無限生成イデアルの有限生成系について

Finite Generators for Ideals from Parameterized Families

九州産業大学理工学部　　渋田 敬史 *1
Takafumi Shibuta
Faculty of Science and Engineering, Kyushu Sangyo University

Abstract

This paper studies ideals that are generated by infinitely many polynomials depending on integer parameters. In general, computing a finite generating set is undecidable. We focus on a simple but useful setting: the exponents depend linearly on the parameters, and the coefficients are parameter polynomials. In this case, we show that one can find a finite generating set whose indices lie in an explicit box. The side lengths of this box depend only on the degrees of the coefficient polynomials. We also discuss binomial ideals with higher-degree exponents to show how the picture changes beyond the linear case.

1　はじめに

ヒルベルトの基底定理により，多項式環 $\mathbb{Q}[x_1,\dots,x_r]$ の任意のイデアルは有限生成である（ネーター性）[3, 2]．しかし，無限個の多項式で生成されたイデアルから具体的な有限生成系を取り出すことは容易でない．

無限個の多項式で生成されるイデアル $I=\langle f_n \mid n\in\mathbb{Z}_{\geq 0}\rangle$ を考える．$I_n:=\langle f_0,\dots,f_n\rangle$ は昇鎖 $I_0\subset I_1\subset\cdots$ をなし，いずれは安定するが，有限区間での見かけの停滞 $I_{n_0}=I_{n_0+1}=\cdots=I_{n_0+k}$ がただちに $I=I_{n_0}$ を意味するわけではない．例として

$$f_n=x+\gcd\bigl(n^5+5,(n+1)^5+5\bigr)\in\mathbb{Q}[x]$$

では $f_0=\cdots=f_{533359}=x+1$ だが $f_{533360}=x+1968751$ となり，結局 $I=\mathbb{Q}[x]$ である．

$p,r,N\in\mathbb{Z}_{>0}$ を固定し，パラメータ $\mathbf{n}=(n_1,\dots,n_p)$ に関する係数多項式 $c_k(\mathbf{n})\in\mathbb{Q}[\mathbf{n}]=\mathbb{Q}[n_1,\dots,n_p]$（$1\leq k\leq N$）と，$\mathbb{Z}^p_{\geq 0}$ に対し非負整数値をとる指数多項式 $\mathbf{p}_k(\mathbf{n})\in(\mathbb{Z}[\mathbf{n}])^r$ に対し，

$$f_{\mathbf{n}}(\mathbf{x})=\sum_{k=1}^{N}c_k(\mathbf{n})\mathbf{x}^{\mathbf{p}_k(\mathbf{n})}\in\mathbb{Q}[\mathbf{x}]=\mathbb{Q}[x_1,\dots,x_r],\qquad I=\langle f_{\mathbf{n}}\mid\mathbf{n}\in\mathbb{Z}^p_{\geq 0}\rangle$$

とすると，まったく一般の枠組では整係数多変数不定方程式の非負整数解の存在の決定不能性（MRDP 定理 [4]）により，I の有限生成系は計算不能である．整数係数多項式 $p(\mathbf{n})\in\mathbb{Z}[\mathbf{n}]$ に対し，イデアル

$$I=\langle x^{p(\mathbf{n})^2}\mid\mathbf{n}\in\mathbb{Z}^p_{\geq 0}\rangle$$

*1 〒 813-8503 福岡市東区松香台 2-3-1　E-mail: tshibuta@ip.kyusan-u.ac.jp

を考える．$D = \min\{p(\mathbf{n})^2 \mid \mathbf{n} \in \mathbb{Z}^p_{\geq 0}\}$ とおくと，I は x^D で生成されるが，$D = 0$ であることと，方程式 $p(\mathbf{n}) = 0$ が非負整数解を持つ事は同値であるので，I の有限生成系を計算するアルゴリズムは存在しないことになる．

一方，Fermat 型の族 $F_n = x^n + y^n - z^n$ に対しては，漸化式

$$F_{n+3} = (xyz)F_n - (xy + yz + zx)F_{n+1} - (x + y + z)F_{n+2}$$

が知られており，$\langle F_n \mid n \geq 3\rangle = \langle F_3, F_4, F_5\rangle$ が成り立つ [1]．

