Journal of Symbolic Computation 45 (2010) 1270–1279

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

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

Saugata Basu [a,1], Marie-Françoise Roy [b]

[a] Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA

[b] IRMAR (URA CNRS 305), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, Cedex, France

ARTICLE INFO

Article history:
Received 24 October 2009
Accepted 2 May 2010
Available online 25 June 2010

Keywords:
Semi-algebraic sets
Bit-sizes

ABSTRACT

We prove an explicit bound 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 weak sign condition involving s polynomials in $\mathbb{Z}[X_1, \ldots, X_k]$ having degrees at most d, and whose coefficients have bitsizes at most τ. Our bound is an explicit function of s, d, k and τ, 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 τ. 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 weak sign condition (see precise definition in Section 2.1), where $\mathcal{P} \subset \mathbb{Z}[X_1, \ldots, X_k]$ is a set of polynomials, with $\#\mathcal{P} = s$, $\deg(P) \leq d$ for $P \in \mathcal{P}$, and the bitsizes of the coefficients of $P \in \mathcal{P}$ are bounded by τ. 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

E-mail addresses: sbasu@math.purdue.edu (S. Basu), marie-francoise.roy@univ-rennes1.fr (M.-F. Roy).

[1] Tel.: +1 765 494 8798; fax: +1 765 494 0548.

0747-7171/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2010.06.009

(Binyamini et al., 2008; Binyamini and Yakovenko, 2008), as well as in proving certain lower bounds in computer science (Hansen et al., 2009).

We obtain explicit upper bounds (in terms of s, d, k and τ) 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 weak sign condition involving polynomials in $\mathbb{Z}[X_1, \ldots, X_k]$ in terms of the number s, the maximum degree d, and the maximum bitsize τ of the coefficients of the defining polynomials, were known before. The best of these bounds were of the form $2^{\tau d^{O(k)}}$ (Basu et al., 2009; Grigoriev and Vorobjov, 1988; Renegar, 1992), with undetermined constants. We do not improve this result, and we believe that there is little hope to improve it 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 τ. This is what we do in this paper.

2. Main results

2.1. Some notation

We first fix some notation.

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

$$\mathrm{Zer}(\mathcal{P}, \mathrm{R}^k) = \left\{ x \in \mathrm{R}^k \;\middle|\; \bigwedge_{P \in \mathcal{P}} P(x) = 0 \right\}.$$

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 σ at $x \in \mathrm{R}^k$ if $\bigwedge_{P \in \mathcal{P}} \mathrm{sign}(P(x)) = \sigma(P)$.

The *realization of the sign condition* σ is

$$\mathrm{Reali}(\sigma) = \left\{ x \in \mathrm{R}^k \;\middle|\; \bigwedge_{P \in \mathcal{P}} \mathrm{sign}(P(x)) = \sigma(P) \right\}.$$

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

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

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

The *realization of the weak sign condition* $\bar{\sigma}$ is

$$\mathrm{Reali}(\bar{\sigma}) = \left\{ x \in \mathrm{R}^k \;\middle|\; \bigwedge_{P \in \mathcal{P}} \mathrm{sign}(P(x)) \in \bar{\sigma}(P) \right\}.$$

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

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

$$\mathrm{bit}(nm) \leqslant \mathrm{bit}(n) + \mathrm{bit}(m), \tag{1}$$

$$\mathrm{bit}\left(\sum_{i=1}^{n} m_i \right) \leqslant \mathrm{bit}(n) + \sup_{i=1}^{n} (\mathrm{bit}(m_i)). \tag{2}$$

