid X_x = a), $$
$$ {}_tp^{i}_x = P(X_{x+t} = i \mid X_x = i), \quad {}_tq^{i}_x = P(X_{x+t} = d \mid X_x = i) $$

と書き，これらが微分方程式

$$\frac{d}{dt}\begin{pmatrix} {}_tp_x^{aa} & {}_tp_x^{ai} & {}_tq_x^{a} \\ 0 & {}_tp_x^{i} & {}_tq_x^{i} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} {}_tp_x^{aa} & {}_tp_x^{ai} & {}_tq_x^{a} \\ 0 & {}_tp_x^{i} & {}_tq_x^{i} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -\mu_{x+t}^{ai} - \mu_{x+t}^{a} & \mu_{x+t}^{ai} & \mu_{x+t}^{a} \\ 0 & -\mu_{x+t}^{i} & \mu_{x+t}^{i} \\ 0 & 0 & 0 \end{pmatrix}$$

を満たすと仮定する．

命題 2.5 任意の $x, t \geqq 0$ に対して次が成立する：

$$ {}_tp_x^{aa} = \exp\left(-\int_0^t (\mu_{x+s}^{ai} + \mu_{x+s}^{a})\, ds\right), \qquad {}_tp_x^{i} = \exp\left(-\int_0^t \mu_{x+s}^{i}\, ds\right),$$

$$ {}_tp_x^{ai} = \int_0^t {}_sp_x^{aa}\mu_{x+s}^{ai}\, {}_{t-s}p_{x+s}^{i}\, ds, \qquad {}_tq_x^{a} = 1 - {}_tp_x^{aa} - {}_tp_x^{ai}, \qquad {}_tq_x^{i} = 1 - {}_tp_x^{i}.$$

証明　まず，

$$\frac{d}{dt}{}_tp_x^{aa} = -{}_tp_x^{aa}(\mu_{x+t}^{ai} + \mu_{x+t}^{a}), \qquad \frac{d}{dt}{}_tp_x^{i} = -{}_tp_x^{i}\mu_{x+t}^{i}$$

と ${}_0p_x^{aa} = {}_0p_x^{i} = 1$ より ${}_tp_x^{aa}$, ${}_tp_x^{i}$ が求められる．次に

$$\frac{d}{dt}{}_tp_x^{ai} = {}_tp_x^{aa}\mu_{x+t}^{ai} - {}_tp_x^{ai}\mu_{x+t}^{i}$$

より

$$\frac{d}{dt}\left(\frac{{}_tp_x^{ai}}{{}_tp_x^{i}}\right) = \frac{({}_tp_x^{aa}\mu_{x+t}^{ai} - {}_tp_x^{ai}\mu_{x+t}^{i})\,{}_tp_x^{i} - {}_tp_x^{ai}(-{}_tp_x^{i}\mu_{x+t}^{i})}{({}_tp_x^{i})^2} = \frac{{}_tp_x^{aa}\mu_{x+t}^{ai}}{{}_tp_x^{i}}$$

なので ${}_tp_x^{ai} = {}_tp_x^{i}\int_0^t ({}_sp_x^{aa}\mu_{x+s}^{ai}/{}_sp_x^{i})\, ds$ であるが，$0 \leqq s \leqq t$ のとき

$$\begin{aligned} {}_tp_x^{i} &= P(X_{x+t} = i \mid X_x = i) = P(X_{x+t} = i,\ X_{x+s} = i \mid X_x = i) \\ &= P(X_{x+t} = i \mid X_{x+s} = i,\ X_x = i)P(X_{x+s} = i \mid X_x = i) \\ &= P(X_{x+t} = i \mid X_{x+s} = i)P(X_{x+s} = i \mid X_x = i) = {}_{t-s}p_{x+s}^{i}\, {}_sp_x^{i} \end{aligned}$$

なので ${}_tp_x^{ai} = \int_0^t {}_sp_x^{aa}\mu_{x+s}^{ai}\, {}_{t-s}p_{x+s}^{i}\, ds$ が得られる．${}_tq_x^{a}$, ${}_tq_x^{i}$ の式は明らかである． ∎

参考文献

[1] Ragnar Norberg, *Basic Life Insurance Mathematics*, `http://www.math.ku.dk/~mogens/lifebook.pdf`, 2002.

[2] 京都大学理学部アクチュアリーサイエンス部門編『確率で考える生命保険数学入門』岩波書店，2012.

[3] 黒田耕嗣，松山直樹『生命保険数理への確率論的アプローチ』培風館，2010.

[4] 藤田岳彦『ファイナンスの確率解析入門』講談社，2002.

[5] 二見隆『生命保険数学』生命保険文化研究所，1992.

[6] 若山正人編，川崎英文・谷口説男著『最適化法，数理ファイナンスへの確率解析入門』講談社サイエンティフィク（現代技術への数学入門シリーズ），2008.

確率過程モデル

増田　弘毅

九州大学マス・フォア・インダストリ研究所

確率過程とは, 連続時間軸に沿って発展する現象を記述する確率モデルであり, 通常, “インデックス集合 $T \subset \mathbb{R}_+$ 上の連続関数もしくはジャンプ不連続点を持つ関数に値をとる無限次元確率変数 $\omega \mapsto \{X_t(\omega)\}_{t\in T}$” を意味する. その確率構造は, 滑らかな被積分関数 f に対しても Riemann-Stieltjes 積分 $\int f\,dX$ を定義できないような “非有界変動” を持つものから, 区分的に定数であるような疎な変動を持つものまで様々に存在し, 信号の伝播, 人口変動, 株価・為替レート・インデックス (TOPIX や日経 225, etc.) の時間変動など, そのモデリング対象は多岐に亘る.

1　Lévy 過程

確率変数 ζ の分布を $\mathcal{L}(\zeta)$ で表す. 原点から出発する実数値確率過程 $X = (X_t)_{t\in\mathbb{R}_+}$ が **Lévy 過程**であるとは, 以下の二つの条件が成り立つことである:

- (独立定常増分性) 任意の有限時点 $0 = t_0 < t_1 < \cdots < t_n$ に対し, 増分 $X_{t_1} - X_{t_0}$, $X_{t_2} - X_{t_1}, \ldots, X_{t_n} - X_{t_{n-1}}$ は独立で, かつ各 j について $\mathcal{L}(X_{t_j} - X_{t_{j-1}}) = \mathcal{L}(X_{t_j - t_{j-1}})$;
- (確率連続性) 各 t について, $s \to t$ のとき X_s は X_t へ確率収束する.

任意の Lévy 過程について, 各時点で右連続かつ左極限を持つバージョンを選ぶことができる. 確率連続性とは, 事前に固定されたジャンプ時点を持たないという要請である; 例えば, i.i.d. 確率変数 $\xi_1, \xi_2, \ldots$ に対して定まる $X_t = \sum_{j=1}^{[t]} \xi_j$ は Lévy 過程ではない. Lévy 過程 X について, 任意の $t > 0$, $n \in \mathbb{N}$ に対して以下のように表せる:

$$X_t = \sum_{j=1}^{n} (X_{jt/n} - X_{(j-1)t/n}).$$

即ち, Lévy 過程は任意の微小時間区間における独立な誤差の累積によって表され, 連続時間ランダムウォークとして自然に解釈される. 後述の確率微分方程式モデルのように, より一般の確率過程を構成する際の素材にもなる. 任意の Lévy 過程 X に対してある無限分解可能分布 $F := \mathcal{L}(X_1)$ が一つ定まり, 逆に任意の無限分解可能分布 F に対して $F = \mathcal{L}(X_1)$ となる Lévy 過程 X が一つ定まる. この事実により, 単位時間区間 $[0,1]$ 上の終点までにかかるノイズとして無限分解可能分布を一つ決めることは, 対応する Lévy 過程を一つ決めることと同等である.

Lévy 過程の定義は一見簡単であるが, それから膨大な結果が帰結する. 特に, 任意の Lévy 過程 X は

$$X_t = bt + \sqrt{c}\, w_t + J_t \tag{1}$$

と表現される (X の標本路の **Lévy-伊藤分解**): ここで $b \in \mathbb{R}$, $c \geq 0$ は定数, w は標準 Wiener 過程, J はジャンプだけで変動する Poisson 型 Lévy 過程で w と独立なものである. 標準 Wiener 過程とは, 各 s, t に対して $\mathcal{L}(w_t - w_s)$ が正規分布 $N(0, |t-s|)$ となる Lévy 過程であり, 連続であるが至る所で微分不可能な標本路を持つ. また, J は Lévy 測度 $\nu(dz)$ で特徴付けられる. 各 Borel 集合 $A \subset \mathbb{R}\backslash\{0\}$ に対し, $\nu(A)$ は単位時間 $[0,1]$ においてサイズが A に属するようなジャンプの期待生起頻度を表す量に相当する; 微小ジャンプは無限回生じ得る ($\nu(A) = \infty$ となり得る). 詳細については [13] を参照されたい. 図 1 に平面上の Wiener 過程と一種の純粋ジャンプ型 Lévy 過程の標本路を示す.

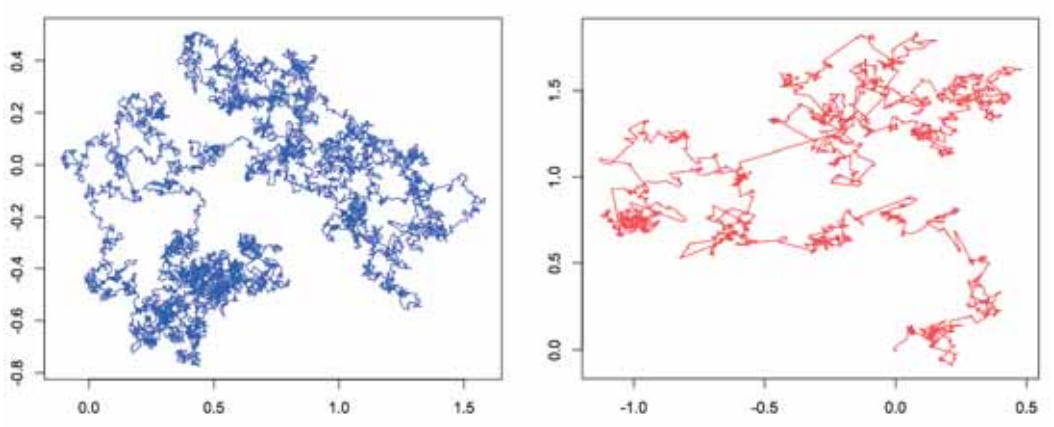


図 1: 平面上の Wiener 過程 (左) とジャンプ型 Lévy 過程 (右; ジャンプ変動も線でつないで表している).

重要なのは, (1) の形の Lévy 過程 X は, 非確率的な三つ組 (b, c, ν) で完全に特徴付けられる点である. このとき, $\mathcal{L}(X_t)$ の特性関数は以下の **Lévy-Khintchine の表現**で与えられる:

$$\int e^{iux} P^{X_t}(dx) = \exp\left[t\left\{iub - \frac{1}{2}cu^2 + \int \left(e^{iuz} - 1 - iuzI_U(z)\right)\nu(dz)\right\}\right], \quad u \in \mathbb{R}.$$

ここで I_U は集合 $U := \{z \in \mathbb{R} : |z| \leq 1\}$ の指示関数を, また P^{X_t} は X_t の像測度を表す.

データ系列が非正規性を呈する状況は多々ある. 近年では, 正規ノイズ過程である Wiener 過程のみによるモデリングではなく, "Wiener 過程 + 複合 Poisson 過程" や, "ジャンプ型 Lévy 過程" を採用することでモデルの適合度や予測精度を向上させる試みが主流になってきている. "ノイズ" を単に非正規型に替えるだけでデータへの適合性が格段に上がり得る実証例は多々存在する; 例えば, 数理ファイナンス・計量経済における一般化双曲型 Lévy 過程およびその部分族の有用性などが挙げられる ([2] 参照).

以下, 具体的な無限分解可能分布を二つ紹介する. 詳細については [8] とその参考文献参照.

以下の確率密度を持つ $\mathbb{R}_+$ 上の分布を**一般化逆正規分布 (Generalized Inverse-Gaussian; GIG) 分布**とよぶ:

$$p_{\mathrm{GIG}}(x; \lambda, \delta, \gamma) = \frac{(\gamma/\delta)^\lambda}{2K_\lambda(\gamma\delta)} x^{\lambda-1} \exp\Big\{-\frac{1}{2}\Big(\frac{\delta^2}{x} + \gamma^2 x\Big)\Big\}, \quad x > 0. \tag{2}$$

ここで $K_\lambda(x)$, $\lambda \in \mathbb{R}$, は指数 λ の変形された第三種 Bessel 関数を表し, パラメータ $(\lambda, \delta, \gamma)$ は以下をみたす:

$$\begin{cases} \lambda > 0 \ \Rightarrow \ \delta \geq 0, \ \gamma > 0; \\ \lambda = 0 \ \Rightarrow \ \delta > 0, \ \gamma > 0; \\ \lambda < 0 \ \Rightarrow \ \delta > 0, \ \gamma \geq 0. \end{cases} \tag{3}$$

GIG 分布の Laplace 変換は陽に計算でき, それより存在する限り任意次数のモーメントを $K_\cdot(\cdot)$ を用いて表現可能である; $\gamma \neq 0$ であれば任意次数のモーメントが存在するが, $\gamma = 0$ のときは $k < -\lambda$ のときにかぎって k 次モーメントが存在する. パラメータ $(\lambda, \delta, \gamma)$ を操作することで, 多くの典型的な $\mathbb{R}_+$ 上の分布が得られる: 例えば, $\delta = 0$, $\gamma > 0$, $\lambda > 0$ でガンマ分布; $\delta > 0$, $\gamma = 0$, $\lambda < 0$ で逆ガンマ分布; $\delta > 0$, $\gamma \geq 0$, $\lambda = -1/2$ で逆正規分布, などなど. また, $\delta/\gamma \to c \in (0, \infty)$ なる条件下で $\delta, \gamma \to \infty$ とすれば, 極限分布として c に退化した一点分布 δ_c が得られる. 更に, GIG 分布を適当に変換 (例えば冪変換) することで, Weibull 分布や対数正規分布などの諸分布が得られる.

定数 μ, β と $\sigma \sim GIG(\lambda, \delta, \gamma)$, および σ と独立な $\eta \sim N(0, 1)$ に対して定まる正規分散平均混合

$$Y := \mu + \beta\sigma + \sqrt{\sigma}\,\eta \tag{4}$$

の分布を**一般化双曲型分布 (Generalized Hyperbolic; GH) 分布**とよび, 通常 $\alpha := \sqrt{\gamma^2 + \beta^2}$ として $GH(\lambda, \alpha, \beta, \delta, \mu)$ で表す. パラメータ空間は (3) に伴って決まる. (2) と (4) より, $\mathcal{L}(Y)$ は密度関数

$$p_{GH}(y; \lambda, \alpha, \beta, \delta, \mu) = C(\lambda, \alpha, \beta, \delta)\{h(y; \delta, \mu)\}^{\lambda - 1/2} K_{\lambda - \frac{1}{2}}\left(\alpha h(y; \delta, \mu)\right) e^{\beta(y-\mu)}, \quad y \in \mathbb{R},$$

を持つことが分かる. ここで h と C は以下で与えられる:

$$h(y; \delta, \mu) := \sqrt{\delta^2 + (y-\mu)^2}, \quad C(\lambda, \alpha, \beta, \delta) = \frac{(\alpha^2 - \beta^2)^{\lambda/2}}{\sqrt{2\pi}\alpha^{\lambda - 1/2}\delta^\lambda K_\lambda(\delta\sqrt{\alpha^2 - \beta^2})}.$$

特に $GH(\lambda, \alpha, \beta, \delta, \mu)$ の裾挙動について

$$p_{GH}(y; \lambda, \alpha, \beta, \delta, \mu) = O\left(|y|^{\lambda - 1} \exp\{-\alpha|y| + \beta y\}\right), \quad |y| \to \infty,$$

が成り立つ. GIG 分布のときと同様に, 適当なパラメータ操作を施すことで, 正規分布, 歪みのある t 分布, 正規逆正規 (normal inverse Gaussian 分布), 双曲型分布, 更には GIG 分布などが特別な場合もしくは極限分布として得られる.

2 伊藤解析と確率微分方程式

伊藤清 (1915–2008) は, Wiener 過程のような非有界変動を持つ確率過程による確率積分の概念を導入し, 特に微分方程式の確率的摂動版の理論を構築した. 今日それらは伊藤解析と総称され, 制御工学, 数理生物学, 金融工学といった広範な分野で用いられている.

伊藤により, 十分滑らかなランダムな関数 Y の標準 Wiener 過程に関する Riemann 和の (確率収束) 極限

$$\lim_{n\to\infty}\sum_{j=1}^{n} Y_{(j-1)t/n}(w_{jt/n}-w_{(j-1)t/n}) \tag{5}$$

の厳密な取り扱いが可能となった (**伊藤積分**). 極限として定まる確率変数をシンボリックに $\int_0^t Y_s\,dw_s$ と表すが, これは Riemann-Stieltjes 積分の意味で定まるものではない. 事実, (5) において "$Y_{(j-1)t/n}$" を台形公式版 "$\{Y_{(j-1)t/n}+Y_{jt/n}\}/2$" に変えたものは Stratonovich 積分とよばれ, 伊藤積分とは異なる極限を導く. 伊藤積分が導入されてから半世紀以上が経つが, 連続時間確率過程モデリングにおける基礎概念としての地位を保ち続けている.

離散時間確率過程におけるマルチンゲール変換は, 伊藤積分の雛形に相当する. (5) において w をより一般の局所マルチンゲール X へ拡げた場合にも伊藤積分は同様に定義され, 例えば, ジャンプ Lévy 過程 J に関する伊藤積分 $\int_0^t Y_{s-}\,dJ_s$ も考えることができる ($Y_{s-}:=\lim_{t\uparrow s} Y_t$).

局所マルチンゲールと有界変動過程の和で表される確率過程をセミマルチンゲールとよぶ. 右連続なセミマルチンゲール X と $\mathcal{C}^2$-関数 f に対して, 確率過程 $t\mapsto f(X_t)$ の時間発展を記述する**伊藤の公式**が成り立つ:

$$\begin{aligned} f(X_t) = f(X_0) &+ \int_0^t f'(X_{s-})\,dX_s + \frac{1}{2}\int_0^t f''(X_{s-})\,d\langle X^c\rangle_s \\ &+ \sum_{0<s\le t}\{f(X_s)-f(X_{s-})-f'(X_{s-})\Delta X_s\}. \end{aligned} \tag{6}$$

ここで X^c は X の連続局所マルチンゲール部分 (Lévy 過程 (1) の場合だと $X^c=\sqrt{c}\,w$), $\Delta X_s:=X_s-X_{s-}$ は時点 s における X のジャンプサイズを表す ($X_s=X_{s-}+\Delta X_s$). また, (6) の右辺の最後の項は t について局所一様に絶対収束する. 伊藤の公式は, Lévy 過程やそれから派生する様々な確率過程モデルの解析において不可欠な道具となる.

Lévy 過程 X と $P_0>0$ に対して $P_t=P_0\exp(X_t)$ で定まる確率過程を幾何 Lévy 過程とよび, 数理ファイナンスにおける株価変動のモデルとしてよく知られている. 伊藤の公式により,

$$P_t = P_0 + \int_0^t P_{s-}\,dX_s + \frac{1}{2}\int_0^t P_{s-}\,d\langle X^c\rangle_s + \sum_{0<s\le t} P_{s-}(e^{\Delta X_s}-1-\Delta X_s).$$

が従う. 特に X が (1) で表される場合には

$$P_t = P_0 + \Big(b+\frac{c}{2}\Big)\int_0^t P_s\,ds + \sqrt{c}\int_0^t P_s\,dw_s + \int_0^t P_{s-}\,dJ_s + \sum_{0<s\le t} P_{s-}(e^{\Delta J_s}-1-\Delta J_s)$$

となり, これは金融工学における Black-Scholes モデルにジャンプを付加したものになっている.

伊藤積分を介して, 方程式 $x_t=x_0+\int_0^t a(x_s)\,ds$ の解を Lévy 過程の畳込み因子である w および J と適当な可測関数 b, c でランダムな摂動を考えることができる (Markov 型の場合):

$$X_t = X_0 + \int_0^t a(X_s)\,ds + \int_0^t b(X_s)\,dw_s + \int_0^t c(X_{s-})\,dJ_s.$$

この積分方程式は, しばしば形式的に

$$dX_t = a(X_t)\,dt + b(X_t)\,dw_t + c(X_{t-})\,dJ_t \tag{7}$$

とも表される. (7) は**確率微分方程式 (Stochastic Differential Equation; SDE)** とよばれる. 適当な条件下で係数関数 a, b, c, および J を特徴付ける Lévy 測度 ν を制限することで, (7) が実際に (X_0, w, J) の汎関数としての解 (強い解) を有することを示せるだけではなく, 周辺分布 $\mathcal{L}(X_t)$ の裾の厚さ, また短期・長期記憶性など, X の様々な特徴を制御可能である. 係数の性質次第では, $\mathcal{L}(X_t)$ の $t \to \infty$ での弱収束極限 $\pi(dx)$ が存在する: $t^{-1}\int_0^t g(X_s)\,ds \to \int g(x)\pi(dx)$, $t \to \infty$ (エルゴード定理: 時間的平均 $\approx$ 空間的平均).

通常の常微分方程式の解の生成における Euler 法に倣った近似理論が整備されており, 乱数を介して X の標本路を計算機上で疑似生成できる. 例えば $[0,1]$ 上で $X = (X_t)_{t\le 1}$ の標本路を疑似生成したい場合, 十分大きい n に対して (十分細かい時間刻み幅で) $X_0, X_{1/n}, \ldots, X_{(n-1)/n}, X_1$ を

$$X_{(j+1)/n} = X_{j/n} + a(X_{j/n})\frac{1}{n} + b(X_{j/n})(w_{j/n} - w_{(j-1)/n}) + c(X_{j/n})(J_{j/n} - J_{(j-1)/n})$$

で Euler 近似して逐次的に発生させることが考えられる; 多くの具体的な J に対して $J_{j/n} - J_{(j-1)/n} \sim$ i.i.d. $\mathcal{L}(J_{1/n})$ の乱数生成アルゴリズムが知られている. 右連続階段関数である X の Euler 近似過程 $X^n = (X^n_t)_{t\in[0,1]}$:

$$X^n_t = X_0 + \sum_{j=1}^{[nt]}(X_{j/n} - X_{(j-1)/n}) = \begin{cases} X_{t_{j-1}} & t \in [(j-1)/n,\ j/n)\,, \\ X_1 & t = 1, \end{cases}$$

の $n \to \infty$ での一種の極限関数として (7) の解 X が得られる (図 2).

一般に, 観測幅 h で離散サンプリングした場合の時系列モデルを考える際, $h \to 0$ の下で SDE モデル (7) で近似できることがある. 例えば計量経済で有用な, 収益率変動を記述する GARCH モデルは拡散近似可能である: [12] 参照. これにより, 例えば拡散過程は定常分布の特定が容易であるなど, 極限モデルの有益な面を元々の離散時間時系列モデルへ反映させることが可能となる.

特に (7) において $a(x) = -\lambda x$, b, c を定数とすれば, ある Lévy 過程 Z に対して $dX_t = -\lambda X_t\,dt + dZ_t$ と書ける. この解は **Lévy-Ornstein-Uhlenbeck (OU) 過程**とよばれ,

$$X_t = e^{-\lambda t}X_0 + \int_0^t e^{-\lambda(t-s)}\,dZ_s, \quad t \in \mathbb{R}_+, \tag{8}$$

で与えられる. OU 過程は一次の自己回帰モデルの連続時間版であり, この場合には, Z の構造と不変分布の一対一対応を簡潔に表現できるなど, 一般の非線形係数の SDE とは共有され得ない固有の性質が知られている. 詳細については [9] とその参考文献参照. 数学的な扱いやすさが幸いし, OU 過程の応用対象は幅広い; 例えば, ボラティリティ変動 [2] や漏出積分発火ニューロンモデルにおける信号 [7] を記述する道具として用いられている.

セミマルチンゲール, 伊藤解析および SDE の理論の詳細については [4, 5] 参照.

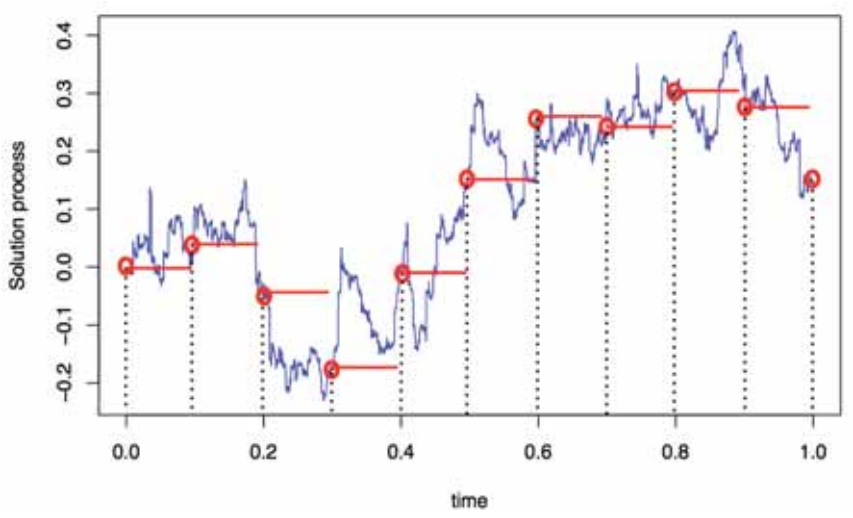


図 2: SDE モデル X (青線) とその Euler 近似過程 X^n の標本路 (赤線) のイメージ.

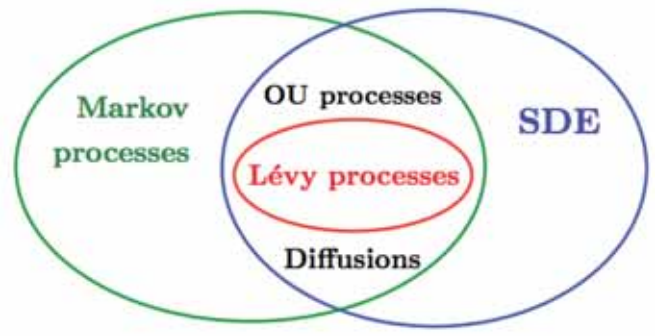


図 3: Lévy 過程, Markov 過程, SDE モデルの位置関係のイメージ. 非 Markov 型の SDE モデルも存在する.

3　統計モデルとしての確率過程

数理統計学とは, データが呈する情報を理論的根拠に基づいて有意義な形式で定量化し, それを将来への様々な意思決定へ役立てる分野を指す. 今日における数理統計学は, 不確実性を伴った実現象を扱う数多の分野に深く浸透しつつ, その実体を多方面へ拡げている. 特に, データ数が大きい場合の統計量の解析は統計的漸近理論と総称され, “分布近似” の観点から数理統計学のコアを成している.

確率過程モデルの尤度解析においては, 局所的 (微小時間) および大域的 (長期期間) な確率構造を適切に捉えて極限定理 (大数の法則, 中心極限定理など) を確保する必要がある. その際には, しばしばマルチンゲール極限理論が重要な役割を演じる. 最尤法を含んだより広い意味での統計的パラメータ推定においては, 通常, 推定量はある目的関数 $\theta \mapsto \mathbb{M}_n(\theta)$, $\theta \in \Theta \subset \mathbb{R}^p$, の最小点または最大点として定義される; 罰則付き最尤法, 最小二乗法, 最小絶対偏差法など. 推定量の漸近的性質の導出では, パラメータ空間上の確率場 $\mathbb{M}_n$ の適当な関数空間における弱収束極限の特定が本質的となる (例えば [14] 参照). 特に SDE モデルの統計的漸近推測は, その高い需要にも関わらず, Lévy 過程の多様性に起因する難解さが災いして基礎が十分に固まっていない. 連続時間観測 $(X_t)_{t\in[0,T]}$ が得られる場合の尤度解析については, 広範な族に対して無限次元確率分布の絶対連続性に基づいた漸近理論が整備されている. 一方, 現実的な離散サンプリングに基づいた推測手法については, いかなる $\mathbb{M}_n$ を構築すればよいか自体が研究対象であり, 目下発展途上である. SDE モデルの推測問題に関する近年の発展については, 論説 [15, 16] とその参考文献を参照されたい.

例 1. 個体数の変動モデル

ロジスティック型 SDE モデルは, 定数 r, K, σ と標準 Wiener 過程 w に対して

$$dX_t = r\,(1 - X_t/K)\,X_t\,dt + X_t\sigma\,dw_t \tag{9}$$

で与えられ, 細胞数や人口といった個体群成長のランダムな変動を記述する基本的なモデルとして知られている; 詳細は [6, §.9.3] 参照. ここで X_t は時刻 t における個体数を表す. (9) は, 常微分方程式で記述されるロジスティック式 $dx_t = r(1 - x_t/K)x_t\,dt$ を, 状態に依存した拡散項でランダムに摂動したモデルである. この例では, 一次元拡散過程の解析結果を用いて X の定常分布, 即ち “長期間を経て落ち着く個体数の分布” を陽に計算できる. モデル適用に際しては, 観測された個体数に基づいたパラメータ (r, K, σ) の推定は基本的な問題である.

例 2. 連続時間隠れマルコフモデルの推定

一般に, 観測されない潜在 Markov 過程 X, および X に更に不確実性が上乗せされて観測される Y から成るモデルは**隠れ Markov モデル (Hidden Markov model; HMM)** とよばれる.

SDE で記述される一種の連続時間 HMM$(X, Y) = \{(X_t, Y_t)\}_{t\in\mathbb{R}_+}$ の推定は, 例えば [1] などで扱われているフィルタリング問題におけるパラメータ推定に直接関与する. この場合の HMM の尤度解析は一般に理論上および計算上の困難が伴われるが, モーメント推定が首尾よく可能となる場合がある [10].

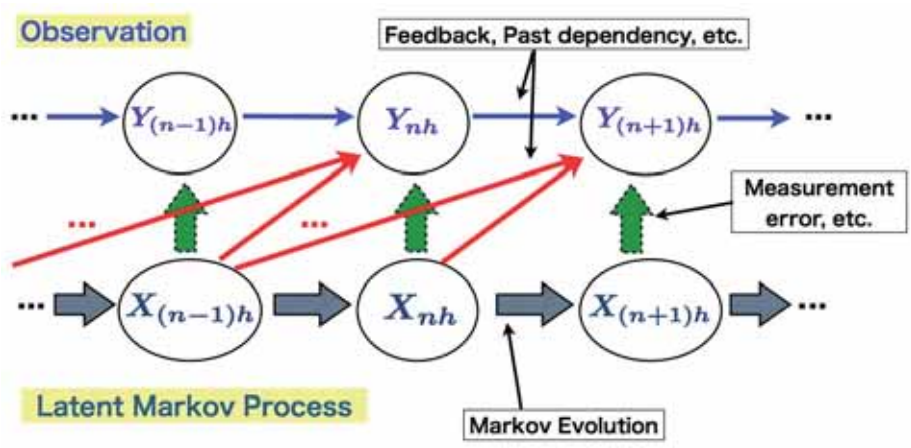


図 4: HMM の時間発展のイメージ.

固定観測幅 $h > 0$ に対して $\{Y_{jh} : j = 0, 1 \ldots .n\}$ が観測されるとする (図 4). 以下では X を (8) で与えられるものとし, $\lambda > 0$ とする. Barndorff-Nielsen と Shephard によって導入された確率ボラティリティ変動モデル [2] は

$$dY_t = (\mu + \beta X_t)\, dt + \sqrt{X_t}\, dw_t + \rho\, dZ_t.$$

で与えられる. 特に $\rho < 0$ とすることで, いわゆる leverage 効果を表現できる. ここで $X_0 > 0$ かつ $\Delta Z_t > 0$ a.s. と仮定しており, このとき任意の $t \in \mathbb{R}_+$ に対して $X_t > 0$ a.s. となることが示される. 観測過程の増分を $y_j := Y_{jh} - Y_{(j-1)h}$ で表すとき, 固定された $m \in \mathbb{N}$ に対して, $\mathcal{L}(y_1, \ldots, y_m)$ のキュムラント $\kappa^{(l)}$ の表現を利用してモーメント推定量 $\hat{\theta}_n = \hat{\theta}_n(y_1, \ldots, y_n)$ を陽に構成できる. 同様のことが連続時間状態空間モデル

$$dY_t = X_t\, dt + dZ_t.$$

についても言える. $\mathcal{L}\{\sqrt{n}(\hat{\theta}_n - \theta_0)\}$ は漸近正規性を有し, 漸近共分散行列の解析的表示も得られる (推定精度が観測幅 h にどう依存するかも明確化される). 鍵となるのは X のミキシング性である; これによってエルゴード定理や一種の中心極限定理が示され, 区間推定や検定, 更にはモデル評価の定式化へつながる.

例 3. 実現多重指数変動による累積ボラティリティの推定

高頻度データの枠組みで, 構造が複雑な確率過程モデル $X = (X_t)$ の “変動の度合い (ボラティリティ)” を簡単な統計量で推定できる.

固定期間を $[0,1]$ とし, 離散時点データ $(X_{j/n})_{j=0}^{n}$ が得られているとする. 定数 m ($\ll n$) と $r>0$ を一つ固定して実現多重指数変動 (realized Multi-Power Variation; MPV) は

$$V_n(m,r) := n^{rm/2-1} \sum_{j=1}^{n-m+1} \prod_{k=1}^{m} |X_{(j+k-1)/n} - X_{(j+k-2)/n}|^r$$

で定義される計算容易な統計量である. $mr=2$ の場合の MPV を用いることで, モデルの詳細な構造を仮定せずに, 当該期間 $[0,1]$ 上の高頻度観測から累積ボラティリティを推定できる ($n\to\infty$); (7) の場合だと推定対象は $\int_0^1 b^2(X_t)\,dt$ であり, これは X の微小区間 $[(j-1)/n,\ j/n]$ における局所的な分散を束ねたものに相当する. 図 5 では X の MPV と比して Y のそれの方が累積ボラティリティに関する "情報量" は大きい. しかしながら, データによっては, あまりに高頻度に拾ってしまうと "ミクロなノイズ" によって逆に累積ボラティリティの推定精度が低下してしまう現象も起こり得る (金融高頻度データにおける "マーケット・マイクロ・ストラクチャー・ノイズ (MMN)" の存在 [3]). この場合は, データをある程度間引くサブサンプリングを行うか, もしくは MMN の影響まで適切に加味した統計モデルとその推定方式を導入することで, より安定した推定が可能となる.

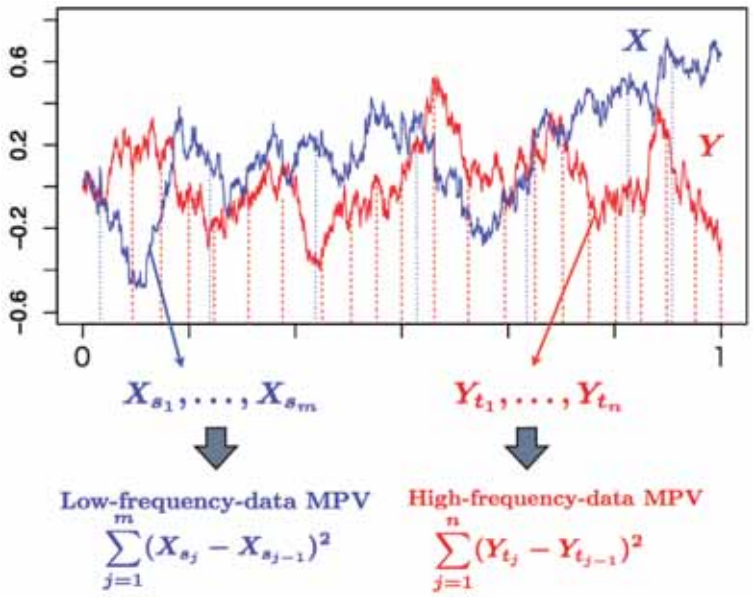


図 5: 観測頻度が異なる確率過程 X, Y から MPV を構成. 質の良いデータであれば, 累積ボラティリティの推定量としては高頻度であればあるほど好ましい.

例えば, ある株価の日内ボラティリティは金融工学におけるオプション価格の公式における必要変数として現れる. 典型的な場合は実現ボラティリティ (Realized Volatility; RV) とよばれるデータ差分二乗和で定義される統計量 $V_n(1,2)$ である. RV はマルチンゲール理論における二次変動の近似に他ならず, MPV の漸近理論の構築においては伊藤解析が本質的な役割を演じている.

$m \geq 2$ の場合が注目され出したのは最近のことである. X がジャンプを持つ確率過程の場合には, 差分二乗和ではなく, 一種の差分絶対値 $V_n(2,1)$ (Bipower Variation) などを考えることで依然累積ボラティリティを推定可能であり, ジャンプの検出, またはジャンプに頑健な推定量として機能する. 詳細については [11] とその参考文献を参照されたい.

参考文献

[1] Ahn, H. and Feldman, R. E. (2000), Optimal filtering of a Gaussian signal in the presence of Lévy noise. *SIAM J. Appl. Math.* **60**, 359–369 (electronic).

[2] Barndorff-Nielsen, O. E. *et al.* ed. (2001), Lévy processes: theory and applications. Birkhäuser.

[3] Hansen, P. R. and Lunde, A. (2006), Realized variance and market microstructure noise. *J. Bus. Econom. Statist.* **24**, 127–218.

[4] Ikeda, N. and Watanabe, S. (1989), Stochastic differential equations and diffusion processes. Second edition. North-Holland Publishing Co., Amsterdam; Kodansha, Ltd., Tokyo.

[5] 伊藤 清 (1990), 確率論. 岩波書店.

[6] 巌佐 庸 (2008), 生命の数理. 共立出版.

[7] Lansky, P. and Ditlevsen, S. (2008), A review of the methods for signal estimation in stochastic diffusion leaky integrate-and-fire neuronal models. *Biol. Cybernet.* **99**, 253–262.

[8] 増田 弘毅 (2002), GIG 分布と GH 分布に関する解析. 統計数理 **50**, 165–199.

[9] Masuda, H. (2004), On multidimensional Ornstein-Uhlenbeck processes driven by a general Lévy process. *Bernoulli* **10**, 97–120.

[10] Masuda, H. (2005), Classical method of moments for partially and discretely observed ergodic models. *Stat. Inference Stoch. Process.* **8**, 25–50.

[11] 増田 弘毅 (2009), 実現多重指数変動に基づく第二特性量行列の推定. 統計数理 **57**, 17–38.

[12] Nelson, D. B. (1990), ARCH models as diffusion approximations. *J. Econometrics* **45**, 7–38.

[13] Sato, K. (1999), Lévy processes and infinitely divisible distributions. Cambridge University Press, Cambridge.

[14] van der Vaart, A. W. (1998), Asymptotic statistics. Cambridge University Press, Cambridge.

[15] 吉田 朋広 (2010), 確率過程の統計学: 概観と展望. 日本統計学会誌 **40**, 47–60.

[16] 吉田 朋広 (2011), 拡散過程の推定における極限定理. 統計数理 **59**, 125–140.

回帰分析とその発展

西井　龍映

九州大学マス・フォア・インダストリ研究所

1　回帰分析の目的

回帰モデルは, 互いに関連する 2 組の変数から両者の関連を定量化する統計モデルであり, 統計手法の中で最も多く利用されている. 図 1 は 32 人の新生児について, 出生時の体重 (Kg) を x 座標, 70 日から 100 日後の体重の増加率 (%) を y 座標として平面上にプロットした [1]. 右下がりの傾向が見て取れるので, 直線的関係があるものとして解析してみよう. 32 ($= n$) 人の (体重, 増加率) を $\{(x_i, y_i) \mid i = 1, 2, \ldots, n\}$ (**教師データ**) とおく. 増加率を出生時の体重で説明するため次の直線的関係 (**線形単回帰モデル**) を仮定する.

$$y_i = \beta_0 + \beta_1 x_i + \epsilon_i, \quad i = 1, 2, \ldots, n. \tag{1}$$

ここで β_0, β_1 は**回帰係数**と呼ばれる全データに共通する未知定数を表し, ϵ_i は**誤差**と呼ばれ, y_i のモデルからのずれをあらわす. 体重の増加率 y_i を**目的変数**, 出生時の体重 x_i を**説明変数**と呼ぶ. なお “線形” は平均構造が説明変数の既知関数の一次結合で与えられることを表すだけであり, $y_i = \beta_0 + \beta_1 \log x_i + \epsilon_i$ も線形モデルである.

未知の回帰係数 β_0, β_1 を最小 2 乗法で推定することにしよう. 誤差の 2 乗和:

$$Q(\boldsymbol{\beta}) \equiv \sum_{i=1}^{n} (y_i - \beta_0 - \beta_1 x_i)^2$$

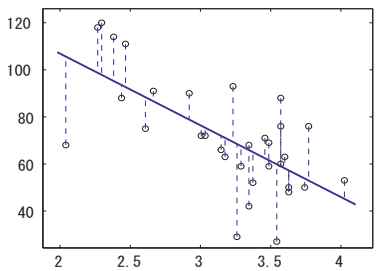


図 1: 新生児の体重 (Kg) と 70 日から 100 日後の体重の増加率 (%), $n = 32$

を最小にする母数を見つける. ただし $\boldsymbol{\beta} = (\beta_0, \beta_1)^T$ は**回帰係数ベクトル**である. $Q(\boldsymbol{\beta})$ は下に凸の関数なので, 極値を与える点が解となる. 偏微分により次の正規方程式を得る.

$$\frac{\partial Q}{\partial \beta_0} = -2n(\bar{y} - \beta_0 - \beta_1 \bar{x}) = 0, \tag{2}$$

$$\frac{\partial Q}{\partial \beta_1} = -2\sum_{i=1}^{n} x_i(y_i - \beta_0 - \beta_1 x_i) = 0. \tag{3}$$

ただし $\bar{x} = \sum_{i=1}^{n} x_i/n$, $\bar{y} = \sum_{i=1}^{n} y_i/n$ である. 連立方程式 (2), (3) の解 (**最小 2 乗解**) は,

$$\widehat{\boldsymbol{\beta}} \equiv \begin{pmatrix} \widehat{\beta}_0 \\ \widehat{\beta}_1 \end{pmatrix} = \begin{pmatrix} \bar{y} - \widehat{\beta}_1 \bar{x} \\ \dfrac{s_{xy}}{s_{xx}} \end{pmatrix} \tag{4}$$

と求められる. ただし $s_{xy} = \sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})$, $s_{xx} = \sum_{i=1}^{n}(x_i - \bar{x})^2 > 0$ を表す.

もし単回帰モデル (1) の誤差 ϵ_i が平均 0, 分散 σ^2 の確率分布に独立に従うなら, (4) 式の推定量 $\widehat{\boldsymbol{\beta}}$ は平均ベクトル $\boldsymbol{\beta}$, 分散共分散行列 $\sigma^2 D_1$ の分布に従う. ただし

$$D_1 = \frac{1}{s_{xx}} \begin{pmatrix} \dfrac{s_{xx}}{n} + \bar{x}^2 & -\bar{x} \\ -\bar{x} & 1 \end{pmatrix}. \tag{5}$$

なお推定量 $\widehat{\boldsymbol{\beta}}$ の分散共分散行列 $\sigma^2 D_1$ は線形不偏推定量のなかで正定値行列の意味で最小である.

さらに誤差が正規分布 $N(0, \sigma^2)$ に従うと仮定できるなら, $\widehat{\boldsymbol{\beta}}$ は 2 変量正規分布に従う. また誤差の推定量 $\widehat{\epsilon}_i = y_i - \widehat{\beta}_0 - \widehat{\beta}_1 x_i$ の 2 乗和 $s_e \equiv \sum_{i=1}^{n} \widehat{\epsilon}_i^2$ (**残差平方和**) はカイ 2 乗分布に従う. すなわち次が成立する.

$$\widehat{\boldsymbol{\beta}} \sim N_2(\boldsymbol{\beta},\ \sigma^2 D_1),\ s_e \sim \sigma^2 \chi^2_{n-2}. \tag{6}$$

また $\widehat{\boldsymbol{\beta}}$ と s_e は独立となる. なお一般の m 次元正規分布 $N_m(\boldsymbol{\mu},\ \Sigma)$ の確率密度関数は次で与えられる.

$$\psi(\boldsymbol{x}|\boldsymbol{\mu}, \Sigma) = (2\pi)^{-m/2}|\Sigma|^{-1/2} \exp\left\{-(\boldsymbol{x} - \boldsymbol{\mu})^T \Sigma^{-1} (\boldsymbol{x} - \boldsymbol{\mu})/2\right\} \tag{7}$$

ただし $\boldsymbol{\mu}$ は平均ベクトル, Σ は分散共分散行列を表す.

(5), (6) によって $\boldsymbol{\beta}$ に関する**信頼区間や有意性検定**が t 分布を用いて可能となる. 例えば傾き β_1 の有意性は, 統計量 $\widehat{\beta}_1 \sqrt{s_{xx}} \Big/ \sqrt{s_e/(n-2)}$ を自由度 $n-2$ の t 分布で検定すればよい. 個々の残差については, $\widehat{\epsilon}_i \Big/ \sqrt{1 - h_{ii}} \Big/ \sqrt{s_e/(n-2)}$ の分布が同じ自由度の t 分布で近似できることでチェックできる ($h_{ii} \equiv 1/n + (x_i - \bar{x})^2/s_{xx}$).

なお単回帰モデル (1) の評価基準として, 予測値 $\widehat{y}_i \equiv \widehat{\beta}_0 + \widehat{\beta}_1 x_i$ が実測値 y_i にどれだけ近いかを見るため, 次の**決定係数** (y_i と $\widehat{y}_i$ の相関係数の 2 乗) を用いる.

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_i - \widehat{y}_i)^2}{\sum_{i=1}^{n}(y_i - \bar{y})^2}. \tag{8}$$

R^2 は 0 以上 1 以下の値をとり, 1 に近いとデータに対するモデルの当てはまりが良いことを表す.

数値例 (新生児の体重増加率)

図 1 で推定された回帰直線は $y = 167.8 - 30.48x$ であり, 新生児の体重が 100g 重いと体重増加率は 3%程度減る傾向があることを意味する. 各観測値から伸びる線分は残差を, 線分と回帰直線の交点の y 座標は予測値を表す. この場合, 回帰係数は両者とも高度に有意であり, 決定係数は 0.4465 であった. なお説明変数 x_i はそのままで, 目的変数 y_i を体重増加率から 70 日から 100 日後の体重に変更したとき, 新しい単回帰モデルの決定係数は 0.4102 と下がる. よって増加率を目的変数とした現在のモデルの方が優れていることがわかる.

2 線形重回帰分析と有意性検定

前節の例では, 目的変数 (体重の増加率) に関連する変数として, 体重のほかに懐妊日数も考えられる. このように複数 (多重) の説明変数を用いて目的変数を説明する解析が**重回帰分析**である.

第 i 番目のサンプルの目的変数を y_i とし, それに関連すると思われる p 個の説明変数を $x_{i1}, \ldots, x_{ip}$ とする. 両者に次の線形回帰モデルが成立していると仮定する.

$$y_i = \beta_0 + \beta_1 x_{i1} + \cdots + \beta_p x_{ip} + \epsilon_i, \quad i = 1, \ldots, n. \tag{9}$$

特に $p = 1$ とおけば, 単回帰モデルに帰着する. さて重回帰分析では, ベクトルと行列を用いると議論の見通しが良くなる. そこで目的変数を観測したベクトル $\boldsymbol{y}$, 説明変数からなる**計画行列** X, **説明変数ベクトル** $\boldsymbol{\beta}$, **誤差ベクトル** $\boldsymbol{\epsilon}$ を次で定義する.

$$\boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \quad X = \begin{pmatrix} 1\, x_{11} \cdots x_{1p} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ 1\, x_{n1} \cdots x_{np} \end{pmatrix} : n \times (p+1), \quad \boldsymbol{\beta} = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_p \end{pmatrix} : (p+1) \times 1, \quad \boldsymbol{\epsilon} = \begin{pmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{pmatrix} \tag{10}$$

ただし, X のランク (階数) は $p+1$ ($\leqq n$) と仮定する. 観測されているものは $\boldsymbol{y}$ と X であり, 回帰係数ベクトル $\boldsymbol{\beta}$ は未知である. なお誤差ベクトルの各成分は独立に $N(0, \sigma^2)$ に従うと仮定する.

重回帰モデル (9) の全標本についてのベクトル表示は次で与えられる.

$$\boldsymbol{y} = X\boldsymbol{\beta} + \boldsymbol{\epsilon}, \quad \boldsymbol{\epsilon} \sim N_n(\mathbf{0}, \sigma^2 I). \tag{11}$$

単回帰と同様, 最小 2 乗法により回帰係数ベクトルを推定しよう. 誤差の 2 乗和を

$$Q(\boldsymbol{\beta}) = \sum_{i=1}^{n}(y_i - \beta_0 - \beta_1 x_{i1} - \cdots - \beta_p x_{ip})^2 = \sum_{i=1}^{n}\epsilon_i^2 = \boldsymbol{\epsilon}^T\boldsymbol{\epsilon} = (\boldsymbol{y} - X\boldsymbol{\beta})^T(\boldsymbol{y} - X\boldsymbol{\beta})$$

と定義する. $Q(\boldsymbol{\beta})$ を $\boldsymbol{\beta}$ の各成分で偏微分して, 0 とおいた連立方程式をベクトル表示すると, 一般の場合の正規方程式:

$$\partial Q(\boldsymbol{\beta})/\partial\boldsymbol{\beta} = -2X^T\boldsymbol{y} + 2X^TX\boldsymbol{\beta} = \mathbf{0}_{p+1} \tag{12}$$

を得る. 方程式 (12) は多変量正規分布に従う次の最小 2 乗解を持つ.

$$\widehat{\boldsymbol{\beta}} = D_pX^T\boldsymbol{y} \sim N_{p+1}(\boldsymbol{\beta},\ \sigma^2 D_p), \tag{13}$$

$$D_p = (X^TX)^{-1}\colon (p+1)\times(p+1). \tag{14}$$

この推定量により $\boldsymbol{y}$ を予測したもの $\widehat{\boldsymbol{y}} \equiv X\widehat{\boldsymbol{\beta}}$ を**予測ベクトル**と呼ぶ. また推定した誤差ベクトル $\widehat{\boldsymbol{\epsilon}} \equiv \boldsymbol{y} - X\widehat{\boldsymbol{\beta}}$ を**残差ベクトル**, その 2 乗和 $s_e \equiv \widehat{\boldsymbol{\epsilon}}^T\widehat{\boldsymbol{\epsilon}}$ を**残差平方和**と呼ぶ. それぞれの確率分布は退化した多次元正規分布および自由度 $n-p-1$ のカイ 2 乗分布に従う.

$$\widehat{\boldsymbol{\epsilon}} \sim N_n(\mathbf{0}, \sigma^2(I-H)), \quad s_e \sim \sigma^2\chi^2_{n-p-1}. \tag{15}$$

ただし $H \equiv XD_pX^T\colon n\times n$. また $\widehat{\boldsymbol{\beta}}$ と s_e は独立である. よって回帰係数 β_j の有意性は行列 D_p の (j,j) 成分 d_{jj} を用いて,

$$\frac{\widehat{\beta}_j/\sqrt{d_{jj}}}{\sqrt{s_e/(n-p-1)}} \sim t_{n-p-1} \tag{16}$$

により検定できる ($j = 0, 1, \ldots, p$). また個々の残差 $\widehat{\epsilon}_i$ の大きさは, 基準化した残差 $\widehat{\epsilon}_i/\sqrt{1-h_{ii}}\,\big/\sqrt{s_e/(n-p-1)}$ の分布が自由度 $n-p-1$ の t 分布に近いことを利用して診断できる. なお h_{ii} は行列 H の (i,i) 成分を表す.

回帰分析は多くの場合, 誤差について等分散性, 独立性, 正規性を仮定して解析される. そこで基準化した残差をプロットし, モデルや個々のデータの妥当性を吟味する必要がある (**回帰診断**).

3 モデルの評価と説明変数の選択

重回帰の場合もモデルの良さの評価基準として, $p+1$ 個の説明変数に基づく予測ベクトル $\widehat{\boldsymbol{y}} = X\widehat{\boldsymbol{\beta}}$ を用いた (8) 式と同様の決定係数 R^2 が用いられる. しかし R^2 は説明変数を追加すれ

ば必ず大きくなるので, 説明変数の選択には役立たない. そこで各項の自由度を考慮した次の**自由度調整済み決定係数**が説明変数の選択に用いられる.

$$R_*^2 = 1 - \frac{\sum_{i=1}^n (y_i - \widehat{y}_i)^2/(n-p-1)}{\sum_{i=1}^n (y_i - \bar{y})^2/(n-1)} : \text{自由度調整済み決定係数} \tag{17}$$

一方, 統計モデルを評価するための代表的な指標として **赤池情報量規準 AIC** (Akaike Information Criterion) があり, モデルに基づく期待対数尤度の不偏推定量として提案された. BIC (Bayesian Information Criterion) もよく似た表現となる. 未知パラメータ $\boldsymbol{\theta}$ で記述される統計モデルに対して, n 個の標本に基づく最尤推定量を $\widehat{\boldsymbol{\theta}}$ としたとき, AIC (BIC) は最大尤度 $L(\widehat{\boldsymbol{\theta}})$ を用いて次の値でモデルの損失を評価する.

$$\begin{aligned} \mathrm{AIC} &= -2\log L(\widehat{\boldsymbol{\theta}}) + 2 \times \dim \widehat{\boldsymbol{\theta}} \quad \Longrightarrow \quad \text{最小} \\ \mathrm{BIC} &= -2\log L(\widehat{\boldsymbol{\theta}}) + \log n \times \dim \widehat{\boldsymbol{\theta}} \quad \Longrightarrow \quad \text{最小} \end{aligned}$$

これを最小にするモデルが選ばれる.

(11) 式で与えられる重回帰モデルの AIC を計算してみよう. 未知母数 $\boldsymbol{\theta}$ は $(\boldsymbol{\beta}, \sigma^2)$ であり, 尤度関数は (7) 式を用いて $L(\boldsymbol{\beta}, \sigma^2) = \psi(\boldsymbol{y}|X\boldsymbol{\beta}, \sigma^2 I)$ で与えられる. この尤度関数を最大にする最尤推定量は $\widehat{\boldsymbol{\beta}} = D_p X^T \boldsymbol{y}$, $\widehat{\sigma}^2 = s_e/n$ であり, これを尤度関数に代入して最大尤度 $L(\widehat{\boldsymbol{\beta}}, \widehat{\sigma}^2) = (2\pi)^{-n/2}\widehat{\sigma}^n \exp(-n/2)$ が得られる. よって $-2\log L(\widehat{\boldsymbol{\beta}}, \widehat{\sigma}^2) = n\log(2\pi e) + n\log\widehat{\sigma}^2$ から**重回帰モデルの AIC や BIC** は次で得られる.

$$\begin{aligned} \mathrm{AIC} &= n\log(2\pi e) + n\log\widehat{\sigma}^2 + 2(p+2) \quad \Longrightarrow \text{ 最小 } \left(\widehat{\sigma}^2 = s_e/n\right) \\ \mathrm{BIC} &= n\log(2\pi e) + n\log\widehat{\sigma}^2 + (p+2)\log n \quad \Longrightarrow \text{ 最小} \end{aligned}$$

ただし $p+2$ は未知母数の数 (回帰係数と分散) を表す. モデルが複雑になれば (手持ちのデータへのフィットを改善すれば) $\widehat{\sigma}^2$ は小さくなるが, 説明変数の数 p が大きくなるという**トレードオフ**の関係がある. AIC は手持ちのデータへのフィットではなく, **将来の値を適切に予測**することができるかを評価している.

AIC (BIC) で最適モデルを探そうとすると, 2^p 通りのモデルについて情報量基準値を計算し, 最小値を与えるモデルを求める必要がある. この探索は $p = 20$ 以上では現実的ではない. モデル探索候補を減らすためには, 変数増加法, 変数減少法, 変数増減法等が用いられる.

なお n が大きいとき, AIC は大きいモデルを選択する傾向がある. そのため真のモデルを漸近的に選ぶ BIC が用いられることがある. 両者の比較は, 全教師データを教師用とテスト用の 2 つの集合に分割し, 教師用データで選んだ最適モデルでテスト用データに適応することで可能である.

相関の高い説明変数を同時に用いた回帰モデルは, $X^T X$ が特異行列に近くなる. そのため, 逆行列が大きくなり推定が不安定になる (**多重共線**). また n より p が大きい場合は $X^T X$ は特異行列となるため母数推定そのものが不可能となり, 説明変数の選択が必須である.

LASSO (Least Absolute Shrinkage and Selection Operator [6]) は推定母数の縮小と選択を

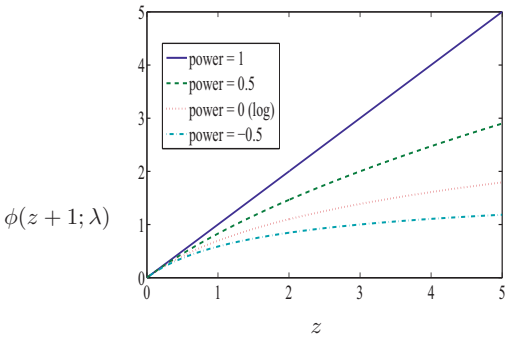


図 2: 非負値の巾変換 ($\lambda =$ power)

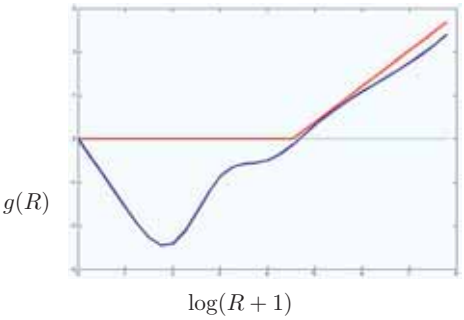


図 3: 森林被覆率に対する起伏量 R の影響
赤: パラメトリックモデル, 青: 自然 3 次スプライン

同時に行う推定法であり, 下記の目的関数を最小にすることで得られる.

$$\sum_{i=1}^{n}(y_i - \beta_0 - \beta_1 x_{i1} - \cdots - \beta_p x_{ip})^2 + \lambda \sum_{j=1}^{p} |\beta_j| : \text{Lasso} \tag{18}$$

$$\sum_{i=1}^{n}(y_i - \beta_0 - \beta_1 x_{i1} - \cdots - \beta_p x_{ip})^2 + \lambda \sum_{j=1}^{p} w_j|\beta_j| : \text{Adaptive Lasso} \tag{19}$$

ここで $\lambda > 0$, $w_1 > 0, \ldots, w_p > 0$ はチューニングパラメータである. (18), (19) 式で与えられる目的関数はオーバーフィットに対する罰則項を追加した尤度関数に由来する. Lasso 等は**変数選択の機能を有する**, すなわちいくつかの β_j がゼロと推定されるため, 特に p が大きいときに有用である.

4 回帰モデルの発展

回帰モデルを実データに適応するとき, 前述のモデルがそのまま使えることは多くはない. そのため良いモデルを得るための様々な工夫が必要であり, いくつかを簡単に紹介する.

(1) 目的変数や説明変数の巾変換
正の目的変数に対して, (a) 説明変数の線形性を高める, (b) 誤差分布が正規分布に近くなるようにする等のモデル改良のために次の巾変換を考えることがある.

$$\phi(z;\lambda) = \begin{cases} \log z & \lambda = 0 \text{ のとき}, \\ \dfrac{z^\lambda - 1}{\lambda} & \lambda \neq 0 \text{ のとき}. \end{cases} \tag{20}$$

また説明変数の効果が目的変数に対して直線的ではない場合にも巾変換を考える.

図 2 は $\phi(z+1;\lambda)$ が λ の正負によらず $z \geqq 0$ の単調増加関数であることを表す. $\lambda < 0$ なら対数関数よりゆっくり増加することがわかる. なお目的変数を変換した場合の AIC

等による評価には, 変換のヤコビアンが必要となる.

(2) 平均構造の基底関数展開

ある説明変数の目的変数に及ぼす影響が非線形である場合, その関数型が既知であれば**非線形回帰モデル**を適用すればよい. 非線形であるとだけわかっている場合は, 基底関数展開で推定する方法がある. (GAM, Generalized Additive Model [4]). 下記の例は x_1 による効果を 3 通りに表現している線形モデルである.

$$\mathrm{E}(y|\boldsymbol{x}) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_p x_p$$

$$\mathrm{E}(y|\boldsymbol{x}) = \beta_0 + \beta_{11} x_1 + \beta_{12} x_1^2 + \cdots + \beta_{1q} x_1^q + \beta_2 x_2 + \cdots + \beta_p x_p$$

$$\mathrm{E}(y|\boldsymbol{x}) = \beta_0 + \beta_{11} b_{11}(x_1) + \beta_{12} b_{12}(x_1) + \cdots + \beta_{1q} b_{1q}(x_1) + \beta_2 x_2 + \cdots + \beta_p x_p$$

上から順に, 通常の回帰モデル, 多項式回帰モデル, 既知の基底関数 $b_{11}(\cdot), \ldots, b_{1q}(\cdot)$ (例: x^2, $\log x$, $\sin x$) を用いた基底展開による回帰モデルである. $\mathrm{E}(y|\boldsymbol{x})$ は説明変数 $\boldsymbol{x}$ が与えられたときの目的変数の期待値を表す.

図 3 は基底関数展開の実例である [12]. ある変数の定義域を 8 区間にわけ, 各区間で 3 次多項式を考え (区分的多項式), それをスムースに繋げた 3 次以下の多項式からなる自然 3 次スプライン (基底関数) により推定した平均曲線である. 基底関数展開により説明変数の大きさによる効果の違い (単調な効果ではない) を検出できている.

(3) 誤差分散のモデル化

誤差の標準偏差 σ を一定として考えてきたが, σ も説明変数ベクトル $\boldsymbol{x}$ の関数として推定する場合もある (GLM, Generalized Linear Model [3]).

$$\sigma = \exp\bigl(\gamma_0 + \boldsymbol{\gamma}^T \boldsymbol{x}\bigr)$$

もちろん平均構造も $\boldsymbol{x}$ の関数として同時に推定する. $\boldsymbol{\gamma} = \mathbf{0}$ のときは分散一定のモデルである.

(4) ランダム効果モデル

いままでのモデルでは, 説明変数の効果はある関数で表現されることが前提であった. ここで血糖を下げる薬を患者に投与する場合を考える. 特定の患者に投与しても日によってその効果は一定ではない. もちろん他の患者に投与すれば, 異なる薬効が得られるであろう. しかしそれぞれの効果を細かく推定できるほどのデータが無いのが普通である. そこで説明変数を, 固定効果を持つ説明変数群とランダム効果を持つ説明変数群にわけて次のモデルを考えることがある.

$$\begin{aligned} \boldsymbol{y} &= X_1 \boldsymbol{\beta}_1 + X_2 \boldsymbol{\beta}_2 + \boldsymbol{\epsilon} \quad \bigl(\boldsymbol{\beta}_1 \sim N_q(H\boldsymbol{\gamma}, \tau^2 D), \quad \boldsymbol{\epsilon} \sim N_n(\mathbf{0}, \sigma^2 I)\bigr) \\ &\sim N_n(X_1 H \boldsymbol{\gamma} + X_2 \boldsymbol{\beta}_2, \ \tau^2 X_1 H D H^T X_1^T + \sigma^2 I) \end{aligned}$$

つまり $\boldsymbol{\beta}_1$ に対応する説明変数はランダム効果を持つというモデルである．ここで H: $q \times r$ は既知行列, $p \geqq q \geqq r$, D: $q \times q$ は既知正定値行列である．よって特殊な分散共分散構造を持つ回帰モデルが得られる．最尤法により未知母数 $\boldsymbol{\gamma}$: $r \times 1$, $\tau^2 \geqq 0$, $\sigma^2 > 0$ の推定, および AIC, BIC によるモデル評価が可能である．なお $\tau = 0$ なら通常の固定効果モデルに帰着する．

(5) 実験計画

説明変数を自由に設定できる物作りの現場では, なるべく少ない実験回数で安定した回帰モデルを推定したい．そこで n 回の実験で回帰モデルが推定できたとする．次に実験可能領域で目的変数の予測分散が最大となる点を求め, そこで追加実験を行う．これを逐次的に行う方法が考えられる．実験点 $\boldsymbol{x}$ が与えられれば, そこでの予測分散は $\sigma^2 \boldsymbol{x}^T (X^T X)^{-1} \boldsymbol{x}$ で与えられる．また実験点を逐次的に追加するときの予測分散は容易に求めることができる．なお追加実験点の探索には種々の最適化法が用いられる [10].

(6) 局所的な線形モデルのグローバル化

LOLIMOT (LOcal LInear MOdel Tree) は説明変数が定義される領域をいくつかに分割し, それぞれの領域で推測した回帰モデルに重みを付けて統合し, グローバルな予測を行う手法である [7]. LOLIMOT を導くには 1) 領域の分割数の決定, 2) 各領域の設定, 3) 各領域でのモデル選択, 4) 各モデルへの重み付け等の相互に関連する細かいチューニングが必要となる．

(7) 時系列データへの応用

時刻 t で観測された時系列データ $\{(\boldsymbol{x}_t, y_t) \mid t = 1, \ldots, T\}$ であれば,

$$y_t = \alpha_0 + \sum_{i=1}^{u} \alpha_i y_{t-i} + \sum_{j=1}^{p} \sum_{k=1}^{v_j} \beta_{jk} x_{j,t-k} + \epsilon_t, \quad t = \max\{u, v_1, \ldots, v_p\} + 1, \ldots, T$$

と過去の目的変数を回帰式に追加する (自己回帰) ことができる (ARX model, AutoRegressive model with eXogenous variables)．このモデルの推定には, 説明変数の選択と同時に時間遅れの次数 $u, v_1, \ldots, v_p$ も選択する必要があり, モデル候補が格段に増える．より一般のモデルに状態空間モデル (state-space model) がある．

(8) 重み付き最小 2 乗法

通常の回帰モデルでは, どの説明変数における目的変数でも一様に良い予測値を得ることが暗黙のうちに要請される．一方では目的変数が大きいときに, より高精度に予測したいケースもありうる．たとえばベルトコンベアで, ベルトの張力が閾値を超える数秒前に警告を発し, ベルトの破断を防ぐ場合がある [9]. この設定では張力に応じた重みを定義した平方和を最小にする必要がある．この推定法は等分散の独立な正規誤差を持つと仮定した場合には最尤法ではない．そのため AIC を一般化した GIC [5] を用いる必要がある．

(9) モデル平均化法

回帰モデルの候補 $M_1, \ldots, M_m$ が与えられているとする. 通常のモデル選択は候補モデルのなかから, ある規準で最適なモデルを唯一選ぶ. モデル平均化法では, 各モデルの情報量規準値に応じた重み付き和で予測する手法である [2]. たとえば AIC を用いた目的変数の予測値は次で定義される.

$$\widehat{y} = \sum_{i=1}^{m} w_i \widehat{y}_i, \quad w_i = \exp(-\mathrm{AIC}_i/2) \Big/ \sum_{j=1}^{m} \exp(-\mathrm{AIC}_j/2)$$

AIC_i はモデル M_i の AIC, $\widehat{y}_i$ は説明変数 $\boldsymbol{x}$ が与えられたときの M_i による予測値を表す. つまり AIC が良い (小さい) モデルには, それによる予測値に大きな重みをつけた加重平均による予測値を得る手法である. これにより安定した予測を目指している.

(10) 時空間データの回帰モデル

各地域ごとの降水量についての異なる時刻で観察した時空間データは, 時間的および空間的に相関を持っている. このような時空間データについての回帰モデルは, 誤差に時間的空間的相関を取り入れたモデル化により, モデルの予測能力を飛躍的に改善することができる. ただ同時分布が多次元正規分布ではないときの母数推定は容易ではない. しかし回帰モデルの平均構造に近傍の説明変数を取り入れた誤差独立を持つ簡易モデルでも, 旧来のモデルをはるかにしのぐ場合がある [8]. このように時空間情報を適切に確率モデルに取り込むことにより良いモデルが得られる.

(11) ロジスティック回帰分析

目的変数が連続値を取る場合の回帰分析を考えてきたが, 2 通りの値しかとらない場合にはロジスティック回帰が用いられる. たとえば説明変数 $\boldsymbol{x}$ を持つ人が肺がんを発症するか否か ($y = 0, 1$) を判定する問題を考える. 発症するかしないかの対数オッズ比 (ロジット) に対して, 次の線形回帰モデルを仮定する.

$$\log\left\{\frac{\Pr(y=1 \mid \boldsymbol{x})}{\Pr(y=0 \mid \boldsymbol{x})}\right\} = \beta_0 + \boldsymbol{\beta}^T \boldsymbol{x}$$

つまりベルヌ―イ分布の成功確率 $\Pr(y=1 \mid \boldsymbol{x}) = \{1 + \exp(-\beta_0 - \boldsymbol{\beta}^T \boldsymbol{x})\}^{-1}$ に対するモデル化であり, 最尤法による母数推定, 回帰係数の有意性検定や説明変数の選択が可能となる. また説明変数の基底展開も考察できる [11]. さらに目的変数の取り得る値が 3 群以上の多項ロジスティック回帰モデルも提案されている.

(12) Zero-Inflated 回帰分析

降水量を統一的に理解する確率モデルには, 降水ゼロの確率および降水があったときの正の実数値上で定義された連続分布が必要となる. そこで気象条件 $\boldsymbol{x}$ のときの降水量 $y \geqq 0$ の確率モデルとして $\Pr(y=0|\boldsymbol{x}) = \Delta(\boldsymbol{x})$ を許容した Zero-Inflated モデル [8] を考える.

$$p(y|\boldsymbol{x}) = \Delta(\boldsymbol{x})\delta(y) + \{1 - \Delta(\boldsymbol{x})\}\, q(y|\boldsymbol{x}) I(y > 0)$$

ただし $\delta(\cdot)$ は Dirac のデルタ関数, $q(y|\boldsymbol{x})$ は正の実数値上の確率密度関数, $I(\cdot)$ は命題の真偽に応じてゼロまたは 1 を取る定義関数である. なおゼロ インフレート確率に対し $\Delta(\boldsymbol{x}) = \{1 + \exp(\alpha_0 + \boldsymbol{\alpha}^T\boldsymbol{x})\}^{-1}$ とロジスティック回帰が可能である.

