Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems

Ryoya Fukasaku\textsuperscript{1}  Hidenao Iwane\textsuperscript{2}  Yosuke Sato\textsuperscript{1}

\textsuperscript{1}Tokyo University of Science
\textsuperscript{2}National Institute of Informatics / Fujitsu Laboratories Ltd

Tuesday 7th July 2015
Contents of My Talks

1 Motivation
   - Todai Robot Project
   - Quantified Formula with Many Equalities
   - Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems

2 Real Root Counting
   - Real Root Counting Theorem
   - Characteristic Polynomial

3 Comprehensive Gröbner System
   - Algebraic Partition
   - Comprehensive Gröbner System

4 Main Algorithm

5 Computation Data

6 Conclusion
Motivation
The motivation of our work has its roots in “Todai Robot Project”.

“Todai Robot Project” is the ongoing research project of artificial intelligence.

The purpose of “Todai Robot Project” is to develop software which automatically produces an answer sheet for an entrance examination of “Todai”.

University of Tokyo is known as “Todai” in Japan.

University of Tokyo is the highest rank university in Japan.

We have to obtain a sufficient score to pass by using our software.
How does our software solve math problems?

- Syntactic Parsing
- Anaphora Resolution
- Discourse Analysis
- Natural Language Processing

Math Problem

Semantic Representation

Formula Rewriting

Input of Solver

Computer Algebra

Math Knowledge Base

- Gröbner Basis
- Quantifier Elimination (QE)
- etc.

Answer
Todai Robot Project

- How does our software solve math problems?

  - Syntactic Parsing
  - Anaphora Resolution
  - Discourse Analysis

Dictionary:
- circle c: $C(C)$
- area of c: $A(C)$
- radius of c: $R(C)$

Math Knowledge Base
- Gröbner Basis
- Quantifier Elimination (QE)
- etc.

Math Problem

“Find the radius $r$ of a circle $c$ s.t. the area is $4\pi$.”

Natural Language Processing

Semantic Representation

Formula Rewriting

Input of Solver

Computer Algebra

Answer

$r = 2.$
Quantified Formula with Many Equalities

- Our software often generates a quantified formula with many equalities.

**Example** \( \triangle ABC \) is inscribed in a circle with the radius 1, \( \tan(\angle CAB) = m \) and \( \tan(\angle ABC) = n \). However \( m, n \geq 3 \). Let \( S \) be the area of \( \triangle ABC \).

(1) Represent \( S \) on the terms of \( m, n \).

Let

- \( \phi_1 \) be \( x_0 x_3 - x_0 x_4 + x_1 x_2 - x_1 x_3 - x_2 x_5 + x_4 x_5 \geq 0 \),
- \( \phi_2 \) be \( (x_5 - x_0) x_4 - x_2 - (x_3 - x_2) x_1 - x_0 \geq 0 \),
- \( \phi_3 \) be \( (x_5 - x_0)((1/2)x_0 + (1/2)x_5 + x_7) + (x_3 - x_2)((1/2)x_2 + (1/2)x_3 - x_6) = 0 \),
- \( \phi_4 \) be \( (x_1 - x_5)((1/2)x_5 + (1/2)x_1 - x_7) + (x_4 - x_3)((1/2)x_3 + (1/2)x_4 - x_6) = 0 \),
- \( \phi_5 \) be \( ((x_7 - x_0)^2 + (x_6 - x_2)^2)^{1/2} = 1 \),
- \( \phi_6 \) be \( |x_0 x_3 - x_0 x_4 + x_1 x_2 - x_1 x_3 - x_2 x_5 + x_4 x_5| / ((x_1 - x_0)(x_5 - x_0) + (x_4 - x_2)(x_3 - x_2)) = m \),
- \( \phi_7 \) be \( |x_0 x_3 - x_0 x_4 + x_1 x_2 - x_1 x_3 - x_2 x_5 + x_4 x_5| / ((x_0 - x_5)(x_1 - x_5) + (x_2 - x_3)(x_4 - x_3)) = n \),
- \( \phi_8 \) be \( m \geq 3 \land n \geq 3 \),
- \( \phi_9 \) be \( |x_5 - x_0 x_4 - x_2 + x_3 - x_2 x_1 - x_0| / 2 = S \) and
- \( \phi \) be \( \exists x_0 \exists x_1 \exists x_2 \exists x_3 \exists x_4 \exists x_5 \exists x_6 \exists x_7 ( \land_{1 \leq i \leq 9} \phi_i ) \).

