数理解析研究所講究録
第1907巻 2014年 132-141

On QE Algorithms over algebraically closed field

東京理科大学 深作 亮也, 井上秀太郎, 佐藤洋祐
Ryoya Fukasaku, Shutaro Inoue, Yosuke Sato
Tokyo university of science

1 はじめに

代数的閉体における限量子消去 (QE) は理論的には実閉体における QE より実装が単純である. そして, これには主に三つの手法がある.

まず, パラメトリックな GCD の計算を利用した手法 (GCD-QE と略記する) である. 特に Mathematica の Reduce, Resolve はこれで実装されているが, グレブナー基底の計算を利用した技巧的な手法によって実装されている ([7]). この実装は他の GCD-QE による実装 ([3] 等) に比べて最も効率的な実装である. しかしながら, GCD-QE は一変数消去を再帰的に繰り返すため, 限量子変数が多い場合, 計算時間が長くなりがちであり, さらにその出力は複雑になりがちである.

次に, characteristic sets の計算を利用した手法 ([11, 12, 13] 参照, CS-QE と略記する) がある. Maple の Projection はこの CS-QE によって実装されている. この手法は GCD-QE と違い, 限量子変数たちを一度に消去できるが, その出力は複雑である. これは regular chains の計算において多様体たちを構成してしまうためである. もし, 我々がその出力を単純化したいのであれば, 他の単純化手法が必要となってしまう.

最後に, 包括的グレブナ基底系 (CGS) を利用した手法 (CGS-QE と略記する) がある. CGS 計算は単純ではないが, 一度 CGS を計算することで即座に, そして一度に限量子変数たちを消去できる. [10, 8, 5, 6, 9] 等の研究結果によって, 我々は CGS 計算のための実用的な実装が可能となった. 特に [9] で提案されたアルゴリズムは多くの場合において最小の分割部 (Definition 3 参照) を持つような CGS を計算する. 従って, このアルゴリズムを利用することで我々は単純な限量子消去された論理式を得ることができる. 我々は計算機代数システム Risa/Asir([1]) にこのアルゴリズムを利用した CGS-QE を実装した. 我々の実験によれば多くの場合において我々の CGS-QE による限量子消去された出力が上記の Mathematica や Maple のプログラムたち以上に単純な出力であった. しかしながら, CGS-QE には欠点がある. それは Rabinovich's trick を利用した非等式に対する新しい変数の導入である. 特に, 非等式の個数が多い場合には CGS-QE の計算はかなり重たいものになってしまう.

そこで我々はそれなりの計算時間で単純な出力をするような QE を実現するために新しい手法 Hybrid-QE を提案する. この手法は CGS-QE をベースにして部分的に GCD-QE を利用する. 我々はこの手法も Risa/Asir に実装し, 数値実験を行った. この数値実験では多くの場合においてこの手法が他の手法に比べて優れていた. また, 我々の新しい手法の主目的は単純化された論理式を得ることであったが, 多くの場合において Mathematica の GCD-QE プログラムだけでなく Maple の CS-QE プログラム以上に計算効率のよいプログラムになった.

以下において, 二章ではCGSとグレブナー基底の安定性に関する最低限の知識のみを紹介する. 三章ではMathematicaに実装されているGCD-QEアルゴリズムを紹介し, 四章ではCGS-QEアルゴリズムを紹介する. 五章では我々の新しいアルゴリズムHybrid-QEを提案し, 六章は我々の実験結果について報告する.

また, 以下のために次のように設定しておく. K を体, $\overline{K}$ をその代数閉包とする. $K[\bar{Y},\bar{X}]$ は $\bar{Y}=Y_1,\ldots,Y_m$ と $\bar{X}=X_1,\ldots,X_n$ を変数とした多項式環とする. σ は $K[\bar{Y}]$ から $\overline{K}$ への準同型写像とし, それは自然に $K[\bar{Y},\bar{X}]$ から $\overline{K}[\bar{X}]$ への準同型写像へと拡張できる. $T(\bar{X})$ は $\bar{X}$ からなる項全体とし, $T(\bar{Y},\bar{X})$ 上の各 X_i が $T(\bar{Y})$ 上の任意の項以上となるような項順序を $\bar{X}\gg\bar{Y}$ と記述することにする. $T(\bar{X})$ 上のある項順序 $>$ を固定したとき $LM(h)$, $LT(h)$, $LC(h)$ は各々, $K[\bar{Y},\bar{X}]$ を多項式環 $(K[\bar{Y}])[\bar{X}]$ とみなしたときの h の先頭単項式, 先頭項, 先頭係数とする. ここで $LM(h)=LC(h)LT(h)$ となることに注意する. また K 上の多項式環のイデアル I に対して, $\overline{K}$ 上のその多様体を $\mathbb{V}(I)$ と書くことにする.