上記以外にも非線形回帰分析, 多変量回帰分析をはじめ回帰分析を発展させた多くの理論が生み出され, 応用されている. 最新の文献や公開されているソフトウェアについては, ウェブで検索してほしい.

回帰分析の “回帰”は Francis Galton (1822–1911) が発見した “回帰直線は平均に近づく (戻る, 回帰する)” という経験則に由来する. 21 世紀になった今でも, 回帰分析が統計学のホットな話題の一つであり続けていることは興味深い.

参考文献

[1] P. Armitage, G. Berry and J. N. S. Matthews (2002). *Statistical Methods in Medical Research* (Fourth Edition). Blackwell Publishing, Malden, USA.

[2] G. Claeskens and N. L. Hjort (2008). *Model Selection and Model Averaging*, Cambridge University Press, Cambridge, UK.

[3] Gamlss page (Generalized Additive Models for Location, Scale and Shape), `http://www.gamlss.org/`

[4] T. J. Hastie and R. J. Tibshirani (1990). *Generalized Additive Models*. Chapman and Hall, London, UK.

[5] S. Konishi and G. Kitagawa (2007). *Information Criteria and Statistical Modeling*, Springer, New York, USA.

[6] Lasso page. `http://www-stat.stanford.edu/~tibs/lasso.html`

[7] O. Nelles (2001). *Nonlinear System Identification*, Springer, New York, USA.

[8] R. Nishii and S. Tanaka (2012). Modeling and inference of forest coverage ratio using zero-one inflated distributions with spatial dependence. *Environmental and Ecological Statistics*, DOI 10.1007/s10651-012-0227-y.

[9] P. Qin and R. Nishii (2010). Selection of ARX models estimated by the penalized weighted least squares method, *Bulletin of Informatics and Cybernetics* **42**, 35–43.

[10] 小平 剛央, 中本 尊元, 小池 真人, 天野 浩平, 西井 龍映, 秦 攀 (2013). 逐次実験計画法の拡張による車体構造の複合領域最適化手法, 自動車技術会論文集 **44**(2) (2013 年 3 月発行予定).

[11] 小西 貞則 (2010). 多変量解析入門—線形から非線形へ—, 岩波書店.

[12] 宮田 大毅, 西井 龍映, 田中 章司郎 (2012). 森林被覆率の非線形回帰モデリング, 統計数理 **60**(1), 109–119.

信号検出と統計的モデル選択

二宮　嘉行
九州大学マス・フォア・インダストリ研究所

1　イントロ

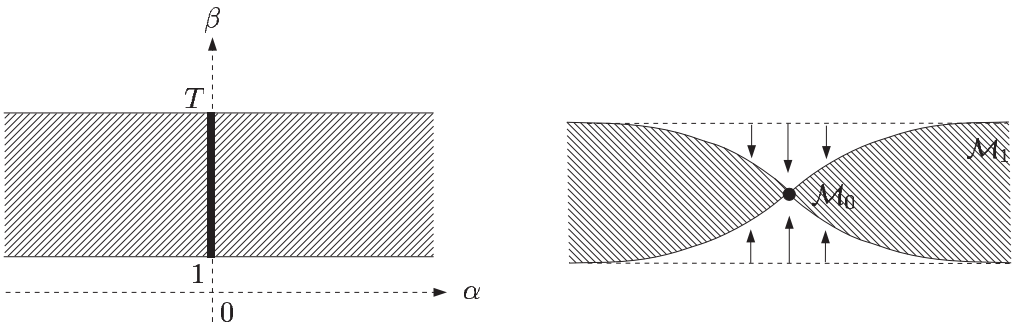
人間の脳のどこに熱さという刺激を感じる部位があるかを調べるための実験を考えよう．まず，ぬるいお湯と熱いお湯を用意する．そこに被験者の手を順に浸し，血流が早くなると色が濃く，遅くなると色が淡くなるような脳画像を撮る．ぬるいお湯に浸しているときの画像に比べ，熱いお湯に浸しているときの画像のある部分の色が「明らかに」濃ければ，その部分が熱さに関連する脳の部位といえるだろう．ここで問題となるのは，どのようなときに「明らかに」濃いといえるのかである．なぜなら，熱さを感じること以外でも，例えば体のバイオリズムや手を浸しているときの環境の変化などが血流を変化させるからである．つまり熱さを感じる部位でなかったとしても，半々の確率で熱いお湯のときの方が血流が早くなるからである．このような予測できない血流の偶然変動によって生じる画像の濃淡は，いわゆるノイズである．一方，熱さを感じたことによって生じる画像の濃淡は，「熱い」という情報を画像に伝達しているということで信号である．信号検出とは，画像の中に信号によるものと思われる濃淡があればそれを検出するというものであるが，その濃淡がノイズによるものかもしれないという難しさがこの問題にはある．そして，ここで必要となるのが統計学である．信号があるのか否かは統計的検定により調べることができ，信号の数は統計的モデル選択により選択することができる．ただし，信号モデルにはある特殊な性質があるためにそれらの適用には注意が必要であり，以下では特に統計的モデル選択に焦点を当ててそれを説明する．

2　信号モデルの識別不能性

上で述べたような設定のうちで最もシンプルなものを，数式を用いたモデルで説明していくことにする．まず，位置 t における画像の差のデータを y_t と記すことにする．画像ならば t は二次元か三次元ということになるが，ここでは簡単のため一次元としておく．この y_t に対し，

$$y_t = \alpha g_t(\beta) + \epsilon_t, \quad \epsilon_t \overset{\text{独立}}{\sim} \mathrm{N}(0, \sigma_0^2), \quad t = 1, \ldots, T \tag{1}$$

というモデルを考える．ここで，$\alpha g_t(\beta)$ は大きさが α で中心位置が β の信号を，ϵ_t はノイズを意味している．そして簡単のためノイズの分散 σ_0^2 と信号の形状 $g_t(\cdot)$ は既知とし，α と β



(a) (b)

図 1：信号モデルの幾何的表現

のみを未知のパラメータとしておく ($\alpha \in \mathbb{R}$, $1 \le \beta \le T$)．(1) より $\boldsymbol{y} = (y_1, \ldots, y_T)$ の確率分布（確率密度関数）は

$$f(\boldsymbol{y}|\alpha,\beta) = \Big(\frac{1}{\sqrt{2\pi\sigma_0^2}}\Big)^T \exp\Big[-\frac{1}{2\sigma_0^2}\sum_{t=1}^{T}\{y_t - \alpha g_t(\beta)\}^2\Big] \tag{2}$$

と書ける．そして信号モデル $\{f(\boldsymbol{y}|\alpha,\beta) \mid \alpha \in \mathbb{R},\ 1 \le \beta \le T\}$ を $\mathcal{M}_1$ と表すことにする．

$\mathcal{M}_1$ をパラメータ (α,β) の空間で表現してみると 図 1 (a) の斜線領域が得られるが，$\mathcal{M}_1$ をこのような斜線領域みたいなものだと思うのは果たして妥当だろうか．$\mathcal{M}_1$ には，$\alpha = 0$ とすると β の値によらず信号のないモデル $y_t = \epsilon_t$ になるという特徴がある．つまり $\beta^\dagger \neq \beta^\ddagger$ であっても $f(\boldsymbol{y}|0,\beta^\dagger)$ と $f(\boldsymbol{y}|0,\beta^\ddagger)$ は同じ確率分布になるのである．信号モデルでは，信号の大きさが 0 であれば当然信号の位置に関係なく同じ無信号モデルになる，というわけである．この無信号モデルを $\mathcal{M}_0 = \{f(\boldsymbol{y}|0,\beta) \mid 1 \le \beta \le T\}$ と表すと，これに属する確率分布は識別できないことから，$\mathcal{M}_1$ は $\mathcal{M}_0$ において識別不能性をもつという．図 1 (a) では $\mathcal{M}_0$ は太線で描かれているが，これは同じ確率分布を意味しているので一点で描かれるべきであり，つまり $\mathcal{M}_1$ は図 1 (b) のように縮退させて描かれるべきなのである．

この信号モデルを一般化する．データ $\boldsymbol{y}$ に対する確率分布の集合 $\mathcal{M}_1 = \{f(\boldsymbol{y}|\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}) \mid \boldsymbol{\alpha} \in \mathbb{R}^p,\ \boldsymbol{\beta} \in \mathbb{R}^q,\ \boldsymbol{\gamma} \in \mathbb{R}^r\}$ において，$f(\boldsymbol{y}|\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma})$ は $\boldsymbol{\alpha} = \boldsymbol{0}$ のときのみに限り確率分布 $f(\boldsymbol{y}|\boldsymbol{0},\boldsymbol{\beta},\boldsymbol{\gamma})$ となり，またこれは $\boldsymbol{\beta}$ によらないとする．このとき，$\mathcal{M}_1$ は $\mathcal{M}_0 = \{f(\boldsymbol{y}|\boldsymbol{0},\boldsymbol{\beta},\boldsymbol{\gamma}) \mid \boldsymbol{\beta} \in \mathbb{R}^q,\ \boldsymbol{\gamma} \in \mathbb{R}^r\}$ において識別不能性をもつといい，$\mathcal{M}_1$ は（$p=1, q=2, r=0$ とすれば）図 2 のように描かれる．$\mathcal{M}_0$ の近傍でみると $\mathcal{M}_1$ は錐とみなせることから，Dacunha-Castelle & Gassiat [3] は $\mathcal{M}_1$ を頂点 $\mathcal{M}_0$ の局所錐モデルとよんだ．ちなみに，通常 $\mathcal{M}_1$ は $(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma})$ とは異なるパラメータで表現されていることが多く，そのときに上記のような $(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma})$ を導くことを局所錐母数化という．

一方，$\alpha_1, \alpha_2 \in \mathbb{R}$ として

$$y_t = \alpha_1 + \epsilon_t, \quad \epsilon_t \overset{\text{独立}}{\sim} \mathrm{N}(0,\sigma_0^2), \quad t = 1, \ldots, T \tag{3}$$

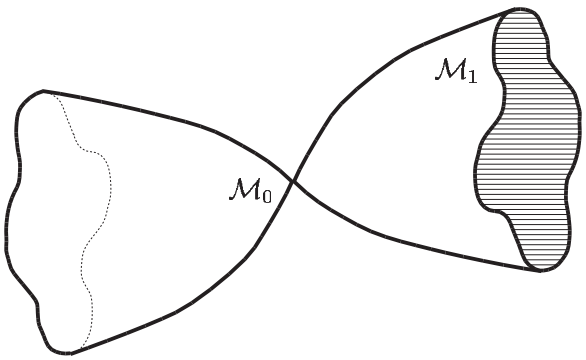


図 2：局所錐モデルの幾何的表現

や

$$y_t = \alpha_1 + \alpha_2 t + \epsilon_t, \quad \epsilon_t \overset{\text{独立}}{\sim} \mathrm{N}(0, \sigma_0^2), \quad t = 1, \ldots, T \tag{4}$$

というモデルを考えると，$\alpha_1 = 0$ あるいは $\alpha_1 = \alpha_2 = 0$ で表される確率分布は他の表現方法をもたない．つまり，これらのモデルは $\alpha_1 = 0$ あるいは $\alpha_1 = \alpha_2 = 0$ において識別不能性をもたないのである．一般化し，データ $\boldsymbol{y}$ に対する確率分布の集合 $\mathcal{M}_1 = \{g(\boldsymbol{y}|\boldsymbol{\alpha}, \boldsymbol{\gamma}) \,|\, \boldsymbol{\alpha} \in \mathbb{R}^p, \boldsymbol{\gamma} \in \mathbb{R}^r\}$ は，その部分集合 $\mathcal{M}_0 = \{g(\boldsymbol{y}|\boldsymbol{0}, \boldsymbol{\gamma}) \,|\, \boldsymbol{\gamma} \in \mathbb{R}^r\}$ において識別不能性をもたないとする．この $\mathcal{M}_1$ と $\mathcal{M}_0$ を $p = 1, r = 0$ あるいは $p = 2, r = 0$ としてパラメータ空間で表現すれば，つまり (3) あるいは (4) に対応するモデルを表現すれば，それぞれ図 3 (a) あるいは図 3 (b) のように描けることとなる．これらは縮退させる必要がないので，$\mathcal{M}_0$ の近傍でみれば $\mathcal{M}_1$ は直線あるいは平面とみなせる．

3　識別不能性をもつモデルにおける統計理論

識別不能性をもつモデルには通常の統計理論があてはまらないことをみるため，まずは通常の統計理論の一つを紹介する．いま，モデル $\mathcal{M}_0$ と $\mathcal{M}_1$ における最大対数尤度を $\hat{l}_0$ と $\hat{l}_1$ で表すことにすると，その差 $\hat{l}_1 - \hat{l}_0$ は $\mathcal{M}_0$ と $\mathcal{M}_1$ を比較する重要な指標とされ，その二倍を尤度比統計量という．前節の識別不能性をもたないモデルの表現を用いれば，これは

$$2\hat{l}_1 - 2\hat{l}_0 = \sup_{\boldsymbol{\alpha}, \boldsymbol{\gamma}} \{2 \log g(\boldsymbol{y}|\boldsymbol{\alpha}, \boldsymbol{\gamma})\} - \sup_{\boldsymbol{\gamma}} \{2 \log g(\boldsymbol{y}|\boldsymbol{0}, \boldsymbol{\gamma})\}$$

と書ける．この統計量に対し，以下の漸近的性質が古くから知られている．

定理 1 (Wilks [7]) $\mathcal{M}_0$ を含む $\mathcal{M}_1$ が $\mathcal{M}_0$ において識別不能性をもたず，また真の分布が $\mathcal{M}_0$ 内にあるならば，ある正則条件のもと，

$$\exists p \in \mathbb{N}; \quad \exists T \sim \chi^2(p); \quad 2\hat{l}_1 - 2\hat{l}_0 \overset{\mathrm{d}}{\to} T$$

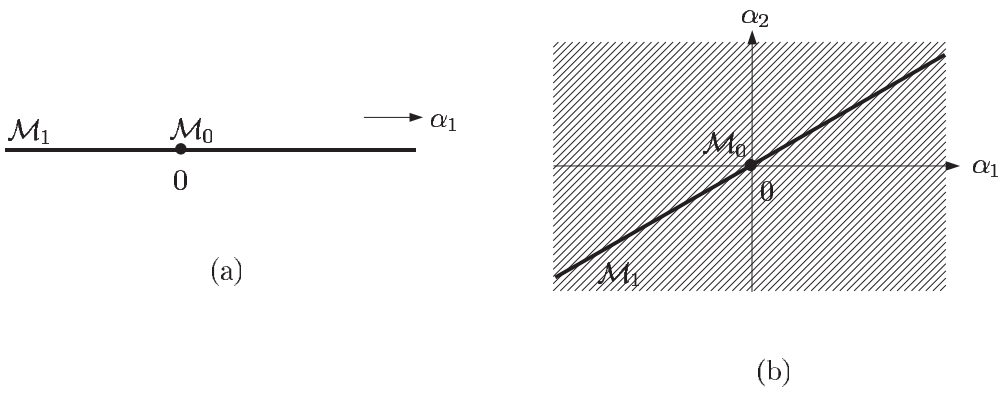


図 3：正則モデルの表現

が成立する．

ここで，$\chi^2(p)$ は自由度 p のカイ二乗分布を，$\stackrel{\mathrm{d}}{\to}$ は分布収束を意味している．この定理は，識別不能性をもたないモデルにおける確率分布が通常どんなものであっても尤度比統計量の漸近分布は同じタイプになる，ということを意味している．そのような現象の成立は，これが漸近的性質であることと真の分布が $\mathcal{M}_0$ の中にあることに起因する．漸近的性質なのでそれに関わるのは真の分布の近傍だけであり，その近傍ではどんな分布でもモデルは直線や平面のような超平面とみなせる，ということが効いているのである．ちなみに，それが直線ならば $\chi^2(1)$ が，平面ならば $\chi^2(2)$ が現れることになる．

一方，識別不能性をもつモデルにおいては，前節で紹介したように $\mathcal{M}_0$ の近傍でモデルは錐となるため，定理 1 は成立しない．前節の識別不能性をもつモデルの表現を用いれば，尤度比統計量は

$$2\hat{l}_1 - 2\hat{l}_0 = \sup_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}} \{2\log f(\boldsymbol{y}|\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma})\} - \sup_{\boldsymbol{\beta},\boldsymbol{\gamma}} \{2\log f(\boldsymbol{y}|\boldsymbol{0},\boldsymbol{\beta},\boldsymbol{\gamma})\}$$

と書け，定理 1 の代わりに以下が得られることになる．

定理 2 (Dacunha-Castelle & Gassiat [3]) $\mathcal{M}_0$ を含む $\mathcal{M}_1$ が $\mathcal{M}_0$ において識別不能性をもち，また真の分布が $\mathcal{M}_0$ 内にあるならば，ある正則条件のもと，

$$\exists p \in \mathbb{N};\quad \exists\{T_{\boldsymbol{\beta}} \sim \chi^2(p)\};\quad 2\hat{l}_1 - 2\hat{l}_0 \stackrel{\mathrm{d}}{\to} \sup_{\boldsymbol{\beta}} T_{\boldsymbol{\beta}}$$

が成立する．

$\boldsymbol{\beta}$ を固定すれば $\mathcal{M}_1$ は識別不能性をもたないモデルとなることと，$\boldsymbol{\beta}$ が未知のときの尤度比統計量は $\boldsymbol{\beta}$ を固定して得られる尤度比統計量の $\boldsymbol{\beta}$ に関する最大値であることから，この定理の成立が直感的に理解できる．

定理 1 や定理 2 に基づけば，データが $\mathcal{M}_0$ にしたがうという帰無仮説とデータが $\mathcal{M}_1 \setminus \mathcal{M}_0$ にしたがうという対立仮説を比較する統計的検定の結果（確率値）を評価することができるが，ここではその詳細に触れず，統計的モデル選択に焦点を当てる．統計的モデル選択とは，モデル候補 $\{\mathcal{M}^{(m)}\}$ からデータに基づいて適切なものを選ぶことであり，統計解析において不可欠な作業である．前節の識別不能性をもたないモデルに関連させていえば，

$$y_t = \sum_{j=0}^{m} \alpha_{j+1} t^j + \epsilon_t, \quad \epsilon_t \overset{\text{独立}}{\sim} \mathrm{N}(0, \sigma_0^2), \quad t = 1, \ldots, T \tag{5}$$

といういわゆる m 次多項式モデルを $\mathcal{M}^{(m)}$ とし，適切な次数 m を選択することが例として挙げられる．

統計的モデル選択において最も多く用いられる指標といえるものに情報量規準 AIC (Akaike [1]) がある．$\mathcal{M}^{(m)}$ における最大対数尤度と $\mathcal{M}^{(m)}$ のパラメータ数をそれぞれ $\hat{l}^{(m)}$ と $q^{(m)}$ とすれば，これは

$$\mathrm{AIC}_{\mathrm{formal}}^{(m)} = -2\hat{l}^{(m)} + 2q^{(m)} \tag{6}$$

という形で与えられ，これを最小にする $\mathcal{M}^{(m)}$ が最適なモデルとされる．ここで，後に識別不能性をもつモデルに対する AIC を再評価するため，(6) において $\mathrm{AIC}_{\mathrm{formal}}^{(m)}$ と表記している．$\mathcal{M}^{(m)}$ が識別不能性をもたないモデルであり，かつ真の分布が $\mathcal{M}^{(m)}$ 内にあれば，$\mathrm{AIC}_{\mathrm{formal}}^{(m)}$ は $\mathcal{M}^{(m)}$ 内のベストな分布と真の分布との Kullback-Leibler 距離 $\mathrm{KL}^{(m)}$（の二倍からある定数をひいたもの）の漸近不偏推定量となっている．したがって，$\mathcal{M}^{(m)}$ と $\mathcal{M}^{(m+1)}$ の比較のみに焦点を当てれば以下の性質が得られる．

命題 1 $\mathcal{M}^{(m)}$ を含む $\mathcal{M}^{(m+1)}$ が $\mathcal{M}^{(m)}$ において識別不能性をもたず，また真の分布が $\mathcal{M}^{(m)}$ 内にあるならば，ある正則条件のもと，$\mathrm{AIC}_{\mathrm{formal}}^{(m+1)} - \mathrm{AIC}_{\mathrm{formal}}^{(m)}$ は $2\mathrm{KL}^{(m+1)} - 2\mathrm{KL}^{(m)}$ の漸近不偏推定量となる．

真の分布が $\mathcal{M}^{(m)}$ 内あるいはその近くにあるとき，$\mathrm{AIC}_{\mathrm{formal}}^{(m+1)} - \mathrm{AIC}_{\mathrm{formal}}^{(m)}$ は命題 1 より $2\mathrm{KL}^{(m+1)} - 2\mathrm{KL}^{(m)}$ の良い推定量となっているため，この $\mathrm{AIC}_{\mathrm{formal}}$ に基づく選択は妥当といえる．一方，真の分布が $\mathcal{M}^{(m)}$ から離れたところにあるとき，$\mathrm{AIC}_{\mathrm{formal}}^{(m+1)} - \mathrm{AIC}_{\mathrm{formal}}^{(m)}$ は良い推定量になっていない．しかし，このケースでは $\mathcal{M}^{(m+1)}$ の当てはまり度といえる $\hat{l}^{(m+1)}$ が $\mathcal{M}^{(m)}$ の当てはまり度といえる $\hat{l}^{(m)}$ よりかなり大きくなるため，$\mathrm{AIC}_{\mathrm{formal}}^{(m+1)} - \mathrm{AIC}_{\mathrm{formal}}^{(m)}$ は通常 0 未満になる．そしてこれは $\mathcal{M}^{(m)}$ より $\mathcal{M}^{(m+1)}$ の方が妥当だという結果につながるので，問題は起こらないのである．以上より，$\mathrm{AIC}_{\mathrm{formal}}$ がうまく働く理由はこの命題が成り立つからであり，逆にこの命題が成り立たないときは $\mathrm{AIC}_{\mathrm{formal}}$ は妥当ではないといえる．

$\mathrm{AIC}_{\mathrm{formal}}^{(m+1)} - \mathrm{AIC}_{\mathrm{formal}}^{(m)}$ は，書き直せば $-2(\hat{l}^{(m+1)} - \hat{l}^{(m)}) + 2(q^{(m+1)} - q^{(m)})$ であり，尤度比統計量に関連したものである．このことから想像できるように，識別不能性のあるモデルにおいては命題 1 は成立せず，したがって $\mathrm{AIC}_{\mathrm{formal}}$ はうまく働かない．例えば前節の信号モデルを拡張した

$$y_t = \sum_{j=1}^{m} \alpha_j g_t(\beta_j) + \epsilon_t, \quad \epsilon_t \overset{\text{独立}}{\sim} \mathrm{N}(0, \sigma_0^2), \quad t = 1, \ldots, T \tag{7}$$

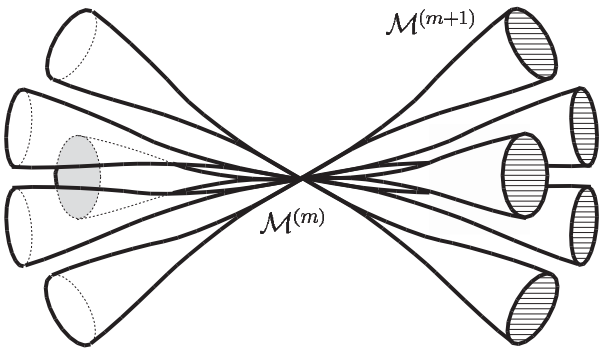


図 4：因子分析モデルの幾何的表現

といういわゆる m 信号モデルを $\mathcal{M}^{(m)}$ とすれば，$\mathcal{M}^{(m+1)}$ は $\mathcal{M}^{(m)}$ において識別不能性をもつため，$\mathrm{AIC}_{\mathrm{formal}}$ を使うことは妥当ではなくなる．

いま，m 信号モデルのような局所錐モデルの候補 $\{\mathcal{M}^{(m)}\}$ を考え，$\hat{l}^{(m)}$ はこの $\mathcal{M}^{(m)}$ のもとでの最大対数尤度とする．このとき，定理 2 より

$$\exists p^{(m)} \in \mathbb{N}; \quad \exists\{T_{\boldsymbol{\beta}}^{(m)} \sim \chi^2(p^{(m)})\}; \quad 2\hat{l}^{(m+1)} - 2\hat{l}^{(m)} \xrightarrow{\mathrm{d}} \sup_{\boldsymbol{\beta}} T_{\boldsymbol{\beta}}^{(m)}$$

が得られる．そしてこれに基づき，新たに AIC の再評価版を

$$\mathrm{AIC}_{\mathrm{proposed}}^{(m)} = -2\hat{l}^{(m)} + 2\sum_{j=1}^{m-1} \mathrm{E}\Big(\sup_{\boldsymbol{\beta}} T_{\boldsymbol{\beta}}^{(j)}\Big) \tag{8}$$

で与える．すると以下の命題が得られる．

命題 2 $\mathcal{M}^{(m)}$ を含む $\mathcal{M}^{(m+1)}$ が $\mathcal{M}^{(m)}$ において識別不能性をもち，また真の分布が $\mathcal{M}^{(m)}$ 内にあるならば，ある正則条件のもと，$\mathrm{AIC}_{\mathrm{proposed}}^{(m+1)} - \mathrm{AIC}_{\mathrm{proposed}}^{(m)}$ は $2\mathrm{KL}^{(m+1)} - 2\mathrm{KL}^{(m)}$ の漸近不偏推定量となる．

これより，$\mathrm{AIC}_{\mathrm{proposed}}$ は識別不能性をもつモデルをうまく選択してくれることが期待できる．ただし，(8) の中に現れる期待値の評価は，一般に困難である．

4　因子分析モデルへの適用

$\mathrm{AIC}_{\mathrm{proposed}}$ の有用性を確認するため，計量心理学において基本的なモデルとして用いられ，かつ識別不能性をもつモデルの典型例である因子分析モデルをここでは扱う．因子分析モデ

表 1：因子分析モデルに対する $\mathrm{AIC}_{\mathrm{proposed}}$ における期待値評価

$p-j$	4	5	6	7	8	9	10
$\mathrm{E}\Big(\max_{1\le\beta\le p-j} T_\beta^{(j)}\Big)$	6.4	8.5	10.5	12.4	14.2	16.0	17.8

ルとは，多変量のデータ $\{\boldsymbol{x}_i \in \mathbb{R}^p \mid 1 \le i \le n\}$ を数個の潜在的な因子で説明する確率モデルである．具体的には，データ $\boldsymbol{x}_i$ が

$$\boldsymbol{z}_i = (z_{i1}, \ldots, z_{im})' \overset{\text{独立}}{\sim} \mathrm{N}(\boldsymbol{0}, \mathrm{diag}(1, \ldots, 1)), \quad \boldsymbol{\epsilon}_i \overset{\text{独立}}{\sim} \mathrm{N}(\boldsymbol{0}, \mathrm{diag}(\psi_1, \ldots, \psi_p))$$

として

$$\boldsymbol{x}_i = \sum_{j=1}^{m} \boldsymbol{\lambda}_j z_{ij} + \boldsymbol{\epsilon}_i = (\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_m)\boldsymbol{z}_i + \boldsymbol{\epsilon}_i, \quad i = 1, \ldots, n \tag{9}$$

と書けるとき，これを p 変量 m 因子モデルという．本節では，これを $\mathcal{M}^{(m)}$ と書くことにし，因子数 m の選択問題を考える．ここで，$\boldsymbol{z}_i$ と $\boldsymbol{\epsilon}_i$ は i 番目のデータに対する m 個の因子を並べたベクトルとノイズであり，因子の未知係数である $\boldsymbol{\lambda}_j$ は因子負荷ベクトルとよばれる．これより $\mathcal{M}^{(m)}$ は

$$\boldsymbol{x}_i \overset{\text{独立}}{\sim} \mathrm{N}\Big(\boldsymbol{0}, \sum_{j=1}^{m} \boldsymbol{\lambda}_j \boldsymbol{\lambda}_j' + \mathrm{diag}(\psi_1, \ldots, \psi_p)\Big), \quad i = 1, \ldots, n \tag{10}$$

とも表現できる．

$m+1$ 因子モデル $\mathcal{M}^{(m+1)}$ は m 因子モデル $\mathcal{M}^{(m)}$ において識別不能性をもち，したがって図 2 で描いたように $\mathcal{M}^{(m)}$ の近傍で $\mathcal{M}^{(m+1)}$ は錐とみなせるわけだが，実はさらなる特徴がある．図 4 で描いたように，$\mathcal{M}^{(m)}$ の近傍において $\mathcal{M}^{(m+1)}$ は $m+1$ 個に分割されていて，かつ各々は縮退しているのである．そして，この特徴を利用すると以下の定理が得られる．

定理 3 (Ninomiya, Yanagihara & Yuan [6]) $\mathcal{M}^{(m)}$ が (10) で定義された因子分析モデルであり，パラメータ空間はコンパクトであることと $\boldsymbol{\lambda}_j \neq \boldsymbol{0}$ $(1 \le j \le m)$ を仮定する．このとき，(8) は $\chi^2(p-j-1)$ にしたがう $T_\beta^{(j)}$ $(1 \le \beta \le p-j)$ を用いて

$$\mathrm{AIC}_{\mathrm{proposed}}^{(m)} = -2\hat{l}^{(m)} + 2\sum_{j=1}^{m-1} \mathrm{E}\Big(\max_{1\le\beta\le p-j} T_\beta^{(j)}\Big) \tag{11}$$

の形に帰着する．

(11) の中の期待値は有限個のカイ二乗統計量の最大値に対するものであるため，その評価は困難ではない．例えばある評価式を用いれば表 1 のように評価でき，したがって容易に統計的モデル選択を行うことができる．

表 2 : Holzinger & Swineford [5] のデータへの AIC の適用

	$AIC_{proposed}$	AIC_{formal}	$AIC_{consistent}$
1 因子	2573.1	2589.4	2780.2
2 因子	2433.7	2419.2	2701.5
3 因子	2374.0	2329.7	**2699.5**
4 因子	**2372.4**	2299.3	2752.6
5 因子	2397.4	**2296.5**	2829.4
6 因子	2462.1	2303.1	2943.0

$AIC_{proposed}$ と AIC_{formal} を比較するため，Holzinger & Swineford [5] のデータにこれらを適用する．このデータは数え上げ・数字認識・文章補完・視覚認識など 24 種のテストの 145 人の得点であり，記憶・数学的能力・スピードなどといった因子の存在を期待される因子分析のベンチマークデータである．表 2 がその結果であり，参考のために Bozdogan [2] が提案した $AIC_{consistent}$ も比較の対象に含めている．各基準が異なる因子数を選択していることから，基準間の違いは小さくないことが確認できる．また，計量心理学者によれば 4 因子が最も合理的であるとされるため (Harman, 1976; p. 164)，その意味で $AIC_{proposed}$ の妥当性も確認できる．

参考文献

[1] Akaike, H. (1973). Information theory and an extension of the maximum likelihood principle. In Petrov, B. N. and Csaki, F. (Eds.), *2nd International Symposium on Information Theory*, 716–723, Budapest: Akademiai Kiado.

[2] Bozdogan, H. (1987). Model selection and Akaike's Information Criterion (AIC): The general theory and its analytical extensions. *Psychometrika*, 52, 345–370.

[3] Dacunha-Castelle, D. and Gassiat, E. (1997). Testing in locally conic models and application to mixture models. *ESAIM Probability and Statistics*, 1, 285–317.

[4] Harman, H. H. (1976). *Modern factor analysis* (3rd ed.). Chicago: The University of Chicago Press.

[5] Holzinger, K. J. and Swineford, F. (1939). A study in factor analysis: The stability of a bi-factor solution. *Supplementary Educational Monographs*, 48. Chicago: University Chicago Press.

[6] Ninomiya, Y., Yanagihara, H. and Yuan, K.-H. (2008). Selecting the number of factors in exploratory factor analysis via locally conic parameterization. *ISM Research Memorandum*, 1078.

[7] Wilks, S. S. (1938). The large-sample distribution of the likelihood ratio for testing composite hypotheses. *Annals of Mathematical Statistics*, 9, 60–62.

離散最適化
―ネットワークフローを中心に―

神山　直之
九州大学マス・フォア・インダストリ研究所

1　はじめに

幾つかの選択肢から最適なものを選ぶ意思決定問題は，実社会のあらゆる場面で現れる．例えば，可能な限り短い時間で決められた都市を回る問題や，可能な限り少ない人数で決められた仕事を完了することができるようなスケジュールを決定する問題などがその例といえよう．この様な意思決定問題を，数理モデルを通じ解決しようとする際に，強力な道具となる数学理論が最適化理論である．最適化問題とは，大雑把に言うなれば幾つかの制約を満たす解の候補の中から，与えられた目的関数を最小化もしくは最大化するものを見つける数学的問題である．特に，解の集合が離散的な構造を有する最適化問題を離散最適化問題と呼ぶ．

離散最適化の研究は，数学の一分野であるグラフ理論や計算機科学の一分野である計算量理論，そして経済学の一分野であるゲーム理論といった様々な分野と深い関わりを持っており，扱う問題は非常に多岐にわたるため，その概要を手短に述べるということは非常に難しい．そこで本章では，話題を離散最適化の中心的な研究対象の一つであるネットワークフローに絞ることにより，具体的な離散最適化の問題例を通じて，その面白さ・有益性を感じ取っていただくことを目標とする．話題を選ぶ基準としては，モデルの応用力の高さに加え，離散構造の豊かさという二面的な性質を持ち合わせているという点を重視した．

本章の構成は以下の通りである．まず第2節において基本的なネットワークフローのモデルとなる静的ネットワークフローの定義および理論的な結果の紹介する．そして第3節においては，静的ネットワークフローに時間の要素を加え拡張した動的ネットワークフローの定義および理論的な結果の紹介する．最後に第4節において，さらに詳しいことを学びたい方への参考文献の紹介を行う．

本章では，$\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{Z}_+$ を用いて実数，非負の実数および非負の整数の集合を表すものとする．有向グラフ $D = (V, A)$ とは，有限な点集合 V と，辺と呼ばれる V の異なる二つの要素からなる順序対の集合 A からなる組である（図1参照）．例えば，点を交差点，辺を通過する方向が指定された道路のようなものだと思っていただければよい．各 $v \in V$ に対して，$\delta(v)$ と $\varrho(v)$ で v から出る辺および v に入る辺の集合を表すとする．また，有向グラフ D 上のパスとは，ある点からある点へ矢印の向きに辿っていったものである．

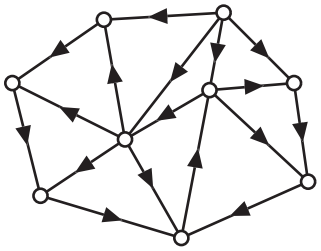


図 1：有向グラフの例.

2　静的ネットワークフロー

本節では基本的なネットワークフローのモデルである静的ネットワークフローを紹介する．直感的には，静的ネットワークフローはパイプライン上を石油が流れ続けているような状況をモデル化したものと思っていただければよい．静的ネットワークフローのモデルにおいては，入力として入口 $s \in V$ と出口 $t \in V$ を持つ有向グラフ $D = (V, A)$ と容量関数 $c\colon A \to \mathbb{R}_+$ が与えられる．例えば，有向グラフ $D = (V, A)$ はパイプライン，s, t は文字通り入口や出口，c は各パイプの幅を表していると思っていただければよい．このとき静的ネットワークフローとは関数 $\xi\colon A \to \mathbb{R}_+$ で以下の二つの条件を満たすものである．

(1) 容量条件：任意の $a \in A$ に対して

$$\xi(a) \leq c(a).$$

(2) 流量保存条件：任意の $v \in V \setminus \{s, t\}$ に対して

$$\sum_{a \in \delta(v)} \xi(a) = \sum_{a \in \varrho(v)} \xi(a).$$

静的ネットワークフロー ξ が与えられたとき，$\xi(a)$ は辺 a に流れるものの量を表していると見なすことができる．また，容量条件は辺の幅以上にものが流れないことを，流量保存条件は入口や出口ではない点においては入ってきた量がちょうど出ていくことを保証している．

次に静的ネットワークフローのモデルにおける基本的な問題である最大流問題と最小費用流問題を紹介する．直感的には，最大流問題は入口から出口まで可能な限り多くのものを流すことを目的とした問題である．形式的には，静的ネットワークフロー $\xi\colon A \to \mathbb{R}_+$ のうち

$$\sum_{a \in \varrho(t)} \xi(a)$$

を最大にするものを求める問題である．ただし $\delta(t) = \emptyset$ を仮定している．この問題に対しては多項式時間アルゴリズム，つまり四則演算や比較などの基本演算の回数が $|V|$ や $|A|$ の多項式で押さえることのできるアルゴリズムが存在することが知られている．（具体的なアルゴリズムや多項式時間アルゴリズム等の基本的な知識に関しては第 4 節の文献を参照.）

続いて，最小費用流問題を紹介しよう．直感的には，各辺に単位量あたりのコストが与えられ，流れるものの量に比例してコストがかかるような状況で，最小費用の静的ネットワークフローを求めることを目的としている．形式的には，最小費用流問題においては費用関数 $c\colon A \to \mathbb{R}$ が与えられる．辺 $a \in A$ に対する費用 $c(a)$ は負となり得ることに注意すること．費用が負となるときは，利得を意味していると理解していただければよい．このとき最小費用流問題とは，静的ネットワークフロー $\xi\colon A \to \mathbb{R}_+$ のうち

$$\sum_{a \in A} c(a)\xi(a)$$

を最小にするものを求める問題である．この最小費用流問題も多項式時間で解くことができることが知られている．

静的ネットワークフローのモデルに対しては，上記の二つの代表的な問題以外にも，いろいろな種類のものが流れている状況をモデル化した多品種流問題や，辺を通過することによってものの量が増える状況をモデル化した一般化流問題などがある．これらのモデルに関しては第 4 節の文献を参照にしていただきたい．

3　動的ネットワークフロー

本節では動的ネットワークフローを紹介する．前節で紹介した静的ネットワークフローは一定の量のものがネットワーク上を流れ続ける状況をモデル化したものであったことを思い出そう．一方，動的ネットワークフローは時々刻々流れる量が変化する状況をモデル化している（図 2 参照）．このモデルは都市や建物における避難計画に関する研究への応用などがある（例えば文献 [9, 17] を参照）．

形式的に動的ネットワークフローの定義を行う．入力としては端子と呼ばれる特別な点集合 $S \subseteq V$ を持つ有向グラフ $D = (V, A)$，容量関数 $c\colon A \to \mathbb{R}_+$，移動時間関数 $\tau\colon A \to \mathbb{Z}_+$，そして制限時間 $T \in \mathbb{Z}_+$ が与えられる．例えば，τ は各辺 a を移動するために必要とする時間を表していると思っていただければよい．このとき，動的ネットワークフロー $f\colon A \times \mathbb{Z}_+ \to \mathbb{R}_+$ とは以下の三つの条件を満たすものである．

(1) 容量条件：各 $a \in A$ および各 $\theta \in \mathbb{Z}_+$ に対して

$$f(a, \theta) \leq c(a).$$

(2) 流量保存則：各 $v \in V \setminus S$ および各 $\theta \in \mathbb{Z}_+$ に対して

$$\mathsf{ex}_f(v, \theta) \geq 0.$$

ただし，各 $v \in V$ および各 $\theta \in \mathbb{Z}_+$ に対して，

$$\mathsf{ex}_f(v, \theta) := \sum_{a \in \varrho(v)} \sum_{t=0}^{\theta - \tau(a)} f(a, t) - \sum_{a \in \delta(v)} \sum_{t=0}^{\theta} f(a, t).$$

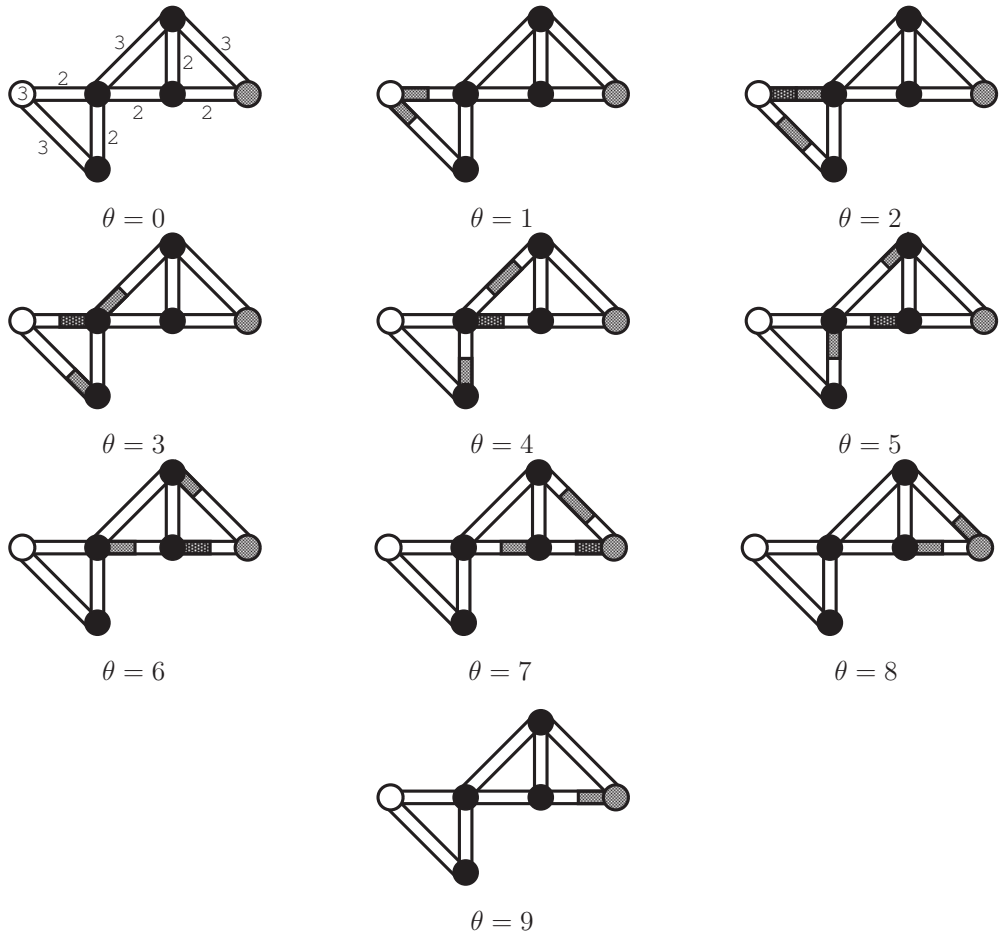


図 2：白点が入口，灰色の点が出口を表している．辺の数字は移動時間を表している．

(3) 要求制約：各 $v \in V \setminus S$ に対して

$$\mathsf{ex}_f(v, T) = 0.$$

動的ネットワークフロー f に対して，$f(a, \theta)$ は時刻 θ に辺 a に流れ込むものの量を表していると思っていただければよい．静的ネットワークフローに対しては，その値は単に辺に流れ込む量のみを表していたのに対し，動的ネットワークフローに対しては，ある時刻に流れ込む量を表している，つまり時間的な要素が加わっていることに注意していただきたい．また，容量条件は辺の幅以上にものが流れないことを，流量保存条件は端点ではない点においてはある時刻にその点から出て行くものの量はその時刻までに入ってきた量以下となることを保証している．ただし，動的ネットワークフローに対する流量保存則においては $\mathsf{ex}_f(v, \theta)$ が正，つまりある時刻 θ において点 v で滞留がおこることを容認していることに注意していただきたい．最後に要求制約は時刻 T 以降は端点以外の点においてはものが残っていないことを保証して

いる．

以下では，動的ネットワークフローにおいて代表的な問題である，最大動的流問題と最速輸送問題を紹介する．直感的に言うなれば，一つ目の問題はある決められた制限時間以内に可能な限り多くのものを流す問題であり，二つ目の問題は，一つの供給点と複数の需要点を持つネットワークにおいて，各需要点に需要を満たすように可能な限り早く供給点からものを流す問題である．

3.1 最大動的流問題

ここでは，最大動的流問題を紹介しよう．最大動的流問題においては，$S = \{s, t\}$ を満たす有向グラフが与えられる．このとき，最大動的流問題の目的は $\mathsf{ex}_f(s, T)$ を最大化する動的ネットワークフロー f を求めることである．これは $\mathsf{ex}_f(t, T)$ を最大化する，つまり t に流れ込むフローの量を最大化することと等価であることに注意されたい．

ここで Ford & Fulkerson [5] によって提案された最大動的流問題に対するアルゴリズムを紹介する．まず，有向グラフ D 上の静的ネットワークフロー ξ を考える．このとき，ξ の価値を

$$(T+1)\sum_{a\in\varrho(t)}\xi(a) - \sum_{a\in A}\tau(a)\xi(a)$$

で定義する．実は，Ford & Fulkerson [5] は，静的ネットワークフローのうち価値が最大のものの価値が最大動的流問題の目的関数の最適値と一致することを証明した．では，最大の価値を持つ静的ネットワークフローはどのように求めるのであろうか．実は，最大の価値を持つ静的ネットワークフローは以下のようにして最小費用流問題に帰着することができる．まず，各辺 $a \in A$ の費用を $\tau(a)$ と定義する．そして，新しい辺 (t, t') を加えこの辺の費用を $-(T+1)$ とする．このとき，s を入口，t を出口としたときの最小費用流問題の解を ξ^* としよう．すると，ξ^* の $-$(費用)

$$(T+1)\xi^*((t,t')) - \sum_{a\in A}\tau(a)\xi^*(a)$$

が最大動的流問題の目的関数の最適値と一致するすることがわかる．

最大動的流問題の目的関数の最適値が，最小費用流問題を解くことにより得られることはわかったが，その最適値を実現する動的ネットワークフローはどのように求めればよいのであろうが．そのためには，まず ξ^* をパス分解する必要がある．パス分解とは s から t へのパスの集合 $\mathcal{P}$ と関数 $\lambda\colon \mathcal{P} \to \mathbb{R}_+$ の組で

$$\sum_{P\in\mathcal{P}\colon a\in P}\lambda(P) = \xi^*(a)$$

を満たすものである．このようなパス分解を多項式時間で求めることが可能であることであることが知られている．このとき，このパス分解を用いて以下のように最大動的流問題の解を構成することができる．各パス $P \in \mathcal{P}$ 上に時刻 0 から $T - \tau(P)$ まで $\lambda(P)$ だけものを流すような動的ネットワークフローを構成する．ただし，$\tau(P)$ は P 上の全ての辺の移動時間の合計

である．この様にして構成された動的ネットワークフローが実行可能であることは容易にわかる．Ford & Fulkerson [5] は，このように構成された動的ネットワークフローが最大動的流問題の最適解となっていることを，静的ネットワークフローに対する最大流最小カット定理というものを使い証明した．このアルゴリズムは，もちろん最大動的流問題を多項式時間で解くことができるという点で素晴らしいのだが，それだけではなく最大動的流問題の解がある種の繰り返しによって構成されている洞察も与えている点も非常に興味深い．

3.2 最速輸送問題

続いて本節では最速輸送問題を紹介する．最速輸送問題においては，入口 s と出口集合 $S = \{s, t_1, t_2, \ldots, t_k\}$ からなる端子を持つ有向グラフおよび要求量 $d_1, d_2, \ldots, d_k \in \mathbb{R}_+$ が与えられる．このとき，目的は全ての $i \in \{1, 2, \ldots, k\}$ に対して

$$\mathsf{ex}_f(t_i, T) = d_i$$

を満たす動的ネットワークフロー f が存在するかを判定する問題である．もし，この問題が解くことができれば動的ネットワークフローが存在する最小の $T \in \mathbb{Z}_+$ を二分探索で求めることができることがわかる．

まず，制限時刻 T 以内に要求量 $d_1, d_2, \ldots, d_k$ を満たす動的ネットワークフローが存在するか否かを判定する問題を考えよう．各点集合 $X \subseteq S$ に対して，$o(X)$ で要求量を無視し，X を出口の集合とみなしたときの最大動的流問題の目的関数の最適値を表すとする．この問題は X を一つの出口に縮約することにより通常の最大動的流問題へと帰着することができるため，$o(X)$ は多項式時間で求めることができる．実は，[7] 中の Klinz との personal communication より，制限時刻 T 以内に要求量 $d_1, d_2, \ldots, d_k$ を満たす動的ネットワークフローが存在する必要十分条件が，全ての $X \subseteq \{t_1, t_2, \ldots, t_k\}$ に対して

$$o(X) \geq d(X)$$

が成り立つことであることが知られている．ただし，$d(X)$ は X の要素に関して要求量を合計したものである．つまり，関数 ρ を $\rho := o - d$ と定義すると，関数 ρ の最小値が 0 以上であることと同値である．ここで，全ての $X, Y \subseteq S$ に対して

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

を満たすことが知られている．この様な関数 ρ は劣モジュラ関数と呼ばれ，劣モジュラ関数の最小化は効率的にできることが知られている [8, 13]．つまり，ρ の最小値を劣モジュラ関数最小化のアルゴリズムを用いて求め，0 と比較することにより，望む動的ネットワークフローの存在性を効率的に判定することができる．

制限時間以内に要求量を満たす動的ネットワークフローが，存在するか否かを多項式時間で判定することができることはわかったが，実際にそのような動的ネットワークフローはどのように求めることができるのであろうか．この問題に対して Hoppe & Tardos [7] は辞書式最大動的流問題という問題へ帰着するアルゴリズムを与えているが，このアルゴリズムは本稿の範疇を超えているため割愛させていただく．

3.3 その他の問題

本節では，動的ネットワークフローのモデルにおける代表的な問題である最大動的流問題と最速輸送問題を扱ったが，ここでは扱うことのできなかった問題をいくつか紹介しよう．通常の静的ネットワークフローにおいて紹介した最小費用流問題は動的ネットワークフローのモデルにおいても研究されているのだが，実は最大動的流問題が多項式時間で解くことができるのとは異なり，この最小費用動的流問題は非常に困難な問題であることが知られている．この問題に関しては [4, 10] を参照して頂きたい．静的ネットワークフローとの関係という点では，動的ネットワークフローのモデルにおける多品種流問題も研究されている [6]．また，静的ネットワークフローとゲーム理論の重要な融合として均衡ネットワークフローというものがある．この均衡ネットワークフローとはネットワーク上を移動するものが，それぞれ自分勝手に動いたらどのような状態になるかを解析するためのものであり，静的ネットワークフローのモデルで非常に多く研究されてきた．近年，この枠組みを動的ネットワークフローにも拡張しようとする試みがなされている [11, 2]．また，Melkonian [12] によって提案された動的ネットワークフローのモデルにおいては，辺の容量がある時刻に辺に入る流量を制限するのではなく，ある時刻に同時に辺上に存在することのできる流量を制限するものとなっているようなものがある．

4 おわりに

本章ではネットワークフローを中心に離散最適化の研究を紹介した．本稿ではモデルを中心に紹介したが，ネットワークフローを含め広く離散最適化の理論を学びたい方への参考文献の紹介を行う．まず，離散最適化全般の参考文献としては Schrijver [14] を挙げる．この本は効率的に解くことのできる離散最適化問題を主に扱っているのだが，効率的に解くことが絶望的な問題，いわゆる **NP** 困難問題に対するアルゴリズムの参考文献としては Williamson & Shmoys [18] を挙げておく．また，本稿で紹介したネットワークフローの基礎的な結果に関しては，その元祖といえる教科書 Ford & Fulkerson [5] や，さらに現代的な趣を持つ Ahuja, Magnati & Orlin [1] を挙げておく．[1] には多くのネットワークフローの現実問題への応用が書かれている．動的ネットワークフローに関しては教科書的な文献がないのだが，Skutella [16] はコンパクトにまとまったサーベイである．また，離散最適化の研究において欠かすことのできない計算量理論に関する教科書として，入門書として Sipser [15]，さらに進んだものとして Arora & Barak [3] を挙げておく．

参考文献

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

[2] E. Anshelevich and S. Ukkusuri. Equilibria in dynamic selfish routing. In *SAGT*, pages 171–182, 2009.

[3] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[4] L. Fleischer and M. Skutella. Minimum cost flows over time without intermediate storage. In *SODA*, pages 66–75, 2003.

[5] L. R. Ford and D. R. Fulkerson. *Flows in Networks*. Princeton University Press, 1962.

[6] A. Hall, S. Hippler, and M. Skutella. Multicommodity flows over time: Efficient algorithms and complexity. *Theoretical Computer Science*, 379(3):387–404, 2007.

[7] B. Hoppe and É. Tardos. The quickest transshipment problem. *Math. Oper. Res.*, 25(1):36–62, 2000.

[8] S. Iwata, L. Fleischer, and S. Fujishige. A combinatorial strongly polynomial algorithm for minimizing submodular functions. *J. ACM*, 48(4):761–777, 2001.

[9] N. Kamiyama, A. Takizawa, N. Katoh, and Y. Kawabata. Evaluation of capacities of refuges in urban areas by using dynamic network flows. In *ISORA*, pages 453–460, 2009.

[10] B. Klinz and G. J. Woeginger. Minimum cost dynamic flows: The series-parallel case. In *IPCO*, pages 329–343, 1995.

[11] R. Koch and M. Skutella. Nash equilibria and the price of anarchy for flows over time. In *SAGT*, pages 323–334, 2009.

[12] V. Melkonian. Flows in dynamic networks with aggregate arc capacities. *Inf. Process. Lett.*, 101(1):30–35, 2007.

[13] A. Schrijver. A combinatorial algorithm minimizing submodular functions in strongly polynomial time. *J. Comb. Theory, Ser. B*, 80(2):346–355, 2000.

[14] A. Schrijver. *Combinatorial Optimization—Polyhedra and Efficiency*. Springer, 2003.

[15] M. Sipser. *Introduction to the theory of computation*. PWS Publishing Company, 1997.

[16] M. Skutella. An introduction to network flows over time. In *Research Trends in Combinatorial Optimization*, pages 451–482. Springer-Verlag, 2009.

[17] A. Takizawa, M. Inoue, and N. Katoh. An emergency evacuation planning model using the universally quickest flow. *The Review of Socionetwork Strategies*, 6:15–28, 2012.

[18] D. P. Williamson and D. B. Shmoys. *The Design of Approximation Algorithms*. Cambridge University Press, 2011.

最適化—半正定値計画を中心に—

脇　隼人
九州大学マス・フォア・インダストリ研究所

1　はじめに

最適化とは, 与えられた条件・制約のもとで, 与えられた関数を最大化または最小化する解やそのときの値を求めることである. 最適化は産業や日常生活の様々な場面で登場する. 金融ではリスク制約のもとで利益を最大化するために, 物流ではコストを最小にする車両配置や在庫管理のために, 製造業ではより良い設計パラメタを求めるため用いられる. 最近さかんにいわれているスマートグリッドでも, 再生エネルギーを効率的に利用するためには最適化が必要となる. また, 大学でも教員に対する授業や教室の割当, 学生の研究室配属などで最適化が利用できる.

最適化問題によって様々なアルゴリズムが提案されている. したがって, 解くべき最適化問題がどのような問題か知ることで, 適切なアルゴリズムやソフトウェアを選択し解を得ることができる. 現実の場面では最適化を行う際, 与えられたデータや現場の状況から最適化問題を作る必要がある. これをモデル化, またはモデリングと呼ぶ. その後, 得られた最適化問題を適切なアルゴリズムで解く, という順になる.

本稿では, その中でも最先端の最適化問題である半正定値計画問題に焦点を合わせて解説する. 半正定値計画問題は 21 世紀の線形計画問題と呼ばれ, 今後も幅広い分野で出現することが期待される最適化問題の一つである.

2　半正定値計画

本節では半正定値計画 (以下 SDP と省略する[1]) について簡単に紹介する. 日本語で紹介されている文献として [3, 6, 17] があげられる. 興味のある読者はこちらも参照してほしい.

SDP は線形計画 (以下 LP と省略する[2]) の行列版ということができる. 実際 SDP は LP の拡張である. 一方で, SDP は非線形な構造を有している, という点が決定的に LP と異なる. 実際, SDP の制約式が構成する領域は曲がった構造をしているのに対して, LP は多面体となっている.

SDP は行列の最適化問題であり, 多くの最適化問題を記述することが可能である. 制御や構造最適化の分野で現れる問題を SDP として記述できる場合がある. 統計分野で現れる相関行

[1] SemiDefinite Programming の略
[2] Linear Programming の略

列を推定する問題や, 最大カット問題などの NP 困難である組合せ最適化問題に対する近似解法で利用されている. 金融や機械学習, 計算量理論の解析でも SDP が現れることがあり, 今後も新しい分野で SDP を利用した研究が行われることが予想される.

LP と同じ様に, より複雑な問題 (例えば 非凸二次最適化問題や多項式最適化問題などの NP 困難な問題) を効率よく解くための手段として用いられることもある. 本稿では, この部分について 3 節で詳しく記述する.

2.1 定式化

$n \times n$ 実対称行列 $\boldsymbol{Z}$ が半正定値であるとは, 任意の $\boldsymbol{x} \in \mathbb{R}^n$ に対して, $\boldsymbol{x}^T \boldsymbol{Z} \boldsymbol{x} \geq 0$ が成り立つことをいう. また, $n \times n$ 実対称行列 $\boldsymbol{Z}$ が正定値であるとは, 任意の $\boldsymbol{x} \in \mathbb{R}^n \setminus \{0\}$ に対して, $\boldsymbol{x}^T \boldsymbol{Z} \boldsymbol{x} > 0$ が成り立つことをいう. $\mathbb{S}^n, \mathbb{S}^n_+, \mathbb{S}^n_{++}$ をそれぞれ $n \times n$ 実対称行列の集合, $n \times n$ 実半正定値対称行列の集合, $n \times n$ 実正定値対称性行列の集合とする. また, $\boldsymbol{Z}, \boldsymbol{W} \in \mathbb{S}^n$ に対して, $\boldsymbol{Z} \bullet \boldsymbol{W} := \sum_{i=1}^n \sum_{j=1}^n Z_{i,j} W_{i,j}$ と定める.

与えられた $\boldsymbol{A}_0, \ldots, \boldsymbol{A}_m \in \mathbb{S}^n$, $b_1, \ldots, b_m \in \mathbb{R}$ に対して, SDP 問題は次の様に定義される[3]:

$$\begin{cases} \text{最小化}: & \boldsymbol{A}_0 \bullet \boldsymbol{X} \\ \text{制約}: & \boldsymbol{A}_j \bullet \boldsymbol{X} = b_j, \ (j = 1, \ldots, m), \ \boldsymbol{X} \in \mathbb{S}^n_+. \end{cases} \tag{1}$$

この SDP では $\boldsymbol{X}$ が変数である. 全ての制約式を満たす $\boldsymbol{X}$ を SDP (1) の実行可能解と呼ぶ.

$\boldsymbol{X} \in \mathbb{S}^n_+$ という制約は, $\boldsymbol{X}$ に対して, 全ての主小行列式が非負の値をとる, ということと等価である. また定義より, $\boldsymbol{X} \in \mathbb{S}^n_+$ は次の式とも等価である:

$$\boldsymbol{v}^T \boldsymbol{X} \boldsymbol{v} \geq 0 \ (\forall \boldsymbol{v} \in \mathbb{R}^n)$$

これは, $\boldsymbol{X}$ が無限本の線形不等式を全て満たさなければならないことを表している. したがって, $\boldsymbol{X} \in \mathbb{S}^n_+$ という制約が非線形な制約ということを表しており, SDP は非線形計画問題の一つと言える. SDP は非線形最適化問題なので, 最小値をとる解が存在しないかもしれないことに注意してほしい. 最小値をとる解が存在しない例を例 2.2 で紹介する[4].

例 2.1 SDP の例題として, 次のような設定を考える (例題は [18] より引用):

$$m = 2, \ n = 3, \ \boldsymbol{A}_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ \boldsymbol{A}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ \boldsymbol{A}_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \ b_1 = 0, \ b_2 = 2.$$

さらに, 変数行列 X を

$$\boldsymbol{X} = \begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{12} & X_{22} & X_{23} \\ X_{13} & X_{23} & X_{33} \end{pmatrix}$$

[3] このように記述された最適化問題は次の様に読む: まず “最小化” の横にある数式は, 最小化したい目的関数である. “制約” の横にある 2 つの数式は, 変数行列 $\boldsymbol{X}$ の満たすべき制約式である. したがって, この最適化問題は変数行列 $\boldsymbol{X}$ が半正定値行列で m 本の数式を満たすもののなかで目的関数を最小化する, と読むことができる.

[4] したがって, ここで書いている “最小化”は, min の意味ではなく inf が適切である.

と書くことにする[5]. この時, $\boldsymbol{X} \in \mathbb{S}^3_+$ は全ての主小行列式が非負の値をとることと等価であるので, 7 本の不等式

$$\begin{cases} X_{11}, X_{22}, X_{33} \geq 0, \\ X_{11}X_{22} - X_{12}^2, X_{11}X_{33} - X_{13}^2, X_{22}X_{33} - X_{23}^2 \geq 0, \\ X_{11}X_{22}X_{33} + 2X_{12}X_{23}^2 - X_{22}X_{13}^2 - X_{33}X_{12}^2 - X_{11}X_{23}^2 \geq 0 \end{cases} \tag{2}$$

を満たさなければならない. さらに, $\boldsymbol{A}_0 \bullet \boldsymbol{X}$ は

$$\boldsymbol{A}_0 \bullet \boldsymbol{X} = 0 \cdot X_{11} + 2 \cdot 0 \cdot X_{12} + 2 \cdot 0 \cdot X_{13} + 0 \cdot X_{22} + 2 \cdot 0 \cdot X_{23} + 1 \cdot X_{33} = X_{33}$$

である. 同様に $\boldsymbol{A}_1 \bullet \boldsymbol{X}$, $\boldsymbol{A}_2 \bullet \boldsymbol{X}$ を計算すると, SDP (1) は次の様に書ける:

$$\begin{cases} \text{最小化}: & X_{33} \\ \text{制約}: & X_{11} = 0,\ 2X_{12} + X_{33} = 2,\ (2) \text{にある全ての制約式.} \end{cases} \tag{3}$$

この例題の場合, $X_{11} = 0$ と (2) の 4, 5, 6 番目の不等式から, $X_{12} = X_{13} = 0$ であることがわかる. これを $2X_{12} + X_{33} = 2$ に代入すると, $X_{33} = 2$ である. したがって, SDP (3) の最小値は 1 であり, 最小解は次の様に書ける:

$$\boldsymbol{X} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & X_{22} & X_{23} \\ 0 & X_{23} & 2 \end{pmatrix} \quad (\text{ただし}, 2X_{22} \geq X_{23}^2 \text{を満たさなければならない})$$

例 2.2 例 2.1 において, $\boldsymbol{A}_0$ と $\boldsymbol{A}_1$ を交換した SDP を考える. つまり,

$$m = 2,\ n = 3,\ \boldsymbol{A}_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ \boldsymbol{A}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \boldsymbol{A}_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix},\ b_1 = 0,\ b_2 = 2,$$

とすると, SDP (1) は, 次の様になる:

$$\begin{cases} \text{最小化}: & X_{11} \\ \text{制約}: & X_{33} = 0,\ 2X_{12} + X_{33} = 2,\ (2) \text{にある全ての制約式.} \end{cases} \tag{4}$$

例 2.1 と同様に, $X_{13} = X_{23} = X_{33} = 0$, $X_{12} = 1$ が言える. 一方, 任意の $\epsilon > 0$ に対して,

$$\boldsymbol{X}_\epsilon := \begin{pmatrix} \epsilon & 1 & 0 \\ 1 & 1/\epsilon & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

とおくと, $\boldsymbol{X}_\epsilon$ は半正定値行列であり, SDP (4) の実行可能解になっている. そのときの目的関数値が ϵ で, このことは任意の $\epsilon > 0$ で成立するので SDP (4) の最小値は 0 であることがわかる. しかしながら, この最小値 0 を達成する解は存在しない. なぜなら, 最小値 0 を達成するためには, $X_{11} = 0$ でなければならないが $X_{12} = 1$ なので, (2) にある不等式 $X_{11}X_{22} - X_{12}^2 \geq 0$ を満たさない. つまり $X_{11} = 0$, $X_{12} = 1$ であるような半正定値行列は存在しない.

[5]変数行列 $\boldsymbol{X}$ は対称行列であるので, ここではそれを考慮して対称行列になる様に要素を記述している

2.2 半正定値計画問題に対するソフトウェア

半正定値計画問題に対するソフトウェアについては, [3] の “半正定値計画問題に対するソルバーの紹介”で 2010 年の状況が詳細に述べられている. 2012 年現在も状況はあまり変化していない. 有償のソフトウェアよりも, 無償のソフトウェアが多い. また, MATLAB で動くものもいくつかある. ここで簡単にあげると, SDPA [14], SeDuMi [16], SDPT3 [15], CSDP [2] 等がある. それぞれのソフトウェアには特徴があり, また, SDP 問題の性質によってどのソフトウェアが有利かは代わることがある. [8] で示されている性能比較を元にソフトウェアを選択するのも一つの手かもしれない.

SDP 問題の規模は通常, 変数行列 $\boldsymbol{X}$ のサイズである n と等式制約の数 m で記述される. しかしながら, これだけで SDP 問題が効率よく解けるかどうか判断するのは難しい. 実際, SDP 問題を解くアルゴリズムである主双対内点法では, 各反復で $m \times m$ の連立方程式を解く必要がある. したがって, あまり m が大きいと高速に解くことが難しくなる. また, $\boldsymbol{X}$ の決定変数は $(n+1)n/2$ 個であり, n が数千くらいが限界である. さらに, 係数行列 $\boldsymbol{A}_j$ の疎性も重要である. できるだけ非零要素が少ない係数行列でモデル化できるなら, その方が高速計算が期待できる.

2.3 主双対内点法

SDP 問題を効率よく解くアルゴリズムとして, 主双対内点法が提案されている. また 2.2 節で記述したソフトウェアには主双対内点法が実装されている[6].

主双対内点法は反復法であり, 双対定理の仮定が成立するもとで収束することが証明されている. 与えられた $\epsilon > 0$ に対して, $O(\sqrt{n}\log(1/\epsilon))$ の反復回数で近似解が得られることが示されている. また, さらに適当な仮定をおくことで, 主双対内点法が超一次収束することも示されている. 一方, 実際に解いてみるとだいたい 20 回から 40 回くらいの反復回数で近似解が得られることが多い. アルゴリズムの詳細は [6, 18] に書かれているので興味のある読者はそちらを参照してほしい.

3 多項式最適化問題に対する半正定値計画緩和

3.1 概要

多項式最適化問題 (以下 POP と省略する[7]) とは, 多項式の不等式で表現される集合上で多項式を最小化する問題のことである. 数式で記述すると, 次のように書ける:

$$\left\{ \begin{array}{ll} \text{最小化}: & f_0(\boldsymbol{x}) \\ \text{制約}: & f_j(\boldsymbol{x}) \geq 0 \ (j = 1, \ldots, m), \end{array} \right. \tag{5}$$

[6] 主双対内点法にも様々な種類があり, どのソフトウェアも全く同じアルゴリズムが実装されているわけではない.

[7] Polynomial Optimization Problems の省略

ただし, 変数 $\boldsymbol{x}$ は実 n 次元ベクトルであり, $f_0, f_1, \ldots, f_m$ は n 変数の多項式である. 例えば, 最大カット問題, 最大重み安定集合問題などの組合せ最適化問題や二次計画問題などは POP として記述できる.

Lasserre [9] や Parrilo [12] によって, POP に対する半正定値計画緩和, つまり, SDP を利用して POP の最小値の下界値を求める手法, が提案されている. これ以降, 注目されるようになった理由として,

- 最大カット問題や安定集合問題などの組合せ最適化問題に対して, 既存の手法よりも良い下界値, つまり元の最適化問題の最適値に非常に近い下界値を与える,
- 凸性のない POP であっても, SDP 緩和によって POP の最小値そのものを得ることができる場合がある,
- また, POP によっては SDP 緩和問題の解から POP の最小解を得ることができる,
- 実代数幾何学や関数解析の分野と密接に関連していて, 数学的にも興味深い,

ことがあげられる.

POP に対する SDP 緩和を実装したソフトウェアとして, Gloptipoly [5], SOSTOOLS [13], SparsePOP [20] が公開されている. いずれも MATLAB と SeDuMi を利用する. ただし, SparsePOP に関しては SDPA を使うこともできる.

SparsePOP は, POP が “疎構造” を持っている場合に, それを利用してよりサイズが小さい SDP 緩和問題を構成する手法を組み込んでいる. 疎構造に関しては, 小節 3.4 で簡単に触れるが, 詳細は [19] の 3 節と 4 節を参照してほしい. 一般に, POP に対する SDP 緩和では, POP の変数の数が多いと, 得られる SDP 緩和問題が大規模になる. 疎構造を利用してこの困難を克服しようとしたのが, [19] やそれを実装した SparsePOP である.

3.2 本節で用いる記号について

いくつか記号を導入する. $\mathbb{N}$ は自然数の集合である. $\boldsymbol{x} \in \mathbb{R}^n$, $\alpha \in \mathbb{N}^n$ に対して, 単項式 $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ を $\boldsymbol{x}^\alpha$ と書くことにする. ただし, $\boldsymbol{x}^0 = 1$ である. また, 多項式 f を

$$f(\boldsymbol{x}) = \sum_{\alpha \in F} f_\alpha \boldsymbol{x}^\alpha$$

と書くことにする. ここで, $F \subseteq \mathbb{N}^n$ は, 係数が零でない単項式 $\boldsymbol{x}^\alpha$ の指数ベクトル α に対応する. F は有限個の要素からなることに注意する.