- \( \phi \) can be not solved within 1 hour by the existing QE software SyNRAC@Maple, RegularChains@Maple, Resolve@Mathematica, Reduce@Mathematica, QEPCAD and RedLog@Reduce.
Quantified Formula with Many Equalities

- We need to establish a practical implementation of QE for a quantified formula with many equalities.

- We improve the following work:


- We call for short “comprehensive Gröbner system” “CGS” and “real QE by computation of CGSs” “CGS-QE”.
Real QE by Computation of CGSs

- CGS-QE is a special QE method for the input formula
  \[ \exists \bar{x}((\bigwedge_i f_i = 0) \land (\bigwedge_i p_i > 0) \land (\bigwedge_i q_i \neq 0)), \]
  where \( \bar{x} = X_1, \ldots, X_n, \bar{Y} = Y_1, \ldots, Y_m, f_i, p_i, q_i \in K[\bar{Y}, \bar{x}] \).

- CGS-QE uses “Real Root Counting Theorem (Pedersen)” and “CGS”.

- In Section Real Root Counting,
  we modify “Real Root Counting Theorem” for improving CGS-QE.

- In Section Comprehensive Gröbner System, we show its definition.
Real Root Counting
Notations

- $R$ denotes a real closed field,
  
  $C$ its algebraic closed extension and
  
  $K$ a computable subfield of $R$.

- Let $\bar{X}$ be variables $X_1, \ldots, X_n$.

- $T(\bar{X})$ denotes the set of all terms consisting of variables in $\bar{X}$.

- In this section, let $I$ be a zero dimensional ideal in $K[\bar{X}]$.

- Let $V_R(I) = \{ \bar{c} \in R^n | \forall f \in I \ f(\bar{c}) = 0 \}$, $V_C(I) = \{ \bar{c} \in C^n | \forall f \in I \ f(\bar{c}) = 0 \}$. 
Real Root Counting Theorem

- Let $v_1, \ldots, v_d$ be the basis of the residue class ring $A = K[\bar{X}]/I$.

- For $p \in A$ and each $i, j$ $(1 \leq i, j \leq d)$, we consider the followings:
  - Let $Q_{p,i,j}$ be the trace of a linear map $A \rightarrow A$ by $f \mapsto pv_i v_j a$ for $a \in A$.
  - Let $M^I_p$ be a symmetric matrix $(M^I_p)_{i,j} = Q_{p,i,j}$.
  - The signature of $M^I_p$ is denoted $\sigma(M^I_p)$.

Pedersen $\sigma(M^I_p) = \#(\{ \bar{c} \in V_R(I) | p(\bar{c}) > 0 \}) - \#(\{ \bar{c} \in V_R(I) | p(\bar{c}) < 0 \})$.

Corollary $\sigma(M^I_1) = \#(V_R(I))$.

Remark We can compute $\sigma(M^I_p)$ by computing the number of the sign changes of the coefficients of the characteristic polynomial of $M^I_p$. 

12 / 35
In CGS-QE, by using the obvious equivalent relations

\[ p > 0 \iff \exists z \ z^2 p = 1 \]

and

\[ q \neq 0 \iff \exists w \ wq = 1 \]

we reduce “the degree of a characteristic polynomial”.
Real Root Counting Theorem

- Let \( p_1, \ldots, p_s \in K[\tilde{X}] \) and \( \tilde{Z} \) be new variables \( Z_1, \ldots, Z_s \).

- Let \( J = I + \langle Z_1^2 p_1 - 1, \ldots, Z_s^2 p_s - 1 \rangle \) be an ideal in \( K[\tilde{X}, \tilde{Z}] \).

**Corollary** \( \#(V_R(J)) = 2^s \#(\{ \tilde{c} \in V_R(I) | p_1(\tilde{c}) > 0, \ldots, p_s(\tilde{c}) > 0 \}) \).

- Let \( I' \) be the elimination ideal \( J \cap K[\tilde{X}] \).

