

<div data-bbox="154 39 678 119" data-label="Section-Header"> <h2>グレブナー基底と高次多変数方程式の解法</h2> </div> <div data-bbox="367 170 463 194" data-label="Text"> <p>鈴木 正幸</p> </div> <div data-bbox="356 225 472 242" data-label="Text"> <p>岩大・非常勤講師</p> </div> <div data-bbox="327 272 501 295" data-label="Text"> <p>November 3, 2019</p> </div> <div data-bbox="297 365 530 491" data-label="Text"> <p>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</p> </div>	<div data-bbox="1061 19 1178 49" data-label="Section-Header"> <h2>Contents</h2> </div> <div data-bbox="822 114 1135 194" data-label="Text"> <p>方程式を解くとは？ 数の集合と基底と最大公約数 多変数方程式をどう解くか？</p> </div> <div data-bbox="822 233 1014 256" data-label="Text"> <p>パズルと基底と簡約</p> </div> <div data-bbox="822 295 1048 347" data-label="Text"> <p>グレブナー基底 項の間の順序と簡約</p> </div> <div data-bbox="822 386 1249 410" data-label="Text"> <p>グレブナー基底から方程式の解を求める方法</p> </div> <div data-bbox="1382 499 1444 523" data-label="Text"> <p>2 / 30</p> </div>	<div data-bbox="1747 19 1897 49" data-label="Section-Header"> <h2>一次方程式</h2> </div> <div data-bbox="1789 188 1856 210" data-label="Equation-Block"> <math display="block">ax = b</math> </div> <div data-bbox="1668 233 1975 256" data-label="Text"> <p>両辺に，<math>a^{-1}</math> を，左から掛ける：</p> </div> <div data-bbox="1776 308 1868 331" data-label="Equation-Block"> <math display="block">x = a^{-1}b</math> </div> <div data-bbox="2089 499 2150 523" data-label="Text"> <p>3 / 30</p> </div>
<div data-bbox="273 550 555 585" data-label="Section-Header"> <h2>連立一次方程式 (系)</h2> </div> <div data-bbox="271 708 557 788" data-label="Equation-Block"> <math display="block">\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \dots &amp; = &amp; b_1, \\ &amp; \dots &amp; \\ a_{n1}x_1 + a_{n2}x_2 + \dots &amp; = &amp; b_n \end{array}</math> </div> <div data-bbox="134 820 486 877" data-label="List-Group"> <ul style="list-style-type: none"> <li>▶ 線形代数, ガウスの消去法</li> <li>▶ 一次方程式, <math>ax = b</math> に帰着させる</li> </ul> </div> <div data-bbox="678 1032 741 1056" data-label="Text"> <p>4 / 30</p> </div>	<div data-bbox="1028 550 1209 580" data-label="Section-Header"> <h2>一変数方程式</h2> </div> <div data-bbox="1021 726 1216 750" data-label="Equation-Block"> <math display="block">a_nx^n + \dots + a_0 = b</math> </div> <div data-bbox="837 772 1404 858" data-label="List-Group"> <ul style="list-style-type: none"> <li>▶ 解の公式, <math>x^n = c</math> に帰着させる.</li> <li>▶ 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.</li> </ul> </div> <div data-bbox="1382 1032 1444 1056" data-label="Text"> <p>5 / 30</p> </div>	<div data-bbox="1648 550 1995 585" data-label="Section-Header"> <h2>多変数 (代数) 方程式 (系)</h2> </div> <div data-bbox="1709 708 1935 788" data-label="Equation-Block"> <math display="block">\begin{array}{rcl} f_1(x, y, \dots, z) &amp; = &amp; 0, \\ &amp; \dots &amp; \\ f_n(x, y, \dots, z) &amp; = &amp; 0 \end{array}</math> </div> <div data-bbox="1541 815 1910 873" data-label="List-Group"> <ul style="list-style-type: none"> <li>▶ 変数消去, 因数分解</li> <li>▶ 必ず解ける方法を知っていますか？</li> </ul> </div> <div data-bbox="2089 1032 2150 1056" data-label="Text"> <p>6 / 30</p> </div>
<div data-bbox="322 1082 508 1112" data-label="Section-Header"> <h2>天秤秤の問題</h2> </div> <div data-bbox="163 1251 665 1303" data-label="Text"> <p>天秤秤と, <math>a</math> グラムの重りと <math>b</math> 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？</p> </div> <div data-bbox="163 1335 577 1359" data-label="Text"> <p>あるいは, <math>c</math> グラムを測る事ができますか？</p> </div> <div data-bbox="678 1565 741 1589" data-label="Text"> <p>7 / 30</p> </div>	<div data-bbox="1012 1082 1225 1112" data-label="Section-Header"> <h2>数の集合と基底</h2> </div> <div data-bbox="822 1155 1102 1185" data-label="Equation-Block"> <math display="block">P = \{ax + by   x, y \in \mathbb{Z}\}</math> </div> <div data-bbox="822 1193 1415 1244" data-label="Text"> <p><math>a</math> の倍数と <math>b</math> の倍数を加えてできる整数の集合 <math>P</math> を考えます. <math>a</math> と <math>b</math> は, <math>P</math> を生成する基底です.</p> </div> <div data-bbox="822 1254 1113 1278" data-label="Text"> <p><math>c \in P</math> ならば問題は解決です.</p> </div> <div data-bbox="822 1291 1355 1321" data-label="Text"> <p><math>\{gz   z \in \mathbb{Z}, g \in P\} = P</math> となる, <math>g</math> があるか？</p> </div> <div data-bbox="837 1334 1420 1511" data-label="List-Group"> <ul style="list-style-type: none"> <li>▶ <math>a</math> と <math>b</math> の組合わせで作れる最小の数は, 最大公約数 <math>g</math> であり, その倍数しか <math>a</math> と <math>b</math> の組合わせでは作れません.</li> <li>▶ <math>ax + by = g</math> となるの <math>x</math> と <math>y</math> は, ユークリッドの互除法によって求められます.</li> <li>▶ 最大公約数 <math>g</math> は, <math>a</math> と <math>b</math> 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.</li> </ul> </div> <div data-bbox="1382 1565 1444 1589" data-label="Text"> <p>8 / 30</p> </div>	<div data-bbox="1498 1082 2150 1115" data-label="Section-Header"> <h2>二つの方程式 <math>f_1(x) = 0, f_2(x) = 0</math> の共通解は？</h2> </div> <div data-bbox="1525 1171 2096 1252" data-label="Text"> <p>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,</p> </div> <div data-bbox="1541 1260 2119 1313" data-label="List-Group"> <ul style="list-style-type: none"> <li>▶ 二つの式 <math>f_1(x), f_2(x)</math> の組み合わせでできる, 多項式全ての集合を考える:</li> </ul> </div> <div data-bbox="1570 1367 2136 1396" data-label="Equation-Block"> <math display="block">\{A(x)f_1(x) + B(x)f_2(x)   A(x), B(x) \text{ は任意の } x \text{ の多項式}\}</math> </div> <div data-bbox="1541 1422 1980 1479" data-label="List-Group"> <ul style="list-style-type: none"> <li>▶ 最も簡単な (次数の低い) 式 (基底) を求め,</li> <li>▶ その解を求める.</li> </ul> </div> <div data-bbox="2089 1565 2150 1589" data-label="Text"> <p>9 / 30</p> </div>

