On Real Roots Counting for Non-radical Parametric Ideals

Ryoya Fukasaku(✉) and Yosuke Sato

Tokyo University of Science, Tokyo, Japan
fukasaku@rs.tus.ac.jp, ysato@rs.kagu.tus.ac.jp

Abstract. An algorithm we have introduced has a great effect on quantifier elimination of a first order formula containing many equalities. When the parametric ideal generated by the underlying equalities is not radical, however, our algorithm tends to produce an unnecessarily complicated formula. In this short paper, we show a result concerning Hermitian quadratic forms. It enables us to improve our algorithm so that we can get a simple formula without any radical computation.

Keywords: Hermitian quadratic form
Comprehensive Gröbner system · Quantifier elimination

1 Introduction

We have introduced an algorithm in [2] as a special type of a Quantifier Elimination (QE) algorithm. It has a great effect on QE of a first order formula containing many equalities. The essential part of the algorithm is to eliminate all existential quantifiers $\exists \bar{X}$ from the following basic first order formula:

$$\phi(\bar{A}) \wedge \exists \bar{X} \, (\bigwedge_{1 \leq i \leq s} f_i(\bar{A}, \bar{X}) = 0 \wedge \bigwedge_{1 \leq i \leq t} h_i(\bar{A}, \bar{X}) > 0) \tag{1}$$

with polynomials $f_1, \ldots, f_s, h_1, \ldots, h_t$ in $\mathbb{Q}[\bar{A}, \bar{X}]$ such that the parametric ideal $I = \langle f_1, \ldots, f_s \rangle$ in $\mathbb{C}[\bar{X}]$ is zero-dimensional for any specialization of the parameters $\bar{A}$ satisfying $\phi(\bar{A})$, where $\phi(\bar{A})$ is a quantifier free formula consisting only of equality $=$ and disequality $\neq$. The algorithm computes a Comprehensive Gröbner System (CGS) of the parametric ideal I, then applies the method of [6] (we call *CGS-QE* method in this paper) which is based on the theory of real roots counting by a Hermitian Quadratic Form (HQF) introduced in [5] with several innovative improvements. The algorithm is further improved by several techniques reported in [3] and implemented in Maple as freeware software [4]. It achieves a good performance for first order formulas containing many equalities as is reported in [1]. When the parametric ideal I is not radical, however, our algorithm tends to produce a unnecessarily complicated formula. Although we may get a simpler formula by computing a CGS of the radical ideal $\sqrt{I}$, such a computation is very heavy in general in a parametric polynomial ring.

J. Blömer et al. (Eds.): MACIS 2017, LNCS 10693, pp. 258–263, 2017.
https://doi.org/10.1007/978-3-319-72453-9_18

In this paper, we study the structure of a HQF and show a result namely Theorem 8. It enables us to compute a quantifier free formula equivalent to (1) which is as simple as the one obtained using a CGS of $\sqrt{I}$ without any radical computation. The paper is organized as follows. In Sect. 2, we give a quick review of our CGS-QE algorithm for understanding our result. In Sect. 3, we introduce our main result together with an example which is simple but enough for understanding how we can improve our CGS-QE algorithm.