**Corollary** \( I' = \langle 1 \rangle \lor p_i \) is invertible in \( K[\tilde{X}]/I' \) for \( i = 1, \ldots, s \).

- We assume that \( p_i \) has the inverse \( p_i' \) in \( K[\tilde{X}]/I' \) for \( i = 1, \ldots, s \).

**Corollary** \( J = I' + \langle Z_1^2 - p_1', \ldots, Z_s^2 - p_s' \rangle \).
Real Root Counting Theorem

- Let $J = I + \langle Z_1^2 - p_1, \ldots, Z_s^2 - p_s \rangle$ with $p_1, \ldots, p_s \in K[\tilde{X}]$.

- Let $B_I = \{t_1, \ldots, t_k\} \subset T(\tilde{X})$ be a basis of $K[\tilde{X}]/I$ and
  \[ B_J = \{ t_1 Z_1^{e_1} Z_2^{e_2} \cdots Z_s^{e_s}, \ldots, t_k Z_1^{e_1} Z_2^{e_2} \cdots Z_s^{e_s} \mid (e_1, e_2, \ldots, e_s) \in \{0, 1\}^s \} \text{.} \]

Then $B_J$ forms a basis of $K[\tilde{X}, \tilde{Z}]/J$.

- For $g \in K[\tilde{X}]$, we consider the followings:
  - $M^J_g$ denote a symmetric matrix such as the matrix of Pedersen for $J, g$ and $\chi^J_g$ its characteristic polynomial.
  - We consider also $M^I_g$ and $\chi^I_g$ similary as $M^J_g$ and $\chi^J_g$.

**Theorem**

$\chi^J_g(2^s X) = c \prod_{(e_1, e_2, \ldots, e_s) \in \{0, 1\}^s} \chi^I_{gp_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}}(X)$ (a non-zero constant $c$).

(\therefore See the proceedings)
**Charateristic Polynomial**

**Example**  We consider $I = \langle (x_1^2 - x_2^2)(x_1 + 2x_2 - 1), (3x_1 + x_2 - 1)^2 \rangle$, $p_1 = x_1 - x_2$ and $p_2 = x_1 + x_2$. Let $J = I + \langle z_1^2 p_1 - 1, z_2^2 p_2 - 1 \rangle$, $I' = J \cap \mathbb{Q}[x_1, x_2]$ and $>$ be a term order such that $z_1 > z_2 > x_1 > x_2$.

- \[ \{ 25x_2^2 - 20x_2 + 4, x_1 + 2x_2 - 1, 9z_2^2 - 25x_2 - 5, z_1^2 - 75x_2 + 35 \} \]
  is a Gröbner basis of $J$ w.r.t. $>$.  

- $I' = \langle 25x_2^2 - 20x_2 + 4, x_1 + 2x_2 - 1 \rangle$.

- Let $p_1' = 15Y - 7$, $p_2' = 5Y + 1$.

- $\chi_{p_1^{-2}p_2^{-2}}(X)\chi_{p_1^{-2}p_2^{-2}}(X)\chi_{p_1^{-2}p_2^{-2}}(X)\chi_{p_1^{-2}p_2^{-2}}(X)$ has a degree 24,

  whereas $\chi_{p_1}(X)\chi_{p_1'}(X)\chi_{p_2'}(X)\chi_{p_1'}(X)$ has a degree 8.

- The original CGS-QE computes $\chi_{p_1^{-2}p_2^{-2}}(X)\chi_{p_1^{-2}p_2^{-2}}(X)\chi_{p_1^{-2}p_2^{-2}}(X)\chi_{p_1^{-2}p_2^{-2}}(X)$. 
Charateristic Polynomial

- We compute the saturation ideal \( I' \) of \( I \) w.r.t. polynomials \( p_1, \ldots, p_s \).

- The dimension of \( K[\bar{x}]/I' \) is smaller than it of \( K[\bar{x}]/I \).

- We can reduce the degree of our characteristic polynomial.

- By using a primary decomposition of \( I \),
  
  we can certainly remove the unnecessary portion from \( I \).

- For parametric polynomial ideals,
  
  this computation or even factorization of a polynomial
  becomes a significantly heavy computation.

