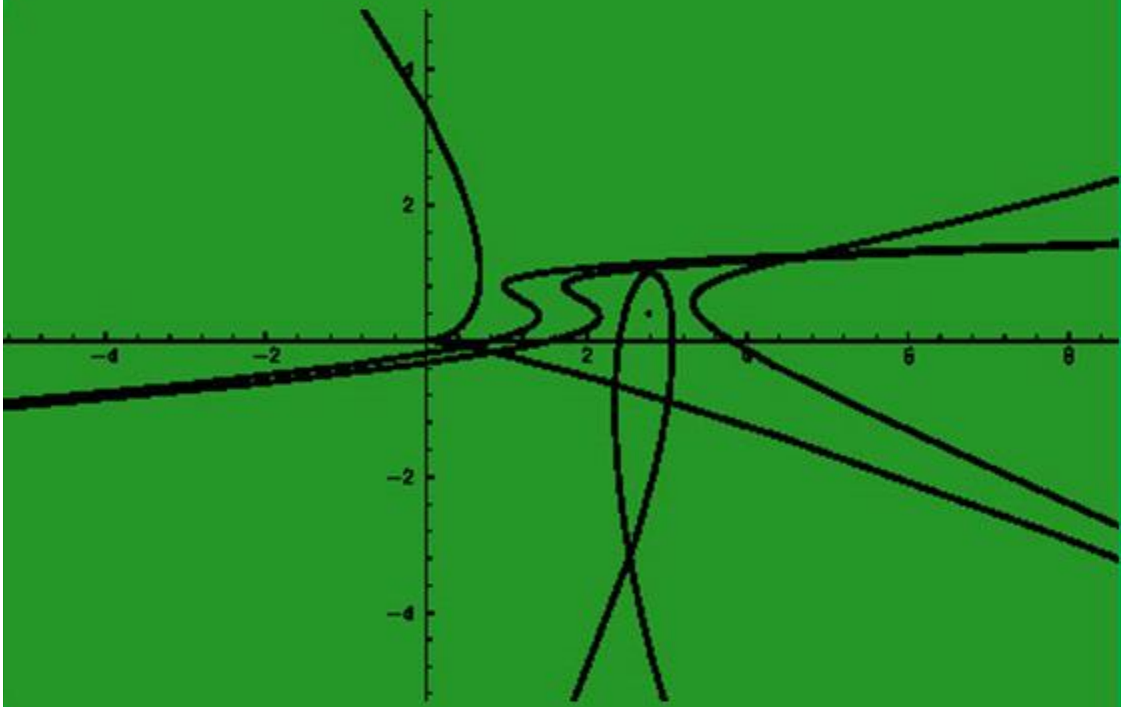
Communications of Japan Society for Symbolic and Algebraic Computation

2018
VOL.3



JSSAC

ISBN978-4-903027-32-6

Aims and Scopes:
Communications of JSSAC (Japan Society of Symbolic and Algebraic Computations) is dedicated to researchers who have a special interest in symbolic and algebraic computation. Communications of JSSAC publishes original articles dealing with every aspect of symbolic and algebraic computation.

Research Areas Include but are not limited to:

・Theoretical and algorithmic issues of symbolic and algebraic computation

・Design and implementation of symbolic and algebraic computation systems

・Applications of symbolic and algebraic computation in education, science, engineering and industry, pure mathematics, etc.

Legal Requirements:
In order to submit a manuscript, at least one of the author(s) should be a member of JSSAC in principle

Manuscript Submission:
A manuscript must be written in English.
It also should be written in Latex.
A submission must include:
(1) a Latex source file
(2) a dvi, ps or pdf file of (1)
(3) a title of the paper as well as the name(s) and affiliation(s) and mailing address(es) of the author(s)
(4) an abstract (no more than 150 words) and key words (5 or less)

For full and complete guide for authors, please refer to the following sites.

http://www.jssac.org/Editor/Style/index.html (in Japanese)
http://www.jssac.org/Editor/Communications/index-e.html (in English)

Every submitted manuscript will undergo a standard review process and the acceptance for publication by the editorial board will be based on its originality, significance of contribution and its relevance to the scope of Communications of JSSAC.

Miscellaneous:

・The copyright of a published paper is transferred to JSSAC.

・Communications of JSSAC has no page charges.

Contents

Communications of JSSAC (2018)
Vol. 3, pp. 1 – 17

Computation and Analysis of Explicit Formulae for the Circumradius of Cyclic Polygons [*]

Shuichi Moritsugu [†]

University of Tsukuba

(Received 27/Nov/2017 Accepted 11/Aug/2018)

Abstract

This paper describes computations of the circumradius of cyclic polygons given by the lengths of the sides. Extending the author's previous paper in 2011, we mainly discuss the computation and analysis of the formulae for cyclic heptagons and octagons. As a result of the present work, we have succeeded in explicitly computing the circumradius of cyclic heptagons, which is converted into an expression in the form of elementary symmetric polynomials for the first time. We have also succeeded in computing 25 out of 39 coefficients in the circumradius formula for cyclic octagons. Moreover, investigating the formulae by the total degree of each term, from triangles to octagons, we have discovered a characteristic structure in common among them, which should be helpful for computing the other huge coefficients remaining in the octagon formula.

Key words: cyclic polygon, circumradius, resultant, elementary symmetric polynomial

1 Introduction

In this study, we consider a classic problem in Euclidean geometry for cyclic polygons; that is, polygons inscribed in a circle. In particular, we focus on computing the circumradius R of cyclic n-gons given by the lengths of sides $a_1, a_2, \ldots, a_n$. In a previous paper [5], the author succeeded in computing explicit formulae for the circumradii of cyclic hexagons and heptagons. However, the algorithms used there were rather straightforward and inefficient from the present point of view. Hence, the aim of this study encompasses the following problems related to circumradius formulae for cyclic polygons:

(1) improvement of the computation algorithm for hexagons and heptagons,

(2) conversion of the heptagon formula into an expression in the form of elementary symmetric polynomials,

[*] This work was supported by a Grant-in-Aid for Scientific Research (25330006) from the Japan Society for the Promotion of Science (JSPS).

[†] moritsug@slis.tsukuba.ac.jp

(3) computation of the explicit formula for cyclic octagons,

(4) analysis of the formulae by an investigation in terms of total degrees.

Since Robbins [10] showed the "area formula (Heron polynomial)" for cyclic pentagons, several authors have studied this problem of the area as described, for example, in the report by Pak [8]. Pech [9] computed the actual form of the area of pentagons using a Gröbner basis technique, and also discussed the circumradius of pentagons. The degree of generalized Heron polynomials was proved by Fedorchuk and Pak [1], and the area formulae for cyclic heptagons and octagons were given by Maley et al. [2]. Independently of these studies, Varfolomeev [12] has discussed the area and the circumradius of cyclic polygons, but has never obtained an explicit formula for $n > 5$.

As a related work, the author derived an "integrated formula" for the relation of circumradius R and area S for $n = 5, 6$ in [6], which is a correction and expansion of the result of Svrtan et al. [11].

In contrast, this paper focuses on the "circumradius formulae" for cyclic polygons, which have not been so closely investigated in the above papers. The reason might be that the computation of circumradius formulae is very simply realized by resultants. If we already have $f_n(a_1, \ldots, a_n; R^2)$ as the circumradius formula for n-gons, with $f_3(a_1, a_2, a_3; R^2)$ as Heron's formula for triangles, the formula for $(n + 1)$-gons is computed inductively by the following equation using a diagonal d, because these three polygons have a circumcircle in common:

$$f_{n+1}(a_1, \ldots, a_{n+1}; R^2) := \mathrm{Res}_d \left(f_n(a_1, \ldots, a_{n-1}, d; R^2), f_3(d, a_n, a_{n+1}; R^2) \right) / (R^2)^\ell, \qquad (1)$$

where the number ℓ of redundant factor R^2 depends on the case. If we could compute the elimination by resultant efficiently, this equation would be easily solved. However, the polynomials f_n for $n \geq 7$ become so huge that we need much more consideration than for a straight computation. Moreover, the polynomial f_{n+1} needs to be factored in some circumstances, so that proper factors should be selected.

To the best of our knowledge, there exist no reports in which the circumradii for $n \geq 6$ are explicitly computed, other than the author's previous paper [5]. In the present paper, we review the computation for heptagons and attempt to compute the octagon formula. We note that some partial results of this study have been already shown in a report by the author [7].