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 $Q \in \mathbb{Z}[X_1, \ldots, X_k]$ be a polynomial of degree d, and suppose that the coefficients of Q in $\mathbb{Z}$ have bitsizes at most τ. Then, every bounded semi-algebraically connected component of $\mathrm{Zer}(Q, \mathbb{R}^k)$ is contained inside a ball, centered at the origin, of radius*

$$k^{1/2}(N+1)2^{ND(\tau+\mathrm{bit}(N)+\mathrm{bit}(d+1)+3)}$$

where

$$\begin{aligned} N &= (d+1)d^{k-1}, \\ D &= k(d-1)+2. \end{aligned}$$

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

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

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

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

$$\begin{aligned} d' &= \sup(2(d+1), 6), \\ D &= k(d'-2)+2, \\ N &= d'(d'-1)^{k-1}, \\ \tau' &= N(\tau_2 + \mathrm{bit}(N) + 2\,\mathrm{bit}(2D+1) + 1), \\ \tau_2 &= \tau_1 + 2(k-1)\,\mathrm{bit}(N) + (2k-1)\,\mathrm{bit}(k), \\ \tau_1 &= D(\tau_0 + 4\,\mathrm{bit}(2D+1) + \mathrm{bit}(N)) - 2\,\mathrm{bit}(2D+1) - \mathrm{bit}(N), \\ \tau_0 &= 2\tau + k\,\mathrm{bit}(d+1) + \mathrm{bit}(2d'). \end{aligned}$$

2.3. Semi-algebraic case

Theorem 3. *Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathbb{Z}[X_1, \ldots, X_k]$, and suppose that $P \in \mathcal{P}$ have degrees at most d, and the coefficients of $P \in \mathcal{P}$ have bitsizes at most τ. Then there exists a ball, centered at the origin, of radius bounded by*

$$k^{1/2}(N+1)2^{2ND(2\tau+\mathrm{bit}(N)+k\,\mathrm{bit}(d+1)+\mathrm{bit}(s)+3)}$$

where

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

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

Theorem 4. *Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset \mathbb{Z}[X_1, \ldots, X_k]$ and suppose that $P \in \mathcal{P}$ have degrees at most d, and the coefficients of $P \in \mathcal{P}$ have bitsizes at most τ. Then there exists a ball, centered at the origin, of radius*

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

where

$$
\begin{aligned}
&d' = \sup(2(d+1), 6),\\
&D = k(d'-2)+2,\\
&N = d'(d'-1)^{k-1},\\
&\tau'' = N(\tau_2' + \operatorname{bit}(N) + 2\operatorname{bit}(2D+1) + 1),\\
&\tau_2' = \tau_1' + 2(k-1)\operatorname{bit}(N) + (2k-1)\operatorname{bit}(k),\\
&\tau_1' = D(\tau_0' + 4\operatorname{bit}(2D+1) + \operatorname{bit}(N)) - 2\operatorname{bit}(2D+1) - \operatorname{bit}(N),\\
&\tau_0' = 2\tau + k\operatorname{bit}(d+1) + \operatorname{bit}(2d') + \operatorname{bit}(s)
\end{aligned}
$$

intersecting every semi-algebraically connected component of the realization of every realizable sign condition (resp. realizable weak sign condition) on $\mathcal{P}$.

Remark 1. Note that all the bounds above are of the form $2^{\tau d^{O(k)}}$, similar to the results obtained in Basu et al. (2009); Grigoriev and Vorobjov (1988); Renegar (1992). 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 at most d in k variables with bitsizes bounded by τ is bounded by $(2^{\tau+1})^{\binom{d+k}{k}} = 2^{\tau d^{O(k)}}$.

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 Basu et al. (2009), is similar in spirit to the techniques in Jeronimo and Perrucci (2010). We reproduce here the results (without proofs which appear in Basu et al. (2009)) for the benefit of the readers.

Let D be an ordered domain contained in a field K. 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

$$\mathcal{G}(Y, Z) = \{ZX_1^{d_1} + Q_1(Y, X), \ldots, ZX_k^{d_k} + Q_k(Y, X)\}$$

with $Q_i \in \mathrm{D}[Y][X_1, \ldots, X_k]$, $\deg_X(Q_i) < d_i$, $\deg_{X_j}(Q_i) < d_j$, $i \neq j$, where $\deg_X$ is the total degree with respect to the variables $X_1, \ldots, X_k$, $\deg_{X_j}$ is the degree with respect to the variables X_j, $d_1 \geq \cdots \geq d_k \geq 1$, and Z is a new variable.

