計算機代数学と数式処理システム

東京理科大学 理学部第一部 応用数学科 准教授　鍋島（なべしま）　克輔（かつすけ）

1．はじめに

1 人の人間が数学のすべての分野をカバーすることは不可能であることから，数学の理論をブラックボックスとして利用することができるソフトウェアが望まれている．そのような数学ソフトウェアは一般に数式処理システムといわれており．数学アルゴリズムの寄せ集めである．

数学で『計算』と言うと数値計算を想像する人が多いと思われるが，数式処理システムと言われるソフトウェアは基本的に記号計算を内蔵している数学ソフトウェアのことである．数値計算のみの場合は数値計算ソフトウェアと言う．例えば，『2 次方程式 $2x^2+7x+2=0$ の解を求めよ』という問題があったとする．このとき，数値計算と記号計算の解は異なり次となる．

数値計算の解：　$x=-0.313859338,\ -3.186140661$

記号計算の解：　$x=\dfrac{-7\pm\sqrt{33}}{4}$

数値計算の解は，近似値であり誤差を含む．現実世界では許容誤差というものがありすごく小さい誤差を含んでも建築や家具などのモノづくりにおいては問題ない．記号計算の解は，誤差の無い解であり，$\sqrt{33}$ は，『2 乗すればルートの中にある数 33 になるもの』とソフトウェア内では認識させており，数値としては扱われていない．高等学校までの数学を知っていれば$\sqrt{33}$を，記号 a を用いて $a=\sqrt{33}$ と置くと，$a^2=33$ となるのと同じである．まさしく，$\sqrt{33}$ は内部で記号として扱われている．高等学校ならびに大学では，多くの人が厳密な数学の理論を学んでいる．その理論に誤差は許されておらず，また，証明や計算には記号計算が頻繁に使用されている．数式処理システムは記号計算を用いた数学アルゴリズムの集合体と言える．

筆者は計算機代数と言われる数学の一分野の研究を行っている．計算機代数とは，20 世紀に発達した計算機科学と，昔からある構成的代数が融合した研究分野で，代数算法の設計，解析，実装から応用まで行う分野である．

数学系の学科に所属する多くの学生が経験することであるが，高等学校までの数学が得意で大学に入学したら，大学の抽象的な数学に面食らい『何をやっているのだろうか？』となる．筆者自身もそうなった．今にして思えば，これは無理もないことであり，不変式論で有名なドイツの数学者ゴルタン（Paul Gordan（1837–1912））ですら，抽象的なヒルベルト（David Hilbert（1862–1943））の数学を『ヒルベルトの理論は数学ではない神学である』と言っている．ゴルタンのような数学者ですらそのように感じているので面食らってもしょうがない．

19 世紀までの数学研究のスタイルは『計算』から定理や理論を導き出している．名立たる数学者の名前を冠した定理の裏には膨大な計算が実は隠されている．（具体的に）計算できる数学を扱っているので，彼らは数学を構成的に扱っている．実際に手に取って『計算と言う武器』により数学を“捏ね繰り回していた”ようである．このような数学を本稿では抽象的数学に対して構成的数学と呼ぶようにする．この構成的数学こそが長年為されていた数学のスタイルであるが，19 世紀末から抽象的数学が花開き，それ以降，現代数学は抽象的数学となった．計算機のない時代には，天才でない限り，昔ながらの計算による研究には限度が訪れるのは言うに及ばず，また，問題が複雑になるとなおさらなことである．時が経つにつれ，抽象的数学という武器を手にした人類は，抽象的数学を使った数学研究をすることは必然であり，構成的数学は時代と共に廃れて行ったと思われる．（高等学校までの数学は構成的な数学であるので，教育の場には残っている．）

20 世紀になり抽象的数学からの理論の集積は，グレブナー基底理論のようなアルゴリズムの存在する数学に還元され，計算機の発達と共にその理論は計算機と結びつくようになった．それこそが計算機代数学という新しい数学の研究分野である．実は，計算機代数学は昔ながらの構成的数学（代数学）の現代版なのである．

構成的代数 ＋ 計算機 → 計算機代数

この計算機代数学が目に見える形となったものが数式処理システム（商用ソフトウェアとして，Wolfram Inc. が開発している Mathematica や，Maplesoft Inc. が開発している Maple の 2 つは世界的に有名）である．現在の数式処理システムは，大学数学はもちろん最先端の数学の研究にも耐えられるレベルになっている．

