数理解析研究所講究録
第2019巻 2017年 113-123

飽和イデアル計算なしのCGS-QE
CGS-QE without saturation ideal computations

深作 亮也
Ryoya Fukasaku
東京理科大学
Tokyo University of Science *

岩根 秀直
Hidenao Iwane
(株)富士通研究所/国立情報学研究所
Fujitsu Laboratories Ltd/National Institute of Informatics †

佐藤 洋祐
Yosuke Sato
東京理科大学
Tokyo University of Science ‡

1 はじめに

[2] で示された Cylindrical Algebraic Decomposition (CAD) を利用する限量子消去 (Quantifier Elimination; QE) アルゴリズム (CAD-QE) は QE 手法の中で最も盛んに研究され, 多くの改良が達成されてきた. 実際に, [8], [18], [9] や [1] 等では様々な改良がなされている. しかし, 入力に等式制約が多い場合に不要な計算を行ってしまう傾向を持つ. そうした不要な計算なしで QE を行うため, [21] でパラメータ付きイデアル操作を行う QE アルゴリズムが示された. パラメータ付きイデアル操作を包括的グレブナー基底系 (Comprehensive Gröbner System; CGS) によって行うので, 本稿では CGS-QE と呼ぶこととする.

CGS-QE は著者らにより [4], [5] 等で改良されたが, 本稿では [4] に着目する. [4] は飽和イデアルを計算することで "[21] で扱われる (後述するような) 対称行列よりも簡略な対称行列を扱う" ような改善をし, CGS-QE 内部で起こる再帰計算出力論理式を簡略化することで, 計算量を改善した. しかし, 一般に飽和イデアルの計算は重い. また, パラメータ付き飽和イデアルの性質はパラメータの値に依存して変化し, あるパラメータの値では考えるイデアル自身が飽和イデアルと等価となり, 飽和イデアル計算自体が不要となるような場合もある. 本稿では, そうした不要なパラメータ付き飽和イデアルの計算を排除する.

*fukasaku@rs.tus.ac.jp
†iwane@jp.fujitsu.com
‡ysato@rs.tus.ac.jp

本稿は次の通りに構成される. まず, **2 節**で本稿の主定理 (考えるイデアル自身が飽和イデアルと等価となるための必要十分条件に関する定理) を示す. **3 節**では CGS-QE アルゴリズムを構成するために必要な (既知である) 多変数実根個数計算定理に関する理論を示し, **4 節**では CGS の定義を示す. そして, **5 節**では改良された CGS-QE アルゴリズムを示す. 本稿の最後では我々の実験データの一部を示す.

2 主定理

K を計算可能な体, C をその代数閉包とする. 更に, $\bar{X}$ を $X_1, \ldots, X_n$ とし, $K[\bar{X}]$ を係数体 K 上多項式環とする. 本節では, 零次元イデアル $I \subset K[\bar{X}]$ と多項式 $h \in K[\bar{X}]$ を考え, 飽和イデアル $I : h^\infty$ が $I : h^\infty = I$ となる必要十分条件を示す. まず, 本節で利用する記号を定義する.

表記 1
剰余環 $A = K[\bar{X}]/I$ の基底を $\{v_1, \ldots, v_d\}$ とする. ここで, 多項式 $r \in K[\bar{X}]$ に対し, 写像 $m_r : A \to A\ ;\ a \mapsto a \cdot r$ を考える. m_r は線形写像であることに注意して, そのトレースを $\mathrm{trace}(m_r)$ で記述する. 更に, (i, j) 成分が $\mathrm{trace}(m_{h \cdot v_i\, v_j})$ となるような対称行列 M_h^I を考える. また, C における I の多様体 $\mathbb{V}_C(I) = \{\bar{c}_1, \ldots, \bar{c}_l\}$ とし, 各 $\bar{c}_i$ の重複度を μ_i とする. ここで, 一般には $l \leq d = \sum_{1 \leq i \leq l} \mu_i$ であるが, I が根基イデアルであるときに限って $l = d$ となることに注意する.

このとき, 以下の構造を持つことがわかる.

補題 2
M_h^I は以下のような構造を持つ.

$$M_h^I = \sum_{1 \leq i \leq l} \mu_i \cdot h(\bar{c}_i) \begin{pmatrix} v_1(\bar{c}_i) \cdot v_1(\bar{c}_i) & \ldots & v_1(\bar{c}_i) \cdot v_d(\bar{c}_i) \\ \vdots & \ddots & \vdots \\ v_1(\bar{c}_i) \cdot v_d(\bar{c}_i) & \ldots & v_d(\bar{c}_i) \cdot v_d(\bar{c}_i) \end{pmatrix}.$$

証明
m_h の固有値全体は μ_1 個の $h(\bar{c}_1), \ldots,$ μ_l 個の $h(\bar{c}_l)$ で構成されることから従う.

更に以下のような行列たちを考えることとする. 以下では転置行列を ^{t} の左付き添字で表現する.