## 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

10 / 30

## 多変数で高次な方程式をどう解くか?

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

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

$$\{A_1(x, \dots, z)f_1(x, \dots, z) + \dots + A_n(x, \dots, z)f_n(x, \dots, z)\}$$

この集合を  $(f_1, \dots, f_n)$  と表し,  $f_1$  から  $f_n$  が作るイデアル  $\mathcal{I}$  と呼ぶ.

$\mathcal{I}$  を作ることでできる多項式の組をイデアルの基底と呼びます.

11 / 30

## 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,

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

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.

12 / 30

## 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.

$$\text{置き換え規則 } G \left\{ \begin{array}{l} B \leftrightarrow WB \\ BS \leftrightarrow W \end{array} \right.$$

### 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?

13 / 30

## 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.

14 / 30

## 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

$$\text{簡約規則 } R \left\{ \begin{array}{l} WB \rightarrow B \\ BS \rightarrow W \end{array} \right.$$

### 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.

15 / 30

## 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:

$$\left\{ \begin{array}{l} WBS \rightarrow WW \\ WBS \rightarrow BS \rightarrow W \end{array} \right.$$

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

$$WW \rightarrow W$$

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.

16 / 30

## 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.

17 / 30

## 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)

18 / 30

## パズルの答え

簡約規則  $R$  を完備化すると:

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

これでパズルの問題が解ける:

- ▶  $BSBS \rightarrow^* W$ ,  $WWWB \rightarrow^* B$ , なので, 置き換え不可
- ▶  $BSBBS \rightarrow^* BW$ ,  $BWWW \rightarrow^* BW$ , 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か?

19 / 30

## 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

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

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。

20 / 30

## 項の間の順序と簡約

いくつかの順序が考えられ, 順序によって完備な簡約系が異なる。

辞書式順序:  $xyz > yz^3 > z^5$

全次数辞書式順序:  $x^5 > x^4y > x^3yz$

21 / 30

## 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

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

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

22 / 30

### 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。

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

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

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

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

23 / 30

## グレブナー基底の定義

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

$$F \xrightarrow{G} F'$$

と表す。

グレブナー基底  $G$

$\mathcal{I}$  の任意の要素  $f$  に対し,

$$f \xrightarrow{G} 0$$

$G$  がグレブナー基底の時,  $f \xrightarrow{\psi} f'$  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。

24 / 30

## $f_1, f_2, f_3$ のグレブナー基底計算 (全次数辞書式順序)

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

s-多項式

$$\begin{aligned} Sp(f_1, f_2) &= (lcm/head(f_1))f_1 - (lcm/head(f_2))f_2 \\ &= (2x_1^3x_2/2x_1^3x_2)f_1 - (2x_1^3x_2/x_1^3x_2)f_2 \\ &= -2x_1^2x_2 - 6x_1^2 - x_1x_2 - 3x_1 - x_2 + 3 \\ &= f'_4 \end{aligned}$$

簡約

25 / 30

### グレブナー基底

$f_1, f_2, f_3$  のグレブナー基底

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

26 / 30

## 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。  
簡単に求める基底から、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。

27 / 30

$f_1, f_2, f_3$  のグレブナー基底

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

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

書き換え規則

$$\left\{\begin{array}{lcl} x_1x_2 & \rightarrow & -x_1+x_2-3 \\ x_1^2 & \rightarrow & \frac{3}{2}x_1-x_2+3 \\ x_2^2 & \rightarrow & 4x_1+\frac{5}{2}x_2+\frac{3}{2} \end{array}\right.$$

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

$x_1 \times$  の行列 (かけ算表)

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

$x_1 \times$  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)

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

$x_2 \times$  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。