数理解析研究所講究録
第1568巻 2007年 48-54

Dynamic Evaluationを用いたDiscrete Comprehensive Gröbner Basesの計算

倉田 陽介
YOSUKE KURATA
神戸大学 自然科学研究科
GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, KOBE UNIVERSITY *

野呂 正行
MASAYUKI NORO
神戸大学 理学部
FACULTY OF SCIENCE, KOBE UNIVERSITY †

1 Introduction

2005年から2006年にかけて，Comprehensive Gröbner Bases (CGB) およびComprehensive Gröbner System (CGS) 計算法 [14]，すなわち係数にパラメータを含むGröbner Bases計算法にSuzuki-Satoによる新しい計算法 [11] が発表された．

Weispfenning [14, 15] やMontes [3, 4] あるいはSuzuki-Sato [8] によるCGB & CGS計算は本質的にはパラメータ多項式を有理関数体 $\mathbb{Q}(\bar{A})$ の元と見なした多項式環 $\mathbb{Q}(\bar{A})[\bar{X}]$ 上に，それぞれに特化したS多項式と単項簡約を定義することによって実現されてきた．しかし，Suzuki-Satoによる新しい計算法は通常の $\mathbb{Q}$ 上の多項式環 $\mathbb{Q}[\bar{A},\bar{X}]$ 上でのGröbner bases計算法を利用した方法であり，いくらかの例で従来の方法よりも高速にCGS & CGBを出力する．

Discrete comprehensive Gröbner bases (DCGB) は2001年にSato-Suzuki [7] によって発表された．DCGBはspecialization homomorphism $K(\bar{A})[\bar{X}] \longrightarrow L[\bar{X}]$ (L は K の代数的閉包) の定義域を0次元多様体に制限した特殊なCGSを与える．DCGBは2003年に同じくSato-Suzuki [9] によって，より一般的な形式が与えられるに至った．パラメータへの代入定義域を決定する0次元多様体 V を定義する0次元根基イデアルを I とすると，$K[V]$ を含む最小のvon Neumann regular ringは $R = K[\bar{A}]/I$ と表され，DCGBの計算は多項式環 $R[\bar{X}]$ 上のGröbner bases計算によって与えられる．

これまで，有限多項式集合 $F \subset K[\bar{A},\bar{X}]$ のDCGB計算はvon Neumann regular ring $K[\bar{A}]/I$ 上のquasi-inverse，およびidempotent演算が現実的でなかったため，I の(最短)素イデアル分解 $I = P_1 \cap \cdots \cap P_k$ を用いて，それぞれの分解成分に対応する体 $K[\bar{A}]/P_i$，$(1 \leq i \leq k)$ 上の多項式環 $(K[\bar{A}]/P_i)[\bar{X}]$ 上で $\phi_{P_i}(F) = \{\phi_{P_i}(f) \mid f \in F\}$，$(\phi_{P_i} : K[\bar{A},\bar{X}] \longrightarrow (K[\bar{A}]/P_i)[\bar{X}])$ のGröbner basis計算を行い，結果をChinese remainder theorem (CRT) によって結合することで，$(K[\bar{A}]/I)[\bar{X}]$ の元に復元してGröbner basisを計算していた．しかし，イデアルの素分解やCRTによる復元の計算コストは一般的に高い．また，問題

*kurata@math.kobe-u.ac.jp
†noro@math.kobe-u.ac.jp

によっては各分解成分に対応する多項式環 $(K[\bar{A}]/P_i)[\bar{X}]$ での $\phi_{P_i}(F)$ の Gröbner basis 計算が i 毎に全て同等になるような場合もあり，計算効率にダメージを与えている．

本論文では DCGB の新しい計算法を提案する．新しい計算法では quasi-inverse を計算するために Noro [6] による Modular Dynamic Evaluation (MDE) を用いる．MDE は dynamic evaluation をイデアル商の観点から見直したものである．0 次元根基イデアル I と $[a]_I \in K[\bar{A}]/I$ に対して，MDE は $[a]_I$ が単元ならば，その逆元 $[a]_I^{-1}$ を計算し，そうでなければ I の分解 $I = (I : a) \cap (I + \langle a \rangle)$ を与える．より具体的には，MDE は $[a]_I$ の逆元計算に失敗した場合，$I : a$ と $I + \langle a \rangle$ のそれぞれの Gröbner bases を計算する．しかもすべての計算を効率的な modular 演算で行うものである．

