Communications of JSSAC (2018)
Vol. 3, pp. 19 – 29

On Hermitian Quadratic Forms of Non-Radical Ideals*

Ryoya Fukasaku†

Tokyo university of science

(Received 23/Mar/2018 Accepted 27/Sep/2018)

Abstract

Hermitian quadratic forms play a key role in a real roots counting theory for zero-dimensional ideals. A method based on the theory has a great effect on quantifier elimination of first order formulas containing many equalities. Its essential part eliminates a block of quantifiers by the parametric Hermitian quadratic forms of the parametric zero-dimensional ideal generated by the equalities and the parametric polynomials constructing the inequalities of the given first order formula. When the parametric ideal is non-radical, the Hermitian quadratic forms are unnecessarily complicated, which produce a complicated quantifier-free formula. We may obtain a simple quantifier-free formula by the Hermitian quadratic forms of the radical. However, the computational complexity of parametric radical is high even in zero-dimensional cases. In the paper, to simplify quantifier-free formulas produced by the quantifier elimination method, we introduce minimal Hermitian quadratic forms which are applied to the theory.

1 Introduction

The concept of Hermitian Quadratic Forms (HQFs) plays a key role in a Real Roots Counting (RRC) theory for univariate polynomials. Independently in [1, 10], the RRC theory was extended to zero-dimensional ideals of multivariate polynomial rings by using the theory of Gröbner Bases (GBs). In the paper, the RRC theory is called "the Hermitian RRC theory". A Quantifier Elimination (QE) method based on the Hermitian RRC theory has a great effect on QE of First Order Formulas (FOFs) which contain many equalities. In the paper, the QE method introduced in [13] and improved in [2, 3, 4, 5] is called "the Hermitian QE method". In the Hermitian QE method, parametric HQFs play an important role to produce quantifier-free formulas (QFFs). In the paper, such QFFs are called "Hermitian QE formulas". In the section, to describe the outline of the essential part of the Hermitian QE method, we introduce $\bar{A} = A_1, \ldots, A_m$ as free variables and $\bar{X} = X_1, \ldots, X_n$ as quantified variables. Let φ be a QFF consisting only of polynomial equalities and disequalities ($=$ and $\neq$) of $\mathbb{Q}[\bar{A}]$. The essential part of the Hermitian QE method is the algorithm which computes a Hermitian QE formula from the given FOF having the following form for polynomials $f_1, \ldots, f_s, p_1, \ldots, p_t \in \mathbb{Q}[\bar{A}, \bar{X}]$:

$$\varphi(\bar{A}) \wedge \exists \bar{X} \in \mathbb{R}^n \; (f_1(\bar{A}, \bar{X}) = 0 \wedge \ldots \wedge f_s(\bar{A}, \bar{X}) = 0 \wedge p_1(\bar{A}, \bar{X}) > 0 \wedge \ldots \wedge p_t(\bar{A}, \bar{X}) > 0), \qquad (1)$$

*This work was partially supported by JSPS KAKENHI Grant Number 17K12642.

†fukasaku@rs.tus.ac.jp

where $f_1, \ldots, f_s$ and $p_1, \ldots, p_t$ satisfy the following property 1 for $\mathcal{P}_\varphi = \{\bar{a} \in \mathbb{C}^m : \varphi(\bar{a})\}$:

1. $I(\bar{a}, \bar{X}) = \langle f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X})\rangle$ is a zero-dimensional ideal of $\mathbb{C}[\bar{X}]$ for any $\bar{a} \in \mathcal{P}_\varphi$.

In the paper, we improve the algorithm introduced in [3] and implemented with several techniques of [4]. Given an admissible term order $>$ on terms consisting of $\bar{X}$, it produces a disjunction equivalent to (1). The disjunction consists of finitely many FOFs such as the following form:

$$\Phi(\bar{A}) \wedge \exists \bar{X} \in \mathbb{R}^n \ (\bigwedge_{g \in G} g(\bar{A}, \bar{X}) = 0 \wedge p_1(\bar{A}, \bar{X}) > 0 \wedge \ldots \wedge p_t(\bar{A}, \bar{X}) > 0), \tag{2}$$

where Φ is a QFF satisfying the following property 2, and G is a finite subset of $\mathbb{Q}[\bar{A}, \bar{X}]$ satisfying the following properties 3 and 4 for the product $p = \prod_{i=1}^{t} p_i$ and $\mathcal{S}_\Phi = \{\bar{a} \in \mathbb{C}^m : \Phi(\bar{a})\}$:

2. Φ consists only of polynomial equalities and disequalities of $\mathbb{Q}[\bar{A}]$, and satisfies $\mathcal{S}_\Phi \subset \mathcal{P}_\varphi$.

3. $\{g(\bar{a}, \bar{X}) : g \in G\}$ is a GB of the saturation $I'(\bar{a}, \bar{X}) = I(\bar{a}, \bar{X}) : p(\bar{a}, \bar{X})^\infty$ for any $\bar{a} \in \mathcal{S}_\Phi$.

4. Each $g \in G$ satisfies $l_g(\bar{a}) \neq 0$ for the leading coefficient $l_g = \mathrm{LC}(g) \in \mathbb{Q}[\bar{A}]$ and any $\bar{a} \in \mathcal{S}_\Phi$.

The disjunction is produced by a Comprehensive Gröbner System (CGS) of the parametric saturation ideal $\langle f_1, \ldots, f_s\rangle : p^\infty$ on $\mathcal{P}_\varphi$ w.r.t. $>$ considering $\bar{A}$ as parameters (See Definition 6 - Remark 8). The concept of CGSs was introduced in [12] as a powerful tool for parametric ideals. We consider it as a system of parametric GBs. With a series of resent results of [6, 7, 8, 9, 11], we now have efficient CGS computation algorithms. Moreover, as a result of [5], we can efficiently compute CGSs of parametric zero-dimensional saturation.

