

# Bounding the radii of balls meeting every connected component of semi-algebraic sets

SAUGATA BASU    MARIE-FRANÇOISE ROY

## Abstract

We prove explicit bounds on the radius of a ball centered at the origin which is guaranteed to contain all bounded connected components of a semi-algebraic set  $S \subset \mathbb{R}^k$  defined by a quantifier-free formula involving  $s$  polynomials in  $\mathbb{Z}[X_1, \dots, X_k]$  having degrees at most  $d$ , and whose coefficients have bit-sizes at most  $\tau$ . Our bound is an explicit function of  $s, d, k$  and  $\tau$ , and does not contain any undetermined constants. We also prove a similar bound on the radius of a ball guaranteed to intersect every connected component of  $S$  (including the unbounded components). While asymptotic bounds of the form  $2^{\tau d^{O(k)}}$  on these quantities were known before, some applications require bounds which are explicit and which hold for all values of  $s, d, k$  and  $\tau$ . The bounds proved in this paper are of this nature.

## 1 Introduction

Let  $S \subset \mathbb{R}^k$  be a semi-algebraic subset of  $\mathbb{R}^k$  defined by a quantifier-free formula whose atoms are of the form  $P \{ >, <, = \} 0, P \in \mathcal{P}$ , where  $\mathcal{P} \subset \mathbb{Z}[X_1, \dots, X_k]$  is a set of polynomials, with  $\#\mathcal{P} = s$ ,  $\deg(P) \leq d$  for  $P \in \mathcal{P}$ , and the bit-sizes of the coefficients of  $P \in \mathcal{P}$  are bounded by  $\tau$ . In this paper we consider the problem of obtaining an upper bound on the radius of a ball guaranteed to *contain* all *bounded* semi-algebraically connected components of  $S$ , as well as on the radius of a ball guaranteed to *meet* every semi-algebraically connected component of  $S$ . Such bounds have many applications in different areas of mathematics as well as computer science. For instance, bounds of these types play a critical role in recent work on proving uniform bounds in the infinitesimal version of Hilbert's sixteenth problem [2, 3], as well as in proving certain lower bounds in computer science [5].

We obtain explicit upper bounds (in terms of  $s, d, k$  and  $\tau$ ) on the radii of such balls in each of the two cases mentioned above. Our bounds are slightly better in the special case when the semi-algebraic set  $S$  is a real algebraic variety defined by one polynomial equation (in this case  $s = 1$ ). Indeed, the bound in the general case is proved by reducing the problem to this special case. Hence, we first prove the results for algebraic sets in Section 4, and prove the bounds for general semi-algebraic sets in Section 5.

### 1.1 History

Asymptotic bounds on the radius of a ball guaranteed to meet all connected components of a semi-algebraic subset of  $\mathbb{R}^k$  defined by a quantifier-free formula involving polynomials in  $\mathbb{Z}[X_1, \dots, X_k]$  in terms of the number  $s$ , the maximum degree  $d$ , and the maximum bit-size  $\tau$  of the coefficients of the defining polynomials, were known before. The best of these bounds were of the form  $2^{\tau d^{O(k)}}$  [1, 4, 7], with undetermined constants, and it seems that there is little hope to improve them in a significant way. While such bounds are already useful in many contexts, certain applications might require more precise and completely explicit estimates valid for all values of  $s, d, k$ , and  $\tau$ . This is what we do in this paper.

## 2 Main Results

### 2.1 Some notation

We first fix some notation.

Let  $\mathbb{R}$  be a real closed field. If  $\mathcal{P}$  is a finite subset of  $\mathbb{R}[X_1, \dots, X_k]$ , we write the **set of zeros** of  $\mathcal{P}$  in  $\mathbb{R}^k$  as

$$\text{Zer}(\mathcal{P}, \mathbb{R}^k) = \{x \in \mathbb{R}^k \mid \bigwedge_{P \in \mathcal{P}} P(x) = 0\}.$$

A **sign condition** on  $\mathcal{P}$  is an element of  $\{0, 1, -1\}^{\mathcal{P}}$ , i.e. a mapping from  $\mathcal{P}$  to  $\{0, 1, -1\}$ .

