トーリックイデアルのグレブナー基底とその応用

大杉 英史 *

関西学院大学 理工学部 数理科学科，2016 年 2 月

1　グレブナー基底

グレブナー基底とは，多項式環のイデアルの生成系の中で特別な性質『多項式をグレブナー基底の元を使って割り算すると，余りが一意に定まる』を持つものである．可換代数，代数幾何に止まらず，離散幾何，統計学，暗号理論などへの応用があり，近年の計算機，および，アルゴリズム・ソフトウエアの発展に伴って広範な研究分野において活発に研究されている．きっと皆さんの研究分野にも何かしら関わりがあると思うので，グレブナー基底の定義だけでも眺めてみて欲しい．

体 K 上の n 変数多項式環 $K[\mathbf{x}] = K[x_1, \ldots, x_n]$ の単項式全体を $\mathcal{M}_n$ で表す．集合 $\mathcal{M}_n$ 上の順序 $<$ が**単項式順序**であるとは，以下の 3 条件をみたすときにいう．

1. $<$ は全順序である．すなわち，任意の 2 つの単項式は比較可能である．
2. $1 \neq \forall u \in \mathcal{M}_n$ に対して，$1 < u$. すなわち，すべての単項式の中で 1 は最小の単項式である．
3. $u, v, w \in \mathcal{M}_n$, $u < v \Rightarrow uw < vw$.

これらの条件は，多項式の割り算と深く関連している．代表的な単項式順序として，辞書式順序，次数辞書式順序，(次数) 逆辞書式順序が挙げられる．

例 1.1 (**辞書式順序** $(x_1 > \cdots > x_n)$)．2 つの単項式を比較する際，まず，x_1 に関して次数を比較して，大きい方が大きい．同じなら x_2 に関して次数を比較して，大きい方が大きい．同じなら x_3 に関して次数を比較して ⋯．

単項式順序 $<$ を 1 つ固定する．多項式 $0 \neq f \in K[\mathbf{x}]$ に現れる単項式の中で $<$ に関して最大のものを $\mathrm{in}_<(f)$ で表し，f の**先頭単項式**という．イデアル $I \subset K[\mathbf{x}]$ に対して，I の元の先頭単項式で生成されるイデアル $\mathrm{in}_<(I) := \langle \mathrm{in}_<(f) \mid 0 \neq f \in I \rangle$ を I の**イニシャルイデアル**という．有限集合 $\mathcal{G} = \{g_1, \ldots, g_t\} \subset I$ が $<$ に関する I の**グレブナー基底**であるとは，$\mathrm{in}_<(I) = \langle \mathrm{in}_<(g_1), \ldots, \mathrm{in}_<(g_t) \rangle$ が成り立つときにいう．これは,『任意の $0 \neq f \in I$ に対して，$\mathrm{in}_<(f)$ はある $\mathrm{in}_<(g_i)$ で割り切れる』という条件と同値である．また,『$K[\mathbf{x}]$ の元を集合 $\mathcal{G}$ を使って割り算すると，余りが一意に定まる』とも同値であるが，多変数多項式の $\mathcal{G}$ による割り算の定義は省略する．

イデアル I と単項式順序が与えられれば，そのグレブナー基底は必ず存在し，I を生成することが知られている．グレブナー基底は一意ではないが，以下のような特別なグレブナー基底を考えれば，一意に存在することが知られている．イデアル $I \subset K[\mathbf{x}]$ のグレブナー基底 $\mathcal{G}$ が **被約**（簡約ともいう）であるとは，任意の $g \in \mathcal{G}$ に対して，g はモニックであり，g に現れる任意の単項式が $\{\mathrm{in}_<(g') \mid g \neq g' \in \mathcal{G}\}$ の元で割り切れないときにいう．グレブナー基底の例を挙げよう．