本論文は以下のような構成である．第 2 節ではいくらかの記述に関する約束と CGB & CGS を定義し，DCGB を定義する．第 3 節では von Neumann regular ring とその上での Gröbner bases を定義し，DCGB との関連について述べる．第 4 節では Modular Dynamic Evaluation について概観し，本論文の主結果である von Neumann regular ring 上の quasi-inverse，および idempotent 演算の方法を与え，DCGB が von Neumann regular ring 上の多項式環で Buchberger Algorithm を実行することで得られることを示す．

2 CGB, CGS, and DCGB

本節では，本論文を通して使われるいくつかの数学的記述および，定義を述べる．

一般的に，f を多項式とし，$<$ を項順序 (term order) とするとき，$\mathrm{HT}_<(f)$ で f の $<$ に関する頭項 (head term) を表し，$\mathrm{HC}_<(f)$ で $\mathrm{HT}_<(f)$ の係数を表す．K, L は体とし，L は K の代数的閉包とする．$\bar{X} = \{X_1, \ldots, X_n\}$, $\bar{A} = \{A_1, \ldots, A_m\}$ をそれぞれ不定元の集合とし，$\bar{A} \cap \bar{X} = \emptyset$ とする．$T(\bar{X})$, $T(\bar{A})$, $T(\bar{A}, \bar{X})$ をそれぞれ $\bar{X}$, $\bar{A}$, $\bar{A} \cup \bar{X}$ の単項 (terms) の集合とする．任意の $\bar{a} \in L^m$ に対して，正則な specialization homomorphism $\sigma_{\bar{a}} : K[\bar{A}] \longrightarrow L$ が定義できる．このとき $\sigma_{\bar{a}}$ は $f(\bar{A}) \in K[\bar{A}]$ に対して $\sigma_{\bar{a}}(f(\bar{A})) = f(\bar{a})$ である．また，$\sigma_{\bar{a}}$ は自然な方法で，homomorphism $\sigma_{\bar{a}} : (K[\bar{A}])[\bar{X}] \longrightarrow L[\bar{X}]$ と拡張できる．$K[\bar{A}]$ の部分集合 F に対して，F で定まる affine 多様体を $\mathbf{V}(F) \subset L^m$ と表し，

$$\mathbf{V}(F) = \{\bar{a} \in L^m \mid f \in F,\ f(\bar{a}) = 0\}$$

とする．また，F が有限集合で $F = \{f_1, \ldots, f_k\}$ となる時は，その affine 多様体を $\mathbf{V}(f_1, \ldots, f_k)$ とも表す．$f \in K[\bar{A}]$ と，有限集合 $G \subset K[\bar{A}]$，項順序 $<_{\bar{A}}$ に対して，$\mathrm{NF}_{G,<_{\bar{A}}}(f)$ で，f の $<_{\bar{A}}$ に関する G を法とした normal form の 1 つを表す．$\mathrm{NF}_{G,<_{\bar{A}}}(f)$ は一般に一意に決定するわけではないが，G が Gröbner basis の時は一意に決定する．また，イデアル $I \subset K[\bar{A}]$ に対して，剰余環 $K[\bar{A}]/I$ の元を $[f]_I$ で表す，G が I の Gröbner basis である時は，$[f]_I = \mathrm{NF}_{G,<_{\bar{A}}}(f)$ で一意的に多項式表現できる．

定義 1 (Comprehensive Gröbner System)
F を $K[\bar{A}, \bar{X}]$ の部分集合とし，$S_1, \ldots, S_l$, $T_1, \ldots, T_l$ をそれぞれ $K[\bar{A}]$ の有限部分集合とする．このとき，有限集合 $\mathcal{G} = \{(S_1, T_1, G_1), \ldots, (S_l, T_l, G_l)\}$ が F の項順序 $<_{\bar{X}}$ に関する *comprehensive Gröbner system* であるとは，$(\mathbf{V}(S_1) \setminus \mathbf{V}(T_1)) \cup \cdots \cup (\mathbf{V}(S_l) \setminus \mathbf{V}(T_l)) = L^m$ かつ，任意の $\bar{a} \in \mathbf{V}(S_i) \setminus \mathbf{V}(T_i)$, $(i = 1, \ldots, l)$ に対して $\sigma_{\bar{a}}(G_i)$ が $L[\bar{X}]$ のイデアル $\langle \sigma_{\bar{a}}(F) \rangle$ の $<_{\bar{X}}$ に関する *Gröbner basis* となるときのことを言う．また，各 (S_i, T_i, G_i) あるいは $(\mathbf{V}(S_i) \setminus \mathbf{V}(T_i), G_i)$ を $\mathcal{G}$ の *segment*，あるいは単に *Gröbner system* と呼ぶ．

