グレブナー基底と高次多変数方程式の解法

鈴木 正幸

岩大・非常勤講師

November 1, 2018

変数が多く,
次数が高い,
方程式の解を,
求めるアルゴリズム

一次方程式

$$ax = b$$

両辺に，a^{-1} を，左から掛ける:

$$x = a^{-1}b$$

連立一次方程式（系）

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots &= b_1, \\
&\ldots \\
a_{n1}x_1 + a_{n2}x_2 + \ldots &= b_n
\end{aligned}
$$

- 線形代数，ガウスの消去法
- 一次方程式，$ax = b$ に帰着させる

一変数方程式

$$a_n x^n + \cdots + a_0 = b$$

- 解の公式，$x^n = c$ に帰着させる．
- 帰着できない時，数値計算（ニュートン法）で近似的に求める．

多変数 (代数) 方程式 (系)

$$
\begin{aligned}
f_1(x, y, \ldots, z) &= 0, \\
\cdots &, \\
f_n(x, y, \ldots, z) &= 0
\end{aligned}
$$

- 変数消去，因数分解
- 必ず解ける方法を知っていますか？

天秤秤の問題

天秤秤と，a グラムの重りと b グラムの重りが無数にあるとします．どんな重さが測れるでしょう？

あるいは，c グラムを測る事ができますか？

数の集合と基底

$P = \{ax + by | x, y \in \mathcal{Z}\}$

a の倍数と b の倍数を加えてできる整数の集合 P を考えます。

a と b は，P を生成する基底です。

$c \in P$ ならば問題は解決です。

$\{gz | z \in \mathcal{Z}, g \in P\} = P$ となる，g があるか？

- a と b の組合わせで作れる最小の数は，最大公約数 g であり，それの倍数しか a と b の組合わせでは作れません.
- $ax + by = g$ となるの x と y は，ユークリッドの互除法によって求められます.
- 最大公約数 g は，a と b の組合わせでできる数の集合のもっとも簡単な基底 となります.

二つの方程式 $f_1(x) = 0, f_2(x) = 0$ の共通解は？

それぞれの方程式の解を求めて，共通な解を求めてもいいですが，
前の議論から，

- 二つの式 $f_1(x), f_2(x)$ の組み合わせでできる，多項式全ての集合を考える:

$$\{A(x)f_1(x) + B(x)f_2(x) | A(x), B(x) \text{ は任意の } x \text{ の多項}$$

- 最も簡単な (次数の低い) 式 (基底) を求め，
- その解を求める.

最大公約多項式

- この基底は，$f_1(x)$ と $f_2(x)$ の最大公約多項式 $(g(x))$ となり，

$$
\begin{aligned}
a(x)f_1(x) + b(x)f_2(x) &= g(x), \\
\deg(a(x)) < \deg(f_2(x)), \\
\deg(b(x)) < \deg(f_1(x))
\end{aligned}
$$

- $g(x)$, $a(x)$, $b(x)$ はユークリッドの互助法で求められる

多変数で高次な方程式をどう解くか?

$$
\begin{aligned}
f_1(x, y, \ldots, z) &= 0, \\
\cdots &, \\
f_n(x, y, \ldots, z) &= 0
\end{aligned}
$$

$f_1, \ldots, f_n$ を組合わせでできる任意の多項式の集合を考える:

$$\{A_1(x, \ldots, z) f_1(x, \ldots, z) + \cdots + A_n(x, \ldots, z) f_n(x, \ldots$$

この集合を $(f_1, \ldots, f_n)$ と表し，f_1 から f_n が作るイデアル $\mathcal{I}$ と呼ぶ.
$\mathcal{I}$ を作ることのできる多項式の組をイデアルの基底と呼びます.

都合の良い基底

方程式を解くのに都合の良い基底を求めることは，

同じ解を持つ，より簡単な方程式系への変換となる．この基底が例えば，

$$(g_1(x, z) = 0, g_2(y, z) = 0, \cdots, g_m(z) = 0)$$

という形で求まれば，
多変数方程式の問題は，　一変数方程式の問題に帰着される．

- 「このような変形はできるのか」，
- 「変形する方針は」，
- 「必ず求まるのか」

などが問題となる．

グラス置き換えパズル

ウィスキーのグラス W，ビールのグラス B，お酒のグラス S が一列に並んでいる．
グラスは次の置き換え規則で，置き換えて良いとする．

$$\text{置き換え規則 } G \begin{cases} B & \longleftrightarrow & WB \\ BS & \longleftrightarrow & W \end{cases}$$

問題

1. $BSBS$ は $WWWB$ に置き換えできるか？
2. $BSBBS$ は BWW に置き換えできるか？

問題の難しい点

- できる場合はその置き換えを示せば良いが,
- できない事を示す事.