Let $p_e = \prod_{i=1}^{t} p_i^{e_i}$ for $e = (e_1, \ldots, e_t) \in \{0, 1\}^t$. The algorithm computes a Hermitian QE formula $\Phi(\bar{A}) \wedge \phi(\bar{A})$ of the FOF (2) such that $\phi(\bar{a})$ is equivalent to

$$\sum_{e \in \{0,1\}^t} \mathrm{sign}(H^{I'(\bar{a},\bar{X})}_{p_e(\bar{a},\bar{X})}) > 0 \qquad (\text{Let } H^{\bar{a}}_e = H^{I'(\bar{a},\bar{X})}_{p_e(\bar{a},\bar{X})}) \tag{3}$$

for any $\bar{a} \in \mathcal{S}_\Phi \cap \mathbb{R}^m$, where each $\mathrm{sign}(H^{\bar{a}}_e)$ is the signature of the HQF of the polynomial $p_e(\bar{a}, \bar{X})$ and the ideal $I'(\bar{a}, \bar{X})$ (See Definition 1 - Theorem 5). The FOF (2) has the properties 2 - 4. So, using G, we are able to compute each parametric HQF, which is the uniform representation of the HQF $H^{\bar{a}}_e$ for any $\bar{a} \in \mathcal{S}_\Phi \cap \mathbb{R}^m$ (See Remark 9, 10). ϕ are produced by the parametric HQFs (See Proposition 11). When $I'(\bar{a}, \bar{X})$ is not radical, unfortunately, the parametric HQFs are unnecessarily complicated, which produces a very complicated ϕ (See Example 12). We may obtain simple ϕ by using the parametric HQF of its radical. However, the computational complexity of parametric radical is high even in zero-dimensional cases.

In the paper, we introduce a concept of minimal HQFs (See Definition 13 - Remark 14), and the Hermitian RRC theory with minimal HQFs. We then show that the concept of minimal HQFs enables us to simplify unnecessarily complicated Hermitian QE formulas without the computations of parametric radical ideals. (See Example 21).

The paper is organized as follow: In Section 2, we give a quick review of the essential part of the Hermitian QE method with an innovative improvement of [3] and several implementation techniques of [4]. More precisely, we describe the Hermitian RRC theory with HQFs in Subsection 2.1, describe CGSs in Subsection 2.2, and describe the essential part in Subsection 2.3. In Section 3, we show the main theorem of the paper.

2 Theoretical Background

We use the following symbols: $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the set of natural numbers, rational numbers, real numbers and complex numbers respectively. $(M)_{(i,j)}$, $\mathrm{rank}(M)$, $\mathrm{tr}(M)$ and $\det(M)$ denote the (i, j)-entry, the rank, the trace and the determinant of a square matrix M respectively. For a real symmetric square matrix H, $\mathrm{sign}(H)$ denotes the number such that "the number of the positive eigenvalues of H" minus "the number of the negative eigenvalues of H". Identifying H with its quadratic form, we obtain that $\mathrm{sign}(H)$ is equal to the signature of H. $\bar{A}$ and $\bar{X}$ denote $A_1, \ldots, A_m$ and $X_1, \ldots, X_n$ respectively. $T(\bar{X})$ denotes a set of terms in $\bar{X}$. Given a term order on $T(\bar{X})$, $\mathrm{LM}(f)$, $\mathrm{LT}(f)$ and $\mathrm{LC}(f)$ denote the leading monomial, the leading term and the leading coefficient of $f \in \mathbb{Q}[\bar{A}, \bar{X}]$ respectively. We have to note $\mathrm{LM}(f) = \mathrm{LC}(f)\mathrm{LT}(f)$ and $\mathrm{LC}(f) \in \mathbb{Q}[\bar{A}]$. $V_{\mathbb{R}}(F)$ and $V_{\mathbb{C}}(F)$ denote the variety of a set $F \subset R[\bar{X}]$ over $\mathbb{R}$ and $\mathbb{C}$ respectively. That is, we obtain

$$V_{\mathbb{R}}(F) = \{\bar{x} \in \mathbb{R}^n : \forall f \in F (f(\bar{x}) = 0)\}, \quad V_{\mathbb{C}}(F) = \{\bar{x} \in \mathbb{C}^n : \forall f \in F (f(\bar{x}) = 0)\}.$$

$\#(S)$ denotes the cardinality of a finite set S.

2.1 Hermitian Quadratic Forms

In the subsection, we give the Hermitian RRC theory shown independently in [1, 10] and show a theorem implying the essential part of [3, 4]. First of all, we define HQFs.

Definition 1 *Let $p \in \mathbb{R}[\bar{X}]$, I be a zero-dimensional ideal of $\mathbb{R}[\bar{X}]$. Considering the residue class ring $\mathbb{R}[\bar{X}]/I$ as a vector space, let $\{v_1, \ldots, v_d\}$ be its basis. For $1 \le i, j \le d$, we give the linear map*

$$h^I_{(p,i,j)} : \mathbb{R}[\bar{X}]/I \to \mathbb{R}[\bar{X}]/I \ ; \ g \mapsto p v_i v_j g.$$

Moreover, we define the d-th real symmetric matrix H^I_p such that each $(H^I_p)_{(i,j)}$ satisfies

$$(H^I_p)_{(i,j)} = \mathrm{tr}(h^I_{(p,i,j)}).$$

The d-th real symmetric matrix H^I_p is called the HQF *of p and I.*

Remark 2 *With the same symbols as Definition 1,* $\mathrm{RT}(G)$ *denotes the set of the reduced terms w.r.t. a GB G of I. That is,* $\mathrm{RT}(G) = \{t \in T(\bar{X}) : \forall g \in G$ (t *is indivisible by* $\mathrm{LT}(g)$)$\}$. $\mathrm{RT}(G)$ *plays a role as a basis $\{v_1, \ldots, v_d\}$ of $\mathbb{R}[\bar{X}]/I$. The k-th column of $h^I_{(p,i,j)}$ is produced by the reminder of $p v_i v_j v_k$ on division by G. $(H^I_p)_{(i,j)}$ is equal to the sum of the diagonal entries of $h^I_{(p,i,j)}$.*

We give the Hermitian RRC theory with HQFs shown independently in [1, 10].

Theorem 3 *For $p \in \mathbb{R}[\bar{X}]$ and a zero-dimensional ideal I of $\mathbb{R}[\bar{X}]$,*

$$\begin{aligned} \mathrm{rank}(H^I_p) &= \#(\{\bar{x} \in V_{\mathbb{C}}(I) : p(\bar{x}) \neq 0\}), & (4)\\ \mathrm{sign}(H^I_p) &= \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) < 0\}). & (5) \end{aligned}$$

We obtain the corollary which follows from Theorem 3 because HQFs are real symmetric.