We say that  $\mathcal{P}$  **realizes** the sign condition  $\sigma$  at  $x \in \mathbb{R}^k$  if  $\bigwedge_{P \in \mathcal{P}} \text{sign}(P(x)) = \sigma(P)$ .

The **realization of the sign condition**  $\sigma$

$$\text{Reali}(\sigma) = \{x \in \mathbb{R}^k \mid \bigwedge_{P \in \mathcal{P}} \text{sign}(P(x)) = \sigma(P)\}.$$

The sign condition  $\sigma$  is **realizable** if  $\text{Reali}(\sigma)$  is non-empty.

Given an integer  $n$ , we denote by  $\text{bit}(n)$  the number of bits of its absolute value in the binary representation.

The main results of the paper can now be stated as follows. Our results in the algebraic case are slightly better than in the semi-algebraic case and we state them separately.

### 2.2 Algebraic Case

**Theorem 1.** *(Ball containing all bounded components) Let  $Q \in \mathbb{Z}[X_1, \dots, X_k]$  be a polynomial with  $\deg(Q) = d$ , and suppose that the coefficients of  $Q$  in  $\mathbb{Z}$  have bitsizes at most  $\tau$ . Then, every bounded semi-algebraically connected component of  $\text{Zer}(Q, \mathbb{R}^k)$  is contained inside a ball centered at the origin of radius*

$$k^{1/2} (N + 1) 2^{N(kd+2)(\tau + \text{bit}(N) + \text{bit}(d+1))}$$

where

$$N = (d + 1)d^{k-1}.$$

In particular, all isolated points of  $\text{Zer}(Q, \mathbb{R}^k)$  are contained inside the same ball.

**Theorem 2.** *(Ball meeting all components) Let  $Q \in \mathbb{Z}[X_1, \dots, X_k]$  be a polynomial of degree with  $\deg(Q) = d$  and suppose that the coefficients of  $Q$  in  $\mathbb{Z}$  have bitsizes at most  $\tau$ . Then there exists a ball centered at the origin of radius bounded by*

$$\left( (2DN(2N-1) + 1) 2^{(2N-1)\tau' + N^2 \text{bit}(N+1)} \right)^{1/2}$$

intersecting every semi-algebraically connected component of  $\text{Zer}(Q, \mathbb{R}^k)$ , where

$$\begin{aligned} D &= kd' - 2(k-1), \\ N &= d'(d'-1)^{k-1}, \\ \tau' &= 2ND\tau + N(\rho + \rho'), \end{aligned}$$

with

$$\begin{aligned} d' &= \sup(2(d+1), 6), \\ \rho &= D(k \operatorname{bit}(d+1) + \operatorname{bit}(d') + 1 + 4 \operatorname{bit}(2D+1) + \operatorname{bit}(N)) - 2 \operatorname{bit}(2D+1), \\ \rho' &= (2k-2) \operatorname{bit}(N) + k \operatorname{bit}(k) + 2 \operatorname{bit}(2DN+1) + 1. \end{aligned}$$

### 2.3 Semi-algebraic case

**Theorem 3.** *Given a set  $\mathcal{P} = \{P_1, \dots, P_s\} \subset \mathbb{Z}[X_1, \dots, X_k]$  with  $\deg(P) \leq d, P \in \mathcal{P}$ , such that the bitsizes of the coefficients of  $P \in \mathcal{P}$  are bounded by  $\tau$ , there exists a ball centered at the origin of radius bounded by*

$$k^{1/2} (N+1) 2^{N(2kd+2)(2\tau + \operatorname{bit}(N) + (k+1)\operatorname{bit}(d+1) + \operatorname{bit}(s))},$$

where

$$N = (2d+1)(2d)^{k-1},$$

which contains every bounded semi-algebraically connected component of the realization of every realizable sign condition on  $\mathcal{P}$ .

