Quantifier elimination for small degree polynomials

Chrysida Galanaki[1] and Elias Tsigaridas[2]

[1] Dept. of Informatics and Telecommunications, University of Athens, Greece.
[2] INRIA Méditerranée, and Laboratoire I3S CNRS and the University of Nice, Sophia-Antipolis France.
chysida(AT)di.uoa.gr, elias.tsigaridas(AT)inria.fr

Abstract. We present a special purpose quantifier elimination algorithm, which can eliminate the quantifier $\exists x$, in the formula $(\exists x \in \mathbb{R})[p(x) \wedge g]$, where $p(x)$ is a polynomial of degree ≤ 4, and g is a polynomial inequality.

Keywords: Quantifier elimination, first order theory of reals, small degree polynomial equations

1 Introduction

The problem of quantifier elimination for the first-order theory of real numbers is an interesting challenge, mostly because it lies in the intersection of many areas of mathematics and theoretical computer science. Since the problem proved decidable, due to a celebrated work of Tarksi [8](see also [7]), a lot of efforts were put on the problem, e.g. [6, 1] and references therein. However, due to high complexity of the general problem, several algorithms and variants were proposed for special cases, e.g. [3, 11, 10, 5, 9, 4]. In this note we present a special purpose algorithm for eliminating the quantifier from the formula

$$(\exists x \in \mathbb{R})[p(x) = 0 \wedge (g(x) \, \sigma \, 0)],$$

where p, considered as a polynomial of degree ≤ 4 w.r.t. x, with coefficients that are polynomials in $\mathbb{R}[y_1, \ldots, y_r]$, such that the leading coefficient is always non-zero, g is a polynomial in $\mathbb{R}[y_1, \ldots, y_r, x]$, and $\sigma \in \{<, =, >\}$. It is without loss of generality to assume that the degree of g with respect to x is strictly smaller than that of p.

Our method is based on the method of *virtual substitution* [9], which can treat in a formal and elegant way the cases where the degree of p is ≤ 2. In these cases, roughly speaking, the real roots of p are computed since only square roots are involved, and their values are substituted in g. However, extending this method to cubics and quartic is a very difficult task, since in this case computation of the real roots using radicals demands computations with complex numbers and estimation of *all* the roots. Nevertheless, Weispfenning [10] treated the cubic case, using the derivatives of p, but it is questionable whether and how his approach could be extended to the quartics.

In what follows we will present an algorithm based on Sturm(-Habicht) sequences, that can be extended up to quintics. The novelty of our approach consists of (i) representing the real roots of a polynomial in isolating interval representation, which could be computed even in the case of parametric coefficients, and (ii) using Sturm-Habicht sequences for sign evaluations, the good specialization properties of which guarantee the correctness of our algorithm for any value of the input parameters. Last but not least, if we are able to treat the case where p is a quartic, then we can extend the algorithm to treat cases, like $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})[(p_1(x, y) = 0 \wedge p_2(x, y) = 0) \wedge (g(x, y) \, \sigma \, 0)]$, where the total degree of p_1 and p_2 is 2. This is so because the resultant of p_1 and p_2 w.r.t. x or y, is a quartic and we can compute the real roots of the system, which are pairs of real algebraic numbers, in *isolating interval representation*, even in the case where the coefficients of the polynomials of the system are parameters.

The rest of the paper is structured as follows. In the next section we present in detail the quadratic case, while Sec. 3 presents the cubic and part of the results for the quartic.