本稿では，指数部分がパラメータに関する一次式で係数がパラメータ多項式の場合に，係数次数のみから決まる上界で有限生成を見つけることができるという主定理を述べ，最後に指数の次数が高い場合の例として二項式イデアルを扱う．

2　指数部分が一次式の場合

論文 [1] では Fermat 型の族 $F_n = x^n + y^n - z^n$ に対する漸化式

$$F_{n+3} = (xyz)F_n - (xy + yz + zx)F_{n+1} - (x + y + z)F_{n+2}$$

を Gröbner 基底を用いて導出したが，これは次のように母関数 $\varphi(t) = \sum_{n\geq 0} F_n t^n$ を考えることで導くこともできる．

$$\sum_{n\geq 0} F_n t^n = \sum_{n\geq 0}(x^n + y^n - z^n)t^n = \frac{1}{1-xt} + \frac{1}{1-yt} - \frac{1}{1-zt}$$

に $(1-xt)(1-yt)(1-zt)$ を掛けて t^{n+3} の係数比較をすると

$$F_{n+3} - (xyz)F_n + (xy + yz + zx)F_{n+1} - (x + y + z)F_{n+2} = 0$$

を得る．このように母関数が分母の定数項が 1 である有理関数になる場合は項の間の漸化式を得ることができ，イデアルの有限生成系を求めることが可能となる．

$p, r, N \in \mathbb{Z}_{>0}$ を固定し，係数多項式 $c_k(\mathbf{n}) \in \mathbb{Q}[\mathbf{n}] = \mathbb{Q}[n_1, \ldots, n_p]$（$1 \leq k \leq N$），指数行列 $A_k \in \mathbb{Z}^{r\times p}_{\geq 0}$，ベクトル $\gamma_k \in \mathbb{Z}^r_{\geq 0}$ に対し

$$f_{\mathbf{n}}(\mathbf{x}) = \sum_{k=1}^{N} c_k(\mathbf{n})\mathbf{x}^{A_k\mathbf{n}+\gamma_k} \in \mathbb{Q}[\mathbf{x}], \qquad I = \langle f_{\mathbf{n}} \mid \mathbf{n} \in \mathbb{Z}^p_{\geq 0}\rangle.$$

各 j に対し $\ell_j := \sum_{k=1}^{N}(\deg_{n_j} c_k + 1) - 1$ と置く．

母関数 $\sum_{\mathbf{n}\in\mathbb{Z}^p_{\geq 0}} f_{\mathbf{n}}(\mathbf{x})\mathbf{t}^{\mathbf{n}}$ が分母の定数項が 1 である有理関数になり，その次数が係数多項式の次数から決定されることはよく知られている．このことを利用すると次の定理を証明することができる．

定理 1 ([5])
$\langle f_{\mathbf{n}} \mid \mathbf{n} \in \mathbb{Z}^p_{\geq 0}\rangle = \langle f_{\mathbf{n}} \mid 0 \leq n_j \leq \ell_j\ (1 \leq j \leq p)\rangle$.

すなわち，係数多項式の次数だけから決まる単純な上界により有限生成系が与えられる．

例 1
$R = \mathbb{Q}[x, y, z]$ とし，

$$f_{n,m} = (n^2 - m)x^{n+m+2} + (nm^4 + m^2)x^{2n+m+1}z^{m+n+3} + (n^5 + n^2)y^{4n+m+2} \in R$$

と定める．係数 $n^2-m,\ nm^4+m^2,\ n^5+n^2$ の n に関する次数は $2,1,5$ であり，m に関する次数は $1,4,0$ である．したがって

$$\ell_1=(2+1)+(1+1)+(5+1)-1=10,\qquad \ell_2=(1+1)+(4+1)+(0+1)-1=7.$$

よって定理 *1* より，$\langle f_{n,m}\mid n,m\in\mathbb{Z}_{\geq 0}\rangle=\langle f_{n,m}\mid 0\leq n\leq 10,\ 0\leq m\leq 7\rangle$.