そして最後に我々は以降, 以下の基本論理式のみを扱うということに注意する.

$$\exists\bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge f_s(\bar{Y},\bar{X})=0\wedge g_1(\bar{Y},\bar{X})\neq 0\wedge\cdots\wedge g_t(\bar{Y},\bar{X})\neq 0) \tag{0}$$

2 グレブナー基底の安定性とCGS

まず, グレブナー基底の安定性に関する [5, 6] で考えられた [4] の Theorem 3.1 からの結果を紹介する.

Theorem 1
I を $K[\bar{Y},\bar{X}]$ のイデアルとし, G を $K[\bar{Y},\bar{X}]$ を多項式環 $(K[\bar{Y}])[\bar{X}]$ とみなしたときの $>$ に関する I のグレブナー基底とする. ここで $G=\{g_1,\ldots,g_s,\ldots,g_t\}$ は以下のような性質 (i), (ii) を持つとする.
(i) $G\cap K[\bar{Y}]=\{g_{s+1},\ldots,g_t\}$
(ii) $\sigma(g_{s+1})=\sigma(g_{s+2})=\cdots=\sigma(g_t)=0$
ここで $\{LT(g_{n_1}),\ldots,LT(g_{n_l})\}$ を $\{LT\ (g_1),\ldots,LT(g_s)\}$ の中で他の項に割り切られる要素を排除した最小の部分集合とする.
このとき, $\sigma(LM(g_{n_1}))\neq 0,\ldots,\sigma(LM(g_{n_l}))\neq 0$ となれば, $G'=\{\sigma(g_{n_1}),\ldots,\sigma(g_{n_l})\}$ は $\langle\sigma(I)\rangle$ の $>$ に関するグレブナー基底となる. この結果は各 $i\in\{1,\ldots,s\}-\{n_1,\ldots,n_l\}$ に対して $\sigma(LM(g_i))=0$ となるかならないかにはよらない.

$(K[\bar{Y}])[\bar{X}]$ 上のグレブナー基底は $K[\bar{Y},\bar{X}]$ 上で $\bar{X}\gg\bar{Y}$ を満足するような項順序を利用したグレブナー基底計算で計算可能である.

Definition 2
$\overline{K}^m$ の部分集合たちによる有限集合 $\{\mathcal{P}_1,\ldots,\mathcal{P}_s\}$ は以下の性質を満たしたとき $\overline{K}^m$ の**分割**と呼ばれる.
(i) $\cup_{i=1}^{s}\mathcal{P}_i=\overline{K}^m$
(ii) 相異なる i,j に対して $\mathcal{P}_i\cap\mathcal{P}_j=\emptyset$
(iii) 各 $\mathcal{P}_i$ が $K[\bar{Y}]$ 上の有限部分集合 P_i,Q_i たちに対して $\mathcal{P}_i=\mathbb{V}(\langle P_i\rangle)-\mathbb{V}(\langle Q_i\rangle)$ となる.

Definition 3
$>$ を $T(\bar{X})$ の項順序とする. $K[\bar{Y},\bar{X}]$ 上の有限部分集合 F に対して有限集合 $\mathcal{G}=\{(\mathcal{P}_1,G_1),\ldots,(\mathcal{P}_s,G_s)\}$ は次の性質 (i)-(iii) を満たすとき F のパラメータ $\bar{Y}$, 主変数 $\bar{X}$ の $>$ に関する *CGS*(**包括的グレブナー基底**