Corollary 4 *The characteristic polynomial of H^I_p is denoted by $\mathfrak{C}^I_p$. We suppose*

$$\begin{aligned} \mathfrak{C}^I_p(Y) &= b^+_d Y^d + b^+_{d-1} Y^{d-1} + \cdots + b^+_0 \in \mathbb{R}[Y],\\ \mathfrak{C}^I_p(-Y) &= b^-_d Y^d + b^-_{d-1} Y^{d-1} + \cdots + b^-_0 \in \mathbb{R}[Y]. \end{aligned}$$

B^{ϱ} denotes the number of sign changes of the coefficient sequence $(b^{\varrho}_d, b^{\varrho}_{d-1}, \dots, b^{\varrho}_0)$ for $\varrho \in \{+,-\}$ (0 is ignored in the sequence). Since each eigenvalue of H^I_p is real, Theorem 3 and Descartes' sign rule imply

$$B^+ - B^- = \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) < 0\}).$$

We conclude the subsection with the theorem which follows from Theorem 3, Corollary 4 and [3] (Corollary 3 - Theorem 5).

Theorem 5 *Let $p_1, \dots, p_t \in \mathbb{R}[\bar{X}]$, I be a zero-dimensional ideal of $\mathbb{R}[\bar{X}]$. Let $\bar{Z} = Z_1, \dots, Z_t$, $p = \prod_{i=1}^t p_i$, and $J = I + \langle 1 - p_1 Z_1^2, \dots, 1 - p_t Z_t^2 \rangle \subset \mathbb{R}[\bar{X}, \bar{Z}]$. Then, we obtain*

$$\#V_{\mathbb{R}}(J) = 2^t \#(\{\bar{x} \in V_{\mathbb{R}}(I) : \bigwedge_{i=1}^t p_i(\bar{x}) > 0\}).$$

by [3] (Corollary 3). Let $I' = I : p^{\infty}$ and $p_e = \prod_{i=1}^t p_i^{e_i}$ for $e = (e_1, \dots, e_t) \in \{0,1\}^t$. We note that I' is equal to the elimination ideal $J \cap \mathbb{R}[\bar{X}]$. Thus, [3] (Corollary 4 and Theorem 5) implies

$$\mathfrak{C}^J_1(Y) = c \prod_{e \in \{0,1\}^t} \mathfrak{C}^{I'}_{p_e}(Y)$$

for some non-zero constant c. For $e \in \{0,1\}^t$, B^+_e and B^-_e denote the number of sign changes in the coefficient sequences of $\mathfrak{C}^{I'}_{p_e}(Y)$ and $\mathfrak{C}^{I'}_{p_e}(-Y)$ respectively. Then, Theorem 3 and Corollary 4 imply

$$0 < \sum_{e \in \{0,1\}^t} (B^+_e - B^-_e) \Leftrightarrow 0 < \#(\{\bar{x} \in V_{\mathbb{R}}(I) : \bigwedge_{i=1}^t p_i(\bar{x}) > 0\}).$$

2.2 Comprehensive Gröbner Systems

We describe CGSs in the subsection. Before defining CGSs, we define algebraic partitions.

Definition 6 *Let $\mathcal{P}$ be a subset of $\mathbb{C}^m$ and $\mathcal{S}_1, \dots, \mathcal{S}_q$ be subsets of $\mathcal{P}$. When the properties such that $\bigcup_{i=1}^q \mathcal{S}_i = \mathcal{P}$ and $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$ for $1 \le i \ne j \le q$ and $\mathcal{S}_i = V_{\mathbb{C}}(S_1) \setminus V_{\mathbb{C}}(S_2)$ with finite $S_1, S_2 \subset \mathbb{Q}[\bar{A}]$ for $1 \le i \le q$ are satisfied, $\{\mathcal{S}_1, \dots, \mathcal{S}_q\}$ is called an* algebraic partition *of $\mathcal{P}$.*

Definition 7 *Let $\mathcal{P} \subset \mathbb{C}^m$ and $\mathcal{S}_1, \dots, \mathcal{S}_q \subset \mathcal{P}$. Let $F, G_1, \dots, G_q$ be finite subsets of $\mathbb{Q}[\bar{A}, \bar{X}]$. Let $\succ$ be a term order on $T(\bar{X})$. When $\mathcal{G} = \{(\mathcal{S}_1, G_1), \dots, (\mathcal{S}_q, G_q)\}$ satisfies the properties such that*

- *$\{\mathcal{S}_1, \dots, \mathcal{S}_q\}$ is an algebraic partition of $\mathcal{P}$, and*
- *$G_i(\bar{a}, \bar{X}) = \{g(\bar{a}, \bar{X}) : g \in G_i\}$ is a GB of $\langle F(\bar{a}, \bar{X}) \rangle \subset \mathbb{C}[\bar{X}]$ w.r.t. $\succ$ for each $\bar{a} \in \mathcal{S}_i$, and*
- *any $g \in G_i$ satisfies $LC(g)(\bar{a}) \ne 0$ for each $\bar{a} \in \mathcal{S}_i$,*

$\mathcal{G}$ is called a CGS *of $\langle F \rangle$ on $\mathcal{P}$ with parameters $\bar{A}$ w.r.t. $\succ$. In addition, each $\mathcal{S}_i$ a* segment*, and each G_i a* parametric GB.

Remark 8 *With the same symbols as (1), let $\mathcal{G}$ be a CGS of $\langle f_1, \dots, f_s \rangle : p^{\infty}$ on $\mathcal{P}_{\varphi}$ with parameters $\bar{A}$ w.r.t. $\succ$ and $\Phi_{\mathcal{S}}$ be a defining formula of $\mathcal{S}$ for $(\mathcal{S}, G) \in \mathcal{G}$. Then, the FOF (1) is equivalent to*

$$\bigvee_{(\mathcal{S},G) \in \mathcal{G}} \left(\Phi_{\mathcal{S}} \wedge \exists \bar{X} \in \mathbb{R}^n \left(\bigwedge_{g \in G} g = 0 \wedge \bigwedge_{i=1}^t p_i > 0 \right) \right).$$

Moreover, each $\Phi_{\mathcal{S}}$ satisfies the property 2, and each G satisfies the properties 3, 4 of (2).

