Semi-regularな斉次多項式列のGröbner基底の各次数における先頭項とその数

The leading terms of the Gröbner bases of semi-regular homogeneous polynomial sequences at each degree

東京大学大学院情報理工学系研究科　　坂田 康亮 *1
Kosuke Sakata
Department of Mathematical Informatics, University of Tokyo

東京大学大学院情報理工学系研究科　　高木 剛 *2
Tsuyoshi Takagi
Department of Mathematical Informatics, University of Tokyo

Abstract

A Gröbner basis is a system in the field of algebra that captures the favorable behavior of ideals generated by polynomial sets. When investigating the ideals of a given polynomial set, computing its Gröbner basis can often lead to solutions, making it a useful tool. Consequently, it finds applications in various fields such as algebraic geometry, discrete mathematics, statistics, and cryptography. Therefore, research on algorithms to compute Gröbner bases and their properties not only impacts algebra but also contributes to the advancement of applications involving Gröbner bases. One specific focus of Gröbner basis research is on polynomial sets known as semi-regular sequences. Polynomial sets generated "randomly" exhibit characteristics known as generic, and it is expected that such sets become semi-regular sequences. Additionally, it is believed that semi-regular homogeneous polynomial sequences satisfy the Moreno-Socías conjecture.

This paper introduces an algorithm to compute the leading terms of Gröbner bases for semi-regular homogeneous polynomial sequences proposed in a previous paper. While obtaining the leading terms of Gröbner bases typically requires complete Gröbner basis calculations, the proposed algorithm computes only the leading terms, allowing for faster computation. By restricting the polynomial sequences to semi-regular homogeneous ones and assuming the Moreno-Socías conjecture, this computation becomes feasible.

1　導入

Gröbner基底とは代数学における分野の一つで，多項式列が生成するイデアルにおける良い振る舞いを生成系である．ある多項式列のイデアルを調べるときに，そのGröbner基底を計算することで解決されることがあり，有用な手段とされる．そのため，応用分野が多く，代数幾何，離散数学，統計学，暗号学など幅広く利用される．よって，Gröbner基底やその特性を求めるアルゴリズムの研究は代数学のみならず，Gröbner

*1 〒 113-8656 東京都文京区本郷 7-3-1　E-mail: sakata-kosuke-rb@g.ecc.u-tokyo.ac.jp
*2 〒 113-8656 東京都文京区本郷 7-3-1　E-mail: takagi@mist.i.u-tokyo.ac.jp

基底の応用研究の発展に影響を与える．Gröbner 基底の研究対象の一つとして semi-regular 列と呼ばれる多項式列がある．“ランダムに” 生成された多項式列は generic と呼ばれる特性を持ち，そのような多項式列は semi-regular 列となることが予想されている [1]．また，semi-regular な斉次多項式列は Moreno-Socías 予想 [1] が成立すると考えられている．

この論文は，論文 [2] で提案された semi-regular な斉次多項式列の Gröbner 基底の各次数における先頭項を算出するアルゴリズムを紹介する．Gröbner 基底の先頭項を得るには Gröbner 基底計算をする必要があるが，提案されたアルゴリズムは Gröbner 基底の先頭項のみを算出するため，高速に計算できる．計算する対象の多項式列を semi-regular な斉次多項式列に限定し，Moreno-Socías 予想を仮定することで，この計算が可能になっている．

2　準備

k は無限体とする．R を k を体，$x_1, ..., x_n$ を変数とする多項式環とする．変数の積で表現される R の要素を単項式と呼ぶ．R_d を R の次数 d の単項式の集合とする．単項式 $t, u \in R$ に関して，t が u を割り切るとき $t \mid u$ と表記する．t の次数は $\deg(t)$ と表記する．R の単項式順序には全次数逆辞書式順序が入っているとする．多項式 $f \in R$ を構成する単項式の中で，単項式順序による最大の単項式を $\mathrm{LM}(f)$ と表記する．$F \subset R$ を多項式列とし，F が生成するイデアルを $\langle F \rangle$ と表記する．$I \subset R$ をイデアル，$G \subset R$ を多項式の集合とする．任意の $f \in R$ に対して，$\mathrm{LM}(g) \mid \mathrm{LM}(f)$ となる $g \in G$ が必ず存在するとき G を I の Gröbner 基底と呼ぶ．

定義 1
[1] I を斉次イデアル，多項式 $f \in R$ の次数は d とする．任意の自然数 $e \geq d$ において，f による線形写像 $(R/I)_{e-d} \to (R/I)_e$ がフルランクのとき，f は R/I 上で semi-regular と呼ぶ．