$r \in \mathbb{N}$, $\boldsymbol{x} \in \mathbb{R}^n$ に対して, $\boldsymbol{u}_r(\boldsymbol{x}) := (1, x_1, \ldots, x_n, x_1^2, \ldots, x_1^r, \ldots, x_n^r)^T$ と定める. $\boldsymbol{u}_r(\boldsymbol{x})$ は次数 0 から次数 r までの単項式を並べた列ベクトルである. このベクトルの要素数は, $\binom{n+r}{r}$ である. ここで, $N(n,r) := \binom{n+r}{r}$ と書くことにする.

このベクトルに対して, 行列 $\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T$ を考える. 例えば, $n = r = 2$ の場合, 以下の様に

なる:

$$\boldsymbol{u}_2(\boldsymbol{x})\boldsymbol{u}_2(\boldsymbol{x})^T = \begin{pmatrix} 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 \\ x_1 & x_1^2 & x_1x_2 & x_1^3 & x_1^2x_2 & x_1x_2^2 \\ x_2 & x_1x_2 & x_2^2 & x_1^2x_2 & x_1x_2^2 & x_2^3 \\ x_1^2 & x_1^3 & x_1^2x_2 & x_1^4 & x_1^2x_2^2 & x_1x_2^3 \\ x_1x_2 & x_1^2x_2 & x_1x_2^2 & x_1^3x_2 & x_1^2x_2^2 & x_1x_2^3 \\ x_2^2 & x_1x_2^2 & x_2^3 & x_1^2x_2^2 & x_1x_2^3 & x_2^4 \end{pmatrix}.$$

行列 $\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T$ は, 半正定値行列である[8]. ここで次の様に定数行列 $\boldsymbol{E}_\alpha$ で記述する:

$$\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T = \boldsymbol{E}_0 + \sum_{\alpha\in\mathbb{N}^n_{2r}\setminus\{0\}} \boldsymbol{E}_\alpha \boldsymbol{x}^\alpha$$

$n = r = 2$ の場合, $\boldsymbol{E}_{(0,0)}$, $\boldsymbol{E}_{(0,2)}$, $\boldsymbol{E}_{(2,2)}$ は実 6×6 対称行列であり次の様になる:

$$\boldsymbol{E}_{(0,0)} = \begin{pmatrix} 1 & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix},\ \boldsymbol{E}_{(2,2)} = \begin{pmatrix} & & & & & \\ & & & & & \\ & & & & & 1 \\ & & & & 1 & \\ & & & 1 & & \\ & & & & & \end{pmatrix},\ \boldsymbol{E}_{(0,2)} = \begin{pmatrix} & & & & & 1 \\ & & & & & \\ & & & & 1 & \\ & & & & & \\ & & & & & \\ 1 & & & & & \end{pmatrix}.$$

ただし, 空欄は 0 を表している.

同様に多項式 f に対して, 行列 $f(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T$ を考える. $f(\boldsymbol{x}) \geq 0$ となるベクトル $\boldsymbol{x}$ に対して, この行列は半正定値行列になる. また, 逆に, この行列がある $\boldsymbol{x}$ で半正定値ならば $f(\boldsymbol{x}) \geq 0$ である. なぜなら, $\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T$ の対角要素に 1 を含んでいるからである.

$d = \deg(f)$ とおくと, 同様に定数行列 $\boldsymbol{G}_\alpha$ を使って次の様に書ける:

$$f(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T = \boldsymbol{G}_0 + \sum_{\alpha\in\mathbb{N}^n_{2r+d}\setminus\{0\}} \boldsymbol{G}_\alpha \boldsymbol{x}^\alpha.$$

$\mathbb{N}^n_{2r+d}$ あれば, 行列 $f(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T$ に現れる全ての単項式が記述できることに注意してほしい. また, いくつかの行列 $\boldsymbol{G}_\alpha$ は零行列かもしれない. 実際, f が定数項を含んでいなければ $\boldsymbol{G}_0$ は零行列になる.

3.3 多項式最適化問題に対する半正定値計画緩和の詳細

POP (5) に対して, $r_0 = \lceil \max\{\deg(f_0), \deg(f_1), \ldots, \deg(f_m)\}/2 \rceil$ とおく. $r \geq r_0$ を満たす $r \in \mathbb{N}$ を選ぶ. また $j = 1, \ldots, m$ に対して, $r_j = r - \lceil \deg(f_j)/2 \rceil$ とおく. これは, (6) で現れる単項式が次数 $2r$ 以下であることを保証するためである. 目的関数 f_0 を次の様に記述する:

$$f_0(\boldsymbol{x}) = \sum_{\alpha\in F_0} (f_0)_\alpha \boldsymbol{x}^\alpha.$$

[8]任意の $\boldsymbol{v} \in \mathbb{R}^{N(n,r)}$ に対して, $\boldsymbol{v}^T(\boldsymbol{u}_r(\boldsymbol{x})\boldsymbol{u}_r(\boldsymbol{x})^T)\boldsymbol{v} = (\boldsymbol{v}^T\boldsymbol{u}_r(\boldsymbol{x}))^2 \geq 0$ であるので, 半正定値行列であることがわかる.

$(f_0)_\alpha$ は多項式 f_0 の単項式 $\boldsymbol{x}^\alpha$ に対応する係数である.

POP (5) に対して, 次の様に制約を追加する:

$$\begin{cases} \text{最小化}: & \sum_{\alpha\in F_0}(f_0)_\alpha \boldsymbol{x}^\alpha \\ \text{制約}: & \boldsymbol{G}_{j,0}+\sum_{\alpha\in\mathbb{N}^n_{2r_j}\setminus\{0\}}\boldsymbol{G}_{j,\alpha}\boldsymbol{x}^\alpha\in\mathbb{S}_+^{N(n,r_j)}\ (j=1,\dots,m) \\ & \boldsymbol{E}_0+\sum_{\alpha\in\mathbb{N}^n_{2r}\setminus\{0\}}\boldsymbol{E}_\alpha\boldsymbol{x}^\alpha\in\mathbb{S}_+^{N(n,r)}. \end{cases} \tag{6}$$

前の小節で述べた様に, 追加した行列の性質から POP (5) と (6) は等価である. つまり最小解も最小値も変わらない. 次に, 単項式 $\boldsymbol{x}^\alpha$ を y_α という変数で置き換える. これを線形化と呼ぶ:

$$\begin{cases} \text{最小化}: & \sum_{\alpha\in F_0}(f_0)_\alpha y_\alpha \\ \text{制約}: & \boldsymbol{G}_{j,0}+\sum_{\alpha\in\mathbb{N}^n_{2r_j}\setminus\{0\}}\boldsymbol{G}_{j,\alpha}y_\alpha\in\mathbb{S}_+^{N(n,r_j)}\ (j=1,\dots,m) \\ & \boldsymbol{E}_0+\sum_{\alpha\in\mathbb{N}^n_{2r}\setminus\{0\}}\boldsymbol{E}_\alpha y_\alpha\in\mathbb{S}_+^{N(n,r)}, \\ & \boldsymbol{x}^\alpha=y_\alpha\ (\alpha\in\mathbb{N}^n_{2r}\setminus\{0\}) \end{cases} \tag{7}$$

(7) の最後の式より, (7) も (6) も同じ最小値と最小解を持つ. したがって, (7) と (5) も等価である. 最後に, (7) から最後の式を除くことで, POP (5) の SDP 緩和問題を得る.

$$\begin{cases} \text{最小化}: & \sum_{\alpha\in F_0}(f_0)_\alpha y_\alpha \\ \text{制約}: & \boldsymbol{G}_{j,0}+\sum_{\alpha\in\mathbb{N}^n_{2r_j}\setminus\{0\}}\boldsymbol{G}_{j,\alpha}y_\alpha\in\mathbb{S}_+^{N(n,r_j)}\ (j=1,\dots,m) \\ & \boldsymbol{E}_0+\sum_{\alpha\in\mathbb{N}^n_{2r}\setminus\{0\}}\boldsymbol{E}_\alpha y_\alpha\in\mathbb{S}_+^{N(n,r)}. \end{cases} \tag{8}$$

(8) は (7) から制約をいくつか除くことで得られるので, (5), (8) の最小値をそれぞれ f^*, p_r^* とおけば, $p_r^*\le f^*$ が成立することがわかる. これは, 全ての $r\ge r_0$ で成り立っている. また r に関して単調性があることもわかる. つまり $p_r^*\le p_{r+1}^*\le f^*$ が成り立つ. 実は, Lasserre [9] では, ある仮定をおくことで $p_r^*\to f^*\ (r\to\infty)$ ということを示している. ここで注目してほしいことは, p_r^* は SDP の最小値である, ということである. したがって, 十分大きい r をとって SDP 緩和問題 (8) を構成し, ソフトウェアで解けば f^* に十分近い値が求められるのである.

では, r を十分を大きくして SDP 緩和問題を構成しそれを SDP のソフトウェアで解けば良いのかというと, そうではない. というのも, SDP 緩和問題のサイズ (変数行列のサイズや等式制約の数など) についても r に関して単調増加性を有している. 実際, SDP 緩和問題 (8) において一番大きい行列のサイズは $N(n,r)=\binom{n+r}{r}$ である. したがって, 現在の計算機の能力では r を大きくして解くのは, n が小さくない限り難しい. ただ, 経験的には $r=2,3$ 位で (5) の最小値かそれに十分近い値が得られている. 現状では, $n=25$ で $r=3$ くらいの SDP 緩和問題を解くのが限界であるといわれている.

3.4 疎構造を持つ多項式最適化問題の簡単な説明

SDP 緩和問題が大規模になりすぎる, という困難を克服しなければならない. [19] では多項式最適化問題 (5) が “疎構造” を持っている場合に, それを利用してよりサイズが小さい SDP

緩和問題を構成する手法を提案している. 疎構造に関しては, [19] の 3 節と 4 節を参照してほしいが, 簡単にいうと (5) の中に現れる変数の組合せをいう. 例えば, 次の様に変数が 2 つの組に分かれている POP を考えてみる:

$$\left\{\begin{array}{ll} \text{最小化}: & f_0(x_1,x_2)+g_0(x_3,x_4) \\ \text{制約}: & f_j(x_1,x_2)\geq 0\ (j=1,\ldots,m), \\ & g_j(x_3,x_4)\geq 0\ (j=1,\ldots,m) \end{array}\right. \tag{9}$$

この場合, $\boldsymbol{u}_r(x_1,\ldots,x_4)$ を使うよりも, $\boldsymbol{u}_r(x_1,x_2)$ と $\boldsymbol{u}_r(x_3,x_4)$ と分けて SDP 緩和問題を構成しても良さそうな気がする. これにより, SDP 緩和問題のサイズが小さくなることがわかる. 実際, この POP は次の様に二つの POP に分けてそれぞれの最小値の和が (9) の最小値になっており, 上記の (9) に対する SDP 緩和は, それぞれを SDP 緩和したことに対応している.

$$\left\{\begin{array}{ll} \text{最小化}: & f_0(x_1,x_2) \\ \text{制約}: & f_j(x_1,x_2)\geq 0\ (j=1,\ldots,m) \end{array}\right. , \quad \left\{\begin{array}{ll} \text{最小化}: & g_0(x_3,x_4) \\ \text{制約}: & g_j(x_3,x_4)\geq 0\ (j=1,\ldots,m) \end{array}\right.$$

では, 以下の 2 つの POP はどうであろうか:

$$\left\{\begin{array}{ll} \text{最小化}: & f_0(x_1,x_2)+g_0(x_2,x_3)+h_0(x_3,x_4) \\ \text{制約}: & f_j(x_1,x_2)\geq 0\ (j=1,\ldots,m), \\ & g_j(x_2,x_3)\geq 0\ (j=1,\ldots,m), \\ & h_j(x_3,x_4)\geq 0\ (j=1,\ldots,m) \end{array}\right. \tag{10}$$

$$\left\{\begin{array}{ll} \text{最小化}: & f_0(x_1,x_2)+g_0(x_1,x_3)+h_0(x_1,x_4) \\ \text{制約}: & f_j(x_1,x_2)\geq 0\ (j=1,\ldots,m), \\ & g_j(x_1,x_3)\geq 0\ (j=1,\ldots,m), \\ & h_j(x_1,x_4)\geq 0\ (j=1,\ldots,m) \end{array}\right. \tag{11}$$

これらは (9) の様に二つの最適化問題に分離できる構造を持っていない. しかし, (10) では, $\{1,2\}$, $\{2,3\}$, $\{3,4\}$ という変数の組がなんとなく見える. また (11) では, $\{1,2\}$, $\{1,3\}$, $\{1,4\}$ という変数の組がなんとなく見える.

このように, 変数は n 個あるがいくつかのグループに変数を分類できる場合がある. これらのグループの要素数が変数の数 n に比べて少ない時に, POP が疎構造を持っていると呼ぶ[9]. [19] では, (i) 疎構造を持っているかどうか確認する方法と, (ii) 疎構造を持っている場合に, 変数のグループを利用して規模の小さい SDP 緩和問題を構成する方法, を提案している. そして, その機能を実装したのが SparsePOP[20] である. (10) では, $\boldsymbol{u}_r(x_1,x_2)$, $\boldsymbol{u}_r(x_4,x_3)$, $\boldsymbol{u}_r(x_3,x_4)$ を使って, (11) では, $\boldsymbol{u}_r(x_1,x_2)$, $\boldsymbol{u}_r(x_1,x_3)$, $\boldsymbol{u}_r(x_1,x_4)$ を使って SDP 緩和問題を本節の方法で構成することでより小さい SDP 緩和問題を構成している. 一方で, $x_1^2+\cdots+x_n^2=1$ のように 1 つの制約式に全ての変数が利用されている場合, 疎構造を有しておらず [19] で提案した手法を適用しても Lasserre の SDP 緩和を適用した場合と大差はない.

[9] もし, グループが 1 つだけの場合, つまり $C_1=\{1,\ldots,n\}$ となっている場合, C_1 の要素数は n であり疎構造を有していない, ということになる.

[19] では, 様々な数値実験を行い, 変数が 20 個以上の POP で疎構造を有している場合には, 疎構造を利用した SDP 緩和を利用するのがよいと結論づけている. 例えば [4] にある “alkyl.gms” という POP に対して数値実験を行っている. この POP は 14 個の変数と 37 本の次数 1 から 3 までの多項式等式・不等式からなり, 疎構造を有している. 前節で述べた SDP 緩和では規模が大きくなりすぎて解けないのに対して, 疎構造を利用すると $r = 3$ でこの POP の最小値が数秒で得られている, ということが報告されている.

4 おわりに

SDP やその他の応用に関しては [3, 6, 17, 18] で良く記述されている. 興味を持たれた読者はぜひ読んでみてほしい. また, [10, 11] では POP に対する SDP 緩和についてまとめられたサーベイである. [1] では, SDP に関する最新の結果が豊富に記載されている. こちらもぜひあわせて読んでほしい.

参考文献

[1] M. Anjos and J. B. Lasserre (eds.): Handbook of Semidefinite, Conic and Polynomial Optimization, Springer, New York, (2011)

[2] CSDP, `https://projects.coin-or.org/Csdp`

[3] 藤澤克樹他, “特集　半正定値計画に対するソルバーと応用例”, オペレーションズ・リサーチ, Vol. 55, No. 7, (2010)

[4] GLOBAL Library, `http://www.gamsworld.org/global/globallib.htm` (2005).

[5] D. Henrion and J. B. Lasserre, “GloptiPoly: Global optimization over polynomials with Matlab and SeDuMi”, ACM Transactions Mathematical Software 29: 165–194, 2003, available from `http://homepages.laas.fr/henrion/software/gloptipoly2/`

[6] 小島政和, 土谷隆, 水野眞治, 矢部博, 内点法, 朝倉書店 (2001).

[7] H. Mittelmann, `http://plato.asu.edu/ftp/sparse_sdp.html`

[8] H. Mittelmann, `http://plato.asu.edu/talks/ismp.pdf`

[9] J. B. Lasserre, “Global optimization with polynomials and the problems of moments”, SIAM Journal on Optimization, 11, 796–817 (2001)

[10] J. B. Lasserre, “Moments, Positive Polynomials and Their Applications”, Imperial College Press Optimization Series Vol. 1, Imperial College Press (2009).

[11] M. Laurent, “Sums of squares, moment matrices and optimization over polynomials”. In Emerging Applications of Algebraic Geometry, M. Putinar and S. Sullivant editors, 157–270, Springer (2009).

[12] P. A. Parrilo, “Semidefinite programming relaxations for semialgebraic problems”, Mathematical Programming, 96, 293–320 (2003)

[13] S. Prajna, A. Papachristodoulou, P. Seiler and P. A. Parrilo, “SOSTOOLS (Sums of squares optimization toolbox for MATLAB) User’s guide”, available from http://www.cds.caltech.edu/sostools/

[14] SDPA, http://sdpa.indsys.chuo-u.ac.jp/sdpa

[15] SDPT3, http://www.math.nus.edu.sg/~mattohkc/sdpt3.html

[16] SeDuMi, http://sedumi.ie.lehigh.edu/

[17] 田村明久, 村松正和, 最適化法, 共立出版 (2005).

[18] M. J. Todd, “Semidefinite optimization”, Acta Numerica, 10, 515–560 (2001)

[19] H. Waki, S. Kim, M. Kojima and M. Muramatsu, “Sums of Squares and Semidefinite Programming Relaxations for Polynomial Optimization Problems with Structured Sparsity”, SIAM Journal on Optimization, 17, 218–242 (2006)

[20] H. Waki, S. Kim, M. Kojima, M. Muramatsu and H. Sugimoto, “SparsePOP: a Sparse SDP Relaxation of Polynomial Optimization Problems”, ACM Transactions on Mathematical Software, 35, 2, 15:1–15:13 (2008), available from http://sourceforge.net/projects/sparsepop/

オートマトン理論, その応用と抽象化

溝口　佳寛
九州大学マス・フォア・インダストリ研究所

1　はじめに

計算理論はコンピュータ (計算機) と密接に関係してるが, コンピュータ誕生前から「計算」の理論は考えられていた. 数学は「数」と「形」と「動」の学問と言われているが, 計算理論は, その中で「動」と密接に関連している. 微積分学は「動」の数学の代表で「数」の動きを記述する. そして, その数は物理現象の中の物理量を表現する. 計算理論は数よりは離散的な対象である文字列 (式) の動きに着目する. そして, その文字列は言語として構造を持ち, 自らの計算の過程をも表現する. 対象が変化する動的な物であるだけでなく, 対象が自己参照する点に難しさが潜んでいる [5].

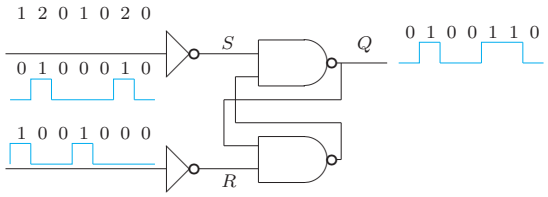
本文では計算モデルである順序機械とオートマトンについて説明する. 特に最も効率の良い有限オートマトン (最小実現と呼ばれる) の存在と構成に関する定理を紹介する. いわゆる一般のオートマトン理論については多くの教科書等 (cf. [1, 2, 6, 7]) が存在するので省略して, 圏論を用いた抽象理論を紹介する [9, 10]. 抽象化とはいえ圏の一般論ではなくオートマトン理論を述べる. オートマトンの最小実現に関する定理は圏論という抽象概念を使うと, 数学的に一般化され, 系の最小実現が像分解という概念を使って説明出来ることがわかる. そして, そのことは, 離散的な機械であるオートマトンの圏についての最小実現定理と連続線形系の圏での最小実現定理とが同時に定式化され, 証明されることを意味する. 考える系に対して最小にする対象や概念が明確でない場合に, その概念の定式化に圏論による抽象的な考え方が役に立つ. 最小にすべきが何かがわかったときには解決への道が見えたようなもので, その最小にすべき概念を構成することが大きな課題である. 圏論による抽象化はその課題解決への糸口となる.

1930 年代 Turing は「チューリング機械」と呼ばれる形式的な計算モデルを構成し, 計算可能性, 万能性に関する計算理論の礎を築いた. 数の計算の実現に計算モデルのテープ上に記述された文字列が重要な役割を果たす. 文字列による計算のモデル「有限オートマトン」の研究は 1950 年代に始まり情報理論の創始者として著名な Shanon と人工知能研究で著名な McCarthy の編集により 1956 年に発行された論文集 [17] に記録されている. 当初は順序回路の抽象化により状態遷移と入出力の関係についての様々な考察がなされていた [11]. その状態集合の中に特別な状態 (受理状態) の集合を導入することにより, 認識機械としての考察が始まり, 言語との重要な関係が導かれ, 有限オートマトンと言語の理論体系が構築された. この有限オートマトン理論の最初の論文が, Rabin と Scott の 1959 年の論文 [16, 15] である. 彼らは本成果により, 1976 年に ACM チューリング賞を受賞している. その後, 形式言語の研究は「自然言語の機械翻訳」「文献データベース」「人工知能」などの研究へと発展している. 近年では形式言語と

オートマトンの理論と応用については LATA 国際会議 [12] などで論理, 計算量理論, データ処理, モデル検査等の応用を意識した研究発表が行われている. 並列計算のモデルとしてのセルオートマトンの研究も盛んで, 理論研究としては情報処理国際連合 (International Federation for Information Processing) の作業班 (TC-1 WG1.5 Cellular Automata and Discrete Complete Systems) らによる Automata 国際会議 [13] 等で進められている. そして, 生物や物理の反応系としての研究から医学への応用, 画像処理, 画像認識, 並列計算, 計算アーキテクチャー, 交通システムなどの産業応用に関する研究は ACRI 国際会議 [18] 等で発表されている.

計算の形式化としてのオートマトン理論は記号論理学における推論過程を利用してプログラムの検証にも応用される (cf. [3, 4]). そこでは様々なオートマトンの拡張や論理の拡張が考察される. 工学システム, 社会システム, 経済システム, 環境システム等々を記述しようとするとき, 対象の前提条件, 対象の行動や状態の表現, それらの関連等を構造を持った集合とその間の関数や関係式で記述する. このようにシステムを定式化してシステムの持つ性質を解明する理論をシステム理論という. 形式的に記述されたシステムの動作が理論的に保証されれば, システム設計, 検証等が容易に行えるようになる. 個々のシステムについて課題解決の道を個別に探すことも必要だが, 圏論により抽象化されたシステムにおいて成立する性質を整理しておくことも重要である. 本文はシステムを圏論の言葉で記述するために必要な事項を具体的なシステムであるオートマトンを用いて解説したものである.

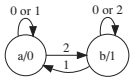
2　順序機械の形式化



上図は順序回路の基本要素のひとつである RS 型フリップフロップ回路の入出力の例である. 順番に入力された信号に従って出力が順番に変化する. 出力はオン (1) かオフ (0) であり, 出力集合は $Y = \{0, 1\}$ と考えられる. 入力は S (セット) と R (リセット) の 2 本あるが, これらを並べて (SR) で 2 進数で考えて入力集合は, $X = \{0 = (00), 1 = (01), 2 = (10)\}$ の 3 つ元の集合と考える. この順序回路は状態集合を $Q = \{a, b\}$ とし, 下表で定義される状態遷移関数 $\delta\colon Q \times X \to Q$, 出力関数 $\beta\colon Q \to Y$ を用いて, 順序機械としてモデル化される. 状態 q のとき, 入力 x があると次の状態 $\delta(q, x)$ に遷移し, $\beta(\delta(q, x))$ が出力される. 例では, 最初の状態を a として, 入力 “0201021” に対する出力が “0110010” となっている.

q	x	$\delta(q,x)$
a	0	a
a	1	a
a	2	b
b	0	b
b	1	a
b	2	b

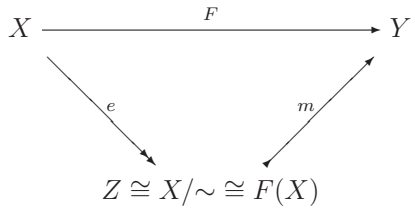
q	$\beta(q)$
a	0
b	1



この順序機械を**状態遷移図** (state transition diagram) で表すと上図 (右) のようになる. 状態を頂点, 遷移を辺で表し, 辺の上に入力文字, 状態の下に出力文字を書く. 入力文字に対し, 辺を辿ることで状態の変化や出力文字を検証出来る.

順序回路とは, 入力の列に対して出力の列が定まる文字列関数と考えることが出来る. すなわち, X^* から Y^* への関数 $f\colon X^* \to Y^*$ である. 但し, ここで, X^* は空列 (ここでは ε で表す) を含む X 上の文字列全体の集合である. 順序回路を状態集合, 遷移関数, 出力関数で定式化し順序機械を定義し, どのような文字列関数が実現可能なのか, また, より少ない状態数での実現が可能かを問題として考える.

命題 2.1 (全射・単射分解) 集合 X から集合 Y への関数 $F\colon X \to Y$ は, $F(x) = m(e(x))$ $(x \in X)$ となる全射 $e\colon X \to Z$ と単射 $m\colon Z \to Y$ の合成で表すことが出来る[1]. このとき, 集合 Z は同型を除いて唯一に定まり, $Z \cong F(X) = \{F(x) \mid x \in X\}$ であり, また, $Z \cong X/\!\sim\, = \{[x] \mid x \in X\}$ でもある. 但し, X 上の同値関係 $\sim$ は, $[x \sim x' \text{ iff } F(x) = F(x')]$ で定め, $[x]$ は x を含む同値類 $\{x' \in X \mid x \sim x'\}$ を表す.



定義 2.2 順序機械 (sequential machine) とは, 状態集合 Q, 入力記号の有限集合 X, 出力記号の有限集合 Y, 状態遷移関数 $\delta\colon Q \times X \to Q$, 出力関数 $\beta\colon Q \to Y$, 初期状態 $q_0 \in Q$ の 6 つ組 $M = (Q, X, Y, \delta, \beta, q_0)$ のことである. 状態集合が有限集合のとき**有限順序機械**という[2].

状態遷移関数 $\delta\colon Q \times X \to Q$ は, $\delta^*(q, \varepsilon) = q$, $\delta^*(q, xw) = \delta^*(\delta(q, x), w)$ $(q \in Q,\ x \in X,\ w \in X^*)$ と定義し, 自然に $\delta^*\colon Q \times X^* \to Q$ に拡張出来る. また, 一般に関数 $f\colon X^* \to Y$ は,

[1] $e\colon X \to Z$ が全射とは任意の元 $z \in Z$ に対して $e(x) = z$ となる元 $x \in X$ が存在することである. また, $m\colon Z \to Y$ が単射とは任意の元 $z_1, z_2 \in Z$ に対して, $z_1 \neq z_2$ ならば $m(z_1) \neq m(z_2)$ であることである.

[2] 本定義は **Moore 型**の順序機械と呼ばれる. 出力関数を β の代わりに $\lambda\colon Q \times X \to Y$ で与える定義を **Mealy 型**の順序機械という. この 2 つは等価なモデルであり, Mealy 型の順序機械は初期状態に対する出力が存在しないが, それ以外は入力と出力の関係が同値であるように相互に変換可能である. また, 初期状態を定義には入れず, 5 つ組で順序機械を定義することもある.

$f_*(\varepsilon) = f(\varepsilon)$, $f_*(wx) = f_*(w)f(wx)$ $(x \in X,\ w \in X^*)$ と定義し, 自然に $f_*\colon X^* \to Y^*$ に拡張出来る. 順序機械 $M = (Q, X, Y, \delta, \beta, q_0)$ に対して, $f_M\colon X^* \to Y$ を $f_M(w) = \beta(\delta^*(q_0, w))$ $(w \in X^*)$ とし, その拡張 $f_{M*}\colon X^* \to Y^*$ を考えると, これが入力と出力の間の文字列関数となっている.

関数 $t\colon X^* \to Y^*$ に対して, 順序機械 M が存在して, $t = f_{M*}$ となるとき, 関数 t は**順序機械で実現可能**という. 関数 $t\colon X^* \to Y^*$ が順序機械で実現可能であるための必要条件は t が, ある関数 $f\colon X^* \to Y$ の拡張 $t = f_*$ であることである. このことは, 任意の $w \in X^*$, $x \in X$ に対して, $t(wx) = t(w)y$ を満たす $y \in Y$ が存在することと同値であることが示される. すなわち $t(wx)$ の前半の出力は前半の入力 w だけに依存し, その後の x には影響されないことである. この条件を満たす関数 $t\colon X^* \to Y^*$ を**順序関数**という.

次に任意の順序関数が順序機械で実現可能であること, すなわち, 関数 $f\colon X^* \to Y$ が与えられたとき, $f = f_M$ となる順序機械 M が存在することを2通りの方法で順序機械を構成して示す. 1つ目は最も形式的な順序機械, 入力文字列全体を状態とする順序機械, $M_I = (X^*, X, Y, \delta_I, f, \varepsilon)$ である. ここで, $\delta_I(w, x) = wx$ $(w \in X^*,\ x \in X)$ とする. 2つ目は最も抽象的な順序機械, 入出力関数全体を状態とする順序機械, $M_T = (Y^{X^*}, X, Y, \delta_T, \beta_T, f)$ である. ここで, Y^{X^*} は X^* から Y への関数全体 $\{f \mid f\colon X^* \to Y\}$ を表し, $\delta_T(f, x)\colon X^* \to Y$ は $\delta_T(f, x)(w) = f(xw)$ $(x \in X,\ w \in X^*)$ で定義し, $\beta_T(f) = f(\varepsilon)$ $(f \in Y^{X^*})$ とする. このとき, $f = f_{M_I} = f_{M_T}$ となるが, M_I も M_T も有限順序機械ではないことに注意する.

有限順序機械で実現可能な関数 $f\colon X^* \to Y$ とは, どのような関数であろうか?

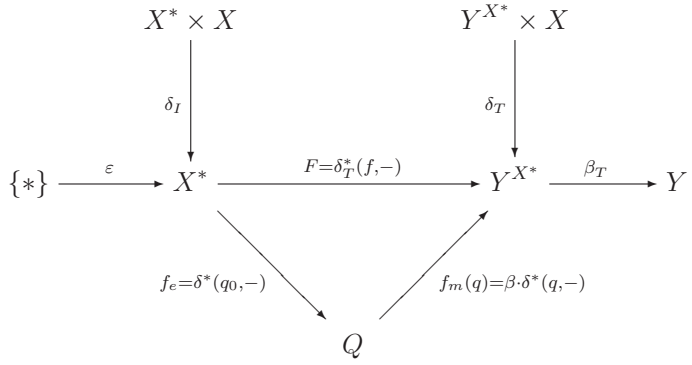
答えは M_T の中にある. 順序機械 M_T の無限にある状態の全ては必要ない. 初期状態 f から全ての入力 w に対して δ_T で状態遷移をした結果が有限の範囲にあれば良い. すなわち, $Z = \{\delta_T^*(f, w) \in Y^{X^*} \mid w \in X^*\}$ が有限集合であれば良い. この条件「Z が有限集合であること」が有限順序機械で実現可能な条件である. $F(w) = \delta_T^*(f, w)$ $(w \in X^*)$ とすると, $F\colon X^* \to Y^{X^*}$ であり, $Z = F(X^*)$ である. 命題 2.1 を使えば, $Z = X^*/\sim$ であり, 同値関係 $(\sim)$ は, $[w \sim w' \text{ iff } \delta_T^*(f, w) = \delta_T^*(f, w')]$, 言い換えると任意の $z \in X^*$ に対して $\delta_T^*(f, w)(z) = \delta_T^*(f, w')(z)$, すなわち, $f(wz) = f(w'z)$ である. この同値関係による同値類が有限個であれば, 有限順序機械で実現可能である. さらに, M_T の状態を Z に制限した順序機械が f を実現する状態数最小の順序機械であることがわかる.

最初に与えられる $f\colon X^* \to Y$ が順序機械 $M = (Q, X, Y, \delta, \beta, q_0)$ から定まる $f_M\colon X^* \to Y$ のとき, $F(w) = \delta_T^*(f_M, w)$ で定まる $F\colon X^* \to Y^{X^*}$ は, $f_e\colon X^* \to Q$ と $f_m\colon Q \to Y^{X^*}$ の合成に分解出来て, $F(W) = f_m(f_e(w))$ となる. ここで, $f_e(w) = \delta^*(q_0, w)$ であり, $f_m(q)(w) = \beta(\delta^*(q, w))$ である $(w \in X^*,\ q \in Q)$[3]. f_e が全射のとき M を**可到達** (reachable), f_m が単射のとき M を**可観測** (observable), または, **既約** (reduced) という. そして, 可到達, かつ, 可観測のとき, 順序機械 M は f_M を実現する状態数最小 (minimal) な実現であることがわかる.

$f_m\colon Q \to Y^{X^*}$ が単射でないときは, さらに, f_m を全射・単射分解することで状態数最小の順序機械を構成することが可能である. このとき, Q 上の同値関係 $[q \sim q' \text{ iff } f_m(q) = f_m(q')]$ は, 任意の $w \in X^*$ に対して, $f_m(q)(w) = f_m(q')(w)$ であること, すなわち, $\beta(\delta^*(q, w)) = \beta(\delta^*(q', w))$

[3] $f_m(q)\colon X^* \to Y$ $(q \in Q)$ であることに注意する.

であることである. Q が有限集合 (サイズを n とする) の場合には, 全ての $w \in X^*$ について調べなくても, 長さ n 以下の w について $\beta(\delta^*(q,w)) = \beta(\delta^*(q',w))$ であれば, $q \sim q'$ であることが示され, 与えられた有限順序機械から状態数最小の順序機械をアルゴリズムに従って具体的に構成することが出来る.



3 順序機械の圏での最小実現定理

本節では有限オートマトンを抽象化した順序機械の圏を考え, その中で最小実現定理がどのように表現され示されるかを見る. 圏論とは, 種々の性質を射の結合, 例えば集合の圏であれば関数の結合の性質だけで示す理論である. 圏論で証明出来ることは, 圏を変えれば他の圏でも証明されたことになる. すなわち, 線形空間の圏に適用して線形空間の定理, 集合の圏に適用して集合に関する定理などと, なるような性質を一般化して証明可能になる. 圏論に関する参考書は [8, 10, 14] などがある.

3.1 圏と像分解系

定義 3.1 圏 C とは, 対象のクラスと射のクラスの対 $(\mathrm{Obj(C)}, \mathrm{Mor(C)})$ である. 2 つの対象 $A, B \in \mathrm{Obj(C)}$ に対して, 射の集合 $\mathrm{Mor(C)}(A,B)$ が定まる. $\mathrm{Mor(C)}(A,B)$ を $\mathrm{C}(A,B)$ と書くこともある. また, $f \in \mathrm{C}(A,B)$ を $f\colon A \to B$ と書き, A を f の domain, B を f の codomain という. 射は以下の性質を満足するものとする.

性質 1 任意の対象 A, B, C に対して, 関数 $\mathrm{C}(A,B) \times \mathrm{C}(B,C) \to \mathrm{C}(A,C)$ が与えられている. $f\colon A \to B$, $g\colon B \to C$ の対, (f,g) に対する関数の値を $g \cdot f$ と書き, f と g の合成という. 任意の対象 A, B, C, D, 任意の射 $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ に対して, 結合法則 $h \cdot (g \cdot f) = (h \cdot g) \cdot f$ が成り立つ.

性質 2 任意の対象 A に対して, $\mathrm{C}(A,A)$ には, 恒等射 id_A と呼ばれる特別な射があり, 対象 B, 射 $f\colon A \to B$, $g\colon B \to A$ に対して, $\mathrm{id}_A \cdot g = g$, $f \cdot \mathrm{id}_A = f$ を満たす.

例 3.2 集合と写像の圏 **Set**, 線形空間と線形写像の圏 **Vect**, 半順序集合と順序保存写像の圏 **Poset** などが圏の例である.

$f\colon A \to B$ に対して, 任意の $C \in \mathrm{Obj}$, $g_1\colon B \to C$, $g_2\colon B \to C$ に対して,「$g_1 \cdot f = g_2 \cdot f \iff g_1 = g_2$」が成り立つとき, f を **epi-射**と呼び, $f\colon A \twoheadrightarrow B$ と書く. $f\colon B \to C$ に対して, 任意の $A \in \mathrm{Obj}$, $g_1\colon A \to B$, $g_2\colon A \to B$ に対して,「$f \cdot g_1 = f \cdot g_2 \iff g_1 = g_2$」が成り立つとき, f を **mono-射**と呼び, $f\colon B \rightarrowtail C$ と書く.

例 3.3 圏 **Set** において, 単射が mono-射, 全射が epi-射に対応する.

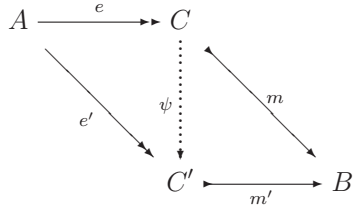
定義 3.4 射 $f\colon A \to B$ は, $k \cdot f = \mathrm{id}_A$, $f \cdot k = \mathrm{id}_B$ を満たす射 $g\colon B \to A$ が存在するとき, **同型射**という. このとき, g を f の逆射という. また, 対象 A と B を**同型**と呼び, $A \cong B$ と書く.

定義 3.5 射のクラスの対 $(\mathbf{E}, \mathbf{M})$ が, 圏 C の**像分解系**であるとは, 以下の性質を満たすことである.

性質 1 $\mathbf{E}$ の要素 $e\colon A \to B$, $e'\colon B \to C$ に対して, $e' \cdot e : A \to C$ も $\mathbf{E}$ の要素である. $\mathbf{M}$ の要素 $m\colon A \to B$, $m'\colon B \to C$ に対して, $m' \cdot m : A \to C$ も $\mathbf{M}$ の要素である.

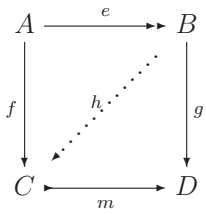
性質 2 $\mathbf{E}$ の要素は全て epi-射である. また, $\mathbf{M}$ の要素は全て mono-射である.

性質 3 任意の射 $f\colon A \to B$ は, $\mathbf{E}$ の要素 $e\colon A \to C$, $\mathbf{M}$ の要素 $m\colon C \to B$ の結合 $f = m \cdot e$ と分解出来る. また, その分解は同型を除いて唯一である. すなわち, 他の分解 $f = m' \cdot e'$, $e'\colon A \to C'$, $m\colon C' \to B$ があったとき, 同型射 $\psi\colon C \to C'$ が存在し, $\psi \cdot e = e'$, $m' \cdot \psi = m$ である.



例 3.6 集合の圏 **Set** に対して, $\mathbf{E} = \{f \mid f \text{ は全射}\}$, $\mathbf{M} = \{f \mid f \text{ は単射}\}$ とすると, $(\mathbf{E}, \mathbf{M})$ は像分解系である.

定理 3.7 $(\mathbf{E}, \mathbf{M})$ を像分解系, $e \in \mathbf{E}$, $m \in \mathbf{M}$ とし, 下の可換図式 $(g \cdot e = m \cdot f)$ を考える. このとき, $h \cdot e = f$, $m \cdot h = g$ を満たす射 $h\colon B \to C$ が唯一存在する.



3.2 順序機械の圏

Σ を入力集合, Q を状態集合, $\delta\colon Q \times \Sigma \to Q$ を遷移関数, $q_0\colon 1 \to Q$ を初期状態, Y を出力集合, $\beta\colon Q \to Y$ を出力関数とするとき, 6 つ組 $M = (\Sigma, Q, \delta, q_0, Y, \beta)$ を**順序機械**という. ここ

で, 1 は圏 **Set** での終対象, すなわち, 1 点集合 $1 = \{*\}$ である. 順序機械について, $q_0 \colon 1 \to Q$ は, Q の元 $q_0(*)$ と同一視することが出来る. $Y = \{0, 1\}$ とするとき, $\beta \colon Q \to Y$ と Q の部分集合 $F_\beta = \{q \in Q \mid \beta(q) = 1\}$ が 1 対 1 に対応する. すなわち, 順序機械は有限オートマトンの一般化である. 初期 (時間 0) のときの状態 $q(0) = q_0$ とし, 時間 t のときの入力記号を $x(t)$, 状態を $q(t)$ とするとき, 時間 t での出力は $y(t) = \beta(q(t))$ であり, 時間 $t+1$ の順序機械の状態は $q(t+1) = \delta(q(t), x(t))$ となる.

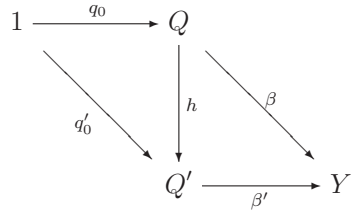
定義 3.8 入力集合 Σ を固定する. 圏 $\mathbf{Dyn}(\Sigma)$ の対象は, 集合 Q と写像 $\delta \colon Q \times \Sigma \to Q$ の対 (Q, δ) であり, Σ-機構と呼ばれる. もうひとつの Σ-機構 (Q', δ') に対して, 圏 $\mathbf{Dyn}(\Sigma)$ の射 $h \colon (Q, \delta) \to (Q', \delta')$ は, 写像 $h \colon Q \to Q'$ で下の可換図式を満たすものとする.

$$\begin{array}{ccc} Q \times \Sigma & \xrightarrow{\delta} & Q \\ {\scriptstyle h \times \mathrm{id}_\Sigma}\downarrow & & \downarrow{\scriptstyle h} \\ Q' \times \Sigma & \xrightarrow[\delta']{} & Q' \end{array}$$

このような射 h を機構射と呼ぶ. 射の結合は圏 **Set** での結合で行う.

$\mathbf{Dyn}(\Sigma)$ が圏であることを確認するのは容易である.

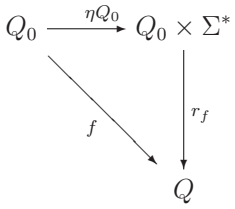
定義 3.9 入力集合 Σ と出力集合 Y を固定する. 圏 $\mathbf{Mach}(\Sigma, Y)$ の対象は順序機械 $M = (\Sigma, Q, \delta, q_0, Y, \beta)$ である. もうひとつの対象 $M' = (\Sigma, Q', \delta', q_0', Y, \beta')$ に対して, 射 $h \colon M \to M'$ は, 機構射 $h \colon (Q, \delta) \to (Q', \delta')$ で, 次の図式を可換にするものとする.

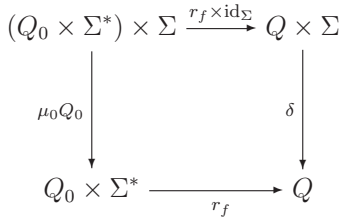


このような射 h を模倣射と呼び, 順序機械 M は順序機械 M' を模倣すると言う.

定義 3.10 任意の集合 Q に対して, $\mu_0 Q \colon (Q \times \Sigma^*) \times \Sigma \to Q \times \Sigma^*$ を $\mu_0 Q((q, w), x) = (q, wx)$ で定義するとき, $(Q \times \Sigma^*, \mu_0 Q)$ は, Σ 機構である. $(Q \times \Sigma^*, \mu_0 Q)$ を Q に対する**自由機構**という.

定理 3.11 (左随伴) $\eta Q_0 \colon Q_0 \to Q_0 \times \Sigma^*$ を $\eta Q_0(q) = (q, \varepsilon)$ とする. 任意の Σ 機構 (Q, δ) と写像 $f \colon Q_0 \to Q$ に対して, 下の図式を可換にする機構射 $r_f \colon (Q \times \Sigma^*, \mu_0 Q) \to (Q, \delta)$ が唯一存在する.

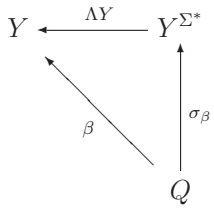


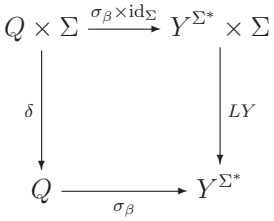


定義 3.12 定理 3.11 において, $\mathrm{id}_Q\colon Q \to Q$ に対する写像 r_{id_Q} を $\delta^*\colon Q \times \Sigma^* \to Q$ と書き, **run-射**という. また, $q_0\colon 1 \to Q$ に対する写像 r_{q_0} を初期状態 q_0 に対する**到達可能射**という. また, 到達可能射が epi-射のとき, Σ-機構 (Q,δ) を**到達可能**という.

定義 3.13 集合 Y に対して, $LY\colon Y^{\Sigma^*} \times \Sigma \to Y^{\Sigma^*}$ を $LY(f,x)(w) = f(xw)$ で定義するとき, (Y^{Σ^*}, LY) は Σ 機構である. (Y^{Σ^*}, LY) を Y に対する**余自由機構**という.

定理 3.14 (右随伴) $\Lambda Y\colon Y^{\Sigma^*} \to Y$ を $\Lambda Y(f) = f(\varepsilon)$ とする. Σ 機構 (Q,δ) と写像 $\beta\colon Q \to Y$ に対して, 下の図式を可換にする機構射 $\sigma_\beta\colon (Q,\delta) \to (Y^{\Sigma^*}, LY)$ が唯一存在する.



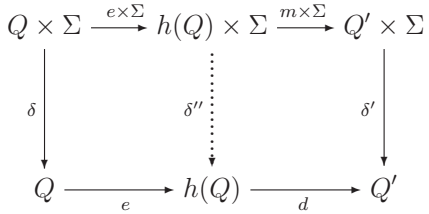


定理 3.14 の写像 $\sigma_\beta\colon Q \to Y^{\Sigma^*}$ を出力写像 $\beta\colon Q \to Y$ に対する**観測可能射**という. また, 観測可能射が mono-射のとき, Σ 機構 (Q,δ) を**観測可能**という. 順序機械 $M = (\Sigma, Q, \delta, q_0, Y, \beta)$ に対して, 到達可能射 $r_{q_0}\colon \Sigma^* \to Q$ と観測可能射 $\sigma_\beta\colon Q \to Y^\Sigma$ の合成 $\tau_M = \sigma^* \cdot r : \Sigma \to Y^{\Sigma^*}$ を全応答射という[4]. 機構射 $\tau\colon (\Sigma^*, \mu_0 1) \to (Y^\Sigma, LY)$ が, ある順序機械 M の全応答射 $\tau = \tau_M$ であるとき, 順序機械 M を τ の**実現**という. 機構射 $\tau\colon (\Sigma^*, \mu_0 1) \to (Y^\Sigma, LY)$ の実現 M_0 が到達可能かつ観測可能なとき**最小実現**という.

例 3.15 機構射 $\tau\colon (\Sigma^*, \mu_0 1) \to (Y^\Sigma, LY)$ に対して, $M_I = (\Sigma, \Sigma^*, \mu_0 1, \eta 1, Y, \Lambda Y \cdot \tau)$ と $M_T = (\Sigma, Y^{\Sigma^*}, LY, \tau \cdot \eta 1, Y, \Lambda Y)$ は実現である. M_I は到達可能, M_T は観測可能である.

命題 3.16 圏 $\mathbf{Mach}(\Sigma, Y)$ での射, すなわち, 模倣射 $h\colon M \to M'$ があるとき, 順序機械 M と M' の全応答射は等しくなる.

定理 3.17 圏 $\mathbf{Dyn}(\Sigma)$ での射 $h\colon (Q,\delta) \to (Q',\delta')$ に対して, 圏 $\mathbf{Set}$ での写像 $h\colon Q \to Q'$ の像分解を $h = m \cdot e$ とする. このとき, $h(Q)$ に唯一の Σ 機構 $\delta''\colon h(Q) \times \Sigma \to h(Q)$ が定まり, $e\colon (Q,\delta) \to (h(Q),\delta'')$, $m\colon (h(Q),\delta'') \to (Q',\delta')$ は機構射となる.

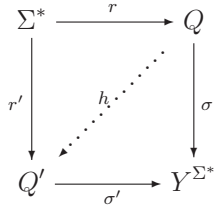


系 3.18 $\mathbf{E}_D = \{f \mid f \text{ は全射である機構射}\}$, $\mathbf{M}_D = \{f \mid f \text{ は単射である機構射}\}$ とすると, $(\mathbf{E}_D, \mathbf{M}_D)$ は圏 $\mathbf{Dyn}(\Sigma)$ での像分解系である.

[4](注意) 全応答射は機構射である. $\tau_M\colon (\Sigma^*, \mu_0 1) \to (Y^\Sigma, LY)$.

定理 3.19 (模倣の定理) 機構射 $\tau\colon (\Sigma^*, \mu_0 1) \to (Y^\Sigma, LY)$ の到達可能な実現 M, 観測可能な実現 M' に対して模倣射 $h\colon M \to M'$ が唯一存在する.

証明 $\tau_M = \sigma \cdot r$, $\tau_{M'} = \sigma' \cdot r'$ とすると, 定理 3.7 により, 下の図式を可換にする射 $h\colon Q \to Q'$ が唯一存在する.



r が epi-射であるので, h は機構射になり, $h\colon M \to M'$ は模倣射である. ∎

定理 3.20 (最小実現定理) 任意の機構射 $\tau\colon (\Sigma^*, \mu_0 1) \to (Y^\Sigma, LY)$ は最小実現 M' を持つ. また, 任意の到達可能な実現 M に対して, 模倣射 $h\colon M \to M'$ が唯一存在する. さらに, 任意の観測可能な実現 M'' に対して, 模倣射 $h'\colon M' \to M''$ が唯一存在する.

4 おわりに

定理 3.20 は像分解系を持つ任意の圏での定理に一般化される. そして, 例えば集合の圏に対しては, 有限オートマトンの最小実現, 線形空間の圏に対しては, 連続線形系の最小実現に関する定理を与えたことになる.

新しい構造物の性質や特徴を求めるときにその特徴を表す対象そのものが何であるかがわからないときがある. 一旦抽象化し, 性質や対象を圏論の言葉で記述したとき, その特徴を表す対象が明らかになる. オートマトンや系の拡張を考える場合には, その圏における機構射の像分解系, 随伴関手, 自由機構, 余自由機構を考察することが大切である. 求める対象が明らかになれば, その対象を構成することも容易になることが多い.

参考文献

[1] 有川節夫, 宮野悟, オートマトンと計算可能性, 培風館, 1986.

[2] 岩間一雄編, 計算論とオートマトン, 知識ベース, 知識の森, 電子情報通信学会, `http://www.ieice-hbkb.org/portal/doc_242.html`, 2010.

[3] 佐藤雅彦, 証明とプログラムの統一, 数理科学臨時別冊 SGC ライブラリ 21 (数学の未解決問題, 21 世紀数学への序章), p. 162–169, サイエンス社, 2003.

[4] 高原康彦, 飯島淳一, システム理論, 共立出版, 1990.

[5] 野崎昭弘, 廣瀬健編, コンピュータから生まれた新しい数学, 数学セミナー別冊 コンピュータと数学 5, 日本評論社, 1986.

[6] A. Salomma, 野崎昭弘他訳, 計算論とオートマトン理論, サイエンス社, 1988.

[7] 藤野精一編集, 計算数学ハンドブック, 朝倉書店, 1977.
[8] S. Mac Lane, 三好博之他訳, 圏論の基礎, シュプリンガー・フェアラーク東京, 2005.
[9] M. A. Arbib and E. G. Manes, Machines in a cagegory, an expository introduction, SIAM Review, 16 (1974), 163–192.
[10] M. A. Arbib, E. G. Manes, Arrows, Structures, and Functors, The Categorical Imperative, Academic Press, 1975.
[11] T. L. Booth, Sequential Machines and Automata Theory, John Wiley & Sons (1967).
[12] A-H. Dediu and C. Martin-Vide (ed.), Languate and Automata Theory and Applications, 6th International Conference, LATA2012, Lecture Notes in Computere Science, Vol. 7183, 2012.
[13] E. Formenti (ed.), Proc. 18th international workshop on Cellular Automata and Discrete Complex Systems (Automata2012) and 3rd international symposium Journées Automates Cellulaires (JAC2012), Electronic Proceedings in Theoretical Computer Science, Vol. 90, 2012.
[14] S. Mac Lane, Categories for the Working Mathematicians, Springer-Verlag, 1972.
[15] E. F. Moore (ed.), Sequential Machines; Selected Papers, Addison-Wesley, 1964.
[16] M. O. Rabin and D. Scott, Finite Automata and Their Decision Problems, IBM Journal, 3 (1959), 114–125.
[17] C. E. Shannon and J. McCarthy (ed.), Automata Studies, Princeton University Press, 1956.
[18] G. C. Sirakoulis and S. Bandini (ed.), Cellular Automata, 10th International Conference on Cellular Automata for Research and Industry, ACRI2012, Lecture Notes in Computer Science, Vol. 7495, 2012.

タンパク質複合体予測問題

丸山　修

九州大学マス・フォア・インダストリ研究所

概 要

本稿では，タンパク質複合体予測に使われる探索技法について概説する．まず，タンパク質複合体予測問題を説明し，予測結果の評価方法を定式化する．次に，代表的な手法であるマルコフ・クラスタリング (Markov clustering) アルゴリズム MCL を概説した後，筆者が現在開発中の予測システム PPSampler について概説する．そして最後に様々な予測アルゴリズムを用いた予測精度の比較実験について述べる．

1　はじめに

タンパク質複合体は，複数のタンパク質が組み合わさった一連の酵素反応を触媒する分子であり，細胞内の様々な機構を記述する上で不可欠の要素である．しかし，網羅的にすべてのタンパク質複合体を実験で同定することは困難なため，計算機による予測手法の確立が期待されている [1].

実際，様々な予測手法がいろいろな研究グループから提案されている．これらの主たる入力情報は，頂点がタンパク質に対応し，辺がタンパク質間相互作用に対応する無向グラフである．このグラフは，タンパク質間相互作用ネットワークともよばれている．そして，提案されている手法の多くは「タンパク質間相互作用ネットワークにおいて密な部分グラフと既知のタンパク質複合体はよく重複している」という所見に基づきスコア関数を定式化している．

本稿では，既存手法の代表的なものとして，MCL（マルコフ・クラスタリング）のアルゴリズムを概観する．そして次に，著者のグループで現在開発中のサンプリング手法に基づくシステム PPSampler について説明する．PPSampler の特徴の一つは，前出の所見に加えて「複合体のサイズ毎の既知複合体の頻度は近似的に冪乗則 (power-law) に従う」という所見も事前知識としてスコア関数に組み込んでいることである．

このような所見に基づきスコア関数を定式化し，さらにそれから確率分布を定義している．PPSampler は，この確率分布からランダム・サンプリングを行うことにより解（タンパク質全体集合の分割）の最適化を行う．

2　予測の評価方法

予測されたクラスター集合の評価を適合率 (precision)，再現率 (recall)，F 値 (F-measure) の 3 つの尺度で行う．これらを定義するため，まず二つのクラスターの重複度 (overlap ratio) を定義する．

クラスター s と t の重複度 $\mathrm{ov}(s,t)$ を，$|s|$ と $|t|$ の幾何平均に対する s と t の共有タンパク質数の割合を用いて次のように定義する：

$$\mathrm{ov}(s,t) = \begin{cases} \frac{|s\cap t|}{\sqrt{|s|\cdot|t|}} & \text{if } |s\cap t|>1, \\ 0 & \text{その他の場合.} \end{cases}$$

そして，$\mathrm{ov}(s,t)$ が予め定められた閾値 η より小さくなければ，s と t はマッチしているという．この重複度 $\mathrm{ov}(s,t)$ は，もしサイズ 2 以上のクラスター s と t が完全に一致しているなら最大値の 1 となる．また，s と t により共有されているタンパク質が 1 個以下ならば 0 となる．

C を予測されたタンパク質複合体の集合とし，K を既知のタンパク質複合体の集合とする．ここで，少なくとも一つの既知複合体とマッチする予測クラスターの個数を $N_{pc}(C,K,\eta)$ と表し，少なくとも一つの予測クラスターとマッチする既知複合体の個数を $N_{kc}(C,K,\eta)$ と表す．すなわち，次のように書ける：

$$N_{pc}(C,K,\eta) = |\{c \mid c\in C,\ \exists k\in K,\ \mathrm{ov}(c,k)\geq\eta\}|,$$
$$N_{kc}(C,K,\eta) = |\{k \mid k\in K,\ \exists c\in C,\ \mathrm{ov}(k,c)\geq\eta\}|.$$

このとき，C の K と η に関する適合率 (precision) を

$$\mathrm{precision}(C,K,\eta) = \frac{N_{pc}(C,K,\eta)}{|C|}$$

と定義し，C の K と η に関する再現率 (recall) を

$$\mathrm{recall}(C,K,\eta) = \frac{N_{kc}(C,K,\eta)}{|K|}$$

と定義する．最後に，C の K と η に関する F 値 (F-measure) を対応する適合率と再現率の調和平均と定義する．つまり，

$$F(C,K,\eta) = 2\cdot\frac{\mathrm{precision}(C,K,\eta)\cdot\mathrm{recall}(C,K,\eta)}{\mathrm{precision}(C,K,\eta)+\mathrm{recall}(C,K,\eta)}$$

となる．

3 MCL

MCL（マルコフ・クラスタリング）[2] とは，Stijn van Dongen らが開発したネットワーク（無向グラフ）の頂点をクラスタリングするツールである．MCL は，タンパク質間相互作用ネットワークなどを表す辺重み付き無向グラフ G が与えられると，G に対応する列が正規化された遷移行列 M を初期行列とし，expansion と inflation という 2 種類の操作により逐次 M を更新し，G の分割を出力する．expansion の操作は，現在の M を M^2 で置き換える．これは，M を M 上の長さ 2 のランダム・ウォークで置き換えることに相当する．inflation の操作

は，M の各 j 列において，各 i 行の要素（頂点 j から頂点 i への遷移確率）m_{ij} を m_{ij}^r で置換し，それらの総和で割って正規化する．ここで r (> 1) は予めユーザから指定された実数パラメータである．これらの操作を交互に繰り返すことにより，密につながっている部分グラフはより密になり最終的にクラスターとして抽出される．タンパク質複合体予測問題を扱った文献 [3, 4] 等において MCL は高い評価を受けているので，後程述べる予測精度比較実験において MCL を比較対象の一つにしている．

4 PPSampler

既知のタンパク質複合体データベースにはサイズの小さな複合体が数多く存在する．例えば，酵母 (*S. cerevisiae*) のタンパク質複合体データベースである CYC2008 [5] は 408 個の複合体を有するが，そのうちの 42%の 172 個が二量体（サイズ 2）である．実際，最頻出のサイズは 2 となっている．従って，サイズ 2 の複合体の予測に重きをおいた予測手法は，予測精度の向上が期待できる．タンパク質二量体の予測手法に関しては，丸山 [6] による教師付き学習手法による予測手法があるが，この手法の対象は二量体のみに限定されている．

さらに，CYC2008 のサイズ分布を調べると，その分布は冪乗則に従うことが分かる．つまり，サイズ k の複合体の頻度は $k^{-\gamma}$（γ は定数）に比例する [7]．そこで，本研究ではこの事実を事前知識として活用する Metropolis-Hastings アルゴリズムに基づく予測手法 PPSampler (Proteins' Partition Sampler) を提案する．PPSampler は, 与えられた確率分布に従ってタンパク質のクラスター集合をサンプルとして生成する．その確率分布は，タンパク質のクラスター集合 C に対する 3 つの異なる評価関数から構成される．これらの評価関数は，それぞれ，C 内のタンパク質間相互作用の重みに基づくもの，C に属する予測されるクラスターのサイズ分布に基づくもの，そして C に含まれるタンパク質の総数に基づくものである．

4.1 PPSampler

本節では，我々の提案手法である PPSampler について説明する．まず，PPSampler の骨格である Metropolis-Hastings (M-H) アルゴリズム [8] をどのように具体化するかを述べる．

4.1.1 M-H アルゴリズム

M-H アルゴリズムはある確率分布からランダムにサンプルを生成するためのマルコフ連鎖モンテカルロ (Markov chain Monte Carlo; MCMC) 法 [9] の一種である．M-H アルゴリズムを図 1 に示している．M-H アルゴリズムは，次の 3 つの構成要素を決めることにより具体化される：

(i) 状態の集合 D

(ii) 状態 $C \in D$ から状態 $C' \in D$ の提案分布 $Q(C'|C)$

(iii) サンプルを生成する確率分布 $P(C)$

次に PPSampler で用いる M-H アルゴリズムの以上の 3 要素を定式化していく．

Input:
温度パラメータ T;
反復回数 K;
初期状態 C_0;
提案分布 $Q\left(C'|C\right)$;
評価関数 $f(C)$;
Output:
サンプルされた状態 K 個の列;
Procedure:
$C = C_0$; /*初期状態の設定*/
for $k = 1$ to K:
$Q\left(C'|C\right)$ より候補状態 C' を提案;
$P(C) \propto \exp\left(-\frac{f(C)}{T}\right)$;
$r = \dfrac{P\left(C'\right)Q\left(C|C'\right)}{P\left(C\right)Q\left(C'|C\right)}$;
区間 $[0,1]$ 上の一様乱数 R の生成;
if $r > R$ **then** $C = C'$;

図 1：Metropolis-Hastings アルゴリズム.

4.1.2 タンパク質間相互作用データ

タンパク質間相互作用データは，タンパク質複合体予測において重要な入力データである．本稿では，このデータを次のように定式化する．V をある生物種のタンパク質の集合とし，タンパク質間相互作用の集合を $E \subseteq V \times V$ で表す．各 $e \in E$ の重みを $w(e) \in \mathbb{R}_+$ で表す．ただし，$e = \{u, v\} \notin E$ に対しては，$w(e) = 0$ と仮定する．

4.1.3 状態

次に M-H アルゴリズムの状態について述べる．V の分割 (partition) を C とする．つまり，C は次のように書ける：

$$C = \left\{ c_1, \ldots, c_n \subseteq V \;\middle|\; \begin{array}{l} \forall i,\ c_i \neq \emptyset, \\ \bigcup_{1 \leq i \leq n} c_i = V, \\ \forall i, j\ (\neq i),\ c_i \cap c_j = \phi \end{array} \right\}.$$

C の要素をクラスターとも呼ぶ．以後，分割はすべて V の分割を意味することとする．個々の分割 C は M-H アルゴリズムにおける 1 つの状態に対応する．

4.1.4 提案分布

次に，分割 C から分割 C' を提案する提案確率 $Q\left(C'|C\right)$ を定義する．C' は，次の二通りの方法により C から派生する．まず，どちらの場合であっても，クラスター間を移動させるタ

ンパク質として，V の中から一様分布に従いランダムに一つのタンパク質 u を選択する．つまり，特定のタンパク質 u が選択される確率は $\frac{1}{|V|}$ となる．次に，C' の二通りの作り方のそれぞれに対する確率 $Q(C'|C)$ を定める．ここで，次の (i) の u のみからなる新しい分割の要素を生成する場合を選択する確率を β とする．

(i) u のみからなる新しい分割の要素を生成する場合．
このときの提案確率は

$$Q(C'|C) = \frac{\beta}{|V|}$$

となる．

(ii) C からランダムに選択したクラスター c に u を移す場合．
u 以外の全タンパク質 $v \in V$ を $w(\{u, v\})$ に従い降順に並び替え，第 i 番目のタンパク質を v_i と記す．つまり，

$$w(\{u, v_1\}) \geq w(\{u, v_2\}) \geq \cdots \geq w(\{u, v_{|V|-1}\})$$

となる．分割 C から c が選ばれる確率は $\sum_{v_i \in c} 1/i$ に比例すると定める．従って，提案分布 $Q\left(C'|C\right)$ は

$$Q\left(C'|C\right) \propto \frac{1-\beta}{|V|} \sum_{v_i \in c} \frac{1}{i}$$

となる．

確率パラメータ β の値は，本稿を通して $\beta = 1/100$ に固定している．

4.1.5 評価関数

次に M-H アルゴリズムで使用する評価関数 f を構成する C の評価関数 f_1, f_2, f_3 を定義する．これらは全て最大化関数である．

まず C に含まれるタンパク質間相互作用の重みに基づく評価関数 $f_1(C)$ を定義する．そのために，まず一つの要素 $c \in C$ に対する評価関数 $f_1(c)$ を次のように定義する：

$$f_1(c) = \begin{cases} 0 & \text{if } |c| = 1, \\ -\infty & \text{else if } |c| > N \text{ または} \\ & \quad \exists u \in c,\ \forall v\,(\neq u) \in c, \quad w(\{u, v\}) = 0, \\ \displaystyle\sum_{u,v(\neq u) \in c} w(u, v) & \text{otherwise.} \end{cases}$$

ただし N はクラスター c のサイズの上限値を与えるパラメータである．上記の $f_1(c)$ の定義における最後の場合は，クラスター c 内の全てのタンパク質ペアの相互作用の重みの総和を表している．次に $f_1(C)$ を次のように定義する：

$$f_1(C) = \sum_{c \in C} f_1(c).$$

次に分割 C のクラスターのサイズ分布に基づく評価関数 $f_2(C)$ を定義する．C に対して $|c| = i\ (= 2, 3, \cdots, N)$ となる $c \in C$ の数の全体に対する割合を $\psi_C(i)$ で表すことにする．各サイズ i のクラスター数の相対頻度の目標値をパラメータ $\psi(i)$ で表す．$\psi(i)$ の値と $\psi_C(i)$ の値の二乗誤差とサイズ i に対する誤差ペナルティ i^2 との積の逆数の積を $f_2(C)$ と定義する．つまり

$$f_2(C) = \prod_{i=2}^{N} \frac{1}{1 + i^2 \cdot (\psi(i) - \psi_C(i))^2}$$

となる．ただし，分母が 0 になることを避けるため分母に 1 を足している．

分割 C のサイズ 2 以上のクラスター c 内のタンパク質の総数を $s(C)$ で表す．つまり，$s(C) = \left| \bigcup_{c \in C \text{ s.t. } |c| \geq 2} c \right|$ と書ける．$s(C)$ をその目標値を表すパラメータ λ の値に近づけるため，第 3 の評価関数 $f_3(C)$ を

$$f_3(C) = \frac{1}{1 + \dfrac{(s(C) - \lambda)^2}{10^3}}$$

と定義する．f_2 と同様に，分母が 0 になることを避けるため 1 を足している．

以上の関数 f_1, f_2, f_3 を組み合わせて最終的な評価関数 f を

$$f(C) = -f_1(C) \cdot f_2(C) \cdot f_3(C)$$

と定義する．

4.1.6 初期状態

次に，図 1 の M-H アルゴリズムが用いる初期状態 C_0 を定める．初期状態 C_0 は，次の 2 種類のクラスターすべてから構成する：

- タンパク質間相互作用の重み $w(u, v)$ が最大である二つのタンパク質 u と v のみから成るクラスター．
- 残りの各タンパク質 $w \in V \setminus \{u, v\}$ のみからなるサイズ 1 のクラスター．

4.1.7 出力

PPSampler は，図 1 が生成する全てのサンプル C の中から確率 $P(C)$ が最大となる C を予測複合体の集合として出力する．ただし，C に含まれるサイズ 1 のクラスターは予測複合体に含めない．また，確率最大のサンプルを選ぶために実際にサンプル C の確率 $P(C)$ を計算する必要はなく，$P(C)$ の比例値である $\exp\left(-\frac{f(C)}{T}\right)$ を用いて個々の $P(C)$ の大小関係を判定すればよい．

5 結果

まず，PPSamplerと既存手法の予測精度の比較を行う．比較対象とするアルゴリズムは，次の7つである．MCL [2] は文献 [3, 4] 等の予測精度の比較実験において高い評価を得ているクラスタリング・アルゴリズムである．MCODE [10] はPPIネットワーク上のタンパク質の連結性に基づく手法である．DPClus [11] はPPIネットワーク上の密な領域を探すアルゴリズムである．CMC [12] は最大クリークに基づく手法である．COACH [13] はコア・アタッチメント構造に基づき複合体の候補を見つけるアルゴリズムである．RRW [14] と NWE [15] は再スタート・ランダム・ウォーク (random walk with restarts) 手法に基づくアルゴリズムである．なお，MCL, RRW, NWE, PPSamplerは，相互作用の重みが与えられたならば，その情報を活用する仕組みを有している．

以上のアルゴリズムに与えるタンパク質間相互作用データは，WI-PHI [16] の全ての相互作用とする．また，既知のタンパク質複合体として408個のCYC2008 [5] の全ての複合体を用いる．重複度の閾値は $\eta = 0.4472\ (= \sqrt{0.2})$ と設定している．

PPSamplerのパラメータに関しては，温度パラメータを $T = 5$ そして反復回数を $K = 10^8$ としている．最大クラスターサイズ N は，CYC2008の最大複合体のサイズが81なので，近似的に $N = 100$ と設定している．タンパク質総数パラメータ λ はデフォルト値 $\lambda = 2000$ としているが，$\lambda = 1000, 3000$ としても比較的よい予測精度が得られることが判明している [17]．

パラメータ $\psi(i)$ は各サイズ $i\ (= 2, 3, \ldots, N)$ のクラスター数の相対頻度の目標値を表すパラメータである．CYC2008に含まれる複合体のサイズ分布を調べると，その分布は冪乗則に従うことが分かる．そこで，$2 \leq i \leq 100$ の範囲で相対頻度の二乗誤差の最小化によりべき乗に回帰させると $1.74 \times i^{-2.02}$ が得られる．そこで本研究では，近似的に，$\psi(i)$ を i^{-2} に比例する形に設定する．つまり，

$$\psi(i) = \frac{i^{-2}}{\sum_{j=2}^{N} j^{-2}}$$

となる．現在のPPSamplerでは，$\psi(i) \propto i^{-\gamma}$ の形でパラメータ $\psi(i)$ を指定可能となっている．一般に，γ の典型的な値は2から3と言われている．γ の値を0.5刻みでPPSamplerの予測精度を調べたところ，$\gamma = 2.0, 2.5, 3.0$ のときにF値が高くなることが確認されている [17]．

RRWとNWEの最小クラスター・サイズ・パラメータを2に設定している．さらにNWEのoverlap ratioのデフォルト値は0.3であるが，これをRRWと同じ0.2にしている．この二つのアルゴリズムのその他のパラメータ値は全てデフォルト値であり，さらに他のアルゴリズムのパラメータ値も全てデフォルト値である．

表1は，N_{pc} や N_{kc} などの各アルゴリズムの予測結果に関する基本情報を示している．PPSamplerのタンパク質数は目標値 $\lambda = 2000$ とほぼ同じ2001であることから，評価関数 f_3 がよく効いていることが分かる．第2行のクラスター数に関しては，アルゴリズムごとに様々な値を取っており，PPSamplerのクラスター数は比較的少なめの350個である．

図2は適合率，再現率，F値をグラフで表している．適合率に関しては，PPSamplerの0.537が他を凌駕しており，2番目に高いCOACHの0.307より約74.9%優れている．再現率では，COACHの0.620が最高値であるが，PPSamplerの0.534は遜色ない値である．再現率と適合率から計算されるF値においては，PPSamplerが最も高い0.536を得ており，その次に良い

表 1：予測精度の比較．#タンパク質は予測クラスターに含まれるたんぱく質の総数を表し，#クラスターは予測されたクラスターの総数を表し，平均サイズは予測クラスターの平均サイズを表している．

	MCL	MCODE	DPClus	CMC	COACH	RRW	NWE	PPSampler
#タンパク質	5869	2432	4888	5868	4094	4240	1626	2001
#クラスター	880	156	925	978	1353	1984	720	350
平均サイズ	6.67	15.59	6.91	20.65	13.29	2.14	2.26	5.72
N_{pc}	206	27	192	79	416	196	204	188
N_{kc}	246	31	219	84	253	204	212	218

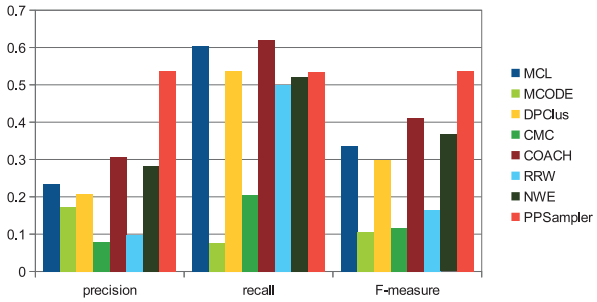
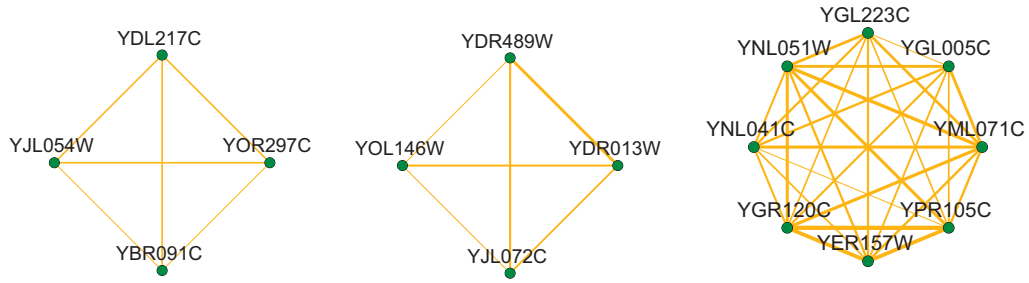


図 2：適合率，再現率，F 値

のは COACH の 0.411 である．よって PPSampler のスコアは COACH よりも約 30%優れていることが分かる．以上より，PPSampler は適合率と再現率の双方においてバランスよく高い値を得ており，その結果，予測精度の総合的評価基準である F 値においても優れた値を得ている．

図 3 は，PPSampler の予測クラスターの重複度は 1 であるが，他のどの手法の予測クラスターの重複度は 1 未満となる既知複合体の例を示している．例えば，mitochondrial inner membrane protein insertion complex に関しては，予測クラスターとの重複度，共有されているタンパク質の個数，そして予測クラスタのサイズは次のようになる：MCL: 0.67, 4, 9; MCODE: 0.5, 2, 4; DPClus: 0.82, 4, 6; CMC: 0.4, 4, 25; COACH: 0.76, 4, 7; RRW: 0.87, 3, 3; NWE: 0.71, 2, 2. MCL, DPClus, CMC そして COACH の予測クラスターは複合体のすべてのタンパク質を含んでいるがそのサイズは大き過ぎることが分かる．



(a) (b) (c)

図 3 : PPSampler の予測クラスターの例．PPSampler が重複度 1 で予測に成功するが他のどの手法の予測クラスターの重複度は 1 未満である既知複合体の例を示している．(a) mitochondrial inner membrane protein insertion complex [18], (b) GINS complex [19], (c) Golgi transport complex [20]．各辺は対応する WI-PHI のタンパク質間相互作用を表し，辺の太さはその相互作用の重みに比例している．

6 まとめ

本稿では，最初にタンパク質複合体予測問題を説明し，そして予測の評価方法を定式化した．次に，代表的な手法であるマルコフ・クラスタリング・アルゴリズム MCL と，筆者が現在開発中の予測システム PPSampler について概説した．これら二つを含む 8 つの予測アルゴリズムを用いた予測精度の比較実験を実施したところ，PPSampler が一番すぐれていることが分かった．なお，さらなる解析として，遺伝子オントロジーに基づく統計的有意性の評価，サイズ 2 とサイズ 3 のタンパク質複合体のみに限定した場合の予測精度の評価，そしてパラメータ γ と λ に関する PPSampler の頑健性を文献 [17] で詳しく述べているので参考にして頂きたい．

参考文献

[1] X. Li, M. Wu, C.-K. Kwoh, and S.-K. Ng, “Computational approaches for detecting protein complexes from protein interaction networks: a survey,” *BMC Genomics*, vol. 11 (suppl 1), p. S3, 2010.

