Discrete Comput Geom (2008) 39: 639–655
DOI 10.1007/s00454-007-9042-x

Certificates of Positivity in the Bernstein Basis

Fatima Boudaoud · Fabrizio Caruso · Marie-Françoise Roy

Received: 3 November 2005 / Revised: 25 August 2007 /
Published online: 5 December 2007

Abstract Let $P \in \mathbb{Z}[\mathbb{X}]$ be a polynomial of degree p with coefficients in the monomial basis of bit-size bounded by τ. If P is positive on $[-1, 1]$, we obtain a certificate of positivity (i.e., a description of P making obvious that it is positive) of bit-size $O(p^4(\tau + \log_2 p))$. Previous comparable results had a bit-size complexity exponential in p and τ (Powers and Reznick in Trans. Am. Math. Soc. 352(10):4677–4692, 2000; Powers and Reznick in J. Pure Appl. Algebra 164:221–229, 2001).

1 Introduction: Certificates of Positivity in the Bernstein Basis

A certificate of positivity on an interval is an algebraic identity certifying the positivity of a given polynomial on an interval. Certificates of positivity on intervals have been considered by many authors (see [10, 12] for a bibliography and some historical remarks). In this paper we concentrate on certificates of positivity in the Bernstein basis, for which quantitative bounds have been obtained recently [12, 13]. However, the exponential character of these bounds was unsatisfactory. Our purpose in this paper is to produce certificates of positivity in the Bernstein basis which are of polynomial size.

We denote by R a real closed field, and consider polynomials in $R[X]$.

F. Boudaoud
Département de Mathématiques, Université d'Oran, Sénia BP 1524, Oran 31000, Algeria
e-mail: fboudaoud@yahoo.fr

F. Caruso
Facult'a di Scienze Mathematiche, Fisiche e Naturali, Universita di Pisa, Via Buonarroti 2, 56127 Pisa, Italy
e-mail: caruso@dm.unipi.it

M.-F. Roy (✉)
IRMAR, Universite de Rennes 1-CNRS, Campus de Beaulieu, 35042 Rennes CEDEX, France
e-mail: marie-francoise.roy@univ-rennesl.fr

Let $\ell < r$ be two elements of R and p be a natural number. The *Bernstein polynomials* of degree p for ℓ, r are

$$\mathrm{Bern}_{p,i}(\ell, r) = \binom{p}{i} \frac{(r-X)^{p-i}(X-\ell)^i}{(r-\ell)^p}, \tag{1}$$

for $i = 0, \ldots, p$.

Note that

- the Bernstein polynomials for ℓ, r take positive values on (ℓ, r)
- $\mathrm{Bern}_{p,0}(\ell, r)$ is positive at ℓ and $\mathrm{Bern}_{p,p}(\ell, r)$ is positive at r; and
- the Bernstein polynomials of degree p for ℓ, r form a basis of the vector-space of polynomials of degree $\leq p$ [1]

If P is a polynomial of degree $\leq p$, we denote by

$$b(P, p, \ell, r) = [b(P, p, \ell, r)_0, \ldots, b(P, p, \ell, r)_p],$$

the ordered list of coefficients of P in the Bernstein basis of degree p for ℓ, r. Note that $b(P, p, \ell, r)_0$ is the value of P at ℓ and $b(P, p, \ell, r)_p$ is the value of P at r.

If all the elements of $b(P, p, \ell, r)$ are positive, the expression of P in the Bernstein basis of degree d for ℓ, r provides a certificate of positivity for P on $[\ell, r]$, referred to as a *global certificate of positivity for P on $[\ell, r]$*.

So, if P is of degree p and all the elements of $b(P, p, -1, 1)$ are positive, P is positive on $[-1, 1]$. Unfortunately, the reciprocal is not true: there are polynomials of degree p which are positive on $[-1, 1]$ and some elements of $b(P, p, -1, 1)$ are negative. Consider for example the polynomial

$$P = 5X^2 - 4X + 1.$$

It is immediate to check that P is positive on $[-1, 1]$, but $b(P, 2, -1, 1) = [10, -4, 2]$ has negative elements. However, since $b(P, 23, -1, 1)$ is

$$\left[10, \frac{202}{23}, \frac{1934}{253}, \frac{1666}{253}, \frac{1418}{253}, \frac{1190}{253}, \frac{982}{253}, \ldots, \frac{14}{253}, \frac{2}{11}, \frac{98}{253}, \frac{170}{253}, \frac{262}{253}, \frac{34}{23}, 2\right],$$

with all entries positive, the polynomial P does have a global certificate of positivity in degree 23 on $[-1, 1]$.

Bernstein proved the following result [3].

Theorem 1 (Bernstein's theorem) *f a nonzero univariate polynomial $P \in \mathbb{R}[X]$ of degree p is positive on $[-1, 1]$, then there exists $d \geq p$ such that all the elements of $b(P, d, -1, 1)$ are positive.*

In other words, by increasing if necessary the degree of the Bernstein basis, a positive polynomial on $[-1, 1]$ always gets a global certificate of positivity.

Bernstein's theorem is equivalent to a famous result of Pólya about certificates of positivity for polynomials on the half line [11].

Theorem 2 (Pólya's theorem) *If a nonzero univariate polynomial $P \in \mathbb{R}[X][X]$ of degree p is positive on $(0, +\infty)$, then there exists $d \geq p$ such that all the coefficients of $(1+X)^{d-p}P$ are positive.*

The equivalence between Bernstein's theorem and Pólya's theorem is immediate through the Goursat transform sending a polynomial P of degree p to

$$(X+1)^p P\left(\frac{1-X}{1+X}\right),$$

since monomials X^i are sent to $(1-X)^i(1+X)^{p-i}$.

In this paper, we are going to consider certificates of positivity for P on $[-1, 1]$ of a more local nature, using also the Bernstein basis. We keep the initial degree, and refine the interval, looking for certificates of positivity on subintervals subdividing $[-1, 1]$.

We notice that it is not necessary that all the elements of $b(P, d, \ell, r)$ are positive to ensure the positivity of P on $[\ell, r]$: if CertPos$(b(P, d, \ell, r))$ holds, i.e., all the elements of $b(P, d, \ell, r)$ are non-negative, with $b(P, d, \ell, r)_0 > 0$, $b(P, d, \ell, r)_d > 0$, then P is positive on $[\ell, r]$.