全ての $i = 1, \ldots, m$ に関して，f_i が $R/\langle f_1, \ldots, f_{i-1} \rangle$ 上で semi-regular のとき，斉次多項式列 $\{f_1, \ldots, f_m\}$ は semi-regular 列と呼ぶ．

$d \geq 0$ を整数とする．以下，$I \subset R$ は斉次イデアルとし，$F = \{f_1, ..., f_m\}$ はイデアル I を生成する斉次多項式列とする．I_d を次のように定義する．

$$I_d = \{f \in I \mid f \text{ は次数 } d \text{ で斉次 }\} \cup \{0\}$$

Hilbert 関数と Hilbert 級数を次のように定義する．

定義 2
剰余環 R/I の Hilbert 関数を次のような関数として定義し，

$$\begin{array}{rccc} h_{R/I}: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & d & \longmapsto & \dim_k(R/I)_d, \end{array}$$

関数 $h_{R/I}$ を用いて，剰余環 R/I の Hilbert 級数 $H_{R/I}(z)$ を次のような級数として定義する．

$$H_{R/I}(z) = \sum_{d \geq 0} h_{R/I}(d) z^d.$$

定義 3
$\sum_{i=0}^{\infty} a_i z^i$ は $a_i \in \mathbb{Z}$ で構成される級数とする．$[\sum_{i=0}^{\infty} a_i z^i]$ は次のようにして得られる数列 $\{b_i\}_{i \geq 0}$ による級数 $\sum_{i=0}^{\infty} b_i z^i$ とする：全ての $0 \leq j \leq i$ に関して $a_j > 0$ のとき $b_i = a_i$ で，そうでないとき $b_i = 0$.

命題 4

$\{f_1, ..., f_m\}$ は斉次多項式列で，f_i の次数は d_i とする．$\{f_1, ..., f_m\}$ が *semi-regular* であることと，次が成り立つことは同値である．

$$\text{全ての } 1 \leq s \leq m \text{ に関して } H_{R/\langle f_1,...,f_s\rangle}(z) = \left[\frac{\prod_{i=1}^{s}(1-z^{d_i})}{(1-z)^n}\right].$$

定義 5

[1] $J \subset R$ を単項式イデアルとする．J は次の条件を満たすとき，*weakly reverse lexicographic ideal* と呼ぶ：任意の *minimal generator* $m \in J$ に関して，$m' > m$ かつ $\deg(m') = \deg(m)$ を満たす $m' \in R$ は $m' \in J$.

次の予想は Moreno-Socías 予想と呼ばれる．

予想 6

[1] F は *generic* な斉次多項式列とする．$I = \langle F\rangle$ とし，$J = \langle \mathrm{LT}(I)\rangle$ とする．このとき，J は *weakly reverse lexicographic ideal* である．

以下，この論文では Moreno-Socías 予想が正しいことを仮定して話を進める．すると，論文 [1] の定理 2 から，generic な斉次多項式列は semi-regular な斉次多項式列と同値である．つまり，semi-regular 列が予想 6 に従うことを仮定する．

3 Gröbner 基底の先頭項を算出するアルゴリズム

論文 [2] は連立二次代数方程式問題 (MQ 問題) を Gröbner 基底計算を用いて高速に解くアルゴリズムを提案している．論文中では，Gröbner 基底の各次数の先頭項を算出するアルゴリズムを提案している．以下に示すアルゴリズムは論文 [2] のアルゴリズムを拡張したアルゴリズムである．

Algorithm 1 Gröbner 基底の先頭項と個数の算出アルゴリズム

Require: 整数 n, m

Ensure: 変数の数 n の semi-regular な斉次多項式列 $F = \{f_1, ..., f_m\}$ の各次数 d の Gröbner 基底の先頭項 $\{L_d\}_{d\geq 0}$ とその数 $\{N_d\}_{d\geq 0}$

$H_{R/\langle F\rangle}(z) \leftarrow \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}, (d_i = \deg(f_i))$
$L_0 \leftarrow \varnothing$
$d \leftarrow 0$
while $H_{R/\langle F\rangle}(z) \neq H_{R/\langle \mathrm{LT}(F)\rangle}$ **do**
  $B_d \leftarrow \{m \in M_d \mid m \notin \langle L_0 \cup \cdots \cup L_{d-1}\rangle\}$
  $N_d \leftarrow \#B_d - h_{R/\langle F\rangle}(d)$
  $L_d \leftarrow \{B_d$の順序が大きい方から N_d個 $\}$
  $d \leftarrow d + 1$
end while
return $\{L_d\}_{d\geq 0}, \{N_d\}_{d\geq 0}$