Define $\overline{\mathrm{Mon}}(\mathcal{G})(Z)$ as the set of elements $Z^{|\alpha|}X^\alpha = Z^{|\alpha|}X_1^{\alpha_1}\cdots X_k^{\alpha_k}$ with $\alpha_i < d_i$ and $\overline{\mathrm{Bor}}(\mathcal{G})(Z)$ as the set of elements $Z^{|\alpha|}X^\alpha$ such that $\alpha_i = d_i$ for some $i \in \{1, \ldots, k\}$ and $\alpha_i \leq d_i$ for any $i \in \{1, \ldots, k\}$.

Note that for every $z \neq 0$, $(y, z) \in \mathrm{K}^{\ell+1}$ with $z \neq 0$, $\mathcal{G}(y, z)$ is a Groebner basis of the ideal $\mathrm{Id}(\mathcal{G}(y, z))$ it generates, $\overline{\mathrm{Mon}}(\mathcal{G})(z)$ is a basis of $\mathrm{K}[X_1, \ldots, X_k]/\mathrm{Id}(\mathcal{G}(y, z))$, and the dimension of $\mathrm{K}[X_1, \ldots, X_k]/\mathrm{Id}(\mathcal{G}(y, z))$ as a vector space is $N = d_1 \ldots d_k$.

The description and complexity analysis of the following algorithm is described in Basu et al. (2009, Algorithm 12.10). Here we just recall the input, output and the estimates on the degrees and bitsizes of the output.

Algorithm 1 (*Parametrized Special Matrices of Multiplication*)**.**

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

$$\mathcal{G} = \{ZX_1^{d_1} + Q_1(Y, X), \ldots, ZX_k^{d_k} + Q_k(Y, X)\} \subset \mathrm{D}[Y, Z][X_1, \ldots, X_k]$$

  with $Y = (Y_1, \ldots, Y_\ell)$.
- *Output:* parametrized matrices of multiplication by the variables in the basis $\overline{\mathrm{Mon}}(\mathcal{G})(Z)$ of the quotient by the ideal generated by $\mathcal{G}(Y, Z)$: i.e. for every variable X_i a matrix $M_i'(Y, Z)$ with entries in $\mathrm{D}[Y, Z]$ such that for every $(y, z) \in \mathrm{K}^{\ell+1}$ with $z \neq 0$, $M_i'(y, z)$ is the matrix of multiplication by $zX_1, \ldots, zX_k$ in the ring $\mathrm{K}[X_1, \ldots, X_k]/\mathrm{Id}(\mathcal{G}(y, z))$, expressed in the basis $\overline{\mathrm{Mon}}(\mathcal{G})(z)$.

Estimates on the Size of the Output. Let $N = d_1 \cdots d_k$, $D = (d_1 + \cdots + d_k - k + 1)$.

Suppose that $\deg_Y(Q_i) \leq \lambda$ for $1 \leq i \leq k$. Then the matrices $M'_i(Y, Z)$ are of dimension N, and the entries of the matrix $M'_i(Y, Z)$ have degrees in Z bounded by D and degrees in Y bounded by $D\lambda$.

When $\mathrm{D} = \mathbb{Z}$, suppose that τ is a bound on the bitsizes of the coefficients of the polynomials in $\mathcal{G}$(Y,Z). Then the bitsizes of entries of the matrix $M'_i(Y, Z)$ are bounded by

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

4. Algebraic case

In this section we prove Theorems 1 and 2.

