

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

Preprint version

Richard Leroy

January 5, 2009

Abstract

We consider the problem of bounding below the minimum value m taken by a positive polynomial $P \in \mathbb{Z}[X_1, \dots, X_k]$ of degree d over the standard simplex $\Delta \subset \mathbb{R}^k$. Using recent algorithmic developments in real algebraic geometry enables 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 works reported in the literature.

1 Introduction

1.1 Problem statement

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

$$\Delta = \left\{ x \in \mathbb{R}_+^k \mid \sum_{i=1}^k x_i \leq 1 \right\}.$$

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 no degeneracy conditions ([C]); in [LS], the authors use the Lojasiewicz inequality, leading to a bound involving a universal constant. The method presented here gives a completely explicit bound, with no extra assumption on P .

1.3 Univariate case

We begin with the univariate case, which contains the basic ideas of the proof in the general case. This situation has already been studied in [BPR], although the proof needs to be corrected. We present here a corrected 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 $R(Z) = \text{Res}_T(P(T) - Z, P'(T)) \in \mathbb{Z}[Z]$. The resultant $R(Z)$ is the determinant of the matrix $\text{Syl}(Z)$, where $\text{Syl}(Z)$ is the following Sylvester matrix:

$$\left(\begin{array}{cccccccccc} a_d & \cdots & \cdots & \cdots & a_1 & a_0 - Z & 0 & \cdots & 0 & \\ 0 & \ddots & & & & & \ddots & \ddots & \vdots & \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 & \\ 0 & \cdots & 0 & a_d & \cdots & \cdots & \cdots & a_1 & a_0 - Z & \\ (d-1)a_{d-1} & \cdots & \cdots & \cdots & a_1 & 0 & \cdots & \cdots & 0 & \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots & \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots & \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 & \\ 0 & \cdots & \cdots & 0 & (d-1)a_{d-1} & \cdots & \cdots & \cdots & a_1 & \end{array} \right) \left. \vphantom{\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}} \right\} \begin{array}{l} d-1 \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}$$

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

Lemma 1.1. *For all $i \in \{0, \dots, d-1\}$, 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 $(A_1, \dots, A_{d-1}, B_1, \dots, B_d)$ denote the rows of the classical Sylvester matrix $S(0)$. Then

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

where (e_1, \dots, 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 $i \in \{0, \dots, d-1\}$, 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, \dots, B_d .

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

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

as announced. \square

Since the minimum m is a root of the resultant $R(Z)$, 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 $R(Z)$. Cauchy's bound (see [BPR]) implies that

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

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 $P_k = X^d + (2^k X - 1)^2$. Here, $\tau = 2k$ and the minimum m_k of P_k satisfies*

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

and thus decreases exponentially with d and τ .

2 Bound on the minimum of multivariate positive polynomial

We now switch to the multivariate case.

2.1 Problem statement

Let $P \in \mathbb{Z}[X_1, \dots, X_k]$ 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, up to a small rise in 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 2.1. If σ is a vertex of Δ , then obviously $m \geq 1$. We now assume that $s \geq 1$.

Denote

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

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 $I = \{i_0, \dots, i_s\}$ of $\{0, \dots, k\}$ such that the vertices of σ are the vertices $(V_i)_{i \in I}$. Let J denote the complementary set of I in $\{0, \dots, k\}$. The face σ is characterized by :

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

We then proceed to 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 $P_\sigma \in \mathbb{Z}[X_{i_1}, \dots, X_{i_s}]$ satisfying :

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

Rewrite the variables X_{i_ℓ} into Y_ℓ .

$P_\sigma \in \mathbb{Z}[Y_1, \dots, Y_s]$ is a polynomial verifying :

Lemma 2.2. *The degree of P_σ is bounded by d . Besides, the bitsize of its coefficients is bounded by τ_σ , where*

$$\tau_\sigma = \tau + 1 + d\text{bit}(k).$$

Proof. The degree of P_σ is clearly lower than d .

We now show the result concerning the bitsizes of the coefficients.

- The result is clear if $s = k$. Assume that $s \leq k - 1$.

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

Replacing X_j by 0 does not change the bitsize of the coefficients, then 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

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

and

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

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. \square

Note that σ can be identified with the standard simplex of \mathbb{R}^s . Since

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

$P_{\sigma} \in \mathbb{Z}[Y_1, \dots, Y_s]$ achieves its minimum in the interior of σ . Consequently, m is attained at a critical point of P_{σ} , ie a point $x \in \mathbb{R}^s$ such that the gradient of P_{σ} is zero. 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 2.3. Let $P \in \mathbb{R}[X]$ be a real univariate polynomial, $x \in \mathbb{R}$ a real number and $\sigma \in \{0, 1, -1\}^{Der(P)}$ a sign condition on the set $Der(P) = \{P, P', \dots, P^{(\deg P)}\}$ of the derivatives of P .

