グレブナー基底と代数多様体

菅崎 賢人

北海道大学大学院理学院数学専攻

2018 年 1 月 31 日

本論文の主な内容

- 多項式連立方程式の解空間をイデアル $\boldsymbol{I}$ のアフィン多様体 $\boldsymbol{V}(\boldsymbol{I})$ として表記し，その性質を調べる.
- イデアルのグレブナー基底を用いて，連立方程式の解の計算や有無が調べられることを証明する.
- 幾何の定理の自動証明に応用する（トレミーの定理を証明する）.

グレブナー基底の方法の歴史

- 1964 年　[局所環上でのグレブナー基底の理論]
  広中平祐が発見．標準基底や Hironaka's standard basis とも呼ばれる．

- 1965 年　[多項式環上のグレブナー基底の理論]
  オーストリアの大学院生ブルーノ・ブッフベルガーが発表,
  彼の指導教授の名前からグレブナー基底と名付けられた．

- [幾何の定理の自動証明]
  実際にコンピュータによって新しい定理群が証明されている．
  近年は人工知能や幾何的造形の研究者に興味を抱かれている．

アフィン多様体

与えられた多項式方程式系に対して，解空間を定義する．

定義 1.1

k を体，$f_1, \ldots, f_s$ を $k[x_1, \ldots, x_n]$ に属する多項式とする．このとき

$$V(f_1, \ldots, f_s) = \{ (a_1, \ldots, a_n) \in k^n \mid 1 \leq \forall i \leq s \\ s.t. \quad f_i(a_1, \ldots, a_n) = 0 \} \subset k^n$$

を $f_1, \ldots, f_s$ で定義されるアフィン多様体という．

- $V(f_1, \ldots, f_s)$ は，$f_1 = \cdots = f_s = 0$ の解空間を意味する．
- 同様にして，イデアル I の共通零点 $V(I)$ が定義される．
- $V(f_1, \ldots, f_s) = V(\langle f_1, \ldots, f_s \rangle)$ が成立する．
- イデアル $\langle f_1, \ldots, f_s \rangle$ の良い基底を選ぶと，解が求めやすくなる．

グレブナー基底

その『良い基底』というのがグレブナー基底である．グレブナー基底を得るにはまず先頭の項に着目して，方程式どうしを計算して次数を下げていく．先頭項や多項式の次数について定義する．

定義 1.2

- $f \in k[x_1, \ldots, x_n]$ の項のうち，ある項の順序付けにおいて最大のものを f の先頭項 (Leading Term) といい，$LT(f)$ と表す．
- $LT(f)$ の次数を表す n 次元ベクトルを f の多重次数という．

グレブナー基底

グレブナー基底を定義する.

定義 1.3

ある項の順序付けで，イデアル I の有限部分集合 $G = \{g_1, \ldots, g_t\}$ が

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$$

を満たすとき，G をグレブナー基底 (標準基底) といい，I の基底をなす.

I のグレブナー基底 $g_1, \ldots, g_t$ は，I の有限基底のうち最も多重次数の下がった組み合わせの一つである.

グレブナー基底

例 1.4

$f_1 = x^3 - 2xy$, $f_2 = x^2y + x - 2y^2$, $I = \langle f_1, f_2 \rangle$ とする.
(x の次数の大きい順に項を並べている.)
$\{f_1, f_2\}$ は I のグレブナー基底となっているのかを調べる.

f_1, f_2 の先頭項は

$$LT(f_1) = x^3, LT(f_2) = x^2y.$$

ここで, $xf_2 - yf_1 = x^2$ もまた I の元だから

$$x^2 = LT(x^2) \in LT(I).$$

しかし x^2 は $\langle LT(f_1), LT(f_2) \rangle = \langle x^3, x^2y \rangle$ に含まれないので

$$\langle LT(f_1), LT(f_2) \rangle \neq \langle LT(I) \rangle .$$

すなわち, この項順序では $\{f_1, f_2\}$ は I のグレブナー基底ではない.

S 多項式

今の例における $xf_2 - yf_1 = x^2$ のように，2 本の多項式の先頭項を消去して次数を下げた式 (先頭の次数を合わせて差し引いたもの) を S 多項式といい，$S(f_1, f_2)$ のように書く．S 多項式を作る操作を繰り返していくことで，グレブナー基底を得ることができる．

例 1.5

$f_1 = x^3 - 2xy, f_2 = x^2y + x - 2y^2, I = \langle f_1, f_2 \rangle$ とする（x の次数の大きい順に項を並べている.） I のグレブナー基底を求める.