定義 2 (Comprehensive Gröbner Bases)
$G \subset K[\bar{A}, \bar{X}]$ が F の *comprehensive Gröbner basis* であるとは，任意の $\bar{a} \in L^m$ に対して $\sigma_{\bar{a}}(G)$ が $\langle \sigma_{\bar{a}}(F) \rangle \subset L[\bar{X}]$ の $<_{\bar{X}}$ に関する *Gröbner basis* となるときのことを言う．

定義 3 (Discrete Comprehensive Gröbner Bases)
Gröbner system (S, T, G) $(S,\ T \subset K[\bar{A}],\ G \subset K[\bar{A}, \bar{X}])$ が *discrete comprehensive Gröbner basis* であるとは，$\mathbf{V}(S)$ が 0 次元多様体で $\mathbf{V}(T)$ が空集合となる時のことである．この時は特に (S, T, G) あるいは

$(\mathbf{V}(S) \setminus \mathbf{V}(T), G)$ を短く (S, G) あるいは $(\mathbf{V}(S), G)$ と表す．また，G を $<_{\bar{X}}$ に関する $\mathbf{V}(S)$ 上の *discrete comprehensive Gröbner basis* とも言う．

3 Gröbner Bases over Von Neumann Regular Rings and DCGB

DCGB 計算は，元来 von Neumann regular ring 上の Gröbner bases として定義されており，その計算法も von Neumann regular ring 上の Gröbner bases 計算で実現していた．本節では，可換な von Neumann regular ring R の定義を行い，R 上の多項式環 $R[\bar{X}]$ に単項簡約を定義する．そして，その単項簡約を用いて，$R[\bar{X}]$ における Gröbner basis の概念を定義する．また，その Gröbner basis 計算は体上の Gröbner basis 計算と同様に Buchberger Algorithm で得られる．

3.1 Von Neumann Regular Rings

定義 4
単位元 1 を持つ可換環 R が *von Neumann regular ring* であるとは，以下の性質を満足する時のことを言う．

$$\text{任意の } a \in R \text{ に対して，ある } b \in R \text{ が存在し，} a^2 b = a \text{ を満足する．}$$

また，このような b に対して，$a^* = ab$，$a^{-1} = ab^2$ と定義し，それぞれ a の *idempotent*，*quasi-inverse* と呼ぶ．

命題 5
R を *von Neumann regular ring* とし，$a \in R$ とする．このとき，それぞれ $aa^* = a$，$aa^{-1} = a^*$，$(a^*)^2 = a^*$ が成立し，a^*，a^{-1} ともに一意的である．

3.2 Monomial Reductions and Gröbner Bases

以下で von Neumann regular ring R 上の多項式環 $R[\bar{X}]$ 上に単項簡約と Gröbner bases の概念を定義する．本節を通して，R は von Neumann regular ring とし，$T(\bar{X})$ 上の項順序 $<_{\bar{X}}$ は $R[\bar{X}]$ の多項式に適用するものとする．また，0 でない $f \in R[\bar{X}]$ に対して，f の頭係数の quasi-inverse $\mathrm{HC}_{<_{\bar{X}}}(f)^{-1}$ をかけたもの $f' = \mathrm{HC}_{<_{\bar{X}}}(f)^{-1} \cdot f$ を f の monic 化という．

定義 6 (monomial reduction)
$f, p \in R[\bar{X}]$ に対して，$f = a\bar{X}^\alpha + g'$，$(a \in R,\ \bar{X}^\alpha \in T(\bar{X})$ で $a\bar{X}^\alpha$ は f の頭項とは限らない$)$ また，$f, p \neq 0$ とする．この時，f が p を法として単項簡約可能であるとは，$a\bar{X}^\alpha$ に対して，ある $\bar{X}^\beta \in T(\bar{X})$ が存在し，$\bar{X}^\beta \cdot \mathrm{HT}_{<_{\bar{X}}}(p) = \bar{X}^\alpha$ かつ，$a \cdot \mathrm{HC}_{<_{\bar{X}}}(p) \neq 0$ のときをいい，

$$g = f - a \cdot \mathrm{HC}_{<_{\bar{X}}}(p)^{-1} \cdot \bar{X}^\beta \cdot p$$