We first introduce some notation. Let R be a real closed field. For any polynomial $P \in \mathrm{R}[X_1, \ldots, X_k]$, let $\mathrm{Zer}_b(P, \mathrm{R}^k)$ denote the union of the semi-algebraically connected components of $\mathrm{Zer}(P, \mathrm{R}^k)$ which are bounded over R.

We denote by $\mathrm{R}\langle\varepsilon\rangle$ the real closed field of algebraic Puiseux series in ε with coefficients in R. The *order* of a Puiseux series $a = \sum_{i \geqslant i_0} a_i \varepsilon^{i/q}$, with $q \in \mathbb{N}, i_0 \in \mathbb{Z}$ is the rational number i_0/q. The elements of $\mathrm{R}\langle\varepsilon\rangle$ with non-negative order constitute a valuation ring denoted $\mathrm{R}\langle\varepsilon\rangle_b$. The elements of $\mathrm{R}\langle\varepsilon\rangle_b$ are exactly the elements of $\mathrm{R}\langle\varepsilon\rangle$ bounded over R (i.e. their absolute value is less than a positive element of R). We denote by $\lim_\varepsilon$ the ring homomorphism from $\mathrm{R}\langle\varepsilon\rangle_b$ to R which maps $\sum_{i\in\mathbb{N}} a_i \varepsilon^{i/q}$ to a_0. The mapping $\lim_\varepsilon$ simply replaces ε by 0 in a bounded Puiseux series.

If S is a semi-algebraic subset of R^k, defined by a quantifier-free first-order formula Φ with coefficients in R (see Basu et al., 2009 (Chapter 2)), $\mathrm{Ext}(S, \mathrm{R}\langle\varepsilon\rangle)$ is the semi-algebraic subset of $\mathrm{R}\langle\varepsilon\rangle^k$ defined by the same formula Φ (now considered as a formula with coefficients in $\mathrm{R}\langle\varepsilon\rangle$).

A subset A of $\mathrm{R}\langle\varepsilon\rangle^k$ is bounded over R if it is contained in a ball of center 0 and radius $r \in \mathrm{R}$, i.e.

$$A \subset \mathrm{Ext}(\overline{B}_k(0, r), \mathrm{R}\langle\varepsilon\rangle) = \{x \in \mathrm{R}\langle\varepsilon\rangle^k \mid |x| \leqslant r\}.$$

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

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

We are going to introduce convenient deformations of Q with coefficients in $\mathbb{R}\langle\zeta\rangle$, where ζ is a new variable, and prove that it is possible to obtain such an interval from an interval $[a_\zeta, b_\zeta]$ such that the cylinder based on $[a_\zeta, b_\zeta]$ contains all the semi-algebraically connected components of the zero sets of these deformations of Q which are bounded over $\mathbb{R}$.

We define

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

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

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

is zero-dimensional.

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

$$C = \lim_\zeta (C_1 \cup \ldots \cup C_c).$$

In order to see this, note that

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

where

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

Moreover, the polynomial $(X_1^{d+1} + \cdots + X_k^{d+1})^2$ is non-negative everywhere in $\mathbb{R}^k$. Now apply Proposition 12.37 in Basu et al. (2009), after noting that by Proposition 12.35 in Basu et al. (2009), $\lim_\zeta$ of a semi-algebraically connected component of $\mathrm{Zer}(Q_\zeta, \mathbb{R}\langle\zeta\rangle^k)$ bounded over $\mathbb{R}$ remains semi-algebraically connected and bounded.

This implies that, denoting by π the projection to the X_1-axis,

$$\pi(C) = \lim_\zeta (\pi(C_1 \cup \ldots \cup C_c)). \tag{3}$$

Let $[a, b] = \pi(C)$, and a_ζ and b_ζ be the minimum and maximum of $\pi(C_1 \cup \ldots \cup C_c)$. It follows from (3) that $\lim_\zeta(a_\zeta) = a$, $\lim_\zeta(b_\zeta) = b$.