例 2
$R=\mathbb{Q}[x,y,z,w]$ とし，

$$g_n=xy^{n+1}+z^{n+1}+w^{n+1},\qquad f_n=g_{n^3}=xy^{n^3+1}+z^{n^3+1}+w^{n^3+1}$$

と定める．イデアル

$$I_1=\langle f_n\mid n\in\mathbb{Z}_{\geq 0}\rangle\subset R,\qquad J_1=\langle f_0,f_1,f_2,f_3\rangle=\langle g_0,g_1,g_8,g_{27}\rangle$$

を考える．*Gröbner* 基底を用いた計算により，$28,29$ は立方数ではないにもかかわらず $g_{28},g_{29}\in J_1$ が成り立つことが分かる．一方，定理 *1* より，

$$\langle g_{n+27}\mid n\in\mathbb{Z}_{\geq 0}\rangle=\langle g_{27},g_{28},g_{29}\rangle.$$

したがって $n\geq 27$ に対して $g_n\in J_1$ が従う．特に $n\geq 3$ なら $f_n=g_{n^3}\in J_1$ である．以上より $I_1=J_1$ を得る．

3　二項式イデアル

イデアルを二項式イデアルに限っても，全く一般の場合は有限生成系を求めることはできない．整数係数多項式 $p(\mathbf{n})\in\mathbb{Z}[\mathbf{n}]$ に対し，

$$\langle x^{p(\mathbf{n})^2+1}-x^{p(\mathbf{n})^2}\mid \mathbf{n}\in\mathbb{Z}^p_{\geq 0}\rangle=\langle x^{p(\mathbf{n})^2}(x-1)\mid \mathbf{n}\in\mathbb{Z}^p_{\geq 0}\rangle$$

が $\langle x-1\rangle$ であることは方程式 $p(\mathbf{n})=0$ が非負整数解を持つ事は同値である．したがって，指数部分の形にある程度の制約を設けなければならない．ここでは，次で定義される形の多項式のみを指数として認めることとする．

定義 2
有限集合 $\Lambda\subset\mathbb{Z}^p_{\geq 0}$ と非負整数 $a_{k_1,\dots,k_p}$ により

$$c(\mathbf{w})=c(w_1,\dots,w_p)=\sum_{(k_1,\dots,k_p)\in\Lambda}a_{k_1,\dots,k_p}\binom{w_1}{k_1}\cdots\binom{w_p}{k_p}$$

と書ける $\mathbf{w}=(w_1,\dots,w_p)$ の多項式全体を $\mathbf{B}_p$ で表す．

$\mathbf{B}_p$ の元 $c(w_1,\dots,w_p)$ について，次が成り立つ：

- 任意の $(n_1,\dots,n_p)\in\mathbb{Z}^p_{\geq 0}$ に対し $c(n_1,\dots,n_p)\in\mathbb{Z}_{\geq 0}$．
- 各 i に対し，差分 $c(\dots,w_i+1,\dots)-c(\dots,w_i,\dots)$ も $\mathbf{B}_p$ に属する．

ある場合にはテレスコープ型変形により，有限生成系を求める問題を，より単純な問題に帰着することができる．可換環 R と $f_n, p_n \in R$ に対し，

$$\langle f_n \mid n \geq 0\rangle = \langle f_0,\ fn+1-p_nf_n \mid n \geq 0\rangle,$$

$f_{n,m}, p_n \in R$ に対し，

$$\langle f_{n,m} \mid n,m \geq 0\rangle = \langle f_{0,m} \mid m \geq 0\rangle + \langle f_{n+1,m} - p_nf_{n,m} \mid n,m \geq 0\rangle$$

が成り立つ．$f_{n+1}-p_nf_n$ や $f_{0,m}, f_{n+1,m}-p_nf_{n,m}$ が元の生成元よりも単純な構造になっていれば，問題が解きやすくなる．

例えば，$p_n \in \mathbb{Q}[x,\mathbf{y}]$ の指数は n の一次式であるとし，$n \in \mathbb{Z}_{\geq 0}$ に対し，多項式列

$$f_n = x^{n^2+1} + p_n \in \mathbb{Q}[x,\mathbf{y}]$$

を考える．

$$\begin{aligned} g_n &:= f_{n+1} - x^{2n+1}f_n \\ &= x^{(n+1)^2+1} + p_{n+1} - x^{2n+1}\Big(x^{n^2+1}+p_n\Big) \\ &= p_{n+1} - x^{2n+1}p_n \end{aligned}$$