系) と呼ばれる.
(i) 各 G_i が $K[\bar{Y},\bar{X}]$ の有限部分集合である.
(ii) $\{\mathcal{P}_1,\ldots,\mathcal{P}_s\}$ は $\overline{K}^m$ の分割である.
(iii) 任意の $\bar{c}\in\mathcal{P}_s$ に対して $G_i(\bar{c},\bar{X})=\{g(\bar{c},\bar{X}):g\in G_i\}$ は $\overline{K}[\bar{X}]$ のイデアル $\langle F(\bar{c},\bar{X})\rangle$ の $>$ に関するグレブナー基底である.
さらに各 $G_i(\bar{c},\bar{X})$ が簡約 (最小) グレブナー基底であるとき, $\mathcal{G}$ は簡約 (最小) 包括的グレブナー基底系と呼ばれる. (ここで各多項式はモニックでなくてもよいこととする.) 各 $\mathcal{P}_i$ は $\mathcal{G}$ の**分割部**と呼ばれる.

最後に $\sqrt{I}$ をイデアル I の根基イデアル, $\neg$ を否定とする.

Lemma 4
$f_1,\ldots,f_s,g_1,\ldots,g_t$ を $K[\bar{Y},\bar{X}]$ の多項式としたとき, 次は等価となる:
(i) $\exists\bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge f_s(\bar{Y},\bar{X})=0\wedge g_1(\bar{Y},\bar{X})\neq 0\wedge\cdots\wedge g_t(\bar{Y},\bar{X})\neq 0)$
(ii) $\exists\bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge f_s(\bar{Y},\bar{X})=0\wedge g_1(\bar{Y},\bar{X})\cdots g_t(\bar{Y},\bar{X})\neq 0)$
(iii) $\neg(\forall\bar{X}(g_1(\bar{Y},\bar{X})\cdots g_t(\bar{Y},\bar{X})\in\sqrt{\langle f_1(\bar{Y},\bar{X}),\cdots,f_s(\bar{Y},\bar{X})\rangle}))$
(iv) $\exists\bar{Z}\bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge f_s(\bar{Y},\bar{X})=0\wedge 1-Z_1g_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge 1-Z_tg_t(\bar{Y},\bar{X})=0)$

3 GCD-QE アルゴリズム

この章では Mathematica の Reduce, Resolve に実装された GCD-QE アルゴリズムを紹介する.
$g(\bar{Y},\bar{X})=g_1(\bar{Y},\bar{X})\cdots g_t(\bar{Y},\bar{X})$ としたとき, Lemma 4 から基本論理式 (0) は以下と等価である.

$$\exists\bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge f_s(\bar{Y},\bar{X})=0\wedge g(\bar{Y},\bar{X})\neq 0) \tag{1}$$

$\exists X_n$ を $\exists X_n(f_1(\bar{Y},\bar{X})=0\wedge\cdots\wedge f_s(\bar{Y},\bar{X})=0\wedge g(\bar{Y},\bar{X})\neq 0)$ から消去して, 等価な限量子消去された論理式を得た場合, それを $\vee\wedge$-canonical form に変換して $\exists X_1\exists X_2\ldots\exists X_{n-1}$ のついた基本論理式たちを計算する. 従って, 一つの限量子変数に対してアルゴリズムを与える限り, すべての限量子変数を消去するためにそれを再帰的に適用する必要がある. $K=\mathbb{Q}$, $\overline{K}=\mathbb{C}$ の場合に対して Mathematica の Reduce, Resolve はグレブナー基底計算を利用し技巧的にこの戦略を採用している. Algorithm 1 においてこのアルゴリズムを示すことにする.

Algorithm 1 GCD-QE algorithm of Mathematica

Input: $\exists X(f_1(\bar{Y},X)=0\wedge\ldots\wedge f_s(\bar{Y},X)=0\wedge g(\bar{Y},X)\neq 0)$;

Output: An equivalent quantifier free formula;

