A bound on the minimum of a real positive polynomial over the standard simplex.

Saugata Basu, Richard Leroy, Marie-Françoise Roy

▶ **To cite this version:**

Saugata Basu, Richard Leroy, Marie-Françoise Roy. A bound on the minimum of a real positive polynomial over the standard simplex.. 2008. hal-00350115v2

HAL Id: hal-00350115
https://hal.science/hal-00350115v2

Preprint submitted on 19 Feb 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A bound on the minimum of a real positive polynomial over the standard simplex

Saugata Basu, Richard Leroy, Marie-Françoise Roy

January 22, 2009

Abstract

We consider the problem of bounding away from 0 the minimum value m taken by a polynomial $P \in \mathbb{Z}[X_1, \ldots, X_k]$ over the standard simplex $\Delta \subset \mathbb{R}^k$, assuming that $m > 0$. Recent algorithmic developments in real algebraic geometry enable us to obtain a positive lower bound on m in terms of the dimension k, the degree d and the bitsize τ of the coefficients of P. The bound is explicit, and obtained without any extra assumption on P, in contrast with previous results reported in the literature.

1 Introduction

1.1 Problem statement

Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ be a multivariate polynomial of degree d taking only positive values on the $k-$dimensional simplex

$$\Delta = \Big\{ x \in \mathbb{R}^k_{\geq 0} \Big| \sum_{i=1}^{k} x_i \leq 1 \Big\}.$$

Let τ be an upper bound on the bitsize of the coefficients of P. Writing

$$m = \min_{\Delta} P > 0,$$

we consider the problem of finding an explicit bound $m_{k,d,\tau}$ depending only on k, d and τ such that $0 < m_{k,d,\tau} < m$.

1.2 Previous work

Several authors have worked on this subject. There are two main approaches: Canny's gap theorem can be used, under non-degeneracy conditions ([C]); in [LS], the authors use the Lojasiewicz inequality, leading to a bound in the general case, but involving a universal constant. The method presented here gives an explicit bound, with no extra assumption on P.

1.3 Univariate case

We begin with the univariate case, which contains some basic ideas of the proof in the general case. This situation has already been studied in [BCR]. We present here a simpler proof, leading to a slightly better bound.

Consider a univariate polynomial of degree d

$$P = \sum_{i=0}^{d} a_i T^i \in \mathbb{Z}[T],$$

taking only positive values on the interval $[0,1]$. Let τ be a bound on the bitsize of its coefficients.
The minimum m of P on $[0,1]$ occurs either at 0 or 1, or at a point x^* lying in the interior $]0,1[$. The first case is trivial, as $P(0), P(1) \in \mathbb{Z}$, so that m is clearly greater than 1. In the second case, $P(x^*) = 0$, so that m is a root of the resultant $R(Z) = \mathrm{Res}_T(P(T) - Z, P'(T)) \in \mathbb{Z}[Z]$. The resultant $R(Z)$ is the determinant of the matrix $\mathrm{Syl}(Z)$, where $\mathrm{Syl}(Z)$ is the following Sylvester matrix:

$$\left.\begin{pmatrix}
a_d & \cdots & \cdots & \cdots & a_1 & a_0 - Z & 0 & \cdots & 0 \\
0 & \ddots & & & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & & & \ddots & 0 \\
0 & \cdots & 0 & a_d & \cdots & \cdots & \cdots & a_1 & a_0 - Z \\
(d-1)a_{d-1} & \cdots & \cdots & \cdots & a_1 & 0 & \cdots & \cdots & 0 \\
0 & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & (d-1)a_{d-1} & \cdots & \cdots & \cdots & a_1
\end{pmatrix}\right\}\begin{matrix} d-1 \\ \\ \\ \\ \\ d \\ \\ \\ \end{matrix}$$

$R(Z) = \sum_{i=0}^{d-1} r_i Z^i$ is thus a polynomial of degree $d-1$ in Z, whose coefficients are controlled in the following fashion:

Lemma 1.1. *For all $i \in \{0, \ldots, d-1\}$, we have*

$$|r_i| < 3^{-d/2} \left[2^\tau \sqrt{(d+1)^3}\right]^d \binom{d-1}{i} \left[2^\tau \sqrt{d+1} - 1\right]^{d-1-i}.$$

Proof. Let $(A_1, \ldots, A_{d-1}, B_1, \ldots, B_d)$ denote the rows of the classical Sylvester matrix Syl(0). Then

$$R(Z) = \det\left(A_1 + Ze_{d+1}, \ldots, A_{d-1} + Ze_{2d-1}, B_1, \ldots, B_d\right),$$

where $(e_1, \ldots, e_{2d-1})$ is the canonical basis of $\mathbb{R}^{2d-1}$. Using the multilinearity of the determinant, we can write $R(Z) = \sum_{i=0}^{d-1} r_i Z^i$, where, for all $i \in \{0, \ldots, d-1\}$, r_i is a sum of $\binom{d-1}{i}$ determinants of matrices built with:

- i rows among the e_j's
- $d-1-i$ rows among the A_j's
- the d rows $B_1, \ldots, B_d$.