2 Preliminary

2.1 Multivariate Real Roots Counting

In the rest of the paper, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of rational numbers, real numbers and complex numbers respectively. $\bar{X}$ and $\bar{A}$ denote some variables $X_1, \ldots, X_n$ and $A_1, \ldots, A_m$. $T(\bar{X})$ denotes a set of terms in $\bar{X}$. For an ideal $I \subset \mathbb{R}[\bar{X}]$, let $V_{\mathbb{R}}(I) = \{\bar{c} \in \mathbb{R}^n | \forall f \in I \ f(\bar{c}) = 0\}$ and $V_{\mathbb{C}}(I) = \{\bar{c} \in \mathbb{C}^n | \forall f \in I \ f(\bar{c}) = 0\}$. Let I be a zero dimensional ideal in a polynomial ring $\mathbb{R}[\bar{X}]$. Considering the residue class ring $\mathbb{R}[\bar{X}]/I$ as a vector space over $\mathbb{R}$, let $v_1, \ldots, v_q$ be its basis. For an arbitrary $h \in \mathbb{R}[\bar{X}]/I$ and each i, j $(1 \leq i, j \leq q)$ we define a linear map $\theta_{h,i,j}$ from $\mathbb{R}[\bar{X}]/I$ to $\mathbb{R}[\bar{X}]/I$ by $\theta_{h,i,j}(f) = hv_iv_jf$ for $f \in \mathbb{R}[\bar{X}]/I$. Let $q_{h,i,j}$ be the trace of $\theta_{h,i,j}$ and M_h^I be a real symmetric matrix such that its (i, j)-th component is given by $q_{h,i,j}$. Regarding a real symmetric matrix as a quadratic form, M_h^I is called, a *Hermitian Quadratic Form (HQF)*. The characteristic polynomial of M_h^I is denoted by $\chi_h^I(x)$. The dimension of $\mathbb{R}[\bar{X}]/I$ is denoted by $\dim(\mathbb{R}[\bar{X}]/I)$. For a polynomial $f(x) \in \mathbb{R}[x]$, the signature of $f(x)$, denoted $\mathrm{sign}(f(x))$, is an integer which is equal to 'the number of positive real roots of $f(x) = 0$' − 'the number of negative real roots of $f(x) = 0$', that is, $\mathrm{sign}(f(x)) = \#(\{c \in \mathbb{R} | f(c) = 0, c > 0\}) - \#(\{c \in \mathbb{R} | f(c) = 0, c < 0\})$. The signature of M_h^I, denoted $\mathrm{sign}(M_h^I)$, is defined as the signature of $\chi_h^I(x)$. The real root counting theorem introduced in [5] is the following assertion.

Theorem 1. $\mathrm{sign}(M_h^I) = \#(\{\bar{x} \in V_{\mathbb{R}}(I) | h(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) | h(\bar{x}) < 0\})$.

2.2 Comprehensive Gröbner System

Definition 2. *For a subset $\mathcal{S}$ of $\mathbb{C}^m$, a finite set $\{\mathcal{S}_1, \ldots, \mathcal{S}_r\}$ of subsets of $\mathbb{C}^m$ which satisfies $\cup_{i=1}^r \mathcal{S}_i = \mathcal{S}$ and $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset (i \neq j)$ is called a* partition *of $\mathcal{S}$. Each $\mathcal{S}_i$ is called a* segment.

Definition 3. *Let $\succ$ be an admissible term order on $T(\bar{X})$. For a polynomial $f \in \mathbb{C}[\bar{A}, \bar{X}]$, regarding f as a member of a polynomial ring $\mathbb{C}[\bar{A}][\bar{X}]$ over a coefficient ring $\mathbb{C}[\bar{A}]$, its leading term and coefficient are denoted by $LT_{\succ}(f)$ and $LC_{\succ}(f)$ respectively. For a finite set $F \subset \mathbb{Q}[\bar{A}, \bar{X}]$ and a subset $\mathcal{S}$ of $\mathbb{C}^m$, a finite set of pairs $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_r, G_r)\}$ with finite sets G_i of $\mathbb{Q}[\bar{A}, \bar{X}]$ for each i satisfying the following properties 1, 2, 3 is called a* (minimal) comprehensive Gröbner system (CGS) *of $\langle F \rangle$ on $\mathcal{S}$ with parameters $\bar{A}$ w.r.t. the term order $\succ$.*

1. $\{\mathcal{S}_1, \ldots, \mathcal{S}_r\}$ *is a partition of* $\mathcal{S}$.
2. *For each* i *and any* $\bar{a} \in \mathcal{S}_i$, $G_i(\bar{a})$ *is a (minimal) Gröbner basis of* $\langle F(\bar{a})\rangle \subset \mathbb{C}[\bar{X}]$ *w.r.t.* $\succ$, *where* $G_i(\bar{a}) = \{g(\bar{a}, \bar{X}) | g(\bar{A}, \bar{X}) \in G_i\}$ *and* $F(\bar{a}) = \{f(\bar{a}, \bar{X}) | f(\bar{A}, \bar{X}) \in F\}$.
3. *For each* i, $\mathrm{LC}_{\succ}(g)(\bar{a}) \neq 0$ *for every* $g \in G_i$ *and* $\bar{a} \in \mathcal{S}_i$.