2 Previously known results for $n = 3, 4, 5$

2.1 Circumradius of a triangle ($n = 3$)

Firstly, we consider the circumradius R of a triangle with side lengths a_1, a_2, and a_3. Every triangle has a circumcircle, and its radius is given by the classical formula of Heron

$$R = \frac{a_1 a_2 a_3}{\sqrt{(a_1 + a_2 + a_3)(-a_1 + a_2 + a_3)(a_1 - a_2 + a_3)(a_1 + a_2 - a_3)}}. \qquad (2)$$

It is straightforward to obtain the above relation using cosine and sine rules. Converting Eq. (2) into a polynomial expression, we obtain

$$\left(a_1^4 + a_2^4 + a_3^4 - 2(a_1^2 a_2^2 + a_2^2 a_3^2 + a_3^2 a_1^2) \right) R^2 + a_1^2 a_2^2 a_3^2 = 0. \qquad (3)$$

In the following, letting $y := R^2$, we consider the defining polynomial in y for each inscribed polygon. From the above equation, we express the defining polynomial for a triangle as

$$\Phi_3(a_1, a_2, a_3;\ y) := \left(a_1^4 + a_2^4 + a_3^4 - 2(a_1^2 a_2^2 + a_2^2 a_3^2 + a_3^2 a_1^2) \right) y + a_1^2 a_2^2 a_3^2. \qquad (4)$$

We note that the leading coefficient is factored into $\prod(a_1 \pm a_2 \pm a_3)$ as the product of all four combinations. In order to express the formula in more compact form, using elementary symmetric polynomials in a_i^2, we rewrite the above result as

$$F_3(s_1, s_2, s_3;\ y) := (s_1^2 - 4s_2)y + s_3, \tag{5}$$

where $s_1 = a_1^2 + a_2^2 + a_3^2$, $s_2 = a_1^2a_2^2 + a_2^2a_3^2 + a_3^2a_1^2$, and $s_3 = a_1^2a_2^2a_3^2$.

The aim of this study is to compute the similar polynomials $\Phi_n(a_i;\ y)$ and $F_n(s_i;\ y)$ for $n \geq 4$ and clarify their characteristics. That is, for a given cyclic n-gon with the length of sides $a_1, \dots, a_n$, we compute the polynomial $\Phi_n(a_1, \dots, a_n;\ R^2)$ where all the possible circumradii R are contained as its roots.

2.2 Circumradius of a cyclic quadrilateral ($n = 4$)

Secondly, we have the classic result of Brahmagupta for a "convex" cyclic quadrilateral:

$$R = \sqrt{\frac{(a_1a_2 + a_3a_4)(a_1a_3 + a_2a_4)(a_1a_4 + a_2a_3)}{(-a_1 + a_2 + a_3 + a_4)(a_1 - a_2 + a_3 + a_4)(a_1 + a_2 - a_3 + a_4)(a_1 + a_2 + a_3 - a_4)}}. \tag{6}$$

From its polynomial expression, we define the circumradius formula as

$$\begin{aligned}\Phi_4^{(+)}(a_i;\ y) := \Big((a_1^4 + a_2^4 + a_3^4 + a_4^4) - 2(a_1^2a_2^2 + a_1^2a_3^2 + a_1^2a_4^2 + a_2^2a_3^2 + a_2^2a_4^2 + a_3^2a_4^2) - 8a_1a_2a_3a_4\Big)\,y \\ + (a_1^2a_2^2a_3^2 + a_1^2a_2^2a_4^2 + a_1^2a_3^2a_4^2 + a_2^2a_3^2a_4^2) + (a_1^2 + a_2^2 + a_3^2 + a_4^2)a_1a_2a_3a_4.\end{aligned} \tag{7}$$

Again, we note that the leading coefficient is factored into

$$\prod^{4\text{ terms}} \left(a_1 + \sum_{j=2}^{4}(-1)^{k_j}a_j\right) \qquad k_j \in \{0, 1\}, \quad \sum_{j=2}^{4} k_j \equiv 1 \pmod 2, \tag{8}$$

which is the product of $a_1 \pm a_2 \pm a_3 \pm a_4$ with even numbers of + sign.

Using elementary symmetric polynomials in a_i^2, we rewrite the above result as

$$F_4^{(+)}(s_i;\ y) := (s_1^2 - 4s_2 - 8\sqrt{s_4})y + (s_3 + s_1\sqrt{s_4}), \tag{9}$$

where $s_1 = a_1^2 + a_2^2 + a_3^2 + a_4^2$, $s_2 = a_1^2a_2^2 + \cdots$, $s_3 = a_1^2a_2^2a_3^2 + \cdots$, and $\sqrt{s_4} = a_1a_2a_3a_4$, which is used as an auxiliary to $s_4 = a_1^2a_2^2a_3^2a_4^2$.

We should note that, letting $a_4 := -a_4$, we obtain another polynomial for "non-convex" quadrilaterals:

$$\Phi_4^{(-)}(a_1, a_2, a_3, a_4;\ y) := \Phi_4^{(+)}(a_1, a_2, a_3, -a_4;\ y). \tag{10}$$

Its elementary symmetric polynomial expression is

$$F_4^{(-)}(s_i;\ y) := (s_1^2 - 4s_2 + 8\sqrt{s_4})y + (s_3 - s_1\sqrt{s_4}), \tag{11}$$

which is obtained by substituting $\sqrt{s_4} := -\sqrt{s_4}$ in the polynomial $F_4^{(+)}(s_i;\ y)$.

2.3 Relation of the formulae for a triangle and a quadrilateral ($n = 3, 4$)

The polynomials $\Phi_4^{(+)}(a_i; y)$ and $\Phi_4^{(-)}(a_i; y)$ are also computed from $\Phi_3(a_1, a_2, a_3; y)$ by the following elimination procedure. We divide a cyclic quadrilateral with side lengths $\{a_1, a_2, a_3, a_4\}$ into two triangles with sides $\{a_1, a_2, d\}$ and $\{d, a_3, a_4\}$ by a diagonal of length d. Since these two triangles have a circumcircle in common, we will obtain the circumradius R of a quadrilateral by eliminating the diagonal d.

In Eq. (4), d will appear with only even degrees in the Heron polynomial. Therefore, we substitute $D := d^2$ into it, and compute the resultant with D. Removing the redundant factor y^2 from the resultant, we have the following relation by factorization:

$$\mathrm{Res}_D(\Phi_3(a_1, a_2, \sqrt{D};\ y),\ \Phi_3(\sqrt{D}, a_3, a_4;\ y))/y^2 = \Phi_4^{(+)}(a_i;\ y) \cdot \Phi_4^{(-)}(a_i;\ y). \tag{12}$$

In the formulation later in this paper, we will also refer to the expanded form of the product on the right-hand side:

$$\begin{array}{rcl} \Phi_4^{(\pm)}(a_i;\ y) & := & \Phi_4^{(+)}(a_i;\ y) \cdot \Phi_4^{(-)}(a_i;\ y) \\ & = & u_2(a_i^2)y^2 + u_1(a_i^2)y + u_0(a_i^2) \qquad \text{(71 terms)}, \end{array} \tag{13}$$

where each coefficient polynomial $u_j(a_i^2)$ has terms with only even degrees in a_i's.

Moreover, we should note that a good insight into the structure of the formulae is provided by the introduction of an auxiliary expression $\sqrt{s_n} = a_1 \cdots a_n$ (for even n), as well as the notion of *crossing parity* ε [10][2], where ε is 0 for a triangle, +1 for a convex quadrilateral, and −1 for a non-convex quadrilateral. Under these notations, the circumradius formulae in $y = R^2$ for $n = 3, 4$ in Eqs. (5), (9), and (11) are written in the following unified form:

$$F_{3,4}(s_i;\ y) := (s_1^2 - 4s_2 - \varepsilon \cdot 8\sqrt{s_4})y + (s_3 + \varepsilon \cdot s_1\sqrt{s_4}). \tag{14}$$

2.4 Circumradius of a cyclic pentagon ($n = 5$)

We start by dividing a cyclic pentagon with side lengths $\{a_1, \ldots, a_5\}$ by a diagonal of length d, into a cyclic quadrilateral of sides $\{a_1, a_2, a_3, d\}$ and a triangle of sides $\{d, a_4, a_5\}$, as shown in Fig. 1.