*ohsugi@kwansei.ac.jp

例 1.2. イデアル $I = \langle x_1x_2 - x_3x_4, x_1x_5 - x_6x_7 \rangle \subset K[x_1, \ldots, x_7]$ と辞書式順序 $< (x_1 > \cdots > x_7)$ に関して，$\{x_1x_2 - x_3x_4,\ x_1x_5 - x_6x_7\}$ は I のグレブナー基底ではない．実際，

$$x_5(x_1x_2 - x_3x_4) - x_2(x_1x_5 - x_6x_7) = x_2x_6x_7 - x_3x_4x_5 \in I$$

の先頭項 $x_2x_6x_7$ は $\langle x_1x_2, x_1x_5 \rangle$ に属さない．実は，$\{x_1x_2 - x_3x_4,\ x_1x_5 - x_6x_7,\ x_2x_6x_7 - x_3x_4x_5\}$ は I の $<$ に関する（被約）グレブナー基底となる．

生成系がグレブナー基底であるかどうかを判定する **Buchberger 判定法**や，生成系からグレブナー基底を計算する **Buchberger アルゴリズム**においては，上の例のような「先頭単項式の打ち消し合い」によって定義される S-多項式が鍵となる．グレブナー基底の最も基本的な応用は，多項式連立方程式の変数消去を行う消去法（消去定理）である（[J, 第 1 章] 参照）．辞書式順序ならば必ず消去法が適用できるが，実際には，辞書式順序のグレブナー基底計算は時間が掛かることが多いため，もう少し工夫が必要となる．このような重要な応用が存在することもあり，グレブナー基底は，`Macaulay2`, `SINGULAR`, `CoCoA`, `Risa/Asir`, `Mathematica`, `Maple` など多くの数式処理ソフトウエアに実装されている．([J, 第 3 章] 参照.)

2　トーリックイデアル

トーリックイデアルとは，有限個の格子点（整数座標を持つ点）に付随するイデアルであり，2 項式で生成されることが知られている．ここで，**2 項式**とは，$x_1x_2 - x_3^2$ のように次数の等しい 2 つの単項式の差として表される多項式をいう．格子点の集合 $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{Z}^d$ が $\mathbb{R}^d$ の**配置**であるとは，$\mathbf{w} \in \mathbb{R}^d$ が存在して，$\mathbf{w} \cdot \mathbf{a}_1 = \cdots = \mathbf{w} \cdot \mathbf{a}_n = 1$ をみたすときにいう．多くの応用でこの条件を必要とするので，定義に含める慣習があるが，教科書・分野によっては仮定しない場合もある．負のべきも許す単項式を**ローラン単項式**といい，それらの線形結合を**ローラン多項式**という．変数 $t_1, \ldots, t_d$ に関するローラン多項式環を $K[\mathbf{t}, \mathbf{t}^{-1}] = K[t_1, t_1^{-1}, \ldots, t_d, t_d^{-1}]$ で表す．また，$\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}^d$ のとき，$\mathbf{t}^\alpha = t_1^{\alpha_1} \cdots t_d^{\alpha_d}$ と表す．配置 A に対して，K 上 $\{\mathbf{t}^{\mathbf{a}_1}, \ldots, \mathbf{t}^{\mathbf{a}_n}\}$ で生成される半群環 $K[A] = K[\mathbf{t}^{\mathbf{a}_1}, \ldots, \mathbf{t}^{\mathbf{a}_n}] \subset K[\mathbf{t}, \mathbf{t}^{-1}]$ を A **のトーリック環**という．体 K 上の n 変数多項式環 $K[\mathbf{x}] = K[x_1, \ldots, x_n]$ に対して，全射準同型 $\pi : K[\mathbf{x}] \longrightarrow K[A]$ を $\pi(x_i) = \mathbf{t}^{\mathbf{a}_i}$ $(1 \leq i \leq n)$ で定義し，その核 $I_A := \ker \pi$ $(\subset K[\mathbf{x}])$ を A **のトーリックイデアル**という．一般に，トーリックイデアルは素イデアルであり，A を $d \times n$ 行列とみなせば，以下のような 2 項式で生成されることが知られている：

$$\left\{ \prod_{b_i > 0} x_i^{b_i} - \prod_{b_j < 0} x_j^{-b_j} \in K[\mathbf{x}] \;\middle|\; \mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{Z}^n,\ A\mathbf{b} = \mathbf{0} \right\}$$

