数理解析研究所講究録
第1955巻 2015年 134-141

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

深作 亮也
RYOYA FUKASAKU
東京理科大学
TOKYO UNIVERSITY OF SCIENCE *
岩根 秀直
HIDENAO IWANE
国立情報学研究所 / (株) 富士通研究所
NATIONAL INSTITUTE OF INFORMATICS / FUJITSU LABORATORIES LTD. †
佐藤 洋祐
YOSUKE SATO
東京理科大学
TOKYO UNIVERSITY OF SCIENCE ‡

Abstract

Our aim is to construct an efficient real quantifier elimination algorithm in the case the input formula contains many equality constraints. In this paper, we improve a real quantifier elimination method based on the theory of real root counting and the computation of comprehensive Gröbner systems introduced by V.Weispfenning. According to our computation experiments, our program is superior to other existing implementations for many examples which contain many equalities.

1 はじめに

等式制約に特化したCylindrical Algebraic Decomposition(CAD)計算による限量子消去アルゴリズム研究として[2, 3]や[1]が挙げられる. これらはCAD計算による限量子消去として一定の成果を残したものの本稿の6章で示されるように計算のとまらない限量子消去問題が存在する.

本研究の目的は等式制約の多い一階述語論理式に対して高速な限量子消去アルゴリズムを構築することであり, 本稿ではV.Weispfenningによって提案された実根個数計算([4])と包括的グレブナー基底系([5])による限量子消去アルゴリズム([6])を改良する.

*1414704@ed.tus.ac.jp
†iwane@nii.ac.jp / iwane@jp.fujitsu.com
‡ysato@rs.kagu.tus.ac.jp

V.Weispfenning による限量子消去アルゴリズムは包括的グレブナー基底系によって暗に含まれた等式制約 (つまり, 等式制約によるイデアルに属する多項式) を利用することができる. 従って, 等式制約の多い一階述語論理式に対し, 効率的な限量子消去アルゴリズムとなる. しかしながら, 入力の $>$ や $\neq$ を表面的にしか利用しないため, 本質的に必要な等式制約を利用することができない. 我々は $h > 0 \Leftrightarrow \exists z\ z^2 h = 1$ 等の事実に着目する. これにより不要な等式制約を排除し, V.Weispfenning によるオリジナルアルゴリズムを改良する.

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章では我々の改良アルゴリズムに関する理論を示し, 5章で我々のアルゴリズムを示す. 6章では我々の実験結果を通して, 我々のアルゴリズムの効率性を示す.

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 [4] の主定理の部分的な結果である.

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
$\mathbb{R}^{n_v}$ 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 $\mathbb{R}^{n_v}$ の分割とよばれる :

1. $\cup_{i=1}^{s} \mathcal{S}_i = \mathbb{R}^{n_v}$.
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 $\mathbb{R}^{n_v}$ 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. $r(\bar{x}) \neq 0 \Leftrightarrow 1 - z_r\, r(\bar{x}) = 0$.

我々の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 6
基本形 (1) は以下と等価である :

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

定理 6 は新しい変数を導入するが, 以下より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わかる.

定理 7

$p_1,\ldots,p_{m_p},q_1,\ldots,q_{m_q},r_1,\ldots,r_{m_r}\in\mathbb{R}[\bar{x}]$ 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.

さらに以下は我々のアルゴリズムがオリジナルアルゴリズムを改良したことを示している.

系 8

$p_1,\ldots,p_{m_p},r_1,\ldots,r_{m_r}\in\mathbb{R}[\bar{x}]$ 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 7 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.

最後に上記補題について $dim(\mathbb{R}[\bar{x},\bar{z}]/J)<2^{m_p}\cdot dim(\mathbb{R}[\bar{x}]/I)$ となる場合について考える. 以下は飽和イデアルを考えることで示される.

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 7 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 $dim(\mathbb{R}[\bar{x},\bar{z}]/J)<2^{m_p}\cdot dim(\mathbb{R}[\bar{x}]/I)$ は以下と等価となる.

$$\exists p_{i_p}(A_I\text{上で積の逆元をもたない.})\vee\exists q_{i_q}(A_I\text{上で積の逆元をもたない.}).$$

5 アルゴリズム

本章では我々のアルゴリズムを示す. まずはトップ関数となるアルゴリズム **MainQE** を示す. 以下のように等式制約が零次元イデアルになる場合とならない場合の処理は異なる.