4　計算実験

3 章のアルゴリズムの性能を計算実験により確かめた．semi-regular な斉次多項式列が与えられたときに，その Gröbner 基底の各次数の先頭項またはその数を計算することを問題設定とし，その計算時間を比較する．比較するアルゴリズムは以下の 3 つとした．

手法 1. 計算ソフト Magma を使用した有理数体上の Gröbner 基底計算

手法 2. 計算ソフト Magma を使用した有限体 $\mathbb{F}_{127}$ の Gröbner 基底計算

手法 3. C++での実装による 3 章のアルゴリズム

従来の方法として，手法 1 と手法 2 では Gröbner 基底計算をすることで Gröbner 基底の各次数の先頭項とその数を求めている．手法 1 では無限体として有理数体を使用しているが，これは整数環よりも計算が速いためであり，無限体の中でも高速なものを選択するためである．手法 2 では有限体を選択しているが，一般に有限体の方が高速に Gröbner 基底を計算でき，これは Magma でも同様であり，比較対象として挙げた．各方法に関して計算時間と使用メモリ量を比較した．

計算に使用した問題は係数がランダムに与えられた semi-regular な多変数二次斉次多項式列で，その変数の数を n，多項式の数を m とする．次の 3 つのタイプの多項式列を計算実験に使用した．

- $n = m - 3$
- $n = m$
- $n = m + 1$

計算実験では Intel Core i7-10850H@2.7GHz の CPU と 16GB の RAM の計算機を使用した．

表 1,2,3 は計算した問題の異なる計算時間の比較の表であり，表 4,5,6 は計算した問題の異なる使用メモリ量の比較の表である．計算時間，使用した計算機の制限，またはプログラム起動によるオーバーヘッド，最低メモリ使用量の制限を踏まえて各グラフの線は描いている．計算時間，メモリ使用量ともに手法 3，手法 2，手法 1 の順番で良い結果が得られている．

計算時間に関して，n と m の差が大きいほど提案手法が効率的であることがわかった．問題のタイプ $n = m - 3$ では手法 1 と手法 3 を比較すると手法 3 は約 170000 倍速い．計算時間と使用した計算機が理由で他の問題のタイプは比較できなかったが，他の問題のタイプでは更なる効率化が見込めることはグラフからわかる．手法 2 と手法 3 を比較すると手法 3 の方が約 270〜3000 倍速い．今回使用したパラメータにおいては以上のような倍率となったが，グラフからわかる通り変数の数が大きくなるほど，つまり，問題が難しくなるほど手法 3 の比較倍率は大きくなる．

メモリ使用量に関しても，n と m の差が大きいほど提案手法が効率的であることがわかった．手法 1 と手法 3 は純粋な比較ができなかったが，手法 3 は圧倒的に使用メモリ量が少ない．手法 2 と手法 3 を比較すると，手法 3 は約 120〜400 倍メモリ使用量が少ない．メモリ使用量に関しても，今回使用したパラメータにおいては以上のような倍率となったが，グラフからわかる通り変数の数が大きくなるほど，つまり，問題が難しくなるほど手法 3 の比較倍率は大きくなる．

手法 3 が高速で省メモリな理由は Gröbner 基底計算をせずに Gröbner 基底の先頭項を求めているからである．

5　アルゴリズムの応用

3 章のアルゴリズムは Gröbner 基底計算をせずに，Gröbner 基底の先頭項を算出することが可能であるため，Gröbner 基底の先頭項を計算したい場合で，計算する対象が semi-regular な斉次多項式列な場合に有効である．

Gröbner 基底計算においては，アルゴリズムの出力のひとつである $\{N_d\}_{d\geq 0}$ が有用である．ある次数 d の Gröbner 基底計算を進めているとする．このとき，現在求まっている次数 d の基底の数が N_d が一致している場合は，以降の計算で次数 d の基底の要素は求まらないことから，次数 d の計算は終えて良いことがわかる．これは Hilbert-driven アルゴリズム [3] の類似であるが，$\{N_d\}_{d\geq 0}$ を先に計算しておいた場合，Hilbert-driven アルゴリズムの手続きにおける多くの回数を必要とされる Hilbert 級数の計算を省くことができるので，高速に計算できる．もし，次数 d の Gröbner 基底計算で基底となる計算のみ可能であった場合 (計算する S 多項式が全て 0 に簡約されない場合)，無駄な多項式の計算をせずに Gröbner 基底が求まる．そのような方法を仮定する場合，F4[4] の更なる高速化が見込める．論文 [2] では，問題の対象を MQ 問題に限定することで，そのような方法が経験的に判明しており，Gröbner 基底計算の高速化に成功している．また，非斉次イデアルの計算に関しては，Gröbner 基底計算の途中まで (計算する多項式の次数が落ちるまで，または，$\{N_d\}_{d\geq 0}$ の 0 でない最大の d まで) 計算に使用できることを論文 [2] に記している．理論は無限体上の多項式環であることを前提に展開されているため，有限体上の多項式環では必ずしも正しくないが，その場合の妥協案と成功確率は論文 [2] に記している．実際，有限体であっても体の要素数が十分に大きければ無限体に近い振る舞い (演算の結果 0 になりにくい) をするためである．

