数理解析研究所講究録
第1927巻 2014年 1-9

包括的グレブナ基底系を利用した限量子消去
Quantifier Elimination by using Complehensive Gröbner Systems

深作 亮也
RYOYA FUKASAKU
東京理科大学
TOKYO UNIVERSITY OF SCIENCE *

Abstract

The concept of a comprehensive Gröbner system is a very powerful tool for solving a parametric system of equations. In 1998, Weispfenning introduced a quantifier elimination method based on the computations of comprehensive Gröbner bases. This method is very efficient in the situation where the input formula contains many equations. In this paper we improve his method based on the fact that any first order formula can be translated into the equivalent formula which contains only equations by introducing new variables.

1 はじめに

Weispfenningはグレブナー基底の性質を利用して, 包括的グレブナー基底 (comprehensive Gröbner basis, 以下CGBと略記する, [13] 参照) による限量子消去 (quantifier elimination, 以下QEと略記する) アルゴリズムを提案した ([14] 参照). このQEアルゴリズムは等式制約が多い場合には非常に有効なアルゴリズムであり, 束縛変数について等式制約が零次元イデアルとなるような場合には非常に高速なQEが可能となる. 近年になりCGB及びその計算に必要な包括的グレブナー基底系 (comprehensive Gröbner system, 以下CGSと略記する) 計算に関する効率的なアルゴリズム ([3, 4, 5, 6, 7, 8, 9, 10, 12]) が提案されている. こうした背景から現在のCGS計算アルゴリズムを利用し, さらにWeispfenningのQEアルゴリズムを改良したアルゴリズムを構築して, 高速なQEに実装を行うことを目標とした.

以降においてWeispfenningが[14]で示したQEアルゴリズム及びDolzmannが[2]で記述したQEアルゴリズムをHermitian-Gröbner-Weispfenning-QE(HGW-QE)とよぶことにする. 名前のHermitianは実根個数計算の分野におけるエルミートの貢献に由来し, Gröbnerは剰余環上の計算におけるグレブナー基底の貢献に由来し, Weispfenningは利用されたCGB及びCGS計算アルゴリズムに由来する. さらに本稿で示されるアルゴリズムはHermitian-Gröbner-Suzuki-Sato-QE(HGSS-QE)とよぶことにする. 名前のSuzuki-Satoは利用するCGS計算アルゴリズムが[12]で提案されたアルゴリズムの改良であることに由来する.

本稿は次のように構成される. 2章では本稿で利用される概念について説明する. 3章では利用するバックグラウンドについて概略を与える. 4章ではHGW-QEアルゴリズムを改良し, HGSS-QEアルゴリズムを示す上で必要な結果を示す. 5章ではHGSS-QEアルゴリズムを示す. 最後に, HGSS-QEアルゴリズムの問題点等を報告する.

*1414704@ed.tus.ac.jp

2 概念

以降では以下のような基本形を扱うことを考える：

$$\begin{aligned}
&\exists \bar{x}(f_1(\bar{y},\bar{x})=0\wedge\ldots\wedge f_{m_f}(\bar{y},\bar{x})=0\wedge\\
&\quad p_1(\bar{y},\bar{x})>0\wedge\ldots\wedge p_{m_p}(\bar{y},\bar{x})>0\wedge\\
&\quad q_1(\bar{y},\bar{x})\geq 0\wedge\ldots\wedge q_{m_q}(\bar{y},\bar{x})\geq 0\wedge\\
&\quad r_1(\bar{y},\bar{x})\neq 0\wedge\ldots\wedge r_{m_r}(\bar{y},\bar{x})\neq 0),\\
&\quad \text{where } f_1,\ldots,f_{m_f},p_1,\ldots,p_{m_p},q_1,\ldots,q_{m_q},r_1,\ldots,r_{m_r}\in\mathbb{Q}[\bar{y},\bar{x}].
\end{aligned}\tag{1}$$