以下は等式制約が零次元イデアルになる場合の処理である.

Algorithm 1 MainQE

Input: $\phi \equiv \exists \bar{x}((\bigwedge_{i_f} f_{i_f} = 0) \wedge (\bigwedge_{i_p} p_{i_p} \neq 0) \wedge (\bigwedge_{i_q} q_{i_q} > 0) \wedge (\bigwedge_{i_r} r_{i_r} \geq 0))$

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

$\mathcal{G} \leftarrow$ a CGS of $\langle f_{i_f} : i_f \rangle$ (main variables $\bar{x}$, parameters $\bar{y}$); $\psi \leftarrow false$;
while $\mathcal{G} \neq \emptyset$ **do**
  $(\mathcal{S}, G) \leftarrow$ the element of $\mathcal{G}$; $\mathcal{G} \leftarrow \mathcal{G} \setminus \{(\mathcal{S}, G)\}$;
  if $\langle G(\bar{c}, \bar{x}) \rangle$ is zero dimensional for $\bar{c} \in \mathcal{S}$ **then**
    $\psi \leftarrow \psi \vee$ **ZeroDimQE**$(\phi, \mathcal{S}, G)$;
  else
    $\psi \leftarrow \psi \vee$ **NonZeroDimQE**$(\phi, \mathcal{S}, G)$;
  end if
end while
Return ψ;

Algorithm 2 ZeroDimQE

Input: $\phi, \mathcal{S}, G$ $\{\phi \equiv \exists \bar{x}((\bigwedge_{i_f} f_{i_f} = 0) \wedge (\bigwedge_{i_p} p_{i_p} \neq 0) \wedge (\bigwedge_{i_q} q_{i_q} > 0) \wedge (\bigwedge_{i_r} r_{i_r} \geq 0)).\}$

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

1: $H \leftarrow G \cup \{1 - z_{i_p} p_{i_p} : i_p\} \cup \{1 - z_{i_q}^2 q_{i_q} : i_q\} \cup \{z_{i_r}^2 - r_{i_r} : i_r\}$;
2: $\mathcal{G}' \leftarrow$ a CGS of $\langle H \rangle$ (main variables $\bar{x}, \bar{z}$, parameters $\bar{y}$); $\psi \leftarrow false$;
3: **while** $\mathcal{G}' \neq \emptyset$ **do**
4: $(\mathcal{S}', G') \leftarrow$the element of $\mathcal{G}'$; $\mathcal{G}' \leftarrow \mathcal{G}' \setminus \{(\mathcal{S}', G')\}$;
5: $V \leftarrow$a basis $(v_1, \ldots, v_d)$ of $A_{G'}$; $\{A_{G'} = \mathbb{R}[\bar{x}, \bar{z}] / \langle G'(\bar{c}, \bar{x}, \bar{z}) \rangle$ for $\bar{c} \in \mathcal{S}'.\}$
6: **for** $1 \leq i, j \leq d$ **do**
7: $M_{ij} \leftarrow$ the trace of the linear map $A_{G'} \to A_{G'}; a \mapsto a v_i v_j$;
8: **end for**
9: $\psi \leftarrow \psi \vee (\mathcal{S}' \wedge$ " the formula such that the signature of $(M_{ij})_{ij}$ is not equal zero");
10: **end while**
11: Return ψ;

最後に等式制約が零次元イデアルにならないような場合に関する処理を示す. 等式制約が零次元イデアルにならないような場合は限量子変数の一部 (極大従属変数たち) を自由変数として再帰的な限量子消去がなされる. また, 我々は別の限量子消去アルゴリズム **OtherQE** を適用する箇所がある. オリジナルアルゴリズムではこうしたことはされず, 論理式の変換によって実根個数計算と包括的グレブナー基底系によって限量子消去をする. しかしながら, この変換によって計算効率が下がることが多いため, 別の限量子消去アルゴリズム **OtherQE** を適用することにした. 我々の実装においては以下コメント文のように SyNRAC を利用している.

