日本応用数理学会

総合講演

グレブナー基底の５０年

日比孝之

大阪大学大学院情報科学研究科情報基礎数学専攻

2009 年 9 月 30 日

１．多変数の多項式の割り算
２．グレブナー基底の定義
３．グレブナー基底の源
４．計算ソフト Macaulay
５．Buchberger アルゴリズム
６．トーリック生成系
７．整数計画
８．凸多面体
９．計算代数統計
１０．総括

$f = x^3 - x^2y - x^2 - 1$ を $g_1 = x^2 - z$ と $g_2 = xy - 1$ で割り算する。（その１）

$$\begin{aligned}
f &= x^3 - x^2y - x^2 - 1 \\
&= x(g_1 + z) - x^2y - x^2 - 1 \\
&= xg_1 - x^2y - x^2 + xz - 1 \\
&= xg_1 - (g_1 + z)y - x^2 + xz - 1 \\
&= xg_1 - yg_1 - x^2 + xz - yz - 1 \\
&= xg_1 - yg_1 - (g_1 + z) + xz - yz - 1 \\
&= (x - y - 1)g_1 + (xz - yz - z - 1)
\end{aligned}$$

は割り算であり、その余りは $xz - yz - z - 1$ である。

$f = x^3 - x^2y - x^2 - 1$ を $g_1 = x^2 - z$ と $g_2 = xy - 1$ で割り算する。（その２）

$$
\begin{aligned}
f &= x^3 - x^2y - x^2 - 1 \\
&= x(g_1 + z) - x^2y - x^2 - 1 \\
&= xg_1 - x^2y - x^2 + xz - 1 \\
&= xg_1 - x(g_2 + 1) - x^2 + xz - 1 \\
&= xg_1 - xg_2 - x^2 + xz - x - 1 \\
&= xg_1 - xg_2 - (g_1 + z) + xz - x - 1 \\
&= (x - 1)g_1 - xg_2 + (xz - x - z - 1)
\end{aligned}
$$

も割り算であり、その余りは $xz - x - z - 1$ である。

（その１）と（その２）の余りは異なる。ところが、g_1 と g_2 に $g_3 = -yz + x$ を加え、f を g_1, g_2, g_3 で割り算すると

$$
\begin{aligned}
f &= (x - y - 1)g_1 + (xz - yz - z - 1) \\
&= (x - y - 1)g_1 + xz + (g_3 - x) - z - 1 \\
&= (x - y - 1)g_1 + g_3 + (xz - x - z - 1)
\end{aligned}
$$

となり、（その１）と（その２）の余りは一致する。

● 実際、任意の多項式を g_1, g_2, g_3 で割り算するときその余りは一意的である。

● 多項式 g_3 は g_1 と g_2 の最高次の項 x^2 と xz を打ち消し合うことで得られる多項式 $g_3 = yg_1 - xg_2$ である。

● 変数 $x_1, \ldots, x_n$ の<u>単項式</u>とは変数の積 $x_1^{a_1} \cdots x_n^{a_n}$
（ $a_1, \ldots, a_n$ は非負整数）のことである。

● 単項式全体の集合における全順序 $<$ が<u>単項式順序</u>であるとは
（a）$1 < u$ が任意の単項式 $u \neq 1$ について成立し、
（b）$u < v$ ならば $uw < vw$ が任意の単項式 u, v, w について
成立するときに言う。

● たとえば、辞書式順序は単項式順序である。

● 割り算を議論するときには単項式順序を一つ固定する。

2．グレブナー基底の定義

$\boxed{\text{定義}}$　多項式の有限集合 $\mathcal{G}$ がグレブナー基底であるとは、任意の多項式 f を $\mathcal{G}$ に属する多項式で割り算するとき、その余りが割り算を実行する手続きとは無関係に一意的に定まるときに言う。

３．グレブナー基底の源

［1］廣中平祐の代数多様体の特異点解消論文（ 1964 年）
［2］Bruno Buchberger の学位論文（ 1965 年）
（師匠は Gröbner ）

歴史を遡ると、グレブナー基底の着想は、Macaulay の Hilbert 函数についての研究（ 1927 年）にその発祥の源を持つと言える。しかし、Macaulay は、その源が大河に育むとは考えず、一般的な理論を展開するには至らなかったようだ。