In order to describe a_ζ and b_ζ, we define the polynomial systems

$$\mathrm{Cr}(Q_\zeta^+) = \left\{(d+1)Q_\zeta^+ - \left(X_2\frac{\partial Q_\zeta^+}{\partial X_2} + \cdots + X_k\frac{\partial Q_\zeta^+}{\partial X_k}\right), \frac{\partial Q_\zeta^+}{\partial X_2}, \ldots, \frac{\partial Q_\zeta^+}{\partial X_k}\right\},$$

$$\mathrm{Cr}(Q_\zeta^-) = \left\{(d+1)Q_\zeta^- - \left(X_2\frac{\partial Q_\zeta^-}{\partial X_2} + \cdots + X_k\frac{\partial Q_\zeta^-}{\partial X_k}\right), \frac{\partial Q_\zeta^-}{\partial X_2}, \ldots, \frac{\partial Q_\zeta^-}{\partial X_k}\right\},$$

which are both parametrized special Groebner bases.

Notice that the zero set of $\mathrm{Cr}(Q_\zeta^+)$ (resp. $\mathrm{Cr}(Q_\zeta^-)$) is the set of critical points on $\mathrm{Zer}(Q_\zeta^+, \mathbb{R}\langle\zeta\rangle^k)$ (resp. $\mathrm{Zer}(Q_\zeta^-, \mathbb{R}\langle\zeta\rangle^k)$) and consider the characteristic polynomials $\chi^+(\zeta, T)$ (resp. $\chi^-(\zeta, T)$) of the multiplication by ζX_1 in the ring $\mathbb{R}\langle\zeta\rangle[X_1, \ldots, X_k]/\mathrm{Id}(\mathrm{Cr}(Q_\zeta^+))$ (resp. $\mathbb{R}\langle\zeta\rangle[X_1, \ldots, X_k]/\mathrm{Id}(\mathrm{Cr}(Q_\zeta^-))$).

Since a_ζ and b_ζ are extremal values of π on $C_1 \cup \ldots \cup C_c$, 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 ζT for T and dividing by the maximum possible power of ζ. Finally, since a_ζ and b_ζ are bounded over R, a and b are roots of $f^+(T) = F^+(0, T)$ or $f^-(T) = F^-(0, T)$.

The bitsizes of the coefficients of the polynomials in $\mathrm{Cr}(Q_\zeta^+)$ (resp. $\mathrm{Cr}(Q_\zeta^-)$) are bounded by

$$\tau + \mathrm{bit}(d+1).$$

According to the degrees and bitsize estimates of Algorithm 1, Parametrized Special Matrices of Multiplication (see Preliminaries), it follows that the matrices M^+ and M^- of multiplication by ζX_1 have dimension

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

and the degrees in ζ of their entries are bounded by

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

since $\mathrm{Cr}(Q_\zeta^+)$, $\mathrm{Cr}(Q_\zeta^-)$ are both parametrized special Groebner bases with

$$d_1 = d+1, d_2 = \cdots = d_k = d, \ell = 0.$$

Moreover, the bitsizes of their entries are bounded by

$$\tau_1 = D(\tau + \mathrm{bit}(d+1) + \mathrm{bit}(N)) - \mathrm{bit}(N).$$

So the characteristic polynomial $\chi^+(\zeta, T)$ (resp. $\chi^-(\zeta, T)$) of M^+ (resp. M^-) is a polynomial in ζ and T with degree in ζ bounded by DN and bitsizes bounded by

$$N(\tau_1 + \mathrm{bit}(N) + \mathrm{bit}(D+1) + 1) \leq ND(\tau + \mathrm{bit}(N) + \mathrm{bit}(d+1) + 3),$$

since

$$\mathrm{bit}(D+1) \leqslant 2D,$$

using Proposition 8.16 of Basu et al. (2009).