を f の p による 1 回の単項簡約といい，これを $f \longrightarrow_p g$ と表す．

これより，部分集合 $P \subset R[\bar{X}]$ による $f \in R[\bar{X}]$ の単項簡約 $\longrightarrow_P$ が自然に定義できる．また，P が有限集合のときは $\longrightarrow_P$ による簡約鎖列は必ず停止する．この単項簡約を用いることで，Gröbner bases の概念を定義することができる．

定義 7 (Gröbner bases)
有限部分集合 $G \subset R[\bar{X}]$ が *Gröbner basis* であるとは，任意の $f \in \langle G \rangle$ に対して，$f \xrightarrow{*}_G 0$ を満たすときのことをいう．また，G がイデアル $I \subset R[\bar{X}]$ の *Gröbner basis* であるとは，任意の $f \in I$ に対して，$f \xrightarrow{*}_G 0$，かつ，$\langle G \rangle = I$ を満たすときのことをいう．

また，Sato [10] 補題 2.2，補題 2.3，補題 2.4 により，体上多項式環と同様に S 多項式により Gröbner bases を特徴付けることができる．ここで，$f,g \in R[\bar{X}]$ の S 多項式とは，

$$\mathrm{spol}(f,g) = \mathrm{HC}_{<_{\bar{X}}}(g)\frac{\mathrm{lcm}(\mathrm{HT}_{<_{\bar{X}}}(f),\mathrm{HT}_{<_{\bar{X}}}(g))}{\mathrm{HT}_{<_{\bar{X}}}(f)}f - \mathrm{HC}_{<_{\bar{X}}}(f)\frac{\mathrm{lcm}(\mathrm{HT}_{<_{\bar{X}}}(f),\mathrm{HT}_{<_{\bar{X}}}(g))}{\mathrm{HT}_{<_{\bar{X}}}(g)}g$$

のことである．

定理 8
有限部分集合 $G \subset R[\bar{X}]$ が *Gröbner basis* であることと，任意の 0 でない相異なる 2 つの多項式 $f,g \in G$ に対して，$\mathrm{spol}(f,g) \xrightarrow{*}_G 0$ となることは必要十分である．

従って，体上多項式環と同様に $R[\bar{X}]$ 上で Buchberger Algorithm を実行することができる．

3.3 Gröbner Bases over Von Neumann Regular Rings and DCGB

以下では von Neumann regular ring R 上で Gröbner bases 計算を行うことで DCGB が得られることを示す．まず，パラメータ空間を決定するイデアル $I \subset K[\bar{A}]$ が von Neumann regular ring を構成することを示す補題からはじめる．

補題 9
$K_1,\ldots,K_s$ をそれぞれ体とする．このとき，直積 $\boldsymbol{K} = K_1 \times \cdots \times K_s$ に自然な演算を定義すると，$\boldsymbol{K}$ は *von Neumann regular ring* を成す．

系 10
$K_1,\ldots,K_s$ をそれぞれ体とし，$\boldsymbol{K} = K_1 \times \cdots \times K_s$ を *von Neumann regular ring* とする．任意の $\boldsymbol{a} = (a_1,\ldots,a_s) \in \boldsymbol{K}$ に対して，$\boldsymbol{a}^* = (a_1',\ldots,a_s')$，$\boldsymbol{a}^{-1} = (a_1'',\ldots,a_s'')$ とすると，

$$a_i' = \begin{cases} 1 & \text{if } a_i \neq 0, \\ 0 & \text{otherwise.} \end{cases} \qquad a_i'' = \begin{cases} \dfrac{1}{a_i} & \text{if } a_i \neq 0, \\ 0 & \text{otherwise.} \end{cases} \qquad (i = 1,\ldots,s)$$

となり，$\boldsymbol{a}^*$, $\boldsymbol{a}^{-1}$ ともに一意的である．

補題 11
$I \subset K[\bar{A}]$ を 0 次元根基イデアルとする．このとき，I の最短素イデアル分解を $I = P_1 \cap \cdots \cap P_s$ とすると，

$$K[\bar{A}]/I \simeq K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_s$$

であり，各 $K[\bar{A}]/P_i$，$(1 \leq i \leq s)$ は体であり，$K[\bar{A}]/I$ は *von Neumann regular ring* を成す．