歴史的に，『計算機に数学をさせる方法』や『計算機に論理処理をさせる方法』は自然言語処理や人工知能の分野と深い関係がある．これらの技法を用いれば（人間が補助につけば）90% 以上の大学入試問題は，証明問題を含め計算機で解くことができるようである．これは，今，流行りの機械学習ではなく，まさしく論理的かつダイレクトに問題を解いているのであり，機械学習に頼らない厳密的な手法を実現させている．

本稿では，科学フォーラムの性質上，専門的にならず読者がイメージしやすい，『連立方程式の解法』と『集合制約問題を代数的に解く方法』について例を交えて解説する．

2．連立方程式

大学 1 年の講義『線形代数学』では連立 1 次方程式の解法として吐き出し法を習う．連立 1 次方程式であれば，理系の学生は解けるようになっていると思われる．例えば，連立 1 次方程式として

$$\begin{cases} x-2y+z=0 \\ x+y-z=1 \\ 2x-y+3z=2 \end{cases}$$

を考える．数式処理システム Mathematica には方程式の解を出すコマンドとして **Solve** が存在する．これを用いると $x=\frac{7}{9}$,$y=\frac{5}{9}$,$z=\frac{1}{3}$ となる．**Solve** の内部では，吐き出し法が使われている（と予想される）．第 2 式から第 1 式を引き，第 3 式から第 1 式を引くとそれぞれの結果の式には変数 x が消える．すなわち，今ある式自体にスカラー倍もしくは加減の操作を行い，1 つの式に変数が 1 個だけにすることができれば解が得られる．1 つの式に複数の変数が介在すると解を求めることは難しいが，1 個であれば解を求めることができる．すなわち，変数消去が連立方程式を解く際の鍵である．そのため，連立方程式を解くということは，式のスカラー倍や加減を繰返すことにより，**“解きやすい式”**（1 変数の式）を探し出していることになる．上の連立 1 次方程式の場合，

$$k_1(x-2y+z)+k_2(x+y-z-1)+k_3(2x-y+3z-2)=0 \quad (\text{ただし，}k_1,k_2,k_3\text{ はスカラー})$$

の形で表すことのできる 1 変数の式を見つけること自体が問題を解くことである．実際，$k_1=\frac{2}{9}$，$k_2=\frac{5}{9}$，$k_3=\frac{1}{9}$，のとき，$x=\frac{7}{9}$ が得られ，x の値が求まる．

ここで，大事なことは k_1,k_2,k_3 が値であることである．もちろん，式変形の際において k_1,k_2,k_3 に x,y,z の多項式を代入しても問題なく新たな式が得られるが，それらの式は基本的には役に立たない．なぜなら，元の式が 1 次式なので変数消去をするには 1 次式で十分だからである．

次に，もう少し複雑な連立方程式を考えてみよう．大学 1 年の講義『微分積分学』で，次のラグランジュ（Lagrange）の未定乗数法を習う．

定理（ラグランジュの未定乗数法）
関数 $f(x,y),g(x,y)$ を領域 D で定義された C^1 級関数とする．x,y が条件 $g(x,y)=0$ を満たしながら動くときに，関数 $z=f(x,y)$ が (a,b) で極値をとるとする．(a,b) が $g(x,y)=0$ の特異点でない場合には，次を満たす w が存在する．

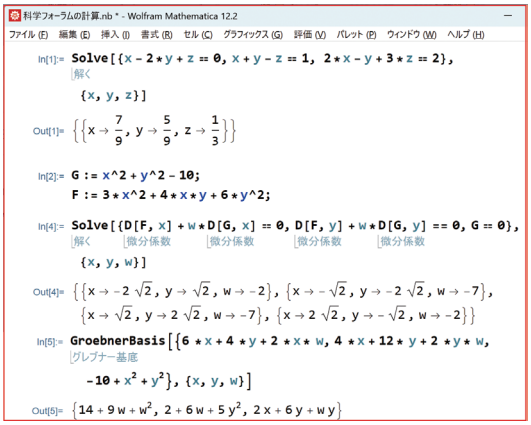
$$\begin{cases} f_x(a,b)+wg_x(a,b) &= 0 \\ f_y(a,b)+wg_y(a,b) &= 0 \\ g(a,b) &= 0 \end{cases}$$

