数理解析研究所講究録 1456 巻 2005 年 206-213

Discrete Comprehensive Gröbner Bases と計算比較

倉田 陽介*
立命館大学 理工学研究科
佐藤 洋祐†
東京理科大学 理学部 情報数理科学科

Abstract

Sato, Suzuki, Nabeshima によって提示された, ACGB on Varieties の理論をもとにした discrete comprehensive Gröbner Bases アルゴリズムで得られる Von Neumann regular ring 上の Gröbner basis と, 通常の体上の Gröbner basis は Sato による Stability of Gröbner bases の理論により同一視することができるが, それらを得るための計算の方法が異なるため, それぞれの方法で計算を行い, それぞれの速度の比較を行った.

1 Introduction

Weispfenning[8] によって提示された, Comprehensive Gröbner Bases の理論とは, 係数にパラメータを含む多項式集合の Gröbner basis を計算する方法論のことである.

Sato, Suzuki[4] による, Alternative Comprehensive Gröbner Bases (ACGB) はオリジナルの Comprehensive Gröbner Bases の別のアプローチを与える. ACGB は commutative Von Neumann regular ring R 上の多項式環 $R[\bar{X}]$ における Gröbner Bases の理論である. これを用いると, K を体とし, $\bar{A}$ をパラメータ, $\bar{X}$ を変数とする多項式環 $K[\bar{A},\bar{X}]$ の有限部分集合 $F_{\bar{A}}$ を $R[\bar{X}]$ での有限部分集合 $F_{R\bar{A}}$ とみなせる. しかも, $\mathrm{Id}(F_{R\bar{A}})$ の stratified Gröbner basis $G_{R\bar{A}} \subset R[\bar{X}]$ が存在し (この $G_{R\bar{A}}$ を ACGB と呼ぶ), 計算をする事ができる. $G_{R\bar{A}}$ のパラメータに値 $\bar{a}$ を代入するだけで $\mathrm{Id}(F_{\bar{a}}) \subset K[\bar{X}]$ の reduced Gröbner basis $G_{\bar{a}}$ が得られる.

Discrete Comprehensive Gröbner Bases の理論は ACGB の拡張概念である ACGB on Varieties の理論 (以下 ACGB-V と略する. Sato, Y., Suzuki, A., Nabeshima, K.[5] による) の subset として考えられている.

ACGB-V とは, 先の説明で用いた $K[\bar{A},\bar{X}]$ において, パラメータ $\bar{A}$ への代入定義域を affine variety とみなす ACGB のことである. さらにこの affine variety のイデアルが zero-dimensional かつ radical となる場合の ACGB-V を特に discrete comprehensive Gröbner basis と呼ぶ.

一方で, specialization 下における Stability of Gröbner basis の性質とは, $K[\bar{A},\bar{X}]$ のイデアル I に対して, (適当な項順序に関する)I の Gröbner basis $G = \{g_1(\bar{A},\bar{X}),\ldots,g_l(\bar{A},\bar{X})\}$ が

*santaro@theory.se.ritsumei.ac.jp
† ysato@rs.kagu.tus.ac.jp

存在するが，ある種の条件のもとに K の代数的閉包 $\bar{K}$ の任意の元 $\bar{a}$ を G に代入した $G_{\bar{a}} = \{g_1(\bar{a},\bar{X}),\ldots,g_l(\bar{a},\bar{X})\}$ が $\mathrm{Id}(G_{\bar{a}}) \subset \bar{K}[\bar{X}]$ の Gröbner basis となるような性質の事をいう．条件なしに一般的にこのような性質が成り立つとは限らない．