表記 3
Δ_μ, Δ_h, Γ を以下のように定義する. ここで, **補題 2** より $M_h^I = {}^t\Gamma \cdot \Delta_\mu \cdot \Delta_h \cdot \Gamma$ に注意する.

$$\Gamma = \begin{pmatrix} v_1(\bar{c}_1) & \ldots & \ldots & v_d(\bar{c}_1) \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ v_1(\bar{c}_l) & \ldots & \ldots & v_d(\bar{c}_l) \end{pmatrix}, \Delta_\mu = \begin{pmatrix} \mu_1 & 0 & \ldots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & \mu_l \end{pmatrix}, \Delta_h = \begin{pmatrix} h(\bar{c}_1) & 0 & \ldots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & h(\bar{c}_l) \end{pmatrix}.$$

更に, $1 \leq k_1 < \ldots < k_l \leq d$ に対して, $M_h^I(k_1, \ldots, k_l)$ を $k_1, \ldots, k_l$ 行と $k_1, \ldots, k_l$ 列から構成される M_h^I の l 次主小行列, $\Gamma(k_1, \ldots, k_l)$ を $k_1, \ldots, k_l$ 行と $k_1, \ldots, k_l$ 列から構成される Γ の l 次主小行列 とする.

上記を利用することで, 次の構造を知ることができる.

補題 4
$1 \leq k_1 < \ldots < k_l \leq d$ に対して,

$$M_h^I(k_1, \ldots, k_l) = {}^t\Gamma(k_1, \ldots, k_l) \cdot \Delta_\mu \cdot \Delta_h \cdot \Gamma(k_1, \ldots, k_l).$$

証明
補題 2 より $M_h^I(k_1, \ldots, k_l)$ は以下の構造を持つため, 主張を満足する.

$$\sum_{1 \leq i \leq l} \mu_i \cdot h(\bar{c}_i) \begin{pmatrix} v_{k_1}(\bar{c}_i) \cdot v_{k_1}(\bar{c}_i) & \ldots & v_{k_1}(\bar{c}_i) \cdot v_{k_l}(\bar{c}_i) \\ \vdots & \ddots & \vdots \\ v_{k_1}(\bar{c}_i) \cdot v_{k_l}(\bar{c}_i) & \ldots & v_{k_l}(\bar{c}_i) \cdot v_{k_l}(\bar{c}_i) \end{pmatrix} = {}^t\Gamma(k_1, \ldots, k_l) \cdot \Delta_\mu \cdot \Delta_h \cdot \Gamma(k_1, \ldots, k_l).$$

更に正方行列 M の行列式を $\det(M)$ とする.

補題 5
$1 \leq k_1 < \ldots < k_l \leq d$ に対して, $\det(M_h^I(k_1, \ldots, k_l))$ は以下のように分解することが可能である.

$$\det(M_h^I(k_1, \ldots, k_l)) = \det(\Gamma(k_1, \ldots, k_l))^2 \cdot \det(\Delta_\mu) \cdot \det(\Delta_h).$$

証明
補題 4 より $M_h^I(k_1, \ldots, k_l)$ は $M_h^I(k_1, \ldots, k_l) = {}^t\Gamma(k_1, \ldots, k_l) \cdot \Delta_\mu \cdot \Delta_h \cdot \Gamma(k_1, \ldots, k_l)$. 更に, $M_h^I(k_1, \ldots, k_l)$, ${}^t\Gamma(k_1, \ldots, k_l)$, Δ_μ, Δ_h, $\Gamma(k_1, \ldots, k_l)$ はいずれも l 次正方行列である. 従って, $\det(M_h^I(k_1, \ldots, k_l)) = \det({}^t\Gamma(k_1, \ldots, k_l) \cdot \det(\Delta_\mu) \cdot \det(\Delta_h) \cdot \det(\Gamma(k_1, \ldots, k_l)) = \det(\Gamma(k_1, \ldots, k_l))^2 \cdot \det(\Delta_\mu) \cdot \det(\Delta_h)$.

以下が本稿の主定理の鍵である.

命題 6
M_h^I の l 次主小行列式の和は以下の構造を持つ.

$$\sum_{1 \leq k_1 < \ldots < k_l \leq d} \det(M_h^I(k_1, \ldots, k_l)) = \sum_{1 \leq k_1 < \ldots < k_l \leq d} \det(\Gamma(k_1, \ldots, k_l))^2 \cdot \det(\Delta_\mu) \cdot \det(\Delta_h).$$

証明
補題 5 から従う.

M_h^I の固有多項式の $d-l$ 次係数を c_h で表現する. このとき, 以下が従う.

命題 7
M_1, M_h^I の固有多項式の $d-l$ 次係数 c_1, c_h に関して, $c_h = \det(\Delta_h) \cdot c_1$.