ただし，f_x,g_x は f と g の x についての偏導関数を表し，f_y,g_y は f と g の y についての偏導関数を表す．

これは，条件付き極値問題を解く際に大活躍する定理であるが，この定理では，存在性は言っているが「具体的にどのように連立方程式を解くのか？」は述べていない．例えば，『条件 $x^2+y^2=0$ のもとで，$f(x,y)=3x^3+9x^2y+6y^3$ の極値を求めよ．』という問題において，w を未定乗数とし $g=x^2+y^2-10$ とすると，ラグランジュの未定乗数法より次の連立方程式が得られる．

$$\begin{cases} 6x+4y+2xw &= 0 \\ 4x+12y+2yw &= 0 \\ x^2+y^2-10 &= 0 \end{cases}$$

これは非線形な連立方程式である．連立 1 次方程式と比べれば非線形な連立方程式の難易度は相当高く，



【図】Mathematica の出力

専門家以外は解くことができないと思われる（上の問題は工夫すれば解けるが，更に次数が大きいものは方針すらわからないであろう）．したがって，『解くこと』を考えれば，大学 1 年生の微分積分の教科書にラグランジュの未定乗数法を載せることは適さないと思われるが，『存在性が重要である』と考えれば微分積分の教科書に載せてもいいかなと思われる．

さて，この連立方程式の解を求めるため，数式処理システム Mathematica の **Solve** を用いると，Mathematica は【図】のように解として次を与える．（複合同順）

$$(x, y, \boldsymbol{w}) = \{(\mp 2\sqrt{2}, \pm\sqrt{2}, -2), (\mp\sqrt{2}, \mp 2\sqrt{2}, -7)$$

どのように計算しているのであろうか？

連立方程式を解く鍵は上述したように変数消去である．3 つの式は非線形であるので，次で表される式の中から解きやすい式を探す必要がある．

$$\begin{aligned} &k_1(x, y, \boldsymbol{w})(6x + 4y + 2x\boldsymbol{w}) \\ &\quad + k_2(x, y, \boldsymbol{w})(4x + 12y + 2y\boldsymbol{w}) \\ &\quad + k_3(x, y, \boldsymbol{w})(x^2 + y^2 - 10) \end{aligned}$$

連立一次方程式との違いは，$k_1(x,y,w), k_2(x,y,w), k_3(x,y,w)$ は x,y,w の 3 変数多項式となることである．

解きやすい形の式の集合（定義する必要があるが難しい定義はここでは述べない）のことをグレブナー基底という．グレブナー基底という多項式の集合には変数消去された多項式が含まれており，その式を解くことにより解を得ることができる．これが，連立方程式の解法の概要である．

さて，上の問題に関するグレブナー基底を Mathematica で求めると図の最後の出力となる（コマンドは **GroebnerBasis**）．変数 w のみの式 $w^2+9w+14$ が含まれている．これは，$w^2+9w+14=0$ を意味し，これを解くことによって，$w=-2,-7$ を得ることができる．この値を他の式に代入することにより x,y,w の値も求められる．

連立方程式を解く際に重要となるのは，グレブナー基底であり，グレブナー基底を求めるアルゴリズムは存在すると共に多くの数式処理システムに実装されている．実際，このグレブナー基底が存在するからこそ計算機代数学の分野は大きく発展している．

3．ブール代数と集合制約問題

集合制約問題を連立方程式と見做し代数的に解く方法について紹介する．

まず，必要な記号と定義を導入する．単位元 1 を持ち，加法と乗法が定義され（かつその演算に閉じている）ような集合 $\mathbb{B}$ の任意の元 a が $a^2=a$ を満たすとき $\mathbb{B}$ をブール環という．$\mathbb{F}_2=\{0,1\}$ とし，任意の $a,b\in\mathbb{F}_2$ に対し，加法を $1+1=0,1+0=0+1=1,0+0=0$ と定義し，乗法を $1\cdot 1=1,1\cdot 0=0\cdot 1=0,0\cdot 0=0$ と定義すると，$\mathbb{F}_2$ はブール環となる．次に，$(\mathbb{F}_2)^3$ を考える．(a_1,a_2,a_3)，$(b_1,b_2,b_3)\in(\mathbb{F}_2)^3$ に対し，加法を $(a_1,a_2,a_3)+(b_1,b_2,b_3)=(a_1+b_1,a_2+b_2,a_3+b_3)$，乗法を $(a_1,a_2,a_3)\cdot(b_1,b_2,b_3)=(a_1\cdot b_1,a_2\cdot b_2,a_3\cdot b_3)$ と定義すると，$(\mathbb{F}_2)^3$ もまたブール環となる．