[2] A. Enright, S. V. Dongen, and C. Ouzounis, “An efficient algorithm for large-scale detection of protein families,” *Nucleic Acids Res.*, vol. 30, pp. 1575–1584, 2002.

[3] S. Brohée and J. van Helden, “Evaluation of clustering algorithms for protein-protein interaction networks,” *BMC Bioinformatics*, vol. 7, p. 488, 2006.

[4] J. Vlasblom and S. Wodak, “Markov clustering versus affinity propagation for the partitioning of protein interaction graphs,” *BMC Bioinformatics*, vol. 10, p. 99, 2009.

[5] S. Pu, J. Wong, B. Turner, E. Cho, and S. Wodak, “Up-to-date catalogues of yeast protein complexes.,” *Nucleic Acids Res.*, vol. 37, pp. 825–831, 2009.

[6] O. Maruyama, "Heterodimeric protein complex identification," in *Proceedings of the 2nd ACM Conference on Bioinformatics, Computational Biology and Biomedicine*, pp. 499–501, 2011.

[7] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, 1999.

[8] W. Hastings, "Monte Carlo sampling methods using Markov chains and their applications," *Biometrika*, vol. 57, pp. 97–109, 1970.

[9] J. S. Liu, *Monte Carlo strategies in scientific computing*. Springer, 2008. New York.

[10] G. D. Bader and C. W. Hogue, "An automated method for finding molecular complexes in large protein interaction networks," *BMC Bioinformatics*, vol. 4, p. 2, 2003.

[11] M. Altaf-Ul-Amin, Y. Shinbo, K. Mihara, K. Kurokawa, and S. Kanaya, "Development and implementation of an algorithm for detection of protein complexes in large interaction networks," *BMC Bioinformatics*, vol. 7, p. 207, 2006.

[12] G. Liu, L. Wong, and H. N. Chua, "Complex discovery from weighted PPI networks," *Bioinformatics*, vol. 25, pp. 1891–1897, 2009.

[13] M. Wu, X. Li, C. Kwoh, and S. Ng, "A core-attachment based method to detect protein complexes in PPI networks," *BMC Bioinformatics*, vol. 10, p. 169, 2009.

[14] K. Macropol, T. Can, and A. Singh, "RRW: Repeated random walks on genome-scale protein networks for local cluster discovery," *BMC Bioinformatics*, vol. 10, p. 283, September 2009.

[15] O. Maruyama and A. Chihara, "NWE: Node-weighted expansion for protein complex prediction using random walk distances," *Proteome Science*, vol. 9 (Suppl 1), p. S14, 2011.

[16] L. Kiemer, S. Costa, M. Ueffing, and G. Cesareni, "WI-PHI: A weighted yeast interactome enriched for direct physical interactions," *Proteomics*, vol. 7, pp. 932–943, 2007.

[17] D. Tatsuke and O. Maruyama, "Sampling strategy for protein complex prediction using cluster size frequency," *Gene*, 2012. to appear.

[18] O. Kerscher, N. B. Sepuri, and R. E. Jensen, "Tim18p is a new component of the Tim54p-Tim22p translocon in the mitochondrial inner membrane," *Mol. Biol. Cell*, vol. 11, pp. 103–116, 2000.

[19] Y. Takayama, Y. Kamimura, M. Okawa, S. Muramatsu, A. Sugino, and H. Araki, "GINS, a novel multiprotein complex required for chromosomal DNA replication in budding yeast," *Genes Dev.*, vol. 17, pp. 1153–1165, 2003.

[20] J. R. Whyte and S. Munro, "The Sec34/35 Golgi transport complex is related to the exocyst, defining a family of complexes involved in multiple steps of membrane traffic," *Dev. Cell*, vol. 1, pp. 527–537, 2001.

非線形シュレディンガー方程式による流れのモデル化

福本　康秀

九州大学マス・フォア・インダストリ研究所

1　はじめに

液体や気体の流れ，その中を運動する物体に働く力を理解し，それを利用したり，さらには制御していこうとする学問が流体力学である．同じ形状の路であっても，流れの速度が遅い場合は整然と流れるが，速くなると乱れが生じる．また，撹乱振幅が小さい場合は撹乱の増幅がみられないが，振幅が大きくなると増幅することもある．このような流れの安定性の問題は，工学から地球惑星，物理学，数学にまたがる大きな分野で，研究が深まるにつれて，偏微分方程式，力学系・パターン形成，特異点論へと，他分野との接点が広がりつつある．

本稿では，水面波の安定性を例に，流れの撹乱を記述する流体方程式を非線形シュレディンガー方程式／ギンツブルグ・ランダウ方程式によってモデル化するアイデアとその具体的な手続きを概説する．そして，前者によって定常状態の安定性と解の分岐を論ずる．背後には，粘性のない流体の運動を支配するオイラー方程式のハミルトン構造があり，ハミルトン系に対する Krein のスペクトル理論が適用できる．それをもとに，散逸が不安定性を引き起こすことを明らかにする．

2　ナビェ・ストークス方程式の導出の概略

水や空気のような通常の流体の運動は Navier-Stokes 方程式によって支配される．この方程式の導出は骨が折れる作業である [2, 6]．本節では，そのあらましをかいつまんで述べる．流体は縮まないとし，密度 ρ はいたるところ一定であると仮定する．流体を無数の流体粒子の集合と考える．流体粒子というのは，分子ではなく，多数の分子を含む極めて微小な体積をもつ流体要素を指し，巨視的な記述の立場では，これを 1 点とみなす．ある流体粒子の時刻 t における位置を $\boldsymbol{x}(t) = (x(t), y(t), z(t)) = (x_1(t), x_2(t), x_3(t))$ とすると，その点における流速 $\boldsymbol{u} = \boldsymbol{u}(\boldsymbol{x}, t)$ が

$$\frac{d\boldsymbol{x}}{dt} = \boldsymbol{u}(\boldsymbol{x}, t) = (u_1(\boldsymbol{x}, t), u_2(\boldsymbol{x}, t), u_3(\boldsymbol{x}, t)) \tag{1}$$

によって定義される．加速度の k 成分は

$$\frac{d^2x_k}{dt^2} = \frac{\partial u_k}{\partial t} + \sum_{j=1}^{3} \frac{\partial u_k}{\partial x_j}\frac{dx_j}{dt} = \frac{\partial u_k}{\partial t} + \sum_{j=1}^{3} u_j \frac{\partial u_k}{\partial x_j} = \frac{\partial u_k}{\partial t} + \sum_{j=1}^{3} (\boldsymbol{u}\cdot\nabla) u_k \tag{2}$$

とあらわされる．

流体の内部では，微小な流体の塊同士が押し合いへし合いしている．ある流体の塊がその境界を通してまわりの流体から受ける力は圧力と粘性応力である．圧力は境界面に垂直方向に押し合う力で，たとえば，断面積 S で，法線方向を x 軸に向けた x と $x+\delta x$ にある平行な側面をもつ薄い板状領域に働く圧力の x 成分の和は

$$p(x,y,z)S - p(x+\delta x,y,z)S = -\left\{\frac{\partial p}{\partial x}(x,y,z)\delta x + O\big((\delta x)^2\big)\right\}S \tag{3}$$

である．圧力だけなら，着目している板状領域に対する Newton の第 2 法則において，厚さ δx を無限小にとる極限で，運動方程式の x 成分が得られる：

$$\rho\delta V\frac{d^2x}{dt^2} = -\frac{\partial p}{\partial x}\delta V \quad (\delta V = S\delta x) \quad \Longleftrightarrow \quad \rho\frac{d^2x}{dt^2} = -\frac{\partial p}{\partial x}. \tag{4}$$

粘性はまわりの流体が着目している流体塊を変形させようとする力で，簡単にいうと内部摩擦である．これには運動量を速度の大きい方から小さい方に拡散させようとする働きがあり，動粘性係数 ν がその拡散係数となる．流体塊には境界面を通してまわりの流体から受ける力に加えて，重力のように直接内部の各点に作用する体積力が働く．単位体積当たりの体積力を $\boldsymbol{b}$ とおくと，結局，Newton の第 2 法則から次のような運動方程式に導かれる．

$$\rho\left[\frac{\partial \boldsymbol{u}}{\partial t} + (\boldsymbol{u}\cdot\nabla)\boldsymbol{u}\right] = -\nabla p + \rho\nu\nabla^2\boldsymbol{u} + \rho\boldsymbol{b}. \tag{5}$$

これを **Navier-Stokes 方程式**とよぶ．非圧縮性流体の場合，これに，任意の流体塊が占める領域 V_t の体積が不変という条件が加わる．

$$\frac{d}{dt}\int_{V_t} dV = \int_{V_t}\nabla\cdot\boldsymbol{u}dV = 0 \quad \Longleftrightarrow \quad \nabla\cdot\boldsymbol{u} = 0. \tag{6}$$

3　流れの安定性とギンツブルグ・ランダウ方程式

重力に代表される体積力は，通常，ポテンシャル関数 $\Phi(\boldsymbol{x})$ を用いて $\boldsymbol{b} = -\nabla\Phi$ とあらわせる．よって，密度 ρ が一定の流体の場合，Navier-Stokes 方程式において，体積力 $\rho\boldsymbol{b}$ は圧力 $-\nabla p$ に組み入れてしまってよい．さて，安定性を議論する対象となる基本流の流速場と圧力場を $\boldsymbol{U}_0(\boldsymbol{x},t)$ と $P_0(\boldsymbol{x},t)$ とおこう．これらは，当然，$\nabla\cdot\boldsymbol{U}_0(\boldsymbol{x},t) = 0$ および Navier-Stokes 方程式 (5) をみたす．

$$\rho\left[\frac{\partial \boldsymbol{U}_0}{\partial t} + (\boldsymbol{U}_0\cdot\nabla)\boldsymbol{U}_0\right] = -\nabla P_0 + \rho\nu\nabla^2\boldsymbol{U}_0. \tag{7}$$

典型的な状況として，定常流をとることが多い：$\partial\boldsymbol{U}_0/\partial t = 0$.

この基本流に撹乱を加える．撹乱の流速場と圧力場を $\tilde{\boldsymbol{u}}(\boldsymbol{x},t)$ と $\tilde{p}(\boldsymbol{x},t)$ とおくと，全速度場 $\boldsymbol{u}(\boldsymbol{x},t)$ と全圧力場 $p(\boldsymbol{x},t)$ は $\boldsymbol{u} = \boldsymbol{U}_0 + \tilde{\boldsymbol{u}}$ と $p = P_0 + \tilde{p}$ で，これらは Navier-Stokes 方程式 (5) をみたす．基本流がみたす方程式 (7) を差し引くと，撹乱場の発展方程式

$$\frac{\partial\tilde{\boldsymbol{u}}}{\partial t} + (\boldsymbol{U}_0\cdot\nabla)\tilde{\boldsymbol{u}} + (\tilde{\boldsymbol{u}}\cdot\nabla)\boldsymbol{U}_0 + (\tilde{\boldsymbol{u}}\cdot\nabla)\tilde{\boldsymbol{u}} = -\frac{1}{\rho}\nabla\tilde{p} + \nu\nabla^2\tilde{\boldsymbol{u}}. \tag{8}$$

この方程式をじっと眺めていると，空間 1 次元の複素数値関数 $\psi(x,t)$ $(\in \mathbb{C})$ に対する時間依存 Ginzburg-Landau 方程式

$$\frac{\partial \psi}{\partial t} + U\frac{\partial \psi}{\partial x} = \mu\psi + \alpha\frac{\partial^2 \psi}{\partial x^2} - \beta|\psi|^2\psi \tag{9}$$

との類似性が浮かび上がってくる [4]．ここで，U, μ, α, β は定数ととる．α, β が複素数の場合を**複素 Ginzburg-Landau 方程式**とよぶ．Ginzburg-Landau 方程式は，いわば，撹乱場の方程式 (8) の 1 次元トイモデルである．60 年代半ばから，特異摂動法によって (8) から (9) を系統的に導く努力が続けられ，これによって，流れの安定性に対する理解が格段に深まっていった．流れの安定性の文脈では，(9) は Landau-Stuart 方程式あるいは Stuart-Stewartson 方程式とよばれる．

係数 $\mu = 0$ で，α と β が純虚数のとき，(9) は非線形 Schrödinger 方程式に帰着する．粘性のない流体の運動にかかわるのはむしろこちらの方である．以下では，水面波を例にとりあげ，その安定性が非線形 Schrödinger 方程式によって記述されることをみていこう．

4　水面波

静止状態においては $z = 0$ を水面（自由表面）とする水（液体）の波について考える．簡単のため，水深を無限大としよう．基本場として流れはなく $\boldsymbol{U}_0 = \boldsymbol{0}$，水面の微小振動のみをゆるすと，(5) において，非線形項を無視できる．ごく微小なスケールの現象を除けば粘性項も無視してよい．外力として重力が働くので，Navier-Stokes 方程式 (5) は

$$\frac{\partial \boldsymbol{u}}{\partial t} = -\frac{1}{\rho}\nabla p - g\boldsymbol{e}_z \tag{10}$$

で近似される．ここで，g は重力加速度で，$\boldsymbol{e}_z$ は z 方向（= 鉛直上向き）の単位ベクトルである．一般に，Navier-Stokes 方程式から粘性項を除いたものを Euler 方程式という．密度 ρ は一定とし，速度場にはソレノイダル条件 (6) を課す．密度 $\rho = \text{const.}$ の場合，$\nabla \times \boldsymbol{u} = \boldsymbol{0}$ ならば，(5) に回転 $(\nabla\times)$ を作用させた方程式が自動的に満足されることがわかる．したがって，$\nabla \times \boldsymbol{u} = \boldsymbol{0}$，すなわち，流れは渦なしと仮定しよう．このとき，$\boldsymbol{u} = \nabla\phi$ ととることができる．ϕ を速度ポテンシャルという．条件 (6) に代入すると，ϕ は

$$\nabla \cdot \nabla\phi = \nabla^2\phi = 0 \tag{11}$$

を満足しなければならないことがわかる．

関係 $\boldsymbol{u} = \nabla\phi$ を (10) に代入すると，これは

$$\nabla\left(\frac{\partial \phi}{\partial t} + \frac{p}{\rho} + gz\right) = 0 \tag{12}$$

となり，

$$\rho\frac{\partial \phi}{\partial t} + p + \rho g z = f(t) \tag{13}$$

のように積分できる．右辺の $f(t)$ は時間 t についての任意関数である．これはポテンシャル流に対する Bernoulli の定理である．静止状態では水面 ($z=0$) で圧力 p が大気圧 p_a に等しいと課すと，$f(t)=p_\mathrm{a}$ と定まる．

さて，水面の変位は y 方向にはよらないと仮定し，水面の微小変位を $\zeta(x,t)$ ととろう．変位した水面 $z=\zeta(x,t)$ においても圧力が大気圧 p_a に等しいことを要請すると，境界条件の一つ

$$\frac{\partial\phi}{\partial t}+g\zeta=0 \quad \text{at} \quad z=\zeta(x,t)\approx 0 \tag{14}$$

が導かれる．線形近似の範囲内で，境界を $z=0$ ととってよい．もう一つの境界条件として，水面 $z=\zeta(x,t)$ の速度の法線成分と液体の速度の法線成分が水面 ($z=\zeta$) で一致することを要請する．水面は $F(x,z,t)=z-\zeta(x,t)=0$ とあらわされるので，法線ベクトルは $\boldsymbol{n}=\nabla F=(-\partial\zeta/\partial x,0,1)$ である．水面速度は $\boldsymbol{u}_\mathrm{s}=(0,0,-\partial\zeta/\partial t)$，流速は $\nabla\phi$ なので，境界条件は，水面 ($z=\zeta$) で $(\boldsymbol{u}_\mathrm{s}-\nabla\phi)\cdot\boldsymbol{n}=0$ とあらわせ，線形近似すると

$$\frac{\partial\zeta}{\partial t}=\frac{\partial\phi}{\partial z} \quad \text{at} \quad z=\zeta(x,t)\approx 0 \tag{15}$$

となる．2 つの境界条件 (14) と (15) から ζ を消去すると，ϕ に対する境界条件

$$\frac{\partial^2\phi}{\partial t^2}=-g\frac{\partial\phi}{\partial z} \quad \text{at} \quad z=0 \tag{16}$$

が導かれる．

水面下 ($z<\zeta(x,t)$) をみたす液体の運動は (11) を解くことによって求められる．水面の形を単色進行波 $\zeta(x,t)=\mathrm{Re}[A\exp\{i(kx-\omega t)\}]$ と仮定しよう．振幅 A は複素数で，Re[·] は実部をとることを意味する．実定数 k, ω をそれぞれ波数，周波数とよび，波長は $\lambda=2\pi/k$，振動数は $f=\omega/(2\pi)$ によって与えられる．この波は, 形を変えないで，x の正の方向に速度 $c_\mathrm{p}=\omega/k$ で伝播する．これを位相速度とよぶ．表面の形に呼応して，水面下の速度ポテンシャルは $\phi=\Phi(z)\exp\{i(kx-\omega t)\}$ の形をとる．無限の深さの場合，底 ($z=-\infty$) で有界であるために $\Phi\propto\exp(kz)$ と定まり，(11) の一般解が，任意定数 C を用いて $\phi=Ce^{kz}e^{i(kx-\omega t)}$ と求められる．これを境界条件 (16) に代入して，$C\neq 0$ を要請すると，ω と k の関係

$$\omega^2=gk \quad i.e.\ \omega=\sqrt{gk} \tag{17}$$

に導かれる．これを**分散関係**とよぶ．詳細については文献 [5] を参照されたい．

位相速度は $c_\mathrm{p}=\sqrt{g/k}$ である．一方，分散関係 $\omega=\omega(k)$ の k についての微分 $c_\mathrm{g}=d\omega/dk=\sqrt{g/k}/2$ を群速度とよぶ．これは波のエネルギーの伝播速度をあらわすのであるが，次節で述べる波の変調 (modulation) において，波群の伝播速度を与えることが明らかになる．

5　波の変調と非線形シュレディンガー方程式

水面波に限らず一般の波について，振幅や位相の変調が非線形 Schrödinger 方程式によって記述されることが簡単な考察からわかる．波をあらわす複素数値関数を $\psi=\psi(x,t)$ とかこう．分散関係が

$$\omega-\omega_0(k)+\gamma|\psi|^2=0 \tag{18}$$

のように振幅 $|\psi|$ に非線形的に依存することを仮定することは，ごく自然である．ここで，γ は定数である．線形部については，たとえば無限水深の水面波の場合，$\omega_0(k)=\sqrt{g/k}$ ととればよい．

前節では波の振幅 $C=\text{const.}$ を仮定したが，$k=k_0$ の近傍で振幅が時間的・空間的にゆっくり変化する（= 変調）としよう．

$$\psi = A(x,t)e^{i(k_0x-\omega_0t)};\quad \omega_0 := \omega_0(k_0). \tag{19}$$

振幅 $=A(x,t)$ は x と t についてゆっくり変化する複素数値関数である．非線形分散関係 (18) を $k=k_0$ のまわりで展開すると，

$$\omega-\omega_0(k_0)-\omega_0'(k_0)(k-k_0)-\frac{1}{2}\omega_0''(k_0)(k-k_0)^2+\gamma|\psi|^2+O\left((k-k_0)^3\right)=0 \tag{20}$$

となる．ここで，上付き記号 $(\,)'$ は微分をあらわす．以下では Taylor 展開の剰余項を無視する．一般に，周波数 ω と波数 k は，$\omega=i\partial/\partial t$, $k=-i\partial/\partial x$ のように，微分演算子で読み替えることが可能である．分散関係の展開形においてこの読み替えを行い，それに (19) を代入すると，振幅関数 A の発展方程式

$$i\frac{\partial A}{\partial t}+i\omega_0'\frac{\partial A}{\partial x}+\frac{1}{2}\omega_0''\frac{\partial^2 A}{\partial x^2}+\gamma|A|^2A=0 \tag{21}$$

が導かれる．引数を省略して，$\omega_0'=\omega_0'(k_0)$, $\omega_0''=\omega_0''(k_0)$ と微分係数を簡単に表示した．これを**非線形 Schrödinger 方程式**といい，さまざまな波動現象で登場する．非線形分散関係 (18)，そして，および波の変調をそれにもとづいて記述することが適切であることを物語っている．

Ginzburg-Landau 方程式 (21) と見比べられたい．虚数単位 i を除けば同じ形をしている．非線形 Schrödinger 方程式 (21) の第 2 項は，振幅の変化が群速度 $\omega_0'(k_0)$ で伝播することを意味する．群速度は文字通り波群が伝わる速度である．群速度 $\omega_0'(k_0)$ で動く座標系に乗ると，この第 2 項は消去できる．以下では，第 2 項を落として考える．

6　ベンジャミン・フェアの不安定性

一般的な形の非線形 Schrödinger 方程式

$$iA_t+\alpha A_{xx}+\gamma|A|^2A=0 \tag{22}$$

にしたがう波の安定性について考える．ここで，$A=A(x,t)$ は空間 1 次元の複素数値関数で，下付き添字はその添字についての偏微分をあらわす．定数 α と γ は実数ととる．定義式 (19) にもどって考えると，A はもとの波動場の振幅をあらわすので，波の振幅についての変調安定性を調べることに相当する．

6.1　ストークス進行波解

まず，(22) の進行波解を探そう．解を，定数 A_0 $(\neq 0)$ と θ_0 を用いて $A=A_0\exp\{i(\kappa x-\varpi t+\theta_0)\}$ とおいて (22) に代入すると，

$$\varpi=\alpha\kappa^2-\gamma|A_0|^2 \tag{23}$$

が得られる．この解があらわす波 (19) を **Stokes 進行波**または単に **Stokes 波**とよぶ．もとの変数 ψ にもどすと，(19) は

$$\psi = A_0 e^{i[(k_0+\kappa)x-(\omega_0+\varpi)t+\theta_0]} \tag{24}$$

となるので，Stokes 進行波の分散関係は

$$\omega_0 + \varpi = \omega_0(k_0) + \alpha\kappa^2 - \gamma|A_0|^2 \tag{25}$$

である．付加的な波数 $\kappa = 0$ のとき，(25) はもくろみ通り非線形分散関係 (18) に帰着する．ここでは，$\kappa \neq 0$ に一般化しておく．

計算するだけなら A を複素数のまま扱った方がエレガントであるが，実数化するとハミルトン構造があらわになる [3]．独立変数を x, t とする 2 個の実数値関数 $u_1(x,t)$ と $u_2(x,t)$ を用いて，振幅関数を $A = u_1 + iu_2$ とあらわそう．これを非線形 Shrödinger 方程式 (22) に代入すると，ベクトル関数 $\boldsymbol{u} = {}^t(u_1, u_2)$ に対する方程式

$$\mathsf{J}\boldsymbol{u}_t + \alpha\boldsymbol{u}_{xx} + \gamma\|\boldsymbol{u}\|^2\boldsymbol{u} = \boldsymbol{0}; \quad \mathsf{J} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{26}$$

に変換できる．ここで，上付き添字 t は転置をあらわす．したがって，$\boldsymbol{u}$ はたてベクトルである．また，$\|\boldsymbol{u}\| = (u_1^2 + u_2^2)^{1/2}$ は通常のベクトルのノルムである．Stokes 進行波解 (24) は，振幅 $A_0 = u_{01} + iu_{02}$ と位相 $\theta = (k_0+\kappa)x - (\omega_0+\varpi)t + \theta_0$ を用いて，

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \mathsf{R}_\theta \begin{pmatrix} ru_{01} \\ u_{02} \end{pmatrix}; \quad \mathsf{R}_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{27}$$

とあらわされる．

6.2 ストークス波の線形安定性

Stokes 波 (27) に，無限小振幅の撹乱 $\mathsf{R}_\theta\boldsymbol{v}(x,t)$; $\boldsymbol{v} = {}^t(v_1, v_2)$ を重畳しよう．撹乱を受けた振幅関数

$$\boldsymbol{u}(\boldsymbol{x},t) = \mathsf{R}_\theta\left[\boldsymbol{u}_0 + \boldsymbol{v}(\boldsymbol{x},t)\right] \tag{28}$$

を (26) に代入する．撹乱 $\boldsymbol{v}$ についての非線形項は無視し，分散関係 (23) から導かれる式 $\mathsf{J}\mathsf{R}_{\theta t} + \alpha\mathsf{R}_{\theta xx} + \gamma\|\boldsymbol{u}_0\|\mathsf{R}_\theta = 0$ や $\mathsf{R}_{\theta x} = \kappa\mathsf{J}\mathsf{R}_\theta$ を用いて簡単化をはかる．しかる後に左から R_θ の転置行列 ${}^t\mathsf{R}_\theta$ をかける．直交行列であることに由来する関係 ${}^t\mathsf{R}_\theta\mathsf{R}_\theta = \mathsf{I}$ (I は 2×2 単位行列)，${}^t\mathsf{R}_\theta\mathsf{J}\mathsf{R}_\theta = \mathsf{J}$ を用いると，撹乱に対する線形化方程式が

$$\mathsf{J}\boldsymbol{v}_t + 2\alpha\kappa\mathsf{J}\boldsymbol{v}_x + \alpha\boldsymbol{v}_{xx} + 2\gamma(\boldsymbol{u}_0\cdot\boldsymbol{v})\boldsymbol{u}_0 = \boldsymbol{0} \tag{29}$$

のように導かれる．

この式に

$$\boldsymbol{v}(\boldsymbol{x},t) = \boldsymbol{v}(t)\cos\sigma x + \boldsymbol{w}(t)\sin\sigma x \tag{30}$$

を代入しよう．同じ $\boldsymbol{v}$ を用いているが，混同しないように．空間依存性は三角関数のみにもたせてあるので，まず，$\cos\sigma x$ を含む項のみを集めると，

$$\mathsf{J}\dot{\boldsymbol{v}} + 2\alpha\kappa\sigma\mathsf{J}\boldsymbol{w} - \alpha\sigma^2\boldsymbol{v} + 2\gamma(\boldsymbol{u}_0\cdot\boldsymbol{v})\boldsymbol{u}_0 = \boldsymbol{0} \tag{31}$$

となる．上付きドットは時間 t についての微分をあらわす．次に，$\sin\sigma x$ を含む項のみを集めると，

$$\mathsf{J}\dot{\boldsymbol{w}} - 2\alpha\kappa\sigma\mathsf{J}\boldsymbol{v} - \alpha\sigma^2\boldsymbol{w} + 2\gamma(\boldsymbol{u}_0\cdot\boldsymbol{w})\boldsymbol{u}_0 = \boldsymbol{0} \tag{32}$$

となる．解を $\boldsymbol{v} = {}^t(q_1,q_2)e^{\lambda t}$, $\boldsymbol{w} = {}^t(p_1,p_2)e^{\lambda t}$ とおいて (31) と (32) に代入すると，λ に対する行列方程式

$$\mathsf{A}\begin{pmatrix}q_1\\q_2\\p_1\\p_2\end{pmatrix} = \boldsymbol{0};\ \mathsf{A} = \begin{pmatrix}-\alpha\sigma^2+2\gamma u_{01}^2 & -\lambda+2\gamma u_{01}u_{02} & 0 & -2\alpha\kappa\sigma\\ \lambda+2\gamma u_{01}u_{02} & -\alpha\sigma^2+2\gamma u_{02}^2 & 2\alpha\kappa\sigma & 0\\ 0 & 2\alpha\kappa\sigma & -\alpha\sigma^2+2\gamma u_{01}^2 & -\lambda+2\gamma u_{01}u_{02}\\ -2\alpha\kappa\sigma & 0 & \lambda+2\gamma u_{01}u_{02} & -\alpha\sigma^2+2\gamma u_{02}^2\end{pmatrix} \tag{33}$$

を得る．これが非自明な解 ${}^t(q_1,q_2,p_1,p_2)\neq\boldsymbol{0}$ をもつための必要十分条件は

$$\det A = \lambda^4 + 2(p^2+4\kappa^2\alpha^2\sigma^2)\lambda^2 + (p^2-4\kappa^2\alpha^2\sigma^2)^2 = 0;\quad p^2 := \alpha^2\sigma^4 - 2\gamma\alpha\|\boldsymbol{u}_0\|\sigma^2 \tag{34}$$

である．これを解くと，固有値が

$$\lambda^2 = -(p\pm 2\kappa\alpha\sigma)^2,\quad \text{すなわち}\quad \lambda = \pm i(p\pm 2\kappa\alpha\sigma) \tag{35}$$

と求まる．固有値，すなわち，スペクトルが 4 つ組であらわれるのは Hamilton 力学系特有の事情である [1]．λ が固有値ならば，その複素共役 $\bar\lambda$ のみならず $-\lambda$ も固有値である．後者は Hamilton 力学系の時間反転対称性を反映している．

実部が正の固有値が一つでもあると時間について指数関数的に増大する撹乱が作られる，すなわち，Stokes 波はスペクトル的不安定である．パラメータ p が実数であれば固有値が 4 個とも純虚数で，Stokes 波はスペクトル的安定であるが，p が純虚数になれば，(35) のうち 2 個の固有値が正の実部をもつようになり，撹乱は指数関数的に増大する，Stokes 波の振幅が小さいうち ($\|\boldsymbol{u}_0\| < \sqrt{\alpha\sigma^2/2\gamma}$) は p は純虚数であるが，振幅が大きくなり $\|\boldsymbol{u}_0\| = \sqrt{\alpha\sigma^2/2\gamma}$ を越えると正の実部をもつ固有値があらわれる．これを **Benjamin-Feir の不安定**という．水槽で Stokes 波をなんとか実現しようとしても，必ず波がくずれてしまうことから，この Benjamin-Feir の不安定性が発見された．これは**側帯波不安定（side-band 不安定）**である．波数 $k = k_0+\kappa$ をもつ Stokes 波 (24) において，k の近傍の有限バンド幅 2σ 内 ($\sigma^2 < 2\gamma\|\boldsymbol{u}_0\|^2/\alpha$) の波数をもつ撹乱が成長する．本小節の線形安定性解析を振り返ると，Stokes 波 (24) の振幅 A_0 に撹乱が加えられている．

$$\psi = [A_0 + B(x,t)]\,e^{i[(k_0+\kappa)x-(\omega_0+\varpi)t+\theta_0]};\quad B = B_0e^{i\sigma x+\lambda t}. \tag{36}$$

Stokes 波の波数 $k = k_0+\kappa$ は撹乱を受けて，$k_\pm = k_0+\kappa\pm\sigma$ に変わる．非線形 Schrödinger 方程式 (22) の非線形項 $\gamma|A|^2A$ を線形化した項は，基本場の波数 k と k_+ を非線形的に結合さ

せて波数 $2k-k+=k_-$ をもつ波を，k と k_- を非線形的に結合させて波数 $2k-k_-=k_+$ をもつ波を生み出す．すなわち，波数 k_+ と k_- をもつ側帯波は，基本場を (24) を介して共鳴して増幅する．

この不安定性をスペクトル的観点からながめてみよう．Stokes 波の振幅 $\|\boldsymbol{u}_0\|$ が小さいうちは固有値 (35) は 4 個とも複素 λ 平面の虚軸上にある．振幅を上げていくと，正の虚軸上，負の虚軸上にそれぞれ 2 個ずつある固有値が互いに接近する．臨界点 $\|\boldsymbol{u}_0\|=\sqrt{\alpha\sigma^2/2\gamma}$ において，固有値の対は $\lambda=2i\kappa\sigma$ と $\lambda=-2i\kappa\sigma$ でそれぞれ衝突し，さらに振幅を上げると，固有値を実部を獲得する．これが Hamiltonian Hopf 分岐である．Krein の理論によると [1, 7]，固有値が衝突後虚軸から逃れるための必要条件は，衝突前の一方の固有モードのエネルギーが正で他方のモードのエネルギーが負であることである．詳細は割愛するが，衝突前 $p>0$ ととると，$\lambda=\pm i(2\kappa\alpha\sigma+p)$ に対応するモードのエネルギーは正で，$\lambda=\pm i(2\kappa\alpha\sigma-p)$ に対応するモードのエネルギーは負であり，Krein 理論のシナリオにしたがう．

7　散逸が誘発する不安定性

散逸には，エネルギーを熱に変えて物体の運動を定常状態に落ち着かせようとする働きがある．この直感に反して，散逸があることによってかえって運動が不安定化することもある．前節の末尾で論じたように，Hamilton 系の不安定性は，典型的に，正エネルギー・モードと負エネルギー・モードの固有値が衝突 (= 縮退) することによって起こる，正エネルギーモードは，散逸によってエネルギーを奪われると振幅が小さくなるが，負エネルギーモードは，エネルギーを奪われると逆に振幅が増幅する．実は散逸に起因する不安定性は珍しいものではない．負エネルギーモードのなせるわざである．本節では，Benjamin-Feir 不安定が起こらないパラメータ領域においても，散逸，とくに，拡散によって不安定性が引き起こされることをみる [3].

7.1　散逸・拡散効果のある非線形シュレディンガー方程式

非線形 Schrödinger 方程式 (22) に散逸および拡散効果を付与しよう．

$$iA_t+(\alpha-ia)A_{xx}+ibA+(\gamma+ic)|A|^2A=0. \tag{37}$$

ここで，a, b, c は正の定数である．もとからあるパラメータを $\alpha=\gamma=0$ として，(37) から散逸および拡散効果のみを抜き取ると，

$$A_t=aA_{xx}-(b+c|A|^2)A \tag{38}$$

となる．右辺第 1 項は拡散項で，a (>0) が拡散係数を与える．残りの項は線形および非線形摩擦項である．

簡単のため $b=c=0$ ととって，拡散の効果だけをみていこう．包括的な解析については文献 [3] を参照されたい．Stokes 進行波解 $A=A_0\exp\{i(\kappa x-\varpi t+\theta_0)\}$ の分散関係は，(37) から

$$\varpi=\alpha\kappa^2-\gamma|A_0|^2-ia\kappa^2 \tag{39}$$

となる．もとの分散関係 (23) に末尾の項が付け加わっている．この項は Stokes 波を減衰させる．

7.2 ストークス波の線形安定性に対する拡散効果

一般化非線形 Schrödinger 方程式 (37) で $b = c = 0$ とおいたものを，$A = u_1 + iu_2$ によって実数値関数 $u_1(x,t)$, $u_2(x,t)$ で表示すると，(26) は

$$\mathsf{J}\boldsymbol{u}_t + \alpha\boldsymbol{u}_{xx} - a\mathsf{J}\boldsymbol{u}_{xx} + \gamma\|\boldsymbol{u}\|\boldsymbol{u} = \boldsymbol{0} \tag{40}$$

で置き換わる．実数表示の振幅を (28) のように Stokes 進行波解と撹乱 $\boldsymbol{v}$ の和であらわして (40) に代入し，撹乱振幅 $\|\boldsymbol{v}\|$ について線形化すると，

$$\mathsf{J}\boldsymbol{v}_t + 2\left(\alpha\kappa\mathsf{J} + a\kappa\right)\boldsymbol{v}_x + \left(\alpha - a\mathsf{J}\right)\boldsymbol{v}_{xx} + 2\gamma(\boldsymbol{u}_0\cdot\boldsymbol{v})\boldsymbol{u}_0 = \boldsymbol{0} \tag{41}$$

となる．空間波数 σ の撹乱形 (30) を (41) を代入すると，その $\cos\sigma x$ 成分および $\sin\sigma x$ 成分は，それぞれ，

$$\mathsf{J}\dot{\boldsymbol{v}} + 2\kappa\sigma\left(\alpha\mathsf{J} + a\right)\boldsymbol{w} - \sigma^2\left(\alpha - a\mathsf{J}\right)\boldsymbol{v} + 2\gamma(\boldsymbol{u}_0\cdot\boldsymbol{v})\boldsymbol{u}_0 = \boldsymbol{0}, \tag{42}$$

$$\mathsf{J}\dot{\boldsymbol{w}} - 2\kappa\sigma\left(\alpha\mathsf{J} + a\right)\boldsymbol{v} - \sigma^2\left(\alpha - a\mathsf{J}\right)\boldsymbol{w} + 2\gamma(\boldsymbol{u}_0\cdot\boldsymbol{w})\boldsymbol{u}_0 = \boldsymbol{0} \tag{43}$$

となる．解を $\boldsymbol{v} = {}^t(q_1, q_2)e^{\lambda t}$, $\boldsymbol{w} = {}^t(p_1, p_2)e^{\lambda t}$ とおいて (42) と (43) に代入すると，(33) における行列が

$$\mathsf{A} = \begin{pmatrix} -\alpha\sigma^2 + 2\gamma u_{01}^2 & -\lambda - a\sigma^2 + 2\gamma u_{01}u_{02} & 2a\kappa\sigma & -2\alpha\kappa\sigma \\ \lambda + a\sigma^2 + 2\gamma u_{01}u_{02} & -\alpha\sigma^2 + 2\gamma u_{02}^2 & 2\alpha\kappa\sigma & 2a\kappa\sigma \\ -2a\kappa\sigma & 2\alpha\kappa\sigma & -\alpha\sigma^2 + 2\gamma u_{01}^2 & -\lambda - a\sigma^2 + 2\gamma u_{01}u_{02} \\ -2\alpha\kappa\sigma & -2a\kappa\sigma & \lambda + a\sigma^2 + 2\gamma u_{01}u_{02} & -\alpha\sigma^2 + 2\gamma u_{02}^2 \end{pmatrix} \tag{44}$$

にとって代わられる．行列方程式 (33) が非自明な解 ${}^t(q_1, q_2, p_1, p_2) \neq \boldsymbol{0}$ をもつための必要十分条件 $\det A = 0$ から λ を求める手続きは前節と同じである．

拡散効果を摂動とみなし，微小パラメータ a/α について 1 次までの項のみを取り込もう．余因子展開を用いて行列式を計算すると，$O(a/\alpha)$ までで，

$$\begin{aligned} \det A = {} & \hat{\lambda}^4 + 2(p^2 + 4\kappa^2\alpha^2\sigma^2)\hat{\lambda}^2 - 32a\alpha\kappa^2\sigma^2(\alpha^2\sigma^2 - \gamma\|\boldsymbol{u}_0\|^2)\hat{\lambda} \\ & + (p^2 - 4\kappa^2\alpha^2\sigma^2)^2 + O\left((a/\alpha)^2\right) \end{aligned} \tag{45}$$

である．ここで，$\hat{\lambda} = \lambda + a\sigma^2$，$p$ は (34) と同じである．同じく，摂動展開で $\det A = 0$ の根を求めると，$p > 0$ の場合には，虚部が正の根は

$$\lambda = i(2\kappa\alpha\sigma \pm p) - a\sigma^2 \mp \frac{2a\kappa\sigma}{p}(\alpha^2\sigma^2 - \gamma\|\boldsymbol{u}_0\|^2) + O\left((a/\alpha)^2\right) \quad \text{（複号同順）} \tag{46}$$

と求まる．虚部が負の側にも根が実軸について対象にあらわれる．Benjamin-Feir 不安定が起こらないパラメータ領域 $p > 0$ においても，拡散効果が加わると，実軸に近い側の根（式 (46)

の下側の符号）の実部が正となり，撹乱は指数関数的に増大する．これは負のエネルギーをもつモードである．上側の符号に対応する正エネルギー・モードの実部は負で，こちらは拡散の効果によって減衰する．

散逸の効果 ($b > 0, c > 0$) もまったく同様に働く [3]．こうして，Hamilton 系に対する Krein の理論は系そのものの分岐構造のみならず，散逸や拡散の効果に対しても示唆するところ大である．最後に，Krein の理論が直接対象とするのは常微分方程式系，すなわち，有限自由度系であることに注意しておこう．本稿で扱っているのは偏微分方程式で記述される無限自由度系である．

8　結びにかえて

散逸（= 摩擦）が誘発する不安定性の例は枚挙にいとまがない．一番想像しやすいのは，垂直に立ってじっとまわっている独楽，すなわち，眠りごまであろう．摩擦がなければずっと立ち続けているが，摩擦の作用でやがて‘目が覚める’．負エネルギーの撹乱モードの存在は，このように，非自明な定常状態に特有である．静止状態（= 自明な定常状態）に加えられた微小撹乱は一般的には正のエネルギーしかもち得ない．われわれを取り囲む多様で変化に富む現象こそが負エネルギー・モードを紡ぎだしているのである．

参考文献

[1] Arnol'd, V. I., *Mathematical Methods of Classical Mechanics*, 2nd ed. (Springer-Verlag, 1989).

[2] Batchelor, G. K., *An Introduction to Fluid Dynamics*, (Cambridge University Press, 1967).

[3] Bridges, T. J. and Dias, F., Enhancement of the Benjamin-Feir instability with dissipation, Phys. Fluids **19** (2007) 104104.

[4] Huerre, P. and Rossi, M., Hydrodynamic instabilities in open flows, In *Hydrodynamics and Nonlinear Iinstabilities* (eds. C. Godrèche and P. Manneville, Cambridge University Press, 1998).

[5] 今井 功，流体力学，岩波全書（岩波書店，1970）．

[6] 今井 功，流体力学，前編（裳華房，1973）．

[7] MacKay, R. S., Stability of equilibria of Hamiltonian systems, In *Nonlinear Phenomena and Chaos* (ed. S. Sarkar, Adam Hilger, Bristol, 1986) pp. 254–270.

一様分布論とその応用

手塚　集

九州大学マス・フォア・インダストリ研究所

1　ディスクレパンシー

“ディスクレパンシー (discrepancy)”という概念は、19 世紀から 20 世紀初頭にかけてエルゴード理論との密接な関係もあって広く研究された「一様分布論」という数論の一分野に起源がある。もともと「一様分布論」は、ある空間における無限点列の（漸近的な）分布を議論する分野であったが、20 世紀前半に「無限点列」を「有限点列」に置き換えた時の分布の様子を研究することが主要なテーマとなっていった。人によってはこの分野を「Irregularities of Distribution（分布の不規則性)」と呼ぶこともある。そこでは、分布の不規則性、すなわち一様分布からのズレを測る尺度としてディスクレパンシーという量が定義され、ディスクレパンシーができるだけ小さい、つまり“一様性のできるだけ高い”有限点列を構成することが主要な研究テーマとなっている。

1.1　一様性の数学的定義

まず、無限点列の一様性から始めよう。その定義は次のようになる。

定義 1　X_n, $n = 0, 1, \ldots,$ を k 次元単位立方体 $[0,1]^k$ 内の無限点列とする。任意の k-次元区間 $[\mathbf{a}, \mathbf{b}) := \prod_{i=1}^{k} [a_i, b_i) \in [0,1]^k$（ここで $\mathbf{a} = (a_1, \ldots, a_k)$ および $\mathbf{b} = (b_1, \ldots, b_k)$ かつ $a_i < b_i$ $(1 \le i \le k)$ とする）に対して、

$$\lim_{N\to\infty} \frac{\#([\mathbf{a}, \mathbf{b}); N)}{N} = \prod_{i=1}^{k} (b_i - a_i),$$

となれば、無限点列 X_n, $n = 0, 1, \ldots$ は一様であるという。ここで、$\#(A; N)$ は区間 A に入る点 X_n, $n = 0, 1, \ldots, N-1$ の数を表す。

さて、この一様性と Riemann 積分の間には次のような関係がある。

定理 1　無限点列 X_n, $n = 0, 1, \ldots,$ が k 次元単位立方体 $[0,1]^k$ 内で一様であるための必要十分条件は、

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f(X_n) = \int_{[0,1]^k} f(\mathbf{x})\, d\mathbf{x},$$

である。ここで、f は $[0,1]^k$ 上で定義される任意の（Riemann 可積分）実数値関数である。

下の例は、一様分布する無限点列の代表的なものであり、1 次元の場合を Weyl 列、高次元の場合を Kronecker 列あるいは Richtmyer 列と呼んでいる。

例 1 点列 $(\{n\theta_1\},\ldots,\{n\theta_k\})$, $n=0,1,\ldots$, は、実数 $1,\theta_1,\ldots,\theta_k$ が有理数体上線形独立ならば一様となる。ここで、$\{x\}$ は実数 x の浮動小数部分をとることを意味している。

さて、次に有限点列の場合を考えよう。ディスクレパンシーの定義にはいくつかあるが、次に示すのが代表的なものである。

定義 2 X_n, $n=0,1,\ldots,N-1$, を k 次元単位立方体 $[0,1]^k$ 内の点集合 P_N とし、$\mathbf{t}=(t_1,\ldots,t_k)$ とする。そのとき、点集合 P_N に対するディスクレパンシーは

$$D_N^{(k)}=\sup_{\mathbf{t}\in[0,1]^k}\left|\frac{\#([\mathbf{0},\mathbf{t});N)}{N}-t_1\times\cdots\times t_k\right|$$

と定義される。

定義 1 と比べると $\mathbf{a}=\mathbf{0}$, $\mathbf{b}=\mathbf{t}$ となるような部分区間のみを対象としていることに注意したい。図 1 に $N=10$ の時の 2 次元の例を示す。この場合は

$$D_{10}^{(2)}=\sup_{(\alpha,\beta)\in[0,1]^2}\left|\frac{\#([(0,0),(\alpha,\beta));10)}{10}-\alpha\beta\right|$$

を計算することになる。

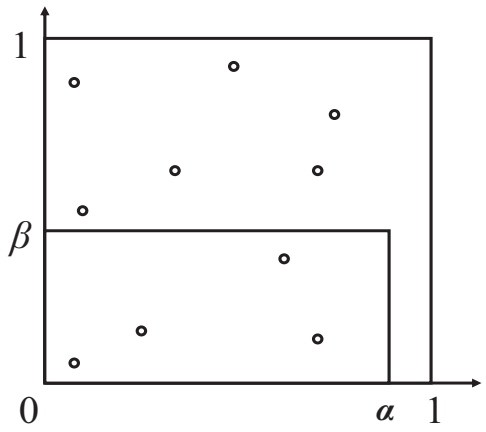


図 1：2 次元ディスクレパンシーの例

定理 1 の“無限点列”を“有限点列”に置き換えたとき、正しい積分値に収束していく様子を教えてくれる重要な定理がある。それは、60 年代に得られた Koksma-Hlawka の定理と呼ばれるもので、積分の収束の様子と先に述べたディスクレパンシーという量を定量的に結びつけた最初の結果として知られている。

定理 2 $D_N^{(k)}$ を k 次元単位立方体 $[0,1]^k$ 内の点列 $X_0,\ldots,X_{N-1}$ の L_∞-ディスクレパンシーとし、$V(f)$ を関数 $f(\mathbf{x})$ の Hardy-Krause の意味での変動とすると

$$\left|\int_{[0,1]^k} f(\mathbf{x})\,d\mathbf{x} - \frac{1}{N}\sum_{n=0}^{N-1} f(X_n)\right| \le V(f)D_N^{(k)}$$

が成り立つ。

この定理の重要な点は、右辺が 2 つのまったく意味の異なる量の積になっている点である。$V(f)$ は被積分関数のみで決まる量であり、点列によらない。一方、$D_N^{(k)}$ は点列の一様性のみで決まり、被積分関数によらない量である。被積分関数が与えられれば、ディスクレパンシーの小さい点列ほど積分誤差は小さくなることを示している。ただし、定義からわかるように、$V(f)$ という量はたとえ有界であっても非常に大きくなる。つまり、実際のアプリケーションで使えるような誤差評価には残念ながらなっていない。重要なことは、この定理により有限離散的な世界での研究対象であった“ディスクレパンシー”と連続無限な世界での研究対象である“積分”が明確につながったという点である。

1.2 超一様分布列

前節においてディスクレパンシーと高次元数値積分の誤差との重要な関係について述べた。簡単に言えば、ディスクレパンシーの小さい点列が数値積分の計算誤差を小さくするのである。では、ディスクレパンシーの小さい点列は実際にはどのように構成するのだろうか。それが本節の主題である。まず超一様分布列を定義しよう。

定義 3 超一様分布列は k 次元単位立方体内の無限点列であり、それを $X_0, X_1, \ldots$ と表す時、先頭の N 点からなる集合 $(X_0,\ldots,X_{N-1})$ がすべての $N>1$ に対して、

$$D_N^{(k)} \le C_k \frac{(\log N)^k}{N}$$

を満足するものである。ここで、C_k は次元 k のみに依存する定数。

$\log N$ の指数が k となっているのは次の理由による。もしそれが k より小さい値、例えば $k-1$ だったとして、次のような k 次元単位立方体内の N 点集合

$$\tilde{X}_n = \left(x_n^{(1)},\ldots,x_n^{(k-1)},\frac{n}{N}\right), \qquad n=0,1,\ldots,N-1,$$

を考えてみる。ここで $X_n = (x_n^{(1)},\ldots,x_n^{(k-1)})$, $n=0,1,\ldots,$ は $k-1$ 次元の超一様分布列とする。すると面白いことに、この N 点集合のディスクレパンシーが、任意の $N>1$ に対して、

$$D_N^{(k)} \le C_k \frac{(\log N)^{k-2}}{N}$$

となることを示すことができるのである。しかし、この結果は現在予想されている k 次元ディスクレパンシーの最適な上界に矛盾するので、結局 $\log N$ の指数は k より小さくできないこと

になる。言い換えれば、超一様分布列というのはディスクレパンシーの意味では最も一様な点列として定義されているのである。

以下、超一様分布列の構成法の1つである Halton 列を紹介しよう。まず、1次元超一様分布列として広く知られている van der Corput 列から始める。それは、基底逆関数と呼ばれるつぎのような写像に基づいている。

定義 4 $b > 1$ を整数とする。非負整数 n に対して、その b 進展開が $n = a_0 + a_1 b + \cdots + a_m b^m$ となるとき、基底逆関数は

$$\phi_b(n) := \frac{a_0}{b} + \frac{a_1}{b^2} + \cdots + \frac{a_m}{b^{m+1}}$$

と定義される。

このとき、van der Corput 列は次のように定義される。

定義 5 1次元点列

$$x_n = \phi_b(n), \quad n = 0, 1, 2, \ldots$$

を基底 b の van der Corput 列と呼ぶ。つまり、

$$x_n = \frac{x_{n,1}}{b} + \frac{x_{n,2}}{b^2} + \cdots + \frac{x_{n,m+1}}{b^{m+1}}$$

と書けば、$x_{n,j} = a_{j-1}$ となる。

基底 $b = 2$ の van der Corput 列は次のような無限列になる。

$$0, \frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{5}{8}, \frac{3}{8}, \frac{7}{8}, \ldots$$

これは、

$$0, \frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \frac{5}{8}, \frac{7}{8}, \ldots, \frac{1}{2^n}, \frac{3}{2^n}, \ldots, \frac{2^n - 1}{2^n}, \ldots$$

という無限列の順番を入れ替えただけであるが、前者は超一様分布列となる一方、後者はそうならないことが証明できる。大きな違いは、van der Corput 列では任意の引き続く2項 (x_n, x_{n+1}) をみると、1/2以上の数と以下の数が交互に現れていることである。さらに詳しく調べてみると、すべての $m > 0$ に対して、任意の $j \geq 0$ について、引き続く 2^m 項 $(x_{j2^m}, x_{j2^m+1}, \ldots, x_{(j+1)2^m-1})$ の各項が、区間 $[0, 1)$ を 2^m 等分した部分区間にちょうど1項ずつ落ちていることがわかる。こういう性質が、この数列を非常に一様なものにしている。

van der Corput 列を単純に k 次元に拡張したものを Halton 列と呼んでいる。

定義 6 k-次元点列

$$X_n = (\phi_{b_1}(n), \ldots, \phi_{b_k}(n)), \quad n = 0, 1, 2, \ldots,$$

を Halton 列という。ここで、$b_1, \ldots, b_k$ はどの2つも互いに素な正整数とする。

Halton 列という名の由来は、Halton が初めてこの数列が超一様分布列になることを証明したからである。具体的には次の定理である。

定理 3 任意の $N > 1$ に対して、Halton 列の先頭の N 点のディスクレパンシーは

$$D_N^{(k)} \leq C(b_1, \ldots, b_k)\frac{(\log N)^k}{N} + O\left(\frac{(\log N)^{k-1}}{N}\right)$$

となる。ここで、$C(b_1, \ldots, b_k)$ は定数。

この定理の証明は、次に示す有名な中国人剰余定理に大きく負っている。

定理 4 $b_1, \ldots, b_k$ をどの 2 つも互いに素な正整数とする。また $e_1, \ldots, e_k$ を正整数とし、$M = b_1^{e_1} \cdots b_k^{e_k}$ とする。任意の整数 $0 \leq N < M$ に対して、

$$N = n_i \pmod{b_i^{e_i}}, \quad i = 1, \ldots, k$$

（ここで $0 \leq n_i < b_i^{e_i}$ とする）と表すと、$(n_1, \ldots, n_k)$ と N は 1 対 1 に対応する。

中国人剰余定理と Halton 列の一様性との関係を見るには次のような部分区間を考えるとわかりやすい。

$$\prod_{i=1}^{k}\left[\frac{j_i}{b_i^{e_i}}, \frac{j_i+1}{b_i^{e_i}}\right)$$

ここで、$0 \leq j_i < b_i^{e_i}$ は整数であり、また部分区間の面積はすべて等しく $1/M$ となっていることに注意する。つまり、定義 6 からいえることは、Halton 列 X_n, $n = 0, 1, \ldots, M-1$ は、上の部分区間のおのおのにちょうど 1 点づつ落ちているということである。そしてこのことは任意の非負整数 $e_1, \ldots, e_k$ に関して言えるのである。Halton 列の持つこの“一様性”が、超一様分布列であることの証明に重要な役割を果たしている。

定理 3 において、係数 $C(b_1, \ldots, b_k)$ を最小にするには小さい順に k 個の素数を $b_1, \ldots, b_k$ に割り当てることである。Halton の証明から 30 年以上たって Atanassov は、k が十分大きければ、$C(b_1, \ldots, b_k) = O(1/(k2^k))$ となって、定数項は 0 に収束することを証明した。

2　金融問題への応用例

科学技術計算の分野において、数値積分の占める割合は非常に大きい。すでに低次元（5, 6 次元以下）では、いろいろ工夫された計算アルゴリズムがあり、その誤差についても、被積分関数の滑らかさに応じて解析がされている。しかし、それ以上に次元が高くなるといわゆる“次元の呪い (the curse of dimensionality)”のために低次元で有効なアルゴリズムがその有効性を失ってしまうことから、“最後の手段 (last resort)”としてのモンテカルロ法が一般に用いられている。ただ、モンテカルロ法は、誤差がサンプル数の平方根に反比例しているため、収束が非常に遅い。例えば、一桁精度を上げようとすれば、さらに 100 倍の計算時間が必要になるのである。そのため、60 年代すでに、このモンテカルロ法の問題点を克服するため先に述

べた“超一様分布列”（当時はまだ、“準乱数”と呼ばれていたが）を用いる試みがなされていた。特に、ソ連において水爆開発に必要となるモンテカルロ計算の高速化にこの超一様分布列が使われていたことは専門家の間ではよく知られている。ところが、そのころの実験結果などから導かれた結論は、高次元（50 次元以上）の数値積分計算では、超一様分布列は有効ではないということだった。文献によっては、せいぜい 12 次元ぐらいでその有効性はなくなるとしたものまであった。しかし、90 年代初め、特に金融工学に関連した高次元数値積分の計算が実用上重要になり、その高速化が不可欠 (Time is Money) なことから、（50 次元以上の）高次元積分の研究が米国において集中的におこなわれ、その結果、非常に高い次元（場合によっては 1000 次元以上）でも問題によっては、超一様分布列による高速化が可能になることがわかった（文献 [1] 参照)。

金融工学の現場において取引されているデリバティブのなかでも、取引量が巨大でかつ商品としても複雑なものが MBS (Mortgage-Backed Securities) という住宅ローン債権を担保として発行される証券である。2008 年のリーマン・ショックの原因となったことから今では一般にも広く知られている金融商品である。MBS の価格計算問題を、パススルー証券と呼ばれる最も単純な証券で説明しよう。考えているのは、貸し出し金利 r_0 の元利均等方式による 30 年の住宅ローンで、毎月の返済額を C とする。そして、各 $k = 1, 2, \ldots, 360$ に対して、

r_k：第 k 月目の金利（月率）

w_k：第 k 月目に（全額）期限前償還が起きる確率

$B_k = C(1 + 1/(1 + r_0) + \cdots + 1/(1 + r_0)^{360-k})$：第 k 月目の元本残高

と定義しよう。

また、金利 r_k は Black モデル、すなわち $k = 1, 2, \ldots, 360$ に対して、

$$r_k = K_0 \exp(\sigma z_k) r_{k-1},$$

に従うものとする。ここで K_0 は定数とし、z_k, $k = 1, 2, \ldots, 360$ は独立な標準正規分布と仮定する。

期限前償還の確率 w_k, $k = 1, 2, \ldots, 360$ は、ここでは、金利 r_k, $k = 1, 2, \ldots, 360$ のみに依存すると考えている。具体的には

$$w_k = K_1 + K_2 \arctan(K_3 r_k + K_4)$$

のようにモデル化する。ここで、K_1, K_2, K_3, および K_4 は定数項であり、金利が低ければ期限前償還が増え、金利が高くなるにつれて減少するように決められている。

さて、このような仮定のもとに第 k ヶ月目のキャッシュフローは

$$M_k(r_1, \ldots, r_k) = (1 - w_1) \cdots (1 - w_{k-1})(C(1 - w_k) + B_k w_k)$$

と表せる。ここで、$w_k(r_1, \ldots, r_k)$, $k = 1, 2, \ldots, 360$ は期限前償還率を表している。すると将来 30 年間（360 ヶ月）にわたって生じるキャッシュフローの現在価値は、割引率

$$d_k(r_1, \ldots, r_{k-1}) = \prod_{i=0}^{k-1} \frac{1}{1 + r_i}$$

を掛けて、

$$PV(r_1,\ldots,r_{360}) = \sum_{k=1}^{360} d_k(r_1,\ldots,r_{k-1}) M_k(r_1,\ldots,r_k) \tag{1}$$

と表すことができる。金利 $r_1,\ldots,r_{360}$ が確率変数 $z_1,\ldots,z_{360}$ の関数であることから、最終的に求めたいものは次のような期待値となる。

$$\mathrm{E}(PV) = \frac{1}{(2\pi)^{180}} \int_{\mathrm{R}^{360}} PV(z_1,\ldots,z_{360}) \exp\left(-\frac{z_1^2+\cdots+z_{360}^2}{2}\right) dz_1\cdots dz_{360}$$

つまり、360 次元の積分を計算するのである。

注 1 このモデルは、非常に単純化したものであることに注意したい。期限前償還は全額返済を仮定しており、また金利モデルも最も単純な幾何 Brown 運動である。実際に金融工学の現場で使われているモデルでは、部分返済も当然考慮されているし、金利モデルももっと複雑なものが使われている。

注 2 ここで紹介した MBS は、パススルー証券といわれる最も単純な MBS である。その他に、CMO (Collateralized Mortgage Obligation) と呼ばれる MBS があり、アメリカでは巨大な市場を形成している。この商品はパススルー証券を小さく切り分けて別々の証券として販売するというもので、この場合の価格計算は非常に複雑になる。

金融工学で現れる積分計算問題は、多くの場合次のような形をとることが知られている。

$$J(p) = \frac{1}{(\sqrt{2\pi})^k |C|^{1/2}} \int_{\mathrm{R}^k} p(\mathbf{v}) \exp\left(-\frac{1}{2}\mathbf{v}C^{-1}\mathbf{v}^{\mathrm{T}}\right) d\mathbf{v},$$

ここで、$p(\mathbf{v})$ は k 次元行ベクトル $\mathbf{v}$ を変数とする支払い関数、C (共分散行列) は対称正定値 $k\times k$ 行列で、$|C|$ は行列式を表す。変数変換すればこの積分は

$$J(p) = \frac{1}{(\sqrt{2\pi})^k} \int_{\mathrm{R}^k} p(A\mathbf{z}^{\mathrm{T}}) \exp\left(-\frac{\|\mathbf{z}\|^2}{2}\right) d\mathbf{z}.$$

となる。ここで、A は $AA^{\mathrm{T}} = C$ を満足する $k\times k$ の実行列である、また $\|\mathbf{z}\|$ は k 次元ベクトル $\mathbf{z} = (z_1,\ldots,z_k)$ の L_2-ノルム（ユークリッドノルム）を表している。

実際のインプリメンテーションでは、この積分の積分区間を、次のように k-次元単位立方体に変数変換している。

$$x_i = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z_i} \exp\left(-\frac{z^2}{2}\right) dz, \quad i = 1,\ldots,k,$$

$$\prod_{i=1}^{k} \frac{dx_i}{dz_i} = \frac{1}{(\sqrt{2\pi})^k} \exp\left(-\frac{\|\mathbf{z}\|^2}{2}\right).$$

つまり、

$$J(p) = \int_{[0,1]^k} p\left(A\left(\mathbb{N}^{-1}(x_1),\ldots,\mathbb{N}^{-1}(x_k)\right)^{\mathrm{T}}\right) d\mathbf{x}.$$

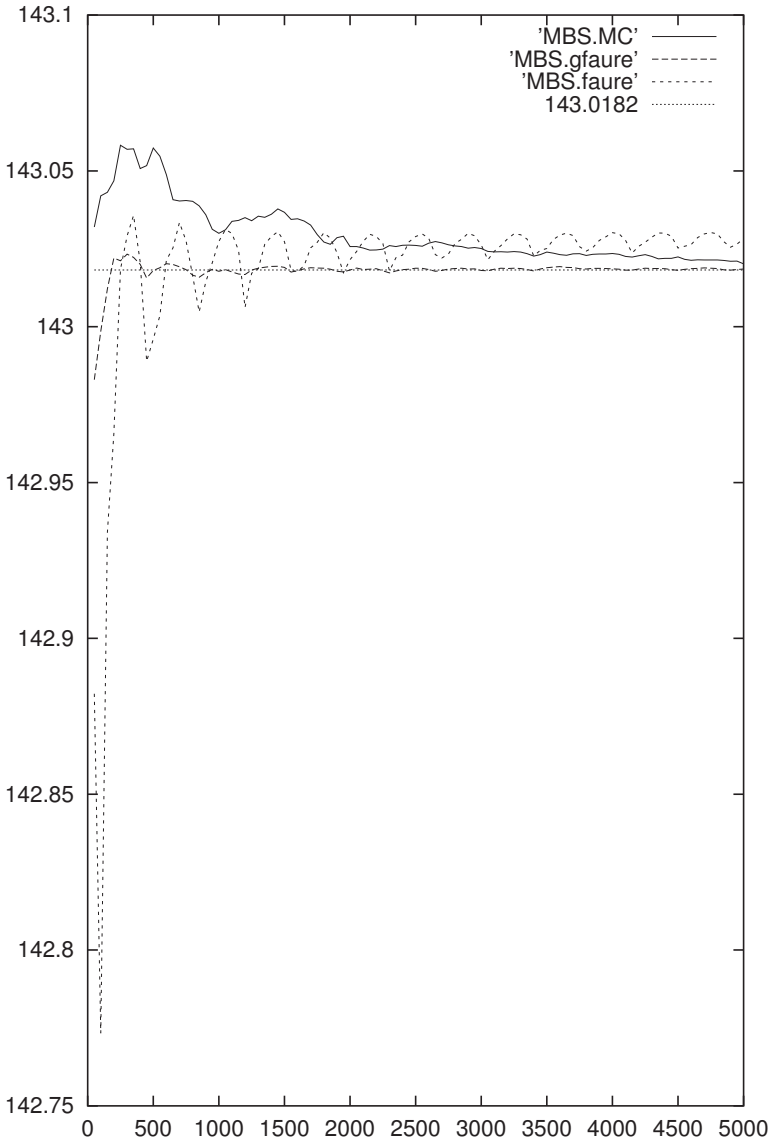


図 2：乱数列と超一様分布列の収束の比較：MBS の場合（縦軸が価格、横軸はサンプル数）

となっている。

先にも述べたように、金融工学では次元 k は数百次元（ときには 1000 次元以上）にもなり、そういった高次元積分を高速に計算することが求められている。

図 2 に計算例を示す。乱数列と超一様分布列の比較である。超一様分布列としては Faure 列と金融の現場で広く用いられている一般化 Faure 列の 2 つを用いた。これらの超一様分布列の詳細については文献 [2] を参照されたい。実線 (MBS.MC) は、乱数列（モンテカルロ法）の結果を示している。2 つの破線（MBS.faure および MBS.gfaure）は、それぞれ 2 種類の超一様分布列の結果である。すると、次の 2 つの比較が可能となる。

(1) 乱数列 vs. 一般化 Faure 列

(2) Faure 列 vs. 一般化 Faure 列

例えば、図 2 において 1000 サンプル点のところでみると一般化 Faure 列の結果はほぼ収束している。一方、乱数列および Faure 列の結果はだいたい同じような精度であり、一般化 Faure 列に比べ約 1 桁精度が低い。もともとモンテカルロ法は確率的な手法であり、それに対し、超一様分布列は決定的な手法なので、両者の収束のスピードを比較するのも簡単ではないが、よく使われるひとつの方法は、精度が 1 桁違うということに着目するもので、それによれば「超一様分布列により約 100 倍のスピードアップが得られた」と言うことができる。また、超一様分布列もその種類によって実用上の有用性には大きな違いがあることが分かる。

参考文献

[1] 手塚　集、ウォール街を動かすソフトウエア、岩波書店、2002.