証明
命題 6 より,

$$c_1 = (-1)^{k-l} \cdot \sum_{1 \leq k_1 < \ldots < k_l \leq d} \det(\Gamma(k_1, \ldots, k_l))^2 \cdot \det(\Delta_\mu)).$$

従って, 我々は主張を満足するような以下の変形を得ることができる.

$$\begin{aligned} c_h &= (-1)^{k-l} \cdot \sum_{1 \leq k_1 < \ldots < k_l \leq d} \det(\Gamma(k_1, \ldots, k_l))^2 \cdot \det(\Delta_\mu) \cdot \det(\Delta_h) \\ &= \det(\Delta_h) \cdot ((-1)^{k-l} \cdot \sum_{1 \leq k_1 < \ldots < k_l \leq d} \det(\Gamma(k_1, \ldots, k_l))^2 \cdot \det(\Delta_\mu)) \\ &= \det(\Delta_h) \cdot c_1. \end{aligned}$$

ここで, $c_h = c \cdot c_1$ となるような c を考えると, 本稿の主定理である以下を満足する.

定理 8
$c \neq 0 \Leftrightarrow I = I : h^\infty$.

証明
命題 7 より $c = \det(\Delta_h)$. 更に, $\det(\Delta_h) = \prod_{1 \leq i \leq l} h(\bar{c}_i)$. また, I は零次元イデアルであることに注意すると, $1 \leq \forall i \leq l\ (h(\bar{c}_i) \neq 0) \Leftrightarrow I = I : h^\infty$. 従って, 主張が満たされる.

定理 8 は我々に飽和イデアルが元々のイデアルと等価になることの計算可能な必要十分条件を示しているが, $\det(m_h) \neq 0 \Leftrightarrow I = I : h^\infty$ であることにも注意しなければならない. しかしながら, **例 9** のように, $\det(m_h) \neq 0$ は ($I = \sqrt{I}$ の場合を除いて) 重複した情報を持ち, $\det(\Delta_h^I) \neq 0$ は我々に飽和イデアルが元々のイデアルと等価になることの計算可能で簡略な必要十分条件を示していることがわかる.

例 9
パラメータ A_1, A_2 に対し $I = \langle (X - A_1)^3 (X - A_2)^{12} \rangle$, $h = X$ とする. 上記と同様の記号 c, m_h を使うと

$$c = A_1 \cdot A_2, \ \ \det(m_h) = A_1^3 \cdot A_2^{12}.$$

3 多変数実根個数計算

本節では前節と同様の記号たちを利用し, R を K を含む実閉体とする. また, **概念 1** で定義された M_h^I と同様に $M_h^{I:h^\infty}$ を定義し, $\mathbb{V}_R(F)$ を多項式集合 F の R における多様体とする. そして, 実対称行列 M に対し, M に対応する二次形式の符号数を $\mathrm{sign}(M)$ で記述する. ここで M_h^I や $M_h^{I:h^\infty}$ は実対称であることに注意する. 以下は [13] における主定理である.

定理 10 (PRS 1993)
$\mathrm{sign}(M_h^I) = \#\{\bar{c} \in \mathbb{V}_R(I) : h(\bar{c}) > 0\} - \#\{\bar{c} \in \mathbb{V}_R(I) : h(\bar{c}) > 0\}$.

有限な $P, \{q_1, \ldots, q_t\} \subset K[\bar{X}], h = \prod_p p^2 \cdot \prod_{1 \leq i \leq t} q_i$, $V = \{\bar{c} \in \mathbb{V}_R(I) : \bigwedge_{p \in P} p \neq 0 \wedge \bigwedge_{1 \leq i \leq t} q_i > 0\}$ を考える. 以下は [21] や [3] が扱う性質である.

定理 11 (W 1998, DG 2004)
$\sum_{(e_1, \ \ldots, e_t) \in \{0,1\}^t} \mathrm{sign}(M_{h\, q_1^{e_1} \cdots q_t^{e_t}}^I) \neq 0 \Leftrightarrow \#V \neq 0$.

更に, 以下は [4] において示された主定理 ([4] **Theorem 6**) から得られる簡単な帰結である.

定理 12 (FIS 2015)
$\sum_{(e_1, \ \ldots, e_t) \in \{0,1\}^t} \mathrm{sign}(M_{q_1^{e_1} \cdots q_t^{e_t}}^{I:h^\infty}) \neq 0 \Leftrightarrow \#V \neq 0$.

節 1 で記述した通り, [4] は [21] や [3] で扱われる対称行列よりも簡略な対称行列を扱うことができる.

例 13
$A^2 - 2A - 1 \neq 0$ なるパラメタ A, $I = \langle X^2 + 2X - 1 \rangle$, $h = (X + A)^2$ を考えたとき,

$$M_1^{I:h^\infty} = \begin{pmatrix} 2 & -2 \\ -2 & 6 \end{pmatrix}, M_h^I = \begin{pmatrix} 2A^2 - 4A + 6 & -2A^2 + 12A - 14 \\ -2A^2 + 12A - 14 & 6A^2 - 28A + 34 \end{pmatrix}.$$

4 包括的グレブナー基底系

本節では前節と同様の記号等を利用することに注意し, $\bar{A} = A_1, \ldots, A_m$, $\mathcal{S}$ を C^m の部分集合とする.