Thus, a and b are roots of a polynomial – either $f^+(T)$ or $f^-(T)$ – of degree at most N and whose bitsizes are bounded by

$$ND(\tau + \mathrm{bit}(N) + \mathrm{bit}(d+1) + 3).$$

Using the Cauchy bound (see Basu et al., 2009 Lemma 10.2) we finally obtain that $|a|$ and $|b|$ are bounded by

$$(N+1)2^{ND(\tau+\mathrm{bit}(N)+\mathrm{bit}(d+1)+3)}.$$

The theorem follows immediately from this. □

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

To deal with unbounded connected components, let ε be a new variable. We define

$$Q_\varepsilon = Q^2 + (\varepsilon(X_1^2 + \cdots + X_k^2) - 1)^2. \tag{4}$$

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

Noting that Q_ε is everywhere non-negative, we can proceed in a way similar to the proof of Theorem 1 and take

$$Q_{\varepsilon,\zeta} = Q_\varepsilon - \frac{\zeta}{d'}\left(X_1^{d'} + \cdots + X_k^{d'} + d'(X_2^2 + \cdots + X_k^2 + 2k)\right),$$

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

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

Note that for every unbounded connected component C of $\mathrm{Zer}(Q, \mathbb{R}^k)$, the elements of $\lim_\zeta(\mathrm{Zer}(\mathrm{Cr}(Q_{\varepsilon,\zeta}), \mathbb{R}\langle\varepsilon\rangle\langle\zeta\rangle))$ meet $\mathrm{Ext}(C, \mathbb{R}\langle\varepsilon\rangle)$ by Proposition 12.37 in Basu et al. (2009).

Moreover, $\mathrm{Cr}(Q_{\varepsilon,\zeta})$ 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 all its zeros are simple (Proposition 12.46).

Using the complexity analysis of Algorithm 8.5 in Basu et al. (2009), (1), (2) , it is easy to see that the bitsizes of the coefficients of Q_ε are bounded by

$$2\tau + k\,\mathrm{bit}(d+1) + 1$$

and the bitsizes of the coefficients of the polynomials in $\mathrm{Cr}(Q_{\varepsilon,\zeta})$ are bounded by

$$\tau_0 = 2\tau + k\,\mathrm{bit}(d+1) + \mathrm{bit}(d') + 1 = 2\tau + k\,\mathrm{bit}(d+1) + \mathrm{bit}(2d').$$

According to the degree and bitsize estimates of Algorithm 1, Parametrized Special Matrices of Multiplication (see Preliminaries), it follows that the matrix M_i of multiplication by ζX_i has dimension

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

Moreover, defining

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

the degree in ε, ζ are bounded by $2D$, while the bitsizes of its entries are bounded by

$$\tau_1 = D(\tau_0 + 4\,\mathrm{bit}(2D+1) + \mathrm{bit}(N)) - 2\,\mathrm{bit}(2D+1) - \mathrm{bit}(N).$$

For every j, denote by L_j the matrix of multiplication by the linear form $\zeta(X_1 + jX_2 + \cdots + j^{k-1}X_k)$, and by $\chi(j, \varepsilon, \zeta, T)$ its characteristic polynomial. Define $G(j, \varepsilon, \zeta, T) \in \mathbb{Z}[\varepsilon, \zeta, T]$ as the polynomial obtained by substituting ζT for T in $\chi(j, \varepsilon, \zeta, T)$ and dividing by the greatest possible power of ζ, and by $g(j, \varepsilon, T)$ the polynomial $G(j, \varepsilon, 0, T)$. It follows from Basu et al. (2009, Algorithm 12.13) that there exists $0 \leq j \leq (k-1)N^2$, such that every point $x(\varepsilon)$ of $\lim_\zeta(\mathrm{Zer}(\mathrm{Cr}(Q_{\varepsilon,\zeta}), \mathbb{R}\langle\varepsilon\rangle\langle\zeta\rangle))$ 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 C of $\mathrm{Zer}(Q, \mathbb{R}^k)$, 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 $r(\varepsilon, t(\varepsilon)) \in \mathrm{Ext}(C, \mathbb{R}\langle\varepsilon\rangle)$.