Remark 9 *With the same symbols as the properties 2 - 4 of (2), let $s \in \mathbb{Q}[\bar{A}, \bar{X}]$. For the reminder of $s(\bar{a}, \bar{X})$ on division by $G(\bar{a}, \bar{X})$, its uniform representation $s' \in \mathbb{Q}(\bar{A})[\bar{X}]$ is produced by the reminder of s on division by G over $\mathbb{Q}(\bar{A})[\bar{X}]$ such that the coefficient field is the rational function field $\mathbb{Q}(\bar{A})$. Because G has the properties 3, 4 of (2). More precisely, each coefficient of s' has a form s_1/s_2 such that $s_1, s_2 \in \mathbb{Q}[\bar{A}]$ satisfy $s_2(\bar{a}) \neq 0$.*

Remark 10 *We use the same symbols as the properties 2 - 4 of (2). The properties 2 - 4 of (2) imply that $\langle G(\bar{a}, \bar{X})\rangle$ is zero-dimensional and $\mathrm{RT}(G(\bar{a}, \bar{X}))$ is invariant. In addition, we have also Remark 2 and 9. Therefore, we can compute the uniform representation $H_{p_e}^{\langle G\rangle}$ of the HQF of $p_e(\bar{a}, \bar{X})$ and $\langle G(\bar{a}, \bar{X})\rangle$, whose each entry has the form s_1/s_2 such that $s_1, s_2 \in \mathbb{Q}[\bar{A}]$ satisfy $s_2(\bar{a}) \neq 0$. In the paper, the symmetric matrix $H_{p_e}^{\langle G\rangle}$ is called the* parametric HQF *of p_e and $\langle G\rangle$. More precisely, each entry also has the form s_1/s_2 such that $s_1, s_2 \in \mathbb{Q}[\bar{A}]$ satisfy $s_2(\bar{a}) \neq 0$.*

2.3 Hermitian Quantifier Elimination

We give the essential part of the Hermitian QE method with [3, 4], which follows from Theorem 5.

Proposition 11 *With the same symbols as the properties 2 - 4 of (2), let $p_e = \prod_{i=1}^{t} p_i^{e_i}$ for $e = (e_1, \ldots, e_t) \in \{0, 1\}^t$. Since Remark 10 implies that each $\mathfrak{C}_{p_e}^{\langle G\rangle}$ has rational functions of $\mathbb{Q}(\bar{A})$ as its coefficients, we suppose*

$$\begin{aligned}
\mathfrak{C}_{p_e}^{\langle G\rangle}(Y) &= b_d^+ Y^d + b_{d-1}^+ Y^{d-1} + \cdots + b_0^+ \in \mathbb{Q}(\bar{A})[Y],\\
\mathfrak{C}_{p_e}^{\langle G\rangle}(-Y) &= b_d^- Y^d + b_{d-1}^- Y^{d-1} + \cdots + b_0^- \in \mathbb{Q}(\bar{A})[Y].
\end{aligned}$$

Let $S_e^{\varrho} = (b_d^{\varrho}, \ldots, b_0^{\varrho})$ for $\varrho \in \{+, -\}$. Let $B_e^{\varrho}(\bar{a})$ be the number of sign changes in $S_e^{\varrho}(\bar{a}) = (b_d^{\varrho}(\bar{a}), \ldots, b_0^{\varrho}(\bar{a}))$ for $\bar{a} \in \mathcal{S}_\Phi \cap \mathbb{R}^m$. Using the numerator and denominator polynomials of S_e^{ϱ}, we compute the QFF $\phi(\bar{A})$ such that $\phi(\bar{a})$ is equivalent to

$$0 < \sum_{e \in \{0,1\}^t} (B_e^+(\bar{a}) - B_e^-(\bar{a}))$$

for $\bar{a} \in \mathcal{S}_\Phi \cap \mathbb{R}^m$. Then, Theorem 5 implies that $\Phi \wedge \phi$ is equivalent to (2).

Although we can obtain a Hermitian QE formula of (2) based on Proposition 11, the Hermitian QE formula is unnecessarily complicated in the case such that the parametric ideal is not radical.

Example 12 *We consider the FOF as like $A \neq 0 \wedge \exists X \in \mathbb{R}\ ((X - A)^2 = 0 \wedge X > 0)$. We treat $I = \langle (X - A)^2\rangle : X^\infty$ with a parameter A. Computing a CGS of I on $\mathcal{S} = \{a \in \mathbb{C} : a \neq 0\}$ w.r.t the term order $\succ$ satisfying $X^0 \prec X^1 \prec \cdots$ with a parameter A, we obtain $\{(\mathcal{S}, \{(X - A)^2\})\}$. Let $G^I = \{(X - A)^2\}$. Since $\mathrm{RT}(G^I) = \{1, X\}$, we obtain*

$$H_1^{\langle G^I\rangle} = \begin{pmatrix} 2 & 2A \\ 2A & 2A^2 \end{pmatrix},\ H_X^{\langle G^I\rangle} = \begin{pmatrix} 2A & 2A^2 \\ 2A^2 & 2A^3 \end{pmatrix}.$$

We have theirs characteristic polynomials

$$\mathfrak{C}_1^{\langle G^I\rangle} = Y^2 - 2(A^2 + 1)Y,\ \ \mathfrak{C}_X^{\langle G^I\rangle} = Y^2 - 2A(A^2 + 1)Y.$$

Let $b_1 = -2(A^2 + 1), b_X = -2A(A^2 + 1) \in \mathbb{Q}[A]$. Then, we obtain the Hermitian QE formula

$$A \neq 0 \wedge b_1 < 0 \wedge b_X < 0.$$

Because, for any ideal I of $\mathbb{R}[\bar{X}]$ and any polynomial p of $\mathbb{R}[\bar{X}]$ with $I : p^\infty = I$, Theorem 3 implies

$$\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) > 0\} \neq \emptyset \Leftrightarrow \left(\mathrm{sign}(H_1^I) > 0 \wedge \left(\bigvee_{0 \le k < \mathrm{sign}(\mathrm{H}_1^\mathrm{I})} (\mathrm{sign}(H_p^I) = \mathrm{sign}(H_1^I) - k)\right)\right).$$

Meanwhile, we consider the parametric radical $J = \sqrt{I}$. We obtain $\{(\mathcal{S}, \{X - A\})\}$ as a CGS of J over $\mathcal{S}$ w.r.t. $>$. Let $G^J = \{X - A\}$. Since $\mathrm{RT}(G^J) = \{1\}$, we obtain

$$H_1^{\langle G^J \rangle} = \left(\begin{array}{c} 1 \end{array} \right),\ H_X^{\langle G^J \rangle} = \left(\begin{array}{c} A \end{array} \right).$$

Moreover, we have theirs characteristic polynomials $\mathfrak{C}_1^{\langle G^J \rangle} = Y - 1$, $\mathfrak{C}_X^{\langle G^J \rangle} = Y - A$. Thus, we obtain also the simple Hermitian QE formula $A \neq 0 \wedge -A < 0$ by using the parametric radical.