Algorithm 3 NonZeroDimQE

Input: $\phi, \mathcal{S}, G$ $\{\phi \equiv \exists \bar{x}((\bigwedge_{i_f} f_{i_f}=0) \wedge (\bigwedge_{i_p} p_{i_p} \neq 0) \wedge (\bigwedge_{i_q} q_{i_q} > 0) \wedge (\bigwedge_{i_r} r_{i_r} \geq 0)).\}$

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

1: $\bar{m} \leftarrow$ a maximal independent set of $\langle G(\bar{c}, \bar{x}) \rangle$ for $\bar{c} \in \mathcal{P}$;
2: $\bar{x}' \leftarrow \bar{x} \setminus \bar{m}$; $\bar{y}' \leftarrow \bar{y} \cup \bar{m}$;
3: **if** $\bar{x}' = \bar{x}$ **then**
4: Return **OtherQE**$(\mathcal{S} \wedge \phi)$; {We use SyNRAC on Maple.}
5: **else**
6: $\phi' \leftarrow \exists \bar{x}'(\mathcal{S}' \wedge \bigwedge_{g \in G'} g=0 \wedge \bigwedge_{i_p=1}^{m_p} p_{i_p} > 0 \wedge \bigwedge_{i_q=1}^{m_q} q_{i_q} \geq 0 \wedge \bigwedge_{i_r=1}^{m_r} r_{i_r} \neq 0)$;
7: **while** the equations of ϕ' contains $\bar{x}$ **do**
8: $\phi' \leftarrow$ **MainQE**(ϕ');
9: **end while**
10: Return **OtherQE**(ϕ'); {We use SyNRAC on Maple.}
11: **end if**

これらアルゴリズムの正確性は前章までの内容から示される. さらに停止性は前章までの内容と極大従属変数が束縛変数の一部であることから従う.

6 ベンチマーク

本章で我々のベンチマークの一部を示す. **Example 1** は [6] のベンチマークであり, **Example 2** - **Example 4** は [1] のベンチマークである.

Example 1

$\forall x \forall y(b^2(x-c)^2 + a^2y^2 = a^2b^2 \Rightarrow x^2 + y^2 \leq 1)$

Example 2

$\exists x \exists y \exists z((1/200)xs(1-(1/400)x) + ys(1-(1/400)x) - (35/2)x = 0 \wedge 250xs(1-(1/600)y)(z+(3/250)) - (55/2)y = 0 \wedge 500(y+(1/20)x)(1-(1/700)z) - 5z = 0)$

Example 3

$\exists c_2 \exists s_2 \exists c_1 \exists s_1(r - c_1 + l(s_1s_2 - c_1c_2) = 0 \wedge z - s_1 - l(s_1c_2 + s_2c_1) = 0 \wedge s_1^2 + c_1^2 - 1 = 0 \wedge s_2^2 + c_2^2 - 1 = 0)$

Example 4

$\exists y \exists z(x^2 + y^2z + z^3 = 0 \wedge 3x^2 + 3y^2 + z^2 - 1 = 0 \wedge x^2 + z^2 - y^3(y-1)^3 < 0)$

Example 5

$\exists x \exists y \exists z(xy + axz + yz - 1 = 0 \wedge xyz + xz + xy = a \wedge xz + yz - az - x - y - 1 = 0 \wedge axy = byz \wedge ayz = bzx)$

Example 6

$\exists x \exists y \exists z(xy + axz + yz - 1 = 0 \wedge xyz + xz + xy + b = 0 \wedge xz + yz - az - x - y - 1 = 0)$

Example 7

$\exists x0 \exists x2 \exists x3(x_0 + 2x_2 \neq 5 \wedge x_0x_2 - 1 = 0 \wedge x_0^2 - 2x_0x_1 + x_2^2 - 2x_2x_3 - x_4 = 0 \wedge -16x_1x_4^2 - 800x_3^3 - 1240x_3^2x_4 - 408x_3x_4^2 - 40x_4^3 + 240x_1x_3 - 532x_1x_4 - 17720x_3^2 - 6214x_3x_4 - 550x_4^2 - 4480x_1 + 25240x_3 + 5695x_4 + 1050 = 0 \wedge 32x_1^2 + 168x_1x_3 + 40x_1x_4 + 8x_3^2 + 20x_3x_4 + 4x_4^2 - 270x_1 - 390x_3 - 105x_4 + 450 = 0 \wedge 320x_1x_3x_4 + 32x_1x_4^2 + 16x_3x_4^2 + 8320x_1x_3 + 264x_1x_4 + 240x_3^2 - 372x_3x_4 - 140x_4^2 - 14840x_1 - 23380x_3 - 2575x_4 + 36750 = 0)$