とおくと，

$$\langle f_n \mid n \geq 0\rangle = \langle f_0\rangle + \langle g_n \mid n \geq 0\rangle$$

となる．g_n は指数部分が一次式となり，定理 1 により有限生成系を求めることができる．

このテレスコープ型の変形と次の補題を組み合わせることで，指数部分が $\mathbf{B}_p$ の形の二項式イデアルを，指数の次数がより低い場合に帰着することができ，定理 1 により有限生成系を求めることができるようになる．

補題 3

$p_n \in \mathbb{Q}[\mathbf{x}]$ が $n \leq m$ のとき $p_n \mid p_m$ を満たすとする．$f_n \in \mathbb{Q}[\mathbf{x}]$ が

$$\langle f_n \mid n \in \mathbb{Z}_{\geq 0}\rangle = \langle f_1, \ldots, f_\ell\rangle$$

を満たすとき，

$$\langle p_nf_n \mid n \in \mathbb{Z}_{\geq 0}\rangle = \langle p_1f_1, \ldots, p_\ell f_\ell\rangle$$

が成り立つ．

証明 $f_m \in \langle f_n \mid n \leq \ell\rangle$ より $f_m = \sum_{n\leq\ell} g_nf_n$ と書ける．よって

$$p_mf_m = \sum_{n\leq\ell} g_n\,(p_m/p_n)\,p_nf_n \ \in \langle p_nf_n \mid n \leq \ell\rangle.$$

∎

さて，$\boldsymbol{\alpha}(\mathbf{w}), \boldsymbol{\beta}(\mathbf{w}) \in \mathbf{B}_p^r$ をとり，

$$f_{\mathbf{n}} = \mathbf{x}^{\boldsymbol{\alpha}(\mathbf{n})} - \mathbf{x}^{\boldsymbol{\beta}(\mathbf{n})} \ \in \mathbb{Q}[\mathbf{x}] = \mathbb{Q}[x_1, \ldots, x_r], \quad I = \langle f_{\mathbf{n}} \mid \mathbf{n} \in \mathbb{Z}_{\geq 0}^p\rangle$$

とする．各 i に対し $\ell_i = \deg_{w_i}(\boldsymbol{\alpha}, \boldsymbol{\beta})$ とおく．ただし，$\boldsymbol{c} = \big(c_1, \ldots, c_r\big) \in \mathbb{Q}[\mathbf{w}]^r$ に対し

$$\deg_{w_i} \boldsymbol{c} := \max\big\{\deg_{w_i} c_1, \ldots, \deg_{w_i} c_r\big\}.$$

このとき，次が成り立つ．

定理 4
$\langle \mathbf{x}^{\boldsymbol{\alpha}(\mathbf{n})} - \mathbf{x}^{\boldsymbol{\beta}(\mathbf{n})} \mid \mathbf{n} \in \mathbb{Z}^p_{\geq 0} \rangle = \langle \mathbf{x}^{\boldsymbol{\alpha}(\mathbf{n})} - \mathbf{x}^{\boldsymbol{\beta}(\mathbf{n})} \mid 0 \leq n_j \leq \ell_j \ (1 \leq j \leq p) \rangle$.

すなわち，指数部分の次数だけから決まる単純な上界により有限生成系が与えられる．

謝　辞

本研究は JSPS 科研費 JP22K03334 の助成を受けたものです．

参 考 文 献

[1] B. Buchberger, J. Elías, *Using Gröbner bases for detecting polynomial identities: a case study on Fermat's ideal*, J. Number Theory **41** (1992), no. 3, 272–279.

[2] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, 3rd ed., Springer, 2007.

[3] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), no. 4, 473–534.

[4] Y. V. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, 1993.

[5] T. Shibuta, *On finite generating sets of infinitely generated ideals*, Proc. Amer. Math. Soc. **153** (2025), no. 11, 4535–4543.