Since this quadrilateral and triangle have circumradius R in common, the cyclic pentagon formula should be obtained if the diagonal d is eliminated from the formulae of Brahmagupta and Heron. Specifically, we need to compute the following resultant:

$$\begin{array}{rcl} \Phi_5(a_i;\ y) & := & \mathrm{Res}_d(\Phi_4^{(+)}(a_1, a_2, a_3, d;\ y),\ \Phi_3(d, a_4, a_5;\ y))/y \\ & = & A_7y^7 + A_6y^6 + A_5y^5 + A_4y^4 + A_3y^3 + A_2y^2 + A_1y + A_0 \\ & & \left(y = R^2, \quad A_i \in \mathbf{Z}[a_1^2, \ldots, a_5^2]\right). \end{array} \tag{15}$$

We note that the leading coefficient and the constant term have the following forms:

$$\left\{ \begin{array}{rcl} A_7 & = & \prod(a_1 \pm a_2 \pm a_3 \pm a_4 \pm a_5) \qquad \text{(all combinations, 16 terms)}, \\ A_0 & = & a_1^6a_2^6a_3^6a_4^6a_5^6. \end{array} \right. \tag{16}$$

This strategy was proposed by Japanese mathematicians in the 17th century. Katahiro Takebe and Tomotoki Izeki showed, independently in 1683 and 1690, the details of the elimination procedures except for the final expanded expression [4]. Their results show that the circumradius formula for cyclic pentagons has 2,922 terms with degree 7 in $y = R^2$, which is equivalent to the results obtained by modern computers [10][9].

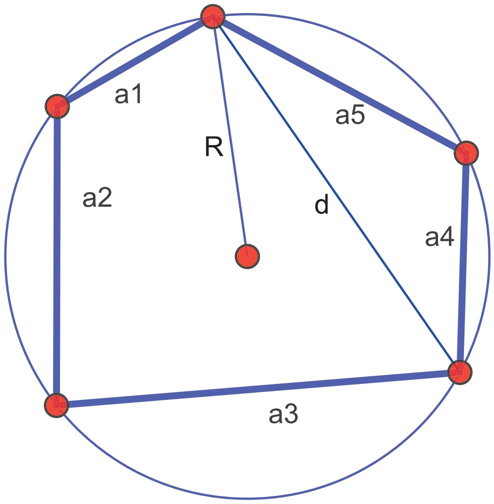


Fig. 1: Division of a cyclic pentagon by a diagonal d

We should note that the identical result is also obtained if we use $\Phi_4^{(-)}$ or $\Phi_4^{(\pm)}$ instead of $\Phi_4^{(+)}$; that is, we have the following relations:

$$\begin{aligned}\Phi_5(a_i;\ y) &= \mathrm{Res}_d(\Phi_4^{(-)}(a_1, a_2, a_3, d;\ y),\ \Phi_3(d, a_4, a_5;\ y))/y \\ &= \mathrm{Res}_D(\Phi_4^{(\pm)}(a_1, a_2, a_3,\ \sqrt{D};\ y),\ \Phi_3(\sqrt{D}, a_4, a_5;\ y))/y,\end{aligned} \tag{17}$$

where $D = d^2$ is substituted in the latter case.

It should also be helpful to reduce the expression for the pentagon case, using the elementary symmetric polynomials $s_1 = a_1^2 + \cdots + a_5^2, \ldots, s_5 = a_1^2 \cdots a_5^2$. For an odd number n, $\sqrt{s_n} = a_1 \cdots a_n$ does not appear in the formulae. As a result, Eq. (15) is rewritten into a simpler form:

$$F_5(s_i;\ y) = \tilde{A}_7 y^7 + \tilde{A}_6 y^6 + \cdots + \tilde{A}_1 y + \tilde{A}_0 \qquad \text{(81 terms)}, \tag{18}$$

where $\tilde{A}_i \in \mathbf{Z}[s_1, \ldots, s_5]$. In this equation, the leading coefficient and the constant term have the following structures:

$$\begin{cases} \tilde{A}_7 &= \left((s_1^2 - 4s_2)^2 - 64s_4\right)^2 - 2048s_5(s_1^3 - 4s_1s_2 + 8s_3), \\ \tilde{A}_0 &= s_5^3, \end{cases} \tag{19}$$

which correspond to Eq. (16).

3 Revision of the computation for hexagons ($n = 6$)

3.1 Robbins' theorem and previous algorithm

The degrees of defining polynomials $\Phi_n(a_i;\ y)$ were proved by Fedorchuk and Pak [1], after having been first conjectured by Robbins [10]. In this study, we define the circumradius formula $\Phi_n(a_i;\ y)$

for a cyclic n-gon as the polynomial factors with the following degree in y. Let

$$k_m := \frac{2m+1}{2}\begin{pmatrix} 2m \\ m \end{pmatrix} - 2^{2m-1} = \sum_{j=0}^{m-1}(m-j)\begin{pmatrix} 2m+1 \\ j \end{pmatrix}; \tag{20}$$

that is, let $k_i := 1, 7, 38, 187, 874, \ldots (i = 1, 2, 3, 4, \ldots)$. Then,

- the degree in y of $\Phi_{2m+1}(a_i;\ y)$ is k_m, and
- the degree in y of $\Phi^{(\pm)}_{2m+2}(a_i;\ y)$ is $2k_m$, where $\Phi^{(\pm)}_{2m+2}$ is factored into the product of two polynomials, $\Phi^{(+)}_{2m+2}$ and $\Phi^{(-)}_{2m+2}$, with each degree k_m.

We should note that $\Phi_{2m+1}(a_i;\ y)$ and $\Phi^{(\pm)}_{2m+2}(a_i;\ y)$ are polynomials only in a_i^2's.

In our previous paper [5], we computed the case of a cyclic hexagon ($m = 2$), dividing it into a pentagon and a triangle with diagonal d. Computing the resultant with $D(= d^2)$, we obtained a polynomial with degree 14 and 497,417 terms as an explicit form:

$$\left\{ \begin{array}{lcl} \Phi^{(\pm)}_6(a_1, \ldots, a_6; y) & := & \mathrm{Res}_D(\Phi_5(a_1, a_2, a_3, a_4, \sqrt{D};\ y), \Phi_3(\sqrt{D}, a_5, a_6;\ y))/y^8 \\ & = & \hat{B}_{14}y^{14} + \cdots + \hat{B}_1 y + \hat{B}_0 \qquad\qquad (\hat{B}_i \in \mathbf{Z}[a_1, \ldots a_6]). \end{array} \right. \tag{21}$$

Next, we factorized $\Phi^{(\pm)}_6(a_i; x)$, and obtained

$$\Phi^{(\pm)}_6(a_i;\ y) = \Phi^{(+)}_6(a_i;\ y) \cdot \Phi^{(-)}_6(a_i;\ y) \qquad (\deg_y \Phi^{(+)}_6 = \deg_y \Phi^{(-)}_6 = 7), \tag{22}$$

where both $\Phi^{(+)}_6$ and $\Phi^{(-)}_6$ have 19,449 terms. We should note that this factorization still needs several hours of CPU time, and might be a bottleneck in these procedures.

3.2 Revised algorithm for the circumradius of a cyclic hexagon

The result described above strongly suggests that we should avoid the factorization of large polynomials such as $\Phi^{(\pm)}_6(a_i;\ y)$. In the new formulation, we divide a cyclic hexagon into two (convex) quadrilaterals, and directly compute the defining polynomial for the circumradius of a convex hexagon as an expanded form:

$$\begin{array}{lcl} \Phi^{(+)}_6(a_i;\ y) & := & \mathrm{Res}_d(\Phi^{(+)}_4(a_1, a_2, a_3, d;\ y),\ \Phi^{(+)}_4(d, a_4, a_5, a_6;\ y))/y \\ & = & B_7 y^7 + B_6 y^6 + \cdots + B_1 y + B_0 \qquad \text{(19,449 terms, approx. 580KB)} \\ & & \qquad\qquad\qquad\qquad\qquad \big(y = R^2, \quad B_i \in \mathbf{Z}[a_1, \ldots, a_6]\big). \end{array} \tag{23}$$

Since the polynomial $\Phi^{(+)}_4(a_i; y)$ contains terms with odd degrees in a_i's, the above resultant should be computed with respect to d itself. We have confirmed that the leading coefficient of $\Phi^{(+)}_6(a_i;\ y)$ has the following form:

$$B_7 = \prod^{\text{16 terms}} \left(a_1 + \sum_{j=2}^{6} (-1)^{k_j} a_j \right) \qquad k_j \in \{0, 1\}, \quad \sum_{j=2}^{6} k_j \equiv 1 \pmod 2, \tag{24}$$

which is the product of $a_1 \pm \cdots \pm a_6$ with even numbers of + sign.

By avoiding factorization requiring several hours of CPU time, the computation of Eq. (23) can be executed in less than one second, which is a drastic improvement on the result reported in our previous paper [5].