- Using the relation \( q \neq 0 \iff \exists W \ Wq = 1 \),
  
  we further can reduce the degree of a characteristic polynomial.
Comprehensive Gröbner System
Notations

- Let $\bar{X}$ be main variables $X_1, \ldots, X_n$.
- Let $\bar{Y}$ be parameters $Y_1, \ldots, Y_m$.
- Given a term order, $LM(f)$, $LT(f)$, $LC(f)$ denotes
  the leading monomial, the leading term, the leading coefficient
  of a polynomial $f$, respectively.
Algebraic Partition

Let $S$ be a subset of an affine space $\mathbb{C}^n$ for some natural number $n$. A finite set $\{S_1, \ldots, S_t\}$ of non-empty subsets of $S$ is called an algebraic partition of $S$ if it satisfies the properties 1, 2, 3:

1. $\bigcup_{i=1}^{t} S_i = S$.

2. $S_i \cap S_j = \emptyset$ if $i \neq j$.

3. For each $i$, $S_i = V_C(I_1) \setminus V_C(I_2)$ for some ideals $I_1, I_2$ of $K[\bar{Y}]$.

- Each $S_i$ is called a segment.

- We identify each $S_i$ with its defining formula.
Comprehensive Gröbner System

Let $S$ be a subset of $C^n$ and $\succ$ be a term order on $T(\bar{X})$.

CGS For finite $F \subset K[\bar{Y}, \bar{X}]$, a finite set $\mathcal{G} = \{(S_1, G_1), \ldots, (S_s, G_s)\}$ satisfying the properties 1, 2, 3, 4 is called a CGS of $F$ over $S$ with parameters $\bar{Y}$ w.r.t. $\succ$:

1. Each $G_i$ is a finite subset of $K[\bar{Y}, \bar{X}]$.

2. $\{S_1, \ldots, S_s\}$ is an algebraic partition of $S$.

3. For each $\bar{c} \in S_i$, $G_i(\bar{c}, \bar{X}) = \{g(\bar{c}, \bar{X}) | g(\bar{Y}, \bar{X}) \in G_i\}$ is a Gröbner basis of the ideal $\langle \{f(\bar{c}, \bar{X}) | f(\bar{Y}, \bar{X}) \in F\} \rangle$ in $C[\bar{X}]$ w.r.t. $\succ$.

4. For each $\bar{c} \in S_i$, $\text{LC}(g)(\bar{c}) \neq 0$ for any element $g$ of $G_i$. 
Main Algorithm
Notations 1

In this section, we assume that $\phi$ forms of a formula

$$(\bigwedge_{1 \leq i \leq r} f_i = 0) \land (\bigwedge_{1 \leq i \leq s} p_i > 0) \land (\bigwedge_{1 \leq i \leq t} q_i \neq 0)$$

where $\bar{X} = X_1, \ldots, X_n$, $\bar{Y} = Y_1, \ldots, Y_m, f_i, p_i, q_i \in \mathbb{Q}[\bar{Y}, \bar{X}], f_i, p_i, q_i \notin \mathbb{Q}[\bar{Y}].$

- **Free**($\psi, \bar{X}$) and **NonFree**($\psi, \bar{X}$) denote the free part and non-free part of $\psi$ w.r.t. the variables $\bar{X}$.

- For an element $(S, G)$ of a CGS $G$ w.r.t. a term order $>$ with main variables $\bar{X}$, $\text{MaxIndVar}(\bar{X}, G, >)$ denotes some maximal independent set among $\bar{X}$ w.r.t. an ideal $\langle G(\bar{c}) \rangle$ for $\bar{c} \in S.$
Let $M$ be a real symmetric matrix, $\chi(X)$ be its characteristic polynomial.

- We assume that $\chi(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$.
- We assume that $\chi(-X) = (-1)^d X^d + b_{d-1}X^{d-1} + \cdots + b_0$.

**Remark** $b_i = a_i$ if $i$ is even, $b_i = -a_i$ if $i$ is odd.

- $S_+$ denotes $(\text{sign changes in } (1, a_{d-1}, \ldots, a_0))$
- $S_-$ denotes $(\text{sign changes in } (-1)^d, b_{d-1}, \ldots, b_0)$.