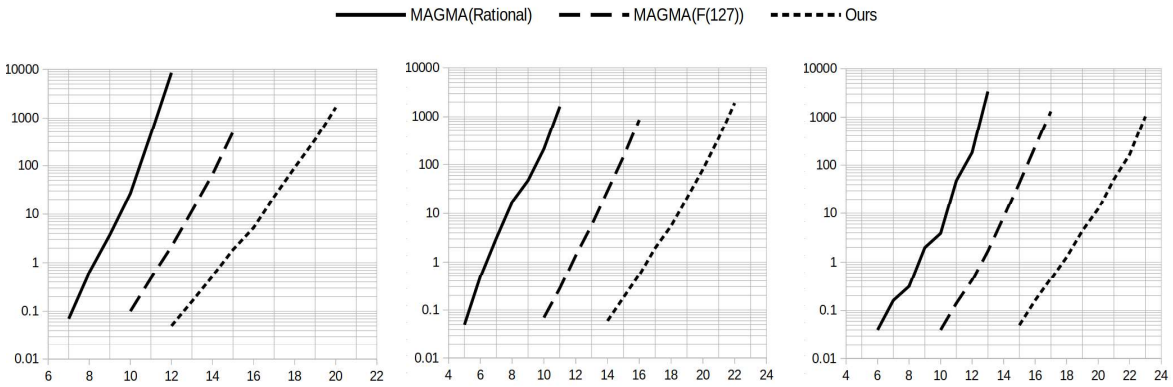

図 1: 計算時間 [s]$(n = m - 3)$　図 2: 計算時間 [s]$(n = m)$　図 3: 計算時間 [s]$(n = m + 1)$

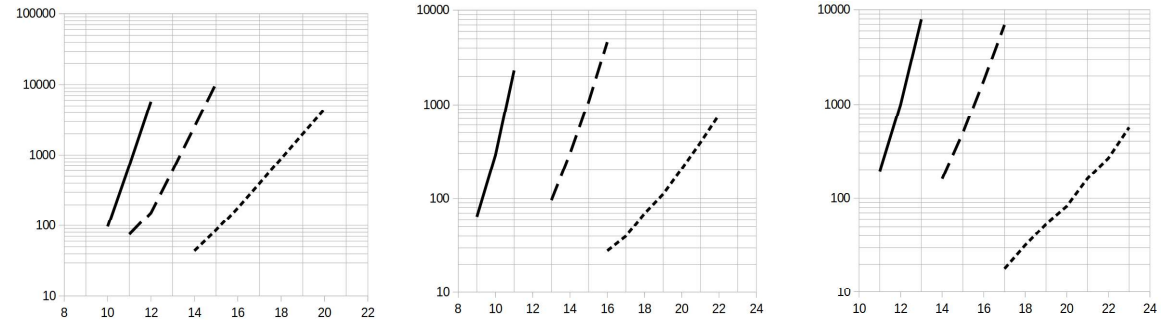

図 4: メモリ使用量 [kB]$(n = m - 3)$　図 5: メモリ使用量 [kB]$(n = m)$　図 6: メモリ使用量 [kB]$(n = m + 1)$

謝　辞

本研究は総務省「電波資源拡大のための研究開発 (JPJ000254)」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の一環として実施したものである.

参 考 文 献

[1] Pardue K., “Generic Sequences of Polynomials”, Journal of Algebra, 324(4), 579-590, 2010.

[2] Sakata K., Takagi T., “An Efficient Algorithm for Solving the MQ Problem using Hilbert Series”, IACR Cryptol. ePrint Arch. 2023: 1650, 2023.

[3] Traverso C., “Hilbert functions and the buchberger algorithm.”, Journal of Symbolic Computation, 22(4), 355-376, 1996.

[4] Faugère J.-C., “A new efficient algorithm for computing Gröbner Bases (F4)”, Journal of Pure and Applied Algebra, 139, 6–88, 1999.