The counterpart of $\Phi_6^{(+)}(a_i;\, y)$ for hexagons of the other group without a convex one is obtained by simple substitution from Robbins' theorem:

$$\Phi_6^{(-)}(a_1, \ldots, a_5, a_6;\, y) := \Phi_6^{(+)}(a_1, \ldots, a_5, -a_6;\, y). \tag{25}$$

In the formulation later in this paper, we will also refer to the expanded form of polynomial $\Phi_6^{(\pm)}(a_i;\, y) = \Phi_6^{(+)}(a_i;\, y) \cdot \Phi_6^{(-)}(a_i;\, y)$ in Eq. (22), which has terms with only even degrees in a_i's.

As the next step, using the elementary symmetric polynomials $s_1 = a_1^2 + \cdots + a_6^2, \ldots, s_5 = a_1^2 a_2^2 a_3^2 a_4^2 a_5^2 + \cdots$, $\sqrt{s_6} = a_1 \cdots a_6$, we rewrite Eq. (23) into a simpler form by the algorithm described later in Subsection 4.2:

$$F_6^{(+)}(s_i;\, y) := \tilde{B}_7 y^7 + \tilde{B}_6 y^6 + \cdots + \tilde{B}_1 y + \tilde{B}_0 \qquad \text{(224 terms)}, \tag{26}$$

where $\tilde{B}_i \in \mathbf{Z}[s_1, \ldots, s_5, \sqrt{s_6}]$. Compared with Eq. (19), the leading coefficient and the constant term have the following forms:

$$\left\{ \begin{array}{rcl} \tilde{B}_7 & = & \tilde{A}_7 + (-384 s_1^5 + 3072 s_1^3 s_2 - 4096 s_1^2 s_3 - 6144 s_1 s_2^2 - 8192 s_1 s_4 \\ & & \qquad + 16384 s_2 s_3 + 32768 s_5)\sqrt{s_6} + (12288 s_1^2 - 32768 s_2)\sqrt{s_6}^2, \\ \tilde{B}_0 & = & \tilde{A}_0 - s_2 s_5^2 \sqrt{s_6} + (s_1 s_3 s_5 - 4 s_4 s_5)\sqrt{s_6}^2 + (-s_1^2 s_4 + 2 s_1 s_5 + 4 s_2 s_4 - s_3^2)\sqrt{s_6}^3 \\ & & \qquad + (s_1^3 - 4 s_1 s_2 + 4 s_3)\sqrt{s_6}^4 - 4\sqrt{s_6}^5. \end{array} \right. \tag{27}$$

Its counterpart is simply computed by substitution:

$$F_6^{(-)}(s_1, \ldots, s_5, \sqrt{s_6};\, y) := F_6^{(+)}(s_1, \ldots, s_5, -\sqrt{s_6};\, y). \tag{28}$$

Since we have also the relation

$$F_5(s_1, \ldots, s_5;\, y) = F_6^{(+)}(s_1, \ldots, s_5, 0;\, y), \tag{29}$$

we can express F_5, $F_6^{(+)}$, and $F_6^{(-)}$ uniformly as polynomial $F_{5,6}(s_1, \ldots, s_5, \varepsilon\sqrt{s_6};\, y)$ similarly to Eq. (14), using the crossing parity ε. The term $\varepsilon\sqrt{s_6}$ means that ε is 0 for pentagons, $+1$ for hexagons that include a convex one, and -1 for the other group of hexagons. This completes the computation for the circumradii of cyclic pentagons and hexagons.

4 Revision of the computation for heptagons ($n = 7$)

4.1 Comparison of the division of cyclic heptagons

In our previous paper [5], the essential computation consisted of the following resultant:

$$\Phi_7(a_i;\, y) := \mathrm{Res}_D(\Phi_6^{(\pm)}(a_1, a_2, a_3, a_4, a_5, \sqrt{D};\, y),\ \Phi_3(\sqrt{D}, a_6, a_7;\, y))/y^6, \tag{30}$$

which means that a cyclic heptagon is divided into a hexagon and a triangle with a common circumcircle. However, there could be several ways to compute the resultant for cyclic heptagons other than Eq. (30). After comparative experiments, we have concluded that the following method of resultant computation seems to be quite practical from the viewpoint of CPU time and memory consumption. In this formulation, we divide a cyclic heptagon into a pentagon and a convex quadrilateral by another diagonal d, and compute the resultant into the expanded form:

$$\begin{array}{rcl} \Phi_7(a_i;\, y) & := & \mathrm{Res}_d(\Phi_5(a_1, a_2, a_3, a_4, d;\, y),\ \Phi_4^{(+)}(d, a_5, a_6, a_7;\, y))/y^6 \\ & = & C_{38} y^{38} + \cdots + C_1 y + C_0 \qquad \text{(337,550,051 terms, approx. 7,407MB)} \\ & & \qquad\qquad\qquad\qquad \left(y = R^2, \quad C_i \in \mathbf{Z}[a_1^2, \ldots, a_7^2]\right). \end{array} \tag{31}$$

We have observed that the leading coefficient and the constant term have the following forms:

$$\left\{\begin{array}{lcll} C_{38} & = & \prod(a_1 \pm a_2 \pm a_3 \pm a_4 \pm a_5 \pm a_6 \pm a_7) & \text{(all combinations, 64 terms)}, \\ C_0 & = & a_1^{20}a_2^{20}a_3^{20}a_4^{20}a_5^{20}a_6^{20}a_7^{20}. & \end{array}\right. \tag{32}$$

It seems difficult to compute the above resultant in Eq. (31) straightforwardly because of the size of polynomial Φ_5. Hence, we divide the computation steps as follows.

Firstly, we collect the coefficients of the two polynomials in d as a preprocessing for the construction of Sylvester matrix:

$$\left\{\begin{array}{lcll} \Phi_5(a_1, a_2, a_3, a_4, d;\ y) & = & y^7 d^{16} + u_{14}d^{14} + \cdots + u_2 d^2 + u_0 & (u_j \in \mathbf{Z}[a_1, a_2, a_3, a_4, y]), \\ \Phi_4^{(+)}(d, a_5, a_6, a_7;\ y) & = & yd^4 + a_5a_6a_7d^3 + (\ \cdots\ )d^2 + (\ \cdots\ )d + (\ \cdots\ ) & \text{(19 terms)}, \end{array}\right. \tag{33}$$

where Φ_5 originally has 2,922 terms (with only even degrees in d).

Secondly, we compute the resultant of these polynomials, regarding $u_0, \ldots, u_{14}$ as independent new variables, that is, Φ_5 as a polynomial with only 9 terms. It is a conventional programming technique in computer algebra to replace large subexpressions with new symbols temporally. Then, we obtain the intermediate form of the resultant polynomial:

$$R(u_0, u_2, \ldots, u_{14}, a_5, a_6, a_7;\ y) := \mathrm{Res}_d(\Phi_5, \Phi_4^{(+)}). \tag{34}$$

Thirdly, we substitute the original coefficient $u_j(a_1, a_2, a_3, a_4, y)$ in Φ_5 into each u_j, and obtain the following polynomial:

$$\bar{R}(a_1, \ldots, a_7;\ y) = \bar{C}_{38}y^{44} + \cdots + \bar{C}_0 y^6, \tag{35}$$

where $\bar{C}_i$'s are not yet expanded, because the Maple computer algebra system does not simplify them automatically.

Finally, if we succeed in expanding each coefficient $\bar{C}_i$ into the simplified form C_i, we obtain the explicit circumradius formula $\Phi_7(a_i;\ y)$ in Eq. (31). This expansion step needs large memory allocation and often fails, and the job of computing C_i's should be divided into several parts of appropriate sizes.

Using the same division of heptagons as in Eq. (31), we could also compute the following resultant, as a third method:

$$\Phi_7(a_i;\ y) := \mathrm{Res}_D(\Phi_5(a_1, a_2, a_3, a_4, \sqrt{D};\ y),\ \Phi_4^{(\pm)}(\sqrt{D}, a_5, a_6, a_7;\ y))/y^6. \tag{36}$$

Since we have $D = d^2$, the resultant with D will give rise to a Sylvester matrix half the size of that with d. Hence, more efficient computation may be expected.

Otherwise, as a fourth method, if we divide a cyclic heptagon into a hexagon and a triangle similarly to Eq. (30), we can also express the formula by the following resultant:

$$\Phi_7(a_i;\ y) := \mathrm{Res}_d(\Phi_6^{(+)}(a_1, a_2, a_3, a_4, a_5, d;\ y),\ \Phi_3(d, a_6, a_7;\ y))/y^6, \tag{37}$$

where $\Phi_6^{(+)}$ has 19,449 terms and might decrease the efficiency of computation.