また，トーリックイデアルの被約グレブナー基底は 2 項式からなることが知られている．トーリックイデアルは可換環論においては古くから研究対象であったが，１９９０年代の３大発明

(a) 整数計画問題への応用 ([CT])

(b) 分割表のマルコフ連鎖モンテカルロ法による検定への応用 ([DS])

(c) 頂点が格子点であるような凸多面体の三角形分割への応用 ([St])

を契機として，様々な分野の研究者によって注目され，研究が進められている．この原稿では，(b), (c) について簡単に紹介する．((a) については，第 10 回城崎新人セミナー報告集の鍬田英也著「グレブナー基底と整数計画問題」参照．また，紹介しきれなかった内容については，[J] を参照.)

3　頂点が格子点であるような凸多面体の三角形分割への応用

集合 $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{Z}^d$ （しばしば $d \times n$ 行列 $A = (\mathbf{a}_1 \cdots \mathbf{a}_n)$ と同一視）に対して，

$$\mathrm{Conv}(A) := \left\{ \sum_{i=1}^{n} r_i \ \mathbf{a}_i \in \mathbb{Q}^d \ \middle| \ 0 \leq r_i \in \mathbb{Q},\ \sum_{i=1}^{n} r_i = 1 \right\}$$

を A の**凸閉包**という．集合 $P \subset \mathbb{Q}^d$ が**整凸多面体**であるとは，$P = \mathrm{Conv}(A)$ をみたす有限集合 $A \subset \mathbb{Z}^d$ が存在するときにいう．

例 3.1. 配置 $A = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$ に対して，$\mathrm{Conv}(A)$ は 3 次元空間に浮かぶ四角形．

整凸多面体 P が**単体**であるとは，P の頂点数が $1 + \dim P$ であるときにいう．例えば，線分，三角形，四面体は単体である．配置 A の**被覆**とは，頂点が全て A の元であるような単体の集合 Δ で，$\mathrm{Conv}(A) = \bigcup_{F \in \Delta} F$ をみたすものをいう．配置 A の被覆 Δ が **三角形分割**であるとは，

1. F' が $F \in \Delta$ の面ならば，$F' \in \Delta$
2. $F, F' \in \Delta$ ならば，$F \cap F'$ は F の面，かつ，F' の面

が成り立つときにいう．配置 $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subset \mathbb{Z}^d$ および $K[\mathbf{x}]$ の単項式順序 $<$ に対して，

$$\Delta(\mathrm{in}_<(I_A)) := \left\{ \mathrm{Conv}(B) \ \middle| \ B \subset A,\ \prod_{\mathbf{a}_i \in B} x_i \notin \sqrt{\mathrm{in}_<(I_A)} \right\}$$

を**イニシャル複体**という．（$\sqrt{\mathrm{in}_<(I_A)}$ は $\mathrm{in}_<(I_A)$ の根基イデアル．）Sturmfels [St] は，イニシャル複体が Gelfand たちが定義した**正則**三角形分割と呼ばれる三角形分割と一致することを示した．特に，以下が成り立つ．