本文では前述の "ある種の条件" として $I_{\bar{A}} = I \cap K[\bar{A}]$ が zero-dimensional proper radical イデアルとなることを考える．詳細は Sato[6] を参照してもらいたいが，この条件のもとで，$K[\bar{A}]/I_{\bar{A}}$ は Von Neumann regular ring となり先の $G \subset K[\bar{A},\bar{X}]$ は $G \subset (K[\bar{A}]/I_{\bar{A}})[\bar{X}]$ と見なすことができるのである．これにより G を得るための計算に関しては，Von Neumann regular ring 上で discrete comprehensive Gröbner basis を計算する手順と，通常の体上の Gröbner basis 計算の 2 通りの方法が考えられる．

さて，我々はこの 2 つの計算法について，$K[\bar{A}]/I_{\bar{A}}$ の満たす条件により G の計算速度にかなりの差が出るだろうと予測しており，いくつかの例についてはこれを確認している．

まず，第 2 節において ACGB，ACGB-V，discrete comprehensive Gröbner basis について簡単に振り返る．第 3 節では Stability of Gröbner basis と ACGB について振り返り，第 4 節では先の 2 通りの計算法で G を計算する速度を検証したデータを示す．

2 Von Neumann regular ring and Gröbner Bases

定義 2.1 (Von Neumann regular ring)
R を単位元 1 を持つ可換環とする．R が Von Neumann regular ring であるとは，

$$\forall a \in R,\ \exists b \in R \quad s.t. \quad a^2 b = a.$$

を満たすときをいう．
また，このような b に対して，a の idempotent $a^* = ab$，a の quasi-inverse $a^{-1} = ab^2$ と定める．このとき a^* および a^{-1} は a に対して一意的に定まる．

K を体とするとき，$K^m \longrightarrow K$ への写像の全体 $K^{(K^m)}$ は Von Neumann regular ring を成す．
次に Von Neumann regular ring R 上多項式環に単項簡約 (monomial reduction) を定義する．

定義 2.2 (monomial reduction)
R を Von Neumann regular ring とし，$f,g,p \in R[\bar{X}]$ かつ $f,p \neq 0$ とし，$P \subset R[\bar{X}]$ とする．このとき，

(i) f の項 t が p を法として g に単項簡約されるとは，$t \in T(f)$ に対して，ある $s \in T(\bar{X})$ が存在し，$s \cdot \mathrm{HT}(p) = t$ かつ，$a \cdot \mathrm{HC}(p) \neq 0$ かつ，

$$g = f - a \cdot \mathrm{HC}(p)^{-1} \cdot s \cdot p \quad (a \text{ は } f \text{ における } t \text{ の係数})$$

を満たすことであり，これを $f \longrightarrow_p g\ [t]$ と表す．

(ii) f が p を法として g に単項簡約されるとは，ある $t \in T(f)$ が存在し，$f \longrightarrow_p g\ [t].$ を満たすことであり，これを $f \longrightarrow_p g$ と表す．

(iii) f が P を法として g に単項簡約されるとは，ある $p \in P$ が存在し，$f \longrightarrow_p g.$ を満たすことであり，これを $f \longrightarrow_P g$ と表す．

(iv) f が p を法として単項簡約可能であるとは，ある $g \in R[\bar{X}]$ が存在し，$f \longrightarrow_p g.$ を満たすことである．

(v) f が P を法として単項簡約可能であるとは，ある $g \in R[\bar{X}]$ が存在し，$f \longrightarrow_P g$. を満たすことである．

f が p(あるいは P) を法として単項簡約不可能であるとき，f は p(あるいは P) を法として正規形 (normal form) であるという．また，$g \in R[\bar{X}]$ が P を法として f の正規形であるとは，g が P を法として正規形であり，かつ，

$$f \xrightarrow{*}_P g$$

を満たすことをいう．また，

$$f \longrightarrow_p g \ [t]$$

において，$t = \mathrm{HT}(f)$ であるとき，これを f の頭項簡約 (top-reduction) という．

この単項簡約を用いて，$R[\bar{X}]$ 上に Gröbner bases を定義することができる．以下，本節では特に断りがない限り R は Von Neumann regular ring を表すこととする．