Since it is almost impossible to find the optimal way to compute $\Phi_7(a_i;\ y)$ in advance, we tried all of these four types of formulations of the resultant. In the process of resultant computation, devices similar to those used in Eqs. (33), (34), and (35) are indispensable. We used the Maple 2016 computer algebra system in two environments:

Machine A Windows, Xeon (8 core, 2.93 GHz) × 2, 192 GB RAM,

Machine B Linux, Xeon (8 core, 2.6 GHz) × 2, 256 GB RAM.

A summary of the CPU times is shown in Table 1. The times include garbage collection; hence, if the memory allocation approaches the hardware limit, the efficiency of computation will be greatly lowered. Among these four methods, those of Eqs. (31) and (36), division into a pentagon and a quadrilateral, are relatively efficient. In contrast, it can be seen that those of Eqs. (30) and (37), division into a hexagon and a triangle, should be avoided. This finding represents a considerable improvement over that reported in our previous paper [5], where Eq. (30) was applied.

Resultant	Machine A	Machine B
Eq. (30)	62,211	67,087
Eq. (31)	†24,941	28,489
Eq. (36)	†25,365	27,978
Eq. (37)	‡238,183	††171,980

†: Job was divided into 4 parts.
‡: Job was divided into 7 parts.
††: Job was divided into 2 parts.

Table 1: CPU times (sec) using Maple 2016 for computing $\Phi_7(a_i;\ y)$

4.2 Conversion into an expression in the form of elementary symmetric polynomials

Since the coefficients in the circumradius formula for a cyclic heptagon are also symmetric with those of a_i^2, the size of the formula can be reduced if the coefficients are expressed by elementary symmetric polynomials.

The conversion has been processed by the following conventional algorithm so far. First, we consider the polynomial ideal with elementary symmetric polynomials of n-th order:

$$I \ = \ \left\{ s_1 - (a_1^2 + \cdots + a_n^2),\ \ \ldots,\ \ s_{n-1} - (a_1^2 \cdots a_{n-1}^2 + \cdots),\ \ s_n - (a_1^2 \cdots a_n^2) \right\}. \tag{38}$$

When the number n is even, we replace the last element s_n with $\sqrt{s_n}$:

$$I' \ = \ \left\{ s_1 - (a_1^2 + \cdots + a_n^2),\ \ \ldots,\ \ s_{n-1} - (a_1^2 \cdots a_{n-1}^2 + \cdots),\ \ s_n' - (a_1 \cdots a_n) \right\}. \tag{39}$$

With a group ordering (“lexdeg” in the Maple computer algebra system), computing the Gröbner basis of I or I' using Maple built-in function “Basis”, we obtain

$$G \ := \ \mathrm{Basis}(I, \{a_1, \ldots, a_n\} \succ \{s_1, \ldots, s_n\}). \tag{40}$$

Next, computing $p := \mathrm{NormalForm}(f, G)$ for a symmetric polynomial f using Maple function “NormalForm”, we obtain the expression p in the form of elementary symmetric polynomials. This algorithm has been effective for polynomials with up to 6 variables, and we have succeeded in computing $F_6^{(+)}(s_i;\ y)$ in Eq. (26).

However, in the case of 7 variables, this naïve algorithm becomes inefficient and cannot be used. For example, the constant term $C_0 = a_1^{20} \cdots a_7^{20}$ in $\Phi_7(a_i;\ y)$ has never been reduced to s_7^{10} by the “NormalForm” function.

This feature means that we should explicitly program the procedure of reduction by elementary symmetric polynomials for $n \geq 7$. Therefore, we have constructed the algorithm as follows.

First, we replace $b_i := a_i^2$ for simplicity, and consider the ideal

$$I = \{s_1 - (b_1 + \cdots + b_7), \ \ldots, \ s_6 - (b_1 \cdots b_6 + \cdots), \ s_7 - (b_1 \cdots b_7)\}. \qquad (41)$$

We compute the Gröbner basis of ideal I with a purely lexicographic order $b_1 \succ \cdots \succ b_7 \succ s_1 \succ \cdots \succ s_7$. Then, we obtain the Gröbner basis $G = \{g_1, \ldots, g_7\}$ with a certain type of structured form, which consists of the following polynomials:

$$\begin{cases} g_1 &= b_1 + (b_2 + \cdots + b_7 - s_1), \\ g_2 &= b_2^2 + h_2(b_2, b_3, \ldots, b_7, s_1, s_2), \\ \quad \cdots & \\ g_6 &= b_6^6 + h_6(b_6, b_7, s_1, \ldots, s_6), \\ g_7 &= b_7^7 - s_1 b_7^6 + s_2 b_7^5 - s_3 b_7^4 + s_4 b_7^3 - s_5 b_7^2 + s_6 b_7 - s_7, \end{cases} \qquad (42)$$

where $h_i(b_i, \ldots, b_7, s_1, \ldots, s_i) \in \mathbf{Z}[b_i, \ldots, b_7, s_1, \ldots, s_i]$ $(2 \leq i \leq 6)$.

Since each head term of g_i is $b_1, b_2^2, \ldots, b_7^7$ respectively, we reduce the symmetric polynomial f using g_i's in this order. Using the "Rem" polynomial remainder function in Maple, we compute the remainder with $b_1, b_2, \ldots, b_7$ sequentially as follows:

$$\begin{cases} r_1 &:= \mathrm{Rem}(f, g_1;\ b_1), \\ r_2 &:= \mathrm{Rem}(r_1, g_2;\ b_2), \\ \quad \cdots & \\ r_6 &:= \mathrm{Rem}(r_5, g_6;\ b_6), \\ p &:= \mathrm{Rem}(r_6, g_7;\ b_7). \end{cases} \qquad (43)$$

As a result, the variables $b_1, \ldots, b_7$ are eliminated from f in this order, and we obtain the expression with $s_1, \ldots, s_7$ only. Applying the above procedure, we have succeeded in converting $\Phi_7(a_i;\ y)$ into

$$F_7(s_i;\ y) = \tilde{C}_{38} y^{38} + \cdots + \tilde{C}_1 y + \tilde{C}_0 \qquad \text{(199,695 terms)}, \qquad (44)$$

where we have $\tilde{C}_i \in \mathbf{Z}[s_1, \ldots, s_7]$, with 78,503 seconds of CPU time on Machine A (described in Subsection 4.1). To the best of our knowledge, this polynomial $F_7(s_i;\ y)$ has not been shown elsewhere. Hence, this result represents a significant improvement to that in our previous paper [5], where only $\Phi_7(a_i;\ y)$ with 337,550,051 terms was obtained.

For reference, the area formula ($n = 7$) reported by Maley et al. [2] has the following form:

$$\tilde{\Psi}_7(s_i;\ x) = x^{38} + \tilde{M}_{37} x^{37} + \cdots + \tilde{M}_1 x + \tilde{M}_0 \qquad \text{(955,641 terms)}, \qquad (45)$$

where $x = (4S)^2$ and $\tilde{M}_i \in \mathbf{Z}[s_1, \ldots, s_7]$. They constructed the formula using elementary symmetric polynomials from the beginning, and their study does not contain a conversion procedure as described above.

5 Attempt at computation for an octagon ($n = 8$)

5.1 Algorithm and current results

We have several ways of dividing a cyclic octagon for computation of the circumradius formula. Dividing an octagon into a heptagon and a triangle, and substituting $D = d^2$, we have the following relation by resultant:

$$\Phi_8^{(\pm)}(a_i;\ y) := \mathrm{Res}_D(\Phi_7(a_1, a_2, a_3, a_4, a_5, a_6, \sqrt{D};\ y),\ \Phi_3(\sqrt{D}, a_7, a_8;\ y))/y^{32}. \qquad (46)$$

deg in y	#terms of $\Phi_8^{(+)}$	t-deg	#terms of $F_8^{(+)}$	deg in $\sqrt{s_8}$
0	5,554,128	70	918	16
1	13,298,304	69	1,870	16
2	26,940,233	68	3,432	16
3	48,012,824	67	5,732	16
4	77,750,132	66	8,931	16
5	114,947,440	65	12,670	16
6	158,302,913	64	17,129	16
7	204,390,480	63	21,592	15
8	250,654,676	62	26,179	15
9	293,931,056	61	30,200	15
10	333,471,187	60	33,748	15
11	367,872,280	59	36,404	14
12	393,876,280	58	38,662	14
13	410,700,024	57	40,052	14
28	126,825,848	42	17,976	10
29	109,294,704	41	16,183	10
30	93,610,141	40	14,513	10
31	79,699,496	39	12,910	9
32	67,463,040	38	11,436	9
33	56,784,240	37	10,026	9
34	47,533,327	36	8,743	9
35	39,574,496	35	7,514	8
36	32,771,272	34	6,385	8
37	26,990,336	33	5,260	8
38	22,105,457	32	4,231	8