3 Minimal Hermitian Quadratic Forms

In cases such as Example 12, the HQFs are unnecessarily complicated, which produces a very complicated Hermitian QE formula. In the section, we introduce a concept of minimal HQF, show the Hermitian RRC theory with minimal HQFs, and reconsider Example 12. In more detail, we prove the main theorem in Subsection 3.1 and reconsider Example 12 in Subsection 3.2. First of all, we introduce the definition of minimal HQFs.

Definition 13 *Let $p \in \mathbb{R}[\bar{X}]$, I be a zero-dimensional ideal of $\mathbb{R}[\bar{X}]$ and $r = \mathrm{rank}(H_p^I)$. We assume*

$$r \neq 0. \tag{6}$$

$H_p^I(C)$ denotes the r-th principal matrix of H_p^I such that each $(H_p^I(C))_{(i,j)}$ satisfies

$$(H_p^I(C))_{(i,j)} = (H_p^I)_{(C_i, C_j)}$$

for $C = (C_1, \ldots, C_r) \in \mathbb{N}^r$ with $1 \le C_1 < \ldots < C_r \le d$. We choose $c = (c_1, \ldots, c_r) \in \mathbb{N}^r$ with

$$\mathrm{rank}(H_p^I(c)) = r \tag{7}$$

and $1 \le c_1 < \ldots < c_r \le d$. Then, the principal matrix $H_p^I(c)$ is called a minimal HQF *of H_p^I.*

Remark 14 *The known fact of linear algebra implies that there are some $c = (c_1, \ldots, c_r) \in \mathbb{N}^r$ with (7) and $1 \le c_1 < \ldots < c_r \le d$ because we assume (6).*

We show the Hermitian RRC theory with minimal HQFs as the main theorem.

Theorem 15 (Main Theorem) *Using the same symbols as Definition 13, we obtain the property*

$$\mathrm{sign}(H_p^I(c)) \quad = \quad \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) < 0\}).$$

Theorem 15 implies the corollary because minimal HQFs also are real symmetric.

Corollary 16 *The characteristic polynomial of $H_p^I(c)$ is denoted by ${}^c\mathfrak{D}_p^I$. In addition, we suppose*

$$\begin{aligned} {}^c\mathfrak{D}_p^I(Y) \quad &= \quad \gamma_r^+ Y^r + \cdots + \gamma_0^+ \in \mathbb{R}[Y], \\ {}^c\mathfrak{D}_p^I(-Y) \quad &= \quad \gamma_r^- Y^r + \cdots + \gamma_0^- \in \mathbb{R}[Y]. \end{aligned}$$

Let Γ^ϱ be the number of sign changes in the coefficient sequence $(\gamma_r^\varrho, \ldots, \gamma_0^\varrho)$ for $\varrho \in \{+, -\}$. Then,

$$\Gamma^+ - \Gamma^- = \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) < 0\})$$

follows from Theorem 15 because all eigenvalues of $H_p^I(c)$ are real.

3.1 Proof of Main Theorem

We use the same symbols as Definition 1, 13, Theorem 3, 15. $\bar{z}'$ denotes the conjugate of $\bar{z} \in \mathbb{C}^m$. We suppose that $\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) \neq 0\}$ and $\{\bar{z} \in V_{\mathbb{C}}(I) \setminus V_{\mathbb{R}}(I) : p(\bar{z}) \neq 0\}$ have the following forms:

$$\begin{aligned} \{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) \neq 0\} &= \{\bar{x}_1, \ldots, \bar{x}_\mu\}, \\ \{\bar{z} \in V_{\mathbb{C}}(I) \setminus V_{\mathbb{R}}(I) : p(\bar{z}) \neq 0\} &= \{\bar{z}_1, \bar{z}_1', \ldots, \bar{z}_\nu, \bar{z}_\nu'\}. \end{aligned}$$

Each σ_k denotes the multiplicity of $\bar{x}_k$ and each ς_k the multiplicity of $\bar{z}_k, \bar{z}_k'$. We start the subsection (that is, the proof of Theorem 15) with the lemma which is used in [10] (Theorem 2.1).

Lemma 17 *Stickelberger's Theorem implies that each entry $(H_p^I)_{(i,j)}$ is equal to*

$$\sum_{k=1}^{\mu} \sigma_k p(\bar{x}_k) v_i(\bar{x}_k) v_j(\bar{x}_k) + \sum_{k=1}^{\nu} (\varsigma_k p(\bar{z}_k) v_i(\bar{z}_k) v_j(\bar{z}_k) + \varsigma_k p(\bar{z}_k') v_i(\bar{z}_k') v_j(\bar{z}_k')).$$

Let $u_i = v_{c_i}$ for $1 \leq i \leq r$. The following lemma follows from Lemma 17.

Lemma 18 *Lemma 17 implies that each entry $(H_p^I(c))_{(i,j)}$ is equal to*

$$\sum_{k=1}^{\mu} \sigma_k p(\bar{x}_k) u_i(\bar{x}_k) u_j(\bar{x}_k) + \sum_{k=1}^{\nu} (\varsigma_k p(\bar{z}_k) u_i(\bar{z}_k) u_j(\bar{z}_k) + \varsigma_k p(\bar{z}_k') u_i(\bar{z}_k') u_j(\bar{z}_k')).$$