1: $R\leftarrow false$;
2: $I\leftarrow\langle f_1,\ldots,f_s\rangle$;
3: $>\leftarrow$ a term order s.t. $X\gg\bar{Y}$;
4: $G\leftarrow$ a reduced Gröbner basis of I w.r.t. $>$ in $K[\bar{Y},X]$;
5: **if** $G=\{1\}$ **then**
6: Return $false$;
7: **else**
8: $\{h_1(\bar{Y}),\ldots,h_t(\bar{Y})\}\leftarrow G\cap K[\bar{Y}]$;
9: $\{g_1(\bar{Y},X),\ldots,g_l(\bar{Y},X)\}\leftarrow G-\{h_1(\bar{Y}),\ldots,h_t(\bar{Y})\}$;
10: **if** $\{g_1(\bar{Y},X),\ldots,g_l(\bar{Y},X)\}\neq\emptyset$ **then**
11: $g_i\leftarrow$ the least degree polynomial for $1\leq i\leq l$;
12: $d\leftarrow$ the degree of g_i;
13: $p(\bar{Y})\leftarrow LC(g_i)\in K[\bar{Y}]$;
14: $r\leftarrow$ the pseudo remainder of $g(\bar{Y},X)^d$ by $g_i(\bar{Y},X)$;
15: $p_1(\bar{Y}),\ldots,p_r(\bar{Y})\leftarrow$ the coefficients of r;
16: $S\leftarrow h_1(\bar{Y})=0\wedge\cdots\wedge h_t(\bar{Y})=0\wedge p(\bar{Y})\neq 0\wedge(p_1(\bar{Y})\neq 0\vee\cdots\vee p_r(\bar{Y})\neq 0)$;
17: $R\leftarrow R\vee S$;
18: $Q\leftarrow\exists X(f_1(\bar{Y},X)=0\wedge\cdots\wedge f_s(\bar{Y},X)=0\wedge p(\bar{Y})=0\wedge g(\bar{Y},X)\neq 0)$;
19: $R\leftarrow R\vee$ **GCD-QE**(Q);
20: **else**
21: $p_1(\bar{Y}),\ldots,p_r(\bar{Y})\leftarrow$ the coefficients of g;
22: $S\leftarrow(h_1(\bar{Y})=0\wedge\cdots\wedge h_t(\bar{Y})=0)\wedge p(\bar{Y})\neq 0\wedge(p_1(\bar{Y})\neq 0\vee\cdots\vee p_r(\bar{Y})\neq 0)$;
23: $R\leftarrow R\vee S$
24: **end if**
25: Return R;
26: **end if**

Algorithm 1 について:

- 各 g_i は $(K[\bar{Y}])[X]$ における多項式とみなす.
- $h_1(\bar{Y})=0\wedge\ldots\wedge h_t(\bar{Y})=0\wedge p(\bar{Y})\neq 0$ である場合, Theorem 1 から簡単に帰着させた結果から $\{g_i(\bar{Y},X)\}$ は $\langle f_1(\bar{Y},X),\ldots,f_s(\bar{Y},X)\rangle$ のグレブナ基底となる. 言い換えれば, $g_i(\bar{Y},X)$ は $f_1(\bar{Y},X),\ldots,f_s(\bar{Y},X)$ の X に関する GCD となる.
- $h_1(\bar{Y})=0\wedge\ldots\wedge h_t(\bar{Y})=0\wedge p(\bar{Y})\neq 0\wedge(p_1(\bar{Y})\neq 0\vee\ldots\vee p_r(\bar{Y})\neq 0)$ とした場合, 入力した論理式は真となる.

4 CGS-QEアルゴリズム

基本論理式 (0) が与えられたとき新しい変数を利用して最小包括的グレブナー基底系を計算すれば全ての限量子を消去できる.

Algorithm 2 CGS-QE algorithm

Input: $\exists \bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\ldots\wedge f_s(\bar{Y},\bar{X})=0\wedge g_1(\bar{Y},\bar{X})\neq 0\wedge\cdots\wedge g_t(\bar{Y},\bar{X})\neq 0)$;

Output: An equivalent quantifier free formula;

1: $\bar{Z} \leftarrow$ new variables $Z_1,\ldots,Z_t$;

2: $F \leftarrow \{f_1(\bar{Y},\bar{X}),\ldots,f_s(\bar{Y},\bar{X}),g_1(\bar{Y},\bar{X})Z_1-1,\ldots,g_t(\bar{Y},\bar{X})Z_t-1\}$;

3: $>\leftarrow$ a term order in $T(\bar{X},\bar{Z})$

4: $\mathcal{G} \leftarrow$ a minimal CGS of F w.r.t. $>$with parameters $\bar{Y}$ and main variables $\bar{X},\bar{Z}$;

5: Let $\mathcal{G}=\{(\mathcal{P}_i,G_i): i=1\ldots,k,\ldots,r,\ldots,u\}$ be indexed as follows :