Table 2: Each coefficient in the octagon formulae $\Phi_8^{(+)}(a_i;\ y)$ and $F_8^{(+)}(s_i;\ y)$

Alternatively, if we divide an octagon into two pentagons, we have a similar relation:

$$\Phi_8^{(\pm)}(a_i,\ y) := \mathrm{Res}_D(\Phi_5(a_1, a_2, a_3, a_4,\ \sqrt{D};\ y),\ \Phi_5(\sqrt{D}, a_5, a_6, a_7, a_8;\ y))/y^{36}. \tag{47}$$

Since the degree in y of $\Phi_8^{(\pm)}(a_i;\ y)$ is 76, it is quite difficult to compute these resultants in Eqs. (46) and (47). Moreover, this polynomial should be factorized as follows:

$$\Phi_8^{(\pm)}(a_i;\ y) = \Phi_8^{(+)}(a_i;\ y) \cdot \Phi_8^{(-)}(a_i;\ y) \qquad (\deg_y \Phi_8^{(+)} = \deg_y \Phi_8^{(-)} = 38), \tag{48}$$

which seems almost impractical. In order to avoid factorization, we should divide an octagon into a (convex) hexagon and a (convex) quadrilateral, and directly compute the following resultant with degree 38 in y:

$$\Phi_8^{(+)}(a_i;\ y) := \mathrm{Res}_d(\Phi_6^{(+)}(a_1, a_2, a_3, a_4, a_5, d;\ y),\ \Phi_4^{(+)}(d, a_6, a_7, a_8;\ y))/y^6. \tag{49}$$

Similarly to Eq. (31), we compute this stepwise.

Firstly, we collect the coefficients of the two polynomials in d:

$$\begin{cases} \Phi_6^{(+)}(a_1, a_2, a_3, a_4, a_5, d;\ y) & = \ y^7 d^{16} - a_1 a_2 a_3 a_4 a_5 y^5 d^{15} + u_{14} d^{14} + \cdots + u_1 d + u_0 \\ & \qquad\qquad (u_j \in \mathbf{Z}[a_1, \ldots, a_5, y]), \\ \Phi_4^{(+)}(d, a_6, a_7, a_8;\ y) & = \ y d^4 + a_6 a_7 a_8 d^3 + (\cdots) d^2 + (\cdots) d + (\cdots) \quad \text{(19 terms)}, \end{cases} \tag{50}$$

where $\Phi_6^{(+)}$ originally has 19,449 terms.

Secondly, we compute the resultant of these polynomials, regarding $u_0, \ldots, u_{14}$ as independent new variables. Then, we obtain the intermediate form of the resultant polynomial:

$$R(u_0, u_1, \ldots, u_{14}, a_1, \ldots, a_8;\ y) := \mathrm{Res}_d(\Phi_6^{(+)}, \Phi_4^{(+)}). \tag{51}$$

Thirdly, we substitute the original coefficient $u_j(a_1, \ldots, a_5, y)$ in $\Phi_6^{(+)}$ into each u_j, and obtain the following polynomial:

$$\bar{R}(a_1, \ldots, a_8;\ y) = \bar{P}_{38} y^{44} + \cdots + \bar{P}_0 y^6. \tag{52}$$

At this point, the $\bar{P}_i$'s have not yet been expanded or simplified and it is difficult to observe their explicit expressions. Finally, if we succeed in expanding each coefficient $\bar{P}_i$, we obtain the circumradius formula $\Phi_8^{(+)}(a_i;\ y)$ in Eq. (49). The current status of computation is expressed as follows:

$$\Phi_8^{(+)}(a_i;\ y) = P_{38} y^{38} + \cdots + P_{28} y^{28} + \left(\bar{P}_{27} y^{27} + \cdots + \bar{P}_{14} y^{14}\right) + P_{13} y^{13} + \cdots + P_0, \tag{53}$$

where coefficients $P_{27}, \ldots, P_{14}$ with much larger sizes have not yet been obtained in expanded form. A summary of the number of terms is shown in Table 2, and the degrees of each coefficient will be discussed later.

The expansion of each coefficient $\bar{P}_i$ needs a large memory allocation and often fails. For example, the size of coefficient P_{13} is approximately 8,644MB in Maple file format (*.m), which is the largest one obtained so far. In order to avoid memory overflow, we need to divide the procedure into a number of smaller problems, which requires much more CPU time. For example, the expansion of $\bar{P}_{28}$ took 371 days of CPU time in total (with 182 jobs, on Machine B described in Subsection 4.1), which is the longest computation executed so far, even though its size is approximately 2,673MB. Although we are considering the specification of data structures in Maple [3], it is unlikely that the remaining computations will be completed in the near future.

Nevertheless, some properties of the octagon formula have been elucidated at this point. We have, for example, succeeded in expanding the leading coefficient and obtained the structure

$$P_{38} = \prod^{64 \text{ terms}} \left(a_1 + \sum_{j=2}^{8} (-1)^{k_j} a_j \right) \qquad k_j \in \{0, 1\}, \quad \sum_{j=2}^{8} k_j \equiv 1 \pmod 2, \tag{54}$$

which is the product of $a_1 \pm a_2 \pm \cdots \pm a_8$ with even numbers of + sign.

When we obtain the coefficient P_i in expanded form, it should be converted into an expression in the form of elementary symmetric polynomials. First, we substitute $a_1 \cdots a_8 = \sqrt{s_8}$ in each coefficient P_i, and rewrite it as a polynomial form in $\sqrt{s_8}$:

$$P_i = h_0(a_1^2, \ldots, a_8^2) + h_1(a_1^2, \ldots, a_8^2)\sqrt{s_8} + \cdots + h_{\ell_i}(a_1^2, \ldots, a_8^2)\sqrt{s_8}^{\ell_i}. \tag{55}$$

In this expression, each coefficient $h_j(a_1^2, \ldots, a_8^2)$ is a symmetric polynomial in $a_1^2, \ldots, a_8^2$ again. Hence, we convert each coefficient using the recurrence relation for elementary symmetric polynomials, which is detailed in the next subsection. At present, we have obtained the coefficients in the form of elementary symmetric polynomials except $\tilde{P}_{27}, \ldots, \tilde{P}_{14}$, as follows:

$$F_8^{(+)}(s_i;\ y) = \tilde{P}_{38} y^{38} + \cdots + \tilde{P}_{28} y^{28} + \left(\bar{P}_{27} y^{27} + \cdots + \bar{P}_{14} y^{14}\right) + \tilde{P}_{13} y^{13} + \cdots + \tilde{P}_0. \tag{56}$$

For example, the constant term is expressed as

$$\tilde{P}_0 = s_7^{10} + s_3 s_7^9 \sqrt{s_8} + \cdots + (3s_1^6 - 8s_1^4 s_2) \sqrt{s_8}^{16} \qquad \text{(918 terms)}, \tag{57}$$

where $s_7^{10} = \tilde{C}_0$ in Eq. (44).

Since we have not completed expanding $\bar{P}_i$ $(27 \geq i \geq 14)$, their expressions in the form of elementary symmetric polynomials $\tilde{P}_i$ $(27 \geq i \geq 14)$ have not yet been obtained.

5.2 Recurrence relation for elementary symmetric polynomials

In this subsection, we consider another algorithm for converting symmetric polynomials $h_j(a_1^2, \ldots, a_8^2)$ in Eq. (55). A memory overflow was caused when the reduction procedure discussed earlier in the relation to Eqs. (42) and (43) was applied to the case of 8 variables. Hence, we tried to use a classical recurrence relation as follows, and to reduce the size of the problems.