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

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

We can now define a rational univariate representation as follows :

Definition 2.4. A s -rational univariate representation u is a $(s+3)$ -tuple of the form

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

such that :

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

Remark 2.5. If $t \in \mathbb{R}$ is a root of F , then $g_0(t) \neq 0$.

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

Definition 2.6. *The point associated to u is the point*

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

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

$$\mathcal{Z}(Q) = \{x \in \mathbb{R}^s \mid Q(x) = 0\}$$

be the (real) zero-set of Q . We are interested in finding a point in each connected component of $\mathcal{Z}(Q)$ included in the unit ball

$$B(0, 1) = \{x \in \mathbb{R}^s \mid \|x\|_2 \leq 1\}.$$

This can be done by applying algorithm 12.15 of [BPR] :

Algorithm 1 Bounded Algebraic Sampling

Require: A polynomial $Q \in \mathbb{Z}[X_1, \dots, X_s]$, nonnegative over \mathbb{R}^s .

Ensure: A set \mathcal{U} of rational univariate representations of the form

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

where the polynomials F, g_0, \dots, g_s have integer coefficients, and such that the associated points meet every connected component of $\mathcal{Z}(Q)$ included in the unit ball $B(0, 1)$.

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 degree of the polynomials F, g_0, \dots, g_k is bounded by

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

2. The bitsize of their coefficients is bounded by

$$(d_Q + 2)(d_Q + 1)^{k-1}(kd_Q + 2)(\tau' + 2\text{bit}(kd + 3) + 3\mu + \text{bit}(4k)),$$

where

$$\tau' = \sup[\tau_Q, d_Q + 2, \text{bit}(2k - 1)] + 1 + 2\text{bit}[k(d_Q + 2)]$$

$$\mu = \text{bit}\left[(d_Q + 2)(d_Q + 1)^{k-1}\right].$$

2.3 The bound

Recall that $P_\sigma \in \mathbb{Z}[Y_1, \dots, Y_s]$ achieves its minimum in the interior of σ . Consequently, this minimum is attained at a critical point of P_σ , ie a point $x \in \mathbb{R}^s$ such that the gradient of P_σ is zero. Consider the set of critical points

$$\mathcal{Z} = \left\{ x \in \mathbb{R}^s \mid \sum_{i=1}^s \left(\frac{\partial P_\sigma}{\partial Y_i} \right)^2 (x) = 0 \right\}.$$

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, $C \subset B(0, 1) \subset \mathbb{R}^s$.

Algorithm 1 then gives a set of rational univariate representations of the form

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

whose associated points meet every connected component of \mathcal{Z} contained in $B(0, 1)$. In particular, they meet every connected component of \mathcal{Z} containing a minimizer of P_σ in σ . We easily control the degree and the bitsize of the coefficients of the polynomials $F(T), g_0(T), g_1(T), \dots, g_s(T)$:

Lemma 2.7. *The degree of the polynomials F, g_0, \dots, g_s is bounded by d_u , where*

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

Moreover, the bitsize of their coefficients is bounded by

$$\tau_u = 2d(2d - 1)^{k-1}(2kd - 2k + 2) [\tau' + 2\text{bit}(2kd - 2k + 3) + 3\mu + \text{bit}(4k)],$$

where

$$\begin{aligned} \tau' &= 2\tau + (2d + 2)\text{bit}(k) + (k + 3)\text{bit}(d) + 4 \\ \mu &= \text{bit} \left[2d(2d - 1)^{k-1} \right]. \end{aligned}$$

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

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

then

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

where

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

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

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

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

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

The result now follows from the complexity analysis of algorithm 1. \square

We can now construct the following polynomials :

$$P_u(T) = g_0(T)^d P_\sigma \left(\frac{g_1(T)}{g_0(T)}, \dots, \frac{g_s(T)}{g_0(T)} \right).$$

We then have :

Lemma 2.8. *The degree of P_u is bounded by $d_{P,u} = d_u d$. Besides, the bitsize of its coefficients is bounded by $\tau_{P,u}$, where*

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

Proof. The result about the degree is clear in sight of the previous lemma. The bound on the bitsize of the coefficients is obtained by substitution, using proposition 8.11 of [BPR]. \square

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 $x_u(t_\pi)$ associated to an already computed rational univariate representation $u = (F(T), g_0(T), g_1(T), \dots, g_s(T), \pi)$.

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

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

Example 2.9. We consider here the following easy example (Berg polynomial, see example 37 in [Sc]):

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

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

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

We now compute a rational univariate representation of this set. Salsa software (see [Sa]) produces the following one :

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

The resultant $R(Z)$ equals

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

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 evaluate 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 2.10. $g_0(T)^d$ is a polynomial of degree less than $d_u d = d_{P,u}$, and the bitsize of its coefficients is bounded by $d(\tau_u + \text{bit}(d_u + 1)) \leq \tau_{P,u}$.