[2] 手塚　集、「超一様分布列の数理」、計算統計 I、岩波書店、2003.

純粋と応用は交錯する
―初期無限解析における観察の一例―

高瀬　正仁
九州大学マス・フォア・インダストリ研究所

1　オイラーの言葉より

歴史家の視点から純粋数学と応用数学の連繋について考察してみたいと思います。数学史を回想すると、数学的科学を純粋と応用に分けようとする意識は早くからあったようで、19 世紀のはじめにクレルレがベルリンで創刊した数学誌の誌名は、すでに「純粋数学と応用数学のためのジャーナル」というのでした。もう少しさかのぼると、純粋数学と応用数学を対比させて語られたオイラーの言葉が念頭に浮かびます。それはオイラーの論文「負数と虚数の対数に関するライプニッツとベルヌーイの論争」(1749/51 年) の書き出しのあたりに出ているのですが、オイラーはこう言っています。

> 数学者たちの考えは応用数学に関連する諸問題については大いに異なることがありうる。応用数学の場では、いろいろなテーマを考察し、それらのテーマを精密な諸概念へと帰着させていく際に採用される道筋の多彩さのため、現実的な論争が引き起こされることがある。
>
> ところが数学の純粋な諸分野はそんな論争の的から完全に免れていて、そこには真実と虚偽のいずれかを証明することのできない事柄は何もないことを、常々誇りにしていたのである。(参考文献 [4])

オイラーの論文に先立って、負数と虚数の対数 $\log(-1)$、$\log(\sqrt{-1})$ の実体をめぐってライプニッツとヨハン・ベルヌーイが論争めいたやりとりを交わしていた一時期があり、オイラーはその論争の成り行きを踏まえたうえで上記のように発言したのでした。オイラーの見るところ、負数と虚数の対数とは何かと問う問いは純粋数学のテーマですが、ライプニッツとヨハン・ベルヌーイの論争は全体に曖昧模糊とした印象に覆われていて、どちらが正しいとも言えないままに推移して、いつしか立ち消えになりました。これを受けてオイラーは、純粋数学では真実と虚偽を識別しえないようなことはありえないのであり、そのことを「常々誇りにしていたのである」というのです。これに対し、応用数学ではそうではなく、現実的な論争が起るのが通常の姿なのだとのこと。数学における純粋と応用の区別をここまで明晰判明に語った言葉を目にしたのははじめてで、その後も見たことがありません。

それでオイラーは何をもって応用数学と見ているのかということが気に掛かりますが、ここから先は自分で考えてみたいと思います。純粋数学という名に相応しい数学が存在することを前提にすると、純粋数学を使って何事かがなされたなら、そこに応用数学が発生する場が開

かれたような印象を受けるのではないかと思います。普通、応用数学と言われている数学はたいていはそのようなものですが、それとは別に、純粋とも応用ともいえない独自の数学的科学も存在するのではないかと、つい最近思い始めました。きっかけになったのはガウスの『誤差論』（参考文献 [1]）です。

2　ガウスの『誤差論』

ガウスの『誤差論』は飛田武幸先生が翻訳した論文集で、昭和 56 年（1981 年）5 月に紀伊国屋書店から刊行されました。全部で 8 篇の論文が収録されていますが、根幹を作るテーマは天体観測における誤差の修正に関する事柄で、誤差を最小にする方法として最小 2 乗法が提案されたり、天体の軌道決定のために確率論的考察が展開されたりしています。天体の軌道決定と確率論がどうして関係があるのかというと、軌道決定というのはつまり将来の位置の予測ということですし、「予測する技術」こそ、確率論の本来の面目であるからです。「予測する技術」というのは、ヤコブ・ベルヌーイの確率論の古典的傑作の書名でもありました。

純粋数学というと「数学のための数学」というか、物理的自然現象や人の世に生起するあれこれのこととはまったく無関係に、どこかしら理念的世界に存在する理論体系のようなイメージがあります。あまり大雑把に考えても仕方がありませんので、数学の世界で実際に見聞した諸事実から拾ってみることにしますが、ガウスの整数論などは純粋数学という感じがします。数論に例を求めるのであれば、フェルマの数論も純粋数学の範疇に入りそうです。ライプニッツとヨハン・ベルヌーイは負数や虚数の対数の姿を追い求め、その思索を継承したオイラーは対数の無限多価性を明らかにしましたが、このような究明も純粋数学というほかはありません。これに対し、応用数学というときの「応用」の一語には、純粋数学の諸理論の応用という感じがあります。実際のところ、応用数学のイメージはだいたいにおいてそんなところなのであろうと思います。

ここでとりあえず述べたのは純粋と応用に対する素朴なイメージですが、ではガウスの『誤差論』はどうでしょうか。天体観測の誤差を修正するための工夫ですから、ちょっと考えると応用数学の典型例のような気がするのですが、実際に手に取ってあちこちを眺めると、応用数学の一般的なイメージとは大きく乖離しています。この方面のことは理解が行き届きませんので、漠然とした印象しか口にできないのですが、何というか、「誤差の修正というテーマの中で新しい数学が創造されている」というのが、この書物から受ける率直な印象です。確率論が応用されているというよりも、かえって誤差論の中から確率論が創造されているという感じですが、こんな印象を受けることになるとはまったく想定していませんでした。

ガウスの『誤差論』から受けた不思議な印象を数学的内容に即して語ることはできませんが、既視感というか、どこか別のところで見たことがあるようでもありました。それで数学史を回想してみたのですが、たとえば草創期の無限解析の中に具体的な事例が観察されるように思います。イギリスのニュートンのことはひとまず措くことにしますが、ヨーロッパ大陸の無限解析はライプニッツの 2 篇の論文に始まります。ひとつは 1684 年の微分計算の論文、もうひとつは 2 年後の 1686 年の積分計算の論文です。この 2 篇の論文がドイツのライプチヒで発行されていた学術誌「アクタ・エルディートルム（数学年報）」に掲載された当時、ベルヌー

イ兄弟（兄のヤコブと弟のヨハン）はスイスのバーゼルにいたのですが、ライプニッツの論文を見て大いに心を惹かれたようで、協力して解読作業を始めました。ところがライプニッツの論文は謎めいた文言に満たされていて、魅了されながらもなかなか理解できなかったため、ライプニッツに手紙を書きました。ライプニッツもこれに応じ、それから往復書簡が交わされ始めて 10 年ほど続きました。無限解析はこの長期にわたる数学的書簡の蓄積の中から、わずかに 3 人の担い手により誕生しました。

無限解析の成立に先立って曲線の理論の時代、すなわち「人々が曲線に関心を寄せた時代」がありました。デカルトの『方法序説』の刊行は 1637 年。序説で表明された方法の適用例として屈折光学、幾何学、気象学が語られましたが、本稿で注目したいのは幾何学です。三部構成で叙述されているのですが、第 2 部には「曲線の性質について」という表題が附され、ここで今日の解析幾何のアイデアが表明されました。後年の解析幾何学の嚆矢ですが、曲線に寄せる関心ということならデカルト以前にも見られ、長い歴史が経過しています。デカルトはそこに「曲線を方程式で表す」というアイデアを提案しました。

3　デカルトの葉

曲線に寄せる関心は非常に古く、古代のギリシアの数学にも、ニコメデスのコンコイド、ディオクレスのシソイド、アルキメデスの螺旋、それにアポロニウスの円錐曲線等々、さまざまな曲線が登場していました。この傾向はヨーロッパ近代の数学にも受け継がれ、発見され、研究される曲線は増えるばかりでした。デカルトが提案したアイデアによれば、それらの曲線はたいていはみな $f(x,y)=0$ という形の方程式で表されます。

「すべての曲線」と言わずに「たいていはみな」と言ったのはなぜかというと、「方程式 $f(x,y)=0$」というとき、「$f(x,y)$ とは何か」というところに大きな問題がひそんでいるからです。後年のオイラーによる関数概念の提案につながる問題ですが、デカルトが「曲線を方程式で表す」というアイデアを提示した段階では $f(x,y)$ は x と y の多項式でした。多項式なら加減乗除の四則演算だけで構成されますから、多項式に限定するという方針を堅持する限り問題は発生しません。ただし、思索の対象は「代数的な曲線」に限定されます。「代数的な曲線」という観念がはじめにあって、それらを多項式を用いて $f(x,y)=0$ と表示したのではなく、多項式を用いて表示される曲線を指して「代数的な曲線」と呼んだことになりますが、ともあれこれで代数曲線全体の作る世界を展望することができるようになりました。

サイクロイドのように、代数的ではないけれども人々の深い関心を集めた曲線もありますが、それらは一括して「超越的な曲線」と呼ばれ、「代数的な曲線」と区別されました。

既知の代数曲線は代数方程式で表示され、さまざまな仕方で描かれる曲線も、それが代数的である限り代数方程式で表示されますが、デカルトのアイデアの真に恐るべき点は、「方程式から出発した」ことでした。一番はじめに代数方程式 $f(x,y)=0$ を書き下し、それにより表示される曲線を考えていくという順序になりますが、このアイデアにより「すべての代数的な曲線の作る世界」が生成されました。『方法序説』が刊行された年の翌 1638 年には、デカルトはメルセンヌに宛てた書簡の中で $x^3+y^3=axy$（a は定数）という方程式を書き、それが表す曲線の概形を描きました。後年、「デカルトの葉」と呼ばれることになる代数的な曲線です。

デカルトは方程式から出発する姿勢をみずから率先して示したかったのでしょう。

4　曲線の理論から無限解析へ

曲線に寄せて異様に熱意のある関心が示された時代は確かに存在し、いろいろな曲線に接線や法線を引いたり、曲がり具合を調べたり、曲線の囲む領域の面積を求めたりと、さまざまに工夫が凝らされたものでした。その際のあれこれの工夫は個々の曲線に付随する固有の性質に沿って個々別々に考案されたのですが、ライプニッツが提案し、ベルヌーイ兄弟との往復書簡を通じて完成された無限解析の出現に伴って、この時代に区切りがつきました。1696 年にはマルキ・ド・ロピタルの著作『曲線の理解のための無限小解析』が刊行されました。これは数学史の流れに登場した一番はじめの微積分のテキストですが、注目に値するのはこの著作のタイトルで、無限解析は「曲線を理解するための理論」であることがはっきりと記されています。

無限解析の力はきわめて強く、接線についていえば、どのような曲線が提示されたとしても、任意の点において自在に接線を引くことができるようになりました。もっとも「接線が存在する場合には」という前提のもとでのことではありますが、もはや個別の工夫は不要になり、そのうえ代数曲線のみならず超越的な曲線をも対象にして、「万能の接線法」が手に入ったことになります。デカルトの『方法序説』が刊行されたのは 1637 年。ライプニッツの微分計算と積分計算の 2 編の論文が公表されたのは、それぞれ 1684 年と 1686 年です。この間に 50 年ほどの歳月が流れ、無限解析の誕生により曲線の理論が完成したのですが、このめざましい情景はガウスの誤差論の開く世界に酷似しています。

ガウスは天体観測の誤差の修正を工夫する中で新しい数学理論を創造しましたが、17 世紀の数学者たちは曲線について知りたいという熱情に心を奪われて、その数学的想念から無限解析という名の理論体系が生成されました。何事かに心を奪われるという状況が先にあり、その何事かを追い求める情熱から数学が生まれるという状況はまったく同じです。何かしら完成した数学理論がはじめに存在していて、それを適用する領域を見つけて新たな知見を得るというのではなく、知りたいという熱情と数学の創造が不可分に連繋しています。熱情のおもむくところに数学が生まれています。それで、ここにおいてあらためて思うのですが、人の熱情の向かう先が天体のような天然自然の現象の場合に生まれる数学がつまり応用数学であり、曲線のような数学的自然内の現象に向かうときに生まれるのが、純粋数学ということなのではないでしょうか。

伝統的な言葉遣いに配慮して純粋数学と応用数学を使い分けてみましたが、実のところ理論そのものには応用も純粋もなく、ただ「数学そのもの」というほかはありません。ガウスの『誤差論』を眺めながら無限解析の形成史を回想し、おおよそこんなことを思いました。

5　オイラーの無限解析

オイラーは数学的科学に「純粋数学」と「応用数学」の区分けが存在することを自覚して、わずかな言葉を書き留めましたが、これだけを手掛かりにして応用数学というものの実体に迫るのは困難でした。ところが飛田先生に教えられてガウスの『誤差論』を見ているうちに、は

たと思い当たるところがありました。それはつまり数学の理論そのものには純粋も応用もないという簡明な一事なのですが、この認識はわれながら意外でもありました。

それでもうひとつの事例としてオイラーの無限解析を挙げてみたいと思います。ライプニッツとベルヌーイ兄弟の手で形成された無限解析により、曲線の理論が終着点に到達したことは上述の通りですが、それならそれ以降の無限解析はどのような道を歩んだのでしょうか。もう少し具体的に言うと、ライプニッツとベルヌーイ兄弟の次の時代を生きたのはオイラーですが、無限解析の領域においてオイラーの心情はどのような事象に向けられていたのでしょうか。曲線の理論に決着がついた以上、オイラーの心はもう曲線から離れていたことと思いますが、オイラーの初期の著作や論文を参照すると、力学と変分法にテーマを求めようとしている様子が顕著です。著作でいうと、1736 年には『力学』が出ています。全 2 巻の作品で、エネストレームナンバーはそれぞれ 15 と 16 です。1736 年のオイラーは 29 歳でした。それから 1744 年には『極大もしくは極小の性質を備えた曲線を見つける方法。すなわちもっとも広い意味で諒解された等周問題の解法』という傑作が出ています。エネストレームナンバーは 65。オイラーは 37 歳でした。

動くものの軌跡は曲線を描きますから、力学は曲線の理論を基礎にして理解できそうです。また、変分法の契機になったのはヨハン・ベルヌーイが提示した最速降下曲線を求める問題ですから、これもまた曲線の理論に端を発しています。こうしてみるとオイラーは曲線の理論を踏まえたうえで、その先に開かれていく世界を展望していたことがわかりますが、力学と変分法に向かったのはなぜかというと、ニュートンの力学が念頭にあったからでした。『力学』というタイトルの著作ばかりではなく、変分法もまたオイラーにとっては力学の基本原理の探究であったことは周知の通りですが、これを要するにライプニッツとベルヌーイ兄弟の無限解析の力をもってニュートンの力学を理解しようとしたところに、オイラーの数学的企図があったということになります。この流れの中で無限解析の姿もまた大きな変容を重ねていきました。

このあたりのことは通説の通りとして、ここで問題にしたいのはオイラーの無限解析は純粋数学なのか、あるいは応用数学と見るべきなのか、どちらなのだろうということです。オイラーの無限解析の実体をひとことで言うと微分方程式の解法理論にほかなりませんが、微分方程式ならライプニッツとベルヌーイ兄弟の時代にもありました。ただし、オイラー以前の微分方程式は曲線の理論の中で考えられていましたから、微分方程式というよりも、曲線の接線や法線の状況を指定する方程式というほどの意味合いのものでした。念頭にあるのはつねに曲線で、接線や法線がかくかくしかじかという状勢下にあることが判明しているとして、そのような曲線の全体像を復元することをねらい、その方法を「逆接線法」と呼んでいました。微分方程式論の視点に立てば、逆接線法というのはつまり積分法と同じです。

曲線に接線を引くのが微分法で、逆接線法が積分法ということになりますが、そんなふうに見ること自体、視点はすでにオイラーの無限解析の世界に移っています。

オイラーの無限解析はもう曲線の理論ではありません。オイラーは関数の概念を数学に導入し、曲線を関数のグラフと見る視点を確立し、曲線から関数へと視線を移しました (参考文献 [2, 3])。こうすることによって無限解析の主役は関数になり、接線や法線に関する情報は微分方程式の形で提示され、逆接線法は積分法になりました。この場合、積分法は微分方程式の解法と同じ意味になります。曲線の理論のはじまりのころ、デカルトは方程式で表される図形

を指して曲線と呼ぶというアイデアを提案しましたが、オイラーはさらにもう一度、曲線の概念を変えたことになります。

オイラーの無限解析の実体は微分方程式の解法理論ですから、それ自体には応用数学という印象はありませんし、むしろ純粋数学のように見えるのですが、出所は力学です。力学に寄せる深刻な関心の中から非常に一般的で抽象的な数学理論が生まれたということになりますが、微分方程式論それ自体は純粋数学でも応用数学でもなく、端的に「数学の理論」というほかはありません。微分方程式論は純粋数学か応用数学かと問うこと自体、あまり意味のないことで、「力学を契機として創造された数学」というくらいに見ておくのが妥当かもしれません。

代数方程式論で考えてみると、3 次方程式や 4 次方程式の代数的解法を探索したりするのは数学の内部で観察される事象の観察ですが、ここからガウスの円周等分方程式論やアーベルの「不可能の証明」やガロアのガロア理論のような数学が生まれました。ほかにもいろいろな事例が挙げられそうに思います。

こうしてみると「数学の世界」というのは確かに実在し、そこにはライプニッツとヨハン・ベルヌーイの無限解析やオイラーの無限解析、ガウスの円周等分方程式論、アーベルの「不可能の証明」、ガロアのガロア理論など、多種多様な理論が共存しています。通常のイメージからすると、それらはみな「純粋数学」と呼ぶのが相応しそうに思います。これに対し、通常の語感からすると保険数学などはいかにも応用数学のような感じがしますが、応用数学を上記のように理解するのであれば、保険数学はむしろ実用数学と呼ぶほうが相応しい感じがします。

オイラーの無限解析の出自は力学ですが、既成の微分方程式論を力学に応用したのではなく、根底には力学を曲線の理論の視点に立って理解しようとする数学的企図が控えていました。曲線の理論を応用したというのでもなく、むしろ「枠組みをあてはめた」というほうがよさそうです。すると、力学の側から要請される事柄もあることですし、従来の曲線の理論の側でも変容を迫られて、オイラーの無限解析、すなわち微分方程式論が生まれるという成り行きになりました。

オイラーは「オイラーの無限解析」を応用数学と見ていたのではないかと、このごろ思うようになりましたが、それは理論形成の契機が数学以外のところにあったという意味であり、「オイラーの無限解析」それ自体は整数論などと同等の数学的科学の一領域であり続けています。それゆえ「純粋と応用は交錯する」と、現在の時点では考えています。

参考文献

[1] ガウス『誤差論』. 飛田武幸・石川耕春訳, 紀伊国屋書店, 昭和 56 年（1981 年）5 月.

[2] 高瀬正仁『オイラーの無限解析』（レオンハルト・オイラーの著作『無限解析序説』全 2 巻の巻 1 の翻訳書）. 海鳴社, 平成 13 年（2001 年）6 月.

[3] 高瀬正仁『オイラーの解析幾何』（レオンハルト・オイラーの著作『無限解析序説』全 2 巻の巻 2 の翻訳書）. 海鳴社, 平成 17 年（2005 年）11 月.

[4] 高瀬正仁『無限解析のはじまり　わたしのオイラー』筑摩書房（ちくま学芸文庫 Math & Science）, 平成 21 年（2009 年）7 月.

ヘッド・ディスク媒体インターフェースの数理モデル

岡田　勘三

九州大学マス・フォア・インダストリ研究所

1　はじめに

磁気ディスク装置はコンピュータを構成する主要な情報機器である。高速で回転する磁気ディスク媒体上に磁気ヘッドを浮上させる浮動ヘッドスライダ機構とそれに伴うトライボロジは磁気ディスク装置の最も特徴的な技術のひとつであり、その高密度化に長期に亘り最も貢献してきた技術である。その最先端は原子・分子レベルの力学現象を探求する科学の領域である。

磁気記録の原理から、記録密度を高めるためには、ヘッド・媒体間の浮上すきまをできる限り小さくする必要がある（図 1 参照）。20 年前に 80 ナノメータくらいの浮上すきまが製品化されており、現在ではそれよりさらに 1 桁少ない数ナノメータの浮上すきまが実験室レベルで実現されている [1]。磁気ディスク業界でよく使われる類比であるが、長さ 0.85 ミリメータのヘッドがディスク媒体面上を 10 ナノメータ前後で浮上していることは、62.8 メータの最新ボーイング 787 機が地上 1 ミリメータ弱で安定飛行しているのと同じである！ 高記録密度化による浮上すきまの著しい減少に伴い、気体分子の平均自由行程（分子の平均衝突頻度の逆数と分子の平均の速さの積で、たとえば 0 °C、1 気圧の空気では 64 ナノメータ程度である）が浮上すきまに比べて無視できなくなった。

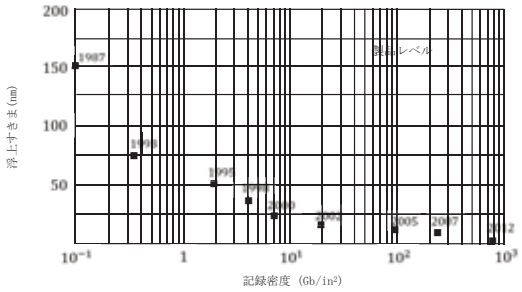


図 1：記録密度 vs. 浮上すきま

浮動ヘッドスライダ機構の場合、系の代表長と内部代表長はそれぞれ気体潤滑の浮上すきま h と気体分子の平均自由行程 λ である。この比 $Kn\ (= \lambda/h)$ はクヌッセン数と呼ばれ、気体の希薄度を表す。一般的に、気体の流れは Kn の値によって分類され、古典的な連続流は $Kn \to 0$

の場合に相当し、$Kn \ll 1$ の流れをスリップ流れ、そして $Kn \simeq 1$ の流れを遷移流れと呼ぶ。上述のボーイング 787 の例で言うと、$Kn \fallingdotseq 6$ で浮動ヘッドにおける流れは遷移流れに分類される。因みに、$Kn \gg 1$ の場合は、自由分子流と呼ばれている。Kn が任意の値をとる場合の気体の振舞を確率・統計的に取り扱うのが分子気体力学 [2] である（図 2 参照）。

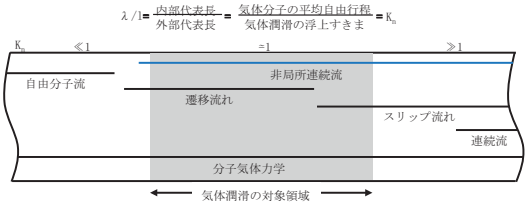


図 2：クヌッセン数 vs. 気体潤滑

本稿の 2 節では、磁気ディスク装置のヘッド・ディスク媒体インターフェースへの応用において発展してきた薄膜気体潤滑理論を境界面においてスリップ流れを導入することで導出された修正レイノルズ方程式 [3] と高次修正レイノルズ方程式 [4]、さらに分子気体力学に基づくボルツマン修正レイノルズ方程式 [5, 6] までを時系列にレビューし、一般化に向けた数理モデルの変遷をみる。

これまでのヘッド浮上解析は気体潤滑モデルだけを適用することで行われてきており、ほとんど浮上すきまのない領域においては新たなブレークスルーが必要であると思われる。3 節では、ボルツマン修正レイノルズ方程式に非局所流体力学 [7] を応用して遠距離分子間力と分子配向効果を考慮することで導出された固体近傍分子数個からなる超薄膜の流動を記述すべく粘性流体モデル [8] を連成することで成り立つと考えられる新しいヘッド・ディスク媒体インターフェースの数理モデルについて触れる。

2　薄膜気体潤滑の数理モデル

先ず気体潤滑の基本である連続流のレイノルズ方程式の導出から始める。次にレイノルズ方程式の速度境界条件として使われるノンスリップ流れの代わりに気体潤滑を考慮したスリップ流れの 1 次と 2 次近似を導入することで、修正レイノルズ方程式と高次修正レイノルズ方程式を導出する。そして、気体分子の挙動を確率・統計的に記述したボルツマン方程式に基づく一般化された気体潤滑方程式であるボルツマン修正レイノルズ方程式を導出する。本節の最後にこれら 4 つの気体潤滑モデルを比較する。

2.1　レイノルズ方程式

図 3 に示すように、通常の 3 次元直交座標系において xy 平面 ($z = 0$) に沿って配置されたディスク媒体面とそれにすきま分布 $z = h(x, y)$ で対向するヘッド浮上面を考える。ヘッドは

動作中にわずかに揺動するが、簡単のため定常状態であるとする。どちらの面も十分硬く表面応力や粘性力などによる変形は無視できるものとする。最小浮上すきまに対してヘッド浮上面の長さが十分大きい場合、レイノルズ数が小さい流れは局所的に平行平面間の流れと相似であると仮定することができ、速度の面内成分とすきま方向の導関数が支配的となる。これがいわゆるレイノルズの潤滑近似である。

この近似を正定数の粘性率 μ の粘性流体に関する運動方程式である圧縮性ナヴィエ・ストークス方程式に適用すると、定常な流れの速度に関する次の近似式が得られる。

$$\mu \frac{\partial^2 \boldsymbol{u}}{\partial z^2} = \nabla p \tag{2.1.1}$$

ここに、$\boldsymbol{u} = (u, v)$ は速度、圧力 p は x と y の関数である。

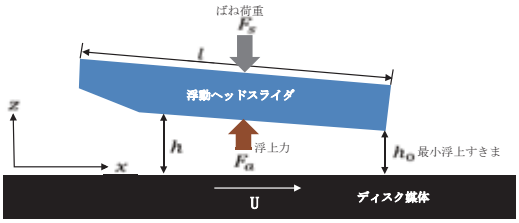


図 3：浮動ヘッドスライダ機構と座標系

本稿で取り扱うすべての潤滑モデルの導出において、一般性を失うことなく、ヘッド幅方向は無限とする。ディスク媒体面は x 方向に一定速度 U で動くとする。これらの条件のもと、速度 $\boldsymbol{u}$ は x 成分のみ、また圧力 p は x だけの関数となる。

流体と境界面での速度についてはノンスリップ流れの条件

$$u = U \quad \text{at} \quad z = 0, \qquad u = 0 \quad \text{at} \quad z = h \tag{2.1.2}$$

を適用し、式 (2.1.1) をすきま方向に積分すれば速度 u が得られる。

$$u(x, z) = -\frac{1}{2\mu}\frac{dp}{dx}(hz - z^2) + U\left(1 - \frac{z}{h}\right) \tag{2.1.3}$$

式 (2.1.3) から、潤滑流れは単純なポアズイユ流れとクエット流れの重ね合わせになっていることが分かる [9]。式 (2.1.3) を連続の式

$$\frac{d}{dx}\left(\rho \int_0^h u \, dz\right) = 0 \tag{2.1.4}$$

に代入して、ノンスリップ速度境界条件のもと、すきま方向に積分すれば定常状態の圧力 p に関する連続流のレイノルズ方程式が得られる。

$$\frac{d}{dx}\left(\rho h^3 \frac{dp}{dx}\right) = 6\mu U \frac{d}{dx}(\rho h) \tag{2.1.5}$$

先ず二つの軸受け面の温度は一定で等しく気体と軸受け面の温度差は非常に小さいとして潤滑領域内のどこでも等温であると仮定する。気体と軸受けが熱的平衡状態にあることから圧力と密度は比例関係にある。

$$p \propto \rho \tag{2.1.6}$$

式 (2.1.6) を式 (2.1.5) に代入すると、レイノルズ方程式は与えられた浮上すきま分布に対して圧力 p に関する非線形微分方程式となる。

$$\frac{d}{dx}\left(ph^3\frac{dp}{dx}\right) = 6\mu U\frac{d}{dx}(ph) \tag{2.1.7}$$

ヘッド浮上面周囲の圧力は xy 平面に投影された境界線に沿って雰囲気圧力 p_a に等しいので、圧力境界条件は次式で与えられる。

$$p_{\mathrm{bdry}} = p_a \tag{2.1.8}$$

従って、連続流のレイノルズ方程式は圧力 p に関する方程式 (2.1.7) と境界条件 (2.1.8) で与えられる。

次項以降の説明の便宜上、x 座標軸をヘッド浮上面の長さ l で、また圧力 p とすきま分布 h をそれぞれ雰囲気圧力 p_a と最小すきま h_0 で無次元化すると、これに対応するレイノルズ方程式と境界条件は次のように書ける。

$$\frac{d}{dX}\left[PH^3\frac{dP}{dX}\right] = \Lambda\frac{d}{dX}(PH) \tag{2.1.9}$$

$$P_{\mathrm{bdry}} = 1 \tag{2.1.10}$$

式 (2.1.9) の右辺の第 2 項にある無次元量 Λ $(= 6\mu Ul/p_a h_0^2)$ はベアリング数と呼ばれ、物理的にはディスク媒体面の走行速度 U によって生じるクエット流れ（せん断流れ）と圧力差によって生じるポアズイユ流れ（圧力流れ）の質量流量の比を表している[*1]。ベアリング数の作用については改めて 2.4 項で触れる。

2.2 修正レイノルズ方程式と高次修正レイノルズ方程式

1 節で述べた通り、薄膜気体潤滑の場合、分子平均自由行程が浮上すきまに比べて無視できず、ナヴィエ・ストークス方程式では現象を正しく記述できない状況があった。そこで Burgdorfer は、クヌッセン数 $Kn \ll 1$ の領域に限定しながらも、式 (2.2.1) と (2.2.2) で与えられる気体と軸受け面に生じるスリップ流れ [10] の 1 次近似を仮定することで連続流のレイノルズ方程式を拡張しモデルの精度を上げることに成功した [3]。

$$u = U + a\lambda\frac{\partial u}{\partial z} - \frac{(a\lambda)^2}{2}\frac{\partial^2 u}{\partial z^2} + \cdots \quad \text{at} \quad z = 0 \tag{2.2.1}$$

$$u = \quad - a\lambda\frac{\partial u}{\partial z} - \frac{(a\lambda)^2}{2}\frac{\partial^2 u}{\partial z^2} - \cdots \quad \text{at} \quad z = h \tag{2.2.2}$$

[*1] 気体潤滑レイノルズ方程式は厳密解があるバーガース方程式と同様な性質を示す。その意味でベアリング数は気体潤滑レイノルズ方程式の数学的解釈を与える上でも重要なパラメータである。

ここに、a は境界面の適応係数 α（2.3 項参照）の関数で $a = (2-\alpha)/\alpha$ で与えられる定数である。気体分子が境界面を離れていく時の形態には鏡面反射と拡散反射があるとされている。鏡面反射と拡散反射の線形内挿で表されたものがマクスウエル型境界条件と呼ばれる。α は境界面の適応係数と呼ばれるもので、鏡面反射と拡散反射はそれぞれ $\alpha = 0$ と $\alpha = 1$ に対応する。以降、簡単のため、$\alpha = 1$ とする。

2.1 項で示された連続流のレイノルズ方程式の導出と同じ要領で、ナヴィエ・ストークス方程式から導かれる運動方程式を式 (2.2.1) と (2.2.2) の 1 次近似を用いて解くと、速度 u は次式で与えられる。

$$u(x,z) = -\frac{1}{2\mu}\frac{dp}{dx}(\lambda h + hz - z^2) + U\left(1 - \frac{z+\lambda}{h+2\lambda}\right) \tag{2.2.3}$$

ここからは連続流のレイノルズ方程式と全く同じ手続きで、レイノルズ方程式の中の圧力流れによる質量流量を表す項に分子平均自由行程 λ の効果を含む新たな量が付加された無次元修正レイノルズ方程式が得られる。

$$\frac{d}{dX}\left[PH^3\left(1 + \frac{6Kn_0}{PH}\right)\frac{dP}{dX}\right] = \Lambda\frac{d}{dX}(PH) \tag{2.2.4}$$

ここに、Kn_0 $(= \lambda/h_0)$ は最小浮上すきま h_0 におけるクヌッセン数である。

修正レイノルズ方程式の予測精度が低下するような微小浮上すきまに対して、スリップ速度の 2 次項まで保持する潤滑モデルを提唱したのが Hsia で、これは高次修正レイノルズ方程式と呼ばれている [4]。高次修正レイノルズ方程式は分子平均自由行程 λ の 2 次の項が修正レイノルズ方程式に単純に付加された形となる。

$$\frac{d}{dX}\left[PH^3\left(1 + \frac{6Kn_0}{PH} + \frac{6Kn_0^2}{P^2H^2}\right)\frac{dP}{dX}\right] = \Lambda\frac{d}{dX}(PH) \tag{2.2.5}$$

2.3 ボルツマン修正レイノルズ方程式

この気体潤滑モデルが発表された 1987 年には磁気ディスク装置に搭載されている浮動ヘッドの最小浮上すきまは既に 150 ナノメータ前後であった（図 1 参照）。浮上すきまは記録の高密度化に伴いますます微小化する傾向にあり、クヌッセン数で言うと $Kn \simeq 1$ の領域に突入しつつあり、連続流の補正的なモデルである単純なスリップ流れよりさらに精度の良い結果が期待されるようになった。このような背景のなか、クヌッセン数が任意の値をとる場合の気体の振舞を取り扱う分子気体力学が着目された。以下、分子気体力学の基礎方程式であるボルツマン方程式に基づいて一般化された福井と金子の薄膜気体潤滑モデル [5, 6] についてレビューする。

分子気体力学の場合、気体の振舞を記述するには密度、流速、温度などの巨視的変数だけでは不十分であり、気体分子が種々な速度で走っていることを表現できる微視的取り扱いが本質的である。単一成分気体 2 体衝突モードと気体分子に外力が働いてない場合を仮定すると、それは位置 $\boldsymbol{x}$、時間 t、位置 $\boldsymbol{x}$ と時間 t における分子速度 $\boldsymbol{\xi}$ を独立変数とする分子速度の分布

関数 $f(\boldsymbol{x},\boldsymbol{\xi},t)$ である。$f(\boldsymbol{x},\boldsymbol{\xi},t)$ は位置 $\boldsymbol{x}$、分子速度 $\boldsymbol{\xi}$ における気体分子を見つける確率を表す。その変化を支配するのがボルツマン方程式である。

$$\frac{\partial f}{\partial t}+\boldsymbol{\xi}\cdot\nabla f=Q(f,f) \tag{2.3.1}$$

ここに、$Q(f,f)$ は速度分布関数 f に関する 2 次の積分作用素で、f の変化を引き起こす分子同士の衝突による得失を表している [2]。

この衝突項は取り扱いが難しい複雑な積分で表されており、この項は通常その本質を失うことなく簡略化された衝突モデルで置き換えられる [11]。これは 3 人の提唱者にちなんで BGK モデル方程式と呼ばれており、実際的な問題に最も良く使われているモデルである。

$$\frac{\partial f}{\partial t}+\boldsymbol{\xi}\cdot\nabla f=\nu(f_e-f) \tag{2.3.2}$$

ここに、ν は気体分子の平均衝突頻度、f_e は気体の定常かつ一様な状態（時間や位置に依存しない平衡状態）のボルツマン方程式の解である局所マクスウエル分布である。

$$f_e(\boldsymbol{\xi})=\frac{\rho}{(2\pi RT)^{3/2}}\exp\left\{-\frac{|\boldsymbol{\xi}\sim\boldsymbol{u}|^2}{2RT}\right\} \tag{2.3.3}$$

実際の浮動ヘッドスライダ機構では、流速が気体の分子速度に比べて十分小さく（マッハ数 $\ll 1$）かつ潤滑領域内の温度変化が十分小さい場合を仮定することができるため、気体分子の速度分布は流速が零である静止平衡分布 f_0 に近いと考えてよい。このことが BGK モデル方程式を静止平衡分布 f_0 まわりで線形化した方程式を薄膜気体潤滑の基礎式として用いる根拠となる。潤滑領域の流れを記述する線形 BGK モデル方程式の無次元表示は次式で与えられる。

$$\varepsilon\zeta_X\frac{\partial\phi}{\partial X}+\zeta_Z\frac{\partial\phi}{\partial Z}=\frac{1}{k_0}(-\phi+\omega+2\zeta_X V_X) \tag{2.3.4}$$

無次元化には、以下の無次元変数を用いた。

$$\begin{gathered}
X=\frac{x}{l},\quad Z=\frac{z}{h_0},\quad \varepsilon=\frac{h_0}{l}\\
\zeta_X=\frac{\xi_x}{\sqrt{2RT}},\quad \zeta_Z=\frac{\xi_z}{\sqrt{2RT}}\\
V_X=\frac{u}{\sqrt{2RT}}=\iiint_{-\infty}^{+\infty}(\zeta_X\phi E)d\boldsymbol{\zeta}\\
\phi=ff_e^{-1}\big|_{u=0}-1\\
\omega=\frac{\rho}{\rho_0}-1=\iiint_{-\infty}^{+\infty}(\phi E)d\boldsymbol{\zeta}
\end{gathered} \tag{2.3.5}$$

ここで、X, Z は無次元座標、ζ_X, ζ_Z は無次元分子速度、V_X は無次元流速、h_0 は最小浮上すきまである。下付き添え字 0 の付いた量は静止平衡状態のものである。ϕ は速度分布関数 f の静

止平衡状態の速度分布関数 f_0 からのずれを f_0 で無次元化したものである。ω は密度 ρ の静止平衡状態の密度 ρ_0 からのずれを ρ_0 で無次元化したものである。E と k_0 は次式で与えられる。

$$E = \pi^{-3/2}\exp(-\boldsymbol{\zeta}^2) \tag{2.3.6}$$

$$k_0 = \frac{\sqrt{\pi}}{2}\left(\frac{\lambda}{h_0}\right) = \frac{\sqrt{\pi}}{2}Kn_0 \tag{2.3.7}$$

基礎式 (2.3.4) の境界条件は次式で与えられる。

$$\phi = \sigma_{W0} + 2\zeta_X V_{W0} \quad \text{at} \quad Z = 0,\ \zeta_Z > 0 \tag{2.3.8}$$

$$\phi = \sigma_{WH} \quad \text{at} \quad Z = H,\ \zeta_Z < 0 \tag{2.3.9}$$

ここに、σ_{W0} と σ_{WH} はそれぞれディスク媒体面とヘッド浮上面での無次元等価密度、V_{W0} は前者の無次元速度 $(= U/\sqrt{2RT})$ である。

次に、基礎式 (2.3.4) の解として次の相似解を考える。

$$\phi = \left(\frac{X}{\varepsilon}\right)\phi_0(\boldsymbol{\zeta}^2) + \zeta_X\phi_1(Z, \zeta_Z, \boldsymbol{\zeta}^2) \tag{2.3.10}$$

式 (2.3.10) を式 (2.3.4) に代入し、その結果を X と ζ_X について整理すると ϕ_0 と ϕ_1 に関する以下の 2 式を得る。

$$\phi_0 = \beta \tag{2.3.11}$$

$$\zeta_Z\frac{\partial\phi_1}{\partial Z} = \frac{1}{k_0}(-\phi_1 + 2V_X) - \beta \tag{2.3.12}$$

ここに、β は無次元圧力勾配 $(= \varepsilon\, dP/dX)$ である。

ここでも、2.1 項および 2.2 項との整合性を考慮して、気体分子が両方の軸受け面で拡散反射する場合を考える。この場合、基礎式 (2.3.12) の境界条件は次式で与えられる。

$$\phi_1 = 2V_{W0} \quad \text{at} \quad Z = 0,\ \zeta_Z > 0 \tag{2.3.13}$$

$$\phi_1 = 0 \quad \text{at} \quad Z = H,\ \zeta_Z < 0 \tag{2.3.14}$$

式 (2.3.12) を境界条件 (2.3.13) と (2.3.14) のもとで ϕ_1 について解くと、未決定の流速 V_X を含む ϕ_1 の解析的表現を得る。

$$\begin{aligned}\phi_1 = {} & 2V_{W0}\exp\left(-\frac{Z}{k_0\zeta_Z}\right) \\ & + \frac{1}{\zeta_Z}\exp\left(-\frac{Z}{k_0\zeta_Z}\right)\int_0^Z\left(\frac{2V_X(Z')}{k_0} - \beta\right)\exp\left(\frac{Z'}{k_0\zeta_Z}\right)dZ' \quad \text{for} \quad \zeta_Z > 0\end{aligned} \tag{2.3.15}$$

$$\phi_1 = \frac{1}{\zeta_Z}\exp\left(-\frac{Z}{k_0\zeta_Z}\right)\int_H^Z\left(\frac{2V_X(Z')}{k_0} - \beta\right)\exp\left(\frac{Z'}{k_0\zeta_Z}\right)dZ' \quad \text{for} \quad \zeta_Z < 0 \tag{2.3.16}$$

ϕ_1 を式 $(2.3.5)_3$ に代入すれば、V_X に関する積分方程式が得られる。

$$V_X(Z) = \frac{1}{\sqrt{\pi}}\left\{V_{W0}T_0\left(\frac{Z}{k_0}\right) + \frac{1}{k_0}\int_0^H T_{-1}\left(\frac{|Z - Z'|}{k_0}\right)\left[V_X(Z') - \frac{k_0\beta}{2}\right]dZ'\right\} \tag{2.3.17}$$

ここに、$T_n(x)$ は Abramowitz 関数 [12] と呼ばれる無限積分である。

$$T_n(x) = \int_0^\infty t^n \exp\left(-t^2 - \frac{x}{t}\right) dt \tag{2.3.18}$$

ここで、福井と金子は V_X を次のような線形和として表した。

$$V_X(Z) = \frac{k_0\beta}{2}(1-\psi_p) + V_{W0}\psi_c \tag{2.3.19}$$

式 (2.3.19) を式 (2.3.17) に代入し、その結果を圧力勾配に依存する量 $k_0\beta/2$ とディスク媒体面速度 U 毎に整理すると、ψ_p と ψ_c は次の積分方程式の解として求まる。

$$\psi_p(Z) = 1 + \frac{1}{\sqrt{\pi}\,k_0}\int_0^H T_{-1}\left(\frac{|Z-Z'|}{k_0}\right)\psi_p(Z')\,dZ' \tag{2.3.20}$$

$$\psi_c(Z) = \frac{1}{\sqrt{\pi}}\left[T_0\left(\frac{Z}{k_0}\right) + \frac{1}{k_0}\int_0^H T_{-1}\left(\frac{|Z-Z'|}{k_0}\right)\psi_c(Z')\,dZ'\right] \tag{2.3.21}$$

式 (2.3.20) と (2.3.21) で与えられる ψ_p と ψ_c が式 (2.3.19) の右辺の第 1 項と第 2 項を通してそれぞれ圧力流れとせん断流れの流速プロファイル与えることは当時既に知られていた [13, 14]。福井と金子はそれに着目し V_X を巧みに式 (2.3.19) の形で表した。即ち、これまでの古典的な潤滑モデルと同様、V_X は圧力流れとせん断流れの流速プロファイルの和として表されることを示したのである。

$$V_X = V_{Xp} + V_{Xc} \tag{2.3.22}$$

ここに、

$$V_{Xp} = \frac{k_0\beta}{2}(1-\psi_p) \tag{2.3.23}$$

$$V_{Xc} = V_{W0}\psi_c \tag{2.3.24}$$

これは任意のクヌッセン数に対しても潤滑流れは単純な圧力流れとせん断流れの重ね合わせになっていることを意味する。従って、全質量流量 q も圧力流れとせん断流れの質量流量 q_p と q_c の和として表される。

$$q = q_p + q_c \tag{2.3.25}$$

せん断流れの流速プロファイルが対称であることを考えると、その質量流量 q_c がクヌッセン数に依存せず連続流の場合と同様 $\rho Uh/2$ になることは明らかである。このことから潤滑領域の全質量流量のクヌッセン数に依存する部分は圧力流れのみに起因していることが分かる。従って、最終的に得られる方程式は古典的な潤滑方程式と同じ形で表され、圧力流れの質量流量のみを新たに求めればよいことになる。

ここで、圧力流れの質量流量 q_p を次のように無次元化し、圧力流れの質量流量係数 Q_p を定義する。

$$Q_p(D) = -\frac{q_p}{h^2\left(\frac{dp}{dx}\right)/\sqrt{2RT}} \tag{2.3.26}$$

ここに、D は逆クヌッセン数と呼ばれ、次のように定義されている。

$$D = \frac{\sqrt{\pi}}{2Kn} \tag{2.3.27}$$

したがって、$Q_p(D)$ を連続流の場合の圧力流れの質量流量 $Q_{\mathrm{con}}(D)$ で正規化すると、ボルツマン修正レイノルズ方程式の無次元表示は次のように表すことができる。

$$\frac{d}{dX}\left[PH^3\left(\frac{Q_p(D)}{Q_{\mathrm{con}}(D)}\right)\frac{dP}{dX}\right] = \Lambda\frac{d}{dX}(PH) \tag{2.3.28}$$

連続流、スリップ 1 次近似、2 次近似の場合の $Q_p(D)$ はそれぞれ $D/6$、$D/6(1+3\sqrt{\pi}/D)$、$D/6(1+3\sqrt{\pi}/D+3\pi/2D^2)$ である。このように、薄膜気体潤滑モデルの一般化は圧力流れの質量流量の一般化であることが分かる。

圧力流れの質量流量 Q_p は積分方程式 (2.3.20) を ψ_p について数値的に解き、その結果を式 (2.3.23) に代入し、それをさらに質量流量の定義に基づきすきま方向に数値積分することで求めることができる。公表されている質量流量のデータベース [15] を使用すれば、従来の気体潤滑モデルの数値シミュレーションプログラムからの改造は比較的容易である。また、文献 [15] には任意の逆クヌッセン数での質量流量はデータベースに適切な内挿方法等を使うことで高速に計算できることも示されている。

2.4 薄膜気体潤滑モデルの比較

2.1〜2.3 項でレビューした 4 つの薄膜気体潤滑モデルの違いは圧力流れの質量流量係数に集約される。圧力流れの質量流量係数と逆クヌッセン数との関係を各モデルについて計算することでその特性を比較することができる。図 4 から、1 次スリップ近似は質量流量を過少に評価するが、2 次スリップ近似の方は逆に過大評価していることがわかる。また、$Kn \ll 1$ の領域では、ボルツマン修正レイノルズ方程式に基づく厳密な漸近解が示されている。

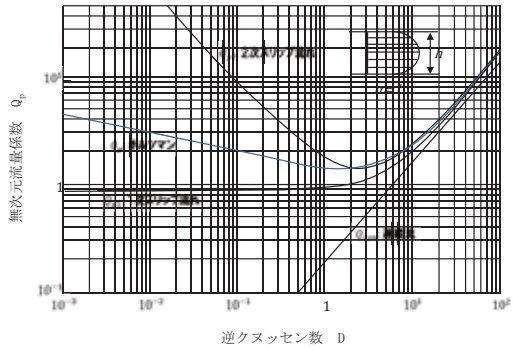


図 4：圧力流れの流量係数 $Q_p(D)$（出典：[5]）

2.1 項で述べたように、ベアリング数 Λ はせん断流れと圧力流れの質量流量の比を表している。仮に Λ が大きくなると、せん断流れが支配的になりクヌッセン数の影響が減少する。そのため、系のベアリング数の大きさによっては、本来クヌッセン数に依存する気体潤滑モデル間の予測精度の差はそれほどつかなくなってしまう。図 5 は浮動ヘッドの設計に重要な負荷容量 W とベアリング数の関係を調べた結果である。これから分かるように、系の代表的逆クヌッセン数 D_0 を固定した状態で Λ が増加すると、どのモデルの W も一定値に漸近し、それぞれの差異は減少する。しかし、圧力流れが支配的となるような実験条件下において、ボルツマン修正レイノルズ方程式の計算結果は実測値に良く合致することが示されており、本モデルの有効性が確認されている [16]。

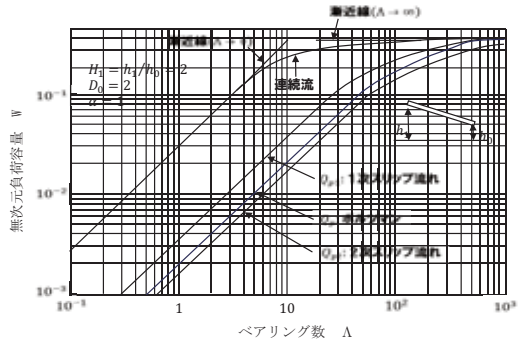


図 5：ベアリング数 Λ と負荷容量 W の関係（出典：[5]）

3 新しいヘッド・ディスク媒体インターフェースについて

浮上すきまが数ナノメータの領域に突入しディスクの表面粗さや液体潤滑膜の影響が顕在化するなか、これまでの薄膜気体潤滑モデルだけでは限界があるのは明らかである。図 6 に示すように、記録密度 $10\,\mathrm{Tb/in^2}$ の実現[*2]に向けて、ヘッドの記録再生部のみが潤滑膜を滑走する一方で、その滑走状態を安定に維持できるよう他の部分を気体潤滑させるアプローチが提案されている [17]。記録密度 $10\,\mathrm{Tb/in^2}$ を実現するためにはヘッドの記録再生部とディスク媒体間の絶対的距離は 2〜3 ナノメータ程度だろうと言われており [1]、もはや気体潤滑流れのみではなく[*3]、相対運動する二つの軸受面間を満たす液体潤滑膜の流動とそのヘッドへの影響を含めた問題に帰着すると思われる。この領域では系の代表長 l と内部代表長 λ の比は $\lambda/l \simeq 1$ で、遠方にある部分要素の相対運動がその他のすべての部分要素に影響を与える遠距離作用とそれらの空間分布が物体の応答に本質的に効いてくるため、従来の連続体力学では扱えず、ス

[*2] 現状の市販ドライブで $750\,\mathrm{Gb/in^2}$、実験室レベルでは既に $1.2\mathrm{Tb/in^2}$ が実現されている。

[*3] このモデル、ディスク媒体表面に最接近するヘッドの記録再生部が液体潤滑膜を滑走しているので、浮上すきまとは言わず記録再生部とディスク媒体間のスペーシングを磁気すきまと呼ぶ。

ケール効果を取り込める力学理論の知見が必要となる。非局所連続体力学 [18] はそのような力学理論として構築されたものである[*4]。

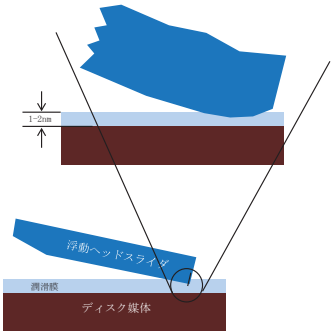


図 6：液体と気体の混合潤滑モデルのイメージ（出典：[17]）

筆者等は非局所連続体力学に基づいて液体粒子の遠距離作用と境界近傍での配向効果を考慮して粘性流体潤滑モデルを導出し、薄膜液体の微視的挙動を記述することに成功した [8]。非局所潤滑方程式の詳細は紙面の都合により参考文献 [8] に譲り、ここでは記録密度 10 $\mathrm{Tb/in^2}$ の実現に向けて提案された上述の浮動ヘッドスライダ機構 [17] の数理モデルとして、以下に提案する気体潤滑と液体潤滑の混合モデルをもって本稿の纏めとする。非局所潤滑方程式により厚さ数ナノメータの液体膜を挟んだ記録再生部とディスク媒体面の間に働く力を正確に予測することができるので、その力をボルツマン修正レイノルズ方程式に反映させることで数ナノメータの磁気すきまを安定に維持しながら滑走するヘッド・ディスク媒体インターフェースを実現することが可能であると考えている。

参考文献

[1] Liu, B. et al., Air-bearing design towards highly stable head-disk interface at ultra-low flying height, IEEE Transactions on Magnetics, Vol. 43, No. 2, pp. 715–720, 2007

[2] Cercignani, C., Rarefied Gas Dynamics – From Basic Concepts to Actual Calculations, Cambridge University Press, 2000

[3] Burgdorfer, A., The influence of the molecular mean free path on the performance of hydrodynamic gas lubricated bearings, Transactions of ASME Journal of Basic Engineering, Vol. 81, pp. 94–100, 1959

[4] Hsia, Y. H. and Domoto, G. A., An experimental investigation of molecular rarefaction effects in gas lubricated bearings at ultra-low clearances, Transactions of ASME Journal of Lubrication Technology, Vol. 105, pp. 120–130, 1983

[*4] 気体潤滑で中心的な役割を担ったボルツマン方程式は時空間において非局所性を有する例として良く知られている [19]。

[5] Fukui, S. and Kaneko, R., Analysis of ultra-thin gas film lubrication based on linearized Boltzmann equation: first report – derivation of a generalized lubrication equation including thermal creep flow, Transactions of ASME Journal of Tribology, Vol. 110, pp. 253–262, 1988
[6] Fukui, S. and Kaneko, R., Molecular gas film lubrication (MGL), Handbook of Micro/Nanotribology, ed. Bushan, B., CRC Press, pp. 559–604, 1995
[7] Eringen, A. C., On nonlocal fluid mechanics, International Journal of Engineering Science, Vol. 10, No. 6, pp. 561–575, 1972
[8] Eringen, A. C. and Okada, K., A lubrication theory for fluids with microstructures, International Journal of Engineering Science, Vol. 33, No. 15, pp. 2297–2308, 1995
[9] 木谷、流体機械に伴う流れ、流体力学ハンドブック、第 22 章、丸善、1987
[10] Schaaf, S. A. and Sherman, F. S., Skin friction in slip flow, Journal of Aeronautical Sciences, Vol. 21, No. 2, pp. 85–90, 1953
[11] Bhatnagar, P. L., Gross, E. P. and Krook, M., A model for collision processes in gases, I, Physical Review, Vol. 94, pp. 511–525, 1954
[12] Abramowitz, M. and Stegan, I. A., Handbook of Mathematical Functions, Dover, 1968
[13] Cercignani, C. and Daneri, A., Flow of a rarefied gas between two parallel plates, Journal of Applied Physics, Vol. 34, No. 12, pp. 3509–3513, 1963
[14] Willis, D. R., Comparison of kinetic theory analyses of linearized Couette flow, Physics of Fluids, Vol. 5, No. 2, pp. 127–135, 1962
[15] Fukui, S. and Kaneko, R., A database for interpolation of Poiseuille flow rates for high Knudsen number lubrication problem, Transactions of ASME Journal of Tribology, Vol. 112, pp. 78–83, 1990
[16] Fukui, S. and Kaneko, R., Experimental investigation of externally pressurized bearings under high Knudsen number conditions, Transactions of ASME Journal of Tribology, Vol. 110, pp. 144–147, 1988
[17] Liu, B. et al., Lube-surfing recording and its feasibility exploration, IEEE Transactions on Magnetics, Vol. 45, No. 2, pp. 899–904, 2009
[18] Eringen, A. C., Nonlocal Continuum Field Theories, Springer-Verlag, New York, 2002
[19] Eringen, A. C., Continuum Physics Volume IV – Polar and Nonlocal Field Theories, Academic Press, New York, 1976

鉄鋼業における数学の活用

中川　淳一
新日鐵住金株式会社

1　はじめに

実世界で頻繁に問題となるのは、高炉プロセスの炉況不調や連続鋳造プロセスの品質欠陥等にみられるような定常状態から大きく乖離したときに発生すると考えられる異常状態である。これらプロセスの操業は、通常、このような異常状態を可能なかぎり回避するように管理されるので、異常状態が定常的に継続するようなことは稀で、我々が、異常状態の解析を行う際に眼にするのは、殆どのケースで、過渡的な遷移過程にあるデータである。

一方、プロセス内の現象を解析するために、熱収支、物質収支または運動量収支等に基づく偏微分方程式で現象を記述し、差分法や有限要素法等の数値解析手法を使って、コンピュータ上に現象を再現する、所謂数値シミュレーション解析がよく行われている。しかし、異常状態を引き起こす原因となる境界条件が、大抵の場合、不明であるため、既存の数値シミュレーションによって異常状態をコンピュータ上に再現することは、困難を極めているのが現状の実態である。

従って、このような問題に対処するには、①過渡的な遷移過程にある状態の普遍的な性質を見出し定量化する必要がある。すなわち、過渡的な遷移過程にあるデータから、異常状態を引き起こす際の法則性を見出す必要がある。これは、非定常状態の同定問題であり、自由度が大きく、かつ、瞬時の状態が問題となるような力学系に対し、システム固有の非線形法則性を見出すことである。これは、鉄鋼業だけでなく、他の材料、化学反応、生物反応等を扱う分野でも高い必要性を有していると考えられる。

また、解析対象となる現象が、溶鉄の熱流動状態の変化に関係している場合は、広範囲の3次元空間内の現象を扱う必要があるが、溶鉄が1500 °C以上の高温状態にあり、また、装置が巨大であるため、流束の直接計測が極めて困難である。従って、装置壁に埋設された熱電対による温度計測値のような限定された間接情報からの推定を余儀なくされている。従って、②熱電対による温度計測の時系列データに埋め込まれた系内の現象に関する情報を抽出する必要がある。これは、特定の数学条件を満たすような変換を施すことで、熱電対温度の時系列データのみから、もとの力学系（すなわち、解析対象の熱流動現象）と1対1に対応するような関数を再構成する問題である。また、一般的に、熱電対埋設位置と解析対象面が離れた位置にあるため、解析対象面の時間変化に対し、熱電対の計測信号は、装置壁材料の伝熱抵抗のため、時間的に減衰するという深刻な問題も有している。さらに、実世界のデータを扱う際に、ノイズ（システムノイズ＋観測ノイズ）の混入は不可避であり、実データの解析の際には、③ノイズに対する高い耐用性が、常に、求められている。

実世界で問題となる上述の課題解決のために、数学を活用し、現象のモデリング、所謂、数学モデルの作成を行う。一般的に、数学モデルとは、現象の本質を抽出し、数量化する作業の成果物であるが、そのプロセスには、2つの重要な工程を含んでいると考えている。ひとつは、解析対象となる現象から本質となる要素を抽出し、方程式等の形式で現象を記述する物理モデリングの工程であり、もうひとつは、物理モデルの解の特性を調べ、現実現象との対応関係を、或る論理構造 (Logical-Path) として記述する工程である。

物理モデリングの工程には、実現象の観察に基づく洞察力を発動し、解析対象となる事象と関係のない枝葉の部分を、時には経験をもとにした大胆な仮定をおいて、刈りとり、いかに現象を単純化して記述できるかが、重要なポイントになる。特に、企業の製造現場への数学モデルの適用を考える場合は、常に、精度の追求と開発工期という2つの相反する観点からの検討が求められ、微視的な精度を追求するあまり、必要以上に問題を複雑にして扱うことが、その後の工程（実現現象とモデル間の論理構造の記述）を含め完成した数学モデルの精度向上を、必ずしも約束するものではない。その意味で、物理モデリングの工程には、工学者や企業に所属する技術者・研究者の洞察力に負う所が多くあると考える。

次の論理構造 (Logical-Path) 導出の工程においては、物理モデルの解と現実の現象との対応関係を分析することになるが、解析対象とする現象が複雑になるにつれ、単に、偏微分方程式の解を求めるだけ、あるいは、物理モデルによる計算結果と実データとの相関を統計的手法で単純に分析するだけでは、対応できなくなるケースが少なくない。物理モデル自体が、現実現象にいくつかの仮定をおいて導出したものであり、物理モデルによる計算結果を、現実現象と完全に一致させる必要はない。むしろ、物理モデルは現実現象の仮想空間へのひとつの写像であると考え、物理モデルと現実現象との1対1の対応関係を、論理構造 (Logical-Path) として、記述することを指向すべきであると考える。ここに、現実現象の解析における数学活用の醍醐味があると思う。

以下に、鉄鋼業の代表的な設備である高炉を題材にして、数学活用の具体的な方法論を示す簡単な事例のひとつを紹介したい。

2　高炉の概要と操業異常

鉄鋼業の製鉄所のように巨大な設備で高温物質を扱う産業では、現場・現物という視点が重要である。例えば、製鉄所の高炉のなかで起きている現象は、非定常で非線形であり、また、多変量の操作因子を扱うため、ほとんどの場合で複雑である。しかし、1500 °C 以上の溶鉄を扱い、また、装置が巨大なために観測できる情報は極めて限定されている。例えば、高炉の場合、溶鉄の熱流動状態が、操業および品質に大きな影響を及ぼすと予想されているが、溶鉄の流速の直接計測が極めて困難であるため、煉瓦に埋設された熱電対の温度計測値のような間接情報からの推定を余儀なくされている。

そのため、我々は、一部の計測データのなかから、現象を支配する法則をいかに見出すかに重点をおき、計測データのなかに隠された現象の本質を解明する努力を日々行っている。

図1に、高炉内部断面の概念図を示す。高炉は、鉄鋼業のシンボル的な存在であり、高さが約 35 m、内径が約 15 m の巨大な反応容器である。高炉は、焼結鉱とコークスを化学反応させ

て、溶銑と呼ばれている銑鉄をとりだす工程である。ここで、焼結鉱とは、粉状の鉄鉱石と石灰石を約 1300 °C の高温で事前に焼き固めて、5 mm～25 mm 程度の均一の塊にしたものである。一方、コークスとは、石炭を蒸し焼きしてできる、高純度の炭素の塊で、焼結鉱から鉄を取り出すための還元剤および熱源として使用する。高炉の上部から焼結鉱とコークスを交互に装入し、下部から約 1200 °C の高温空気を吹き込むと、炉内温度は 2000 °C 以上の高温状態になり、化学反応が促進され焼結鉱から鉄が還元・分離され、銑鉄はトピードカーと呼ばれる運搬容器に入れて、次の工程である製鋼工場に輸送される。また、焼結鉱に含まれるさまざまな不純物は、スラグとして取り出される。

図 1 に、高炉炉底の煉瓦に埋設された熱電対による温度計測データを示す。図 1 のグラフの中で、1 点鎖線で囲った時間帯が異常状態を示し、正常時の温度に対し、1.7 倍程度の高い温度値を示しており、この異常状態が 2 ヶ月以上継続している。図 1 の矢印で示したタイミングで休風を実施している。ここで、休風とは、高炉に高温空気を吹き込むことを止め、銑鉄の製造を 1 日程度休止する操作である。休風の本来の目的は、定期的な設備の保守・点検であるが、図 1 では、炉の温度を下げるため、非定期な休風を 5 回も実施している。大型の高炉では、一日に約 10000 トンの銑鉄を製造しており、休風の間は、銑鉄の製造が出来ないため、これらの非定期的な休風は大きなコスト損失になる。「何故、このような異常状態が突然発生するのか？ 正常状態から異常状態に移行する際の現象に内在する論理構造を、数学的に明らかにする。」ことが重要であり、以下に、その解析の一例を示す。

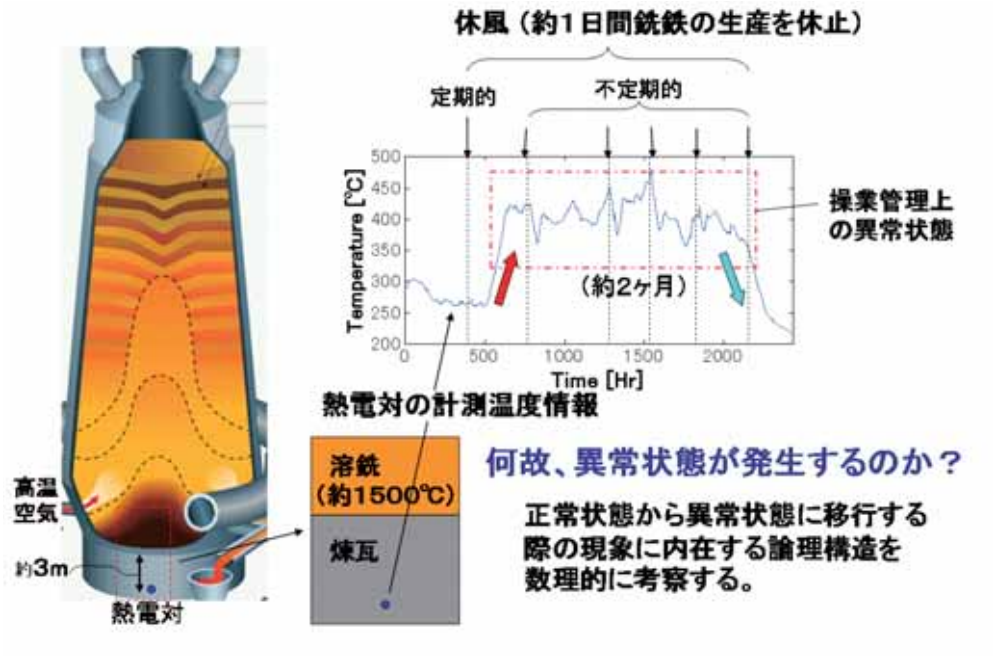


図 1：高炉における数学の課題設定

3　高炉煉瓦内部の伝熱現象の物理モデリング

図 2 は、図 1 の煉瓦断面図を拡大したものである。高炉は、炉底と呼ばれる約 15 m の内径の溶銑浴を囲むように 2 m〜3 m の大きさの煉瓦が積まれており、本来は 3 次元形状の解析対象物である。しかし、溶銑との接触面から煉瓦内部を熱伝導で移動する熱量は、溶銑との接触面に対し鉛直軸方向の熱伝導が、放射軸方向（水平方向）に対し圧倒的に大きいため、鉛直軸方向の 1 次元非定常熱伝導問題として、物理モデリングを行うことで、(1) 式に示すような簡単な偏微分方程式で、現象を記述できる。

$$\frac{\partial T}{\partial t} = \lambda \frac{\partial^2 T}{\partial x^2} \tag{1}$$

ここで、T は煉瓦の温度、t は時間、λ は煉瓦の熱伝導率、x は溶銑との接触面から鉛直軸方向の距離を表す。

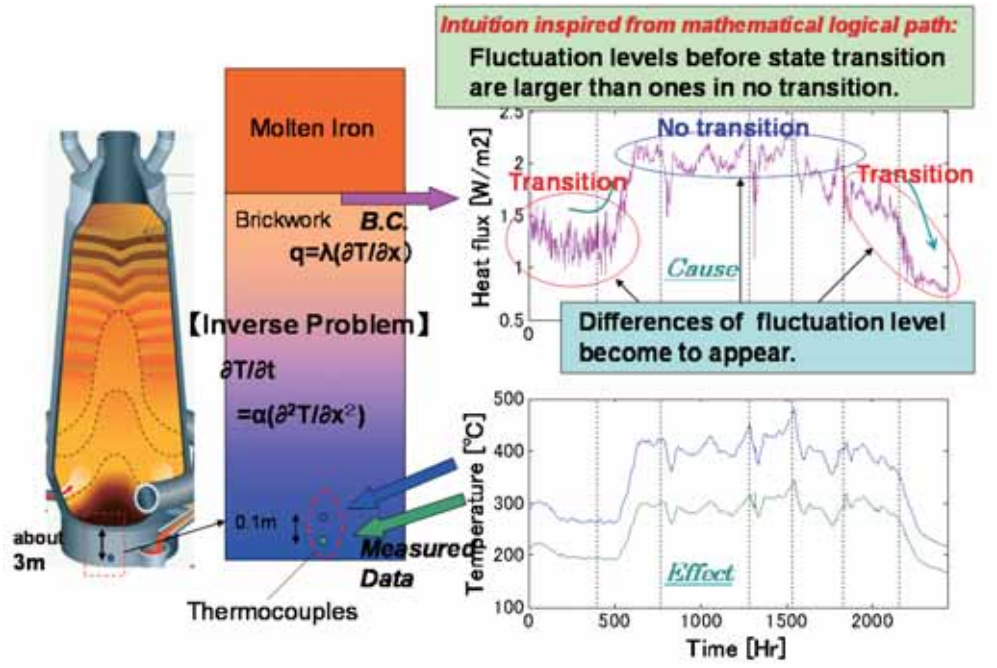


図 2：論理構造 1：原因系の物理量の再構成

4　論理構造の導出 1「原因系の物理量の再構成」

上述の式 (1) は、適切な初期条件と境界条件を設定すれば、簡単に解くことができる。しかし、高炉は、一旦稼動すると、12 年から 15 年の期間、昼夜に亘り連続して運転される。従っ

て、煉瓦も 12 年から 15 年間の長期間に亘り、交換せず連続して使用する必要があり、その間に、煉瓦の溶損が進行するので、炉内監視用として煉瓦に埋設される熱電対の位置は、溶銑との接触面に対し、2〜3 m程度、離れた位置に設置せざるを得ない。

これは、異常状態が発生したときに煉瓦内部の伝熱現象を解析する際に、式 (1) を得るために必要な初期条件、すなわち、煉瓦内部の初期温度分布の情報が得られないことを意味する。

その代替手段として、溶銑との接触面から 2 m 以上、離れた位置に設置された複数の熱電対温度の時間挙動から炉内状況を予測することが行われているが、溶銑との接触面と熱電対位置の間には、大きな伝熱抵抗が存在するため、熱電対による温度計測値には、炉内の動的な熱変化に対し、大きな熱伝導遅れが生じる。

従って、炉内の動的な挙動を熱電対で監視するためには、炉内の動的変化の結果である熱電対温度計測値から、その原因系を代表する物理量を推定する必要がある。これが、「原因系の物理量の再構成」という、ひとつの論理構造 (Logical-Path) であり、ここに、「逆問題」[1] という数学を適用する。具体的には、煉瓦の温度が、式 (1) の非定常熱伝導方程式で記述できると仮定し、煉瓦内部の複数の温度計測値が、式 (1) を満足するように、その境界条件である熱流束と初期温度分布を同時に決定する。ここでは、温度計測値が「結果」であり、熱流束推定値が「原因」となっており、逆問題という数学の適用により、因果関係を逆に遡ることが可能になる。

図 2 に、逆問題で推定した熱流束値を示す。ここで、注目したいのは、正常状態から異常状態、および、異常状態から正常状態に遷移する前および遷移中の熱流束値の変動が、状態遷移のない場合と比較して、大きくなっていることである。これは、もとの温度計測値の挙動を眺めているだけでは、気づくのは極めて困難であり、数学の適用により触発され、技術者の現象を診る眼が格段に向上することを示す格好の事例である。

5　論理構造の導出「時系列データに内在する法則性の導出」

次に、上記の熱流束変動の大きさの差異が、どのような法則にもとづいて起きているのかを考察する。これが、「時系列データに内在する法則性の導出」という、もうひとつの論理構造 (Logical-Path) である。