さらに以下の概念を利用する．

$\bar{y}=y_1,\ldots,y_{n_y}$, $\bar{x}=x_1,\ldots,x_{n_x}$, $\bar{z}=z_{1_p},\ldots,z_{m_p},z_{1_q},\ldots,z_{m_q},z_{1_r},\ldots,z_{m_r}$ とする．$T(\bar{x})$ は $\bar{x}$ からなる項全体とする．さらに $T(\bar{x})$ の項順序 $\succ$ を固定したとき，$LM(h)$, $LT(h)$ と $LC(h)$ をそれぞれ $h\in\mathbb{Q}[\bar{y},\bar{x}]$ の $\mathbb{Q}[\bar{y},\bar{x}]$ を係数環 $\mathbb{Q}[\bar{y}]$ 上の多項式環 $(\mathbb{Q}[\bar{y}])[\bar{x}]$ とみなしたときの $\succ$ に関する先頭単項式，先頭項，先頭係数とする．ここで $LM(h)=LC(h)LT(h)$ に注意する．$\mathbb{Q}$ 上の多項式環のイデアル I に対して，$\mathbb{C},\mathbb{R}$ 上の多様体をそれぞれ $\mathbb{V}_{\mathbb{C}}(I),\mathbb{V}_{\mathbb{R}}(I)$ と記述する．$\mathbb{R}[\bar{x}]$ 上の有限集合 F について，それで生成されるイデアルは $\langle F\rangle$ で記述する．さらに適当な集合 S についてその要素数を $\#S$ で記述する．

3 バックグラウンド

まず多変数実根個数計算に関する以下の結果を示す．これは [11] の主定理の部分的な結果である．HGW-QE アルゴリズムは彼の主定理と [1] で導入されたテクニックを利用するが，HGSS-QE アルゴリズムは以下さえ扱えればよい．

定理 1
I を $\mathbb{Q}[\bar{x}]$ の零次元イデアルとする．このとき，剰余環 $A=\mathbb{R}[\bar{x}]/I$ は $\mathbb{R}$-ベクトル-空間として有限次元であるので，その基底を $(t_1,\ldots,t_d)$ とする．このとき，写像 $m_{ij}:A\mapsto A;a\mapsto at_it_j$ は線形写像となるので $(t_1,\ldots,t_d)$ に関するそれの表現行列を m'_{ij} とし，そのトレースを M_{ij} とする．さらに $(d\times d)$ 対称行列 $M=(M_{ij})$ を考え，ρ をその符号数とする．このとき以下が成立する：

$$\rho=\#V_{\mathbb{R}}(I)$$

以下はデカルトの符号律と実対称行列の固有値は実であるという事実から示される．

系 2
M を対称行列として，$\chi_+(X)$ を次数 d の M の固有多項式とし $\chi_-(X)=\chi_+(-X)$ とする．このとき，$\chi_+(X)$ の次数 i に関する係数を a_i で記述し，$\chi_-(X)$ の次数 i に関する係数を b_i で記述する．さらに係数列 $(a_d,a_{d-1},\ldots,a_0)$ に関する符号の変化数を S_+ として，$(b_d,b_{d-1},\ldots,b_0)$ に関する符号の変化数を S_- とする．ここで 0 は無視する．このとき以下がいえる：

1. $S_+=\#\{c\in\mathbb{R}|c>0\wedge\chi_+(c)=0\}$.
2. $S_-=\#\{c\in\mathbb{R}|c<0\wedge\chi_+(c)=0\}$.

最後に定義を与える．まずは分割と分割部についての定義である．

定義 3
$\mathbb{R}^{n_y}$ 上の部分集合による $\{\mathcal{S}_1, \ldots, \mathcal{S}_s\}$ は以下を満たすとき $\mathbb{R}^{n_y}$ の分割とよばれる：

1. $\cup_{i=1}^{s} \mathcal{S}_i = \mathbb{R}^{n_y}$.
2. 相異なる i, j について $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$.