- $G_1,\ldots,G_k \leftarrow$ the sets of polynomials which contains at least one polynomial including some main variable;
- $G_{k+1},\ldots,G_r \leftarrow$ the sets of polynomials which contains only non-constant polynomials consisting only of parameters;
- $G_{r+1},\ldots,G_u \leftarrow$ the sets of polynomials which consists of a non-zero constant;

6: **if** $k=u$ **then**

7: Return *true*;

8: **else**

9: $R \leftarrow false$
Let $G_i=\{h_1^i(\bar{Y}),\ldots,h_{c_i}^i(\bar{Y})\}$ for $i=k+1,\ldots,r$.
Let $\mathcal{P}_i=\mathbb{V}(\langle P_i\rangle)-\mathbb{V}(\langle Q_i\rangle)$ for $i=1,\ldots,r$ with
$P_i=\{p_1^i(\bar{Y}),\ldots,p_{a_i}^i(\bar{Y})\}$
$Q_i=\{q_1^i(\bar{Y}),\ldots,q_{b_i}^i(\bar{Y})\}$.

10: **for** $1\leq i\leq k$ **do**

11: $S \leftarrow p_1^i(\bar{Y})=0\wedge\cdots\wedge p_{a_i}^i(\bar{Y})=0\wedge(q_1^i(\bar{Y})\neq 0\vee\cdots\vee q_{b_i}^i(\bar{Y})\neq 0)$;

12: $R \leftarrow R\vee S$

13: **end for**

14: **for** $k+1\leq i\leq r$ **do**

15: $S \leftarrow q_1^i(\bar{Y})=0\wedge\cdots\wedge q_{a_i}^i(\bar{Y})=0\wedge(q_1^i(\bar{Y})\neq 0\vee\cdots\vee q_{b_i}^i(\bar{Y})\neq 0)\wedge h_1^i(\bar{Y})=0\wedge\cdots\wedge h_{c_i}^i(\bar{Y})=0$;

16: $R \leftarrow R\vee S$

17: **end for**

18: Return R;

19: **end if**

Algorithm 2 について:
Lemma4 と Hilbert's weak Nullstellensatz からこのアルゴリズムは正確である.

非等式について $g_1 \cdots g_t \neq 0$ として新しい変数を一つにすることも可能である. しかし, 我々の実験結果によれば $g_1 \cdots g_t$ を考えて大きな次数を持つ多項式を扱うよりも新しい変数の個数が多い方が計算効率がよい.

5 Hybrid-QEアルゴリズム

CGS-QE アルゴリズムで CGS を計算できれば, あとは簡単に限量子消去された論理式を計算できる. 一章で記述したように実用的な CGS 計算アルゴリズムは存在する. その中でも [9] で提案されたアルゴリズムは大体の場合において最小の分割部を持つような CGS を計算するので, CGS-QE において単純な限量子消去された論理式を出力する. まず, [9] で提案されたアルゴリズムを紹介することにする. このアルゴリズムは二つの Algorithms 3, 4 から構成されている.

Algorithm 3 CGS

Input: a finite set $F \subset K[\bar{Y}, \bar{X}]$,
a term order$>_{Y,X}$ on $T(\bar{Y}, \bar{X})$ such that $\bar{Y} \gg \bar{X}$. (Its restriction on $T(\bar{X})$ is denoted $>_X$.)
Output: a minimal CGS of F w.r.t. $>_X$ with parameters $\bar{Y}$ and main variables $\bar{X}$;
1: $G \leftarrow$ the reduced Gröbner basis of $\langle F \rangle$ w.r.t. $>_{Y,X}$ in $K[\bar{Y}, \bar{X}]$;
2: **if** $1 \in G$ **then**
3: Return $\{(\overline{K}^m, \{1\})\}$;
4: **else**
5: $\mathcal{G} \leftarrow \mathrm{CGSMain}(F, >_{Y,X})$;
6: $\mathcal{P} \leftarrow \cup\{\mathcal{P}_i : (\mathcal{P}_i, G_i) \in \mathcal{G}\}$;
7: Return $\{(\overline{K}^m \setminus \mathcal{P}, \{1\})\} \cup \mathcal{G}$
8: **end if**