そのために使用するのが、時系列データからのアトラクタの再構成に関する数学理論であり、その手法の概要を図 3 に示す。これは、我々が実際に観測できる時系列データは限られているが、たった 1 変数の時系列データのみから、直接知ることのできない非線形力学系のアトラクタの軌道を、再び構成する手法である。具体的なアトラクタの再構成手法は、時間遅れ座標系への変換であり、1 変数の観測値 $x(t)$ を用いて、時間遅れの大きさを D とする n 次元の再構成状態空間における n 次元ベクトルを作成すると、次元数 n を適切に選択することにより、再構成されたアトラクタは、もとの力学系との 1 対 1 対の対応が可能になる。理論の詳細は、合原一幸著の「カオス学入門」(放送大学教育振興会) [2] を参照されたい。

図 4-1 に示す熱流束の時系列データから、再構成した n 次元アトラクタを、図 4-2 に示す。次元数 n は、相関次元解析 [2] により算出した相関次元値をもとに、埋め込み定理 [4] を考慮し

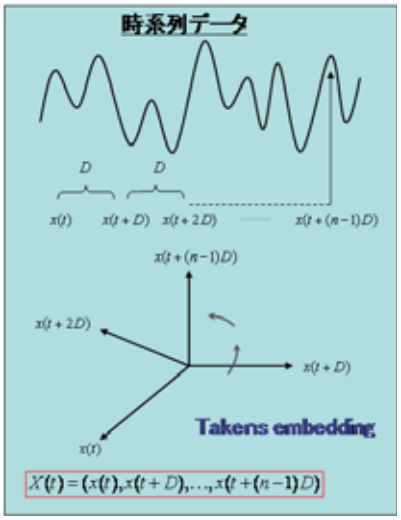


図 3：時系列データからの非線形力学系の再構成
（東京大学生産技術研究所　合原一幸教授からの提供）

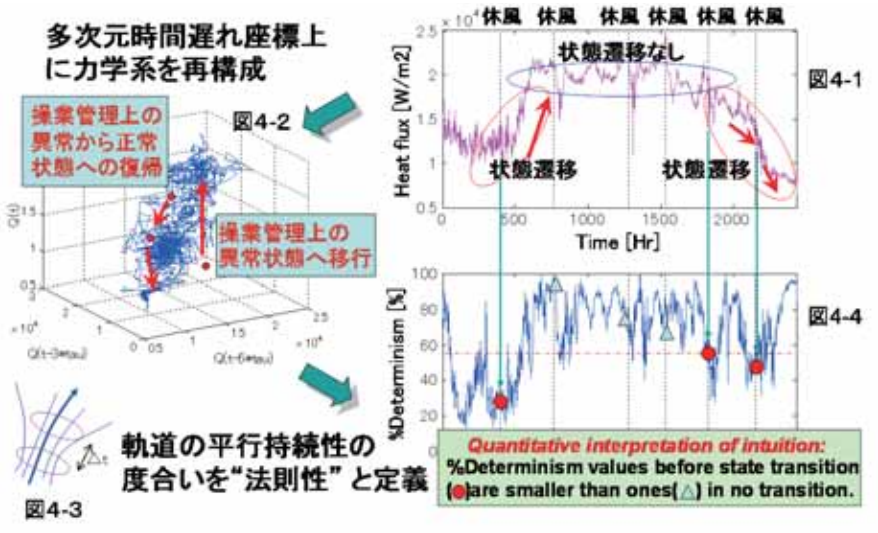


図 4：論理構造 2：時系列データに内在する法則性の導出

て 7 と決定した [5]。尚、図 4-2 では、表記の便宜上、第 1 次元、第 4 次元および第 7 次元成分のみからなる 3 次元図としてアトラクタの挙動を表示している。

状態の挙動を Δt の時間スケールで観測したときに、時間発展の様子が決定論的、すなわち

或る法則性に支配されて推移するように見えるということは、図 4-3 に示すように再構成された軌道群の近接した部分が Δt 後に近接した部分に移されることを意味する。これは、アトラクタ軌道が周囲の近傍点の軌道に対し、平行に走ることを意味しており、図 4-3 の n 次元再構成アトラクタの軌道の平行線の持続性を、ある時刻 t における再構成アトラクタ上の点の周囲にある近傍点の集合が、$t + \Delta t$ において近傍点として存在する割合を%Determinism と定義し([5])、計算した結果を図 4-4 に示す。

図 4-4 では、状態遷移の前および状態遷移中の%Determinism 値が、状態遷移のない場合と比較して、小さくなっていることである。これは、図 2 に前述した「正常状態から異常状態、および、異常状態から正常状態に遷移する前および遷移中の熱流束値の変動が、状態遷移のない場合と比較して、大きくなっている。」という観察結果を定量化したものであり、「観察結果を代表物理量として定量化する」という数学の重要な活用事例を示していると考える。これは、一見するとホワイトノイズとして処理されてしまうような図 4-1 の熱流束の変動の意味を数学的に解釈することによって得られる新しい知見である。

ノイズの物理的意味を数学的に解釈することにより、ノイズのなかから種々の情報を引き出す可能性を有しているという点からも、数学活用の意義は大きいと思う。

6　複数の論理構造の組み合わせによる工学原理の導出

図 5 に、解析結果の総括を示す。前述したように、今回の事例では、数学により導出した 2 つの論理構造 (Logical-Path) を使って、正常状態から異常状態、異常状態から正常状態へ遷移する際に、熱電対による煉瓦内部の温度計測データ（図 5-1）に内在する法則性の分析を行った。その結果を図 5-4 に示す。図 5-4 は、休風直前の%Determinism 値（図 5-3 参照）と休風による熱流束変化量（図 5-2 参照）の関係を示す。休風直前の%Determinism 値が低下するにつれ、休風による熱流束変化量が増加するという相関関係が見出せる。この結果から、「%Determinism 値が低下しているときに、休風のような激しいアクションを行うと、大きな状態遷移を引き起こし易くなる」という、ひとつの製造原理を導出できた。

もし、論理構造-1「原因系の物理量の再構成」を経ずに、図 5-1 の熱電対温度データのみから、直接、論理構造-2「時系列データに内在する法則性の導出」を行った場合の結果を、図 6 に示す。図 6 では、休風直前の%Determinism 値と休風による熱流束変化量の間に、図 5-4 のような相関関係を見出すことは出来ない。複数の論理構造 (Logical-Path) を組み合わせることにより、製造現場の計測データから、これまで見えなかった法則性を見出すことが可能になることが判る。

7　数学研究への期待

図 7 は、現実世界の現象を、定常、非定常、線形および非線形という 4 つのカテゴリーに分類したものである。高炉に代表されるような製造現場で起きている複雑な現象は、非定常で非線形の領域に属するが、この領域を正面に見据えて解析できる一般的な方法論を、我々は持ち合わせていない。前述したように、現実世界で問題となるのは、高炉の炉況不調や連続鋳造プ

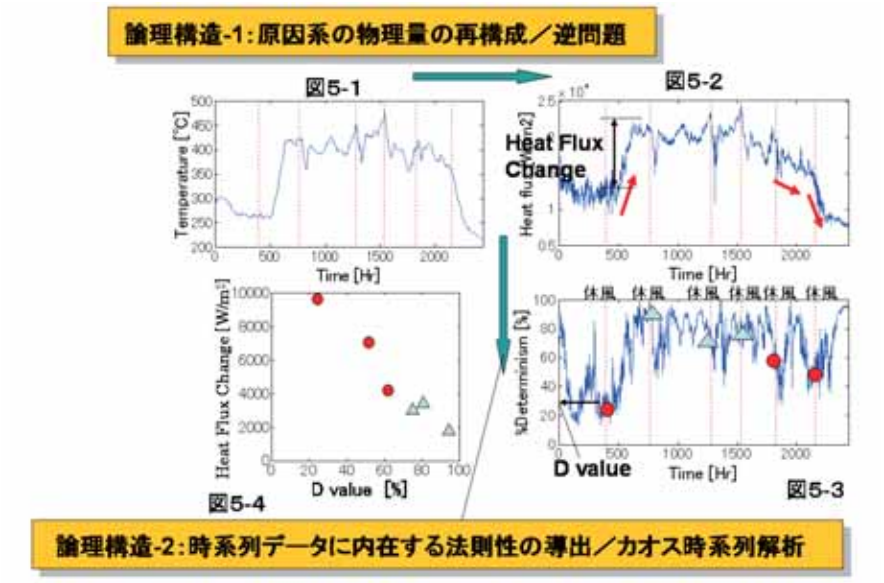


図 5：複数の論理構造のインテグレーションの効果

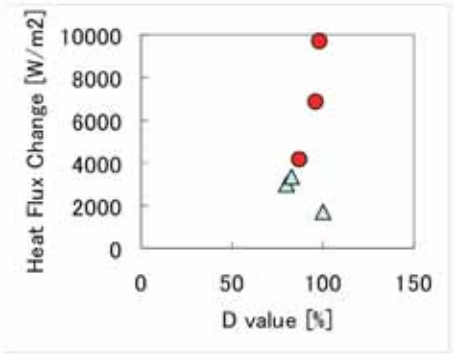


図 6：論理構造-2 のみの解析結果

ロセスの品質欠陥等にみられるような定常状態から乖離したときに発生すると考えられる異常状態である。これらプロセスの操業は、通常、異常状態を可能なかぎり回避するように管理されるので、異常状態が定常的に継続するようなことは稀で、我々が眼にするのは、過渡的な遷移過程のデータである。従って、このような問題に対処するには、過渡的な遷移過程にあるデータから、異常状態を引き起こす際の法則性を見出す必要がある。現状は、現場の経験と勘と呼ばれる定性的なアプローチを拠り所に、現実現象の解明に取り組んでいる。

もし、この非定常で非線形の領域に、新しい数学理論が適用出来れば、現実現象に数学論理をリンクさせ、新しいものの見方・考え方を製造現場に導入し、製造技術の効率化の追求や新

しい技術概念の創出が可能になると考える。この領域への数学者の参入を大いに期待する。

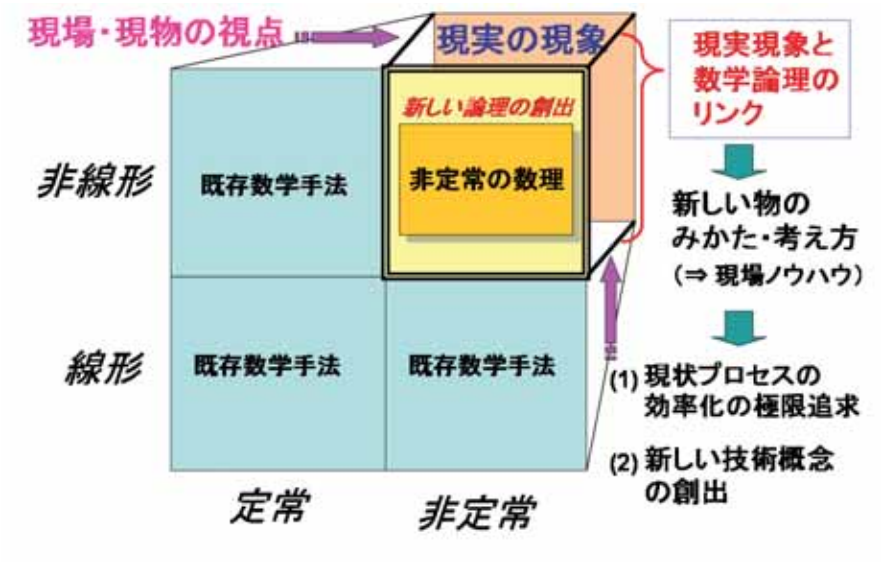


図 7：製造現場からの数学研究への期待

具体的な課題を普遍的なものに置き換え考えるという数学的思考の利点を現実世界で最大限発揮できるよう、

(1) 数学により抽象化した枠組みのなかで現実世界の問題をとらえ問題の根源を明らかにすること、

(2) 数学により構築した枠組みをもとに既存の技術概念の再構築を図ること、

(3) 技術の出口をつくり技術の製造現場や社会への浸透を図りイノベーションに繋げること、

これらが数学をコアにした産学連携の目指すものであるといえる。

CT スキャン、暗号理論、ウエーブレット等、数学者が純粋な数学的興味から作った理論が、時を隔てて数学者以外により思わぬ応用が見いだされ、応用面からの刺激で数学の分野が新たな次元で発展するという構図をとっており、これまでの歴史が実証するところによれば、数学・数理科学の他分野への応用及び応用からの刺激による理論研究の発展・深化は殆ど常にこの形で起こっている [6]。数学をコアにした産学連携は、数学理論と社会を動かす技術実現の時間の隔たりを劇的に短縮する大きな可能性を有しているといえる。

また、数学は普遍的であるがゆえに、個別の現象やデータに依存せずとも理論が成立し、中立を保つことができる。この中立性こそ、数学がイノベーションの源泉として、諸科学、工学、産業界に対し、ギブ・アンド・ギブン (Give & Given) の課題解決型の新たな連携スタイルを構築できる大きな強みになるはずである。

参考文献

[1] 山本昌宏，“逆問題入門”，岩波書店 (2002).

[2] 合原一幸，“カオス学入門”，放送大学教育振興会 (2001).

[3] P. Grassberger and I. Procaccia, “Characterization of strange attractors,” Phys. Rev. Lett., vol. 50, no. 5, pp. 346–349, 1983.

[4] F. Takens, “Detecting strange attractors in turbulence,” in Dynamical Systems of Turbulence, ed. D. A. Rand and B. S. Young, vol. 898 of Lecture Notes in Mathematics, pp. 366–381, 1981.

[5] 中川淳一, 合原一幸, “リカレンスプロットによる高炉の非定常解析”, 信学論 (A), vol. J187-A, no. 10, pp. 1303–1309, 2004.

[6] 九州大学，東京大学，新日鐵，日本数学会，文部科学省委託事業「数学・数理科学と他分野の連携・協力の推進に関する調査・検討〜第 4 期科学技術基本計画の検討に向けて〜」報告書 (2010).

時間周期非線形定常場の高速求解法

宮田　健治

(株) 日立製作所日立研究所

1　はじめに

時間微分項をもつ支配方程式で記述される現象には時間周期性をもつ場合が少なくない．その周期的な場が非線形性をもつ場合，複数の周波数成分をもつために，周波数領域解析で複素数表現による解を求めることは困難である．このため，時間領域で時間ステップを追いながら解析する step-by-step 法で解を求めることになるが，収束解を得るための時定数が長い場合，定常場を得るまでに多大な計算時間を要することになる．このため，時間周期非線形定常場を高速に求めるには何らかの工夫が必要になる．

これまで，時間周期非線形定常場を高速に求める努力が数多くなされてきた．非線形回路での周期解を得るために Aprille らは shooting 法を用いた方法 [1] を提案しており，電気回路系の解析に利用されている．また，有限要素法解析では，原らが，時間軸にも未知数を配置して時間周期境界条件を付加して解を求める時間周期有限要素法 [2] を提案しており，二次元解析で利用されている．しかし，両解法ともに，大規模体系での解析では過大な計算コストが足かせとなる．このほか，敢えて周波数領域で解析する山田らの調波有限要素法 [3] や時間領域 Galerkin 法 [4] があるが，これらについても同様である．単一周波数でかつ非線形性を考慮したハイブリッド解法 [5] もあるが，これは近似的な解を求めるには有効であるが，真の定常解を得るには，得られた近似解を初期値とした長時間の過渡解析が必要になる．このようにいくつかの解法が提案利用されてきたが，さらに有力で実用的な解法が望まれていた．

このような状況の中，2008 年に徳増により EEC (Explicit Error Correction) 法 [6, 7] をベースにした TP-EEC (Time Periodic Explicit Error Correction) 法 [8, 9, 10] が考案され，実用的な解法として広く利用されるようになった．これは，半周期性をもつ時間周期問題の場合，半周期の過渡解析で得られる解を利用して，効率的に解を補正し，周期解への収束を飛躍的に高めた方法である．さらに多相系で各相が近似的に互いに平等性を有する場合に有用な方法として，多相交流 TP-EEC 法 [11] が考案され，異なる相の情報を利用してさらに定常場への収束を高めた方法も登場し，中でも特に三相交流 TP-EEC 法がよく使われている．これに対し，筆者は高調波の影響が少ない場合に限定する方法として，TDC (Time Differential Correction) 法 [12] を，さらに正弦波ならびに複数の高調波ソースに限定する方法として，harmonic TDC 法 [13] を提案した．高調波ソース成分が少ない場合，TDC 法の方が補正のための過渡解析が少なく済む分有利な方法であるが，高調波ソース成分が多い場合は，TP-EEC 法や多相交流 TP-EEC 法の方が有利になるので使い分けが必要である [14]．ここでは， TP-EEC 法，三相

交流 TP-EEC 法ならびに TDC 法について概説する．なお，TDC 法および harmonic TDC 法について総括した内容は文献 [15] を参照されたい．

2　各種高速求解法の原理

2.1　TP-EEC 法

まず，TP-EEC 法のベースとなる EEC 法について述べる．解析対象の時間微分項をもつ支配方程式を時間一周期分を時間軸上で離散化して，複数の方程式で構成された連立方程式を考え，式 (1) のように行列方程式で表現する．

$$A\boldsymbol{x} = \boldsymbol{b} \tag{1}$$

ここで，$\boldsymbol{x}$, $\boldsymbol{b}$ はそれぞれ場を表すベクトル変数ならびにソース項を表すベクトル変数であり，1 周期を n 分割したときの各時刻のベクトル量 $\boldsymbol{x}_i$, $\boldsymbol{b}_i$ $(i = 1, 2, \ldots, n)$ を縦に時系列に並べて合成したベクトル量である．この行列方程式に時間周期境界条件式を導入すれば，式 (1) は時間周期非線形問題と考えることができる．時間領域で時間ステップを追いながら解析する step-by-step 法で解を求める操作は，式 (1) を block Gauss-Seidel 法で陽的に順次近似解を求めながら，反復収束させる操作と等価である．式 (1) の左辺の係数行列の条件数が大きく，解の収束性が悪い状況において，解を高速に求めるためには，行列方程式を変形させて，係数行列の条件数を小さくして 1 に近づければ良い．ほとんどの場合，式 (1) を

$$\boldsymbol{x} = \widehat{\boldsymbol{x}} + B\boldsymbol{p} \tag{2}$$

$$\begin{pmatrix} A & AB \\ CA & CAB \end{pmatrix} \begin{pmatrix} \widehat{\boldsymbol{x}} \\ \boldsymbol{p} \end{pmatrix} = \begin{pmatrix} \boldsymbol{b} \\ C\boldsymbol{b} \end{pmatrix} \tag{3}$$

とすることで収束性は向上される．また，行列 A が対称な場合，$C = B^T$ とすることで式 (3) の係数行列も対称性が維持される．式 (3) の解 $\widehat{\boldsymbol{x}}$ と $\boldsymbol{p}$ を同時に解くのが陰的誤差修正法であり，$\widehat{\boldsymbol{x}}$ と $\boldsymbol{p}$ を交互に反復させながら解くのが陽的誤差修正法である．式 (2) の第 1 項目の $\widehat{\boldsymbol{x}}$ を補正前の解と考え，第 2 項目の補正項 $B\boldsymbol{p}$ を加えることで，より定常解に近い解 $\boldsymbol{x}$ を求めることができる．この場合，補正項 $B\boldsymbol{p}$ を求める方程式は，式 (3) より，

$$B^T AB\boldsymbol{p} = B^T(\boldsymbol{b} - A\widehat{\boldsymbol{x}}) \tag{4}$$

となる．ここで収束が緩慢な減衰項を 1 周期において近似的に定数項と見なすと，行列 B を定数項抽出写像行列とみなせ，

$$B = (I, I, \ldots, I)^T \tag{5}$$

（I：単位行列）とおき，$\boldsymbol{p}$ は次式で求められる．

$$\left(\sum_{i,j} A_{ij}\right)\boldsymbol{p} = \sum_{i=1}^{n} \boldsymbol{r}_i \tag{6}$$

ここに，$\boldsymbol{r}_i$ は 1 周期を n 分割したときの i 番目の時刻における残差ベクトル

$$\boldsymbol{r}_i = \boldsymbol{b}_i - (A\widehat{\boldsymbol{x}})_i \tag{7}$$

である．

ここで，具体例として，非線形時間周期場を支配する非線形方程式

$$S(\boldsymbol{x}) + C\frac{\partial \boldsymbol{x}}{\partial t} = \boldsymbol{b} \tag{8}$$

について考える．ここに，$S(\boldsymbol{x})$ は非線形項であり，C は定数である．ここで，後方 Euler 法で時間軸を離散化すると，

$$(S_i + \widetilde{C})\boldsymbol{x}_i - \widetilde{C}\boldsymbol{x}_{i-1} = \boldsymbol{b}_i \qquad (\widetilde{C} = C/\Delta t,\ i = 1, \ldots, n) \tag{9}$$

となる．ここでは半周期性の問題を考えることにし，周期を T として，半周期境界条件 $\boldsymbol{x}(t + T/2) = -\boldsymbol{x}$ を考慮すると，式 (1) に相当する式は

$$\begin{bmatrix} S_1 + \widetilde{C} & 0 & \cdots & 0 & \widetilde{C} \\ -\widetilde{C} & S_2 + \widetilde{C} & \cdots & 0 & 0 \\ 0 & -\widetilde{C} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & -\widetilde{C} & S_n + \widetilde{C} \end{bmatrix} \begin{Bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_n \end{Bmatrix} = \begin{Bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{Bmatrix} \tag{10}$$

となる．第 1 行 n 列目の行列 $\widetilde{C}$ は半周期境界条件によるものである．ここで，式 (6) を用いて 0 次の補正項 $\boldsymbol{p}$ を求める．そのためには，式 (6) に含まれる残差ベクトル $\boldsymbol{r}_i$ を求めなければならない．各時刻において方程式 (8) の解を求めているために $i = 2, \ldots, n$ については $\boldsymbol{r}_i = \boldsymbol{0}$ となる．これに対して $\boldsymbol{r}_1$ のみが特別である．周期定常場に至るまでの過渡過程におけるある時刻の解 $\widehat{\boldsymbol{x}}_0$ と半周期後の解 $\widehat{\boldsymbol{x}}_n$ の間には，まだ半周期境界条件が厳密に満足されていないため，残差ベクトル $\boldsymbol{r}_1$ は非ゼロの有意なベクトル量となる．式 (10) の先頭行の関係式から残差 $\boldsymbol{r}_1$ が発生するため，

$$\boldsymbol{r}_1 = \boldsymbol{b}_1 - (S_i + \widetilde{C})\widehat{\boldsymbol{x}}_i - \widetilde{C}\widehat{\boldsymbol{x}}_n \tag{11}$$

と書ける．ここで，$i = 1$ の場合の式 (9) を過渡過程の解ベクトル $\widehat{\boldsymbol{x}}_0$, $\widehat{\boldsymbol{x}}_1$ で表現した

$$(S_i + \widetilde{C})\widehat{\boldsymbol{x}}_1 - \widetilde{C}\widehat{\boldsymbol{x}}_0 = \boldsymbol{b}_1 \tag{12}$$

を用いてソース項 $\boldsymbol{b}_1$ を消去できる．これにより，残差ベクトル $\boldsymbol{r}_i$ を整理すると，

$$\boldsymbol{r}_1 = -\widetilde{C}(\widehat{\boldsymbol{x}}_0 + \widehat{\boldsymbol{x}}_n), \qquad \boldsymbol{r}_i = \boldsymbol{0} \quad (i = 2, \ldots, n) \tag{13}$$

となる．

ここで，式 (10) の左辺の係数行列から $\sum_{i,j} A_{ij}$ を求め，これと式 (13) を式 (6) に代入すると，

$$\left(2C + \Delta t \sum_{i=1}^{n} S_i\right)\boldsymbol{p} = -C(\widehat{\boldsymbol{x}}_0 + \widehat{\boldsymbol{x}}_n) \tag{14}$$

が得られる．これが，TP-EEC 法の 0 次補正に関する基本式である．補正のためには半周期毎に式 (14) の行列方程式を解く必要がある．ここで，式 (14) の左辺の括弧内の係数行列のうち，第 2 項目の S_i の総和の項の影響が C に比べて無視できる場合，式 (14) から

$$\boldsymbol{p} \cong -\frac{1}{2}(\widehat{\boldsymbol{x}}_0 + \widehat{\boldsymbol{x}}_n) \tag{15}$$

が得られる．式 (2), (5) より，簡易 TP-EEC 法による第 n ステップ目のベクトル量 $\boldsymbol{x}_n$ に関する補正式

$$\boldsymbol{x}_n^{\mathrm{new}} = \frac{1}{2}(\widehat{\boldsymbol{x}}_n - \widehat{\boldsymbol{x}}_0) \tag{16}$$

が得られる．式 (16) は単純な式であり，補正のための計算コストはゼロに近い．

2.2 三相交流 TP-EEC 法

前節に述べた TP-EEC 法は，多相交流系でももちろん利用できる．多相交流系には異なる相の情報を補正に利用できるので，半周期問題でも半周期よりも短い時間内の過渡解析で補正が可能になる．ここでは多相交流系の中でも良く利用されている三相交流系について述べる．三相交流系は 1/6 周期経過すると，三相の位相が順次入れ替わった位置に移動する．そこで，1/6 周期にわたる時系列ベクトル $\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ を考える．ここで，

$$\boldsymbol{x}_0 = \begin{Bmatrix} \boldsymbol{U}_0 \\ \boldsymbol{V}_0 \\ \boldsymbol{W}_0 \end{Bmatrix}, \qquad \boldsymbol{x}_n = \begin{Bmatrix} \boldsymbol{U}_n \\ \boldsymbol{V}_n \\ \boldsymbol{W}_n \end{Bmatrix} \tag{17}$$

とおくと，図 1 より

$$\boldsymbol{x}_0 = -G\boldsymbol{x}_n, \qquad G = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I} \\ \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I} & \boldsymbol{0} \end{bmatrix} \tag{18}$$

とおける．

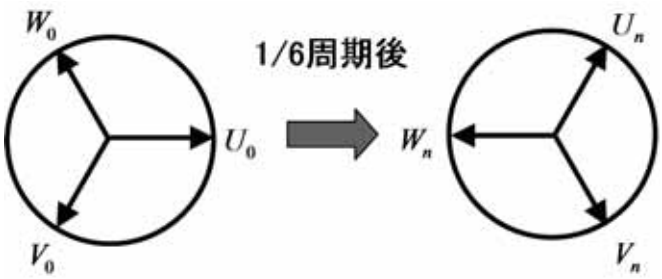


図 1：三相交流系における三相の時間変化

このため，式 (10) は次式のようになる．

$$\begin{bmatrix} S_1+\widetilde{C} & 0 & \cdots & 0 & \widetilde{C}G \\ -\widetilde{C} & S_2+\widetilde{C} & \cdots & 0 & 0 \\ 0 & -\widetilde{C} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & -\widetilde{C} & S_n+\widetilde{C} \end{bmatrix} \begin{Bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \vdots \\ \boldsymbol{x}_n \end{Bmatrix} = \begin{Bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \\ \vdots \\ \boldsymbol{b}_n \end{Bmatrix} \tag{19}$$

また，式 (11) は

$$\boldsymbol{r}_1 = -\widetilde{C}(\widehat{\boldsymbol{x}}_0 + G\widehat{\boldsymbol{x}}_n), \qquad \boldsymbol{r}_i = \boldsymbol{0} \quad (i = 2, \ldots, n) \tag{20}$$

となり，EEC 法による 0 次補正に関する基本式 (6) は，

$$\left(C(I+G) + \Delta t \sum_{i=1}^{n} S_i \right) \boldsymbol{p} = -C(\widehat{\boldsymbol{x}}_0 + G\widehat{\boldsymbol{x}}_n) \tag{21}$$

となる．これが三相交流 TP-EEC 法による補正項 $\boldsymbol{p}$ を求める式であり，1/6 周期毎に補正が可能である．ここで，式 (21) の左辺の括弧内の係数行列のうち，第 2 項目の S_i の総和の項の影響が $C(I+G)$ に比べて無視できる場合，式 (21) から

$$(I+G)\boldsymbol{p} \cong -(\widehat{\boldsymbol{x}}_0 + G\widehat{\boldsymbol{x}}_n) \tag{22}$$

が得られる．式 (2), (5) より，三相交流簡易 TP-EEC 法による補正式

$$\begin{aligned} \boldsymbol{U}_n^{\mathrm{new}} &= (d\boldsymbol{U} + d\boldsymbol{V} - d\boldsymbol{W})/2, & d\boldsymbol{U} &= \widehat{\boldsymbol{U}}_n - \widehat{\boldsymbol{U}}_0 \\ \boldsymbol{V}_n^{\mathrm{new}} &= (d\boldsymbol{V} + d\boldsymbol{W} - d\boldsymbol{U})/2, & d\boldsymbol{V} &= \widehat{\boldsymbol{V}}_n - \widehat{\boldsymbol{V}}_0 \\ \boldsymbol{W}_n^{\mathrm{new}} &= (d\boldsymbol{W} + d\boldsymbol{U} - d\boldsymbol{V})/2, & d\boldsymbol{W} &= \widehat{\boldsymbol{W}}_n - \widehat{\boldsymbol{W}}_0 \end{aligned} \tag{23}$$

が得られる．ここで，$\widehat{\boldsymbol{U}}_n$ は過渡過程における $\boldsymbol{U}_n$ の解であり，他も同様である．

式 (23) は三相交流簡易 TP-EEC 法による補正式としてよく使われているが，式 (18) は三相交流系におけるあるひとつの関係式に過ぎない．ここで議論している三相交流系は，$U_n+V_n+W_n = 0$ の平衡状態を暗に仮定しているので，式 (18) は

$$\begin{aligned} \boldsymbol{x}_0 &= -\begin{bmatrix} \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I} \\ \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I} & \boldsymbol{0} \end{bmatrix} \boldsymbol{x}_n - \begin{Bmatrix} \beta_1(\boldsymbol{U}_n + \boldsymbol{V}_n + \boldsymbol{W}_n) \\ \beta_2(\boldsymbol{U}_n + \boldsymbol{V}_n + \boldsymbol{W}_n) \\ \beta_3(\boldsymbol{U}_n + \boldsymbol{V}_n + \boldsymbol{W}_n) \end{Bmatrix} \\ &= -\begin{bmatrix} \beta_1\boldsymbol{I} & \beta_1\boldsymbol{I} & (1+\beta_1)\boldsymbol{I} \\ (1+\beta_2)\boldsymbol{I} & \beta_2\boldsymbol{I} & \beta_2\boldsymbol{I} \\ \beta_3\boldsymbol{I} & (1+\beta_3)\boldsymbol{I} & \beta_3\boldsymbol{I} \end{bmatrix} \boldsymbol{x}_n \\ &\triangleq -G\boldsymbol{x}_n \end{aligned} \tag{24}$$

という形で一般化できる．式 (24) で新たに定義した G を用いて，式 (21) および式 (22) がそのまま使える．このとき，式 (23) は

$$\begin{aligned}\boldsymbol{U}_n^{\mathrm{new}} &= \alpha_1(d\boldsymbol{U} + d\boldsymbol{V} + d\boldsymbol{W}) - d\boldsymbol{W}\\ \boldsymbol{V}_n^{\mathrm{new}} &= \alpha_2(d\boldsymbol{V} + d\boldsymbol{W} + d\boldsymbol{U}) - d\boldsymbol{U}\\ \boldsymbol{W}_n^{\mathrm{new}} &= \alpha_3(d\boldsymbol{W} + d\boldsymbol{U} + d\boldsymbol{V}) - d\boldsymbol{V}\end{aligned} \tag{25}$$

となる．ここで，

$$\alpha_1 = \frac{1+\beta_3}{\beta}, \quad \alpha_2 = \frac{1+\beta_1}{\beta}, \quad \alpha_3 = \frac{1+\beta_2}{\beta}, \quad \beta = 2+\beta_1+\beta_2+\beta_3 \tag{26}$$

である．三相 U, V, W は互いに平等なので，補正も平等に取り扱うという観点から，$\alpha_1 = \alpha_2 = \alpha_3 = \alpha$ とおくのが自然であろう．この場合，式 (25) より，$\alpha = 1/3$ のときに三相交流系の平衡条件 $\boldsymbol{U}_n^{\mathrm{new}} + \boldsymbol{V}_n^{\mathrm{new}} + \boldsymbol{W}_n^{\mathrm{new}} = 0$ が厳密に満足される．なお，$\alpha = 1/2$ にした方が時間高調波源が存在する場合にも概ね強い補正効果を発揮する．

なお，式 (25) は EEC 法を使わなくとも，複素空間におけるフェーザ図を利用して直視的に求めることができることを付記しておく．

2.3 TDC 法

EEC 法を用いない誤差修正法として，TDC (Time Differential Correction) 法がある．これは，対象場の時間微分を利用した方法である．

TDC 法の補正原理を説明するために，半周期性をもつ一変数場 $x(t)$ を考える．基本角周波数を ω とおき，減衰係数 γ の減衰場を考慮すると，$x(t)$ は例えば

$$x(t) = a_0 e^{-\gamma t} + a_1 \sin\omega t + b_1 \cos\omega t + \sum_{n=1}^{\infty}\bigl[a_n \sin(2n+1)\omega t + b_n \cos(2n+1)\omega t\bigr] \tag{27}$$

と書ける．対象は非線形場であるため，上記の基本波ならびに高調波の係数 a_n, b_n $(n = 1, 2, \dots)$ は式 (27) の右辺第 1 項に示した減衰項の影響を受け，時間とともに変化しながら定常場に達する．定常場に近い場を得るには，定常場の主要項である基本波成分を抽出することが肝要である．そのために $x(t)$ の時間微分を用いる．時間微分により，減衰が緩慢な減衰項の全体に占める割合は大きく低下する．その代わり，高調波成分の全体に占める割合は大きくなるため，平均化処理で高調波成分をなるべく低く抑える．高調波成分は，定常場への収束が比較的速いため，補正回数が多くない限り，補正の障害にはならない．概念的ではあるが，以上が TDC 法の補正原理である．

それでは，以下具体的な補正法について述べる．便宜上，時間変数 t の代わりに位相変数 θ $(= \omega t)$ を用いる．ここで，平均化処理のための時間積分位相幅を 2ϕ とおく．$x(\theta)$ の基本波成分を $x_1(\theta)$ とおき，$x_1(\theta)$ の平均値を $\langle x_1\rangle$ と表す．現時刻に対応する位相 θ を平均化積分の上端とすると，

$$\langle x_1\rangle = \frac{1}{2\phi}\int_{\theta-2\phi}^{\theta} x_1(\theta')\,d\theta' = \left(\frac{\sin\phi}{\phi}\right) x_1(\theta-\phi) \tag{28}$$

を得る．$x_1(\theta)$ が基本正弦波であることを考慮すると，

$$\frac{d^2\langle x_1\rangle}{d\theta^2} = -\left(\frac{\sin\phi}{\phi}\right)x_1(\theta-\phi) \tag{29}$$

となり，次の補正式が得られる．

$$x^{\mathrm{new}}(\theta-\phi) = -\left(\frac{\phi}{\sin\phi}\right)\frac{d^2\langle x\rangle}{d\theta^2} \tag{30}$$

ここで，添え字 new は補正後の値を示す．1 階の時間微分を用いた補正も考えられるが，2 階の時間微分項に比べ 1 階の時間微分項には緩慢な減衰項が比較的多めに残留してしまうため，2 階の時間微分項のみを用いる式 (30) が最も高い補正能力を有する．

このほかにも高次の時間微分を使えば多種多様な補正式を作ることはできるが，時間微分が 3 階以上になると高調波による影響が大きくなるため，実用的ではない．

TDC 法は，TP-EEC 法のように行列方程式を解くという煩わしい計算処理を必要とせず，補正に要する計算コストは実質ゼロに近い．また，TP-EEC 法では 1 回の補正のために半周期の過渡解析を実行する必要があるが，TDC 法では時間平均幅を半周期よりも短く設定できるため，半周期よりも短いステップの過渡解析を実施すれば，補正をかけることができる．なお，TDC 法には 1 個〜3 個までの高調波を考慮した補正法も考案されている [13].

3　補正法に関する数値実験

前章にて提示した各種補正法を用いた数値計算例について紹介する．

3.1　3 変数連立微分方程式

まずは最も単純な例題のひとつとして式 (31) に示す 3 変数 U, V, W の解析について示す．

$$\begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}\begin{Bmatrix} dU/d\theta \\ dV/d\theta \\ dW/d\theta \end{Bmatrix} + \begin{Bmatrix} U \\ V \\ W \end{Bmatrix} = \begin{Bmatrix} \cos n\theta \\ \cos n(\theta-2\pi/3) \\ \cos n(\theta-4\pi/3) \end{Bmatrix}, \qquad (n=1,2,\dots) \tag{31}$$

この方程式の理論定常解は

$$U_{\mathrm{th}} = a\cos(n\theta+\varphi_n),\ V_{\mathrm{th}} = a\cos\left[n\left(\theta-\frac{2\pi}{3}\right)+\varphi_n\right],\ V_{\mathrm{th}} = a\cos\left[n\left(\theta-\frac{4\pi}{3}\right)+\varphi_n\right] \tag{32}$$

である．ここに，

$$a_n = \frac{1}{\sqrt{1+g_n^2}},\quad \varphi_n = -\tan^{-1}g_n,\quad g_n = n\left[3-2\cos\left(\frac{2n\pi}{3}\right)\right] \tag{33}$$

である．U, V, W の初期値を全てゼロに設定し，右辺ソース項に基本波 $n=1$ のみが存在する場合の計算結果を図 2 に示す．1 周期の時間分割数を 192 に設定した．高調波を含まない場

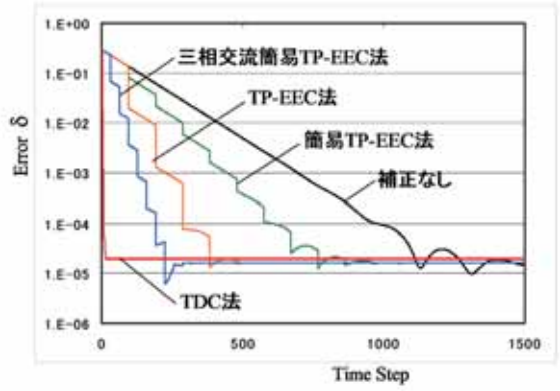


図 2：各種補正法の比較（基本波のみの場合）

合，TDC 法では平均化処理は不要である．図に示した誤差 δ は次式で定義された値である．また，全ての補正法の補正回数には制限を加えなかった．

$$\delta = \sqrt{(U - U_{\rm th})^2 + (V - V_{\rm th})^2 + (W - W_{\rm th})^2} \tag{34}$$

図が示すように，高調波を含まなければ，TDC 法が最大の補正能力を示す．1 回当たりの補正量も TDC 法が最大であり，その次が TP-EEC 法である．三相交流簡易 TP-EEC 法は 1 回当たりの補正量は TP-EEC 法より小さいものの，補正頻度が TP-EEC 法の 3 倍あるために，TP-EEC 法よりも補正能力は大きい．

次に基本波振幅 1 に対して，1%の振幅を有する 5 次および 7 次の高調波を含む場合の計算結果を図 3 に示す．この場合も U, V, W の初期値を全てゼロに設定した．このときの TDC 法における平均化処理に用いた時間幅をステップ数に換算すると 19 である．これは 5 次の高調波の半周期にわたるステップ数に相当する．なお，TDC 法の補正回数は 3 回に限定し，その他の補正については補正回数に制限を加えなかった．

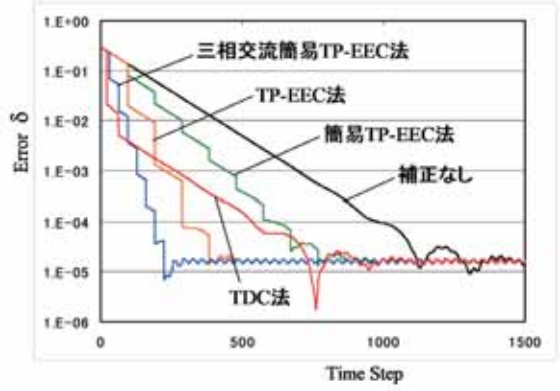
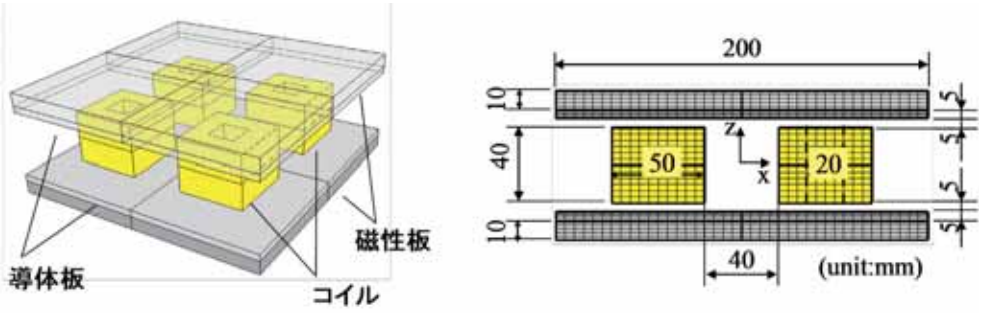


図 3：各種補正法の比較（高調波を含む場合）

図 3 が示すように，高調波が存在しても，TP-EEC 法系の 3 種の補正法はすべてほとんど影響を受けていない．これに対して，TDC 法では大きく影響を受け，正弦波のときの場合と比べて補正能力は低下していることがわかる．TDC 法は高次よりも低次の高調波の影響を受けやすい．高調波による副作用の影響のため，通常，TDC 法の補正回数は 3 回が限度である．

3.2 渦電流を伴う静止器磁界解析

渦電流を伴う静止器磁界解析における定常場解析例を示す．解析に用いたメッシュ分割図を図 4 に示す．4 個の矩形状コイルの上下に正方形の導体板と磁性板を重ねて配置したモデルになっている．側面は，どの面から見ても同サイズである．導体板の導電率は 3.6×10^7 S/m，コイル電流は $100\cos(2\pi ft)$ kAT，周波数 f は 200 Hz とし，電流は全てのコイルで同方向に流れるとした．磁性板は電磁鋼板 35A300 と同じ初磁化曲線を用いた．モデルの対称性により，1/8 領域を切り出して解析した．また，要素数は 41,650 で，すべて六面体で構成した．上面および側面には磁場が面に平行になる Dirichlet 境界条件を課し，下面には磁場が面に直交する Neumann 境界条件を課した．1 周期の時間分割数を 40 とした（時間分割幅：0.125 ms）．



(a) 解析モデル鳥瞰図　　(b) 解析モデルサイズ及びメッシュ分割図

図 4：静止器モデル

図 5 に磁性板内の $x = y = 42$ mm, $z = 35$ mm の位置における磁束密度の x 成分，z 成分の時間変化を，図 6 に導体板に発生する渦電流損の時間変化を補正なしの場合および TDC 法と簡易 TP-EEC 法による補正結果を比較して示す．補正回数はともに 3 回である．なお，顕著な高調波は存在しないため，TDC 法では時間平均処理は不要である．図が示すように，定常に達するまでの時間ステップ数は，簡易 TP-EEC 法では 60 ステップ（1 周期半）であるのに対して，TDC 法では 14 ステップである．

3.3 電源回路連成同期モータ磁界解析

次に電源回路と連結した同期モータの磁界解析における定常場解析例を示す．検証に用いた同期モータのメッシュ分割図を図 7 に，またモータの諸量を表 1 に示す．4 極 6 スロットモータで 2 周期構造をもつため，1 周期分に相当する 1/2 モデルとした．要素数は 8,682 である．回転子・固定子間のスライド面は周方向に 180 等分割した．コイルには抵抗 R が直列接続さ

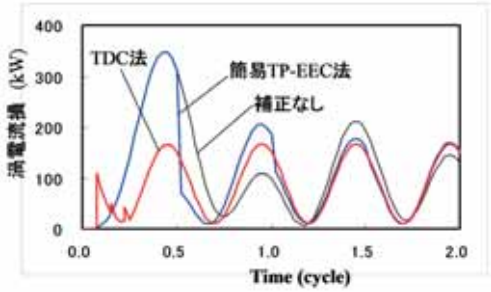


図 5：渦電流損の時間変化

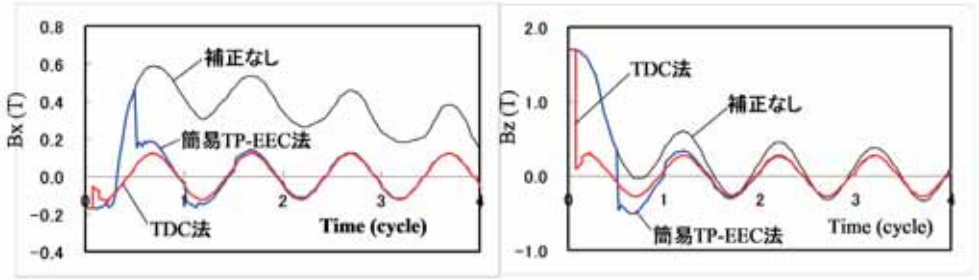


図 6：磁束密度の時間変化（磁性板内の $x = y = 42\,\mathrm{mm}$, $z = 35\,\mathrm{mm}$ の位置）

れ，3 相 Y 結線で電圧源と接続されている．抵抗はコイル抵抗も含めて 0.2 Ω とし，外部インダクタンス L は 0 に設定した．また，相電圧の実効値を 100 V に設定した．スライド面周方向 1 分割ずつ回転移動しながら解析した．

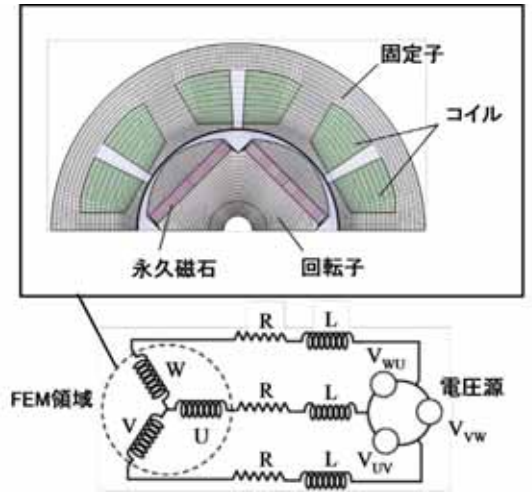


表1　同期モータの諸量

回転子最大外径	54.8mm
固定子内径	56.0mm
固定子外径	103mm
最小エアギャップ	0.6mm
モータコア部長さ	55mm
永久磁石 残留磁束密度	1.315T

図 7：電源回路連成同期モータ解析モデル

図 8 に U 相コイル電流，図 9 にトルクの解析における補正なしの場合と簡易 TP-EEC 法，三相交流簡易 TP-EEC 法，および TDC 法による補正した結果を示す．両補正ともに時間微分項を形成するコイル領域にある磁気ベクトルポテンシャルの未知変数に関して補正をかけた．補正回数はそれぞれ，簡易 TP-EEC 法は 6 回（3 回では不十分），三相交流簡易 TP-EEC 法ならびに TDC 法が 3 回である．なお，TDC 法では 3 ステップ平均を用いた．

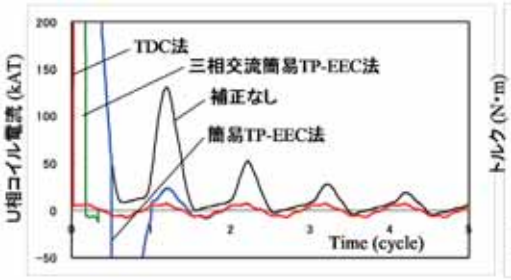


図 8：U 相コイル電流波形

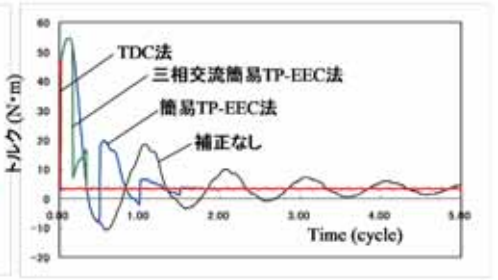


図 9：トルク波形

この場合，簡易 TP-EEC 法が 90 ステップ毎にしか補正がかけられないのに対して，三相交流簡易 TP-EEC 法は 30 ステップ毎に，また TDC 法は 6 ステップ毎に補正がかけられる．このため，定常に達するまでの時間ステップ数は，簡易 TP-EEC 法では 400 ステップ（2.2 周期）であるのに対して，三相交流簡易 TP-EEC 法では 93 ステップ，TDC 法では 33 ステップである．

4　おわりに

半周期の時間周期性をもつ非線形定常場を高速に求めるための数値解析法について述べた．TP-EEC 法は半周期性問題に適用した場合，半周期毎の補正に限定される．これに対して多相交流系では，異なる相の情報を有効利用できるために，相の数の倍率で補正に必要な時間ステップ数を縮減できる．例えば三相交流形では 1/3 に縮減できるために，三相交流 TP-EEC 法を用いると 1/6 周期毎の過渡解析で補正が可能になる．これに対して，補正原理が全く異なる TDC 法はこの縛りがなくなる．TDC 法は時間微分を利用するために概ね 1/6 周期よりも短い過渡解析で補正が可能になるが，高調波の影響を受け易いため，TP-EEC 法や多相交流系 TP-EEC 法と使い分けする必要がある．

なお，半周期性はなく一周期性のみをもつ問題については，TP-EEC 法が利用可能であり，さらに収束性向上に向けて検討が進みつつある．非線形の周期場を高速に求めるための方法は，まだ工夫の余地があり，今後さらに発展する可能性を秘めている．

参考文献

[1] T. J. Aprille Jr. and T. N. Trick, Steady-state analysis of nonlinear circuits with periodic inputs, Proc. IEEE, **60** (1972), no. 1, 108–114.

[2] 原，ほか，時間周期有限要素法による高圧・回転機コロナシールド部の電界解析，電学論 B，**102-B** (1982), no. 7, 423–430.
[3] 山田，ほか，調波有限要素法による磁気飽和を考慮した交流定常磁界解析，電学論 D，**109-D** (1989), no. 10, 756–762.
[4] R. Albanese, E. Coccorese, et al., Periodic Solutions of Nonlinear Eddy Current Problems in Three-Dimensional Geometries, IEEE Trans. Magn., **28** (1992), no. 2, 1118–1121.
[5] 山崎，新福，中性点電位変動を考慮した誘導電動機の特性解析，電気学会静止器・回転機合同研究会資料，SA-99-23/RM-99-77 (1999).
[6] T. Iwashita, T. Mifune, and M. Shimasaki, Similarities between implicit correction multigrid method and A-phi formulations in electromagnetic field analysis, IEEE Trans. Magn., **31** (2008), no. 3, 946–949.
[7] 美舩健, 守口総一, 岩下武史, 島崎眞昭, 高アスペクト比のメッシュを用いた有限要素法のための Implicit error correction 法及び Explicit error correction 法に関する基礎検討，電気学会マグネティックス・静止器・回転機合同研究会研究資料，MAG-08-19/SA-08-7/RM-08-7 (2008).
[8] 徳増正，藤田真史，上田隆司，2 次元電磁界解析の有効利用に残された課題（その 3），電気学会静止器・回転機合同研究会研究資料，SA-08-62/RM-08-69 (2008).
[9] 高橋康人，徳増正，若尾真治，岩下武史，金沢正憲，時間周期有限要素法と EEC 法に基づく非線形過渡電磁場解析の収束特性改善に関する基礎的検討，電気学会静止器・回転機合同研究会研究資料，SA-08-63/RM-08-70 (2008).
[10] 高橋康人，徳増正，藤田真史，若尾真治，岩下武史，金沢正憲，時間周期有限要素法と EEC 法に基づく非線形過渡電磁場解析における時間積分の収束性改善，電気学会論文誌 B，**129** (2009), no. 6, 791–798.
[11] 徳増正，藤田真史，上田隆司，2 次元電磁界解析の有効利用に残された課題（その 4），電気学会静止器・回転機合同研究会研究資料，SA-09-6/RM-09-6 (2009).
[12] 宮田健治，時間周期非線形場の高速求解法，電気学会マグネティックス・静止器・回転機合同研究会研究資料，MAG-10-8/SA-10-8/RM-10-8 (2010).
[13] 宮田健治，時間周期非線形場高速解析のための harmonic TDC 法および TDC・簡易 TP-EEC 併用法，電気学会静止器・回転機合同研究会研究資料，SA-10-91/RM-10-100 (2010).
[14] Y. Takahashi, T. Tokumasu, et al., Comparison between fast steady-state analysis methods for time-periodic nonlinear magnetic field problems, IEEE Trans. Magn., **48** (2012), no. 2, 235–238.
[15] K. Miyata, Fast analysis method of time-periodic nonlinear fields, J. Math Indust., **3** (2011), 2011B-7, 131–140.

産業界において計算科学は如何に実践されているか
―生物、化学そして物理の計算科学―

中村　振一郎

理化学研究所・社会知創成事業・中村特別研究室
三菱化学フェロー

1　はじめに

今日、自然科学の対象は多様であり、空間スケールにおいては素粒子から原子分子、生体、そして宇宙まで広がり、時間スケールにおいては、宇宙の始まりから未来までを相手とする。その広大無辺な自然科学の中でたった一つ、実験をしなくとも決着をつけることができる分野、それが数学である。化学徒の筆者に、この事実は真に不思議としか言えない。計算科学は数学を基礎に持つが、数学そのものではなく、その真偽を論じる根拠はまたしても実験であり、実験結果と相補的な役割をするのが計算科学である。

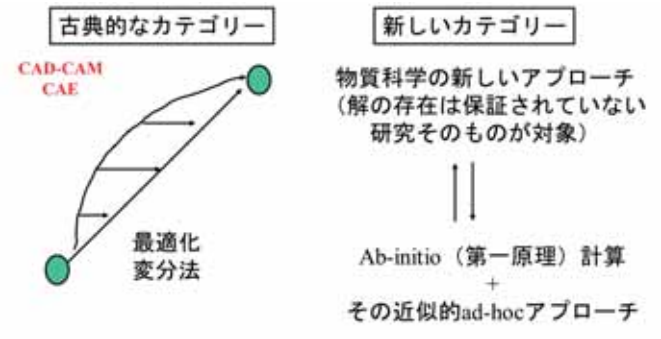
本章は、数学徒を想定読者として、化学徒が計算科学について書いたものである。生命科学、物質科学を扱う計算科学に何らかの意味で関心は在っても自らの手で実行するまでには至っていない研究者、学生諸君を対象とする計算科学の短い案内書である。

筆者は総合化学企業・民間企業の研究開発業務に長年携わり、産業界の計算科学に従事してきた。これからの若い数学の徒に、教職、サービス業、IT 業務だけに限らず、製造業を始めとした産業界の全体を射程として、そこに身を投じ自分を試す場と考えさえすれば、そこにも桁違いに面白い展開があり得ること、これを伝えたいという思いから記されたものである。つまり産業界を自分の事として、もっと目を向けていただきたいとの思いを主たる動機として書かれたものある。

2　産業界における計算科学の二つの系譜

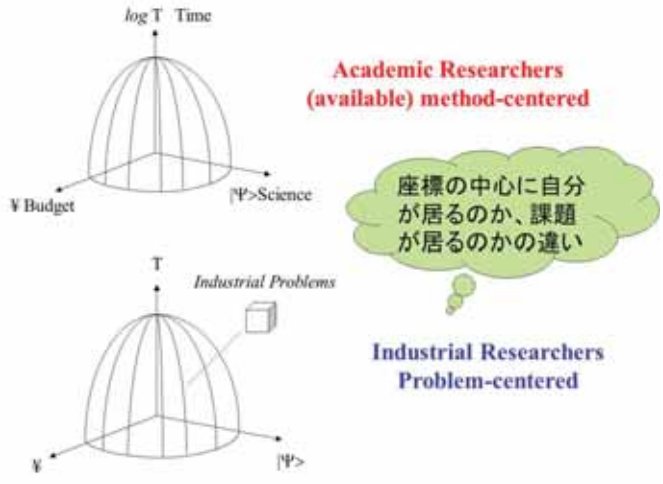
産業界における筆者の経験によれば、計算科学は下図に示すように、大きく二つのカテゴリーに分類することができる。第一は左図に示された古典的計算とでも称すべき範疇である。日本でも、70 年代飛躍的に進展し、すでに確立した分野である。機械工業、自動車工業、化学工業（プラントエンジニアリング）において不可欠で、総じてエンジニアリングの計算科学と言うことができる [1]。構造体の強度計算、機械的変形予測など、有限要素法を始めとして確立した巨大な分野である。加えて流体力学や塗布加工の計算、音響シミュレーション、そして物理音源の計算も重要である。手法的に一応の確立を観たとはいえ、産業界の現場の問題の大半は、解析解からは程遠い難問ばかりであり、今日でも創造的な創意工夫が商品設計の極め

となることから、大学よりもむしろ企業のなかで休むことなく進化している。これらの特徴は第二のカテゴリーと違い、インプットとアウトプットは決まっており、その最適化プロセスが課題である。



本稿で主に扱うのは上図右のカテゴリーに属するものである。代表的なものはシュレージンガー方程式を基礎とする ab-initio（第一原理）計算である。上記の左のカテゴリーでは（容易に見出しうるかどうかは別として）どこかに最適解が存在する。一方、この右のカテゴリーの計算科学では課題は「新しい触媒を見出せ」あるいは「新しい薬を見出せ」という設問に代表されるものである。そもそも解が存在するかどうか、その保証は何処にもない。それ故に、経験知、暗黙知が命運を分ける領域である。厳しさの中に、滅多なことでは得られない面白さが潜んでいる。

3　産業界の計算科学の特殊性



上図に示したのは、産業界における計算科学の過酷な特殊性を表す模式図である。産業界に出現する課題は、計算であれ実験であれ、アカデミック界が直面する課題とは様相を異にす

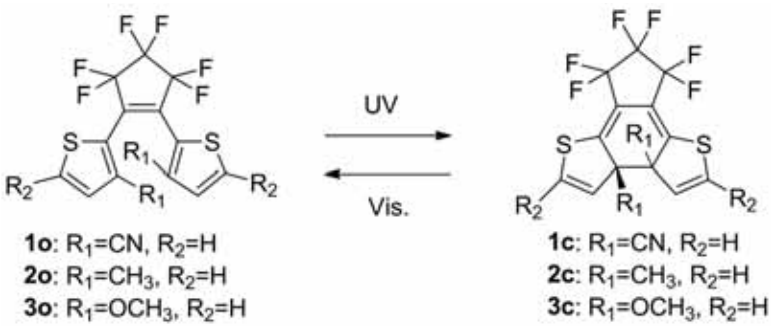
る。上図は経済、サイエンスそして時間という 3 次元で張られた空間における半球であり、これをテクノロジー球と呼ぶことにしよう。この球の中は既知のテクノロジーである。官学の任務は人類の英知としてこの球を着実に拡大してゆくことにある。論文として確実な成果を蓄積してゆくためには、手法を地道に構築して進まねばならない。一方、産業界ではその中に止まっている限り、扱う現象や物では差別化できず価値を生むことができない。よって必然的に直面する課題はその球の表皮（極端な場合にはその外）にある。

4　分子および固体系を対象とする計算科学の概説

優れた概説書が既に十分に存在する。ここで屋上屋を架すことを止め、文献を示し [2–6]、背景を述べる。1970 年代後半に量子化学の非経験的分子軌道法計算の汎用ソフトウエアのプロトタイプ（殆どが FORTRAN 言語で書かれ、短いものでも 3–5 万ステップという大量のプログラムである）がほぼ出揃い、今日では Gaussian、GAMESS をはじめとして、世界中で活用されている [2]。日本の原子分子物理・それに繋がる量子化学の完成度は高く 70–80 年代には国産のソフトも存在したが現在は欧米のソフトにほぼすべてが取って変わられてしまった（勿論、電子状態の個別の問題に優れた機能をもつルーチンでは我が国の研究者は依然として気鋭である）。一方、固体のバンド構造を求める第一原理計算は量子化学に比べて、まだ自作のソフトを構築し活用する学問的に健全なプロセスが継続しつつある [3]。さらに疎視化シミュレーション、統計力学に立脚した古典 MD シミュレーション、マルチスケールの計算科学、ゆらぎのエネルギー論という脈々とした計算科学の進展は目覚ましくさらなる展開が期待される [4–6]。

5　有機光応答性分子のポテンシャル超曲面を用いた分子設計

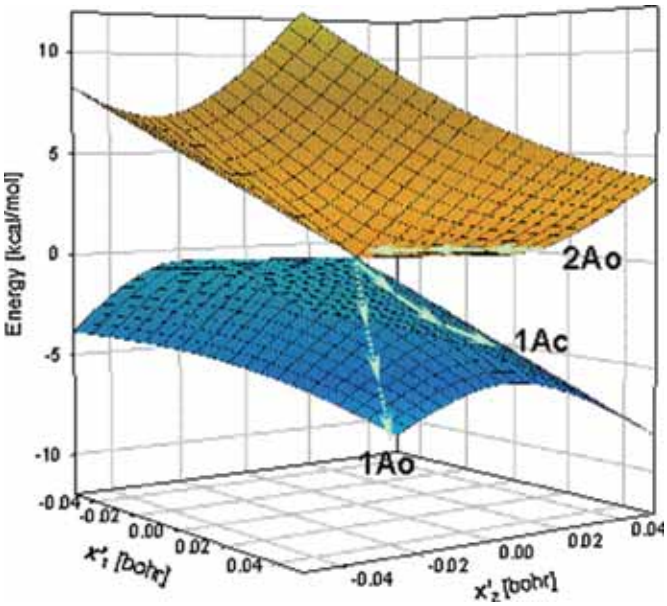
計算機という特殊な機械がこのあと何処まで進展するのか誰にも予想できないように、計算科学というテクノロジーが秘める可能性と展望は膨大にして多岐にわたり、予想するのは難しい。その全容を述べるのは筆者の任ではない。本稿の趣旨に沿って筆者が自ら手掛けた具体例を示すことにしよう [7]。それは計算科学を駆使して分子メモリーを設計したという実例である。下記は光刺激により分子構造（したがってそれに付随する分子の特性、色や極性など）が変化するジアリールエテンという有機分子である。



1o: R_1=CN, R_2=H
2o: R_1=CH_3, R_2=H
3o: R_1=OCH_3, R_2=H

1c: R_1=CN, R_2=H
2c: R_1=CH_3, R_2=H
3c: R_1=OCH_3, R_2=H

紫外 (UV) 光により左の分子が右の分子に変化し、また可視 (Vis) 光により右の分子が左に変形する。このように一分子が一ビットの情報記憶を担えば、究極の分子メモリーが実現される。筆者らはその実現を目指して分子設計に携わった [7]。分子メモリーが実現するには、熱安定性、耐久性、レーザー光への感受性など、工業化のための幾つもの必要条件を満たさねばならない。そのなかで量子収率の最適化という課題は実験科学のみでは到達困難な課題であった。これは、フォトン刺激に対して最適の反応収率を与える分子構造を求めよという設問である。下に示すのは分子（$3N-6$ 次元の自由度を持つ、N は原子数）の多次元ポテンシャル面を 3 次元に簡略して示したものである。結論から言えば、円錐交差というポテンシャル面上の特異点を設計することにより光化学反応の量子収率をデザインすることができる。これは励起状態の量子化学計算無くしては到達することができない。



光応答分子のポテンシャル曲面

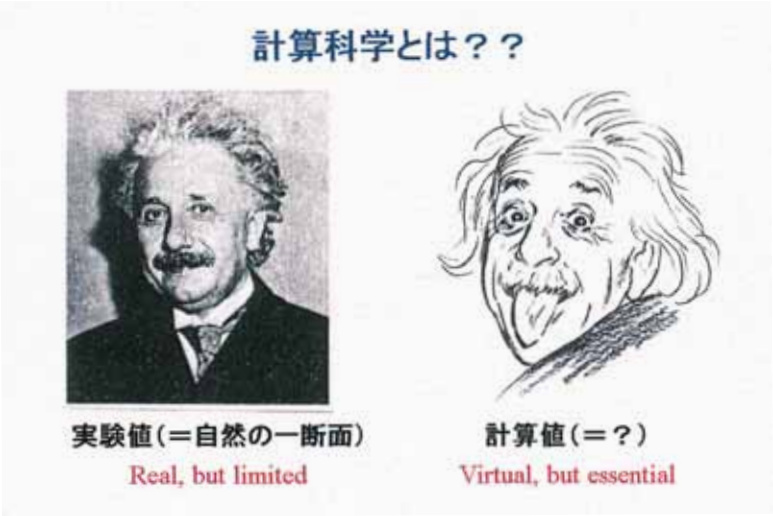
光励起した分子の置かれた状態を示すポテンシャル面が上図黄色の曲面であり、分子の基底状態に対応するのが青色の下の面である。この二つの面が接しているところで状態の遷移が起こり、この遷移の頻度が量子収率を決める。半古典量子ダイナミクス計算を行えばその予測ができる。筆者らはジアリールエテンという分子に即してそれを示した [7]。

これを実験的手法のみで行うのはおそらく不可能である。計算科学とは、そのような指針を示すための新しい科学である。それはしかし、一般に誤解されているように、実験事実そのものを代替することとは、わけが違う。実験、すなわち自然は豊かにして無限であり、けして抽象的な計算で代替することはできない。では計算科学とはいかなるものであろうか。本稿の最後にそれを要約しよう。

6　計算科学は実験を代替するものでは無い

これまで人類が造ってきたあらゆる測定機器は人間の五感を延長したものである。顕微鏡は視覚を、高感度マイクは聴覚を、AFM は触覚を延長した。脳を延長したもの、それがコンピュータであろう。脳を単純に感覚器官と言えないように、コンピュータも測定機器であるだけではない。脳という舞台を駆け巡っている思考や想念の実体が何であるかという明言は筆者には荷が重いが、計算機を舞台に駆け巡るものが計算科学である。

シミュレーション計算科学の効用の第一は、実験の数を減らすことである。それ故に、世上に跋扈する大きな誤解は、「シミュレーションが実験そのものを代替する」という誤った認識である。計算によって得られる結果は断じて実験を代替するものではない。下図に端的に示したように、計算科学シミュレーションは時として実像より実像らしい（？）質を取り出すことができる。これが計算科学の真の役割である。結果として実験の数そのものを減らすことができる所以である。



物理、化学、生物のサイエンスとテクノロジーに関する限り、実験で実証されないものは真実と認められない。真実に迫って新たな物質やデバイスを設計しようとするなら、最低限度の実験は、必ず行わなければならない。シミュレーション計算科学が参加することにより、実験では得られない知見（上記の右図、本質と喩えて良いかもしれない）を手にすることができる。これが計算科学の神髄である。その計算科学は数学に立脚している。

参考文献

[1] 穂坂衛，佐多登志夫「統合化 CAD/CAM システム」（オーム社）
[2] 平尾公彦，武次徹也「すぐできる量子化学計算ビギナーズマニュアル」（講談社サイエンティフィック）
[3] 笠井秀明，吉田博，赤井久純「計算機マテリアルデザイン入門」（大阪大学出版会）

[4] 長岡正隆「すぐできる分子シミュレーションビギナーズマニュアル」(講談社サイエンティフィック)
[5] 岡崎進「コンピュータ・シミュレーションの基礎」(化学同人)
[6] R. H. Landau, M. J. P. Mejia,「計算物理学」(上) 基礎編、(下) 応用編、小柳義夫・監訳、狩野覚、春日隆、善甫康成・訳 (朝倉書店)
[7] S. Nakamura, T. Kobayashi, A. Takata, K. Uchida, Y. Asano, A. Murakami, A. Goldberg, D. Guillaumont, S. Yokojima, S. Kobatake, M. Irie, J. Phys. Org. Chem. 2007, (20) 821–829

物質科学における第一原理計算の数理モデル

小林　一

ソニー株式会社　先端マテリアル研究所

1　はじめに

様々な物質の多様な性質は電子状態に支配されており、それらは量子力学で記述することができる。即ち、多原子系のシュレディンガー方程式を解いてやれば、全エネルギー、エネルギー準位、電子密度、静電ポテンシャル、双極子モーメント、振動数、弾性率など、非相対論的な領域のあらゆる物性がわかる。時間に依存しない多原子系のシュレディンガー方程式は以下の通りである。

$$H\Psi = E\Psi \tag{1.1}$$

$$H = \sum_{A}^{N_n}\left(-\frac{\hbar^2}{2M_A}\nabla_A^2\right) + \sum_{i}^{n}\left(-\frac{\hbar^2}{2m}\nabla_i^2\right) - \sum_{i}^{n}\sum_{A}^{N_n}\frac{Z_A e^2}{r_{iA}} + \sum_{i<j}^{n}\frac{e^2}{r_{ij}} + \sum_{A<B}^{N_n}\frac{Z_A Z_B e^2}{R_{AB}} \tag{1.2}$$

N_n は原子核の数、n は電子の数、M_A、Z_A はそれぞれ A 番目の原子核の質量、電荷、R_{AB} は原子核 A と原子核 B 間の距離、m は電子の質量、r_{iA} は i 番目の電子と A 番目の原子核間の距離、r_{ij} は i 番目と j 番目の電子間の距離である。右辺の各項は順に、原子核の運動エネルギー、電子の運動エネルギー、原子核と電子のクーロンエネルギー、電子と電子のクーロンエネルギー、原子核と原子核のクーロンエネルギーである。この基本方程式は量子力学の完成直後の 1920 年代に得られたが、実際に解けるのは水素原子等に限られる。3 体以上は解析的に解けない上に、多体系では計算量が膨大になり数値計算でも困難になるためである。これについてディラックは次のように述べている [1]。

> 「物理の大部分と全ての化学の数学的理論に必要な基本的な物理法則はこのように完全にわかっている。唯一の困難は、これらの法則を厳密に適用すると複雑すぎて解くことができない方程式に行きつくことである。」
>
> “The underlying physical laws necessary for the mathematical theory of a large part of physics and the whole chemistry are thus completely known, and the difficulty is only that the exact application of these laws leads to equations much too complicated to be soluble.”