**Remark** $S_+ = \#(\{c \in \mathbb{R} | c > 0 \land \chi(c) = 0\})$,

$$S_- = \#(\{c \in \mathbb{R} | c < 0 \land \chi(c) = 0\}).$$
Notations 3

Let $I$ be a zero dimensional ideal in a polynomial ring over $\mathbb{Q}$.

Using the same notations as in Real Roots Counting Theorem, let $S_+$ and $S_-$ be defined from $M_1^I$ as in Notations 2.

Remark $\#(V_\mathbb{R}(I)) = \sigma(M_1^I) > 0 \iff S_+ \neq S_-.$

We can write $S_+ \neq S_-$ as a quantifier free first order formula. We denote such a formula by $I_d(a_0, \ldots, a_{d-1})$. 
Main Algorithm

Algorithm MainQE

Input: a basic quantified formula $\exists \bar{X} \phi \{ \phi \equiv (\land_{1 \leq i \leq r} f_i = 0) \land (\land_{1 \leq i \leq s} p_i > 0) \land (\land_{1 \leq i \leq t} q_i \neq 0). \}$

Output: an equivalent quantifier free formula $\psi$;

{In MainQE, we consider the dimension of a ideal generated by polynomials consiting of equalities.}

\[
\begin{align*}
1: \ & \bar{Z} = Z_1, \ldots, Z_s, \bar{W} = W_1 \ldots, W_t \leftarrow \text{new variables;} \\
2: \ & > \leftarrow \text{a term order of } T(\bar{X}, \bar{Z}, \bar{W}) \text{ such that } \bar{Z}, \bar{W} \gg \bar{X}; \\
3: \ & F \leftarrow \{ f_1, \ldots, f_r, Z_1^2 p_1 - 1, \ldots, Z_s^2 p_s - 1, W_1 q_1 - 1, \ldots, W_t q_t - 1 \}; \\
4: \ & G \leftarrow \text{a CGS of } F \text{ w.r.t. } > \text{ with parameters } Y; \quad \psi \leftarrow false; \\
5: \ & \text{for } (S, G) \in G \text{ do} \\
6: \ & \text{if } G(\bar{c}, \bar{X}, \bar{Z}, \bar{W}) \text{ is } \{0\} \text{ for } \bar{c} \in S \text{ then} \\
7: \ & \quad \psi \leftarrow \psi \lor S; \quad \{(G \cap \mathbb{R}[\bar{X}]) (\bar{c}, \bar{X}) = \{0\}.\} \\
8: \ & \text{else if } \langle G(\bar{c}, \bar{X}, \bar{Z}, \bar{W}) \rangle \text{ is zero dimensional for } \bar{c} \in S \text{ then} \\
9: \ & \quad \psi \leftarrow \psi \lor \text{ZeroDimQE}(S, G, >); \quad \{(G \cap \mathbb{R}[\bar{X}]) (\bar{c}, \bar{X}) \text{ is also zero dimensional.}\} \\
10: \ & \text{else} \\
11: \ & \quad \psi \leftarrow \psi \lor \text{NonZeroDimQE}(\phi, S, G, >); \quad \{(G \cap \mathbb{R}[\bar{X}]) (\bar{c}, \bar{X}) \text{ is not also zero dimensional.}\} \\
12: \ & \text{end if} \\
13: \ & \text{end for} \\
14: \ & \text{return } \psi;
\end{align*}
\]
**Main Algorithm**

**Algorithm ZeroDimQE**

**Input:** a component $(S, G)$ of a CGS w.r.t. a term order $>$ of $T(\tilde{X}, \tilde{Z}, \tilde{W})$ produced in MainQE s.t. $\langle G(\bar{c}, \tilde{X}, \tilde{Z}, \tilde{W}) \rangle$ is zero dimensional for $\bar{c} \in S$;