The matrix M of multiplication by the linear form $\zeta(X_1 + jX_2 + \cdots + j^{k-1}X_k)$ has entries with bitsizes bounded by

$$\tau_2 = \tau_1 + 2(k-1)\,\mathrm{bit}(N) + (2k-1)\,\mathrm{bit}(k).$$

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

$$\tau' = N(\tau_2 + \mathrm{bit}(N) + 2\,\mathrm{bit}(2D+1) + 1)$$

using Proposition 8.16 of Basu et al. (2009). The same estimate holds for the bitsize of $g(j, \varepsilon, T)$.

Now let $u_0 \in \mathrm{R}$, 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 $\lim_\zeta(\mathrm{Zer}(\mathrm{Cr}(Q_{\varepsilon,\zeta}), \mathbb{R}\langle\varepsilon\rangle\langle\zeta\rangle))$, such that $x(\varepsilon) = r(\varepsilon, t(\varepsilon))$, the function $r(u, t(u))$ is defined from $(0, u_0)$ to $\mathrm{Zer}(Q, \mathbb{R}^k)$. The graph of this function is connected and intersects D, since $r(\varepsilon, t(\varepsilon)) \in \mathrm{Ext}(D, \mathbb{R}\langle\varepsilon\rangle)$.

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 Basu et al., 2009 Notation 4.22 and Proposition 8.15), the polynomials in $\mathcal{A}(\varepsilon)$ have degrees in ε bounded by

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

and bitsizes bounded by

$$(2N-1)(\tau' + \mathrm{bit}(2N-1) + \mathrm{bit}(2DN+1) + \mathrm{bit}(N!)).$$

Choosing u_0 smaller that 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 the Cauchy bound (see Basu et al., 2009 Lemma 10.2) we see that we can choose the rational number u_0 such that $|\frac{1}{u_0}|$ is bounded by

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

5. Semi-algebraic case

Proof of Theorem 3. Suppose that C' is a bounded semi-algebraically connected component of the realization of a weak sign condition on $\mathcal{P}$, and let $a \in \mathbb{R}$ be an extremal value (either maximum or minimum) of the X_1-co-ordinate realized on C'. Then, there exists $\mathcal{P}' \subset \mathcal{P}$ and a bounded semi-algebraically connected component C of the algebraic set $\mathrm{Zer}(\mathcal{P}', \mathbb{R}^k)_a$ such that $C \subset C'$ (where π is the projection map on the X_1-co-ordinate). Indeed, let $A = \{x \in C' | \pi(x) = a\}$. For any point $x \in A$, let $\mathcal{P}_x = \{P \in \mathcal{P} \mid P(x) = 0\}$. We choose $x \in A$ such that $\mathcal{P}_x$ is maximal with respect to inclusion y and let $\mathcal{P}' = \mathcal{P}_x$.

$$Q = \sum_{P \in \mathcal{P}'} P^2.$$

Let C be the semi-algebraically connected component of $\mathrm{Zer}(Q, \mathbb{R}^k)_a$ which contains x. Then, $C \subset C'$ by the maximality of $\mathcal{P}'$. Otherwise, choose a semi-algebraic path $\gamma : [0, 1] \to C$, such that $\gamma(0) = x$, and $\gamma(1) \in C \setminus C'$. Then, there exists $t_0 \in (0, 1]$, with $y = \gamma(t_0) \in C$, $\gamma([0, t_0]) \subset C'$, and some $P \in \mathcal{P} \setminus \mathcal{P}'$, with $P(y) = 0$. This contradicts the maximality of $\mathcal{P}'$, since $y \in C'$, $\pi(y) = a$, and $\mathcal{P}_y$ is strictly bigger than $\mathcal{P}'$. Also, C is bounded, since C' is bounded.