A *subdivision L of $[-1, 1]$ of length n* is an ordered list $\ell_0 = -1 < \ell_1 < \cdots < \ell_n = 1$. We denote by $b(P, p, L)$ the finite list whose elements are the $b(P, p, \ell_{i-1}, \ell_i)$, $i = 1, \ldots, n$. We define CertPos$(b(P, p, L))$ holds for every $i = 1, \ldots, n$, CertPos$(b(P, p, \ell_{i-1}, \ell_i))$ holds.

The fact that CertPos$(b(P, p, L))$ holds is referred to as a *local certificate of positivity for P on $[-1, 1]$*.

The difference between local and global certificates of positivity is illustrated by the following example.

We consider again $P = 5X^2 - 4X + 1$, and notice that P has a local certificate of positivity since CertPos$(b(P, p, L))$ holds, with $L = [-1, 0, 1/2, 1]$,

$$b(P, 2, L) = [[10, 3, 1][1, 0, 1/4], [1/4, 1/2, 2]],$$

which reads as

- $b(P, 2, -1, 0) = [10, 3, 1]$
- $b(P, 2, 0, 1/2) = [1, 0, 1/4]$
- $b(P, 2, 1/2, 1) = [1/4, 1/2, 2]$

It is clear that the local certificate of positivity given by $b(P, 2, L)$ is shorter than the global certificate of positivity given by $b(P, 23, -1, 1)$ discussed earlier.

The reason $b(P, 2, L)$ is shorter than $b(P, 23, -1, 1)$ is that the various subintervals defined by L are of different length, short intervals being concentrated on parts of $|-1, 1]$ where the sign of P is not obvious. This adaptability is the key to shorter positivity certificates.

The purpose of the paper is to prove the existence of local certificates of positivity, shorter (of polynomial size rather than of exponential size) than the global ones in the integer case. The paper is organized as follows. In Sect. 2 we prove the existence of a local certificate of positivity in any real closed field. In Sect. 3 we prove, in the integer case, the existence of a local certificate of positivity of size polynomial in the degree

and the bit-size of the coefficients. In Sect. 4 we compare the size of the global and local certificates and prove that the global certificates can indeed be exponentially big. Finally, in Sect. 5, we prove that our local of certificate can be used to produce a Positivstellensatz identity of size polynomial in d and τ.

2 Certificates of Positivity in a General Real Closed Field

In this section we prove that while global certificates of positivity do not always exist in a general real closed field, local certificates of positivity always do.

We first prove that in a nonarchimedean real closed field R, Bernstein's theorem does not hold. For this purpose, we exhibit a very simple $P \in R[X]$, positive on $[-1, 1]$, and such that there does not exist $d \in \mathbb{N}$ such that all the elements of $b(P, d, -1, 1)$ are positive.

Example 1 Let R be a nonarchimedean real closed field and ε an element of R which is infinitesimal, i.e., positive and smaller than any positive rational number. It is clear that the polynomial $P = (1-\varepsilon)X^2 + \varepsilon$ is positive on $[-1, 1]$. However, we are going to prove that for every $d \in \mathbb{N}$, there exists a negative element in $b(P, d, -1, 1)$. Indeed, we have $b(P, 2, -1, 1) = [1, 2\varepsilon - 1, 1]$, thus for any $d \geq 2$

$$2^d P = \big((1-X)^2 + (4\varepsilon - 2)(1-X)(X+1) + (X+1)^2\big)((1-X) + (X+1))^{d-2}.$$

Hence, if $n \leq d-2$,

$$\binom{d}{n} b(P, d, -1, 1)_n = \binom{d-2}{n-2} + \binom{d-2}{n-1}(4\varepsilon - 2) + \binom{d-2}{n}. \tag{2}$$

– If d is even, taking $n = d/2$, it follows from (2) that

$$b(P, d, -1, 1)_n = \frac{d\varepsilon - 1}{d-1}.$$

– If d is odd, taking $n = (d-1)/2$, it follows from (2) that

$$b(P, d, -1, 1)_n = \frac{(d+1)\varepsilon - 1}{d}.$$

Since ε is infinitesimal and $d \in \mathbb{N}$, $b(P, d, -1, 1)_n < 0$ in both cases for any natural number d.

We now prove the existence of local certificates of positivity in a general real closed field R. Given ℓ, r in R, we denote by $C(\ell, r) \subset R^2$ the open disk with diameter $[\ell, r]$, i.e., the open disk with center $(\frac{\ell+r}{2}, 0)$ and radius $\frac{\ell-r}{2}$ and identify the algebraically closed field $C = R[i]$ with R^2.

We use the following classical result (see [1], Theorem 10.44(a), noticing that the separability hypothesis is not necessary for (a)). We denote by $\mathrm{Var}(a)$ the number of sign variations in a list of numbers a.

Theorem 3 *If P has no root in $\mathcal{C}(\ell, r)$, then* $\mathrm{Var}(b(P, p, \ell, r)) = 0$.

Theorem 4 (Existence of local certificates of positivity) *If $P \in R[X]$ of degree p is positive on $[-1, 1]$, then there exists a subdivision L of $[-1, 1]$, of length at most $p + 1$ such that* $\mathrm{CertPos}(b(P, p, L))$ *holds.*

Proof Let $y_1 < \cdots < y_r$, $2r \leq p$, be the elements of $[-1, 1]$ which are the projections of a set of roots Z_j, $j = 1, \ldots, r$ of P in $C = R[i]$.

If $y_1 \neq -1$ and $y_r \neq 1$, let $\delta > 0$ be not greater than $(y_1 + 1)$, $(1 - y_r)$, $\min_{j=1\ldots r,\ z\in Z_j} |z - y_j|$ and $\min_{j=1\ldots r-1}(y_{j+1} - y_j)$. Define $n = 2r + 1$, $\ell_0 = -1$, $\ell_{2j-1} = y_j - \delta$, $\ell_{2j} = y_j + \delta$, $j = 1, \ldots, r$, $\ell_{2r+1} = 1$. Since, for $i = 1, \ldots, n$, P has no root in $\mathcal{C}(\ell_{i-1}, \ell_i)$, $\mathrm{CerPos}(b(P, p, \ell_{i-1}, \ell_i))$ holds by Theorem 3 [1].