Hadamard's bound (see [BPR]) implies that, for all i:

$$\begin{aligned}
|r_i| &\leq \binom{d-1}{i} \sqrt{\left[(d+1)\left(2^{2\tau}-1\right)\right]^{d-1-i}} \sqrt{\left[\frac{d(d+1)(2d+1)}{6}\left(2^{2\tau}-1\right)\right]^{d-1-i}} \\
&< \binom{d-1}{i} \left[2^\tau \sqrt{d+1} - 1\right]^{d-1-i} \left[2^\tau \sqrt{\frac{(d+1)^3}{3}}\right]^d \\
&\leq 3^{-d/2} \left[2^\tau \sqrt{(d+1)^3}\right]^d \binom{d-1}{i} \left[2^\tau \sqrt{d+1} - 1\right]^{d-1-i},
\end{aligned}$$

as claimed. □

Since the minimum m is a root of $R(Z)$, Cauchy's bound finally implies the following theorem

Theorem 1.2. *Let $P \in \mathbb{Z}[T]$ be a univariate polynomial of degree d taking only positive values on the interval $[0,1]$. Let τ be an upper bound on the bitsize of the coefficients of P. Let m denote the minimum of P over $[0,1]$. Then*

$$m > \frac{3^{d/2}}{2^{(2d-1)\tau}(d+1)^{2d-1/2}}.$$

Proof. If m is attained at 0 or 1, then the result is obvious. If not, m is a root of the resultant $R(Z)$. Since R has at least one non-zero root ($R(m) = 0$), Cauchy's bound (see [BPR]) implies

$$\begin{aligned}\frac{1}{m} &\leq \sum_{i=0}^{d-1} |r_i| \\ &< \sum_{i=0}^{d-1} 3^{-d/2} \left[2^\tau \sqrt{(d+1)^3}\right]^d \binom{d-1}{i} \left[2^\tau \sqrt{d+1} - 1\right]^{d-1-i} \\ &\leq 3^{-d/2} \left[2^\tau \sqrt{(d+1)^3}\right]^d \left[2^\tau \sqrt{d+1}\right]^{d-1},\end{aligned}$$

from which the result follows easily. □

Remark 1.3. *Our bound is slightly better than a recent one presented in [BCR], which was already almost sharp. Indeed, following [BCR], consider the polynomial* $P_k = X^d + \left(2^k X - 1\right)^2$. *Here,* $\tau = 2k$ *and the minimum* m_k *of* P_k *satifies*

$$m_k \leq P_k\left(2^{-k}\right) = 2^{-d\tau/2},$$

and thus decreases exponentially with d *and* τ.

2 Bound on the minimum of multivariate positive polynomial

We now consider the multivariate case.

2.1 Notation and problem statement

The following notation will be useful:

Notation 2.1. *We write* $\mathrm{bit}(n)$ *for the bitsize of an integer* $n \in \mathbb{N}$.

Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ be a polynomial of degree d, and τ a bound on the bitsize of its coefficients. Moreover, assume that

$$m = \min_{\Delta} P > 0.$$

In order to find an explicit lower bound $0 < m_{k,d,\tau} < m$, we generalize the proof of the univariate case. We first show that, at the cost of slightly increasing the bitsize of the coefficients, we can assume that the minimum

is attained in the interior of the simplex. Obviously, there exists a face σ of Δ, of dimension $0 \leq s \leq k$, such that the minimum m is attained at a point of the interior of σ (with its induced topology). In the following we consider such a face σ, of minimal dimension s.

Remark 2.2. *If σ is a vertex of Δ, then obviously $m \geq 1$. We now assume that $s \geq 1$.*

Denote by

$$\begin{cases} V_0 = 0 \\ V_i = e_i \quad (1 \leq i \leq k) \end{cases}$$

the vertices of Δ, and

$$\begin{cases} \lambda_0 = 1 - \sum X_i \\ \lambda_i = X_i \quad (1 \leq i \leq k) \end{cases}$$

the associated barycentric coordinates.