定義 2.3 (Gröbner basis)
G を $R[\bar{X}]$ の有限部分集合とする．このとき，

$$\text{任意の } f \in \mathrm{Id}(G) \text{ に対して } f \xrightarrow{*}_G 0$$

を満たすとき，G を Gröbner basis と呼ぶ．また，I を $R[\bar{X}]$ のイデアルとするとき，I の Gröbner basis とは，Gröbner basis $G \subset I$ であって，$\mathrm{Id}(G) = I$ を満足することである．

また，体上多項式環のイデアルは有限生成であり，その Gröbner basis は必ず存在したが，一般に Von Neumann regular ring は Noether 環とは限らず，そのイデアルが有限生成である保証はない．しかし，生成元を与えられたイデアルには，その Gröbner basis が存在することが保証されている．

しかも，体上多項式環では reduced Gröbner basis の一意性が保証されていたが，regular ring 上ではこの一意性は保証されない．しかし，以下の拡張された定義によって一意性が保証されている．

定義 2.4 (stratified Gröbner basis)
$G \subset R[\bar{X}]$ を reduced Gröbner basis とする．G が以下の 2 条件，

(i) 任意の $g \in G$ に対して，$\mathrm{HC}(g) = \mathrm{HC}(g)^*$.
(ii) $g_1, g_2 \in G$ に対して，$g_1 \neq g_2 \implies \mathrm{HT}(g_1) \neq \mathrm{HT}(g_2)$.

を満たすとき，G を stratified Gröbner basis という．stratified Gröbner basis は一意的である．

Sato, Suzuki[4] において提案された，ACGB は，$K^{(K^m)}$ の部分環として terrace と呼ばれる $K[\bar{A}]$ を含む computable な最小の Von Neumann regular ring を定義し，その上で Gröbner bases の理論を展開している．詳しくは [4] を参照してもらいたい．

定義と重要な定理を提示しておく．

定義 2.5 (ACGB)
K を体とし，$\bar{A} = A_1, \ldots, A_m$，$\bar{X} = X_1, \ldots, X_n$ を変数とし，$F \subset K[\bar{A}, \bar{X}]$ を有限集合とする．このとき，$K^{(K^m)}[\bar{X}]$ のイデアル $\mathrm{Id}(F)$ の stratified Gröbner basis G をパラメータ $\bar{A}$ に関する F の ACGB という．

次に，$h \in K^{(K^m)}[\bar{X}]$ とすると，h の任意の係数 c は $c \in K^{(K^m)}$ であったから，これを $c(\bar{A})$ と表す．また $\bar{a} \in K^m$ に対して，$h_{\bar{a}}$ を h のすべての係数 $c(\bar{A})$ に $\bar{a}$ を代入することとする．さらに，$G \subset K^{(K^m)}[\bar{X}]$ に対して，$G_{\bar{a}} = \{g_{\bar{a}} | g \in G\}$ と定義する．

定理 2.6 (Suzuki-Sato, 2003)
$F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\} \subset K[\bar{A}, \bar{X}]$ とする．$G = \{g_1, \ldots, g_l\}$ をパラメータ $\bar{A}$ に関する F の ACGB とする．このとき，任意の $\bar{a} \in K^m$ に対して $G_{\bar{a}} - \{0\}$ は $K[\bar{X}]$ のイデアル $\mathrm{Id}(f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X}))$ の reduced Gröbner basis である．

Introduction でも触れたが，ACGB におけるパラメータへの代入定義域は affine variety へと一般化できる．詳しくは Sato, Suzuki, Nabeshima[5] を参照してもらいたい．

定義 2.7 (ACGB-V)
K を体とし，$\bar{A} = A_1, \ldots, A_m$，$\bar{X} = X_1, \ldots, X_n$ を変数とし，$F \subset K[\bar{A}, \bar{X}]$ を有限集合とする．また，I を $K[\bar{A}]$ のイデアルとする．このとき，$K^{\mathbf{V}(I)}[\bar{X}]$ のイデアル $\mathrm{Id}(F)$ の stratified Gröbner basis G をパラメータ $\bar{A}$ と多様体 $\mathbf{V}(I)$ に関する F の ACGB-V という．