Algorithm 4 CGSMain

Input: a finite set $F \subset K[\bar{Y}, \bar{X}]$,
a term order $>_{Y,X}$ on $T(\bar{Y}, \bar{X})$ such that $\bar{Y} \gg \bar{X}$. (Its restriction on $T(\bar{X})$ is denoted $>_X$.)
1: $G \leftarrow$ the reduced Gröbner basis of $\langle F \rangle$ w.r.t. $>_{Y,X}$ in $K[\bar{Y}, \bar{X}]$;
2: **if** $1 \in G$ **then**
3: Return $\emptyset$;
4: **else**
5: $\{LT(g_{n_1}), \ldots, LT(g_{n_l})\} \leftarrow$ the minimal subset of $\{LT(g_i) : g_i \in G \setminus K[\bar{Y}]\}$ concerning the order of divisibility;
6: $H_i \leftarrow \{LC(g) : LT(g) = LT(g_{n_i})$ and $g \in G \setminus K[\bar{Y}]\}$ for each $i = 1 \ldots, l$;
7: Return
$\{(\mathbb{V}(\langle G \cap K[\bar{Y}] \rangle) \setminus \cup_{i=1..l} \mathbb{V}(H_i), G \setminus \{g \in G : LT(g) \neq LT(g_{n_i})$ for each $i = 1, \ldots, l\})\} \cup$
$\mathrm{CGSMain}(F \cup H_1, >_{Y,X}) \cup \cdots \cup \mathrm{CGSMain}(F \cup H_l, >_{Y,X})$;
8: **end if**

Algorithm 3 について: Theorem 1 からこのアルゴリズムの正確性は保証される. 上記のアルゴリズムでは $\mathcal{P}_i$' が互いに素であることが保証されないが, 我々の実装では技巧的に互いに素となるような実装をしている.

このアルゴリズムは大体の場合において最小の分割部を持つ CGS を出力するが, CGS 計算がとまらない限り, CGS-QE アルゴリズムに対してその計算をブラックボックスとして扱うことはできない. [8, 5, 6, 9] で提案されたアルゴリズムは [10] で提案された Suzuki-Sato's CGS algorithm の変形である. これらのアルゴリズムはパラメトリックな空間を分割していきながら各空間に対して並列にグレブナ基底の計算を行う. 我々の計算実験によれば CGS 計算が現実的な時間でとまらないとき, 多くの場合において極僅かなグレブナ基底計算がとまらないような空間が存在してしまっていた. つまり, 大半の CGSMain の stage 7 における再帰的呼び出しはとまるが, 極僅かとまらない呼び出しが存在する. 限量子消去において, 実際には CGS は必要ない. 分割された空間においてグレブナ基底計算が現実的な時間でとまらない場合, 分割されたパラメトリックな空間に対応するような条件を入力論理式に付け加えた論理式を考えればよい. この単純なアイデアは劇的な QE アルゴリズムの改良を与える. 以下が GCD-QE と CGS-QE を連結した我々の新しいアルゴリズム Hybrid-QE である.

Algorithm 5 Hybrid-QE algorithm

Input: $\exists \bar{X}(f_1(\bar{Y},\bar{X})=0\wedge\ldots\wedge f_s(\bar{Y},\bar{X})=0\wedge g_1(\bar{Y},\bar{X})\neq 0\wedge\cdots\wedge g_t(\bar{Y},\bar{X})\neq 0)$;

Output: An equivalent quantifier free formula;