**Theorem 4.** *Given a set  $\mathcal{P} = \{P_1, \dots, P_s\} \subset \mathbb{Z}[X_1, \dots, X_k]$  with  $\deg(P) \leq d, P \in \mathcal{P}$ , such that the bitsizes of the coefficients of  $P \in \mathcal{P}$  are bounded by  $\tau$ , there exists a ball centered at the origin of radius*

$$\left( (2DN(2N-1) + 1) 2^{(2N-1)\tau'' + N^2 \operatorname{bit}(N+1)} \right)^{1/2}$$

intersecting every semi-algebraically connected component of  $\operatorname{Zer}(Q, \mathbb{R}^k)$ , where

$$\begin{aligned} D &= kd' - 2(k-1), \\ N &= d'(d'-1)^{k-1}, \\ \tau'' &= 2ND(2\tau + k \operatorname{bit}(d+1) + \operatorname{bit}(s)) + N(\rho + \rho'), \end{aligned}$$

with

$$\begin{aligned} d' &= \sup(2(d+1), 6), \\ \rho &= D(k \operatorname{bit}(d+1) + \operatorname{bit}(d') + 1 + 4 \operatorname{bit}(2D+1) + \operatorname{bit}(N)) - 2 \operatorname{bit}(2D+1), \\ \rho' &= (2k-2) \operatorname{bit}(N) + k \operatorname{bit}(k) + 2 \operatorname{bit}(2DN+1) + 1, \end{aligned}$$

which meets every semi-algebraically connected component of the realization of every realizable sign condition on  $\mathcal{P}$ .

**Remark 5.** Note that all the bounds above are of the form  $2^{\tau d^{O(k)}}$ , similarly to the results obtained in [1, 4, 7]. The only point which needs some explanation is the fact that  $s$  plays a role in our estimates for the semi-algebraic case, while it does not appear in the formula  $2^{\tau d^{O(k)}}$ . This is because the total number of polynomials of degree  $d$  in  $k$  variables with bitsize bounded by  $\tau$  is bounded by  $(2^\tau)^{\binom{d+k}{k}} = 2^{\tau d^{O(k)}}$ .  $\square$

## 3 Preliminaries

In order to prove the bounds on the radii of various balls we need a careful analysis of the bit sizes of the entries of certain matrices corresponding to multiplication by certain variables in a zero-dimensional ideal of a very special type. This analysis appearing in [1] is similar in spirit to the techniques in [6]. We reproduce here the results (without proofs which appear in [1]) for the benefit of the readers.

Let  $D$  be an ordered domain. We first define a special type of Groebner basis with coefficients in  $D$ . We say that  $\mathcal{G}(Y, Z)$  is a **parametrized special Groebner basis** if it is of the form

$$\mathcal{G}(Y, Z) = \{Z X_1^{d_1} + Q_1(Y, X), \dots, Z X_k^{d_k} + Q_k(Y, X)\}$$

with  $Q_i \in D[Y][X_1, \dots, X_k]$ ,  $\deg(Q_i) < d_i$ ,  $\deg_{X_j}(Q_i) < d_j$ ,  $i \neq j$ , where  $\deg$  is the total degree with respect to the variables  $X_1, \dots, X_k$ ,  $d_1 \geq \dots \geq d_k \geq 1$ , and  $Z$  is either a new variable or one of the variables  $Y_1, \dots, Y_\ell$ . Define  $\overline{\text{Mon}}(\mathcal{G})(Z)$  as the set of elements  $Z^{|\alpha|} X^\alpha = Z^{|\alpha|} X_1^{\alpha_1} \dots X_k^{\alpha_k}$  with  $\alpha_i < d_i$  and  $\overline{\text{Bor}}(\mathcal{G})(Z)$  as the set of elements  $Z^{|\alpha|} X^\alpha$  such that  $\alpha_i = d_i$  for some  $i \in \{1, \dots, k\}$  and  $\alpha_i \leq d_i$  for any  $i \in \{1, \dots, k\}$ .

The following algorithm is described in [1]. Here we just recall the input, output and the estimates on the bit-sizes of the output.

**Algorithm 1. [Parametrized Special Matrices of Multiplication]**

- **Structure:** a ring  $D$  contained in a field  $K$ .
- **Input:** a parametrized special Grobner basis

$$\mathcal{G} = \{Z X_1^{d_1} + Q_1(Y, X), \dots, Z X_k^{d_k} + Q_k(Y, X)\} \subset D[Y, Z][X_1, \dots, X_k]$$

with  $Y = (Y_1, \dots, Y_\ell)$ .