定理 2.8
I を $K[\bar{A}]$ のイデアルとし，$F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\} \subset K[\bar{A}, \bar{X}]$ とする．$G = \{g_1, \ldots, g_l\}$ をパラメータ $\bar{A}$ と $\mathbf{V}(I)$ に関する F の ACGB-V とする．このとき，任意の $\bar{a} \in \mathbf{V}(I)$ に対して $G_{\bar{a}} - \{0\}$ は $K[\bar{X}]$ のイデアル $\mathrm{Id}(f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X}))$ の reduced Gröbner basis である．

定義 2.9 (discrete comprehensive Gröbner basis)
$V \subset K^m$ を $K[\bar{A}]$ のイデアルで定義された多様体とし，$F \subset K[\bar{A}, \bar{X}]$ を有限集合とする．$\mathbf{I}(V)$ が zero-dimensional であるとき，パラメータ $\bar{A}$ と多様体 V に関する F の ACGB-V を discrete comprehensive Gröbner basis という．

discrete comprehensive Gröbner bases には，ACGB および ACGB-V にはない顕著な特徴がある．ACGB では $K[\bar{A}]$ を含む最小の computable な Von Neumann regular ring を定義し，その上で ACGB を構成していたが，discrete comprehensive Gröbner bases の場合では $K[\bar{A}]$ を含む最小の computable な Von Neumann regular ring として $K[V] \simeq K[\bar{A}]/\mathbf{I}(V)$ をとれば十分である．

定理 2.10
I を $K[\bar{A}]$ の zero-dimensional proper radical イデアルとし，$F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\} \subset K[\bar{A}, \bar{X}]$ とする．$G = \{g_1, \ldots, g_l\}$ をパラメータ $\bar{A}$ と $\mathbf{V}(I)$ に関する F の discrete comprehensive Gröbner basis とする．このとき，

(i) G の任意元は $K[\bar{A}, \bar{X}]$ の元で表現できる．
(ii) $\bar{K}$ を K の代数的閉包とすると，任意の $\bar{a} \in \mathbf{V}(I) \subset \bar{K}^m$ に対して $G_{\bar{a}} - \{0\}$ は $\bar{K}[\bar{X}]$ のイデアル $\mathrm{Id}(f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X}))$ の Gröbner basis である．

計算機代数システム Risa/Asir 上に Asir 言語で実装した discrete comprehensive Gröbner basis を構成するアルゴリズムの概要は以下に示すものである．

(1) $(K[\bar{A}]/I)[\bar{X}]$ の元を $(K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_k)[\bar{X}]$ の元に変換する．
(2) $(K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_k)[\bar{X}]$ の元を $(K[\bar{A}]/P_1)[\bar{X}] \times \cdots \times (K[\bar{A}]/P_k)[\bar{X}]$ の元に変換する．
(3) 各 $(K[\bar{A}]/P_i)[\bar{X}]$, $(1 \leq i \leq k)$ で Gröbner basis を計算する．

(4) 各 $(K[\bar{A}]/P_i)[\bar{X}]$, $(1 \leq i \leq k)$ での Gröbner basis を $(K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_k)[\bar{X}]$ の元に復元する.

(5) $(K[\bar{A}]/I)[\bar{X}]$ の元に復元する.

特に, 手順 (3), (4) の方法で本当に discrete comprehensive Gröbner basis を得る保証があるのかは気になるところであるが, これについては数学的にその安全性が保証されている.

3 Stability of Gröbner basis and ACGB

Sato[6] により, 通常の体上多項式環の Gröbner basis と Von Neumann regular ring 上の Gröbner basis である ACGB との間に関係があることが示されている. その主結果は以下に示すものである.

