グレブナー基底について

(元) 岩手大学・工学部 鈴木正幸

平成 29 年 11 月 24 日

- 変数が多くて，
- 次数が高い，
- 方程式の根を求める (逐次) アルゴリズム

1 方程式を解くとは？

- 一次方程式, $ax = b$

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

- 連立一次方程式 (系)

$$(a_{11}x_1 + a_{12}x_2 + \ldots = c_1,$$

$$\cdots,$$

$$a_{n1}x_1 + a_{n2}x_2 + \ldots = c_n)$$

  – 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, $a_nx^n + \cdots + a_0 = b$

  - 根の公式, $x^n = c$ 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) $(f_1(x, \dots, z) = 0, \cdots, f_n(x, \dots, z) = 0)$
  - 変数消去, 因数分解
  - 必ず解ける方法を知っていますか？

1.1　基底とは

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？

- この問題は，不定方程式 $ax + by = c$ を満たす，整数 x, y を求める問題となる.
- この解は，a と b の最大公約数を求める問題に帰着されます.
- a と b の組合わせで作れる最小の数は，最大公約数であり，それの倍数しか a と b の組合わせでは作れません.
- 最大公約数は a と b の組合わせでできる数の集合の**基底**となります.
- 上の問題は，a と b の最大公約数を g とすると，c は g の倍数でなければ解が存在しないこと，$ax + by = g$ の x と y は，Euclid の互除法によって求められます.

問題

二つの方程式 $f_1(x)=0, f_2(x)=0$ の共通根は？

それぞれの方程式の根を求めて, 共通な根を求めてもいいですが,

- 上の議論から，二つの式 $f_1(x), f_2(x)$ の組み合わせでできる, 最も簡単な (次数の低い) 式 (基底) を求め, その根を求める.
- 基底は，$f_1(x)$ と $f_2(x)$ の最大公約多項式 $(g(x))$ となり,

$$A(x)f_1(x)+B(x)f_2(x)=g(x),$$

$$\deg(A(x))<\deg(f_2(x)),$$

$$\deg(B(x))<\deg(f_1(x))$$

1.2 多変数方程式 をどう解くか?

$$(f_1(x,\ldots,z)=0,\cdots,f_n(x,\ldots,z)=0)$$

に対し，$f_1,\ldots,f_n$ を組合わせでできる任意の多項式

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

の集合を考えます.

この集合を $(f_1,...,f_n)$ 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.

方程式を解くのに都合の良い基底を求めることは，同じ根を持つ，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.

2 パズルと基底

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.

$$\text{簡約規則 } R \left\{ \begin{array}{ccc} WB & \to & B \\ BS & \to & W \end{array} \right.$$

- これ以上簡約できないもの (正規形)
- 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.

- 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

$$\left\{ \begin{array}{ccccc} WBS & \to & WW & & \\ WBS & \to & BS & \to & W \end{array} \right.$$

  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同やって見付けるかが問題となる.

- 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.

簡約系の**完備化**という. 完備な系とは,

- 正規系は有限ステップで求まる. (**停止性**)
- ある項の正規系は, 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,

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

が得られる. これで, $BSBS \to^* W$, $WWWB \to^* B$, なので, 置き換え可能ではない.

$BSBBS \to^* BW$, $BWWW \to^* BW$, なので, 置き換え可能となる.

これがどう方程式と関係しているのでしょう？

3　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.

3.1 項の間の順序

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: $x^5 > x^4y > x^3yz$

3.2 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.

例２．１： g_1 を g_2 で M 簡約

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

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

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

3.3 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。

$$Sp(f_1, f_2) = \frac{lcm}{head(f_1)}f_1 - \frac{lcm}{head(f_2)}f_2 \tag{1}$$

例２．２： g_1 と g_2 の S 多項式

$g_1 = x^3yz - xz^2$, $head(g_1) = x^3yz$

$g_2 = x^2y^2 - z^2, \quad head(g_2) = x^2y^2$

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

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

3.4 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，

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

と表す.

$\mathcal{I}$ の任意の要素 f に対し，

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

という性質を持つとき，G をグレブナー基底と呼ぶ。

G がグレブナー基底の時，$f \stackrel{\psi}{\longmapsto} f'$ 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.

例２．３：f_1, f_2, f_3 のグレブナー基底を求める。(全次数辞書式順序)

$$\begin{cases} f_1 = 2{x_1}^3x_2 + 6{x_1}^3 - 2{x_1}^2 - x_1x_2 - 3x_1 - x_2 + 3 \\ \\ f_2 = {x_1}^3x_2 + 3{x_1}^3 + {x_1}^2x_2 + 2{x_1}^2 \\ \\ f_3 = 3{x_1}^2x_2 + 9{x_1}^2 + 2x_1x_2 + 5x_1 + x_2 - 3 \end{cases}$$

(ｓ多項式の例)

$$\begin{aligned} Sp(f_1, f_2) &= (lcm/head(f_1))f_1 - (lcm/head(f_1))f_2 \\ &= (2{x_1}^3x_2/2{x_1}^3x_2)f_1 - (2{x_1}^3x_2/{x_1}^3x_2)f_2 \\ &= -2x_1^2x_2 - 6x_1^2 - x_1x_2 - 3x_1 - x_2 + 3 = f_4' \end{aligned}$$

（M簡約の例）

$$\begin{array}{ccl} f_4' & \xmapsto{f_3} & f_4' - (-2x_1^2x_2/head(f_3))f_3 \\ & = & x_1x_2 + x_1 - x_2 + 3 \end{array}$$

＜ f_1, f_2, f_3 のグレブナー基底＞

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

4　グレブナー基底から方程式の根を求める方法

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，根を求める手法として固有値法がある.

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 に関する根となる.

例３．１：例２．３の f_1, f_2, f_3 の根を求める。

＜ f_1, f_2, f_3 のグレブナー基底＞

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

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

＜書き換え規則＞

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

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

＜$x_1\times$ の行列＞

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

＜$x_2\times$ の行列＞

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

＜x_1 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 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 の根である。

参考文献

[1] **Beker,T., Weispfenning, V.: Gröbner Bases. GTM bf 141, Springer-Verlag, 1993**