- **Output:** parametrized matrices of multiplication by the variables in the basis  $\overline{\text{Mon}}(\mathcal{G})(Z)$ : i.e. for every variable  $X_i$  the matrix  $M'_i(Y, Z)$  with entries in  $D[Y, Z]$  such that for every  $(y, z) \in \mathbb{C}^{\ell+1}$  such that  $z \neq 0$ , the matrix  $M'_i(y, z)$  is the of multiplication by  $z X_1, \dots, z X_k$ , expressed in the basis  $\overline{\text{Mon}}(\mathcal{G})(z)$ .

**Bit-size estimate:**

Let  $N = d_1 \dots d_k$ ,  $D = (d_1 + \dots + d_k - k + 1)$ . The entries of the matrix  $M'_i$  of multiplication by  $Z X_i$  in  $\overline{\text{Mon}}(\mathcal{G})(Z)$ , have degrees in  $Z$  bounded by  $D$  and degrees in  $Y$  bounded by  $D \lambda$ .

When  $D = \mathbb{Z}$ , the bitsize of the matrix  $M'_i$  of multiplication by  $Z X_i$  in  $\overline{\text{Mon}}(\mathcal{G})(Z)$  are bounded by

$$D(\tau + 2\ell \text{bit}(D \lambda + 1) + \text{bit}(N)) - \ell \text{bit}(D \lambda + 1) - \text{bit}(N). \quad \square$$

## 4 Algebraic Case.

In this section we prove Theorems 1 and 2.

We first introduce some notation. Let  $\mathbb{R}$  be a real closed field. For any polynomial  $P \in \mathbb{R}[X_1, \dots, X_k]$ , let  $\text{Zer}_b(P, \mathbb{R}^k)$  denote the union of the semi-algebraically connected components of  $\text{Zer}(P, \mathbb{R}^k)$  which are bounded over  $\mathbb{R}$ . We denote by  $\mathbb{R}\langle\varepsilon\rangle$  the real closed field of algebraic Puiseux series in  $\varepsilon$  with coefficients in  $\mathbb{R}$ . The elements of  $\mathbb{R}\langle\varepsilon\rangle$  with non-negative order constitute a valuation ring denoted  $\mathbb{R}\langle\varepsilon\rangle_b$ . The elements of  $\mathbb{R}\langle\varepsilon\rangle_b$  are exactly the elements of  $\mathbb{R}\langle\varepsilon\rangle$  bounded over  $\mathbb{R}$  (i.e. their absolute value is less than a positive element of  $\mathbb{R}$ ). We denote by  $\lim_\varepsilon$  the ring homomorphism from  $\mathbb{R}\langle\varepsilon\rangle_b$  to  $\mathbb{R}$  which maps  $\sum_{i \in \mathbb{N}} a_i \varepsilon^{i/q}$  to  $a_0$ . The mapping  $\lim_\varepsilon$  simply replaces  $\varepsilon$  by 0 in a bounded Puiseux series.

**Proof of Theorem 1:** In order to find a bound on the radius of a ball containing  $\text{Zer}_b(Q, \mathbb{R}^k)$ , it is enough to find an interval  $[a, b]$  such that.

$$\text{Zer}_b(Q, \mathbb{R}^k) \subset [a, b] \times \mathbb{R}^{k-1}.$$

We are going to prove that it is possible to obtain such an interval from an interval  $[a', b']$  such that the cylinder based on  $[a', b']$  contains all the connected components bounded over  $\mathbb{R}$  of the zero sets of a convenient deformation of  $Q$ .

Let  $\zeta$  be a new variable. We define

$$\begin{aligned} Q_\zeta^+ &= Q + \frac{\zeta}{d+1} (X_1^{d+1} + \dots + X_k^{d+1}), \\ Q_\zeta^- &= Q - \frac{\zeta}{d+1} (X_1^{d+1} + \dots + X_k^{d+1}). \end{aligned}$$

Observe that  $\text{Zer}(Q_\zeta^+, \mathbb{R}\langle \zeta \rangle^k)$  (resp.  $\text{Zer}(Q_\zeta^-, \mathbb{R}\langle \zeta \rangle^k)$ ) is an hypersurface with isolated singular points since the ideal generated by

$$\frac{\partial Q_\zeta^+}{\partial X_1}, \dots, \frac{\partial Q_\zeta^+}{\partial X_k} \left( \text{resp. } \frac{\partial Q_\zeta^-}{\partial X_1}, \dots, \frac{\partial Q_\zeta^-}{\partial X_k} \right)$$

is zero-dimensional.