定理 3.1
K : 体, $I \subset K[\bar{A}, \bar{X}]$: イデアル, また, $I \cap K[\bar{A}] \subset K[\bar{A}]$ は zero-dimensional proper radical イデアルとする. $\bar{X} \gg \bar{A}$ なる term order による, $I \subset K[\bar{A}, \bar{X}]$ の Gröbner basis を G とする時, $G \subset (K[\bar{A}]/(I \cap K[\bar{A}]))[\bar{X}]$ とみなすと, G は先の term order に付随した, discrete comprehensive Gröbner basis になる.

さらにこの定理に関連して, 以下のような事実も成立する.

定理 3.2
K : 体, $I \subset K[\bar{A}, \bar{X}]$: イデアル, また, $I \cap K[\bar{A}] \subset K[\bar{A}]$ は zero-dimensional maximal イデアルとする. $\bar{X} \gg \bar{A}$ なる term order による, $I \subset K[\bar{A}, \bar{X}]$ の reduced Gröbner basis を G とする時, $G - G \cap K[\bar{A}] \subset (K[\bar{A}]/(I \cap K[\bar{A}]))[\bar{X}]$ とみなすと, $G - G \cap K[\bar{A}]$ は先の term order に付随した, $(K[\bar{A}]/(I \cap K[\bar{A}]))[\bar{X}]$ 上の stratified Gröbner basis になる.

以上の事実により, $I \subset K[\bar{A}, \bar{X}]$ で, $I \cap K[\bar{A}] \subset K[\bar{A}]$ が zero-dimensional maximal イデアルとなる場合に体上で通常の I の Gröbner basis を計算する方法と discrete comprehensive Gröbner basis 経由で I の Gröbner basis を計算する方法の 2 通りの方法が考えられる.

例えば, 辞書式順序 $X > Y > t > A$ で $I = \mathrm{Id}(X^2 - A,\ Y^3 - A,\ X + Y - t,\ A^2 - 3) \subset \mathbb{Q}[A, X, Y, t]$ の Gröbner basis を計算することを考えると, $I_A = I \cap \mathbb{Q}[A] = \mathrm{Id}(A^2 - 3)$ であり, I_A は zero-dimensional maximal イデアルであるから, 定理 3.2 により I の Gröbner basis G に対して, $G - G \cap \mathbb{Q}[A]$ は, $(\mathbb{Q}[A]/I_A)[X, Y, t]$ 上の辞書式順序 $X > Y > t$ での stratified Gröbner basis になるはずである.

実際, I の $\mathbb{Q}[A, X, Y, t]$ での Gröbner basis は $G = (g_1, g_2, g_3, g_4) = (A^2 - 3,\ t^6 - 3At^4 - 2At^3 + 9t^2 - 18t - 3A + 3,\ -11559Y + (216A - 1536)t^5 + (81A - 576)t^4 + (5120 * A - 2160)t^3 + (4992A - 2106)t^2 + (3816A - 11724)t - 2457A + 17472,\ -11559X + (-216A + 1536)t^5 + (-81A + 576)t^4 + (-5120A + 2160)t^3 + (-4992A + 2106)t^2 + (-3816A + 23283)t + 2457A - 17472)$ であり, $G - G \cap \mathbb{Q}[A] = \{g_2, g_3, g_4\}$ である. 一方, 制約イデアル I_A のもとで I の discrete comprehensive Gröbner basis を計算すると, $G' = (g'_1, g'_2, g'_3) = ((64A + 27)X - 8At^5 - 3At^4 + 80t^3 + 78t^2 + (-120A + 9)t + 91A,\ (64A + 27)Y + 8At^5 + 3At^4 - 80t^3 - 78t^2 + (56A - 36)t - 91A,\ (64A + 27)t^6 + (-81A - 576)t^4 + (-54A - 384)t^3 + (576A + 243)t^2 + (-1152A - 486)t + 111A - 495)$ となるが, このとき, $(64A + 27)g_2 \equiv g'_3 \mod I_A$, $(64A + 27)g_3 \equiv -11559g'_2 \mod I_A$, $(64A + 27)g_4 \equiv -11559g'_1 \mod I_A$ となる.