定義 14
以下を満足する $\mathcal{S}$ の部分集合で構成される有限集合 $\{\mathcal{S}_1, \ldots, \mathcal{S}_u\}$ は $\mathcal{S}$ の構成的分割と呼ばれる. 更に, $\mathcal{S}_i$ は分割部と呼ばれ, 本稿ではその定義論理式と同一視することとする.

- $1 \leq \forall i, \forall j \leq u$ $(\mathcal{S}_i \cap \mathcal{S}_j = \emptyset)$.
- $\cup_{1 \leq i \leq u} \mathcal{S}_i = \mathcal{S}$.
- $1 \leq \forall i \leq u$ $\exists E_i, N_i \subset K[\bar{A}]$ $(E_i, N_i$ は有限であり, $\mathcal{S}_i = \mathbb{V}_C(E_i) \setminus \mathbb{V}_C(N_i))$.

$\bar{c} \in C^m$, $G \subset K[\bar{A}, \bar{X}]$ に対して $G(\bar{c}, \bar{X}) = \{g(\bar{c}, \bar{X}) : g \in G\}$ とする. $\bar{X}$ による項全体を $T(\bar{X})$ とする. 更に, $T(\bar{X})$ の項順序に関する $g \in K[\bar{A}, \bar{X}]$ の先頭係数を $\mathrm{HC}(g) \in K[\bar{A}]$ で記述することとする.

定義 15
$T(\bar{X})$ の項順序 $\succ$, 有限な $F \subset K[\bar{A}, \bar{X}]$ を考える. このとき, 以下を満たすような $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_u, G_u)\}$ を $\langle F \rangle$ の項順序 $\succ$ に関する $\mathcal{S}$ における *CGS* とよぶ.

- $\{\mathcal{S}_1, \ldots, \mathcal{S}_u\}$ は $\mathcal{S} \subset C^m$ の分割である.
- $1 \leq \forall i \leq u$ $\forall \bar{c} \in \mathcal{S}_i$ $(G_i(\bar{c}, \bar{X}))$ は $\langle F(\bar{c}, \bar{X}) \rangle$ の $\succ$ に関するグレブナー基底である).
- $1 \leq \forall i \leq u$ $\forall \bar{c} \in \mathcal{S}_i \forall g \in G_i$ $(\mathrm{HC}(g)(\bar{c}) \neq 0)$.

5 アルゴリズム

まずは, 前節までに利用してきた記号に加えて本節で扱う記号を定義する.

表記 16
イデアル J の次元を $\dim(J)$ で記述し, 極大従属集合を $\max(J)$ で記述する. また, $(e_1, \ldots, e_t) \in \{0,1\}^t$ に対するパラメータ付き d 次対称行列 $M_{(e_1, \ \ldots \ ,e_t)}$ たちに対し, "$\sum_{(e_1,\ldots,e_t) \in \{0,1\}^t} \mathrm{sign}(M_{(e_1,\ldots,e_t)}) \neq 0$ なる論理式" を $I_d(M_{(e_1, \ \ldots ,e_t)} : (e_1, \ldots, e_t) \in \{0,1\}^t)$ で記述する. また, $\bar{A}$ と $\bar{X}$ による論理式 ψ の選言標準形を $\mathrm{dnf}(\psi)$ で記述する. 更に, $\mathrm{dnf}(\psi)$ の任意の最小項 ϕ に対し, $\mathrm{free}(\phi, \bar{X})$ と $\mathrm{nonfree}(\phi, \bar{X})$ によって ϕ の $\bar{X}$ による *free part* と *non free part* を記述する.

有限な $F, P, \{q_1, \ldots, q_t\} \subset K[\bar{A}, \bar{X}]$ $(\forall r \in F \cup P \cup \{q_1, \ldots, q_t\}$ $(r \notin K[\bar{A}]))$ を考え, 次を ϕ とする.

$$\exists \bar{X} \ (\bigwedge_{f \in F} f = 0 \wedge \bigwedge_{p \in P} p \neq 0 \wedge \bigwedge_{1 \leq i \leq t} q_i > 0).$$

以下は本稿によって改善された CGS-QE アルゴリズムの概略である.

定理 17
CGS-QE は入力 $\exists \bar{X}\ \phi$ に対し, 等価な限量子なし論理式を出力する.

証明
ステップ *6* から ステップ *20* までの妥当性は**定理 8** 及び**定理 12** から従う. その他の妥当性や停止性は *[4]* **Theorem 16** と同様であることに注意する.