The special cases where $y_1 = -1$ or $y_r = 1$ are similar. □

Remark 1 If F is an ordered field, R its real closure and $P \in F[X]$, the statement of Theorem 4 is not valid with the extra property "the elements of L belong to F". Indeed, let $F = \mathbb{R}(\varepsilon)$ ordered by $\varepsilon > 0$ and smaller than any positive $r \in \mathbb{R}$, and $\mathbb{R}\langle\varepsilon\rangle$ its real closure, i.e., the field of algebraic Puiseux series with coefficients in $\mathbb{R}$ ([1], Corollary 2.98). Take $P = X^4 + 2\varepsilon^2 X^2 - 2\varepsilon X^2 + \varepsilon^4 + 2\varepsilon^3 + \varepsilon^2$, whose roots are $\pm\sqrt{\varepsilon} \pm i\varepsilon$. So, P is positive on $[-1, 1]$. For ℓ, r in $\mathbb{R}(\varepsilon)$ with $-1 \leq \ell < \sqrt{\varepsilon} < r \leq 1$, denoting by $\overline{\ell}, \overline{r}$ the real numbers infinitely close to ℓ, r, we have $\overline{\ell} \leq 0$, $\overline{r} > 0$. One can compute—using, for example, SARAG [5]—that

$$b(P, 4, \ell, r) = \left[\varepsilon^2 + \cdots, ?, -\frac{\varepsilon}{3}\overline{r}^2 + \cdots, ?, \overline{r}^4 + \cdots\right], \quad \text{if } \overline{\ell} = 0,$$

$$b(P, 4, \ell, r) = \left[\overline{\ell}^4 + \cdots, \overline{\ell}^3\overline{r} + \cdots, \overline{\ell}^2\overline{r}^2 + \cdots, \overline{\ell}\overline{r}^3 + \cdots, \overline{r}^4 + \cdots\right], \quad \text{if } \overline{\ell} < 0,$$

where $+\cdots$ stands for "+ terms of higher order in ε", and ? for a quantity whose sign is not determined. It is easy to check that $b(P, \ell, r)$ has two sign changes if $\overline{\ell} = 0$, and $b(P, \ell, r)$ has four sign changes if $\overline{\ell} < 0$. So for every choice of ℓ, r in $\mathbb{R}(\varepsilon)$ with $-1 \leq \ell < \sqrt{\varepsilon} < r \leq 1$, $\mathrm{CertPos}(P, 4, \ell, r)$ does not hold, which implies that, for every subdivision L with elements in $\mathbb{R}(\varepsilon)$, $\mathrm{CertPos}(P, 4, L)$ does not hold.

On the other hand, taking $L = [-1, -\sqrt{\varepsilon} - \varepsilon, -\sqrt{\varepsilon} + \varepsilon, \sqrt{\varepsilon} - \varepsilon, \sqrt{\varepsilon} + \varepsilon, 1]$, the proof of Theorem 4 implies that $\mathrm{CertPos}(P, 4, L)$ does hold, with some elements of L belonging to $\mathbb{R}\langle\varepsilon\rangle \setminus \mathbb{R}(\varepsilon)$, and this can be checked by a direct computation.

3 Local Certificates of Positivity in the Case of Integer Coefficients

Let $P \in \mathbb{Z}[\mathbb{X}]$ be a polynomial of degree p with coefficients in the monomial basis of bit-size bounded by τ (i.e., the absolute values of the coefficients of P are $< 2^\tau$). The purpose of this section is to construct a local certificate of positivity for P on $[-1, 1]$ whose size is polynomial in p and τ.

We introduce the following notation. If L is a rational subdivision of $[-1, 1]$ of length n (i.e., a subdivision with elements in $\mathbb{Q}$) and $C = (c_1, \ldots, c_n) \in (\mathbb{Q}^+)^n$, we denote by $b(CP, p, L)$ the list $b(c_i P, p, \ell_{i-1}, \ell_i)$ for $i = 1, \ldots, n$. We say

that $\mathrm{CertPos}_{\mathbb{Z}}(b(CP, p, L))$ holds if $\mathrm{CertPos}(b(CP, p, L))$ holds and, for every $i = 1, \ldots, n$ and every $j = 0, \ldots, p$, $b(P, p, \ell_{i-1}, \ell_i) \in \mathbb{Z}$.

In this section we give, if $P \in \mathbb{Z}[X]$ is positive on $[-1, 1]$, an algorithm constructing L and C such that $\mathrm{CertPos}_{\mathbb{Z}}(b(CP, p, L))$ holds, with the bit-size of $\mathrm{CertPos}_{\mathbb{Z}}(b(CP, p, L))$ polynomial in p and τ.

More precisely, we consider a polynomial $P \in \mathbb{Z}[X]$ and construct

- a certificate of positivity if the polynomial is positive on $[-1, 1]$
- a certificate of negativity if the polynomial is negative on $[-1, 1]$ and
- a point x of $[-1, 1]$ such that $P(x) = 0$, otherwise

The algorithm decides first whether P has a root on $[-1, 1]$ and if it is not the case proceeds by dichotomy, in a way similar to the Real Root Isolation Algorithm (see [1], Algorithm 10.4).

The algorithm used to compute the Bernstein coefficients on a subinterval is a straightforward variant of the classical De Casteljau Algorithm avoiding denominators, named Special Bernstein Coefficients (cf. [1], Algorithm 10.3 for the subdivision in two equal segments, the general case being a straightforward generalization) with complexity $O(p^2)$. A fast algorithm in $\tilde{O}(p)$ with the same output can also be designed (see [1], Remark 10.39), where $\tilde{O}(p) = p \log(p)^{O(1)}$.

Algorithm 1 (Certificate of positivity)

- Input: a nonzero polynomial $P \in \mathbb{Z}[X]$.
- Output:
  - POS if $P > 0$ on $[-1, 1]$, a rational subdivision L of $[-1, 1]$ of length $n \leq p+1$, and $C \in (\mathbb{Q}^+)^{n+1}$ such that $\mathrm{CertPos}_{\mathbb{Z}}(b(CP, p, L))$.
  - NEG if $P < 0$ on $[-1, 1]$, a rational subdivision L of $[-1, 1]$ of length $n \leq p+1$, and $C \in (\mathbb{Q}^+)^{n+1}$ such that $\mathrm{CertPos}_{\mathbb{Z}}(b(-CP, p, L))$.
  - Otherwise, a value x such that $P(x) = 0$, or a segment $[\ell, r]$ and a divisor Q of P such that $Q(\ell)Q(r) < 0$.
- Procedure:
  - Preparatory Phase
    - Apply the Real Root Isolation Algorithm to P ([1], Algorithm 10.4) and decide whether there is a root of P between -1 and 1.
    - If the answer is YES, return
      - → A value x such that $P(x) = 0$.
      - → Or a divisor Q of P (in fact the separable part of P computed in the Real Root Isolation Algorithm) and a segment $[\ell, r]$ such that $Q(\ell)Q(r) < 0$ which are intermediate results computed by the Real Root Isolation Algorithm applied to P.
  - Otherwise compute $c \in \mathbb{Q}^+$ such that $b = b(cP, -1, 1) \in \mathbb{Z}^{p+1}$ ([1], Corollary 10.30). If $P(-1) = b_0 < 0$, replace P by $-P$. Place $[[-1, 1], c, b(cP, p, -1, 1)]$ in M.
  - Dichotomy Phase. Initialize $N = \emptyset$. While M is nonempty:
    - Remove an element $[[\ell, r], c, b(cP, p, \ell, r)]$ from M.
    - If $\mathrm{Var}(b(cP, p, \ell, r)) = 0$, add $[[\ell, r], c, b(cP, p, \ell, r)]$ to N.