The imaginary unit is denoted by $\mathbb{I}$. We introduce the real numbers $p_k^{\mathrm{R}}, p_k^{\mathrm{I}}, u_{(i,k)}^{\mathrm{R}}, u_{(i,k)}^{\mathrm{I}} \in \mathbb{R}$ satisfying

$$\varsigma_k p(\bar{z}_k) = (p_k^{\mathrm{R}} + \mathbb{I} p_k^{\mathrm{I}})^2, \quad u_i(\bar{z}_k) = u_{(i,k)}^{\mathrm{R}} + \mathbb{I} u_{(i,k)}^{\mathrm{I}},$$

for $1 \leq k \leq \nu$, $1 \leq i \leq r$. Noting that (4) implies $r = \mu + 2\nu$, we introduce the r-th matrix

$$U = \begin{pmatrix} u_1(\bar{x}_1) & \cdots & u_r(\bar{x}_1) \\ \vdots & & \vdots \\ u_1(\bar{x}_\mu) & \cdots & u_r(\bar{x}_\mu) \\ p_1^{\mathrm{R}} u_{(1,1)}^{\mathrm{R}} - p_1^{\mathrm{I}} u_{(1,1)}^{\mathrm{I}} & \cdots & p_1^{\mathrm{R}} u_{(r,1)}^{\mathrm{R}} - p_1^{\mathrm{I}} u_{(r,1)}^{\mathrm{I}} \\ p_1^{\mathrm{R}} u_{(1,1)}^{\mathrm{I}} + p_1^{\mathrm{I}} u_{(1,1)}^{\mathrm{R}} & \cdots & p_1^{\mathrm{R}} u_{(r,1)}^{\mathrm{I}} + p_1^{\mathrm{I}} u_{(r,1)}^{\mathrm{R}} \\ \vdots & & \vdots \\ p_\nu^{\mathrm{R}} u_{(1,\nu)}^{\mathrm{R}} - p_\nu^{\mathrm{I}} u_{(1,\nu)}^{\mathrm{I}} & \cdots & p_\nu^{\mathrm{R}} u_{(r,\nu)}^{\mathrm{R}} - p_\nu^{\mathrm{I}} u_{(r,\nu)}^{\mathrm{I}} \\ p_\nu^{\mathrm{R}} u_{(1,\nu)}^{\mathrm{I}} + p_\nu^{\mathrm{I}} u_{(1,\nu)}^{\mathrm{R}} & \cdots & p_\nu^{\mathrm{R}} u_{(r,\nu)}^{\mathrm{I}} + p_\nu^{\mathrm{I}} u_{(r,\nu)}^{\mathrm{R}} \end{pmatrix}.$$

In addition, we introduce the r-th diagonal matrix V whose the diagonal entry are

$$\sigma_1 p(\bar{x}_1), \ldots, \sigma_\mu p(\bar{x}_\mu), 2, -2, \cdots, 2, -2.$$

${}^{\mathrm{t}}H$ denotes the transpose of a matrix H. Then, we obtain the following proposition.

Proposition 19 $H_p^I(c) = {}^{\mathrm{t}}UVU$.

Proof: Lemma 18 implies that each entry $(H_p^I(c))_{(i,j)}$ is equal to

$$\begin{aligned} \sum_{k=1}^{\mu} \sigma_k p(\bar{x}_k) u_i(\bar{x}_k) u_j(\bar{x}_k) + \sum_{k=1}^{\nu} ((p_k^{\mathrm{R}} + \mathbb{I} p_k^{\mathrm{I}})^2 (u_{(i,k)}^{\mathrm{R}} + \mathbb{I} u_{(i,k)}^{\mathrm{I}})(u_{(j,k)}^{\mathrm{R}} + \mathbb{I} u_{(j,k)}^{\mathrm{I}}) + \\ (p_k^{\mathrm{R}} - \mathbb{I} p_k^{\mathrm{I}})^2 (u_{(i,k)}^{\mathrm{R}} - \mathbb{I} u_{(i,k)}^{\mathrm{I}})(u_{(j,k)}^{\mathrm{R}} - \mathbb{I} u_{(j,k)}^{\mathrm{I}})). \end{aligned}$$

Since V is diagonal, each entry $({}^{\mathrm{t}}UVU)_{(i,j)}$ *has the form as like*

$$\sum_{k=1}^{r}({}^{\mathrm{t}}U)_{(i,k)}(V)_{(k,k)}(U)_{(k,j)} = \sum_{k=1}^{r}(U)_{(k,i)}(V)_{(k,k)}(U)_{(k,j)}.$$

Therefore, each entry $({}^{\mathrm{t}}UVU)_{(i,j)}$ *is equal to*

$$\sum_{k=1}^{\mu}\sigma_k p(\bar{x}_k)u_i(\bar{x}_k)u_j(\bar{x}_k) + \sum_{k=1}^{\nu}(2(p_k^{\mathrm{R}}u_{(i,k)}^{\mathrm{R}} - p_k^{\mathrm{I}}u_{(i,k)}^{\mathrm{I}})(p_k^{\mathrm{R}}u_{(j,k)}^{\mathrm{R}} - p_k^{\mathrm{I}}u_{(j,k)}^{\mathrm{I}}) - 2(p_k^{\mathrm{R}}u_{(i,k)}^{\mathrm{I}} + p_k^{\mathrm{I}}u_{(i,k)}^{\mathrm{R}})(p_k^{\mathrm{R}}u_{(j,k)}^{\mathrm{I}} + p_k^{\mathrm{I}}u_{(j,k)}^{\mathrm{R}})).$$

Using the above expression of the entry $(H_p^I(c))_{(i,j)}$ *and* $({}^{\mathrm{t}}UVU)_{(i,j)}$*, we introduce*

$$\begin{aligned}
\beta_k &= (p_k^{\mathrm{R}} + \mathbb{I}p_k^{\mathrm{I}})^2(u_{(i,k)}^{\mathrm{R}} + \mathbb{I}u_{(i,k)}^{\mathrm{I}})(u_{(j,k)}^{\mathrm{R}} + \mathbb{I}u_{(j,k)}^{\mathrm{I}}) + (p_k^{\mathrm{R}} - \mathbb{I}p_k^{\mathrm{I}})^2(u_{(i,k)}^{\mathrm{R}} - \mathbb{I}u_{(i,k)}^{\mathrm{I}})(u_{(j,k)}^{\mathrm{R}} - \mathbb{I}u_{(j,k)}^{\mathrm{I}}),\\
\gamma_k &= 2(p_k^{\mathrm{R}}u_{(i,k)}^{\mathrm{R}} - p_k^{\mathrm{I}}u_{(i,k)}^{\mathrm{I}})(p_k^{\mathrm{R}}u_{(j,k)}^{\mathrm{R}} - p_k^{\mathrm{I}}u_{(j,k)}^{\mathrm{I}}) - 2(p_k^{\mathrm{R}}u_{(i,k)}^{\mathrm{I}} - p_k^{\mathrm{I}}u_{(i,k)}^{\mathrm{R}})(p_k^{\mathrm{R}}u_{(j,k)}^{\mathrm{I}} - p_k^{\mathrm{I}}u_{(j,k)}^{\mathrm{R}}).
\end{aligned}$$

Then, we obtain $\beta_k = \gamma_k$ *for* $1 \le k \le \nu$*. Therefore, the assertion is satisfied.* □

In addition, we show the following proposition by using the property (7) of minimal HQFs.