Algorithm 1 CGS-QE

Input: a basic quantified formula $\exists \bar{X}\ \phi$;

Output: an equivalent quantifier free formula ψ;

$\succ \leftarrow$ a term order of $T(\bar{X})$;
$\mathcal{G} \leftarrow$ a CGS of $\langle F \rangle$ with parameters $\bar{A}$ w.r.t. $\succ$ over C^m;
$h \leftarrow$ a polynomial product $\prod_{p \in P} p \cdot \prod_{1 \leq i \leq t} q_i$;
$\psi \leftarrow false$;
for $(\mathcal{S}, G) \in \mathcal{G}$ **do**
  if $\dim(\langle G(\bar{a}, \bar{X}) \rangle) = 0$ for $\bar{a} \in \mathcal{S}$ **then**
    $c_1 \leftarrow$ the tail coefficient of the characteristic polynomial of $M_1^{\langle G \rangle}$;
    ▷ We assume that the tail coefficient is $(d-l)$-th coefficient.
    $c_h \leftarrow$ the $(d-l)$-th coefficient of the characteristic polynomial of $M_h^{\langle G \rangle}$;
    $c \leftarrow$ the numer of the factor c' s.t. $c_h = c' \cdot c_1$;
    $\mathcal{S}_1 \leftarrow \mathcal{S} \wedge (c \neq 0)$;
    for $(e_1, \ldots, e_t) \in \{0,1\}^t$ **do**
      $M_{(e_1, \ldots, e_t)} \leftarrow$ the symmetric matrix $M^{\langle G \rangle}_{\prod_{1 \leq i \leq t} q_i^{e_i}}$ on $\mathcal{S}_1$;
    end for
    $\psi \leftarrow \psi \vee (\mathcal{S}_1 \wedge I_d(M_{(e_1, \ldots, e_t)} : (e_1, \ldots, e_t) \in \{0,1\}^t))$;
    $\mathcal{S}_2 \leftarrow \mathcal{S} \wedge (c = 0)$;
    for $(e_1, \ldots, e_t) \in \{0,1\}^t$ **do**
      $M_{(e_1, \ldots, e_t)} \leftarrow$ the symmetric matrix $M^{\langle G \rangle \cdot h}_{\prod_{1 \leq i \leq t} q_i^{e_i}}$ on $\mathcal{S}_2$;
    end for
    $\psi \leftarrow \psi \vee (\mathcal{S}_2 \wedge I_d(M_{(e_1, \ldots, e_t)} : (e_1, \ldots, e_t) \in \{0,1\}^t))$;
  else if $0 < \dim(\langle G(\bar{a}, \bar{X}) \rangle) < n$ for $\bar{a} \in \mathcal{S}$ **then**
    $\bar{M} \leftarrow \max(\langle G \rangle)$;
    $\bar{X}' \leftarrow \bar{X} \setminus \bar{M}$;
    $\phi_1' \leftarrow \mathrm{free}(\phi, \bar{X}')$;
    $\phi_2' \leftarrow \mathrm{nonfree}(\phi, \bar{X}')$;
    $\phi' \leftarrow \mathrm{dnf}(\phi_2 \wedge \mathbf{CGS\text{-}QE}(\exists \bar{X}'\ \phi_1))$;
    ▷ We assume that ϕ' is $\phi_1 \vee \ldots \vee \phi_s$.
    for $1 \leq i \leq s$ **do**
      $\phi_1'' \leftarrow \mathrm{free}(\phi, \bar{M})$;
      $\phi_2'' \leftarrow \mathrm{nonfree}(\phi, \bar{M})$;
      $\psi \leftarrow \psi \vee (\phi_2'' \wedge \mathbf{CGS\text{-}QE}(\exists \bar{M}\ \phi_1''))$;
    end for
  else
    $\psi \leftarrow \psi \vee \mathbf{OtherQE}(\exists \bar{X}\ \phi)$;
  end if
end for

上記アルゴリズムにおいて登場する **OtherQE** に関して, 以下に注意する.

注意 18
OtherQE は CGS-QE 以外による QE 論理式を表現している. ここで, ステップ *32* の **If** 文の条件は限量子変数等式制約が存在しないことを意味していることに注意すると, "限量子変数等式制約が存在しない場合に我々は CGS-QE 以外のアルゴリズムを適用している" ということになる. つまり, **CGS-QE** は入力の一階述語論理式 $\exists \bar{X} \phi$ から等式制約多項式集合 F を利用可能な限り利用し, "束縛変数等式制約を一切含まない論理式" に変換 (簡略化) し, **OtherQE** を利用する. ここでは "束縛変数等式制約を一切含まない論理式" に対する *CAD* の強力な結果 *[18]* を利用できることにも注意しなければならない.

本稿の改良点は以下である.

注意 19
ステップ *6* から ステップ *20* までが *[4]* の **ZeroDimQE** を改良していることを注意する. これら以外は *[4]* で示されたアルゴリズムと変わりない. 主な改良点は以下 2 点である.

- ステップ *13:* **定理 8** により飽和イデアルの計算なしで**定理 12** の構造が利用可能となった.
- ステップ *20:* **定理 8** により得た自由変数等式制約 $c = 0$ を飽和イデアル計算で利用可能となった.