Remark 4. *The set of leading terms of* $G_i(\bar{a})$ *is invariant for each* $\bar{a} \in \mathcal{S}_i$, *hence the dimension of the ideal* $\langle G_i(\bar{a})\rangle$ *is also invariant. A minimal CGS is desirable for their computation. When the ideal* $\langle G_i(\bar{a})\rangle$ *is zero-dimensional for* $\bar{a} \in \mathcal{S}_i$, *using* $(\mathcal{S}_i, G_i)$ *we can also compute a uniform representation of the HQF* M_h^I *on* $\mathcal{S}_i \cap \mathbb{R}^m$ *for any polynomial* $h \in \mathbb{Q}[\bar{A}, \bar{X}]$. *More precisely, each element is represented by a rational function* $p(\bar{A})/q(\bar{A})$ *with* $p(\bar{A}), q(\bar{A}) \in \mathbb{Q}[\bar{A}]$ *such that* $q(\bar{a}) \neq 0$ *is guaranteed for any* $\bar{a} \in \mathcal{S}_i \cap \mathbb{R}^m$.

2.3 CGS-QE Algorithm

The following result is the most important contribution of our paper [2] for the elimination of the quantifiers $\exists \bar{X}$ from the basic first order formula (1) given in Sect. 1.

Theorem 5. *Let* $\mathcal{S} = \{\bar{a} \in \mathbb{C}^m | \phi(\bar{a})\}$ *and* $\mathcal{G} = \{(\mathcal{S}_1, G_1), \ldots, (\mathcal{S}_r, G_r)\}$ *be a minimal CGS of the parametric saturation ideal* $I : h^\infty$ *on* $\mathcal{S}$ *with parameters* $\bar{A}$ *w.r.t. an arbitrary term order, where* $I = \langle f_1, \ldots, f_s\rangle$ *and* $h = \prod_{1 \leq i \leq t} h_i$. *For each* i *and any* $\bar{a} \in \mathcal{S}_i \cap \mathbb{R}^m$, *the followings are equivalent:*

1. $\exists \bar{X}\ (\bigwedge_{1 \leq i \leq s} f_i(\bar{a}, \bar{X}) = 0 \wedge \bigwedge_{1 \leq i \leq t} h_i(\bar{a}, \bar{X}) > 0)$.
2. $\sum_{(e_1, \ldots, e_t) \in \{0,1\}^t} \mathrm{sign}(M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1} \cdots h_t^{e_t}(\bar{a})}) > 0$.

By Remark 4, for each i we have a uniform representation of $M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1} \cdots h_t^{e_t}(\bar{a})}$ for $\bar{a} \in \mathcal{S}_i \cap \mathbb{R}^m$. Using it together with Descartes' rule of signs, we can construct a quantifier free first order formula $\psi_i(\bar{A})$ such that $\psi_i(\bar{a})$ is equivalent to the property 2 of Theorem 5 for each $\bar{a} \in \mathcal{S}_i \cap \mathbb{R}^m$, then we have a quantifier free first order formula $\phi(\bar{A}) \wedge (\bigvee_{1 \leq i \leq r} \psi_i(\bar{A}))$ equivalent to (1).

An essential and important difference between our CGS-QE algorithm of [2] and the original CGS-QE algorithm of [6] is that our algorithm computes a CGS of the saturation ideal $I : h^\infty$ whereas the original computes a CGS of I and use the relation $\sum_{(e_1, \ldots, e_t) \in \{1,2\}^t} \mathrm{sign}(M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1} \cdots h_t^{e_t}(\bar{a})}) > 0$ which is also equivalent to the property 1 of Theorem 5. When $I : h^\infty \neq I$, we have $\dim(\mathbb{R}[\bar{X}]/I) > \dim(\mathbb{R}[\bar{X}]/I : h^\infty)$ and the size of $M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1} \cdots h_t^{e_t}(\bar{a})}$ is smaller in our algorithm, which enables us to have a simpler representation formula of $\psi_i(\bar{A})$. Even when $I : h^\infty = I$, we also have its simpler representation since the polynomial $h_1^{e_1} \cdots h_t^{e_t}$ becomes more complicated if we allow $e_1, \ldots, e_t$ to be 2.