4．計算ソフト Macaulay

● グレブナー基底は、廣中と Buchberger の仕事の後、20 余年はそれほどの着目はされなかったようであるが、

● 1980 年代後半、David Bayer と Michael Stillman が可換代数と代数幾何の計算ソフト Macaulay を開発し、

● その背景にはグレブナー基底が潜むことから、グレブナー基底は可換代数と代数幾何の研究者の周知の概念となる。

● その後、CoCoA、Singular あるいは Macaulay2 など、幾多の計算ソフトが現れ、1990 年代以降の可換代数と代数幾何の進展に大きく貢献している。

5．Buchberger アルゴリズム

● $\underline{S\ \text{多項式}}$の定義

$$f = \underline{x_1 x_4} - x_2 x_3,\ \ g = \underline{x_4 x_7} - x_5 x_6$$

$$S(f, g) = x_7 f - x_1 g = x_1 x_5 x_6 - x_2 x_3 x_7$$

● Buchberger の顕著な功績の一つは、多項式の有限集合 $\mathcal{G}$ があったとき、それがグレブナー基底であるか否かを効果的に判定する方法（Buchberger Criterion）を発見したことである。

（Buchberger 判定法）多項式の有限集合 $\{f_1, \ldots, f_s\}$ がグレブナー基底となるためには、条件「任意の $1 \leq i < j \leq s$ について $S(f_i, f_j)$ を $f_1, \ldots, f_s$ で割り算するとき（うまく割り算すれば）余りを 0 とすることができる」が満たされることが必要十分である。

● Buchberger 判定法は、多項式の有限集合から出発し、自然に得られるグレブナー基底を探すアルゴリズム（Buchberger Algorithm）を導く。

昨今、Buchberger アルゴリズムには日進月歩の多角的な改良が施されており、グレブナー基底を高速に計算するソフトウエアも開発され、計算速度は飛躍的に進歩している。

たとえば、富士通と富士通研究所において開発が始まった計算機代数ソフトウエア Risa/Asir は、高速なグレブナー基底の計算ソフトウエアの一つとして高い評価を受けている。
2000 年 9 月以降は、その開発の拠点が神戸大学理学部に移り、高山信毅と野呂正行を中心としたグループによって開発が続けられている。

６．トーリック生成系

行列 $A = (a_{ij})_{\substack{i=1,\dots,d \\ j=1,\dots,n}} \in \mathbb{Z}^{d\times n}$ が<u>配置行列</u>であるとは、R^n の原点を通過しない超平面で、A の列ベクトルのすべてを含むものが存在するときに言う。

- 変数 $x_1, \dots, x_n, y_1, \dots, y_d$ を準備する。
- 連立方程式系

$$x_j - y_1^{a_{1j}} y_2^{a_{2j}} \cdots y_d^{a_{dj}} = 0, \quad j = 1, \dots, n$$

から $y_1, y_2, \dots, y_d$ を消去する。

- すると、$x_1, \ldots, x_n$ の連立方程式系

$$f_1 = 0, \ldots, f_s = 0$$

が得られる。

- 二項式（binomial）の集合

$$I_A = \{f_1, \ldots, f_s\}$$

を配置 A の<u>トーリック生成系</u>と呼ぶ。

$\boxed{\text{例}}$ $$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{bmatrix}$$

$$\begin{aligned} x_1 - y_1 &= 0 \\ x_2 - y_1 y_2 &= 0 \\ x_3 - y_1 y_2^2 y_3 &= 0 \\ x_4 - y_1 y_2 y_3^2 &= 0 \\ x_5 - y_1 y_3 &= 0 \end{aligned}$$

$$I_A = \{x_2 x_5^2 - x_1^2 x_4, x_2 x_4 - x_3 x_5, x_2^2 x_5 - x_1^2 x_3\}$$

たとえば、二項式 $x_2x_5^2 - x_1^2x_4$ を整数ベクトル $[-2, 1, 0, -1, 2]^\top$ と同一視すると

$$A\begin{bmatrix} -2 \\ 1 \\ 0 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{bmatrix}\begin{bmatrix} -2 \\ 1 \\ 0 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

となる。

７．整数計画

● グレブナー基底が応用数学の舞台に登壇したのは、整数計画問題を解くためのグレブナー基底を使ったアルゴリズムを Conti と Traverso が提唱（1991 年）したときである。