各 $\mathcal{S}_i$ は分割部とよばれる. 以降, 分割部をその定義論理式と同一視することにする.

次に CGS の定義を与える.

定義 4
$\succ$ を $T(\bar{x})$ の項順序とする. $\mathbb{Q}[\bar{y}, \bar{x}]$ 上の有限集合 F に対し, 以下を満たすとき有限集合 $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_s, G_s)\}$ をパラメータ $\bar{y}$ と主変数 $\bar{x}$ の $\succ$ に関する CGS とよぶ：

1. 各 G_i が $\mathbb{Q}[\bar{y}, \bar{x}]$ の有限部分集合である.
2. $\{\mathcal{S}_1, \ldots, \mathcal{S}_s\}$ が $\mathbb{R}^{n_y}$ の分割である.
3. $\bar{c} \in \mathcal{S}_s$ に対して $G_i(\bar{c}, \bar{x}) = \{g(\bar{c}, \bar{x}) : g \in G_i\}$ が $\langle F(\bar{c}, \bar{x})\rangle$ の $\succ$ に関するグレブナー基底である.

各 $G_i(\bar{c}, \bar{x})$ が簡約 (極小) であれば $\mathcal{G}$ も簡約 (極小) とよばれる. (モニックであることは必要ないとする.)

4 理論

まず、以下の事実たちを与える.

補題 5
$p, q, r \in \mathbb{R}[\bar{x}]$ として z_p, z_q, z_r を変数とする. このとき以下がいえる：

1. $p(\bar{x}) > 0 \Leftrightarrow 1 - z_p^2\, p(\bar{x}) = 0$.
2. $q(\bar{x}) \geq 0 \Leftrightarrow z_q^2 - q(\bar{x}) = 0$.
3. $r(\bar{x}) \neq 0 \Leftrightarrow 1 - z_r\, r(\bar{x}) = 0$.

補題 6
$p, q \in \mathbb{R}[\bar{x}]$ として $c_1, c_2 \in \mathbb{R}$ とする. $c_1 < c_2$ を仮定する. このとき以下がいえる：

1. $c_1 < p(\bar{x}) \wedge p(\bar{x}) < c_2 \Leftrightarrow (p(\bar{x}) - c_1)(c_2 - p(\bar{x})) > 0$.
2. $c_1 \leq q(\bar{x}) \wedge q(\bar{x}) \leq c_2 \Leftrightarrow (q(\bar{x}) - c_1)(c_2 - q(\bar{x})) \geq 0$.

HGSS-QE アルゴリズムでは補題 5 を使って示される以下を使う.

定理 7
基本形 (1) は以下と等価である：

$$
\begin{aligned}
\exists \bar{z}, \bar{x} (& f_1(\bar{y}, \bar{x}) = 0 \wedge \ldots \wedge f_{m_f}(\bar{y}, \bar{x}) = 0 \wedge \\
& 1 - z_{1_p}^2 p_1(\bar{y}, \bar{x}) = 0 \wedge \ldots \wedge 1 - z_{m_p}^2 p_{m_p}(\bar{y}, \bar{x}) = 0 \wedge \\
& z_{1_q}^2 - q_1(\bar{y}, \bar{x}) = 0 \wedge \ldots \wedge z_{m_q}^2 - (\bar{y}, \bar{x}) = 0 \wedge \\
& 1 - z_{1_r} r_1(\bar{y}, \bar{x}) = 0 \wedge \ldots \wedge 1 - z_{m_r} r_{m_r}(\bar{y}, \bar{x}) = 0).
\end{aligned}
$$

HGSS-QE は新しい変数を定理 7 のように導入するが, これを戦略的に行うことですべての新しい変数も含めて束縛変数を消去できることが以下よりわかる.