ブール環を $\mathbb{B}$ と表し，任意の $a,b\in\mathbb{B}$ に対し，ブール演算子 $\vee,\wedge,\neg$ を $a\vee b=a+b+a\cdot b, a\wedge b=a\cdot b, \neg a=1+a$ と定義すると，$(\mathbb{B},\vee,\wedge,\neg)$ はブール代数となり，逆に，$+,\cdot$ を $a+b=(\neg a\wedge b)\vee(a\wedge\neg b)$ と $a\cdot b=a\wedge b$ と定義すると，$(\mathbb{B},+,\cdot)$ はブール環となる．ブール代数は，『集合』や『論理』を代数的に取り扱う際に有効であることが知られている．（ここでは，要素でない 1 は集合全体を表し，0 は空集合を表す．）すなわち，集合 A,B において演算 $\cup,\cap$ を $A\cup B=A+B+A\cdot B, A\cap B=A\cdot B$ と定義するとブール代数となる．例えば，$\{a,b,c,d\}$ を要素とし，集合 $A=\{a,b,d\}, B=\{b,c,d\}$ とする．ここで，$\mathcal{P}(\{a,b,c,d\})$ を $\{a,b,c,d\}$ の冪集合（部分集合の集合）とすると，$\mathcal{P}(\{a,b,c,d\})$ は $(\mathbb{F}_2)^4$ と見なすことができる．これは，第 1 成分が 1 なら a を持ち，0 なら a を持たないことを表し，第 2 成分が 1 なら b を持ち 0 なら b を持たない，第 3 成分が 1 なら c を持ち 0 なら c を持たない，第 4 成分が 1 なら d を持ち 0 なら d を持たないことを表す．このとき，$A=(1,1,0,1), B=(0,1,1,1)$ と書くことができるので，$A\cap B$ は $A\cdot B=(1,1,0,1)\cdot(0,1,1,1)=(0,1,0,1)$ と計算すれば $A\cap B=\{b,d\}$ が得られ，$A\cup B$ は，$A+B+A\cdot B=(1,1,0,1)+(0,1,1,$

1)+(0,1,0,1)=(1,1,1,1) とすれば $A\cup B=\{a,b,c,d\}$ が得られる．重要なことは，代数的計算によって集合の演算は計算できることである．

ブール環 $\mathbb{B}$ を係数とする n 変数 $x_1,x_2,\ldots,x_n$ からなる多項式の集合を $\mathbb{B}[x_1,x_2,\ldots,x_n]$ と書き，$x_1^2=x_1,x_2^2=x_2,\ldots,x_n^2=x_n$ となる条件をその多項式の集合に加えた集合を $\mathbb{B}(x_1,x_2,\ldots,x_n)$ と書くようにする．本稿では，$\mathbb{B}(x_1,x_2,\ldots,x_n)$ をブール多項式環と呼ぶ．すなわち，数学の記号で書くと剰余環 $\mathbb{B}[x_1,x_2,\ldots,x_n]/\langle x_1^2-x_1,x_2^2-x_2,\ldots,x_n^2-x_n\rangle$ がブール多項式環である．このとき，任意の $f\in\mathbb{B}(x_1,x_2,\ldots,x_n)$ に対して，$f^2=f$ となることが確かめられるので，$\mathbb{B}(x_1,x_2,\ldots,x_n)$ はブール環である．

具体的な集合制約問題として次の簡単な問題をブール多項式上で考え問題を解く．

問題：ある高等学校の体育祭で 2 年生の出場する種目は，学級対抗リレー，障害物競走，騎馬戦，二人三脚である．2 年 A 組の 40 人のうち s_1,s_2,s_3,s_4 さんの 4 人の種目がまだ決まっていない．生徒の性別は s_1,s_2 は女，s_3,s_4 は男で，各生徒の要望は以下である．
s_1 の希望：二人三脚，s_1 の不得意種目：リレー，
s_2 の希望：障害物競走，s_2 の不得意種目：二人三脚，
s_3 の希望：騎馬戦，s_3 の不得意種目：騎馬戦，
s_4 の希望：学級対抗リレー，s_4 の不得意：二人三脚，
種目については次の条件がある．