パズル解法への道

簡単な方へ置き換える（簡約化）ことにする

$$\text{簡約規則 } R \begin{cases} WB & \to & B \\ BS & \to & W \end{cases}$$

正規形

- これ以上簡約できないものを正規形と言う
- 置き換え規則 G で置き換え可能な列の要素は簡約規則 R で同じ正規系を持つか？
- この性質が成り立てば，簡約系で正規形が同じであれば，置き換え系で，置き換え可能となる．

簡約規則の追加

置き換え可能なのに，同じ正規形を持たない場合は，そのような簡約規則を追加すればよい．
例えば，WBS は二つの置き換えが可能:

$$\begin{cases} WBS & \to & WW \\ WBS & \to & BS & \to & W \end{cases}$$

置き換え系では，WW と W は，WBS を通して置き換え可能であるから，簡約系で

$$WW \to W$$

を新しい簡約規則として採用すればいい事になる．
この追加される簡約規則をどうやって見付けるかが問題となる．

新しい規則を見つける

- 簡約規則の左項中で，重なりが生ずるような二つの規則を探す．
  (この二つの簡約規則を危険対と呼ぶ)．
  今の場合，BS と WB は 重なりを持つ項，WBS を別の正規形に簡約する可能性を持つ．
- この操作を次々に繰り返し，危険対が全て同じ簡約形を持つようになった時，置き換え可能である物は，全て同じ正規形を持つ事になる．

これを，簡約系の完備化という．

完備な系

- 正規形は有限ステップで求まる．(停止性)
- ある項の正規形は，簡約順序によらず同じになる.(合流性)

パズルの答え

簡約規則 R を完備化すると:

$$\text{簡約規則 } R' \begin{cases} WB & \to & B \\ BS & \to & W \\ WW & \to & W \end{cases}$$

これでパズルの問題が解ける:

- $BSBS \to^* W$, $WWWB \to^* B$, なので, 置き換え不可
- $BSBBS \to^* BW$, $BWWW \to^* BW$, なので, 置き換え可

これがどう方程式と関係しているのでしょう？

グレブナー基底

与えられた方程式 f_i の最高順位項を $head(f_i)$ 、残りの項を $rest(f_i)$ とすると，

$$f_i = head(g_i) + rest(g_i) = 0$$

から

$$head(g_i) \to -rest(g_i)$$

という簡約規則を作る事ができる．
このような簡約系を作るには，項間の順序，簡約，危険対の求め方を，方程式用に決める必要がある．

項の間の順序と簡約

いくつの順序が考えられ，順序によって完備な簡約系が異る．

辞書式順序: ： $xyz > yz^3 > z^5$

全次数辞書式順序: $x^5 > x^4y > x^3yz$

簡約

簡約

基底の先頭項を残りの項で置き換える簡約規則と見て，項をより低順位項で置き換える操作.

g_1 を g_2 で簡約

- $g_1 = x^4yz - xyz^2$ ($head(g_1) = x^4yz$, $rest(g_1) = xyz^2$)
- $g_2 = x^3yz - xz^2$ ($head(g_2) = x^3yz$, $rest(g_2) = xz^2$)

$$\begin{aligned} g' &= g_1 - (head(g_1)/head(g_2))g_2 \\ &= g_1 - (x^4yz/x^3yz)g_2 \\ &= x^2z^2 - xyz^2 \end{aligned}$$

S 多項式

新たな簡約規則を得るための計算.

２つの多項式 f_1, f_2 の S 多項式を $Sp(f_1, f_2)$ と書き、以下のように計算する。

$$Sp(f_1, f_2) = \frac{lcm}{head(f_1)} f_1 - \frac{lcm}{head(f_2)} f_2$$

$$\begin{aligned} g_1 &= x^3yz - xz^2, & head(g_1) &= x^3yz, \\ g_2 &= x^2y^2 - z^2, & head(g_2) &= x^2y^2 \end{aligned}$$

$$lcm(head(g_1), head(g_2)) = x^3y^2z$$

$$\begin{aligned} Sp(g_1, g_2) &= (lcm/head(g_1))g_1 - (lcm/head(g_1))g \\ &= (x^3y^2z/x^3yz)g_1 - (x^3y^2z/x^2y^2)g \\ &= -xyz^2 + xz \end{aligned}$$

グレブナー基底の定義

イデアル $\mathcal{I}$ の基底を $G = \{f_1, \cdots, f_n\}$ とする。
F を可能な限り M 簡約した結果を F' とし，

$$F \overset{G}{\longmapsto} F'$$

と表す.