定理 8

$p_1,\ldots,p_{m_p},q_1,\ldots,q_{m_q},r_1,\ldots,r_{m_r}\in\mathbb{R}[\bar{x}]$ として I を $\mathbb{R}[\bar{x}]$ の零次元イデアルとする．さらに J を $\mathbb{R}[\bar{x},\bar{z}]$ のイデアル $I+\langle 1-Z_{1_p}^2p_1\ldots,1-Z_{m_p}^2p_{m_p},Z_{1_q}^2-q_1,\ldots,Z_{m_q}^2-q_{m_q},1-Z_{1_r}r_1,\ldots,1-Z_{m_r}r_{m_r}\rangle$ とする．このとき J は $\mathbb{R}[\bar{x},\bar{z}]$ の零次元イデアルとなる．

証明

$\mathbf{V}_{\mathbb{C}}(I)$ が $\mathbb{C}^{n_x}$ 上で有限である．従って $\#\mathbf{V}_{\mathbb{C}}(J)$ も $\mathbb{C}^{n_x+m_p+m_q+m_r}$ 上で有限である．従って J は $\mathbb{R}[\bar{x},\bar{z}]$ の零次元イデアルである．

さらに以下によって HGSS-QE が HGW-QE を改良したことがわかる．ここで剰余環 A に対して，その次元を $dim(A)$ と記述する．

系 9

$p_1,\ldots,p_{m_p},r_1,\ldots,r_{m_r}\in\mathbb{R}[\bar{x}]$ として，I を $\mathbb{R}[\bar{x}]$ の零次元イデアルとする．ここで定理 8 より $J=I+\langle 1-Z_{1_p}^2p_1\ ,\ldots,1-Z_{m_p}^2p_{m_p}\ ,1-Z_{1_r}r_1,\ldots,1-Z_{m_r}r_{m_r}\rangle$ は $\mathbb{R}[\bar{x},\bar{z}]$ の零次元イデアルとなる．このとき $dim(\mathbb{R}[\bar{x},\bar{z}]/J)\leq 2^{m_p}\cdot dim(\mathbb{R}[\bar{x}]/I)$ となる．

5 アルゴリズム

[14] で (1) を扱う場合，$2^{m_q}2^{m_r}$ 個の論理式を扱う必要があり，[2] では 2^{m_q} 個の論理式を扱う必要がある．まずは以下に HGSS-QE のトップ関数 **MainQE** を記述する．この関数の正確性及び停止性は CGS の定義と他の関数の正確性及び停止性から示されることに注意する．さらに他関数に渡される G は分割部に対応する等式制約イデアルのグレブナー基底である．よって以下における他関数の入力 G は分割部に対応するそれのグレブナー基底になっていることとする．

Algorithm 1 MainQE

Input: a formula ϕ such as (1),

Output: the free quantified formula ψ; $\{\phi\Leftrightarrow\psi.\}$

1: $\prec\leftarrow$ a term order of $T(\bar{x})$;
2: $\mathcal{G}\leftarrow$ a minimal CGS of $\langle f_1(\bar{y},\bar{x}),\ldots,f_{m_f}(\bar{y},\bar{x})\rangle$ with main variables $\bar{x}$, parameters $\bar{y}$ with respect to $\prec$;
3: $\psi\leftarrow false$;
4: **while** $\mathcal{G}\neq\emptyset$ **do**
5: $\quad(\mathcal{S},G)\leftarrow$ the element of $\mathcal{G}$;
6: $\quad\mathcal{G}\leftarrow\mathcal{G}\setminus\{(\mathcal{S},G)\}$;
7: $\quad$**if** $\langle G(\bar{c},\bar{x})\rangle$ is zero dimensional for $\bar{c}\in\mathcal{S}$ **then**
8: $\quad\quad\psi'\leftarrow$ **ZeroDimQE**$(\phi,\mathcal{S},G)$;
9: $\quad$**else**
10: $\quad\quad\psi'\leftarrow$ **NonZeroDimQE**$(\phi,\mathcal{S},G,\prec)$; or $\psi'\leftarrow$ **OtherQE**$(\phi,\mathcal{S},G)$;
11: $\quad$**end if**
12: $\quad\psi\leftarrow\psi\vee\psi'$;
13: **end while**
14: Return ϕ;