ここで，0 次元根基イデアル $I \subset K[\bar{A}]$ と $f = \sum_{i=0}^{k} a_i(\bar{A})\bar{X}^{\alpha_i} \in (K[\bar{A}])[\bar{X}]$，$(a_i(\bar{A}) \in K[\bar{A}])$ に対して，写像 $\phi_I : K[\bar{A},\bar{X}] \longrightarrow (K[\bar{A}]/I)[\bar{X}]$ を $\phi_I(f) = \sum_{i=0}^{k}[a_i(\bar{A})]_I\bar{X}^{\alpha_i} \in (K[\bar{A}]/I)[\bar{X}]$ で定める．ϕ_I は全射準同型写像である．

以下の定理は Sato [10] の定理 3.3 である．これは von Neumann regular ring 上の多項式環の Gröbner bases と DCGB との関連を記述する．

定理 12 (Sato)
$I \subset K[\bar{A}]$ を 0 次元根基イデアル．F, $G \subset K[\bar{A},\bar{X}]$ を有限部分集合とする．このとき $\phi_I(G)$ が $\langle\phi_I(F)\rangle \subset (K[\bar{A}]/I)[\bar{X}]$ の $<_{\bar{X}}$ に関する *von Neumann regular ring* 上の *Gröbner basis* ならば，G は $<_{\bar{X}}$ に関する $\mathbf{V}(I)$ 上の *discrete comprehensive Gröbner basis* である．

4 Computation of the Quasi-inverse and the Idempotent in a $K[\bar{A}]/I$

本節では，我々の主結果である $K[\bar{A}]/I$ における quasi-inverse および idempotent 演算について述べる．まず Noro [5] による MDE の中心となる命題からはじめる．

命題 13
$I \subset K[\bar{A}]$ を 0次元根基イデアルとし，$I = P_1 \cap \cdots \cap P_s$ を I の最短素 (極大) イデアル分解とする．$a \in K[\bar{A}]$ に対して，$A = \{i \mid a \in P_i,\ 1 \leq i \leq s\}$，$B = \{i \mid a \notin P_i,\ 1 \leq i \leq s\}$ とするとき，

1. $I : a = \bigcap_{i \in B} P_i$　　2. $I + \langle a \rangle = \bigcap_{i \in A} P_i$　　3. $I = (I : a) \cap (I + \langle a \rangle)$
4. $[a]_{I:a}$ は $K[\bar{A}]/(I : a)$ において単元である．

がそれぞれ成立する．

次に $I : a$ の Gröbner basis 計算は以下の命題を元にしている．

命題 14 (Inverse or Quotient)
$I \subset K[\bar{A}]$ を 0次元根基イデアルとし，G をその $<_{\bar{A}}$ に関する *Gröbner basis* とする．このとき，$a \in K[\bar{A}]$ に対して，以下の 2つのうちどちらかが成り立つ．

1. ある $b \in K[\bar{A}]$ に対して $[ab]_I = [1]_I$ が成り立ち，$[a]_I^{-1} = [b]_I$ である．
2. 全ての $b \in K[\bar{A}]$ に対して $[ab]_I \neq [1]_I$ が成り立ち，$H = \{[b]_I \in K[\bar{A}]/I \mid [ab]_I = [0]_I\}$ とすると，H の K 線型基底 $G_H = \{g_1, \ldots, g_l\}$ を全ての頭項が異なるようにとれば，$G \cup G_H$ は $I : a$ の $<_{\bar{A}}$ に関する *Gröbner basis* である．

MDE では $[a]_I$ の逆元計算を行い，成功すればその代表元を $K[\bar{A}]/I$ における逆元として出力し，失敗すればその情報から G_H を構成し出力する．以下，本論文を通してこの関数を $\texttt{InvOrSplit}(G, f, <_{\bar{A}})$ と表し，

$$\texttt{InvOrSplit}(G, a, <_{\bar{A}}) = \begin{cases} b & \text{if } \exists b \in K[\bar{A}] \text{ such that } [a]_I[b]_I = [1]_I, \\ G \cup G_H & \text{otherwise.} \end{cases}$$