**Output:** a quantifier free formula $\psi$ s.t. $S \land \exists \tilde{X} \phi \Leftrightarrow \psi$;

{In ZeroDimQE, we use Real Root Counting Theorem.}

1: if $\langle G(\bar{c}, \tilde{X}, \tilde{Y}, \tilde{Z}) \rangle$ is $\langle 1 \rangle$ for $\bar{c} \in S$ then
2: return $false$;
3: else
4: $I \leftarrow \langle f_1', \ldots, f_{r'}' \rangle$;
   \hspace{1em} \{ $G$ has a form $\{f_i, u_j z_j^2 - p_j', v_k \tilde{W}_k - q_k' \mid 1 \leq i \leq r', 1 \leq j \leq s, 1 \leq k \leq t \}$ for $f_i', p_j', q_k' \in \mathbb{Q}[\tilde{Y}, \tilde{X}], u_i, v_i \in \mathbb{Q}[\tilde{Y}]$. Consider $\tilde{Y}$ as parameters in the following.\}
5: $\chi(X) \leftarrow \prod_{(e_1, e_2, \ldots, e_s) \in \{0,1\}^s} \chi_{h_1^e_1 h_2^e_2 \ldots h_s^e_s}(X)$ with $h_i = p_i'/u_i$ for $i = 1, \ldots, s$;
   \hspace{1em} \{For the construction of symmetric matrices, we need to use rational functions $\mathbb{Q}(\tilde{Y})$. Let $\chi(X) = X^d + a_{d-1} X^{d-1} + \ldots + a_0$ for $a_{d-1}, \ldots, a_0 \in \mathbb{Q}(\tilde{Y})$.\}
6: return $S \land l_d(a_0, \ldots, a_{d-1})$;
   \hspace{1em} \{Note also that we can easily transform the formula $l_d(a_0, \ldots, a_{d-1})$ into a formula using only polynomials. Reducing the degree, we can get a more simplified QE formula.\}
7: end if
Main Algorithm

Algorithm NonZeroDimQE

Input: a basic quantified formula $\exists \bar{X} \phi$ and a component $(S, G)$ of a CGS w.r.t. a term order $>$ of $T(\bar{X}, \bar{Z}, \bar{W})$ produced in MainQE;

Output: a quantifier free formula $\psi$ s.t. $S \wedge \exists \bar{X} \phi \leftrightarrow \psi$;

{In NonZeroDimQE, we use recursive computations.}

1: $\bar{U} \leftarrow \text{MaxIndVar}(\bar{X}, G, >); \bar{X}' \leftarrow \bar{X} \setminus \bar{U};$ \{We consider $\bar{X}'$ as new quantified variables.\}
2: if $\bar{X}' = \emptyset$ then
3: \hspace{1em} return $\text{OtherQE}(S \wedge \exists \bar{X} \phi);$ \{The equalitonal constraints are all vanish. Then we does not use CGS-QE. We use the other QE algorithm\}
4: else
5: \hspace{1em} $\phi_1 \leftarrow \text{Free}(\phi, \bar{X}'); \phi_2 \leftarrow \text{NonFree}(\phi, \bar{X}'); \varphi \leftarrow \phi_1 \wedge \text{MainQE}(\exists \bar{X}' \phi_2);$ \{Let $\varphi_1 \vee \cdots \vee \varphi_l$ be a disjunctive normal form of $\varphi.$\}
6: \hspace{1em} for $1 \leq i \leq l$ do
7: \hspace{2em} $\varphi_i^1 \leftarrow \text{Free}(\varphi_i, \bar{U}); \varphi_i^2 \leftarrow \text{NonFree}(\varphi_i, \bar{U}); \psi_i \leftarrow \varphi_i^1 \wedge \text{MainQE}(\exists \bar{U} \varphi_i^2);$ \hspace{1em} end for
8: \hspace{1em} end for
9: $\psi \leftarrow S \wedge (\psi_1 \vee \cdots \vee \psi_l);$ 
10: \hspace{1em} return $\psi;$ \{As long as the equalitonal constraints with quantifiers exists, CGS-QE do not use CAD, etc.\}
11: end if
Computation Data
We implemented our CGS-QE algorithm using “SyNRAC” on “Maple”.

We draw a comparison between the followings and our package (o).