(1)	$\Delta < 0$	$\{\}$		$\{+1\}$
(2)	$\Delta = 0$	$\{2\}$	$\gamma_1 = -\frac{a_1}{2a_2}$	$\{+1, 0, +1\}$
(3)	$\Delta > 0$	$\{1, 1\}$	$\gamma_1 \cong [f, (-\infty, -\frac{a_1}{2a_2})]$	$\{+1, 0, -1, 0, +1\}$
			$\gamma_2 \cong [f, (-\frac{a_1}{2a_2}, +\infty)]$	

Table 1. IDS of a quadratic polynomial

2 Quadratic polynomials

Let *Isolation and Discrimination System (IDS)* of a polynomial $p \in \mathbb{R}[x]$ be the finite sequence of different values of $\text{sgn}(p(x))$, as x ranges from $-\infty$ to $+\infty$, and the *isolating interval representation* of its real roots, e.g. [2]. This representation is one of representations of real algebraic numbers and it consists of an interval that contains the real root and a square-free polynomial that has only this real number, as a real root in this interval.

2.1 IDS

Let $p = a_2x^2 + a_1x + a_0$ be a quadratic polynomial, where for reason of simplicity, we assume that $a_2 > 0$. The IDS of p appears in Tab. 1, where $\Delta = a_1^2 - 4a_0a_2$ is its discriminant. The second column contains polynomial inequalities that the coefficients of the polynomial should satisfy, so that the finite sequence of different values of $\text{sgn}(p(x))$ is that of the last column. In the third column there are the multiplicities of the real roots, and in the fourth their isolating interval representation, if any. We say that p is of *type 1*, T_1, if its discriminant is negative, that is it has no real roots. In this case $\text{sgn}(f(x)) = +1$, for all $x \in \mathbb{R}$.

The IDS allows us, given a quadratic polynomial with parametric coefficients, to determine quantifier free formulae $T_i(a_2, a_1, a_0)$, where $1 \leq i \leq 3$, that hold in $\mathbb{R}$, if and only if the polynomial is of type i.

Lemma 1. *Let $p = a_2x^2 + a_1x + a_0$, with parametric coefficients, $a_2 > 0$ and $\Delta = a_1^2 - 4a_0a_2$. Then (i) p of type 1 $\Leftrightarrow T_1 \Leftrightarrow \Delta < 0$, (ii) p of type 2 $\Leftrightarrow T_2 \Leftrightarrow \Delta = 0$, and (iii) p of type 3 $\Leftrightarrow T_3 \Leftrightarrow \Delta > 0$.*

Slightly modifications are needed in the case where $a_2 < 0$. If $a_2 = 0$, we refer the reader to [5] for an extended study.

2.2 Sign evaluation

Assume that we have a polynomial $p \in \mathbb{R}[x]$, with positive leading coefficient, of degree 2, and of some type (either 1, 2 or 3). Assume further a univariate polynomial g with parametric coefficients. Our purpose is to compute quantifier free formulae for the sign of g evaluated over a real root of p. To be more concrete, we want to compute quantifier free formulae $\psi_{d,n,i,j,\sigma}$, where

- d is the degree of p.
- $n = \deg(g) \leq 1$,
- $i =$ real root type of f from IDS (refer to Tab. 1),
- $j =$ root index of f (either 1 or 2), and
- $\sigma \in \{-1, 0, +1\}$, s.t $\sigma = \text{sign}(g(\gamma_j))$.

When p is T_1 the problem is trivial. Moreover, it is without loss of generality to assume that the degree of g is ≤ 2. Thus we have the following cases:

– Let $\deg(g) = 0$, i.e. $g = b_0$. If p is either T_2 or T_3, then

$$\begin{aligned}\psi_{2,0,?,?,-1} &:= b_0 < 0,\\ \psi_{2,0,?,?,0} &:= b_0 = 0,\\ \psi_{2,0,?,?,+1} &:= b_0 > 0,\end{aligned}$$

where the question-mark means that the formula holds for any legal value.