Proposition 20 $\mathrm{rank}(U) = r$.

Proof: Let E_μ *be the* μ*-th identity matrix. Moreover, we introduce the matrices* P_k *and* J *satisfying*

$$P_k = \begin{pmatrix} p_k^{\mathrm{R}} & -p_k^{\mathrm{I}} \\ p_k^{\mathrm{I}} & p_k^{\mathrm{R}} \end{pmatrix}, \quad J = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -\mathbb{I} & \mathbb{I} \end{pmatrix}$$

for $1 \le k \le \nu$*. In addition, we introduce the r-th matrices* U_1*,* U_2 *and* U_3 *which have the forms*

$$U_1 = \begin{pmatrix} E_\mu & 0 & \cdots & 0 \\ 0 & P_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & P_\nu \end{pmatrix}, \quad U_2 = \begin{pmatrix} E_\mu & 0 & \cdots & 0 \\ 0 & J & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J \end{pmatrix},$$

$$U_3 = \begin{pmatrix} u_1(\bar{x}_1) & \cdots & u_r(\bar{x}_1) \\ \vdots & & \vdots \\ u_1(\bar{x}_\mu) & \cdots & u_r(\bar{x}_\mu) \\ u_{(1,1)}^{\mathrm{R}} + \mathbb{I}u_{(1,1)}^{\mathrm{I}} & \cdots & u_{(r,1)}^{\mathrm{R}} + \mathbb{I}u_{(r,1)}^{\mathrm{I}} \\ u_{(1,1)}^{\mathrm{R}} - \mathbb{I}u_{(1,1)}^{\mathrm{I}} & \cdots & u_{(r,1)}^{\mathrm{R}} - \mathbb{I}u_{(r,1)}^{\mathrm{I}} \\ \vdots & & \vdots \\ u_{(1,\nu)}^{\mathrm{R}} + \mathbb{I}u_{(1,\nu)}^{\mathrm{I}} & \cdots & u_{(r,\nu)}^{\mathrm{R}} + \mathbb{I}u_{(r,\nu)}^{\mathrm{I}} \\ u_{(1,\nu)}^{\mathrm{R}} - \mathbb{I}u_{(1,\nu)}^{\mathrm{I}} & \cdots & u_{(r,\nu)}^{\mathrm{R}} - \mathbb{I}u_{(r,\nu)}^{\mathrm{I}} \end{pmatrix}.$$

We have to note $U = U_1U_2U_3$*. In addition, we obtain* $\det(U_1) = \prod_{k=1}^{\nu}((p_k^{\mathrm{R}})^2 + (p_k^{\mathrm{I}})^2)$ *and* $\det(U_2) = \mathbb{I}^\nu$*. Therefore, we obtain also*

$$\det(U_1) \ne 0, \quad \det(U_2) \ne 0$$

since $\{\bar{z}_1, \bar{z}_1', \ldots, \bar{z}_\nu, \bar{z}_\nu'\} = \{\bar{z} \in V_{\mathbb{C}}(I) \setminus V_{\mathbb{R}}(I) : p(\bar{z}) \neq 0\}$*. Let* U_4 *be the r-th diagonal matrix having*

$$\sigma_1 p(\bar{x}_1), \ldots, \sigma_\mu p(\bar{x}_\mu), \varsigma_1 p(\bar{z}_1), \varsigma_1 p(\bar{z}_1'), \ldots, \varsigma_\nu p(\bar{z}_\nu), \varsigma_\nu p(\bar{z}_\nu')$$

as its diagonal entries. Lemma 18 implies $H_p^I(c) = {}^{\mathrm{t}}U_3 U_4 U_3$*, so the property (7) give the property*

$$\det(U_3) \neq 0.$$

Thereby, we obtain $\mathrm{rank}(U_1) = r$*,* $\mathrm{rank}(U_2) = r$ *and* $\mathrm{rank}(U_3) = r$*. Since we have also* $U = U_1 U_2 U_3$ *shown in the above, the assertion is satisfied.* □

We conclude the subsection with the proof of Theorem 15 by using Proposition 19, 20.

Proof of Theorem 15: Proposition 19, 20 and Sylvester's law of inertia imply

$$\mathrm{sign}(H_h^I(c)) = \mathrm{sign}(V).$$

Because V is the diagonal matrix with the diagonal entries $\sigma_1 p(\bar{x}_1), \ldots, \sigma_\mu p(\bar{x}_\mu), 2, -2, \cdots, 2, -2$,

$$\mathrm{sign}(V) = \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) : p(\bar{x}) < 0\}).$$

Therefore, we obtain the claim. □

3.2 Application

We reconsider Example 12 in the subsection.

Example 21 *With the same symbols as Example 12, we have to note that* $H_1^{\langle G(a,X)\rangle}$ *and* $H_X^{\langle G^I(a,X)\rangle}$ *satisfy the assumption (6) for any* $a \in \mathcal{S}$*. In addition, we have to note also that theirs determinants are equal to* 0 *for any* $a \in \mathcal{S}$*. First of all, by using the script* $(1) \in \mathbb{N}^1$ *we compute*

$$H_1^{\langle G^I\rangle}(1) = \begin{pmatrix} 2 \end{pmatrix},\ H_X^{\langle G^I\rangle}(1) = \begin{pmatrix} 2A \end{pmatrix}.$$

We compute theirs characteristic polynomials

$$\mathfrak{D}_1^{\langle G^I\rangle}(Y) = Y - 2, \quad \mathfrak{D}_X^{\langle G^I\rangle}(Y) = Y - 2A.$$

Let $\mathcal{S}_{(1,1)} = \mathcal{S} \cap (V_{\mathbb{C}}(0) \setminus V_{\mathbb{C}}(-2)) \cap (V_{\mathbb{C}}(0) \setminus V_{\mathbb{C}}(-2A))$*. Then, we obtain* $\mathcal{S}_{(1,1)} = \mathcal{S}$*. Therefore, we are able to obtain the simple Hermitian QE formula* $A \neq 0 \wedge -2A < 0$*.*

In addition, we consider a more general example.