とする．また，$I + \langle f \rangle$ の Gröbner basis も MDE では modular 演算で得ている．詳細は Noro [5] の Section 2.3 を参照されたい．以下，本論文を通して $I + \langle f \rangle$ の $<_{\bar{A}}$ に関する Gröbner basis 計算を $\texttt{GBrem}(G, f, <_{\bar{A}})$ と表す．

次の命題は決定的である．

命題 15
$I \subset K[\bar{A}]$ を 0次元根基イデアルとし，$K[\bar{A}]/I$ を *von Neumann regular ring* と見なす．このとき，任意の $[a]_I \in K[\bar{A}]/I$ に対して，$[a]_I^* = [a^*]_I$, $[a]_I^{-1} = [a^{-1}]_I$ なる a^*, $a^{-1} \in K[\bar{A}]$ が存在して，

1. $[a^*]_{I:a} = [1]_{I:a}$　かつ　$[a^*]_{I+\langle a \rangle} = [0]_{I+\langle a \rangle}$.
2. $[a^{-1}]_{I:a} = [a]_{I:a}^{-1}$　かつ　$[a^{-1}]_{I+\langle a \rangle} = [0]_{I+\langle a \rangle}$.

である．

この命題により，$K[\bar{A}]/I$ における quasi-inverse 計算は MDE との親和性が大変良いと分かる．したがって，以下の quasi-inverse および idempotent 計算アルゴリズムが得られる．

Algorithm `QuasiInverse`

`INPUT:` A Gröbner basis G of a zero-dimensional radical ideal $I \subset K[\bar{A}]$, a polynomial $a \in K[\bar{A}]$ considered as an element of $K[\bar{A}]/I$, and a term order $<_{\bar{A}}$.

`OUTPUT:` A polynomial $a^{-1} \in K[\bar{A}]$ considered as the quasi-inverse element of a.

```
BEGIN
    G_q ← InvOrSplit(G, a, <_Ā);
    IF G_q is a polynomial THEN
        a^{-1} ← G_q;
    ELSE
        b^{-1} ← InvOrSplit(G_q, a, <_Ā);
        G_r ← GBrem(G, a, <_Ā);
        a^{-1} ← IPol((G_q, b^{-1}), (G_r, 0), G, <_Ā);
    END
    return a^{-1};
END
```

Algorithm `Idempotent`

`INPUT:` A Gröbner basis G of a zero-dimensional radical ideal $I \subset K[\bar{A}]$, a polynomial $a \in K[\bar{A}]$ considered as an element of $K[\bar{A}]/I$, and a term order $<_{\bar{A}}$.

`OUTPUT:` A polynomial $a^* \in K[\bar{A}]$ considered as the idempotent element of a.

```
BEGIN
    G_q ← InvOrSplit(G, a, <_Ā);
    IF G_q is a polynomial THEN
        a* ← 1;
    ELSE
        G_r ← GBrem(G, a, <_Ā);
        a* ← IPol((G_q, 1), (G_r, 0), G, <_Ā);
    END
    return a*;
END
```

ここで，$\mathtt{IPol}((G_1,a_1),(G_2,a_2),G,<_{\bar{A}})$ は $\mathrm{NF}_{G,<_{\bar{A}}}(a)=a$ かつ，$\mathrm{NF}_{G_1,<_{\bar{A}}}(a)=a_1$ かつ，$\mathrm{NF}_{G_2,<_{\bar{A}}}(a)=a_2$ を満足する $a \in K[\bar{A}]$ を計算する．G, G_1, G_2 がそれぞれ 0 次元イデアルの Gröbner basis であるときは，G に附随した標準単項式基底と未定係数法を用いた線型方程式を解くことで条件を満足する a を計算できる．今回のケースであれば補題 11 より解の存在が保証される．

定理 16

$I \subset K[\bar{A}]$ を 0 次元根基イデアルとし，G を $<_{\bar{A}}$ に関する I の Gröbner basis とする．$K[\bar{A}]/I$ を von Neumann regular ring と見なすとき，$[a]_I \in K[\bar{A}]/I$ に対して，アルゴリズム $\mathtt{QuasiInverse}(G,a,<_{\bar{A}})$, および $\mathtt{Idempotent}(G,a,<_{\bar{A}})$ は，それぞれ $[a]_I$ の quasi-inverse $[a]_I^{-1}$ の多項式表現 $a^{-1} \in K[\bar{A}]$, および idempotent $[a]_I^*$ の多項式表現 $a^* \in K[\bar{A}]$ を出力する．