  つまり, 軽量な計算量を持つ傾向がある飽和イデアル計算が利用可能となった.

  自由変数等式制約 $c = 0$ は *[21]* で扱う $M^{\langle G \rangle}_{h \cdot \prod_{1 \leq i \leq t} q_i^{e_i}}$ も簡略化する.

  ステップ *18* では $M^{\langle G \rangle}_{h \cdot \prod_{1 \leq i \leq t} q_i^{e_i}}$ を利用することも可能である.

本節における改良は必要最小限の飽和イデアル計算で**例 13** で示されたような簡略な対称行列の構造を利用することを可能にした. つまり, [4] の不要な飽和イデアルの計算を完璧に取り除いたのである. 更に言えば, 飽和イデアル計算が必要なときでさえ, 軽量な計算で済むという効果すらも発生させた. 次節では本節で示されたアルゴリズムの効果を我々の実験データを通して示す.

6 実験

我々はこれまで数式処理システム **Maple** 上に CGS-QE アルゴリズムを実装した **CGSQE** パッケージを公開してきた. 本節では, 2016 年に公開したバージョンの **CGSQE** パッケージ (以下では old と記述する) とともに, **Algorithm 1 CGS-QE** を実装した新バージョンの **CGSQE** パッケージ (以下では new と記述する) を比較する. 2016 年に公開したバージョンの **CGSQE** パッケージは以下で公開されているため, 誰もが利用可能である.

`http://www.rs.tus.ac.jp/fukasaku/software/CGSQE-20160509/`

更に QE パッケージとして公開されている次のパッケージも比較する: 富士通によって公開されている **Maple** 上の **SyNRAC** パッケージ (下表では syn と記述する, [19]), **Maple** 上の **RegularChains** パッケージ (下表では rc と記述する, [16]), 数式処理システム **Mathematica** 上に実装された **Reduce** パッケージ (下表では red と記述する, [15]) と **Resolve** パッケージ (下表では res と記述する, [17]), 数式処理システム **Reduce** 上に実装された **rlhqe** パッケージ (下表では rlh と記述する, [14]) と **rlqe** パッケージ (下表では rl と記述する, [14]), **QEPCAD** パッケージ (以下では qep と記述する, [12]).

数式処理システムたちに関するバージョンは次の通りである: **Maple** のバージョンは **Maple 2015**, **Mathematica** のバージョンは **Mathematica 11**, **Reduce** のバージョンは **Reduce (Free CSL version), 04-Aug-11**, **QEPCAD** のバージョンは **Version B 1.69, 16 Mar 2012**.

以下で示される実験はいずれも 16 GB のメモリを持つ, 4 つの Intel(R) Core(TM) i7-3635QM CPU @ 2.40GHz によって, Ubuntu 14.04 上において行われた.

本稿では我々の実験結果の一部として以下の入力に関する計算時間を示す.

1. $\exists x_1\exists x_2\exists x_6\exists x_7(\bigwedge_{1\leq i\leq 6} F_i{=}0 \wedge \bigwedge_{1\leq i\leq 7} P_i{\neq}0 \wedge Q{>}0)$.
   $F_1{=}x_5x_1x_4^2{+}x_4^2{-}x_1x_2x_4{-}x_2x_4{+}x_1x_2{+}3x_2, F_2{=}x_1x_4{+}x_3{-}x_1x_2, F_3{=}x_3x_4{-}2x_2^2{-}x_1x_2{-}1, F_4{=}2x_1x_2^2{+}2x_1^2x_2^2{-}2x_1^2x_2{+}x_1^2{+}x_1,$
   $F_5{=}x_1x_3^2{+}x_3^2{-}x_1^2x_2x_3{-}x_1x_2x_3{+}x_1^3x_2{+}3x_1^2x_2, F_6{=}{-}x_3{+}x_1x_2x_3{-}2x_1x_2^2{-}x_1^2x_2{-}x_1,$
   $P_1{=}x_1^2{+}x_2{+}x_3^2{+}x_4, P_2{=}x_6{-}x_3{-}1, P_3{=}x_2{-}x_1, P_4{=}x_2{-}x_3, P_5{=}x_7{-}x_1, P_6{=}x_6{-}x_2,$
   $P_7{=}x_8^7x_1{+}x_8^6x_2{+}x_8^5x_3{+}x_8^4x_4{+}x_8^3x_5{+}x_8^2x_6{+}x_8x_7{-}x_1{-}x_2{-}x_3{-}x_4{-}x_5{-}x_6{-}x_7^3,$
   $Q{=}x_1x_7{+}x_2x_6{-}x_3^{100}$.

2. $\exists v_1\exists v_2(F{=}0 \wedge P{\neq}0)$.
   $F{=}av1^3{+}3v1^3v2{+}2v1v2{+}bv2^3,$
   $P{=}v1v2(v2{-}1)(3v1{-}v2)(v1{+}v2)(av1{+}27bv1{+}9v1^2{+}6)(av1^3{+}3v1^3{+}b{+}2v1)(av1{-}bv1{-}3v1^2{-}2)$.