定理 3.2. イニシャル複体 $\Delta(\mathrm{in}_<(I_A))$ は A の三角形分割である．

配置 $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ に対して，$\mathbb{Z}A := \{\sum_{i=1}^n z_i \mathbf{a}_i \mid z_i \in \mathbb{Z}\}$ と定義する．配置 A の被覆 Δ に属する任意の極大単体 σ の頂点集合 B に対して，指数 $[\mathbb{Z}A : \mathbb{Z}B]$ を σ の**正規化体積**という．特に，σ の正規化体積が 1 であることと，$\mathbb{Z}A = \mathbb{Z}B$ は同値である．配置 A の被覆（三角形分割） Δ が **unimodular** であるとは，Δ に属する任意の極大単体 σ の正規化体積が 1 であるときにいう．もし，unimodular な三角形分割が構成できれば，極大単体の数を数えることで $\mathrm{Conv}(A)$ の正規化体積が計算できる．以下が成り立つ [St]．

定理 3.3. $\Delta(\mathrm{in}_<(I_A))$ が unimodular $\iff \sqrt{\mathrm{in}_<(I_A)} = \mathrm{in}_<(I_A)$.

また，unimodular な三角形分割の存在は，A に良い性質を保証することが知られている．例えば，以下のような性質がよく研究されている：

(i) A は **unimodular** (任意の三角形分割は unimodular) （$\Leftrightarrow$ $\sqrt{\mathrm{in}_<(I_A)} = \mathrm{in}_<(I_A)$ for $\forall <$）

(ii) A は **compressed** （$\Leftrightarrow$ 任意の逆辞書式順序 $<$ に対して，$\sqrt{\mathrm{in}_<(I_A)} = \mathrm{in}_<(I_A)$ ）

(iii) A は unimodular な正則三角形分割を持つ（$\Leftrightarrow$ $\sqrt{\mathrm{in}_<(I_A)} = \mathrm{in}_<(I_A)$ for some $<$）

(iv) A は unimodular な三角形分割を持つ

(v) A は unimodular な被覆を持つ

(vi) $K[A]$ は **正規** $(\Leftrightarrow\ \mathbb{Z}_{\geq 0}A = \mathbb{Z}A \cap \mathbb{Q}_{\geq 0}A\ )$

一般に，(i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (v) ⇒ (vi) が成り立つが，それぞれの逆は正しくない．特に，条件 (vi) は可換環論だけではなく，次章で述べる代数統計の分野でも重要であり，その十分条件としてグレブナー基底に関連した条件 (i), (ii), (iii) がよく研究されている．ただし，一般論で色々なことを証明するのはなかなか困難である．有限グラフやマトロイドなど，組合せ論的な対象から配置（トーリックイデアル）を構成し，その配置がいつ上記の条件をみたすかをグラフやマトロイドの言葉で記述するような研究が盛んになされており，有用な特徴付けを活用して重要な例も構成されている．例えば [OH] では，グラフに付随する辺凸多面体で (iv) をみたすが (iii) をみたさないものを構成しているが，このような例は辺凸多面体以外では見つかっていない．

4　分割表のマルコフ連鎖モンテカルロ法による検定への応用

例えば，以下の表 ([J, 第 4 章]) は 5×5 の 2 元分割表である．

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**

このデータに関して，代数と統計の成績に関連があるのかどうかを調べるため，関連がないという仮説（帰無仮説）を立て，検定するという手法が取られる．通常は，検定統計量の漸近分布を利用するが，例えば，この例のように 0 が多い表の場合，漸近分布の当てはまりが良くないことがある．その場合，もとのデータと同じ行和，列和を持つ表全体

$$F = \left\{ T = (t_{ij}) \;\middle|\; \begin{array}{ccccc|c} & & t_{ij} & & & \mathbf{4} \\ & & & & & \mathbf{14} \\ & & & & & \mathbf{5} \\ & & & & & \mathbf{2} \\ & & & & & \mathbf{1} \\ \hline \mathbf{10} & \mathbf{6} & \mathbf{5} & \mathbf{2} & \mathbf{3} & \mathbf{26} \end{array} \;,\quad 0 \leq t_{ij} \in \mathbb{Z} \right\}$$