Example 8

$$\exists x_0\exists x_1\exists x_2\exists x_3\exists x_4\exists x_5\exists x_6\exists x_7(x_2\neq 0\wedge x_3\neq 0\wedge x_4=0\wedge x_5=0\wedge x_2-x_3\neq 0\wedge x_0x_8+x_1x_9-1=0\wedge 2x_0x_2+2x_1x_3+2x_4x_5-x_0-x_1-x_4=0\wedge x_0x_6+x_0x_7-x_1x_7-x_4x_6-x_0+x_8=0\wedge x_2x_6+x_2x_7-x_3x_7-x_5x_6-x_2+x_9=0\wedge 2x_0x_2-2x_0x_4+2x_1x_3-2x_1x_5-x_2^2-x_3^2+x_4^2+x_5^2=0\wedge x_0^2+x_1^2-x_2^2-x_3^2+x_4^2-x_5^2+x_2+x_3+x_5=0\wedge 14x_9^3+2x_8^2-12x_8x_9-16x_9^2+4x_8+17x_9-10=0\wedge 14x_8x_9^2-3x_8^2-10x_8x_9-11x_9^2+x_8+20x_9-6=0\wedge 14x_8^2x_9-6x_8^2-20x_8x_9+20x_9^2+16x_8-9x_9+2=0\wedge 14x_8^3-19x_8^2+58x_8x_9+5x_9^2-17x_8-32x_9+46=0)$$

Example 9

$$\exists x_0\exists x_2\exists x_5\exists x_3\exists x_1\exists x_4((\exists x_{10}\exists x_9(0=(x_5-x_0)(1/2x_0+1/2x_5-x_{10})+(x_3-x_2)(1/2x_2+1/2x_3-x_9)\wedge 0=(x_1-x_5)(1/2x_5+1/2x_1-x_{10})+(x_4-x_3)(1/2x_3+1/2x_4-x_9)\wedge((x_{10}-x_0)^2+(x_9-x_2)^2)^{1/2}=1\wedge 0<((x_{10}-x_0)^2+(x_9-x_2)^2)^{1/2}))\wedge(0\leq x_0x_3-x_0x_4+x_1x_2-x_1x_3-x_2x_5+x_4x_5\wedge 0\leq(x_5-x_0)(x_4-x_2)-(x_3-x_2)(x_1-x_0))\wedge 3\leq|x_0x_3-x_0x_4+x_1x_2-x_1x_3-x_2x_5+x_4x_5|/((x_1-x_0)(x_5-x_0)+(x_4-x_2)(x_3-x_2))\wedge 3\leq|x_0x_3-x_0x_4+x_1x_2-x_1x_3-x_2x_5+x_4x_5|/((x_0-x_5)(x_1-x_5)+(x_2-x_3)(x_4-x_3))\wedge x_8=|x_0x_3-x_0x_4+x_1x_2-x_1x_3-x_2x_5+x_4x_5|/((x_1-x_0)(x_5-x_0)+(x_4-x_2)(x_3-x_2))\wedge x_7=|x_0x_3-x_0x_4+x_1x_2-x_1x_3-x_2x_5+x_4x_5|/((x_0-x_5)(x_1-x_5)+(x_2-x_3)(x_4-x_3))\wedge x_6=1/2|(x_5-x_0)(x_4-x_2)-(x_3-x_2)(x_1-x_0)|)$$