3. $\exists c_2\exists s_2\exists c_1\exists s_1\exists t(\bigwedge_{1\leq i\leq 4} F_i{=}0 \wedge Q{>}0)$.
   $F_1{=}r{-}c_1{+}l(s_1s_2{+}c_1c_2), F_2{=}z{-}s_1{-}l(s_1c_2{-}s_2c_1){-}c_1, F_3{=}s_1^2{+}c_1^2{-}1, F_4{=}s_2^2{+}c_2^2{-}1,$
   $Q{=}4c_1r{+}2c_1z{+}2c_2l{+}5s_1^2{-}t$.

4. $\exists x\exists y\exists z\exists w(\bigwedge_{1\leq i\leq 5} F_i{=}0 \wedge P{\neq}0 \wedge Q{>}0)$.
   $F_1{=}xyw{+}axz{+}yz{-}1,\ F_2{=}xyz{+}xz{+}xy{-}a,\ F_3{=}xz{+}yz{-}az{-}x{-}y{-}1,\ F_4{=}axy{-}byz,\ F_5{=}ayz{-}bzx,$
   $P{=}w(-w^6{-}9w^4{-}135w^2{-}27),$
   $Q{=}w{-}c$.

5. $\exists x\exists y(F{=}0 \wedge P{\neq}0)$.
   $F{=}ax^3{-}x^2y^3{+}bxy{+}x{+}y,$
   $P{=}(x{+}1)(y{+}1)xy(x{+}y)(x{-}y)(ax^2{-}1)(x^3{+}ax{+}b)((-x^4){+}ax^2{-}bx{-}2)(ax^3{+}bx{+}x^2{-}x{+}1)$.

6. $\exists x\exists y\exists z(\bigwedge_{1\leq i\leq 4} F_i{=}0 \wedge \bigwedge_{1\leq i\leq 2} P_i{\neq}0)$.
   $F_1{=}xy{+}axz{+}yz{-}1, F_2{=}xyz{+}xz{+}xy{-}a, F_3{=}xz{+}yz{-}az{-}x{-}y{-}1, F_4{=}axy{-}byz,$
   $P_1{=}ayz{-}bzx, P_2{=}azx{-}bxy$.

7. $\exists x\exists y\exists z\exists u\exists v\exists w(\bigwedge_{1\leq i\leq 6} F_i{=}0 \wedge P{\neq}0 \wedge \bigwedge_{1\leq i\leq 3} Q_i{>}0)$.
   $F_1{=}xyu{+}axz{+}yz{-}1, F_2{=}xyzv{+}xz{+}xy{-}b, F_3{=}axy{-}byz, F_4{=}ayz{-}bzx, F_5{=}azu{-}buv, F_5{=}auv{-}bvx, F_6{=}avx{-}bxy,$
   $P{=}axy - wy + y^2 + b,$
   $Q_1{=}axyz - buv, Q_2{=}ax + y + bz - w, Q_3{=}{-}buv + ax$.

8. $\exists s\exists t(F{=}0 \wedge \bigwedge_{1\leq i\leq 3} P_i{\neq}0)$.
   $F{=}(t{-}a)(s{-}b){+}(t^4{-}a^4)(s^4{-}b^4){-}1,$
   $P_1{=}t{-}a, P_2{=}s{-}b, P_3{=}a{-}b$.

9. $\exists b_1\exists b_2\exists c_1\exists c_2\exists d_1\exists d_2\exists e_1\exists e_2\exists f_1\exists f_2\exists h_1\exists h_2\exists k_1\exists k_2(\bigwedge_{1\leq i\leq 20} F_i{=}0 \wedge \bigwedge_{1\leq i\leq 4} P_i{\neq}0)$.
   $F_1{=}b_1, F_2{=}b_2, F_3{=}c_1^2{-}1, F_4{=}c_2, F_5{=}(a_1{-}d_1)(b_1{-}c_1){+}(a_2{-}d_2)(b_2{-}c_2), F_6{=}(b_1{-}e_1)(a_1{-}c_1){+}(b_2{-}e_2)(a_2{-}c_2),$

F_7=$(c_1-f_1)(a_1-b_1)+(c_2-f_2)(a_2-b_2)$,$F_8$=$a_1-h_1-k_1(a_1-d_1)$,$F_9$=$a_2-h_2-k_1(a_2-d_2)$,$F_{10}$=$b_1-h_1-k_2(b_1-e_1)$,
F_{11}=$b_2-h_2-k_2(b_2-e_2)$,F_{13}=$(o_1-b_1)^2+(o_2-b_2)^2-r$,$F_{14}$=$(o_1-c_1)^2+(o_2-c_2)^2-r$,$F_{15}$=$(o_1-e_1)^2+(o_2-e_2)^2-r$,
F_{16}=$(o_1-f_1)^2+(o_2-f_2)^2-r$,$F_{17}$=$(o_1-a_1)^2+(o_2-a_2)^2-r$,$F_{18}$=$(o_1-f_1)^2+(o_2-f_2)^2-r$,$F_{19}$=$(o_1-h_1)^2+(o_2-h_2)^2-r$,
F_{20}=$(o_1-e_1)^2+(o_2-e_2)^2-r$,
P_1=$a_2(a_2^2-1)$,P_2=$a_2r-2ro_2-\frac{1}{2}a_2$,$P_3$=$(-f_2^2)+2f_2o_2+o_1^2$,$P_4$=$f_2^9-o_1^9$.