○障害物競走は女のみ，
○騎馬戦は男のみ，
○リレーと二人三脚は男女が出場可能，

以上の条件で，種目の振り分けはどのようになるか？

まず，問題を整理するため記号を設定する．a をリレー，b を障害物競走，c を騎馬戦，d を二人三脚の集合とする．また，we を女の集合，ma を男の集合，hr を a を希望している生徒の集合，hs を b を希望している生徒の集合，hk を c を希望している生徒の集合，hn を d を希望している生徒の集合とする．

問題を集合表記の式で書くと次となる．

$ma\cup we=\{s_1,s_2,s_3,s_4\},s_1,s_2\in we,s_3,s_4\in ma,ma\cap we=\emptyset,b\subset we,c\subset ma,s_1\notin a,s_2\notin d,s_3\notin c,s_4\notin d,s_1\in hn,s_2\in hs,s_3\in hk,s_4\in hr,a\subset hr,b\subset hs,c\subset hk,d\subset hn.$

次に，$\mathbb{B}=\mathcal{P}(\{s_1,s_2,s_3,s_4\})$ とし $\mathbb{B}(ma,we,hn,hs,hk,hr,a,b,c,d)$ のブール多項式環上の多項式として集合の関係式を表すと次となる．（ただし，=0 の記述は省略している．）

$ma+we+ma\cdot we+\{s_1,s_2,s_3,s_4\},\{s_1,s_2\}\cdot we+\{s_1,s_2\},\{s_3,s_4\}\cdot ma+\{s_3,s_4\},ma\cdot we,b\cdot we+b,c\cdot we+c,\{s_1\}\cdot a,\{s_2\}\cdot d,\{s_3\}\cdot c,\{s_4\}\cdot d,\{s_1\}\cdot hn+\{s_1\},\{s_2\}\cdot hs+\{s_2\},\{s_3\}\cdot hr+\{s_3\},\{s_4\}\cdot hk+\{s_4\},a\cdot hr+a,b\cdot hs+b,c\cdot hk+c,d\cdot hn+d.$

これを連立方程式と見做すことにより，集合制約問題を解く．連立方程式を解く鍵は変数消去であったので，$\mathbb{B}(ma,we,hn,hs,hk,hr,a,b,c,d)$ 上のグレブナー基底（正確にはブーリアン・グレブナー基底）が役に立つ．上の連立方程式のグレブナー基底を数式処理システム Risa/Asir で計算すると次を出力する．

```
[1*ma+[s3,s4],1*we+[s1,s2],1*hn+([s1,s2,s4]+1)*d+[s1],[s1]
*hs*b+[s1]*b,[s2]*hs+[s2],[s4]*hk+[s4],([s1,s3]+1)*hr*a+
([s1,s3]+1)*a,[s3]*hr+[s3],[s1]*a,([s1,s2]+1)*b,([s4]+1)*c,
[s1,s2,s4]*d+[s1]]
```

ここで，[s1,s2,s4]*d+[s1]は $\{s_1,s_2,s_4\}\cap d=\{s_1\}$ を意味しており，a,b,c,d はシングルトンということなので $d=\{s_1\}$ を得る．また，([s4]+1)*c は $\{s_1,s_2,s_3\}\cap c=\emptyset$を意味しているので，$c=\{s_4\}$ または空集合となるが，c は空集合ではないので，$c=\{s_4\}$ となる．([s1,s2]+1)*b は，$\{s_3,s_4\}\cap b=\emptyset$を意味しているので，$b$ の可能性として，$\{s_1\},\{s_2\},\{s_1,s_2\},\emptyset$となるが，シングルトンということと $d=\{s_1\}$ がわかっているので，$b=\{s_2\}$ である．残りは，$a=\{s_3\}$ となる．

もとの連立方程式では解の様相が分からないので加法と乗法を使い，グレブナー基底という形の多項式の集合に変形したことで“情報が読み取りやすい”状況となった．この処理を可能とするのが数式処理システムの強みである．また，代数的な視点から集合制約問題を考えているので，集合制約問題の代数構造についてもそのグレブナー基底から読み取ることができる．

世界的なパズルとして知られている数独は集合制約問題である．上記の手法を用いることにより問題を解くことができる．また，代数的構造を解析することにより数独の難易度を数学的に定義できることが知られている．

現在の数式処理システムには，本稿で取り上げたこと以外に偏微分方程式，スキーム，コホモロジーなど数学に馴染みのものから物理学や電磁気学などたくさんの計算機代数学を利用した処理ツールが存在する．鍋島研究室では，『計算機に高度な数学をさせる』ことを目指し，代数的算法の設計，解析，実装から応用までの研究を行っている．