● トーリック生成系とそのグレブナー基底を世に披露し、整数計画問題の最適解の一つがグレブナー基底による割り算の余りから求められることを唱ったのである。

● 彼らのアルゴリズムは、グレブナー基底の代数的な純粋理論からの興味はきわめて深く、グレブナー基底の理論を紹介する講義には不可欠な話題である。

たとえば、標準型の整数計画問題

$$\min\{c \cdot z \,:\, Az = b,\ z \in \mathbf{Z}^5_{\geq 0}\}$$

を考える。但し、$z = [z_1, z_2, z_3, z_4, z_5]^\top$**、**$b = [25, 34, 18]^\top$**、**
$c = [0, 1, 0, 1, 1]$**、**

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{bmatrix}$$

$$\begin{aligned} I_A &= \{x_2x_5^2 - x_1^2x_4, x_2x_4 - x_3x_5, x_2^2x_5 - x_1^2x_3\} \\ \mathcal{G} &= \{x_3x_5^3 - x_1^2x_4^2, x_2x_5^2 - x_1^2x_4, x_2x_4 - x_3x_5, \\ &\qquad x_2^2x_5 - x_1^2x_3, x_2^3x_4 - x_1^2x_3^2\} \end{aligned}$$

- 単項式順序 $<_c$ は、単項式と非負整数ベクトル（たとえば $x_1^2 x_4$ と $[2,0,0,1,0]^\top$ ）を同一視し、c と非負整数ベクトルの内積を考え、その内積の大小によって単項式の大小を決める。タイブレークのときは辞書式順序で決着をつける。
- 実行可能解の一つ $[1,10,10,4,0]^\top$ に単項式 $x_1 x_2^{10} x_3^{10} x_4^4$ を対応させる。その単項式を $\mathcal{G}$ で割り算する。余りは $x_1^7 x_3^{17} x_5$ となる。すると、$[7,0,17,0,1]^\top$ が最適解の一つとなる。

8．凸多面体

グレブナー基底が純粋数学における市民権を獲得したのは、グレブナー基底と凸多面体のテキスト

［3］B. Sturemfels, “Gröbner Bases and Convex Polytopes,” Amer. Math. Soc., 1995.

の影響も大きい。Gelfand–Kapranov–Zelevinsky らの正則三角形分割の理論を、トーリック生成系のグレブナー基底を使って解釈し、その後の凸多面体の組合せ論の潮流を示唆した。

[4] **H. Ohsugi and T. Hibi, A normal** $(0,1)$**-polytope none of whose regular triangulations is unimodular, Discrete and Comput. Geom. 21 (1999), 201–204.**

における「最大個数の単体から成る三角形分割も最小個数からなる三角形分割も両者とも正則ではない」という凸多面体の発見はそのような潮流におけるもっとも顕著な成果の一つである。

9．計算代数統計

グレブナー基底の統計数学への画期的な応用は

［5］P. Diaconis and B. Sturmfels, Algebraic algorithms for sampling from conditional distributions, The Annals of Statistics 26 (1998), 363–397.

に始まる。マルコフ基底がトーリック生成系のグレブナー基底と対応することを示し、計算代数統計と呼ばれる斬新な研究分野が誕生する契機となった。我が国では、東京大学の竹村彰通のグループが計算代数統計の研究を強力に推進している。

Hardy–Weinberg モデル　（ ABO 式血液型）

遺伝子型	AA	AB	AO	BB	BO	OO
人数（観測値）	23	10	15	6	17	29

$$\begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 23 \\ 10 \\ 15 \\ 6 \\ 17 \\ 29 \end{bmatrix} = \begin{bmatrix} 71 \\ 39 \\ 90 \end{bmatrix}$$

Veronese 配置　　　　十分統計量

遺伝子型と期待値

AA	AB	AO	BB	BO	OO
12.6025	13.845	31.95	3.8025	17.55	20.25

- 人数が“少ない”から漸近分布論は（？）
- Fisher の正確確率検定は人数が“多い”から（？）
- マルコフ連鎖モンテカルロ法が一つの有効な方法（！）

$$\begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} x_{AA} \\ x_{AB} \\ x_{AO} \\ x_{BB} \\ x_{BO} \\ x_{OO} \end{bmatrix} = \begin{bmatrix} 71 \\ 39 \\ 90 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} y_{AA} \\ y_{AB} \\ y_{AO} \\ y_{BB} \\ y_{BO} \\ y_{OO} \end{bmatrix} = \begin{bmatrix} 71 \\ 39 \\ 90 \end{bmatrix}$$