There exists a subset $I = \{i_0, \ldots, i_s\}$ of $\{0, \ldots, k\}$ such that the vertices of σ are the vertices $(V_i)_{i \in I}$. Let $J = \{0, \ldots, k\} \backslash I$. The face σ is characterized by:

$$\sigma = \{x \in \Delta \,|\forall j \in J,\ \lambda_j(x) = 0\,\}.$$

We make the following substitutions in P:

- If $j \in J$ and $j > 0$, replace the variable X_j by 0
- If $j \in J$ and $j = 0$, replace the variable X_{i_0} by $1 - \sum_{\ell=1}^{s} X_{i_\ell}$

We then obtain a polynomial $P_\sigma \in \mathbb{Z}\,[X_{i_1}, \ldots, X_{i_s}]$ satisfying :

$$\min_{\Delta} P = \min_{\mathring{\sigma}} P_\sigma.$$

Renaming the variables X_{i_ℓ} into Y_ℓ, we obtain that $P_\sigma \in \mathbb{Z}\,[Y_1, \ldots, Y_s]$ is a polynomial verifying:

Lemma 2.3. *The degree of P_σ is bounded by d.*
Moreover, the bitsize of its coefficients is bounded by τ_σ, where

$$\tau_\sigma = \tau + 1 + d\,\mathrm{bit}(k). \tag{2.1}$$

Proof. The degree of P_σ is clearly at most d. We now show the result concerning the bitsizes of the coefficients.

The result is clear if $s = k$.

Assume that $1 \leq s \leq k-1$.

Since replacing X_j by 0 does not change the bound on the bitsize of the coefficients, only the replacement of Y_0 by $1 - \sum_{i=1}^{s} Y_i$ has to be taken into account.

If

$$P = \sum_{\substack{\alpha \in \mathbb{N}^k \\ |\alpha| \leq d}} a_\alpha X^\alpha,$$

then

$$P_\sigma = \sum_{\substack{\gamma \in \mathbb{N}^s \\ |\gamma| \leq d}} b_\gamma Y^\gamma,$$

where

$$b_\gamma = \sum_{\beta \in I_\gamma} \pm \binom{|\beta|}{\beta} a_{(\gamma_1 - \beta_1, \ldots, \gamma_k - \beta_k)},$$

and

$$I_\gamma = \{\beta \in \mathbb{N}^{s+1} \Big| |\beta| \leq d \text{ and } \forall i \in \{1, \ldots, s\},\ \beta_i \leq \gamma_i\}.$$

Hence, we have

$$\begin{aligned}
|b_\gamma| &\leq 2^\tau \sum_{\beta \in I_\gamma} \binom{|\beta|}{\beta} \\
&\leq 2^\tau \sum_{\substack{\beta \in \mathbb{N}^{s+1} \\ |\beta| \leq d}} \binom{|\beta|}{\beta} \\
&\leq 2^\tau \sum_{p=0}^{d} \sum_{\substack{\beta \in \mathbb{N}^{s+1} \\ |\beta| = p}} \binom{|\beta|}{\beta} \\
&\leq 2^\tau \sum_{p=0}^{d} (s+1)^p \\
&\leq 2^\tau \frac{(s+1)^{d+1}}{s} \\
&\leq 2^\tau \times 2(s+1)^d \\
&\leq 2^{\tau+1} k^d,
\end{aligned}$$

and the conclusion follows. □

Since

$$m = \min_{\Delta} P = \min_{\overset{\circ}{\sigma}} P_\sigma,$$

$P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ achieves its minimum in the interior of σ. Consequently, m is attained at a critical point of P_σ, *i.e.* a point $x \in \mathbb{R}^s$ such that the gradient of P_σ is zero at x. We are thus interested in computing the values of P at the zeros of its gradient. We aim at giving a univariate reformulation of this problem, enabling us to use resultant methods. The following section introduces the necessary material.

2.2 Rational univariate representation

We first introduce the notion of Thom encoding:

Definition 2.4. *Let $P \in \mathbb{R}[X]$ be a real univariate polynomial, $x \in \mathbb{R}$ a real number and $\sigma \in \{0, 1, -1\}^{\mathrm{Der}(P)}$ a sign condition on the set $\mathrm{Der}(P) = \left\{P, P', \ldots, P^{(\deg P)}\right\}$ of the derivatives of P.*

The sign condition σ is a Thom encoding of x if $\sigma(P) = 0$ and

$$\forall i, \quad \mathrm{Sign}\left(P^{(i)}(x)\right) = \sigma\left(P^{(i)}\right).$$

We can now define a rational univariate representation as follows:

Definition 2.5. *An $s-$rational univariate representation u is an $(s+3)-$tuple of the form*

$$u = (F(T), g_0(T), \ldots, g_s(T), \pi)$$

such that:

1. *$F, g_0, \ldots, g_s \in \mathbb{R}[T]$,*
2. *F and g_0 are coprime,*
3. *π is a Thom encoding of a root $t_\pi \in \mathbb{R}$ of F.*

Remark 2.6. *If $t \in \mathbb{R}$ is a root of F, then $g_0(t) \neq 0$.*

We now define the point associated to the rational univariate representation:

Definition 2.7. *The point associated to u is defined by*

$$x_u = \left(\frac{g_1(t_\pi)}{g_0(t_\pi)}, \ldots, \frac{g_s(t_\pi)}{g_0(t_\pi)} \right).$$

Hence, a rational univariate representation gives rise to a point whose coordinates are rational fractions evaluated at a root of F.