– Let $\deg(g) = 1$, i.e. $g = b_1 x + b_0$, and let $\alpha = -\frac{a_1}{2a_2}$ and $\beta = -\frac{b_0}{b_1}$.
If p is T_2, it has one double real root, which is $\gamma = -\frac{a_1}{2a_2}$ (Tab. 1). In this case $\text{sign}(g(\gamma)) = \text{sign}(g(-\frac{a_1}{2a_2})) = \text{sign}(-b_1 a_1 + 2\, b_0 a_2) = g[\alpha/x]$, and

$$\begin{aligned}\psi_{2,1,2,1,-1} &:= g[\alpha/x] < 0,\\ \psi_{2,1,2,1,0} &:= g[\alpha/x] = 0,\\ \psi_{2,1,2,1,+1} &:= g[\alpha/x] > 0.\end{aligned}$$

If f is T_3, then we proceed as follows. The isolating interval representation of the first real root is $\gamma_1 \cong (f, (-\infty, -\frac{a_1}{2a_2}))$. If $-\frac{b_0}{b_1} \geq -\frac{a_1}{2a_2} \Leftrightarrow g[\alpha/x] \leq 0$, then $\text{sign}(g(\gamma_1)) = -1$. Otherwise $\text{sign}(g(\gamma_1)) = -\text{sign}(f(-\frac{b_0}{b_1})) = -f[\beta/x]$. Hence,

$$\begin{aligned}\psi_{2,1,3,1,-1} &:= g[\alpha/x] \leq 0 \vee (g[\alpha/x] > 0 \wedge f[\beta/x] < 0),\\ \psi_{2,1,3,1,0} &:= g[\alpha/x] > 0 \vee f[\beta/x] = 0,\\ \psi_{2,1,3,1,+1} &:= g[\alpha/x] > 0 \vee f[\beta/x] > 0.\end{aligned}$$

The representation of the second root is $\gamma_2 \cong [f, (-\frac{a_1}{2a_2}, \infty)]$. Now, if $-\frac{b_0}{b_1} \leq -\frac{a_1}{2a_2} \Leftrightarrow g[\alpha/x] \geq 0$, then $\text{sign}(g(\gamma)) = 1$. Otherwise, $\text{sign}(g(\gamma)) = -\text{sign}(f(-\frac{b_0}{b_1})) = -f[\beta/x]$. Hence,

$$\begin{aligned}\psi_{2,1,3,2,-1} &:= g[\alpha/x] < 0 \vee f[\beta/x] > 0,\\ \psi_{2,1,3,2,0} &:= g[\alpha/x] < 0 \vee f[\beta/x] = 0,\\ \psi_{2,1,3,2,+1} &:= g[\alpha/x] \geq 0 \vee (g[\alpha/x] < 0 \wedge f[\beta/x] < 0).\end{aligned}$$

2.3 The general case

Now we consider

$$(\exists x \in \mathbb{R})[p(x) := a_2\, x^2 + a_1\, x + a_0 = 0 \wedge (g(x)\, \sigma\, 0)] \Leftrightarrow \Phi,$$

where $a_2 > 0$, $\sigma \in \{>, =, <\}$, g is a polynomial of degree at most 1, with positive leading coefficient, and Φ is quantifier free formula. The other cases, that is when $a_2 \leq 0$ and/or $\deg(g) > 2$ could be treated similarly. Using the results of the previous sections, and the notation that if $\sigma =<$, resp. $=$ or $>$, then $s = -1$, resp. 0 or 1, it holds that

$$\begin{aligned}\Phi = &((b_1 = 0) \wedge (\psi_{2,0,?,?,\sigma}))\\ &\vee\\ &((b_1 \neq 0) \wedge ((T_2 \wedge \psi_{2,1,2,1,\sigma}) \vee (T_3 \wedge \psi_{2,1,3,1,\sigma} \wedge \psi_{2,1,3,2,\sigma}))).\end{aligned}$$

3 Cubic polynomials

To treat the case of the cubic we work as in the case of the quadratic polynomial. The IDS of the cubic could be seen at Tab. 2. To construct the quantifier free elimination formulae, ψ, that correspond to the sign of