Example 10

$$\exists x_0\exists x_1\exists x_7(x_5x_7-x_6x_7+x_1-x_5=0\wedge x_0^2+x_1^2-1=0\wedge x_3^4x_7^2-4x_3^3x_4x_7^2+6x_3^2x_4^2x_7^2+2x_3^2x_5^2x_7^2-4x_3^2x_5x_6x_7^2+2x_3^2x_6^2x_7^2-4x_3x_4^3x_7^2-4x_3x_4x_5^2x_7^2+8x_3x_4x_5x_6x_7^2-4x_3x_4x_6^2x_7^2+x_4^4x_7^2+2x_4^2x_5^2x_7^2-4x_4^2x_5x_6x_7^2+2x_4^2x_6^2x_7^2+x_5^4x_7^2-4x_5^3x_6x_7^2+6x_5^2x_6^2x_7^2-4x_5x_6^3x_7^2+x_6^4x_7^2+2x_0x_3^3x_7-6x_0x_3^2x_4x_7+6x_0x_3x_4^2x_7+2x_0x_3x_5^2x_7-4x_0x_3x_5x_6x_7+2x_0x_3x_6^2x_7-2x_0x_4^3x_7-2x_0x_4x_5^2x_7+4x_0x_4x_5x_6x_7-2x_0x_4x_6^2x_7+2x_1x_3^2x_5x_7-2x_1x_3^2x_6x_7-4x_1x_3x_4x_5x_7+4x_1x_3x_4\ x_6x_7+2x_1x_4^2x_5x_7-2x_1x_4^2x_6x_7+2x_1x_5^3x_7-6x_1x_5^2x_6x_7+6x_1x_5x_6^2x_7-2x_1x_6^3x_7-2x_3^4x_7+6x_3^3x_4x_7-6x_3^2x_4^2x_7-4x_3^2x_5^2x_7+6x_3^2x_5x_6x_7-2x_3^2x_6^2x_7+2x_3x_4^3x_7+6x_3x_4x_5^2x_7-8x_3x_4x_5x_6x_7+2x_3x_4x_6^2x_7-2x_4^2x_5^2x_7+2x_4^2x_5x_6x_7-2x_5^4x_7+6x_5^3x_6x_7-6x_5^2x_6^2x_7+2x_5x_6^3x_7+x_0^2x_3^2-2x_0^2x_3x_4+x_0^2x_4^2+2x_0x_1x_3x_5-2x_0x_1x_3x_6-2x_0x_1x_4x_5+2x_0x_1x_4x_6-2x_0x_3^3+4x_0x_3^2x_4-2x_0x_3x_4^2-2x_0x_3x_5^2+2x_0x_3x_5x_6+2x_0x_4x_5^2-2x_0x_4x_5x_6+x_1^2x_5^2-2x_1^2x_5x_6+x_1^2x_6^2-2x_1x_3^2x_5+2x_1x_3^2x_6+2x_1x_3x_4x_5-2x_1x_3x_4x_6-2x_1x_5^3+4x_1x_5^2x_6-2x_1x_5x_6^2+x_3^4-2x_3^3x_4+x_3^2x_4^2+2x_3^2x_5^2-2x_3^2x_5x_6-x_3^2x_6^2-2x_3x_4x_5^2+2x_3x_4x_5x_6+2x_3x_4x_6^2-x_4^2x_6^2+x_5^4-2x_5^3x_6+x_5^2x_6^2-x_5^2x_6^2+2x_5x_6x_6^2-x_6^2x_6^2=0)$$

以下表は計算時間であり, 単位は秒である. >1h は 1 時間計算しても計算がとまらなかったもの, er はエラーを出力したものである. さらに mem はメモリが使い果たされたために計算をあきらめている. また, **Our** は我々の実装, **SyN** は SyNRAC, **Reg** は maple の RegularChain パッケージ, **Res** は mathematica の Resolve, **Red** は mathematica の Reduce, **QC** は qepcad, **rdlg** は Reduce の RedLog パッケージの rlhqe である.

表 1: Computation Time

	Our	**SyN**	**Reg**	**Res**	**Red**	**QC**	**rdlg**
1	2	2	298	0	1	2	>1h
2	1	>1h	4	0	30	er	>1h
3	1	1	29	0	>1h	>1h	0
4	1	1	1	0	0	er	95
5	0	er	>1h	250	>1h	>1h	er
6	10	>1h	>1h	>1h	>1h	mem	>1h
7	2	er	>1h	586	587	>1h	420
8	1	>1h	mem	>1h	>1h	>1h	>1h
9	791	>1h	>1h	>1h	>1h	er	>1h
10	83	>1h	>1h	>1h	>1h	>1h	>1h

7 まとめ

前章の通り, 我々は等式制約の多い入力に対して, 効率的なアルゴリズム (プログラム) を構築することができた. しかしながら, CAD に比べて出力が複雑となる場合があった. 今後はこれを改善したい.

参 考 文 献

[1] Chen, C. and Maza, M, M. : Quantifier Elimination by Cylindrical Algebraic Decomposition Based on Regular Chains. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.91-98, ACM, 2014.

[2] McCallum, S. : On Projection in CAD-Based Quantifier Elimination with Equational Constraint. Proceedings of the International Symposium on Symbolic and Algebraic Computation, pp.145-149, ACM,1999.

[3] McCallum, S. : On Propagation of Equational Constraints in CAD-Based Quantifier Elimination. Proceedings of the International Symposium on Symbolic and Algebraic Computation, pp.223-231, ACM,2001.

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

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

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