  - Otherwise compute $b(c'P, p, \ell, m)$ and $b(c'P, p, m, r)$, with $m = (\ell + r)/2$, using Special Bernstein Coefficients Algorithm with input $b(cP, p, \ell, r)$, and add

$$([\ell, m], c', b(c'P, p, \ell, m)), ([m, r], c', b(c'P, p, m, r))$$

    to M.
  - Output N.
- Compression Phase. Initialize $L = [-1]$, $C = T := \emptyset$. While N is nonempty:
  - If N has one single element, place it at the end of T.
  - Otherwise, remove from N its first element $[[\ell, r], c, b(cP, p, \ell, r)]$.
  - Apply Special Bernstein Coefficients Algorithm to $[[\ell, r], c, b(cP, p, \ell, r)]$ and the end point m of the segment associated to the first element of N to get $b(c'P, p, \ell, m) \in \mathbb{Z}^{p+1}$.
  - If $\mathrm{Var}(b(c'P, \ell, m)) = 0$, replace the first element of N by

$$[[\ell, m], c', b(c'P, \ell, m)].$$

  - Otherwise, place r at the end of L, c at the end of C and $b(cP, p, \ell, r)$ at the end of T.
- If $b_0 > 0$, return POS and $b(cP, p, L) = T$.
- If $b_0 < 0$, output NEG and $b(cP, p, L) = -T$.

Example 2 Let us explain the process of Algorithm 1 for $P = X^4 + (8X - 1)^2$.

The Real Root Isolation Algorithm first decides that P has no root on $[-1, 1]$. The dichotomy phase proceeds as follows:

- $\mathrm{Var}(b(3P/2, 4, -1, 1) = [123, 12, -29, -12, 75]) = 2$, so it is necessary to refine $[-1, 1]$.
- The elements of $b(3P, 4, -1, 0) = [246, 135, 59, 15, 3]$ are all positive, while $\mathrm{Var}(b(3P, 4, 0, 1) = [3, -9, 11, 63, 150]) = 2$, so it is necessary to refine $[0, 1]$.
- $\mathrm{Var}(b(32^4P, 4, 0, 1/2) = [48, -48, -16, 144, 435]) = 2$, so it is necessary to refine $[0, 1/2]$, while the elements of $b(32^4P, 4, 1/2, 1) = [435, 726, 1148, 1704, 2400]$ are all positive.
- $\mathrm{Var}(b(32^8P, 4, 0, 1/4) = [768, 0, -256, 0, 771]) = 2$, so it is necessary to refine $[0, 1/4]$, while the elements of $b(32^8P, 4, 1/4, 1/2) = [771, 1542, 2828, 4632, 6960]$ are all positive.
- The isolation phase stops since the elements of $b(32^{12}P, 4, 0, 1/8) = [12288, 6144, 2,048, 0, 3]$, and $b(32^{12}P, 4, 1/8, 1/4) = [3, 6, 2060, 6168, 12336]$ are all positive.

So we obtained a local certificate of positivity for P.

Finally, this certificate is compressed in $L = [-1, 0, 1/8, 1]$, $C = [3, 32^{12}, 32^{12}]$ and $b(CP, p, L)$ is

$$[[246, 135, 59, 15, 3], [12288, 6144, 2048, 0, 3], [3, 24, 100544, 302592, 614400]].$$

Theorem 5 *Let $P \in \mathbb{Z}[X]$ be a univariate polynomial of degree p with coefficients of bit-size bounded by τ.*

The binary complexity of Algorithm 1 is $\tilde{O}(p^4\tau^2)$ *using fast algorithms.*

If $P > 0$ *on* $[-1, 1]$, *Algorithm 1 gives a certificate of positivity of bit-size* $O(p^4(\tau + \log_2 p))$.

If $P < 0$ *on* $[-1, 1]$, *Algorithm 1 gives a certificate of negativity of bit-size* $O(p^4(\tau + \log_2 p))$.

If there exist $x \in [-1, 1]$ *such that* $P(x) = 0$, *Algorithm 1 provides either a rational number* x *such that* $P(x) = 0$, *or rational numbers* ℓ, r *such that* $Q(\ell)Q(r) < 0$ *with* Q *a divisor of* P. *The rational numbers* x, ℓ, r *have numerators and denominators of bit-size at most* $O(p(\tau + \log_2 p))$.

Proof The complexity of the Preparatory Phase is $O(p^5(\tau + \log_2 p)^2)$ using classical arithmetic, and $\tilde{O}(p^4\tau^2)$ using fast algorithms (see [1], pp. 377–378).

For the case where P does not vanish on $[-1, 1]$, there are $O(p(\tau + \log_2 p))$ calls to the Special De Casteljau Algorithm in the Dichotomy Phase according to the complexity analysis of the Real Root Isolation Algorithm by [6] (see [1], p. 377), and Theorem 3. The bit-size of the Bernstein coefficients in each node is $O(p^2(\tau + \log_2 p))$ (see [1], pp. 377–378), since the elements of L are of the form $\ell'/2^k$ with ℓ' an integer of bit-size at most k and k is estimated by $O(p(\tau + \log_2 p))$. Moreover, there are $O(p^2)$ additions (resp. $\tilde{O}(p)$ arithmetic operations if fast algorithms are used) to perform at each node. The complexity of the Dichotomy Phase is $O(p^5(\tau + \log_2 p)^2)$ using classical arithmetic (resp. $\tilde{O}(p^4\tau^2)$ using fast algorithms) (see [1], pp. 377–378).