グレブナー基底とマルコフ基底

$$
\begin{array}{rl}
x_1x_4 - x_2^2 & [1,-2,0,1,0,0]^\top \\
x_1x_6 - x_3^2 & [1,0,-2,0,0,1]^\top \\
x_4x_6 - x_5^2 & [0,0,0,1,-2,1]^\top \\
x_2x_3 - x_1x_5 & [-1,1,1,0,-1,0]^\top \\
x_2x_5 - x_3x_4 & [0,1,-1,-1,1,0]^\top \\
x_3x_5 - x_2x_6 & [0,-1,1,0,1,-1]^\top
\end{array}
$$

2×2 **分割表**　　**（代数と統計の成績）**

代数 \ 統計	5	4	3	2	1	計
5	2	1	1	0	0	4
4	8	3	3	0	0	14
3	0	2	1	1	1	5
2	0	0	0	1	1	2
1	0	0	0	0	1	1
計	10	6	5	2	3	26

$$
\begin{bmatrix}
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1\\
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1
\end{bmatrix}
$$

Segre 配置

- 現実の社会で遭遇する統計の問題では、膨大なデータの処理を必要とし、グレブナー基底が計算できれば解析が可能になるとしても、計算量の問題が克服できず、現状では、その実用化が困難である。
- ところが、可換代数の世界では、従来から、多種多様なグレブナー基底が生息している。
- すると、逆転の発想ではあるが、既知のグレブナー基底をマルコフ基底とする統計的モデルを（よしんば人工的であれ）設定すれば、その検定を実施することが可能となる。

$$
\begin{bmatrix}
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\
2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2
\end{bmatrix}
$$

Segre–Veronese 配置

● **グレブナー基底が既知（！）**

［6］H. Ohsugi and T. Hibi, Compressed polytopes, initial ideals and complete multipartite graphs, Illinois Journal of Mathematics 44 (2000), 391–406.

例 （ Groupwise Selection Problem ）

● ２種類のケーキ（Ｃケーキとｔケーキ）が沢山ある。

● 小テーブルが幾つかあり、それぞれの小テーブルには小皿２枚、中皿２枚、大皿２枚がある。

● 一つの小テーブルに一人が座り、ケーキを６個選び、１枚の皿に１個ずつ置く。

小皿中皿大皿／小皿中皿大皿	人数	小皿中皿大皿／小皿中皿大皿	人数
ＣＣＴ／ＣＣＴ	10	ＴＴＴ／ＴＣＴ	6
ＣＣＴ／ＴＴＴ	27	ＴＴＴ／ＣＣＣ	6
ＣＣＴ／ＴＣＴ	12	ＴＣＴ／ＴＣＴ	0
ＣＣＴ／ＣＣＣ	9	ＴＣＴ／ＣＣＣ	2
ＴＴＴ／ＴＴＴ	7	ＣＣＣ／ＣＣＣ	0

十分統計量

小皿C	小皿T	中皿C	中皿T	大皿C	大皿T
85	73	105	53	17	141

[7] S. Aoki, T. Hibi, H. Ohsugi and A. Takemura, Markov basis and Gröbner basis of Segre–Veronese configuration for testing independence in group-wise selections, Annals of the Institute of Statistical Mathematics, to appear, arXiv:0704.1074v2 [math.ST].

- 大学入試センター試験の科目選択の統計的検証
- Oguma et al., 2004 の遺伝子データの検証

１０．総括

科学技術振興機構（ＪＳＴ）の戦略的創造推進研究事業の研究領域「数学と諸分野の協働によるブレークスルーの探索」の CREST の研究課題

現代の産業社会とグレブナー基底の調和

（ 2008 年 10 月 – 2014 年 3 月）

http://www.math.jst.go.jp/ja/scientists/teamhibi/index.html

は、以上のような背景を踏まえ、研究活動を展開している。

- 1964 年　廣中平祐の特異点解消論文
- 1965 年　Bruno Buchberger の学位論文
- 1986 年　Macaulay
- 1991 年　整数計画
- 1995 年　凸多面体
- 1998 年　計算代数統計
- 2008 年 10 月　JST CREST Gröbner Bases
- 2014 年 3 月