1: $\bar{Z} \leftarrow$ new variables $Z_1,\ldots,Z_t$;
2: $F \leftarrow \{f_1(\bar{Y},\bar{X}),\ldots,f_s(\bar{Y},\bar{X}),g_1(\bar{Y},\bar{X})Z_1-1,\ldots,g_t(\bar{Y},\bar{X})Z_t-1\}$;
3: Apply the minimal CGS computation algorithm to F with parameters $\bar{Y}$ and main variables $\bar{X},\bar{Z}$;
4: **if** the computation terminates at stage 3 **then**
5: Return false;
6: **else**
7: For $\mathcal{G}=\{(\mathbb{V}(\langle G\cap K[\bar{Y}]\rangle)\setminus\cup_{i=1..l}\mathbb{V}(H_i), G\setminus\{g\in G : LT(g)\neq LT(g_{n_i}) \text{ for each } i=1,\ldots,l\})\}$ obtained at the stage 7 of CGSMain, proceed the stage 5 of CGS-QE algorithm. {Let this output be ϕ.}
8: **end if**
9: For each $i=1\ldots,l$
10: $\theta_i \leftarrow \wedge_{h(\bar{Y})\in H_i} h(\bar{Y})=0$;
$\psi_i \leftarrow \exists\bar{X}(\theta_i\wedge f_1(\bar{Y},\bar{X})=0\wedge\ldots\wedge f_s(\bar{Y},\bar{X})=0\wedge g_1(\bar{Y},\bar{X})\ldots g_t(\bar{Y},\bar{X})\neq 0)$;
11: Proceed CGSMain$(F\cup H_i,>_{Y,X})$ and GCD-QE(ψ_i) in parallel;
12: **if** CGSMain$(F\cup H_i,>_{Y,X})$ terminates in first **then**
13: $\mathcal{G} \leftarrow$ CGSMain$(F\cup H_i,>_{Y,X})$;
Proceed the stage 5 of CGS-QE algorithm to $\mathcal{G}$;
Let this output be ϕ_i;
14: **else**
15: $\phi_i \leftarrow$ GCD-QE(ψ_i);
16: **end if**
17: Return $\phi\vee\phi_1\vee\cdots\vee\phi_l$;

6 計算実験

Risa/Asir にこれまでの章のすべての QE アルゴリズムを実装した. 並列計算のために Risa/Asir の OpenXM 環境を利用した. 本章では我々の Hybrid-QE の有効性を確認するために行った計算実験について報告する. 多くの例を Maple の Projection, Mathematica の Reduce, Resolve と一緒に我々の実装も使うことで確認した. この章のすべての計算データは CPU Intel(R) Core(TM) i7-3632QM, Memory 8GB, OS Ubuntu12.10 の PC から得られた.

我々の目的は早く出力するようなアルゴリズムを構築することではなく, 単純な出力を現実的な時間で出力するようなアルゴリズムを構築することである. しかしながら, 我々の新しいアルゴリズムは期待以上に早く出力するようなアルゴリズムとなった. 百以上の例が我々の GCD-QE プログラム, CGS-QE プログラム, Mathematica の Reduce, Resolve, Maple の Projection では一時間ではとまらなかったが, Hybrid-QE プログラムでは数分でとまった.

以下はそうした例の一つである.

$$\exists(X,Y)((AX+BY)^{26}-1=0 \wedge (AXY+BX+CY)^{26}-B=0 \wedge AX+BY\neq 0)$$

Hybrid-QE プログラムでは 139.7 秒でとまったが, 他のプログラムでは一時間ではとまらなかった.

24 例が GCD-QE プログラム, CGS-QE プログラム, Mathematica の Reduce, Resolve では一時間で止まらなかったが, Maple の Projection と Hybrid-QE プログラムでは数分で止まった.

次の例はそうした例の一つでどちらのプログラムでも数秒でとまるような例である.

$$\exists(X,Y,Z)\in\mathbb{C}^3(AXZ+BX-1=0 \wedge (BX+CY)^{14}-1=0 \wedge AX+BZ\neq 0) \tag{2}$$

Maple の Projection の出力:

$$(ABC\neq 0)\vee(C(A^2+B^3)\neq 0)\vee(C=0\wedge AB(A^{12}+7A^4B^{12}-14A^2B^{15}+7B^{18})\neq 0)\vee(C=0\wedge AB(A^{12}-2A^{10}B^3+4A^8B^6-8A^6B^9+9A^4B^{12}-4A^2B^{15}+B^{18})\neq 0)\vee(C=0\wedge AB(A^2+2B^3)\neq 0)\vee(C=0\wedge AB\neq 0)\vee(A=0\wedge C=0\wedge B\neq 0)\vee(A^{12}-2A^{10}B^3+4A^8B^6-8A^6B^9+9A^4B^{12}-4A^2B^{15}+B^{18}=0\wedge C=0\wedge AB(47A^{10}-284A^8B^3+568A^6B^6-519A^4B^9+214A^2B^{12}-47B^{15})(94A^{10}+117A^8B^3-783A^6B^6+1017A^4B^9-468A^2B^{12}+117B^{15})(3844755A^{10}-9231137A^8B^3+7214722\,A^6B^6-403976A^4B^9-832313A^2B^{12}+474788B^{15})\neq 0)\vee(A^{12}+7A^4B^{12}-14A^2B^{15}+7B^{18}=0\wedge C=0\wedge AB(42701A^{10}-346432A^8B^3+896904A^6B^6-1411539A^4B^9+1193297A^2B^{12}-396739B^{15})(69310A^{10}-221942A^8B^3+412158A^6B^6-411014\,A^4B^9+176253A^2B^{12}-17157B^{15})(2186507864386A^{10}-27064\,46731217A^8B^3-61230596433A^6B^6+10476412105940A^4B^9-16403396742588A^2B^{12}+7291066799632B^{15})\neq 0)$$