3 New Multivariate Real Roots Counting

As is mentioned at the end of the last section, the size of the HQF $M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ effects the simplicity of the representation formula of $\psi_i(\bar{A})$. Note that we can replace $M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ with $M^{\sqrt{\langle G_i(\bar{a})\rangle}}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ in Theorem 5. If $\langle G_i(\bar{a})\rangle$ is not a radical ideal, $\dim(\mathbb{R}[\bar{X}]/\langle G_i(\bar{a})\rangle) > \dim(\mathbb{R}[\bar{X}]/\sqrt{\langle G_i(\bar{a})\rangle})$ and we may have a simpler representation formula of $\psi_i(\bar{A})$ using a CGS of the radical ideal $\sqrt{I:h^\infty}$.

Example 6. *Consider the following simple example in a form of the basic first order formula:* $A \neq 0 \wedge \exists X((X-A)^2 = 0 \wedge X > 0)$. $\phi(A)$ *is* $A \neq 0$, *the parametric ideal* I *is* $\langle (X-A)^2\rangle$ *and* $h = X$. *A minimal CGS* $\mathcal{G}$ *of the parametric saturation ideal* $I : h^\infty$ *on* $\mathcal{S} = \{a \in \mathbb{C} | a \neq 0\}$ *has the form* $\mathcal{G} = \{(\mathcal{S}, \{(X-A)^2\})\}$, *whereas a minimal CGS* $\mathcal{G}'$ *of the radical ideal* $\sqrt{I:h^\infty}$ *on* $\mathcal{S}$ *has the form* $\mathcal{G}' = \{(\mathcal{S}, \{X-A\})\}$. *Let* $G = \{(X-A)^2\}$ *and* $G' = \{X-A\}$. *We have the following uniform representations of the HQFs on* $\mathcal{S} \cap \mathbb{R}$:

$$M_1^{\langle G\rangle} = \begin{pmatrix} 2 & 2A \\ 2A & 2A^2 \end{pmatrix}, \quad M_X^{\langle G\rangle} = \begin{pmatrix} 2A & 2A^2 \\ 2A^2 & 2A^3 \end{pmatrix}, \quad M_1^{\langle G'\rangle} = \begin{pmatrix} 1 \end{pmatrix}, \quad M_X^{\langle G'\rangle} = \begin{pmatrix} A \end{pmatrix}.$$

Applying Descartes' rule of signs and the simplification technique introduced in the Sect. 3 of [3] *to the characteristic polynomials of* $M_1^{\langle G\rangle}$ *and* $M_X^{\langle G\rangle}$, *(although we do not need them for this simple example), we have an equivalent quantifier free formula:*

$$A \neq 0 \wedge A^2 + 1 > 0 \wedge A^3 + A > 0.$$

On the other hand, if we use the characteristic polynomials of $M_1^{\langle G'\rangle}$ *and* $M_X^{\langle G'\rangle}$, *we have a much simpler equivalent quantifier free formula:*

$$A \neq 0 \wedge 1 > 0 \wedge A > 0.$$

3.1 Main Result

Though a CGS of the radical ideal $\sqrt{I:h^\infty}$ may reduce the size of HQFs, a radical computation is generally very heavy for a parametric polynomial ring. In this section, we show a new result Theorem 8. It brings us a new CGS-QE method which does not use any radical computation but produces a quantifier free formula as simple as the one obtained using a CGS of the radical ideal.

Notation 7. *For a* $q \times q$ *square matrix* M *and* $1 \leq b_1 < \ldots < b_k \leq q$, $M(b_1, \ldots, b_k)$ *denotes a* $k \times k$ *square matrix such that its* (i,j)*-th component is the* (b_i, b_j)*-th component of* M *for each* $i, j (1 \leq i, j \leq k)$.

We have the following property similar to Theorem 1.

Theorem 8. *Let* I *be a zero-dimensional ideal of* $\mathbb{R}[\bar{X}]$ *such that* $\dim(R[\bar{X}]/I) = q$ *and* $\mathrm{rank}(M_1^I) = k$, *note that* M_1^I *is a* $q \times q$ *matrix, hence* $k \leq q$. *Then there exists a* $k-$*tuple* $(b_1, \ldots, b_k)$ *of integers such that* $1 \leq b_1 < \ldots < b_k \leq q$ *and*

$\det(M_1^I(b_1,\ldots,b_k)) \neq 0$. *For any such a* $k-$*tuple, we have the following equation for every polynomial* $h \in \mathbb{R}[\bar{X}]$*:*

$$\mathrm{sign}(N_h^I) = \#(\{\bar{x} \in V_{\mathbb{R}}(I) | h(\bar{x}) > 0\}) - \#(\{\bar{x} \in V_{\mathbb{R}}(I) | h(\bar{x}) < 0\}),$$

where N_h^I *denote a* $k \times k$ *real symmetric matrix* $M_h^I(b_1,\ldots,b_k)$.