次に等式制約が零次元イデアルとなる分割部に対する処理を行う関数として **ZeroDimQE**, **SignatureNonZero** を与える．これらの停止性は CGS の定義から従い，正確性は定理 1, 定理 7, 定理 8 から従う．

ここで **ZeroDimQE** のステップ 16 のような対称行列について HGW-QE と HGSS-QE を比較するために $m_q, m_r = 0$ とする．このとき等式制約のイデアルによる剰余環の次元を d とすると，[14] において HGW-QE はちょうど $d \cdot 2^{m_p}$ 次の対称行列を扱うことになる．しかし HGSS-QE は系 9 より $d \cdot 2^{m_p}$ 次以下の対称行列を扱うことができる．また系 9 を拡張することで，[2] についても，そこで HGW-QE が扱う対称行列よりサイズの小さい対称行列を HGSS-QE は扱えることがわかる．さらに補題 6 を利用すればさらにサイズの小さい対称行列を扱える．

次に **SignatureNonZero** のステップ 4 の $I_d(a_0, \ldots, a_{d-1})$ について定義する．$(d \times d)$ 対称行列 $M = (M_{ij})$ を $M_{ij} \in \mathbb{Q}(\bar{y})$ とする．このとき $\chi_+(X)$ をその固有多項式としてさらに $\chi_-(X) = \chi_+(-X)$ とする．そして系 2 のように $(a_0, \ldots, a_{d-1})$, $(b_0, \ldots, b_{d-1})$ を構成し，同様に C_+, C_- を構成する．このとき，$1 \leq i \leq d$ に対して，$a_i, b_i \in \mathbb{Q}(\bar{y})$ となり，$a_i = b_i$ (i : 偶数), $a_i = -b_i$ (i : 奇数) となる．従って $C_+ \neq C_-$ となるような論理式 $I_d(a_0, \ldots, a_{d-1})$ を論理記号と $a_i \sigma_i 0 (\sigma_i \in \{<, >, =\})$ のみで構成できる．このとき，$I_d(a_0, \ldots, a_{d-1})$ は M の符号数が零でないことと等価である．さらに $I_d(a_0, \ldots, a_{d-1})$ は前もって簡略化できる．

以降記述される **NonZeroDimQE** の再帰計算に注意すると上記二点は出力の簡略化だけでなく計算効率にも重要となる．

Algorithm 2 ZeroDimQE

Input: a formula ϕ such as (1), a segment $\mathcal{S}$, a finite set G of $\mathbb{Q}[\bar{y}, \bar{x}]$,

Output: the free quantified formula ψ; $\{ (\mathcal{S} \wedge \phi) \Leftrightarrow \psi. \}$