Hybrid-QE プログラムの出力:

$$(C=0\wedge AB\neq 0)\vee(B=0\wedge AC\neq 0)\vee(A=0\wedge C=0\wedge B\neq 0)\vee(A=0\wedge BC\neq 0)\vee(ABC\neq 0)$$

見ての通り, Hybrid-QE の出力の方が単純であることがわかる.
次の表は Hybrid-QE プログラムと Maple の Projection でとまった 24 例について分割部の個数を比較している. 分割部の個数が単純な論理式の尺度になるわけではないが, 少なからず指標にはなる. そして, 表の通り, 明らかに Hybrid-QE プログラムの方が優れていることがわかる.

Number of output segments

program	minimum	maximum	average
Projection	3	454	34.3333
Hybrid-QE	3	15	6.95833

7 結論

Hybrid-QE には GCD-QE の一変数消去に着目した並列性と CGS 計算における並列性がある. 今回の実装及び実験ではそうした並列性には着目していない. こうした並列性に着目した実装及び実験は今後の課題である.

また、Hybrid-QE において GCD-QE のかわりに CS-QE を利用することも可能である. これの実装及び実験も今後の課題である.

参考文献

[1] A computer algebra system Risa/Asir. http://www.math.kobe-u.ac.jp/Asir/asir.html

[2] Fortuna,E., Gianni,P. and Trager,B. (2001). Degree reduction under specialization. J. Pure Appl. Algebra, 164, pp. 153-164, 2001.

[3] Harrison,J. Complex Quantifier Elimination in HOL.(2001). In Richard J. Boulton and Paul B.Jackson,editors,TPHOLs Supplemental Proceedings, pages 159—174. Division of Informatics, University of Edinburgh, 2001. Published as Informatics Report Series EDI-INF-RR-0046. Available on the Web at http://www.informatics.ed.ac.uk/publications/report/0046.html.

[4] Kalkbrener, M. On the Stability of Gröbner Bases Under Specializations. *J. Symbolic Computation.* Vol. 24/1, pp. 51–58. 1997.

[5] Kapur, D., Sun, Y., and Wang, D. (2010). A New Algorithm for Computing Comprehensive Gröbner Systems. In International Symposium on Symbolic and Algebraic Computation, pp. 29-36. ACM-Press, 2010.

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

[7] Mathematica Tutorial: tutorial/ComplexPolynomialSystems

[8] Nabeshima, K. (2007). A Speed-Up of the Algorithm for Computing Comprehensive Gröbner Systems. International Symposium on Symbolic and Algebraic Computation, pp. 299-306. ACM-Press, 2007.

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

[10] Suzuki,A. and Sato,Y. (2006). A Simple Algorithm to Compute Comprehensive Grbner Bases Using Gröbner Bases. International Symposium on Symbolic and Algebraic Computation, pp. 326-331. ACM-Press, 2006.

[11] Gao, X., Wang, D., 2003. Zero decomposition theorems for counting the number of solutions for parametric equation systems. In: Proc. ASCM 2003. pp. 129-144

[12] Wang, D.,2004. The projection property of regular systems and its application to solving parametric polynomial systems. In: Dolzmann, A., Seidl, A., Sturm, T. (Eds.), Algorithmic Algebra and Logic. Herstellung und Verlag, Norderstedt, pp. 269-274.

[13] Chen, C., Golubitsky, O., Lemaire, F., Moreno Maza, M., Pan, W., 2007. Comprehensive Triangular Decomposition. Vol. 4770 of LNCS. Springer Verlag, pp. 73-101.