そこで近似が必要となる。“第一原理計算”とは経験的パラメータを使わないという意味であって、近似は使う。ここで、できるだけ精度を落とさずに計算量を減らせる様々な数理モデルが必要となる [2–4]。

2　第一原理計算の数理モデル

2.1　ボルン・オッペンハイマー近似

原子核は電子に比べるとはるかに重いので、速度は非常に遅い。そこで、原子核は静止しているとみなす。これをボルン・オッペンハイマー近似と呼ぶ。すると、(1.2) の第 1 項は無視でき、第 5 項は定数となる。従って、残りの電子に関係する項を分離することができ、電子に関するシュレディンガー方程式を以下のように表すことができる。

$$H_e \Psi_e = E_e \Psi_e \tag{2.1}$$

$$H_e = \sum_i^n \left(-\frac{\hbar^2}{2m} \nabla_i^2 \right) - \sum_i^n \sum_A^{N_n} \frac{Z_A e^2}{r_{iA}} + \sum_{i<j}^n \frac{e^2}{r_{ij}} \tag{2.2}$$

2.2　分子軌道法

n 個の電子の波動関数について考えるために、まず、1 電子のハミルトニアン h_i を考える。1 電子波動関数 ϕ_i に対して以下の式が成り立つ。

$$h_i \phi_i = \varepsilon_i \phi_i \tag{2.3}$$

ϕ_i は 1 つの電子の座標だけを含む軌道関数で、分子軌道と呼ぶ。h_i が電子間相互作用を平均化した形で取り込んでいるとすると、n 電子系のハミルトニアンは h_i の和で表わすことができる。

$$H_e = \sum_i^n h_i \tag{2.4}$$

全波動関数 Ψ_0 を n 個の電子の軌道関数 ϕ_i の積で表すと、Ψ_0 は H_e の固有関数となる。

$$\Psi_0 = \phi_1 \phi_2 \cdots \phi_n \tag{2.5}$$

$$H_e \Psi_0 = E \Psi_0 \tag{2.6}$$

従って、Ψ_0 は Ψ_e の候補の 1 つである。Ψ_0 をハートリー積と呼ぶ。この時、全エネルギー固有値 E は 1 電子エネルギー固有値 ε_i の和となる。

$$E = \sum_i^n \varepsilon_i \tag{2.7}$$

分子軌道法では 1 電子軌道関数 ϕ_i を N 個の基底関数の重ね合わせで表現する。

$$\phi_i = \sum_{\nu=1}^N C_{\nu i} \chi_\nu \tag{2.8}$$

$C_{\nu i}$ は分子軌道係数である。基底関数として原子軌道を用いることが多く、これを LACO (Linear Combination of Atomic Orbitals) 近似と呼ぶ。原子軌道の形は良くわかっているので、その重

ね合わせで分子軌道（必ずしも分子でなくても良いが）を表す近似である。原子軌道として、ガウス型関数を使うことが多い。分子軌道は正規直交性を持つ。

$$\int \phi_i^* \phi_j \, dr = \delta_{ij} \tag{2.9}$$

これで n 電子系の問題は1電子のシュレディンガー方程式を解く問題になった。ここでは平均場の仮定を使っている。この近似の影響については後述する。

2.3 パウリの排他原理

パウリの排他原理によれば、2つの電子の交換に対して波動関数は反対称でなければならない。(2.5) のハートリー積はその条件を満たしていないので、次のスレーター行列式を用いる。

$$\Psi = \frac{1}{\sqrt{n!}} \begin{vmatrix} \phi_1(1) & \phi_2(1) & \cdots & \phi_n(1) \\ \phi_1(2) & \phi_2(2) & \cdots & \phi_n(2) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_1(n) & \phi_2(n) & \cdots & \phi_n(n) \end{vmatrix} \tag{2.10}$$

スレーター行列式 Ψ はハートリー積 Ψ_0 と反対称演算子 $\widehat{A}$ を使って次のように書ける。

$$\Psi = \sqrt{n!}\, \widehat{A} \Psi_0 \tag{2.11}$$

$$\widehat{A} = \frac{1}{n!} \sum_{p_n}^{n!} (-1)^{p_n} \widehat{P}_n \tag{2.12}$$

$\widehat{P}_n$ は置換演算子で、p_n は置換の回数である。上の Ψ は正規直交化されている。

$$\int \Psi^* \Psi \, dr = 1 \tag{2.13}$$

スレーター行列式をこのまま使うのは大変なので、便利な関係式を導出しておく。2つの座標の交換に対して対称な演算子 $\widehat{S}$ の期待値について考える。

$$\int \Psi^* \widehat{S} \Psi \, dr = n! \int \widehat{A} \Psi_0^* \widehat{S} \widehat{A} \Psi_0 \, dr \tag{2.14}$$

$\widehat{A}$ はエルミートなので、

$$\int \Psi^* \widehat{S} \Psi \, dr = n! \int \Psi_0^* \widehat{A} \widehat{S} \widehat{A} \Psi_0 \, dr \tag{2.15}$$

$\widehat{S}$ は対称なので $\widehat{A}\widehat{S} = \widehat{S}$。従って、

$$\int \Psi^* \widehat{S} \Psi \, dr = n! \int \Psi_0^* \widehat{S} \widehat{A} \Psi_0 \, dr$$

$$\therefore \quad \int \Psi^* \widehat{S} \Psi \, dr = \sum_{p_n}^{n!} (-1)^{p_n} \int \Psi_0^* \widehat{S} \widehat{P}_n \Psi_0 \, dr \tag{2.16}$$

これで、スレーター行列式で行うべき物理量の計算をハートリー積で行うことができる。

2.4 ハートリー・フォック法

(2.2) を次のように 1 電子部分と 2 電子部分に分けて書く。

$$H_e = \sum_i^n h_i + \sum_{i<j}^n g_{ij} \tag{2.17}$$

$$h_i = -\frac{\hbar^2 \nabla_i^2}{2m} - \sum_A^{N_n} \frac{Z_A e^2}{r_{iA}} \tag{2.18}$$

$$g_{ij} = \frac{e^2}{r_{ij}} \tag{2.19}$$

エネルギー期待値は、

$$\begin{aligned} E_e &= \int \Psi^* H \Psi \, dr \\ &= \sum_i^n \int \Psi^* h_i \Psi \, dr + \sum_{i<j} \int \Psi^* g_{ij} \Psi \, dr \end{aligned} \tag{2.20}$$

(2.16) を使って変形すると、

$$E_e = \sum_i^n \sum_{p_n}^{n!} (-1)^{p_n} \int \Psi_0^* h_i \widehat{P}_n \Psi_0 \, dr + \sum_{i<j}^n \sum_{p_n}^{n!} (-1)^{p_n} \int \Psi_0^* g_{ij} \widehat{P}_n \Psi_0 \, dr \tag{2.21}$$

軌道の直交性から、第 1 項が 0 でないのは $\widehat{P}_n$ が恒等置換のときのみである。

$$(2.21) \text{ の第 1 項} = \sum_i^n \int \phi_i^* h_i \phi_i \, dr \tag{2.22}$$

第 2 項が 0 でないのは $\widehat{P}_n$ が恒等置換のときと、i と j を入れ替えたときである。

$$(2.21) \text{ の第 2 項} = \sum_{i<j}^n \iint \phi_i^* \phi_j^* g_{ij} \phi_i \phi_j \, dr_1 \, dr_2 - \sum_{i<j}^n \iint \phi_i^* \phi_j^* g_{ij} \phi_j \phi_i \, dr_1 \, dr_2 \tag{2.23}$$

$$= \frac{1}{2} \left(\sum_{i,j}^n \iint \phi_i^* \phi_j^* g_{ij} \phi_i \phi_j \, dr_1 \, dr_2 - \sum_{i,j}^n \iint \phi_i^* \phi_j^* g_{ij} \phi_j \phi_i \, dr_1 \, dr_2 \right) \tag{2.24}$$

従って、

$$E_e = \sum_i^n h_{ii} + \frac{1}{2} \sum_{i,j}^n (J_{ij} - K_{ij}) \tag{2.25}$$

ここで、

$$h_{ii} = \int \phi_i(1)^* h_1 \phi_i(1) \, dr_1 \tag{2.26}$$

$$J_{ij} = \iint \phi_i^*(1) \phi_j^*(2) g_{12} \phi_i(1) \phi_j(2) \, dr_1 \, dr_2 \qquad \text{クーロン積分} \tag{2.27}$$

$$K_{ij} = \iint \phi_i^*(1) \phi_j^*(2) g_{12} \phi_j(1) \phi_i(2) \, dr_1 \, dr_2 \qquad \text{交換積分} \tag{2.28}$$

である。電子の区別はつかないので、h_{ii} は電子 1 の座標、J_{ij}、K_{ij} は電子 1 と電子 2 の座標で表すのが慣例となっている。

変分原理から、(2.25) の E_e を最小とする Ψ が現実の物理系が取りうる解である。これは即ち、$\int \phi_i^* \phi_j \, dr = \delta_{ij}$ の条件のもとで E_e を最小とする ϕ_i のセットを見つけることであり、それに対応する (2.8) の $C_{\nu i}$ のセットを見つけるという問題になる。ラグランジュの未定乗数法を使って $C_{\nu i}$ の満たすべき条件を求めると以下のようになる。

$$\sum_{\nu=1}^{N} (F_{\mu\nu} - \varepsilon_i S_{\mu\nu}) C_{\nu i} = 0 \tag{2.29}$$

ここで、

$$F_{\mu\nu} = h_{\mu\nu} + \sum_{\lambda,\sigma}^{N} P_{\lambda\sigma} \{2(\mu\nu|\lambda\sigma) - (\mu\sigma|\lambda\nu)\} \qquad \text{フォック行列} \tag{2.30}$$

$$h_{\mu\nu} = \int \chi_\mu^*(1) h_1 \chi_\nu(1) \, dr_1 \qquad 1 \text{ 電子積分} \tag{2.31}$$

$$(\mu\nu|\lambda\sigma) = \iint \chi_\mu^*(1) \chi_\nu(1) g_{12} \chi_\lambda^*(2) \chi_\sigma(2) \, dr_1 \, dr_2 \qquad 2 \text{ 電子積分} \tag{2.32}$$

$$P_{\lambda\sigma} = \sum_{i}^{n/2} C_{\lambda i}^* C_{\sigma i} \qquad \text{密度行列} \tag{2.33}$$

$$S_{\mu\nu} = \int \chi_\mu^*(1) \chi_\nu(1) \, dr_1 \qquad \text{重なり積分} \tag{2.34}$$

である。(2.29) をハートリー・フォック・ローターン方程式と呼び、行列方程式であらわすこともできる。

$$\mathbf{FC} = \mathbf{SC}\boldsymbol{\varepsilon} \tag{2.35}$$

これで (1.1) の多原子系のシュレディンガー方程式を解く問題は (2.35) のハートリー・フォック・ローターン方程式を解く問題となった。この方法をハートリー・フォック法と呼ぶ。$\mathbf{F}$ の中に $\mathbf{P}$ があり $\mathbf{P}$ の中に $\mathbf{C}$ があるので、この方程式は非線形である。$\mathbf{C}$ は軌道関数を多項式で表した時の展開係数なので、非線形方程式の多項式最適化問題である。

2.5 方程式を解く手順

非線形方程式なので、通常 SCF（self consistent field：自己無撞着場）の手続きで解く。一般に原子軌道は直交していないので、$\mathbf{S} \neq \mathbf{I}$ であり、(2.35) は一般化固有値問題である。実際にコンピュータで計算する際には、高速化のため $\mathbf{S}$ を正規直交化して通常の固有値問題にしてから解く。$\mathbf{S}$ はエルミート行列なので、以下のように $\mathbf{S}$ を正規直交化するユニタリー行列 $\mathbf{U}$ が存在する。

$$\mathbf{U}^\dagger \mathbf{S} \mathbf{U} = \mathbf{I} \tag{2.36}$$

$\mathbf{U}$ を使って、

$$\mathbf{F}' = \mathbf{U}^{\dagger}\mathbf{F}\mathbf{U} \tag{2.37}$$

$$\mathbf{C}' = \mathbf{U}^{-1}\mathbf{C} \tag{2.38}$$

とすると、(2.35) は

$$\mathbf{F}'\mathbf{C}' = \mathbf{C}'\boldsymbol{\varepsilon} \tag{2.39}$$

となり、通常の固有値問題となる。$\mathbf{F}'$ を対角化して $\mathbf{C}'$ が得られれば、

$$\mathbf{C} = \mathbf{U}\mathbf{C}' \tag{2.40}$$

で $\mathbf{C}$ が求まる。Fig. 1 に SCF 計算のフローチャートを示す。

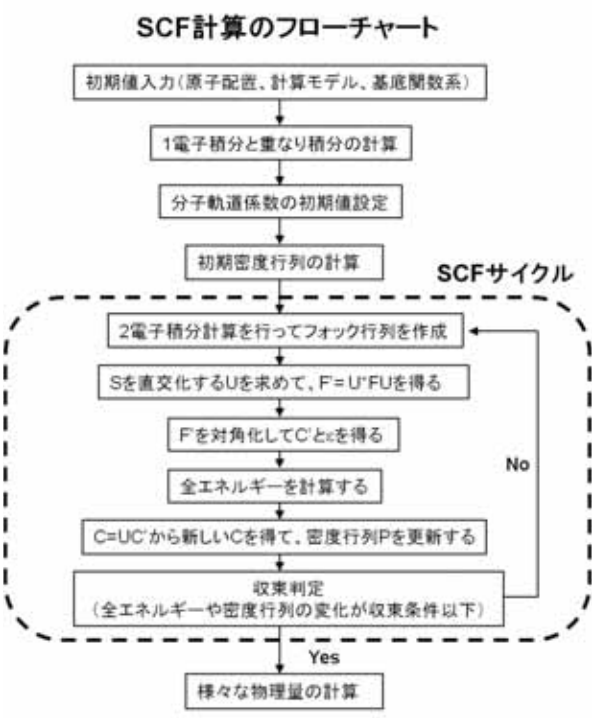


Fig. 1

2.6 占有軌道と非占有軌道

(2.8) で示したように N 個の基底関数を用いてハートリー・フォック・ローターン方程式を解くと、N 個の分子軌道関数とエネルギー準位が得られる。スピンを考慮すると 1 つの軌道に 2 個の電子が入るので、基底状態ではエネルギーの低い軌道から 2 つずつ電子が埋まり、n 個の電子がある場合、$n/2$ 個の分子軌道が埋まる（占有軌道）。残りの $N - n/2$ 個の軌道を非占有軌道と呼ぶ (Fig. 2)。非占有軌道は、熱や光による励起状態や化学反応を考える際に重要な物理的意味を持つ。また、電子相関を考慮する際にも大きな役割を果たす（後述）。

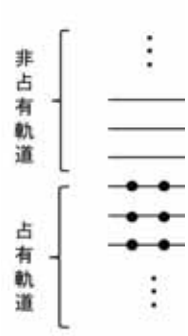


Fig. 2

2.7　計算上の課題

以上、第一原理計算の数理モデルの基本であるハートリー・フォック法について概要を説明した。後はコンピュータを駆使して Fig. 1 のフローチャートに従って計算を行えばよいわけだが、実際に計算を行うといろいろな問題に直面する。Fig. 3 の①の様に、できるだけ短い時間で全エネルギーが収束するのが望ましいが、系が大きくなると以下の様な状況がしばしば起こる。

(A) 全エネルギーが収束せず振動する

Fig. 3 の②のように、全エネルギーが収束せず、計算がいつまでも終了しないケースがある。この様な場合、基底関数系の選択や構造（原子配置）が重要となる。また、SCF 計算の解法によっても大きく変わる。代表的な解法に、最急降下法、共役勾配法、DM 法 [5]、QC 法 [6]、DIIS 法 [7]、EDIIS 法 [8] などあるが、それぞれ一長一短があり、収束性が悪い場合、系に対して適切な方法を選ぶ必要がある。第一原理計算は非経験的手法だが、実際に SCF 計算をする際は経験に基づく“職人芸的”なノウハウがしばしば必要となる。“誰でも使える”ツールにするには、系に依存しない解法、もしくは与えられた系に対して適切な方法を自動的に選択するようなアルゴリズムが求められる。

(B) 収束はするが 1 回の SCF 計算に時間がかかる

Fig. 3 の③は、全エネルギーは収束するが、1 回の SCF 計算に時間がかかる例である。1 回の SCF サイクル中では 2 電子積分の計算に最も時間がかかるため、例えば、並列化アルゴリズム [9] などを用いて高速化を図る。また、大きな系では 2 電子積分のデータ量が膨大になるため、積分データをメモリに置くかハードディスクに置くか、保存しないで必要な時に毎回計算するといった選択肢があり、計算時間に影響を与える。計算する系の規模と CPU・メモリ・ハードディスク・I/O の性能を考慮して最適化する必要があり、これらは、ハードウェアに密接に関連した計算機科学の重要なテーマである。

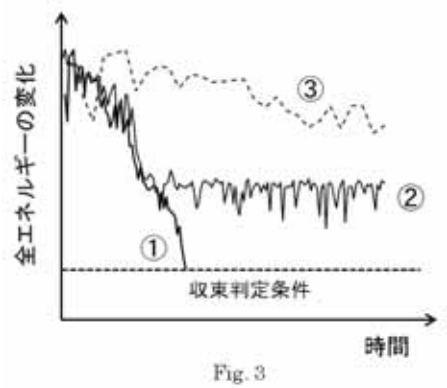


Fig. 3

2.8 電子相関

ハートリー・フォック法は第一原理計算の基本である。しかし、1 個の電子が他の全ての電子が作るポテンシャルの中を運動するという平均場近似を用いているので、電子同士の散乱や、反発して広がるといった電子-電子相互作用（電子相関）は含まれていない。従って、電子相関の強い系（電子が局在化している系）では精度が落ちる。このような場合、電子相関を考慮したポスト・ハートリー・フォック法と呼ばれる方法が使われる。主なものに配置間相互作用法（CI 法)、結合クラスター法（CC 法)、摂動法があり、いずれの方法も、電子相関による電子の再配置の状態を表すために、先に述べた非占有軌道を利用する。基底状態 Φ_0 にはハートリー・フォック法のスレーター行列式を使い、これに非占有軌道に電子を励起させた状態を加えて、電子配置の空間自由度を大きくする (Fig. 4)。

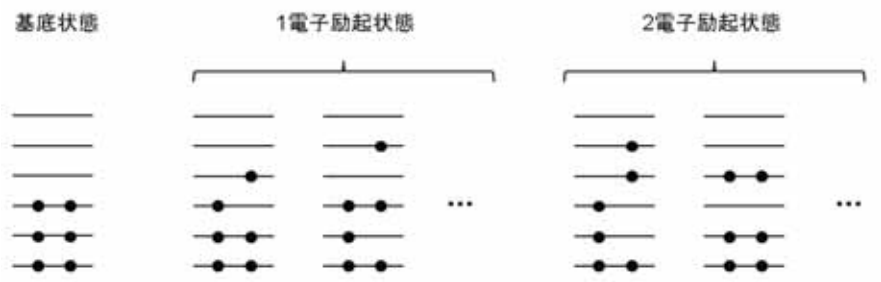


Fig. 4

CI 法では、励起状態を線形に重ね合わせた波動関数を考える。基底状態 Φ_0 に作用して i 個の電子励起状態を得る励起演算子を $\widehat{T}_i$ とすると、以下の式で表される。

$$\Psi^{\mathrm{CI}} = \Phi_0 + \left(\sum_i C_i^{\mathrm{CI}} \widehat{T}_i \right) \Phi_0 \tag{2.41}$$

励起状態にもスレーター行列式を用いることで、Ψ^{CI} もパウリの排他律を満足する。展開係数 C_i^{CI} を変分法で求めることで、電子相関を含んだ波動関数を得ることができる。n 個の電子全てについてあらゆる励起状態の組み合わせを考えれば、厳密な電子相関が得られる (full CI)。

CC 法では、以下の波動関数を考える。

$$\Psi^{\mathrm{CC}} = \exp\left(\sum_i C_i^{\mathrm{CC}} \widehat{T}_i\right)\Phi_0 \tag{2.42}$$

これをテーラー展開すると、

$$\Psi^{\mathrm{CC}} = \Phi_0 + \left\{\left(\sum_i C_i^{\mathrm{CC}} \widehat{T}_i\right) + \frac{1}{2}\left(\sum_i C_i^{\mathrm{CC}} \widehat{T}_i\right)^2 + \cdots\right\}\Phi_0 \tag{2.43}$$

CI 法との違いは $\frac{1}{2}\left(\sum_i C_i^{\mathrm{CC}} \widehat{T}_i\right)^2 + \cdots$ の項である。CC 法は展開係数の数は CI と同じだが、このように高次励起の電子相関も含んでいるので、より高い精度が得られる。現実には full CI や full CC の計算は大変なので 2〜3 電子励起までを考えることが多い。

摂動法では、既知の主要部分の結果に対して弱い相互作用の効果を逐次的に求めていく。

$$H = H_0 + V \tag{2.44}$$

H_0 が主要部分の無摂動項、V が弱い相互作用による摂動項である。H_0 については、波動関数とエネルギー固有値が得られているとする。

$$H_0\Psi_i^{(0)} = E_i^{(0)}\Psi_i^{(0)} \tag{2.45}$$

( ) 内は摂動の次数を表す。エネルギーが縮退していないとすると、真の波動関数 Ψ_i とエネルギー固有値 E_i は以下のようになる。

$$H\Psi_i = E_i\Psi_i \tag{2.46}$$

$$\Psi_i = \Psi_i^{(0)} + \Psi_i^{(1)} + \Psi_i^{(2)} + \cdots \tag{2.47}$$

$$= \Psi_i^{(0)} + \sum_{n\neq i} \frac{\int \Psi_n^{(0)} V \Psi_i^{(0)}\, dr}{E_i^{(0)} - E_n^{(0)}}\Psi_n^{(0)} + \cdots \tag{2.48}$$

$$E_i = E_i^{(0)} + E_i^{(1)} + E_i^{(2)} + \cdots \tag{2.49}$$

$$= E_i^{(0)} + \int \Psi_i^{(0)} V \Psi_i^{(0)}\, dr + \sum_{n\neq i} \frac{\left|\int \Psi_i^{(0)} V \Psi_n^{(0)}\, dr\right|^2}{E_i^{(0)} - E_n^{(0)}} + \cdots \tag{2.50}$$

摂動法は、V が H_0 に比べて十分に小さい場合に有効である。MP 法（Møller-Plesset 法）では、H_0 に基底状態（ハートリー・フォック配置）を用いる。通常、ハートリー・フォックエネルギーが系全体の 99%以上を占め電子相関のエネルギーは 1%以下なので、これは良い近似である（今はそのわずかな電子相関が重要になる場合を論じているわけだが）。手順としては、まずハートリー・フォック法で通常の SCF 計算を行ってから 1 次、2 次の摂動項を逐次計算し

ていく。この部分はSCF計算ではないので、収束性の問題はない。摂動法も次数を上げていけば基本的に精度は上がるが、例えば、3次の方が2次よりも精度が落ちる場合があるので注意が必要である。

これらのポスト・ハートリー・フォック法はいずれも、基底状態のみを計算するハートリー・フォック法に比べると膨大な計算時間がかかるので、ここでもさらなる高速化が必要とされている。

ポスト・ハートリー・フォック法と並んで良く使われる方法に、密度汎関数法がある。これは、波動関数を使わずに電子密度を使った平均場ポテンシャルで電子相関を考慮する方法である。ハートリー・フォック法と同程度の計算量で、より高い精度を得ることができる。

2.9 精度と計算時間

第一原理計算における計算精度は、基底関数系の大きさと計算モデルのレベルの2つで決まる。大きな基底関数系を使って、3電子励起まで考えたCC法を使うと、驚くほど高い精度が得られる（例えば、フッ化水素のエネルギーは0.02 eVで実験と一致する）。しかし、精度を上げるほど計算コストは増大するので、両者はトレードオフの関係にある。必要な精度を満たす範囲で計算コストを下げるように、計算モデルや基底関数系を選択することが重要になる（上の3電子励起のCC法だとスーパーコンピュータを使ってもせいぜい数十原子の計算が限界である）。

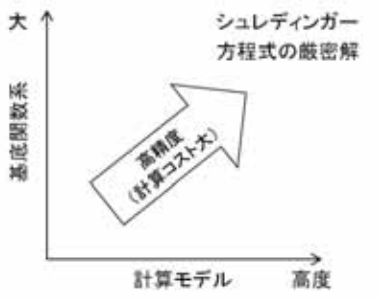


Fig. 5

2.10 構造最適化

計算を始める際には、まず系の構造が入力として必要である。実験的に精度の高い構造がわかっていればよいが、正確な構造がわかっていない場合がある（むしろその方が多い）。その場合、計算で構造最適化を行うことができる。

(2.2)で無視した(1.2)式の第5項（原子核と原子核のクーロンエネルギー）を考慮してSCF計算を行う。収束後に、ポテンシャルエネルギーを空間微分して各原子核に働く力を求めて、それに応じて原子核を変位させる。得られた新しい構造について新たにSFC計算を行う。これを繰り返して収束条件（例えば、各原子核に働く力の平均の変化が設定値以下）を満たすまで繰り返す。このようにして、より安定な（ポテンシャルエネルギーの低い）構造を探索す

る。即ち、N 個の原子核が作る $3N$ 次元空間のポテンシャルエネルギー面の最小点を求める問題である。極小解に収束して誤った構造を得ることのないように、広い範囲を効率的に探索して最小解を求めることが要求される。SCF 計算と構造探索計算の 2 重ループになるので、より計算コストがかかる。効率的に探索するために、まず簡易な計算モデルでラフに探索してから、順次高度な計算モデルで探索を進めていくのが一般的である。また、単純に力に比例させて変位させるのではなく、Berny 法 [10]、GDIIS 法 [11]、eigenvalue-following 法 [12] といった様々なアルゴリズムがあるが、さらに高速で信頼性の高いアルゴリズムが望まれている。

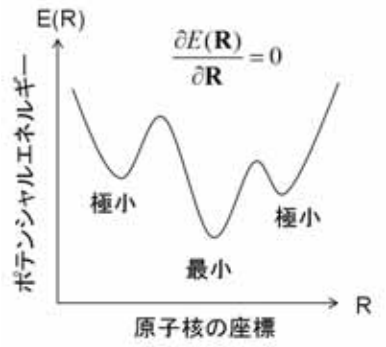


Fig. 6

3　おわりに

第一原理計算の基本方程式は厳密に解くことが難しいため、様々な近似が使われる。実際に計算を行う際には、これらの近似が最終的な計算精度にどの程度影響しているかを把握することが重要である。近い系の実験値があれば、その系の計算をまず行って精度を確認するのが良い。実験値がない場合でも、幸い第一原理計算では Fig. 5 に示したように、基底関数系を大きくして計算モデルも高度にすれば確実に精度が上がるので、1 度だけ時間をかけて（気合いを入れて）高精度計算をすれば精度の確認ができる。

繰り返し述べたように、現在でも SCF 計算、構造最適化等で、より高速で信頼性の高い解法が求められている。第一原理計算用のソフトウェアは数多く存在するが、バージョンアップのたびに解法を改良して高速化を図り、それを売りにしている。また、大規模系の計算にはスーパーコンピュータの活用が不可欠である。そのためには大規模並列化のための優れたアルゴリズムが必要となる。京コンピュータに象徴されるように、ハードウェアの進歩は著しいが、それに比べてソフトウェアの進歩が追い付いていない感がある。仮に 1 万コア使えても、並列化効率の悪いソフトウェアだと数 100 コア程度で計算速度が飽和してしまう。これでは宝の持ち腐れである。また、並列化効率が良くても収束性の悪いアルゴリズムでは計算が終わらない。新しいアプローチによる斬新な解法（アルゴリズム）が期待されている分野である。

参考文献

[1] P. A. M. Dirac, “Quantum mechanics of many-electron systems”, Proc. Roy. Soc. A **123**, 714 (1929).

[2] 中嶋隆人著,「量子化学」, 裳華房 (2009).

[3] A. ザボ, N. S. オストランド著, 大野公男, 阪井健男, 望月祐志訳,「新しい量子化学」, 東京大学出版会 (1987).

[4] J. B. Foresman, Æ. Frisch, 田崎健三訳,「電子構造論による化学の探求」, ガウシアン社 (1998).

[5] R. Seeger and J. A. Pople, “Self-consistent molecular orbital methods. XVI. Numerically stable direct energy minimization procedures for solution of Hartree-Fock equations”, J. Chem. Phys. **65**, 265 (1976).

[6] G. B. Bacskay, “A quadratically convergent Hartee-Fock (QC-SCF) method. Application to closed shell systems”, Chem. Phys. **61**, 385 (1981).

[7] P. Pulay, “Improved SCF convergence acceleration”, J. Comp. Chem. **3**, 556 (1982).

[8] K. N. Kudin and G. E. Scuseria, “A black-box self-consistent field convergence algorithm: One step closer”, J. Chem. Phys. **116**, 8255 (2002).

[9] S. Obara and A. Saika, “Efficient recursive computation of molecular integrals over Cartesian Gaussian function”, J. Chem. Phys. **84**, 3963 (1986).

[10] H. B. Schlegel, “Optimization of equilibrium geometries and transition structures”, J. Comp. Chem. **3**, 214 (1982).

[11] Ö. Farkas and H. B. Schlegel, “Methods for optimizing large molecules. II. Quadratic search”, J. Chem Phys. **111**, 10806 (1999).

[12] C. J. Cerjan and W. H. Miller, “On finding transition states”, J. Chem. Phys. **75**, 2800 (1981).

ものづくりと数学—Symbolic Approaches

益岡　竜介[1,2]　　穴井　宏和[1,3]

[1] (株)富士通研究所，[2] 国際公共政策研究センター
[3] 九州大学マス・フォア・インダストリ研究所

1　はじめに

本稿ではものづくりと数学、その中でも、ものづくりへの symbolic approaches の適用を見ていく。

ハードウェアでもソフトウェアでも、それらのものづくりにおいて数値解析や最適化アルゴリズムをはじめとして数学はいろいろな場面で使われている。ものづくりの各過程にあわせて数学を適用する課題を切り出すと次のようになろう。

(1) モデル化：どのように対象のシステムをモデル化すべきか？
(2) 解析：どのような解析をそのシステムで行うべきか？
(3) 設計：
- 問題をどのように定式化し、何を設計目的とするか？
- どのように設計を行う（設計問題を解く）か？

(4) 検証：
- システムの設計は正しいか、不具合はないか？
- システムが望ましくない状態に陥らないか？

例えばこれを本稿の第 2 章で取り上げている HDD（ハードディスクドライブ）のヘッドの場合に当てはめると以下のようになる。

(1) モデル化：制御をするための機構の数理モデルを作る。具体的にはアクチュエータにどんな入力を入れたらどの位置に行くか（出力）の入出力モデルを作る。
(2) 解析：コントローラでの動作をシミュレーションし、解析を行う。具体的にはモデルでパラメータを変え、どのように動くかのシミュレーションを行う。
(3) 設計：ヘッドの浮上量や角度などのあるべき状態を最適値とする目的関数を作り、その目的関数を最適化する設計パラメータを決定する。
(4) 検証：実際に (1), (2) を使い、(3) で設計したものが条件を満たすか（与えられた仕様内に入っているか）どうかを検証する。

ものづくりの中でも、本稿では特に symbolic approaches の適用を見ていく。ここでいう symbolic approaches とは変数を持った数式を数式のまま処理して解を導くものである。それはどういうもので、数値解析や最適化アルゴリズムなどの numeric approaches とどう違うのか？

例えば設計の都合上、どんな x の値に対しても $x^2+bx+c>0$ となっていないといけないとしよう。例えば x はアームが動く範囲、HDD ヘッドの浮上量が x^2+bx+a と表され、その

浮上量が d より大きい必要があるとすると、その条件は $c = a - d$ とすれば上記と同値になる。そのとき適切な設計パラメータ b, c を決定するという問題を考えよう。Numeric approaches であれば、b, c, x に具体的な数字をランダムに入れたり、漸次的に変更していったりして適切な値を見つけるというものになる。それはそれで式の形や要素に依存しないで解けるのでいいのであるが、一方で（悪い言い方をすると）行き当たりばったりで、また得られた解がどの程度いいものなのかを判断することは難しい。

Symbolic approaches では b と c の範囲は $b^2 - 4c < 0$ として厳密に与えられる。この範囲は二次元の座標系で簡単にプロットすることができ（二次関数で区切られた一つの領域となる）、その中から b と c を選べばよい。 そのとき重要なのは設計パラメータの解 (b, c) の空間の見通しが非常によくなることである。これは設計パラメータを与えても必ず誤差がでてしまうものづくりにとって非常に重要なことである。b, c を領域内の点だが（二次関数で与えられる）境界に近くにとってしまうと、製造誤差で仕様を満たさなくなる可能性が高い。Numeric approaches では得られた解が解集合全体の中でどのようなところにあるのか分からないため、そのような製造誤差への対処が難しい。 一方 symbolic approaches だと解の領域が分かっているため、解を領域内の十分余裕がある点とし、それを設計パラメータと与えることにより、製造誤差を吸収して歩留まりを高めることができる。

あるいは Web サイトの安全性を高めるため Web サイトのプログラムが SQL Injection 攻撃の可能性がないことをテストしたいとしよう。SQL Injection 攻撃は Web サイトの入力フィールド（やアドレスバーなど）に特別な文字列を入力し、それがプログラムで処理され、Web サイトのデータベースに渡す SQL コマンド文字列に変換されたときに、データベースに意図されていない行動を起こさせる攻撃である。 例えば SQL コマンド文字列のどこかに “;SHUTDOWN;” 部分文字列を仕込めれば、データベースが意図しないときに終了する。

今まではこういった攻撃の可能性がないことを検証するためには、（numeric approaches ではないが、具体的な値を使うという意味で numeric approaches に近い手段で）人が Web サイトの入力フィールドに実際にいろいろな文字列を入れて、意図しない危険な SQL コマンド文字列が生成されないことを確かめる。 これは人でなく、コンピュータで Web サイトの入力フィールドへの文字列を生成、自動入力することにより多少効率的にはなるが、本質は変わらない。すなわち入力テキストには無限の可能性があり、その全てを試すことはできない。Hacker の人たちは非常に創造的でどんどん新しい手段を使ってくるので[1] 、事前に分かっている文字列を試すだけでは Web サイトの安全性はあまり高まらない。

Symbolic approaches では入力フィールドへの入力 s を具体的な文字列ではなく、変数のままプログラムを実行する。入力が変数のままでは条件分岐を一つに決定できないが、その条件を式に付け加え、各条件をそれぞれたどって行く。最後に SQL コマンド文字列を作るところでは、その SQL コマンド文字列が入力の変数を含む式 SQL(s) で表現される。そこで SQL(s) が “;SHUTDOWN;” を含むという式をたて、その式に解があるかどうかを決定し、もし解がある場合は具体的な解を導出する。もしその式に解がなければ、そのような攻撃ができないということができる。もし解 s_0 があれば、その s_0 を入力として与えれば、データベースが予期

[1] 例えば SQL コマンドを HEX で与え、それを SQL コマンド文字列生成の段階で通常の文字列に直す攻撃などもある。

せず終了する可能性があるので、入力に s_0 を排除するコードを付け加えればより安全な Web サイトとなる。

最初の方法では、無限にある入力の空間を有限の（それもかなり限られた）点でカバーしようとしているのに対し、symbolic approaches では、無限にある入力の空間の中から解（= 攻撃）を見つけてくる。もし解がないのなら、そのような攻撃はありえないということを言うことができる。

このように symbolic approaches は非常に強力である。ただもちろん万能ではない。まず対象をモデル化をする部分に課題がある。現実を操作可能な式に落とす際にはどうしても失われるものがある。現実は数多くの要素からなり、非常に複雑であり、完全に数式であらわせると考えるのは naive である。ハードウェアの場合であれば、全ての物理現象を式に落とし込むというのは不可能である。 またソフトウェアの場合であっても、非常に小さなソフトウェアであれば完全に解くことも不可能ではないが、現在の 10 万行、100 万行といった巨大なプログラムになると、必要な部分以外をある程度抽象化しないと、現実的に解くことはできない。

すなわちものづくりでの symbolic approaches の適用ではいかに現実を、あまり関係ない部分を抽象化あるいは省略し、symbolic approaches に乗るようにするかが肝要である。またもう一つは、より高性能なコンピュータあるいは cloud computing による分散コンピューティングを使い、symbolic approaches の適用範囲を広げることである。

以下では、第 2 章ではハードウェアである HDD ヘッドの設計を例に、第 3 章ではソフトウェアの検証を例に、具体的にいかに現実を symbolic approaches に乗せ、また symbolic approaches の適用範囲を広げて実際の問題に適用しているかを記述している。最後の第 4 章でまとめと将来への展望を記述する。

2　ハードウェア設計

さまざまな「ものづくり」における設計過程の効率化・コスト削減、さらに、設計結果の高付加価値化を実現していく上で、最適化技術の発展が 1 つの鍵である。現在、最適化技術の発展は、numeric approaches を前提とした各種アルゴリズムにより支えられている。これらの技術も普及してきたが、より実用的で重要な問題に適用しようとすると numeric approaches だけでは本質的な解決が難しいことも明らかになってきた。例えば、機械系システム設計において、機構系と制御系を同時に最適設計しようとすれば、非凸最適化問題を解くことが必要となるが、numeric approaches では大域的最適解を導くことは容易ではない。また、各種設計における最適な設計パラメータの決定は一般に、さまざまなパラメータ値に対してシミュレーションを繰り返すことが求められ、よりよい解を見通しよく求めること、複数の要求仕様を同時に満たす解を求めることは非常に手間のかかる作業となっている。

ここでは symbolic approaches を用いた最適化手法を紹介する。Symbolic approaches は不定元やパラメータなどの記号が入った式を多項式としてそのまま扱うことを特徴としており、一般には処理時間がかかり扱える問題規模に制約があるが、numeric approaches では処理が困難である課題に対して有効な方法論を提供することができる。具体的には、非線形あるいは非凸な制約問題も正確に解くことが可能となり、また、パラメータをそのまま扱うこと（パラ

メトリック最適化）が可能となる。Symbolic approaches を活用することで、設計仕様を満たす設計パラメータの値をパラメータ空間内の可能領域として正確に求めることができるため、対象となる設計問題の特性を深く理解できよりよい解（よりロバストな解など）の探索や複数仕様設計問題に対しても系統的な設計フローを提供することが可能となる。

最近では、symbolic approaches による最適化手法をさまざまな分野の設計・検証問題に適用する研究が盛んになってきた [1]。特に、不等式制約問題の代数的算法である限量記号消去 (quantifier elimination: QE) を用いてさまざまな問題を解く試みがなされており、ある程度実用的な問題へ適用できるレベルになってきている。次項では、QE とはどういうアルゴリズムか説明し、QE による最適化を導入する（QE について詳細は [1] を参照されたい）。その後で、QE による最適化手法の適用事例として HDD の形状設計の事例を紹介する。

2.1 Symbolic Approaches に基づく最適化

Symbolic approaches によるパラメトリック最適化を実現するための基本技術が QE である。QE は、多項式等式、不等式、限量記号 ($\forall$, $\exists$)、そしてブール演算（$\wedge$, $\vee$, $\Rightarrow$, $\neg$ 等）からなる一階述語論理式に対し、等価で限量記号を含まない式を導く算法である。出力される式は入力式が真であるための限量記号のない変数の可能な領域を示す。例えば、式 $\forall x(x^2+bx+c>0)$ に対し QE によって等価な式 $b^2-4c<0$ が導かれる。QE を用いて最適化問題をどのように解くか説明する。

$$\begin{aligned} &\text{目的関数：} f(x_1,\ldots,x_n) \to \text{最小} \\ &\text{制約条件：} g_1(x_1,\ldots,x_n)\,\rho_1\,0,\ \ldots,\ g_k(x_1,\ldots,x_n)\,\rho_k\,0 \end{aligned} \tag{1}$$

ここで、$\rho_i \in \{\neq, <, >, \leq, \geq\}$ である。最適化問題 (1) を QE 問題として解くには、新たな変数（ここでは k）を導入して、$k-f(x_1,\ldots,x_n)=0$ という式を作り、制約条件と合わせて以下の一階述語論理式を構成する。

$$\exists x_1 \cdots \exists x_n (k-f(x_1,\ldots,x_n)=0 \wedge \varphi(x_1,\ldots,x_n)) \tag{2}$$

ここで $\varphi(x_1,\ldots,x_n) \equiv \bigwedge_i (g_i(x_1,\ldots,x_n)\,\rho_i\,0)$ である。一階述語論理式 (2) に QE を適用すると k の満たす論理式 $\psi_1(k)$ が得られる。この式を満たすような k の値の中での最小値を求めるとそれが目的関数 f の最小値になる。得られた結果が示すのは目的関数のすべての正確な実行可能領域である。よって、大域的な最適値がもとまることになり、上限値や下限値があるかどうか不明な問題の場合にも有効である。全変数に限量記号が付いているときには、QE は入力式の真／偽を判定する。まとめると、制約問題や最適化問題の手法として QE は

- 全ての実行可能解をパラメータ空間内の領域として正確に求めることができる
- 非凸な最適化問題も正確に解くことができる
- 実行可能解が存在しない場合も正確に判定できる

という特長を持っている。QE を巧く用いることにより、さまざまな解析・設計問題から得られる制約・最適化問題をパラメトリックに正確に解くことができるようになり、設計の効率化・高度化を図るために有効である。

例　次式で与えられる最適化問題を QE で解いてみる。

$$\begin{aligned} &\text{目的関数：} 2x_1 + x_2 \to \text{最小} \\ &\text{制約条件：} 4x_1 + x_2 \le 9,\ x_1 + 2x_2 \ge 4,\ 2x_1 - 3x_2 \ge -6 \end{aligned} \tag{3}$$

この場合、次の一階述語論理式に対して QE を適用する。

$$\exists x_1 \exists x_2 (k - (2x_1 + x_2) = 0 \wedge 4x_1 + x_2 \le 9 \wedge x_1 + 2x_2 \ge 4 \wedge 2x_1 - 3x_2 \ge -6) \tag{4}$$

QE を適用すると、k の実行可能領域 $2 \le k \le 6$ が得られる。これより k すなわち目的関数 $2x_1 + x_2$ の最大値が 6 で最小値が 2 であることがわかる。

次に、以下の多目的最適化問題を考える。多目的最適化は、複数の目的関数を同時に最小化する問題である。通常考える場合には目的関数の間にトレードオフの関係があるため、目的関数の空間における実行可能領域の中で最小化可能なぎりぎりのトレードオフの境界（パレートフロント）を求めるのが目指すところである。多目的最適化についての詳しい解説は [2] を参照されたい。

$$\begin{aligned} &\text{目的関数：} f_1(x_1, x_2),\ f_2(x_1, x_2) \to \text{最小} \\ &\qquad f_1 = x_1^2 + x_2^2,\ f_2 = 5 + x_2^2 - x_1 \\ &\text{制約条件：} -5 \le x_1 \le 5,\ -5 \le x_2 \le 5. \end{aligned} \tag{5}$$

目的空間における f_1, f_2 の実行可能領域を求めるには以下の一階述語論理式を QE で解く。

$$\exists x_1 \exists x_2 (y_1 = x_1^2 + x_2^2 \wedge y_2 = 5 + x_2^2 - x_1 \wedge -5 \le x_1 \le 5 \wedge -5 \le x_2 \le 5) \tag{6}$$

その結果、次式の y_1, y_2 の実行可能領域、すなわち f_1-f_2 空間の実行可能領域（図 1 (a) のグレーの領域）を得る。

$$\begin{aligned} &(y_2 - y_1 + 25 \ge 0 \ \wedge\ y_2^2 - 60y_2 - y_1 + 925 \ge 0 \ \wedge \\ &\ y_2 \le 30 \ \wedge\ y_1 \ge 25) \vee \\ &(4y_2 - 4y_1 - 21 \le 0 \ \wedge\ y_2 \ge 30 \ \wedge\ 4y_1 \le 101) \vee \\ &(y_2 - y_1 + 15 \ge 0 \ \wedge\ y_2^2 - 60y_2 - y_1 + 925 \le 0) \vee \\ &(y_2 - y_1 + 25 \ge 0 \ \wedge\ y_2^2 - 10y_2 - y_1 + 25 \le 0) \vee \\ &(4y_2 - 4y_1 - 21 \le 0 \ \wedge\ y_2 \ge 5 \ \wedge\ y_1 \le 25 \wedge \\ &\ 4y_1 \ge 1). \end{aligned}$$

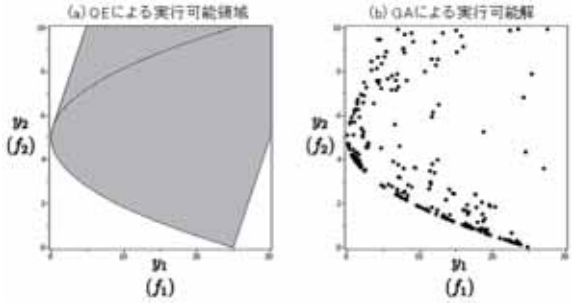


図 1：多目的最適化問題 (5) に対する目的関数の実行可能領域

この図から、正確なパレートフロントが求まっていることがわかる。同じ問題を数値的な多目的最適化手法である遺伝アルゴリズム (genetic algorithm; GA) によって解いた結果が図 1 (b) である。GA などの numeric approaches ではくり返し計算が進むにつれてパレート付近の実行可能解が増えていく方法なので実行可能領域全体を推測するのは容易ではない。

2.2　適用事例—HDD のスライダ形状設計

ものづくりへの適用例として、HDD のスライダ部分の形状（図 2）の最適設計への応用について紹介する。

スライダは、先端の磁気ヘッドで情報の読み取り・書き込みを行う役割を担っており、ディスクに近いほど読み取り・書き込みエラーが少なくなるが、一方で、ディスクに接触するとクラッシュの原因になる。そのため、スライダとディスク面を適度な距離になるように動作させることが求められる。スライダは、ディスクの回転で生じる空気の流れで浮上しており、浮上量は高度（気圧）などの環境変化によっても変化する。また、浮上時の角度も、アームの位置により空気の流れが変わることや、スライダに縦・横方向への回転が生じることなどで変化する。スライダの浮上量や姿勢は、先端にある ABS（Air Bearing Surface、図 2 の一番右）の形状を工夫することによって調整がなされている。したがって、HDD の設計では、適切なスライダの浮上量や安定な位置・姿勢を実現するための ABS の形状設計が重要になる。

図 2：HDD のスライダと ABS

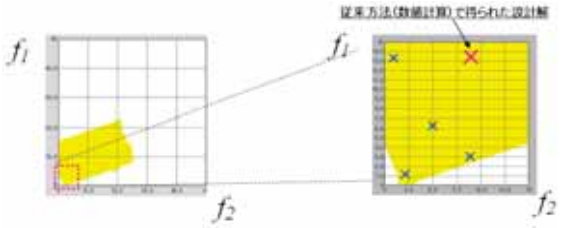


図 3：目的関数 f_1, f_2 の実行可能領域

このような ABS の最適な形状設計問題を多目的最適化問題として捉える。いくつかの高度下での浮上量や姿勢が目標の状態で安定していることを目的関数として数式で表現し、それらの複数の目的関数を最小化する多目的最適化問題として定式化し、前項で紹介した QE による多目的最適化手法を適用する。その結果、ある 2 つの目的関数 f_1, f_2 について、QE により目的関数空間での実行可能領域を求め可視化したのが図 3 である。

数値最適化の手法で得られた設計解に比べ、効率的かつ正確にパレート解を構成することが可能となり、また、数値最適化の手法で得られた設計解よりも、どちらの目的関数に重点をおいてどのぐらいまで最適化できそうかといった知見も得ることが可能になった。その結果、実際の設計工数の大幅な削減が実現できた（ある設計工程では、14 日間かかっていたところを 1 日に短縮できた）。

3　ソフトウェア検証

3.1　背景—なぜ社会にとって重要か

ソフトウェアが社会のいろいろな側面に入り込んでいる。個人が使う PC から、スマートフォン、タブレットなどではソフトウェアが大きな役割を果たしているのが明確であるが、比

較的一般から見えない部分でもソフトウェアの存在感が日に日に増している。金融システム、交通システムなどの社会を支える巨大なソフトウェアから、家電などもコンピュータチップと共にソフトウェアがコントロールしている。最近の車には200以上のコンピュータチップが入り、ソフトウェアが大きな役目を果たしている。Smart Grid（電力網を賢くする取り組み)、Smart City、Smart Homeなどが提案され、ソフトウェアがより重要となる方向は加速こそすれ、とどまることはない。

それらのソフトウェアのバグは金銭的な被害だけではなく、社会や人命にも関わる重大な帰結をもたらしうる。例えば放射線治療の装置のソフトウエアのバグで放射線を大量に浴びた少なくとも6人が亡くなったことがあった。その他にも [3] の記事はソフトウェアバグがどのようなことを引き起こしうるかを示すもので、是非一読ありたい。

そしてソフトウェアのバグは残念だがなくならないであろう。それにはいくつかの要因がある。 一つは現在のソフトウェアあるいはシステムは巨大で、複雑になり、人がその全てを把握することはできなくなってきている。巨大なシステムはまず分割して、それぞれのモジュールが「何」をするものか（仕様書等）を書くのだが、全体が見えない中、また多くの関係するモジュールの関係の中、それぞれのモジュールの「何」を間違えなく書けるかという問題がある。また通常「何」は自然言語で記述されているので、曖昧さも排除できない。そういった面からバグが入り込む余地がある。

また「何」が完璧にかけたとしても、プログラム（すなわちソフトウェア）を作るということはその「何」[2]を「どう」[3]やって実現するのかの手順を記述することである。この「何」とそれを「どう」実現するかの間にギャップが起き得てそこに間違いが入り込む可能性がある。

もちろんソフトウェアは実際に使われる前に意図したとおりに動くかどうか検証（テスト）が行われるのだが、巨大かつ複雑なソフトウェアの全ての状態を検証することは不可能である。それでもできるだけ適切な検証を行おうとするのだが、ソフトウェアが大きくなればなるほど、ソフトウェアを書くためにかかるリソースに比較してその検証を行うために必要なリソースの方が飛躍的に伸びていく。さらには現在の人手による労働集約的な検証[4]には膨大な金額・時間が必要なのだが、世の中はよりコストに厳しい方向に向かっており、検証にかけられるリソースも限られて、バグが見つけられず残ってしまう可能性が高まる。

そのテストの工程を一部でも自動化し、よりコスト効率的に行う、あるいはソフトウェアのより広い部分をカバーする検証を可能にするのがソフトウェア検証である[5]。

3.2 ソフトウェア検証の歴史

ソフトウェア検証の試みは1960年頃から始まった。当初はプログラムが行う「何」を厳密に書き、それと実際に書かれたプログラムが正確に一致しているかを厳密に「証明」すると

[2]例えば「与えられた直径の円の面積を求める」としよう。

[3]例えば先の簡単な円の面積の例に対しても「直径を2で割った値を r に記録し、$3.1415 \times r \times r$ を計算して返す」とか、「与えられた直径 d を使って $d^2 \times 0.7854$ を計算して返す」など「どう」は無限にありうる。

[4]例えばWebサイトのシステムでは人がWebブラウザーからいろいろなデータを入力し、想定通りの動作をするかを検証する。

[5]ソフトウェア検証についての一般的な紹介については [4] や [5] を参照されたい。**??**で紹介している米国富士通研究所で研究開発されているSymbolic実行については [6] を参照されたい。

いったことを行っていた。

しかしそれでは「何」を書くために全く別の書式を学ばないとならず、また「何」を書くだけで別にプログラムを書く程度の労力が必要となる。そのため小さなプログラムにしか適用できず、また広く使われることにはならなかった。つまり当初のアプローチは大規模なソフトウェアに対しては無力であった。

その潮目が変わったのは 1998 年頃で、それまでの正確性を証明などによって保証するという立場から、厳密性・完全性は犠牲になるかもしれないができるだけ多くのバグを見つけようという立場に変わっていった。以前のアプローチは無駄ではなかったが、やはり象牙の塔の中の研究であったことは否めず、産業界からのそれが何の役に立つの？ という問いかけに対して、実際のプログラムを直接検証できるようにしようという方向に変わった。それからは CMU、Stanford 大学、Microsoft、NASA、UC Berkeley、NEC、そして富士通などがソフトウェア検証をより大きなソフトウェアに適用可能にする努力を続けてきた。

3.3 Symbolic 実行

ソフトウェア検証の symbolic 実行についてその手法を簡単な例をもって以下に説明し、そのメリット、限界、今後を議論する。

```
foo(a, b, c) {
  int a,b,c;
  c = a + b;
  if (c > 0) {
    c++;
  }
  return c;
}
```

図 4：プログラム

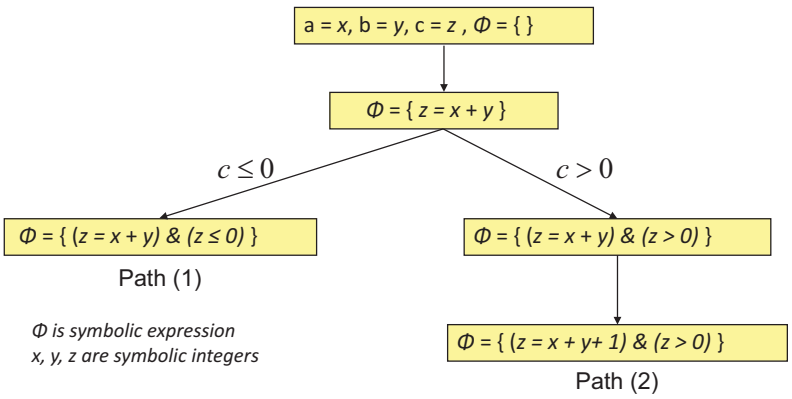


図 5：Symbolic 実行の流れ

プログラムの例として次のような簡単な関数（図 4）を考える。この関数は手続きとして書かれているが、その関数の役割から

$$(a > 1) \wedge (b > 0) \rightarrow (c > 4) \tag{7}$$

という条件を満たさないといけないとしよう。このプログラムが本当にこの条件を満たすものになっているかどうかを確認するためには以下のようにする。

まず条件 (7) の結論を否定したもの

$$(a > 1) \wedge (b > 0) \rightarrow (c \leq 4) \tag{8}$$

を用意する。関数の実行の最後でこの結論を否定した条件 (8) を満たす a, b, c がもし存在しなければ、このプログラムはもともと与えられた条件 (7) を満たし、もし存在すればこのプログラムは条件 (7) を満たさ**ない**と結論付けることができる。

そのために関数（図 4）を図 5 のように変数 a, b, c に symbolic な変数 x, y, z を代入してそのまま実行する。代入文 ($c = a + b$) があれば、それを対応する条件 ($z = x + y$) を symbolic 表現に付け加え、条件文 (if ($c > 0$)) のところでは、その真偽を決定できないので、条件文の条件式（$z \leq 0$ と $z > 0$）をそれぞれに加えて、両方の分岐を別々にたどっていく。それら二つの経路、Path (1) も Path (2) もやがて関数の終わりにたどり着き、それぞれの経路をたどる条件がそれぞれの Φ に蓄えられる。

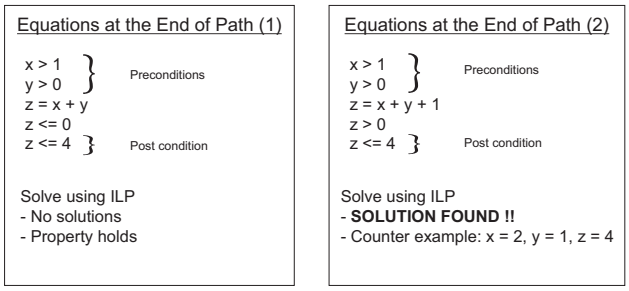


図 6：各経路の実行終了時の式

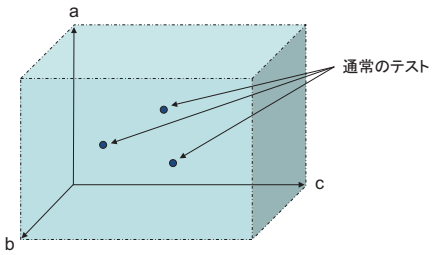


図 7：通常テストと Symbolic 実行

図 6 のように、Φ のそれぞれに条件 (8)（図の中では Precondition と Post Condition とに分けている）を組み合わせ、それぞれの式のセットを例えば ILP (Integer Linear Programming) を使って解く。Path (1) の場合には解がなく条件 (7) を満たし、Path (2) の場合には解（例えば $x = 2, y = 1, z = 4$）が存在し、条件 (7) を満たさ**ない**ことが分かる。Path (2) の場合に得られた解は実際に（与えられた条件 (7) を満たさないという意味で）エラーを引き起こす入力として関数にテストデータとして与え、バグの存在確認にも使うことができる。

図 7 で模式的に表されるように、通常のテストでは変数空間内の限られた点でしか与えられた条件を満たすかどうか検証できないのに対して、この symbolic 実行では変数空間全体で一気にその条件を満たすかを検証することができる。

これは一般にも有効であるが、terminal condition[6]での検証や、通常のプログラムの実行ではまれにしか通らない経路での検証[7]などに特に力を発揮する。

このように symbolic 実行は強力ではあるが、もちろんその限界がある。条件分岐があれば経路がどんどん増えていき、探索すべき状態空間が爆発し、計算機の処理能力の限界を超してしまう。またより多くの変数を symbolic として扱えば、計算量的負担はさらに増える。Symbolic 実行はだいぶ実用のレベルに近づいてきたが、実際のより巨大なプログラムに symbolic にする変数の数などの制約がより少なく、実用的に適用できるようにするためにさらに工夫を重ねる必要がある。

[6] c が実数で $c > 545$ といった条件。$c = 546, 545.1, 545.01, \ldots$ とどこまで 545 に近い値を入れても完全には検証できない。

[7] 具体的な値を必要とする通常のテストではその経路を通るようにすることが難しい。Symbolic 実行では全ての経路を同じようにたどり検証することができる。

その更なる実用化には二つの方向から取り組まれている。一つはプログラムの適切な抽象化を行い、状態空間の爆発を抑え込むものである。例えば、注目するモジュールだけ厳密にsymbolic 実行を行い、それ以外の関係するモジュールは簡単化したり、注目している部分に関係しないコードを削除してしまったり、数値変数を整数や実数ではなく正負とゼロの場合だけにしてしまうことなどが行われており、さらにいろいろな新しいアイデアも導入されている。

もう一つの方向はcloud computingなど分散コンピューティング技術を使って経路探索を複数の計算ノードに分散して、扱える状態空間のサイズを大きくするといったものである。

4 おわりに

本稿では、数学を活用した「ものづくり」の効率化・高度化のための方法論としてsymbolic approachesを説明し、ハードとソフトの開発での適用事例を紹介した。

ものづくりの現場では、開発対象の複雑化や開発期間の短縮化が進むにつれ、効率化・コスト削減・高付加価値化の実現のためモデルベース設計が注目されている。その高度化には、本稿で紹介したsymbolic approachesをはじめとした各手順を支える数理的手法の継続的な革新が必須である。さらに、数理的手法を積極的に用いた設計手法を、広く有効活用してもらうにはわかりやすさや使いやすさを考慮したツールとして提供することも大切な点であり、将来的には、数学問題をコンピュータが自動で解くような研究 [7] も活用されるであろう。

最後に、ものづくりの分野で蓄積されてきた数理的な分析・最適化・検証手法の重要性は、ものづくりに留まらず社会システム、エネルギーマネージメントなど広範な領域においても今後ますます高まっていくと思われる。

参考文献

[1] 穴井宏和，横山和弘，『QEの計算アルゴリズムとその応用—数式処理による最適化』東京大学出版会，2011.

[2] 中山弘隆，岡部達哉，荒川雅生，尹禮分，『多目的最適化と工学設計—しなやかシステム工学アプローチ』現代図書，2008.

[3] “Epic failures: 11 infamous software bugs,” ComputerWorld, Sep. 9, 2010, `http://www.computerworld.com/s/article/9183580`.

[4] Cadar, C., Godefroid, P., Khurshid, S., Pasareanu, C., Sen, K., Tillmann, N., “Symbolic Execution for Software Testing in Practice: Preliminary Assessment,” ICSE'11.

[5] D'Silva, V., Kroening, D., Weissenbacher, G., “A Survey of Automated Techniques for Formal Software Verification,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), July 2008.

[6] Li, G., Ghosh, I., Rajan, S. P., “KLOVER: A Symbolic Execution and Automatic Test Generation Tool for C++ Programs,” CAV 2011.

[7] 相澤彰子，松崎拓也，穴井宏和，“自然言語処理と計算代数の接合による数学問題へのアプローチ”人工知能学会誌 27 (5), pp. 483–491, 2012.

暗号のシステム応用

秋山　浩一郎

株式会社東芝　研究開発センター

概 要

暗号は数理的な知見が反映されている技術であるが、それが身近に応用されていることは意外と知られていない。本稿では暗号が応用された事例の中で典型的なものであるDVD/BD（ブルーレイ）向けのコンテンツ保護とクラウドストレージサービスを例にとって解説する。

1　はじめに

暗号は特定の人のみに情報を伝達するアルゴリズムとして、最初は軍事向けに開発された。暗号には大きく分けて共通鍵暗号と公開鍵暗号がある。共通鍵暗号は高速ではあるが、1つの鍵（共有鍵）を共有している相手としか暗号通信できない。公開鍵暗号は低速であるが、公開鍵と呼ばれる不特定多数に公開できる暗号化鍵で暗号化を実現し、秘密鍵を呼ばれる自分だけが知る復号鍵で復号することができる。共通鍵暗号ではデータをビット毎に分解し、スクランブルを行っている。スクランブルのパターンを決めるのが鍵（共通鍵）であり、暗号化で使った鍵を復号で利用しない限り、コンテンツは復号できない。一方、公開鍵暗号は、これに加えて、公開された公開鍵から秘密鍵が求められないという非対称な性質を実現するため [1] で紹介されているような数理が使われている。多くのシステムでは、コンテンツの暗号化には高速な共通鍵暗号を、そこで使われる共通鍵の暗号化には公開鍵暗号を利用する方式（ハイブリッド方式）が取られることが多い。本稿ではこれら暗号のシステム応用に焦点をあて、その代表的な2つの事例を紹介する。

暗号の応用がどのように始まったのかを理解するために、暗号の歴史を簡単に振り返ってみよう。暗号は1960年代までは主に軍事目的で研究され、その内容も軍事機密であり公表されることはあまりなかった。しかし、1970年代後半に公開鍵暗号が開発されるに至って、公開の場での安全性に関する学術的な議論が盛んになり、1980年代後半までには [1] で紹介されているRSA暗号やその安全性など公開鍵暗号の基礎が整備されてきた。その後は1990年代半ばに始まる機器のデジタル化や情報システムのネットワーク化に伴って、暗号は安全を守る技術として広く応用されるようになってきた。応用された身近な例としてSSL (Secure Socket Layer) による通信がある。ここでは、インターネット上で会員登録やショッピングなどをする際、住所やクレジットカード番号などの個人情報を第三者に秘匿する目的で暗号が利用されている。

一方、産業界では1980年代半ばにCDが発売され、それまでにないデジタル音声による、極めてクリアな音が楽しめるようになった。しかし、それまでのアナログ録音とは違ってコピー

すれば全く同じものができてしまうという問題が指摘されていた。実際、CD はこれから述べるようなコピー制御手段を定めずに販売されてしまったため、後にコピー制限を加えるまでは、コピーし放題とも言える状況となった。1996 年に発売された DVD ではその反省を生かし、設計段階からコピー制御機構が検討され、実際にコピー制御機構を導入したものが発売されている。コピー制御は簡単に言うと、コンテンツを暗号化して、コピー制御された機器のみに復号して再生させる仕組みである。ここでは暗号方式に加えて、復号鍵をどのようにコピー制御された機器にのみ渡すか？ という問題がある。このような仕組み全体はコンテンツ保護と呼ばれており、その概要を 2 節で述べる。

一方、2000 年代後半からクラウドと呼ばれる大量の資源を持った計算機環境が提唱されてきた。クラウドではそれら大量の資源を複数の利用者で共有することで、計算機の導入コストを大幅に下げることができる。一方で、他人と共有することからデータを覗き見られる恐れがあるだけでなく、大量のデータが集まることから、サイバー攻撃を受けやすい。そこで、機密性の高いデータを中心に暗号化して保存する方法が取られている。しかし、クラウドの計算機環境を有効に利用するためには、可能な限りクラウド内で処理する必要があり、暗号化したまま処理できる暗号方式が求められている。残念ながら、現状では、全ての処理が暗号化したまま可能となる訳ではなく、実用的な暗号方式を目指した研究が進められている。3 節ではそれら実用的な暗号のうち、再暗号化技術を紹介する。

2　コンテンツ保護

コンテンツ保護の目的は視聴（あるいは閲覧）する権利のある人（通常はコンテンツ購入者）にのみにコンテンツを見る権利を付与することである。映画などの DVD コンテンツを不正コピーされると当該コンテンツを視聴する権利のない人でも見ることができてしまう。このことからコピー制御はコンテンツ保護の中で重要な役割を果たしていることが分かる。しかし、コピーする能力のある録画再生機器を遠隔で監視・制御することはできない。そこでコピー制御では、適切にコピー制御を行う機器にのみコンテンツを視聴させるという手法を採用している。

特定の人（ここでは機器）にのみコンテンツを視聴させるようにするには、コンテンツを共通鍵暗号で暗号化し、そこで使われる鍵を公開鍵暗号で暗号化して送るという手法が一般的であった。しかし、DVD/BD はメディアであるので、メディアに（特定の機器でのみ復号できる形で暗号化して）コンテンツを復号できる共通鍵を書き込んでおく。この共通鍵をメディア鍵という。

本節では、DVD に採用されている CPPM (Content Protection for Prerecorded Media) の仕組みについて解説する。図 1 を見て頂きたい。DVD メディアに書かれているメディア鍵は Lead-in 領域と呼ばれる通常読み込めない領域に機器毎に異なる形で暗号化された鍵束として記録されている。この鍵束を MKB (Media Key Block) と呼んでいる。MKB は多数存在する機器向けのメディア鍵を効率良く暗号化して束にしたもので、単純に機器毎に暗号化したものを束にしたものと比較して、データサイズを圧倒的に小さく抑えることができる。

機器固有の鍵（デバイス鍵）を用いることで MKB からメディアに固有の鍵（メディア鍵）

を復元する（MKB 処理）。メディア鍵はこのメディアに暗号化して記録されているコンテンツを復号するための起点となる鍵である。タイトルを復号するときはタイトルに対応するアルバム ID を DVD から抽出し、アルバム ID とメディア鍵から一方向性関数を利用してアルバム固有鍵を出力する。更に、コンテンツを復号するためにはアルバム固有鍵と 2048 ビット毎に定められた鍵変換データを繰り返し適用することによって、コンテンツ鍵を抽出する必要がある。コンテンツ鍵が出力されれば、それを使ってコンテンツを復号することによって視聴が可能となる。

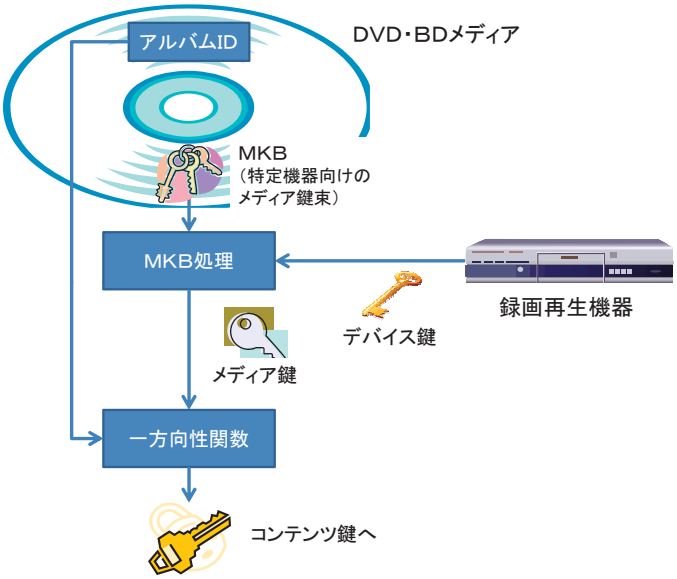


図 1：CPPM の概要

CPPM におけるコンテンツ保護はデバイス鍵が起点となっている。即ち、デバイス鍵が露見してしまうと、そのデバイス鍵を用いることで、メディア鍵が取り出せてしまう。DVD ではデバイス鍵は機種毎に設定されているが、ある機種のデバイス鍵が露見すると、その機種になりすました不正再生ソフトを作ることが可能になる。そのような場合に対抗するため、新たに発売されるメディア（ディスク）からは、その MKB に当該機種向けの鍵を含めないという取り決めがある。即ち、メディア鍵が露見した機種では、新しく発売されるコンテンツを復号できなくなり、新しいコンテンツの不正コピーができないだけでなく、再生もできなくなる。では、新しいコンテンツが再生できなくなった機種はどうするのであろうか？ デバイス鍵が露見した原因を特定した上で、可能ならインターネット経由などでシステム更新を行う。

DVD よりも大容量メディアである BD では、セキュリティを強化したコンテンツ保護方式 AACS (Advanced Access Conent System) が採用されている。BD は DVD よりも容量が大きくなり、高精細で付加価値の高いコンテンツを楽しむことができるようになった。このため、CPPM の実用化により明らかとなった問題点を改善するセキュリティ機能を盛り込んだ方式

となっている。ここでは、それらの機能のうちの 2 つを紹介する。

- 再生機器を同定する機構 (Sequence Key Block)
  CPPM では不正機器を特定することが困難であった。この反省から再生されたコンテンツから再生機器を特定できる機構を導入した。再生機器にシーケンス鍵セットを持たせ、これらシーケンス鍵によって、復号されるコンテンツが異なるようにしておく。異なるコンテンツと言っても内容が異なっては困るので、電子透かし[1]などを使って人間の目に分からない程度に差異を設けておくのである。
- 不正コンテンツの無効化（コンテンツ証明書）
  CPPM ではコピー防止はできたが、海賊版などの不正コンテンツも再生できてしまうという問題があった。そこで AACS では正当なコンテンツに対しては証明書（コンテンツ証明書）を付与することになった。コンテンツ証明書は機器に備えられている公開鍵で認証することで正当なコンテンツであることが分かり、正当なコンテンツのみを再生できるようになった。

3　クラウド向け暗号

クラウドは大量の計算機と大きな記憶容量を備えた計算環境である。利用者は利用するソフトウェアやデータも含めて処理に関係するほとんど全ての部分をクラウド側に持たせて処理することができる。このため、利用者はネットワークに接続可能なクライアント端末（PC 等）以外の設備投資をすることがなく、導入コストを下げられるため、近年個人も含めて利用が進んでいる。

一方で、クラウドには多くのデータが集まるためサイバー攻撃の対象となりやすい。そのため、外部からの侵入を防止するための数々のセキュリティ対策が取られている。しかし、サイバー攻撃も日に日に進歩しているため、常に新しい攻撃が出現する。そこで、（個人情報等の）漏れてはいけないデータをクラウドで処理するためには、暗号化して保管することが必須である。暗号化して保管したものは（通常は）復号しないと処理することができないが、クラウド上で復号するとサイバー攻撃を受けやすい。その一方で、クライアントで復号する場合、クラウドからデータを転送する必要があり、大容量のデータであればあるほど、現実的ではない。

そこで、暗号化したまま処理可能な方式があれば理想的である。実際に、暗号化したまま共有する方式、暗号化したまま演算する方式、暗号化したまま検索する方式が知られている。

暗号化したまま共有する方式には、暗号文を（復号する個人向けに）変換する技術と、（復号できるグループ向けに）暗号化する技術が知られている。前者は再暗号化技術と呼ばれ、元の暗号文の変換を基本とするためアクセス権を変更しやすいが、変換のための再暗号化鍵が必要であり、それを管理する管理サーバが必要である。後者は予め定められたグループの人のみが復号できる形で暗号化する技術で、管理サーバの必要はないが、グループの構成メンバに変更があった場合は対応が難しい。

暗号化したまま演算する方式は（完全）準同型暗号と呼ばれ、暗号化したまま足し算と引き算ができる方式を準同型暗号、掛け算も可能な方式を完全準同型暗号という。準同型暗号は、

[1]画像の一部に人目では分からないような情報を埋め込む技術

その名の通り、暗号化関数が準同型性を持つ暗号方式である。即ち、暗号化関数を E とするとき、

$$E(x) + E(y) = E(x + y)$$

という性質を満たすのが準同型暗号、

$$E(x)E(y) = E(xy)$$

も満たすのが完全準同型暗号である。式を見れば明らかなように暗号化された数値同士を足し算、掛け算した結果が、(暗号化していない) 数値同士を足し算、掛け算したものを暗号化した暗号文となっている。これを複数回組み合わせることで、大量の (暗号化された) データの足し算や掛け算をすることができる。準同型暗号を実現する暗号方式には格子暗号などが知られている。

暗号化したまま検索する方式は検索可能暗号と呼ばれており、テキスト文書の中のキーワードを暗号化したまま検索する方式である。応用先によっては検索するキーワードも秘匿したいという要求もあり、検索するキーワードを秘匿する方式も多い。

本節では特に再暗号化技術を取り上げて原理を詳しく説明する。再暗号化技術は暗号文を (復号する個人向けに) 変換する技術である。図 2 を見て欲しい。取引先の担当者がプロジェクトグループのメンバに文書を送る際、管理者 X からそのプロジェクトグループに割り当てられた公開鍵で暗号化してクラウドにアップロードする。再暗号化サーバは再暗号化鍵を使ってグループのメンバが復号できるような形に変換する。例えばメンバ A 向けに再暗号化鍵 $K_{X \to A}$ を使ってメンバ A の秘密鍵で復号できるような形に変換する。このようにすることで、メンバは個別の鍵 (秘密鍵) を持ちながら同じ暗号化データを共有することができる。

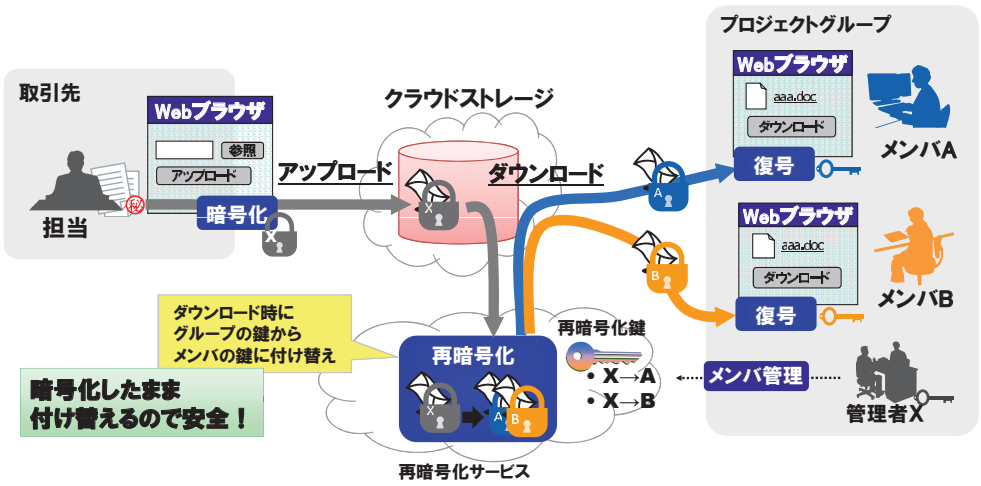


図 2：再暗号化

このような特性を持った暗号はペアリングを利用して構成する。ペアリングとは楕円曲線 E/F_p の上の 2 点 P, Q のペアで定義される量 $e(P, Q)$ であり、楕円曲線の定義体 F_p の拡大体 F_{p^k} 上に値を取る。

楕円曲線上の点には加算（点加算）が定義できるので、2 点 P, Q に対して $P+Q$ が計算できる。実際にどのように計算するのかは [1] に記述があるので、そちらを参照願いたい。同様に同じ点の加算もできるので P の 2 倍点 $2P = P + P$ も定義できる。更に $3P = 2P + P$ が計算できることを考えると a を正整数としたとき、点 P の a 倍点 aP も計算できる。また、$P = (x, y)$ に対して $-P = (x, -y)$ と定義できるため、更に一般化して、a を非零整数としたとき、点 P の a 倍点 aP も計算できることになる。このような演算を点 P のスカラー倍算と呼ぶ。このようなスカラー倍をした点 aP, bQ に対して、ペアリングは下記のような性質を満たす。

$$e(aP, bQ) = e(P, Q)^{ab}$$

この性質は双線形性と呼ばれる。

これを使って、まずは再暗号化の暗復号アルゴリズムを紹介する。

[システムパラメータ]

素数位数 l の楕円曲線 E/F_p とその生成元を P とする。生成については [1] を参照。この楕円曲線 E/F_p 上で定義されるペアリング $e(P, P)$ が含まれる有限体を $K\ (= F_{p^k})$ とおく。

[公開鍵および秘密鍵]

秘密鍵 $s \in \{1, 2, \ldots, l-1\}$ に対して、$Q_s = sP$ を公開鍵とする。

[暗号化]

平文 m を有限体 K の元とする。乱数 $r \in \{1, 2, \ldots, l-1\}$ を発生して、システムパラメータ P と公開鍵 Q_s を使って、

$$C_1 = rQ_s \in E/F_p, \quad c_2 = m \cdot e(P, P)^r$$

を計算し、(C_1, c_2) を暗号文とする。

[復号]

暗号文 (C_1, c_2) に対して、秘密鍵 s を利用して、復号

$$c_2/e(s^{-1}C_1, P) = m \cdot e(P, P)^r / e(s^{-1}rsP, P) = m \cdot e(P, P)^r / e(P, P)^r = m$$

を行う。

次に、再暗号化の主要部分、暗号文を（復号する個人向けに）変換する再暗号化処理と、その復号について詳しく説明する。

[システムパラメータ]

前記と同じ。

[（個人（メンバ A）向けの）公開鍵および秘密鍵]

秘密鍵 $a \in \{1, 2, \ldots, l-1\}$ に対して、$Q_a = aP$ を公開鍵とする。

[再暗号化鍵]

$(a/s)P$.