- **SN**: SyNRAC@Maple: It is implemented CAD-QE, VS-QE.
- **Reg**: RegularChains@Maple: It is implemented CAD-QE by regular chains.
- **Res**: Resolve@Mathematica: It is implemented CAD-QE, VS-QE.
- **Red**: Reduce@Mathematica: It is implemented CAD-QE, VS-QE.
- **QEPCAD**: QEPCAD: It is implemented CAD-QE.
- **hqe**: rlhqe@RedLog@Reduce: It is implemented CGS-QE.
- **rqe**: rlqe@RedLog@Reduce: It is implemented CAD-QE, VS-QE.

All the computations were done by the computer environment with an Intel CORE i7 CPU 2.40 GHz with 64 GB memory OS Ubuntu14.04.

We show a part of our computation data.
Computation Data

1. \(\exists c_2 \exists s_2 \exists c_1 \exists s_1 (r - c_1 + l(s_1 s_2 - c_1 c_2) = 0 \land z - s_1 - l(s_1 c_2 + s_2 c_1) = 0 \land s_1^2 + c_1^2 - 1 = 0 \land s_2^2 + c_2^2 - 1 = 0)\)

2. \(\exists x \exists y \exists z (x y + a x z + y z - 1 = 0 \land x y z + x z + x y = a \land x z + y z - a x - y - 1 = 0 \land a x y = byz \land a y z = b x z)\)

3. \(\exists x \exists y \exists z (x y + a x z + y z - 1 = 0 \land x y z + x z + x y = b \land x z + y z - a x - y - 1 = 0)\)

4. \(\exists x_0 \exists x_1 \exists x_2 \exists x_3 \exists x_4 \exists x_5 \exists x_6 \exists x_7 \)

\[\sqrt{(x_7 - x_0)^2 + (x_6 - x_2)^2} = 1 \land \frac{|x_0 x_3 - x_0 x_4 + x_1 x_2 - x_1 x_3 - x_2 x_5 + x_4 x_6|}{(x_1 - x_0)(x_5 - x_0) + (x_4 - x_2)(x_3 - x_2)} = m \land \frac{|x_0 x_3 - x_0 x_4 + x_1 x_2 - x_1 x_3 - x_2 x_5 + x_4 x_6|}{(x_0 - x_5)(x_1 - x_5) + (x_2 - x_3)(x_4 - x_3)} = n \land\]

\(x_0 x_3 - x_0 x_4 + x_1 x_2 - x_1 x_3 - x_2 x_5 + x_4 x_6 \geq 0 \land (x_5 - x_0)x_4 - x_2 - (x_3 - x_2)x_1 - x_0 \geq 0 \land\)

\((x_5 - x_0)(\frac{1}{2} x_0 + \frac{1}{2} x_5 + x_7) + (x_3 - x_2)(\frac{1}{2} x_2 + \frac{1}{2} x_3 - x_6) = 0 \land\)

\((x_1 - x_5)(\frac{1}{2} x_5 + \frac{1}{2} x_1 - x_7) + (x_4 - x_3)(\frac{1}{2} x_3 + \frac{1}{2} x_4 - x_6) = 0 \land\)

\(m \geq 3 \land n \geq 3 \land \frac{|x_5 - x_0 x_4 - x_2 + x_3 - x_2 x_1 - x_0|}{2} = S\)

- The above 4 is the **Example** of Section **Motivation**.
Computation Data

Computing time is written in second.

‘0’ means that the computation time is within 1 second,

‘×’ means that the computation does not terminate within 1 hour,

‘m’ means memory exhaust and

‘e’ means the computation was crashed with some error.

<table>
<thead>
<tr>
<th></th>
<th>O</th>
<th>SN</th>
<th>Reg</th>
<th>Res</th>
<th>Red</th>
<th>QC</th>
<th>hqe</th>
<th>rqe</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>29</td>
<td>0</td>
<td>×</td>
<td>×</td>
<td>0</td>
<td>×</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>e</td>
<td>×</td>
<td>250</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>m</td>
<td>×</td>
<td>e</td>
</tr>
<tr>
<td>4</td>
<td>791</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>e</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
Conclusion
Conclusion

Today, I talked the followings:

- CGS-QE

  CGS-QE use the followings:

  - Real Root Counting
    (Improving CGS-QE, we modify “Real Root Counting”)

  - CGS

- Computation Data

Our future work is the simplification of outputs.

- CGS-QE may return the complicated outputs.
Thank you for your attention!!