さて，我々はこの2通りの計算法に関して，

- $I \cap K[\bar{A}]$ が maximal の場合，通常の lex order を使ったときと $(K[\bar{A}]/(I \cap K[\bar{A}]))[\bar{X}]$ で Gröbner basis を計算したときでどちらが高速であるか？
- $I \cap K[\bar{A}]$ が複雑な maximal イデアルの場合は，後者の方法による計算が高速になるのではないか．

と予想をしている．単純な maximal イデアルと現在想定しているものは，$K[\bar{A}]/(I \cap K[\bar{A}])$ を線型空間として見たときの次元が小さいものの事を言う．特に次元が2〜3程度のものを想定している．複雑であるとは単純でないときを言う．

次節にていくつかの例についてこの予想の検証を行う．

4 Timing Data

以下の2つのベンチマークは，代数体上の代数的数の最小多項式を表現するための計算法である．

例えば，$a \in \mathbf{V}(A^2-3)$ に対して，前節の I の Gröbner basis の計算によって $\alpha = a^{1/2}+a^{1/3}$ の $\mathbb{Q}(a)$ 上の最小多項式の計算ができている．$G = \{g_1, g_2, g_3, g_4\}$ のうち，A, t のみの式である $g_2 = t^6-3At^4-2At^3+9t^2-18t-3A+3$ の $A = a$ と代入して得られる式 $t^6-3at^4-2at^3+9t^2-18t-3a+3$ が α の $\mathbb{Q}(a)$ 上の最小多項式である．

また，discrete comprehensive Gröbner basis を計算しても同様に先の α の最小多項式を計算することができている．ここでは g_3' がそれにあたる．では，実際にこれら最小多項式を得るのにかかる計算時間を比較してみる．計算には Risa/Asir のユーザー言語である Asir 言語によって実装した discrete comprehensive Gröbner basis 計算プログラムを用いる．

bench mark 1

$a \in \mathbf{V}(A^n+6)$，代数的数 $a^{1/2}+a^{1/3}$ の最小多項式を t で表すための計算をする．

$I_1 = \{X^2-A,\ Y^3-A,\ X+Y-t,\ A^n+6\} \subset \mathbb{Q}[A,X,Y,t]$ とし，I_1 の $\mathbb{Q}$ 上の Gröbner basis 計算時間と $\mathbb{Q}[A]/\mathrm{Id}(A^n+6)$ 上の discrete comprehensive Gröbner basis 計算時間を比較する．アイゼンシュタインの既約性判定より，A^n+6 は既約多項式であり，$\mathrm{Id}(A^n+6)$ は zero-dimensional maximal 制約イデアルである．辞書式順序 $X > Y > t > A$ を使用する．

計算環境は，CPU: Athlon 2GHz，RAM: 1GB，OS: Vine Linux 2.6 であり，制約イデアル $\mathrm{Id}(A^n+6)$ に対して，$n = 1, \ldots, 60$ までを検査したものが図1である．

bench mark 2

$a \in \mathbf{V}(A^n+2A^{n-1}+\cdots+2A+6)$，代数的数 $a^{1/2}+a^{1/3}$ の最小多項式を t で表すための計算をする．

$I_2 = \{X^2-A,\ Y^3-A,\ X+Y-t,\ A^n+2A^{n-1}+\cdots+2A+6\} \subset \mathbb{Q}[t,A,X,Y]$ とし，I_2 の $\mathbb{Q}$ 上の Gröbner basis 計算時間と $\mathbb{Q}[A]/\mathrm{Id}(A^n+2A^{n-1}+\cdots+2A+6)$ 上の discrete comprehensive Gröbner basis 計算時間を比較する．同様にアイゼンシュタインの既約性判定より，$A^n+2A^{n-1}+\cdots+2A+6$ は既約多項式であり，$\mathrm{Id}(A^n+2A^{n-1}+\cdots+2A+6)$ は zero-dimensional maximal 制約イデアルである．辞書式順序 $X > Y > t > A$ を使用する．