下表は単位を "秒" とした, 上記入力 1 から 9 に対する, 計算時間である. E_t は t 秒で何かしらのエラーが発生してしまったことを意味し, $>_{3600}$ は 3600 秒では計算が止まらなかったため計算を終了させたことを意味する.

表 1: 計算時間

入力	new	old	syn	rc	red	res	rl	rlh	qep
1	55	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$
2	3	$>_{3600}$	E_{978}	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	1990
3	2	$>_{3600}$	E_{12}	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$
4	45	127	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$
5	2	$>_{3600}$	E_{539}	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$
6	46	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	E_{2026}	$>_{3600}$
7	7	2240	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	E_{189}	$>_{3600}$	$>_{3600}$
8	11	$>_{3600}$	$>_{3600}$	$>_{3600}$	260	256	$>_{3600}$	$>_{3600}$	133
9	19	$>_{3600}$	$>_{3600}$	234	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$	$>_{3600}$

上表の通り, 計算量は改善した. ここで, 特筆すべきは, 等式制約が少ないような入力 (例えば, 入力 2, 5 及び 8) に対しても, 本稿によって, 改善したことである.

7 まとめ

本稿では, **定理 8** により飽和イデアルの計算なしで**定理 12** の構造が利用可能な分割部を構築した. 更に言えば, そうでない分割部における計算ですらも, **定理 8** により得た自由変数等式制約 $c=0$ を利用可能となり, 軽量な計算量で限量子を消去した論理式を計算することも可能にした.

また, CGS-QE の進歩は近年の CGS アルゴリズムの進歩 ([20] が CGS アルゴリズムのブレイクスルーとなり, その改良 [6], [7], [10], [11] が達成された) の貢献が大きいと思われる. しかしながら, CGS-QE では, CGS の性質の全てを使わない. 従って, CGS-QE に特化した CGS の計算も必要であるように思われる.

参 考 文 献

[1] Chen, C., 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] Collins, G, E.: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Proceedings of Automata theory and formal languages, Lecture Notes in Computer Science Vol.33, pp.134-183, Springer, 1975.

[3] Dolzmann, A., Gilch, L. A.: Generic Hermitian Quantifier Elimination. Proceedings of Artificial Intelligence and Symbolic Computation, Lecture Notes in Computer Science Vol.3249, pp.80-93, Springer, 2004.

[4] Fukasaku, R., Iwane, H., Sato, Y: Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp.173-180, ACM, 2015.

[5] Fukasaku, R., Iwane, H., Sato, Y: On the Implementation of CGS Real QE. Proceedings of Mathematical Software - ICMS 2016 - 5th International Conference, Lecture Notes in Computer Science Vol.9725, pp.165-172, Springer, 2016.

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

[7] Kurata, Y.: Improving Suzuki-Sato ' s CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation. Communications of the Japan Society for Symbolic and Algebraic Computation Vol.1, pp. 39-66, 2011.

[8] 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.

[9] 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.

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

[11] Nabeshima, K.: tability Conditions of Monomial Bases and Comprehensive Gröbner systems. Proceedings of Computer Algebra in Scientific Computing, Lecture Notes in Computer Science Vol.7442, pp.248-259, Springer, 2012

[12] QEPCAD: `https://www.usna.edu/CS/qepcadweb/B/QEPCAD.html`.

[13] Pedersen, P., Roy, M.-F., Szpirglas, A.: Counting real zeroes in the multivariate case. Proceedings of Effective Methods in Algebraic Geometry, Progress in Mathematics Vol.109, pp.203-224, Springer, 1993.

[14] Redlog Package: `http://www.redlog.eu/`.

[15] Reduce Package: `https://reference.wolfram.com/language/ref/Reduce.html`.

[16] RegukarChains Package: `http://www.regularchains.org/`.

[17] Resolve Package: `https://reference.wolfram.com/language/ref/Resolve.html`.

[18] Strzebonski, A.: Solving Systems of Strict Polynomial Inequalities. Journal of Symbolic Computation Vol.29 No.3, pp.471-480, 2000.

[19] SyNRAC Package: `http://www.fujitsu.com/jp/group/labs/en/resources/tech/freeware/synrac/`.

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

[21] Weispfenning, V.: A New Approach to Quantifier Elimination for Real Algebra. Quantifier Elimination and Cylindrical Algebraic Decomposition, Part of the series Texts and Monographs in Symbolic Computation, pp.376-392, 1998.