Note that if  $C$  is a bounded semi-algebraically connected component of  $\text{Zer}(Q, \mathbb{R}^k)$ , there exists a finite number of semi-algebraically connected components  $C_1, \dots, C_c$  of  $\text{Zer}(Q_\zeta^+, \mathbb{R}\langle \zeta \rangle^k) \cup \text{Zer}(Q_\zeta^-, \mathbb{R}\langle \zeta \rangle^k)$ , bounded over  $\mathbb{R}$  such that

$$C = \lim_{\zeta} (C_1 \cup \dots \cup C_c).$$

In order to see this first observe that

$$\text{Zer}(Q_\zeta^+, \mathbb{R}\langle \zeta \rangle^k) \cup \text{Zer}(Q_\zeta^-, \mathbb{R}\langle \zeta \rangle^k) = \text{Zer}(Q_\zeta, \mathbb{R}\langle \zeta \rangle^k),$$

where

$$Q_\zeta = Q^2 - \left( \frac{\zeta}{d+1} \right)^2 (X_1^{d+1} + \dots + X_k^{d+1})^2,$$

Moreover, the polynomial  $(X_1^{d+1} + \dots + X_k^{d+1})^2$  is non-negative everywhere in  $\mathbb{R}^k$ . Now apply Proposition 12.37 in [1], after noting that by Proposition 12.35  $\lim_{\zeta}$  of a semi-algebraically connected component of  $\text{Zer}(Q_\zeta, \mathbb{R}\langle \zeta \rangle^k)$  bounded over  $\mathbb{R}$  remains semi-algebraically connected and bounded over  $\mathbb{R}$ .

This implies that, denoting by  $\pi$  the projection to the  $X_1$ -axis,

$$\pi(C) = \lim_{\zeta} (\pi(C_1 \cup \dots \cup C_c)). \quad (1)$$

Let  $[a, b] = \pi(C)$ , and  $a_\zeta$  and  $b_\zeta$  be the minimum and maximum of  $\pi(C_1 \cup \dots \cup C_c)$ . It follows from (1) that  $\lim_{\zeta} (a_\zeta) = a$ ,  $\lim_{\zeta} (b_\zeta) = b$ .

In order to describe  $a_\zeta$  and  $b_\zeta$ , we introduce zero-dimensional polynomial systems whose solutions correspond to critical points of  $\text{Zer}(Q_\zeta^+, \mathbb{R}\langle \zeta \rangle^k)$  (resp.  $\text{Zer}(Q_\zeta^-, \mathbb{R}\langle \zeta \rangle^k)$ ) in the  $X_1$ -direction, and compute the characteristic polynomials  $\chi^+(\zeta, T)$  (resp.  $\chi^-(\zeta, T)$ ) of the multiplication by  $\zeta X_1$  (to avoid denominators). Since  $a_\zeta$  and  $b_\zeta$  are extremal values of  $\pi$  on  $C_1 \cup \dots \cup C_c$ , they are roots of the polynomials  $F^+(\zeta, T) \in \mathbb{R}[\zeta, T]$  and  $F^-(\zeta, T) \in \mathbb{R}[\zeta, T]$  obtained by substituting  $\frac{T}{\zeta}$  to  $T$  and multiplying by the minimum power of  $\zeta$  necessary to avoid denominators  $\square$

**Proof of Theorem 2:** For bounded connected components of  $\text{Zer}(Q, \mathbb{R}^k)$ , we apply the previous theorem.