［（メンバ A 向けの）再暗号化］
暗号文 $(C_1, c_2) = (rQ_s, m \cdot e(P,P)^r)$ に対して、メンバ A 向けの再暗号化鍵 $(a/s)P$ を利用して $e(C_1, (a/s)P)$ を計算する。これは

$$e(rQ_s, (a/s)P) = e(rsP, (a/s)P) = e(P,P)^{ar}$$

となり、これを C_{1A} とする。c_{2A} は c_2 をそのまま継承して、暗号文 (C_1, c_2) はメンバ A 向けの暗号文 $(C_{1A}, c_{2A}) = (e(P,P)^{ar}, m \cdot e(P,P)^r)$ に変換される。

［復号］
秘密鍵 a を使って、

$$\frac{c_{2A}}{C_{1A}^{a^{-1}}} = m\frac{e(P,P)^r}{e(P,P)^r} = m$$

により復号される。

再暗号化方式はメンバに個別の鍵を持たせ、データへのアクセス制御を再暗号化サーバで管理できるため、組織変更などによるメンバの脱退・加入に対応しやすいという特質があり、クラウドストレージサービスとして実用化されている。今後の発展が楽しみな技術である。

4　おわりに

本稿では、数理的に構成された暗号が実際のシステムに応用されている典型的な事例を紹介した。暗号技術は情報セキュリティの主要技術であるため、今後とも活用が進むと考えられる。これからは新興国を中心に電気・ガス・水道・交通などの社会インフラがインターネットに繋がっていくため、これらに向けた活用が進むものと考えられる。これらのシステムは、機器や施設を制御するため、非権限者によりシステムが勝手に操作されることを避けなければならない。即ち、権限者と非権限者を分けるための仕組みが重要となる。このような仕組みは認証と呼ばれ、やはり暗号技術により構成される。

また、暗号実装のことにも少し触れておかなくてはいけない。暗号はアルゴリズムレベルで安全であっても実装により鍵が漏れることがある。たとえば、暗号をソフトウェアで実装した場合、鍵がソフトウェア内部に存在すれば、デバッグツールなどを使って解析することにより露見してしまう。ハードウェアで実装した場合でも、ハードウェア内部には鍵があり、その鍵を使って暗復号処理が進むので、その消費電力波形から鍵が漏れることがある。なぜなら、鍵により処理パターンが決まり、その処理パターンにより消費電力が変化するからである。最近のシステムでは、このような攻撃にも対抗できる方式が用いられている。

このように、暗号への攻撃（解読）の試みも進められており、常に最新の技術を参照しながらシステム開発やメンテナンスをしていく必要がある。

参考文献

[1] 高木剛，公開鍵暗号入門，本書所収.

確率推論に基づく復号法と疎行列に基づく誤り訂正符号

内川　浩典

株式会社東芝　セミコンダクター&ストレージ社
半導体研究開発センター

1　はじめに

現在，身の回りにある機器の多くが情報の蓄積や伝送を行うディジタル機器である．そしてそのようなディジタル機器では，記録データを読み出す際や伝送データを受け取る際，データに生じた誤りを訂正するため誤り訂正符号が用いられている．たとえば音楽 CD などで，盤面に少し傷がついたとしても再生可能であるのは，誤り訂正符号のおかげである．

本稿では，誤り訂正符号の中でも理論限界に迫る訂正能力を実用可能な計算量で実現できることから，近年ハードディスク装置やデジタル放送システムなどで実際に製品化が開始されている LDPC (Low Density Parity Check) 符号と，その復号法である sum-product 復号を紹介する[1]．特に確率推論の観点から最適な復号アルゴリズムが，LDPC 符号により実行可能な形に導かれることを述べる．

2　通信システムモデルと誤り訂正符号

誤り訂正符号を議論する際の通信システムモデルは図 1 のように表される．まず，情報を表す長さ k のメッセージ $\mathbf{m} = m_1 m_2 \dots m_k$ は，通信路での誤りに耐えられるよう，符号化処理によって長さ n の符号語 $\mathbf{x} = x_1 x_2 \dots x_n$ へと変換される．ただし $n > k$ である．符号語 $\mathbf{x}$ は，通信路において誤りが加わり受信語 $\mathbf{y} = y_1 y_2 \dots y_n$ となる．ここで通信路は，送信された符号語 $\mathbf{x}$ に対する条件付き確率 $P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x})$ でモデル化される．受信語 $\mathbf{y}$ は復号処理により，もとの符号語の推定語 $\hat{\mathbf{x}}$ もしくはメッセージの推定語 $\hat{\mathbf{m}}$ へと変換される[2]．なお本稿では議論を簡単にするため，メッセージのシンボル m_i $(1 \le i \le k)$，符号語のシンボル x_i $(1 \le i \le n)$ および受信語のシンボル y_i $(1 \le i \le n)$ はそれぞれ $\{0, 1\}$ いずれかをとるものとし，通信路はシンボルごとに独立かつ同一の条件付き確率

$$P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i),$$

[1] 本稿は数学セミナー 2012 年 11 月号に掲載した「確率推論による復号と LDPC 符号」に加筆修正をおこなったものである．

[2] 通信システムとしてはもとのメッセージの推定語 $\hat{\mathbf{m}}$ が得られるまでを通信システムモデルとすべきだが，メッセージ $\mathbf{m}$ と符号語 $\mathbf{x}$ とは 1 対 1 対応の関係があるため，符号語の推定語 $\hat{\mathbf{x}}$ が得られるまでを通信システムモデルとすることが多い．

ただし

$$P_{Y|X}(y_i|x_i) = \begin{cases} 1-p & x_i = y_i \\ p & x_i \neq y_i \end{cases}$$

でモデル化された 2 元対称通信路とする．ただし，p は反転確率と呼び，通信路でシンボルが誤る確率をあらわす．

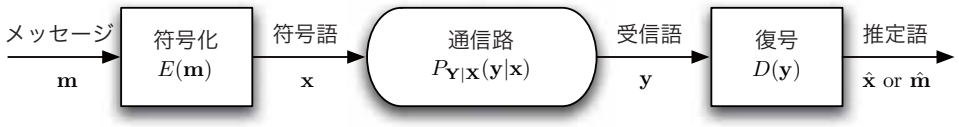


図 1：通信システムモデル

通信の伝送速度を $R = k/n$ と定義したとき，通信路モデルから導出される通信路容量 C を超えない範囲 $R \leq C$ で，誤り率を任意に小さくできる誤り訂正符号が存在することが知られている [1]．そして誤り訂正符号に携わる技術者にとっては，限りなく C に近い伝送速度 R を計算量的に実行可能な符号化復号処理で実現することが，大きな目標となっている．

3　確率推論による復号

誤り訂正符号の復号処理とは，通信路で誤りが生じた受信語 $\mathbf{y}$ から，もっともらしい符号語 $\mathbf{x}$ を推定する推論問題と考えることができる．そしてこの「もっともらしさ」を定量的に扱う道具として，確率を用いる．

いま，送信者が長さ n の符号語 $\mathbf{x} = x_1 x_2 \cdots x_n$ を一様に選んで送信し，通信路を介して受信者が受信語 $\mathbf{y} = y_1 y_2 \cdots y_n$ を受信することとする．このとき，符号語シンボル x_i の誤り率をもっとも小さくする復号アルゴリズムは次のように与えられる．

$$\hat{x}_i = \underset{x_i \in \{0,1\}}{\operatorname{argmax}} P_{X|\mathbf{Y}}(x_i|\mathbf{y}) \tag{1}$$

ただし $\underset{x_i \in \{0,1\}}{\operatorname{argmax}}$ は右項を最大にする引数 x_i を返す関数で，$P_{X|\mathbf{Y}}(x_i = 0|\mathbf{y})$ と $P_{X|\mathbf{Y}}(x_i = 1|\mathbf{y})$ とを比較し，確率値の大きい x_i を推定シンボル $\hat{x}_i$ とする．事後確率と呼ばれる $P_{X|\mathbf{Y}}(x_i|\mathbf{y})$ を最大化するシンボルを推定シンボルとすることから，この復号アルゴリズムは最大事後確率復号[3]と呼ばれる．

[3]送信された符号語 $\mathbf{X}$ の事後確率を最大化する最大事後確率復号と区別するため，シンボル最大事後確率復号や最大事後周辺確率復号と呼ばれることもある．

式 (1) を通信路の条件付き確率 $P_{Y|X}(y|x)$ で計算できる形に式変形すると，次のようになる．

$$\begin{aligned}
\hat{x}_i &= \operatorname*{argmax}_{x_i \in \{0,1\}} P_{X|\mathbf{Y}}(x_i|\mathbf{y}) \\
&= \operatorname*{argmax}_{x_i \in \{0,1\}} \sum_{\sim x_i} P_{\mathbf{X}|\mathbf{Y}}(\mathbf{x}|\mathbf{y}) && (2) \\
&= \operatorname*{argmax}_{x_i \in \{0,1\}} \sum_{\sim x_i} \frac{P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) P_{\mathbf{X}}(\mathbf{x})}{P_{\mathbf{Y}}(\mathbf{y})} && (3) \\
&= \operatorname*{argmax}_{x_i \in \{0,1\}} \sum_{\sim x_i} P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) P_{\mathbf{X}}(\mathbf{x}) && (4) \\
&= \operatorname*{argmax}_{x_i \in \{0,1\}} \sum_{\sim x_i} \left(\prod_{j=1}^{n} P_{Y|X}(y_j|x_j) \right) \mathbb{I}[\mathbf{x} \in C] && (5)
\end{aligned}$$

なお，$\sum_{\sim x_i}$ は x_i を除くすべてのシンボルの，すべての値に対する総和記号で，例えば $\sum_{\sim x_1}$ は

$$\sum_{x_2 \in \{0,1\}} \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}}$$

を表す．式 (2) は周辺確率の計算式[4]から得られ，式 (2) から式 (3) への変形は

$$\begin{aligned}
P_{\mathbf{Y},\mathbf{X}}(\mathbf{y},\mathbf{x}) &= P_{\mathbf{X}|\mathbf{Y}}(\mathbf{x}|\mathbf{y}) P_{\mathbf{Y}}(\mathbf{y}) \\
&= P_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) P_{\mathbf{X}}(\mathbf{x})
\end{aligned}$$

というベイズ則から得られる．そして $P_{\mathbf{Y}}(\mathbf{y})$ が $\operatorname*{argmax}_{x_i \in \{0,1\}}$ の操作に寄与しないことから，式 (4) が得られる．さらに各シンボルの誤り率が独立なことと，各符号語の送信される確率が一様であるという仮定から式 (5) を得た．ただし $\mathbb{I}$[条件] は指示関数で，条件を満たすときには 1 を返し，そうでない場合は 0 を返す．

式 (5) であれば，通信路の条件付き確率から直接計算できるものの，$\sum_{\sim x_i}$ で総和をとる項数が符号の長さ n に対して指数的に増加するため，一定以上の長さの符号に対してこの計算をこのまま実行することは現実的ではない．では効率的に計算するには，どのようにすればよいだろうか？

4　分配則による演算数の削減

前節の式 (5) を見るとわかるように，事後確率の計算は積和演算の形をとる．もし，和の項に共通する因子を和記号の外にくくり出す，つまり分配則が適用できれば，演算数を削減できる（図 2）．

[4]多変数の同時確率から計算される単一変数の確率を，周辺確率と呼ぶ．たとえば 2 変数の同時確率 $P_{AB}(a,b)$ が与えられたとき，確率変数 A の周辺確率は $P_A(a) = \sum_{b \in \mathcal{B}} P_{AB}(a,b)$ により得られる．ただし $\mathcal{B}$ は確率変数 B の定義域を表す．

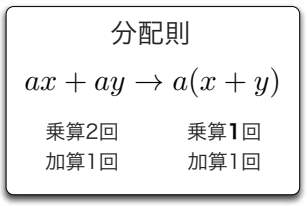


図 2：分配則により，乗算数を 1 つ減らせる例.

分配則により事後確率の計算式が簡単になることを示すため，以下ではパリティ検査行列

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{6}$$

で定義される符号

$$C_1 = \{\mathbf{x} \in \{0,1\}^7 | H_1 \mathbf{x}^{\mathsf{T}} = \mathbf{0}\}$$

を用いて，送信シンボル x_1 に対する事後確率の計算式を導く.

まず，式 (5) より，送信シンボル x_1 に対する事後確率は次のように与えられる.

$$P_{X|\mathbf{Y}}(x_1|\mathbf{y}) = \sum_{\sim x_1} \mathbb{I}[H_1 \mathbf{x}^{\mathsf{T}} = \mathbf{0}] \prod_{j=1}^{7} P_{Y|X}(y_j|x_j) \tag{7}$$

なお，$\mathbf{x}^{\mathsf{T}}$ はベクトル $\mathbf{x}$ の転置を表す．ここで，指示関数の条件となっている $H_1 \mathbf{x}^{\mathsf{T}} = \mathbf{0}$ がパリティ検査行列中の各検査式の充足条件の積で記述できることを利用すると，式 (7) は

$$P_{X|\mathbf{Y}}(x_1|\mathbf{y}) = \sum_{\sim x_1} \mathbb{I}_1 \mathbb{I}_2 \mathbb{I}_3 \prod_{j=1}^{7} P_{Y|X}(y_j|x_j)$$

と変形できる．ただし

$$\begin{aligned} \mathbb{I}_1 &= \mathbb{I}[x_1 + x_4 + x_5 = 0], \\ \mathbb{I}_2 &= \mathbb{I}[x_1 + x_2 + x_6 = 0], \\ \mathbb{I}_3 &= \mathbb{I}[x_2 + x_3 + x_7 = 0] \end{aligned}$$

で，指示関数の条件はそれぞれ 1 行目から 3 行目のパリティ検査式に対応している．さらに，

総和に含まれる共通因子と指示関数の条件に着目すると，次のように変形できる．

$$P_{X|\mathbf{Y}}(x_1|\mathbf{y}) = P_{Y|X}(y_1|x_1) \sum_{\sim x_1} \mathbb{I}_1\mathbb{I}_2\mathbb{I}_3 \prod_{j=2}^{7} P_{Y|X}(y_j|x_j) \tag{8}$$

$$= P_{Y|X}(y_1|x_1) \left(\sum_{x_4x_5} \mathbb{I}_1 \prod_{j'\in\{4,5\}} P_{Y|X}(y_{j'}|x_{j'}) \right) \left(\sum_{x_2x_3x_6x_7} \mathbb{I}_2\mathbb{I}_3 \prod_{j''\in\{2,3,6,7\}} P_{Y|X}(y_{j''}|x_{j''}) \right) \tag{9}$$

$$= P_{Y|X}(y_1|x_1) \left(\sum_{x_4x_5} \mathbb{I}_1 \prod_{j'\in\{4,5\}} P_{Y|X}(y_{j'}|x_{j'}) \right) \times \left(\sum_{x_2x_6} \mathbb{I}_2 \prod_{j''\in\{2,6\}} P_{Y|X}(y_{j''}|x_{j''}) \left(\sum_{x_3x_7} \mathbb{I}_3 \prod_{j'''\in\{3,7\}} P_{Y|X}(y_{j'''}|x_{j'''}) \right) \right) \tag{10}$$

なお $\sum_{x_ax_b}$ はシンボル x_a と x_b のすべての要素についての総和記号を表す．例えば $\sum_{x_4x_5}$ は $\sum_{x_4\in\{0,1\}} \sum_{x_5\in\{0,1\}}$ を表す．

まず，すべての和の項に含まれる $P_{Y|X}(y_1|x_1)$ を和記号の外へくくり出すことで，式 (8) が得られる．次に，検査式 $x_1 + x_4 + x_5 = 0$ で変数の組が決まる x_4x_5 をくくり出し，式 (9) が得られる．最後に，残りの検査式に対応する指示関数 $\mathbb{I}_2, \mathbb{I}_3$ ごとに積和をまとめることで，式 (10) を得た．変形前の式 (7) では，乗算の数が 96，加算の数が 14 必要であったのに対し，変形後の式 (10) では，乗算の数が 20，加算の数が 6 となり，演算数の少ない計算式を得ていることがわかる．この例ではもとの式 (7) の演算数がもともと大きくないため，分配則による演算数削減の恩恵が少ないように感じるかもしれないが，変形前の式は符号長が長くなると演算数が指数的に増加し，直接計算することが難しくなる．一方，式 (10) は次節以降で述べる sum-product アルゴリズムを用いることで，非常に効率よく計算することができる．

5　木と sum-product アルゴリズム

前節では，事後確率の計算式が分配則により指示関数ごとの積和式の積へ簡略化できることを，例を用いて説明した．どのようなパリティ検査行列に対しても，上述したような簡略化が適用できれば好ましいのだが，残念ながらこのような式変形はパリティ検査式を 2 部グラフで表現した際に，そのグラフ構造が木になっている場合のみに限られる．

図 3 に式 (6) のパリティ検査式の 2 部グラフ表現を示す．2 部グラフは，符号語シンボルに対応する変数ノード（○）と，パリティ検査式に対応する検査ノード（□）の 2 種類のノードから構成される無向グラフである．変数ノード v と検査ノード c とを接続するエッジ (v, c) は，符号シンボルとパリティ検査式との関係を表す．例えば x_1 に対応する変数ノード v_1 は，1 行目と 2 行目のパリティ検査式に対応する検査ノード c_1 と c_2 に接続されていることがわかる．

グラフ構造が木とは，任意のノード a からその他の任意のノード b への経路が 1 つしかないということを表し，閉路を持たないグラフを意味する．図 3 を見ると，グラフに閉路がなく，

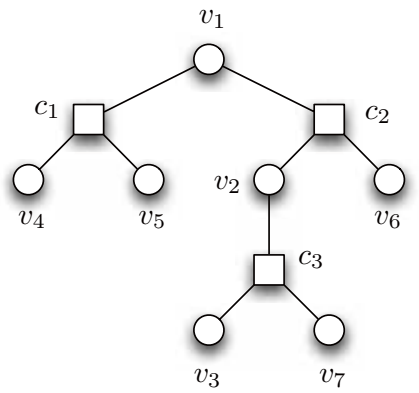


図 3：式 (6) のパリティ検査式の 2 部グラフ表現

木になっていることがわかるだろう．グラフが木の場合，sum-product アルゴリズムにより組織的に事後確率を計算することができる．

sum-product アルゴリズムでは，事後確率を計算したいノード（図 3 では v_1）をルートノードにし，ルートノードからの経路の末端にある葉ノード（図 3 では $v_2, v_3, \ldots, v_7$）からルートノードに向かって，ノードごとに式 (11), (12) の処理を行い，生成したメッセージをルートノードの方向へ送る．そしてルートノードは接続しているすべてのエッジからメッセージを受け取った後，式 (13) の一時推定処理をすることで，事後確率を得る．

変数ノード処理

$$M_{v_j \to c_i}(x_j) = P_{Y|X}(y_j|x_j) \prod_{i' \in \mathcal{I}(j) \backslash \{i\}} M_{c_{i'} \to v_j}(x_j) \tag{11}$$

検査ノード処理

$$M_{c_i \to v_j}(x_j) = \sum_{\sim x_j} \mathbb{I}_i \prod_{j' \in \mathcal{J}(i) \backslash \{j\}} M_{v_{j'} \to c_i}(x_{j'}) \tag{12}$$

一時推定処理

$$g(x_j) = P_{Y|X}(y_j|x_j) \prod_{i \in \mathcal{I}(j)} M_{c_i \to v_j}(x_j) \tag{13}$$

なお，$\mathcal{I}(j)$ は変数ノード v_j に接続する検査ノードのインデックス（シンボル x_j が含まれるパリティ検査式の行インデックス）を表し，$\mathcal{J}(i)$ は検査ノード c_i に接続する変数ノードのインデックス（i 行目のパリティ検査式に含まれるシンボル x_j のインデックス）を表す．また $\mathcal{S} \backslash \{i\}$ は，集合 $\mathcal{S}$ から集合 $\{i\}$ を除いた差集合を表す．

たとえば葉ノード v_3 は変数ノードなので，式 (11) よりメッセージ

$$M_{v_3 \to c_3}(x_3) = P_{Y|X}(y_3|x_3)$$

を生成し，検査ノード c_3 へ送る．すべての葉ノードはエッジが 1 本のため，式 (11) 中のメッセージの積の項を持たない．ここでは紙面の都合によりノード v_1 の計算例のみを示したが，他のノードに対しても同様に計算できる．

6 同時更新型 sum-product 復号

復号の際には，すべてのシンボル x_j $(1 \le j \le n)$ に対して事後確率を計算するが，各シンボルに対応する変数ノードをルートノードとして計算を繰り返すことは，シンボル間に共通するメッセージが存在するため，効率がよくない．そこで通常は，各ノードの処理を同時に行い，収束するまで繰り返し処理をする同時更新型 sum-product アルゴリズムが用いられる．以下では，同時更新型 sum-product アルゴリズムを使った復号法の手順を紹介する．

同時更新型 sum-product 復号アルゴリズム

手順 1 初期化
K に最大繰り返し回数を設定し，k に 1 を代入する．そしてすべての $M_{c_i \to v_{j''}}(x_{j''})$ $(1 \le i \le m,\ j'' \in \mathcal{J}(i),\ x_{j''} \in \{0,1\})$ に 1 を代入する．

手順 2 変数ノード処理
すべての変数ノード v_j $(1 \le j \le n)$ において，変数ノード処理（式 (11)）を実行する．

手順 3 検査ノード処理
すべての検査ノード c_i $(1 \le i \le m)$ において，検査ノード処理（式 (12)）を実行する．ただし，m はパリティ検査行列の行数を表す．

手順 4 パリティ検査処理
すべての変数ノード v_j $(1 \le j \le n)$ において，一時推定処理（式 (13)）を実行する．そしてすべてのシンボル x_j $(1 \le j \le n)$ に対して一時推定シンボル

$$\tilde{x}_j = \begin{cases} 0 & (g(x_j = 0) \ge g(x_j = 1)), \\ 1 & (\text{その他}), \end{cases}$$

を得て，一時推定語 $\tilde{\mathbf{x}} = \tilde{x}_1 \tilde{x}_2 \ldots \tilde{x}_n$ を得る．ここで，$H\tilde{\mathbf{x}}^{\mathsf{T}} = \mathbf{0}$ であれば $\tilde{\mathbf{x}}$ を推定語 $\hat{\mathbf{x}}$ として出力し終了する．その他の場合は**手順 5** へ．

手順 5 終了判定
$k = K$ の場合は $\tilde{\mathbf{x}}$ を推定語 $\hat{\mathbf{x}}$ として出力し終了する．その他の場合には k へ $k+1$ を代入し，**手順 2** へ．

ここまで，2 部グラフが木の場合に限って説明してきたが，実用化されている誤り訂正符号のパリティ検査行列の 2 部グラフは木とはなっていない．2 部グラフが木でない場合，sum-product アルゴリズムで計算した値は事後確率の近似値となるが，任意のノードに対して深さ

6から8程度までの部分グラフ（以下，近傍グラフと呼ぶ）が木になっていれば，良好な復号特性を得られることが経験的に知られている．なお深さとは，任意のノードaをルートにして2部グラフを木のように展開したとき，経路に含まれるエッジの数のことを指す．

では，近傍グラフがなるべく木になるようにパリティ検査行列を構成するには，どうすればよいのだろうか？ 実はその答えが，LDPC符号のパリティ検査行列を特徴づける“疎”の部分にあることを次節で紹介する．

7 LDPC符号のパリティ検査行列

LDPC符号は「疎（低密度）なパリティ検査行列で定義される符号」と定義される．疎なパリティ検査行列とは，パリティ検査行列中に含まれる非零要素，2元の場合には“1”の数が少ないパリティ検査行列を表す．どの程度少ないのかというと，1列に含まれる非零要素の平均個数lが符号長nに依存せず，$2 \leq l \leq 8$が一般的に用いられる．1ビット訂正符号として知られるハミング符号のパリティ検査行列に含まれる非零要素数が，平均で少なくとも$\frac{\log_2 n}{2}$個になることと比較しても，LDPC符号のパリティ検査行列が疎であることがわかる．パリティ検査行列が疎であるということは，対応する2部グラフに含まれるエッジの数が少なくなるため，閉路が生成されにくくなる．つまりLDPC符号のパリティ検査行列は，疎にすることで近傍グラフが木になりやすくなり，sum-productアルゴリズムで得られる事後確率の近似精度を上げることに成功しているのである．

以下では，LDPC符号の発明者であるGallager教授が，彼の博士論文[2]で提案したパリティ検査行列の構成法を紹介する．この構成法は，1列に含まれる非零要素の数がlで，1行に含まれる非零要素の数がrとなるような長さnのパリティ検査行列$H^{(n,l,r)}$を生成する．ここでは説明を簡単にするため，nはrの倍数であるものとする．

まず，サブ行列$H_0^{(n,l,r)}$をつぎのように定義する．

$$H_0^{(n,l,r)} := \begin{bmatrix} \mathbf{h}(r) \\ s^{(r)}(\mathbf{h}(r)) \\ s^{(2r)}(\mathbf{h}(r)) \\ \vdots \\ s^{(n-r)}(\mathbf{h}(r)) \end{bmatrix}$$

ただし$\mathbf{h}(r)$は先頭に非零要素がr個連続でならび，残りはすべて0となる長さnのベクトルである．また$s^{(r)}(\mathbf{h})$は，ベクトル$\mathbf{h}$を右方向にr要素分巡回シフトしたベクトルを返す関数とする．

このサブ行列$H_0^{(n,l,r)}$を使って，パリティ検査行列$H^{(n,l,r)}$が次のように得られる．

$$H^{(n,l,r)} = \begin{bmatrix} H_0^{(n,l,r)} \\ \pi_1(H_0^{(n,l,r)}) \\ \vdots \\ \pi_{l-1}(H_0^{(n,l,r)}) \end{bmatrix} \tag{14}$$

なお，$\pi_i(H_0^{(n,l,r)})$ $(1 \leq i \leq l-1)$ は，サブ行列 $H_0^{(n,l,r)}$ の列ベクトルをランダムに並べ替える関数とする．

例として，上記構成法で生成した $H^{(8,2,4)}$ を示す．

$$H^{(8,2,4)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

最後に，2 元対称通信路における LDPC 符号の復号誤り率に関する数値実験結果を図 4 に示す．LDPC 符号のパリティ検査行列は，式 (14) の構成法で生成した 510×1020 のパリティ検査行列で，列と行の非零要素数はそれぞれ $l = 3, r = 6$ である．復号処理は最大繰り返し回数を 500 回とした同時更新型 sum-product 復号を用いた．また比較のため，ランダム誤りに対する誤り訂正符号として一般に用いられる BCH (Bose-Chaudhuri-Hocquenghem) 符号 [3] の結果も図 4 に示す．BCH 符号は長さが 1023 ビットで設計距離 103（訂正可能ビット数 51 ビット）の符号を用い，符号長および伝送速度が評価する LDPC 符号と同等になるようにした．

図 4 をみると，シンボル反転確率が 0.06 のとき，BCH 符号の復号誤り率はほぼ 1 となってしまうのに対し，LDPC 符号の復号誤り率は $\dfrac{1}{100}$ を達成していることがわかる．

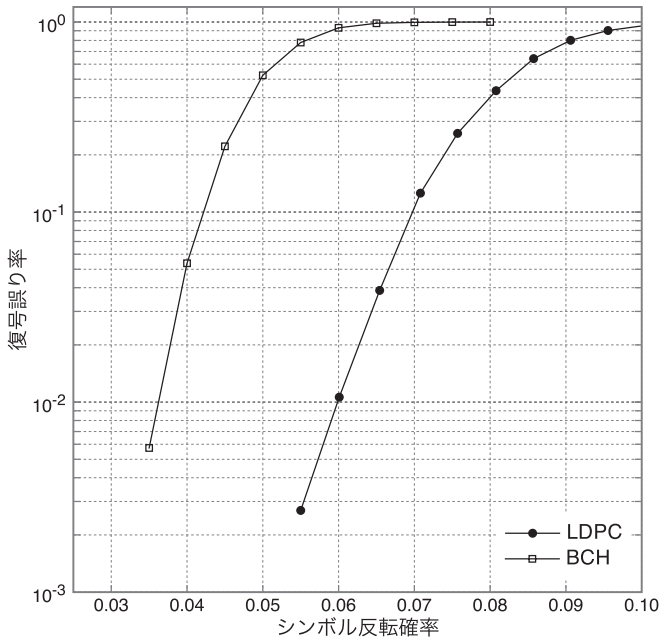


図 4：2 元対称通信路における復号誤り率に関する数値実験結果

8　むすび

本稿では，確率推論の観点から最適な最大事後確率復号が，分配則を用いることで効率良く実行できることを紹介し，具体的な復号アルゴリズムである sum-product 復号を与えた．さらに sum-product 復号によって精度の高い最大事後確率が計算できるパリティ検査行列の構成として，LDPC 符号のような疎なパリティ検査行列が与えられることを述べた．

本稿は直感的な理解が得られるよう，厳密な定理や証明を与えるよりは，例を通してそのエッセンスを紹介した．本稿を読んで LDPC 符号に興味を持たれた方は文献 [4, 5] を参照することで，より深い知識を得ることができるだろう．また，LDPC 符号に関わる深い数理に興味がある方は文献 [6] を参照することをおすすめする．一方，数理的な内容よりも符号の設計手法や復号アルゴリズムなど，実用的なトピックに興味がある方は，文献 [7] が参考になるであろう．

参考文献

[1] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, 1948.

[2] R. G. Gallager, *Low-density parity-check codes*. MIT Press, 1963.

[3] S. Lin and D. J. Costello, *Error Control Coding*. Prentice Hall, 2nd ed., 2004.

[4] 和田山 正，**誤り訂正技術の基礎**．森北出版，2010.

[5] 萩原 学，**符号理論 デジタルコミュニケーションにおける数学**．日本評論社，2012.

[6] T. J. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[7] W. E. Ryan and S. Lin, *Channel Codes: Classical and Modern*. Cambridge University Press, 2009.

デリバティブ取引とリスク管理
―数学の実務への展開―

新長　義己

三菱 UFJ モルガン・スタンレー証券株式会社
市場商品本部

1　はじめに

数学の専門家でも学者でもない私が（そもそも「理科系」の学部の卒業生でもない）このような場に文章を書くのははなはだ気がひけるのだが、数学の専門家でなくとも数学の成果を使わざるを得ない、という事実を知ってもらうだけでも意味があるかと思い、執筆させていただくことにした。本稿は 2011 年 7 月に九州大学で行った講演の原稿を要約・修正したものだが、文章の執筆にあたっては、当社フィナンシャルエンジニアリング部吉岡明広氏、市場商品統括部畠篤史氏の助言と協力をいただいたことを予めお断りしておくとともに両氏にこの場を借りて深く感謝申し上げる。

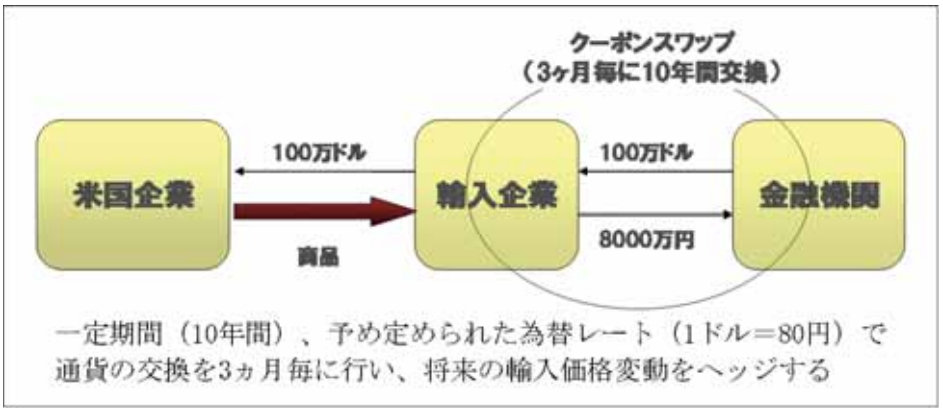
金融業界では個々の取引のリスク評価から会社全体が保有するリスクの評価にいたるまで、さまざまなリスクの計測と管理が数学・統計学の手法を用いて行われるようになっている。こうした技術は、デリバティブ取引の実用化の歴史とともに成長してきた。まず、デリバティブ取引とは何か、から話を始めたいと思う。

2　デリバティブ取引

デリバティブとは金融・ファイナンスの世界で、株・金利・為替などのさまざまな商品（原資産）の価値や値などにより、相対的にその価値が求められる金融商品や契約の総称であり、金融派生商品ともいう。その発想自体はかなり昔から存在しており、古代ギリシャにおいてオリーブ圧搾機を借りる権利に関してオプション取引がなされていたという話があるし、また、17 世紀のオランダのチューリップの球根市場がオプション取引の原型であるといわれているほか、18 世紀の江戸時代、大阪の堂島で米商人たちが行っていた米の売買価格を収穫前に決める取引（帳合米取引（ちょうあいまいとりひき））が先物取引の原型である、といった説がある。いずれにしても、ある現物の取引の価格を基にして、その価格の動きにリンクする商品や取引を作り出す、という発想は相当に古くから存在する。

さて、デリバティブ取引はさまざまな金融取引や商品などの相場変動によるリスクを回避（ヘッジ）するために開発された。以下にごく簡単なデリバティブ取引の例をあげる。これは、

日本の輸入企業が（すなわちホームカレンシーが円である企業）が、クーポンスワップというデリバティブ取引によって為替リスクをヘッジする例である。



上記の例では、米国企業から商品を買ってドルを支払う（図の左側）契約を持っている輸入企業が、金融機関とドルを受け取って円を支払う契約を結ぶ（図の右側）ことによって実質的にドルの支払いを円に転換している。

まず図の左側の「商品を買ってドルを支払う」という経済活動は、この企業にとってリスクを持つものである。なぜなら、（図には描いていないが）この企業はドルで買った商品を日本で売却して円を受け取る。支払いの通貨と受取りの通貨が違うわけだから、ここに為替リスクが存在している。次に、図の右側の取引はドルを受け取って円を払う、という為替リスクそのものの取引である。これを左側の取引と合わせることで、ドルのキャッシュフローが相殺され、あたかもホームカレンシーである円だけで取引をしたかのような効果が残る。

このように、デリバティブ取引とは、実物資産の取引（図の左側）に内在するリスクだけを抽出して商品化したもの（図の右側のクーポンスワップ）、ともいえる。

デリバティブ取引はリスクを回避するリスクヘッジの手段として用いられるが、気をつけなければいけないのは、「ヘッジ」とは、ある特定のリスクに対して、そのリスクの持つ方向（円高に入ったら損をする、とか、株が下がったら損をする、という「方向」）と逆向きのリスクをぶつけることで相殺するだけであり、もともと存在するリスクがなくなってしまうわけではない。要するに、あるベクトルに対してそれとは逆向きのベクトルを合成してできるだけゼロに近づけよう、とするものだから、合成するベクトルの量が多すぎたり、向きがずれていたりしたら、別のリスクを抱えてしまうことになってしまう。だから、デリバティブの取引を行ったり管理したりする際には、そのリスクをさまざまな角度から分析し計量化することが求められるのである。

繰り返すが、デリバティブとは原資産に内在するリスクを抽出して商品化したもので、リスクそのものともいえる。だから、逆向きのリスクにぶつければヘッジになるが、このリスクを運用商品（債券や株式など）に組み込めば、原資産では実現できない経済性を作り出すことが可能である。一種類だけでなくいろいろな種類のリスクを自由に組み合わせることができるから、運用商品の設計にデリバティブは幅広く利用されている。

3　デリバティブの評価

デリバティブとはリスクを計量化して商品化したものだと述べたが、次にデリバティブの評価の基本的な考え方について触れることにする。

デリバティブは、一部の例外を除いてその契約ごとの価格を市場で直接観測することは難しい（一部の例外とは、流動性の高い上場先物取引や、市場である程度定型化された金利スワップなどである）。デリバティブの評価とは、市場では（頻繁には）流通しないものをどうやって体系的に評価するかという課題である。特に、オーダーメード的に組成される複雑なデリバティブ商品の価格は市場では観測されない。

そこで、「今後の市場はこう動く」という仮説を（すなわち、原資産が従う確率過程を確率微分方程式として）モデル化する。それによって将来価値の期待値を計算し、欲しいデリバティブの商品価格とする。

例えば、株価がブラック・ショールズモデルに従うと仮定する場合、株価 $S(t)$ は次の確率微分方程式 $dS(t)/S(t) = \mu\, dt + \sigma\, dW(t)$ に従う。ここで、μ（ドリフト項）と σ（ボラティリティ）はモデルパラメータ（定数）であり、$W(t)$ は標準ブラウン運動である。μ は市場で観測できる金利及び株価配当から、σ は当該株価（もしくは類似商品）の変動率から推定される。

このようにして得られるモデルは決して普遍的なものではなく、ビジネスの前提や市場環境の変化に応じてより適切なものに変更していく必要がある。

いくつか例を挙げると、円の金利が 5%ぐらいあった時に使えたモデルは、今（短期金利はほとんどゼロである）の環境下では、マイナス金利になる可能性を大きく見積もり過ぎてしまうこともある（市場環境の変化への対応）。従来は株や為替を原資産とするデリバティブでは金利の変動性による評価への影響はあまり深刻には考えられていなかったが、超長期（たとえば 30 年ものなど）の商品が流行した結果、それも無視できないものとなった（商品性の拡張）。また、年に数件しか取引がなかったものが、相場の好転などで取引が活発化し、年に数千件も取引をされるようになると、最初は簡易なモデルでも許容されていたものが高い精度を求められるようになる（ビジネスの拡大による精緻化の要請）。このように、今使えているモデルが将来も使えるわけではなく、市場との適合性を定期的に検証しながらモデルを修正していくことが求められる。

4　技術的な発展

デリバティブ商品の開発に伴う技術は、モデルの市場適合性向上と価格算出における数値計算手法の精緻化を通じて発展してきた。

デリバティブの黎明期においては、原資産が対数正規分布に従うと仮定したブラック・ショールズモデルや、原資産が正規分布に従うと仮定したガウシアンモデルを用いて、価格が解析的に計算できる商品を中心に開発が行われた。解析解を用いることの利点は、価格計算が高速な点、また、トレーダーがリスクコントロールの際に用いる、デリバティブ評価の原資産等への感応度を示すグリークスと呼ばれる数値が、差分や微分により安定的に計算できる点にある。

1990年代になり、複雑なキャッシュフローを持つ商品や経路依存性が高い商品のように、解析的には価格計算できない商品が主流になるのに伴って、格子法や有限差分法、モンテカルロ法などの数値計算手法の開発が進むことになる。

もう少し具体的にみるために、金利のモデル化を例にとろう。金利には為替や株と異なり、期間構造がある。つまり、1年物金利、2年物金利、…、10年物金利、…、20年物金利、…というように期間毎に金利が異なっている。このとき、期間毎の金利を個別ファクターと捉え、それらの変動を相関も反映した形で定式化できれば、後はモンテカルロ法を用いて、金利を原資産とするデリバティブ商品の価格を計算することができるだろう。しかしながら、ファクター数が多い場合、高い収束精度の価格を得るために必要な計算時間も多くなり、結果として、トレーダーが要求する計算速度と計算精度を同時に実現することは、1990年代後半当時のコンピュータ処理速度の下では困難であった。そのため、当時は、商品の価格計算に必要な市場変動の特性をなるべく少ないファクター数で適切に表現できるモデルを構築することが実務の中心となった。また、グリークスは差分により計算されるが、少ないファクター数のモデルであれば、モンテカルロ法よりも安定的な数値が得られる格子法や有限差分法もよく使用されていた。

2000年代に入り、デリバティブ市場が一層発展してくると、従来の単純なモデルでは合理的な説明が困難な市場データが多く観測されるようになり、より現実に即した、複雑なモデルの開発が必要となってきた。また、仕組債や仕組預金のビジネスが活況となり、商品が更に多様化、長期化、複雑化する中、格子法や有限差分法では対応が難しい、多くの資産に依存する商品も出現してくるようになる。この状況下、早期償還条項（すなわち最適停止問題）を持つ商品の価格計算に適用できる最小二乗モンテカルロ法の開発や、準乱数を用いた価格収束性の向上など、モンテカルロ法の計算効率向上のための技術革新が行われた。また、分散コンピューティング技術の発達やXML活用によるシステム間連携の効率化、取引明細記述言語の発展などITも含めた技術の発展もあって、今では多くの商品がモンテカルロ法で価格計算されるようになっている。また、従来は差分計算されていたグリークスも、より安定的で高い精度が得られる手法により計算されている。

モデルの市場適合性向上と価格算出における数値計算手法の精緻化は、各々の金融機関の市場競争力強化に直結するため、今後も引き続き、切磋琢磨が行われていくであろう。

5　新しい問題

当然のことながら、経済環境・金融環境が時代とともに変化していく以上、金融技術もそれに応じて変化・成長していかなければならない。言い方を変えると、経済環境の変化によって従前はなかったリスク、あるいは微少なリスクとしてこれまでは無視してきたリスクが顕在化してきた場合、金融市場に参加する者はそれに適切に対応していかなければならない。リーマンショック後の市場において以前よりもより強く意識されるようになったリスクとして、カウンターパーティリスクがあげられる。

デリバティブの評価ロジックを構築する基本概念の一つに無リスク金利（リスクのない資産から得ることができる利回り）というのがあり、従来デリバティブの評価では、LIBOR（London

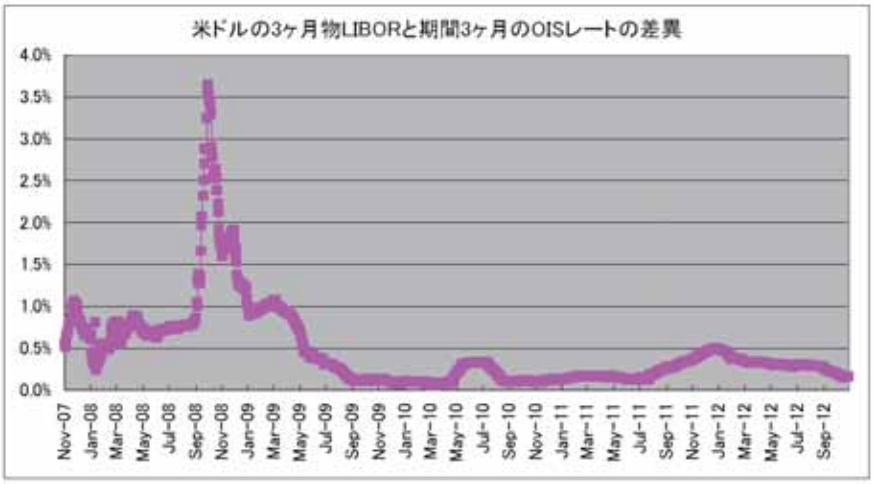
Interbank Offered Rate：ロンドン銀行間取引金利）を実務上無リスクの金利として利用してきた。「LIBORは無リスクの金利である」という考え方はLIBORの取引主体である銀行は破綻しない、ということを前提としていた。ところがリーマンショック前後からデリバティブの取引相手である金融機関の破綻が現実のものとなり、LIBORは無リスクの金利ではなく、「LIBOR＝無リスク金利＋銀行の破綻リスク」であることが認識された。例えば、一定期間の間、固定金利と変動金利を交換する金利スワップという取引がある。2年物金利や5年物金利といった固定金利と将来の各時点で決定される（つまり変動する）3ヶ月物や6ヶ月物の短期金利を交換するものである。従前は3ヶ月物LIBORと6ヶ月物LIBORとの金利差は単に金利の期間構造と捉えられていたものが、実は受渡し期間の差によるカウンターパーティリスクを内包したものということになる。LIBORは3ヶ月とか6ヶ月といった期間の資金の貸し借りの金利であり、その期間の間に相手方が倒産しているかもしれない（というリスクがある）。こうした新しい認識から、新たな無リスク金利の指標としては無担保オーバーナイト翌日物金利と固定金利を交換するOvernight Index Swap（以下OIS）をベースとして求める手法が標準化されつつある。これを総じてOISディスカウントと言う。オーバーナイト翌日物は今日借りて明日返す取引なのでカウンターパーティリスクは最も低いはずである（全くないわけではないが）。

グラフ1は、米ドルの3ヶ月物LIBORと期間3ヶ月のOISレートの差異（以下、LIBOR-OISスプレッド）のヒストリカルデータである。リーマンショックの時期、銀行の破綻懸念が増大したが、それはLIBOR-OISスプレッドの拡大という形で市場に反映されていることが分かる。

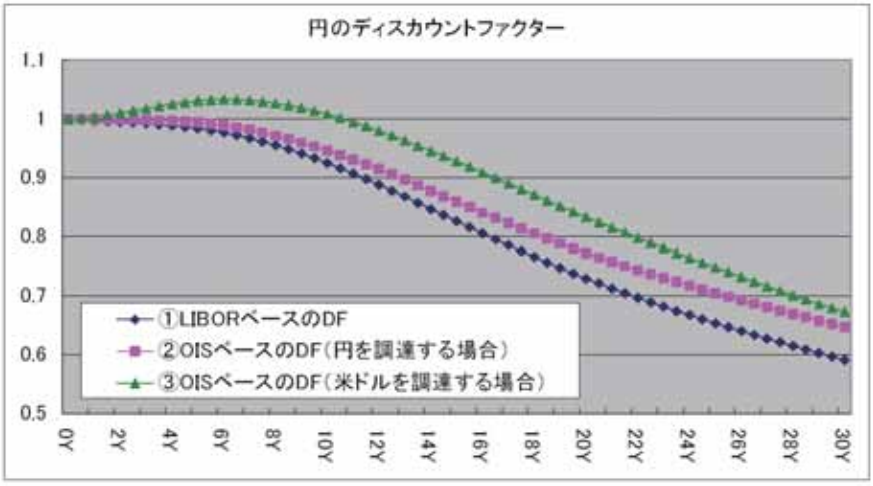
無リスク金利の指標がLIBORベースからOISベースに変わることの影響を、もう少し具体的に見てみよう。その前に、ディスカウントファクター（以下DF）という概念を紹介する。ディスカウントファクターとは、将来時点の1円を現在時点に換算すると何円になるか、という比率のことである。グラフ2は、①円LIBORベースのDF、②円OISベースのDF（円を調達する場合）、③円OISベースのDF（米ドルを調達する場合）を比較したものである。一般には、OISの方がLIBORよりも金利が低いため、OISベースのDFの方がLIBORベースのDFよりも大きくなる。また、③をみると、DFが1を超えている期間があることに気づく。これは、米ドルを調達し、それを通貨スワップで円に交換して運用した場合、マイナス金利が発生することを示している。

OISディスカウントの適用は従前の評価モデルの前提を根底から変更することであり、全てのデリバティブの評価やリスク管理に大きな影響を与えるものである。ただ、OISディスカウントがデリバティブ評価の標準となる、といっても、3ヶ月や6ヶ月のLIBORをベースとした従来型のデリバティブが市場からなくなることを意味するわけではない。なぜなら、デリバティブをヘッジとして利用する事業会社などの最終利用者は、金融市場に恒常的に参加する金融機関とは異なりオーバーナイト取引で自社の資金調達をまかなっているところなどはほとんどなく、例えば3ヶ月や6ヶ月といった期間での資金調達を主に行っているからである。最終利用者のキャッシュフローがその単位なのであれば、市場でもそれに合った商品は生き残る。大事なことはLIBORをベースにする取引が内包するリスクを計量化（認識）し、個々の取引の価格（評価）に反映させ、さまざまなリスク指標を算出して日々管理していくことである。

近年顕著になってきたカウンターパーティリスクの顕在化への対応のもうひとつの例とし



グラフ 1（米ドルの LIBOR-OIS スプレッドのヒストリカルデータ、出所：Bloomberg）



グラフ 2（円のディスカウントファクターの比較）

て Credit Value Adjustment（以下 CVA）がある。

CVA とは、カウンターパーティが倒産するリスクを金融取引の価格や評価に織り込むことといって良い。デリバティブ取引は、それを約定した時点での評価は、その時点での市場価格をベースに取引されたのであれば、本来ゼロである。それが時間の経過とともに市場価格が変化することに伴って正の価値（含み益の状態）や負の価値（含み損の状態）を持つことになる。その取引が正の価値を持っている時にカウンターパーティが倒産すれば、得られるべき利益を得られないことから損失をこうむることになる（デリバティブ取引も有担保が通常なので、正確には担保でもカバーされない場合、ということになる）。この経済価値を取引価格の算定や評価に織り込むことが CVA である。欧米では金融機関に対してすでにこの CVA 相当額の会

計報告が義務付けられている。

CVA はカウンターパーティの倒産の可能性を取引の評価に織り込むものであるから、その取引相手ごとに CVA を集計する必要がある。いろいろな種類の取引を「取引先」という別の切り口で集計するわけだから、金利や為替、株式といった異なる複数の資産をベースとするデリバティブを同一の前提の上で考える必要がある。デリバティブの評価は商品の開発とともに発展してきた歴史から、原資産が異なれば別々にモデル化されていることのほうが普通であるが、CVA を適用するには金利・為替・株式といったそれぞれ性質の異なるリスクを整合的に包含するモデルを構築しなければならない。その結果モデルがより一層複雑化し、単純に適用すると時価評価やリスク計測に膨大なコンピューターリソースが必要となる。多くの金融機関は既にデリバティブ関連でスーパーコンピュータ並みの設備での計算処理を日々行っているが、更なる投資は大幅なコスト負担となってしまう。もちろん、全くの負担なしにより高度なリスク管理を行うのは無理な話ではあるが、より効率的な計算手法の開発と同時に情報処理技術側からのアプローチが要求されるチャレンジングな課題である。

6　最後に

デリバティブ商品の開発に伴って発展してきた金融技術であるが、いまはむしろ個々の商品を開発するというよりも、前章で述べたように会社が負っているリスクを分析し計量化することにウェイトをおいているように見える。いまの市場環境がリスクを取るよりもリスクを回避する流れにあることが背景にあると感じている。

今後、市場環境や社会環境がどちらの方向に向かうにせよ、リスクをいろいろな角度から分析し、計量化することの重要性は変わらない。リスクを計量化することによって、そのリスクを取引し、管理することが可能になるからである。それを支えているのが数学であり IT を含めた技術力なのである。

参考文献

本稿を通じ金融工学に御興味を持たれた方に、御参考までに当社もしくはその前身にて、第一版から日本語訳を行っている金融工学の入門書を紹介する。

ジョン　ハル『フィナンシャルエンジニアリング　第 7 版』三菱 UFJ 証券市場商品本部訳、金融財政事情研究会、2009

また、数学者ではなく物理学者の話で恐縮であるが、物理学者が金融の世界に飛び込み奮闘する様を赤裸々に綴った、次の本も興味のある方はご一読頂ければと思う。

エマニュエル　ダーマン『物理学者、ウォール街を往く。』森谷博之他訳、東洋経済新報社、2005

最後に大学院修士課程や博士課程にて数学等を履修し、当社にモデル開発担当候補として入社する社員に最初に学習させている本を紹介する。

S. E. シュリーブ『ファイナンスのための確率解析 I』『同 II』長山いずみ他訳、丸善出版、2012

編集後記

本書「科学・技術の研究課題への数学アプローチ」（通称 手引き）はどのような数学が他分野・産業に貢献しているか、今後貢献する可能性があるかを紹介することを目的としました。読者としては、高学年の大学生、大学院生、および企業の方を想定しています。基礎編、応用編の 6 責任者と編集担当者が編集委員となり、マス・フォア・インダストリ研究所 (IMI) の全教員および IMI と繋がりのある企業の方に寄稿をお願いしました。IMI 全教員が執筆することにこだわったのは、本書を各教員の研究紹介の拡大版ととらえているためです。今後いろいろな場面で（たとえば企業との共同研究のため、教員のバックグラウンドを知ってもらう）本書を活用してほしいものです。ご多忙の中で原稿を書き上げてくださった企業人の方々に厚くお礼を申し上げます。

最初の原稿提出締め切りは 2012 年 11 月 16 日でした。危惧されていた通り、原稿の集まりが悪く、バナナの叩き売り状態で締め切りの延長に継ぐ延長、督促に継ぐ督促でした。印刷業者に記事を渡す翌年 2 月 12 日朝にようやく全教員の記事が集まりました。全教員参加をあきらめかけていましたが、達成できたことはうれしい限りです。

そろった原稿を読むと、いまさらですが数学のダイナミックレンジの広さと、他分野・産業への応用可能性を再認識することができます。本書の発行目的は達成されたのではないかと自画自賛しています。本書や個々の記事をいろいろな場面で活用していただくことを希望します。

なお本書の英語版も予定しています。お気づきの点があれば、著者にご連絡くださいますよう、よろしくお願いします。

編集委員長　　西井 龍映

MI レクチャーノートシリーズ刊行にあたり

本レクチャーノートシリーズは、文部科学省 21COE プログラム「機能数理学の構築と展開」(H.15-19 年度) において作成した COE Lecture Notes の続刊である。 今後、レクチャーノートは、文部科学省大学院教育改革支援プログラム「産業界が求める数学博士と新修士養成」(H19-21 年度) および、新しく採択された同グローバル COE プログラム「マス・フォア・インダストリ教育研究拠点」(H.20-24 年度) の推進において招聘する国内外の研究者による講義の講義録として出版するものである。

平成 20 年 7 月
グローバル COE プログラム
マス・フォア・インダストリ教育研究拠点
拠点リーダー　若山正人

科学･技術の研究課題への数学アプローチ

―数学モデリングの基礎と展開―

発　行　　2013年2月28日
編　集　　西井龍映（委員長），栄伸一郎，岡田勘三，落合啓之，
小磯深幸，斎藤新悟，白井朋之
発　行　　九州大学マス・フォア・インダストリ研究所
九州大学大学院数理学研究院
グローバル COE プログラム「マス・フォア・インダストリ教育研究拠点」
〒819-0395 福岡市西区元岡744
九州大学伊都キャンパス数理学研究教育棟 GCOE 事務室
TEL 092-802-4404　FAX 092-802-4405
URL http://gcoe-mi.jp/

印　刷　　城島印刷株式会社
〒810-0012 福岡市中央区白金 2 丁目 9 番 6 号
TEL 092-531-7102　FAX 092-524-4411

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note	Mitsuhiro T. NAKAO Kazuhiro YOKOYAMA	Computer Assisted Proofs - Numeric and Symbolic Approaches - 199pages	August 22, 2006
COE Lecture Note	M.J.Shai HARAN	Arithmetical Investigations - Representation theory, Orthogonal polynomials and Quantum interpolations- 174pages	August 22, 2006
COE Lecture Note Vol.3	Michal BENES Masato KIMURA Tatsuyuki NAKAKI	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2005 155pages	October 13, 2006
COE Lecture Note Vol.4	宮田　健治	辺要素有限要素法による磁界解析 - 機能数理学特別講義 21pages	May 15, 2007
COE Lecture Note Vol.5	Francois APERY	Univariate Elimination Subresultants - Bezout formula, Laurent series and vanishing conditions - 89pages	September 25, 2007
COE Lecture Note Vol.6	Michal BENES Masato KIMURA Tatsuyuki NAKAKI	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2006 209pages	October 12, 2007
COE Lecture Note Vol.7	若山　正人 中尾　充宏	九州大学産業技術数理研究センター キックオフミーティング 138pages	October 15, 2007
COE Lecture Note Vol.8	Alberto PARMEGGIANI	Introduction to the Spectral Theory of Non-Commutative Harmonic Oscillators 233pages	January 31, 2008
COE Lecture Note Vol.9	Michael I.TRIBELSKY	Introduction to Mathematical modeling 23pages	February 15, 2008
COE Lecture Note Vol.10	Jacques FARAUT	Infinite Dimensional Spherical Analysis 74pages	March 14, 2008
COE Lecture Note Vol.11	Gerrit van DIJK	Gelfand Pairs And Beyond 60pages	August 25, 2008
COE Lecture Note Vol.12	Faculty of Mathematics, Kyushu University	Consortium “MATH for INDUSTRY” First Forum 87pages	September 16, 2008
COE Lecture Note Vol.13	九州大学大学院 数理学研究院	プロシーディング「損保数理に現れる確率モデル」 ― 日新火災・九州大学 共同研究 2008 年 11 月 研究会 ― 82pages	February 6, 2009

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.14	Michal Beneš, Tohru Tsujikawa Shigetoshi Yazaki	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2008 77pages	February 12, 2009
COE Lecture Note Vol.15	Faculty of Mathematics, Kyushu University	International Workshop on Verified Computations and Related Topics 129pages	February 23, 2009
COE Lecture Note Vol.16	Alexander Samokhin	Volume Integral Equation Method in Problems of Mathematical Physics 50pages	February 24, 2009
COE Lecture Note Vol.17	矢嶋　　徹 及川　正行 梶原　健司 辻　　英一 福本　康秀	非線形波動の数理と物理 66pages	February 27, 2009
COE Lecture Note Vol.18	Tim Hoffmann	Discrete Differential Geometry of Curves and Surfaces 75pages	April 21, 2009
COE Lecture Note Vol.19	Ichiro Suzuki	The Pattern Formation Problem for Autonomous Mobile Robots —Special Lecture in Functional Mathematics— 23pages	April 30, 2009
COE Lecture Note Vol.20	Yasuhide Fukumoto Yasunori Maekawa	Math-for-Industry Tutorial: Spectral theories of non-Hermitian operators and their application 184pages	June 19, 2009
COE Lecture Note Vol.21	Faculty of Mathematics, Kyushu University	Forum “Math-for-Industry” Casimir Force, Casimir Operators and the Riemann Hypothesis 95pages	November 9, 2009
COE Lecture Note Vol.22	Masakazu Suzuki Hoon Hong Hirokazu Anai Chee Yap Yousuke Sato Hiroshi Yoshida	The Joint Conference of ASCM 2009 and MACIS 2009: Asian Symposium on Computer Mathematics Mathematical Aspects of Computer and Information Sciences 436pages	December 14, 2009
COE Lecture Note Vol.23	荒川　恒男 金子　昌信	多重ゼータ値入門 111pages	February 15, 2010
COE Lecture Note Vol.24	Fulton B.Gonzalez	Notes on Integral Geometry and Harmonic Analysis 125pages	March 12, 2010
COE Lecture Note Vol.25	Wayne Rossman	Discrete Constant Mean Curvature Surfaces via Conserved Quantities 130pages	May 31, 2010
COE Lecture Note Vol.26	Mihai Ciucu	Perfect Matchings and Applications 66pages	July 2, 2010

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.27	九州大学大学院 数理学研究院	Forum “Math-for-Industry” and Study Group Workshop Information security, visualization, and inverse problems, on the basis of optimization techniques 100pages	October 21, 2010
COE Lecture Note Vol.28	ANDREAS LANGER	MODULAR FORMS, ELLIPTIC AND MODULAR CURVES LECTURES AT KYUSHU UNIVERSITY 2010 62pages	November 26, 2010
COE Lecture Note Vol.29	木田　雅成 原田　昌晃 横山　俊一	Magma で広がる数学の世界 157pages	December 27, 2010
COE Lecture Note Vol.30	原　　隆 松井　　卓 廣島　文生	Mathematical Quantum Field Theory and Renormalization Theory 201pages	January 31, 2011
COE Lecture Note Vol.31	若山　正人 福本　康秀 高木　　剛 山本　昌宏	Study Group Workshop 2010 Lecture & Report 128pages	February 8, 2011
COE Lecture Note Vol.32	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2011 “TSUNAMI-Mathematical Modelling” Using Mathematics for Natural Disaster Prediction, Recovery and Provision for the Future 90pages	September 30, 2011
COE Lecture Note Vol.33	若山　正人 福本　康秀 高木　　剛 山本　昌宏	Study Group Workshop 2011 Lecture & Report 140pages	October 27, 2011
COE Lecture Note Vol.34	Adrian Muntean Vladimír Chalupecký	Homogenization Method and Multiscale Modeling 72pages	October 28, 2011
COE Lecture Note Vol.35	横山　俊一 夫　　紀恵 林　　卓也	計算機代数システムの進展 210pages	November 30, 2011
COE Lecture Note Vol.36	Michal Beneš Masato Kimura Shigetoshi Yazaki	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2010 107pages	January 27, 2012
COE Lecture Note Vol.37	若山　正人 高木　　剛 Kirill Morozov 平岡　裕章 木村　正人 白井　朋之 西井　龍映 栄　伸一郎 穴井　宏和 福本　康秀	平成 23 年度 数学・数理科学と諸科学・産業との連携研究ワークショップ　拡がっていく数学　～期待される “見えない力” ～ 154pages	February 20, 2012

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.38	Fumio Hiroshima Itaru Sasaki Herbert Spohn Akito Suzuki	Enhanced Binding in Quantum Field Theory 204pages	March 12, 2012
COE Lecture Note Vol.39	Institute of Mathematics for Industry, Kyushu University	Multiscale Mathematics: Hierarchy of collective phenomena and interrelations between hierarchical structures 180pages	March 13, 2012
COE Lecture Note Vol.40	井ノ口順一 太田　泰広 筧　　三郎 梶原　健司 松浦　　望	離散可積分系・離散微分幾何チュートリアル 2012 152pages	March 15, 2012
COE Lecture Note Vol.41	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2012 “Information Recovery and Discovery” 91pages	October 22, 2012
COE Lecture Note Vol.42	佐伯　　修 若山　正人 山本　昌宏	Study Group Workshop 2012 Abstract, Lecture & Report 178pages	November 19, 2012
COE Lecture Note Vol.43	Institute of Mathematics for Industry, Kyushu University	Combinatorics and Numerical Analysis Joint Workshop 103pages	December 27, 2012
COE Lecture Note Vol.44	萩原　　学	モダン符号理論からポストモダン符号理論への展望 107pages	January 30, 2013
COE Lecture Note Vol.45	金山　　寛	Joint Research Workshop of Institute of Mathematics for Industry (IMI), Kyushu University “Propagation of Ultra-large-scale Computation by the Domain-decomposition-method for Industrial Problems (PUCDIP 2012)” 121pages	February 19, 2013