1: $\bar{z} \leftarrow$ new variables $z_{1_p}, \ldots, z_{m_p}, z_{1_q}, \ldots, z_{m_q}, z_{1_r}, \ldots, z_{m_r}$;
2: $H \leftarrow G \cup \bigcup_{i=1}^{m_p} \{1 - z_{i_p}^2 p_i\} \cup \bigcup_{i=1}^{m_r} \{1 - z_{i_r} r_i\}$;
3: $\prec' \leftarrow$ a term order of $T(\bar{x}, z_{1_p}, \ldots, z_{m_p}, z_{1_r}, \ldots, z_{m_r})$;
4: $\mathcal{G}' \leftarrow$ a minimal CGS of H with parameters $\bar{y}$ main variables $\bar{x}, z_{1_p}, \ldots, z_{m_p}, z_{1_r}, \ldots, z_{m_r}$ with respect to $\prec'$;
5: $\psi \leftarrow false$;
6: **while** $\mathcal{G}' \neq \emptyset$ **do**
7: $(\mathcal{S}', G') \leftarrow$ the element of $\mathcal{G}'$;
8: $\mathcal{G}' \leftarrow \mathcal{G}' \setminus \{(\mathcal{S}', G')\}$;
9: $H' \leftarrow G' \cup \bigcup_{i=1}^{m_q} \{z_{i_q}^2 - q_i\}$;
10: $(t_1, \ldots, t_d) \leftarrow$ a basis of the residue class ring $\mathbb{R}[\bar{x}, \bar{z}] / \langle H'(\bar{c}, \bar{x}, \bar{z}) \rangle$ for $\bar{c} \in \mathcal{S}'$;
11: **for** $1 \leq i, j \leq d$ **do**
12: $m_{ij} \leftarrow$ the linear map $a \mapsto a t_i t_j$;
13: $m'_{ij} \leftarrow$ the representing matrix of m_{ij} with respect to $(t_1, \ldots, t_d)$;
14: $M_{ij} \leftarrow$ the trace of m'_{ij};
15: **end for**
16: $M \leftarrow$ the matrix (M_{ij});
17: $\psi' \leftarrow$ **SignatureNonZero**(M);
18: $\psi \leftarrow \psi \vee (\mathcal{S}' \wedge \psi')$;
19: **end while**
20: Return ψ;

Algorithm 3 SignatureNonZero

Input: a symmetric matrix M;

Output: the equivalent formula such that the signature of M noes not equal zero;

1: $\chi(X) \leftarrow$ the characteristic polynomial of M;

2: $d \leftarrow$ the degree of $\chi(X)$;

3: $a_0, \ldots, a_{d-1} \leftarrow$ the coefficient sequence of $\chi(X)$ with respect to the degree of X;

4: Return $I_d(a_0, \ldots, a_{d-1})$;

次に等式制約が零次元イデアルとならない分割部に対する処理を行う関数として **NonZeroDimQE**, **OtherQE** を与える.

OtherQE において我々はステップ 2 で他の QE アルゴリズムを利用する. したがって, 停止性及び正確性はその利用したアルゴリズムから従う.

NonZeroDimQE は他関数を利用するため, その停止性及び正確性は他関数に依存している. よって **NonZeroDimQE** の停止性は CGS の定義, 束縛変数の有限性及び他関数の停止性より従い, 正確性は他関数の正確性より従うことに注意しなければならない.

NonZeroDimQE において我々は極大独立変数を自由変数とみていることに注意する. これにより適用された **NonZeroDimQE** 内部で利用される **ZeroDimQE** の出力によっては **NonZeroDimQE** の記述の通り, 再帰計算を行うことになる.

アルゴリズム **MainQE** のステージ 10 における **NonZeroDimQE** と **OtherQE** を利用した場合の比較を行う. **NonZeroDimQE** 内部で利用される **ZeroDimQE** の出力が複雑になっている場合や極大独立変数の個数が多い場合は **OtherQE** を利用したほうが効率的となる. しかしながら, これの出力が簡略であるときや極大独立変数の個数が少ないときは **NonZeroDimQE** を利用したほうが効率的である.

実験によると本アルゴリズムによる実装は他のアルゴリズム (つまり他のプログラム) よりも効率的となる場合が多い. それはアルゴリズム **MainQE** のステージ 10 で **OtherQE** を利用した場合も同様である. その理由は CGS の分割部による場合わけで入力が簡略化されるためである. つまり CGS 計算は問題の簡略化を行うこともできる. このようにアルゴリズム **MainQE** のステージ 10 で **OtherQE** を利用した場合でも CGS 計算は無駄にならない.

NonZeroDimQE による HGSS-QE は HGW-QE に近いそれの改善アルゴリズムになっているが, 以下に記述するような違いが存在する. それは **NonZeroDimQE** の中で等式制約がなくなった場合の処理の違いである. こうした場合に我々は **OtherQE**(つまり, 他のアルゴリズム) を利用する. HGW-QE において論理式の変換によって HGW-QE 自体を利用する. ここで他のアルゴリズムを利用した理由はその変換により処理しなければならない論理式が増えるためである.