グレブナー基底 Gは

$\mathcal{I}$ の任意の要素 f に対し，

$$f \overset{G}{\longmapsto} 0$$

G がグレブナー基底の時，$f \overset{\psi}{\longmapsto} f'$ を計算し，$f' = 0$ を調べることで、$f \in \mathcal{I}$ であるかを簡単に決定できる.

f_1, f_2, f_3 のグレブナー基底計算 (全次数辞書式順序)

$$\begin{cases} f_1 = 2{x_1}^3 x_2 + 6{x_1}^3 - 2{x_1}^2 - x_1 x_2 - 3x_1 - x_2 + 3 \\ f_2 = {x_1}^3 x_2 + 3{x_1}^3 + {x_1}^2 x_2 + 2{x_1}^2 \\ f_3 = 3{x_1}^2 x_2 + 9{x_1}^2 + 2x_1 x_2 + 5x_1 + x_2 - 3 \end{cases}$$

S-多項式

$$\begin{aligned} Sp(f_1, f_2) &= (lcm/head(f_1))f_1 - (lcm/head(f_1))f_2 \\ &= (2{x_1}^3 x_2/2{x_1}^3 x_2)f_1 - (2{x_1}^3 x_2/{x_1}^3 x_2)f_2 \\ &= -2x_1^2 x_2 - 6x_1^2 - x_1 x_2 - 3x_1 - x_2 + 3 \\ &= f_4' \end{aligned}$$

グレブナー基底

f_1, f_2, f_3 のグレブナー基底

$$G = \{ \begin{array}{l} x_1x_2 + x_1 - x_2 + 3, \\ 2{x_1}^2 - 3x_1 + 2x_2 - 6, \\ 2{x_2}^2 - 8x_1 - 5x_2 - 3\} \end{array}$$

グレブナー基底から方程式の解を求める方法

辞書式順序で基底計算を行うと、連立方程式の解が求めやすいが、基底計算に時間がかかる上に計算量が多くなる.
簡単に求まる基底から，解を求める手法として固有値法がある.

固有値法

1. 任意の多項式を，グレブナー基底 G で簡約した多項式の集合 $\mathcal{P}^s/\mathcal{I}$ は，ベクトル空間をなす.
2. グレブナー基底の最高順位項で割り切れない全ての項の集合を Normal set といい、 $\mathcal{P}^s/\mathcal{I}$ ベクトル空間の基底となる。
3. Normal set により $x_i\times$ を行列で表す事ができる.
4. その行列の固有値は，$\mathcal{I}$ の x_i に関する解となる.

f_1, f_2, f_3 のグレブナー基底

$$G = [x_1x_2{+}x_1{-}x_2{+}3, 2{x_1}^2{-}3x_1{+}2x_2{-}6, 2{x_2}^2{-}8x_1{-}5$$

$$Normal\ Set = \{1, x_2, x_1\}$$

書き換え規則

$$\begin{cases} x_1x_2 & \to -x_1 + x_2 - 3 \\ {x_1}^2 & \to \frac{3}{2}x_1 - x_2 + 3 \\ {x_2}^2 & \to 4x_1 + \frac{5}{2}x_2 + \frac{3}{2} \end{cases}$$

$$P = c_1\vec{x_1} + c_2\vec{x_2} + c_3$$

$x_1\times$ の行列 (かけ算表)

$$\begin{array}{r c}
 & \begin{array}{ccc} 1 & x_2 & x_1 \end{array} \\
\begin{array}{r} x_1 \times 1 \\ x_1 \times x_2 \\ x_1 \times x_1 \end{array} & \begin{pmatrix} 0 & 0 & 1 \\ -3 & 1 & -1 \\ 3 & -1 & 3/2 \end{pmatrix}
\end{array}$$

$x_1\times$ の固有値

$$\left[0,\ \frac{5}{4} + \frac{1}{4}\sqrt{65},\ \frac{5}{4} - \frac{1}{4}\sqrt{65}\right]$$

$x_2\times$ の行列 (かけ算表)

$$\begin{array}{r c}
 & \begin{array}{ccc} \quad 1 \quad & \quad x_2 \quad & \quad x_1 \quad \end{array} \\
\begin{array}{r} x_2 \times 1 \\ x_2 \times x_2 \\ x_2 \times x_1 \end{array} & \begin{pmatrix} 0 & 1 & 0 \\ 3/2 & 5/2 & 4 \\ -3 & 1 & -1 \end{pmatrix}
\end{array}$$

$x_2\times$ の固有値

$$\left[3,\ -\frac{3}{4}+\frac{1}{4}\sqrt{65},\ -\frac{3}{4}-\frac{1}{4}\sqrt{65}\right]$$

これらの固有値が f_1, f_2, f_3 の解である。