$S(f_1, f_2) = x^2 = f_3$, $S(f_1, f_3) = f_1 - xf_3 = -2xy = f_4$,
$S(f_2, f_3) = x - 2y^2 = f_5$, $S(f_4, f_5) = -4y^3 = f_6$ とおく.
残りの S 多項式と f_1, f_2 は，$\{f_3, f_4, f_5, f_6\}$ によって割り切れていることが分かる．($S(f_1, f_4) = 4xy^2 = -2yf_4$ など.)
以上より，I のグレブナー基底は

$$\{f_3, f_4, f_5, f_6\} \text{ つまり } \{x^2, xy, x - 2y^2, y^3\}$$

であると分かる.

S 多項式

定理 1.6 (ブッフベルガーのアルゴリズム)

$k[x_1, \ldots, x_n]$ の 0 でないイデアル $I = \langle f_1, \ldots, f_s \rangle$ のグレブナー基底は，次のアルゴリズムにより有限回のステップで構成することができる.

Input: $F = \{f_1, \ldots, f_s\}$
Output: a Groebner basis $G = (g_1, \ldots, g_t)$ for I, with $F \subset G$
$G := F$
REPEAT
  $G' := G$
  FOR each pair $\{p, q\}$, $p \neq q$ in G' DO
    $S := \overline{S(p,q)}^{G'}$
    IF $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

現在の計算ソフトでは，より効率的に計算できるよう改良されたものが用いられている.

グレブナー基底による求解

例 1.7

$\mathbb{C}$ において次の連立方程式を解く

$$\begin{aligned} x^2+y+z&=1,\\ x+y^2+z&=1,\\ x+y+z^2&=1. \end{aligned} \qquad \cdots (1)$$

$I=\langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1\rangle \subset \mathbb{C}[x,y,z]$ とおくと，アルゴリズムにより I のグレブナー基底は

$$\begin{aligned} g_1&=x+y+z^2-1,\\ g_2&=y^2-y-z^2+z,\\ g_3&=2yz^2+z^4-z^2,\\ g_4&=z^6-4z^4+4z^3-z^2. \quad \leftarrow z \text{ のみの式} \end{aligned}$$

これは (1) と同じ解を持つことが分かる．g_4 は x と y が消去されている

$$g_4=z^2(z-1)^2(z^2+2z-1) \quad \therefore z=0,1,-1\pm\sqrt{2}.$$

$g_1=g_2=g_3=0$ に代入すると x と y の値も決められる（拡張）

$$(1,0,0),(0,1,0),(0,0,1),(-1\pm\sqrt{2},-1\pm\sqrt{2},-1\pm\sqrt{2}).$$

消去・拡張ができない例

このような変数の消去や解の拡張 (代入) は，うまくいかない場合もある.

- 【消去できない例】：$\langle xy \rangle$
  x や y の 1 変数にすることはできない.

- 【拡張できない例】：$\langle xy-1, xz-1 \rangle$
  x を消去すると
  $$(xy-1)z-(xz-1)y = y-z.$$
  よって $y=z=a \in \mathbb{C}$ で，$(x,y,z)=(1/a,a,a)$ なので
  $y=z=0$ の場合は x が存在しないため，拡張できない.

幾何の定理の自動証明

- 幾何的性質を代数的言語 (方程式) に翻訳する.
- 図形の座標や辺の長さ，角度などを変数として，連立方程式を立てる.
- 示したい命題の仮定と結論をそれぞれ方程式にして，仮定の式から結論の式が従うかどうかを判定する.

幾何の定理の自動証明

以下のような翻訳がプログラムされている.

例 1.8

- $AB \parallel CD \iff (AB \text{ の傾き }) = (CD \text{ の傾き})$.
- $AB \perp CD \iff \overrightarrow{AB} \cdot \overrightarrow{CD} = 0$.
- 点 C が中心 A，半径 AB の円周上にある $\iff AB = AC$.
- 点 C が AB の中点である
  $\iff A, C, B$ が同一直線上にあり，かつ $AB = CB$.
- BD は $\angle ABC$ を 2 等分する $\iff \angle ABD = \angle CBD$.
- 円周角の定理，接弦定理，三角関数など.

定理の真偽判定

幾何の定理を次のように書き直す.

【仮定】: $h_1(x_1,\ldots,x_n)=\cdots=h_n(x_1,\ldots,x_n)=0$

としたとき

【結論】: $g(x_1,\ldots,x_n)=0$

が導くことができるかが問題となる.