Let $Q \in \mathbb{R}^s$ be a nonnegative polynomial over $\mathbb{R}^s$, and

$$\mathcal{Z}(Q) = \left\{ x \in \mathbb{R}^s \middle| Q(x) = 0 \right\}$$

be the set of real zeros of Q. We are interested in finding a point in each bounded connected component of $\mathcal{Z}(Q)$. This can be done by applying Algorithm 12.15 of [BPR], which we recall here for convenience.

Algorithm 2.8 (Bounded Algebraic Sampling)**.**

Require: *A polynomial $Q \in \mathbb{Z}[X_1, \ldots X_s]$, of degree bounded by d_Q, nonnegative over $\mathbb{R}^s$.*
Ensure: *A set $\mathcal{U}$ of rational univariate representations of the form*

$$(F(T), g_0(T), \ldots, g_s(T), \pi),$$

where the polynomials $F, g_0, \ldots, g_s$ have integer coefficients, and such that the associated points meet every bounded connected component of $\mathcal{Z}(Q)$.

We indicate the main ideas behind the algorithm, referring the reader to [BPR] for details:

- replace Q by a deformation $\mathrm{Def}(Q, d_Q, \zeta)$ of degree bounded by $d_Q + 2$, where ζ is an infinitesimal,
- consider the critical points $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ of $\mathrm{Def}(Q, d_Q, \zeta)$ in the X_1-direction,
- due to the properties of $\mathrm{Def}(Q, d_Q, \zeta)$,
  - $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ has a finite number of points,
  - the quotient ring defined by the equations of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$ is a vector space of dimension at most

$$(d_Q + 2)(d_Q + 1)^{k-1},$$

– its multiplication table can be easily computed,

- find rational univariate representations of the points of $\mathrm{Cr}(\mathrm{Def}(Q, d_Q, \zeta))$,
- take their limits with respect to ζ, which define a finite set of points intersecting all the bounded connected components of $\mathcal{Z}(Q)$.

The complexity analysis in [BPR] shows that, if d_Q is a bound on the degree of Q and τ_Q a bound on the bitsize of its coefficients, then:

1. The degrees of the polynomials $F, g_0, \ldots, g_k$ are bounded by
$$(d_Q + 2)(d_Q + 1)^{k-1}$$
2. The bitsize of their coefficients is bounded by
$$(d_Q + 2)(d_Q + 1)^{k-1}(kd_Q + 2)\left(\tau' + 2\,\mathrm{bit}(kd_Q + 3) + 3\mu + \mathrm{bit}(k)\right),$$
where
$$\tau' = \sup\left[\tau_Q, \mathrm{bit}(2k)\right] + 2\,\mathrm{bit}\left[k(d_Q + 2)\right] + 1$$
$$\mu = \mathrm{bit}\left[(d_Q + 2)(d_Q + 1)^{k-1}\right].$$

2.3 The bound

Recall that $P_\sigma \in \mathbb{Z}[Y_1, \ldots, Y_s]$ achieves its minimum in the interior of σ. Consequently, this minimum is attained at a critical point of P_σ, *i.e.* a point $x \in \mathbb{R}^s$ at which the gradient of P_σ is zero. Consider the set of critical points
$$\mathcal{Z} = \left\{ x \in \mathbb{R}^s \,\middle|\, \frac{\partial P_\sigma}{\partial Y_1}(x) = \cdots = \frac{\partial P_\sigma}{\partial Y_s}(x) = 0 \right\}.$$

Note that P_σ is constant on each connected component of $\mathcal{Z}$. So, we aim at computing a set $\mathcal{U}$ of rational univariate representations u whose associated points x_u meet every connected component of $\mathcal{Z}$, together with the values $P_\sigma(x_u)$.

Remark 2.9. *When $\mathcal{Z}$ has a finite number of points, then Gröbner basis techniques can be used to obtain rational univariate representations of these points (see [R]). The method we present hereafter, based on Algorithm 2.8, computes a point in every connected component of $\mathcal{Z}$ even if $\mathcal{Z}$ is infinite. Moreover Algorithm 2.8 makes it possible to control the degree and the bitsize of the coefficients of the output, in contrast with Gröbner basis methods.*

It is easy to see that if C is a connected component of $\mathcal{Z}$ containing a minimizer of P_σ in σ, then $C \subset \overset{\circ}{\sigma}$ by minimality of the dimension s of σ. In particular, C is bounded. Algorithm 2.8 then gives a set of rational univariate representations of the form

$$u = (F(T), g_0(T), g_1(T), \ldots, g_s(T), \pi),$$

whose associated points meet every bounded connected component of $\mathcal{Z}$. In particular, they meet every connected component of $\mathcal{Z}$ containing a minimizer of P_σ in σ.