$F \subset K[\bar{A},\bar{X}]$ の $\mathbf{V}(I)$ に関する DCGB を得るための $K[\bar{A}]/I$ での Gröbner basis 計算は，これまでは補題 11 にあるように I の素イデアル分解による同型 $K[\bar{A}]/I \simeq K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_s$ を用いて，各体 $K[\bar{A}]/P_i$ 上で $\phi_{P_i}(F)$ の Gröbner basis を計算し，それぞれで得られた Gröbner bases $G_{P_1},\ldots,G_{P_s}$ を CRT で結合して，$K[\bar{A}]/I$ の Gröbner basis G_I を得ていた．

しかし，本節にて $K[\bar{A}]/I$ の quasi-inverse 計算の方法を与えたので，von Neumann regular ring $K[\bar{A}]/I$ の Gröbner bases 計算を Buchberger Algorithm で直接与えることができる．von Neumann regular ring 上の多項式環での Buchberger Algorithm について，詳しくは Weispfenning [13] を参照のこと．

5 Conclusion

Von Neumann regular ring $K[\bar{A}]/I$ 上の quasi-inverse および idempotent 演算を MDE を用いることで実現できることが示せ，これを組み込むことで DCGB を Buchberger Algorithm で直接計算できることを示した．

また，$\mathbb{Q}[\bar{A},\bar{X}]$ 上で DCGB を計算する implementation を計算機代数システム Risa/Asir [6] 上にユーザー言語である Asir 言語で書いた．implementation には以下に示す工夫を盛り込んでいる．

- The Sugar strategy [2].

- Gebauer-Möller's useless pairs detection [1] on a von Neumann regular ring $K[\bar{A}]/I$.
- Göbner trace algorithm [12] on a von Neumann regular ring $K[\bar{A}]/I$.

実装は，まだ正式公開はしていない．
また，DCGB 計算と Suzuki-Sato による新しい CGS 計算法 [11] とを連携させることで，その CGS 計算の高速化に寄与できる可能性も高く，今後はそれらの検証を進めていきたい．

参 考 文 献

[1] Gebauer, R. and Möller, H.M.(1989). On an installation of Buchberger's algorithm. J. Symbolic Computation. Vol 6/2/3, pp 275-286.

[2] Giovini, A., Mora, T., Nielsi, G., Robbiano, L. and Traverso, C.(1991). "One sugar cube, please" OR Selection strategies in the Buchberger algorithm. International Symposium on Symbolic and Algebraic Computation(ISSAC '91), Proceedings. pp.49-54.

[3] Montes, A.(2002). A new algorithm for discussing Gröbner bases with parameters. J. Symbolic Computation. Vol 33/2, pp 183-208.

[4] Manubens, M and Montes, A.(2006). Improving DISPGB algorithm using the discriminant ideal. J. Symbolic Computation. Vol 41, pp 1245-1263.

[5] Noro, M.(2006). Modular Dynamic Evaluation. International Symposium on Symbolic and Algebraic Computation(ISSAC '06), Proceedings. pp.262-268.

[6] Noro, M. et al.(2006). A Computer Algebra System Risa/Asir. `http://www.math.kobe-u.ac.jp/Asir/asir.html`.

[7] Sato, Y. and Suzuki, A.(2001). Discrete Comprehensive Gröbner Bases. International Symposium on Symbolic and Algebraic Computation(ISSAC '01), Proceedings. pp.292-296.

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

[9] Sato, Y., Suzuki, A and Nabeshima, K.(2003). ACGB on Varieties. Proceedings of the 6th International Workshop on Computer Algebra in Scientific Computing(CASC 2003), pp 313-318.

[10] 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.

[11] Suzuki, A. and Sato, Y.(2006). A Simple Algorithm to compute Comprehensive Gröbner Bases using Gröbner Bases. International Symposium on Symbolic and Algebraic Computation(ISSAC '06), Proceedings. pp.326-331.

[12] Traverso, C.(1988). Gröbner trace algorithms. International Symposium on Symbolic and Algebraic Computation(ISSAC '88), Proceedings. pp.125-138.

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

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

[15] Weispfenning, V.(2003). Canonical Comprehensive Gröbner bases. J. Symbolic Computation. Vol 36, pp 669-683.