(1)	$\Delta_1 < 0 \wedge P = 0$	$\{1,1,1\}$	$\gamma_1 \cong \left(h, (-\infty, -\frac{2a_2}{3a_3})\right)$ $\gamma_2 = -\frac{2a_2}{3a_3}$ $\gamma_3 \cong \left(h, (-\frac{2a_2}{3a_3}, +\infty)\right)$	$\{-1,0,+1,0,-1,0,+1\}$
(2)	$\Delta_1 < 0 \wedge P < 0$	$\{1,1,1\}$	$\gamma_1 \cong \left(f, (-\infty, -\frac{W}{2\Delta_2})\right)$ $\gamma_2 \cong \left(f, (-\frac{W}{2\Delta_2}, -\frac{a_2}{3a_3})\right)$ $\gamma_3 \cong \left(f, (-\frac{2a_2}{3a_3}, +\infty)\right)$	$\{-1,0,+1,0,-1,0,+1\}$
(3)	$\Delta_1 < 0 \wedge P > 0$	$\{1,1,1\}$	$\gamma_1 \cong \left(f, (-\infty, -\frac{a_2}{3a_3})\right)$ $\gamma_2 \cong \left(f, (-\frac{a_2}{3a_3}, -\frac{W}{2\Delta_2})\right)$ $\gamma_3 \cong \left(f, (-\frac{W}{2\Delta_2}, +\infty)\right)$	$\{-1,0,+1,0,-1,0,+1\}$
(4)	$\Delta_1 > 0 \wedge a_0 = 0$	$\{1\}$	$\gamma_1 = 0$	$\{-1,0,+1\}$
(5)	$\Delta_1 > 0 \wedge a_0 < 0$	$\{1\}$	$\gamma_1 \cong (f, (0, +\infty))$	$\{-1,0,+1\}$
(6)	$\Delta_1 > 0 \wedge a_0 > 0$	$\{1\}$	$\gamma_1 \cong (f, (-\infty, 0))$	$\{-1,0,+1\}$
(7)	$\Delta_1 = 0 \wedge \Delta_2 \neq 0$	$\{1,2\}$	$\gamma_1 = \min\left\{\frac{-W}{2\Delta_2}, \frac{-a_2\Delta_2 + a_3 W}{a_3 \Delta_2}\right\}$ $\gamma_2 = \max\left\{\frac{-W}{2\Delta_2}, \frac{-a_2\Delta_2 + a_3 W}{a_3 \Delta_2}\right\}$	$\{-1,0,-1,0,+1\}$ $\{-1,0,+1,0,+1\}$
(8)	$\Delta_1 = 0 \wedge \Delta_2 = 0$	$\{3\}$	$\gamma_1 = -\frac{2a_2}{3a_3}$	$\{-1,0,+1\}$

Table 2. The IDS of the cubic.

the evaluations of a polynomial g over the roots of p, we will use signed polynomial remainder sequences, and to be more specific Sturm-Habicht sequences [1]. Now, it is without loss of generality to assume that the degree of g is at most 2. By $\mathbf{SR}(P,Q)$ we denote the signed polynomial remainder sequence of P and Q, by $\mathbf{SR}(P,Q\,;\,a)$ the evaluation of the sequence over a number a, and by $\textsc{var}[\mathbf{SR}(P,Q\,;\,a)]$ the number of the sign variations of the evaluated sequence. We need the following lemma

Lemma 2 (Schwartz-Sharir). *Let $P, Q \in \mathbb{R}[x]$ be (relatively prime) polynomials. If $a < b$ are both non-roots of P and γ ranges over the roots of P in $[a,b]$, then*

$$\textsc{var}[\mathbf{SR}(P,Q\,;\,a)] - \textsc{var}[\mathbf{SR}(P,Q\,;\,b)] = \sum_{\gamma} \operatorname{sign}(P'(\gamma)Q(\gamma)).$$

where P' is the derivative of P.

Notice that, if P has *only one* real root in $[a,b]$, then the previous lemma computes $\operatorname{sign}(Q(\gamma))$.