To deal with unbounded connected components, let  $\varepsilon$  be a new variable. We define

$$Q_\varepsilon = Q^2 + (\varepsilon(X_1^2 + \cdots + X_k^2) - 1)^2. \quad (2)$$

Notice that the extension to  $\mathbb{R}\langle\varepsilon\rangle$  of every unbounded connected component of  $\text{Zer}(Q, \mathbb{R}^k)$  meets  $\text{Zer}(Q^2 + (\varepsilon(X_1^2 + \cdots + X_k^2) - 1)^2, \mathbb{R}\langle\varepsilon\rangle^k)$  and that  $\text{Zer}(Q_\varepsilon, \mathbb{R}\langle\varepsilon\rangle^k)$  is contained in the ball  $\overline{B}(0, \varepsilon^{-1/2})$ . So  $\overline{B}(0, \varepsilon^{-1/2})$  intersects the extension to  $\mathbb{R}\langle\varepsilon\rangle$  of every unbounded connected component of  $\text{Zer}(Q, \mathbb{R}^k)$ . We then replace  $\varepsilon$  by a small enough positive  $u \in \mathbb{R}$  and prove that  $\overline{B}(0, u^{-1/2})$  intersects every unbounded connected component of  $\text{Zer}(Q, \mathbb{R}^k)$ .

Noting that  $Q_\varepsilon$  is everywhere non-negative, we can proceed as in the proof of Theorem 1 and take

$$Q_{\varepsilon, \zeta} = Q_\varepsilon - \frac{\zeta}{d'}(X_1^{d'} + \cdots + X_k^{d'} + d'(X_1^2 + \cdots + X_k^2) + k(d' + 1)),$$

$$\text{Cr}(Q_{\varepsilon, \zeta}) = \left\{ d' Q_{\varepsilon, \zeta} - \left( X_2 \frac{\partial Q_{\varepsilon, \zeta}}{\partial X_2} + \cdots + X_k \frac{\partial Q_{\varepsilon, \zeta}}{\partial X_k} \right), \frac{\partial Q_{\varepsilon, \zeta}}{\partial X_2}, \dots, \frac{\partial Q_{\varepsilon, \zeta}}{\partial X_k} \right\},$$

with  $d' = \sup(2(d+1), 6)$ .

Note that for every unbounded connected component  $D$  of  $\text{Zer}(Q, \mathbb{R}^k)$ , the elements of  $\lim_\zeta (\text{Zer}(\text{Cr}(Q_{\varepsilon, \zeta}), \mathbb{R}\langle\varepsilon\rangle\langle\zeta\rangle))$  meet  $\text{Ext}(D, \mathbb{R}\langle\varepsilon\rangle)$  by Proposition 12.37 of [1].

Moreover,  $\text{Cr}(Q_{\varepsilon, \zeta})$  is a parametrized special Groebner basis with

$$Z = \zeta, Y_1 = \zeta, Y_2 = \varepsilon, d_1 = d', d_2 = \cdots = d_k = d' - 1, \ell = 2, \lambda = 2,$$

and the bitsizes of the coefficients bounded by

$$2\tau + k \text{bit}(d+1) + \text{bit}(d') + 1.$$

According to the complexity analysis of Algorithm Parametrized Special Matrices of Multiplication, it follows that the matrix  $M_i$  of multiplication by  $\zeta X_i$  has dimension

$$N = d'(d' - 1)^{k-1},$$

and the bitsizes of its entries is bounded by

$$D(2\tau + k \text{bit}(d+1) + \text{bit}(d') + 1 + 4 \text{bit}(2D+1) + \text{bit}(N)) - 2 \text{bit}(2D+1) - \text{bit}(N),$$

where

$$D = d' + (k-1)(d'-1) - k + 1 = kd' - 2(k-1),$$

while the degree in  $\varepsilon, \zeta$  of its entries is bounded by  $2D$ .

For every  $j$ , denote by  $L_j$  the matrix of multiplication by the linear form  $\zeta(X_1 + jX_2 + \cdots + j^{k-1}X_k)$ , by  $\chi(j, \varepsilon, \zeta, T)$  its characteristic polynomial and by  $G(j, \varepsilon, \zeta, T)$  the polynomial obtained by substituting  $\frac{T}{\zeta}$  to  $T$  in  $\chi(j, \varepsilon, \zeta, T)$  and multiplying by the minimum power of  $\zeta$  necessary to avoid denominators, and by  $g(j, \varepsilon, T)$  the polynomial  $G(j, \varepsilon, 0, T)$ . It follows from [1] that there exists  $0 \leq j \leq (k-1)N^2$ , such that every point  $x(\varepsilon)$  of  $\lim_\zeta (\text{Zer}(\text{Cr}(Q_{\varepsilon, \zeta}), \mathbb{R}\langle\varepsilon\rangle\langle\zeta\rangle))$  is of the form  $r(\varepsilon, t(\varepsilon))$  where  $t(\varepsilon)$  is a root of  $g(j, \varepsilon, T)$  and  $r(\varepsilon, T)$  is a rational function with denominator a derivative of  $g(j, \varepsilon, T)$ . Finally, for every unbounded connected component  $D$  of  $\text{Zer}(Q, \mathbb{R}^k)$ , there is a root  $t(\varepsilon)$  of  $g(j, \varepsilon, T)$  and a rational function  $r(\varepsilon, T)$  with denominator a derivative of  $g(j, \varepsilon, T)$  such that  $r(\varepsilon, t(\varepsilon)) \in \text{Ext}(D, \mathbb{R}\langle\varepsilon\rangle)$ .