Since a is a local extremum of X_1 on $\mathrm{Zer}(Q, \mathbb{R}^k)$, we can choose r positive and small enough, so that a remains an extremal value of $\pi(C'')$, where C'' is the semi-algebraically connected component of $\mathrm{Zer}(Q, \mathbb{R}^k)_{[a-r,a+r]}$ containing C. As in the proof of Theorem 1, there exists a finite number of semi-algebraically connected components $C_1, \ldots, C_c$ of $\left(\mathrm{Zer}(Q_\zeta^+, \mathbb{R}\langle\zeta\rangle^k) \bigcup \mathrm{Zer}(Q_\zeta^-, \mathbb{R}\langle\zeta\rangle^k)\right)_{[w-r,w+r]}$ which are bounded over $\mathbb{R}$ and such that

$$C'' = \lim_\zeta (C_1 \cup \cdots \cup C_c).$$

Suppose now, without loss of generality, that w is the maximal value of X_1-co-ordinate realized on C''. Let a_ζ be the maximum of $\pi(C_1 \cup \cdots \cup C_c)$. It follows from the above that $\lim_\zeta(a_\zeta) = a$.

We now apply the same technique as in the proof of Theorem 1 above to bound $|a|$, noting that the degree of Q is bounded by $2d$ and the bitsizes of its coefficients are bounded by

$$2\tau + k\,\mathrm{bit}(d+1) + \mathrm{bit}(s).$$

Applying the same technique as in the proof of Theorem 1, we obtain that

$$|a| \leq (N+1)2^{ND(2\tau+\mathrm{bit}(N)+(k+1)\,\mathrm{bit}(d+1)+\mathrm{bit}(s)+3)},$$

where

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

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 $\mathrm{Zer}(\mathcal{P}', \mathbb{R}^k)$, 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 degree of the polynomial $\sum_{P\in\mathcal{P}'} P^2$ is bounded by $2d$, and the bitsizes of its coefficients are bounded by

$$2\tau + k\,\mathrm{bit}(d+1) + \mathrm{bit}(s)$$

using the complexity analysis of Algorithm 8.5 in Basu et al. (2009) and (2). Note also that we can use directly $\sum_{P\in\mathcal{P}'} P^2$ without squaring in (4).

The theorem is then a straightforward consequence of Theorem 2. $\square$

Acknowledgements

The authors gratefully acknowledge the contributions of two anonymous referees whose detailed reading of the manuscript and suggested changes greatly improved the paper. The first author was supported in part by NSF grant CCF-0915954.

References

Basu, S., Pollack, R., Roy, M.-F., 2009. Algorithms in Real Algebraic Geometry. In: Algorithms and Computation in Mathematics, vol. 10. Springer-Verlag, Berlin, online version posted on 07/31/2009, available at http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted1.html. MR 1998147 (2004g:14064).

Binyamini, G., Novikov, D., Yakovenko, S., On the number of zeros of Abelian integrals: A constructive solution of the infinitesimal Hilbert sixteenth problem, 2008, Preprint at arXiv:0808.2952.

Binyamini, G., Yakovenko, S., Polynomial bounds for oscillation of solutions of Fuchsian systems, 2008, Preprint at arXiv:0808.2950.

Grigoriev, D.Yu., Vorobjov Jr., N.N., 1988. Solving systems of polynomial inequalities in subexponential time. J. Symbolic Comput. 5 (1–2), 37–64. MR 949112 (89h:13001).

Hansen, Kristoffer Arnsfelt, Koucký, Michal, Miltersen, Peter Bro, 2009. Winning concurrent reachability games requires doubly-exponential patience. In: LICS. IEEE Computer Society, pp. 332–341.
Jeronimo, Gabriela, Perrucci, Daniel, 2010. On the minimum of a positive polynomial over the standard simplex. J. Symbolic Comput. 45 (4), 434–442.
Renegar, J., 1992. On the computational complexity and geometry of the first-order theory of the reals. I–III. J. Symbolic Comput. 13 (3), 255–352.