The idea is the following. We want to compute $\operatorname{sign}(\gamma)$, where γ is a real root of f, which we have in isolating interval representation. We can compute symbolically the two evaluated sequences of Lem. 2, and we can consider all the possible sign variations. This will give us all the possible formulae ψ. To make this more clear, let $\gamma \cong (f, (\mathrm{a}, \mathrm{b}))$, where $f = a_3x^3 + a_2x^2 + a_1x + a_0$, $g = b_2x^2 + b_1x + b_0$, and $a_3b_2 \neq 0$. We pre-compute the Sturm-Habicht sequences for symbolic values of the coefficients. That is, let $\mathbf{SR}(p,g) = (\mathbf{SR}_2, \mathbf{SR}_2, \mathbf{SR}_1, \mathbf{SR}_0)$, where

$$\begin{aligned}
\mathbf{SR}_3 &= f \\
\mathbf{SR}_2 &= h_{22}x^2 + h_{21}x + h_{20} \\
\mathbf{SR}_1 &= h_{11}x + h_{10} \\
\mathbf{SR}_0 &= h_0
\end{aligned}$$

and

$$\begin{aligned}
h_{22} &= K_1 \\
h_{21} &= K_2 \\
h_{20} &= K_3 \\
h_{11} &= -K_1K_7 + K_2K_6 \\
h_{10} &= -K_1K_4 + K_3K_6 \\
h_0 \;\; &= -K_1K_7K_5 + K_1K_4K_8 - K_6K_3K_8 + K_6K_2K_5 - K_7K_2K_4 + K_3{K_7}^2
\end{aligned}$$

(1) $\Delta_1 > 0 \wedge T > 0 \wedge \Delta_2 > 0$	$\{1,1,1,1\}$
(2) $\Delta_1 > 0 \wedge (T \leq 0 \vee \Delta_2 \leq 0)$	$\{\}$
(3) $\Delta_1 < 0$	$\{1,1\}$
(4) $\Delta_1 = 0 \wedge T > 0$	$\{2,1,1\}$
(5) $\Delta_1 = 0 \wedge T < 0$	$\{2\}$
(6) $\Delta_1 = 0 \wedge T = 0 \wedge \Delta_2 > 0 \wedge R = 0$	$\{2,2\}$
(7) $\Delta_1 = 0 \wedge T = 0 \wedge \Delta_2 > 0 \wedge R \neq 0$	$\{3,1\}$
(8) $\Delta_1 = 0 \wedge T = 0 \wedge \Delta_2 < 0$	$\{\}$
(9) $\Delta_1 = 0 \wedge T = 0 \wedge \Delta_2 = 0$	$\{4\}$

Table 3. Part of the IDS of the quartic

where $K_i, 1 \leq i \leq 8$ elements of the Bézout matrix of p and g, which is

$$\text{Bézout}(f,g) = \begin{pmatrix} K_1 & K_2 & K_3 \\ K_6 & K_7 & K_4 \\ K_7 & K_8 & K_5 \end{pmatrix} = \begin{pmatrix} b_2 & b_1 & b_0 \\ a_3b_1 - b_2a_2 & b_0a_3 - b_2a_1 & -b_2a_0 \\ b_0a_3 - b_2a_1 & b_0a_2 - b_2a_0 - a_1b_1 & -a_0b_1 \end{pmatrix}$$

Now we observe that

$$\begin{pmatrix} a_3 & a_2 & a_1 & a_0 \\ 0 & h_{22} & h_{21} & h_{20} \\ 0 & 0 & h_{11} & h_{10} \\ 0 & 0 & 0 & h_0 \end{pmatrix} \begin{pmatrix} \mathsf{a}^3 & \mathsf{b}^3 \\ \mathsf{a}^2 & \mathsf{b}^2 \\ \mathsf{a} & \mathsf{b} \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{SR}_3(\mathsf{a}) & \mathbf{SR}_3(\mathsf{b}) \\ \mathbf{SR}_2(\mathsf{a}) & \mathbf{SR}_2(\mathsf{b}) \\ \mathbf{SR}_1(\mathsf{a}) & \mathbf{SR}_1(\mathsf{b}) \\ \mathbf{SR}_0 & \mathbf{SR}_0 \end{pmatrix} = (\, M_1 \;\; M_2 . \,)$$