を考え，F に属するすべての表について，統計量を計算し，もとのデータの統計量と比較する手法が取られる（Fisher の正確検定）．ところが，F の元が列挙不可能なほど多いときにはこの方法も使えない.（この例の場合，$\sharp|F| = 229,174$ である.）そのような場合には，マルコフ連鎖モンテカルロ法を用いて，F 上をランダムウォークして，F の元をサンプリングし，統計量を計算することによって分析する．例えば，$\sum \alpha_i = \sum \beta_j$ をみたす α_i, β_j に対して，

$$F = \left\{ T = (t_{ij}) \;\middle|\; \begin{array}{ccc|c} t_{11} & t_{12} & t_{13} & \alpha_1 \\ t_{21} & t_{22} & t_{23} & \alpha_2 \\ \hline \beta_1 & \beta_2 & \beta_3 & \end{array} \;,\ 0 \leq t_{ij} \in \mathbb{Z} \right\}$$

の任意の 2 元は $M = \left\{ \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \right\}$ の元を足したり引いたりすることで F の元を経由して移り合えるので，これを用いて F 上のランダムウォークを行う．このような M を**マルコフ基底**という．この例（2×3 分割表）の場合，配置として以下のような行列を考えれば，I_A の生成系と，M が対応していることが見て取れる：

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \quad A \begin{pmatrix} t_{11} \\ t_{12} \\ t_{13} \\ t_{21} \\ t_{22} \\ t_{23} \end{pmatrix} = \begin{pmatrix} t_{11}+t_{12}+t_{13} \\ t_{21}+t_{22}+t_{23} \\ t_{11}+t_{21} \\ t_{12}+t_{22} \\ t_{13}+t_{23} \end{pmatrix}.$$

$$I_A = \langle x_1x_5 - x_2x_4, \quad x_1x_6 - x_3x_4, \quad x_2x_6 - x_3x_5 \rangle .$$

（注意：2 元表の場合は，トーリックイデアルを持ち出さなくてもマルコフ基底は容易に分かる．）一般に以下が成り立つ [DS].

定理 4.1. 検定を行う統計モデルに対応する行列 A の核に属する有限個の整数行列からなる集合がマルコフ基底であることと，対応する 2 項式の集合が I_A の生成系をなすことは同値である．

よって，I_A の有限生成系を求めることができれば，マルコフ基底を構成することができる．例えば，簡単のため，各 $\mathbf{a}_i$ が非負整数ベクトルであるとすると，$J_A = \langle x_1 - \mathbf{t}^{\mathbf{a}_1}, \ldots, x_n - \mathbf{t}^{\mathbf{a}_n} \rangle \subset K[\mathbf{x}, \mathbf{t}]$ に対して $I_A = J_A \cap K[\mathbf{x}]$ が成り立つので消去法によって I_A の有限生成系が求まる．しかし，残念ながら多くの場合にこの方法は非実用的である．高次元の表に対しては，（いくつかのクラスを除いて）I_A の生成系は未解明であり，計算困難である．そのため，toric fiber 積 [Su] や，入れ子配置 [AHOT] など，大規模なトーリックイデアルを，いくつかの小規模なトーリックイデアルに分解するような理論の開発が試みられている．

参考文献

[AHOT] S. Aoki, T. Hibi, H. Ohsugi and A. Takemura, Gröbner bases of nested configurations, *J. Algebra* **320** (2008), 2583–2593.

[CT] P. Conti and C. Traverso, Buchberger algorithm and integer programming, *in* Proceedings of AAECC-9 (New Orleans) Springer LNCS 539 (1991), 130–139.

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

[J] JST CREST 日比チーム編，グレブナー道場，共立出版，2011.

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

[St] B. Sturmfels, Gröbner bases of toric varieties, *Tohoku Math. J.* **43** (1991), 249–261.

[Su] S. Sullivant, Toric fiber products, *J. Algebra* **316** (2007), 560–577.