Example 22 *Let* Φ *be the QFF* $A_1A_2 \neq 0 \wedge A_2^2 - 4A_3^3 = 0$ *and* $\mathcal{S} = \{\bar{a} \in \mathbb{C}^3 : \Phi(\bar{a})\}$*. We consider*

$$\Phi \wedge \exists \bar{X} \in \mathbb{R}^2\ (A_1X_2 + A_2X_1 + A_3^3 = 0 \wedge X_1^2 - A_1X_2 = 0 \wedge X_1 > 0).$$

As a CGS of $I = \langle A_1X_2 + A_2X_1 + A_3^3, X_1^2 - A_1X_2\rangle : X_1^\infty$ *on* $\mathcal{S}$ *w.r.t the lexicographic term order* $>$ *satisfying* $X_1 < X_2$ *with parameters* A_1, A_2, A_3*, we obtain*

$$\{(\mathcal{S}, \{-4A_1X_2 - 4A_2X_1 - A_2^2, (2X_1 + A_2)^2\})\}.$$

Let $G^I = \{-4A_1X_2 - 4A_2X_1 - A_2^2, (2X_1 + A_2)^2\}$*. Since* $\mathrm{RT}(G^I) = \{1, X_1\}$*, we obtain the HQFs*

$$H_1^{\langle G^I\rangle} = \frac{1}{2}\begin{pmatrix} 4 & -2A_2 \\ -2A_2 & A_2^2 \end{pmatrix},\ H_{X_1}^{\langle G^I\rangle} = \frac{1}{4}\begin{pmatrix} -4A_2 & 2A_2^2 \\ 2A_2^2 & -A_2^3 \end{pmatrix}.$$

We have theirs characteristic polynomials

$$\mathfrak{C}_1^{\langle G' \rangle} = Y^2 - (2 + \frac{A_2^2}{2})Y, \quad \mathfrak{C}_X^{\langle G' \rangle} = Y^2 + \frac{A_2}{2}(2 + \frac{A_2^2}{2})Y.$$

Let $b_1 = -(2 + \frac{A_2^2}{2})Y, b_X = \frac{A_2}{2}(2 + \frac{A_2^2}{2}) \in \mathbb{Q}[A]$. *Then, we obtain the Hermitian QE formula*

$$\Phi \wedge b_1 < 0 \wedge b_X < 0.$$

By using the script $(1) \in \mathbb{N}^1$ *we compute the minimal HQF*

$$H_1^{\langle G' \rangle}(1) = \begin{pmatrix} 2 \end{pmatrix}, \; H_X^{\langle G' \rangle}(1) = \begin{pmatrix} -\frac{A_2}{2} \end{pmatrix}.$$

We compute theirs characteristic polynomials

$$\mathfrak{D}_1^{\langle G' \rangle}(Y) = Y - 2, \quad \mathfrak{D}_X^{\langle G' \rangle}(Y) = Y + \frac{A_2}{2}.$$

Let $\mathcal{S}_{(1,1)} = \mathcal{S} \cap (V_{\mathbb{C}}(0) \setminus V_{\mathbb{C}}(-2)) \cap (V_{\mathbb{C}}(0) \setminus V_{\mathbb{C}}(\frac{A_2}{2}))$. *Then, we obtain* $\mathcal{S}_{(1,1)} = \mathcal{S}$. *Therefore, we are able to obtain the simple Hermitian QE formula* $\Phi \wedge \frac{A_2}{2} < 0$.

4 Conclusion

We have introduced minimal HQFs, and showed the Hermitian RRC theory with minimal HQFs as the main theorem. As like Example 21, 22, we can obtain a Hermitian QE formula of (2) by combining Theorem 15, Corollary 16 with Proposition 11. We may compute a partition such that

$$\text{its cardinality is equal to } \sum_{1 \le r \le d} ({}_d\mathrm{C}_r)^{2^t}$$

at worst. So, we need to carefully choose each minimal parametric HQF, and carefully implement the Hermitian QE with the concept of minimal HQFs. Moreover, there are some choices having a little effect on simplification. When we choose not $H_1^{\langle G' \rangle}(1)$ and $H_X^{\langle G' \rangle}(1)$ but one of the followings in Example 21 at the first, the choices have a little effect on simplification:

$$\begin{aligned} &H_1^{\langle G' \rangle}(2) \text{ and } H_X^{\langle G' \rangle}(2), \\ &H_1^{\langle G' \rangle}(2) \text{ and } H_X^{\langle G' \rangle}(1), \text{ or} \\ &H_1^{\langle G' \rangle}(1) \text{ and } H_X^{\langle G' \rangle}(2) \end{aligned}$$

For example, when we choose the first one, we obtain $A \neq 0 \wedge -2A^2 < 0 \wedge -2A^3 < 0$. That is, in this paper, there are the following problems when we compute a Hermitian QE formula of (2) by combining Theorem 15, Corollary 16 with Proposition 11.

- We may compute a partition such that its cardinality is equal to $\sum_{1 \le r \le d} ({}_d\mathrm{C}_r)^{2^t}$ at worst.
- There are some choices having a little effect on simplification.

The author try to solve the problems as future works. That is, the author try to obtain a solution to has a partition such that its cardinality is less than $\sum_{1 \le r \le d} ({}_d\mathrm{C}_r)^{2^t}$ even at worst, and a solution to has only some choices having a great effect on simplification.

References

[1] Becker, E., Wörmann, T.: On the Trace Formula for Quadratic Forms. Proceedings of Recent Advances in Real Algebraic Geometry and Quadratic Forms, Contemporary Mathematics Vol.155, pp.271-291, American Mathematical Society, 1994.

[2] Fukasaku, R.: QE Software Based on Comprehensive Gröbner Systems. Proceedings of Mathematical Software - ICMS 2014 - 4th International Congress, Lecture Notes in Computer Science Vol.8592, pp.512-517, Springer, 2014.

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

[4] 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.

[5] Fukasaku, R., Sato, Y: On Multivariate Hermitian Quadratic Forms. Submitted in Mathematics in Computer Science (MCS), Springer.

[6] Kapur, D., Sun, Y., Wang, D.: A New Algorithm for Computing Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC) 2010, 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 Japan Society for Symbolic and Algebraic Computation Vol.1, pp.39-66, 2011.

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

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

[10] 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.

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

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

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