Let s_k be the kth elementary symmetric polynomial with $x_1, \ldots, x_n$, and let t_k be the kth elementary symmetric polynomial with $x_2, \ldots, x_n$. Then, we have the following relations:

$$\left\{ \begin{array}{lcl} s_1 & = & x_1 + t_1, \\ s_2 & = & t_1 x_1 + t_2, \\ \cdots & \cdots & \cdots \\ s_{n-1} & = & t_{n-2} x_1 + t_{n-1}, \\ s_n & = & t_{n-1} x_1. \end{array} \right. \tag{58}$$

If we solve the ith equation with t_i, and substitute it into the next equation for $i = 1, \ldots, n-1$ repeatedly, we obtain the following relations:

$$\left\{ \begin{array}{lclcl} t_1 & = & s_1 - x_1, & & \\ t_2 & = & s_2 - t_1 x_1 & = & s_2 - s_1 x_1 + x_1^2, \\ \cdots & \cdots & \cdots & & \\ t_{n-1} & = & s_{n-1} - t_{n-2} x_1 & = & s_{n-1} - \cdots + (-1)^{n-1} x_1^{n-1}, \end{array} \right. \tag{59}$$

which means that $t_1, \ldots, t_{n-1}$ are expressed as polynomials in $x_1, s_1, \ldots, s_{n-1}$. Finally, substituting into the nth line in Eq. (58), we obtain the polynomial relation:

$$g(x_1) = (-1)^{n-1} x_1^n + \cdots + s_{n-1} x_1 - s_n = 0. \tag{60}$$

Using these relations, expressions in the form of elementary symmetric polynomials with n variables are computed by the following procedure.

Firstly, we order the given symmetric expression with n variables into the polynomial in x_1:

$$f(x_1, \ldots, x_n) = a_\ell(x_2, \ldots, x_n) x_1^\ell + \cdots + a_1(x_2, \ldots, x_n) x_1 + a_0(x_2, \ldots, x_n), \tag{61}$$

where each coefficient $a_j(x_2, \ldots, x_n)$ is symmetric in $x_2, \ldots, x_n$.

Secondly, applying Eqs. (42) and (43) to the $n-1$ variable case, we convert $a_j(x_2, \ldots, x_n)$ into the expression by t_k:

$$f'(x_1, t_1, \ldots, t_{n-1}) = a'_\ell(t_1, \ldots, t_{n-1}) x_1^\ell + \cdots + a'_1(t_1, \ldots, t_{n-1}) x_1 + a'_0(t_1, \ldots, t_{n-1}). \tag{62}$$

This process means that one problem with n variables is divided into ℓ problems with $n-1$ variables.

Thirdly, applying Eq. (59) to Eq. (62), we express t_k by $x_1, s_1, \ldots, s_k$, and reorder it with x_1:

$$f''(x_1, s_1, \ldots, s_{n-1}) = a''_m(s_1, \ldots, s_{n-1}) x_1^m + \cdots + a''_1(s_1, \ldots, s_{n-1}) x_1 + a''_0(s_1, \ldots, s_{n-1}). \tag{63}$$

Finally, using Eq. (60), we compute the remainder of f'' by $g(x_1)$ with x_1. As a result, the variable x_1 is completely eliminated and we obtain the expression in the form of elementary symmetric polynomials as $\tilde{f}(s_1, \ldots, s_n)$.

When we tried to apply this procedure to the computation of Eq. (44) with 7 variables, the computation time was not necessarily reduced, even though memory consumption could be suppressed. However, for the case with 8 variables in Eq. (55), the above procedure with a recurrence relation was found to be indispensable to avoid memory overflow.

5.3 Confirmation of the results for octagons

At present, we have succeeded in computing the coefficients P_i and $\tilde{P}_i$ $(i = 0, \ldots, 13, 28, \ldots, 38)$ in Eqs. (53) and (56). We have confirmed their correctness in the following two ways:

Check (1) We assumed that the heptagon formulae in Eqs. (31) and (44) were correctly computed. Then, we substituted $a_8 := 0$ or $\sqrt{s_8} := 0$ into P_i and $\tilde{P}_i$, and compared them with coefficients C_i and $\tilde{C}_i$ in the heptagon formulae. For the coefficients P_i and $\tilde{P}_i$ obtained so far, all of the values were confirmed to be identical.

Check (2) The resultant in Eq. (49) is easily computed under the substitution $a_j := p_j$, where p_j's are randomly chosen prime numbers. Then, we compared these values with the coefficients P_i in $\Phi_8^{(+)}(p_j;\ y)$ under the substitution $a_j := p_j$, and confirmed that they were identical.

Since the expression $\tilde{P}_i$ in the form of elementary symmetric polynomials is successfully computed from P_i, we may conclude that P_i is truly a symmetric polynomial. Adding the above checks to this result, we believe that the octagon formula, computed so far, is surely the correct expansion of the heptagon formula.

6 Analysis of the forms of circumradius formulae

deg in y	#terms in $\Phi_4^{(+)}$	t-deg	#terms in $F_4^{(+)}$	deg in $\sqrt{s_4}$
0	8	3	2	1
1	11	2	3	1

Table 3: Each coefficient in the quadrilateral formulae $\Phi_4^{(+)}(a_i;\ y)$ and $F_4^{(+)}(s_i;\ y)$

In this section, we investigate the shapes of circumradius formulae by focusing on the degrees in each coefficient. First, we introduce the notion of the total degree of a power product in a_i^2's.

Definition 1
We define the total degree of a power product in a_i^2's as follows:

$$\text{t-deg}\left(a_1^{2m_1} a_2^{2m_2} \cdots a_n^{2m_n}\right) := m_1 + m_2 + \cdots + m_n. \tag{64}$$

Under this definition, elementary symmetric polynomials with n variables have the following structures composed of homogeneous power products:

$$\left\{\begin{array}{lcll} s_1 & = & a_1^2+\cdots+a_n^2 & \text{is homogeneous with t-deg } 1, \\ s_2 & = & a_1^2a_2^2+\cdots & \text{is homogeneous with t-deg } 2, \\ & \cdots & & \cdots \\ s_{n-1} & = & a_1^2a_2^2\cdots a_{n-1}^2+\cdots & \text{is homogeneous with t-deg } n-1, \\ s_n & = & a_1^2a_2^2\cdots a_n^2 & \text{has t-deg } n. \end{array}\right. \tag{65}$$

Adding to the above, only for the case of even number n, we define t-deg$(\sqrt{s_n}) = n/2$, where $\sqrt{s_n} = a_1a_2\cdots a_n$. We also note that the total degree in elementary symmetric polynomials is given by

$$\text{t-deg}\left(s_1^{m_1}s_2^{m_2}\cdots s_n^{m_n}\right) = m_1+2m_2+\cdots+nm_n. \tag{66}$$

First, we investigate the triangle formula $\Phi_3(a_1,a_2,a_3;\ y)$ in Eq. (4).

- The constant term has the form $a_1^2a_2^2a_3^2$ with t-deg 3.
- The coefficient of $y(=R^2)$ is $a_1^4+a_2^4+a_3^4-2(a_1^2a_2^2+a_2^2a_3^2+a_3^2a_1^2)$ and it is homogeneous with t-deg 2.

These relations are also observed in the expression $F_3(s_1,s_2,s_3;\ y)$ in the form of elementary symmetric polynomials in Eq. (5), where we have t-deg$(s_3)=3$ and t-deg$(s_1^2-4s_2)=2$.

Similarly, we analyze the quadrilateral formulae $\Phi_4^{(+)}(a_i;\ y)$ and $F_4^{(+)}(s_i;\ y)$ in Eqs. (7) and (9), noting that t-deg$(\sqrt{s_4})$ = t-deg$(a_1a_2a_3a_4)$ = 2. The number of terms and the total degrees are shown in Table 3. From these results, it can be seen that the triangle formula is a part of the quadrilateral formula as shown in Eq. (14).

deg in y	#terms in $\Phi_6^{(+)}$	t-deg	#terms in $F_6^{(+)}$	deg in $\sqrt{s_6}$
0	533	15	12	5
1	1,632	14	23	4
2	2,688	13	33	4
3	3,597	12	37	4
4	3,888	11	36	3
5	3,234	10	33	3
6	2,338	9	29	3
7	1,539	8	21	2

Table 4: Each coefficient in the hexagon formulae $\Phi_6^{(+)}(a_i;\ y)$ and $F_6^{(+)}(s_i;\ y)$

Next, we investigate the hexagon formulae $\Phi_6^{(+)}(a_i;\ y)$ and $F_6^{(+)}(s_i;\ y)$ in Eqs. (23) and (26), noting that t-deg$(\sqrt{s_6})$ = t-deg$(a_1\cdots a_6)=3$. The number of terms and the total degrees are shown in Table 4, and it is naturally confirmed by the observation that the pentagon formulae $\Phi_5(a_i;\ y)$ and $F_5(s_i;\ y)$ in Eqs. (15) and (18) have the same distribution of total degrees.

Finally, we analyze the octagon formulae $\Phi_8^{(+)}(a_i;\ y)$ and $F_8^{(+)}(a_i;\ y)$ in Eqs. (53) and (56), although it should be noted that this attempt is still ongoing. As discussed earlier, we have completed the computations P_i and $\tilde{P}_i$ for $i=0,\dots,13$ and $i=28,\dots,38$. The number of terms and the total degrees of these coefficients are shown in Table 2.