The correctness of the compression phase is clear since if ℓ_i and ℓ_j in L are such that there exists no root z of P with real part in $[\ell_{i-1}, \ell_j]$, CertPos$(b(P, p, \ell_{i-1}, \ell_j))$ holds by Theorem 3. There are at most $p + 1$ intervals output since there are at most $p/2$ elements of L if p is even (resp. $(p - 1)/2$ elements of L if p is odd) such that there exists a root z of P with real part in $[\ell_{i-1}, \ell_i]$, so the total number of coefficients in $b(cP, p, L)$ is $O(p^2)$. In the Compression Phase, there are $O(p(\tau + \log_2 p))$ calls to the Special Bernstein Coefficients Algorithm; the number of arithmetic operations in each call is $O(p^2)$ (resp. $\tilde{O}(p)$ if fast algorithms are used) and the bit-size of the integers are $O(p^2(\tau + \log_2 p))$. The complexity of the Compression Phase is $O(p^7(\tau + \log_2 p)^3)$ (resp. $\tilde{O}(p^4\tau^2)$ using fast algorithms).

Finally, the binary complexity of Algorithm 1 is $O(p^7(\tau + \log_2 p)^3)$ (resp. $\tilde{O}(p^4\tau^2)$ using fast algorithms).

Since the total number of coefficients in $b(cP, p, L)$ is $O(p^2)$, and the bit-size of the integers in $b(cP, p, L)$ is $O(p^2(\tau + \log_2 p))$, it follows that the bit-size of the certificate of positivity is at most $O(p^4(\tau + \log_2 p))$ when $P > 0$ on $[-1, 1]$.

The statement in the case P vanishes on $[-1, 1]$ is clear given the bit-size estimates of the subdivision. □

4 Comparison Between Global and Local Certificates of Positivity

In this section we compare in theory and in practice our local certificate with the global one obtained by Bernstein's theorem and prove that our result provides an improvement from exponential to polynomial size. We consider $P \in \mathbb{Z}[X]$ *of degree* p with coefficients of *bit-size bounded by* τ, and denote by ν *the bit-size of the degree* p.

If P is positive on $[-1,1]$, the smallest natural number d such that all the coefficients of $b(P,d,-1,1)$ are positive is called the *Bernstein degree* of P. Powers and Reznick proved in [13] a quantitative bound on the Bernstein degree, estimating it by

$$\frac{p(p-1)}{2}\frac{M}{\lambda}, \tag{3}$$

where p is the degree of P, λ is the minimum of $P(x)$ on $[-1,1]$ and M is the maximum value of the elements of $b(P,p,-1,1)$. Note that the estimate $\frac{p(p-1)}{2}\frac{M}{\lambda} - p$ given in [13] needs to be corrected as in (3) [14]. We shall see that such a bound is exponential in the degree p and the bit-size τ, and that the corresponding certificate of positivity can indeed be exponentially large in some special cases.

4.1 Estimates on the Minimum of a Polynomial as a Function of p and τ

We now estimate the minimum of $P \in \mathbb{Z}[X]$ positive on $[-1,1]$ in terms of the parameters p and τ and exhibit situations where this estimation is almost sharp.

We denote by ν the bit-size of p.

Theorem 6 *If $P \in \mathbb{Z}[X]$ is positive on $[-1,1]$, its minimum on $[-1,1]$ is at least $2^{-2p(1+\tau+\nu)+(\tau+1)}$.*

In order to estimate the minimum of $P(x)$, we consider the polynomial

$$(Y) = \prod_{z \in \mathrm{Zer}(P',C)} Y - P(z),$$

whose roots in $C = R[i]$ are the values of P at the elements of $\mathrm{Zer}(P', C)$, i.e., the roots of P' in C.

Using classical results on resultants (see [1], for example), we obtain

$$Q = \mathrm{Res}_X\left(P - Y, P'\right) = \det(S_Y) \in \mathbb{Z}[Y],$$

where

$$S_Y = \begin{bmatrix} a_p & \cdots & \cdots & \cdots & a_1 & a_0 - Y & 0 & \cdots & 0 \\ 0 & \ddots & & & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & a_p & \cdots & \cdots & \cdots & a_1 & a_0 - Y \\ pa_p & \cdots & \cdots & \cdots & a_1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & pa_p & \cdots & \cdots & \cdots & a_1 \end{bmatrix}.$$

We denote by S the classical Sylvester matrix of P and P', i.e.

$$S = \begin{bmatrix} a_p & \cdots & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ 0 & \ddots & & & & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & a_p & \cdots & \cdots & \cdots & a_1 & a_0 \\ pa_p & \cdots & \cdots & \cdots & a_1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & pa_p & \cdots & \cdots & \cdots & a_1 \end{bmatrix}.$$

The proof of Theorem 6 relies on two lemmas.

Lemma 1 *Let M be a square matrix of size $2p-1$ such that each of its $(p-1)$ first rows contains at most $p+1$ nonzero coefficients with absolute value estimated by 2^τ, and such that its p last rows contains at most p nonzero coefficients with absolute value estimated by $p2^\tau$. Then*

$$|\det(M)| \le 2^{(2p-1)\tau+(4p-1)\nu/2}.$$

Proof Using Hadamard's bound (see [1])

$$|\det(M)| \le \sqrt{\left((p+1)2^{2\tau}\right)^{p-1}\left(pp^2 2^{2\tau}\right)^p}.$$

Since $p < 2^\nu$, we get the claim. □

Lemma 2 *The coefficients of Q are estimated by $2^{p(2\tau+2\nu+1)-(\tau+\nu/2+1)}$.*

Proof It is clear that $Q = \det(S_Y)$ is a polynomial in Y of degree $p-1$. In order to compute the bit-size of the coefficients of Q, we consider an arbitrary

$$f : \{1, \ldots, p-1\} \to \{0, 1\}$$

and denote by S_f the matrix in which a_0 is replaced by -1 in the ith row of the Sylvester matrix S when $f(i) = 1$. Denoting by

$$n(f) = \#\{i \mid f(i) = 1\},$$

$$Q(Y) = \sum_{f\in\{1,\ldots,p-1\}\to\{0,1\}} Y^{n(f)} \det(S_f).$$

The coefficient of Y^i in Q is the sum of at most 2^{p-1} determinants S_f. Applying Lemma 1, we get that the coefficients of Q are bounded by

$$2^{p-1}2^{(2p-1)\tau+(4p-1)\nu/2} = 2^{p(2\tau+2\nu+1)-(\tau+\nu/2+1)}.$$ □

Proof of Theorem 6 The minimum of P on $[-1, 1]$ is obtained either at -1 or 1, or at a root of P' in $(-1, 1)$, and the corresponding minimum value of P is a nonzero root of Q.

The values of P at -1 and 1 are nonzero integers.