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 than τ_u . When multiplying a univariate polynomial f by g_0 , the rise of the bitsize of the coefficients is at most $\tau_u + \text{bit}(d_u + 1)$. Indeed, the coefficients of $f g_0$ are sums of at most $(d_u + 1)$ products of a coefficient of f by a coefficient of g_0 . The conclusion follows. \square

The resultant $R(Z)$ is the determinant of the matrix $\text{Syl}(Z)$, where

$Syl(Z)$ is the following Sylvester matrix :

$$\left(\begin{array}{cccccccccccc} a_{d_{P,u}} - b_{d_{P,u}}Z & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 - b_0Z & 0 & \cdots & 0 & & \\ 0 & \ddots & & & & & & \ddots & \ddots & \vdots & & \\ \vdots & \ddots & \ddots & & & & & & \ddots & 0 & & \\ 0 & \cdots & 0 & a_{d_{P,u}} - b_{d_{P,u}}Z & \cdots & \cdots & \cdots & \cdots & \cdots & a_0 - b_0Z & & \\ f_{d_u} & \cdots & \cdots & \cdots & f_0 & 0 & \cdots & \cdots & \cdots & 0 & & \\ 0 & \ddots & & & & \ddots & \ddots & & & \vdots & & \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & & \vdots & & \\ \vdots & & \ddots & \ddots & & & & \ddots & & 0 & & \\ 0 & \cdots & \cdots & 0 & f_{d_u} & \cdots & \cdots & \cdots & \cdots & f_0 & & \end{array} \right) \left. \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} d_u \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ d_{P,u} \end{array}$$

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

Lemma 2.11. For all $i \in \{0, \dots, d_u\}$,

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

Proof. We proceed as in the proof of lemma 1.1.

With obvious notations, write

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

the rows of the Sylvester matrix $Syl(Z)$. Using the multilinearity of the determinant, we can write $R(Z) = \sum_{i=1}^{d_u} r_i Z^i$, where, for all $i \in \{0, \dots, d_u\}$, 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 $C_1, \dots, C_{d_{P,u}}$.

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

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

as announced. \square

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

Theorem 2.12. *Let $P \in \mathbb{Z}[X_1, \dots, X_k]$ 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 standard simplex Δ . Assume that $m > 0$.*

Moreover, let \mathcal{U} be a set of rational univariate representations of the form

$$u = (F(T), g_0(T), \dots, g_k(T), \pi)$$

giving a point in each connected component included in the ball $B(0, 1) \subset \mathbb{R}^s$ of

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

for all face σ of V .

Besides, let d_u (resp. τ_u) be a bound on the degree (resp. the bitsize of the coefficients) of the polynomials occurring in the rational univariate representations of \mathcal{U} .

We then write

$$d_{P,u} = d_u d$$

and

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

the bounds on the degree and on the bitsize of the coefficients of the polynomials

$$P_u(T) = g_0(T)^d P_\sigma \left(\frac{g_1(T)}{g_0(T)}, \dots, \frac{g_s(T)}{g_0(T)} \right).$$

Then :

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

where

$$m_{d,\tau,u} = \frac{1}{[2^{\tau_{P,u}+1} \sqrt{d_{P,u}+1}]^{d_u} [2^{\tau_u} \sqrt{d_u+1}]^{d_{P,u}}}.$$

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

$$R(Z) = \sum_{i=c}^{d_u} r_i Z^i,$$

with $d_u > c$ and $r_c r_{d_u} \neq 0$.

Cauchy's bound then implies :

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

as announced. \square

Corollary 2.13. *In particular, one can choose*

$$\begin{aligned}
d_u &= 2d(2d-1)^{k-1} \\
\tau_u &= 2d(2d-1)^{k-1}(2kd-2k+2) [\tau' + 2\text{bit}(2kd-2k+3) + 3\mu + \text{bit}(4k)],
\end{aligned}$$

where

$$\begin{aligned}
\tau' &= 2\tau + (2d+2)\text{bit}(k) + (k+3)\text{bit}(d) + 4 \\
\mu &= \text{bit} \left[2d(2d-1)^{k-1} \right].
\end{aligned}$$

The bound corresponding to this choice is the bound $m_{k,d,\tau}$ we were aiming at.

Remark 2.14. *In [LS], the authors give the following estimate :*

$$\frac{1}{m} \leq (2^\tau)^{D^{c(k+1)}} 2^{D^{c(k+1)}} \quad (\dagger)$$

where D denotes a bound on $\max(d+1, k+1)$ and c is (unknown) universal constant. With our method, repetitive but straightforward estimations lead to the following simple bound :

$$\frac{1}{m_{k,d,\tau}} \leq (2^\tau)^{2^{2k+3} d^{2k+2} (k+1)} 2^{2^{2k+8} (d+1)^{2k+2} (k+1)^2}.$$

In particular, we have :

$$\frac{1}{m} \leq (2^{\tau})^{D^{4k+6}} 2^{D^{4k+12}}.$$

Thus, we can take $c = 12$ in the bound (†).

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 Pólya's theorem on positive definite forms*, *Journal of Pure and Applied Algebra*, Volume 108, Issue 3, 231-240 (1996)
- [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)