Since the distribution of degrees is quite regular, it seems possible to readily estimate the forms of $\tilde{P}_i$ $(i = 14, \ldots, 27)$, the expanded forms of which we have not yet obtained. For example, $\tilde{P}_{20}$ should have t-deg 50 and degree 12 in $\sqrt{s_8}$. Therefore, it should have the following form:

$$\tilde{P}_{20} = u_0(s_1, \ldots, s_7) + u_1(s_1, \ldots, s_7)\sqrt{s_8} + \cdots + u_{12}(s_1, \ldots, s_7)\sqrt{s_8}^{12}, \tag{67}$$

where u_j is homogeneous with t-deg$(u_j) = 50 - 4j$ $(j = 0, \ldots, 12)$. In particular, $u_0(s_1, \ldots, s_7)$ should be identical with coefficient $\tilde{C}_{20}$ of the heptagon formula $F_7(s_i;\ y)$ in Eq. (44).

7 Concluding remarks

In this study, we have shown continued progress in the computation of circumradius formulae for cyclic polygons since our previous paper [5] as follows.

(1) The computation algorithms for cyclic hexagons and heptagons have been significantly improved.

(2) The circumradius formula for heptagons has been converted into an expression in the form of elementary symmetric polynomials for the first time.

(3) The current status of computation for the octagon formula is shown, and 25 out of 39 coefficients have been explicitly obtained so far. However, it might be quite difficult to expand the remaining polynomials $\tilde{P}_i$ $(i = 14, \ldots, 27)$ because of their size.

(4) The common structure of the circumradius formulae has been investigated by the distribution of total degrees.

Although the computations for the octagon formula have not yet been completed, we believe that significant knowledge in a unified form has been obtained for the circumradii of cyclic n-gons $(n = 3, \ldots, 8)$. As a result, it has become possible to predict the structure of each coefficient, such as Eq. (67) in the octagon formula. Using this knowledge, it is expected that another approach such as a numerical interpolation algorithm will be able to be applied to this problem in the future.

References

[1] Fedorchuk, M. and Pak, I.: Rigidity and Polynomial Invariants of Convex Polytopes, *Duke Math. J.*, **129**(2), 2005, 371–404.

[2] Maley, F. M., Robbins, D. P., and Roskies, J.: On the Areas of Cyclic and Semicyclic Polygons, *Advances in Applied Mathematics*, **34**(4), 2005, 669–689.

[3] Monagan, M. and Pearce, R.: The Design of Maple's Sum-of-products and POLY Data Structures for Representing Mathematical Objects, *ACM Communications in Computer Algebra*, **48**(4), 2014.

[4] Moritsugu, S.: Radius Computation for an Inscribed Pentagon in *Sanpou-Hakki* (1690), *ACM Communications in Computer Algebra*, **44**(3), 2010, 127–128.

[5] Moritsugu, S.: Computing Explicit Formulae for the Radius of Cyclic Hexagons and Heptagons, *Bulletin of Japan Soc. Symbolic and Algebraic Computation*, **18**(1), 2011, 3–9.

[6] Moritsugu, S.: Integrated Circumradius and Area Formulae for Cyclic Pentagons and Hexagons, *ADG 2014* (Botana, F. and Quaresma, P., eds.), *LNAI*, **9201**, Springer, 2015, 94–107.

[7] Moritsugu, S.: Revisiting the Computation of Circumradius for Inscribed Polygons, *Kyoto University RIMS Kokyuroku*, **2054**, 2017, 153–161. (in Japanese).

[8] Pak, I.: The Area of Cyclic Polygons: Recent Progress on Robbins' Conjecture, *Advances in Applied Mathematics*, **34**(4), 2005, 690–696.

[9] Pech, P.: Computations of the Area and Radius of Cyclic Polygons Given by the Lengths of Sides, *ADG2004* (Hong, H. and Wang, D., eds.), *LNAI*, **3763**, Gainesville, Springer, 2006, 44–58.

[10] Robbins, D. P.: Areas of Polygons Inscribed in a Circle, *Discrete & Computational Geometry*, **12**(1), 1994, 223–236.

[11] Svrtan, D., Veljan, D., and Volenec, V.: Geometry of Pentagons: from Gauss to Robbins, arXiv:math.MG/0403503 v1, 2004.

[12] Varfolomeev, V. V.: Inscribed Polygons and Heron Polynomials, *Sbornik: Mathematics*, **194**(3), 2003, 311–331.

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 $\succ$ 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. $\succ$ 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*

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

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 $pv_iv_jv_k$ 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 $1 \leq i \neq j \leq q$ 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 $1 \leq i \leq q$ 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 $>$ 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. $>$ for each $\bar{a} \in \mathcal{S}_i$, and*
- *any $g \in G_i$ satisfies $LC(g)(\bar{a}) \neq 0$ 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. $>$. 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. $>$ 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* RT$(G(\bar{a}, \bar{X}))$ *is invariant. In addition, we have also Remark 2 and 9. Therefore, we can compute the uniform representation $H^{\langle G\rangle}_{p_e}$ 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 $H^{\langle G\rangle}_{p_e}$ 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 $\mathfrak{C}^{\langle G\rangle}_{p_e}$ has rational functions of $\mathbb{Q}(\bar{A})$ as its coefficients, we suppose*

$$\begin{aligned} \mathfrak{C}^{\langle G\rangle}_{p_e}(Y) &= b^+_d Y^d + b^+_{d-1} Y^{d-1} + \cdots + b^+_0 \in \mathbb{Q}(\bar{A})[Y], \\ \mathfrak{C}^{\langle G\rangle}_{p_e}(-Y) &= b^-_d Y^d + b^-_{d-1} Y^{d-1} + \cdots + b^-_0 \in \mathbb{Q}(\bar{A})[Y]. \end{aligned}$$

Let $S^{\varrho}_e = (b^{\varrho}_d, \ldots, b^{\varrho}_0)$ for $\varrho \in \{+, -\}$. Let $B^{\varrho}_e(\bar{a})$ be the number of sign changes in $S^{\varrho}_e(\bar{a}) = (b^{\varrho}_d(\bar{a}), \ldots, b^{\varrho}_0(\bar{a}))$ for $\bar{a} \in \mathcal{S}_\Phi \cap \mathbb{R}^m$. Using the numerator and denominator polynomials of S^{ϱ}_e, 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* RT$(G^I) = \{1, X\}$, *we obtain*

$$H^{\langle G^I\rangle}_1 = \begin{pmatrix} 2 & 2A \\ 2A & 2A^2 \end{pmatrix},\ H^{\langle G^I\rangle}_X = \begin{pmatrix} 2A & 2A^2 \\ 2A^2 & 2A^3 \end{pmatrix}.$$

We have theirs characteristic polynomials

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

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

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

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

$$H_1^{\langle G^J \rangle} = \begin{pmatrix} 1 \end{pmatrix}, \ H_X^{\langle G^J \rangle} = \begin{pmatrix} A \end{pmatrix}.$$

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 $r = \operatorname{rank}(H_p^I)$. 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

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

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*

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

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*

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

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:

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

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

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

${}^{\mathrm{t}}H$ 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 $1 \leq k \leq \nu$. Therefore, the assertion is satisfied. □

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

Proposition 20 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 $1 \leq k \leq \nu$. 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*

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

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* $A_1 A_2 \neq 0 \wedge A_2^2 - 4A_3^3 = 0$ *and* $\mathcal{S} = \{\bar{a} \in \mathbb{C}^3 : \Phi(\bar{a})\}$. *We consider*

$$\Phi \wedge \exists \bar{X} \in \mathbb{R}^2 \ (A_1 X_2 + A_2 X_1 + A_3^3 = 0 \wedge X_1^2 - A_1 X_2 = 0 \wedge X_1 > 0).$$

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

$$\{(\mathcal{S}, \{-4A_1 X_2 - 4A_2 X_1 - A_2^2, (2X_1 + A_2)^2\})\}.$$

Let $G^I = \{-4A_1 X_2 - 4A_2 X_1 - A_2^2, (2X_1 + A_2)^2\}$. *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

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

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*

$$H_1^{\langle G'\rangle}(1) = \left(\ 2 \ \right), \ H_X^{\langle G'\rangle}(1) = \left(\ -\frac{A_2}{2} \ \right).$$

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:

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

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.

Communications of JSSAC Vol. 3 2018
Publisher Japan Society for Symbolic and Algebraic Computation
Office zip 124–0011
Katsushika-ku Yotsugi 1–26–2 AlphaOmega Inc.