According to Cauchy's bound [1], the nonzero root with smallest absolute value λ of

$$Q = c_{p-1}X^{p-1} + \cdots + c_q X^q, \quad p-1 > q, c_{p-1}c_q \neq 0$$

is bigger than $(\sum_{q\leq i\leq p-1} |\frac{c_i}{c_q}|)^{-1}$. Using Lemma 2,

$$\lambda \geq \frac{1}{p2^{p(2\tau+2\nu+1)-(\tau+\nu/2+1)}} \geq 2^{-2p(\tau+\nu+1)+(\tau+1)}.$$

This concludes the proof. □

Remark 2 Our result is very slightly better than a recent result due to Bugeaud and Mignotte [4].

Example 3 The estimate of Theorem 6 is rather accurate. Following a suggestion by Bugeaud and Mignotte [4], we consider the family of polynomials

$$A(k, p) = X^{2p} + \left(2^k X - 1\right)^2.$$

For every k, p, the minimum of $A(k, p)$ is close to the estimation of Theorem 6. Indeed, $\tau = 2k$, and the minimum of $A(k, p)$ on $[-1, 1]$ is smaller than the value $2^{-p\tau}$ obtained at $x = 2^{-k}$, and depends exponentially on p and τ.

4.2 Comparison Between the Size of Local and Global Certificates of Positivity

Coming back to the bound of Powers and Reznick we have established that the Bernstein degree is estimated by

$$p(p-1)2^{p(2\tau+3\nu+3)+\nu+2}, \tag{4}$$

using the estimation on λ given by Theorem 6 and $L \leq 2^{p\nu+p+\tau+\nu}$ ([1], by Corollary 10.30, paying a special attention to the constants involved in the O). Note that the bound given by (4) is exponential in τ and p in contrast with the bound of Theorem 5 which is polynomial in τ and p.

Let us examine now examples where this exponential gap is really present.

4.2.1 Size of Certificates of Positivity with Respect to the Bit-Size

Powers and Reznick's bound (3) is sharp, as proved [13] where they provide a family of polynomials of degree 2 index by $k \in \mathbb{N}$, namely

$$P_k = \left(2^k - 1\right)X^2 + 1$$

for which the Bernstein degree is precisely $2^k - 1$. So, this proves the existence a family of polynomials for which the Bernstein certificate of positivity is exponential in $\tau = k$.

On the other hand, the local certificate of positivity given by Theorem 5 is particularly short because it is linear in $\tau = k$. More precisely our certificate of positivity for P_k is the following: $L = [-1, 0, 1]$, $b(P_k, 2, L) = [[2^k, 1, 1], [1, 1, 2^k]]$, which means

- $b(P_k, 2, -1, 0) = [2^k, 1, 1]$
- $b(P_k, 2, 0, 1) = [1, 1, 2^k]$

4.2.2 Size of Certificates of Positivity with Respect to the Degree

We prove now that the situation is similar with respect to the degree.

The family of polynomials

$$A(k, p) = X^{2p} + \left(2^k X - 1\right)^2$$

introduced earlier has a very small minimum and appears thus as a good test family for the comparison between the size of the certificate of positivity given by Theorem 5 and the certificate of positivity given by Bernstein's theorem. Numerical experiments performed using SARAG [5] do indicate that the difference between the sizes of the two certificates is huge even for small degrees.

For example, when $k = 1$:

- When $p = 1$, $A(1, 1) = 5X^2 - 4X + 1$ is the example already considered in the introduction, the Bernstein degree is 23.
- When $p = 2$, $A(1, 2) = X^4 + (2X - 1)^2$, its Bernstein degree is 82, the coefficients of $(1311795/2)A(1, 2)$ in the Bernstein basis of degree 82 for $-1, 1$ are

6558975, 6303015, 6054955, 5814558, 5581593, 5355835, 5137065, 4925070,

4719643, 4520583, 4327695, 4140790, 3959685, 3784203, 3614173, 3449430,

3289815, 3135175, 2985363, 2840238, 2699665, 2563515, 2431665, 2303998,

2180403, 2060775, 1945015, 1833030, 1724733, 1620043, 1518885, 1421190,

1326895, 1235943, 1148283, 1063870, 982665, 904635, 829753, 757998, 689355,

623815, 561375, 502038, 445813, 392715, 342765, 295990, 252423, 212103,

175075, 141390, 111105, 84283, 60993, 41310, 25315, 13095, 4743, 358, 45,

3915, 12085, 24678, 41823, 63655, 90315, 121950, 158713, 200763, 248265,

301390, 360315, 425223, 496303, 573750, 657765, 748555, 846333, 951318,

1063735, 1183815, 1311795

while our certificate of positivity is given by $L = [-1, 0, 1/2, 1]$, $C = [3, 48, 48]$ and

$$b(CA(1,2), 4, L) = [[30, 18, 11, 6, 3], [48, 24, 8, 0, 3], [3, 6, 20, 48, 96]].$$

We can in fact prove that the Bernstein degree of $A(1, p)$ is exponential in p.

Let us express $b(A(1, p), 2N, 0, 1)_N$, and prove that it is negative for any $N < 2^{2p-1} + p$.

Since $X^{2p} = X^{2p}(X + (1 - X))^{2N-2p}$,

$$\begin{aligned} b\big(X^{2p}, 2N, 0, 1\big)_N = & \frac{\binom{2N-2p}{N-2p}}{\binom{2N}{N}} = \frac{(2N-2p)!N!}{(N-2p)!(2N)!} \\ & = \frac{N(N-1)\cdots(N-2p+1)}{2N(2N-1)\cdots(2N-2p+1)}. \end{aligned}$$

Similarly since $(2X - 1)^2 = (X - (1 - X))^2(X + (1 - X))^{2N-2}$,

$$\begin{aligned} b\big((2X-1)^2, 2N, 0, 1\big)_N &= \frac{2\left(\binom{2N-2}{N-2} - \binom{2N-2}{N-1}\right)}{\binom{2N}{N}} \\ &= 2\frac{(2N-2)!N!}{(N-2)!(2N)!} - 2\frac{(2N-2)!N!^2}{(N-1)!^2(2N)!} \\ &= \frac{N-1}{2N-1} - \frac{N}{(2N-1)} \\ &= \frac{-1}{(2N-1)}. \end{aligned}$$

Let us prove that

$$\frac{N(N-1)\cdots(N-2p+1)}{2N(2N-1)\cdots(2N-2p+1)} - \frac{1}{(2N-1)} < 0,$$

or equivalently

$$(N-1)\cdots(N-2p+1) < 2(2N-2)\cdots(2N-2p+1) \tag{5}$$

when $N < p + 2^{2p-1}$.