計算環境は先と同じで，制約イデアル $\mathrm{Id}(A^n+2A^{n-1}+\cdots+2A+6)$ に対して，$n = 1, \ldots, 60$ までを検査したものが図2である．

	n	1	2	3	4	5	⋯	10	⋯
DCGB	CPU time	0.07	0.09	0.1	0.09	0.12	⋯	0.13	⋯
	GC time	0.02	0.01	0.02	0.02	0.01	⋯	0.03	⋯
	Total time	0.084669	0.10186	0.12191	0.13663	0.13384	⋯	0.16794	⋯
GB	CPU time	0.05	0.39	0.73	1.05	1.56	⋯	5.82	⋯
	GC time	0.02	0.08	0.16	0.27	0.36	⋯	1.93	⋯
	Total time	0.077978	0.52656	0.9241	1.3695	1.9393	⋯	7.8765	⋯

⋯	15	⋯	20	⋯	30	⋯	40	⋯	50	⋯	60
⋯	0.1	⋯	0.17	⋯	0.29	⋯	0.48	⋯	0.72	⋯	1.06
⋯	0.04	⋯	0.04	⋯	0.06	⋯	0.05	⋯	0.08	⋯	0.09
⋯	0.219842	⋯	0.27659	⋯	0.403374	⋯	0.585335	⋯	0.85485	⋯	1.18041
⋯	15.53	⋯	32.51	⋯	96.06	⋯	212.73	⋯	399.81	⋯	677.72
⋯	5.67	⋯	7.99	⋯	18.84	⋯	27.33	⋯	32.79	⋯	39.59
⋯	21.2649	⋯	40.6502	⋯	114.965	⋯	240.163	⋯	432.68	⋯	717.437

図 1: $I_1 = \{X^2 - A,\ Y^3 - A,\ X + Y - t,\ A^n + 6\}$, 制約イデアル $\mathrm{Id}(A^n + 6)$

これら2つの計算例に関しては, $\mathbb{Q}$ 上での Gröbner basis 計算時に辞書式順序を用いていること, および最小多項式の計算という目的から特に最小多項式を表す多項式において著しい係数膨張が起こっており, これにより計算時間が圧迫されている. しかし, discrete comprehensive Gröbner basis の場合は係数膨張が起こらず, 計算がスムーズに進行している.

また, 両 bench mark について $\mathbb{Q}[A]/\mathrm{Id}(A^n + 6)$ および $\mathbb{Q}[A]/\mathrm{Id}(A^n + 2A^{n-1} + \cdots + 2A + 6)$ の線型次元はともに $n - 1$ であるから, この2つの bench mark については我々の予想通りの結果が得られたといえる.

5 Conclusion

第3節の予想は今回の計算例では確認できたといえるが, では逆にどのような条件のもとに計算速度に差が生まれるのかはよく分かっておらず, 今後の研究課題である.

また, 1番の研究テーマは $I \cap K[\bar{A}]$ が zero-dimensional ではあるが maximal イデアルではない場合の計算をどうするかにある. これに対し, 私の開発した discrete comprehensive Gröbner basis 計算の方法とその実装は1つの解であるが, 計算効率上考えられる選択肢としては, $K[\bar{A}]/(I \cap K[\bar{A}])$ が Von Neumann regular ring となることから, Von Neumann regular ring としての本来の構造をそのまま実装することが挙げられる. この場合は regular ring の構造をそのまま実装するので, 計算速度の向上が期待される. また, regular ring の idempotent 演算や quasi-inverse 演算の方法の考案, 効率化等, アルゴリズムレベルでの研究が必要になり, 今後の重要な研究課題である.