The matrix  $M$  of multiplication by the linear form  $\zeta(X_1 + jX_2 + \dots + j^{k-1}X_k)$  has entries with bitsizes bounded by  $2DN\tau + \rho + \sigma$ , with

$$\begin{aligned}\rho &= D(k \operatorname{bit}(d+1) + \operatorname{bit}(d') + 1 + 4 \operatorname{bit}(2D+1) + \operatorname{bit}(N)) - 2 \operatorname{bit}(2D+1), \\ \sigma &= (2k-3) \operatorname{bit}(N) + k \operatorname{bit}(k).\end{aligned}$$

So the characteristic polynomial,  $\chi(j, \varepsilon, \zeta, T)$  of  $M$  is a polynomial in  $\varepsilon, \zeta, T$  with degree in  $T$  bounded by  $N$ , degree in  $\varepsilon, \zeta$  bounded by  $2DN$ , and bitsize bounded by

$$\tau' = 2ND\tau + N(\rho + \rho')$$

with

$$\rho' = (2k-2) \operatorname{bit}(N) + k \operatorname{bit}(k) + 2 \operatorname{bit}(2DN+1) + 1,$$

using Proposition 8.16 of [1]. The same estimate holds for the bitsize of  $g(j, \varepsilon, T)$ .

Now let  $u_0 \in \mathbb{R}$ , with  $u_0 > 0$ , be such that the number and multiplicities of the real roots of  $g(j, u, T)$  stay constant for all  $u \in (0, u_0)$  and denote by  $t(u)$  the root of  $g(u, T)$  having the same number as  $t(\varepsilon)$  as a root of  $g(j, \varepsilon, T)$ . Then for every point  $x(\varepsilon)$  of  $\lim_{\zeta} (\operatorname{Zer}(\operatorname{Cr}(Q_{\varepsilon, \zeta}), \mathbb{R}(\varepsilon)\langle \zeta \rangle))$ , such that  $x(\varepsilon) = r(\varepsilon, t(\varepsilon))$ , the function  $r(u, t(u))$  is defined from  $(0, u_0)$  to  $\operatorname{Zer}(Q, \mathbb{R}^k)$ . The graph of this function is connected and intersect  $D$ , since  $r(\varepsilon, t(\varepsilon)) \in \operatorname{Ext}(D, \mathbb{R}(\varepsilon))$ .

Let  $\mathcal{A}(\varepsilon)$  be the set of all subresultants of  $g(\varepsilon, T)$  and  $g^{(\ell)}(\varepsilon, T)$ ,  $1 \leq \ell \leq N-1$ , with respect to the variable  $T$ . From the definition of the subresultants (see [1]), the polynomials in  $\mathcal{A}(\varepsilon)$  have degrees in  $\varepsilon$  bounded by

$$2DN(2N-1)$$

and bitsizes bounded by

$$(2N-1)\tau' + N^2 \operatorname{bit}(N+1).$$

Choosing  $u_0$  smaller than the smallest positive root of the polynomials in  $\mathcal{A}(\varepsilon)$ , the number and multiplicities of the real roots of  $g(j, u, T)$  stay constant for all  $u \in (0, u_0)$  by using the properties of subresultants.