Indeed, since $N - p - i < N - 1 - i$, for $i \in \mathbb{N}$,

$$(N-1)\cdots(N-2p+1) < (N-1)(N-2)^2\cdots(N-p)^2$$

and, since $2(N - i) < 2N - 2i + 1$, for $i \in \mathbb{N}$,

$$\begin{aligned} & 2^{2p}(N-1)(N-2)^2\cdots(N-p)^2 \\ & \quad = 2(2N-2)(2N-4)^2\cdots(2N-2p+2)^2(2N-2p)^2 \\ & \quad < 2(2N-2)(2N-3)\cdots(2N-2p+1)(2N-2p). \end{aligned}$$

So, if $2N - 2p < 2^{2p}$, or equivalently $N < 2^{2p-1} + p$, (5) holds.

Since, with $2N = 2^{2p} + 2p - 2$, $b(A(1, p), 2N, 0, 1)_N < 0$, it is clear that there is at least one negative coefficient in $b(A(1, p), N, -1, 1)$, by De Casteljau Algorithm and so the Bernstein degree of $A(1, p)$ is bigger than $2^{2p} + 2p - 1$.

5 Positivstellensatz Identity of Polynomial Size

We now explain how, when P of degree $\leq p$, p even, is positive on $[-1, 1]$, the local positivity certificate $b(cP, p, L)$ can be used to provide a positivstellensatz identity [2, 16] certifying that P is positive on $[-1, 1]$. We shall prove that the degree of this positivstellensatz identity is $O(p^2)$ when $P \in R[X]$, where R is a general real closed field, and the bit-size of the identity is $O(p^4(\tau + \log_2 p))$ when $P \in \mathbb{Z}[X]$.

It follows from Theorem 4 that if P is positive on $[-1, 1]$, there exists a subdivision $L = [-1 = \ell_0, \ell_1, \ldots, \ell_n = 1]$ of $[-1, 1]$ of length $n \leq p + 1$ such that $\mathrm{CertPos}(b(P, p, L))$ holds. We can suppose without loss of generality that all the elements of $b(P, p, \ell_{i-1}, \ell_i)$ are positive, doubling if necessary the number of intervals. Indeed, if $\mathrm{CertPos}(b(P, p, \ell, r))$ holds and $m = (\ell + r)/2$, it is easy to see that all the elements of $b(P, p, \ell, m)$ and $b(P, p, m, r)$ are positive. We can also suppose without loss of generality that n is odd, subdividing if necessary one of the intervals.

Denoting by a_i the minimum of the $b_{i,j} = b(P, p, \ell_{i-1}, \ell_i)_j$, $j = 0, \ldots, p$, the identity

$$P = \sum_{j=0}^{p} b_{i,j} \operatorname{Bern}_{p,j}(\ell_{i-1}, \ell_i) = a_i + \sum_{j=0}^{p} (b_{i,j} - a_i) \operatorname{Bern}_{p,j}(\ell_{i-1}, \ell_i)$$

can be rewritten as

$$\begin{aligned} &a_i + \sum_{j=0}^{p/2} (b_{i,2j} - a_i) \operatorname{Bern}_{p,2j}(\ell_{i-1}, \ell_i) - P \\ &\quad = -\sum_{j=1}^{p/2} (b_{i,2j-1} - a_i) \operatorname{Bern}_{p,2j-1}(\ell_{i-1}, \ell_i). \end{aligned} \tag{6}$$

Multiplying together these $n \leq 2p + 3$ identities, we obtain

$$a + T - SP = -U,$$

where

- $a + T = \sum_{\substack{I \subset \{1,\ldots n\} \\ \sharp(I) \text{ odd}}} \prod_{i \in I} (a_i + \sum_{j=0}^{p/2} (b_{i,2j} - a_i) \operatorname{Bern}_{p,2j}(\ell_{i-1}, \ell_i)) P^{n - \sharp(I)}$, with $a = \prod_{i=1}^{n} a_i$ is a positive number and T is sum of squares of degree at most np,
- $S = \sum_{\substack{I \subset \{1,\ldots n\} \\ \sharp(I) \text{ even}}} \prod_{i \in I} (a_i + \sum_{j=0}^{p/2} (b_{i,2j} - a_i) \operatorname{Bern}_{p,2j}(\ell_{i-1}, \ell_i)) P^{n - \sharp(I) - 1}$ is sum of squares of degree at most $(n - 1)p$,

→ $U = \prod_{i=1}^{n}(\sum_{j=1}^{p/2}(b_{i,2j-1} - a_i)\,\mathrm{Bern}_{p,2j-1}(\ell_{i-1}, \ell_i))$ is a sum of components of degree at most np of the form $Q^2(X+1)^j(1-X)^k$ with $j \le p$, $k \le p$, j and k odd, since n is odd and, for every $i = 1, \ldots, n-1$, and every j' and k' odd,

$$(X - \ell_i)^{j'}(\ell_i - X)^{k'} = -(X - \ell_i)^{j'+k'}$$

is the opposite of a square.

In other words

$$a - SP + T + U = 0. \tag{7}$$

This is a *positivstellensatz identity* [2, 16] certifying that $P(x) > 0$ on $[-1, 1]$. Indeed, if we suppose that there exists x such that $P(x) \le 0$, $-1 \le x \le 1$, evaluating (7) at x gives a contradiction

$$a + b = 0$$

with a positive and b non-negative elements of R.

So we have proved the following result.

Theorem 7 *If $P \in R[X]$ is > 0 on $[-1, 1]$, of degree $\le p$ where p is even, there exists a positivstellensatz identity*

$$a - SP + T + U = 0, \tag{8}$$

certifying the positivity of P on $[-1, 1]$, where a is a positive element of R, S and T are sum of squares in $R[X]$ of degree at most $p(2p+3)$, and U is the sum of finite number of components of degree at most $p(2p+3)$ of the form $Q^2(1-X)^j(X+1)^k$ with $j \le p$, $k \le p$, $Q \in R[X]$.

Theorem 8 *If $P \in \mathbb{Z}[X]$ is > 0 on $[-1, 1]$, of degree $\le p$ where p is even, there exists a positivstellensatz identity*

$$a - SP + T + U, \tag{9}$$

certifying the positivity of P on $[-1, 1]$, where a is a positive integer, S and T are sum of squares in $\mathbb{Z}[X]$ of degree at most $p(2p+3)$, and U is the sum of finite number of components of degree at most $p(2p+3)$ of the form $Q^2(1-X)^j(X+1)^k$ with $j \le p$, $k \le p$, $Q \in \mathbb{Z}[X]$. Moreover the total bit-size in (8) is at most $O(p^4(\tau + \log_2 p))$.