Algorithm 4 OtherQE

Input: a formula ϕ such as (1), a segment $\mathcal{S}$, a finite set G of $\mathbb{Q}[\bar{y}, \bar{x}]$;

Output: the free quantified formula ψ; { $\psi \Leftrightarrow (\mathcal{S} \wedge \phi)$. }

1: $\phi' \leftarrow \exists \bar{x}(\mathcal{S} \wedge \bigwedge_{g \in G} g = 0 \wedge \bigwedge_{i_p=1}^{m_p} p_{i_p} > 0 \wedge \bigwedge_{i_q=1}^{m_q} q_{i_q} \geq 0 \wedge \bigwedge_{i_r=1}^{m_r} r_{i_r} \neq 0)$;

2: $\psi \leftarrow$ the output of the other QE algorithm applying with ϕ';

3: Return ψ;

Algorithm 5 NonZeroDimQE

Input: a formula ϕ such as (1), a segment $\mathcal{S}$ of $\mathbb{R}^{n_x}$, a finite set G of $\mathbb{Q}[\bar{y}, \bar{x}]$, a term order $\prec$ of $T(\bar{x})$;

Output: the free quantified formula ψ; { $(\mathcal{S} \wedge \phi) \Leftrightarrow \psi$. }

$\bar{m} \leftarrow$ the maximal independent set of $\langle G(\bar{a}) \rangle$ for $\bar{a} \in \mathcal{S}$;
$\bar{x}' \leftarrow \bar{x} \setminus \bar{m}$;
if $\bar{x}' = \bar{x}$ **then**
  $\psi \leftarrow$ **OtherQE**(ϕ,$\mathcal{S}$,G);
  Return ψ;
else
  $\bar{y}' \leftarrow \bar{y} \cup \bar{m}$;
  $\prec' \leftarrow$ a term order of $T(\bar{x}')$;
  $\mathcal{G}' \leftarrow$ a minimal CGS of G with respect to with main variables $\bar{x}'$, parameters $\bar{y}'$ with respect to $\prec'$;
  $\psi \leftarrow false$;
  while $\mathcal{G}' \neq \emptyset$ **do**
    $(\mathcal{S}', G') \leftarrow$ the element of $\mathcal{G}'$;
    $\mathcal{G}' \leftarrow \mathcal{G}' \setminus \{(\mathcal{S}', G')\}$;
    $\phi' \leftarrow \exists \bar{x}'(\mathcal{S}' \wedge \bigwedge_{g \in G'} g = 0 \wedge \bigwedge_{i_p=1}^{m_p} p_{i_p} > 0 \wedge \bigwedge_{i_q=1}^{m_q} q_{i_q} \geq 0 \wedge \bigwedge_{i_r=1}^{m_r} r_{i_r} \neq 0)$;
    if $\langle G'(\bar{c}', \bar{x}') \rangle$ is zero dimensional for $\bar{c}' \in \mathcal{S}'$ **then**
      $\psi' \leftarrow$ **ZeroDimQE**($\psi', \mathcal{S}', G'$);
    else
      $\psi' \leftarrow$ **NonZeroDimQE**($\phi', \mathcal{S}', G', \prec'$);
    end if
    $\psi'_1, \ldots, \psi'_l \leftarrow$ formulas such that $\psi'_1 \vee \ldots \vee \psi'_l$ is the disijunctive normal form of ψ' , where ψ'_i is form of (1) without quantifiers;
    $\psi'' \leftarrow false$;
    for $1 \leq i \leq l$ **do**
      $\psi''_i \leftarrow$ **MainQE**($\exists \bar{m}(\psi'_i)$);
      $\psi'' \leftarrow \psi'' \vee \psi''_i$;
    end for
    $\psi \leftarrow \psi \vee \psi''$;
  end while
  Return ψ;
end if

HGSS-QE は上記のような関数で構成されている. **NonZeroDimQE** のように正確性及び停止性が他関数の正確性及び停止性から従っていることがあった. しかしながら HGSS-QE 全体としての正確性及び停止性は **ZeroDimQE**(, **SignatureZeo**) 及び **OtherQE** の正確性及び停止性から従う. これは HGSS-QE の末端にはこれらのいずれかがいるためである.