Lemma 2.10. *The degree of the polynomials $F, g_0, \ldots, g_s$ is bounded by d_u, where*

$$d_u = 2d(2d-1)^{k-1}.$$

Moreover, the bitsize of their coefficients is bounded by

$$\tau_u = d_u(2kd - 2k + 2)\left[\tau' + 2\,\mathrm{bit}(2kd - 2k + 3) + 3\,\mathrm{bit}(d_u) + \mathrm{bit}(k)\right],$$

where

$$\tau' = 2\tau + (2d+2)\,\mathrm{bit}(k) + (k+3)\,\mathrm{bit}(d) + 5.$$

Proof. Let Q denote the polynomial

$$Q = \sum_{i=1}^{s} \left(\frac{\partial P_\sigma}{\partial Y_i}\right)^2.$$

Clearly, its degree is bounded by $d_Q = 2d - 2$. Moreover, we can bound the bitsize of its coefficients as follows.
If

$$P_\sigma = \sum_{\substack{\gamma \in \mathbb{N}^s \\ |\gamma| \le d}} b_\gamma Y^\gamma,$$

then

$$\left(\frac{\partial P_\sigma}{\partial Y_i}\right)^2 = \sum_{\substack{\gamma \in \mathbb{N}^s \\ |\gamma| \le d}} c_\gamma Y^{\gamma - 2e_i},$$

where

$$c_\gamma = \sum_{\substack{\alpha \in \mathbb{N}^s \\ \alpha \le \gamma}} \alpha_i(\gamma_i - \alpha_i) a_\alpha a_{\gamma - \alpha}.$$

Write $Q = \sum_{\substack{\delta\in\mathbb{N}^s \\ |\delta|\le d-2}} d_\delta Y^\delta$. Since $Q = \sum_{i=1}^{s} \left(\frac{\partial P_\sigma}{\partial Y_i}\right)^2$, its coefficients are bounded as follows:

$$\begin{aligned} |d_\delta| &\le s \sum_{\substack{\alpha\in\mathbb{N}^s \\ \alpha\le\gamma}} \alpha_i(\gamma_i-\alpha_i) a_\alpha a_{\gamma-\alpha} \\ &\le s d^2 2^{2\tau_\sigma} d^k \\ &\le k 2^{2\tau_\sigma} d^{k+2}. \end{aligned}$$

Hence, the bitsize of the coefficients of Q is bounded by τ_Q, where

$$\tau_Q = 2\tau_\sigma + (k+2)\,\mathrm{bit}(d) + \mathrm{bit}(k) = 2\tau + (2d+1)\,\mathrm{bit}(k) + (k+2)\,\mathrm{bit}(d) + 2,$$

where the last equality follows from equation (2.1). The result now follows from the complexity analysis of Algorithm 2.8. □

Let $P_u(T) = g_0(T)^d P_\sigma\left(\frac{g_1(T)}{g_0(T)}, \ldots, \frac{g_s(T)}{g_0(T)}\right)$. We have:

Lemma 2.11. *The degree of P_u is bounded by $d_{P,u} = d_u d$.*
The bitsize of its coefficients is bounded by $\tau_{P,u}$, where

$$\tau_{P,u} = d\,[\tau_u + \mathrm{bit}(d_u+1)] + \tau + d\,\mathrm{bit}(k) + d + k + 1.$$

Proof. The result about the degree is clear from the previous lemma.
The bound on the bitsize of the coefficients is obtained by substitution, using Proposition 8.11 of [BPR]. □

The minimum m of P_σ over σ is attained at a point $x \in \sigma$ contained in a connected component of $\mathcal{Z}$ included in the ball $B(0,1)$. Since P_σ is constant on such a component, m is also attained at some point x_u associated to an already computed rational univariate representation $u = (F(T), g_0(T), g_1(T), \ldots, g_s(T), \pi)$.

Since t_π is a root of F, the minimum $m = P_\sigma(x_u)$ is a root of the resultant

$$R(Z) = \mathrm{Res}_T\left(P_u(T) - g_0(T)^d Z, F(T)\right).$$

Example 2.12. *We consider here the following easy example (Berg polynomial, see Example 37 in [Sc]):*

$$B := x^2y^2(x^2+y^2-1)+1.$$

It is easy to show that B is positive on Δ. We now compute its minimum.