or in a more compact form

$$\text{sign}(g(\gamma)) = [\text{VAR}(M_1) - \text{VAR}(M_2)] \cdot [\text{sign}(f(\mathsf{a}) - f(\mathsf{b}))].$$

We (pre-)compute all the possible sign combinations, there are $\leq 2 \times 3^5 = 486$, and derive the corresponding formulae $\psi_{2,?,?,\{-1,0,-1\}}$. Nevertheless, we are not sure that all the conditions are realizable. There are techniques to further simplify these formulae.

It is important to state that the previous technique could be applied, only in the case where we have isolating intervals for the real roots, even in the case where the coefficients of the polynomials are parameters. This is exactly the use-fullness of the IDS.

The IDS of the quartic is a little more complicated, and we omit its detailed presentation for reasons of space. Part of it could be seen in Tab. 3, where ($\Delta_1 = A^3 - 27B^2$), and

$$\begin{array}{llll} \Delta_2 = b^2 - ac, & \Delta_3 = c^2 - bd, & T = -9W_1^2 + 27\Delta_2\Delta_3 - 3W_3\Delta_2, \\ A = W_3 + 3\Delta_3, & \Delta_4 = d^2 - ce, & T_1 = -W_3\Delta_2 - 3\,W_1^2 + 9\,\Delta_2\Delta_3, \\ B = -dW_1 - e\Delta_2 - c\Delta_3, & W_1 = ad - bc, & T_2 = AW_1 - 9\,bB, \\ W_2 = be - cd, & W_3 = ae - bd, & R = aW_1 + 2b\Delta_2. \end{array}$$

Acknowledgments The second author is partially supported by contract ANR-06-BLAN-0074 "Decotes". We thank prof. Volker Weispfenning for various discussions on the subject.

References

1. S. Basu, R. Pollack, and M-F.Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2nd edition, 2006.

2. I. Emiris and E. Tsigaridas. Real algebraic numbers and polynomial systems of small degree. *Theoretical Computer Science*, 409(2):186–199, 2008.
3. H. Hong. Quantifier elimination for formulas constrained by quadratic equations via slope resultants. *The Computer Journal*, 36(5):439–449.
4. D. Lazard. Quantifier elimination: optimal solution for two classical examples. *Journal of Symbolic Computation*, 5(1-2):261–266, 1988.
5. R. Loos and V. Weispfenning. Applying linear quantifier elimination. *The Computer Journal*, 36(5):450–462, 1993.
6. J. Renegar. On the Computational Complexity and Geometry of the First-Order Theory of the Reals. (Parts I–III). *Journal of Symbolic Computation*, 13:255–352, 1992.
7. A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, pages 365–374, 1954.
8. A. Tarski and J. McKinsey. A decision method for elementary algebra and geometry. *Bull. Amer. Math. Soc. 59 (1953), 91-93. DOI: 10.1090/S0002-9904-1953-09664-1 PII: S*, 2(9904):09664–1, 1953.
9. V. Weispfenning. *A new approach to quantifier elimination for real algebra*. Fak. für Math. und Informatik, Univ. Passau; Niedersächsische Staats-und Universitätsbibliothek, 1993.
10. V. Weispfenning. Quantifier elimination for real algebra-the cubic case. In *Proceedings of the international symposium on Symbolic and algebraic computation*, pages 258–263. ACM New York, NY, USA, 1994.
11. V. Weispfenning. Quantifier elimination for real algebra–the quadratic case and beyond. *Applicable Algebra in Engineering, Communication and Computing*, 8(2):85–101, 1997.