6 まとめ

前節でアルゴリズム **MainQE** のステージ 10 における **NonZeroDimQE** と **OtherQE** を利用した場合の比較を行った. **NonZeroDimQE** が非効率的となる場合の原因は前述の通り, **NonZeroDimQE** 内部で利用される **ZeroDimQE** の出力が複雑になっていることや極大独立変数の個数が多いことである. 極大独立変数のとり方によって我々はこれを改善することができるかもしれない. しかしながら, **NonZeroDimQE** 内部で利用される **ZeroDimQE** の出力の簡略化が改善するための鍵であると考えている. これに関して **SignatureZero** の出力の簡略化 (つまり $I_d(a_0, \ldots, a_{d-1})$ の簡略化) により **NonZeroDimQE** 内部で利用される **ZeroDimQE** の出力はかなり改善されてきている. しかしながら, これとは別の簡略化手法も考える必要があるように考えている.

参 考 文 献

[1] Ben-Or, M., Kozen, D. and Reif, J. : The Complexity of Elementary Algebra and Geometry, Proceedings of the sixteenth annual ACM symposium on Theory of computing, 1986, pp.251-264.

[2] Dolzmann, A., Gilch, L. : Generic Hermitian Quantifier Elimination, Lecture Notes in Computer Science Vol.3249, 2004, pp.80-93.

[3] Kapur, D., Sun, Y. and Wang, D. : A New Algorithm for Computing Comprehensive Gröbner Systems, Proceedings of International Symposium on Symbolic and Algebraic Computation, 2010, pp.29-36.

[4] Kurata, Y. : Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation, Communications of JSSAC Vol.1, 2011, pp.39-66.

[5] Montes, A. : A new algorithm for discussing Gröbner bases with parameters, Journal of Symbolic Computation Vol.33-2, 2002, pp.183-208.

[6] Manubens, M. and Montes, A. : Improving DISPGB algorithm using the discriminant ideal, Journal of Symbolic Computation Vol.41, 2006, pp.1245-1263.

[7] Manubens, M. and Montes, A. : Minimal Canonical Comprehensive Gröbner System, Journal of Symbolic Computation Vol.44, 2009, pp.463-478.

[8] Montes, A. and Wibmer, M. : Gröbner Bases for Polynomial Systems with parameters, Journal of Symbolic Computation Vol.45, 2010, pp.1391-1425.

[9] Nabeshima, K. : A Speed-Up of the Algorithm for Computing Comprehensive Gröbner Systems, Proceedings of International Symposium on Symbolic and Algebraic Computation, 2007, pp.299-306.

[10] Nabeshima, K. : Stability Conditions of Monomial Bases and Comprehensive Gröbner systems, Lecture Notes in Computer Science Vol.7442, 2012, pp.248-259.

[11] Pedersen, P., Roy, M, F. and Szpirglas, A. : Counting real zeroes in the multivariate case, Progress in Mathematics Vol.109, 1993, pp.203-224.

[12] Suzuki, A. and Sato, Y. : A Simple Algorithm to Compute Comprehensive Groöbner Bases Using Gröbner Bases, Proceedings of International Symposium on Symbolic and Algebraic Computation, 2006, pp.326-331.

[13] Weispfenning, V. : Comprehensive Gröbner Bases. Journal of Symbolic Computation Vol.14-1, 1992, pp.1-29.

[14] Weispfenning, V. : A New Approach to Quantifier Elimination for Real Algebra, Quantifier Elimination and Cylindrical Algebraic Decomposition, 1998, pp.376-392.