- *On the three vertices of* Δ*, we have* $B = 1$*.*
- *On the faces* $\{x = 0\}$ *and* $\{y = 0\}$*, we have* $B = 1$*.*
- *Consider the face* $\{x + y = 1\}$*. Replacing* x *by* $1 - y$ *leads to consider the (univariate) polynomial*

$$B_{\{x+y=1\}} = 2y^6 - 6y^5 + 6y^4 - 2y^3 + 1.$$

Since $B'_{\{x+y=1\}} = 6y^2(y-1)^2(2y-1)$*, the minimum of* $B_{\{x+y=1\}}$ *is* $31/32$*, attained at* $y = 1/2$*.*

- *We now compute the values of* B *at its critical points contained in the interior of* Δ*. It is easy to show that those points* (x, y) *satisfy*

$$\begin{aligned} 2x^2 + y^2 &= 1 \\ x^2 + 2y^2 &= 1. \end{aligned}$$

Note that this easily implies that there is only a finite number of such critical points. A rational univariate representation of this set can then be computed (using for example Salsa software, see [Sa]):

$$\begin{aligned} F &= (3T^2 - 1)(T^2 - 3) \\ g_0 &= T(3T^2 - 5) \\ g_1 &= T^2 + 1 \\ g_2 &= 2(T^2 - 1). \end{aligned}$$

The resultant $R(Z)$ *is equal to*

$$\begin{aligned} R(Z) &= \mathrm{Res}_T\left(g_0(T)^6 B\left(\frac{g_1(T)}{g_0(T)}, \frac{g_2(T)}{g_0(T)}\right) - Z g_0(T)^6, F(T)\right) \\ &= 2^{48}3^6(27Z - 26)^4. \end{aligned}$$

The only root $26/27 < \min(1, 31/32)$ *is thus the minimum of* B *over* Δ*, corresponding to the root* $\sqrt{3}$ *of* F*, and giving the minimizer*

$$\left(\frac{g_1(\sqrt{3})}{g_0(\sqrt{3})}, \frac{g_2(\sqrt{3})}{g_0(\sqrt{3})}\right) = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right).$$

In order to obtain a lower bound on the minimum depending only on k, d and τ, one needs to bound the roots of $R(Z)$. This can be done by controlling the size of the coefficients of $R(Z)$ and then using Cauchy's bound. Write

$$F(T) = \sum_{i=0}^{d_u} f_i T^i,$$

$$P_u(T) = \sum_{i=0}^{d_{P,u}} a_i T^i$$

and

$$g_0(T)^d = \sum_{i=0}^{d_u d} b_i T^i = \sum_{i=0}^{d_{P,u}} b_i T^i.$$

Lemma 2.13. *The polynomial $g_0(T)^d$ has degree bounded by $d_u d = d_{P,u}$, and the bitsize of its coefficients is bounded by $d(\tau_u + \mathrm{bit}(d_u + 1)) \leq \tau_{P,u}$.*

Proof. The degree of $g_0(T)^d$ is clearly less than $d_u d = d_{P,u}$. We now show the bound on the bitsize of its coefficients. Recall that the degree of g_0 is bounded by $d_u$and that the bitsize of its coefficients is less thanτ_u. When multiplying a univariate polynomial f by g_0, the increase in the bitsize of the coefficients is at most $\tau_u + \mathrm{bit}(d_u + 1)$. Indeed, the coefficients of fg_0 are sums of at most $(d_u + 1)$ products of a coefficient of f by a coefficient of g_0. The conclusion follows easily. □

The resultant $R(Z)$ is the determinant of the matrix $\mathrm{Syl}(Z)$, where $\mathrm{Syl}(Z)$ is the following Sylvester matrix:

$$\begin{pmatrix}
a_{d_{P,u}} - b_{d_{P,u}} Z & \cdots & \cdots & & \cdots & \cdots & a_0 - b_0 Z & 0 & \cdots & 0 \\
0 & \ddots & & & & & & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & & & & & & \ddots & 0 \\
0 & \cdots & 0 & a_{d_{P,u}} - b_{d_{P,u}} Z & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 - b_0 Z \\
f_{d_u} & \cdots & \cdots & \cdots & f_0 & 0 & \cdots & \cdots & & 0 \\
0 & \ddots & & & & \ddots & \ddots & & & \vdots \\
\vdots & \ddots & \ddots & & & & \ddots & \ddots & & \vdots \\
\vdots & & \ddots & \ddots & & & & & \ddots & 0 \\
0 & \cdots & \cdots & 0 & f_{d_u} & \cdots & \cdots & \cdots & & f_0
\end{pmatrix}
\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}
\left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} d_u
\left.\begin{matrix} \\ \\ \\ \\ \\ \end{matrix}\right\} d_{P,u}$$

$R(Z) = \sum_{i=0}^{d_u} r_i Z^i$ is a polynomial of degree $\leq d_u$ in Z, whose coefficients are controlled in the following fashion:

Lemma 2.14. *For all $i \in \{0, \ldots, d_u\}$,*

$$|r_i| < \binom{d_u}{i} \left[2^{\tau_{P,u}} \sqrt{d_{P,u}+1}\right]^{d_u} \left[2^{\tau_u} \sqrt{d_u+1}\right]^{d_{P,u}}.$$

Proof. We proceed as in the proof of lemma 1.1.
Let (with obvious notation)

$$\left(A_1 + ZB_1, \ldots, A_{d_u} + ZB_{d_u}, C_1, \ldots, C_{d_{P,u}}\right)$$

be the rows of the Sylvester matrix $\mathrm{Syl}(Z)$. Using the multilinearity of the determinant, we can write $R(Z) = \sum_{i=1}^{d_u} r_i Z^i$, where, for all $i \in \{0, \ldots, d_u\}$, r_i is a sum of $\binom{d_u}{i}$ determinants of matrices built with:

- i rows among the B_j's
- $d_u - i$ rows among the A_j's
- the $d_{P,u}$ rows $C_1, \ldots, C_{d_{P,u}}$.

Hadamard's bound (see [BPR]) implies that, for all i:

$$\begin{aligned} |r_i| &\leq \binom{d_u}{i} \sqrt{\left[(d_{P,u}+1)\left(2^{2\tau_{P,u}}-1\right)\right]^{d_u}} \sqrt{\left[(d_u+1)\left(2^{2\tau_u}-1\right)\right]^{d_{P,u}}} \\ &< \binom{d_u}{i} \left[2^{\tau_{P,u}} \sqrt{d_{P,u}+1}\right]^{d_u} \left[2^{\tau_u} \sqrt{d_u+1}\right]^{d_{P,u}}, \end{aligned}$$

as claimed. □

Since the minimum m is a root of $R(Z)$, Cauchy's bound finally gives the estimate we were looking for.

Let $\mathcal{U}$ be a set of rational univariate representations whose associated points meet every bounded connected component of

$$\mathcal{Z}_\sigma = \left\{ x \in \mathbb{R}^s \,\middle|\, \frac{\partial P_\sigma}{\partial Y_1}(x) = \cdots = \frac{\partial P_\sigma}{\partial Y_s}(x) = 0 \right\},$$

for each face σ of Δ.

Also, let d_u (resp. τ_u) be a bound on the degree (resp. the bitsize of the coefficients) of the polynomials occuring in the rational univariate representations of $\mathcal{U}$, and $d_{P,u}$ (resp. $\tau_{P,u}$) be a bound on the degree (resp. the bitsize of the coefficients) of the polynomial P_u. Then:

Theorem 2.15.

$$m > \frac{1}{\left[2^{\tau_{P,u}+1}\sqrt{d_{P,u}+1}\right]^{d_u}\left[2^{\tau_u}\sqrt{d_u+1}\right]^{d_{P,u}}}.$$

Proof. Since R has at least one non-zero root ($R(m) = 0$), we can write

$$R(Z) = \sum_{i=q}^{p} r_i Z^i,$$

with $q < p \leq d_u$ and $r_q r_p \neq 0$.

Cauchy's bound then implies:

$$\begin{aligned}
\frac{1}{m} &\leq \sum_{i=0}^{d_u} |r_i| \\
&< \sum_{i=0}^{d_u} \binom{d_u}{i} \left[2^{\tau_{P,u}}\sqrt{d_{P,u}+1}\right]^{d_u} \left[2^{\tau_u}\sqrt{d_u+1}\right]^{d_{P,u}} \\
&\leq 2^{d_u} \left[2^{\tau_{P,u}}\sqrt{d_{P,u}+1}\right]^{d_u} \left[2^{\tau_u}\sqrt{d_u+1}\right]^{d_{P,u}} \\
&\leq \left[2^{\tau_{P,u}+1}\sqrt{d_{P,u}+1}\right]^{d_u} \left[2^{\tau_u}\sqrt{d_u+1}\right]^{d_{P,u}},
\end{aligned}$$

as announced. □

Using Lemmas 2.10 and 2.11, Theorem 2.15 immediately implies:

Theorem 2.16. *Let $P \in \mathbb{Z}[X_1, \ldots, X_k]$ be a polynomial of degree d, τ a bound on the bitsize of its coefficients and $m = \min_{\Delta} P$ the minimum of P over the simplex Δ. Assume that $m > 0$.*
Let

$$\begin{aligned}
D &= 2d(2d-1)^{k-1}, \\
\rho &= D(2kd - 2k + 2)\left[\tau' + 2\,\mathrm{bit}(2kd - 2k + 3) + 3\,\mathrm{bit}(D) + \mathrm{bit}(k)\right], \\
\rho' &= d\left[\rho + \mathrm{bit}(D+1)\right] + \tau + d\,\mathrm{bit}(k) + d + k + 1,
\end{aligned}$$

where

$$\tau' = 2\tau + (2d+2)\,\mathrm{bit}(k) + (k+3)\,\mathrm{bit}(d) + 5.$$

Then:

$$m > m_{k,d,\tau},$$

where

$$m_{k,d,\tau} = \frac{1}{\left[2^{\rho'+1}\sqrt{dD+1}\right]^{D}\left[2^{\rho}\sqrt{D+1}\right]^{dD}}.$$