By this theorem, we can replace $M^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ with $N^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ in Theorem 5. Since $\dim(\mathbb{R}[\bar{X}]/\sqrt{\langle G_i(\bar{a})\rangle}\ ) = \mathrm{rank}(M_1^{\langle G_i(\bar{a})\rangle})$ by the theory of roots counting, $N^{\langle G_i(\bar{a})\rangle}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ and $M^{\sqrt{\langle G_i(\bar{a})\rangle}}_{h_1^{e_1}\cdots h_t^{e_t}(\bar{a})}$ have a same size and we can obtain a simple formula.

Example 9. *For the HQF* $M_1^{\langle G\rangle}$ *in the previous example,* $q = 2$ *and* $k = 1$*. We may have* $b_1 = 1$ *or* $b_1 = 2$*. For* $b_1 = 1$*, we have* $N_1^{\langle G\rangle} = (2)$ *and* $N_X^{\langle G\rangle} = (2A)$ *which produces the same formula* $A \neq 0 \wedge 1 > 0 \wedge A > 0$ *as the formula obtained using the radical ideal. On the other hand, for* $b_1 = 2$*, we have* $N_1^{\langle G\rangle} = (2A)$ *and* $N_X^{\langle G\rangle} = (2A^3)$ *which produces the formula* $A \neq 0 \wedge A^2 > 0 \wedge A^3 > 0$.

4 Conclusion and Remarks

In Example 9, the obtained formula for $b_1 = 2$ does not look much simpler than the one obtained using $M_1^{\langle G\rangle}$ and $M_X^{\langle G\rangle}$. Though the formula obtained using any k-tuple $(b_1,\ldots,b_k)$ is generally simple for a more complicated non-radical ideal I, the choice of k-tuple makes a strong effect on its simplicity. For the choice of a k-tuple we also have obtained the following criterion. Let $\succ$ be an admissible term order of $T(\bar{X})$ and $\{v_1,\ldots,v_q\} = \{v \in T(\bar{X}) | v \notin LT(I)\}$. We can choose $(b_1,\ldots,b_k)$ so that each v_{b_i} is not dividable by v_j for any $j \in \{1,\ldots,q\} \setminus \{b_1,\ldots,b_k\}$. Such a k-tuple produces a simple formula. Note that in the previous example, $b_1 = 1$ satisfies this criterion but $b_1 = 2$ does not.

References

1. http://www.rs.tus.ac.jp/fukasaku/software/CGSQE-20160509/
2. Fukasaku, R., Iwane, H., Sato, Y: Real quantifier elimination by computation of comprehensive Gröbner systems. In: Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 173–180, ACM-Press (2015)
3. Fukasaku, R., Iwane, H., Sato, Y.: On the implementation of CGS real QE. In: Greuel, G.-M., Koch, T., Paule, P., Sommese, A. (eds.) ICMS 2016. LNCS, vol. 9725, pp. 165–172. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-42432-3_21
4. Fukasaku, R., Iwane, H., Sato, Y.: CGSQE/SyNRAC: a real quantifier elimination package based on the computation of comprehensive Gröbner systems. ACM Comm. Comput. Algebra **50**(3), 101–104 (2016)

5. Pedersen, P., Roy, M.-F., Szpirglas, A.: Counting real zeros in the multivariate case. In: Eyssette, F., Galligo, A. (eds.) Computational Algebraic Geometry. PM, vol. 109, pp. 203–224. Birkhäuser Boston, Boston (1993). https://doi.org/10.1007/978-1-4612-2752-6_15
6. Weispfenning, V.: A new approach to quantifier elimination for real algebra. In: Caviness, B.F., Johnson, J.R. (eds.) Quantifier Elimination and Cylindrical Algebraic Decomposition, pp. 376–392. Springer, Vienna (1998). https://doi.org/10.1007/978-3-7091-9459-1_20