Finally, applying Cauchy bound (see [1]), we see that we can choose the rational number  $u_0$  of bitsize bounded by

$$(2DN(2N-1) + 1) 2^{(2N-1)\tau' + N^2 \operatorname{bit}(N+1)}. \quad \square$$

## 5 Semi-algebraic case

### Proof of Theorem 3:

We first observe that given a bounded semi-algebraically connected component  $D$  of a basic semi-algebraic set defined by  $P_1 \geq 0, \dots, P_s \geq 0$ , and let  $w \in \mathbb{R}$  be an extremal value (either maximum or minimum) of the  $X_1$ -co-ordinate realized on  $D$ . Then, there exists  $\{i_1, \dots, i_m\} \subset \{1, \dots, s\}$  and a bounded semi-algebraically connected component  $C$  of the algebraic set  $\operatorname{Zer}(\{P_{i_1}, \dots, P_{i_s}\}, \mathbb{R}^k)$  such that  $C \subset D$  and  $w$  is the extremal value of the  $X_1$ -co-ordinate realized on  $C$ . Indeed, let  $W \subset D$  be the set of points of  $D$  with their first co-ordinate equal to  $w$ . For any point  $x \in W$  let  $\mathcal{P}_x = \{P \in \mathcal{P} \mid P(x) = 0\}$ . We choose  $x \in W$  such that  $\mathcal{P}_x = \{P_{i_1}, \dots, P_{i_m}\}$  is maximal with respect to inclusion. Let  $C$  be the connected component of  $\operatorname{Zer}(\{P_{i_1}, \dots, P_{i_s}\}, \mathbb{R}^k)$  which contains  $x$ . Then,  $C \subset D$  by the maximality of  $\mathcal{P}_x = \{P_{i_1}, \dots, P_{i_m}\}$  and clearly  $C$  is bounded since  $D$  is bounded, and moreover  $w$  is an extremal value of  $C$ .

We now apply Theorem 1 above, noting that for any subset  $\mathcal{P}' \subset \mathcal{P}$ , the bit-sizes of the coefficients of the polynomial  $\sum_{P \in \mathcal{P}'} P^2$  is bounded by  $2\tau + k \text{bit}(d+1) + \text{bit}(s)$ , and its degree is bounded by  $2d$ . Applying Theorem 1 we obtain that

$$w \leq (N+1)2^{N(2kd+2)(2\tau+\text{bit}(N)+(k+1)\text{bit}(d+1)+\text{bit}(s))},$$

where

$$N = (2d+1)(2d)^{k-1}. \quad \square$$

**Proof** of Theorem 4. Since every semi-algebraically connected component of the realization of a weak sign condition on  $\mathcal{P}$  must contain a connected component of some algebraic set  $\text{Zer}(\mathcal{P}', \mathbb{R}^k)$ , where  $\mathcal{P}' \subset \mathcal{P}$ , it suffices to apply Theorem 2 to obtain an upper bound on the radius of a ball guaranteed to meet all such components. Note that for any subset  $\mathcal{P}' \subset \mathcal{P}$ , the bit-sizes of the coefficients of the polynomial  $\sum_{P \in \mathcal{P}'} P^2$  is bounded by  $2\tau + k \text{bit}(d+1) + \text{bit}(s)$ , and its degree is bounded by  $2d$ . Note also that we can use directly  $\sum_{P \in \mathcal{P}'} P^2$  without squaring in (2). The theorem is then a straightforward consequence of Theorem 2.  $\square$

## Bibliography

1. S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2009, online version.
2. G. Binyamini, D. Novikov, and S. Yakovenko. On the number of zeros of abelian integrals: A constructive solution of the infinitesimal hilbert sixteenth problem, 2008. preprint at [arXiv:0808.2952].
3. Gal Binyamini and Sergei Yakovenko. Polynomial bounds for oscillation of solutions of fuchsian systems, 2008.
4. D. Yu. Grigoriev and N. N. Vorobjov, Jr. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5(1-2):37–64, 1988.
5. K.A. Hansen, M. Koucky, and P.B. Miltersen. Winning concurrent reachability games requires doubly-exponential patience, 2009. Proceedings of LICS, 2009.
6. G. Jeronimo and D. Perrucci. On the minimum of a polynomial on the standard simplex, 2009. preprint at [arXiv:0906.4377].
7. J. Renegar. On the computational complexity and geometry of the first-order theory of the reals. I-III. *J. Symbolic Comput.*, 13(3):255–352, 1992.