Remark 2.17. *We now give a more compact bound, derived from the last corollary. This will enable us to compare our results to those of de Loera and Santos ([LS]) and Canny ([C]).*
The following estimates

$$\begin{aligned} D+1 &\leq 2^k d^k \\ \frac{\rho}{2^{k+1}d^{k+1}k} &\leq 2\tau + (2d+5)\,\mathrm{bit}(k) + (4k+5)\,\mathrm{bit}(d) + 6k + 9 \\ \frac{\rho'}{2^{k+1}d^{k+2}k} &\leq 2\tau + (2d+5)\,\mathrm{bit}(k) + (4k+5)\,\mathrm{bit}(d) + 6k + 9 \end{aligned}$$

lead to the bound:

$$\frac{1}{m_{k,d,\tau}} \leq (2^{\tau})^{2^{k+3}d^{k+1}k}\, 2^{2^{k+6}d^{k+2}k^2} k^{2^{k+5}d^{k+2}k} d^{2^{k+5}d^{k+1}k^2}. \tag{2.2}$$

In [LS], the authors give the following estimate:

$$\frac{1}{m_{k,d,\tau}} \leq (2^{\tau})^{B^{c(k+1)}}\, 2^{B^{c(k+1)}}, \tag{$\dagger$}$$

where B denotes a bound on $\max(d+1, k+1)$ and c is an (unknown) universal constant. Note that bound (2.2) *implies that*

$$\frac{1}{m_{k,d,\tau}} \leq (2^{\tau})^{2^{k+3}d^{k+1}k}\, 2^{2^{k+7}d^{k+2}k^2},$$

giving an explicit version of estimate ($\dagger$).

Moreover, a direct application of Canny's theorem ([C]), under a non-degeneracy assumption on the following polynomial system (with unknowns $m, Y_1, \ldots, Y_s$)

$$\begin{cases} P_\sigma(Y_1, \ldots, Y_s) = m \\ \dfrac{\partial P_\sigma}{\partial Y_1}(Y_1, \ldots, Y_s) = \cdots = \dfrac{\partial P_\sigma}{\partial Y_s}(Y_1, \ldots, Y_s) = 0, \end{cases} \tag{S}$$

leads to the estimate

$$\frac{1}{m_{k,d,\tau}} \leq \left(3d2^{\tau_\sigma}\right)^{(k+1)d^{k+1}} = \left(6dk^d 2^d 2^{\tau}\right)^{(k+1)d^{k+1}}. \tag{$\ddagger$}$$

In the general case, (2.2) *implies*

$$\frac{1}{m_{k,d,\tau}} \leq \left(dk^d 2^d 2^\tau\right)^{2^{k+5}k^2 d^{k+1}},$$

where the main difference with (‡) *is the presence of the exponent* 2^{k+5}*. This essentially comes from doubling the degree of the system* (S) *by replacing the equations*

$$\frac{\partial P_\sigma}{\partial Y_1} = \cdots = \frac{\partial P_\sigma}{\partial Y_s} = 0$$

by the following single one

$$Q = \sum_{i=1}^{s} \left(\frac{\partial P_\sigma}{\partial Y_i}\right)^2 = 0,$$

in order to cover the degenerate cases as well.

References

[BCR] F. Boudaoud, F. Caruso, M.-F. Roy, *Certificates of Positivity in the Bernstein Basis*, Discrete and Computational Geometry, Volume 39, Number 4, 639-655 (2008)

[BPR] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in Real Algebraic Geometry*, Springer (2006), up-to-date electronic version available at:
`http://perso.univ-rennes1.fr/marie-francoise.roy`

[C] J. Canny, *The complexity of robot motion planning*, MIT Press (1987)

[LS] J. A. de Loera, F. Santos, *An effective version of Pölya's theorem on positive definite forms*, Journal of Pure and Applied Algebra, Volume 108, Issue 3, 231-240 (1996)

[R] F. Rouillier. *Solving zero-dimensional systems through the rational univariate representation*, Journal of Applicable Algebra in Engineering, Communication and Computing, Volume 9, Issue 5, 433-461 (1999)

[Sa] Salsa software, available at
`http://fgbrs.lip6.fr/salsa/Software/`

[Sc] M. Schweighofer, *Global optimization of polynomials using gradient tentacles and sums of squares*, SIAM Journal on Optimization, Volume 17, Issue 3, 920-942 (2006)