定理 1.9 (真偽の判定条件)

$h_1=\cdots=h_n=0$ の解 ($V(h_1,\ldots,h_n)$ 上の点) が $g=0$ を満たせば定理が証明される. さらに, $g=0$ となるためには次のどちらかが成立すればよい

$$g\in\sqrt{\langle h_1,\ldots,h_n\rangle}\iff\langle h_1,\ldots,h_n,1-yg\rangle=\langle 1\rangle\,.$$

(幾何的側面) (代数的側面)

ここで, y は新たに加えた変数である.

トレミーの定理の自動証明

当論文では，独自に以下の定理の自動証明を考えた.

例 1.10

[トレミーの定理] ある円に内接する任意の四角形 $ABCD$ に対して，次の等式が成立する

$$AB \cdot CD + BC \cdot DA = AC \cdot BD.$$

- 四辺の長さは以下のように分かっているものとする
$$AB = a,\ BC = b,\ CD = c,\ DA = d \in \mathbb{R}^{\times}.$$

- 四角形 $ABCD$ がある円に内接する
$$\iff \text{対角の和が } \pi \text{ である}$$
$$\iff \angle A + \angle C = \pi,\ \ \angle B + \angle D = \pi.$$
角度はできるだけ三角関数に置き換えて翻訳する
$$cos\,\angle A + cos\,\angle C = 0,$$
$$cos\,\angle B + cos\,\angle D = 0.$$

トレミーの定理の自動証明

- 四角形であることから，対角線によって 4 つの三角形が存在するので余弦定理が選択できる

$$
\begin{aligned}
BD^2 &= a^2 + d^2 - 2ad\ cos\angle A,\\
BD^2 &= b^2 + c^2 - 2bc\ cos\angle C,\\
AC^2 &= a^2 + b^2 - 2ab\ cos\angle B,\\
AC^2 &= c^2 + d^2 - 2cd\ cos\angle D.
\end{aligned}
$$

- 未知の変数 $BD = X$, $AC = Y$, $cos\angle A = A$, $cos\angle B = B$, $cos\angle C = C$, $cos\angle D = D$ をおく.

- C, D を消去して，仮定となる $\mathbb{R}[A, B, X, Y]$ の元を考える

$$
\begin{aligned}
h_1 &:= \ \ 2adA + X^2 - a^2 - d^2,\\
h_2 &:= -2bcA + X^2 - b^2 - c^2,\\
h_3 &:= \ \ 2abB + Y^2 - a^2 - b^2,\\
h_4 &:= -2cdB + Y^2 - c^2 - d^2.
\end{aligned}
$$

トレミーの定理の自動証明

- 一方，成立を確かめたい結論の式は
$$XY = ac + bd$$
簡単のため次の等式を示すことにする
$$X^2Y^2 = (ac + bd)^2$$
整理して，結論となる $\mathbb{R}[A, B, X, Y]$ の元が以下である
$$g := X^2Y^2 - (ac + bd)^2.$$

- （ア） $I = \langle h_1, h_2, h_3, h_4 \rangle$ とおいたときに $g \in \sqrt{I}$,

  （イ） $\widetilde{I} = \langle h_1, h_2, h_3, h_4, 1 - yg \rangle$ とおいたときに $\widetilde{I} = \langle 1 \rangle$

  のどちらかを示せば，仮定から結論が導かれることになる.

トレミーの定理の自動証明

- S 多項式を用いて A, B を消去する
  $2abcd \cdot S(h_1, h_2) = (ad+bc)X^2 - (ac+bd)(ab+cd) =: h_5,$
  $2abcd \cdot S(h_3, h_4) = (ab+cd)Y^2 - (ac+bd)(ad+bc) =: h_6$
  ブッフベルガーのアルゴリズムにより，このときの I のグレブナー基底は $\{h_1, h_2, h_3, h_4, h_5, h_6\}$ であることが分かる.

- （ア） $(ad+bc) \cdot g = (ad+bc)X^2Y^2 - (ac+bd)^2(ad+bc)$
  $= Y^2 \cdot h_5 + (ac+bd) \cdot h_6 \in I$
  $ad+bc$ を可逆元とすると，$g \in I$ であり，$g \in \sqrt{I}$ が示された.

  （イ） $yY^2 \cdot h_5 + y(ac+bd) \cdot h_6 + (ad+bc) \cdot (1-yg)$
  $= ad+bc \in \widetilde{I}$
  上と同様にして，$1 \in \widetilde{I}$ すなわち $\widetilde{I} = \langle 1 \rangle$ である.

これでトレミーの定理が証明された.

参考文献

『グレブナ基底と代数多様体入門　上・下』　丸善出版
著者：デビッド・コックス，ドナル・オシー，ジョン・リトル
翻訳：落合 啓之，西山 享，山本 敦子，示野 信一，室 政和