Proof The only change to perform to the construction of (8) is to replace (6) by

$$\begin{aligned} a_i - c_i P + \sum_{j=0}^{p/2}(b_{i,2j} - a_i)\,\mathrm{Bern}_{p,2j}(\ell_{i-1}, \ell_i) \\ = -\sum_{j=1}^{p/2}(b_{i,2j-1} - a_i)\,\mathrm{Bern}_{p,2j-1}(\ell_{i-1}, \ell_i), \end{aligned} \tag{10}$$

with $c_i \in \mathbb{N}$, $c_i \neq 0$. The result is an immediate consequence of the bit-size estimate $O(p^2(\tau + \log_2 p))$ on the elements of $b(cP, p, L)$ given in the proof of Theorem 5 and of the construction of (8). □

Remark 3 Note that this method does not give degree estimates for positivstellensatz identities in the field generated by the coefficients of P (even though such rational positivstellensatz do exist [2, 16]) since by Remark 1 it is really necessary to use subdivisions with endpoints in R in the construction.

6 Future Work and Open Problems

(a) In this paper we concentrated on certificates of positivity in the Bernstein basis. But there are other kind of certificates of positivity on an interval. For instance the following holds [8–10] (for a proof see [17], p. 4).

Theorem 9 *If a nonzero univariate polynomial $P \in R[X]$ of degree p is positive on $[-1, 1]$, then*

- *If $p = 2m$ there exist $A \in R[X]$ of degree m and $B \in R[X]$ of degree $m - 1$, with A and $(1 - X^2)B$ not vanishing simultaneously on $[-1, 1]$, such that*

$$P = A^2 + (X - 1)(1 + X)B^2. \tag{11}$$

- *If $p = 2m + 1$ there exist A and B in $R[X]$ of degree m, with $(1 - X)A$ and $(1 + X)B$ not vanishing simultaneously on $[-1, 1]$, such that*

$$P = (X - 1)A^2 + (1 + X)B^2. \tag{12}$$

Note that the Markov/Lukacs result provides a global certificate of positivity without increasing the degree, which is valid for a general real closed field. It would be quite interesting to study the size of the certificate of positivity provided by (11) and (12) and compare it to the size of our local certificates of positivity. In the case of integer coefficients, the coefficients of A and B can be chosen to be real algebraic numbers, and it should be possible to estimate the degree and bit-size of the polynomials in $\mathbb{Z}[X]$ defining these real algebraic numbers.

(b) Given the results obtained in the univariate case, it is natural to wonder whether there are efficient local certificates of positivity in the multivariate case as well. For global certificates of positivity, the situation is well understood: Pólya's theorem is valid in the multivariate case and the quantitative results of Powers and Reznick hold also in this case, and it is possible to extend the definition of Bernstein polynomials to a simplex and to prove a multivariate Bernstein's theorem in this case [13]. The existence of local certificates of positivity is rather easy [7], at least in the archimedean case, using approximation properties of Bernstein coefficients [15] instead of real root isolation. However, no good quantitative bound is known for these local certificates in the integer case, the main missing ingredient seems to be a generalized notion of sign variation having subadditivity properties with respect to subdivision (see [1], Proposition 10.41).

Acknowledgements Thanks to Michel Coste and Henri Lombardi for useful discussions and to Vikram Sharma and the anonymous referees for relevant remarks and advice on a previous version of the paper.

References

1. Basu, S., Pollack, R., Roy, M.-F.: Algorithms in Real Algebraic Geometry, 2nd edn. Springer, Berlin (2006). Revised version of the first edition online at http://perso.univ-rennes1.fr/marie-francoise.roy/
2. Bochnak, J., Coste, M., Roy, M.-F.: Real Algebraic Geometry, 2nd edn. Springer, Berlin (1998)
3. Bernstein, S.: Sur la représentation des polynômes positifs. Soobshch. Har'k. Mat. Obshch. **2**(14), 227–228 (1915). Collected Papers of S.N. Bernstein, vol. 1, Constructive Theory of Functions (1905–1930), pp. 251–252. Academy of Sciences, USSR (1952)
4. Bugeaud, Y., Mignotte, M.: Private communication (2005)
5. Caruso, F.: The SARAG library. In: Proceedings of the ICMS '06. Springer, Berlin (2006). Stable version included in maxima: http://maxima.sourceforge.net/, last version online at http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-posted1.html
6. Eigenwillig, A., Sharma, V., Yap, C.K.: Almost tight recursion tree bounds for the Descartes method. In: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, Italy, pp. 71–78. ACM, New York (2006)
7. Leroy, R.: Certificates of positivity in the multivariate Bernstein basis, in preparation
8. Lukacs, F.: Verschärfung des ersten Mittelwertsatzes der Integralrechnung fur rationale Polynome. Math. Z. **2**, 295–315 (1918)
9. Markov, A.A.: Lectures notes on functions with the least deviation from zero (1906). Reprinted in Achiezer, N. (ed.) Selected Papers, pp. 244–291. Gos TechIzdat (1948)
10. Nesterov, Y.: Squared functional systems and optimization problems. In: Frenk, H., Roos, K., Terlaky, T., Zhang, S. (eds.) High Performance Optimization, pp. 405–440. Kluwer Academic, Dordrecht (2000)
11. Polya, G.: Über positive Darstellung von Polynomen. Vierteljahrsschr. Nat. Forsch. Ges. Zür. **73**, 141–145 (1928). Collected Papers, vol. 2, pp. 309–313. MIT (1974)
12. Powers, V., Reznick, B.: Polynomials that are positive on an interval. Trans. Am. Math. Soc. **352**(10), 4677–4692 (2000)
13. Powers, V., Reznick, B.: A new bound for Polya's Theorem with applications to polynomials positive on polyhedra. J. Pure Appl. Algebra **164**, 221–229 (2001)
14. Powers, V., Reznick, B.: Private communication (2006)
15. Reif, U.: Sharp, quantitative bounds on the distance between a polynomial piece and its Bezier control polygon. Comput. Aided Geom. Des. **17**, 579–589 (2000)
16. Stengle, G.: A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. Math. Ann. **207**, 87–97 (1974)
17. Szegö, G.: Orthogonal Polynomials. AMS Colloquium Publications, vol. XXIII (1939)