参 考 文 献

[1] Kalkbrener, M.(1997). On the Stability of Gröbner Bases under specializations. J.Symb.Comp. Vol 24/1, pp 51-58.

[2] Noro, M. and Takeshima, T.(1992). Risa/Asir – A Computer Algebra System. International Symposium on Symbolic and Algebraic Computation(ISSAC '92), Proceedings. pp 387-396.

	n	1	2	3	4	5	⋯	10	⋯
DCGB	CPU time	0.05	0.09	0.09	0.11	0.1	⋯	0.14	⋯
	GC time	0.03	0.02	0.03	0.02	0.04	⋯	0.04	⋯
	Total time	0.085481	0.12112	0.13784	0.14646	0.16351	⋯	0.20783	⋯
GB	CPU time	0.07	0.46	0.86	1.16	1.71	⋯	7.3	⋯
	GC time	0.02	0.09	0.19	0.33	0.55	⋯	2.45	⋯
	Total time	0.09460	0.60380	1.0927	1.6837	2.3381	⋯	10.033	⋯

⋯	15	⋯	20	⋯	30	⋯	40	⋯	50	⋯	60
⋯	0.19	⋯	0.29	⋯	0.79	⋯	1.89	⋯	4.08	⋯	8.16
⋯	0.07	⋯	0.1	⋯	0.19	⋯	0.21	⋯	0.54	⋯	1.41
⋯	0.28888	⋯	0.412937	⋯	0.996361	⋯	2.11406	⋯	4.67213	⋯	9.58848
⋯	19.58	⋯	40.71	⋯	119.64	⋯	263.7	⋯	496.42	⋯	841.14
⋯	7.04	⋯	11.05	⋯	19.39	⋯	14.86	⋯	29.81	⋯	53.54
⋯	26.7215	⋯	51.824	⋯	139.11	⋯	278.632	⋯	526.362	⋯	894.815

図 2: $I_2 = \{X^2 - A,\ Y^3 - A,\ X + Y - t,\ A^n + 2A^{n-1} + \cdots + 2A + 6\}$, 制約イデアル $\mathrm{Id}(A^n + 2A^{n-1} + \cdots + 2A + 6)$

[3] Sato, Y., Suzuki, A. and Nabeshima, K.(2003). Discrete Comprehensive Gröbner Bases II. Computer Mathematics III, Lecture Notes Series on Computing, pp 240-247 World Scientific, 2003.

[4] Suzuki, A. and Sato, Y.(2003). An alternative approach to Comprehensive Gröbner Bases. J.Symb.Comp. Vol 36/3-4, pp 649-667.

[5] Sato, Y., Suzuki, A and Nabeshima, K.(2003). ACGB on Varieties. Proceedings of the Sixth International Workshop on Computer Algebra in Scientific Computing(CASC 2003), pp 313-318.

[6] Sato, Y.(2005). Stability of Gröbner bases and ACGB. Proceedings of Algorithmic Algebra and Logic 2005, Conference in Honor of the 60th Birthday of Volker Weispfenning, pp 223-228.

[7] Weispfenning, V.(1989). Gröbner bases for polynomial ideals over commutative regular rings. Proceedings of EUROCAL '87, Leipzig, Springer LNCS Vol. 378, pp 336-347.

[8] Weispfenning, V.(1992). Comprehensive Gröbner bases. J.Symb.Comp. Vol 14/1, pp 1-29.

[9] Becker, T. and Weispfenning, V. *Gröbner Bases.* Springer-Verlag, 1993.

[10] Cox, D., Little, J. and O'Shea, D. *Ideals, Varieties, and Algorithms.* Springer-Verlag, 1992. UTM.

[11] 野呂正行・横山和弘.「グレブナー基底の計算 基礎編——計算機代数入門」東京大学出版会, 2003.